Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών

Τμήμα Μαθηματικών

Μεταπτυχιακό Πρόγραμμα στη Λογική και Θεωρία Αλγορίθμων και Υπολογισμού

$\mu\Pi\lambda\forall$

Μη Διαλογικά Συστήματα Απόδειξης στην Κρυπτογραφία Ζευγμάτων και Εφαρμογές στις Ομαδικές Υπογραφές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θωμάς Ζαχαρίας

Επιβλέπων: **Άρης Παγουρτζής**, Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2012

Abstract

In this thesis, we initially provide a general introduction to pairing-based cryptography, consisting of the presentation of the established methods for constructing and computing a pairing and some of the most fundamental pairing-based schemes and protocols. We then focus on the analysis of the seminal Groth-Sahai system for the construction of efficient non-interactive NIWI and NIZK proofs. Finally, we examine the applications of the Groth-Sahai proof system to group signature schemes and especially their contribution to achieving the required security properties without random oracles.

Keywords: pairing, bilinear map, pairing-based cryptography, Groth-Sahai proof system, group signatures.

Περίληψη

Στην παρούσα διπλωματική εργασία, παρέχουμε αρχικά μία γενική εισαγωγή στην κρυπτογραφία ζευγμάτων, αποτελούμενη από την παρουσίαση των καθιερωμένων μεθόδων κατασκευής και υπολογισμού ζευγμάτων και μερικών εκ των θεμελιωδέστερων σχημάτων και πρωτοκόλλων που βασίζονται σε ζεύγματα. Στη συνέχεια, επικεντρωνόμαστε στην ανάλυση του επιδραστικού συστήματος Groth-Sahai για την κατασκευή αποδοτικών μη διαλογικών NIWI και NIZK αποδείξεων. Τελικώς, εξετάζουμε τις εφαρμογές του συστήματος απόδειξης Groth-Sahai σε σχήματα ομαδικών υπογραφών και ειδικότερα τη συμβολή τους στην επίτευξη των απαιτούμενων ιδιοτήτων ασφάλειας χωρίς τη χρήση τυχαίων μαντείων.

Λέξεις κλειδιά: pairing, διγραμμική απεικόνιση, pairing-based cryptography, Groth-Sahai proof system, group signatures.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους καθηγητές μου στο ΜΠΛΑ, οι οποίοι μου παρείχαν το γνωστικό υπόβαθρο και με εισήγαγαν στην ερευνητική μεθοδολογία για να ανταπεξέλθω στην παρούσα εργασία και συγκεκριμένα τα μέλη της τριμελούς εξεταστικής επιτροπής, κυρίους Ευστάθιο Ζάχο, Άγγελο Κιαγιά και Άρη Παγουρτζή, γιατί με τη διδασκαλία τους ήρθα σε γνωριμία με το αντικείμενο της κρυπτογραφίας. Ειδικότερα, ευχαριστώ τον κύριο Παγουρτζή, ο οποίος ως επιβλέπων καθηγητής μου με καθοδήγησε σημαντικά κατά τη διάρκεια συγγραφής της εργασίας. Θέλω τελικώς να εκφράσω τις ευχαριστίες μου στον κύριο Δημήτριο Θηλυκό για την επιρροή του στον επιστημονικό τρόπο σκέψης μου κατά τη διάρκεια των προπτυχιακών και μεταπτυχιακών μου σπουδών.

Πρόλογος

Η σύγχρονη κρυπτογραφία, κατά την εξέλιξή της, οικειοποιείται ως εργαλεία έννοιες από το χώρο των μαθηματικών και της υπολογιστικής πολυπλοκότητας. Τα *ζεύγματα* (pairings, bilinear maps), δηλαδή οι διγραμμικές, μη εκφυλιστικές και αποδοτικά υπολογίσιμες απεικονίσεις, εφαρμόστηκαν αρχικά σε μεθόδους κρυπτανάλυσης για συστήματα του προβλήματος του *διακριτού λογαρίθμου* [MOV93], [FR94] πάνω σε μία ειδική αλλά σπάνια, όπως μετέπειτα αποδείχτηκε [BK98], κατηγορία ελλειπτικών καμπυλών. Στις αρχές της περασμένης δεκαετίας, πρωτοπόροι ερευνητές εκμεταλλεύτηκαν τις ιδιαιτερότητες αυτών των καμπυλών για να κατασκευάσουν ζεύγματα που ορίζονται σε σύντομα αναπαραστάσιμες ομάδες και να τα χρησιμοποιήσουν σε καινούριες εφαρμογές, γεννώντας με αυτόν τον τρόπο τον κλάδο της *κρυπτογραφίας ζευγμάτων* (pairing-based cryptography). Οι καλές ιδιότητες των ζευγμάτων βοήθησαν στην επίλυση ανοιχτών προβλημάτων, όπως η *τριμερής ανταλλαγή κλειδιών σε ένα γύρο* [Jou00] και κυρίως η κατασκευή του πρώτου λειτουργικού και αποδεδειγμένα ασφαλούς *σχήματος κρυπτογράφησης βάσει ταυτοτήτων* (Identity-Based encryption Scheme) [BF01]. Η *κρυπτογραφία βάσει ταυτοτήτων* (Identity-Based Cryptography - IBC) είναι μία κατηγορία ασύμμετρης κρυπτογραφίας που εισήγαγε ο A.Shamir [Sha85] με υποδομή διαφορετική της κλασικής υποδομής PKI (Public Key Infrastucture): μία πλήρως έμπιστη *Γεννήτρια Ιδιωτικών Κλειδιών* (Private Key Generator - PKG) δημιουργεί τις παραμέτρους του συστήματος και κατέχει ένα μυστικό κλειδί μέσω του οποίου δημιουργεί τα ιδιωτικά κλειδιά των χρηστών. Παράλληλα, τα δημόσια κλειδιά προκύπτουν από την ταυτότητα των χρηστών ή κάποιο άλλο προσωπικό τους στοιχείο. Το πρωτόκολλο ανταλλαγής κλειδιού βάσει ταυτοτήτων του [SOK00] ήταν και η απαρχή της κρυπτογραφίας ζευγμάτων.

Μεγάλο πλήθος κατηγοριών σχημάτων υπογραφών με ενδιαφέροντα χαρακτηριστικά βασίζονται στα ζεύγματα. Μία από αυτές είναι και οι *ομαδικές υπογραφές* (group signatures), όπου τα μέλη μίας ομάδας μπορούν να υπογράφουν ανώνυμα εκ μέρους ή στα πλαίσια αυτής. Σε περίπτωση διαφωνίας, ένας *διαχειριστής ομάδας* (group manager) έχει την εξουσία να αποκαλύψει την ταυτότητα του υπογράφοντος. Οι πρώτες και δημοφιλέστερες ομαδικές υπογραφές από την κρυπτογραφία ζευγμάτων παρουσιάστηκαν στα [BBS04], [BS04], με μικρό μέγεθος υπογραφής και υψηλή ταχύτητα υπολογισμού.

Από την άλλη πλευρά, τα *μη διαλογικά συστήματα απόδειξης* (non-interactive proof systems - NIPS), όπου ο επαληθευτής πείθεται για την αλήθεια μίας πρότασης μαθαίνοντας τίποτα πέραν της απόδειξης που του δίνεται, ορίστηκαν αρχικά στο [BFM88] και έκτοτε καθιερώθηκαν στην κρυπτογραφία με σημαντικές εφαρμογές,

όπως την κατασκεύη σχήματος κρυπτογράφησης δημόσιου κλειδιού με CCA ασφάλεια. Τα πρώτα συστήματα κατασκευής μη διαλογικών αποδείξεων *μηδενικής γνώσης* (non-interactive zero knowledge - NIZK) με υποθέσεις από προβλήματα της κρυπτογραφίας ζευγμάτων ήταν των [GOS06a], [GOS06b]. Επειδή όμως οι τεχνικές τους είναι πολύπλοκες, η εφαρμογή τους οδηγεί σε σχετικά βαριά κρυπτογραφικά σχήματα στην πράξη, όπως τα σχήματα ομαδικών υπογραφών [BW06], [Gro06]. Σημείο αναφοράς για τη σύγχρονη έρευνα αποτελεί το αποδοτικό σύστημα μη διαλογικών αποδείξεων Groth-Sahai [GS08] για την επαληθευσιμότητα συνόλου εξισώσεων που περιέχουν ζεύγματα, και το οποίο εφαρμόζεται στην κατασκευή σχημάτων στο standard μοντέλο.

Η δομή της εργασίας έχει ως εξής:

- Στο Κεφάλαιο 1, παρέχεται το απαραίτητο θεωρητικό υπόβαθρο ώστε να γίνουν κατανοητοί ο ορισμός και ο τρόπος υπολογισμού των γνωστών μέχρι σήμερα ζευγμάτων. Το κεφάλαιο κλείνει με μία σύντομη αναφορά σε νεότερα σχετικά αποτελέσματα.

- Στο Κεφάλαιο 2, δίνεται ο γενικός ορισμός του ζεύγματος που χρησιμοποιείται στις εφαρμογές καθώς και ορισμένα σημαντικά προβλήματα των οποίων η δυσκολία υποτίθεται στα πλαίσια της κρυπτογραφίας ζευγμάτων. Παρουσιάζονται τα θεμελιώδη σχήματα των [SOK00], [Jou00], [BF01], [BLS01] και αναφέρονται οι κυριότερες επεκτάσεις τους. Από μετέπειτα σχήματα, μελετώνται οι υπογραφές του [BB04c] στο standard μοντέλο.

- Το Κεφάλαιο 3, αφιερώνεται σε μεγάλο βαθμό στην πλήρη παρουσίαση του συστήματος απόδειξης Groth-Sahai. Διατυπώνονται επίσης οι προαπαιτούμενες έννοιες για την κατανόησή του, ενώ στο τέλος παρατίθενται ορισμένες μετέπειτα βελτιώσεις στην επίδοσή του.

- Στην αρχή του Κεφαλαίου 4, περιγράφονται τα κυριότερα μοντέλα σύνταξης και ασφάλειας των ομαδικών υπογραφών. Στη συνέχεια, περιγράφονται οι ομαδικές υπογραφές [BBS04] και [BS04], με ασφάλεια στο *μοντέλο τυχαίου μαντείου* (random oracle model - ROM). Στο υπόλοιπο του κεφαλαίου μελετώνται τα σχήματα ομαδικών υπογραφών των [BW06], [Gro07], [LCSL07], [LV09], [LPY12a] στο standard μοντέλο. Η εργασία ολοκληρώνεται με κάποιες επιπλέον σχετικές αναφορές στη βιβλιογραφία μαζί με συμπεράσματα και ιδέες για την εδραίωση των ομαδικών υπογραφών στη σύγχρονη κρυπτογραφία.

Η εργασία χωρίζεται σε ένα γενικό και ένα ειδικό μέρος. Σκοπός των δύο πρώτων κεφαλαίων είναι να υπάρξει στην ελληνική βιβλιογραφία, ένα όσο το δυνατόν περιε-

κτικό και γενικό σημείο αναφοράς για τους μελετητές της κρυπτογραφίας ζευγμάτων. Στο ειδικό μέρος, που περιλαμβάνει τα δύο τελευταία κεφάλαια, επιχειρείται μία ενημερωμένη συλλογή των σημαντικότερων σχημάτων ομαδικών υπογραφών που στηρίζονται στο σύστημα απόδειξης Groth-Sahai.

Περιεχόμενα

Κεφάλαιο 1

Μέθοδοι Κατασκευής Ζευγμάτων

Οι καθιερωμένες μέθοδοι κατασκευής ζευγμάτων είναι οι αποδοτικοί υπολογισμοί των ζευγμάτων Tate και Weil, και των παραλλαγών τους, πάνω σε κατάλληλα επιλεγμένες ελλειπτικές καμπύλες. Για την κατανόησή τους, απαραίτητη είναι η γνώση θεωρίας διαιρετών, στοιχεία της οποίας παρατίθενται σε αυτό το κεφάλαιο. Για εκτενή μελέτη της θεωρίας των ελλειπτικών και γενικότερα των αλγεβρικών καμπυλών, ο αναγνώστης παραπέμπεται στα [Sil86], [Ste94]. Επιπλέον, γίνεται μία σύντομη παρουσίαση του ορισμού και του τρόπου υπολογισμού των ζευγμάτων Tate και Weil, ενώ αναλυτικότερη περιγραφή τους μπορεί να βρεθεί στο [BSS05 §IX]. Το κεφάλαιο ολοκληρώνεται με ζητήματα χρονικής πολυπλοκότητας, νεότερες προτάσεις μεθόδων κατασκευής καθώς και ορισμένα ανοιχτά ερωτήματα.

1.1 Ελλειπτικές Καμπύλες

Ο αυστηρός μαθηματικός ορισμός της ελλειπτικής καμπύλης προέρχεται από τη θεωρία αλγεβρικών καμπυλών. Σύμφωνα με αυτόν, *ελλειπτική καμπύλη* είναι μία προβολική αλγεβρική καμπύλη γένους 1, εφοδιασμένη με ένα ακριβώς επ' άπειρον σημείο, το $[0 : 1 : 0] \in \mathbb{P}^2$. Στην κρυπτογραφία χρησιμοποιείται συνήθως ο παρακάτω απλός εναλλακτικός ορισμός στο αφινικό επίπεδο.

Ορισμός 1.1.1. Έστω σώμα K και $\bar{K}$ η αλγεβρική του κλειστότητα και έστω η εξίσωση

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6, \tag{1.1}$$

όπου $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6 \in \bar{K}$. Μία *ελλειπτική καμπύλη* E είναι το σύνολο των ζευγών του αφινικού επιπέδου $A^2(\bar{K}) = \bar{K} \times \bar{K}$ που αποτελούν λύσεις της (1.1)

μαζί με ένα σημείο $\mathcal{O}$, που ονομάζεται *επ΄ άπειρον σημείο*.

Αν $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6 \in K$, τότε λέμε ότι η ελλειπτική καμπύλη *ορίζεται υπεράνω του* K και συμβολίζεται E/K. Συχνά το σημείο $\mathcal{O}$ αφήνεται να εννοηθεί, οπότε η καμπύλη χαρακτηρίζεται και ονοματίζεται από την αντίστοιχη εξίσωση. Ισοδύναμα, η καμπύλη E/K χαρακτηρίζεται από το πολυώνυμο

$$f(x,y) = y^2 + \alpha_1 xy + \alpha_2 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6 \in K[x,y]$$

μέσω της εξίσωσης

$$E : f(x,y) = 0.$$

Η γενική εξίσωση (1.1) καλείται *εξίσωση Weierstrass* και μπορεί να απλοποιηθεί ανάλογα με την χαρακτηριστική του σώματος K, $char(K)$, στις παρακάτω μορφές με κατάλληλη αλλαγή συντεταγμένων:

(i). $y^2 + \gamma y = x^3 + \alpha x + \beta$ ή $y^2 + xy = x^3 + \alpha x + \beta$, εάν $char(K) = 2$.

(ii). $y^2 = x^3 + \alpha x + \beta x + \gamma$, εάν $char(K) = 3$.

(iii). $y^2 = x^3 + \alpha x + \beta$, εάν $char(K) \neq 2, 3$.

Απαιτούμε η καμπύλη να είναι *μη ιδιάζουσα* (*non-singular, smooth*), δηλαδή οι μερικές παράγωγοι $\left(\frac{\partial f}{\partial x}\right)$ και $\left(\frac{\partial f}{\partial y}\right)$, ορισμένες από τη φυσική γενίκευση από το $\mathbb{R}[x,y]$ στον δακτύλιο πολυωνύμων τυχαίου σώματος $\mathbb{F}[x,y]$, δεν μηδενίζονται ταυτόχρονα σε κανένα σημείο της E. Αποδεικνύεται ότι εάν η ελλειπτική καμπύλη $E/K : f(x,y) = 0$ είναι μη ιδιάζουσα, τότε είναι *ανάγωγη* (*irreducible*), δηλαδή δε γράφεται ως ένωση δύο αλγεβρικών καμπυλών που είναι γνήσια υποσύνολά της [Kim07 Proposition 2]. Για λόγους απλότητας, η ανάλυση περιορίζεται στο εξής σε μη ιδιάζουσες ελλειπτικές καμπύλες με εξίσωση E: $y^2 = x^3 + \alpha x + \beta$.

Πρόταση 1.1.2. *Έστω E/K: $y^2 = x^3 + \alpha x + \beta$. Τα ακόλουθα είναι ισοδύναμα:*

(i). Η E είναι μη ιδάζουσα.

(ii). $4\alpha^3 + 27\beta^2 \neq 0$.

(iii). Το πολυώνυμο $x^3 + \alpha x + \beta$ δεν έχει πολλαπλές ρίζες.

Απόδειξη. $(i) \Leftrightarrow (ii)$. Έστω $P = (x_0, y_0)$ ιδιάζον σημείο της E. Έχουμε

$$\left(\frac{\partial f}{\partial x}\right)_P = \left(\frac{\partial f}{\partial y}\right)_P = 0 \Leftrightarrow -3x_0^2 - \alpha = 2y_0 = 0 \overset{char(K)\neq 2}{\Leftrightarrow} y_0 = 0,\ \alpha = -3x_0^2 \Leftrightarrow$$

$$\Leftrightarrow x_0^3 + \alpha x_0 + \beta = 0,\ \alpha = -3x_0^2 \Leftrightarrow 4\alpha^3 + 27\beta^2 = 0.$$

$(i) \Leftrightarrow (iii)$. Εάν x_0 είναι πολλαπλή ρίζα του $x^3 + \alpha x + \beta$, τότε $x_0^3 + \alpha x_0 + \beta = 0$ και $(x^3 + \alpha x + \beta)' \mid_{x_0} = 3x_0^2 + \alpha = 0$. Επομένως το $(x_0, 0)$ είναι ιδιάζον σημείο της καμπύλης, σύμφωνα με τις παραπάνω ισοδυναμίες.

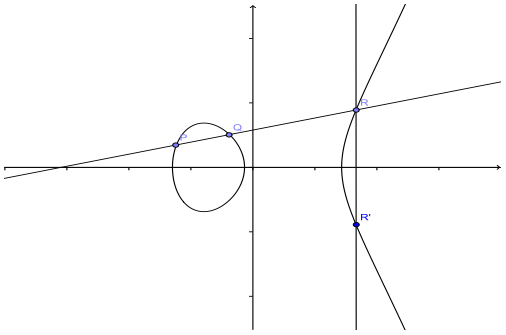
Εφαπτόμενες ευθείες και σημεία τομής. Σε κάθε σημείο $P = (x_0, y_0)$ μίας ελλειπτικής καμπύλης $E : f(x, y) = 0$, οι μερικές παράγωγοι $\left(\frac{\partial f}{\partial x}\right)_P$ και $\left(\frac{\partial f}{\partial y}\right)_P$ δεν μηδενίζονται ταυτόχρονα αφού η E είναι μη ιδιάζουσα. Συνεπώς, η εφαπτόμενη ευθεία της E στο P, T_P, ορίζεται μη τετριμμένα ως

$$T_P : \left(\frac{\partial f}{\partial x}\right)_P \cdot (x - x_0) + \left(\frac{\partial f}{\partial y}\right)_P \cdot (y - y_0) = 0. \tag{1.2}$$

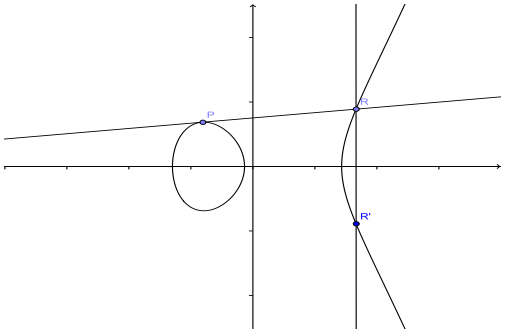
Έστω τώρα ευθεία $L : \alpha x + \beta y + \gamma = 0 \subset A^2(\bar{K})$. Η E είναι τρίτου βαθμού και το $\bar{K}$ είναι αλγεβρικά κλειστό, άρα η L τέμνει την E σε τρία, όχι κατ' ανάγκη διακεκριμένα, σημεία. Εξάλλου, όπως στο $\mathbb{R}^2$, έτσι και σε κάθε αφινικό επίπεδο δύο διακεκριμένα σημεία ορίζουν ακριβώς μια ευθεία. Τα παραπάνω καθιστούν δυνατό τον ορισμό *αθροίσματος* δύο σημείων μιας ελλειπτικής καμπύλης.

Ορισμός 1.1.3. (*Κανόνας χορδής εφαπτομένης*). Έστω ελλειπτική καμπύλη E και $P, Q \in E$ και R το τρίτο σημείο τομής της ευθείας $\overline{PQ}$ (εφαπτόμενη στην E αν $P = Q$). Τότε ως $P + Q$ ορίζεται το τρίτο σημείο τομής της ευθείας $\overline{\mathcal{O}R}$.

Γεωμετρική εποπτεία του κανόνα αθροίσματος 1.1.3 σε καμπύλη υπεράνω του $\mathbb{R}$ φαίνεται στα παρακάτω διαγράμματα για τις περιπτώσεις $P \neq Q$ και $P = Q$. Εδώ ως $P + Q$ θεωρείται το σημείο R'.



1. $P \neq Q$.



2. $P = Q$.

Θεώρημα 1.1.4. *Μια ελλειπτική καμπύλη E εφοδιασμένη με πράξη τον κανόνα χορδής - εφαπτομένης συνιστά Αβελιανή ομάδα.*

Απόδειξη. (i). (*Ύπαρξη ουδέτερου στοιχείου*). Αν $P = \mathcal{O}$, τότε $\overline{PQ} = \overline{\mathcal{O}Q}$, επομένως το R είναι το τρίτο σημείο τομής της $\overline{\mathcal{O}Q}$ και άρα το Q είναι το τρίτο σημείο τομής της $\overline{\mathcal{O}R}$. Προκύπτει ότι

$$P + Q = \mathcal{O} + Q = Q.$$

Ομοίως αν $Q = \mathcal{O}$ παίρνουμε

$$P + Q = P + \mathcal{O} = P.$$

(ii). (*Ύπαρξη αντίθετου στοιχείου*). Είναι προφανές από τον ορισμό του κανόνα ότι τα $P + Q, R, \mathcal{O}$ είναι τα τρία σημεία τομής της ευθείας $\overline{\mathcal{O}R}$ με την E. Ως εκ τούτου, ισχύει ότι

$$(P + Q) + R = \mathcal{O}. \tag{1.3}$$

Η (1.3) για $Q = \mathcal{O}$ γίνεται $(P + \mathcal{O}) + R = \mathcal{O} \Rightarrow R = -P$, δηλαδή το αντίθετο στοιχείο ενός τυχαίου σημείου P είναι το τρίτο σημείο τομής της ευθείας $\overline{\mathcal{O}P}$ με την E.

(iii). (*Προσεταιριστικότητα*). Η απόδειξη είναι μακροσκελής λόγω περιπτωσεολογίας και ο αναγνώστης μπορεί να ανατρέξει στο [Sil86 III.2.2.(e)].

(iv). (*Μεταθετικότητα*). Από το γεγονός ότι οι ευθείες $\overline{PQ}$, $\overline{QP}$ ταυτίζονται.

$\dashv$

Όπως σε κάθε προσθετική ομάδα, ορίζουμε το *m-οστό πολλαπλάσιο* ενός σημείου P με $m \in \mathbb{Z}$ ως

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ φορές}}, \ m > 0$$
$$[0]P = \mathcal{O}$$
$$[-m]P = [m](-P), \ m < 0.$$

Πρόταση 1.1.5. *(Αλγεβρική έκφραση του κανόνα χορδής - εφαπτομένης). Έστω καμπύλη E: $y^2 = x^3 + \alpha x + \beta$ και σημεία $P = (x_P, y_P), Q = (x_Q, y_Q) \in E \backslash \{\mathcal{O}\}$. Τότε προκύπτει ότι το σημείο $R = P + Q$ δίνεται από τους παρακάτω τύπους:*

(i). Εάν $x_P = x_Q$ τότε είτε

(a). $R = \mathcal{O}$ είτε

(b). $x_R = \lambda^2 - x_P - x_Q, \quad y_R = -\lambda x_R - \nu,$
όπου $\lambda = \dfrac{3x_P^2 + \alpha}{2y_P}$ *και* $\nu = \dfrac{-x_P^3 + \alpha x_P + 2\beta}{2y_P}$.

(ii). Εάν $x_P \neq x_Q$ τότε $x_R = \lambda^2 - x_P - x_Q, \quad y_R = -\lambda x_R - \nu,$
όπου $\lambda = \dfrac{y_Q - y_P}{x_Q - x_P}$ *και* $\nu = \dfrac{x_Q y_P - x_P y_Q}{x_Q - x_P}$.

Απόδειξη. (i). $x_P = x_Q \Rightarrow y_P^2 = y_Q^2 \Rightarrow y_P = \pm y_Q$.

(*a*). $y_P = -y_Q$, επομένως το Q είναι το συμμετρικό ως προς άξονα $0x$ σημείο του P, δηλαδή το τρίτο σημείο τομής της ευθείας $\overline{\mathcal{O}P}$ με την E. Από το Θεώρημα 1.1.4 έχουμε ότι $Q = -P \Leftrightarrow R = \mathcal{O}$.

(*b*). $y_P = y_Q \Rightarrow P = Q$. Η εφαπτόμενη ευθεία T_P έχει εξίσωση $\lambda x + \nu = y$ όπου

$$\lambda = \frac{3x_P^2 + \alpha}{2y_P} \quad \text{και} \quad \nu = \frac{-x_P^3 + \alpha x_P + 2\beta}{2y_P}.$$

Από τον Ορισμό 1.1.3 προκύπτει ότι το R είναι το συμμετρικό ως προς άξονα $0x$ του σημείου τομής της T_P με την E. Οι συντεταγμένες (x_R, y_R) υπολογίζονται

$$x_R = \lambda^2 + x_P - x_Q$$

$$y_R = -\lambda x_R - \nu.$$

(ii). $x_P \neq x_Q$. Όπως και στην περίπτωση $(ii).(b)$ μόνο που αντί της T_P θεωρούμε την ευθεία $\overline{PQ}$: $\lambda x + \nu = y$, όπου

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \text{ και } \nu = \frac{x_Q y_P - x_P y_Q}{x_Q - x_P}.$$

⊣

Αντίστοιχοι τύποι υπάρχουν και για τη γενική περίπτωση που η E ορίζεται από την εξίσωση (1.1) (βλ. [Sil86 III.2.3]).

Πόρισμα 1.1.6. *Έστω ελλειπτική καμπύλη E. Το σύνολο*

$$E(K) = (E \cap K^2) \cup \{\mathcal{O}\}$$

είναι υποομάδα της E.

Απόδειξη. Αφού το K είναι σώμα, οι υπολογισμοί στους τύπους της Πρότασης 1.1.5 εκτελούνται εντός του K.

⊣

Ελλειπτικές καμπύλες υπεράνω πεπερασμένων σωμάτων. Στην κρυπτογραφία, οι ελλειπτικές καμπύλες ορίζονται υπεράνω πεπερασμένων σωμάτων $\mathbb{F}_q$ πλήθους $q = p^r$, όπου p είναι η χαρακτηριστική του σώματος. Όπως προαναφέρθηκε, θα περιοριστούμε στην περίπτωση όπου $p \neq 2, 3$. Η αλγεβρική κλειστότητα ενός πεπερασμένου σώματος είναι το σώμα $\bar{\mathbb{F}} = \bigcup_{i \geqslant 1} \mathbb{F}_{q^i}$, το οποίο δεν είναι πεπερασμένο. Εντούτοις, σύμφωνα με το Πόρισμα 1.1.6, το σύνολο $E(\mathbb{F}_q)$ αποτελεί πεπερασμένη ομάδα. Η τάξη της $E(\mathbb{F}_q)$ δεν μπορεί μπορεί να είναι μεγαλύτερη από $2q + 1$, συνυπολογίζοντας και το $\mathcal{O}$, αφού για κάθε $x \in \mathbb{F}_q$ το πολύ δύο ζεύγη του εφινικού επιπέδου μπορούν να είναι λύσεις της $y^2 = x^3 + \alpha x + \beta = 0$. Ένα αυστηρότερο φράγμα δίνεται από το επόμενο σημαντικό θεώρημα.

Θεώρημα 1.1.7. *(Θεώρημα Hasse).*

$$| \#E(\mathbb{F}_q) - q - 1 | \leqslant 2\sqrt{q} \quad .$$

Απόδειξη. [Sil86 V.1.1]. ⊣

Ορισμός 1.1.8. Έστω $t = q + 1 - \#E(\mathbb{F}_q)$. Η ελλειπτική καμπύλη E καλείται *υπεριδιάζουσα* (*supersingular*), εάν $p \mid t$. Διαφορετικά, η E καλείται *συνήθης* (*ordinary*).

Η ποσότητα t ονομάζεται *ίχνος* (*trace*) της E και από το Θεώρημα 1.1.7 έχουμε ότι $\mid t \mid \leqslant 2\sqrt{q}$. Οι υπεριδιάζουσες καμπύλες είναι μία ιδιαίτερης σημασίας κατηγορία ελλειπτικών καμπυλών, τόσο για την ελλειπτική κρυπτογραφία όσο και για την κρυπτογραφία ζεύγματος, όπως θα δούμε σε επόμενα κεφάλαια.

Μπορούμε τώρα να δώσουμε ένα υπολογιστικό παράδειγμα όσων αναφέρθηκαν σε αυτήν την ενότητα, σημειώνοντας ότι για καμπύλες $E/\mathbb{F}_q$ ο κανόνας αθροίσματος στερείται γεωμετρικής ερμηνείας και αποδίδεται μόνο αλγεβρικά από τους τύπους της Πρότασης 1.1.5.

Παράδειγμα 1.1.9. Έστω ελλειπτική καμπύλη $E/\mathbb{F}_{23}$: $y^2 = x^3 + x$. Η ομάδα $E(\mathbb{F}_{23})$ συνίσταται από τα παρακάτω 24 σημεία:

$\mathcal{O}$	(0,0)	(1,5)	(1,18)
(9,5)	(9,18)	(11,10)	(11,13)
(13,5)	(13,18)	(15,3)	(15,20)
(16,8)	(16,15)	(17,10)	(17,13)
(18,10)	(18,13)	(19,1)	(19,22)
(20,4)	(20,19)	(21,6)	(21,17)

Πίνακας 1.1. Η ομάδα $E(\mathbb{F}_{23})$.

Έστω $P = (1, 5)$, $Q = (9, 18)$. Τότε από τους τύπους της Πρότασης 1.1.4

$$\lambda = (18 - 5)/(9 - 1) = 13/8 = 13 \cdot 3 = 16$$
$$\nu = (9 \cdot 5 - 1 \cdot 18)/(9 - 1) = 27/8 = 27 \cdot 3 = 12$$

επομένως το σημείο $R = P + Q = (x_R, y_R)$ υπολογίζεται

$$x_R = \lambda^2 + x_P - x_Q = 16^2 - 1 - 9 = 3 - 10 = -7 = 16$$
$$y_R = -\lambda x_R - \nu = -16 \cdot 16 - 12 = -268 = -15 = 8$$

δηλαδή $R = (16, 8) \in E(\mathbb{F}_{23})$.

Το ίχνος της E είναι $t = \#E(\mathbb{F}_q) - q - 1 = 24 - 23 - 1 = 0$ και φυσικά $23 \mid 0$, δηλαδή η E είναι υπεριδιάζουσα.

1.2 Ρητές Συναρτήσεις και Διαιρέτες

Έστω E/K: $f(x, y) = 0$ και $\langle f(x, y)\rangle = \{g(x, y) \cdot f(x, y) \mid g(x, y) \in K[x, y]\}$ το κύριο ιδεώδες του δακτυλίου $K[x, y]$ που παράγεται από το $f(x, y)$. Ως *δακτύλιο συντεταγμένων* (*coordinate ring*) $K[E]$ της E ορίζουμε τον δακτύλιο πηλίκο $K[x, y]/\langle f(x, y)\rangle$. Η E είναι ανάγωγη, το οποίο ισοδυναμεί με ότι a) το $\langle f(x, y)\rangle$

είναι πρώτο ιδεώδες και *b*) ο $K[E]$ είναι ακέραια περιοχή [Kun05 Corollary 1.12]. Ορίζεται λοιπόν ως συνήθως το *σώμα πηλίκο* του $K[E]$, το οποίο συμβολίζεται $K(E)$. Εντελώς παρόμοια ορίζονται ο $\bar{K}[E]$ και το $\bar{K}(E)$.

Ορισμός 1.2.1. Το σώμα πηλίκο $\bar{K}(E)$ καλείται το *σώμα συναρτήσεων* (*function field*) της E. Τα στοιχεία του $\bar{K}(E)$ ονομάζονται *ρητές συναρτήσεις* (*rational functions*).

Εξ ορισμού, δύο ρητές συναρτήσεις g_1/h_1, g_1/h_2 ταυτίζονται ανν $g_1h_2 = g_2h_1$. Μία ρητή συνάρτηση είναι διαίρεση κλάσεων ισοδυναμίας

$$\frac{g(x,y) + \langle f(x,y)\rangle}{h(x,y) + \langle f(x,y)\rangle},$$

επειδή όμως στα σημεία της καμπύλης E η $f(x,y)$ εξ ορισμού μηδενίζεται, κάθε κλάση $r(x,y) + \langle f(x,y)\rangle \in \bar{K}[E]$ ορίζει καλώς, μέσω του αντιπροσώπου της $r(x,y)$, μία πολυωνυμική συνάρτηση $E \longrightarrow \bar{K}$. Μπορούμε επομένως να γράφουμε τα στοιχεία του δακτυλίου πολυωνύμων ως πολυωνυμικές συναρτήσεις και τις ρητές συναρτήσεις ως πηλίκα πολυωνύμων.

Μία μη μηδενική ρητή συνάρτηση r *ορίζεται* στο σημείο $P \neq \mathcal{O}$, αν μπορεί να γραφεί ως $r = g/h$, $g, h \in \bar{K}[E]$ με $h(P) \neq 0$. Αν η f δεν ορίζεται στο P, γράφουμε $f(P) = \infty$. Ο ορισμός της r στο $\mathcal{O}$ απαιτεί γνώσεις θεωρίας αλγεβρικών καμπυλών που ξεφεύγουν από τους σκοπούς της παρούσας εργασίας. Από καθαρά υπολογιστική σκοπιά, έχουμε ότι για κάθε $k \in \bar{K}[E]$ η εξίσωση της καμπύλης E επιτρέπει αντικαθιστώντας τους όρους $y^{2n}, n \in \mathbb{N}$ με την παράσταση $(x^3+\alpha x+\beta)^n$, να γραφεί το k σε *κανονική μορφή* ως

$$k(x,y) = S(x) + yT(x) \in \bar{K}[E].$$

Στη συνέχεια ορίζεται ως *βαθμός* του a η ποσότητα

$$deg(k) = max\{2 \cdot deg_x(S), 3 + 2 \cdot deg_x(T)\}. \tag{1.4}$$

όπου $deg_x(S), deg_x(T)$ οι βαθμοί των πολυωνύμων $S(x), T(x)$. Βάσει του βαθμού ενός στοιχείου του δακτυλίου συντεταγμένων ορίζουμε για την $r = g/h$

$$r(\mathcal{O}) = \begin{cases} 0, & deg(g) < deg(h) \\ \dfrac{\alpha_g}{\alpha_h}, & deg(g) = deg(h) \\ \infty, & deg(g) > deg(h) \end{cases} \tag{1.5}$$

όπου α_g, α_h οι συντελεστές κύριων όρων των g, h σε κανονική μορφή.

Παράδειγμα 1.2.2. Θεωρούμε την καμπύλη $E/\mathbb{F}_7$: $y^2 = x^3 + x + 1$ και τη ρητή συνάρτηση

$r = g/h = \dfrac{x^5 + 2x^2y + y^2 + 1}{2x^4 + 3y^3 + 5}$. Αντικαθιστώντας τον όρο y^2 με $x^3 + x + 1$ έχουμε

$$r = \frac{x^5 + 2x^2y + (x^3 + x + 1) + 1}{2x^4 + 3(x^3 + x + 1)y + 5} = \frac{(x^5 + x^3 + x + 2) + y(2x^2)}{(2x^4 + 5) + y(3x^3 + 3x + 3)}$$

Άρα $deg(g) = max\{2 \cdot 5, 3 + 2 \cdot 2\} = 10$ και $deg(h) = max\{2 \cdot 4, 3 + 2 \cdot 3\} = 9$ και τελικά από (1.5) παίρνουμε $r(\mathcal{O}) = \infty$.

Πρόταση 1.2.3. *Έστω $f, g \in \bar{K}[E]$. Ισχύει ότι*

$$deg(f \cdot g) = deg(f) + deg(g).$$

Απόδειξη. Έστω $f(x, y) = S_f(x) + yT_f(x)$ και $g(x, y) = S_g(x) + yT_g(x)$. Τότε

$$f \cdot g = (S_f(x) + yT_f(x)) \cdot (S_g(x) + yT_g(x)) = S_{f\cdot g}(x) + yT_{f\cdot g}(x)$$

όπου αντικαθιστώντας τον όρο y^2 με $x^3 + \alpha x + \beta$ έχουμε

$$\begin{gathered} S_{f\cdot g}(x) = S_f(x)S_g(x) + (x^3 + \alpha x + \beta)T_f(x)T_g(x) \text{ και} \\ T_{f\cdot g}(x) = T_f(x)S_g(x) + T_g(x)S_f(x). \end{gathered}$$

Η (1.5) δίνει

$$deg(f \cdot g) = max\{2 \cdot deg(S_{f\cdot g}), 3 + 2 \cdot deg(T_{f\cdot g})\}$$

Όμως

$$\begin{aligned} deg(S_{f\cdot g}) &= max\{deg(S_f) + deg(S_g), 3 + deg(T_f) + deg(T_g)\} \\ deg(T_{f\cdot g}) &= max\{deg(T_f) + deg(S_g), deg(T_g) + deg(S_f)\} \end{aligned} \tag{1.6}$$

Διακρίνουμε τις εξής περιπτώσεις:

(i). $deg(f) = 2 \cdot deg(S_f)$ και $deg(g) = 2 \cdot deg(S_g)$. Συνεπώς

$$\left.\begin{aligned} 2 \cdot deg(S_f) &\geqslant 3 + 2 \cdot deg(T_f) \\ 2 \cdot deg(S_g) &\geqslant 3 + 2 \cdot deg(T_g) \end{aligned}\right\} \Rightarrow$$

$$\left.\begin{aligned} 2 \cdot (deg(S_f) + deg(S_g)) &\geqslant 2 \cdot (3 + deg(T_f) + deg(T_g)) \\ deg(S_f) &\geqslant deg(T_f) \\ deg(S_g) &\geqslant deg(T_g) \end{aligned}\right\} \Rightarrow$$

$$\left.\begin{aligned} deg(S_f) + deg(S_g) &\geqslant 3 + deg(T_f) + deg(T_g) \\ 2 \cdot (deg(S_f) + deg(S_g)) &\geqslant (3 + 2 \cdot deg(T_f)) + 2 \cdot deg(S_g) \\ 2 \cdot (deg(S_f) + deg(S_g)) &\geqslant (3 + 2 \cdot deg(S_f)) + 2 \cdot deg(T_g) \end{aligned}\right\} \overset{(1.6)}{\Rightarrow}$$

$$\left.\begin{array}{c} deg(S_{f\cdot g}) = deg(S_f) + deg(S_g) \\ 2\cdot deg(S_f) + deg(S_g) \geqslant 3 + 2\cdot deg(T_{f\cdot g})\} \end{array}\right\} \Rightarrow$$

$$2\cdot deg(S_{f\cdot g}) \geqslant 3 + 2\cdot deg(T_{f\cdot g}) \Rightarrow$$

$$deg(f\cdot g) = 2\cdot deg(S_{f\cdot g}) = 2\cdot deg(S_f) + 2\cdot deg(S_g)) = deg(f) + deg(g).$$

Ανάλογα εργαζόμαστε για τις υπόλοιπες περιπτώσεις:

(ii). $deg(f) = 2\cdot deg(S_f)$ και $deg(g) = 3 + 2\cdot deg(T_g)$.

(iii). $deg(f) = 3 + 2\cdot deg(T_f)$ και $deg(g) = 2\cdot deg(S_g)$.

(iv). $deg(f) = 3 + 2\cdot deg(T_f)$ και $deg(g) = 3 + 2\cdot deg(T_g)$.

⊣

Ορισμός 1.2.4. Ένα σημείο P της E ονομάζεται *ρίζα* αν $f(P) = 0$ και *πόλος* αν $f(P) = \infty$.

Ορισμός 1.2.5. Έστω $P \in E$. Μια ρητή συνάρτηση u είναι *παράμετρος ομοιομορφίας* (*uniformizing parameter, uniformizer*) για το σημείο P αν έχει τις εξής ιδιότητες:

(i). $u(P) = 0$.

(ii). $(\forall f \in \bar{K}(E)\backslash\{0\})(\exists d \in \mathbb{Z}, s \in \bar{K}(E)) : (s(P) \neq 0, \infty) \wedge (f = u^d \cdot s)$.

Για συναρτήσεις $f \in \bar{K}(E)\backslash\{0\}$ με $f(P) \neq 0, \infty$, τετριμμένα γράφουμε $f = u^0 \cdot f$. Το θεώρημα που ακολουθεί, εξασφαλίζει την ύπαρξη παραμέτρου ομοιομορφίας για κάθε σημείο μια ελλειπτικής καμπύλης.

Θεώρημα 1.2.6. *Έστω $P \in E$ και ευθεία L: $\lambda x + \mu y + \nu = 0$ που διέρχεται από το P και δεν εφάπτεται στην E. Τότε η L είναι παράμετρος ομοιομορφίας για το σημείο P.*

Απόδειξη. [Men93 2.22]. ⊣

Πόρισμα 1.2.7. *Μία παράμετρος ομοιομορφίας για σημείο $P \in E$: $x^3 + \alpha x + \beta$ είναι η συνάρτηση*

(i). $u(x, y) = x - x_P$, εάν $P = (x_P, y_P) \neq \mathcal{O}$ και η τάξη του P δεν είναι 2.

(ii). $u(x, y) = y$, εάν η τάξη του P είναι 2.

(iii). $u(x,y) = \dfrac{x}{y}$, *εάν* $P = \mathcal{O}$.

Απόδειξη. Θα δείξουμε πρώτα ότι

$$rank(P) = 2 \Leftrightarrow [2]P = P + P = 0 \Leftrightarrow P = -P \overset{1.1.5}{\Leftrightarrow} y_P = -y_P \Leftrightarrow y_P = 0. \quad (1.7)$$

(i). Άμεσα έχουμε $u(P) = x_P - x_P = 0$. Από την (1.2), η εφαπτόμενη ευθεία T_P έχει εξίσωση

$$-(3x_P^2 + \alpha x_P) \cdot (x - x_P) + 2y_P(y - y_P) = 0$$

και είναι διάφορη της $x - x_P = 0$ αφού $(1.7) \Rightarrow y_P \neq 0$. Λόγω του Θεωρήματος 1.2.6, η $u(x,y) = x - x_P$ είναι παράμετρος ομοιομορφίας για το σημείο P.

(ii). $(1.7) \Rightarrow y_P = 0$, άρα $u(P) = y_P = 0$. Επιπλέον

$$T_P : x - x_P = 0$$

που είναι διάφορη της $u(x,y) = y$, επομένως λόγω του Θεωρήματος 1.2.6, η $u(x,y) = y$ είναι παράμετρος ομοιομορφίας για το σημείο P.

(iii). Το ότι $u(\mathcal{O}) = 0$ προκύπτει από τις (1.4), (1.5) και από το γεγονός πως $deg(x) = 2$, $deg(y) = 3$. Έστω τώρα $f = g/h \in \bar{K}(E)\backslash\{0\}$ με $f(P) \in \{0, \infty\}$ (μη τετριμμένη περίπτωση). Από (1.4) έχουμε $d = deg(f) - deg(g) \neq 0$. Εφαρμόζοντας την Πρόταση 1.2.3 προκύπτει

$$\begin{aligned} deg(y^d f) - deg(x^d g) &= (deg(y^d) + deg(f)) - (deg(x^d) + deg(g)) \\ &= 3d + deg(f) - 2d - deg(g) \\ &= d - deg(f) - deg(g) \neq 0 \end{aligned}$$

και άρα $[(\dfrac{y}{x})^d f(x,y)](\mathcal{O}) \neq 0$. Γράφουμε την f ως

$$f = (\frac{x}{y})^d \cdot [(\frac{y}{x})^d f(x,y)].$$

Η $u(x,y) = \dfrac{x}{y}$ είναι λοιπόν παράμετρος ομοιομορφίας.

$\dashv$

Ορισμός 1.2.8. Έστω $P \in E$ και u παράμετρος ομοιομορφίας για το σημείο P. Ορίζουμε *τάξη* μίας συνάρτησης $f = g/h \in \bar{K}(E)\backslash\{0\}$ και γράφουμε $ord_P(f)$ τον αριθμό $d \in \mathbb{Z}$ ώστε

$$f = u^d \cdot s,$$

όπου $s \in \bar{K}(E) : s(P) \notin \{0, \infty\}$. Αν το P είναι ρίζα της f, τότε λέμε ότι το P έχει *πολυπλοκότητα* $ord_P(f)$, ενώ αν το P είναι πόλος της f, τότε λέμε ότι το P έχει πολυπλοκότητα $-ord_P(f)$.

Η επόμενη πρόταση αποδεικνύει ότι ο παραπάνω ορισμός είναι καλός.

Πρόταση 1.2.9. *(Μοναδικότητα του αριθμού d). Έστω u, v παράμετροι ομοιομορφίας για το σημείο $P \in E$ και $f \in \bar{K}(E)\backslash\{0\}$.*
Αν $f = u^d \cdot s$ και $f = v^{d'} \cdot t$ με $s, t \in \bar{K}(E) : s(P), t(P) \notin \{0, \infty\}$, τότε $d = d'$.

Απόδειξη. Αφού οι u, v είναι παράμετροι ομοιομορφίας υπάρχουν $\alpha, \beta \in \mathbb{Z}$ και ρητές συναρτήσεις $q, r \in \bar{K}(E)$: $q(P), r(P) \notin \{0, \infty\}$ ώστε

$$\begin{aligned} u &= v^{\alpha} \cdot q \\ v &= u^{\beta} \cdot r\ . \end{aligned} \tag{1.8}$$

Οι εξισώσεις (1.8) δίνουν

$$u = u^{\alpha\beta} \cdot qp^{\alpha}.$$

Είναι προφανές ότι μία παράμετρος ομοιομορφίας δεν μπορεί να είναι μηδενική συνάρτηση, άρα υπάρχει ρητή συνάρτηση u^{-1}. Επομένως ισχύει ότι

$$u^{\alpha\beta-1} \cdot qp^{\alpha} = 1 \Rightarrow \alpha\beta = 1$$

διότι διαφορετικά θα είχαμε $[u^{\alpha\beta-1} \cdot qp^{\alpha}](P) \in \{0, \infty\}$. Αν $\alpha = \beta = -1$ έχουμε

$$u = v^{-1}q \Leftrightarrow uv = q \Rightarrow q(P) = u(P)v(P) = 0$$

που είναι άτοπο από την επιλογή της q. Υποχρεωτικά λοιπόν $\alpha = \beta = 1$ και άρα

$$f = u^d \cdot s = v^{d'} \cdot t = (uq)^{d'} \cdot t = u^{d'}(q^{d'} \cdot t) \Rightarrow u^{d-d'} = q^{d'} \cdot ts^{-1}.$$

Από την επιλογή των q, s, t ισχύει $q^{d'} \cdot ts^{-1} \neq 0$. Συμπεραίνουμε ότι

$$d - d' = 0 \Leftrightarrow d = d'.$$

$\dashv$

Διαθέτουμε πλέον όλα τα εργαλεία ώστε να ορίσουμε την έννοια του διαιρέτη. Η *ομάδα διαιρετών* μίας ελλειπτικής καμπύλης E, $Div(E)$, είναι η ελεύθερη αβελιανή ομάδα που παράγεται από τα σημεία της καμπύλης.

Ορισμός 1.2.10. Ένας *διαιρέτης* (*divisor*) $D \in Div(E)$ είναι ένα τυπικό άθροισμα σημείων

$$D = \sum_{P \in E} n_P(P),$$

όπου το πλήθος των μη μηδενικών $n_P \in \mathbb{Z}$ είναι πεπερασμένο.

Το *άθροισμα* δύο διαιρετών στην $Div(E)$ ορίζεται ως

$$\sum_{P \in E} n_P(P) + \sum_{P \in E} m_P(P) = \sum_{P \in E} (n_P + m_P)(P).$$

Το σύνολο $supp(D) = \{P \in E \mid n_P \neq 0\}$ ονομάζεται *φορέας* (*support*) του D.

Ο *βαθμός* του D είναι το άθροισμα

$$deg(D) = \sum_{P \in E} n_P.$$

Οι διαιρέτες μηδενικού βαθμού συνιστούν υποομάδα της $Div(E)$, η οποία συμβολίζεται $Div^0(E)$.

Διαιρέτες από ρητές συναρτήσεις. Έστω $f = g/h \in \bar{K}(E)$. Το πλήθος των ριζών και των πόλων της f είναι πεπερασμένο καθώς φράσσεται από το πλήθος των ριζών των πολυωνύμων $g(x, y), h(x, y)$. Αυτό σημαίνει πως τα σημεία όπου η f έχει μη μηδενική τάξη είναι πεπερασμένα. Μπορούμε επομένως να ορίσουμε το *διαιρέτη της* f ως το τυπικό άθροισμα

$$div(f) = \sum_{n_P \in E} ord_P(f)(P). \tag{1.9}$$

Αν u παράμετρος ομοιομορφίας για τυχαίο σημείο P και $f = u^d \cdot s$, $g = u^{d'} \cdot t$, τότε $f \cdot g = u^{d+d'} \cdot (st)$ και $f/g = u^{d-d'} \cdot (s/t)$. Συνεπώς

$$\begin{aligned} ord_P(f \cdot g) &= ord_P(f) + ord_P(g) \\ ord_P(f/g) &= ord_P(f) - ord_P(g). \end{aligned}$$

Εφαρμόζοντας τις παραπάνω σχέσεις στο άθροισμα όλων των σημείων της E του ορισμού (1.9), προκύπτουν οι παρακάτω χρήσιμες σχέσεις.

$$\begin{aligned} div(f \cdot g) &= div(f) + div(g) \\ div(f/g) &= div(f) - div(f). \end{aligned} \tag{1.10}$$

Ένας διαιρέτης $D \in Div(E)$ για τον οποίο υπάρχει $f \in \bar{K}(E)$ ώστε $D = div(f)$ ονομάζεται *κύριος*. Αποδεικνύεται [Sil86 II.3.1] ότι κάθε κύριος διαιρέτης είναι μηδενικού βαθμού. Δύο διαιρέτες D_1, D_2 καλούνται *ισοδύναμοι* ως προς τη σχέση $\sim$, εάν η διαφορά τους είναι κύριος διαιρέτης, δηλαδή

$$D_1 \sim D_2 \Leftrightarrow \exists f \in \bar{K}(E) : D_1 - D_2 = div(f).$$

Παρατηρούμε ότι αν $D_1 \sim D_1'$ και $D_2 \sim D_2'$ τότε $D_1 + D_2 \sim D_1' + D_2'$. Συνεπώς το σύνολο κλάσεων ισοδυναμίας $Div(E)/\sim$ γίνεται ομάδα αν εφοδιαστεί με την καλώς ορισμένη πράξη

$$[D_1] \oplus [D_2] = [D_1 + D_2].$$

Η ομάδα πηλίκο $Div(E)/\sim$ καλείται *ομάδα Picard* της E και συμβολίζεται $Pic(E)$. Ως *ομάδα κλάσεων διαιρετών* (*divisor class group*) της E ορίζουμε την ομάδα

$$Pic^0(E) = Div^0(E)/\sim .$$

Λήμμα 1.2.11. *Η απεικόνιση*

$$\begin{aligned} \sigma : E &\longrightarrow Pic^0(E) \\ \sigma(P) &\longmapsto [(P) - (\mathcal{O})] \end{aligned}$$

είναι ομομορφισμός ομάδων.

Απόδειξη. Έστω $P, Q \in E$, $\overline{PQ} \equiv l(x,y) : \lambda x + \mu y + \nu = 0$ και R το τρίτο σημείο τομής της $\overline{PQ}$ με την E. Η τάξη της συνάρτησης $l(x,y)$ είναι μη μηδενική μόνο στις ρίζες (τα σημεία τομής με την $E\backslash\{\mathcal{O}\}$) και τους πόλους της (το σημείο $\mathcal{O}$). Διακρίνουμε τις εξής περιπτώσεις:

(i). $\mu = 0$. Τότε $l(x,y) : \lambda x + \nu = 0$ και $\lambda \neq 0$. Για το σημείο $\mathcal{O}$ έχουμε ότι

$$\lambda x + \nu = \left(\frac{x}{y}\right)^{-2} \cdot \left(\frac{x}{y}\right)^2 \cdot (\lambda x + \nu) = \frac{\lambda x^3 + \nu x^2}{x^3 + \alpha x + \beta}$$

και από το Πόρισμα 1.2.7.(iii)

$$deg(\lambda x^3 + \nu x^2) = deg(x^3 + \alpha x + \beta) = 6 \Rightarrow [\left(\frac{x}{y}\right)^2 l(x,y)](P) \notin 0, \infty \Rightarrow$$

$$\Rightarrow ord_{\mathcal{O}}(l) = -2.$$

Αφού η $\overline{PQ}$ είναι κάθετη στον άξονα x, ισχύει ότι $R = \mathcal{O}$ και άρα οι ρίζες της $l(x,y)$ είναι ακριβώς τα σημεία P, Q. Εξάλλου, γνωρίζουμε ότι ο βαθμός του $div(l)$ είναι μηδέν, άρα υποχρεωτικά

$$div(l) = \begin{cases} (P) + (Q) - 2(\mathcal{O}), & P \neq Q \\ 2(P) - 2(\mathcal{O}), & P = Q \end{cases}$$

(ii). $\mu \neq 0$. Με παρόμοια ανάλυση καταλήγουμε ότι $ord_{\mathcal{O}}(l) = -2$ και άρα

$$div(l) = \begin{cases} (P) + (Q) + (R) - 3(\mathcal{O}), & P \neq Q \\ 2(P) + (R) - 3(\mathcal{O}), & P = Q \end{cases}$$

Σε κάθε περίπτωση λοιπόν μπορούμε να γράψουμε

$$div(\lambda x + \mu y + \nu) = (P) + (Q) + (R) - 3(\mathcal{O})$$

.

Ομοίως για την ευθεία $\overline{\mathcal{O}R} : x - x_R = 0$ παίρνουμε

$$div(x - x_R) = (R) + (P + Q) - 2(\mathcal{O}).$$

Αφαιρούμε κατά μέλη και έχουμε

$$div(\lambda x + \mu y + \nu) - div(x - x_R) = (P) + (Q) - (P + Q) - (\mathcal{O}) \overset{(1.10)}{\Rightarrow}$$

$$(P + Q) - (\mathcal{O}) = (P) - (\mathcal{O}) + (Q) - (\mathcal{O}) - div(\frac{\lambda x + \mu y + \nu}{x - x_R}) \Rightarrow$$

$$[(P + Q) - (\mathcal{O})] = [(P) - (\mathcal{O}) + (Q) - (\mathcal{O})] \Rightarrow$$
$$[(P + Q) - (\mathcal{O})] = [(P) - (\mathcal{O})] \oplus [(Q) - (\mathcal{O})] \Rightarrow$$
$$\sigma(P + Q) = \sigma(P) \oplus \sigma(Q).$$

⊣

Με βάση το Λήμμα 1.2.11 αποδεικνύεται το ακόλουθο βασικό θεώρημα:

Θεώρημα 1.2.12. *Έστω διαιρέτης $D = \sum_{P_E} n_P(P)$ μηδενικού βαθμού. Ο D είναι κύριος αν και μόνο αν*

$$\textstyle\sum_{P_E} [n_P]P = \mathcal{O}.$$

Απόδειξη. Θεωρούμε τον ομομορφισμό του Λήμματος 1.2.11 $P \overset{\sigma}{\longmapsto} [(P) - (\mathcal{O})]$.

$$\sum_{P \in E} [n_P]P = \mathcal{O} \Leftrightarrow \sigma(\sum_{P \in E} [n_P]P) = 0_\sim \Leftrightarrow \sum_{P \in E} n_P \sigma(P) = 0_\sim \Leftrightarrow$$

$$\sum_{P \in E} n_P[(P) - (\mathcal{O})] = 0_\sim \Leftrightarrow [\sum_{P \in E} n_P(P)] \ominus [\sum_{P \in E} n_P(\mathcal{O})] = 0_\sim \Leftrightarrow$$

$$[D] \ominus [0 \cdot (\mathcal{O})] = 0_\sim \Leftrightarrow [D] = 0_\sim ,$$

δηλαδή ο D είναι κύριος.

⊣

Ο Ορισμός 1.2.10 επεκτείνεται σε κάθε αλγεβρική καμπύλη και αποτελεί ειδική έκφραση του *διαιρέτη Weil* (*Weil divisor*) για αλγεβρικές πολλαπλότητες. Οι διαιρέτες είναι ένα εργαλείο με εφαρμογή σε μερικά από τα σπουδαιότερα θεωρήματα της θεωρίας αλγεβρικών καμπυλών, με χαρακτηριστικότερο ίσως παράδειγμα το *θεώρημα Riemann-Roch* που λειτουργεί ως συνδετικός κρίκος μεταξύ της αλγεβρικής και της τοπολογικής προσέγγισης μίας καμπύλης [Ste94 §4.3]. Εδώ διατυπώνουμε ένα απαραίτητο θεώρημα για τον ορισμό των ζευγμάτων Tate και Weil, γνωστό και ως *νόμος αμοιβαιότητας του Weil*.

Θεώρημα 1.2.13. *Έστω* $f, g \in \bar{K}(E)$. *Τότε*

$$f(div(g)) = g(div(f)).$$

Απόδειξη. [BSS05 IX.Appendix] και [CC90 §7]. ⊣

1.3 Το ζεύγμα Tate

Ο υπολογισμός του ζεύγματος Tate πάνω σε πεπερασμένα σώματα, προτάθηκε από τους G.Frey και H.G.Rück [FR94], [FMR99] . Αρχικώς δίνουμε τον γενικό ορισμό του ζεύγματος Tate, όπως εισήγαγε ο J.Tate [Tat57], για ελλειπτικές καμπύλες.

Θεωρούμε ελλειπτική καμπύλη E/K_0 και $n \in \mathbb{Z}^+$ σχετικά πρώτο με τη χαρακτηριστική του σώματος K_0. Για τυχαίο σώμα F, όπου $K_0 \subseteq F \subseteq \bar{K}$ ορίζουμε τις εξής υποομάδες τις $E(F)$:

- Η υποομάδα των *σημείων m-συστροφής* (*m-torsion points*) είναι

  $$E(F)[m] = \{P \in E(F) \mid [m]P = \mathcal{O}\}$$

  δηλαδή η υποομάδα των στοιχείων της $E(F)$ που η τάξη τους διαιρεί το m. Για $F = \bar{K}$ γράφουμε απλώς $E[m]$.

- Η $mE(F) = \{[m]P \mid P \in E(F)\}$.

- Το σύνολο πηλίκο $E(F)/mE(F)$ που είναι ομάδα, αφού η $mE(F)$ είναι κανονική ως υποομάδα αβελιανής ομάδας.

Θεώρημα 1.3.1. *Έστω ελλειπτική καμπύλη* $E/\mathbb{F}_q$, $q = p^r$. *Εάν* $m \in \mathbb{Z}^+$: $gcd(m, q) = 1$ *τότε* $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$. *Εάν* $m = p^e$ *τότε*

$$E[p^e] \cong \begin{cases} \{\mathcal{O}\}, & \textit{υπεριδιάζουσα} \\ \mathbb{Z}_{p^e}, & \textit{συνήθης} \end{cases} \tag{1.11}$$

Απόδειξη. [Sil86 3.6.4, 5.3.1]. ⊣

Ορίζουμε το σύνολο των n-οστών ριζών της μονάδας $U_n = \{u \in \bar{K} \mid u^n = 1\}$ και $K = K_0(U_n)$ την επέκταση του K που παράγεται από το U_n. Ορίζουμε επίσης την υποομάδα $(K^*)^n = \{u^n \mid u \in K^*\}$ της πολλαπλασιαστικής ομάδας K^*.

Αν οι φορείς του διαιρέτη ρητής συνάρτησης f και ενός διαιρέτη $D = \sum_{P \in E} n_P(P)$ μηδενικού βαθμού είναι ξένοι μεταξύ τους, ορίζουμε την ποσότητα

$$f(D) = \prod_{P \in supp(D)} f(P)^{n_P}. \tag{1.12}$$

Λήμμα 1.3.2. *Έστω $D \in Div^0(E)$, $f \in \bar{K}(E)$: $supp(div(f)) \cap supp(D) = \varnothing$. Τότε για κάθε $g = c \cdot f$, $c \in K^*$*

$$f(D) = g(D).$$

Απόδειξη. Ισχύει ότι $supp(div(f)) = supp(div(g))$ και επομένως ορίζεται η ποσότητα $g(D)$. Αν $D = \sum_{P \in E} n_P(P)$ τότε $\sum_{P \in E} n_P = \sum_{P \in supp(D)} n_P = 0$ και άρα

$$\begin{aligned} g(D) = \prod_{P \in supp(D)} g(P)^{n_P} &= \prod_{P \in supp(D)} ([c \cdot f](P))^{n_P} = c^{\sum_{P \in supp(D)} n_P} \cdot \prod_{P \in supp(D)} f(P)^{n_P} \\ &= c^0 \cdot \prod_{P \in supp(D)} f(P)^{n_P} = f(D). \end{aligned}$$

⊣

Ορισμός 1.3.3. Έστω $P \in E(K)[n]$ και $f \in K(E)$ ώστε $div(f) = n(P) - n(\mathcal{O})$. Έστω επίσης $Q \in E(K)$ και διαιρέτης $D \in Div^0(E)$ ώστε $D \sim (Q) - (\mathcal{O})$ και $supp(div(f)) \cap supp(D) = \varnothing$. Ως *ζεύγμα Tate* (*Tate pairing*) ορίζουμε την απεικόνιση

$$\langle , \rangle_n : E(K)[n] \times E(K)/nE(K) \longrightarrow K^*/(K^*)^n$$
$$\langle P, Q \rangle_n = f(D).$$

Θα δείξουμε την ορθότητα του Ορισμού 1.3.3. Τα $Q, f(D)$ είναι αντιπρόσωποι των συμπλόκων $Q + nE(K) \in E(K)/nE(K)$ και $f(D) \cdot (K^*)^n \in K^*/(K^*)^n$ αντίστοιχα. Η ύπαρξη ρητής συνάρτησης ώστε $div(f) = n(P) - n(\mathcal{O})$ εξασφαλίζεται από το ότι $P \in E(K)[n] \Leftrightarrow [n]P = \mathcal{O} = [n]\mathcal{O}$. Εξάλλου, ένας διαιρέτης μηδενικού βαθμού D με τις ιδιότητες του ορισμού μπορεί να βρεθεί εύκολα επιλέγοντας σημείο $S \notin \{\mathcal{O}, -Q, P, P - Q\}$ και ορίζοντας $D = (Q + S) - (S)$: τότε $deg(D) = 0$ και από το Θεώρημα 1.2.12

$$D - Q + \mathcal{O} = \mathcal{O} \Leftrightarrow (D) \sim (Q) - (\mathcal{O}).$$

Επιπλέον έχουμε $supp(div(f)) \cap supp(D) = \{Q+S, S\} \cap \{P, \mathcal{O}\} = \varnothing$, επομένως

$$f(D) = \prod_{P \epsilon supp(D)} f(P)^{n_P} = \frac{f(Q+S)}{f(S)} \neq 0 \Rightarrow f(D) \in K^*.$$

Λήμμα 1.3.4. *Για δύο οποιαδήποτε σημεία $P \in E(K)[n], Q \in E(K)$ η εικόνα $\langle P, Q \rangle_n$ δεν εξαρτάται από την επιλογή των f, D.*

Απόδειξη. Έστω f_1, f_2 και D_1, D_2 που πληρούν τις προϋποθέσεις του Ορισμού 1.3.3. Θα δείξουμε ότι οι $f_1(D_1)$ και $f_2(D_2)$ είναι αντιπρόσωποι του ίδιου συμπλόκου της ομάδας πηλίκο $K^*/(K^*)^n$, δηλαδή ότι υπάρχει $r \in K^* : f_1(D_1) = f_2(D_1)r^n$. Για κάποια σταθερά $c \in K$, $f_2 = c \cdot f_1$, αφού

$$div(f_1) = div(f_2) = n(P) - n(\mathcal{O}) \overset{(1.10)}{\Rightarrow} div(f_1/f_2) = 0,$$

δηλαδή η f_1/f_2 είναι σταθερή. Από το Λήμμα 1.3.2 έχουμε $f_1(D_1) = f_2(D_1)$ και $f_1(D_2) = f_2(D_2)$ και μπορούμε λοιπόν να επιλέξουμε $f = f_1$ ή $f = f_2$ χωρίς να επηρεαστεί το αποτέλεσμα. Αν $D_1 \sim D_2 \sim (Q) - (\mathcal{O})$ και οι φορείς των D_1, D_2 είναι ξένοι με τον φορέα του διαιρέτη της f, τότε για κάποια $g \in \bar{K}(E)$ έχουμε

$$D_1 = D_2 + div(g) \Leftrightarrow \sum_{supp(D_1)} n_P^1(P) = \sum_{supp(D_2)} n_P^2(P) + \sum_{supp(div(g))} n_P^g(P).$$

$supp(div(g)) \subseteq supp(D_1) \cup supp(D_2) \Rightarrow supp(div(g)) \cap supp(div(f)) = \varnothing$, συνεπώς

$$\begin{aligned} f(D_1) = f(D_2 + div(g)) &= \prod_{P \epsilon supp(D_2 + div(g))} f(P)^{n_P^1} = \\ &= \prod_{P \epsilon supp(D_2)} f(P)^{n_P^2} \cdot \prod_{P \epsilon supp(div(g))} f(P)^{n_P^g} = \\ &= f(D_2) \cdot f(div(g)) \overset{1.2.13}{=} f(D_2) \cdot g(div(f)) = \\ &= f(D_2) \cdot g(n(P) - n(\mathcal{O})) = f(D_2) \cdot (\frac{g(P)}{g(\mathcal{O})})^n. \end{aligned}$$

Αφού $P, \mathcal{O} \notin supp(g)$ έχουμε ότι $\dfrac{g(P)}{g(\mathcal{O})} \in K^*$. Σημειώνουμε επίσης την αναγκαιότητα της χρήσης του νόμου αμοιβαιότητας του Weil στην απόδειξη των παραπάνω ισοτήτων.

$\dashv$

Το ζεύγμα Tate υπεράνω πεπερασμένων σωμάτων. Έστω $E/\mathbb{F}_q$, $q = p^r$. Τότε $K = \mathbb{F}_q(U_n)$ είναι πεπερασμένη επέκταση του K_0. Ο μικρότερος ακέραιος k ώστε $\mathbb{F}_{q^k} = K$ ονομάζεται *βαθμός εμβάπτισης* (*embedding degree*) της E ως προς n. Από τη θεωρία πεπερασμένων σωμάτων έχουμε ότι ο βαθμός εμβάπτισης k είναι ο μικρότερος ακέραιος ώστε

$$n \mid q^k - 1 = \#\mathbb{F}_{q^k}^* \,. \tag{1.13}$$

Συνεπώς το ζεύγμα Tate υπεράνω του πεπερασμένου σωμάτος $\mathbb{F}_q$ ορίζεται ως

$$\langle , \rangle_n : E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n,$$

$$(P, Q) \overset{\langle , \rangle_n}{\longmapsto} f(D) \,.$$

Σημαντική παρατήρηση είναι πως η εικόνα $\langle P, Q\rangle_n = f(D)$ δεν είναι μία συγκεκριμένη τιμή αλλά κλάση ισοδυναμίας στην ομάδα $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$, κάτι γενικώς ανεπιθυμήτο στις εφαρμογές. Το πρόβλημα ξεπερνάται υψώνοντας την εικόνα στην $\frac{q^k-1}{n}$-οστή δύναμη: αν $P_1, P_2 \in E(\mathbb{F}_{q^k})[n]$ και $Q_1, Q_2 \in E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})$ ώστε $\langle P_1, Q_1\rangle_n$, $\langle P_2, Q_2\rangle_n$ να είναι αντιπρόσωποι της ίδιας κλάσης, τότε για κάποια σταθερά $c \in \mathbb{F}_{q^k}^* : \langle P_1, Q_1\rangle_n = \langle P_2, Q_2\rangle_n \cdot c^n$. Επομένως

$$(\langle P_1, Q_1\rangle_n)^{\frac{q^k-1}{n}} = (\langle P_2, Q_2\rangle_n \cdot c^n)^{\frac{q^k-1}{n}} = (\langle P_2, Q_2\rangle_n)^{\frac{q^k-1}{n}} \cdot c^{q^k-1} = (\langle P_2, Q_2\rangle_n)^{\frac{q^k-1}{n}}.$$

Συχνά στη βιβλιογραφία, ορίζεται εναλλακτικά το *ανηγμένο ζεύγμα Tate* (*reduced Tate pairing*) υπεράνω του $\mathbb{F}_q$

$$t_n(P, Q) = \langle P, Q\rangle_n^{\frac{q^k-1}{n}}.$$

Θεώρημα 1.3.5. *Έστω $E/\mathbb{F}_q$, ακέραιος $n \in \mathbb{Z}$ ώστε $gcd(char(\mathbb{F}_q), n) = 1$ και έστω $\mathbb{F}_{q^k} = \mathbb{F}_q(U_n)$. Τότε το ζεύγμα Tate ικανοποιεί τις εξής ιδιότητες:*

(i). Διγραμμικότητα (Bilinearity):
για κάθε $P, P_1, P_2 \in E(\mathbb{F}_{q^k})[n]$ και $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})$:

$$\langle P_1 + P_2, Q\rangle_n = \langle P_1, Q\rangle_n \langle P_2, Q\rangle_n$$

$$\langle P, Q_1 + Q_2\rangle_n = \langle P, Q_1\rangle_n \langle P, Q_2\rangle_n.$$

(ii). Μη εκφυλισμός (Non-degeneracy):

$$(\forall P \in E(\mathbb{F}_{q^k})[n]\backslash\{\mathcal{O}\})(\exists Q \in E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})) : \langle P, Q\rangle_n \neq 1 \quad \text{και}$$

$$(\forall Q \in [E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})]\backslash\{nE(\mathbb{F}_{q^k})\})(\exists P \in E(K)[n]) : \langle P, Q\rangle_n \neq 1.$$

Απόδειξη. (i). Έστω $P_3 = P_1 + P_2$ και g, f_1, f_2 ώστε

$$(P_3) - (\mathcal{O}) = (P_1) - (\mathcal{O}) + (P_2) - (\mathcal{O}) + div(g)$$
$$div(f_1) = n(P_1) - n(\mathcal{O})$$
$$div(f_2) = n(P_2) - n(\mathcal{O}).$$

Υψώνοντας την πρώτη ισότητα στη n-οστή δύναμη και προσθέτοντας κατά μέλη έχουμε

$$div(f_1 \cdot f_2 \cdot g^n) = n(P_3) - n(\mathcal{O}).$$

Έστω διαιρέτης $D \sim (Q) - (\mathcal{O}) : supp(D) \cap \{P_1, P_2, P_3, \mathcal{O}\} = \varnothing$. Τότε

$$\langle P_1 + P_2, Q\rangle_n = \langle P_3, Q\rangle_n = [f_1 \cdot f_2 \cdot g^n](D) = f_1(D) \cdot f_2(D) \cdot g(D)^n$$

το οποίο είναι ισοδύναμο με $\langle P_1, Q\rangle_n \cdot \langle P_2, Q\rangle_n$, αφού $g(D)^n \in (\mathbb{F}_{q^k}^*)^n$.

Έστω $Q_3 = Q_1 + Q_2$ και διαιρέτες $D_1 \sim (Q_1) - (\mathcal{O})$, $D_2 \sim (Q_2) - (\mathcal{O})$. Τότε $D_1 + D_2 \sim (Q_1) - (\mathcal{O}) + (Q_2) - (\mathcal{O}) \sim (Q_1 + Q_2) - (\mathcal{O}) \sim (Q_3) - (\mathcal{O})$ και αφού $supp(D_1 + D_2) = supp(D_1) \cup supp(D_2)$, έχουμε ότι αν για τυχαία f ορίζεται η τιμή $f(D_1 + D_2)$, τότε ορίζονται και οι $f(D_1), f(D_2)$ επομένως

$$\langle P, Q_1 + Q_2\rangle_n = \langle P, Q_3\rangle_n = f(D_1 + D_2) = f(D_1) \cdot f(D_2)$$

το οποίο είναι ισοδύναμο με $\langle P, Q_1\rangle_n \cdot \langle P, Q_2\rangle_n$.

(ii). [FR94 Proposition 2.1] και [Hess04 Theorem 3].

⊣

Το τροποποιημένο ζεύγμα Tate. Η ιδιότητα του μη εκφυλισμού του ζεύγματος Tate εξασφαλίζει την ύπαρξη ενός σημείου $Q \in (E(K)/nE(K))\backslash\{nE(K)\}$ ώστε $\langle P, Q\rangle_n \neq 1$ (και αντίστοιχα για το δεύτερο όρισμα). Αυτό είναι αρκετό από μαθηματικής σκοπιάς, στην πράξη όμως ενδιαφερόμαστε και για την εύρεση ενός τέτοιου σημείου. Για το λόγο αυτό, συχνά λαμβάνεται μια παραλλαγμένη εκδοχή του κλασικού ορισμού, χωρίς φυσικά να χάνεται η ιδιότητα της διγραμμικότητας. Η μέθοδος που θα παρουσιάσουμε οφείλεται στον Verheul [Ver01] και χρησιμοποιεί παραμορφωτικές απεικονίσεις.

Ορισμός 1.3.6. Έστω ελλειπτική καμπύλη $E/\mathbb{F}_q$, $q = p^r$, $n \in \mathbb{Z} : gcd(p, n) = 1$ και $P \in E(\mathbb{F}_q)[n]$. Μία *παραμορφωτική απεικόνιση* (*distortion map*) ως προς P είναι ένας ενδομορφισμός $\phi \in End(E)$ που απεικόνιζει το P σε ένα σημείο $\phi(P)$ γραμμικώς ανεξάρτητο του P.

Για έναν ενδομορφισμό ϕ ισχύουν τα εξής:

- Αφού η ϕ είναι ομομορφισμός ισχύει ότι $\phi(\mathcal{O}) = \mathcal{O}$, επομένως η ϕ δεν μπορεί να είναι παραμορφωτική απεικόνιση ως προς $\mathcal{O}$.
- $\phi(E[n]) \subseteq E[n]$, δηλαδή $\phi \in End(E[n])$. Συνεπώς $\phi(P) \in E[n]$.
- Από το Θεώρημα 1.3.1, η $E[n]$ παράγεται από δύο γραμμικώς ανεξάρτητα σημεία της και μία βάση της είναι η $\{P, \phi(P)\}$. Έτσι, εάν $E[n] \nsubseteq E(\mathbb{F}_q)$, τότε η εικόνα $\phi(P)$ δεν ανήκει στην $E(\mathbb{F}_q)$. Επιπλέον, η ομάδα $E(\mathbb{F}_q)[n]$ είναι κυκλική και ένας γεννήτοράς της είναι το P.

Στο επόμενο λήμμα παραθέτουμε έναν ισοδύναμο χαρακτηρισμό των υπεριδιαζουσών καμπυλών.

Λήμμα 1.3.7. *Μια ελλειπτική καμπύλη είναι υπεριδιάζουσα αν και μόνο αν ο δακτύλιος των ενδομορφισμών $End(E)$ είναι μη μεταθετικός.*

Απόδειξη. [Sil86 V.3.1& III.9.4]. ⊣

Πρόταση 1.3.8. *Έστω συνήθης ελλειπτική καμπύλη $E/\mathbb{F}_q$ $q = p^r$, $n \in \mathbb{Z}$: $gcd(p, n) = 1$ και $P \in E(\mathbb{F}_q)[n]$. Εάν $E[n] \nsubseteq E(\mathbb{F}_q)$, τότε δεν υπάρχει παραμορφωτική απεικόνιση ως προς P.*

Απόδειξη. Έστω ότι υπάρχει παραμορφωτική απεικόνιση ως προς P, ϕ και $\phi(P) = Q \notin E(\mathbb{F}_q)$, αφού $E[n] \nsubseteq E(\mathbb{F}_q)$. Θεωρούμε τον *ενδομορφισμό Frobenius* στην q-οστή δύναμη

$$F_q : (x, y) \longmapsto (x^q, y^q),$$

ο οποίος σταθεροποιεί τα σημεία του $\mathbb{F}_q$. Πράγματι, $(x^q, y^q) = (x, y) \Leftrightarrow x^q - x = 0$, $y^q - y = 0$ και τα πολυώνυμα $x^q - x = 0$, $y^q - y = 0$ έχουν το πολύ q ρίζες ενώ κάθε στοιχείο $\mathbb{F}_q$ είναι ρίζα τους από το θεώρημα του Euler. Συμπεραίνουμε ότι τα σταθερά σημεία της F_q είναι ακριβώς τα ζεύγη $(x, y) \in \mathbb{F}_q^2$. Επομένως

$$F_q(\phi(P)) = F_q(Q) \neq Q = \phi(P) = \phi(F_q(P)) \Rightarrow F_q \circ \phi \neq \phi \circ F_q$$

και άρα ο $End(E)$ είναι μη μεταθετικός, που είναι άτοπο από το Λήμμα 1.3.7.

⊣

Σύμφωνα με την Πρόταση 1.3.8, για μία μεγάλη κλάση συνήθων καμπυλών δεν υπάρχει παραμορφωτική απεικόνιση. Αντίθετα, ο E.Verheul έδειξε ότι για όλες τις υπεριδιάζουσες καμπύλες μπορούν πάντα να βρεθούν παραμορφωτικές απεικονίσεις ως προς τα σημεία της ομάδας $E[n]$, όπου n πρώτος και $n \neq p$ [Ver04 Theorem 5]. Αυτό είναι ένα από τα πλεονεκτήματα της χρήσης υπεριδιαζουσών καμπυλών στην κρυπτογραφία ζευγμάτων, αλλά όχι το σπουδαιότερο, όπως θα φανεί στην ενότητα 1.5.

Σε μία καμπύλη $E/\mathbb{F}_q$, για την οποία υπάρχει παραμορφωτική απεικόνιση ϕ ως προς όλα τα σημεία της εκτός του $\mathcal{O}$, το *τροποποιημένο ζεύγμα Tate*, (*modified Tate pairing*) ορίζεται ως

$$\langle P, Q\rangle_n^{\phi} = \langle P, \phi(Q)\rangle_n.$$

Θεώρημα 1.3.9. *Έστω $E/\mathbb{F}_q$, n πρώτος ώστε $n \nmid q-1$ και $P \in E(\mathbb{F}_q)[n]\backslash\{\mathcal{O}\}$. Αν ορίζεται τροποποιημένο ζεύγμα Tate στην καμπύλη E, τότε*

$$\langle P, P\rangle_n^{\phi} \neq 1.$$

Απόδειξη. Αφού $n \nmid q-1$ ο βαθμός εμβάπτισης k της E είναι μεγαλύτερος του 1 οπότε $\mathbb{F}_q \nsubseteq (\mathbb{F}_{q^k})$. Επειδή το $\mathbb{F}_{q^k}$ είναι το μικρότερο σώμα που περιέχει τα $\mathbb{F}_q, U_n$, έχουμε ότι $\mathbb{F}_q \subseteq (\mathbb{F}_{q^k})^n$. Επιπλέον, η E και το σημείο P ορίζονται υπεράνω του $\mathbb{F}_q$, επομένως από τον ορισμό 1.3.3 έχουμε ότι

$$\langle P, P\rangle_n \in \mathbb{F}_q \Rightarrow \langle P, P\rangle_n = 1.$$

Είναι εύκολο να δείξουμε πως κάθε σύμπλοκο $E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})$ περιέχει ένα σημείο $R \in E[n]$ [Sco02]. Έστω λοιπόν τυχαίο $Q \in \mathbb{F}_{q^k}$ και $R \in E[n]$ που ανήκει στο ίδιο σύμπλοκο με το Q. Υπάρχει επομένως $R' \in \mathbb{F}_{q^k}$ ώστε $Q = R + nR'$. Γνωρίζουμε ήδη ότι σε κάθε περίπτωση το σύνολο $\{P, \phi(P)\}$ είναι μία βάση του $E[n]$. Συνεπώς υπάρχουν $\lambda, \mu \in \{0, 1, \ldots, n-1\}$ ώστε $R' = [\lambda]P + [\mu]\phi(P)$ άρα

$$\begin{aligned}\langle P, R\rangle_n = \langle P, R'\rangle_n = \langle P, R'\rangle = \langle P, [\lambda]P + [\mu]\phi(P)\rangle_n = \\ = (\langle P, P\rangle_n)^{\lambda} \cdot (\langle P, \phi(P)\rangle_n)^{\mu} = (\langle P, \phi(P)\rangle_n)^{\mu},\end{aligned} \tag{1.14}$$

όπου η τρίτη ισότητα προκύπτει λόγω διγραμμικότητας. Η (1.14) συνεπάγεται ότι αν $\langle P, P\rangle_n^{\phi} = \langle P, \phi(P)\rangle_n = 1$ τότε το ζεύγμα Tate είναι εκφυλιστικό, άτοπο.

⊣

Εναλλακτικά των παραμορφωτικών απεικονίσεων, μπορούμε να χρησιμοποιήσουμε την *απεικόνιση ίχνους* (*trace map*):

$$Tr : E(\mathbb{F}_{q^k}) \longrightarrow E(\mathbb{F}_q)$$

$$Tr((x, y)) = \sum_{i=0}^{k-1} (x^{q^i}, y^{q^i}).$$

Το άθροισμα συμβολίζει πράξεις στην $E(\mathbb{F}_{q^k})$ και άρα η απεικόνιση ίχνους είναι ομομορφισμός. Με παρόμοια ανάλυση προκύπτει ότι αν n πρώτος και $Q \in E(\mathbb{F}_{q^k})[n]\backslash E(\mathbb{F}_q)[n]$ ώστε $Tr(Q) \neq \mathcal{O}$, τότε $\langle Tr(Q), Q\rangle_n \neq 1$. Η μέθοδος αυτή μπορεί να εφαρμοστεί και σε συνήθεις ελλειπτικές καμπύλες (βλ. [BSS05 IX.7.4]).

Υπολογισμός του ζεύγματος Tate. Ο V.Miller [Mil86] παρουσίασε έναν αλγόριθμο για τον αποδοτικό υπολογισμό του ζεύγματος Weil (βλ. §1.4), με τη χρήση ρητών συναρτήσεων f των οποίων οι διαιρέτες είναι της μορφής

$$div(f) = i(P) - ([i]P) - (i-1)(\mathcal{O}), \quad i \in \mathbb{N}.$$

Η απλή double-and-add τεχνική που εφαρμόζει μπορεί να χρησιμοποιηθεί για τον υπολογισμό του ανηγμένου ζεύγματος Tate. Η ορθότητα του αλγορίθμου στηρίζεται στο επόμενο λήμμα.

Λήμμα 1.3.10. *Έστω $P \in E/\mathbb{F}_q$ και οικογένεια συναρτήσεων $\mathcal{F} = (f_i)_{i\in I}$ ώστε $div(f_i) = i(P) - ([i]P) - (i-1)(\mathcal{O})$. Οι $(f_i)_{i\in I}$ ικανοποιούν τις εξής ιδιότητες:*

(i). Η f_1 είναι σταθερή.

(ii). Αν $l = \overline{[i]P[j]P}$ και v είναι οι ευθείες που χρησιμοποιούνται στο άθροισμα $[i]P + [j]P = [i+j]P$, τότε

$$f_{i+j} = f_i \cdot f_j \cdot (l/v).$$

Απόδειξη. Η (i) είναι προφανής για $i = 1$. Για την (ii) έχουμε όπως και στην απόδειξη του Λήμματος 1.2.11 ότι

$$\begin{aligned} div(l/v) &= div(l) - div(v) = \\ &= (([i]P) + ([j]P) + (R_{ij}) - (3\mathcal{O})) - ((R_{ij}) + ([i+j]P) - (2\mathcal{O})) = \\ &= ([i]P) + ([j]P) - ([i+j]P) - (\mathcal{O}), \end{aligned}$$

όπου R_{ij} το τρίτο σημειο τομής της ευθείας l. Συνεπώς

$$\begin{aligned} div(f_i \cdot f_j \cdot (l/v)) &= (i(P) - ([i]P) - (i-1)(\mathcal{O})) + ((j(P) - ([j]P) - (j-1)(\mathcal{O})) + \\ &\quad + (([i]P) + ([j]P) - ([i+j]P) - (\mathcal{O})) = \\ &= (i+j)(P) - ([i+j]P) - (i+j-1)(\mathcal{O}) = div(f_{i+j}). \end{aligned}$$

⊣

Ο αλγόριθμος Miller εφαρμόζει το Λήμμα 1.3.10 εκκινώντας από το σημείο P και τη συνάρτηση $f_1 = 1$ ώστε να υπολογιστούν τελικά τα $[n]P$, $f_n(D) = \langle P, Q\rangle_n$. Επιλέγουμε S, $D = (Q+S) - (S) \sim (Q) - (\mathcal{O})$ και εκμεταλλευόμαστε την ιδιότητα 1.3.9.(ii), ώστε να υπολογίζουμε τις ενδιάμεσες τιμές $f_{i+j}(D)$. Η επιλογή του S μπορεί να γίνει τυχαία, υπάρχουν όμως και ντετερμινιστικές μέθοδοι επιλογής [BSS05 §IX.8]. Επισημαίνεται ότι εάν $P \in E[n]$, τότε $div(f_n) = n(P) - n(\mathcal{O})$.

Ο αλγόριθμος Miller για το ζεύγμα Tate
Είσοδος: $P, Q \in E(K)$, P τάξης n.
Έξοδος: $t_n(P,Q) = \langle P, Q \rangle_n^{\frac{q^k-1}{n}}$.
1. Διάλεξε κατάλληλο $S \in E(K)$.
2. $Q' \longleftarrow Q + S$.
3. $T \longleftarrow P$.
4. $m \longleftarrow \lfloor log(n) - 1 \rfloor$, $f \longleftarrow 1$.
5. **Όσο** $m \geqslant 0$:
6. Υπόλογισε τις ευθείες l, v του αθροίσματος $T + T = [2]T$.
7. $T \longleftarrow [2]T$.
8. $f \longleftarrow f^2 \cdot \frac{l(Q')v(S)}{v(Q')l(S)}$.
9. **Εάν** το m-οστό bit του n είναι 0 **τότε**:
10. Υπολόγισε τις ευθείες l, v του αθροίσματος $T + P$.
11. $T \longleftarrow T + P$.
12. $f \longleftarrow f \cdot \frac{l(Q')v(S)}{v(Q')l(S)}$.
13. $m \longleftarrow m - 1$.
14. **Επίστρεψε** f.

Η καρδιά του αλγορίθμου βρίσκεται στον κύριο βρόγχο του (γραμμές 5-13), ο οποίος καλείται *βρόγχος Miller* (*Miller loop*). Τα βήματα υπολογισμού εκτελούνται με τρόπο παρόμοιο του αλγορίθμου *Επαναλαμβανόμενου Τετραγωνισμού* (*Repeated Squaring*) για ύψωση δυνάμεων modulo m. Ο αριθμός εκτελέσων του βρόγχου είναι $\log(n)$ και της πρόσθεσης στις γραμμές 10-12 όσος και το πλήθος των μονάδων στη δυαδική αναπαράσταση (*βάρος Hamming*) του n. Συνεπώς, ο αλγόριθμος Miller είναι πολυωνυμικού χρόνου.

1.4 Το ζεύγμα Weil

Το ζεύγμα Weil προκύπτει από τον εναλλακτικό ορισμό του αρχικού ορισμού που εισήγαγε ο A.Weil [Sil86 §III.8], λόγω της δυνατότητας υπολογισμού που προσφέρει ο πρώτος. Μία απόδειξη της συσχέτισης των δύο ορισμών δίνεται στο [CC90 §10].

Ορισμός 1.4.1. Έστω E/K_0, $n \in \mathbb{Z}$ σχετικά πρώτος με την χαρακτηριστική του K_0 και $P, Q \in E[n]$. Έστω επίσης διαιρέτες $D \sim (P) - (\mathcal{O})$, $D' \sim (Q) - (\mathcal{O})$ με ξένους φορείς και ρητές συναρτήσεις f, g ώστε $div(f) = nD$ και $div(g) = nD'$. *Το ζεύγμα Weil* (*Weil pairing*) ορίζεται ως

$$e_n : E[n] \times E[n] \longrightarrow U_n$$
$$e_n(P,Q) = \frac{f(D')}{g(D)}.$$

Η ύπαρξη κατάλληλων συναρτήσεων f, g εξασφαλίζεται από το Θεώρημα 1.2.12 και την παρατήρηση ότι

$$P, Q \in E[n] \Rightarrow [n]P - [n]\mathcal{O} = [n]Q - [n]\mathcal{O} = \mathcal{O}.$$

Θα δείξουμε τώρα ότι ο Ορισμός 1.4.1 είναι καλός.

Θεώρημα 1.4.2. *Το ζεύγμα Weil έχει ως πεδίο τιμών το U_n και η τιμή $e_n(P,Q)$ είναι ανεξάρτητη της επιλογής των D, D', f, g.*

Απόδειξη. Από το νόμο αμοιβαιότητας του Weil έχουμε

$$(e_n(P,Q))^n = \left(\frac{f(D')}{g(D)}\right)^n = \frac{f(nD')}{g(nD)} = \frac{f(div(g))}{g(nD)} = \frac{g(div(f))}{g(nD)} = \frac{g(nD)}{g(nD)} = 1.$$

Επιπλέον, αν $D'' \sim (Q) - \mathcal{O}$, είναι διαιρέτης ώστε $supp(D'') \cap supp(D) = \varnothing$, τότε υπάρχει ρητή συναρτήση r ώστε $D'' = D' + div(r)$ Έστω τώρα ρητή συναρτήση h με $div(h) = nD''$. Τότε $div(h) = div(nD' + ndiv(r)) = div(g \cdot r^n) \overset{1.3.2}{\Rightarrow} h(D) = [g \cdot r^n](D)$ και άρα

$$\frac{f(D'')}{h(D)} = \frac{f(D') \cdot f(div(r))}{[g \cdot r^n](D)} = \frac{f(D') \cdot f(div(r))}{g(D) \cdot r^n(D)} = \frac{f(D') \cdot r(div(f))}{g(D) \cdot r(nD)} = \frac{f(D')}{g(D)}.$$

Εντελώς ανάλογα αποδεικνύεται και η ανεξαρτησία επιλογής ως προς D, f.

⊣

Θεώρημα 1.4.3. *Έστω E/K_0, $n \in \mathbb{Z}$ σχετικά πρώτος με την χαρακτηριστική του K_0. Το ζεύγμα Weil ικανοποιεί τις εξής ιδιότητες:*

(i). Διγραμμικότητα: για κάθε $P, P', Q, Q' \in E[n]$,

$$e_n(P + P', Q) = e_n(P,Q) \cdot e_n(P',Q),$$

$$e_n(P, Q + Q') = e_n(P,Q) \cdot e_n(P,Q').$$

(ii). Μη εκφυλισμός: εάν $P \neq \mathcal{O}$, τότε υπάρχει $Q \in E[n]$ ώστε $e_n(P,Q) = 1$.

(iii). Εναλλάσσουσα (Alternating): $e_n(P,Q) = e_n(Q,P)^{-1}$.

Απόδειξη. (i). Έστω $D \sim (P)-(\mathcal{O})$, $D' \sim (P')-(\mathcal{O})$ και $D'' \sim (Q)-(\mathcal{O})$ διαιρέτες ώστε $supp(D) \cap supp(D'') = \varnothing$ και $supp(D') \cap supp(D'') = \varnothing$. Τότε από το Λήμμα 1.2.11 $\Rightarrow D + D' \sim (P) + (P') - (\mathcal{O})$ και $supp(D + D') \cap supp(D'') = \varnothing$. Έστω επίσης ρητή συνάρτηση h ώστε $div(h) = nD + nD'$. Αν f, f' οι συναρτήσεις που επιλέγονται για τα $e_n(P, Q)$ και $e_n(P', Q)$, τότε $div(h) = div(f \cdot f') \overset{1.3.2}{\Rightarrow} h(D) = [f \cdot f'](D)$ και άρα

$$e_n(P + P', Q) = \frac{h(D'')}{g(D + D')} = \frac{[f \cdot f'](D'')}{g(D) \cdot g(D')} = \frac{f(D'') \cdot f'(D'')}{g(D) \cdot g(D')} = \\ = e_n(P, Q) \cdot e_n(P', Q).$$

Ανάλογα αποδεικνύεται και η γραμμικότητα ως προς το Q.

(ii). Έστω $P \in E[n] : (\forall Q \in E[n]) : e_n(P, Q) = 1$ και $S \notin \{\mathcal{O}, P, -Q, P - Q\}$. Τότε $D = (P - S) - (-S) \sim (P) - (\mathcal{O})$ και $D' = (Q + S) - (S) \sim (Q) - (\mathcal{O})$, επομένως για κατάλληλες f, g

$$e_n(P, Q) = \frac{f((Q + S) - (S))}{g((P - S) - (S))} = \frac{f((Q + S))}{f((S))} \cdot g(D).$$

Αφού $e_n(P, Q) = 1$ έχουμε ότι

$$f((Q + S)) = g(D) \cdot f((S)). \tag{1.15}$$

Από την ανεξαρτησία επιλογής του σημείου S για την τιμή $e_n(P, Q)$, μπορούμε να επιλέξουμε $Q + S$ αντί για S. Εκκινώντας από την (1.15) και με επαγωγή στο n προκύπτει ότι

$$f(([n]Q + S)) = g^n(D) \cdot f((S)) \overset{Q \in E[n]}{\Rightarrow} g^n(D) = 1. \tag{1.16}$$

Από τις (1.15) και (1.16) συμπεραίνουμε ότι $(\forall Q \in E[n]) : f^n((Q+S)) = f^n((S))$. Η f^n παραμένει σταθερή για μετατοπίσεις κατά $Q \in E[n]$, επομένως από γνωστό θεώρημα [Sil86 III.4.10], για κάποια $h \in \bar{K}(E) : f^n = h \circ [n]$, όπου $[n]$ είναι ο πολλαπλασιασμός $P \longmapsto [n]P$, που είναι συνάρτηση επί ως μη σταθερός μορφισμός [Sil86 II.2.3 & III.4.2.(a)]. Προς απαγωγή σε άτοπο, υποθέτουμε πως η h έχει ρίζα R και έστω $R' : [n]R' = R$. Τότε λόγω της (1.16), η $h \circ [n]$ μηδενίζεται σε όλο το σύνολο $\{[n](R' + Q) \mid Q \in E[n]\}$. Όμως από την Πρόταση 1.2.3 έχουμε $div(h \circ [n]) = div(f^n) = n \cdot div(f) = n^2(P) - n^2(\mathcal{O})$, άρα η $h \circ [n]$ έχει ως μόνη ρίζα το σημείο P. Επομένως η h είναι σταθερή και άρα

$$div(h \circ [n]) = 0 \Rightarrow n^2(P) - n^2(\mathcal{O}) = 0 \Rightarrow P = \mathcal{O}.$$

(iii). Η διγραμμικότητα μας δίνει

$$e_n(P+Q,P+Q) = e_n(P,P)\cdot e_n(P,Q)\cdot e_n(Q,P)\cdot e_n(Q,Q),$$

αρκεί λοιπόν να δείξουμε ότι για τυχαίο σημείο $R \in E[n]$ ισχύει ότι $e_n(R,R)=1$. Έστω $D, D' \sim (R)-(\mathcal{O})$ ώστε $supp(D)\cap supp(D')=\varnothing$ και ρητές συναρτήσεις f, f' με $div(f)=nD$ και $div(f')=nD'$. Τότε υπάρχει ρητή συναρτήση r ώστε $D'=D+div(r)$. Έχουμε ότι

$$div(f') = nD + n\cdot div(r) = div(f\cdot r^n) \overset{1.3.2}{\Rightarrow} f'(D) = [f\cdot r^n](D).$$

Συνεπώς

$$\begin{aligned} e_n(R,R) &= \frac{f(D')}{f'(D)} = \frac{f(D')}{f'(D)\cdot r^n(D)} = \frac{f(D')}{f'(D)\cdot r(nD)} = \frac{f(D)}{f'(D)\cdot r(div(f))} \overset{1.2.13}{=} \\ &= \frac{f(D)}{f'(D)\cdot f(div(r))} = \frac{f(D)}{f'(D)\cdot f(D'-D)} = \frac{f(D)\cdot f'(D)}{f'(D)\cdot f(D)} = 1. \end{aligned}$$

⊣

Ένα πολύ σημαντικό ζήτημα που ενδιαφέρει στις κρυπτογραφικές εφαρμογές, είναι το μέγεθος του πεδίου ορισμού του ζεύγματος Weil, δηλαδή πόσο μεγάλη είναι η ελάχιστη επέκταση του $\mathbb{F}_q$ ώστε να περιέχει το $E[n]$. Η απάντηση δίνεται από τους R.Balasubramanian και N.Koblitz [BK98] στο επόμενο θεώρημα.

Θεώρημα 1.4.4. *Έστω $E/\mathbb{F}_q$ και n πρώτος ώστε $n \mid \#E(\mathbb{F}_q)$ και $n \nmid q-1$. Τότε $E[n]\subseteq E(\mathbb{F}_{q^k})$ αν $n \mid q^k-1$.*

Απόδειξη. [BK98 Theorem 1] και Θεώρημα 1.3.1. ⊣

Οι προϋποθέσεις του Θεωρήματος 1.4.4 αποτελούν πολύ συχνά κριτήριο επιλογής παραμέτρων κατά το Setup ένός σχήματος στην κρυπτογραφία ζευγμάτων, όπως θα δούμε στο κεφάλαιο 2.

Το τροποποιημένο ζεύγμα Weil. Έστω ελλειπτική καμπύλη $E/\mathbb{F}_q$, $q=p^r$ και $n\neq p$ πρώτος. Έστω επίσης ότι για υπάρχει παραμορφωτική απεικόνιση ϕ ως προς κάθε $P\in E(\mathbb{F}_q)[n]\backslash\{\mathcal{O}\}$. Τότε το *τροποποιημένο ζεύγμα Weil* (*modified Weil pairing*) ορίζεται ως

$$e_n^{\phi}(P,Q) = e_n(P,\phi(Q)).$$

Όπως και στην περίπτωση του ζεύγματος Tate, καταλήγουμε στο ακόλουθο θεώρημα:

Θεώρημα 1.4.5. *Έστω $E/\mathbb{F}_q$, n πρώτος και $P\in E(\mathbb{F}_q)[n]$. Αν ορίζεται το τροποποιημένο ζεύγμα Weil στην καμπύλη E, τότε*

$$e_n^{\phi}(P,P)\neq 1.$$

Απόδειξη. Καθώς το σύνολο $\{P, \phi(P)\}$ είναι βάση της ομάδας $E[n]$, έχουμε ότι για τυχαίο $R \in E[n]$ υπάρχουν $\lambda, \mu \in \{0, \ldots, n-1\}$ ώστε $R = [\lambda]P + [\mu]\phi(P)$. Επομένως

$$e_n(P, R) = e_n(P, [\lambda]P + [\mu]\phi(P)) = e_n(P, P)^{\lambda} \cdot e_n(P, \phi(P))^{\mu} \overset{1.4.3.(iii)}{=} e_n^{\phi}(P, P)^{\mu}.$$

Από το αυθαίρετο της επιλογής του σημείου R, προκύπτει ότι αν $e_n^{\phi}(P, P)^{\mu} = 1$, τότε η e_n είναι εκφυλιστική, άτοπο.

$\dashv$

Είναι προφανές με την έως τώρα ανάλυση ότι η απεικόνιση ίχνους μπορεί να χρησιμοποιηθεί και για το ζεύγμα Weil.

Υπολογισμός του ζεύγματος Weil. Το 1986, ο V.Miller [Mil86] παρουσίασε έναν αλγόριθμο ο οποίος με είσοδο μια αλγεβρική καμπύλη C γένους g, σημείο $P \in C$ και διαιρέτη D μηδενικού βαθμού, επιστρέφει ως έξοδο ρητή συνάρτηση f ώστε $div(f) = D + g(P) - D'$, όπου D' διαιρέτης βαθμού g και $D' = g(P)$ ανν ο D είναι κύριος. Η πρώτη εφαρμογή του αλγορίθμου ήταν ο υπολογισμός του ζεύγματος Weil για ελλειπτικές καμπύλες όπου $g = 1$.

Για $P, Q \in E[n]$, $Q \neq P$ [1], επιλέγονται $S, T \in E$ ώστε τα $P, P+S, Q, Q+T$ να είναι διαφορετικά μεταξύ τους. Θέτουμε διαιρέτες $D_P = (P+S) - (S)$ και $D_Q = (Q+T) - (T)$. Έστωσαν $f_{n,P}$, $f_{n,Q}$ ώστε $div(f_{n,P}) = n(P+S) - n(S)$ και $div(f_{n,Q}) = n(Q+T) - n(T)$. Το ζεύγμα Weil υπολογίζεται ως

$$e_n(P, Q) = \frac{f_{n,P}(D_Q)}{f_{n,Q}(D_P)} = \frac{f_{n,P}((Q+T) - (T))}{f_{n,Q}((P+S) - (S))} = \frac{f_{n,P}(Q+T) f_{n,Q}(S)}{f_{n,Q}(P+S) f_{n,P}(T)}.$$

Για τον υπολογισμό του $f_{n,P}(D_Q)$ δημιουργείται αθροιστική αλυσίδα, εξαρτώμενη από τη δυαδική αναπαράσταση του n, από συναρτήσεις $(f_{i,P})_{i \in [t]}$ ώστε

$$(\forall i \leqslant t) : div(f_{i,P}) = i(P+S) - i(S) - ([i]P) + (\mathcal{O}),$$

οι οποίες πληρούν την ιδιότητα (ii) του Λήμματος 1.3.10. Αφού $P \in E[n]$, προκύπτει ότι $div(f_{n,P}) = n(P) - n(\mathcal{O}) = nD_P$. Για τη συνάρτηση εκκίνησης f_1 ισχύει ότι

$$f_{1,P}(D_Q) = \frac{v(Q+T)}{l(Q+T)} \cdot \frac{l(T)}{v(T)},$$

όπου l, v οι ευθείες που χρησιμοιούνται στο άθροισμα $P + S$. Οι ενδιάμεσες τιμές $f_{i,P}(D_Q)$ υπολογίζονται όπως φαίνεται από τον ακόλουθο αλγόριθμο:

[1] για $P = Q$ τετριμμένα ισχύει $e_n(P, Q) = 1$

Ο αλγόριθμος Miller για το ζεύγμα Weil
Είσοδος: $P, Q, \in E[n]$, $S, T \in E$.
Έξοδος: $f_{n,P}(n(Q+T) - n(T))$, όπου $div(f_{n,P}) = n(P+S) - n(S)$.
1. Υπόλογισε τις ευθείες l, v του αθροίσματος $P + S$.
2. $R \longleftarrow P$, $f \longleftarrow \frac{v(Q+T)}{l(Q+T)} \cdot \frac{l(T)}{v(T)}$, $f_1 \longleftarrow f$.
3. $m \longleftarrow \lfloor log(n) - 1 \rfloor$.
4. **Όσο** $m \geqslant 0$:
5. Υπόλογισε τις ευθείες l, v του αθροίσματος $R + R = [2]R$.
6. $R \longleftarrow [2]R$.
7. $f \longleftarrow f^2 \cdot \frac{l(Q+T)}{v(Q+T)} \cdot \frac{v(T)}{l(T)}$.
8. **Εάν** το m-οστό bit του n είναι 0 **τότε**:
9. Υπολόγισε τις ευθείες l, v του αθροίσματος $R + P$.
10. $R \longleftarrow R + P$.
11. $f \longleftarrow f \cdot f_1 \cdot \frac{l(Q+T)}{v(Q+T)} \cdot \frac{v(T)}{l(T)}$.
12. $m \longleftarrow m - 1$.
13. **Επίστρεψε** f.

Ανάλογα υπολογίζουμε και την τιμή $f_{n,Q}(D_P)$.

1.5 Χρονική Πολυπλοκότητα και Βελτιώσεις

Παρατηρώντας τους αλγορίθμους που παρουσιάστηκαν στις ενότητες 1.4 και 1.5, γίνεται εμφανές ότι το ζεύγμα Tate υπερτερεί του ζεύγματος Weil από άποψη ταχύτητας υπολογισμού. Πιο συγεκριμένα, ο αλγόριθμος Miller εκτελείται δύο φορές για το ζεύγμα Weil, καθώς απαιτείται η εύρεση δύο κατάλληλων ρητών συναρτήσεων. Αυτό αποδεικνύεται και μαθηματικά, αφού συχνά η διγραμμική απεικονίση Weil υπολογίζεται από τη σχέση

$$e_n(P, Q) = \frac{\langle P, Q \rangle_n}{\langle Q, P \rangle_n},$$

όπου η $\langle , \rangle_n$ για ζεύγος $(Q, P) \in E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_q)[n]$ ορίζεται παρόμοια με τον Ορισμό 1.3.3. Συνεπώς, ο αναμενόμενος χρόνος εκτέλεσης είναι περίπου διπλάσιος από ότι για το ζεύγμα Tate, για δεδομένη καμπύλη E και ακέραιο n. Οι S.Galbraith, K.Harrison και D.Soldera [GHS02] επισημαίνουν πως η διαφορά είναι ακόμη μεγαλύτερη λόγω του περισσότερου χρόνου που χρειάζεται για τον υπολογισμό της τιμής $\langle Q, P \rangle_n$ από την $\langle P, Q \rangle_n$ (οι E.Brown, E.Errthum και D.Fu [BEF03]

εντοπίζουν πειραματική διαφορά $\approx 70\%$). Το μειονέκτημα του ζεύγματος Weil δεν μπορεί να αντισταθμιστεί ούτε από την επιπλέον ύψωση σε δύναμη που χρειάζεται για τον τελικό υπολογισμό του ζεύγματος Tate.

Μία άμεση βελτίωση της κλασικής μεθόδου υπολογισμού για το ζεύγμα Tate είναι η αντικατάσταση της f στον αλγόριθμο Miller από f_1, f_2 ώστε $f = f_1/f_2$. Ως αποτελέσμα, αποφεύγονται οι χρονοβόρες ενδιάμεσες διαιρέσεις. Στις γραμμές $8, 12$ οι f_1, f_2 υπολογίζονται χωριστά και η f προκύπτει από μία τελική διαίρεση. Οι P.Barretto κ.ά. [BKLS02], [BLS03a] απέδειξαν ότι για γραμμικώς ανεξάρτητα P, Q ισχύει

$$\langle P, Q\rangle_n^{\frac{q^k-1}{n}} = f(Q)^{\frac{q^k-1}{n}}.$$

Επομένως, οι ποσότητες $l(S), v(S)$ μπορούν να παραλειφθούν και οι γραμμές $8, 12$ να απλουστευτούν περισσότερο στις

$$8.\ f_1 = f_1^2 l(Q) \text{ και } f_2 = f_2^2 v(Q).$$

$$12.\ f_1 = f_1^2 l(Q) \text{ και } f_2 = f_2^2 v(Q).$$

Για περισσότερες λεπτομέρειες σχετικά με τα παραπάνω παραπέμπουμε στο [BSS05 §IX.14].

Καμπύλες κατάλληλες για ζεύγματα (*Pairing-friendly Curves*). Ο υπολογισμός ενός ζεύγματος είναι τις περισσότερες φορές η πιο επίπονη διαδικασία στις εφαρμογές της κρυπτογραφίας ζεύγμάτων. Η επιλογή μίας καμπύλης με παραμέτρους που την επιταχύνουν είναι αναμφισβήτητα το απαραίτητο πρώτο βήμα στην κατασκευή αποδοτικών σχημάτων. Αναφέρουμε εν συντομία κάποια γενικά κριτήρια για κάθε παράμετρο:

- Ο ακέραιος n πρέπει να είναι αρκετά μεγάλος ώστε το *πρόβλημα διακριτού λογαρίθμου σε ελλειπτική καμπύλη* (*ECDLP*) στις υποομάδες τάξης n της $E/\mathbb{F}_q$ όπου ορίζεται το ζεύγμα, να παραμένει δύσκολο για επιθέσεις μεθόδου Pollard-rho (βλέπε [Sti06 6.2.2]). Επιπλέον προτιμώνται ακέραιοι n χαμηλού βάρους Hamming ώστε να περιοριστούν οι προσθέσεις στο εσωτερικό του βρόγχου Miller.

- Οι επιθέσεις MOV/FR [MOV93], [FR94] ανάγουν το ECDLP σε ομάδα του πεδίου ορισμού του ζεύγματος στο *πρόβλημα διακριτού λογαρίθμου* (*DLP*) σε υποομάδα του πεδίου τιμών του. Επομένως, ο βαθμός εμβάπτισης k και το πλήθος στοιχείων q πρέπει να είναι αρκετά μεγάλα ώστε το DLP στην $\mathbb{F}_{q^k}$ να παραμένει δύσκολο για επιθέσεις μεθόδου Index Calculus (βλέπε [Sti06 6.2.4]). Εντούτοις, μικρές τιμές του k είναι αναγκαίες καθώς όλες οι πράξεις εκτελούνται στο $\mathbb{F}_{q^k}$, που είναι και το μικρότερο σώμα που περιέχει τις n-οστές

ρίζες της μονάδας. Ενδεικτικές τιμές για ασφάλεια 128-bit είναι $n \approx 2^{256}$ και $q^k \approx 2^{3072}$.

Οι πρώτες καμπύλες που χρησιμοποιήθηκαν στην κρυπτογραφία ζευγμάτων ήταν οι υπεριδιάζουσες ελλειπτικές καμπύλες εξαιτίας του μικρού βαθμού εμβάπτισής τους.

Θεώρημα 1.5.1. *Οι δυνατές τιμές του βαθμού εμβάπτισης μίας υπεριδιάζουσας ελλειπτικής καμπύλης είναι* $1, 2, 3, 4, 6$.

Απόδειξη. [MOV93 4.Table 1]. ⊣

Αρχικά τα πρωτόκολλα και σχήματα που παρουσιάστηκαν στηρίχθηκαν σε αυτήν την κατηγορία καμπυλών, αφού για τυχαία επιλεγμένη ελλειπτική καμπύλη και πρώτο p το ενδεχόμενο ο βαθμός εμβάπτισης να είναι μικρός είναι πολύ σπάνιο [BK98 Theorem 2]. Η ανάγκη όμως για μεγαλύτερη ασφάλεια και ταχύτερη υλοποίηση, οδήγησε τους ερευνητές να αναζητήσουν ειδικές συνήθεις ελλειπτικές καμπύλες αλλά και αλγεβρικές καμπύλες μεγαλύτερου γένους. Οι A.Miyaji, M.Nakabayashi και S.Takano [MNT01] κ.ά. με τη χρήση των CM-μεθόδων (βλ. [BSS99 §VIII]) για την κατασκευή καμπυλών δεδομένων γένους g και ίχνους t, πρότειναν τρόπους επιλογής συνήθων ελλειπτικών καμπυλών πρώτης τάξης με $k = 3, 4, 6$ και q πρώτο. Τα αποτελέσματά τους στηρίχθηκαν στο ακόλουθο θεώρημα, όπου διατυπώνονται τα γνωστά *MNT-κριτήρια*.

Θεώρημα 1.5.2. *Έστω συνήθης ελλειπτική καμπύλη* $E/\mathbb{F}_q$ *ώστε* $\#E(\mathbb{F}_q) = q + 1 - t$ *να είναι πρώτος. Τότε ο παρακάτω πίνακας περιέχει όλες τις δυνατές περιπτώσεις για τα ζεύγη τιμών* (q, t) *όταν* $k \in \{3, 4, 6\}$, $l \in \mathbb{Z}$.

k	q	t
3	$12l^2 - 1$	$-1 \pm 6l$
4	$l^2 + l + 1$	$-l$ ή $l + 1$
6	$4l^2 + 1$	$1 \pm 2l$

Πίνακας 1.2.

Απόδειξη. [MNT01 Theorems 2,3,4]. ⊣

Οι MNT-μέθοδοι γρήγορα γενικεύτηκαν για τιμές του k διάφορες των $3, 4, 6$ διατηρώντας το q πρώτο [DEM02], [BLS03b]. Οι μέθοδοι που προαναφέρθηκαν δέχονται ως είσοδο μία επιθυμητή τιμή για το k και ένα κάτω φράγμα r για την ύπαρξη υποομάδας τάξης πρώτου r και επιστρέφουν πρώτο q και καμπύλη $E/\mathbb{F}_q$ που πληρούν τις προϋποθέσεις. Οι καμπύλες που κατασκευάζονται υπόκεινται στον περιορισμό

$$\rho = log(q)/log(r) \leqslant 2 \Leftrightarrow r \leqslant \sqrt{q},$$

δημιουργώντας έτσι ένα σχετικά χαμηλό άνω φράγμα για την τάξη της υποομάδας. Όπως ήταν λογικό, η ελάττωση του λόγου ρ αποτέλεσε κεντρικό πεδίο έρευνας στην κρυπτογραφία τα ακόλουθα χρόνια. Ιδανικά θα θέλαμε επίσης η τάξη της καμπύλης να είναι πρωτός αριθμός, δηλαδή η ζητούμενη υποομάδα να είναι η ίδια η καμπύλη. Σπουδαία αποτελέσματα δόθηκαν από τους P.Barreto και M.Noehrig [BN05], οι οποίοι πρότειναν έναν απλό αλγόριθμο για κατασκευή ελλειπτικών καμπυλών πρώτης τάξης και $k = 12$. Οι *BN-καμπύλες*, όπως ονομάστηκαν, αποτελούν έως σήμερα από τις καλύτερες επιλογές στις εφαρμογές τόσο λόγω τις ταχύτητας υπολογισμού τους, όσο και των standard ασφαλείας που επιτυγχάνουν (βλ. §2.6). Επιπλέον, στο [BN05] αναλύεται μέθοδος που οδηγεί σε τιμές $\rho \approx r/(r-1)$, για $k = 2r$ και r πρώτο. Ιδιαίτερο ενδιαφέρον παρουσιάζει και η εργασία των D.Freeman, M.Scott και E.Teske [FST06] , όπου περιγράφονται και αξιολογούνται οι κυριότερες μέθοδοι που αναπτύθηκαν έως τότε για κατασκευή ελλειπτικών καμπυλών κατάλληλων για ζεύγματα, και προτείνονται καμπύλες με επιθυμητά χαρακτηριστικά για $k \leqslant 50$.

Μία επιστημονική διαμάχη, η οποία αφήνει ανοιχτά αρκετά ερωτήματα, είναι κατά πόσον η χρήση καμπυλών μεγαλύτερου γένους, και ιδιαιτέρως των υπερελλειπτικών καμπυλών, μπορεί να έχει εμφανή πλεονεκτήματα στις εφαρμογές. Μία *υπερελλειπτική καμπύλη* C γένους g είναι μια αλγεβρική καμπύλη με εξίσωση

$$C : y^2 + h(x)y = f(x),$$

όπου $h(x), f(x) \in \mathbb{F}_q[x]$ συνήθως επιλέγονται ώστε $deg(f(x)) = 2g + 1$ και $deg(h(x)) \leqslant g$. Παρατηρούμε ότι για $g = 1$ έχουμε την ειδική περίπτωση της ελλειπτικής καμπύλης. Οι προσθέσεις μεταξύ σημείων και μεταξύ διαιρετών μιας υπερελλειπτικής καμπύλης μπορούν να οριστούν καλώς, επομένως είναι δυνατή η ανάπτυξη υπερελλειπτικής κρυπτογραφίας ζεύγματος. Ένα από τα σπουδαιότερα πλεονέκτηματα είναι το μεγαλύτερο εύρος τιμών του βαθμού εμβάπτισης k μίας υπεριδιάζουσας υπερελλειπτικής καμπύλης (βλ. [Gal01 Definition 2] για τον ορισμό της υπεριδιάζουσας αλγεβρικής καμπύλης). Ο S.Galbraith [Gal01] προσδιόρισε ένα άνω φράγμα $k(g)$ για το k εξαρτώμενο μόνο από γένος της καμπύλης. Ενδεικτικές τιμές δίνονται στον επόμενο πίνακα.

g	1	2	3	4	5	6
$k(g)$	6	12	30	60	120	210

Πίνακας 1.3.

Εξάλλου, για την ομάδα κλάσεων διαιρετών της C ισχύει ότι $\#Pic^0_{\mathbb{F}_q}(C) \approx q^g$, άρα για να έχουμε ομάδα μεγέθους m bits αρκεί να χρησιμοποιήσουμε σώμα m/g bits. Εντούτοις στην πράξη, οι υπερελλειπτικές καμπύλες, αν και έχουν ενδιαφέρουσες

ιδιότητες, δεν ξεπερνούν γενικώς σε ταχύτητα υπολογισμού τις ελλειπτικές. Ο λόγος ρ που πλέον ορίζεται ως

$$\rho = log(q^g)/log(n) = glog(q)/log(n),$$

δεν έχει ακόμα προσεγγίσει τις τιμές που φτάνουν οι ελλειπτικές καμπύλες. Στο [KT08] επιτυγχάνεται $3 \leqslant \rho \leqslant 4$ για αυθαίρετη τιμή του k, ενώ στο [GV11] παρουσιάζονται οικογένειες καμπυλών με $2.25 \leqslant \rho \leqslant 4$, φράσσοντας όμως το $k \in [5, 35]$. Από όσο γνωρίζουμε, τιμές του $\rho < 2$ δεν έχουν γίνει ακόμη εφικτές. Αν συνυπολογίσουμε και την πληθώρα αποτελεσματικών τεχνικών που υπάρχουν για κατασκευή κατάλληλων ελλειπτικών καμπυλών, γίνεται κατανοητή η δυσπιστία της κρυπτογραφικής κοινότητας, τουλάχιστον με τα σημερινά δεδομένα, απέναντι στη χρήση υπερελλειπτικών καμπυλών. Μία πολύ κατατοπιστική σύγκριση και αξιολόγηση των πλεονεκτημάτων των ελλειπτικών και υπερελλειπτικών καμπυλών δίνεται στα πρακτικά των ομιλιών των S.Galbraith, F.Hess και F.Vercauteren [GHV07] στα πλαίσια του συνεδρίου PAIRING 2007. Διατυπώνονται επίσης σημαντικά ανοιχτά προβλήματα και παρατίθεται εκτενής σχετική βιβλιογραφία.

Το ζεύγμα Ate. Το 2006, οι F.Hess, N.Smart και F.Vercauteren [HSV06], ακολουθώτας τα βήματα των P.Barreto κ.ά. [BGhS04] στην αναζήτηση νέων μεθόδων υπολογισμού ζευγμάτων, εισήγαγαν το ζεύγμα Ate, περιορίζοντας το πεδίο ορισμού του ζεύγματος Tate σε ιδιοχώρους του ενδομορφισμού Frobenius.

Ορισμός 1.5.3. Έστω ελλειπτική καμπύλη $E/\mathbb{F}_q$, και n πρώτος $r \mid \#E(\mathbb{F}_q)$. Έστω επίσης $T = t - 1$, όπου t το ίχνος της E και $F_q : (x, y) \longmapsto (x^q, y^q)$ ο ενδομορφισμός Frobenius στην q-οστή δύναμη. Για $Q \in \mathbb{G}_2 = E[r] \cap Ker(F_q - [q])$, $P \in \mathbb{G}_1 = E[r] \cap Ker(F_q - [1]])$, δηλαδή $F_q(Q) = [q]Q$ και $F_q(P) = P$. Επιλέγουμε ρητή συνάρτηση $f_{T,Q}$ ώστε $div(f_{T,Q}) = T(Q) - ([T]Q) - (T - 1)(\mathcal{O})$. Το *ζεύγμα Ate* είναι η απεικόνιση

$$\mathbb{G}_2 \times \mathbb{G}_1 \longmapsto \mathbb{F}_{q^k}/(\mathbb{F}_{q^k})^r$$

$$a_r(Q, P) = f_{T,Q}(P).$$

Πρόταση 1.5.4. *Το ζεύγμα Ate ικανοποιεί τις εξής ιδιότητες:*

(i). Η a_r είναι διγραμμική.

(ii). Αν k ο βαθμός εμβάπτισης της E, $N = gcd(T^k - 1, q^k - 1)$ και $T^k - 1 = mN$, τότε

$$(\langle Q, P \rangle_r)^m = a_n(Q, P)^{c(q^k-1)/N},$$

όπου $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \, mod \, (r)$.

(iii). Αν $r \nmid m$, τότε η a_r είναι μη εκφυλιστική.

Απόδειξη. [HSV06] Theorem 1. ⊣

Από την 1.5.4.(ii) εξάγουμε το *ανηγμένο ζεύγμα Ate*, $\hat{a}_r = a_r(Q,P)^{(q^k-1)/r} \in U_r$. Παράλληλα ορίζεται και μία διαφορετική εκδοχή του ζεύγματος Ate, το *συνεστραμμένο ζεύγμα Ate* (*twisted Ate pairing*). Η ονομασία προέρχεται από μία ειδική κατηγορία ισομορφισμών μεταξύ μιας ελλειπτικής καμπύλης E' υπεράνω ελαχιστικής ως προς το βαθμό επέκτασης του σώματος $\mathbb{F}_q$ και της E που καλούνται *twists* και επιτρέπουν το σημείο Q να ληφθεί από μια διαφορετική υποομάδα της E, αποδοτικότερα αναπαραστάσιμη από την $\mathbb{G}_2$.

Παρατηρούμε ότι ο χρόνος εκτέλεσης Miller των δύο ζευγμάτων εξαρτάται πλέον από το ίχνος $t = q + 1 - \#E(\mathbb{F}_q)$ της καμπύλης, το οποίο δεν τυγχάνει πάντα μικρό. Ένα κάτω φράγμα για το πλήθος εκτελέσεων του βρόγχου Miller είναι το $log(r)/\phi(k)$, όπου $\phi(k)$ ο βαθμός του k-οστού κυκλοτομικού πολυωνύμου

$$\Phi_k(x) = \prod_{u_k \epsilon U_k} (x - u_k).$$

Καμπύλες στις οποίες το ζεύγμα Ate υπολογίζεται κοντά σε αυτό το φράγμα έχουν ίχνος $t = r^{1/\phi(k)}$ και κάποιες μπορούν να βρεθούν στα [BLS03b], [DCC05] . Τα αντίστοιχα ζεύγματα που προκύπτουν ονομάστηκαν από τον F.Vercauteren *βέλτιστα* (*optimal*) [Ver10]. Στην ίδια εργασία δίνεται αλγόριθμος συστηματικής παραγωγής βέλτιστων Ate ζευγμάτων και η εφαρμογή του σε ευρεία λίστα κατάλληλων ελλειπτικών καμπυλών. Τα βέλτιστα ζεύγματα εμφανίζουν πειραματικά κορυφαίες επιδόσεις και ώθησαν ιδιαίτερα την πρόσφατη έρευνα (βλ. Πίνακας 1.4).

Σε σύντομο χρονικό διάστημα προτάθηκαν παραλλαγές πάνω στον αρχικό Ορισμό 1.5.4 με σκοπό να αντιμετωπιστούν κάποιες αδυναμίες που εμφανίζει. Οι S.Matsuda κ.ά. [MKHO07] πρότειναν τη θεώρηση ακεραίου $S \equiv q \bmod (m)$, $r \geqslant 5$, αντί του $T = t - 1$ και μια παρόμοια αλλαγή στον ορισμό του συνεστραμμένου ζεύγματος Ate. Τα *βελτιστοποιημένα* (*optimised*) ζεύγματα που προκύπτουν υπολογίζονται τουλάχιστον όσο γρήγορα όσο το αντίστοιχο ζεύγμα Tate, ενώ φτανούν να είναι εώς δύο φορές ταχύτερα. Μια γενίκευση του ορισμού συμβαίνει αν λάβουμε $T_i = (t-1)^i \equiv q^i \bmod (r)$, $0 < i < k$, αντί για T, οπότε ορίζεται το *ζεύγμα Ate$_i$*: $a_{i,n}(Q,P) = f_{T_i,Q}(P)$ [ZZH07]. Το κέρδος είναι ότι το ζεύγμα Ate$_i$ μπορεί να υπολογιστεί επιτυγχάνοντας το βέλτιστο $T_i \approx r^{1/\phi(k)}$ σε περισσότερες οικογένειες κατάλληλων ελλειπτικών καμπυλών . Το πλεονέκτημα αυτό επαυξάνεται στην περαιτέρω γενίκευση του ζεύγματος Ate$_i$, το *ζεύγμα R-ate*, το οποίο ορίζεται αυστηρά στο [LLP08]. Ένας πιο απλός ορισμός που χρησιμοποιείται συνήθως στους υπολογισμούς είναι ο εξής:

$$R_{A,B}(Q,P) = f_{a,[B]Q}(P)^r \cdot f_{b,Q}(P) \cdot G_{aB,b,Q}(P),$$

όπου $A, B, a, b \in \mathbb{Z} : A = aB + b$ και $G_{aB,b,Q}$ ρητή συνάρτηση ώστε

$$div(G_{aB,b,Q}) = ([aB]Q) + ([b]Q) - ([aB+b]Q) - (\mathcal{O}).$$

Ισχύει ότι

$$\begin{aligned} div(f_{aB,Q}) &= (aB)(Q) - ([aB]Q) - (aB-1)(\mathcal{O}) = \\ &= a(B(Q) - ([B]Q) - (B-1)(\mathcal{O})) + \\ &\quad + (a([B]Q) - ([aB]Q) - (a-1)(\mathcal{O})) = \\ &= a \cdot div(f_{B,Q}) + div(f_{a,[B]Q}). \end{aligned}$$

Επομένως $f_{aB,Q} = f_{B,Q}^a \cdot f_{a,[B]Q}$ μέχρι σταθεράς, άρα

$$\begin{aligned} f_{A,Q}(P) = f_{aB+b,Q}(P) &= f_{aB,Q}(P) \cdot f_{b,Q}(P) \cdot G_{aB,b,Q}(P) = \\ &= f_{B,Q}^a(P) \cdot f_{a,[B]Q}(P) \cdot f_{b,Q}(P) \cdot G_{aB,b,Q}(P) = \\ &= f_{B,Q}(P)^a \cdot R_{A,B}(Q,P), \end{aligned}$$

όπου η δεύτερη ισότητα προκύπτει από το Λήμμα 1.3.10. Για $A = q^i$ και $B = r$ έχουμε ότι $T_i = (t-1)^i = b \bmod (r)$ άρα

$$\begin{aligned} f_{q^i,Q}(P) = f_{ar+b,Q}(P) = f_{ar,Q}(P) \cdot f_{b,Q}(P) = f_{r,Q}^a(P) \cdot f_{T_i,Q}(P) \Rightarrow \\ \Rightarrow a_r(Q,P) = R_{q^i,r}(Q,P). \end{aligned}$$

Πράγματι λοιπόν το ζεύγμα Ate_i αποτελεί ειδική περίπτωση του ζεύγματος R-ate. Τέλος, αξίζει να αναφέρουμε ότι ο ορισμός του ζεύγματος Ate επεκτείνεται σε υπερελλειπτικές καμπύλες όπου, όπως αποδεικνύεται στο [GHO+07], η εικόνα υπολογίζεται απευθείας στο U_n χωρίς να εκτελείται η συνήθης τελική ύψωση σε δύναμη. Αντίστοιχα ορίζεται και το *υπερελλειπτικό ζεύγμα R-ate*.

Παραλλαγές του ζεύγματος Weil. Το 2008, ο F.Hess [Hes08] εισήγαγε μία νέα οικογένεια ζευγμάτων η οποία σχετίζεται άμεσα με το ζεύγμα Weil. Στιγμιότυπα της οικογένειας αφήνουν υποσχέσεις για ακόμα αποδοτικότερες μεθόδους κατασκευής ζευγμάτων, αφού προσφέρονται για παράλληλο υπολογισμό.

Θεώρημα 1.5.5. *Έστω συνήθης ελλειπτική καμπύλη $E/\mathbb{F}_q$ με $k \geqslant 2$ και $r \geqslant 5$ πρώτος παράγοντας της $\#E(\mathbb{F}_q)$ Θεωρούμε πρωταρχική k-οστή ρίζα $s \equiv 1 \, mod(r^2)$, $h(x) = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x] : h(S) \equiv 0 \, mod(r)$, $R \in E(\mathbb{F}_{q^k})[r]$ και τη μοναδική μονική ρητή συνάρτηση $f_{s,h,R}$, ώστε*

$$(f_{s,h,R}) = \sum_{i=0}^{d} h_i(([s^i]R) - (\mathcal{O})).$$

Εάν $k \mid \#Aut(E)$, *τότε υπάρχει* $w \in \mathbb{F}_q \cap U_{\epsilon.\kappa.\pi.(2,k)}$ *ώστε η απεικόνιση*

$$E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] \longmapsto U_r.$$
$$e_{s,h}(P,Q) = w \cdot \frac{f_{s,h,P}(Q)}{f_{s,h,Q}(P)},$$

να είναι διγραμμική. Επιπλέον, $e_{r,s,h}$ *είναι μη εκφυλιστική αν* $h(s) \not\equiv 0 \ mod(r^2)$. *Ισχύει ότι*

$$e_{r,s,h}(P,Q) = e_r(P,Q)^{h(s)/r}.$$

Απόδειξη. [Hes08 Theorem 1]. ⊣

Πρόσφατα, οι D.Aranha κ.ά. [AKMRH11], επιλέγοντας παραμέτρους προσαρμοσένες σε BN-καμπύλες και $h_\alpha(x) = (2z+1) + (6z^2+2z)x$, $h_\beta(x) = (6z+2) + x - x^2 + x^3$, $z \in \mathbb{Z}$, όρισαν τα ζεύγματα α *Weil* και β *Weil* και έδειξαν ότι υπερτερούν σε ταχύτητα των βέλτιστων ζευγμάτων Ate σε υλοποιήσεις με εκτέλεση 8 threads ανά πυρήνα. Το γεγονός αυτό σε συνδυασμό με την τάση προς μεθόδους παράλληλου υπολογισμού των ζευγμάτων καθιστά πιθανή την έξοδο του ζεύγματος Weil από το ερευνητικό περιθώριο που είχε βρεθεί, καθώς οι περισσότεροι μελετητές είχαν επικεντρωθεί σε τεχνικές που αφορούσαν το ζεύγμα Ate και τις παραλλαγές του.

Ολοκληρώνουμε την ενότητα παραθέτοντας κάποιες από τις κορυφαίες επιδόσεις υπολογισμού ζευγμάτων που σημειώθηκαν τα τελευταία χρόνια. Για όλα τα αποτελεσμάτα έχουν επιλεχθεί BN-καμπύλες που πλήρουν τα standards ασφάλειας των 128-bits.

Εργασία	Είδος ζεύγματος	Κύκλοι υπολογισμού	Επεξεργαστής
[HMS08]	R-ate	10^7	single core
[NNS10]	βέλτιστο Ate	4.38×10^6	single core
[BGDM$^+$10]	βέλτιστο Ate	2.33×10^6	single core
[AKL$^+$11]	βέλτιστο Ate	1.573×10^6	single core
[AKMRH11]	βέλτιστο Ate	1.107×10^6	8 threads/core
[AKMRH11]	α Weil	0.936×10^6	8 threads/core
[AKMRH11]	β Weil	0.84×10^6	8 threads/core

Πίνακας 1.4.

1.6 Σύνοψη Κεφαλαίου

Παραθέσαμε στοιχεία της θεωρίας ελλειπτικών καμπυλών και της θεωρίας διαιρετών που είναι απαραίτητα για τη διατύπωση των ορισμών και την απόδειξη

των ιδιοτήτων των ζευγμάτων Tate και Weil. Μελετήσαμε τροποποιήσεις τους που χρησιμοποιούνται στην κρυπτογραφία και τον αλγόριθμο Miller για τον υπολογισμό τους. Στη συνέχεια, σταθήκαμε σε κάποια βασικά σημεία που αφορούν στην χρονική πολυπλοκότητά του αλγορίθμου Miller και στα κριτήρια επιλογής μίας καμπύλης κατάλληλης για την κατασκευή ζευγμάτων. Αναφέραμε τα κυριότερα σχετικά αποτελέσματα μέχρι και την καθιέρωση των BN-καμπυλών. Εντέλει, περιγράψαμε τις παραλλαγές των ζευγμάτων Tate και Weil, Ate, R-Ate, α Weil και β Weil, παρέχοντας επιπλέον μία λίστα ορισμένων εκ των ταχύτερων χρόνων υπολογισμού τους.

Κεφάλαιο 2

Πρωτόκολλα, Σχήματα και Εργαλεία

Ζεύγματα εμφανίστηκαν πρώτη φορά σε εφαρμογές της κρυπτογραφίας το 1993, όταν οι A.Menezes, T.Okamoto και S.Vanstone [MOV93] έδειξαν ότι το ECDLP μπορεί μέσω του ζεύγματος Weil να αναχθεί σε πρόβλημα διακριτού λογαρίθμου (DLP) σε πεπερασμένα σώματα. Ένα χρόνο αργότερα, οι G.Frey και H.G.Rück [FR94] πρότειναν μία παρόμοια επίθεση χρησιμοποιώντας το ζεύγμα Tate. Για αρκετό καιρό, οι δύο παραπάνω μέθοδοι κρυπτανάλυσης ήταν τα μόνα δείγματα χρήσης των ζευγμάτων στην κρυπτογραφία, εν μέρει διότι απαιτούσαν μεγάλο χρόνο υπολογισμού για τα δεδομένα της εποχής. Η κατάσταση άλλαξε ριζικά το 2000, με τις εργασίες των R. Sakai, K. Ohgishi και M. Kasahara [SOK00] και του A.Joux [Jou00], οπότε και παρουσιάστηκαν σχήματα υπογραφής και πρωτόκολλα ανταλλαγής κλειδιού βασισμένα σε ζεύγματα. Ήταν η αρχή μιας εντατικής ερευνητικής δραστηριότητας μέχρι τα μέσα περίπου της περασμένης δεκαετίας, τα αποτελέσματα της οποίας έθεσαν τα θεμέλια της κρυπτογραφίας ζευγμάτων και αποτελούν μέχρι σήμερα κύρια σημεία αναφοράς για τους ερευνητές. Εξέχουσα θέση κατέχει το *Σχήμα Κρυπτογράφησης Βάσει Ταυτοτήτων* (*Identity-Based Encryption Scheme - IBE-Scheme*) των D.Boneh και M.Franklin [BF01] , το οποίο έδωσε πλήρη απάντηση στο επί χρόνια ανοιχτό ερώτημα ύπαρξης ένος τέτοιου αποδεειγμένα λειτουργικού σχήματος από τον [Sha85]. Στο κεφάλαιο περιγράφονται ορισμένα από τα βασικότερα πρωτόκολλα και σχήματα στην κρυπτογραφία ζευγμάτων, ακολουθώντας κυρίως τη ροή του [BSS05 §X], με αναφορές στη σχετική βιβλιογραφία όπου είναι αναγκαίο.

2.1 Τα ζεύγματα ως «μαύρα κουτιά»

Το προηγούμενο κεφάλαιο αφιερώθηκε σε θέματα που αφορούν στη φύση και τον υπολογισμό των κυριότερων ζευγμάτων που είναι γνωστά έως τώρα. Εντούτοις, υπάρχουν κάποια κοινά επιθυμητά χαρακτηριστικά τα οποία επιτρέπουν να αντιμετωπίζουμε σε επίπεδο εφαρμογής τα ζεύγματα μακροσκοπικά, δηλαδή ως απεικονίσεις μεταξύ ομάδων με συγκεκριμένες ιδιότητες, χωρίς να ενδιαφέρει η προέλευσή τους. Πιο συγκεκριμένα, περιορίζουμε το πεδίο ορισμού στο καρτεσιανό γινόμενο κυκλικών ομάδων τάξης r, $\langle P\rangle = \mathbb{G}_1 \times \mathbb{G}_2 = \langle Q\rangle$, όπου P, Q κατάλληλα επιλεγμένα σημεία της καμπύλης. Το πεδίο τιμών, όπως έχουμε δει, είναι οι r-οστές ρίζες της μονάδας του $\mathbb{F}_{q^k}$, όταν χρησιμοποιούμε το ζεύγμα Weil ή το ανηγμένο ζεύγμα Tate. Επιπλέον, εάν απαιτείται το ζεύγος (P, P) να μην απεικονίζεται στη μονάδα, τροποποιούμε τα ζεύγματα όπως στις ενότητες 1.3 και 1.4. Η ικανοποίηση των συνθηκών του Θεωρήματος 1.4.4, η δυνατότητα τροποποίησης των ζευγμάτων και πολλές μέθοδοι κατασκευής κατάλληλων ελλειπτικών καμπυλών προϋποθέτουν οι $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ να είναι πρώτης τάξης, κάτι που στο εξής θα εννοείται εκτός εάν δηλώνεται διαφορετικά. Τελικώς οδηγούμαστε στον ακόλουθο ορισμό:

Ορισμός 2.1.1. Έστω $\mathbb{G}_1, \mathbb{G}_2$ προσθετικές κυκλικές ομάδες τάξης r και $\mathbb{G}_T$ πολλαπλασιαστική κυκλική ομάδα τάξης r, όπου r πρώτος. Μία απεικόνιση

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

καλείται *ζεύγμα* (*pairing, bilinear map*) εάν ικανοποιεί τις εξής ιδιότητες:

(i). *Διγραμμικότητα*: για κάθε $P, P' \in \mathbb{G}_1$, $Q, Q' \in \mathbb{G}_2$

$$e(P + P', Q) = e(P, Q) \cdot e(P', Q),$$
$$e(P, Q + Q') = e(P, Q) \cdot e(P, Q').$$

(ii). *Μη εκφυλισμός*: αν P, Q είναι γεννήτορες των $\mathbb{G}_1, \mathbb{G}_2$ αντίστοιχα τότε

$$e(P, Q) \neq 1.$$

(iii). Η e_r υπολογίζεται αποδοτικά.

Από την 2.1.1.(i) έχουμε ότι $e([\alpha]P, [\beta]Q) = e(P, Q)^{\alpha\beta}$, ενώ από την 2.1.1.(ii) και αφού $\#\mathbb{G}_T = r$, η εικόνα $e(P, Q)$ είναι γεννήτορας της $\mathbb{G}_T$. Εάν $\mathbb{G}_1 = \mathbb{G}_2$ το ζεύγμα καλείται *συμμετρικό*, διαφορετικά καλείται *ασύμμετρο*. Τα συμμετρικά ζεύγματα υπολογίζονται σε υπεριδιάζουσες καμπύλες μέσω παραμορφωτικών απεικονίσεων, ενώ τα ασύμμετρα σε συνήθεις. Τα ασύμμετρα ζεύγματα χωρίζονται σε δύο υποκατηγορίες, ανάλογα με το αν υπάρχει αποδοτικά υπολογίσιμος ισομορφισμός μεταξύ των $\mathbb{G}_2$ και $\mathbb{G}_1$. Συνεπώς μπορούμε να διακρίνουμε τρεις διαφορετικούς τύπους ζευγμάτων:

- *Τύπος 1.* $\mathbb{G}_1 = \mathbb{G}_2$.
- *Τύπος 2.* $\mathbb{G}_1 \neq \mathbb{G}_2$ και υπάρχει ισομορφισμός $\phi : \mathbb{G}_2 \longrightarrow \mathbb{G}_1$ που υπολογίζεται αποδοτικά.
- *Τύπος 3.* $\mathbb{G}_1 \neq \mathbb{G}_2$ και δεν υπάρχει ισομορφισμός $\phi : \mathbb{G}_2 \longrightarrow \mathbb{G}_1$ που υπολογίζεται αποδοτικά.

Για ένα ζεύγμα e Τύπου 2 θεωρούμε ότι δεν υπάρχει αποδοτικά υπολογίσιμος ισομορφισμός $\psi : \mathbb{G}_1 \longrightarrow \mathbb{G}_2$, διαφορετικά το e μπορεί να ερμηνευτεί ισοδύναμα ως το Τύπου 1 ζεύγμα $e' : (P, P') \longmapsto e(P, \psi(P'))$. Ως ισομορφισμός $\phi : \mathbb{G}_2 \longrightarrow \mathbb{G}_1$ μπορεί να ληφθεί η απεικόνιση ίχνους περιορισμένη στη $\mathbb{G}_2$. Παρατηρούμε ότι ένα ζεύγμα Τύπου 1 είναι μεταθετικό, δηλαδή $e(P, Q) = e(Q, P)$.

Η αφ' υψηλού θεώρηση των ζευγμάτων που προκύπτει από τον Ορισμό 2.1.1 παρακάμπτει τις αυστηρές μαθηματικές λεπτομέρειες, αλλά ταυτόχρονα κρύβει και πολλές ιδιαιτερότητες εξαρτώμενες από τα χαρακτηριστικά τους. Οι S.Galbraith, K.Paterson και N.Smart [GPS08] επισημαίνουν πως η ευκολία υπολογισμού, η σύντομη αναπαράσταση των στοιχείων των $\mathbb{G}_1, \mathbb{G}_2$ και η δυνατότητα hashing στις $\mathbb{G}_1, \mathbb{G}_2$ δεν είναι πάντα εφικτά σε όλους τους τύπους ζευγμάτων. Παραθέτουν επίσης συνοπτικά τον βαθμό δυσκολίας μιας σειράς σημαντικών τεχνικών ζητημάτων για κάθε τύπο ζεύγματος, για ασφάλεια 80 και 256 bits [GPS08 Table 3]. Γενικώς ισχύει ότι τα ασύμμετρα ζεύγματα σε επίπεδα ασφάλειας 256 bits έχουν σύντομες αναπαραστάσεις και εκτελέσεις αθροίσεων στις $\mathbb{G}_1, \mathbb{G}_2$, ενώ ειδικά τα ζεύγματα Τύπου 3 είναι υπολογίζονται ταχύτερα, κάτι που τα καθιστά προτιμότερα στις σύγχρονες εφαρμογές.

2.2 Προβλήματα βασισμένα σε ζεύγματα

Η ασφάλεια στην κρυπτογραφία ζευγμάτων βασίζεται σε υποθέσεις υπολογιστικής δυσκολίας κάποιων νέων προβλημάτων που ορίζονται πάνω στις ομάδες ορισμού ή τιμών ενός ζεύγματος. Τα περισσότερα από αυτά είναι επεκτάσεις του *υπολογιστικού προβλήματος Diffie Hellman* (*CDH*) και του *προβλήματος απόφασης Diffie Hellman* (*DDH*). Υπενθυμίζουμε κάποιες απαραίτητες έννοιες και συμβολισμούς.

Ορισμός 2.2.1. Μια συνάρτηση $\epsilon : \mathbb{N} \longrightarrow \mathbb{R}$ καλείται *αμελητέα* εάν

$$(\forall c \in \mathbb{N})(\exists n_c \ni \mathbb{N})(\forall n > n_c) : |\epsilon(n)| < \frac{1}{n^c}.$$

Περιγραφικά, λέμε ότι μία συνάρτηση ϵ είναι αμελητέα εάν $\epsilon(n) = o(\mathrm{Poly}(n))$. Ως *αντίπαλο* (*adversary*) καλούμε κάθε non-uniform πιθανοτικό αλγόριθμο πολυωνυμικού χρόνου (PPT), $\{\mathcal{A}_k\}_{k\in\mathbb{N}}$, όπου k η παράμετρος ασφάλειας του σχήματος. Συχνά, όταν η παράμετρος ασφάλειας υπονοείται, θα γράφουμε απλώς $\mathcal{A}$.

Ορισμός 2.2.2. Δύο οικογένειες τυχαίων μεταβλητών (τ.μ.) $\{U_n\}_{n\in\mathbb{N}}, \{V_n\}_{n\in\mathbb{N}}$ ονομάζονται *υπολογιστικά μη διακρίσιμες* (*computationally indistinguishable*), εάν για κάθε PPT αλγόριθμο D και κάθε πολυώνυμο p, υπάρχει x αρκετά μεγάλου μήκους ώστε

$$|\ \mathbf{Pr}[D(U_n) = 1] - \mathbf{Pr}[D(V_n) = 1]\ | < \frac{1}{p(n)}.$$

Σύμφωνα με τον Ορισμό 2.2.2, δύο μη διακρίσιμες οικογένειες τ.μ. επιβάλλουν αμελητέα διαφορά στην τελική απόφαση ενός PPT αλγορίθμου.

Ορισμός 2.2.3. Ένα υπολογιστικό πρόβλημα Π_f με ζητούμενο την τιμή της εικόνας $f(x_1, \ldots, x_n)$ θεωρείται *δύσκολο* εάν για κάθε αντίπαλο $\mathcal{A}$ υπάρχει αμελητέα συνάρτηση $\epsilon_{\mathcal{A}}$ ώστε

$$\mathbf{Pr}[\mathcal{A}(x_1, \ldots, x_n, 1^k) = f(x_1, \ldots, x_n)] \leqslant \epsilon_{\mathcal{A}}(k).$$

Ένα πρόβλημα απόφασης Π_R με ζητούμενο τον έλεγχο της σχέσης $R(x_1, \ldots, x_n)$ θεωρείται *δύσκολο* εάν οι είσοδοι $(x_1, \ldots, x_n) \in R$ και οι τυχαίες είσοδοι είναι μη διακρίσιμες οικογένειες τ.μ. ως προς την παράμετρο ασφάλειας k. Οι πιθανότητες λαμβάνονται πάνω σε όλες τις εισόδους και τις ρίψεις νομίσματος του $\mathcal{A}$.

Υπενθυμίζουμε τα παρακάτω καθιερωμένα προβλήματα της κρυπτογραφίας δημόσιου κλειδιού για πολλαπλαστικές[1] κυκλικές ομάδες τάξης n:

Πρόβλημα του διακριτού λογαρίθμου στην $\mathbb{G}$ (DLP($\mathbb{G}$)): δεδομένων γεννήτορα g και $g^x \in \mathbb{G}$ να υπολογιστεί το $x \in \mathbb{Z}_n$.

Υπολογιστικό πρόβλημα Diffie-Hellman στην $\mathbb{G}$ (CDH($\mathbb{G}$)): δεδομένων γεννήτορα g και $g^x, g^y \in \mathbb{G}$ να υπολογιστεί το $g^{xy} \in \mathbb{G}$.

Το πρόβλημα απόφασης Diffie-Hellman στην $\mathbb{G}$ (DDH($\mathbb{G}$)): δεδομένων γεννήτορα g και $g^x, g^y, u \in \mathbb{G}$ να αποφασιστεί εάν $u = g^{xy}$.

Είναι γνωστή η παρακάτω αλυσίδα πολυωνυμικών ($\leqslant_{\mathrm{P}}$) αναγωγών:

$$\mathrm{DDH}(\mathbb{G}) \leqslant_{\mathrm{P}} \mathrm{CDH}(\mathbb{G}) \leqslant_{\mathrm{P}} \mathrm{DLP}(\mathbb{G}).$$

Σύμφωνα με τον Ορισμό 2.2.3, η υπόθεση DDH($\mathbb{G}$) απαιτεί οι οικογένειες τ.μ.

$$\{(n, \mathbb{G}) \leftarrow \mathcal{G}(1^k); x, y \xleftarrow{\$} \mathbb{Z}_n : (g^x, g^y, g^{xy})\}_k \text{ και}$$
$$\{(n, \mathbb{G}) \leftarrow \mathcal{G}(1^k); x, y \xleftarrow{\$} \mathbb{Z}_n : (g^x, g^y, g^z)\}_k \quad ,$$

είναι μη διακρίσιμες. Ο συμβολισμός $\xleftarrow{\$}$ δηλώνει τυχαία επιλογή στοιχείων και η $\mathcal{G}$ είναι γεννήτρια της ομάδας $\mathbb{G}$, και άρα $\#\mathbb{G} = n = \mathrm{Poly}(k)$.

[1] Η επαναδιατύπωση των παραπάνω προβλημάτων για αθροιστικές υποομάδες πάνω σε ελλειπτικές καμπύλες γίνεται εύκολα με την βοήθεια του βαθμωτού γινομένου.

Στη συνέχεια παραθέτουμε τρία θεμελιώδη προβλήματα στην κρυπτογραφία ζευγμάτων και τις σχέσεις που υπάρχουν τόσο μεταξύ τους, όσο και με τα παραπάνω προβλήματα. Έστω ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$. Ορίζουμε τα εξής:

Υπολογιστικό Διγραμμικό Πρόβλημα Diffie-Hellman (*Computational Bilinear Diffie-Hellman - CBDH*)**:** δεδομένων γεννητόρων P, Q των $\mathbb{G}_1, \mathbb{G}_2$ αντίστοιχα και $[\alpha]P$, $[\beta]P$, $[\beta]Q$, $[\gamma]Q$, να υπολογιστεί το $e(P,Q)^{\alpha\beta\gamma} \in \mathbb{G}_T$.

Σημείωση. Το BCDHP($\mathbb{G}_1, \mathbb{G}_2$) ορίζεται συχνά σε συμμετρικά ζεύγματα για $P = Q$, οπότε ζητείται η τιμή $e_r(P,P)^{\alpha\beta\gamma}$.

Διγραμμικό πρόβλημα απόφασης Diffie-Hellman (*Decisional Bilinear Diffie-Hellman - DBDH*)**:** δεδομένων γεννητόρων P, Q των $\mathbb{G}_1, \mathbb{G}_2$ αντίστοιχα και $[\alpha]P$, $[\beta]P$, $[\beta]Q$, $[\gamma]Q$, $u \in \mathbb{G}_T$, να αποφασιστεί εάν $u = e(P,Q)^{\alpha\beta\gamma}$.

Το συζευκτικό πρόβλημα CDH (*co-CDH*)**:** δεδομένων γεννητόρων P, Q των $\mathbb{G}_1, \mathbb{G}_2$ αντίστοιχα και $[\alpha]P$, $[\beta]Q$, να υπολογιστεί το $[\alpha\beta]P \in \mathbb{G}_1$.

Πρόταση 2.2.4. *Ισχύουν οι εξής πολυωνυμικές και πιθανοτικές πολυωνυμικές* ($\leqslant_{\mathrm{RP}}$) *αναγωγές:*

(i). $DLP(\mathbb{G}_1) \leqslant_{\mathrm{RP}} DLP(\mathbb{G}_T)$ *και* $DLP(\mathbb{G}_2) \leqslant_{\mathrm{RP}} DLP(\mathbb{G}_T)$.

(ii). $DDH(\mathbb{G}_1) \leqslant_{\mathrm{P}} DBDH$, $DDH(\mathbb{G}_2) \leqslant_{\mathrm{RP}} DBDH$ *και* $DBDH \leqslant_{\mathrm{P}} DDH(\mathbb{G}_T)$.

(iii). $CBDH \leqslant_{\mathrm{P}} CDH(\mathbb{G}_1)$, $CBDH \leqslant_{\mathrm{P}} CDH(\mathbb{G}_2)$ *και* $CBDH \leqslant_{\mathrm{P}} CDH(\mathbb{G}_T)$.

(iv). $CBDH \leqslant_{\mathrm{P}}$ *co-CDH.*

(v). $DBDH \leqslant_{\mathrm{P}} CBDH$.

Απόδειξη. Θα αποδείξουμε τα (i),(iii). Ανάλογα αποδεικνύονται τα (ii),(iv),(v).

(i). Έστω PPT αλγόριθμος $\mathcal{A}_T$ για το DLP($\mathbb{G}_T$). Θεωρούμε τον αλγόριθμο $\mathcal{A}_1(P, S = [\alpha]P)$:

1. Διάλεξε τυχαίο γεννήτορα Q της $\mathbb{G}_2$.
2. $u \longleftarrow e(P,Q)$, $v \longleftarrow e(S,Q)$.
3. Επίστρεψε($\mathcal{A}_T(u,v)$).

Το u είναι γεννήτορας για την $\mathbb{G}_T$ και $v = u^{\alpha}$. Επομένως $\mathcal{A}_T(u,v) = \alpha$ και άρα ο $\mathcal{A}_1$ επιλύει το DLP($\mathbb{G}_1$). Όμοια δουλεύουμε για το DLP($\mathbb{G}_2$) (Αναγωγή MOV/Frey-Rück).

(iii). Έστω PPT αλγόριθμος $\mathcal{A}_T$ για το CDH($\mathbb{G}_T$). Θεωρούμε τον αλγόριθμο $\mathcal{A}(P, Q, S = [\alpha]P, R = [\beta]P, R' = [\beta]Q, T = [\gamma]Q)$:

1. $u \longleftarrow e(P,Q)$, $v \longleftarrow e(S,Q)$, $w \longleftarrow e(R,T)$.
2. Επίστρεψε($\mathcal{A}_T(u,v,w)$).

Ισχύει ότι $v = u^{\alpha}$, $w = u^{\beta\gamma}$, άρα $\mathcal{A}(P,Q,S,R,R',T) = e(P,Q)^{\alpha\beta\gamma}$, δηλαδή ο $\mathcal{A}_1$ επιλύει το DDH($\mathbb{G}_1$).

Εάν υπάρχει PPT αλγόριθμος $\mathcal{A}_1$ για το CDH($\mathbb{G}_1$), τότε υπολογίζουμε εύκολα

$$e(\mathcal{A}_1(P,S,R),T) = e([\alpha\beta]P,[\gamma]Q) = e(P,Q)^{\alpha\beta\gamma}.$$

Τέλος, δεδομένου PPT αλγορίθμου $\mathcal{A}_2$ για το CDH($\mathbb{G}_2$) μπορούμε να επιλύσουμε το CBDH από την εξίσωση

$$e(S,\mathcal{A}_2(Q,R',T)) = e([\alpha]P,[\beta\gamma]Q) = e(P,Q)^{\alpha\beta\gamma}.$$

$\dashv$

Ομάδες χάσματος Diffie-Hellman. Τα *προβλήματα χάσματος* (*gap problems*) είναι μία κατηγορία προβλημάτων που εισήγαγαν οι T.Okamoto και D.Pointcheval [OP01], όπου ζητείται η επίλυση ενός υπολογιστικού προβλήματος με τη βοήθεια ενός μαντείου για το αντίστοιχο πρόβλημα απόφασης. Ειδικότερα, για τα προβλήματα Diffie-Hellman ορίζεται το εξής νέο πρόβλημα.

Πρόβλημα χάσματος Diffie Hellman στην $\mathbb{G}$ (GDH($\mathbb{G}$)): δεδομένων γεννήτορα g και $g^x, g^y \in \mathbb{G}$ να υπολογιστεί το $g^{xy} \in \mathbb{G}$ με τη βοήθεια μαντείου DDH($\mathbb{G}$).

Είναι φανερό ότι το GDH($\mathbb{G}$) παρουσιάζει ενδιαφέρον σε ομάδες όπου το CDH($\mathbb{G}$) θεωρείται δύσκολο αλλά το DDH($\mathbb{G}$) είναι εύκολο. Ομάδες που έχουν αυτή την ιδιότητα ονομάζονται *ομάδες χάσματος Diffie-Hellman* (*GDH Groups*) και μπορούν να χρησιμοποιηθούν σε σχήματα υπογραφών όπως παρακάτω:

Σχήμα Υπογραφών GDH

Έστω ομάδα χάσματος Diffie-Hellman $\mathbb{G}$ και g ένας γεννήτοράς της. Έστω επίσης συνάρτηση hash $H : \{0,1\}^* \longrightarrow \mathbb{G}^*$. Για να στείλει ο A ένα τυχαίο μήνυμα $M \in \{0,1\}^*$ υπογεγραμμένο στον B εκτελούνται τα εξής βήματα:

1. Ο A επιλέγει μυστικό κλειδί $s \in \mathbb{Z}_n^*$ και υπολογίζει $m = H(M)$, την υπογραφή $\sigma = m^s$ και το δημόσιο κλειδί $h = g^s$. Αποστέλλει στον B την τριάδα (h, M, σ).

2. Ο B υπολογίζει $m = H(M)$ και αποδέχεται ανν DDH($\mathbb{G}$)$(g,h,m,\sigma) = 1$.

Η εγκυρότητα της υπογραφής αποδεικνύεται εύκολα αφού

$$h^{log_g(m)} = m^{log_g(h)} = m^s = \sigma.$$

Επιπλέον, CDH($\mathbb{G}$)$(g, h, m) = \sigma$, άρα η δυνατότητα πλαστογράφησης ανάγεται στη δυσκολία επίλυσης του CDH($\mathbb{G}$).

Στην επόμενη πρόταση αποδεικνύεται ότι οι ομάδες του πεδίου ορισμού ενός ζεύγματος μπορούν να θεωρηθούν υπό προϋποθέσεις ομάδες χάσματος Diffie-Hellman.

Πρόταση 2.2.5. *Έστω ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$. Το DDH($\mathbb{G}_1$) είναι εύκολο αν το e είναι Τύπου 1 και το DDH($\mathbb{G}_2$) είναι εύκολο αν το e είναι Τύπου 2.*

Απόδειξη. Αν το e είναι Τύπου 1, τότε για κάθε είσοδο $P, S = [\alpha]P, R = [\beta]P, T$ του DDH($\mathbb{G}_1$) ελέγχουμε σε πολυωνυμικό χρόνο ότι

$$[\alpha\beta]P = T \Leftrightarrow e(S, R) = e(P, T).$$

Επιπλέον, αν το e είναι Τύπου 2 και $\phi : \mathbb{G}_2 \longrightarrow \mathbb{G}_1$ αποδοτικός ισομορφισμός, τότε για κάθε είσοδο $Q, S = [\alpha]Q, R = [\beta]Q, T$ του DDH($\mathbb{G}_2$) πάλι σε πολυωνυμικό χρόνο ελέγχουμε ότι

$$[\alpha\beta]Q = T \Leftrightarrow e(\phi(S), R) = e(\phi(Q), T).$$

⊣

2.3 Το Μη Διαλογικό Σχημα Διανομής Κλειδιού Βάσει Ταυτοτήτων των Sakai-Ohgishi-Kasahara

Το 2000, οι R.Sakai, K.Ohgishi και M.Kasahara [SOK00], [SOK01] χρησιμοποίησαν ζεύγματα για να παράξουν σχήματα υπογραφής, διανομής κλειδιού και κρυπτογράφησης βάσει ταυτοτήτων. Το έργο τους αν και αρχικά παραγνωρισμένο, θεωρείται σήμερα η απαρχή της κρυπτογραφίας ζευγμάτων. Ειδικότερα το *Μη Διαλογικό Σχημα Διανομής Κλειδιού Βάσει Ταυτοτήτων* (*Identity-Based Non-Interactive Key Distribution Scheme - IB-NIKDS*) που θα περιγράψουμε υπήρξε σημαντική επιρροή για το πρότυπο σχήμα κρυπτογράφησης βάσει ταυτοτήτων των D.Boneh και M.Franklin [BF01] .

Στην κρυπτογραφία βάσει ταυτοτήτων (IBC), όπως την οραματίστηκε ο A.Shamir [Sha85], μία *Γεννήτρια Ιδιωτικών Κλειδιών* (*Private Keu Generator - PKG*) δημιουργεί τις παραμέτρους του συστήματος και κατέχει ένα μυστικό κλειδί μέσω του οποίου παράγει τα ιδιωτικά κλειδιά των χρηστών. Παράλληλα, τα δημόσια κλειδιά προκύπτουν από την ταυτότητα των χρηστών ή κάποιο άλλο προσωπικό τους στοιχείο. Στο SOK00 ID-Based NIKDS, η PKG δημιουργεί τις παραμέτρους

$(r, \mathbb{G}_1, \mathbb{G}_T, e)$ ενός συμμετρικού ζεύγματος $e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_T$ καθώς και μία συνάρτηση hash $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$ και επιλέγει μυστικό κλειδί $s \in \mathbb{Z}_r^*$. Το ιδιωτικό και δημόσιο κλειδί ενός χρήστη A με ταυτότητα ID_A είναι τα $sk_A = [s]H_1(ID_A)$, $pk_A = H_1(ID_A)$ αντίστοιχα. Ομοίως για χρήστη B έχουμε $sk_B = [s]H_1(ID_B)$, $pk_B = H_1(ID_B)$. Οι A, B συμφωνούν στο κοινό κλειδί

$$K_{AB} = e(sk_A, pk_B) = e([s]H_1(ID_A), H_1(ID_B)) = \\ = e(pk_A, sk_B) = e(H_1(ID_A), [s]H_1(ID_B)) = e(H_1(ID_A), H_1(ID_B))^s.$$

Εργαζόμενοι ανεξάρτητα, οι R.Dupont και A.Enge [DE02] επινόησαν ένα παρόμοιο σχήμα για ασύμμετρα ζεύγματα το οποίο γενικεύει το SOK00. Η απόδειξη ασφάλειας του DE02 προσαρμόζεται εύκολα στο SOK00 όπως στην επόμενη πρόταση:

Πρόταση 2.3.1. *Η ασφάλεια του SOK00 ID-Based NIKDS ανάγεται στη δυσκολία του CBDH.*

Απόδειξη. Έστω επιτιθέμενος E που μπορεί να παρακολουθεί τα κανάλια διανομής ιδιωτικών κλειδιών και έστω PPT αλγόριθμος $\mathcal{A}$ που επιλύει το BCDH. Ο E εξάγει από το κανάλι ζεύγος $(P, [s]P)$, και υπολογίζει το K_{AB} ως

$$\mathcal{A}(P, H_1(ID_A) = [x]P, [s]P, H_2(ID_B) = [y]P) = e(P,P)^{xsy} = K_{AB}.$$

⊣

Ένα ισχυρότερο αποτέλεσμα για την ασφάλεια του DE02 είναι ότι το σχήμα είναι ισοδύναμο με το CBDH [DP02 Proposition 1&Theorem 2]. Η απόδειξη γίνεται στο *μοντέλο τυχαίου μαντείου* (*random oracle model - ROM*) [BR93], όπου οι συναρτήσεις hash θεωρούνται τυχαίες με την έννοια ότι για κάθε όρισμα (ερώτημα) x η εικόνα (απάντηση) $H(x)$ επιλέγεται ανεξάρτητα και ομοιόμορφα από το πεδίο τιμών, παραμένοντας όμως σταθερή για μετέπειτα ερωτήματα x.

2.4 Το Τριμερές Πρωτόκολλο Ανταλλαγής Κλειδιού Ενός Γύρου του Joux

Πολύ κοντά χρονικά με τους R.Sakai, K.Ohgishi και M.Kasahara, ο A.Joux [Jou00] πρότεινε ένα πρωτόκολλο ανταλλαγής κλειδιού ενός γύρου που μπορεί να εκληφθεί ως το τριμερές ανάλογο του κλασικού πρωτοκόλλου Diffie-Hellman. Για να το πετύχει, εκμεταλλεύτηκε τη διγραμμικότητα του ζεύγματος Weil.

Έστω λοιπόν σύστημα με παραμέτρους $(r, \mathbb{G}_1, \mathbb{G}_T, e, P, Q)$, όπου P, Q γραμμικώς ανεξάρτητοι γεννήτορες της $\mathbb{G}_1 \cong \mathbb{Z}_r \oplus \mathbb{Z}_r$. Τρεις χρήστες του συστήματος A, B, C

που επιθυμούν να επικοινωνήσουν επιλέγουν τιμές $\alpha, \beta, \gamma \in \mathbb{Z}_r^*$ αντίστοιχα. Ο A αποστέλλει τα $([\alpha]P, [\alpha]Q)$ στους B, C και όμοια οι B, C αποστέλλουν τα $([\beta]P, [\beta]Q)$, $([\gamma]P, [\gamma]Q)$ στους άλλους δύο χρήστες. Και οι τρεις πλεύρες συμφωνούν στο κοινό κλειδί

$$K_{ABC} = e([\beta]P, [\gamma]Q)^{\alpha} = e([\alpha]P, [\gamma]Q)^{\beta} = e([\alpha]P, [\beta]Q)^{\gamma} = e(P, Q)^{\alpha\beta\gamma}.$$

Απαραίτητη προϋπόθεση για τη λειτουργία του πρωτοκόλλου είναι να ισχύει ότι $e(P, Q) \neq 1$, το οποίο εξασφαλίζεται από την ανεξαρτησία των P, Q. Ο E.Verheul [Ver01] στην εργασία που αναλύει τη μέθοδο τροποποίησης ζευγμάτων μέσω παραμορφωτικών απεικονίσεων, βελτίωνει το πρωτόκολλο Jou00 χρησιμοποιώντας μοναδικό γεννήτορα P σε τροποποιημένο ζεύγμα Weil, $\hat{e}$. Το αποτέλεσμα είναι να περιοριστούν οι απαιτήσεις σε bandwidth κατά το ήμισυ καθώς συνολικά αποστέλλονται μόνο τα $[\alpha]P, [\beta]P, [\gamma]P$. Το κοινό κλειδί είναι το $K_{ABC} = \hat{e}(P, P)^{\alpha\beta\gamma}$, όπου $\hat{e}(P, P) \neq 1$ από το Θεώρημα 1.4.4 .

Η ασφάλεια του συστήματος στηρίζεται στο CBDH, αφού κάθε επιτεθέμενος έχει στη διάθεσή του στιγμιότυπα του εν λόγω προβλήματος. Είναι εμφανές ότι το πρωτόκολλο Jou00, όπως και το πρωτόκολλο Diffie-Hellman, είναι ευάλωτο σε *επιθέσεις ενδιάμεσου προσώπου* (*man-in-the-middle attacks*) [GB08 11.1.5]. Πράγματι, ένας ενεργά συμμετέχων επιτιθέμενος μπορεί να επιλέξει $([\alpha]P, [\alpha]Q)$ και να συμφωνήσει σε κοινό κλειδί με τους B, C παραπλανώντας τους ότι είναι ο A. Οι S.Al-Riyami και K.Paterson [ARP02] αντιμετώπισαν αποτελεσματικά το πρόβλημα αποφεύγοντας τη χρήση υπογραφής για τις αποστελλόμενες τιμές και έδειξαν ότι η αυθεντικοποίηση του πρωτοκόλλου Jou00 στερεί οποιοδήποτε πλεονέκτημα έναντι των καθιερωμένων πρωτοκόλλων με MACs. Περαιτέρω αναφορές στη βιβλιογραφία βρίσκονται στο [BSS05 X.6.2].

2.5 Το Σχήμα Κρυπτογράφησης βάσει Ταυτοτήτων των Boneh-Franklin

Η εργασία των D.Boneh και M.Franklin [BF01] συνέβαλε, ίσως περισσότερο από οποιαδήποτε άλλη, στη ραγδαία ανάπτυξη της κρυπτογραφίας ζευγμάτων. Οι ιδέες στα [SOK00], [SOK01] στερούνται αυστηρής θεμελίωσης μοντέλων ασφάλειας, ενώ το πρωτόκολλο [Jou00] αντιμετωπίστηκε μάλλον σαν ενδιαφέρουσα παρατήρηση παρά σαν υποσχόμενη εφαρμογή. Αντίθετα, η δημοσίευση του πρώτου χρηστικού και αποδεδειγμένα ασφαλούς IBE-σχήματος [2] καθιέρωσε τα ζεύγματα ως εργαλείο της ασύμμετρης κρυπτογραφίας. Στο [BF01] αναπτύσσονται δύο IBE-σχήματα,

[2] Αργότερα αποκαλύπτηκε ότι ο C.Cocks [Coc01] εφηύρε ένα IBE-σχήμα εκτός της κρυπτογραφίας ζευγμάτων νωρίτερα του [BF01], χωρίς ωστόσο να το δημοσιεύσει πρώτος.

όπου το πρώτο σχήμα *BasicIdent* λειτουργεί ως βάση για το πλήρες από άποψη λειτουργικότητας και ασφάλειας δεύτερο σχήμα *FullIdent* .

Το IBE-σχήμα *BasicIdent*. Το σχήμα συνίσταται από τους αλγορίθμους $Setup$, $Extract, Encrypt, Decrypt$ ως εξής:

Setup(1^k)**:** όπως στην υποδομή του SOK00, η PKG με παράμετρο ασφάλειας k επιλέγει πρώτο r, μυστικό κλειδί $s \in \mathbb{Z}_r^*$ και παράγει ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_T$, όπου $\mathbb{G}_1 = \langle P \rangle$, $P_0 = [s]P$ και $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_T \longrightarrow \{0,1\}^n$ συναρτήσεις hash, όπου n το μήκος μηνυμάτων. Οι δημόσιες παράμετροι του συστήματος είναι οι $(r, \mathbb{G}_1, \mathbb{G}_T, e, n, P, P_0, H_1, H_2)$.

Extract(s, ID)**:** για τυχαία ταυτότητα $ID \in \{0,1\}^*$, υπολογίζεται το ιδιωτικό κλειδί $d_{ID} = [s]H_1(ID)$.

Encrypt(M, ID_A)**:** ο χρήστης B για να κρυπτογραφήσει μήνυμα M προς τον A, επιλέγει τυχαίο $t \in \mathbb{Z}_r^*$ και υπολογίζει το κρυπτοκείμενο

$$C = \langle [t]P, M \oplus H_2(e(H_1(ID_A), P_0)^t)) \rangle.$$

Decrypt(C, d_{ID_A})**:** ο A αποκρυπτογραφεί το $C = \langle U, V \rangle$ από τη σχέση

$$M = V \oplus H_2(e(d_{ID_A}, U)).$$

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος απαιτεί συνολικά δύο υπολογισμούς πάνω στο ζεύγμα e. Η ορθότητα του σχήματος παρέχεται απο τη διγραμμικότητα του e και τις ακόλουθες ισότητες.

$$\begin{aligned} V \oplus H_2(e(d_{ID_A}, U)) &= M \oplus H_2(e(H_1(ID_A), P_0)^t) \oplus H_2(e(d_{ID_A}, [t]P)) = \\ &= M \oplus H_2(e(H_1(ID_A), [s]P)^t) \oplus H_2(e([s]H_1(ID_A), [t]P)) = \\ &= M \oplus H_2(e(H_1(ID_A), P)^{st}) \oplus H_2(e(H_1(ID_A), P)^{st}) = M. \end{aligned}$$

Είναι εύκολο να δούμε σε περιγραφικό επίπεδο πως, όπως και στο πρωτόκολλο Joux00, εάν δεχτούμε το ROM, η ασφάλεια του BasicIdent εξαρτάται από τη δυσκολία του BCDHP$(\mathbb{G}_1, \mathbb{G}_2)$. Έχουμε ότι για κάποιο $x \in \mathbb{Z}_r^*$: $[s]H_1(ID_A) = [x]P$ και άρα ένας επιτιθέμενος που παρακολουθεί την κίνηση μεταξύ των χρηστών, όχι όμως και το κανάλι διανομής των ιδιωτικών κλειδιών, έχει στη διάθεσή του τα $P, [s]P, [t]P, [x]P$. Επομένως, αν μπορεί να υπολογίσει το $e(P,P)^{stx} = e(d_{ID_A}, U)$, αρκεί να θέσει στο μαντείο το ερώτημα $H_2(e(d_{ID_A}, U))$.

Για να διατυπώσουμε αυστηρότερα το παραπάνω, χρειαζόμαστε μοντέλα ασφάλειας προσαρμοσμένα στην κρυπτογραφια βάσει ταυτοτήτων. Ανακαλούμε πρώτα κάποιους απαραίτητους ορισμούς μοντέλων ασφάλειας για την κλασική κρυπτογραφία δημόσιου κλειδιού.

Ορισμός 2.5.1. Έστω σχήμα κρυπτογράφησης δημόσιου κλειδιού $\mathbf{C}= (\mathcal{G}, \mathcal{E}, \mathcal{D})$, όπου $\mathcal{G}$ η γεννήτρια ιδιωτικών και δημόσιων κλειδιών και $\mathcal{E}, \mathcal{D}$ οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης. Θεωρούμε το ακόλουθο παίγνιο μεταξύ του *προκαλούντος* (*challenger*) $\mathcal{C}$ και του αντιπάλου $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$:

Παίγνιο Μη Διακρισιμότητας (*Indistinguishability Game*)**:**

1. Ο $\mathcal{C}$ με παράμετρο ασφάλειας k εκτελεί τον $\mathcal{G}$ και εξάγει ζεύγος κλειδιών sk, pk.
2. Ο $\mathcal{A}$ εκτελεί τον $\mathcal{A}_1$ με είσοδο pk και επιστρέφει μηνύματα M_0, M_1 και πληροφορία s.
3. Ο $\mathcal{C}$ επιλέγει τυχαίο bit $b \in \{0, 1\}$ και υπολογίζει το κρυπτοκείμενο
$$C = \mathcal{E}(M_b, pk).$$
4. Ο $\mathcal{A}$ εκτελεί τον $\mathcal{A}_2$ με είσοδο (C, pk, s) και επιστρέφει bit $b' \in \{0, 1\}$.

Ο $\mathcal{A}$ κερδίζει αν $b' = b$. Ως πλεονέκτημα του $\mathcal{A}$ στο παίγνιο μη διακρισιμότητας ορίζεται η ποσότητα

$$Adv_{\mathcal{A}}^{IND} = \mid \mathbf{Pr}[b' = b] - \frac{1}{2} \mid .$$

Εάν ο αντίπαλος $\mathcal{A}$ δεν έχει πρόσβαση σε *μαντείο αποκρυπτογράφησης* (*decryption oracle*) τότε λέμε ότι εκτελεί *επίθεση επιλογής μηνυμάτων* (*chosen plaintext attack - CPA*). Εάν μόνο ο $\mathcal{A}_1$ έχει πρόσβαση σε μαντείο αποκρυπτογράφησης τότε ο $\mathcal{A}$ εκτελεί *επίθεση μη προσαρμοσμένης επιλογής κρυπτοκειμένων* (*non-adaptive chosen plaintext attack - CCA1*). Τέλος, εαν και οι δύο αλγόριθμοι $\mathcal{A}_1, \mathcal{A}_2$ έχουν πρόσβαση σε μαντείο αποκρυπτογράφησης, τότε ο $\mathcal{A}$ εκτελεί *επίθεση προσαρμοσμένης επιλογής κρυπτοκειμένων* (*adaptive chosen plaintext attack - CCA2*). Στην τελευταία περίπτωση, δεν επιτρέπεται στον $\mathcal{A}$ να θέσει ερώτημα αποκρυπτογράφησης για το κρυπτοκείμενο πρόκλησης C.

Ορισμός 2.5.2. Το σχήμα κρυπτογράφησης δημοσίου κλειδιού $\mathbf{C}= (\mathcal{G}, \mathcal{E}, \mathcal{D})$ έχει *ασφάλεια IND-CPA/CCA1/CCA2* εάν δεν υπάρχει αντίπαλος που κερδίζει το παίγνιο μη διακρισιμότητας με μη αμελητέο πλεονέκτημα εκτελώντας αντίστοιχα CPA/CCA1/CCA2.

Είναι φανερό ότι το πιο ισχυρό επίπεδο ασφάλειας παρέχεται από το μοντέλο IND-CCA2, το οποίο αποτελεί το πλέον αποδεκτό standard ασφάλειας. Το IND-CCA2 αποδεικνύεται ισοδύναμο με τα μοντέλα SS-CCA2 και NM-CCA2 που ορίζονται μέσω δύο διαφορετικών προσεγγίσεων της ασφάλειας κρυπτοσυστημάτων, της (*semantic*) και της (*non-malleable*) ασφάλειας, που όμως δε θα επεκταθούμε περαιτέρω (βλ. [BDPR98], [WSI03]).

Στην κρυπτογραφία βάσει ταυτοτήτων, ένα IBE-σχήμα μοντελοποιείται από μία τετράδα $\mathbf{C}_{IB}= (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$, όπου $\mathcal{G}$ η γεννήτρια των παραμέτρων του συστήματος, $\mathcal{X}$ ο αλγόριθμος εξαγωγής ιδιωτικού κλειδιού και $\mathcal{E}, \mathcal{D}$ οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης, όπως οι Setup ,Extact, Encrypt, Decrypt στο Basic-Ident. Στο [BF01] ορίζεται ένα καινούργιο παίγνιο που αποτυπώνει ένα ρεαλιστικά σενάριο επίθεσης για το $\mathbf{C}_{IB}$.

Ορισμός 2.5.3. Έστω IBE-σχήμα $\mathbf{C}_{IB}= (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$. Θεωρούμε το ακόλουθο παίγνιο μεταξύ του προκαλούντος $\mathcal{C}$ και του αντιπάλου $\mathcal{A}$:

Παίγνιο Μη Διακρισιμότητας Επιθέσεως Επιλεγμένων Κρυπτοκειμένων Βάσει Ταυτοτήτων (*Indistinguishability under Identity-Based Chosen Ciphertext Attack - IND-ID-CCA*)**:**

1. **Setup:** ο $\mathcal{C}$ επιλέγει παράμετρο ασφάλειας k και εκτελεί τον $\mathcal{S}$ δημιουργώντας τις δημόσιες παραμέτρους, τις οποίες δίνει στον $\mathcal{A}$, και το κύριο κλειδί s που κρατά μυστικό.

2. **Φάση 1:** ο $\mathcal{A}$ θέτει ερωτήματα $q_1, \ldots, q_m$ όπου το q_i μπορεί να είναι:

   - *Ερώτημα εξαγωγής ιδιωτικού κλειδιού* $\langle ID_i \rangle$: ο $\mathcal{C}$ εκτελεί τον $\mathcal{X}$ και απαντά αποστέλλοντας το αντίστοιχο ιδιωτικό κλειδί d_i στον $\mathcal{A}$.
   - *Ερώτημα αποκρυπτογράφησης* $\langle ID_i, C_i \rangle$: ο $\mathcal{C}$ εκτελεί τους $\mathcal{X}, \mathcal{D}$ για να αποκρυπτογραφήσει το κρυπτοκείμενο C_i με το ιδιωτικό κλειδί d_i και απαντά αποστέλλοντας το αντίστοιχο μήνυμα.

   Το ερώτημα q_i μπορεί να τίθεται προσαρμοσμένο στις απαντήσεις των $q_1, \ldots, q_{i-1}$.

3. **Πρόκληση:** ο $\mathcal{A}$ επιλέγει ταυτότητα $ID \notin \{ID_1, \ldots, ID_m\}$ και μηνύματα M_0, M_1 και τα αποστέλλει στον $\mathcal{C}$. Ο $\mathcal{C}$ επιλέγει τυχαίο bit $b \in \{0, 1\}$ και υπολογίζει το κρυπτοκείμενο $C = \mathcal{E}(M_b, ID)$, με το οποίο προκαλεί τον $\mathcal{A}$.

4. **Φάση 2:** ο $\mathcal{A}$ θέτει νέα ερωτήματα $q_{m+1}, \ldots, q_n$ όπως στη Φάση 1 με τον περιορισμό $\langle ID_i \rangle \neq ID$ και $\langle ID_i, C_i \rangle \neq \langle ID, C \rangle$.

5. **Απόκριση:** ο $\mathcal{A}$ μαντεύει bit $b' \in \{0, 1\}$ και κερδίζει αν $b' = b$.

Ως πλεονέκτημα του $\mathcal{A}$ ορίζεται η ποσότητα

$$Adv_{\mathcal{A}}^{ID-CCA} = | \mathbf{Pr}[b' = b] - \frac{1}{2} | .$$

Το κρυπτοσύστημα $\mathbf{C}_{IB}$ έχει *ασφάλεια IND-ID-CCA* εάν δεν υπάρχει αντίπαλος που κερδίζει το παίγνιο IND-ID-CCA με μη αμελητέο πλεονέκτημα. Εάν το $\mathbf{C}_{IB}$ αντιστέκεται σε αντιπάλους που δεν έχουν τη δυνατότητα να θέτουν ερωτήματα αποκρυπτογράφησης, τότε λέμε ότι το $\mathbf{C}_{IB}$ έχει *ασφάλεια IND-ID-CPA*.

Τα μοντέλα ασφάλειας IND-ID-CPA και IND-ID-CCA επεκτείνουν φυσικά τα μοντέλα IND-CPA και IND-CCA2 αντίστοιχα. Για το σχήμα BasicIdent ισχύει το ακόλουθο θεώρημα.

Θεώρημα 2.5.4. *Έστω ότι οι H_1, H_2 είναι τυχαία μαντεία. Αν το σχήμα BasicIdent δεν έχει ασφάλεια IND-ID-CPA, τότε υπάρχει PPT αλγόριθμος $\mathcal{B}$ που επιλύει το CBDH με μη αμελητέο πλεονέκτημα.*

Απόδειξη. [BF03 Theorem 4.1]. ⊣

Το IBE-σχήμα FullIdent. Είναι λογικό να θεωρήσουμε ότι το BasicIdent απέχει από τα επιθυμητά επίπεδα ασφάλειας. Για αυτό το λόγο μετατρέπεται στο σχήμα FullIdent ακολουθώντας την *τεχνική υβριδικής κρυπτογράφησης Fujisaki-Okamoto* [FO99] ώστε να επιτευχθεί ασφάλεια IND-ID-CCA υποθέτοντας τη δυσκολία του CBDH.

Θεώρημα 2.5.5. *Έστω κρυπτοσύστημα δημοσίου κλειδιού $\boldsymbol{C}_{Pub} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$. Με $\mathcal{E}_{pk}(M; r)$ συμβολίζουμε την κρυπτογράφηση του μηνύματος M υπό το δημόσιο κλειδί pk όταν ο αλγόριθμος $\mathcal{E}$ χρησιμοποιεί τα τυχαία bits r. Έστω επίσης σχήμα $\boldsymbol{C}^{Hyb}_{Pub}$ όπου η κρυπτογράφηση του M ορίζεται ως*

$$\mathcal{E}^{Hyb}_{pk}(M) = \langle \mathcal{E}_{pk}(\sigma; H(\sigma, M)), G(\sigma) \oplus M \rangle,$$

όπου σ κατάλληλο τυχαίο string και H, G κατάλληλες τυχαίες συναρτήσεις hash. Αν το $\boldsymbol{C}_{Pub}$ έχει ασφάλεια IND-CPA, τότε το $\boldsymbol{C}^{Hyb}_{Pub}$ έχει ασφάλεια IND-CCA2.

Απόδειξη. [FO99 Theorem 12]. ⊣

Ως εκ τούτου, το σχήμα FullIdent καθορίζεται από τους αλγορίθμους Setup, Extract, Encrypt, Decrypt ως εξής:

Setup(1^k)**:** όπως και στο BasicIdent, παράγονται οι δημόσιες παράμετροι του συστήματος $(r, \mathbb{G}_1, \mathbb{G}_T, e, n, P, P_0, H_1, H_2)$ και επιπροσθέτως οι συναρτήσεις hash $H_3 : \{0,1\}^n \times \{0,1\}^n \longmapsto \mathbb{Z}^*_r$, $H_4 : \{0,1\}^n \longmapsto \{0,1\}^n$.

Extract(s, ID)**:** για τυχαία ταυτότητα $ID \in \{0,1\}^*$, υπολογίζεται το ιδιωτικό κλειδί $d_{ID} = [s]H_1(ID)$.

Encrypt(M, ID_A)**:** ο χρήστης B για να κρυπτογραφήσει μήνυμα M για τον A επιλέγει τυχαίο $\sigma \in \mathbb{Z}^*_r$, θέτει $t = H_3(\sigma, M)$ και υπολογίζει το κρυπτοκείμενο

$$C = \langle [t]P, \sigma \oplus H_2(e(H_1(ID_A), P_0)^t), M \oplus H_4(\sigma)) \rangle.$$

Decrypt(C, d_{ID_A})**:** ο A αποκρυπτογραφεί το $C = \langle U, V, W \rangle$ υπολογίζοντας $\sigma' = V \oplus H_2(e(d_{ID_A}, U))$, $M' = W \oplus H_4(\sigma')$ και $t' = H_3(\sigma', M')$. Εάν $U = [t']P$, τότε αποκρυπτογραφεί το C ως M', διαφορετικά απορρίπτει.

Επεκτάσεις του IBE-σχήματος FullIdent . Το FullIdent που μόλις περιγράψαμε μπορεί να προσαρμοστεί εύκολα ώστε να υποστηρίζει τη χρήση περισσότερων από μία έμπιστων αρχών PKG, τόσο σε οριζόντιο όσο και σε διαβαθμισμένο επίπεδο. Θα μελετήσουμε και τις δύο εκδοχές.

Η χρήση πολλαπλών PKG στο ίδιο επίπεδο γίνεται με φυσικό τρόπο. Κάθε αρχή TA_i, $i = 1 \ldots, n$ κρατά μυστικό τα κύριο κλειδί της s_i και οι δημόσιες παράμετροι είναι οι $(r, \mathbb{G}_1, \mathbb{G}_T, e, P, [s_1]P, \ldots, [s_n]P, H_1, H_2, H_3, H_4)$. Το ιδιωτικό κλειδί κάθε χρήστη A υπολογίζεται ως

$$d_A = \sum_{i=1}^{n} [s_i]H_1(ID_A) = [\sum_{i=1}^{n} s_i]H_1(ID_A).$$

Η κρυπτογράφηση ενός μηνύματος M για τον A παράγει το κρυπτοκείμενο

$$C = \langle [H_3(\sigma, M)]P, \sigma \oplus H_2(e(H_1(ID_A), \sum_{i=1}^{n} [s_i]P)^t), M \oplus H_4(\sigma)) \rangle.$$

Η παραπάνω διαδικάσια μπορεί να επεκταθεί περαιτέρω σε ένα *σχήμα κατωφλιού Shamir* (Shamir threshold scheme) με t-out-of-n *μεσεγγύηση κλειδιού* (*key escrow*) για το κύριο κλειδί s και κατ' επέκταση για το d_A (βλ. [Sti06 §13.1],[BF01 §5). Για δημόσια γνωστές τιμές $x_1, \ldots, x_n$ υπολογίζεται το μοναδικό πολυώνυμο p βαθμού $t-1$ ώστε $p(x_0) = s$ και $p(x_i) = s_i$, $i = 1 \ldots, n$. Ο A επιλέγει t έμπιστες αρχές $\mathrm{TA}_{\sigma(i)}$, $i = 1 \ldots, t$ λαμβάνει τα μερικά ιδιωτικά κλειδιά $[s_{\sigma(i)}]H_1(ID_A)$ και ο A υπολογίζει το ιδιωτικό του κλειδί ως

$$d_A = \sum_{i=1}^{t} \lambda_{i,t} [s_{\sigma(i)}]H_1(ID_A),$$

όπου $\lambda_{i,t} = \prod_{j=1, j\neq i}^{t} \dfrac{x_{\sigma(j)} - x_0}{x_{\sigma(j)} - x_{\sigma(i)}}$ οι αντίστοιχοι συντελεστές Lagrange. Επιπλέον, ο A μπορεί να εντοπίσει μια ανέντιμη αρχη $\mathrm{TA}_\sigma(i)$ ελέγχοντας απλά

$$e([s_{\sigma(i)}]H_1(ID_A), P) = e(H_1(ID_A), [s_\sigma(i)]P),$$

χάρη στην ευκολία του $\mathrm{DDH}(\mathbb{G}_1)$. Εφαρμογές του σχήματος FullIdent με πολλαπλές PKG δίνονται μεταξύ άλλων στα [CHSS02], [MPB03].

Το πρώτο λειτουργικό *ιεραρχικό IBE-σχήμα* (*hierarchical IBE- HIBE*) επινοήθηκε από τους C.Gentry και A.Silverberg [GS02] με την ένταξη κάθε οντότητας του σχήματος σε ένα επίπεδο ιεραρχίας, όπου η *μητρική αρχή* (*root authority*) βρίσκεται στο επίπεδο 0. Κάθε οντότητα A επιπέδου $t > 0$ ορίζεται από τις ταυτότητες $\langle ID_A^1, \ldots, ID_A^t \rangle$ και έχει ως ανώτερές του τη μητρική αρχή και τις οντότητες $\langle ID_A^1, \ldots, ID_A^i \rangle$, $0 < i < t$. Η A μπορεί να παράγει κλειδιά για οντότητες επιπέδου

$t+1$, όπως ορίζει το σχήμα FullHIBE, το οποίο συνίσταται από τους εξής πέντε αλγορίθμους:

RootSetup: όπως και στο FullIdent, η μητρική αρχή δημιουργεί το κύριο κλειδί s_0 και τις δημόσιες παράμετρους του συστήματος

$$(r, \mathbb{G}_1, \mathbb{G}_T, e, P_0, Q_0 = [s_0]P_0, H_1, H_2, H_3, H_4).$$

LowerLevelSetup: μία οντότητα επιπέδου t επιλέγει μυστικό κλειδί $s_t \in \mathbb{Z}_r^*$.

Extract: το ιδιωτικό κλειδί μίας οντότητας $E_t \equiv \langle ID_1, \ldots, ID_t \rangle$, υπολογίζεται από τον γονέα της $\langle ID_1, \ldots, ID_{t-1} \rangle$, ο οποίος εκτελεί τα ακόλουθα βήματα:

1. Υπολογίζεται το $P_t = H_1(ID_1, \ldots, ID_t)$.
2. Υπολογίζεται το ιδιωτικό κλειδί $S_t = S_{t-1} + s_{t-1}P_t$ και αποστέλλεται ασφαλώς στην E_t. Ορίζεται $S_0 = 1_{\mathbb{G}_1}$.
3. Δίνονται στην E_t οι τιμές $Q_i = [s_i]P_0$, $1 \leqslant i < t$.

Encrypt: για την κρυπτογράφηση μηνύματος M για την E_t επιλέγεται τυχαίο $\sigma \in \{0,1\}^*$ και υπολογίζονται τα $P_i = H_1(ID_1, \ldots, ID_i)$, $1 \leqslant i \leqslant t$ και $r = H_3(\sigma, M)$. Το κρυπτοκείμενο είναι το

$$C = \langle [r]P_0, [r]P_2, \ldots, [r]P_t, \sigma \oplus H_2(e(Q_0, P_1)^r), M \oplus H_4(\sigma)) \rangle.$$

Decrypt: η E_t αποκρυπτογραφεί το $C = \langle U_0, U_2, \ldots, U_t, V, W \rangle$ εκτελώντας τους ακόλουθους υπολογισμούς:

$$\sigma' = V \oplus H_2(\frac{e(U_0, S_t)}{\prod_{i=2}^{t} e(Q_{i-1}, U_i)}), \quad M' = W \oplus H_4(\sigma), \quad r' = H_3(\sigma', M').$$

Εάν $\text{Encrypt}(\langle ID_1, \ldots, ID_t \rangle, M'; r') = \langle U_0, U_2, \ldots, U_t, V \rangle$, επιστρέφει M', διαφορετικά απορρίπτει.

Η παράλειψη της ποσότητας $[r]P_1$ κατά την κρυπτογράφηση δεν γίνεται τυχαία καθώς η γνώση της θα επέτρεπε σε έναν επιτιθέμενο να υπολογίσει την μάσκα

$$H_2(e(Q_0, P_1)^r) = H_2(e(Q_0, [r]P_1)).$$

Η κρυπτογράφηση απαιτεί έναν υπολογισμό ζεύγματος, αλλά το μήκος των κρυπτοκειμένων μεγαλώνει όσο αυξάνει το t. Η αποκρυπτογράφηση του C απαιτεί t υπολογισμούς ζεύγματος και είναι εφικτή για κάθε πρόγονο της E_t από την εξίσωση

$$V \oplus H_2(\frac{e(U_0, S_j)}{\prod_{i=2}^{j} e(Q_{i-1}, U_i)}) = \sigma'.$$

2.6 Το Σχήμα Υπογραφών των Boneh-Lynn-Shacham

Σύντομα μετά τη δημοσίευση του [BF01], εμφανίστηκαν διάφορα σχήματα υπογραφών που εκμεταλλεύτηκαν την υποδομή των BasicIdent και FullIdent. Επιδραστικότερο όλων υπήρξε το σχήμα σύντομων υπογραφών των D.Boneh, B.Lynn και H.Shacham [BLS01], οι οποίοι στηρίχθηκαν επίσης στο σχήμα υπογραφών GDH (βλ. §2.2) και στην παρακάτω γενική παρατήρηση από τον M.Naor [BF01 §5].

Η παρατήρηση του Naor. Κάθε IBE-σχήμα $\mathbf{C}_{IB}= (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$ μπορεί να μετατραπεί εύκολα σε σχήμα υπογραφής **DS** ως εξής:

- Το ιδιωτικό κλειδί του **DS** είναι το κύριο κλειδί s του $\mathbf{C}_{IB}$.
- Το δημόσιο κλειδί του **DS** είναι οι δημόσιες παράμετροι του $\mathbf{C}_{IB}$.
- Η υπογραφή ενός μηνύματος $M = ID$ είναι το κλειδί $[s]M$.
- Η επαλήθευση της υπογραφής γίνεται με την κρυπτογράφηση ενός τυχαίου μηνύματος M' με το κλειδί ID και στη συνέχεια τον έλεγχο της ισότητας

$$\mathcal{D}(\mathcal{E}(M', ID), [s]ID) \stackrel{?}{=} M'.$$

Στην περίπτωση όπου το IBE-σχήμα είναι το BasicIdent το *σχήμα υπογραφής BLS* συνίσταται από τους εξής αλγορίθμους:

Keygen(1^k)**:** δημιουργούνται το ιδιωτικό κλειδί s και το δημόσιο κλειδί $pk = (r, \mathbb{G}_1, \mathbb{G}_T, e, n, P, [s]P, H)$, όπου $H : \{0,1\}^* \longrightarrow \mathbb{G}_1$.

Sign(s, M)**:** η υπογραφή ενός μηνύματος M είναι η $\sigma = [s]H(M)$.

Verify(pk, M, σ)**:** η επαλήθευση της υπογραφής γίνεται με τον έλεγχο της ισότητας

$$e(\sigma, P) \stackrel{?}{=} e(H(M), [s]P).$$

Η αποδοτικότητα του αλγορίθμου $Verify$ προκύπτει από την ευκολία του DDH$(\mathbb{G}_1)$ σε ζεύγμα Τύπου 1. Για την ασφάλεια του σχήματος BLS χρειαζόμαστε τον επόμενο ορισμό μοντέλου ασφάλειας για σχήματα υπογραφής

Ορισμός 2.6.1. Έστω σχήμα υπογραφών **DS**$= (\mathcal{K}, \mathcal{S}, \mathcal{V})$. Θεωρούμε το ακόλουθο παίγνιο μεταξύ του προκαλούντος $\mathcal{C}$ και του αντιπάλου $\mathcal{A}$:

Παίγνιο Υπαρξιακής Μη Πλαστογράφησης ενάντια σε Επίθεση Επιλεγμένων Μηνυμάτων (*Existential Unforgeability against Chosen-Message Attacks - EUF-CMA*)**:**

1. Ο $\mathcal{C}$ εκτελεί τον $\mathcal{K}$ παράγει ζεύγος ιδιωτικού και δημόσιου κλειδιού pk, sk και δίνει το pk στον A.

2. Ο $\mathcal{A}$ θέτει ερωτήματα υπογραφής για μηνύματα M_i, $i = 1, \ldots, m$ της επιλογής του και ο $\mathcal{C}$ απαντά αντίστοιχα $\sigma_i = \mathcal{S}(sk, M_i)$.

3. Ο $\mathcal{A}$ εξάγει ζεύγος (M, σ), όπου $M \neq M_i$, $i = 1, \ldots, m$ και κερδίζει εάν

$$\mathcal{V}(pk, M, \sigma) = 1.$$

Ως πλεονέκτημα του A ορίζεται η ποσότητα

$$Adv_{\mathcal{A}}^{EUF-CMA} = \mathbf{Pr}[\mathcal{V}(pk, M, \sigma) = 1 \mid (M, \sigma) \longleftarrow \mathcal{A}^{\mathcal{S}(sk)}(pk); (pk, sk) \xleftarrow{\$} \mathcal{K}],$$

όπου ο συμβολισμός $\mathcal{A}^{\mathcal{S}(sk)}(pk)$ δηλώνει την εκτέλεση του αλγορίθμου $\mathcal{A}$ με είσοδο pk και συμβουλές από μαντείο $\mathcal{S}$ με είσοδο sk. Το **DS** έχει *ασφάλεια EUF-CMA* εάν δεν υπάρχει αντίπαλος που κερδίζει το παίγνιο EUF-CMA με μη αμελητέο πλεονέκτημα.

Πρόταση 2.6.2. *Το σχήμα υπογραφών BLS έχει ασφάλεια EUF-CMA εάν η H θεωρηθεί τυχαίο μαντείο, δεδομένου ότι το CDH*$(\mathbb{G}_1)$ *είναι δύσκολο.*

Απόδειξη. [BLS01 Lemma 5]. ⊣

Το μήκος μίας υπογραφής BLS εξαρτάται αποκλειστικά από το μέγεθος αναπαράστασης της $\mathbb{G}_1 \subseteq E(\mathbb{F}_q)$ και είναι περίπου log(q) bits. Βασική προϋπόθεση είναι το DLP$(E(\mathbb{F}_q))$ να παραμένει δύσκολο ακόμη και σε επιθέσεις MOV [MOV93] μέσω του ζεύγματος e. Έτσι σε πρώτη ανάλυση, η χρήση υπεριδιάζουσων ελλειπτικών καμπυλών με βαθμό εμβάπτισης 6 (και επομένως χαρακτηριστικής 3, από [Men93 Table 5.2]) φαίνεται επαρκής για ασφάλεια 80 bit. Σε αυτό το επίπεδο επιτυγχάνονται υπογραφές BLS μήκους $\approx$ 160 bits, αρκετά μικρότερες των 1024-bit RSA και 320-bit DSA.

Εντούτοις, στο πλήρες paper [BLS03c] επισημαίνεται ότι η ύπαρξη ειδικών αλγορίθμων για επίλυση του DLP σε σώματα μικρής χαρακτηριστικής καθιστά τις υπογραφές BLS πιο ευάλωτες σε σύγκριση με τους ανταγωνιστές τους. Οι D.Boneh, B.Lynn και H.Shacham, θεωρούν ως λύση την εύρεση καμπυλών με βαθμό εμβάπτισης $\geqslant 10$ και $E(\mathbb{F}_q)$ πρώτης τάξης, ένα πρόβλημα που παρέμεινε ανοιχτό μέχρι την ανακάλυψη των BN-καμπυλών από τους P.Barreto και M.Naehrig [BN05]. Δεδομένης μίας τέτοιας ελλειπτικής καμπύλης, το σχήμα BLS προσαρμόζεται σε ασύμμετρα ζεύγματα Τύπου 2 ως εξής:

Keygen(1^k)**:** δημιουργούνται το ιδιωτικό κλειδί s και το δημόσιο κλειδί $pk = (r, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_2, [s]P_2, H)$, όπου P_2 γεννήτορας της $\mathbb{G}_2$.

Sign(s, M)**:** η υπογραφή ενός μηνύματος M είναι η $\sigma = [s]H(M)$.

Verify$(params, M, \sigma)$**:** η επαλήθευση της υπογραφής γίνεται με τον έλεγχο της ισότητας

$$e(\sigma, P_2) \stackrel{?}{=} e(H(M), [s]P_2).$$

Η ασφάλεια του τροποποιημένου σχήματος BLS εξαρτάται πλεόν από τη δυσκολία του co-CDH στις $\mathbb{G}_1, \mathbb{G}_2$ θεωρώντας την H στο ROM. Η ύπαρξη αποδοτικού ισομορφισμού $\psi : \mathbb{G}_2 \longrightarrow \mathbb{G}_1$ είναι απαραίτητη στην απόδειξη ([BLS03 §4.2&Theorem 3.2]).

Επεκτάσεις του σχήματος υπογραφών BLS. Πολλά σχήματα υπογραφών με ενδιαφέρουσες ιδιότητες βασίστηκαν σε τροποποιήσεις των υπογραφών BLS . Χαρακτηριστικά παραδείγματα είναι οι *multi υπογραφές*, *threshold υπογραφές* και *τυφλές υπογραφές* (*blind signatures*) της A.Boldyreva [Bol02], οι *proxy υπογραφές* των F.Zhang, R.Safavi και C.Lin [ZSNL03] και το *σχήμα κρυπτυπογράφησης* (*signcryption scheme*) των B.Libert και J.Quisiquater [LQ04], ένα εργαλείο όπου κρυπτογράφηση και η υπογραφή γίνεται ταυτόχρονα σε μία ενέργεια. Οι Stanfield κ.ά. [SBWP03] επεκτείνοντας το σχήμα υπογραφών BLS επινόησαν τις *universal designated-verifier υπογραφές*, όπου ο χρήστης B μπορεί να επαληθεύσει την υπογραφή-πιστοποιητικό του A, δεν μπορεί όμως να πείσει κάποιον άλλον χρήστη για την εγκυρότητά της. Ένα άλλο πολύ ενδιαφέρον εργαλείο είναι οι *αθροιστικές υπογραφές* (*aggregate signatures*), οι οποίες παρουσιάστηκαν μαζί με σχήματα υπογραφών δακτυλίου (*ring signatures*) και *verifiably encrypted* υπογραφών στην εργασία των D.Boneh κ.ά. [BGLS03] . Οι αθροιστικές υπογραφές εξελίσσουν τις multi υπογραφές με την έννοια ότι ένα σύνολο n μελών μπορεί να υπογράψει συνολικά δημιουργώντας μία σύντομη υπογραφή, επαρκή ώστε να πείσει για τη συμμετοχή όλων των μελών στη διαδικασία. Τα βήματα που εκτελούνται είναι τα ακόλουθα:

- Σε διακεκριμένα μηνύματα M_i, $i = 1, \ldots, m$ λαμβάνονται από όλα τα μέλη υπογραφές BLS $\sigma_i = H(M_i)$. Το δημόσιο κλειδί είναι το

$$(r, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_2, [s_1]P_2, \ldots, [s_m]P_2, H).$$

- Οι σ_i αθροίζονται στην συνολική υπογραφή $\sigma = \sum_{i=1}^{m} \sigma_i \in \mathbb{G}_1$.

- Η επαλήθευση γίνεται με τον έλεγχο της ισότητας

$$e(\sigma, P_2) \stackrel{?}{=} \prod_{i=1}^{m} e(H(M), [s_i]P_2).$$

Το παίγνιο ασφάλειας για τις αθροιστικές υπογραφές είναι παρόμοιο με το EUF-CMA με τη διαφορά ότι στο τέλος ο αντίπαλος $\mathcal{A}$ παράγει $n - 1$ νέα κλειδιά

$pk_2, \ldots, pk_m$ και κερδίζει εάν δημιουργήσει έγκυρη συνολική υπογραφή σ από τα μηνύματα $M_1, \ldots, M_m$ με δημόσια κλειδιά $pk, pk_2, \ldots, pk_m$. Η ασφάλεια του σχήματος απαιτεί τα μηνύματα να είναι διακεκριμένα [BGLS03 §3.2]. Ο περιορισμός αυτός αργότερα αφαιρέθηκε από τους M.Bellare, C.Namprempre και G.Neven [BNN06].

2.7 Κρυπτογραφία Δημόσιου Κλειδιού Χωρίς Πιστοποιητικά

Η εντατική έρευνα σε IBC εφαρμογές που ακόλουθησε τη δημοσίευση του [BF01], οδήγησε σε μια σειρά IB-σχημάτων κρυπτογράφησης [Lyn02], [MSK02], [CHK03], υπογραφών [Hes02], [Pat02b], [LQ03], [CC03] και ανταλλαγής κλειδιού [Sma02], αναπόφευκτα όμως και στην αναζήτηση των περιπτώσεων που η IBC είναι σημαντικά προτιμότερη της κλασικής κρυπτογραφίας δημοσίου κλειδιού (PKC). Αναφέρουμε κάποια βασικά σημεία σύγκρισης και παραπέμπουμε στο [Pat02a] για αναλυτικότερη προσέγγιση του θέματος.

Αυθεντικότητα Παραμέτρων Συστήματος: τόσο στην IBC όσο και στην PKC, οποιαδήποτε κακόβουλη αλλοίωση των παραμέτρων του συστήματος μπορεί να προκαλέσει και την ολική κατάρρευσή του.

Διανομή Ιδιωτικών Κλειδιών: στην IBC, η απώλεια ολικού ελέγχου ενός χρήστη στο ιδιωτικό του κλειδί δημιουργεί την απαίτηση ύπαρξης ασφαλούς καναλιού μεταξύ χρήστη και PKG. Από την άλλη δεν υπάρχει η ανάγκη υποδομής διανομής κλειδιών όπως στην PKC.

Μεσεγγύηση Κλειδιού: η PKG σε ένα IB-σύστημα έχει πλήρη ισχύ πάνω στους χρήστες, με την έννοια ότι μπορεί να αποκρυπτογραφήσει κρυπτοκείμενα που τους αφορούν αλλά και να πλαστογραφήσει υπογραφές τους. Κάτι τέτοιο δεν είναι δυνατό στην PKC παρά μόνο με συμφωνία μεταξύ χρηστών και *αρχής πιστοποίητικών* (*certificate authority - CA*). Η μεσεγγύηση κλειδιού μπορεί να αντιμετωπιστεί με τη χρήση πολλαπλών PKG.

Ανάκληση: στην IBC υπάρχει ιδιαίτερη δυσκολία στην ανάκληση του δημόσιου κλειδιού ενός χρήστη καθώς προκύπτει κάνοντας hashing στην ταυτότητά του. Η εύκολη λύση χρησιμοποίησης ληξημπρόθεσμων ταυτοτήτων στερεί από το σχήμα τον IB χαρακτήρα του.

Διαχείριση Κύριου Κλειδιού: η εξασφάλιση της μυστικότητας του κύριου κλειδιού από την PKG είναι ζωτικής σημασίας για ένα IB-σύστημα. Αυτό καθιστά την PKG βασικό στόχο επίθεσης και επομένως τίθενται ζητήματα διαχείρισης κύριου κλειδιού. Η συχνή αλλαγή του κύριου κλειδιού δεν είναι πάντα συνετή λύση

καθώς επιβαρύνει το σύστημα με την ενημέρωση των παραμέτρων και των δημόσιων κλειδιών των χρηστών.
Δυνατότητα Διεύρυνσης: η PKG, σε αντίθεση με την CA στην PKC δεν επιβαρύνεται με τον έλεγχο των πιστοποιητικών, έχει όμως την ευθύνη εγγραφής και δημιουργίας ιδιωτικών κλειδιών των χρηστών. Ο φόρτος εργασίας μπορεί να επιμεριστεί σε περισσότερες PKG με τη χρήση ενός ιεραρχικού IB-σχήματος, όπως στο [GS02] .

Μαζί με τα προηγούμενα πρέπει να συνυπολογίσουμε την καθιερωμένη εμπιστοσύνη που υπάρχει στην PKC λόγω της μακρόχρονης χρήσης PKC-συστημάτων, αλλά και τους περιορισμούς που επιβάλλουν διάφοροι κανονισμοί και νομοθεσίες. Για παράδειγμα, σύμφωνα με την οδηγία 1999/93/EC της Ευρωπαϊκής Ένωσης ο χρήστης πρέπει να έχει αποκλειστικό έλεγχο του ιδιωτικού του κλειδιού ώστε να εντοπίζονται τυχούσες αλλαγές στα δεδομένα με τα οποία συνδέεται η ηλεκτρονική υπογραφή του. Γενικότερα, η IBC φαίνεται προβληματική σε εφαρμογές που ενδιαφέρει η *μη απάρνηση* (*non-repudiation*) ενέργειας από ένα χρήστη και, παρόλο που διαθέτει κάποια σημαντικά πλεονεκτήματα, δεν μπορεί να αντικατάστήσει την κλασική κρυπτογραφία εξ ολοκλήρου. Αντίθετα, η επιλογή ενός IB-σχήματος θέλει ιδιαίτερη επί τούτου μελέτη ανάλογα με τις ανάγκες της εκάστοτε εφαρμογής.

Ακολουθώντας την παραπάνω ανάλυση, οι A.Al-Riyami και K.Paterson [ARP03] επινόησαν μια νέα εκδοχή κρυπτογραφίας δημοσίου κλειδιού, όπου δεν απαιτούνται πιστοποιητικά αλλά και δεν υφίσταται το πρόβλημα μεσεγγύησης κλειδιού. Το υβριδικό είδος κρυπτογραφίας που αποφεύγει τα παραπάνω εγγενή προβλήματα της PKC και IBC αντίστοιχα ονομάστηκε *Κρυπτογραφία Δημόσιου Κλειδιού χωρίς Πιστοποιητικά* (*Certificateless Public-Key Cryptography - CL-PKC*) και προσδιορίζται από την παρακάτω υποδομή:

- Μία έμπιστη τρίτη αρχή που καλείται *Κέντρο Παραγωγής Κλειδιών* (*Key Generating Center - KGC*), παρέχει μέσω ασφαλούς καναλιού σε μια οντότητα A ένα *μερικό ιδιωτικό κλειδί* d_A, το οποίο υπολογίζει από την ταυτότητα του A, ID_A, και ένα κύριο κλειδί.

- Η A συνδυάζοντας το d_A με κάποια μυστική της πληροφορία παράγει το πραγματικό ιδιωτικό της κλειδί S_A.

- Το δημόσιο κλειδί P_A της A υπολογίζεται από την μυστική της πληροφορία και τις δημόσιες παραμέτρους του συστήματος

Οι βασικές διαφορές με την υποδομή της IBC είναι εμφανείς: η KGC δεν έχει πρόσβαση στα ιδιωτικά κλειδιά των μελών του συστήματος και τα δημόσια κλειδιά δεν καθορίζονται μοναδικά από τις ταυτότητές τους. Σε επίπεδο ασφάλειας,

η εμπιστοσύνη που υπάρχει KGC πλησιάζει την αντίστοιχη στην CA στην PKC. Θεωρούμε δηλαδή ότι η KGC μπορεί να παρακολουθεί την επικοινωνία και να θέτει ερωτήματα αποκρυπτογράφησης, όχι όμως και να αλλοιώνει τα δημόσια κλειδιά. Λόγω έλλειψης πιστοποιητικών πρέπει να υποθέσουμε ότι ένα CL-PKC-σχήμα είναι ασφαλές ακόμη και απέναντι σε αντιπάλους που μπορούν, εκτός του να θέτουν ερωτήματα εξαγωγής (μερικών) ιδιωτικών κλειδιών και αποκρυπτογράφησης όπως στο παίγνιο IND-ID-CCA, να αντικαθιστούν το δημόσιο κλειδί μιας οντότητας με κλειδιά της επιλογής τους. Ως πρώτο δείγμα CL-PKC-συστήματος, οι A.Al-Riyami και K.Paterson παρουσίασαν ένα CL-PKC-σχήμα κρυπτογράφησης το οποίο βασίζεται στο BasicIdent καθορίζεται από τους εξής επτά αλγορίθμους:

Setup$(\mathbf{1^k})$**:** όπως και στο *Setup* του BasicIdent, η KGC επιλέγει κύριο κλειδί $s \in \mathbb{Z}_r^*$ και δημιουργεί τις παραμέτρους του συστήματος

$$(r, \mathbb{G}_1, \mathbb{G}_T, e, n, P, P_0, H_1, H_2).$$

PartialPrivateKeyExtract(s, ID_A)**:** η KGC υπολογίζει για τον χρήστη A με ταυτότητα ID_A το μερικό ιδιωτικό κλειδί $d_A = [s]H_1(ID_A)$.

SetSecretValue$(\cdot)$**:** ο A επιλέγει μυστική πληροφορία $x_A \in \mathbb{Z}_r^*$.

SetPrivateKey(d_A, x_A)**:** ο A υπολογίζει το ιδιωτικό κλειδί του ως

$$S_A = [x_A]d_A = [x_A s]H_1(ID_A).$$

SetPublicKey(x_A)**:** ο A υπολογίζει το δημόσιο κλειδί του ως

$$P_A = \langle X_A, Y_A \rangle = \langle [x_A]P, [x_A]P_0 \rangle.$$

Encrypt(M, P_A, ID_A)**:** για την κρυπτογράφηση μηνύματος $M \in \{0,1\}^n$ για το χρήστη A εκτελούνται τα ακόλουθα βήματα:

1. Ελέγχεται εάν $e(X_A, P_0) \stackrel{?}{=} e(Y_A, P)$.
2. Επιλέγεται τυχαίο $t \in \mathbb{Z}_r^*$.
3. Υπολογίζεται το κρυπτοκείμενο

$$C = \langle [t]P, M \oplus H_2(e(H_1(ID_A), Y_A)^t) \rangle.$$

Decrypt(C, S_A)**:** για την αποκρυπτογράφηση του $C = \langle U, V \rangle$ υπολογίζουμε

$$M = V \oplus H_2(e(S_A, U)).$$

Παρόμοια με τα βήματα στο [BF01], εφαρμόζοντας την τεχνική Fujisaki-Okamoto το παράπάνω σχήμα μετατρέπεται σε ένα CL-PKC-σχήμα με ασφάλεια IND-CCA

στο ROM δεδομένης της υπολογιστικής δυσκολίας του CBDH σε συμμετρικά ζεύγματα [ARP03 Theorem 1].

Στο [ARP03] περιγράφονται επίσης CL-PKC-σχήματα υπογραφών, συμφωνίας κλειδιού και ιεραρχικής κρυπτογράφησης, βασισμένα στα αντίστοιχα σχημάτα των [Hes02], [SOK00] και [GS02] . Οι ιδέες των A.Riyami και K.Paterson έτυχαν μεγάλης απήχησης από την κρυπτογραφική κοινότητα με συνέπεια τον εμπλουτισμό της κρυπτογραφίας ζεύγματος, και όχι μόνο, με ποικίλες μεθόδους κατασκευής CL-PKC-συστημάτων [YL04], [ARP05], [LQ06], [ZWXF06], [BF08].

2.8 Κρυπτογραφία Ζευγμάτων στο Standard Μοντέλο

Οι αποδείξεις ασφάλειας των αρχικών σχημάτων που εμφανίστηκαν στην κρυπτογραφία ζεύγμάτων στηρίχθηκαν στο μοντέλο τυχαίου μαντείου. Λογικά επακόλουθη ήταν η αναζήτηση νέων σχημάτων που παρείχαν ασφάλεια στο *standard μοντέλο*, όπου ο αντίπαλος περιορίζεται μόνο από υποθέσεις υπολογιστικής πολυπλοκότητας. Στα [CHK03], [BB04a] προτείνονται IBE-σχήματα με αυτή την ιδιότητα, αλλά με σημαντική έκπτωση στο μοντέλο επίθεσης του αντιπάλου. Το πρώτο IBE-σχήμα που είναι IND-ID-CCA ασφαλές στο *standard μοντέλο* παρουσιάστηκε στην εργασία των D.Boneh και X.Boyen [BB04b] και βελτιώθηκε σε αποδοτικότητα από τον B.Waters [Wat05]. Πέραν αυτών, οι υπογραφές στο *standard μοντέλο* των [BB04c], [CL04], [Wat05] επέδρασαν καταλυτικά ώστε στα περισσότερα από τα μετέπειτα ενδιαφέροντα σχήματα να επιδιώκεται ασφάλεια χωρίς τη θεώρηση τυχαίων μαντείων [BBS04], [BBG05], [SW05] [Gen06]. Σε αυτήν την ενότητα μελετούμε το σχήμα υπογραφών των D.Boneh και X.Boyen [BB04c], το οποίο υπήρξε η βάση για μετέπειτα σχήματα *ομαδικών υπογραφών* (*group signatures*), όπως θα δούμε αναλυτικά στο Κεφάλαιο 4.

Για την ασφάλεια των υπογραφών BB, οι D.Boneh και X.Boyen εισήγαγαν το παρακάτω νέο πρόβλημα πάνω σε ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$:

***q*-Ισχυρό πρόβλημα Diffie-Hellman** *(q-Strong Diffie-Hellman - q-SDH):* δεδομένων γεννητόρων P, Q των $\mathbb{G}_1, \mathbb{G}_2$ αντίστοιχα και $P, [x]P, [x^2]P, \ldots, [x^q]P$, $[x]Q$, να βρεθεί ζεύγος $[(x+c)^{-1}]P$, όπου $c \in \mathbb{Z}_r \backslash \{-x\}$.

Το σχήμα υπογραφών BB συνίσταται από τους παρακάτω αλγορίθμους:

Keygen(1^k)**:** δημιουργούνται το ιδιωτικό κλειδί $sk = (P, x, y) \in \mathbb{Z}_r^* \times \mathbb{Z}_r^*$ και το δημόσιο κλειδί $pk = (r, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, Q, X = [x]Q, Y = [y]Q, z = e(P, Q))$.

Sign(sk, M)**:** για μήνυμα $M \in \mathbb{Z}_r^*$ επιλέγεται $t \in \mathbb{Z}_r \backslash \{(-x + M)/y\}$ και παράγεται

η υπογραφή

$$(t, \sigma) = (t, [(M + x + yt)^{-1}]P) \in \mathbb{Z}_r \backslash \{(-x + M)/y\} \times \mathbb{G}_1.$$

Verify$(pk, M, \sigma) = 1 \Leftrightarrow e(\sigma, X + [t]Y + [M]Q) = z.$

Το σχήμα υπογραφών BB είναι συνεπές. Πράγματι,

$$e(\sigma, X+[t]Y+[M]Q) = e([(M+x+yt)^{-1}]P, [x+yt+M]Q) = e(P, Q)^{\frac{x+yt+M}{x+yt+M}} = z.$$

Για την απόδειξη ασφάλειας του σχήματος χρειαζόμαστε τους ορισμούς των παρακάτω παιγνίων. Η ασφάλεια SEUF-CMA και SEUF-WCMA ορίζονται ανάλογα.

Παίγνιο Ισχυρής Υπαρξιακής Μη Πλαστογράφησης ενάντια σε Επίθεση Επιλεγμένων Μηνυμάτων (*Strong Existential Unforgeability against Chosen-Message Attacks - EUF-CMA*)**:** όπως στο παίγνιο EUF-CMA, ο προκαλών $\mathcal{C}$ δίνει στον αντίπαλο $\mathcal{A}$ δημόσιο κλειδί pk και απαντά σε ερωτήματα του $\mathcal{A}$ για μηνύματα M_i, $i = 1, \ldots, m$ με υπογραφές $\sigma_i = \mathcal{S}(sk, M_i)$. Ο $\mathcal{A}$ κερδίζει αν παράξει έγκυρο ζεύγος (M, σ) με τον περιορισμό το (M, σ) να είναι διάφορο των (M_i, σ_i).

Παίγνιο Ισχυρής Υπαρξιακής Μη Πλαστογράφησης ενάντια σε Ασθενή Επίθεση Επιλεγμένων Μηνυμάτων (*Strong Existential Unforgeability against Weak Chosen-Message Attacks - SEUF-WCMA*)**:** όπως το SEUF-CMA, με τη διαφορά ότι ο $\mathcal{A}$ υποχρεούται να θέσει τα ερωτήματά του στον $\mathcal{C}$ προτού ο $\mathcal{C}$ του δώσει το pk.

Η διαφορά της ασφάλειας SEUF από την EUF είναι ότι στην πρώτη, ο αντίπαλος όχι μόνο δεν μπορεί να πλαστογραφήσει υπογραφή σε νέο μήνυμα, αλλά ούτε να πλαστογραφήσει διαφορετική υπογραφή σε ένα ήδη υπογεγραμμένο μήνυμα. Η ασφάλεια SEUF αφορά κυρίως σχήματα όπου υπεισέρχεται τυχαίοτητα κατά την υπογραφή ενός μηνύματος, οπότε επιτρέπονται πολλές υπογραφές για συγκεκριμένο μήνυμα. Σε ντετερμινιστικά σχήματα, όπως το weak-BB που θα δούμε στο επόμενο θεώρημα, οι ασφάλειες SEUF και EUF ταυτίζονται.

Θεώρημα 2.8.1. *Εάν το q-SDHP είναι δύσκολο, τότε το σχήμα υπογραφών BB έχει ασφάλεια SEUF-CMA.*

Απόδειξη. Θεωρούμε το απλούστερο σχήμα υπογραφών weak-BB:

Keygen(1^k)**:** $sk = (P, x, y)$, $pk = \langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, Q, X = [x]Q, z = e(P, Q) \rangle$.

Sign$(sk, M) = [(M + x)^{-1}]P$.

Verify$(pk, M, \sigma) = 1 \Leftrightarrow e(\sigma, X + [M]Q) = z.$

Ισχυρισμός 1: *Εάν το q-SDH για τις $\mathbb{G}_1, \mathbb{G}_2$ είναι δύσκολο τότε το σχήμα υπογραφών weak-BB έχει ασφάλεια SEUF-WCMA* [BB04c Lemma 9].

Έστω αντίπαλος $\mathcal{A}$ του σχήματος υπογραφής weak-BB που κερδίζει το παίγνιο EUF-WCMA με μη αμελητέο πλεονέκτημα. Κατασκευάζουμε αλγόριθμο $\mathcal{B}$ που επιλύει το q-SDH σε πολυωνυμικό χρόνο. Για είσοδο $(P, R_1, ...R_q, Q, U)$, όπου $U = [x]Q$, $R_i = [x^i]P$, ο $\mathcal{B}$ προκαλεί τον $\mathcal{A}$ ο οποίος με τη σειρά του θέτει ερωτήματα M_i, $i = 1, \ldots, q$. Ο $\mathcal{B}$ επιλέγει τυχαίο $\theta \in \mathbb{Z}_r$ και έχοντας το πολυώνυμο $f(X) = \prod_{i=1}^{q}(X + M_i) = \sum_{i=1}^{q} \alpha_i X^i$ υπολογίζει

$$P' = \sum_{i=1}^{q} [\alpha_i \theta] R_i = [\theta f(x)]P.$$

Ο $\mathcal{B}$ δίνει στον $\mathcal{A}$ το $pk = \langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, Q, X = [x]Q, z' = e(P', Q) \rangle$ και απαντά στα ερωτήματα με τις υπογραφές

$$\sigma_i = \sum_{i=1}^{q} [\beta_i \theta] R_i = [\theta f_i(x)]P = [(x + M_i)^{-1}]P',$$

όπου $f_i(X) = f(X)/(X + M_i) = \prod_{j=1, j\neq i}^{q}(X + M_j) = \sum_{j=0}^{q-1} \beta_j X^j$. Ολοκληρώνοντας την αλληλεπίδρασή του με τον $\mathcal{B}$, ο $\mathcal{A}$ επιστρέφει έγκυρο ζεύγος (M, σ). Επομένως ισχύει

$$e(\sigma, X + [M]Q) = e(P', Q) \Rightarrow \sigma = [\frac{\theta f(x)}{x + M}]P. \tag{2.1}$$

Εφαρμόζοντας διαίρεση πολυωνύμων προκύπτει

$$f(X) = (X + M)g(X) + \upsilon = (X + M) \sum_{j=0}^{q-1} \gamma_j X^j + \upsilon. \tag{2.2}$$

Από τις (2.1) και (2.2) έχουμε

$$\sigma = [\theta(\frac{\upsilon}{x + M} + \sum_{j=0}^{q-1} \gamma_j X^j)]P.$$

Τελικώς, ο $\mathcal{B}$ υπολογίζει

$$w = [\upsilon^{-1}] \left([\theta^{-1}]\sigma + \sum_{i=0}^{q-1} [-\gamma_i] R_i \right) = [(x + M)^{-1}]P,$$

και επιστρέφει ζεύγος (M, w).

Ισχυρισμός 2: *Εάν το το σχήμα υπογραφών BB έχει ασφάλεια SEUF-CMA, τότε σχήμα υπογραφών weak-BB έχει ασφάλεια SEUF-WCMA* [BB04c Lemma 10].

Έστω αντίπαλος $\mathcal{A}$ του σχήματος υπογραφών BB που κερδίζει το παίγνιο SEUF-CMA. Κατασκευάζουμε αντίπαλο $\mathcal{B}$ του σχήματος υπογραφών weak-BB που κερδίζει το παίγνιο SEUF-WCMA. Ο $\mathcal{B}$ θέτει ερωτήματα M_i, $i = 1, \ldots, q$ λαμβάνοντας ως απάντηση το $pk = \langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, Q, U, z \rangle$ και τις υπογραφές σ_i, $i = 1, \ldots, q$. Οι σ_i είναι μοναδικές για κάθε M_i αφού υποθέτοντας $M \neq -x$ [3] έχουμε

$$e(\sigma_i, U + [M]Q) = e(\sigma_i', U + [M]Q) = z \Rightarrow e(\sigma_i - \sigma_i', [x + M]Q) = 1_{\mathbb{G}_T} \Rightarrow \sigma = \sigma_i.$$

Ο $\mathcal{B}$ δίνει στον $\mathcal{A}$ δημόσιο κλειδί $pk' = \langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, Q, [x]Q, [y]Q, z \rangle$. Ακολούθως ο $\mathcal{A}$ θέτει ερωτήματα M_i', $i = 1, \ldots, q$ και ο $\mathcal{B}$ επιλέγοντας κατάλληλα $t_i \in \mathbb{Z}_r$ απαντά με τα ζεύγη (σ_i, t_i), $i = 1, \ldots, q$. Ο $\mathcal{A}$ επιστρέφει έγκυρο ζεύγος $(M_*, (\sigma_*, t_*))$. Η αλληλεπίδραση του $\mathcal{B}$ με τον $\mathcal{A}$ διαφοροποιείται σύμφωνα με τις τις εξής περιπτώσεις:

1. Ο $\mathcal{A}$ δεν επιστρέφει ζεύγος $(M_*, (\sigma_*, t_*))$ ώστε $ty + M_* \notin \{M_1, \ldots, M_q\}$.
   Τότε ο y επιλέγεται τυχαία και $[x]Q = U$. Επομένως ισχύει ότι

   $$e(\sigma, U + [t][y]Q + [M_*]Q) = z \Leftrightarrow e(\sigma, U + [ty + M_*]Q) = z,$$

   δηλαδή το $(ty + M, \sigma)$ είναι έγκυρο ζεύγος για το σχήμα υπογραφής weak-BB.

2. Ο $\mathcal{A}$ επιστρέφει ζεύγος $(M_*, (\sigma_*, t_*))$ ώστε $ty + M_* \in \{M_1, \ldots, M_q\}$.
   Τότε το x επιλέγεται τυχαία και $[y]Q = U$. Για κάποιο $i \in \{1, \ldots, q\}$ έχουμε $M_i' + yt_i = M + yt$. Επιπλέον,

   $$\begin{aligned}(M_i', t_i) = (M_*, t_*) &\Rightarrow e(\sigma_i, [x + yt_i + M_i]Q) = e(\sigma_*, [x + yt_* + M_*]Q) = z \\ &\Rightarrow \sigma_i = \sigma_* \Rightarrow (M_i, (\sigma_i, t_i)) = (M_*, (\sigma_*, t_*)),\end{aligned}$$

   το οποίο είναι άτοπο από τους περιορισμούς του παιγνίου SEUF-CMA, και αφού $M_i' + yt_i = M + yt$ ισχύει ότι $M_i' \neq M_*$ και $t_i \neq t_*$. Συνεπώς ο $\mathcal{B}$ μπορεί να υπολογίσει το ιδιωτικό κλειδί $y = (M_i' - M_*)(t_i - t_*)^{-1}$ που αντιστοιχεί στο δημόσιο κλειδί που του δόθηκε και να πλαστογραφήσει υπογραφή σε οποιοδήποτε μήνυμα της αρεσκείας του.

Η απόδειξη του θεωρήματος είναι άμεση συνέπεια των δύο ισχυρισμών.

⊣

Οι υπογραφές BB έχουν μήκος $\approx 2\log(r)$ όπως και οι υπογραφές DSA και υπερτερούν των υπογραφών BLS τόσο σε χρόνο υπογραφής καθώς δεν απαιτείται hashing, όσο και σε χρόνο επαλήθευσης όπου εκτελείται μόνο ένας υπολογισμός ζεύγματος.

[3] για $x + M = 0$ θέτουμε $\sigma = 0_{\mathbb{G}_1}$

Επιπροσθέτως, στο [BB04c §5] δίνεται ένα άλλο σχήμα υπογραφής βασισμένο στο weak-BB μήκους $\approx log(r)$, το οποίο έχει ασφάλεια SEUF-CMA στο ROM δεδομένης της δυσκολίας του q-SDH ενώ διατηρεί τα υπολογιστικά πλεονεκτήματα του αρχικού σχήματος BB.

2.9 Σύνοψη Κεφαλαίου

Δώσαμε το γενικό ορισμό του ζεύγματος και διατυπώσαμε τα βασικά προβλήματα από την κρυπτογραφία ζευγμάτων CBDH, DBDH και co-CDH, συγκρίνοντας τη δυσκολία τους τόσο μεταξύ τους όσο και με τα καθιερωμένα προβλήματα της ασύμμετρης κρυπτογραφίας DLP, CDH και DDH. Στη συνέχεια μελετήσαμε τέσσερα θεμελιώδη σχήματα της κρυπτογραφίας ζευγμάτων: το πρωτόκολλο ανταλλαγής κλειδιού βάσει ταυτοτήτων SOK00, το τριμερές πρωτόκολλο ανταλλαγής κλειδιού Jou00, το σχήμα κρυπτογράφησης βάσει ταυτοτήτων FullIdent (BF01) και το σχήμα υπογραφών BLS01. Αναφέραμε επίσης κάποιες σημαντικές επεκτάσεις τους δίνοντας έμφαση στο ιεραρχικό σχήμα κρυπτογράφησης βάσει ταυτοτήτων CG02, τις αθροιστικές υπογραφές BGLS03 και το πρότυπο σχήμα κρυπτογράφησης χωρίς πιστοποιητικά ARP03. Από τα νεότερα σχήματα στο standard μοντέλο, επιλέξαμε να παρουσιάσουμε τις υπογραφές BB, λόγω της εφαρμογής τους σε σχήματα ομαδικών υπογραφών που θα αναλύσουμε στο τελευταίο κεφάλαιο.

Κεφάλαιο 3

Το Μη Διαλογικό Σύστημα Απόδειξης **Groth-Sahai**

Τα συστήματα απόδειξης άρχισαν να χρησιμοποιούνται ευρέως στην κρυπτογραφία όταν, ένα χρόνο μετά τον ορισμό των *αποδείξεων μηδενικής γνώσης* (*zero knowledge proofs - ZK proofs*) από τους S.Goldwasser, S.Micali και C.Rackoff [GMR85], οι O.Goldreich, S.Micali και A.Widgerson [GMW86] περιέγραψαν μια γενική μεθοδολογία σχεδιασμού κρυπτογραφικών ZK πρωτοκόλλων. Λίγο αργότερα, οι M.Blum, P.Feldman και S.Micali [BFM88] κατασκεύασαν το πρωτο σχήμα κρυπτογράφησης δημόσιου κλειδιού με CCA ασφάλεια εισάγοντας και χρησιμοποιώντας τα *μη διαλογικά συστήματα απόδειξης μηδενικής γνώσης* (*non-interactive zero knowledge - NIZK - proof systems*), μία ειδική κατηγορία ZK συστημάτων απόδειξης όπου ο επαληθευτής πείθεται για την αλήθεια μίας πρότασης μαθαίνοντας τίποτα πέραν της απόδειξης που του δίνεται. Σε όλα τα χρόνια που ακολούθησαν, τα μη διαλογικά συστήματα απόδειξης ήταν στο επίκεντρο της κρυπτογραφικής έρευνας, με διάφορες τροποποιήσεις του αρχικού ορισμού προς εξυπήρετηση των εκάστοτε ειδικών απαιτήσεων. Το 2006, οι J.Groth, R.Ostrovsky και A.Sahai έλυσαν το ανοιχτό πρόβλημα ύπαρξης μη διαλογικών επιχειρημάτων στατιστικής μηδενικής γνώσης για κάθε γλώσσα στο **NP** [GOS06b] και εισήγαγαν νέες NIZK τεχνικές [GOS06a] χρησιμοποιώντας υποθέσεις από την κρυπτογραφία ζευγμάτων. Οι ιδέες τους χρησιμοποίηθηκαν στην κατασκευή σχημάτων ομαδικών υπογραφών στο standard μοντέλο [BW06], [Gro06].

Εντούτοις, η μεγάλη πρακτική χρησιμότητα των ζευγμάτων δεν είχε φανεί μέχρι την παρουσίαση μίας απλής και γενικής μεθοδολογίας κατασκευής σύντομων NIZK αποδείξεων επαληθευσιμότητας εξισώσεων που βασίζονται σε ζεύγματα. Οι δημιουργοί αυτών των αποδείξεων είναι οι J.Groth και A.Sahai και η εργασία τους με τίτλο «*Efficient Non-interactive Proof Systems for Bilinear Groups*» [GS08] συνιστά το κεντρικό αντικείμενο μελέτης του κεφαλαίου. Κατά την απόδοση των

προαπαιτούμενων εννοιών, ακολουθούμε το φορμαλισμό του [Gol04 §4], αποδοσμένο μέσω της ορολογίας που χρησιμοποιείται στο [Ζάχ07 §17].

3.1 Διαλογικά Συστήματα Απόδειξης

Ορισμός 3.1.1. Μία *διαλογική μηχανή Turing* (*interactive Turing machine - ITM*) είναι μία πολυταινιακή TM με μία read-only ταινία εισόδου, μία read-only τυχαία ταινία, μία read-and-write ταινία εργασίας, μία write-only ταινία εξόδου, μία read-and-write ταινία ενός κελιού εναλλαγής των καταστάσεων *ενεργός/αδρανής* και ένα ζεύγος ταινιών επικοινωνίας με τα εξής χαρακτηριστικά:

- μία read-only ταινία παραλαβής μηνυμάτων,
- μία write-only ταινία αποστολής μηνυμάτων.

Λέμε επίσης ότι δύο ITM *συνδέονται*, εάν οι τανίες εισόδου τους συμπίπτουν, η read-only ταινία παραλαβής μηνυμάτων της μίας είναι η write-only ταινία αποστολής μηνυμάτων της άλλης, οι τυχαίες ταινίες και οι ταινίες εξόδου τους είναι διαφορετικές μεταξύ τους και οι ταινίες εναλλαγής τους συμπίπτουν συμπληρωματικά, δηλαδή όταν η μία TM είναι ενεργός, τότε η άλλη είναι αδρανής. Δύο συνδεόμενες ITM *διαλέγονται* εάν εκτελούν κάποιον υπολογισμό με κοινή είσοδο. Με $\langle \mathcal{A}, \mathcal{B} \rangle(x)$ συμβολίζουμε την τυχαία μεταβλητή που αναπαριστά την έξοδο της $\mathcal{B}$ όταν αυτή διαλέγεται με την $\mathcal{A}$ με κοινή είσοδο x. Μία ITM $\mathcal{A}$ έχει *χρονική πολυπλοκότητα* $t : \mathbb{N} \longrightarrow \mathbb{N}$ εάν σε κάθε διαλογικό υπολογισμό της με είσοδο x τερματίζει σε $t(|x|)$ βήματα.

Ορισμός 3.1.2. Ένα ζεύγος συνδεόμενων ITM $(\mathcal{P}, \mathcal{V})$ καλείται *διαλογικό σύστημα απόδειξης* (*interactive proof system - IPS*) για τη γλώσσα L, εάν η $\mathcal{V}$ είναι πολυωνυμικού χρόνου και ικανοποιούνται οι εξής δύο συνθήκες

(i). *Πληρότητα* (*Completeness*): για κάθε $x \in L$

$$\mathbf{Pr}[\langle \mathcal{P}, \mathcal{V} \rangle(x) = 1] \geqslant \frac{2}{3}.$$

(ii). *Ορθότητα* (*Soundness*): για κάθε $x \notin L$ και κάθε ITM $\mathcal{P}^*$

$$\mathbf{Pr}[\langle \mathcal{P}^*, \mathcal{V} \rangle(x) = 1] \leqslant \frac{1}{3}.$$

Η κλάση όλων των γλωσσών που επιδέχονται IPS ονομάζεται **IP**. Η ITM $\mathcal{P}$ καλείται *αποδείκτης* (*prover*), ενώ η $\mathcal{V}$ *επαληθευτής* (*verifier*). Ο αποδείκτης θεωρείται χωρίς περιορισμούς υπολογιστικών πόρων.

Όπως στην περίπτωση της κλάσης **BPP**, η πιθανότητα σφάλματος μπορεί να γίνει αμελητέα έπειτα από πολυωνυμικό πλήθος εκτελέσεων. Εξάλλου, κάθε $L \in \mathbf{BPP}$ θεωρείται ότι έχει επαληθευτή ο οποίος αποκρίνεται χωρίς αλληλεπίδραση, ενώ κάθε $L \in \mathbf{NP}$ έχει IPS μηδενικής πιθανότητας σφάλματος, από τους ορισμούς των δύο κλάσεων. Ισχύει επομένως ότι

$$\mathbf{BPP} \cup \mathbf{NP} \subseteq \mathbf{IP}.$$

Ένα ισχυρότερο αποτέλεσμα που οφείλεται στον A.Shamir είναι το:

Θεώρημα 3.1.3. IP = PSPACE.

Απόδειξη. [Sha92]. ⊣

Παραθέτουμε ένα αντιπροσωπευτικό παράδειγμα γλώσσας που βρίσκεται στο **IP** [Gol04 §4.2.2].

Παράδειγμα 3.1.4. *Μη Ισομορφισμός Γραφημάτων.*

$$GNI = \{\langle G_0 = (V_0, E_0), G_1 = (V_1, E_1)\rangle \mid \text{δεν υπάρχει ισομορφισμός } \phi : G_0 \to G_1\}.$$

Ο $\mathcal{V}$ επιλέγει τυχαίο $i \in \{0,1\}$ και τυχαία μετάθεση $\sigma : V_i \longrightarrow V_i$. Δημιουργεί τελικά τυχαίο γράφημα $H = \sigma(G_i)$ ισομορφικό του G_i και το στέλνει στον $\mathcal{P}$ ζητώντας του $j \in \{0,1\}$ τέτοιο ώστε το G_j να είναι ισομορφικό του H. Εάν $(G_0, G_1) \in GNI$, τότε ο $\mathcal{P}$, που δεν περιορίζεται χρονικά, βρίσκει ποιο από τα δύο γραφήματα είναι ισομορφικό με το H και στέλνει στον $\mathcal{V}$ το σωστό j. Εάν $(G_0, G_1) \notin GNI$, τότε ο $\mathcal{P}$ δεν μπορεί να διακρίνει από ποιο γράφημα προέκυψε το H, οπότε στέλνει τυχαίο $j' \in \{0,1\}$. Εφόσον οι (G_0, G_1) είναι ισομορφικοί, τότε τα σύνολα

$$\{\sigma : V_0 \longrightarrow V_0 \mid \sigma(G_0) = H\} \quad \text{και} \quad \{\sigma : V_1 \longrightarrow V_1 \mid \sigma(G_1) = H\}$$

είναι ισοπληθικά. Επομένως, ένας τυχαίος αποδείκτης $\mathcal{P}^*$ δε λαμβάνει σημαντική πληροφορία για το j από την σ και άρα δεν μπορεί να ξεγελάσει τον $\mathcal{V}$ ώστε να αποδεχτεί με πιθανότητα μεγαλύτερη του $1/2$.

Κατά την εκτέλεση ενός διαλογικού πρωτοκόλλου, είναι πιθανό οι δύο πλευρές, πέραν της αλληλεπίδρασής τους, να διαχειρίζονται προς όφελός τους και κάποια ιδιωτική πληροφορία προερχόμενη είτε από το περιβάλλον του συστήματος είτε από εσωτερική εμπειρία πρότερων εκτελέσεων. Το φαινόμενο μοντελοποιείται επαυξάνοντας τον Ορισμό 3.1.1 με την πρόσθεση μίας read-only βοηθητικής ταινίας εισόδου που περίεχει την επιπλέον πληροφορία που μπορεί να δεχθεί κάποια ITM. Η χρονική πολυπλοκότητα μίας *διαλογικής μηχανής Turing με βοηθητική είσοδο* (*ITM with*

auxiliay input - aux-ITM) ορίζεται όπως πριν. Ανάλογα με τον Ορισμό 3.1.1 επαυξάνεται και ο Ορισμός 3.1.2 ώστε να προκύψει το μοντέλο του *διαλογικού συστήματος απόδειξης με βοηθητική είσοδο* (*IPS with auxiliay input - aux-IPS*). Οι συνθήκες που πρέπει να ικανοποιούνται τώρα είναι

(i). *Πληρότητα*: για κάθε $x \in L$, υπάρχει y ώστε για κάθε z

$$\mathbf{Pr}[\langle \mathcal{P}(y), \mathcal{V}(z) \rangle(x) = 1] \geqslant \frac{2}{3}.$$

(ii). *Ορθότητα*: για κάθε $x \notin L$ και κάθε ITM $\mathcal{P}^*$, και για κάθε y, z

$$\mathbf{Pr}[\langle \mathcal{P}^*(y), \mathcal{V}(z) \rangle(x) = 1] \leqslant \frac{1}{3}.$$

Με $\langle \mathcal{A}(y), \mathcal{B}(z) \rangle(x)$ συμβολίζουμε την τυχαία μεταβλητή που αναπαριστά την έξοδο της $\mathcal{B}$ όταν αυτή διαλέγεται με την $\mathcal{A}$ με κοινή είσοδο x και οι βοηθητικές είσοδοι των $\mathcal{A}, \mathcal{B}$ είναι y, z αντίστοιχα. Στο εξής, για ευκολία θα αναφερόμαστε γενικά σε ITM και IPS υποδηλόνωντας τη βοηθητική είσοδο από τους συμβολισμούς.

Σημαντική εφαρμογή στην μοντελοποίηση κρυπτογραφικών πρωτοκόλλων βρίσκει η ασθενέστερη απαίτηση της *υπολογιστικής ορθότητας*, όπου αρκεί ο επαληθευτής να παραπλανάται με αμελητέα πιθανότητα για αποδείκτες *πολυωνυμικού* χρόνου. Ένα υπολογιστικά ορθό IPS καλείται *επιχείρημα* (*argument*).

Αποδείξεις γνώσης. Συχνά σε ένα πρωτόκολλο μεταξύ των $\mathcal{P}, \mathcal{V}$ ζητάμε από τον $\mathcal{P}$ αντί για την απόδειξη μίας πρότασης, την απόδειξη κάποιας ειδικής γνώσης, όπως για παράδειγμα το ιδιωτικό κλειδί που αντιστοιχεί σε ένα δημόσιο κλειδί. Τυπικά, για κάποια διμελή σχέση R θέλουμε για κοινή είσοδο x ο $\mathcal{P}$ να αποδείξει στον $\mathcal{V}$ ότι γνωρίζει ένα w ώστε $R(x, w)$.

Ορισμός 3.1.5. Ένα πρωτόκολλο συνδεόμενων ITM $(\mathcal{P}, \mathcal{V})$, όπου $\mathcal{V}$ πολυωνυμικού χρόνου, είναι *απόδειξη γνώσης* (*Proof of knowledge - PoK*) για τη διμελή σχέση R με σφάλμα γνώσης κ εάν ικανοποιούνται οι εξής συνθήκες:

(i). *Τέλεια πληρότητα*: για κάθε $(x, w) \in R$

$$\mathbf{Pr}[\langle \mathcal{P}(w), \mathcal{V} \rangle(x) = 1] = 1.$$

(ii). *Εγκυρότητα* (*Validity*): υπάρχει PPT ITM $\mathcal{K}$ ώστε για κάθε ITM $\mathcal{P}^*$, και για κάθε x, w'

$$\mathbf{Pr}[\langle \mathcal{P}^*(w'), \mathcal{V} \rangle(x) = 1] - \mathbf{Pr}[y \leftarrow \mathcal{K}^{\mathcal{P}^*(x,w')}(x) : R(x, w) = 1] \leqslant \kappa(|x|)$$

Η $\mathcal{K}$ ονομάζεται *εξαγωγέας γνώσης* (*knowledge extractor*) για την R. Η ποσότητα $\kappa(|x|)$ υπονοεί την πιθανότητα να πειστεί ο $\mathcal{V}$ χωρίς ο $\mathcal{P}^*$ να έχει πρόσβαση στην trapdoor πληροφορία που του παρέχει ο μάρτυρας w. Εάν το $\kappa(|x|)$ είναι αμελητέο, τότε έπεται η ορθότητα του $(\mathcal{P}, \mathcal{V})$, το οποίο καλείται *διαλογικό σύστημα απόδειξης γνώσης* (IPS-PoK).

Παράδειγμα 3.1.6. Το παρακάτω πρωτόκολλο τριών γύρων (*πρωτόκολλο του Schnorr*)

	$\mathcal{P}(w,x)$		$\mathcal{V}(x)$
1. Δέσμευση:	$r \xleftarrow{\$} \mathbb{Z}_p; z = g^r$	$\xrightarrow{r}$	
2. Πρόκληση:		$\xleftarrow{b}$	$b \xleftarrow{\$} \mathbb{Z}_{2^t}$
3. Απάντηση:	$a = r + bw$	$\xrightarrow{a}$	$\mathcal{V}(x) = 1 \Leftrightarrow g^a = z \cdot x^b$

είναι απόδειξης γνώσης του διακριτού λογαρίθμου $\log_g(x) \in \mathbb{Z}_p$.

Η πληρότητα είναι άμεση αφού $R(x,w) \Leftrightarrow w = \log_g(x) \Rightarrow z \cdot x^b = g^r \cdot g^{bw} = g^a$. Η εγκυρότητα έπεται από την κατασκευή του εξαγωγέα γνώσης $\mathcal{K}$ ο οποίος για είσοδο x και αποδείκτη $\mathcal{P}^*$:

1. Εκτελεί τον $\mathcal{P}^*(x)$ και λαμβάνει z.
2. Στέλνει στον $\mathcal{P}^*$ πρόκληση b_0 και λαμβάνει απάντηση a_0.
3. Επαναφέρει τον $\mathcal{P}^*$ στην κατάσταση πριν το Βήμα 2 και τον προκαλεί εκ νέου με $b_1 \neq b_0$ λαμβάνοντας a_1.
4. Επιστρέφει την τιμή $(a_1 - a_0)/(b_1 - b_0)$.

Παρατηρούμε ότι αν τα a_0, a_1 είναι ορθές απαντήσεις τότε

$$a_1 - a_0 = \log_g(z \cdot x^{b_1}) - \log_g(z \cdot x^{b_0}) = (b_1 - b_0) \cdot \log_g(x) \Leftrightarrow$$
$$\Leftrightarrow \log_g(x) = (a_1 - a_0) \cdot (b_1 - b_0)^{-1},$$

επομένως ένας αποδείκτης που δε γνωρίζει τον μάρτυρα w μπορεί να απαντήσει σωστά το πολύ σε μία πρόκληση με πιθανότητα $1/2^t$. Η δυνατότητα εξαγωγής γνώσης από δύο ορθές απαντήσεις σε διαφορετικές προκλήσεις υπό την ίδια δέσμευση καλείται *ειδική ορθότητα* (*special soundness*).

3.2 Αποδείξεις Μηδενικής Γνώσης και Μη Διακρισιμότητας Μάρτυρος

Σε μία διαλογική απόδειξη, ιδιαίτερο ενδιαφέρον υπάρχει για το τι ωφέλιμη πληροφορία μαθαίνει ο επαληθευτής κατά το διάλογό του με τον αποδείκτη. Στις κρυπτογραφικές εφαρμογές ζητείται η πληροφορία να είναι η ελάχιστη δυνατή, ώστε να αποφεύγεται η πρόσληψη γνώσης που μπορεί να αποβεί σημαντικό πλεονέκτημα για κάποιον αντίπαλο. Η απαίτηση αυτή ικανοποιείται με τον καλύτερο τρόπο στις αποδείξεις μηδενικής γνώσης, αλλά και η ασθενέστερη ιδιότητα της μη διακρισιμότητας μάρτυρος είναι πολλές φορές επαρκώς επιθυμητή. Ο αυστηρός ορισμός της μηδενικής γνώσεις είναι ο ακόλουθος:

Ορισμός 3.2.1. Έστω IPS $(\mathcal{P}, \mathcal{V})$) για τη γλώσσα L. Το $(\mathcal{P}, \mathcal{V})$ είναι *τέλειας μηδενικής γνώσης* (*perfect zero-knowledge - PZK*) εάν για κάθε PPT ITM $\mathcal{V}^*$ υπάρχει PPT αλγόριθμος $\mathcal{S}$ ώστε για κάθε $x \in L$ οι τ.μ. $\langle \mathcal{P}, \mathcal{V}^* \rangle(x)$ και $\mathcal{S}(x)$ έχουν όμοια κατανομή, δηλαδή

$$\forall \alpha \in \{0,1\}^* : \mathbf{Pr}[\langle \mathcal{P}, \mathcal{V}^* \rangle(x) = \alpha] = \mathbf{Pr}[\mathcal{S}(x) = \alpha].$$

Ο αλγόριθμος $\mathcal{A}$ ονομάζεται *προσομοιωτής* της αλληλεπίδρασης του $\mathcal{P}$ με τον $\mathcal{V}$. Σύμφωνα με τον Ορισμό 3.2.1, ένα IPS είναι μηδενικής γνώσης εάν ένας πολυωνυμικά φραγμένος επαληθευτής δεν μπορεί να αποκτήσει καμία σημαντική επιπρόσθετη γνώση από αυτή που θα κέρδιζε εκτελώντας κάποιον κατάλληλο πολυωνυμικό αλγόριθμο. Δύο χαλαρώσεις του αρχικού ορισμού προκύπτουν από τις έννοιες της υπολογιστικής και της στατιστικής μη διακρισιμότητας οικογενειών τ.μ.. Η υπολογιστική μη διακρισιμότητα οικογενειών τ.μ. επαναδιατυπώνεται συμβατικά με τους συμβολισμούς του κεφαλαίου.

Ορισμός 3.2.2. Έστω γλώσσα $L \in \{0,1\}^*$. Δύο οικογένειες τ.μ. $\{U_x\}_{x \in L}$ και $\{V_x\}_{x \in L}$ ονομάζονται *υπολογιστικά μη διακρίσιμες* (*computationally indistinguishable*), εάν για κάθε *PPT* αλγόριθμο D και κάθε πολυώνυμο p, υπάρχει x αρκετά μεγάλου μήκους ώστε

$$| \mathbf{Pr}[D(U_x, x) = 1] - \mathbf{Pr}[D(V_x, x) = 1] | < \frac{1}{p(|x|)}.$$

Ορισμός 3.2.3. Έστω γλώσσα $L \in \{0,1\}^*$. Δύο οικογένειες τ.μ. $\{U_x\}_{x \in L}$ και $\{V_x\}_{x \in L}$ ονομάζονται *στατιστικά μη διακρίσιμες* (*statistically indistinguishable*), εάν η στατιστική διαφορά τους $\Delta(|x|)$ είναι αμελητέα, δηλαδή εάν για κάθε πολυώνυμο p, υπάρχει x αρκετά μεγάλου μήκους ώστε

$$\Delta(|x|) = \frac{1}{2} \sum_{\alpha} | \mathbf{Pr}[U_x = \alpha] - \mathbf{Pr}[V_x = \alpha] | < \frac{1}{p(|x|)}.$$

Σύμφωνα με τους Ορισμούς 3.2.2 και 3.2.3, έχουμε τους εξής ορισμούς:

Ορισμός 3.2.4. Έστω IPS $(\mathcal{P}, \mathcal{V})$ για τη γλώσσα L. Το $(\mathcal{P}, \mathcal{V})$) είναι *υπολογιστικής* (*στατιστικής*) *μηδενικής μηδενικής γνώσης* (*computatational* (*statistical*) *zero-knowledge* - *CZK* (*SZK*)), εάν για κάθε PPT ITM $\mathcal{V}^*$ υπάρχει PPT αλγόριθμος $\mathcal{S}$ ώστε οι οικόγενειες τ.μ. $\{\langle \mathcal{P}, \mathcal{V}^* \rangle(x)\}_{x \in L}$ και $\{\mathcal{S}(x)\}_{x \in L}$ να είναι υπολογιστικά (στατιστικά) μη διακρίσιμες.

Προφανώς ισχύουν οι συνεπαγωγές $PZK \Rightarrow SZK \Rightarrow CZK$. Επειδή στην κρυπτογραφία ενδιαφέρουν οι πολυωνυμικοί υπολογισμοί, όταν αναφερόμαστε σε συστήματα μηδενικής γνώσης (ZK) θα υπονοούμε PZK, ενώ οι άλλες δύο εκδοχές θα δηλώνονται ρητά. Μία χρήσιμη ιδιότητα, ασθενέστερη της μηδενικής γνώσης, είναι η ύπαρξη προσομοιωτή μόνο για το διάλογο του αποδείκτη με τον καθορισμένο επαληθευτή $\mathcal{V}$ (*honest verifier zero-knowledge* - *HVZK*).

Εναλλακτικά, μπορούμε να ορίσουμε τη μηδενική γνώση με την ύπαρξη προσομοιωτή $\mathcal{S}$ για την *άποψη* του τυχαίου επαληθευτή $\mathcal{V}^*$, $view^{\mathcal{P}}_{\mathcal{V}^*}(x)$, δηλαδή την ακολουθία που περιγράφει την τυχαία ταινία του $\mathcal{V}^*$ μαζί με τα μηνύματα που ανταλλάσσονται κατά την αλληλεπίδραση του $\mathcal{V}^*$ με τον $\mathcal{P}$. Σε αυτήν την περίπτωση ζητούμε τη μη διακρισιμότητα των οικογενειών τ.μ. $view^{\mathcal{P}}_{\mathcal{V}^*}(x)_{x \in L}$ και $\{\mathcal{S}(x)\}_{x \in L}$.

Η έννοια της μηδενικής γνώσης επεκτείνεται φυσικά σε aux-IPS, οριζόμενη ως η μη διακρισιμότητα των οικογενειών τ.μ.

$$\{\langle \mathcal{P}(y_x), \mathcal{V}^*(z) \rangle(x)\}_{x \in L, z \in \{0,1\}^*} \text{ και } \{\mathcal{A}(x, z)\}_{x \in L, z \in \{0,1\}^*},$$

όπου y_x ικανοποιεί την συνθήκη πληρότητας ως προς x. Ο προσομοιωτής $\mathcal{A}$ εκτός από την κοινή είσοδο διαθέτει πλέον και τη βοηθητική είσοδο του επαληθευτή, προφανώς όμως όχι και του αποδείκτη.

Παράδειγμα 3.2.5. *Ισομορφισμός Γραφημάτων* [Gol04 §4.3.2].

$$GI = \{\langle G_0 = (V_0, E_0), G_1 = (V_1, E_1) \rangle \mid \text{ υπάρχει ισομορφισμός } \phi : G_0 \to G_1\}.$$

Ο $\mathcal{P}$ επιλέγει τυχαίο $i \in \{0, 1\}$ και τυχαία μετάθεση $\sigma : V_i \longrightarrow V_i$. Δημιουργεί τελικά γράφημα $H = \sigma(G_i)$ ισομορφικό του G_i και το στέλνει στον $\mathcal{V}$. Ο $\mathcal{V}$ επιλέγει τυχαίο $j \in \{0, 1\}$ και ζητά από τον $\mathcal{P}$ να του αποδείξει ότι το G_j είναι ισομορφικό του H. Εάν $i = j$, ο $\mathcal{P}$ αποστέλλει την μετάθεση $h = \sigma$. Εάν $i \neq j$, τότε

1. Εάν $\langle G_0, G_1 \rangle \in GI$, τότε ο $\mathcal{P}$ υπολογίζει ισομορφισμό $\tau : G_j \longrightarrow G_i$ και αποστέλλει την $h = \sigma \circ \tau$.

2. Εάν $\langle G_0, G_1 \rangle \notin GI$, τότε ο $\mathcal{P}$ αποστέλλει τυχαία μετάθεση h.

Σε κάθε περίπτωση, ο $\mathcal{V}$ ελέγχει εάν $h(G_j) = H$ και εξαπατάται μόνο εάν $i = j$ και $\langle G_0 = (V_0, E_0), G_1 = (V_1, E_1)\rangle \in GI$ με πιθανότητα σφάλματος $1/2$. Το $(\mathcal{P}, \mathcal{V})$ είναι PZK αφού η μόνη πληροφορία που λαμβάνει ο $\mathcal{V}^*$ είναι το H, το οποίο θα μπορούσε να παράγει επιλέγοντας κατάλληλη τυχαία μετάθεση.

Οι O.Goldreich, S.Micali και A.Widgerson [GMW86] έδειξαν ότι εάν υπάρχουν *συναρτήσεις μονής κατεύθυνσης* (*one-way functions - OWF*), τότε κάθε γλώσσα στο **NP** έχει ZK-IPS, κατασκευάζοντας αρχικά ένα τέτοιο σύστημα απόδειξης για το **NP**-πλήρες πρόβλημα του χρωματισμού γραφήματος με 3 χρώματα.

Οι ZK αποδείξεις έχουν ευρεία εφαρμογή στο σχεδιασμό ασφαλών πρωτοκόλλων όπου δεν υπάρχει εμπιστοσύνη μεταξύ των μελών. Σε ένα πρωτόκολλο μηδενικής γνώσης, ένα μέλος αποδεικνύει την τιμιότητά του χωρίς να αποκαλύψει μυστικές του πληροφορίες, όπως στο *πρωτόκολλο αναγνώρισης* (*identification protocol*) των U.Feige, A.Fiat και A.Shamir [FFS88], το οποίο περιγράφεται παρακάτω.

Setup:

1. Μία τρίτη έμπιστη αρχή TTP επιλέγει τυχαίους μυστικούς πρώτους p, q και υπολογίζει δημόσιο $n = pq$.
2. Ο $\mathcal{P}$ επιλέγει τυχαία για ιδιωτικό του κλειδί το $sk = s_1, \ldots, s_k \in \mathbb{Z}_n$.
3. Ο $\mathcal{P}$ υπολογίζει το δημόσιο κλειδί $pk = p_1, \ldots, p_k$, όπου $p_i \equiv \pm s_i^{-2} \bmod (n)$, $i = 1, \ldots, k$.

Πρωτόκολλο αναγνώρισης:

1. Ο $\mathcal{P}$ επιλέγει τυχαίο $r \in \mathbb{Z}_n$ και στέλνει στον $\mathcal{V}$ την τιμή $x \equiv \pm r^2 \bmod (n)$.
2. Ο $\mathcal{V}$ επιλέγει τυχαία $(b_1, \ldots, b_k) \in \{0,1\}^k$ τα οποία και στέλνει στον $\mathcal{P}$.
3. Ο $\mathcal{P}$ υπολογίζει την τιμή $y = r \cdot \prod_{E_i=1} s_i$ και τη στέλνει στον $\mathcal{V}$.
4. Ο $\mathcal{V}$ αποδέχεται ανν $x = \pm y^2 \cdot \prod_{E_i=1} p_i$.

Το πρωτόκολλο στηρίζεται στη δυσκολία υπολογισμού τετραγωνικών ριζών $\bmod (n)$ και είναι ιδιαίτερα γρήγορο καθώς οι υπολογισμοί περιλαμβάνουν μόνο πολλαπλασιασμούς. Ο $\mathcal{P}^*$ μπορεί να ξεγελάσει τον $\mathcal{V}$ με πιθανότητα $1/2^k$.

Το πρόβλημα του παράλληλου υπολογισμού. Είναι φανερό ότι η μηδενική γνώση είναι μία ιδιότητα του αποδείκτη ενός IPS. Η μηδενική γνώση διατηρείται σε σειριακή σύνθεση εκτελέσεων ZK-IPS, εάν οι αποδείκτες είναι aux-ITM [GO94 §3.3], όχι όμως και στη γενική περίπτωση του Ορισμού 3.2.4 [GK96 Theorem 4.1]. Όταν εκτελείται παράλληλος υπολογισμός, η ιδιότητα δε διατηρείται ούτε στο ακόμα

ισχυρότερο μοντέλο, όπου θεωρείται ότι υπάρχει *καθολικός προσομοιωτής* (*black-box simulator*) $M_{\mathcal{P}}$ του διαλόγου μεταξύ του αποδείκτη $\mathcal{P}$ με κάθε επαληθευτή $\mathcal{V}^*$, με τον $M_{\mathcal{P}}$ να καλεί τον εκάστοτε $\mathcal{V}^*$ ως μαντείο [GK96 §5]. Το μειονέκτημα της μη διατήρησης υπό παράλληλη σύνθεση δεν εμφανίζεται σε μία πιο ασθενή ιδιότητα του αποδείκτη, την μη διακρισιμότητα μάρτυρος, την οποία εισήγαγαν οι U.Feige και A.Shamir [FS90].

Ορισμός 3.2.6. Έστω aux-IPS $(\mathcal{P}, \mathcal{V})$ για τη γλώσσα $L \in \mathbf{NP}$ και έστω R_L *σχέση μαρτυρίας* (*witness relation*) για την L [1]. Λέμε ότι το $(\mathcal{P}, \mathcal{V})$ έχει *μη διακρισιμότητα μάρτυρος* (*witness indisinguishability - WI*), εάν για κάθε πολυωνυμικό επαληθευτή V^* και κάθε δύο ακολουθίες $\{w_x^1\}_{x\in L}$, $\{w_x^2\}_{x\in L}$ οι οικόγενειες τ.μ.

$$\{\langle \mathcal{P}(w_x^1), \mathcal{V}^*(z)\rangle(x)\}_{x\in L, z\in\{0,1\}^*} \text{ και } \{\langle \mathcal{P}(w_x^2), \mathcal{V}^*(z)\rangle(x)\}_{x\in L, z\in\{0,1\}^*},$$

είναι υπολογιστικά μη διακρίσιμες.

Περιγραφικά, ένα σύστημα είναι WI εάν ο επαληθευτής δεν μπορεί να διακρίνει αποδείξεις που χρησιμοποιούν διαφορετικούς μάρτυρες. Τετριμμένα ισχύει ότι κάθε IPS χωρίς βοηθητικές εισόδους αλλά και κάθε αποδεικτικό σύστημα όπου για κάθε x ο R_L-μάρτυρας w του x για την L είναι μοναδικός είναι WI. Κάθε ZK-IPS είναι και WI-IPS, αφού η έξοδος ενός προσομοιωτή συστήματος μηδενικής γνώσης είναι ανεξάρτητη από τον μάρτυρα που χρησιμοποιεί ο αποδείκτης. Το αντίστροφο δεν ισχύει, όπως φαίνεται στο επόμενο παράδειγμα.

Παράδειγμα 3.2.7. Έστω μετάθεση μονής κατεύθυνσης f. Ορίζουμε γλώσσα

$$L_0 = \{y \mid \text{το πρώτο bit του } f^{-1}(y) \text{ είναι } 0\},$$

καθώς επίσης σχέση μαρτυρίας $R_L = \{(f(w), w) \mid w \in \{0,1\}^*\}$. Έστω aux-IPS $(\mathcal{P}, \mathcal{V})$ για την L_0 όπου ο $\mathcal{P}$ με κοινή είσοδο y και βοηθητική είσοδο $f^{-1}(y)$, στέλνει $f^{-1}(y)$ στον $\mathcal{V}$. Το $(\mathcal{P}, \mathcal{V})$ είναι WI αλλά όχι ZK.

Απόδειξη. Το $(\mathcal{P}, \mathcal{V})$ είναι προφανώς WI λόγω μοναδικότητας των μαρτύρων $f^{-1}(y)$. Από την άλλη, χωρίς τη γνώση του $f^{-1}(y)$ ο επαληθυτής δεν μπορεί να επιτύχει τίποτα σημαντικά καλύτερο από το να ρίξει ένα νόμισμα, αφού η f είναι μονής κατεύθυνσης. Επομένως το $(\mathcal{P}, \mathcal{V})$ δεν είναι ZK.

⊣

Στο επόμενο θεώρημα αποδεικνύεται ότι η ιδιότητα της μη διακρισιμότητας μάρτυρος διατηρείται στην περίπτωση της *πολυωνυμικής γενικής σύνθεσης*, όπου πεπερασμένα το πλήθος IPS με αποδείκτες πολυωνυμικού χρόνου εκτελούνται ταυτόχρονα

[1] δηλ. $R_L(x, w) \Leftrightarrow |w| \leqslant poly(|x|) \wedge x \in L$ και η R_L είναι πολυωνυμικά επαληθεύσιμη.

και πολυωνυμικά, ως προς το μέγεθος των εισόδων, πολλές φορές με σειριακό ή παράλληλο τρόπο ή και με οποιαδήποτε παρεμβολή μεταξύ των σταδίων των πρωτοκόλλων. Το ισχυρό αυτό μοντέλο αποτυπώνει ρεαλιστικά τις δυνατότητες εκμετάλλευσης πληροφοριών από ένα κακόβουλο χρήστη (επαληθευτή).

Θεώρημα 3.2.8. *Έστωσαν WI-IPS* $(\mathcal{P}_i, \mathcal{V}_i)$ *για τις σχέσεις* R_{L_i}, $i = 1, \ldots, t$ *και* $(\mathcal{P}, \mathcal{V})$ *το IPS που προκύπτει από τη γενική σύνθεση* $(\mathcal{P}_{i_1}, \mathcal{V}_{i_1}), \ldots, (\mathcal{P}_{i_{q(n)}}, \mathcal{V}_{i_{q(n)}})$, *όπου* q *πολυώνυμο και* $i_j \in [t]$, $j = 1, \ldots, q(n)$. *Εάν οι* $\mathcal{P}_i$, $i = 1, \ldots, t$ *είναι πολυωνυμικού χρόνου, τότε το* $(\mathcal{P}, \mathcal{V})$ *είναι WI για τη σχέση*

$$R_L = \{(\bar{x}, \bar{w} \mid \forall j, (x_j, w_j) \in R_{L_{i(j)}}\},$$

όπου $\bar{x} = (x_1, \ldots, x_{q(n)})$, *η κοινή είσοδος του* $(\mathcal{P}, \mathcal{V})$ *και* $\bar{w} = (w_1, \ldots, w_{q(n)})$ *η βοηθητική είσοδος του* $\mathcal{P}$.

Απόδειξη. (*Σκιαγράφηση*). Έστω επαληθευτής V^* που διακρίνει τους μάρτυρες $\bar{w^1} = (w_1^1, \ldots, w_{q(n)}^1)$, $\bar{w^2} = (w_1^2, \ldots, w_{q(n)}^2)$ της κοινής εισόδου $\bar{x}$. Εφαρμόζοντας *υβριδικό επιχείρημα* (*hybrid argument*) έχουμε ότι για κάποιο k ο V^* διακρίνει τους μάρτυρες

$$(w_1^1, \ldots, w_k^1, w_{k+1}^2, \ldots, w_{q(n)}^2) \quad \text{και} \quad (w_1^1, \ldots, w_{k+1}^1, w_{k+2}^2, \ldots, w_{q(n)}^2).$$

Κατασκευάζουμε επαληθευτή V_{k+1}^*, ο οποίος έχοντας ως βοηθητική είσοδο τα $\bar{x}$ και $w_1^1, \ldots, w_k^1, w_{k+2}^2, \ldots, w_n^2$, προσομοιώνει το διάλογο των $\mathcal{P}_{i_j}, \mathcal{V}_{i_j}$, $j \neq k+1$ ως εξής: επιλέγει για κάθε j-οστή εκτέλεση, $j \neq k+1$, κοινή είσοδο x_j και βοηθητική είσοδο αποδείκτη w_j. Στη συνέχεια καλεί τους $\mathcal{P}, \mathcal{V}^*$ και για κάθε μήνυμα $m_1, \ldots, m_{q(n)}$ που στέλνει ο $\mathcal{V}^*$, ο V_{k+1}^* προωθεί κάθε m_j, $j \in [q(n)] \backslash \{k+1\}$ στον αντίστοιχο αποδείκτη P_{i_j}. Ως αποτέλεσμα, αφήνεται «ελεύθερος» μόνο ο διάλογος των $\mathcal{P}_{i_{k+1}}, \mathcal{V}_{k+1}^*$. Συνεπώς έχουμε ότι για κοινή είσοδο x_{k+1}

$$| \mathbf{Pr}[\langle \mathcal{P}_{i_{k+1}}(w_{k+1}^1), \mathcal{V}_{k+1}^*(z) \rangle (x_{k+1})) = 1] - \mathbf{Pr}[\langle \mathcal{P}_{k+1}(w_{k+1}^2), \mathcal{V}_{k+1}^*(z) \rangle (x_{k+1})) = 1] \mid =$$

$$= | \mathbf{Pr}[\langle \mathcal{P}(\bar{w^1}), \mathcal{V}^*(z) \rangle (\bar{x})) = 1] - \mathbf{Pr}[\langle \mathcal{P}(\bar{w^2}), \mathcal{V}^*(z) \rangle (\bar{x})) = 1] \mid,$$

Επομένως ο V_{k+1}^* μπορεί να διακρίνει τους w_{k+1}^1, w_{k+1}^2 και άρα το $(\mathcal{P}_{i_{k+1}}, \mathcal{V}_{i_{k+1}})$ δεν είναι WI, άτοπο.

$\dashv$

3.3 Μη Διαλογικά Συστήματα Απόδειξης

Τα μη διαλογικά συστήματα απόδειξης είναι μία εκδοχή των IPS όπου δεν υπάρχει καμία παραπάνω αλληλεπίδραση πέρα από την αποστολή της απόδειξης στον επαληθευτή. Στο συνηθέστερο μη διαλογικό μοντέλο, οι δύο πλευρές έχουν πρόσβαση,

πέραν της κοινής εισόδου, σε ένα τυχαίο *string κοινής αναφοράς* (*common reference string - CRS*). Ο ορισμός των μη διαλογικών συστημάτων απόδειξης στο CRS δόθηκε M.Blum, P.Feldman και S.Micali [BFM88], οι οποίοι επίσης απέδειξαν την ύπαρξη NIZK σύστηματος απόδειξης για έναν ισχυρισμό «$x \stackrel{?}{\in} L$», για κάθε γλώσσα L στο **NP**. Οι M.Blum κ.ά. [BSMP91], επέκτειναν το [BFM88], σε NIZK σύστημα απόδειξης πολυωνυμικού πλήθους ισχυρισμών. Και οι δύο παραπάνω κατασκευές στηρίζονται στην *υπόθεση τετραγωνικών υπολοίπων* (*quadratic residue assumption -QRA*) και παρουσιάζουν κυρίως θεωρητικό ενδιαφέρων καθώς είναι αρκετά πολύπλοκες. Σημαντική ωστόσο απόρροια της απόδειξης του [BSMP91] είναι ότι ο αποδείκτης μπορεί να είναι μία PPT TM με βοηθητική είσοδο έναν μάρτυρα της κοινής εισόδου x. Νωρίτερα, οι U.Feige, D.Lapidot και A.Shamir [FLS90], στηριζόμενοι σε γενικές υποθέσεις πολυπλοκότητας, κατασκεύασαν NIZK σύστηματα αποδειξης για κάθε γλώσσα στο **NP** και παράλληλα έδειξαν πώς πολυωνυμικού πλήθους αποδείκτες μπορούν να μοιραστούν το ίδιο CRS. Δεχόμενοι την ύπαρξη trapdoor μεταθέσεων, οι αποδείκτες στο [FLS90] μπορούν να είναι πολυωνυμικού χρόνου όπως παραπάνω.

Σε ένα μη διαλογικό σύστημα απόδειξης οι ορισμοί της μηδενικής γνώσης και της μη διακρισιμότητας μάρτυρος είναι απλούστεροι, αφού η μη αλληλεπίδραση με τον αποδείκτη καθιστά επαρκή την προσομοίωση της δράσης μόνο του αρχικού επαληθευτή. Απαραίτητη για την κατασκευή ασφαλών σχημάτων κρυπτογράφησης είναι η θεώρηση κακόβουλων αποδεικτών και προσομοιωτών που λειτουργούν *προσαρμοστικά*. Επομένως, τροποποιούμε τον αρχικό ορισμό του [BFM88], υποθέτοντας ότι η κοινή είσοδος x επιλέγεται από τον αντίπαλο αφού γνωστοποιηθεί το CRS και ο προσομοιωτής εξάγει CRS της επιλογής του. Τυπικά έχουμε

Ορισμός 3.3.1. Ένα ζεύγος πιθανοτικών TM $(\mathcal{P}, \mathcal{V})$ καλείται *μη διαλογικό σύστημα απόδειξης* (*non-interactive proof system - NIPS*) για μία γλώσσα L εάν η $\mathcal{V}$ είναι πολυωνυμικού χρόνου και ικανοποιούνται οι δύο εξής συνθήκες:

(i). *Πληρότητα*: για κάθε $x \in L$

$$\mathbf{Pr}[\pi \leftarrow \mathcal{P}(w_x, x, r) : \mathcal{V}(x, r, \pi) = 1] \geqslant \frac{2}{3},$$

όπου r είναι τυχαίο string ομοιόμορφα κατανεμημένο στο $\{0,1\}^{poly(|x|)}$ και w_x μάρτυρας του x για την L.

(ii). *Ορθότητα*: για κάθε TM $\mathcal{B}$

$$\mathbf{Pr}[(x, \pi) \leftarrow \mathcal{B}(r) : \mathcal{V}(x, r, \pi) = 1 \wedge x \notin L] \leqslant \frac{1}{3},$$

όπου r όπως πριν.

Σημειώνουμε ότι ο ορισμός της προσαρμοστικής πληρότητας, αν και δυνατός, δεν είναι αναγκαίος καθώς όλα τα συνήθη κρυπτογραφικά πρωτόκολλα έχουν τέλεια πληρότητα, δηλαδή μηδενική πιθανότητα σφάλματος.

Ορισμός 3.3.2. Ένα NIPS $(\mathcal{P}, \mathcal{V})$ είναι *μηδενικής γνώσης* (*NIZK-PS*), εάν υπάρχει PPT αλγόριθμος $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ ώστε για κάθε αντίπαλο $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$

$$\mathbf{Pr}[r \xleftarrow{\$} \{0,1\}^{poly(n)}; (x, w_x) \leftarrow \mathcal{A}_1(r); \pi \leftarrow \mathcal{P}(w_x, x, r) : \mathcal{A}_2(r, x, \pi) = 1]$$

$$\approx \mathbf{Pr}[(r, \tau) \leftarrow \mathcal{S}_1(1^n); (x, w_x) \leftarrow \mathcal{A}_1(r); \pi \leftarrow \mathcal{S}_2(x, \tau) : \mathcal{A}_2(r, x, \pi) = 1],$$

όπου $\approx$ συμβολίζει την αμελητέα διαφορά των δύο πιθανοτήτων και w_x μάρτυρας του x για την L.

Ορισμός 3.3.3. Ένα NIPS $(\mathcal{P}, \mathcal{V})$ έχει *μη διακρισιμότητα μάρτυρος* (*NIWI-PS*), εάν για κάθε αντίπαλο $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ και κάθε δύο ακολουθίες $\{w_x^1\}_{x \in L}$, $\{w_x^2\}_{x \in L}$

$$\mathbf{Pr}[r \xleftarrow{\$} \{0,1\}^{poly(n)}; (x, w_x^1, w_x^2) \leftarrow \mathcal{A}_1(r); \pi \leftarrow \mathcal{P}(w_x^1, x, r) : \mathcal{A}_2(r, x, \pi) = 1]$$

$$\approx \mathbf{Pr}[r \xleftarrow{\$} \{0,1\}^{poly(n)}; (x, w_x^1, w_x^2) \leftarrow \mathcal{A}_1(r); \pi \leftarrow \mathcal{P}(w_x^2, x, r) : \mathcal{A}_2(r, x, \pi) = 1],$$

όπου w_x^1, w_x^2 μάρτυρες του x για την L.

Παράδειγμα 3.3.4. Δεδομένου σχήματος κρυπτογράφησης $\mathbf{C} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ με ασφάλεια CPA και ενός NIZK-PS για **NP** γλώσσες $(\mathcal{P}, \mathcal{V})$ κατασκευάζεται σχήμα κρυπτογράφησης $\mathbf{C}^*$ με ασφάλεια CCA1 που συνίσταται από τους παρακάτω αλγορίθμους:

- $\mathcal{G}^*(1^k)$. Εκτελείται δύο φορές ο $\mathcal{G}(1^k)$ και παράγονται ζεύγη κλειδιών (sk_1, pk_1), (sk_2, pk_2). Επιλέγεται τυχαίο $r \in \{0,1\}^{poly(k)}$ και το ζεύγος δημόσιου και ιδιωτικού κλειδιού στο νέο σχήμα είναι $sk^* = sk_1$, $pk^* = (pk_1, pk_2, r)$.

- $\mathcal{E}^*(pk^*, M)$. Επιλέγονται τυχαία $w_1, w_2 \in \{0,1\}^*$, υπολογίζονται τα κρυπτοκείμενα $C_1 = \mathcal{E}(M||w_1)$, $C_2 = \mathcal{E}(M||w_2)$ και ο $\mathcal{P}$ εξάγει την απόδειξη $\mathcal{P}(r, (c_1, c_2), (w_1, w_2, M))$. Το κρυπτοκείμενο για το M είναι το

$$C = \langle C_1, C_2, \pi \rangle.$$

- $\mathcal{C}^*(sk^*, C)$. Εάν $\mathcal{V}(r, (c_1, c_2), \pi) = 1$, τότε υπολογίζεται το $\mathcal{D}(sk_1, C_1)$, αλλιώς επιστρέφεται $\perp$.

Η αναλυτική παρουσίαση και η απόδειξη ασφάλειας του σχήματος δίνονται στο [NY90].

Μη διαλογικά συστήματα στο ROM. Ένα διαφορετικό μοντέλο κατασκευής μη διαλογικών πρωτοκόλλων προκύπτει εάν αντί του CRS θεωρηθεί ότι ο αποδείκτης και ο επαληθευτής έχουν κοινή γνώση ενός τυχαίου μαντείου H. Η πληρότητα και η ορθότητα ενός NIPS ορίζονται για οποιαδήποτε H αντίστοιχα με τον Ορισμό 3.3.1. Η βασική ιδέα μετατροπής διαλογικών πρωτοκόλλων σε NIPS στο ROM αποδίδεται στον M.Blum ο οποίος χρησιμοποιώντας τις ευρετικές τεχνικές των A.Fiat και A.Shamir [FS86], αντικατέστησε τα ερωτήματα ενός επαληθευτή με hashing γνωστών μηνυμάτων. Αυστηρός ορισμός της μηδενικής γνώσης στο ROM δόθηκε από τους M.Bellare και A.Rogaway [BR93 §5]: ο αποδείκτης διαθέτει βοηθητική είσοδο w και ο επαληθευτής ιδιωτικό τυχαίο string r. Ο προσομοιωτής $\mathcal{S}$ επιτρέπεται να προγραμματίσει ένα πολυωνυμικό τμήμα του τυχαίου μαντείου R, δηλαδή πολυωνυμικό πλήθος ζευγών $(x_1, y_1), \ldots, (x_t, y_t)$ όπου $R(x_i) = y_i$, $i = 1, \ldots, t$, ενώ το υπολόποιπο μέρος του R θεωρείται τυχαίο για τον $\mathcal{S}$. Όπως και πριν, η μηδενική γνώση προκύπτει από την μη διακρισιμότητα των $\{\langle \mathcal{P}(w), \mathcal{V}(r)\rangle(x)\}_{x\in L}$ και $\{\mathcal{S}(x)\}_{x\in L}$. Στο [BR93 §5.2] δίνεται γενική μέθοδος κατασκευής NIZK-PS στο ROM από τυχαίο IPS-ZK για γλώσσα L. Πρόσφατη μελέτη της μηδενικής γνώσης στο ROM βρίσκεται στα [Pas03], [Wee09].

Η επόμενη πρόταση αφορά στην κατασκευή NIZK-PS στο ROM από τα πολύ διαδεδομένα Σ-πρωτόκολλα.

Ορισμός 3.3.5. Ένα πρωτόκολλο $(\mathcal{P}, \mathcal{V})$ τριών γύρων είναι Σ-*πρωτόκολλο* για τη γλώσσα L εάν ικανοποιούνται οι εξής συνθήκες:

(i). *Πληρότητα*.

(ii). *Ειδική Ορθότητα*: με κοινή είσοδο x, για κάθε ζεύγος αποδεκτικών διαλόγων δέσμευσης, πρόκλησης, απάντησης (r, b, a) και (r, b', a'), όπου $b \neq b'$, μπορεί να εξαχθεί μάρτυρας w του x για την L.

(iii). *Ειδική HVZK*: υπάρχει προσομοιωτής $\mathcal{S}$, οποίος με είσοδο x και πρόκληση b επιστρέφει αποδεκτικό διάλογο (r, b, a) που ακολουθεί την ίδια κατανομή με τον πραγματικό διάλογο μεταξύ των $\mathcal{P}, \mathcal{V}$ με κοινή είσοδο x.

Εύκολα προκύπτει ότι το πρωτόκολλο του Schnorr (Παράδειγμα 3.1.6) ικανοποιεί την ειδική HVZK και άρα είναι Σ-πρωτόκολλο.

Πρόταση 3.3.6. *Έστω Σ-πρωτόκολλο $(\mathcal{P}, \mathcal{V})$: $\mathcal{P} \xrightarrow{r} \mathcal{V}$, $\mathcal{P} \xleftarrow{b} \mathcal{V}$, $\mathcal{P} \xrightarrow{a} \mathcal{V}$. Έστω $(\mathcal{P}^H, \mathcal{V}^H)$ το σύστημα που προκύπτει από το $(\mathcal{P}, \mathcal{V})$ αν ο $\mathcal{P}$ αντικαταστήσει τον γύρο $\mathcal{P} \xleftarrow{b} \mathcal{V}$ με ερώτημα σε τυχαίο μαντείο H για το (r, x), όπου x η κοινή είσοδος, υπολογίσει το a βάσει του $b = H(r, x)$ και αποστείλει την απόδειξη (r, a). Ο $\mathcal{V}^H$ θέτει το ερώτημα $H(r, x)$ για να λάβει το b και στη συνέχεια επαληθεύει όπως ο $\mathcal{V}$. Το $(\mathcal{P}^H, \mathcal{V}^H)$ είναι NIZK-PS-PoK στο ROM .*

Απόδειξη. (*Σκιαγράφηση*) Η πληρότητα του $(\mathcal{P}^H, \mathcal{V}^H)$ είναι προφανής. Για τη μηδενική γνώση, παρατηρούμε πρώτα ότι η ειδική HVZK συνεπάγεται την HVZK. Πράγματι, δεδομένου προσομοιωτή ειδικής HVZK $\mathcal{S}$ κατασκευάζουμε HVZK προσομοιωτή $\mathcal{S}'$, ο οποίος με είσοδο x επιλέγει τυχαίο b, καλεί τον $\mathcal{S}$ με είσοδο (x, b) και επιστρέφει την έξοδο του $\mathcal{S}$, (r, b, a). Ο ZK προσομοιωτής $\mathcal{S}^*$ καλεί τον $\mathcal{S}'$ με είσοδο x και λαμβάνει τριάδα (r, b, a). Προγραμματίζει την H ως $b = H(r, x)$ και επιστρέφει την τριάδα (r, b, a) που ακολουθεί την ίδια κατανομή με την $(r, H(r, x), a)$ του πραγματικού διαλόγου[2].

Η απόδειξη γνώσης προκύπτει από την ύπαρξη εξαγωγέα γνώσης $\mathcal{K}$, ο οποίος από αποδείκτη $\mathcal{P}^*$, λαμβάνει την απόδειξη (r, a), επαναπρογραμματίζει την H ως $b' = H(r, x)$, $b' \neq b$ και περιμένει νέα απάντηση (r, a') από τον $\mathcal{P}^*$. Εάν οι (r, a), (r, a') είναι αποδεκτές, τότε εξάγει μάρτυρα w του x από τις τριάδες (r, b, a) και (r, b', a'), όπως εγγυάται η ειδική ορθότητα του $(\mathcal{P}, \mathcal{V})$.

⊣

Οι O.Goldreich και Y.Oren έδειξαν ότι δεν υπάρχουν IPS ενός γύρου και μηδενικής γνώσης για γλώσσες εκτός του **BPP** στο standard μοντέλο [GO94 Theorem 4.3], το οποίο συνεπάγεται ότι το μοντέλο CRS είναι απαραίτητο στην κατασκευή ενδιαφέροντων κρυπτογραφικών σχημάτων που χρησιμοποιούν NIZK-PS και δε στηρίζουν την ασφάλειά τους στο ROM. Για αυτόν το λόγο πολλοί ερευνητές υπονοούν την ύπαρξη CRS, παραγόμενου από μία έμπιστη αρχή, όταν αναφέρονται σε σχήματα στο standard μοντέλο, όπως θα δούμε στο κεφάλαιο 4. Ο R.Pass [Pas03] εντοπίζει την εγγενή αδυναμία των NIZK-PS στο μοντέλο CRS να πληρούν την ιδιότητα της *διαψευσιμότητας* (*deniability*), δηλαδή της εκτέλεσης του προσομοιωτή από τον ίδιο τον επαληθευτή διότι σε ένα μη διαλογικό πρωτόκολλο, το CRS είναι μία δημόσια και προκαθορισμένη πληροφορία. Επομένως, σε εφαρμογές όπου η διαψευσιμότητα είναι βασικός στόχος (βλ. [DNS98 §1.3]) τα NIZK-PS στο μοντέλο CRS είναι ακατάλληλα.

3.4 Το σύστημα απόδειξης Groth-Sahai

Οι μη διαλογικές αποδείξεις αναπαριστούν με ακρίβεια κρυπτογραφικά πρωτόκολλα όπου η αλληλεπίδραση είτε δεν είναι δυνατή ή είναι αποφευκτέα. Ένα από τα σημαντικότερα πρακτικά προβλήματα που εμφανίζει το CRS μοντέλο είναι η πιθανή αναγωγή σε **NP**-πλήρη γλώσσα (π.χ. Circuit-SAT). Μέχρι πρόσφατα, το ROM ήταν το κύριο μοντέλο συστηματικής κατασκευής αποδοτικών μη διαλογικών πρωτοκόλλων, το οποίο όμως έχει υποστεί αμφισβήτηση, αρχής γενομένης στο [CGH98], ως προς το κατά πόσον παρέχει πραγματική ασφάλεια. Εξάλλου, για

[2] Είναι φανερό ότι η HVZK είναι ικανή για την ZK του $(\mathcal{P}^H, \mathcal{V}^H)$

την κατασκευή NIPS με την ασφάλεια του CRS μοντέλου εφαρμόσιμων στην κρυπτογραφία ζευγμάτων είναι χρήσιμος ο συσχετισμός με γλώσσες που προέρχονται από προβλήματα βασισμένα σε ζεύγματα. Τα πρώτα σημαντικά αποτελέσματα προς αυτήν την κατεύθυνση συναντώνται στις μη διαλογικές αποδείξεις των [GOS06a], [GOS06b], [Gro06], στερούνται όμως αποδοτικότητας καθώς συνίστανται από ευθύ συνδυασμό πολλών μικρότερων. Η σπουδαιότητα της εργασίας των J.Groth και A.Sahai [GS08] είναι η επινόηση μίας γενικής μεθοδολογίας για την κατασκευή σύντομων μη διαλογικών αποδείξεων για γλώσσες που στηρίζονται σε προβλήματα ζευγμάτων (group-depended languages). Ανάλογες αποδείξεις μηδενικής γνώσης για τέτοιες γλώσσες δεν προϋπήρχαν ούτε στην ευρύτερη κατηγορία των IPS.

Για την καλύτερη παρουσίαση των GS-αποδείξεων προσαρμόζουμε το συμβολισμό γνωστών εννοιών στη γραφή του [GS08].

- Έστω σχέση R που αποτελείται από τριάδες (gk, x, w) όπου gk το Setup, x ο ισχυρισμός και w ο αντίστοιχος μάρτυρας. Μία γλώσσα L που αποτελείται από ισχυρισμούς της R στηρίζεται σε ζεύγματα εάν το gk περιγράφει κάποιο ζεύγμα.

- Ένα NIPS για τη σχέση R είναι μία τετράδα PPT αλγορίθμων $(\mathcal{G}, \mathcal{K}, \mathcal{P}, \mathcal{V})$ όπου ο $\mathcal{G}$ επιστρέφει ζεύγος Setup, πρόσθετης (πιθανώς κενής) πληροφορίας (gk, sk), ο $\mathcal{K}$ με είσοδο (gk, sk) κατασκευάζει το CRS σ, ο αποδείκτης $\mathcal{P}$ με είσοδο (gk, σ, x, w) παράγει απόδειξη π και ο επαληθευτής $\mathcal{V}$ ελέγχει την εγκυρότητα της απόδειξης με είσοδο (gk, σ, x, π). Η πληρότητα του $(\mathcal{G}, \mathcal{K}, \mathcal{P}, \mathcal{V})$ απαιτείται τέλεια, δηλαδή

  $$\mathbf{Pr}[\mathcal{V}(gk, \sigma, x, \pi) = 1 \mid (gk, x, w) \in R] = 1,$$

  ενώ η ορθότητα εξασφαλίζεται θεωρώντας αμελητέα την πιθανότητα

  $$\mathbf{Pr}[(x, \pi) \leftarrow \mathcal{A}(gk, \sigma) : V(gk, \sigma, x, \pi) = 1 \mid x \notin L],$$

  για κάθε αντίπαλο $\mathcal{A}$.

- Στο συνήθη ορισμό της ορθότητας, ο αντίπαλος επιχειρεί να πείσει τον $\mathcal{V}$ για $x \in \bar{L}$. Επεκτείνοντας τον ορισμό έχουμε την ιδιότητα της L_{co}-*ορθότητας*, όπου L_{co} τυχαία γλώσσα εξαρτώμενη από τα gk, σ. Επομένως θεωρούμε αμελητέα την πιθανότητα

  $$\mathbf{Pr}[(x, \pi) \leftarrow \mathcal{A}(gk, \sigma) : V(gk, \sigma, x, \pi) = 1 \mid x \in L_{co}],$$

  για κάθε αντίπαλο $\mathcal{A}$.

- Ο ορισμός της μη διακρισιμότητας μάρτυρος ισχυροποιείται στη *συνθέσιμη WI* (*composable WI - co-WI*), όπου ο προσομοιωτής $\mathcal{S}$ δημιουργεί ένα CRS το οποίο είναι μη διακρίσιμο από αυτό που παράγει ο $\mathcal{K}$ και παράλληλα δεν παρέχει καμία πληροφορία που θα καθιστά διακρίσιμους δύο διαφορετικούς μάρτυρες. Τυπικά για κάθε αντίπαλο $\mathcal{A}$ ζητούμε

$$\begin{aligned}\mathbf{Pr}[(gk, sk) \leftarrow \mathcal{G}(1^k); \sigma \leftarrow \mathcal{K}(gk, sk) : \mathcal{A}(gk, \sigma) = 1] \approx \\ \approx \mathbf{Pr}[(gk, sk) \leftarrow \mathcal{G}(1^k); \sigma \leftarrow \mathcal{S}(gk, sk) : \mathcal{A}(gk, \sigma) = 1]\end{aligned}$$

και

$$\begin{aligned}\mathbf{Pr}[\sigma \leftarrow \mathcal{S}(gk, sk); (x, w_0, w_1) \leftarrow \mathcal{A}(gk, \sigma); \pi \leftarrow \mathcal{P}(gk, \sigma, x, w_0) : \mathcal{A}(\pi) = 1] \approx \\ \approx \mathbf{Pr}[\sigma \leftarrow \mathcal{S}(gk, sk); (x, w_0, w_1) \leftarrow \mathcal{A}(gk, \sigma); \pi \leftarrow \mathcal{P}(gk, \sigma, x, w_1) : \mathcal{A}(\pi) = 1].\end{aligned}$$

- Ανάλογα ενισχύουμε τον ορισμό της μηδενικής γνώσης στη *συνθέσιμη ZK* (*composable ZK - co-ZK*) υποθέτοντας ότι ο προσομοιωτής $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ παράγει μη διακρίσιμο CRS σ και πρόσθετη πληροφορία τ η οποία δεν προσδίδει κάποιο σημαντικό πλεονέκτημα στον αντίπαλο ώστε να διακρίνει τις προσομοιωμένες αποδείξεις. Ισχύει δηλαδή ότι

$$\begin{aligned}\mathbf{Pr}[(gk, sk) \leftarrow \mathcal{G}(1^k); \sigma \leftarrow \mathcal{K}(gk, sk) : \mathcal{A}(gk, \sigma) = 1] \approx \\ \approx \mathbf{Pr}[(gk, sk) \leftarrow \mathcal{G}(1^k); (\sigma, \tau) \leftarrow \mathcal{S}_1(gk, sk) : \mathcal{A}(gk, \sigma) = 1]\end{aligned}$$

και

$$\begin{aligned}\mathbf{Pr}[(\sigma, \tau) \leftarrow \mathcal{S}_1(gk, sk); (x, w) \leftarrow \mathcal{A}(gk, \sigma, \tau); \pi \leftarrow \mathcal{P}(gk, \sigma, x, w) : \mathcal{A}(\pi) = 1] \approx \\ \approx \mathbf{Pr}[(\sigma, \tau) \leftarrow \mathcal{S}_1(gk, sk); (x, w) \leftarrow \mathcal{A}(gk, \sigma, \tau); \pi \leftarrow \mathcal{S}_2(gk, \sigma, \tau, x) : \mathcal{A}(\pi) = 1],\end{aligned}$$

όπου $(gk, x, w) \in R$.

Οι εξισώσεις Groth-Sahai. Το μη διαλογικό σύστημα απόδειξης Groth-Sahai *GSPS* παράγει αποδείξεις για την ταυτόχρονη ισχύ συνόλου εξισώσεων που ανήκουν στις παρακάτω κατηγορίες:
Έστω ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, όπου $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ τάξης n και μεταβλητές $X_1, \ldots, X_m \in \mathbb{G}_1$, $Y_1, \ldots, Y_n \in \mathbb{G}_2$, $x_1, \ldots, x_{m'}, y_1, \ldots, y_{n'} \in \mathbb{Z}_{\mathbf{n}}$.

Εξίσωση γινομένου-ζεύγματος:

$$\prod_{i=1}^{n} e(A_i, Y_i) \cdot \prod_{i=1}^{m} e(X_i, B_i) \cdot \prod_{i=1}^{m} \prod_{j=1}^{n} e(X_i, Y_j)^{\gamma_{ij}} = t_T, \tag{3.1}$$

όπου $A_i \in \mathbb{G}_1, B_i \in \mathbb{G}_2, t_T \in \mathbb{G}_T, \gamma_{ij} \in \mathbb{Z}_{\mathbf{n}}$.

Εξίσωση βαθμωτού πολλαπλασιασμού στην $\mathbb{G}_1$:

$$\sum_{i=1}^{n'}[y_i]A_i + \sum_{i=1}^{m}[b_i]X_i + \sum_{i=1}^{m}\sum_{j=1}^{n'}[\gamma_{ij}y_j]X_i = T_1, \tag{3.2}$$

όπου $A_i, T_1 \in \mathbb{G}_1$ και $b_i, \gamma_{ij} \in \mathbb{Z}_{\mathbf{n}}$.

Εξίσωση βαθμωτού πολλαπλασιασμού στην $\mathbb{G}_2$:

$$\sum_{i=1}^{n}[a_i]Y_i + \sum_{i=1}^{m'}[x_i]B_i + \sum_{i=1}^{m'}\sum_{j=1}^{n}[\gamma_{ij}x_j]Y_i = T_2, \tag{3.3}$$

όπου $B_i, T_2 \in \mathbb{G}_2$ και $a_i, \gamma_{ij} \in \mathbb{Z}_{\mathbf{n}}$.

Τετραγωνική Εξίσωση στην $\mathbb{Z}_n$:

$$\sum_{i=1}^{n'}a_iy_i + \sum_{i=1}^{m'}x_ib_i + \sum_{i=1}^{m'}\sum_{j=1}^{n'}\gamma_{ij}x_iy_j = t, \tag{3.4}$$

όπου $a_i, b_i, \gamma_{ij}, t \in \mathbb{Z}_{\mathbf{n}}$.

Για την απλοποίηση των (3.1-4) είναι χρήσιμη η παρακάτω έννοια:

Ορισμός 3.4.1. Έστω μεταθετικός δακτύλιος $(\mathcal{R}, +, \cdot, 0, 1)$. Μια αβελιανή ομάδα $\mathbb{G}$ είναι $\mathcal{R}$-*πρότυπο* ($\mathcal{R}$-*module*) εάν ο $\mathcal{R}$ δρα πάνω στην $\mathbb{G}$ έτσι ώστε για κάθε $r, s \in \mathcal{R}$ και $x, y \in \mathbb{G}$:

$$(r+s)x = rx + sx \wedge r(x+y) = rx + ry \wedge r(sx) = (rs)x \wedge 1x = x.$$

Σύμφωνα με τον Ορισμό 3.4.1, οι $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ είναι $\mathbb{Z}_n$-πρότυπα. Επίσης για διγραμμική απεικόνιση $f : G_1 \times G_2 \longrightarrow G_T$ και $x_1, \ldots, x_m \in G_1$ και $y_1, \ldots, y_n \in G_2$ θεωρούμε την γενική τετραγωνική εξίσωση

$$\vec{a} \cdot \vec{y} + \vec{x} \cdot \vec{b} + \vec{x} \cdot \Gamma\vec{y} = t, \tag{3.5}$$

όπου $\Gamma \in Mat_{m\times n}(\mathcal{R})$ και $\vec{p} \cdot \vec{q} = \sum_i f(p_i, q_i)$.

Είναι φανερό ότι οι (3.1-4) αποτελούν ειδικές περιπτώσεις της (3.5) και μπορούν να γραφούν ως

Εξίσωση γινομένου-ζεύγματος:

$$G_1 = \mathbb{G}_1, G_2 = \mathbb{G}_2, G_T = \mathbb{G}_T, f(X,Y) = e(X,Y)$$
$$(\vec{A} \cdot \vec{Y})(\vec{X} \cdot \vec{B})(\vec{X} \cdot \Gamma\vec{Y}) = t_T. \tag{3.6}$$

Εξίσωση βαθμωτού πολλαπλασιασμού στην $\mathbb{G}_1$:

$$G_1 = \mathbb{G}_1, G_2 = \mathbb{Z}_{\mathbf{n}}, G_T = \mathbb{G}_1, f(X, y) = [y]X$$
$$\vec{A} \cdot \vec{y} + \vec{X} \cdot \vec{b} + \vec{X} \cdot \Gamma\vec{y} = T_1. \tag{3.7}$$

Εξίσωση βαθμωτού πολλαπλασιασμού στην $\mathbb{G}_2$:

$$G_1 = \mathbb{Z}_{\mathbf{n}}, G_2 = \mathbb{G}_2, G_T = \mathbb{G}_2, f(x, Y) = [x]Y$$
$$\vec{a} \cdot \vec{Y} + \vec{x} \cdot \vec{B} + \vec{x} \cdot \Gamma\vec{Y} = T_2. \tag{3.8}$$

Τετραγωνική Εξίσωση στην $\mathbb{Z}_{\mathbf{n}}$:

$$G_1 = \mathbb{Z}_{\mathbf{n}}, G_2 = \mathbb{Z}_n, G_T = \mathbb{Z}_{\mathbf{n}}, f(x, y) = xy \mod \mathbf{n}$$
$$\vec{a} \cdot \vec{y} + \vec{x} \cdot \vec{b} + \vec{x} \cdot \Gamma\vec{y} = t. \tag{3.9}$$

Σχήματα δέσμευσης από πρότυπα. Ένα μη διαλογικό *σχήμα δέσμευσης* (*commitment scheme*) είναι ένα ζεύγος αλγορίθμων $(Setup, Commit)$ με τις ιδιότητες της

• *απόκρυψης* (*hiding*) της τιμής x κατά τη φάση δέσμευσης:
Υπάρχει αντίπαλος $\mathcal{A}$ ώστε

(i). $\{Setup(1^k)\} \approx \{\mathcal{A}(1^k)\}$.

(ii). Για κάθε x_1, x_2

$$\mathbf{Pr}[params \leftarrow \mathcal{A}(1^k); r \xleftarrow{\$} \{0,1\}^{poly(k)} : Commit(params, x_1, r) = c] \approx$$
$$\approx \mathbf{Pr}[params \leftarrow \mathcal{A}(1^k); r \xleftarrow{\$} \{0,1\}^{poly(k)} : Commit(params, x_2, r) = c]$$

• *συσχέτισης* (*binding*) μίας δέσμευσης c με την τιμή x κατά την φάση αποκάλυψης:
Για κάθε αντίπαλο $\mathcal{A}$ η πιθανότητα

$$\mathbf{Pr}[params \leftarrow Setup(1^k); c, x, x', r, r' \leftarrow \mathcal{A}(params) :$$
$$x \neq x' \wedge c = Commit(x, r) \wedge c = Commit(x', r')]$$

είναι αμελητέα.

Τα σχήματα δέσμευσης συχνά συνιστούν πρωτόκολλα μηδενικής γνώσης. Στο [GS08] κατασκευάζουνται NIWI-PS και NIZK-PS όπου δεσμεύονται οι μεταβλητές $\vec{x} = x_1, \ldots, x_m \in G_1$ και $\vec{y} = y_1, \ldots, y_n \in G_2$ μιας γενικής εξίσωσης (3.5).

Έστω $\mathcal{R}$-πρότυπα $\mathbb{A}_1, \mathbb{A}_2, \mathbb{A}_T$ και $\mathbb{B}_1, \mathbb{B}_2, \mathbb{B}_T$, $\mathcal{R}$-γραμμικές απεικονίσεις $\iota_1, \iota_2, \iota_T$, p_1, p_2, p_T και διγραμμικές απεικονίσεις f, F, όλες εκτός της p_T αποδοτικά υπολογίσιμες, όπως το παρακάτω σχήμα μετάβασης:

$$\begin{array}{ccccc} \mathbb{A}_1 & \times & \mathbb{A}_2 & \xrightarrow{f} & \mathbb{A}_T \\ \iota_1 \downarrow\uparrow p_1 & & \iota_2 \downarrow\uparrow p_2 & & \iota_T \downarrow\uparrow p_T \\ \mathbb{B}_1 & \times & \mathbb{B}_2 & \xrightarrow{F} & \mathbb{B}_T \end{array}$$

Άμεσα προκύπτουν οι παρακάτω σχέσεις:

$$\begin{array}{l} (\forall x \in \mathbb{A}_1)(\forall y \in \mathbb{A}_2) : F(\iota_1(x), \iota_2(y)) = \iota_T(f(x,y)) \\ (\forall x \in \mathbb{B}_1)(\forall y \in \mathbb{B}_2) : f(p_1(x), p_2(y)) = p_T(F(x,y)) \end{array} \tag{3.10}$$

Για $\vec{x} \in \mathbb{B}_1^m$, $\vec{y} \in \mathbb{B}_2^m$ ορίζουμε

$$\vec{x} * \vec{y} = \sum_{i=1}^{m} F(x_i, y_i).$$

Θέτουμε ως Setup και CRS

$gk = (\mathcal{R}, \mathbb{A}_1, \mathbb{A}_2, \mathbb{A}_T, f)$ και $\sigma = (\mathbb{B}_1, \mathbb{B}_2, \mathbb{B}_T, F, \iota_1, \iota_2, \iota_T, p_1, p_2, p_T, \vec{u}, \vec{v}, H_1, \ldots, H_q)$,

όπου $\vec{u} = u_1, \ldots, u_{\hat{m}} \in \mathbb{B}_1$, $\vec{v} = v_1, \ldots, v_{\hat{n}} \in \mathbb{B}_2$ και $H_1, \ldots, H_q \in Mat_{\hat{m}\times\hat{n}}(\mathcal{R})$ ώστε $\vec{u} * H_i\vec{v} = 0$.

Οι δεσμεύσεις στις τιμές $x_i \in \mathbb{A}_1$, $y_j \in \mathbb{A}_2$ υπολογίζονται επιλέγοντας τυχαία στοιχεία $r_{i1}, \ldots, r_{i\hat{m}}$ και $s_{j1}, \ldots, s_{j\hat{n}}$ του $\mathcal{R}$ ως

$$c_i = \iota_1(x_i) + \sum_{t=1}^{\hat{m}} r_{it}u_i \quad \text{και} \quad d_i = \iota_2(y_j) + \sum_{t=1}^{\hat{n}} s_{jt}u_j.$$

Συνεπώς καταληγούμε στις καθολικές δεσμεύσεις

$$\vec{c} = \iota_1(\vec{x}) + R\vec{u} \text{ και } \vec{d} = \iota_2(\vec{y}) + S\vec{v}, \tag{3.11}$$

όπου $R \in Mat_{m\times\hat{m}}(\mathcal{R})$, $S \in Mat_{n\times\hat{n}}(\mathcal{R})$ τυχαίοι πίνακες.

Το πρώτο βήμα στην αλληλεπίδραση του αποδείκτη $\mathcal{P}$ και του επαληθευτή $\mathcal{V}$ είναι ο υπολογισμός των δεσμεύσεων $\vec{c}, \vec{d}$ για τους μάρτυρες $\vec{x}, \vec{y}$ αντίστοιχα. Στη συνέχεια ζητείται από τον $\mathcal{P}$ να πείσει για την ισχύ μίας τετραγωνικής εξίσωσης της μορφής (3.5) με τη χρήση των $\vec{c}, \vec{d}$. Έτσι, το κύριο μέρος της μη διαλογικής απόδειξης αποτελείται από τα εξής στάδια:

Ισχυρισμός: Τα $\vec{c}, \vec{d}$ είναι δεσμεύσεις για $\vec{x}, \vec{y}$ τέτοια ώστε:

$$\vec{a} \cdot \vec{y} + \vec{x} \cdot \vec{b} + \vec{x} \cdot \Gamma \vec{y} = t.$$

Απόδειξη: Επίλεξε τυχαία $T \in Mat_{\hat{m} \times \hat{n}}$ και $r_1, \ldots, r_q \in \mathcal{R}$. Υπολόγισε

$$\vec{\theta} = S^\top \iota_1(\vec{a}) + S^\top \Gamma^\top \iota_1(\vec{x}) + T\vec{u}$$

$$\vec{\pi} = R^\top \iota_2(\vec{b}) + R^\top \Gamma \iota_2(\vec{b}) + R^\top \Gamma S \vec{v} - T^\top \vec{v} + \sum_{i=1}^{q} r_i H_i \vec{v}$$

και επίστρεψε την απόδειξη $(\vec{\theta}, \vec{\pi})$.

Επαλήθευση: Επίστρεψε 1 ανν

$$\iota_1(\vec{a}) * \vec{d} + \vec{c} * \iota_2(\vec{b}) + \vec{c} * \Gamma \vec{d} = \iota_T(t) + \vec{u} * \vec{\pi} + \vec{\theta} * \vec{v}.$$

Θεώρημα 3.4.2. *(Τέλεια πληρότητα) Έστω* $\vec{x} \in \mathbb{A}_1^m, \vec{y} \in \mathbb{A}_2^n, R \in Mat_{m \times \hat{m}}(\mathcal{R})$, $S \in Mat_{n \times \hat{n}}(\mathcal{R})$ *ώστε*

$$\vec{c} = \iota_1(\vec{x}) + R\vec{u}, \quad \vec{d} = \iota_2(\vec{y}) + S\vec{v}, \quad \vec{a} \cdot \vec{y} + \vec{x} \cdot \vec{b} + \vec{x} \cdot \Gamma \vec{y} = t.$$

Τότε για κάθε επιλογή των $T, r_1, \ldots, r_q$ *ο* $\mathcal{V}$ *αποδέχεται τις* $\vec{\theta}, \vec{\pi}$.

Απόδειξη. Από τις σχέσεις (3.11) έχουμε

$$\begin{aligned} \iota_1(\vec{a}) * \iota_2(\vec{y}) + \iota_1(\vec{x}) * \iota_2(\vec{b}) + \iota_1(\vec{x}) * \Gamma \iota_2(\vec{y}) &= \iota_T(\vec{a} \cdot \vec{y}) + \iota_T(\vec{x} \cdot \vec{b}) + \iota_T(\vec{x} \cdot \Gamma \vec{y}) = \\ &= \iota_T(\vec{a} \cdot \vec{y} + \vec{x} \cdot \vec{b} + \vec{x} \cdot \Gamma \vec{y}) = \iota_T(t). \end{aligned}$$

Αντικαθιστώντας την παραπάνω εξίσωση στον έλεγχο του $\mathcal{V}$ έχουμε

$$\begin{aligned} & \iota_1(\vec{a}) * \vec{d} + \vec{c} * \iota_2(\vec{b}) + \vec{c} * \Gamma \vec{d} = \\ &= \iota_1(\vec{a}) * \iota_2(\vec{y}) + \iota_1(\vec{x}) * \iota_2(\vec{b}) + \iota_1(\vec{x}) * \Gamma \iota_2(\vec{y}) + \\ &\quad + R\vec{u} * \iota_2(\vec{b}) + R\vec{u} * \Gamma \iota_2(\vec{y}) + R\vec{u} * \Gamma S \vec{v} + \iota_1(\vec{a}) * S\vec{v} + \iota_1(\vec{x}) * \Gamma S \vec{v} \overset{\vec{u} * H_i \vec{v} = 0}{=} \\ &= \iota_T(t) + \vec{u} * (R^\top \iota_2(\vec{b}) + R^\top \Gamma \iota_2(\vec{y}) + R^\top \Gamma S \vec{v}) + \textstyle\sum_{i=1}^{n} r_i (\vec{u} * H_i \vec{v}) - \vec{u} * T^\top \vec{v} + \\ &\quad + T\vec{u} * \vec{v} + (S^\top \iota_1(\vec{a}) + S^\top \Gamma^\top \iota_1(\vec{x})) * \vec{v} = \\ &= \iota_T(t) + \vec{u} * \vec{\pi} + \vec{\theta} * \vec{v}. \end{aligned}$$

⊣

Το $(\mathcal{P}, \mathcal{V})$ είναι NIWI-PS, υπό τις προϋποθέσεις που ορίζουν τα επόμενα δύο θεωρήματα:

Θεώρημα 3.4.3. *(Προϋποθέσεις ορθότητας) Έστω ότι* $p_1(\vec{u}) = \vec{0}$, $p_2(\vec{v}) = \vec{0}$ *και οι απεικονίσεις* $\iota_1 \circ p_1$, $\iota_2 \circ p_2$, $\iota_T \circ p_T$ *δεν είναι τετριμμένες . Τότε μία έγκυρη απόδειξη* $(\vec{\theta}, \vec{\pi})$ *συνεπάγεται την ισότητα*

$$p_1(\iota_1(\vec{a})) \cdot p_2(\vec{d}) + p_1(\vec{c}) \cdot p_2(\iota_2(\vec{b}) + p_1(\vec{c}) \cdot \Gamma p_2(\vec{d})) = p_T(\iota(t)).$$

Απόδειξη. Αφού η $(\vec{\theta}, \vec{\pi})$ είναι έγκυρη ισχύει ότι

$$\iota_1(\vec{a}) * \vec{d} + \vec{c} * \iota_2(\vec{b}) + \vec{c} * \Gamma\vec{d} = \iota_T(t) + \vec{u} * \vec{\pi} + \vec{\theta} * \vec{v}.$$

Επομένως από τις (3.10) και εφόσον $p_1(\vec{u}) = 0$, $p_2(\vec{v}) = 0$ έχουμε

$$\begin{aligned} & p_1(\iota_1(\vec{a})) \cdot p_2(\vec{d}) + p_1(\vec{c}) \cdot p_2(\iota_2(\vec{b}) + p_1(\vec{c}) \cdot \Gamma p_2(\vec{d})) = \\ &= p_T(\iota_1(\vec{a}) * \vec{d}) + p_T(\vec{c} * \iota_2(\vec{b})) + p_T(\vec{c} * \Gamma\vec{d}) = \\ &= p_T(\iota_T(t) + \vec{u} * \vec{\pi} + \vec{\theta} * \vec{v}) = \\ &= p_T(\iota_T(t)) + p_1(\vec{u}) \cdot p_2(\vec{\pi}) + p_1(\vec{\theta}) \cdot p_2(\vec{v}) = p_T(\iota(t)). \end{aligned}$$

⊣

Σύμφωνα με τις προϋποθέσεις ορθότητας, οι δέσμευσεις $\vec{c}, \vec{d}$ περιέχουν τις μη τετριμμένες πληροφορίες $p_1(\vec{c}) = p_1(\iota(\vec{x}))$ και $p_2(\vec{d}) = p_2(\iota(\vec{y}))$ για τις $\vec{x}, \vec{y}$. Επιπλέον, εάν οι $\iota_1 \circ p_1$, $\iota_2 \circ p_2$ και $\iota_T \circ p_T$ είναι οι ταυτοτικές απεικονίσεις των $\mathbb{A}_1, \mathbb{A}_2, \mathbb{A}_T$, τότε έχουμε τέλεια συσχέτιση των δεσμεύσεων, δηλαδή $\vec{x} = p_1(\vec{c})$ και $\vec{y} = p_2(\vec{d})$, και *τέλεια ορθότητα* αφού ικανοποιείται η $\vec{a} \cdot p_1(\vec{c}) + p_2(\vec{d}) \cdot \vec{b} + p_1(\vec{c}) \cdot \Gamma p_2(\vec{d}) = t$. Όταν δεν προκύπτουν οι ταυτοτικές απεικονίσεις, μπορούμε να επιτύχουμε L_{co}-ορθότητα για κατάλληλη γλώσσα L_{co}.

Θεώρημα 3.4.4. *(Προϋποθέσεις WI) Έστω ότι* $\iota_1(\mathbb{A}_1) \subseteq \langle u_1, \ldots, u_{\hat{m}} \rangle$, $\iota_2(\mathbb{A}_2) \subseteq \langle v_1, \ldots, v_{\hat{n}} \rangle$ *και οι πίνακες* $H_1, \ldots, H_q$ *παράγουν το* $\mathcal{R}$*-πρότυπο*

$$\mathbb{H} = \{H \in Mat_{\hat{m} \times \hat{n}}(\mathcal{R}) \mid \vec{u} * H\vec{v} = 0\}.$$

Τότε όλοι οι κατάλληλοι μάρτυρες $\vec{x}, \vec{y}$ *συνεπάγονται αποδείξεις* $(\vec{\theta}, \vec{\pi})$ *που είναι ομοιόμορφα κατανεμημένες υπό τη συνθήκη ότι ικανοποιούν την εξίσωση επαλήθευσης.*

Απόδειξη. Εφόσον $\iota_1(\mathbb{A}_1) \subseteq \langle u_1, \ldots, u_{\hat{m}} \rangle$ και $\iota_2(\mathbb{A}_2) \subseteq \langle v_1, \ldots, v_{\hat{n}} \rangle$ υπάρχουν πίνακες A, B, X, Y ώστε $\iota_1(\vec{a}) = A\vec{u}, \iota_1(\vec{x}) = X\vec{u}, \iota_2(\vec{b}) = B\vec{v}$ και $\iota_2(\vec{y}) = Y\vec{v}$. Έπομένως έχουμε $\vec{c} = (X + R)\vec{u}$ κα $\vec{d} = (Y + S)\vec{v}$ και οι $\vec{\theta}, \vec{\pi}$ γράφονται ως

$$\begin{aligned} \vec{\theta} &= (S^\top A + S^\top \Gamma^\top X + T)\vec{u} \\ \vec{\pi} &= (R^\top B + R^\top \Gamma Y + R^\top \Gamma S - T^\top)\vec{v} + (\textstyle\sum_{i=1}^{q} r_i H_i)\vec{v} \end{aligned} \tag{3.12}$$

Η τυχαία επιλογή του T επιτρέπει να θεωρούμε τη $\vec{\theta}$ ως ομοιόμορφη τ.μ. μέσω της $\vec{\theta} = \Theta\vec{u}$, για τυχαία επιλέγμενο πίνακα Θ και την $\vec{\pi}$ ως $\vec{\pi} = \Pi\vec{v}$, όπου Π είναι τ.μ. εξαρτώμενη από τον Θ. Από το Θεώρημα 3.4.2 όλοι οι μάρτυρες συνεπάγονται $(\vec{\theta}, \vec{\pi})$ ώστε

$$\iota_1(\vec{a}) * \vec{d} + \vec{c} * \iota_2(\vec{b}) + \vec{c} * \Gamma\vec{d} - \iota_T(t) - \vec{\theta} * \vec{v} = \vec{u} * \vec{\pi} = \vec{u} * \Pi\vec{v}.$$

Συνεπώς, δεδομένου Θ για δύο λύσεις $\vec{\pi}, \vec{\pi}'$ έχουμε

$$\vec{u} * (\Pi - \Pi')\vec{v} = 0 \Rightarrow \Pi - \Pi' \in \mathbb{H} \Rightarrow \Pi = \Pi' + \sum_{i=1}^{q} z_i H_i,$$

για κάποια $z_1, \ldots, z_q \in \mathcal{R}$. Επομένως, σε συνδυασμό με τις (3.12) συμπεραίνουμε ότι δεδομένης $\vec{\theta}$, άρα και δεδομένου T, οι λύσεις $(\vec{\theta}, \vec{\pi})$ κατανέμονται ομοιόμορφα σύμφωνα με τα $r_1, \ldots, r_q \in \mathcal{R}$. Η απόδειξη είναι πλήρης από την ομοιόμορφη επιλογή της $\vec{\theta}$.

$\dashv$

Οι προϋποθέσεις WI εξασφαλίζουν την τέλεια απόκρυψη των δεσμεύσεων $\vec{c}, \vec{d}$. Η συνθεσιμότητα επιτυγχάνεται θεωρώντας ότι πραγματικά και προσομοιωμένα CRS σ και σ' αντίστοιχα υπολογίζονται με μη διακρίσιμο τρόπο, όπως θα δούμε και στα στιγμιότυπα που ακολουθούν. Για συντομία, κατά την περιγραφή των σ, σ' όλες οι παράμετροι εκτός των $\vec{u}, \vec{v}$ θα παραλείπονται ως υπονοούμενες.

Δύο ενδιαφέρουσες ειδικές περιπτώσεις είναι όταν $\vec{a} = 0$ και $\Gamma = 0$, όποτε προκύπτει η απλή *γραμμική* εξίσωση

$$\vec{x} \cdot \vec{b} = t,$$

καθώς και η *συμμετρική* περίπτωση $\mathbb{B}_1 = \mathbb{B}_2 = \mathbb{B}$, $\hat{m} \geqslant \hat{n}$, $u_i = v_i$ για $i \leqslant \hat{m}$ και $F(x, y) = F(y, x)$ για κάθε $x, y \in \mathbb{B}$. Στην τελευταία προσθέτοντας $\hat{n} - \hat{m}$ μηδενικά στη θ προκύπτει $\vec{\theta'}$ ισομήκης με την $\vec{\pi}$. Ο αποδείκτης αποστέλλει την απόδειξη $\vec{\phi} = \vec{\pi} + \vec{\theta'}$ και ο επαληθευτής ελέγχει την ισότητα

$$\iota_1(\vec{a}) * \vec{d} + \vec{c} * \iota_2(\vec{b}) + \vec{c} * \Gamma\vec{d} = \iota_T(t) + \vec{u} * \vec{\phi}.$$

Το παραπάνω NIPS επεκτείνεται στο σύστημα απόδειξης GSPS για την ικανοποιησιμότητα N τετραγωνικών εξισώσεων με παραμέτρους $\{\vec{a_i}, \vec{b_i}, \Gamma_i, t_i\}_{i=1}^N$. Τα gk, σ καθώς και οι δεσμεύσεις $\vec{c}, \vec{d}$ για τους αντίστοιχους μάρτυρες $\vec{x}, \vec{y}$ ορίζονται όπως πριν. Ο αποδείκτης υπολογίζει για κάθε τετράδα παραμέτρων ζεύγος $(\vec{\theta_i}, \vec{\pi_i})$ και αποστέλλει τελικώς ην απόδειξη $(\vec{c}, \vec{d}, \{(\vec{\theta_i}, \vec{\pi_i})\}_{i=1}^N)$. Με τη σειρά του ο επαληθευτής με είσοδο $gk, \sigma, \{\vec{a_i}, \vec{b_i}, \Gamma_i, t_i\}_{i=1}^N$, $(\vec{c}, \vec{d}, \{(\vec{\theta_i}, \vec{\pi_i})\}_{i=1}^N)$ αποδέχεται ανν

$$\forall i \in [N] : \iota_1(\vec{a_i}) * \vec{d} + \vec{c} * \iota_2(\vec{b_i}) + \vec{c} * \Gamma_i\vec{d} = \iota_T(t_i) + \vec{u} * \vec{\pi_i} + \vec{\theta_i} * \vec{v}.$$

Εάν οι μεταβλητές $\vec{x} = x_1, \ldots, x_m$, $\vec{y} = y_1, \ldots, y_n$, δεσμεύονται μέσω των $\vec{u} = u_1, \ldots, u_{\hat{m}}$, $\vec{v} = v_1, \ldots, v_{\hat{m}}$, τότε $\vec{c} \in \mathbb{B}_1^m, \vec{d} \in \mathbb{B}_2^n$ και $\pi_i \in \langle u_1, \ldots, u_{\hat{m}} \rangle^{\hat{m}}$, $\theta_i \in \langle v_1, \ldots, v_{\hat{n}} \rangle^{\hat{n}}$ επομένως το μέγεθος της απόδειξης $(\vec{c}, \vec{d}, \{(\vec{\theta_i}, \vec{\pi_i})\}_{i=1}^N)$ είναι $m + N\hat{m}$ στοιχεία του $\mathbb{B}_1$ και $n + N\hat{n}$ στοιχεία του $\mathbb{B}_2$.

Για το GSPS έχουμε το ακόλουθο κύριο θεώρημα.

Θεώρημα 3.4.5. *Το GSPS έχει τέλεια πληρότητα, τέλεια L_{co}-ορθότητα και συνθέσιμη μη διακρισιμότητα μάρτυρος, όπου L_{co} είναι η γλώσσα*

$$\left\{\{\vec{a_i}, \vec{b_i}, \Gamma_i, t_i\}_{i=1}^N \mid (\forall \vec{x}, \vec{y})(\exists i) : p_1(\iota_1(\vec{a_i})) \cdot \vec{y} + \vec{x} \cdot p_2(\iota_2(\vec{b_i})) + \vec{x} \cdot \Gamma_i \vec{y} \neq p_T(\iota_T(t_i))\right\}$$

Απόδειξη. Η τέλεια πληρότητα έπεται από το Θεώρημα 3.4.2.

Για την ορθότητα θεωρούμε απόδειξη $(\vec{c}, \vec{d}, \{(\vec{\theta_i}, \vec{\pi_i})\}_{i=1}^N)$ από το $\sigma \leftarrow \mathcal{K}(gk, sk)$. Θέτουμε $\vec{x} = p_1(\vec{c}), \vec{y} = p_2(\vec{d})$ και από το Θεώρημα 3.4.3 έχουμε

$$\forall i \in [N] : p_1(\iota_1(\vec{a_i})) \cdot \vec{y} + \vec{x} \cdot p_2(\iota_2(\vec{b_i})) + \vec{x} \cdot \Gamma_i \vec{y} = p_T(t_i).$$

Επομένως $\{\vec{a_i}, \vec{b_i}, \Gamma_i, t_i\}_{i=1}^N \notin L_{co}$ και άρα προκύπτει τέλεια L_{co}-ορθότητα.

Έστω τώρα προσομοιωμένο CRS $\sigma' \leftarrow \mathcal{S}(gk, sk)$ το οποίο υποθέτουμε μη διακρίσιμο από αυτά που παράγει ο $\mathcal{K}$. Τα $\vec{c}, \vec{d}$ αποκρύπτουν υπολογιστικά τους μάρτυρες $\vec{x}, \vec{y}$ και από το Θεώρημα 3.4.4 για κάθε εξίσωση δύο μάρτυρες οδηγούν σε έγκυρες αποδείξεις που ακολουθούν την ίδια ομοιόμορφη κατανομή. Εφαρμόζοντας υβριδικό επιχείρημα έχουμε τέλεια WI.

⊣

Το GSPS στην κρυπτογραφία ζευγμάτων. Στο πλήρες paper [GS07], οι J. Groth και A.Sahai παραθέτουν τρία στιγμιότυπα εφαρμογής του GSPS βασισμένα στα ακόλουθα υποτιθέμενα δύσκολα προβλήματα σε ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$.

Πρόβλημα απόφασης υποομάδας στην $\mathbb{G}$ (*Subgroup decision problem - SDP*)**:** δεδομένων $n = pq$, όπου p, q άγνωστοι πρώτοι, ώστε $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G} = \mathbb{G}_p \times \mathbb{G}_q$ και x τυχαία επιλεγμένου είτε από την $\mathbb{G}$ είτε από την $\mathbb{G}_q$, να αποφασιστεί εάν $x \in \mathbb{G}_q$.

Υπόθεση συμμετρικού εξωτερικού Diffie-Hellman (*Symmetric external Diffie-Hellman - SXDH - assumption*)**:** δεδομένων P, Q γεννητόρων των $\mathbb{G}_1, \mathbb{G}_2$ αντίστοιχα, τα DDH($\mathbb{G}_1$) και DDH($\mathbb{G}_2$) είναι δύσκολα προβλήματα.

Γραμμικό πρόβλημα απόφασης στην $\mathbb{G}$ (*Decisional Linear problem - DLin*)**:** δεδομένων γεννήτορα P της $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ και $([\alpha]P, [\beta]P, [r\alpha]P, [s\beta]P, [t]P) \in \mathbb{G}^5$, να αποφασιστεί εάν $t = r + s$.

Περιγραφικά μπορούμε να πούμε ότι στο SDP [BGN05] ένας αντίπαλος δεν μπορεί να διακρίνει ένα τυχαίο στοιχείο της $\mathbb{G}$ από ένα τυχαίο στοιχείο της $\mathbb{G}_q$, ενώ

στο DLin [BBS04] είναι δύσκολο να διακριθεί αν $t = r + s$ ή το t είναι τυχαίο. Το DLin χρησιμοποιείται σε ομάδες όπου το DDH είναι εύκολο, καθώς εύκολα προκύπτει ότι $\mathrm{DDH}(\mathbb{G}) \leqslant \mathrm{DLin}(\mathbb{G})$[3]. Επιπλέον, η SXDH είναι ισχυροποίηση της *εξωτερικής υπόθεσης Diffie-Hellman* (*XDH*) όπου υποθέτουμε ότι ένα εκ των $\mathrm{DDH}(\mathbb{G}_1)$, $\mathrm{DDH}(\mathbb{G}_2)$ είναι δύσκολα. Τα αντίστοιχα στιγμιότυπα GS-αποδείξεων είναι τα εξής:

SDP [GS07 Istantiation 1]: $\mathrm{Setup} : (gk, sk) = ((\mathbf{n}, \mathbb{G}, \mathbb{G}_T, e, P), (\mathbf{p}, \mathbf{q}))$, όπου $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$ ζεύγμα Τύπου 1 και P γεννήτορας της $\mathbb{G}$ τάξης $\mathbf{n} = \mathbf{p} \cdot \mathbf{q}$, $\mathbf{p}, \mathbf{q}$ πρώτοι. Ζητούμε την ικανοποιησιμότητα συνόλου εξισώσεων τύπου (3.6),(3.8),(3.9) επομένως δεσμευόμαστε είτε για στοιχεία της $\mathbb{G}$ είτε για στοιχεία του $\mathbb{Z}_{\mathbf{n}}$. Θέτουμε τα πρότυπα $\mathbb{B}_1 = \mathbb{B}_2 = \mathbb{G}$ και $\mathbb{B}_T = \mathbb{G}_T$ καθώς επίσης $F(X, Y) = e(X, Y)$. Ο αλγόριθμος $\mathcal{K}$ εξάγει $\sigma = U = [r\mathbf{p}]P$ για τυχαίο $r \in \mathbb{Z}_{\mathbf{n}}$. Για $Z \in \mathbb{G}$, $z \in \mathbb{Z}_{\mathbf{n}}$ ορίζουμε

$$\iota(Z) = Z,\ \ p(Z) = [\lambda]Z,\ \ \iota'(z) = [z]P,\ \ p'([z]P) = \lambda z,$$

όπου $\lambda \equiv 1 \mod \mathbf{p}$ και $\lambda \equiv 0 \mod \mathbf{p}$. Διακρίνουμε τις εξής περιπτώσεις:

(i). για $Y \in \mathbb{G}$ και για τυχαίο $s \in \mathbb{Z}_{\mathbf{n}}$ η δέσμευση $D = \iota(Y) + [s]U$ αποκρύπτει τέλεια το Y. Εάν $U \in \mathbb{G}_{\mathbf{q}}$ τότε

$$p(D) = p(\iota(Y)) + [s]p(U) = \lambda Y + [\lambda][s]U = \lambda Y + \mathcal{O} = \lambda Y,$$

δηλαδή το Y προσδιορίζεται μοναδικά στην $\mathbb{G}_{\mathbf{p}}$.

(ii). για $x \in \mathbb{Z}_{\mathbf{n}}$ και για τυχαίο $r \in \mathbb{Z}_{\mathbf{n}}$ η δέσμευση $C = \iota'(x) + [r]U$ αποκρύπτει τέλεια το x εάν $U \in \mathbb{G}_{\mathbf{q}}$, τότε η C προσδιορίζει το $p'(C) = \lambda x \equiv x \mod \mathbf{q}$.

Παρατηρούμε ότι οι $\iota \circ p$, $\iota' \circ p'$ προβάλλουν στοιχεία των $\mathbb{G}, \mathbb{Z}_{\mathbf{n}}$ στις αντίστοιχες υποομάδες τάξης $\mathbf{p}$, $\mathbb{G}_{\mathbf{p}}$ και $\mathbb{Z}_{\mathbf{p}}$. Στη συνέχεια κατασκευάζουμε για κάθε τύπο τετραγωνικής εξίσωσης κατάλληλες συναρτήσεις ι_T, p_T ώστε να ικανοποιούνται οι (3.10) και η απεικόνιση $\iota_T \circ p_T$ να προβάλει στοιχεία της $\mathbb{G}_T$ στην υποομάδα τάξης $\mathbf{p}$. Ως αποτέλεσμα η απόδειξη έχει τέλεια L_{co}-ορθότητα, όπου L_{co} είναι η γλώσσα των συνόλων τετραγωνικών εξισώσεων που δεν ικανοποιούνται στις υποομάδες τάξης $\mathbf{p}$ των $\mathbb{G}, \mathbb{G}_T, \mathbb{Z}_{\mathbf{n}}$. Εξάλλου, το DSP συνεπάγεται την μη διακρισιμότητα του πραγματικού CRS $\sigma = [r\mathbf{p}]P$ τάξης $\mathbf{q}$ από ένα προσομοιωμένο CRS $\sigma' = [r']P$ για τυχαίο $r' \in \mathbb{Z}_{\mathbf{n}}$ τάξης $\mathbf{n}$. Ο μοναδικός πίνακας-στοιχείο $H \in Mat_{1\times 1}(\mathcal{R})$ που ικανοποιεί την $F(U, HU) = e(U, HU) = 1$ είναι ο $H = 0$ και δεν περιλαμβάνεται στα CRS. Συνεπώς, αφού οι δεσμεύσεις C, D που προκύπτουν από το σ' αποκρύπτονται τέλεια, τελικά έχουμε co-WI.

[3]Η (P, Q, R, S) είναι DDH-τετράδα ανν η $(P, Q, R, S, [2]R)$ είναι DLin-πεντάδα

Το παράδειγμα αποτελεί εφαρμογή της συμμετρικής περίπτωσης και το μέγεθος της απόδειξης είναι $m+n+N$ στοιχεία $\mathbb{G}$, όπου m,n το πληθός των προς δέσμευση στοιχείων των $\mathbb{G}, \mathbb{Z}_{\mathbf{n}}$ αντίστοιχα και N το πλήθος των εξισώσεων.

SXDH [GS07 Istantiation 2]: Setup : $(gk, sk) = ((\mathbf{p}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1, P_2), \Lambda)$, όπου $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ ασύμμετρο ζεύγμα Τύπου 3 [4] και P_1, P_2 γεννήτορες των $\mathbb{G}_1, \mathbb{G}_2$ τάξης $\mathbf{p}$, όπου $\mathbf{p}$ πρώτος. Ορίζονται τα $B_1 = \mathbb{G}_1^2$, $B_2 = \mathbb{G}_2^2$ με πρόσθεση κατά σημείο και $B_T = \mathbb{G}_T^4$ με πολλαπλασιασμό κατά σημείο. Θέτουμε επίσης

$$F(\begin{pmatrix} X_1 \\ X_2 \end{pmatrix}, \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix}) = \begin{pmatrix} e(X_1, Y_1) & e(X_1, Y_2) \\ e(X_2, Y_1) & e(X_2, Y_2) \end{pmatrix}.$$

Ως CRS έχουμε το $\sigma = (u_1, u_2, v_1, v_2)$, όπου $u_1 = (P_1, [\alpha_1]P_1), v_1 = (P_2, [\alpha_2]P_2)$, $u_2 = [t_1]u_1, v_2 = [t_2]v_1$ για τυχαία $\alpha_1, \alpha_2 \in \mathbb{Z}_{\mathbf{p}}^*$ και $t_1, t_2 \in \mathbb{Z}_{\mathbf{p}}^*$.

Δεσμευόμαστε για μεταβλητές $X_1, \ldots, X_m \in \mathbb{G}_1$, $Y_1, \ldots, Y_n \in \mathbb{G}_2$, $x_1, \ldots, x_{m'}$, $y_1, \ldots, y_{n'} \in \mathbb{Z}_{\mathbf{p}}$ συνόλου τετραγωνικών εξισώσεων τύπου (3.6-9). Για την $\mathbb{G}_1$ ορίζουμε $\iota_1(Z) = (\mathcal{O}, Z)$, $p_1(Z_1, Z_2) = Z_2 - [\alpha_1]Z_1$ και παρατηρούμε ότι $p_1(u_1) = p_1(u_2) = \mathcal{O}$ και $\iota_1 \circ p_1 = id_{\mathbb{G}_1}$. Για τη δέσμευση ενός στοιχείου $X \in \mathbb{G}_1$ επιλέγουμε τυχαία $r_1, r_2 \in \mathbb{Z}_{\mathbf{p}}$ και υπολογίζουμε

$$C = \iota_1(X) + r_1 u_1 + r_2 u_2.$$

Όμοια εργαζόμαστε για την $\mathbb{G}_2$. Για $x \in \mathbb{Z}_{\mathbf{p}}$ ορίζουμε $\iota_1'(z) = z(u_2 + (\mathcal{O}, P_1))$, $p_1'([z_1]P_1, [z_2]P_1) = z_2 - \alpha_1 z_1$ και τη δέσμευση $c = \iota_1'(x) + r u_1$, όπου το r επιλέγεται τυχαία στο $\mathbb{Z}_{\mathbf{p}}$. Προκύπτει ότι $p_1'(u_1) = 0$ και $\iota_1' \circ p_1' = id_{\mathbb{Z}_{\mathbf{p}}}$. Αντίστοιχα υπολογίζουμε τα ι_2', p_2', d για $y \in \mathbb{Z}_{\mathbf{p}}$.

Οι ι_T, p_T για κάθε τύπο εξίσωσης κατασκευάζονται ώστε $\iota_T' \circ p_T' = id_{\mathbb{G}_T}$, οπότε και έχουμε τέλεια ορθότητα από το Θεώρημα 3.4.3. Η co-WI επιτυγχάνεται με την προσομοίωση $\sigma' = (u_1, u_2, v_1, v_2)$ με u_1, v_1 όπως πριν και $u_2 = t_1 u_1 - (\mathcal{O}, P_1)$, $v_2 = t_2 v_1 - (\mathcal{O}, P_2)$ για τυχαία $t_1, t_2 \in \mathbb{Z}_{\mathbf{p}}^*$. Εάν υπάρχει non-uniform αλγόριθμος $\{\mathcal{A}_k\}_{k \in \mathbb{N}}$ που μπορεί να διακρίνει τα σ, σ', δηλαδή τετράδες

$$(P, [\alpha], [t]P, [\alpha t]P) \quad \text{και} \quad (P, [\alpha'], [t']P, [\alpha' t' - 1]P),$$

τότε κατασκευάζουμε αλγόριθμο που αποφασίζει αν μία τετράδα (P, Q, U, V) είναι λύση του DDH στην $\mathbb{G}_i$, $i \in \{1, 2\}$ καλώντας τον $\mathcal{A}_k$ να αποφασίσει για τις τετράδες (P, Q, U, V) και $(P, Q, U, V - P)$. Κάτι τέτοιο όμως αντιβαίνει στην υπόθεση SXDH.

Παρατηρούμε ότι τα u_1, u_2 είναι γραμμικά ανεξάρτητα. Πράγματι, εάν $u_1 = k u_2$ για κάποιο $k \in \mathbb{Z}_{\mathbf{p}}$ τότε αφού ο P_1 είναι γεννήτορας της $\mathbb{G}_2$ έχουμε

[4] αν το e είναι Τύπου 2, τότε από Πρόταση 2.2.7 το DDH($\mathbb{G}_2$) είναι εύκολο και επομένως δεν ισχύει η SDXH.

$$kt_1 \equiv 1 \bmod \mathbf{p} \quad \text{και} \quad a_1 \equiv a_1 kt_1 - k \bmod \mathbf{p}$$

το οποίο είναι αδύνατο. Όμοίως τα v_1, v_2 είναι γραμμικά ανεξάρτητα. Επομένως τα $F(u_1, v_1), F(u_1, v_2),\ F(u_2, v_1), F(u_2, v_2)$ είναι γραμμικά ανεξάρτητα και άρα ο μοναδικός πίνακας $H \in Mat_{2\times 2}(\mathcal{R})$ ώστε $\vec{u} * H\vec{v} = 0$ είναι ο μηδενικός και δεν περιλαμβάνεται στα CRS. Επιπλέον, λόγω ανεξαρτησίας των u_1, u_2 και v_1, v_2 έχουμε ότι $\iota_2(\mathbb{G}_1) \subseteq \langle u_1, u_2\rangle = \mathbb{G}_1^2$ και $\iota_2(\mathbb{G}_2) \subseteq \langle v_1, v_2\rangle = \mathbb{G}_2^2$. Επίσης $\iota_1'(\mathbb{Z}_\mathbf{p}) \subseteq \langle u_1\rangle$ και $\iota_2'(\mathbb{Z}_\mathbf{p}) \subseteq \langle v_1\rangle$. Συνεπώς τα στοιχεία του $\sigma' = (u_1, u_2, v_1, v_2)$ εκ κατασκευής αποκρύπτουν ομοιόμορφα τις δεσμευμένες τιμές και έχουμε τέλεια WI. Το μέγεθος της απόδειξης είναι $2m + 2m' + 4N_1 + 2N_2 + 4N_3 + 2N_4$ στοιχεία της $\mathbb{G}_1$ και $2n + 2n' + 4N_1 + 4N_2 + 2N_3 + 2N_4$ στοιχεία της $\mathbb{G}_2$, όπου N_1, N_2, N_3, N_4 το πλήθος τετραγωνικών εξισώσεων τύπου (3.6),(3.7),(3.8),(3.9) αντίστοιχα, όταν αυτές δεν εμπίπτουν στην ειδική περίπτωση γραμμικής εξίσωσης.

DLin [GS07 Istantiation 3]: Setup : $(gk, sk) = ((\mathbf{p}, \mathbb{G}, \mathbb{G}_T, e, P), \Lambda)$. Όπως και στο SDP, δεσμευόμαστε για μεταβλητές $Y_1, \ldots, Y_n \in \mathbb{G}_2,\ x_1, \ldots, x_{m'} \in \mathbb{Z}_\mathbf{p}$ συνόλου τετραγωνικών εξισώσεων τύπου (3.7),(3.8) και (3.10). Συγκεκριμένα, θέτουμε $\mathbb{B}_1 = \mathbb{B}_2 = \mathbb{G}^3$, $\mathbb{B}_T = \mathbb{G}^9$ και οι διγραμμικές απεικονίσεις

$$\tilde{F}(\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix}, \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix}) = \begin{pmatrix} e(X_1, Y_1) & e(X_1, Y_2) & e(X_1, Y_3) \\ e(X_2, Y_1) & e(X_2, Y_2) & e(X_2, Y_3) \\ e(X_3, Y_1) & e(X_3, Y_2) & e(X_3, Y_3) \end{pmatrix}.$$

$$F(x, y) = \frac{1}{2}\tilde{F}(x, y) + \frac{1}{2}\tilde{F}(y, x).$$

Ο $\mathcal{K}$ εξάγει $\sigma = (u_1, u_2, u_3)$, όπου $u_1 = ([\alpha]P, \mathcal{O}, P)$, $u_2 = (\mathcal{O}, [\beta]P, P)$ και $u_3 = ru_1 + su_2$ τυχαία $\alpha, \beta \in \mathbb{Z}_\mathbf{p}^*$ και $r, s \in \mathbb{Z}_\mathbf{p}$. Για $Z, Z_1, Z_2, Z_3 \in \mathbb{G}$, $z.z_1, z_2, z_3 \in \mathbb{Z}_\mathbf{p}$ ορίζουμε

$$\iota(Z) = (\mathcal{O}, \mathcal{O}, Z) \qquad p(Z_1, Z_2, Z_3) = Z_3 - [\alpha^{-1}]Z_1 - [\beta^{-1}]Z_2$$

$$\iota'(z) = zu \qquad p'([z_1]P, [z_2]P, [z_3]P) = z_3 - \alpha^{-1}z_1 - \beta^{-1}z_2$$

Οι 3×3 πίνακες που ικανοποιούν την $\vec{u} * H\vec{v} = 0$ υπολογίζονται σταθεροί για τις $F, \tilde{F}$ και παραλείπονται. Για $Y \in \mathbb{G}$ υπολογίζουμε $C = \iota(Y) + s_1u_1 + s_2u_2 + s_3u_3$, ενώ για $x \in \mathbb{Z}_\mathbf{p}$ έχουμε $c = \iota'(x) + r_1u_1 + r_2u_2$, όπου s_1, s_2, s_3, r_1, r_2 επιλέγονται τυχαία από το $\mathbb{Z}_\mathbf{p}$.

Ισχύει ότι $\iota(\mathbb{G}) \subseteq \langle u_1, u_2, u_3\rangle$, $\iota'(\mathbb{Z}_\mathbf{p}) \subseteq \langle u_1, u_2\rangle$, $p(u_1) = p(u_2) = p(u_3) = \mathcal{O}$, $p'(u_1) = p'(u_2) = 0$ και $\iota \circ p$, $\iota' \circ p'$ είναι ταυτοτικές απεικονίσεις. Ένα προσομοιωμένο CRS $\sigma' = (u_1, u_2, u_3)$, όπου u_1, u_2 όπως πριν και $u_3 = ru_1 + su_2 - (\mathcal{O}, \mathcal{O}, P)$, με επιχειρηματολογία ανάλογη του στιγμιότυπου SXDH, είναι μη διακρίσιμο από το

σ δεδομένης της δυσκολίας του DLin. Μέσω των $F, \tilde{F}$ κατασκεύαζονται κατάλληλες ι_T, p_T, ωστε η $\iota_T \circ p_T$ να είναι η ταυτοτική και τελικά έχουμε τέλεια ορθότητα και co-WI. Οι πίνακες $H \in Mat_{3\times 3}(\mathcal{R})$ ώστε $\vec{u} * H\vec{v} = 0$ προκύπτουν σταθεροί για τις $\tilde{F}, F$ και δεν περιλαμβάνονται στα CRS. Το μέγεθος της απόδειξης είναι $3m + 3n + 9N_1 + 9N_2 + 6N_3$ στοιχεία της $\mathbb{G}$, όπου N_1, N_2, N_3 το πλήθος τετραγωνικών εξισώσεων τύπου (3.6),(3.8),(3.9) αντίστοιχα, , όταν αυτές δεν εμπίπτουν στην ειδική περίπτωση γραμμικής εξίσωσης.

Εγκυρότητα και μηδενική γνώση στο GSPS. Παρατηρουμε ότι το GSPS είναι απόδειξης γνώσης μηδενικού σφάλματος, αφού εάν ο $\mathcal{K}$ παράγει πρόσθετη πληροφορία (π.χ. την παραγοντοποίηση του $\mathbf{n}$ για το στιγμιότυπο SDP) ικανή για τον υπολογισμό των p_1, p_2, τότε μπορούν να εξαχθούν οι μάρτυρες $\vec{x} = p_1(\vec{c})$ και $\vec{y} = p_2(\vec{d})$. Επιπροσθέτως, για μία ευρεία κλάση τετραγωνικών εξισώσεων το GSPS μπορεί εύκολα να μετατραπεί σε NIZK-PS. Προτού καθορίσουμε αυτές τις κατηγορίες περιγράφουμε τη γενική εικόνα μέσω $\mathcal{R}$-προτύπων.

Στην περίπτωση όπου $\mathbb{A}_1 = \mathcal{R}$, $\mathbb{A}_2 = \mathbb{A}_T$ και $f(x, y) = xy$ κατασκευάζουμε προσομοιωτή $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ ως εξής:

- Ο $\mathcal{S}_1$ με είσοδο gk, sk παράγει το σ και πρόσθετη πληροφορία $\tau = \vec{s}$, ώστε $\iota_1(1) = \iota_1(0) + \vec{s}^\top \vec{u}$.
- Ο $\mathcal{S}_2$ με είσοδο $gk, \sigma, \vec{s}$ και τις τετραγωνικές εξισώσεις $\{(\vec{\theta}_i, \vec{\pi}_i)\}_{i=1}^N$:
  1. Μετατρέπει κάθε εξίσωση στη μορφή
  $$\vec{a}_i \cdot \vec{y} + \vec{x} \cdot \vec{b}_i + f(\delta, -t_i) + \vec{x} \cdot \Gamma_i \vec{y} = 0.$$
  Ορίζει επίσης $\vec{x} = \vec{0}, \vec{y} = \vec{0}, \delta = 0$, που είναι μάρτυρας για όλες τις τροποποιημένες εξισώσεις.
  2. Επιλέγει τυχαίους $R \in Mat_{m\times\hat{m}}(\mathcal{R})$, $S \in Mat_{n\times\hat{n}}(\mathcal{R})$ και υπολογίζει τις δεσμεύσεις $\vec{c} = \vec{0} + R\vec{u}$, $\vec{d} = \vec{0} + S\vec{v}$ και $\iota_1(1) = \iota_1(0) + \vec{s}^\top \vec{u}$ για τις μεταβλητές $\vec{x}, \vec{y}, \delta$ αντίστοιχα.
  3. Υπολογίζει κανονικά αποδείξεις (θ_i, π_i) για κάθε εξίσωση $(\vec{a}_i, \vec{b}_i, -t_i, \Gamma_i, 0)$ και επιστρέφει την προσομοιωμένη απόδειξη $(\vec{c}, \vec{d}, \{(\theta_i, \pi_i)\}_{i=1}^N)$.

Η πληρότητα της προσομοιωμένης απόδειξης προκύπτει από το γεγονός ότι ο $\mathcal{S}_2$ γνωρίζει τον μάρτυρα $\vec{0}, \vec{0}, 0$ και το Θεώρημα 3.4.2, επομένως η $(\vec{c}, \vec{d}, \{(\theta_i, \pi_i)\}_{i=1}^N)$ ικανοποιεί για κάθε i την εξίσωση

$$\iota_1(\vec{a}_i) * \vec{d} + \vec{c} * \iota_2(\vec{b}_i) + F(\iota_1(1), -\iota_2(t_i)) + \vec{c} * \Gamma_i \vec{d} = \iota_T(0) + \vec{u} * \vec{\pi}_i + \vec{\theta}_i * \vec{v}. \quad (3.13)$$

Προσθέτοντας κατά μέλη στην (3.13) τον όρο $F(\iota_1(1), \iota_2(t_i))$ και λαμβάνοντας $F(\iota_1(1), \iota_2(t_i)) = \iota_T(f(1, t_i)) = \iota_T(t_i)$ από τις (3.10) συμπεραίνουμε ότι η προσομοιωμένη απόδειξη ικανοποιεί την εξίσωση επαλήθευσης.

Η μηδενική γνώση του συστήματος σε ένα προσομοιωμένο CRS είναι συνθέσιμη και τέλεια. Οι δεσμεύσεις $\vec{c}, \vec{d}, c$ ακολουθούν την ίδια κατανομή είτε υπολογίζονται πάνω σε «αυθεντικό» μάρτυρα $\vec{x}, \vec{y}$ είτε στον κατασκευασμένο, μέσω της trpadoor πληροφορίας μάρτυρα, $\vec{0}, \vec{0}, 0$. Από το Θεώρημα 3.4.4 έχουμε ότι σε κάθε περίπτωση οι $\{(\theta_i, \pi_i)\}_{i=1}^N$ κατανέμονται ομοιόμορφα στο πλήθος των τιμών που ικανοποιούν την εξίσωση επαλήθευσης.

Εντελώς παρόμοια μεθοδολογία ακολουθούμε για την περίπτωση $\mathbb{A}_2 = \mathcal{R} = \mathbb{Z}_{\mathbf{n}}$, $\mathbb{A}_1 = \mathbb{A}_T$. Η εφαρμογή στις εξισώσεις (3.6-9) που αφορούν την κρυπτογραφία ζεύγμάτων είναι άμεση καθώς οι συνθήκες $\mathbb{A}_1(\mathbb{A}_2) = \mathcal{R} = \mathbb{Z}_{\mathbf{n}}$, $\mathbb{A}_2(\mathbb{A}_1) = \mathbb{A}_T$ και $f(x, y) = xy$ ικανοποιούνται στις (3.7-9). Κάτι τέτοιο δεν ισχύει γενικά για μία εξίσωση γινομένου-ζεύγματος (3.6)

$$(\vec{A} \cdot \vec{Y})(\vec{X} \cdot \vec{B})(\vec{X} \cdot \Gamma\vec{Y}) = t_T,$$

διότι ακόμη και η γνώση trapdoor πληροφορίας πιθανόν να μην είναι αρκετή για την εξαγωγή ενός μάρτυρα αφού η τιμή $f(\delta, -t_T)$ δεν ορίζεται. Στην ειδική όμως περίπτωση όπου $t_T = 1$ τότε ο $\vec{\mathcal{O}}, \vec{\mathcal{O}}$ είναι ένας κατάλληλος μάρτυρας για τον προσομοιωτή. Επομένως, εάν $t_T = 1$, τότε μπορούμε να κατασκευάζουμε NIZK αποδείξεις και για εξισώσεις τύπου (3.6).

Μία ενδιαφέρουσα τεχνική κατασκευής NIZK αποδείξεων για εξισώσεις γινομένου-ζεύγματος είναι στην ειδική περίπτωση $t_T = \prod_{i=1}^n e(P_i, Q_i)$, όπου εισάγουμε τεχνητές μεταβλητές Z_i και εξισώσεις τύπου (3.8) $\delta Z_i - \delta Q_i = \mathcal{O}$ και ξαναγράφουμε την εξίσωση γινομένου-ζεύγματος ως $(\vec{A} \cdot \vec{Y})(\vec{X} \cdot \vec{B})(\vec{P} \cdot \vec{Z})(\vec{X} \cdot \Gamma\vec{Y}) = 1$ που είναι ξανά τύπου (3.6) με $t_T = 1$.

Η διόρθωση των στιγμιοτύπων SDXH και DLin και η υπόθεση SDLin. Το 2009, οι E.Ghadafi, N.Smart και B.Warinschi [GSW09] εντόπισαν ένα λεπτό αλλά σημαντικό λάθος που υπήρχε στα αρχικά στιγμιότυπα SDXH και DLin του GSPS που δόθηκαν από τους J.Groth και A.Sahai όσον αφορά στην ικανοποίηση των σχέσεων μετάβασης (3.10). Συγκεκριμένα, για εξισώσεις τύπου (3.7-9) η συνάρτηση ι_T ορίζεται έτσι ώστε η ιδιότητα

$$\forall x \in A_1 \forall y \in A_2 : F(\iota_1(x), \iota_2(y)) = \iota_T(f(x, y))$$

να μην ικανοποιείται για μη τετριμμένες $\iota_T \circ f$. Το αποτέλεσμα είναι ότι η πληρότητα του Θεωρήματος 3.4.2 δεν ευσταθεί, δηλαδή οι NIWI αποδείξεις δεν επαληθεύονται γενικά. Στο [GSW09] προτείνονται διαφορετικές ι_T για το στιγμιότυπο SDXH που αντιμετωπίζουν το πρόβλημα. Ενδεικτικά, για εξισώσεις βαθμωτού πολλαπλασια-

σμού στην $\mathbb{G}_2$ ορίζουμε $\iota_T : \mathbb{G}_2 \longrightarrow \mathbb{G}_T^4$ ως

$$\iota_T(Z) = F(u, (\mathcal{O}, Z)),$$

όπου $u = u_2 + (\mathcal{O}, P_1)$. Επομένως για κάθε $x \in \mathbb{Z}_p, Y \in \mathbb{G}_2$ έχουμε

$$F(\iota_2'(x), \iota_2(Y)) = F(xu = ([x]X_u, [x]Y_u), (\mathcal{O}, Y)) = \begin{pmatrix} 1 & e([x]X_u, Y) \\ 1 & e([x]Y_u, Y) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & e(X_u, [x]Y) \\ 1 & e(Y_u, [x]Y) \end{pmatrix} = F(u, (\mathcal{O}, [x]Y)) = \iota_T([x]Y) = \iota_T(f(x, Y)).$$

Βασικός λόγος που το πρόβλημα δεν είχε εντοπιστεί νωρίτερα είναι ότι δεν εμφανίζεται στις NIZK αποδείξεις που παράγονται με τη μεθοδολογία που περιγράψαμε στην προηγούμενη παράγραφο για τους τρεις αυτούς τύπους τετραγωνικών εξισώσεων. Αυτό συμβαίνει γιατί οι τροποποιημένες εξισώσεις

$$\vec{a}_i \cdot \vec{y} + \vec{x} \cdot \vec{b}_i + f(\delta, -t_i) + \vec{x} \cdot \Gamma_i \vec{y} = 0$$

είναι ομογενείς, άρα ισχύει ότι $\iota_T(0) = 0$. Ακολουθώντας τις παρατηρήσεις του [GSW09] οι J.Groth και A.Sahai διόρθωσαν το παράδειγμα DLin και παρουσίασαν ορθά τις τρεις εφαρμογές του GSPS στο [GS07] .

Τα συμμετρικά ζεύγματα ανταποκρίνονται λιγότερο από τα ασύμμετρα στα σημερινά επίπεδα ασφάλειας (βλ. [GPS08]). Από τα τρία προαναφερθέντα στιγμιότυπα το μόνο που λειτουργεί στην ασύμμετρη περίπτωση είναι το SDXH, το οποίο όμως αφορά μόνο ζεύγματα Τύπου 3. Καθώς τα ασύμμετρα ζεύγματα υπολογίζονται συνήθως πάνω στις ιδιαίτερα καθιερωμένες BN-καμπύλες, φαίνεται ότι είναι χρήσιμο ένα στιγμιότυπο GS-αποδείξεων που εφαρμόζεται και σε ζεύγματα Τύπου 2. Οι E.Ghadafi, N.Smart και B.Warinschi παρουσίασαν ένα τέτοιο παράδειγμα εισάγοντας μία ισχυρότερη εκδοχή του DLin σε ασύμμετρα ζεύγματα.

Υπόθεση Συμμετρικού γραμμικού προβλήματος απόφασης (*Symmetric DLin - SDLin - assumption*)**:** το Dlin είναι δύσκολο πρόβλημα στις $\mathbb{G}_1$, $\mathbb{G}_2$.

Όπως και στο αρχικό παράδειγμα DLin, $\mathbb{B}_1 = \mathbb{B}_2 = \mathbb{G}^3$, $\mathbb{B}_T = \mathbb{G}^9$ και

$$F(\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix}, \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix}) = \begin{pmatrix} e(X_1, Y_1) & e(X_1, Y_2) & e(X_1, Y_3) \\ e(X_2, Y_1) & e(X_2, Y_2) & e(X_2, Y_3) \\ e(X_3, Y_1) & e(X_3, Y_2) & e(X_3, Y_3) \end{pmatrix}.$$

Οι $\iota_1, p_1, \iota_2, p_2$ και τα σ, σ' επίλογονται όπως πριν για καθεμία από τις $\mathbb{G}_1, \mathbb{G}_2$. Επομένως έχουμε για $i = 1, 2$ και τυχαία $\alpha_i, \beta_i, r_i, s_i \in \mathbb{Z}_\mathbf{p}$:

$$\sigma = (u_i = ([\alpha_i]P_i, \mathcal{O}, P_i), v_i = (\mathcal{O}, [\beta_i]P_1, P_i), w_i = r_i u_i + s_i v_i) \quad \text{και}$$

$$\sigma' = (u_i = ([\alpha_i]P_i, \mathcal{O}, P_i), v_i = (\mathcal{O}, [\beta_i]P_1, P_i), w_i = r_i u_i + s_i v_i - (\mathcal{O}, \mathcal{O}, P_i))$$

Υπόθετοντας την SDLin τα σ, σ' είναι μη διακρίσιμα. Επίσης ορίζουμε
•$\mathbb{A}_i = \mathbb{Z}_p$: για $q_i = w_i + (\mathcal{O}, \mathcal{O}, P_i)$

$$\iota_i(z) = [z]q_i, \;\; p_i([z_1]P_i, [z_2]P_i, [z_3]P_i) = z_3 - \alpha_i^{-1} z_1 - \beta_i^{-1} z_2$$

$$c_i = \iota_i(Y) + \textstyle\sum_{i=1}^{2} t_i u_i, \quad t_1, t_2 \xleftarrow{\$} \mathbb{Z}_{\mathbf{p}}^3$$

•$\mathbb{A}_i = \mathbb{G}_i$:

$$\iota_i(z) = (\mathcal{O}, \mathcal{O}, Z), \;\; p_i(Z_1, Z_2, Z_3) = Z_3 - [\alpha_i^{-1}]Z_1 - [\beta_i^{-1}]Z_2$$

$$c_i = \iota_i(Y) + \textstyle\sum_{i=1}^{3} t_i u_i, \quad t_1, t_2, t_3 \xleftarrow{\$} \mathbb{Z}_{\mathbf{p}}^2.$$

Οι παραπάνω επιλογές εξασφαλίζουν την τέλεια απόκρυψη και συσχέτιση των δεσμεύσεων. Για την τέλεια ορθότητα υπολογίζονται ι_T, p_T ώστε $\iota_T \circ p_T = id_{\mathbb{B}_T}$ για κάθε τύπο εξίσωσης. Παραδείγματος χάριν, για τετραγωνικές εξισώσεις στο $\mathbb{Z}_p$ όπου $G_1 = G_2 = G_T = \mathbb{Z}_{\mathbf{p}}$ και $f(x, y) = xy \mod \mathbf{p}$ έχουμε

$$\iota_T(z) = F(q_1, q_2)^z$$

$$p_T\left(\begin{pmatrix} \zeta^{s_{11}} & \zeta^{s_{12}} & \zeta^{s_{13}} \\ \zeta^{s_{21}} & \zeta^{s_{22}} & \zeta^{s_{23}} \\ \zeta^{s_{31}} & \zeta^{s_{32}} & \zeta^{s_{33}} \end{pmatrix}\right) = s_3 - \alpha_2^{-1} s_1 - \beta_2^{-1} s_2,$$

όπου $\zeta = e(P_1, P_2)$ και $s_i = s_{3i} - \alpha_1^{-1} s_{1i} - \beta_1^{-1} s_{2i}$. Για πληρότητα ελέγχουμε τη σχέση

$$\forall x, y \in \mathbb{Z}_{\mathbf{p}} : F(\iota_1(x), \iota_2(y)) = F(xq_1, yq_2) = F(q_1, q_2)^{xy} = \iota_T(xy) = \iota_T(f(x, y)).$$

3.5 Επαληθευτές στίβας για το σύστημα απόδειξης Groth-Sahai

Το GSPS έδωσε μεγάλη ώθηση στην κρυπτογραφία ζεύγμάτων καθώς εισήγαγε νέες γενικές τεχνικές για την κατασκευή σύντομων μη διαλογικών αποδείξεων. Εντούτοις, οι πρακτικές εφαρμογές απαιτούν όλο και ταχύτερες διαδικασίες για αυτό και ο περιορισμός των αναγκαίων υπολογισμών, και ιδιαίτερα των υπολογισμών ζεύγματος, αποτελεί σημαντικό στόχο. Ακολουθώντας τη μεθοδολογία του [FGHP09] για την ασφαλή επαλήθευση συνόλου *εξισώσεων ζεύγματος* (*pairing-based equations*), οι O.Blazy κ.ά. [BFI+10], συντόμευσαν κατά πολύ τη διαδικασία

επαλήθευσης στο GSPS. Περιγράφουμε τα αποτελέσματά τους, δινόντας πρώτα τον κλασικό ορισμό του επαληθευτή στίβας προσαρμοσμένο στην κρυπτογραφία ζεύγμάτων.

Ορισμός 3.5.1. Έστω ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$. Ένας *γενικός ισχυρισμός* X είναι μία σχέση για την $3n+1$-άδα $(P_1, \ldots, P_n, Q_1, \ldots, Q_n, c_1, \ldots, c_n, t)$ που αντιστοιχεί στην εξίσωση $\prod_{i=1}^{n} e(P_i, Q_i)^{c_i} = A$. Ένας *επαληθευτής στίβας* (*batch verifier*) για σύνολο γενικών ισχυρισμών $X_1, \ldots, X_m$ είναι ένας PPT αλγόριθμος, ο οποίος με είσοδο τις παραμέτρους των $X_1, \ldots, X_m$:

- αποδέχεται αν ισχύουν όλοι οι $X_1, \ldots, X_m$.
- απορρίπτει με αμελητέα πιθανότητα σφάλματος εάν δεν ισχύει κάποιος από τους $X_1, \ldots, X_m$.

Μία βασική τεχνική για την επαλήθευση εξισώσεων της μορφής $y_i = g^{x_i}$, $i \in [n]$ γνωστή και ως *test με μικρούς εκθέτες* (*small exponents test*) [BGR98] , είναι η επιλογή εκθετών δ_i μεγέθους l bits και ο έλεγχος της ισότητας $\prod_{i=1}^{n} y_i^{\delta_i} = g^{\sum_{i=1}^{n} x_i \delta_i}$. Το αποτέλεσμα είναι ένας συμβιβασμός μεταξύ αποδοτικότητας και ασφάλειας που για τις εξισώσεις ζευγμάτων αποτυπώνεται στο παρακάτω θεώρημα.

Θεώρημα 3.5.2. *Έστω $X_1, \ldots, X_m$ γενικοί ισχυρισμοί $\prod_{i=1}^{n_j} e(P_{ij}, Q_{ij})^{c_{ij}} = t_i$ και $\delta_1, \ldots, \delta_m$ εκθέτες μεγέθους l bits. Έστω PPT αλγόριθμος $\mathcal{B}$ που ελέγχει την ισότητα $\prod_{i=1}^{m} \prod_{i=1}^{n_j} e(P_{ij}, Q_{ij})^{c_{ij}\delta_i} = \prod_{i=1}^{n} t_i^{\delta_i}$. Ο $\mathcal{B}$ είναι επαληθευτής στίβας με πιθανότητα σφάλματος 2^{-l}.*

Απόδειξη. Για απλότητα θεωρούμε ότι όλοι οι γενικοί ισχυρισμοί αντιστοιχούν σε ισότητες της μορφής $A_j = Y_j$, $j = 1, \ldots, n$. Η πληρότητα του $\mathcal{B}$ προκύπτει εύκολα, αφού αν $\forall j \in [n] : A_j = Y_j$, τότε $\prod_{i=1}^{n} A_j^{\delta_j} = \prod_{i=1}^{n} Y_j^{\delta_j}$. Για την απόδειξη της ορθότητας, έχουμε ότι $A_j = e(P,Q)^{\alpha_j}$ και $Y_j = e(P,Q)^{y_j}$ για κάποια $\alpha_j, y_j \in \mathbb{Z}_p$ και γεννήτορες P, Q. Επομένως η εξίσωση επαλήθευσης στίβας γράφεται ως

$$e(P,Q)^{\sum_{i=1}^{n} \alpha_j} = e(P,Q)^{\sum_{i=1}^{n} y_j}.$$

Εάν ο $\mathcal{B}$ αποδέχεται ισχύει ότι $\sum_{i=1}^{n} \beta_j \delta_j \equiv 0 \bmod q$, όπου $\beta_j = \alpha_j - y_j$. Έστω χωρίς βλάβη της γενικότητας ότι δεν ικανοποιείται η $A_1 = Y_1$. Τότε $\beta_1 \not\equiv 0 \bmod q$ και άρα το β_1 έχει αντίστροφο $\bmod (q)$. Επομένως

$$\delta_1 \equiv -\beta_1^{-1} \sum_{i=2}^{n} \beta_j \delta_j \bmod q. \tag{3.14}$$

Σύμφωνα με την (3.14), για δεδομένα $\delta_2, \ldots, \delta_n$ ο Q_1 δεν ικανοποιείται για μία ακριβώς τιμή του δ_1. Συνεπώς

$$\begin{aligned}\mathbf{Pr}[\text{σφάλματος}] &= \sum_{i=1}^{2^{l(n-1)}} \mathbf{Pr}[\text{σφάλματος} \mid \delta_2, \ldots, \delta_n] \cdot \mathbf{Pr}[\delta_2, \ldots, \delta_n] = \\ &= \sum_{i=1}^{2^{l(n-1)}} \mathbf{Pr}[\delta_1 \equiv -\beta_1^{-1} \sum_{i=2}^{n} \beta_j \delta_j \mid \delta_2, \ldots, \delta_n] \cdot \mathbf{Pr}[\delta_2, \ldots, \delta_n] = \\ &= 2^{l(n-1)}(2^{-l} \cdot 2^{-l(n-1)}) = 2^{-l}.\end{aligned}$$

⊣

Για την μετατροπή της εξίσωσης επαλήθευσης του $\mathcal{B}$ σε μια όσο δυνατόν αποδοτικότερη ισοδύναμη περιγραφή της, εφαρμόζονται οι ακόλουθες τεχνικές:

Μετακίνηση του εκθέτη μέσα στο ζεύγμα: η άθροιση στις $\mathbb{G}_1, \mathbb{G}_2$, όχι όμως στην $\mathbb{G}_2$ για ζεύγματα Τύπου 2 (βλ. [GPS08]), είναι συχνά ταχύτερη από τον πολλαπλασιασμό στην $\mathbb{G}_T$, οπότε αντικαθιστούμε $e(P,Q)^{\theta} \longrightarrow e([\theta]P, Q)$.

Αθροιστικός υπολογισμός γινομένου: όταν r ζεύγματα έχουν ένα κοινό όρισμα τότε μπορούμε να μειώσουμε το πλήθος υπολογισμών ζεύγματος σε έναν αντικαθιστώντας $\prod_{i=1}^{r} e([\theta_i]P_i, Q) \longrightarrow e(\sum_{i=1}^{r}[\theta_i]P_i, Q)$.

Εναλλαγή αθροισμάτων: είναι δυνατό η ταχύτητα υπολογισμού του ζεύγματος να βελτιώνεται εάν αλλάξουμε το όρισμα στο οποίο υπολογίζεται ένα άθροισμα, δηλαδή $e(\sum_{i=1}^{r}[\theta_i]P_i, Q_i) \longleftrightarrow e(P_i, \sum_{i=1}^{r}[\theta_i]Q_i)$.

Εφαρμόζοντας τις παραπάνω τεχνικές οι O.Blazy κ.ά. [BFI+10], κατασκεύασαν επαληθευτές στίβας για σύνολα τετραγωνικών εξισώσεων στο GSPS. Ο συμβιβασμός έγκειται στην ορθότητα του συστήματος, όπου υπεισέρχεται αμελητέα πιθανότητα σφάλματος. Ο περιορισμός του πλήθους των υπολογισμών ζεύγματος για κάθε περίπτωση φαίνεται στον παρακάτω πίνακα:

Εξίσωση	**SXDH**		**DLin**	
	Απλός επαληθευτής	Επαληθευτής στίβας	Απλός επαληθευτής	Επαληθευτής στίβας
Εξίσωση γινομένου ζεύγματος	$5m + 3n + 16$	$m + 2n + 8$	$12n + 27$	$3n + 6$
Βαθμωτού πολ/σμού στις $\mathbb{G}_1$, $\mathbb{G}_2$	$8m + 2n + 14$	$\min\{2n + 9, 2m + n + 7\}$	$9n + 12m + 27$	$3n + 3m + 6$
Τετραγωνική εξίσωση στην $\mathbb{Z}_p$	$8m + 8n + 12$	$2{\cdot}\min\{m, n\}{+}8$	$18n + 24$	$3n + 6$

Πίνακας 3.2.

Παράδειγμα 3.5.3. Για εξίσωσεις γινομένου-ζεύγματος στο στιγμιότυπο SXDH η εξίσωση επαλήθευσης έχει τη μορφή

$$\iota_1(\vec{A}) * \vec{D} + \vec{C} * \iota_2(\vec{B}) + \vec{C} * \Gamma\vec{D} = \iota_T(t) + \vec{U} * \vec{\pi} + \vec{\theta} * \vec{V}.$$

$$\begin{bmatrix} (\mathcal{O}, A_1) \\ \vdots \\ (\mathcal{O}, A_n) \end{bmatrix} * \begin{bmatrix} (D_{11}, D_{12}) \\ \vdots \\ (D_{n1}, D_{n2}) \end{bmatrix} + \begin{bmatrix} (C_{11}, C_{12}) \\ \vdots \\ (C_{m1}, C_{m2}) \end{bmatrix} * \begin{bmatrix} (\mathcal{O}, B_1) \\ \vdots \\ (\mathcal{O}, B_m) \end{bmatrix} + \begin{bmatrix} (C_{11}, C_{12}) \\ \vdots \\ (C_{m1}, C_{m2}) \end{bmatrix} * \Gamma \begin{bmatrix} (D_{11}, D_{12}) \\ \vdots \\ (D_{n1}, D_{n2}) \end{bmatrix} =$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & t \end{pmatrix} + \begin{bmatrix} (U_{11}, U_{12}) \\ (U_{21}, U_{22}) \end{bmatrix} * \begin{bmatrix} (\pi_{11}, \pi_{12}) \\ (\pi_{21}, \pi_{22}) \end{bmatrix} + \begin{bmatrix} (\theta_{11}, \theta_{12}) \\ (\theta_{21}, \theta_{22}) \end{bmatrix} * \begin{bmatrix} (V_{11}, V_{12}) \\ (V_{21}, V_{22}) \end{bmatrix}$$

Συνεπώς απαιτείται η επαλήθευση των παρακάτω τεσσάρων γενικών ισχυρισμών

$$X_{11} : \prod_{i=1}^{m} e(C_{i1}, \sum_{j=1}^{n} [\gamma_{ij}] D_{j1}) \stackrel{?}{=} \prod_{i=1}^{2} e(U_{i1}, \pi_{i1}) e(\theta_{i1}, V_{i1})$$

$$X_{12} : \prod_{i=1}^{m} e(c_{i1}, B_i) + \prod_{i=1}^{m} e(c_{i1}, \sum_{j=1}^{n} [\gamma_{ij}] D_{j2}) \stackrel{?}{=} \prod_{i=1}^{2} e(U_{i1}, \pi_{i2}) e(\theta_{i1}, V_{i2})$$

$$X_{13} : \prod_{j=1}^{n} e(A_j, D_{j1}) + \prod_{j=1}^{n} e(\sum_{i=1}^{m} [\gamma_{ij}] C_{i2}, D_{j1}) \stackrel{?}{=} \prod_{i=1}^{2} e(U_{i2}, \pi_{i1}) e(\theta_{i2}, V_{i1})$$

$$X_{14} : \prod_{j=1}^{n} e(A_j, D_{j2}) (\prod_{i=1}^{m} e(c_{i2}, B_i) + \prod_{i=1}^{m} e(c_{i2}, \sum_{j=1}^{n} [\gamma_{ij}] D_{j2})) \stackrel{?}{=}$$

$$\stackrel{?}{=} t \prod_{i=1}^{2} e(U_{i2}, \pi_{i2}) e(\theta_{i2}, V_{i2}).$$

Συνολικά απαιτούνται $m+(2m)+(2n)+(n+2m) = 5m+3n$ υπολογισμοί ζεύγματος για τα δεξιά μέλη των ισοτήτων και $4 \cdot 4 = 16$ για τα αριστερά. Επιλέγοντας μικρούς εκθέτες $\delta_{11}, \delta_{12}, \delta_{21}, \delta_{22}$ και εφαρμόζοντας τις παραπάνω τεχνικές καταλήγουμε στον έλεγχο της ισότητας

$$\prod_{j=1}^{n} e([\delta_{11}] \sum_{i=1}^{m} [\gamma_{ij}] C_{i1} + [\delta_{21}](A_j + \sum_{i=1}^{m} [\gamma_{ij}] C_{i2}), D_{j1}) \cdot$$

$$\cdot \prod_{j=1}^{n} e([\delta_{12}] \sum_{i=1}^{m} [\gamma_{ij}] C_{i1} + [\delta_{22}](A_j + \sum_{i=1}^{m} [\gamma_{ij}] C_{i2}), D_{j2}) \cdot \prod_{i=1}^{m} e([\delta_{12}] C_{i1} + [\delta_{22} C_{i2}, B_i) =$$

$$= t^{\delta_{22}} \prod_{i=1}^{2} e([\delta_{1i}] U_{11} + [\delta_{2i}] U_{12}, \pi_{1i}) \cdot e([\delta_{1i}] U_{21} + [\delta_{2i}] U_{22}, \pi_{2i}) \cdot$$

$$\cdot e([\delta_{1i}]\theta_{11} + [\delta_{2i}]\theta_{12}, V_{1i}) \cdot e([\delta_{1i}]\theta_{21} + [\delta_{2i}]\theta_{22}, V_{2i}).$$

Ο επαληθευτής στίβας αρκεί να εκτελέσει $m + 2n + 8$ υπολογισμούς ζεύγματος.

3.6 Σύνοψη κεφαλαίου - Εφαρμογές του GSPS

Δόθηκε το αναγκαίο θεωρητικό υπόβαθρο για την πλήρη παρουσίαση του συστήματος Groth-Sahai (GSPS) για την κατασκευή σύντομων μη διαλογικών αποδείξεων. Συγκεκριμένα, οι ορισμοί του διαλογικού και του μη διαλογικού συστήματος απόδειξης, της μη διακρισιμότητας οικογενειών τυχαίων μεταβλητών, της μηδενικής γνώσης και της μη διακρισιμότητας μάρτυρος, καθώς επίσης και χαρακτηριστικά παραδείγματα των εν λόγω εννοιών. Στη συνέχεια, μελετήθηκε εκτενώς το GSPS, μαζί με στιγμιότυπα και βελτιώσεις του.

Η αποδοχή του GSPS από την κρυπτογραφική κοινότητα υπήρξε ευρεία διότι αποτέλεσε γενικό μοντέλο κατασκευής χρήσιμων μη διαλογικών πρωτοκόλλων χωρίς τη χρήση τυχαίων μαντείων. Κάποιες από τις πιο ενδιαφέρουσες εφαρμογές ανήκουν στον χώρο των ομαδικών υπογραφών και στις οποίες αφιερώνεται μέρος του τελευταίου κεφαλαίου της εργασίας. Αξιοσημειώτες εφαρμογές και εργαλεία είναι επίσης μεταξύ άλλων οι *P-υπογραφές*, τα συστήματα e-Cash και τα *ανώνυμα διαπιστευτήρια* (*anonymous credentials*) των M.Belenkiy κ.ά. [BCKL08], [BCKL09], [BCC+09], οι *υπογραφές διατήρησης δομής* (*structure-preserving signatures*) των Abe κ.ά. [AFG+10], δηλαδή σχήματα υπογραφής όπου τα μηνύματα, οι υπογραφές και τα κλειδιά επαλήθευσης είναι στοιχεία ομάδας ζεύγματος και η επαλήθευση γίνεται με τον έλεγχο συνόλου εξισώσεων γινομένου ζεύγματος, οι *αδιαμφισβήτητες υπογραφές* (*undeniable signatures*) των L.Phong, K.Kurosawa και [PKO09], τα κρυπτογραφικά σχήματα *ανθεκτικότητας σε συνεχή διαρροή* (*continuous-leakage resilient*) πληροφορίας κατά την ανανέωση ιδιωτικών κλειδιών των Y.Dodis κ.ά. [AFG+10] και τα σχήματα υπογραφών *ανθεκτικότητας σε πλήρη διαρροή* (*fully-leakage resilient*) των T.Malkin κ.ά. [MTVY10] και E.Boyle, G.Segev και D.Wichs [BSW11].

Κεφάλαιο 4

Ομαδικές Υπογραφές στην Κρυπτογραφία Ζευγμάτων

Οι ομαδικές υπογραφές είναι μία κατηγορία ψηφιακών υπογραφών, όπου ένα μέλος μπορεί να υπογράψει ανώνυμα είτε εκ μέρους μίας ομάδας χρηστών που πιθανόν να μοιράζονται μια κοινή ιδιότητα, όπως για παράδειγμα να ανήκουν στο ίδιο τμήμα μιας εταιρίας, είτε στα πλαίσια αυτής, όπως ένας ενδιαφερόμενος σε διαγωνισμό ανάθεσης έργου. Επινοήθηκαν το 1991 από τους D.Chaum και E.Heyst [CvH91] με βασικές απαιτήσεις τη δυνατότητα υπογραφής μόνο από τα μέλη της ομάδας και την ύπαρξη μίας έμπιστης αρχής που θα αποκαλύπτει την ταυτότητα του υπογράφοντος σε περίπτωση αμφισβήτησης. Η επαλήθευση μίας υπογραφής, είναι δυνατή σε εξωτερικούς χρήστες του συστήματος, μέσω ενός δημόσιου ομαδικού κλειδιού. Με την πάροδο του χρόνου, προστέθηκαν διάφορες επιθυμητές ιδιότητες, που συγκεντρώθηκαν κυρίως στο λειτουργικό σχήμα των G.Ateniese κ.ά. [ACJT00]. Η πρώτη αυστηρή διατύπωση μοντέλου ομαδικών υπογραφών για στατικές ομάδες δόθηκε από τους M.Bellare, D.Micciano και B.Warinschi [BMW03] . Λίγο αργότερα, οι Α.Κιαγιάς και M.Yung [KY04] και οι M.Bellare, H.Shi και C.Zhang [BSZ05] όρισαν ανεξάρτητα τις ομαδικές υπογραφές στο πιο ρεαλιστικό μοντέλο της *δυναμικής ομάδας*, όπου ο αριθμός των μελών και οι ταυτότητές τους δεν έχουν προκαθοριστεί. Οι σύντομες ομαδικές υπογραφές των D.Boneh, X.Boyen και H.Shacham [BBS04] και D.Boneh και H.Shacham [BS04] έχουν καθιερωθεί στην κρυπτογραφία ζευγμάτων, με πλήθος εφαρμογών, το ενδιαφέρον όμως των ερευνητών δεν εξαντλείται σε αυτές τις δύο περιπτώσεις. Οι ομαδικές υπογραφές ήταν η πρώτη κατηγορία σχημάτων που εφαρμόστηκαν οι καινοτόμες NIZK τεχνικές με τη χρήση ζευγμάτων των J.Groth, R.Ostrovsky και A.Sahai [GOS06a], [GOS06b] ([Gro06], [BW06]) και αποτελούν από τα σημαντικότερα δείγματα της χρησιμότητας του συστήματος απόδειξης Groth-Sahai [Gro07], [LV09], [LPY12a].

4.1 Μοντέλα Ομαδικών Υπογραφών

Το μοντέλο BMW03. Θεμελιώδεις απαιτήσεις των ομαδικών υπογραφών, πέραν φυσικά από την επαληθευσιμότητα και την μη πλαστογράφηση μίας έγκυρης υπογραφής, είναι η δυνατότητα εντοπισμού του υπογράφοντος σε περίπτωση αμφισβήτησης από μία έμπιστη αρχή που ονομάζεται *διαχειριστής ομάδας* (*group manager - GM*) (*ανιχνευσιμότητα*) αλλά και η γνώση μίας υπογραφής να μην αποκαλύπτει την ταυτότητα του μέλους της ομάδας που την παρήγαγε σε κανέναν πλην του GM (*ανωνυμία*). Τα κλειδιά του συστήματος θεωρούνται ότι παράγονται και διανέμονται από μία τρίτη έμπιστη αρχή, η οποία μπορεί να αποσυρθεί στο τέλος της διαδικασίας, αφού η ομάδα είναι στατική.

Ορισμός 4.1.1. Ένα σχήμα ομαδικών υπογραφών $\mathbf{GS} = (\mathrm{GKey}, \mathrm{GSign}, \mathrm{GVer}, \mathrm{Open})$ για *στατική ομάδα* n χρηστών με ταυτότητες $1, 2, \ldots, n$ συνίσταται από τους παρακάτω τέσσερις αλγορίθμους:

- τον PPT αλγόριθμο GKey που με είσοδο $(1^k, 1^n)$, όπου k η παράμετρος ασφάλειας, παράγει το ομαδικό δημόσιο κλειδί gpk, το ιδιωτικό κλειδί του διαχειριστή ομάδας $gmsk$ και n ιδιωτικά κλειδιά $gsk[i]$ για κάθε μέλος i.
- τον PPT αλγόριθμο GSign που με είσοδο $(gsk[i], M)$ παράγει υπογραφή σ.
- τον πολυωνυμικό αλγόριθμο GVer που με είσοδο (gpk, M, σ) ελέγχει την εγκυρότητα της σ.
- τον πολυωνυμικό αλγόριθμο Open που με είσοδο $(gmsk, M, \sigma)$ επιστρέφει είτε μια ταυτότητα i, είτε $\perp$ σε περίπτωση αποτυχίας.

Απαιτούμε πρωτίστως το σχήμα να είναι *ορθό*, δηλαδή μία έγκυρη υπογραφή να είναι πάντα επαληθεύσιμη και να επιτρέπει στον GM αποκαλύπτει την ταυτότητα του υπογράφοντος. Επομένως για κάθε $k, n \in \mathbb{N}$, $i \in [n]$ και $M \in \{0,1\}^*$ πρέπει να ισχύει

$$\mathrm{GVer}(gpk, M, \mathrm{GSign}(gsk[i], M)) = 1 \quad \text{και} \quad \mathrm{Open}(gmsk, \mathrm{GSign}(gsk[i], M)) = i.$$

Επιπλέον επιθυμούμε το **GS** να είναι *εύχρηστο* (*compact*), με την έννοια ότι τα κλειδιά και οι υπογραφές του σχήματος να μην αυξάνονται αναλογικά με το πλήθος των μελών. Για κάποια πολυώνυμα p_1, p_2 λοιπόν έχουμε ότι

$$|gpk|, |gmsk|, |gsk[i]| \leqslant p_1(k, \log(n)) \quad \text{και} \quad |\sigma| \leqslant p_2(k, \log(n), |M|),$$

για κάθε $k, n \in \mathbb{N}$, $i \in [n]$, $M \in \{0,1\}^*$ και $\sigma \in \{r \mid r \longleftarrow \mathrm{GSign}(gsk[i], M)\}$.

Θεωρούμε τα δύο ακόλουθα παίγνια μεταξύ προκαλούντος $\mathcal{C}$ και αντιπάλου $\mathcal{A}$:

Παίγνιο Ανωνυμίας:

1. **Setup:** ο $\mathcal{C}$ επιλέγει παράμετρο ασφάλειας k και εκτελεί τον $\mathcal{GK}$ παράγοντας τα κλειδιά $gpk, gmsk, gsk[1], \ldots, gsk[n]$.
2. **Επιλογή:** ο $\mathcal{A}$ με είσοδο τα $gpk, gsk[1], \ldots, gsk[n]$ θέτει ερωτήματα (M_i, σ_i) στον $\mathcal{C}$, ο οποίος απαντά ως μαντείο $\mathrm{Open}(gmsk, \cdot, \cdot)$. Στο τέλος ο $\mathcal{A}$ επιστρέφει δύο έγκυρες ταυτότητες i_0, i_1 και μήνυμα M, τα οποία αποστέλλει στον $\mathcal{C}$, καθώς και πρόσθετη πληροφορία τ.
3. **Πρόκληση:** ο $\mathcal{C}$ επιλέγει τυχαία bit $b \in \{0,1\}$ και υπολογίζει την υπογραφή $\sigma \longleftarrow \mathrm{GSign}(gsk[i_b], M)$, με την οποία προκαλεί τον $\mathcal{A}$.
4. **Απόκριση:** ο $\mathcal{A}$ με είσοδο τ, σ θέτει εκ νέου ερωτήματα, εκτός της υπό πρόκληση υπογραφής σ, στο μαντείο $\mathrm{Open}(gmsk, \cdot, \cdot)$ και τελικά μαντεύει bit $b' \in \{0,1\}$. Ο $\mathcal{A}$ κερδίζει αν $b' = b$.

Ως πλεονέκτημα του $\mathcal{A}$ ορίζεται η ποσότητα

$$Adv_{\mathcal{A}}^{anon}(k,n) = \mid \mathbf{Pr}[b' = b] - \frac{1}{2} \mid .$$

Παίγνιο Ανιχνεύσιμότητας:

1. **Setup:** ο $\mathcal{C}$ επιλέγει παράμετρο ασφάλειας k και εκτελεί τον $\mathcal{GK}$ παράγοντας τα κλειδιά $gpk, gmsk, gsk[1], \ldots, gsk[n]$.
2. **Επιλογή:** ο $\mathcal{A}$ με είσοδο τα $gpk, gmsk$ και θέτοντας προσαρμοστικά ερωτήματα υπογραφής $\langle i, M_i \rangle$ και εξαγωγής ιδιωτικού κλειδιού j στον $\mathcal{C}$, ο οποίος απαντά ως μαντείο $\mathrm{GSign}(gsk[\cdot], \cdot)$, $gsk[\cdot]$ επιλέγει υποσύνολο πλήρως ελεγχόμενων χρηστών $S \subseteq [n]$.
3. **Απόκριση:** ο $\mathcal{A}$ θέτει νέα ερωτήματα υπογραφής, παράγει ζεύγος (M, σ) και κερδίζει εάν
   - η σ είναι έγκυρη υπογραφή για το M.
   - $\mathrm{Open}(gpk, M, \sigma) = \perp$ ή $\mathrm{Open}(gpk, M, \sigma) = j \notin S$ και το $\langle j, M \rangle$ δεν τέθηκε ως ερώτημα από τον $\mathcal{A}$.

Ως πλεονέκτημα του $\mathcal{A}$, $Adv_{\mathcal{A}}^{trace}(k,n)$ ορίζεται η πιθανότητα νίκης του $\mathcal{A}$.

Χρειαζόμαστε τον επόμενο ορισμό που γενικεύει την έννοια της αμελητέας συνάρτησης για συναρτήσεις που δέχονται δύο ορίσματα:

Ορισμός 4.1.2. Μία συνάρτηση $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ είναι αμελητέα, εάν για κάθε πολυωνυμικά φραγμένη συνάρτηση $t : \mathbb{N} \longrightarrow \mathbb{N}$ η συνάρτηση $f_t : \mathbb{N} \longrightarrow \mathbb{N}$, όπου $f_t(k) = f(k, t(k))$ είναι αμελητέα.

Βάσει του Ορισμού 4.4.2, οι δύο κύριες απαιτήσεις ενός σχήματος διατυπώνονται τυπικά ως εξής:

Ορισμός 4.1.3. Ένα σχήμα ομαδικών υπογραφών έχει *πλήρη ανωνυμία* (*full anonymity*), εάν για κάθε αντίπαλο $\mathcal{A}$, το $Adv_{\mathcal{A}}^{anon}(k,n)$ είναι αμελητέο, και *πλήρη ανιχνευσιμότητα* (*full traceability*), εάν για κάθε αντίπαλο $\mathcal{A}$, το $Adv_{\mathcal{A}}^{trace}(k,n)$ είναι αμελητέο.

Περιγραφικά, η ιδιότητα της πλήρους ανιχνευσιμότητας εξασφαλίζει ότι κανένα σύνολο συμπαιγνίας μελών δεν μπορεί να παράγει μη ανιχνεύσιμες υπογραφές ή έγκυρες υπογραφές όπου ο GM ξεγελάται συμπεραίνοντας ότι προέρχονται από μέλος εκτός του συνόλου. Οι ορισμοί πλήρους ανωνυμίας και ανιχνευσιμότητας, όπως σημειώνεται στο [BMW03 §3], συμπεριλαμβάνουν τις επιθυμητές ιδιότητες των ομαδικών υπογραφών που είχαν διατυπωθεί άτυπα έως τότε.

Μη πλαστογράφηση υπογραφής (*unforgeability*)**:** η θεμελιώδης απαίτηση ασφάλειας για κάθε σχήμα υπογραφών επιτυγχάνεται θεωρώντας αντιπάλους που εκτελούν το παίγνιο ανιχνευσιμότητας, χωρίς γνώση του $gmsk$ και έλεγχο στα μέλη της ομάδας.

Ανωνυμία: πρόκειται για παλαιότερη και ασθενέστερη έννοια της πλήρους ανωνυμίας, όπου ο αντίπαλος δεν έχει πρόσβαση σε μαντείο ανιχενυσιμότητας και γνώση των ιδιωτικών κλειδιών των μελών.

Αντίσταση σε συμπαιγνία (*coalition resistance*)**:** είναι η ιδιότητα της αδυναμίας συγκρότησης συνόλου μελών που μπορούν να παράγουν υπογραφές οι οποίες δεν ανιχνεύονται προς αυτά χωρίς ωστόσο να έχουν γνώση του ιδιωτικού κλειδιού του GM. Επικαλύπτεται από την πλήρη ανιχενυσιμότητα, μαζί με την αρχική έννοια της ανιχνευσιμότητας που σήμαινε την ορθή λειτουργία του αλγορίθμου Open.

Απαλλαξιμότητα (*exculpability*)**:** είναι η ιδιότητα της αδυναμίας οποιουδήποτε, ακόμα και του GM, να υπογράφει εκ μέρους κάποιου μέλους. Εά κάποιο μέλος i έχει αυτήν την δυνατότητα, τότε ένας αντίπαλος κερδίζει το παίγνιο ανιχνευσιμότητας θέτοντας μόνο το ερώτημα $gsk[i]$. Στην περίπτωση που ο GM καταφέρνει να υπογράψει εκ μέρους κάποιου μέλους, τότε ο αντίπαλος κερδίζει το παίγνιο ανιχνευσιμότητας ακολουθώντας απλώς την στρατηγική του GM.

Αντίσταση σε σκευωρία (*framing resistance*)**:** παραλλαγή της αντίστασης σε συμπαιγνία, όπου ακόμα και αν όλοι οι χρήστες πλην του μέλους i συνασπιστούν γνωρίζοντας το $gmsk$, δεν μπορούν να παράξουν έγκυρη υπογραφή η οποία ανιχνεύεται στον i. Η αντίσταση σε σκευωρία καλύπτεται από την πλήρη ανιχνευσιμότητα, ως ειδική περίπτωση.

Ασύνδετο υπογραφών (*unlinkability*)**:** είναι αδύνατον να διακρίνει κανείς εάν δύο ζεύγη μηνύματος - υπογραφής προέρχονται από το ίδιο μέλος. Το ασύνδετο υπογραφών δύσκολα μπορεί να οριστεί τυπικά καθώς δεν είναι πάντα ξεκάθαρος ο τρόπος που αντιμετωπίζει την παραγωγή υπογραφών ο αντίπαλος. Στα περισσότερα μοντέλα καταλήγει ισοδύναμη τεχνικά της ανωνυμίας.

Όλες οι παραπάνω ιδιότητες, εκτός της αντίστασης σε σκευωρία την οποία εισήγαγαν οι L.Chen και T.Pedersen [CP94], πληρούνται στο σχήμα του [ACJT00].

Το μοντέλο KY04. Μία διαφορετική προσέγγιση στη δημιουργία ανώνυμων υπογραφών, αποδίδεται στους A.Κιαγιά, I.Τσιούνη και M.Yung [KTY04] , οι οποίοι πρότειναν ένα νέο εργαλείο, τις *ανιχνεύσιμες υπογραφές* (*traceable signatures*). Στα σχήματα ανιχνεύσιμων υπογραφών η απαίτηση της ανιχνευσιμότητας υλοποιείται επιλεκτικά χωρίς να αποκαλύπτονται υπογραφές των έντιμων μελών και επιπλέον κάθε μέλος μπορεί να ισχυριστεί αποδεδειγμένα ότι έχει υπογράψει ένα μήνυμα. Ένα σχήμα ανιχνεύσιμης υπογραφών **TS** διαχειρίζεται από μία έμπιστη αρχή GM και περιλαμβάνει ένα σύνολο μη έμπιστων αρχών που καλούνται *ανιχνευτές* (*tracers*). Το **TS** συνίσταται από τα ακόλουθα εννέα πρωτόκολλα και αλγορίθμους:

Setup: με παράμετρο ασφάλειας k, ο GM παράγει δημόσιο κλειδί και ιδιωτικό $gmpk$, $gmsk$.

Join:πρωτόκολλο μεταξύ υποψήφιου νέου μέλους i και του GM, όπου μέσω του $gmsk$, καταλήγει στην απόδοση πιστοποιητικού εγγραφής $cert_i$ στο μέλος. *Αντίγραφο* (*transcript*) του πρωτοκόλλου αποθηκεύεται σε ιδιωτική βάση δεδομένων του GM.

(**Sign**, **Verify**)**:** η υπογραφή και η επαλήθευση συνιστούν μη διαλογικό πρωτόκολλο, από την εφαρμογή ευρετικών τεχνικών Fiat-Shamir σε διαλογικό πρωτόκολλο απόδειξης γνώσης του $cert_i$ τριών γύρων με τυχαία πρόκληση (βλ. Πρόταση 3.3.6).

Open:PPT αλγόριθμος που δεχόμενος ως είσοδο υπογραφή σ, το $gmsk$ και με πρόσβαση στα αντίγραφα του Join, επιστρέφει την ταυτότητα του υπογράφοντος και απόδειξη ορθής λειτουργίας.

Reveal:PPT αλγόριθμος που εκτελείται από τον GM και δεχόμενος ως είσοδο υπογραφή σ και το αντίγραφο του Join πρωτοκόλλου ενός μέλους i, εξάγει trapdoor πληροφορία $trace_i$ για τον i.

Trace: PPT αλγόριθμος που εκτελείται από τους ανιχνευτές και δεχόμενος ως είσοδο τις $\sigma, trace_i$, ελέγχει εάν ο i έχει δημιουργήσει την υπογραφή σ.

(**Claim**, **Claim_Verify**)**:** μη διαλογικό πρωτοκόλλο όπου το μέλος ως αποδείκτης επιχειρεί με τη χρήση του $cert_i$ να πείσει ότι έχει συμμετάσχει σε πρωτόκολλο Sign − Verify.

Το **TS** είναι *ορθό*, εάν όλοι οι παρακάτω έλεγχοι

- $\text{Verify}(M, gmpk, \text{Sign}_U(M)) = 1$
- $\text{Open}(gmsk, transcripts, \text{Sign}_U(M)) = U$
- $\text{Trace}(\text{Reveal}(U, transcripts), \text{Sign}_U(M)) = 1$ και
  $\text{Trace}(\text{Reveal}(U, transcripts), \text{Sign}_{U'}(M)) = 0,\ U' \neq U$
- $\text{Claim\_Verify}(M, \text{Sign}_U(M), \text{Claim}_\text{U}(M, \text{Sign}_U(M))) = 1,$

εμφανίζουν αμελητέα πιθανότητα σφάλματος για κάθε μήνυμα M και μέλος U. Οι απαιτήσεις ανωνυμίας, ανιχνευσιμότητας και αντίστασης σε σκευωρία του **TS** καθορίζονται από μοντέλα ασφάλειας ανάλογα με των ομαδικών υπογραφών. Στο [K-TY04] δίνεται κατασκευή ασφαλούς σχήματος ανιχνεύσιμων υπογραφών, βασισμένη σε τεχνικές του [ACJT00].

Η επινόηση των ανιχενύσιμων υπογραφών, επέτρεψε στους A.Κιαγιά και M.Yung [KY04] την μοντελοποίηση των ομαδικών υπογραφών σε δυναμικές ομάδες στα πλαίσια του σχήματος των Ateniese κ.ά., χωρίς τον διαχωρισμό των έμπιστων αρχών έγινε μετέπειτα όπως στο [BSZ05] . Βάσει του φορμαλισμού του [KY04] ένα σχήμα ομαδικών υπογραφών **GS** περιλαμβάνει τις εξής λειτουργίες:

Setup: με παράμετρο ασφάλειας k, παράγονται κλειδιά gpk, $gmsk$ καθώς και string καταστάσεων $St = (St_{users}, St_{trans})$ με αρχικές τιμές $St_{users} = \varnothing$, $St_{trans} = \epsilon$.

Join: πρωτόκολλο μεταξύ διαλογικών αλγορίθμων $\langle J_{user}, J_{GM}(St, gmsk)\rangle(1^k, gpk)$ που αντιστοιχούν στις πλευρές του μέλους i και του GM. Το αποτέλεσμα είναι η ιδιωτική έξοδος $(i, cert_i, sec_i)$ για το i, η δημόσια πληροφορία $(i, transcript_i)$ και η ενημέρωση του $St : St_{users} \cup \{i\} \leftarrow St_{users}$, $St_{trans}||(i, transcript) \leftarrow St_{trans}$.

Sign: το μήνυμα M υπογράφεται από το i ως $\sigma = \text{Sign}(gpk, cert_i, sec_i, M)$.

Verify: ο έλεγχος επαλήθευσης είναι ο $\text{Verify}(gpk, M, \sigma) \stackrel{?}{=} 1$.

Open: η ανίχνευση της προέλευσης μιας υπογραφής γίνεται από τον υπολογισμό

$$\text{Open}(gpk, gmsk, St, M, \sigma) \in St \cup \perp.$$

Το σχήμα είναι ορθό εάν το πλήθος των αντιγράφων στο St_{trans} ισούται με την πληθικότητα του St_{users}, οποιοδήποτε $cert_i$ που παράγεται από ένα συγκεκριμένο πρωτόκολλο Join αντιστοιχεί στο sec_i που δημιουργήθηκε από το ίδιο πρωτόκολλο και βεβαίως οι έγκυρες υπογραφές επαληθεύονται και ανιχνεύονται σωστά. Όσον αφορά την ασφάλεια του **GS**, ο αντίπαλος $\mathcal{A}$ θεωρείται ότι εκτελεί παίγνιο με διεπιφάνεια $\mathcal{I}$ αρχικής κατάστασης $state_\mathcal{I} := (St, gpk, gmsk) \leftarrow Setup(1^k)$. Τα τυχαία μαντεία που χρησιμοποιούνται είναι τα:

$\text{Q}_\text{pub}, \text{Q}_\text{key}$: η $\mathcal{I}$ επιστρέφει τα gpk, $gmsk$ αντίστοιχα.

$\mathrm{Q}_{\mathcal{A}-\mathrm{join}}$: η $\mathcal{I}$ εκκινεί με τον $\mathcal{A}$ το πρωτόκολλο Join προσομοιώνοντας τον GM και ενημερώνει το St καταχωρώντας νέο μέλος στο σύνολο των ελεγχόμενων από τον αντίπαλο μελών $U^{\mathcal{A}}$.

$\mathrm{Q}_{\mathrm{b}-\mathrm{join}}$: η $\mathcal{I}$ εκκινεί με τον αντίπαλο το πρωτόκολλο Join προσομοιώνοντας το μέλος. Ενημερώνει το St και κρατά την ιδιωτική πληροφορία $(cert_i, sec_i)$ μυστική από τον $\mathcal{A}$. Το νέο μέλος καταχωρείται στο σύνολο U^b.

$\mathrm{Q}_{\mathrm{read}}$: επιστρέφονται τα περιεχόμενα της $state_{\mathcal{I}}$ εκτός των gpk, $gmsk$ και της πληροφορίας που δημιουργήθηκε από ερωτήματα στο $\mathrm{Q}_{\mathrm{b}-\mathrm{join}}$.

$\mathrm{Q}_{\mathrm{write}}$: η $\mathcal{I}$ τροποποιεί αυθαίρετα δεδομένα εκτός της αλλοίωσης προϋπάρχοντων δεδομένων του St.

$\mathrm{Q}_{\mathrm{sign}}(i, M)$: η $\mathcal{I}$ δημιουργεί υπογραφή στο M βάσει των προσωπικών στοιχείων $cert_i, sec_i$ μέλους $i \in U^b$.

$\mathrm{Q}_{\mathrm{open}}(M, \sigma)$: η $\mathcal{I}$ εκτελεί τον Open και επιστρέφει την προέλευση της σ ή $\perp$ σε περίπτωση αποτυχίας εντοπισμού.

Το **GS** είναι ασφαλές αν ο αντίπαλος κερδίζει με αμελητέο πλεονέκτημα τα παρακάτω παίγνια:

Ανωνυμία: με την $\mathcal{I}$ σε αρχική κατάσταση, ο $\mathcal{A}$ θέτει ερωτήματα $\mathrm{Q}_{\mathrm{pub}}, \mathrm{Q}_{\mathcal{A}-\mathrm{join}}$, $\mathrm{Q}_{\mathrm{read}}, \mathrm{Q}_{\mathrm{open}}$ και παράγει ορθά ζεύγη $(cert_0, sec_0)$, $(cert_1, sec_1)$ μήνυμα M και πρόσθετη πληροφορία τ. Η $\mathcal{I}$ προκαλεί τον $\mathcal{A}$ επιλέγοντας τυχαίο $b \in \{0, 1\}$ και υπολογίζοντας $\sigma = \mathrm{Sign}(gpk, cert_i, sec_i, M)$. Ο $\mathcal{A}$ θέτει νέα ερωτήματα $\mathrm{Q}_{\mathrm{pub}}, \mathrm{Q}_{\mathcal{A}-\mathrm{join}}, \mathrm{Q}_{\mathrm{read}}$ και $\mathrm{Q}_{\mathrm{open}}$ εκτός της σ, επιλέγει $b' \in \{0, 1\}$ και κερδίζει εάν $b' = b$.

Εσφαλμένη αναγνώριση (*misidnetification*)**:** με την $\mathcal{I}$ σε αρχική κατάσταση, ο $\mathcal{A}$ θέτει ερωτήματα $\mathrm{Q}_{\mathrm{pub}}$, $\mathrm{Q}_{\mathcal{A}-\mathrm{join}}, \mathrm{Q}_{\mathrm{read}}, \mathrm{Q}_{\mathrm{open}}$ και παράγει ζεύγος (M, σ). Κερδίζει εάν $\mathrm{Verify}(gpk, M, \sigma) = 1$ και $\mathrm{Open}(gpk, gmsk, St, M, \sigma) = i \notin U^{\mathcal{A}}$.

Σκευωρία: με την $\mathcal{I}$ σε αρχική κατάσταση, $\mathcal{A}$ θέτει ερωτήματα $\mathrm{Q}_{\mathrm{pub}}, \mathrm{Q}_{\mathrm{key}}, \mathrm{Q}_{\mathcal{A}-\mathrm{join}}$, $\mathrm{Q}_{\mathrm{read}}, \mathrm{Q}_{\mathrm{write}}, \mathrm{Q}_{\mathrm{sign}}$ και παράγει ζεύγος (M, σ). Κερδίζει εάν $\mathrm{Verify}(gpk, M, \sigma) = 1$, $\mathrm{Open}(gpk, gmsk, St, M, \sigma) = i \in U^b$ και το $\langle i, M \rangle$ δεν τέθηκε ως ερώτημα στο $\mathrm{Q}_{\mathrm{sign}}$, δηλαδή αν καταφέρει να υπογράψει έγκυρα ένα μήνυμα, αποδίδοντας την ενέργεια σε μέλος έξω από τον έλεγχό του.

Το μοντέλο BSZ05. Οι Ορισμοί 4.1.1 και 4.1.3 αφορούν την περίπτωση που η ομάδα είναι στατική, δηλαδή τα μέλη και οι ταυτότητές τους είναι αμετάβλητα. Καθώς όμως η πλειοψηφία των εφαρμογών αφορά ομάδες δυναμικής φύσης, είναι απαραίτητη η επαύξηση των αρχικών ορισμών. Οι M.Bellare, H.Shi και C.Zhang [BSZ05] ακολούθησαν αυτήν την κατεύθυνση για ομαδικές υπογραφές σε ομάδες χωρίς *ανάκληση* (*revocation*) των μελών (*partially dynamic groups*). Η βασική καινοτομία ήταν η θεώρηση δύο έμπιστων αρχών, ενός *ανιχνευτή* (*open-*

er) προέλευσης υπογραφών και ενός *διανομέα* (*issuer*) ιδιωτικών κλειδιών στους χρήστες. Κάθε μία από τις δύο αρχές διαθέτει το προσωπικό της ιδιωτικό κλειδί.

Ορισμός 4.1.4. Ένα σχήμα ομαδικών υπογραφών **DGS** = (GKey, UKey, Join, Issue, GSign, GVer, Open, Judge) για *δυναμική ομάδα* συνίσταται από οκτώ πολυωνυμικούς αλγορίθμους ως εξής:

- μία τρίτη έμπιστη αρχή εκτελεί τον αλγόριθμο GKey που με είσοδο 1^k, όπου k η παράμετρος ασφάλειας, παράγει το ομαδικό δημόσιο κλειδί gpk, το ιδιωτικό κλειδί του ανιχνευτή osk και το ιδιωτικό κλειδί του διανομέα isk.

- ένας χρήστης i που θέλει να γίνει μέλος της ομάδας, εκτελεί τον αλγόριθμο UKey με είσοδο 1^k λαμβάνοντας ζεύγος προσωπικού ιδιωτικού και δημόσιου κλειδιού $upk[i], usk[i]$. Η πιστοποίηση και διανομή των $upk[i]$, γίνεται για προστασία από σκευωρία, ανεξάρτητα από τις έμπιστες αρχές της ομάδας, π.χ. μέσω PKI.

- ο χρήστης i όταν λάβει τα $upk[i], usk[i]$, εκκινεί διαλογικό πρωτόκολλο σε ασφαλές κανάλι με τον διανομέα. Οι αλγόριθμοι Join, Issue υλοποιούν τις πλευρές του i και του διανομέα αντίστοιχα. Σε κάθε στάδιο του πρωτοκόλλου, ο ενεργός αλγόριθμος έχει είσοδο μήνυμα M_{in} και κατάσταση $State(\cdot)$ και επιστρέφει έξοδο M_{out}, μία ανεωμένη κατάσταση και απόφαση $dec \in \{accept, reject, continue\}$. Εάν ο διανομέας αποδεχτεί, η τελική κατάσταση του Issue είναι τα περιεχόμενα της καταχώρησης $reg[i]$ στον πίνακα εγγεγραμμένων μελών **reg**. Εάν το i αποδεχτεί, η τελική κατάστασή του Join είναι το ιδιωτικό κλειδί $gsk[i]$.

- το μέλος i για να υπογράψει το μήνυμα M εκτελεί τον αλγόριθμο GSign με είσοδο $gsk[i], M$.

- η εγκυρότητα μίας υπογραφής ελέγχεται εκτελώντας τον αλγόριθμο GVer με είσοδο gpk, M, σ.

- ο ανιχνευτής, έχοντας πρόσβαση στον **reg**, εκτελεί τον αλγόριθμο Open για έγκυρη υπογραφή σ με είσοδο $(osk, M, \sigma, \mathbf{reg})$ και λαμβάνει ζεύγος (i, π). Εάν $i \geqslant 1$, αποκρίνεται ότι η σ δημιουργήθηκε από το μέλος i, ενώ εάν $i = 0$, τότε αποκρινεται ότι η σ δεν δημιουργήθηκε από κανένα μέλος της όμαδας. Η π αποτελεί απόδειξη του τελευταίου ισχυρισμού και επαληθεύεται μέσω του αλγορίθμου Judge.

- ο Judge δεχόμενος ως είσοδο το gpk, ακέραιο j και το αντίστοιχο δημόσιο κλειδί $upk[j]$, έγκυρο ζεύγος (M, σ) και πληροφορία π, ελέγχει αν η π αποδεικνύει ότι το j δημιούργησε την σ.

Για την αυστηρή διατύπωση των επιθυμητών απαιτήσεων του **DGS** θεωρούμε ότι ο αλγόριθμος $\mathrm{GKey}(1^k)$ εκτελείται από μία τρίτη έμπιστη αρχή και ότι ο αντίπαλος $\mathcal{A}$ θέτει ερωτήματα στα παρακάτω μαντεία (βλ. [BSZ05 §3]):

Μαντείο	**Όρισμα**	**Λειτουργία**	**Έξοδος**
$\mathrm{AddU}(\cdot)$	i	Δημιουργία έντιμου μέλους i : • $upk[i], usk[i] \leftarrow UKey(1^k)$ • $reg[i] \leftarrow State(\mathrm{Issue})$ • $gsk[i] \leftarrow State(\mathrm{Join})$	$upk[i]$
$\mathrm{CrptU}(\cdot,\cdot)$	$\langle i, upk\rangle$	Αλλοίωση προσωπικού δημόσιου κλειδιού του i: • $upk[i] \leftarrow upk$ • αρχικοποίηση $State(\mathrm{Issue})$	1
$\mathrm{SendToI}(\cdot,\cdot)$	$\langle i, M_{in}\rangle$	εκτέλεση $(\mathrm{Join}, \mathrm{Issue})$ - ο $\mathcal{A}$ παίζει το ρόλο του i: • $reg[i] \leftarrow State(\mathrm{Issue})$	M_{out}
$\mathrm{SendToU}(\cdot,\cdot)$	$\langle i, M_{in}\rangle$	εκτέλεση $(\mathrm{Join}, \mathrm{Issue})$ - ο $\mathcal{A}$ παίζει το ρόλο του διανομέα: • $gsk[i] \leftarrow State(\mathrm{Join})$	M_{out}, dec
$\mathrm{USK}(\cdot)$	i	Δημιουργία μυστικών κλειδιών για το μέλος i	$usk[i], gsk[i]$
$\mathrm{RReg}(\cdot)$	i	Άντληση περιεχομένων του **reg** για το μέλος i	$reg[i]$
$\mathrm{WReg}(\cdot,\cdot)$	$\langle i, \rho\rangle$	Τροποποίηση περιεχομένων του **reg** για τον i: • $reg[i] \leftarrow \rho$	Λ
$\mathrm{GSign}(\cdot,\cdot)$	$\langle i, M\rangle$	υπογραφή του M υπό το $gsk[i]$	$\mathrm{GSign}(gpk, gsk[i], M)$
$\mathrm{Open}(\cdot,\cdot)$	$\langle M, \sigma\rangle$	ανίχνευση υπογραφής	$\mathrm{Open}(gpk, ok, \mathbf{reg}, M, \sigma)$

Πίνακας 4.1

Με τη χρήση των μαντείων του Πίνακα 4.1 οι ιδιότητες του **DGS** ορίζονται ως εξης:

Ορθότητα: ο αντίπαλος $\mathcal{A}$ κατέχει το gpk και θέτει ερωτήματα στα $\mathrm{AddU}, \mathrm{RReg}$. Επιστρέφει ζεύγος i, M και κερδίζει εάν συμβαίνει ένα εκ των παρακάτω:

1. Η υπογραφή $\sigma = \mathrm{GSign}(gpk, gsk[i], M)$ δεν είναι έγκυρη.
2. $(j, \pi) \leftarrow \mathrm{Open}(gpk, ok, \mathbf{reg}, M, \sigma)$ και $j \neq i$, δηλαδή ο υπογράφων ανιχνεύεται εσφαλμένα.
3. $(i, \pi) \leftarrow \mathrm{Open}(gpk, ok, \mathbf{reg}, M, \sigma)$ και $\mathrm{Judge}(gpk, i, upk[i], M, \sigma, \pi) = 0$, δηλαδή η απόδειξη του ανιχνευτή δεν γίνεται αποδεκτή.

Το **DGS** είναι *ορθό* εάν η πιθανότητα νίκης του $\mathcal{A}$ είναι μηδενική.

Ανωνυμία: ο αντίπαλος $\mathcal{A}$ κατέχει τα gpk, isk και θέτει ερωτήματα στα SndToU, SndToI, RReg, WReg, Open, USK, CrptU. Έχει επομένως πλήρη έλεγχο του διανομέα, και επιτρέπεται επίσης να αποκτήσει τα ιδιωτικά κλειδιά, να αλλοιώσει τα δημόσια κλειδιά και να διαλεχθεί με τον διανομέα εκ μέρους οποιουδήποτε χρήστη, να διαβάσει και να μεταβάλει το **reg**. Στο τέλος, όπως και στην πλήρη ανωνυμία, αποστέλλει μήνυμα M και ταυτότητες i_0, i_1, και προκαλείται να μαντέψει σωστά τον υπογράφοντα i_b, $b \in \{0, 1\}$ θέτοντας ερωτήματα ανίχνευσης σε υπογραφές της επιλογής του εκτός της ύπο πρόκληση υπογραφής. Το **DGS** έχει *ανωνυμία* εάν το $Adv_{\mathcal{A}}^{anon}(k) =\mid \mathbf{Pr}[b' = b] - \frac{1}{2} \mid$ είναι αμελητέο.

Ανιχνευσιμότητα: ο αντίπαλος $\mathcal{A}$ κατέχει τα gpk, osk και θέτει ερωτήματα στα SndToI, AddU, RReg, USK, CrptU. Επομένως επιτρέπεται να προσθέσει νέους χρήστες, να αποκτήσει τα ιδιωτικά κλειδιά και να αλλοιώσει τα δημόσια κλειδιά οποιουδήποτε χρήστη, να διαβάσει το **reg** και να διαλεχθεί με τον διανομέα εκ μέρους οποιουδήποτε χρήστη. Στο τέλος κερδίζει εάν παράξει έγκυρο ζεύγος (σ, M) ώστε να συμβαίνει ένα εκ των παρακάτω:

1. $(0, \pi) \longleftarrow \text{Open}(gpk, ok, \mathbf{reg}, M, \sigma)$, δηλαδή ο ανιχνευτής δεν μπορεί να βρει την προέλευση της υπογραφής.
2. $(i, \pi) \leftarrow \text{Open}(gpk, ok, \mathbf{reg}, M, \sigma)$ και $\text{Judge}(gpk, i, upk[i], M, \sigma, \pi) = 0$, δηλαδή ο ανιχνευτής δεν μπορεί να αποδείξει ότι βρήκε την προέλευση της υπογραφής.

Το **GSD** έχει *ανιχνευσιμότητα* εάν η πιθανότητα νίκης του $\mathcal{A}$ είναι αμελητέα.

Αντίσταση σε Σκευωρία: ο αντίπαλος $\mathcal{A}$ κατέχει τα gpk, osk, isk, θέτει ερωτήματα στα SndToU, WReg, GSign, USK, CrptU και παράγει μήνυμα M, υπογραφή σ, ταυτότητα i και απόδειξη π. Ο $\mathcal{A}$ κερδίζει εάν συμβαίνουν τα εξής:

1. Η υπογραφή $\sigma = \text{GSign}(gpk, gsk[i], M)$ είναι έγκυρη.
2. Ο i είναι έντιμο μέλος και $\text{Judge}(gpk, i, upk[i], M, \sigma, \pi) = 1$, δηλαδή η απόδειξη του $\mathcal{A}$ γίνεται αποδεκτή.
3. Ο $\mathcal{A}$ δεν έθεσε ερωτήματα $i, \langle i, M \rangle$ στα USK, GSign αντίστοιχα.

Το **GSD** έχει *αντίσταση σε σκευωρία* εάν η πιθανότητα νίκης του $\mathcal{A}$ είναι αμελητέα.

Παρατηρούμε ότι ο αντίπαλος έχει περισσότερη ισχύ στο μοντέλο αντίστασης σε σκευωρία παρά στης ανιχνευσιμότητας, για αυτό και οι δύο ιδιότητες αντιμετωπίζονται χωριστά εν αντιθέσει με την στατική περίπτωση. Γενικά, οι M.Bellare, H.Shi

και C.Zhang εντοπίζουν τρία επίπεδα εμπιστοσύνης για τον διανομέα και τον ανιχνευτή: *αδιάφθοροι*, *μερικώς διεφθαρμένοι* (ο αντίπαλος κατέχει το ιδιωτικό τους κλειδί) ή *πλήρως διεφθαρμένοι* (ο αντίπαλος έχει τον πλήρη έλεγχο και μπορεί να τους ωθήσει σε παρέκκλιση από τα προγράμματά τους). Για τις τρεις απαιτήσεις που ορίστηκαν, τα επίπεδα εμπιστοσύνης έχουν όπως στον παρακάτω πίνακα:

Απαίτηση	**Ανιχνευτής**	**Διανομέας**
Ανωνυμία	Αδιάφθορος	Πλήρως διεφθαρμένος
Ανιχνευσιμότητα	Μερικώς διεφθαρμένος	Αδιάφθορος
Αντίσταση σε σκευωρία	Πλήρως διεφθαρμένος	Πλήρως διεφθαρμένος

Πίνακας 4.2

Είναι φανερό ότι οι ισχυρότεροι αντίπαλοι λαμβάνονται υπόψη για την αντίσταση σε σκευωρία, ενώ οι ασθενέστεροι για την ανιχνευσιμότητα. Στο [BSZ05 Appendix A] αναλύεται πώς οι τρεις ιδιότητες περικλείουν όλες τις παλαιότερες άτυπες απαιτήσεις ασφάλειας, κατά αναλογία με το μοντέλο BMW03.

Αξίζει να αναφέρουμε ότι τα μοντέλα ασφάλειας KY04 και BSZ05 ικανοποιούν μία ισχυρότερη εκδοχή απαλλαξιμότητας από το BMW03, όπου ούτε καν ο διανομέας των κλειδιών δεν μπορεί να υπογράψει εκ μέρους κάποιου μέλους της ομάδας. Οι A.Κιαγιάς και M.Yung στην ίδια εργασία [KY04] κατασκεύασαν ένα ασφαλές και λειτουργικό σχήμα ομαδικής υπογραφής στο ROM. Από την άλλη πλευρά, οι M.Bellare, H.Shi και C.Zhang [BSZ05] θεωρούν ισχυρότερους αντιπάλους για τα παίγνια ανωνυμίας και σκευωρίας και παρουσιάζουν ένα σχήμα που πληροί τις δικές τους προδιαγραφές ασφάλειας στο standard μοντέλο. Καθώς όμως χρησιμοποιούν γενικές NIZK τεχνικές για γλώσσα στο **NP**, η κατασκευή τους είναι θεωρητικού ενδιαφέροντος.

Ανάκληση μελών. Μέχρι τώρα ασχοληθήκαμε με ομάδες που λειτουργούν δυναμικά μόνο ως προς την προσθήκη νέων μελών. Στην πράξη όμως, είναι φυσικό κάποιο μέλος να αποχωρήσει είτε έκούσια είτε επιβεβλημένα, οπότε και πρέπει να ανακληθεί η ταυτότητά του. Είναι επομένως επιτακτική η εύρεση ενός ασφαλούς μηχανισμού ανάκλησης, αφού ο χρήστης θα πρέπει να μπορεί να αποδείξει ότι είναι ενεργός χωρίς να αποκαλύπτει σημαντική πληροφορία για την ταυτότητά του. Οι πρώτες απόπειρες αντιμετώπισης του δύσκολου αυτού προβλήματος [BS01], [AST01], [Son01], εμπεριείχαν την γραμμική εξάρτηση κάποιας λειτουργίας τους είτε από το πλήθος των μελών της ομάδας είτε των διαγραφόμενων μελών. Λειτουργική λύση έδωσαν οι J.Camenisch και A.Lysynskaya [CL02] εισάγοντας την έννοια του δυναμικού συσσωρευτή.

Ορισμός 4.1.5. Ένας *δυναμικός συσσωρευτής* (*dynamic accumulator*) για ένα σύνολο τιμών X είναι μία οικογένεια συναρτήσεων $\mathcal{F}_X$ με τις εξής ιδιότητες:

(i). Υπάρχει PPT αλγόριθμος $\mathcal{G}$ που παράγει ένα τυχαίο $f \in \mathcal{F}_X$ και trapdoor πληροφορία aux_f.

(ii). Κάθε $f \in \mathcal{F}_X$ έχει πεδίο ορισμού $U_f \times X$, όπου τα στοιχεια του U_f λαμβάνονται σε πολυωνυμικό χρόνο (*efficiently samplable*), και για $(u, x) \in U_f \times X$, το $f(u, x)$ υπολογίζεται σε πολυωνυμικό χρόνο.

(iii). Για κάθε $f \in \mathcal{F}_X$, $u \in U_f$ και $x_1, x_2 \in X$:

$$f(f(u, x_1), x_2) = f(f(u, x_2), x_1).$$

(iv). Μία τιμή $w \in U_f$ καλείται *μάρτυρας του* x *στην* v εάν $v = f(w, x)$. Η πιθανότητα ένας αντίπαλος $\mathcal{A}$ να εξάγει μάρτυρα w για $x \notin X$

$$\mathbf{Pr}[f \leftarrow \mathcal{G}(1^k); u \leftarrow U_f; (x, w, \{x_1, \ldots, x_m\}) \leftarrow \mathcal{A}(f, U_f, u) : \\ \{x_1, \ldots, x_m\} \subseteq X \wedge x \notin \{x_1, \ldots, x_m\} \wedge f(w, x) = f(u, \{x_1, \ldots, x_m\})],$$

όπου $f(u, \{x_1, \ldots, x_m\}) = f(f(\ldots f(u, x_1), \ldots), x_m)$, είναι αμελητέα.

(v). Η συσσώρευση των τιμών είναι δυναμικής φύσης, δηλαδή υπάρχουν PPT αλγόριθμοι $\mathcal{D}$, $\mathcal{W}$ ώστε εάν $S \subseteq X$, $v = f(u, S)$, $x, x' \in S$ και $f(w, x) = v$ τότε

- $\mathcal{D}(aux_f, v, x') = v'$ ώστε $v' = f(u, S \backslash \{x'\})$.
- $\mathcal{W}(f, v, v', x, x') = w'$ ώστε $f(w', x) = v'$.

Η τελευταία ιδιότητα εκφράζει την ισχυρή απαίτηση η διαγραφή τιμών από τον συσσωρευτή να εκτελείται σε χρόνο ανεξάρτητο του μεγέθους του S, εξασφαλίζει ωστόσο ότι αν ένας αντίπαλος $\mathcal{A}$ επιλέξει προσαρμοστικά εξ αρχής σύνολο S, δεν μπορεί να εξάγει w για $x \notin S$ ώστε $f(w, x) = f(u, S)$ [CL02 Theorem 2]. Η προσθήκη τιμών σε χρόνο ανεξάρτητο του μεγέθους του S δεν αποτελεί ξεχωριστή ιδιότητα αλλά έπεται από την 4.1.5.(iii) όπως φαίνεται από την επόμενη πρόταση

Πρόταση 4.1.6. *Έστω* $v = f(u, S)$ *η τρέχουσα τιμή του συσσωρευτή,* x' *νέα υπό προσθήκη τιμή και* $v' = f(v, x')$. *Έστω επίσης* $x \in S$ *και* w *μάρτυρας του* x *στην* v. *Ο υπολογισμός ενός μάρτυρα* w' *του* x *στην* v' *είναι ανεξάρτητος του μεγέθους του* S.

Απόδειξη. Θέτουμε $w' = f(w, x')$. Ισχύει ότι

$$f(w', x) = f(f(w, x'), x) \overset{4.1.5.(iii)}{=} f(f(w, x), x') = f(v, x').$$

⊣

Στο [CL02] κατασκευάζεται δυναμικός συσσωρευτής για το έως τότε state-of-the-art σχήμα [ACJT00]. Ο μηχανισμός ανάκλησης, όπου γίνεται ενημέρωση του δημοσίου κλειδιού και των ιδιωτικών κλειδιών των μελών σε κάθε μεταβολή της σύστασης της ομάδας, που απορρέει από την κατασκευή εφαρμόστηκε μεταξύ άλλων στις ομαδικές υπογραφές BBS04, όπως θα δούμε στην επόμενη ενότητα.

4.2 Οι ομαδικές υπογραφές των Boneh - Boyen - Shacham και Boneh - Shacham

Οι ομαδικές υπογραφές ACJT00 συγκέντρωσαν στις αρχές της περασμένης δεκαετίας το μεγαλύτερο μέρος του ενδιαφέροντος που υπήρχε για τις ομαδικές υπογραφές λόγω της αποδοτικότητάς τους και των πολλών καλών ιδιοτήτων που συγκεντρώνουν. Η κατάσταση άλλαξε με την κατασκευή σύντομων ομαδικών υπογραφών στα πλαίσια της κρυπτογραφίας ζευγμάτων από τους J.Camenisch και A.Lysynskaya [CL04] και περισσότερο από τους D.Boneh, X.Boyen και H.Shacham [BBS04] και D.Boneh και H.Shacham [BS04].

Οι ομαδικές υπογραφές BBS04. Το σχήμα BBS04 κατασκευάζεται από την εφαρμογή ευρετικών τεχνικών Fiat-Shamir σε ZK-PK διαλογικό πρωτόκολλο απόδειξης γνώσης μίας λύσης για το SDH ([BBS04 §4]). Θεωρούμε ομάδα n μελών και ζεύγμα $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ ομάδων τάξης πρώτου p ώστε υπάρχει αποδοτικά υπολογίσιμος ισομορφισμός $\psi : \mathbb{G}_2 \longrightarrow \mathbb{G}_1$ (Τύπου 1 ή 2). Έστω επίσης συνάρτηση hash $H^* : \{0,1\} \longrightarrow \mathbb{Z}_p$. Για συμβατότητα με το [BBS04], θεωρούμε τις ομάδες πολλαπλασιαστικές, δηλαδή αντί για $[\alpha]P + [\beta]Q$, γράφουμε $P^\alpha \cdot Q^\beta$. Αυτός ο τρόπος γραφής των ζευγμάτων θα διατηρηθεί στο κεφάλαιο καθώς ακολουθείται σε όλες τις εργασίες που θα μελετηθούν.

Σύμφωνα με το φορμαλισμό του BMW03, το σχήμα BBS04 συνίσταται από τους παρακάτω αλγορίθμους:

Keygen(n)**:** επιλέγονται τυχαία γεννήτορας $g_2 \in \mathbb{G}_2$, $\xi_1, \xi_2, \gamma \in \mathbb{Z}_p^*$, $h \in \mathbb{G}_1 \backslash \{1\}$ και υπολογίζονται τα $g_1 = \psi(g_2)$, u, v ώστε $u^{\xi_1} = v^{\xi_2} = h$ και $w = g_2^\gamma$. Για κάθε χρήστη $i \in [n]$, δημιουργούμε λύση του SDH (A_i, x_i) επιλέγοντας $x_i \neq -\gamma \in \mathbb{Z}_p^*$ και θέτοντας $A_i = g_1^{1/(\gamma + x_i)}$. Τα κλειδιά του σχήματος είναι τα $gpk = (g_1, g_2, h, u, v, w)$, $gmsk = (\xi_1, \xi_2)$, $gsk[i] = (A_i, x_i)$. Η τιμή γ μένει μυστική από όλους τους χρήστες, ακόμα και του GM, εκτός του διανομέα.

Sign$(gpk, gsk[i], M)$**:** για την υπογραφή μηνύματος M υπολογίζονται τα εξής:

1. $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$; $T_1 = u^\alpha$, $T_2 = v^\beta$, $T_3 = A_i \cdot h^{\alpha+\beta}$, $\delta_1 = x_i\alpha$, $\delta_2 = x_i\beta$.

2. $r_\alpha, r_\beta, r_{x_i}, r_{\delta_1}, r_{\delta_2} \xleftarrow{\$} \mathbb{Z}_p$; $R_3 = e(T_3, g_2)^{r_{x_i}} \cdot e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-r_{\delta_1} - r_{\delta_2}}$,

$$R_1 = u^{r_\alpha},\ R_2 = v^{r_\beta},\ R_4 = T_1^{r_{x_i}} \cdot u^{-r_{\delta_1}},\ R_5 = T_2^{r_{x_i}} \cdot v^{-r_{\delta_2}}.$$

3. $c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$.
4. $s_\alpha = r_\alpha + c\alpha,\ s_\beta = r_\beta + c\beta,\ s_{x_i} = r_{x_i} + cx_i,\ s_{\delta_1} = r_{\delta_1} + c\delta_1,\ s_{\delta_2} = r_{\delta_2} + c\delta_2$.
5. $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2})$.

Verify(gpk, M, σ)**:** για την επαλήθευση της σ εκτελούνται τα ακόλουθα βήματα:

1. Υπολογίζονται τα

$$\tilde{R}_1 = u^{s_\alpha} \cdot T_1^{-c}, \quad \tilde{R}_2 = v^{s_\beta} \cdot T_2^{-c}, \quad \tilde{R}_4 = u^{-s_{\delta_1}} \cdot T_1^{s_{x_i}}, \quad \tilde{R}_5 = v^{-s_{\delta_2}} \cdot T_2^{s_{x_i}},$$

$$\tilde{R}_3 = e(T_3, g_2)^{s_{x_i}} \cdot e(h, w)^{-s_\alpha - s_\beta} \cdot e(h, g_2)^{-s_{\delta_1} - s_{\delta_2}} \cdot (e(T_3, w)/e(g_1, g_2))^c.$$

2. η σ γίνεται αποδεκτή ανν

$$c \stackrel{?}{=} H(M, T_1, T_2, T_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5).$$

Open$(gpk, gmsk, M, \sigma)$**:** ο GM ανιχνεύει την προέλευση της σ

1. Ελέγχοντας αν η σ είναι έγκυρη.
2. Αποκαλύπτοντας την ταυτότητα του i μέσω του υπολογισμού $A_i = T_3/(T_1^{\xi_1} \cdot T_2^{\xi_2})$ και έχοντας γνώση των $\{A_1, \ldots, A_n\}$.

Μία υπογραφή BBS04 αποτελείται από τρία στοιχεία της $\mathbb{G}_1$ και έξι στοιχεία της $\mathbb{Z}_p$. Επιλέγοντας p μεγέθους 170 bits επιτυγχάνεται μήκος υπογραφής < 200 bytes, σημαντικά μικρότερο του 1Kbyte που έχει μία υπογραφή ACJT00, και με ασφάλεια περίπου ίδια μίας 1024-RSA υπογραφής. Για τη δημιουργία της, επειδή οι τιμές $e(h, w), e(h, g_2), e(g_1, g_2)$ και $e(A_i, g_2)$ μπορούν να αποθηκευτούν και αφού $e(T_3, g_2) = e(A_i, g_2) \cdot e(h, g_2)^{\alpha+\beta}$, δεν απαιτείται κανένας υπολογισμός ζεύγματος. Επιπλέον, κατά την επαλήθευση, ο μόνος απαραίτητος υπολογισμός ζεύγματος είναι ο $e(T_3, w^c \cdot g_2^{s_{x_i}}) = e(T_3, g_2)^{s_{x_i}} \cdot e(T_3, w)^c$ κατά την εξαγωγή του $\tilde{R}_3$.

Η πληρότητα του BBS04 ελέγχεται εύκολα. Η ασφάλεια ακολουθεί το μοντέλο του BMW03, με τη διαφορά ότι ζητείται μία ασθενέστερη ιδιότητα της πλήρους ανωνυμίας, καλούμενη *CPA-πλήρης ανωνυμία* (*CPA-full-anonymity*), η οποία όμως διατηρεί την ανωνυμία και το ασύνδετο υπογραφών. Σε αυτό το μοντέλο, ο αντίπαλος δεν έχει πρόσβαση στο μαντείο $Open(gmsk, \cdot, \cdot)$, δηλαδή δεν θέτει ερωτήματα ανίχνευσης. Για την απόδειξη της CPA-πλήρους ανωνυμίας και πλήρους ανιχνευσιμότητας, οι D.Boneh, X.Boyen και H.Shacham εισήγαγαν για πρώτη φορά το πρόβλημα DLin, του οποίου τη δυσκολία αποδεικνύουν [BBS04 Theorem 8.1] για αλγορίθμους που δεν χειρίζονται ειδικά την κωδικοποίηση των στοιχείων των

ομάδων (generic αλγόριθμοι). Θα δείξουμε την CPA-πλήρη ανωνυμία του BBS04 και παραπέμπουμε στο [BBS04 Theorem 5.3] για την απόδειξη της πλήρους ανιχνευσιμότητας. Θεωρούμε πρώτα το παρακάτω σχήμα:

Ορισμός 4.2.1. Ως *Γραμμική κρυπτογράφηση* (*Linear Encryption*) ορίζεται το παρακάτω σχήμα:

1. Το δημόσιο κλειδί είναι η τριάδα γεννητόρων $pk = (u, v, h) \in \mathbb{G}^3$ και το ιδιωτικό κλειδί το ζεύγος $sk = (x, y) \in \mathbb{Z}_p^2$ ώστε $u^x = v^y = h$.
2. Ένα μήνυμα M κρυπτογραφείται επιλέγοντας τυχαία $\alpha, \beta \in \mathbb{Z}_p$ και υπολογίζοντας το κρυπτοκείμενο $C = \langle u^\alpha, v^\beta, Mh^{\alpha+\beta} \rangle$.
3. Ένα κρυπτοκείμενο $C = \langle T_1, T_2, T_3 \rangle$ αποκρυπτογραφείται ως $T_3/(T_1^x \cdot T_2^y)$.

Η Γραμμική κρυπτογράφηση επεκτείνει το σχήμα κρυπτογράφησης El Gamal και είναι IND-CPA ασφαλής ακόμα και σε ομάδες που το DDH($\mathbb{G}$) είναι επιλύσιμο, αφού στηρίζεται στη δυσκολία του DLin στην $\mathbb{G}$. Πράγματι, εάν $\mathcal{A}$ είναι ένας αλγόριθμος που σπάει τη Γραμμική κρυπτογράφηση, τότε κατασκευάζουμε αλγόριθμο απόφασης για το DLin $\mathcal{B}$, ο οποίος με είσοδο $(u, v, h, u^\alpha, v^\beta, z)$:

1. δίνει στον $\mathcal{A}$ το (u, v, h) ως δημόσιο κλειδί.
2. επιλέγοντας $b \in \{0, 1\}$, απαντά στα μηνύματα επιλογής του $\mathcal{A}$ M_0, M_1 ως $\langle u^\alpha, v^\beta, M_b \cdot z \rangle$.
3. απαντά 1 εάν $b = b'$, όπου b' η απόκριση του $\mathcal{A}$.

Εύκολα παρατηρούμε ότι

$$\begin{aligned} Adv_{\mathcal{B}} =& \mid \mathbf{Pr}[\text{ο } \mathcal{B} \text{ κερδίζει}] - \frac{1}{2} \mid = \\ =& \mid \mathbf{Pr}[\text{ο } \mathcal{B} \text{ κερδίζει} \mid z \text{ τυχαίο}] + \mathbf{Pr}[\text{ο } \mathcal{B} \text{ κερδίζει} \mid z = h^{x+y}] - \frac{1}{2} \mid = \\ =& \mid \mathbf{Pr}[\text{ο } \mathcal{A} \text{ κερδίζει} \mid z \text{ τυχαίο}] + \mathbf{Pr}[\text{ο } \mathcal{A} \text{ κερδίζει} \mid z = h^{x+y}] - \frac{1}{2} \mid = \\ =& \mid \frac{1}{2} + Adv_{\mathcal{A}} - \frac{1}{2} \mid = Adv_{\mathcal{A}}. \end{aligned}$$

Θεώρημα 4.2.2. *Εάν η Γραμμική κρυπτογράφηση είναι IND-CPA ασφαλής, τότε το σχήμα ομαδικών υπογραφών BBS04 έχει CPA-πλήρη ανωνυμία στο ROM.*

Απόδειξη. Έστω PPT αλγόριθμος $\mathcal{A}$ που καταργεί την ανωνυμία του BBS04 θέτοντας q_H ερωτήματα στην H. Κατασκευάζουμε PPT αλγόριθμο $\mathcal{B}$ που σπάει τη Γραμμική κρυπτογράφηση.

Δεδομένου $pk = (u, v, h) \in \mathbb{G}_1^3$, ο $\mathcal{B}$ παράγει τις υπόλοιπες παραμέτρους του BBS04 και παρέχει στον $\mathcal{A}$ τα $gpk = (g_1, g_2, h, u, v, w)$ και (A_i, x_i), $i \in [n]$.

Ο $\mathcal{A}$ θέτει ερωτήματα στα οποία ο $\mathcal{B}$ απαντά ως τυχαίο μαντείο. Στη συνέχεια ο $\mathcal{A}$ ζητά να προκληθεί σε ταυτότητες i_0, i_1 και μήνυμα M.

Ο $\mathcal{B}$ με τη σειρά του ζητά να προκληθεί στα ιδιωτικά κλειδιά A_{i_0}, A_{i_1} και λαμβάνει Γραμμικό κρυπτοκείμενο $\langle T_1, T_2, T_3\rangle$ του $A_{i_b}, b \in \{0,1\}$. Από το $\langle T_1, T_2, T_3\rangle$ παράγει R_1, R_2, R_3, R_4, R_5 επιλέγοντας τυχαία $c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2} \in \mathbb{Z}_p$ και εκτελώντας τους αντίστοιχους υπολογισμούς του αλγορίθμου Sign. Προγραμματίζει την H ως $H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) = c$ και προκαλεί τον $\mathcal{A}$ με υπογραφή $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2})$.

Ο $\mathcal{A}$ αποκρίνεται b' στον $\mathcal{B}$, ο οποίος απαντά όμοια στην δική του πρόκληση. Ο $\mathcal{B}$ έχει επομένως το ίδιο πλεονέκτημα διάκρισης της τριάδας $\langle T_1, T_2, T_3\rangle$ με το πλεονέκτημα κατάργησης της ανωνυμίας της σ του $\mathcal{A}$. Εάν ο $\mathcal{A}$ τρέχει σε χρόνο t, τότε ο $\mathcal{B}$ τρέχει σε χρόνο $t + q_H O(1)$, αφού απαντά στα ερωτήματα του $\mathcal{A}$ και παράγει υπογραφή σ σε σταθερό χρόνο.

$\dashv$

Ανάκληση μελών στο BBS04. Οι μηχανισμοί ανάκλησης που προτάθηκαν στο [CL02] μπορούν να εφαρμοστούν και στο BBS04. Έστω χωρίς βλάβη της γενικότητας ότι πρέπει να ανακληθούν οι χρήστες $\{1, \ldots, r\}$. Μία έμπιστη αρχή δημοσιεύει *λίστα ανάκλησης* (*revocation list*) $\mathrm{RL} = \{(A_i^*, x_i)\}_{i\in[r]}$, όπου $A_i^* = g_2^{1/(\gamma+x_i)} = \psi(A_i^*) \in \mathbb{G}_2$ και στην περίπτωση που $\mathbb{G}_1 \neq \mathbb{G}_2$, η μυστική τιμή γ χρειάζεται για τον υπολογισμό των A_i^*. Η RL δίνεται στους υπογράφοντες και τους επαληθευτές του συστήματος προς ενημέρωση του δημόσιου κλειδιού $gpk = (g_1, g_2, h, u, v, w)$.

Θέτουμε $\bar{g}_1 = g_1^{1/y}$, $\bar{g}_2 = g_2^{1/y}$ και $\bar{w} = \bar{g}_2^{\gamma}$, όπου $y = \prod_{i=1}^{r}(\gamma + x_i) \in \mathbb{Z}_p^*$. Οποιοσδήποτε μπορεί τωρα να υπολογίσει το νέο δημόσιο κλειδί $(\bar{g}_1, \bar{g}_2, h, u, v, \bar{w})$ και επιπλέον ένα ενεργό μέλος μπορεί να ανανεώσει κατάλληλα το ιδιωτικό του κλειδί. Αυτό επιτυγχάνεται επαναλαμβάνοντας τα παρακάτω βήματα για $i = 1, \ldots, r$:

1. Από τα (g_1, g_2, h, u, v, w), (A_i^*, x_i) υπολογίζουμε το νέο δημόσιο κλειδί $(\hat{g}_1, \hat{g}_2, h, u, v, \hat{w})$, όπου

$$\hat{g}_2 = g_2^{1/(\gamma+x_i)} = A_i^*, \quad \hat{g}_1 = g_1^{1/(\gamma+x_i)} = A_i = \psi(A_i^*), \quad \hat{w} = g_2(A_i^*)^{-x_i} = \hat{g}_2^{\gamma}.$$

2. Ένα μέλος με ιδιωτικό κλειδί (A, x) υπολογίζει το $\hat{A} = \psi(A_i^*)^{1/(x-x_i)}/A^{1/(x-x_i)}$ και θέτει ως νέο ιδιωτικό κλειδί το $(\hat{A}, x)$. Ισχύει ότι $(\hat{A})^{\gamma+x} = \psi(A_i^*) = \hat{g}_1$ και επομένως το $(\hat{A}, x)$ είναι έγκυρο ως προς το $(\hat{g}_1, \hat{g}_2, h, u, v, \hat{w})$.

Παρατηρούμε ότι τα περιεχόμενα της RL συσσωρεύονται στα ανανεωμένα κλειδιά μέσω των συναρτήσεων f_1, f_2, f_3, f_4, όπου

$$f_1(g_1, (A_i^*, x_i)) = g_1^{1/(\gamma+x_i)}, \qquad f_2(g_2, (A_i^*, x_i)) = g_2^{1/(\gamma+x_i)},$$

$$f_3(g_2,(A_i^*,x_i)) = g_2(A_i^*)^{-x_i}, \quad f_4((A,x),(A_i^*,x_i)) = (\psi(A_i^*)^{1/(x-x_i)}/A^{1/(x-x_i)},x).$$

Για όλες τις παραπάνω συναρτήσεις είναι εύκολο να δείξουμε ότι ισχύει η 4.1.5.(iii). Ειδικά για τον υπολογισμό της f_4 απαιτείται η trapdoor πληροφορία (A,x). Από την απόδειξη της πλήρους ανιχνευσιμότητας έπεται ότι ένας χρήστης που έχει ανακληθεί δεν μπορεί να κατασκευάσει ένα νέο ιδιωτικό κλειδί για το $(\bar{g}_1,\bar{g}_2,h,u,v,\bar{w})$ δεδομένης της δυσκολίας του $(n+1)$-SDH.

Οι VLR-ομαδικές υπογραφές BS04. Οι ιδιότητες των ομαδικών υπογραφών είναι επιθυμητές για το Trusted Computing, ιδιαίτερα κατά τη διαδικασία επικύρωσης των εξαρτημάτων ενός υπολογιστή χωρίς την αποκάλυψη της ταυτότητάς του (privacy-preserving attestation). Με κίνητρο την ασφαλή ανάκληση ενός χρήστη-υπολογιστή, οι D.Boneh και H.Shacham [BS04] κατασκεύασαν ένα σχήμα ομαδικών υπογραφών συγγενές με το BBS04 με έναν μηχανισμό ανάκλησης, όπου μηνύματα ανάκλησης επεξεργάζονται μόνο από τους επαληθευτές και ο οποίος είχε χρησιμοποιηθεί ήδη στα [AST01], [Bri03], [KTY04], Οι ομαδικές υπογραφές με αυτό τον μηχανισμό καλούνται ομαδικές υπογραφές με *Τοπική Ανάκληση από τον Επαληθευτή* (*Verifier- Loval Revocation - VLR*) και είναι κατάλληλες σε εφαρμογές όπου οι επαληθευτές είναι σημαντικά λιγότεροι από τους χρήστες. Στο σχήμα VLR-ομαδικών υπογραφών BS04 η τοπική ανάκληση γίνεται δίνοντας ως είσοδο στον αλγόριθμο επαλήθευσης μία λίστα *τεκμηρίων ανάκλησης* (*revocation tokens*) RL για κάθε μέλος που έχει έως εκείνη τη στιγμή ανακληθεί.

Θεωρούμε ομάδα n μελών και ζεύγμα $e:\mathbb{G}_1\times\mathbb{G}_2\longrightarrow\mathbb{G}_T$ ομάδων τάξης πρώτου p, και αποδοτικά υπολογίσιμο ισομορφισμό $\psi:\mathbb{G}_2\longrightarrow\mathbb{G}_1$. Θεωρούμε επίσης συναρτήσεις hash $H_0:\{0,1\}\longrightarrow\mathbb{G}_2^2$, $H:\{0,1\}\longrightarrow\mathbb{Z}_p$. Το σχήμα VLR-ομαδικών υπογραφών BS04 συνίσταται από τους εξής αλγορίθμους:

Keygen(n)**:** επιλέγονται τυχαία γεννήτορας $g_2\in\mathbb{G}_2$, $\gamma\in\mathbb{Z}_p^*$ και υπολογίζονται τα $g_1=\psi(g_2)$ και $w=g_2^{\gamma}$. Επίσης, για κάθε μέλος $i\in[n]$, δημιουργούμε λύση του SDHP (A_i,x_i) επιλέγοντας $x_i\neq-\gamma\in\mathbb{Z}_p^*$ και θέτοντας $A_i=g_1^{1/(\gamma+x_i)}$. Τα κλειδιά του σχήματος είναι τα $gpk=(g_1,g_2,w)$, $gsk[i]=(A_i,x_i)$ καθώς και τα τεκμήρια ανάκλησης $grt[i]=A_i$. Η τιμή γ μένει μυστική από όλους τους χρήστες, εκτός του διανομέα.

Sign$(gpk,gsk[i],M)$**:** για την υπογραφή μηνύματος M υπολογίζονται τα εξής:

1. $r\xleftarrow{\$}\mathbb{Z}_p$; $(\hat{u},\hat{v})\longleftarrow H_0(gpk,M,r)$; $u=\psi(\hat{u})$, $v=\psi(\hat{v})$.
2. $\alpha\xleftarrow{\$}\mathbb{Z}_p$; $T_1=u^{\alpha}$, $T_2=A_i\cdot v^{\alpha}$, $\delta=x_i\alpha$.
3. $r_{\alpha},r_{x_i},r_{\delta}\xleftarrow{\$}\mathbb{Z}_p$; $R_1=u^{r_{\alpha}}$, $R_3=T_1^{r_{x_i}}u^{-r_{\delta}}$,

$$R_2=e(T_3,g_2)^{r_{x_i}}\cdot e(v,w)^{-r_{\alpha}-r_{\beta}}\cdot e(v,g_2)^{-r_{\delta}}.$$

4. $c \leftarrow H(gpk, M, r, T_1, T_2, R_1, R_2, R_3)$.

5. $s_\alpha = r_\alpha + c\alpha,\ s_{x_i} = r_{x_i} + cx_i,\ s_{\delta_1} = r_\delta + c\delta$.

6. $\sigma = (T_1, T_2, c, s_\alpha, s_{x_i}, s_\delta)$.

Verify$(gpk, \mathrm{RL}, M, \sigma)$**:** η εγκυρότητα σ γίνεται αποδεκτή ανν αποδέχονται οι δύο ακόλουθοι έλεγχοι:

1. Έλεγχος επαλήθευσης:

1. Υπολογίζονται τα $\hat{u}, \hat{v}, u, v$ όπως πριν και στη συνέχεια τα

$$\tilde{R}_1 = u^{s_\alpha} \cdot T_1^{-c}, \quad \tilde{R}_3 = T_1^{s_{x_i}} \cdot u^{-s_\delta}$$

$$\tilde{R}_2 = e(T_2, g_2)^{s_{x_i}} \cdot e(v, w)^{-s_\alpha} \cdot e(v, g_2)^{-s_\delta} \cdot (e(T_2, w)/e(g_1, g_2))^c.$$

2. η σ γίνεται αποδεκτή ανν

$$c \stackrel{?}{=} H(gpk, M, r, T_1, T_2, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3).$$

2. Έλεγχος ανάκλησης: για κάθε $A \in \mathrm{RL} \subset grt[i \cdots n]$ ελέγχεται εάν

$$e(T_2/A, \hat{u}) \stackrel{?}{=} e(T_1, \hat{v}),$$

δηλαδή εάν κάποιο A έχει κωδικοποιηθεί ως (T_1, T_2). Εάν αυτό δε συμβαίνει, τότε ο υπογράφων της σ δεν έχει ανακληθεί.

Το σχήμα BS04 ακολουθεί τα πρότυπα του μοντέλου [BMW03], με τη διαφορά πως η ανίχνευση μίας υπογραφής σ εκτελείται από μια έμπιστη αρχή που κατέχει όλο το $grt[i \cdots n]$ εκτελώντας τον **Verify** με $\mathrm{RL} = grt[i]$, $i = 1, \ldots n$ και δίνοντας ως απάντηση την ταυτότητα του πρώτου χρήστη για τον οποίον ο **Verify** επιστρέφει 0, ή $\perp$ εάν η σ γίνεται αποδεκτή για όλους τους χρήστες. Στο παίγνιο ανιχνευσιμότητας ο αντίπαλος έχει γνώση των $gpk, grt[i \cdots n]$ και θέτει προσαρμοστικά ερωτήματα υπογραφής για χρήστες και μηνύματα της επιλογής του.

Στο BS04 ένα μέλος εξάγει άμεσα το τεκμήριο ανάκλησης του από το ιδιωτικό του κλειδί. Μπορεί επομένως να επαληθεύσει εάν μια υπογραφή έχει παραχθεί από το ιδιωτικό του κλειδί, όχι όμως και να εξάγει οποιαδήποτε πληροφορία σε διαφορετική περίπτωση. Η νεά αυτή ιδιότητα ονομάζεται *ανιδιοτελής ανωνυμία* (*selfless anonymity*). Το BS04 αποδεικνύεται τελικώς ασφαλές στο ROM [BS04 §6]. Ο αλγόριθμος επαλήθευσης αν και προστατεύει την ανωνυμία των ενεργών μελών, συνεπάγεται αναπόφευκτα τη μη διατήρηση του ασυνδέτου υπογραφών για ένα διεγραμμένο μέλος: δύο υπογραφές σ_1, σ_2 αποδίδονται στον ίδιο διεγραμμένο μέλος i εάν είναι αποδεκτές με είσοδο την RL προτού το i ανακληθεί και μη αποδεκτές με είσοδο $\mathrm{RL} \cup \{grt[i]\}$.

Οι υπογραφές BS04 έχουν μήκος ακόμα μικρότερο των BBS04. Η επαλήθευση μίας υπογραφής έχει την αδυναμία της γραμμικής εξάρτησης από το πλήθος των διαγραφόμενων χρηστών, κατί που πιθανώς δεν είναι ιδιαίτερο πρόβλημα σε συστήματα όπου οι επαληθευτές είναι λιγότεροι ή σημαντικά ισχυρότεροι υπολογιστικά. Εντούτοις, τροποποιώντας ελαφρώς το αρχικό σχήμα, επιτυγχάνουμε επαλήθευση σε σταθερό χρόνο, με αντίτιμο την μερική απώλεια ανωνυμίας (βλ. [BS04 §7]). Η τελευταία μετατροπή μπορεί να είναι χρήσιμη σε εφαρμογές όπου ο γρήγορος μηχανισμός ανάκλησης είναι πρώτη προτεραιότητα.

Ισχυρή απαλλαξιμότητα στις BBS04 και BS04. Οι ομαδικές υπογραφές BBS04 και BS04, μπορούν να προσρμόσουν την απαίτηση ισχυρής απαλλαξιμότητας στα πλαίσια του μοντέλου ασφάλειας KY04, αν η διανομή ιδιωτικών κλειδιών πραγματοποιείται μέσω ενός πρωτοκόλλου Join μεταξύ του χρήστη και του διανομέα. Το ιδιωτικό κλειδί του i είναι τελικώς μία τριάδα (A_i, x_i, y_i) ώστε $A_i^{\gamma+x_i} \cdot h_1^{y_i} = g_1$, για κάποια δημόσια παράμετρο h_1, όπου το y_i επιλέγεται από τον i μυστικά από το διανομέα.

4.3 Οι ομαδικές υπογραφές των Boyen-Waters

Η καθιέρωση των υπογραφών BBS04 και BS04 έλυσε πολλά πρακτικά προβλήματα, σε επίπεδο ασφάλειας όμως παρέμενε η εξάρτηση από το ROM. Τα σχήματα ομαδικών υπογραφών στο standard μοντέλο των [BMW03] και [BSZ05], χρησιμοποιούσαν γενικές ZK τεχνικές και ήταν αδύνατο να εφαρμοστούν. Η πρώτη προσπάθεια ήταν αυτή των Ateniese κ.ά. [ACHdM05] , οι οποίοι παρουσίασαν ένα πολύ αποδοτικό σχήμα, η ασφάλειά του όμως στηρίζεται σε ορισμένες νέες και αρκετά ισχυρά υποθέσεις ενώ η ανωνυμία εξασφαλίζεται μόνο απέναντι σε αντιπάλους που δεν γνωρίζουν ιδιωτικά κλειδιά των χρηστών. Τα επόμενα αποτελέσματα βασίστηκαν στις τεχνικές των J.Groth, R.Ostrovsky και A.Sahai για κατασκευές NIZK αποδείξεων για γλώσσες στο **NP** με υποθέσεις από προβλήματα ζευγμάτων [GOS06a], [GOS06b] . Το σχήμα που πρότεινε ο J.Groth [Gro06] αποδεικνυέται ασφαλές στο μοντέλο BSZ05, αλλά το μήκος των υπογραφών, αν και σταθερό, εξαρτάται από πολύ μεγαλές σταθερές που καθιστούν απαγορευτική την εφαρμογή του. Ισορροπημένη πρόταση αποτελεί το σχήμα των X.Boyen και B.Waters [BW06] που στηρίζεται σε γενικές υποθέσεις και ασφάλεια πλήρους ανιχνευσιμότητας και CPA-πλήρους ανωνυμίας. Το σημαντικότερο πρόβλημα που εμφανίζει είναι η λογαριθμική εξάρτηση του μήκους των υπογραφών από το πλήθος των μελών. Στην πράξη όμως οι υπογραφές BW06 είναι συντομότερες των Gro06. Ένα χρόνο αργότερα, οι X.Boyen και B.Waters [BW07] αντιμετώπισαν το πρόβλημα της λογα-

ριθμικής εξάρτησης, όχι όμως και της μη πλήρους ανωνυμίας, με ένα διαφοροποιημένο σχήμα, του οποίου η ασφάλεια απαιτεί ισχυρότερες υποθέσεις.

Οι ομαδικές υπογραφές BW06 χτίζονται πάνω σε ένα ιεραρχικό σχήμα υπογραφών **HiSS** με δύο επίπεδα ιεραρχίας, το οποίο έπεται από το σχήμα κρυπτογράφησης βάσει ταυτοτήτων στο standard μοντέλο του [Wat05]. Στο **HiSS**, κάθε υπογραφή σε μήνυμα M_1 δρα ως ενδιάμεσο ιδιωτικό κλειδί για την υπογραφή μηνύματος $M_1||M_2$.

Θεωρούμε ζεύγμα $e : \mathbb{G} \times \mathbb{G} \longleftarrow \mathbb{G}_T$, όπου η $\mathbb{G}$ είναι σύνθετης τάξης $n = pq$, p, q πρώτοι. Υποθέτουμε g γεννήτορα της $\mathbb{G}_p \leqslant \mathbb{G}$ και συμβολίζουμε με l, m με $l < m$ τα μήκη των ταυτοτήτων των χρηστών και των μηνυμάτων αντίστοιχα. Το **HiSS** αποτελείται από τους παρακάτω αλγορίθμους:

Setup(1^k)**:** επιλέγονται τυχαία $\alpha, y', z' \in \mathbb{Z}_p$ και διανύσματα $\bar{y} = (y_1, \ldots, y_l) \in \mathbb{Z}_p^l$, $\bar{z} = (z_1, \ldots, y_m) \in \mathbb{Z}_p^m$ και υπολογίζονται τα $A = e(g, g)^\alpha \neq 1$, $u' = g^{y'}, v' = g^{z'}$, $u_1 = g^{y_1}, \ldots, u_l = g^{y_l}$ και $v_1 = g^{z_1}, \ldots, v_m = g^{z_m}$. Οι δημόσιες παράμετροι και το κύριο μυστικό κλειδί είναι αντίστοιχα τα

$$params = (p, G, G_T, e, g, u', u_1, \ldots, u_l, v', v_1, \ldots, v_m, A) \quad \text{και} \quad msk = g^\alpha.$$

Extract$(params, msk, ID)$**:** για τη δημιουργία ιδιωτικού κλειδιού του χρήστη ταυτότητας $ID = \langle \kappa_1 \cdots \kappa_l \rangle \in \{0,1\}^l$ επιλέγεται τυχαίο $r \in \mathbb{Z}_p$ και υπολογίζεται το

$$K_{ID} = (K_1, K_2) = (g^\alpha \cdot (u' \prod_{i=1}^{l} u_i^{\kappa_i})^r, g^{-r}).$$

Sign$(params, K_{ID}, M)$**:** η υπογραφή ενός μηνύματος $M = \langle \mu_1 \cdots \mu_m \rangle \in \{0,1\}^m$ υπό το K_{ID} παράγεται επιλέγοντας αρχικά τυχαίο $s \in \mathbb{Z}_p$ ως

$$\sigma = (K_1 \cdot (v' \prod_{j=1}^{m} v_j^{\mu_j})^s, K_2, g^{-s}).$$

Verify$(params, ID, M, \sigma)$**:** για την επαλήθευση της υπογραφής $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ ελέγχεται η ισότητα

$$e(\sigma_1, g) \cdot e(\sigma_2, u' \prod_{i=1}^{l} u_i^{\kappa_i}) \cdot e(\sigma_3, v' \prod_{j=1}^{m} v_j^{\mu_j}) \stackrel{?}{=} A.$$

Θεώρημα 4.3.1. *Εάν το CDH*$(\mathbb{G})$ *είναι δύσκολο, τότε το* **HiSS** *έχει ασφάλεια EUF-CMA.*

Απόδειξη. [BW06 Appendix C]. ⊣

Βάσει του **HiSS** κατασκευάζουμε το σχήμα ομαδικών υπογραφών BW06 ως εξής:

Setup(1^k)**:** επιλέγονται αρχικά γεννήτορες $g \in \mathbb{G}$ και $h \in \mathbb{G}_q$. Στη συνέχεια επιλέγονται τυχαίο $\alpha \in \mathbb{Z}_n$ και γεννήτορες $u', u_1, \ldots, u_l, v', v_1, \ldots, v_m \in \mathbb{G}$. Οι δημόσιες παράμετροι είναι οι

$$params = (n, G, G_T, e, g, h, , u', u_1, \ldots, u_l, v', v_1, \ldots, v_m, A = e(g,g)^\alpha)$$

Το κύριο κλειδί για την εγγραφή μελών και το ιδιωτικό κλειδί του GM είναι τα

$$msk = g^\alpha \quad \text{και} \quad gmsk = q.$$

Enroll$(params, msk, ID)$**:** για τη δημιουργία ιδιωτικού κλειδιού μέλους ταυτότητας $ID = \langle \kappa_1 \cdots \kappa_l \rangle \in \{0,1\}^l$ επιλέγεται τυχαίο $s \in \mathbb{Z}_p$ και υπολογίζεται το

$$K_{ID} = (K_1, K_2, K_3) = (g^\alpha \cdot (u' \prod_{i=1}^{l} u_i^{\kappa_i})^s, g^{-s}, h^s).$$

Sign$(params, ID, K_{ID}, M)$**:** η υπογραφή ενός μηνύματος $M = \langle \mu_1 \cdots \mu_m \rangle \in \{0,1\}^m$ υπό το K_{ID} παράγεται επιλέγοντας αρχικά τυχαία $t_1, \ldots, t_l \in \mathbb{Z}_p$ και υπολογίζοντας για κάθε $i \in [l]$ τα

$$c_i = u_i^{\kappa_i} \cdot h^{t_i}, \qquad \pi_i = (u_i^{2\kappa_i - 1} \cdot h^{t_i})^{t_i},$$

$$t = \sum_{i=1}^{l} t_i, \quad c = u' \prod_{i=1}^{l} c_i = (u' \prod_{i=1}^{l} u_i^{\kappa_i}) \cdot h^t, \quad V = v' \prod_{i=1}^{m} v_i^{\mu_i}.$$

Στη συνέχεια επιλέγονται τυχαία $s_1, s_2 \in \mathbb{Z}_p$ και παράγονται τα

$$\sigma_1 = K_1 \cdot K_3^t c^{s_1} \cdot V^{s_2}, \quad \sigma_2 = K_2 \cdot g^{-s_1}, \quad \sigma_3 = g^{-s_2}.$$

Τελικώς εξάγεται η υπογραφή

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, c_1, \ldots, c_l, \pi_1, \ldots, \pi_l) \in \mathbb{G}^{2l+3}.$$

Verify$(params, ID, M, \sigma)$**:** η επαλήθευση πραγματοποιείται σε δύο στάδια:

1. Υπολογίζεται το $c = u' \prod_{i=1}^{l} c_i$ και ελέγχονται οι ισότητες

$$e(c_i, u_i^{-1} \cdot c_i) \stackrel{?}{=} e(h, \pi_i), \quad \forall i \in [l].$$

2. Υπολογίζεται το $V = v' \prod_{i=1}^{m} v_i^{\mu_i}$ και ελέγχεται η ισότητα

$$e(\sigma_1, g) \cdot s(\sigma_2, c) \cdot e(\sigma_3, V) \stackrel{?}{=} A.$$

Open$(params, gmsk, \sigma)$**:** υποθέτουμε ότι η εγκυρότητα της σ έχει ελεγχθεί, επομένως το M είναι περιττό. Η ανίχνευση της ταυτότητας του υπογράφοντος, γίνεται ανακτώντας ένα ένα τα bits. Για $i = 1, \ldots, l$ θέτουμε

$$\kappa_i = \begin{cases} 0, & (c_i)^q = g^0 \\ 1, & \text{αλλιώς} \end{cases} \tag{4.1}$$

Η ταυτότητα που επιστρέφεται απο τον αλγόριθμο είναι η $ID = \langle \kappa_1, \ldots, \kappa_l \rangle$.

Παρατηρούμε ότι οι τιμές c_i και π_i αποτελούν NIZK αποδείξεις και η ανά bit κατασκευή τους οδηγεί στη λογαριθμική εξάρτηση του μήκους της υπογραφής από το πλήθος των μελών της ομάδας. Πρόκειται για εφαρμογή της τεχνικής που χρησιμοποιείται στο [GOS06b] με σκοπό την κατασκευή NIZK απόδειξης για το Circuit-SAT υπό την υπόθεση δυσκολίας του προβλήματος απόφασης υποομάδας (SDP). Συγκεκριμένα, κάθε π_i αποδεικνύει ότι το c_i κρυπτογραφεί πράγματι ένα bit (το κ_i). Επιγραμματικά, ικανοποιούνται οι

- **Πληρότητα:** εάν πράγματι $\kappa_i \in \{0, 1\}$ τότε
  1. $\kappa_i = 0 : c_i = h^{t_i}, \pi_i = u^{-t_i} \cdot h^{t_i^2} \Rightarrow e(c_i, u^{-1} \cdot c_i) = e(h^{t_i}, u^{-1} \cdot h^{t_i}) = e(h, \pi).$

  2. $\kappa_i = 1 : c_i = u_i \cdot h^{t_i}, \pi_i = u^{t_i} \cdot h^{t_i^2} \Rightarrow e(c_i, u^{-1} \cdot c_i) = e(u_i \cdot h^{t_i}, h^{t_i}) = e(\pi, h) = e(h, \pi).$

- **Ορθότητα:** για αποδεκτό έλεγχο $e(c_i, u^{-1} \cdot c_i) = e(h, \pi)$ έχουμε

  $e(c_i, u^{-1} \cdot c_i)^q = e(h, \pi)^q = e(h^q, \pi) = e(1, \pi) = 1 \Rightarrow c_i^q = 1 \vee (u^{-1} c_i)^q = 1$
  $\Rightarrow (u_i^{\kappa_i})^q (h^{t_i})^q = (u_i^{\kappa_i})^q = 1 \vee (u_i^{\kappa_i - 1})^q (h^{t_i})^q = (u_i^{\kappa_i - 1})^q = 1 \Rightarrow \kappa_i \in \{0, 1\}.$

- **Μηδενική γνώση:** σε ένα προσομοιωμένο CRS:=$params$, ο προσομοιωτής δεν μπορεί να διακρίνει εάν το τυχαία επιλεγμένο h είναι γεννήτορας της $\mathbb{G}_q$ ή όχι, λόγω της υπόθεσης SDP.

Είναι εύκολο να δούμε ότι οι παραπάνω αποδείξεις πλησιάζουν τη μεθοδολογία του στιγμιότυπου SDP για το GSPS. Για περισσότερες λεπτομέρειες, ο αναγνώστης μπορεί να ανατρέξει στο [GOS06b §4]. Στα δύο επόμενα θεωρήματα αποδεικνύουμε την ασφάλεια του BW06.

Θεώρημα 4.3.2. *Εάν το SDP είναι δύσκολο, τότε το BW06 έχει CPA-πλήρη ανωνυμία.*

Απόδειξη. Έστω $Adv_{\mathcal{A}}^{\text{SDP}}$ το πλεονέκτημα επίλυσης του SDP ενός αντιπάλου $\mathcal{A}$ και $Adv_{\mathcal{A}}$ το πλεονέκτημα του $\mathcal{A}$ για το παίγνιο CPA-πλήρους ανωνυμίας. Θεωρούμε παίγνιο H_1 παρόμοιο με το παίγνιο CPA-πλήρους ανωνυμίας, με μόνη διαφορά ότι το h είναι τυχαία επιλεγμένος γεννήτορας της $\mathbb{G}$. Ορίζουμε ως $Adv_{\mathcal{A}}^{H_1}$ το πλεονέκτημα του $\mathcal{A}$ για το H_1.

Ισχυρισμός 1: *Εάν το SDP είναι δύσκολο, τότε η ποσότητα* $Adv_{\mathcal{A}} - Adv_{\mathcal{A},H_1}$ *είναι αμελητέα.*

Κατασκευάζουμε αλγόριθμο $\mathcal{B}$ για το SDP. Ο $\mathcal{B}$ με είσοδο $(n, \mathbb{G}, \mathbb{G}_T, e, w)$ δημιουργεί δημόσιες παραμέτρους του BW06 με μόνο περιορισμό $h = w$ και εκτελεί το παίγνιο ανωνυμίας με τον $\mathcal{A}$, χωρίς πρόφανώς να γνωρίζει εάν πρόκειται για το παίγνιο CPA-πλήρους ανωνυμίας (δηλ. $w \xleftarrow{\$} \mathbb{G}_q$) ή για το H_1 (δηλ. $w \xleftarrow{\$} \mathbb{G}$).

Ο $\mathcal{A}$ επιλέγει να προκληθεί σε ταυτότητες ID_0, ID_1 και μήνυμα M, οπότε ο $\mathcal{B}$ επιλέγει $b \in \{0,1\}$, προκαλώντας τον $\mathcal{A}$ με υπογραφή σ. Ο $\mathcal{A}$ αποκρίνεται $b' \in \{0,1\}$ και κερδίζει εάν $b' = b$. Σε περίπτωση νίκης του $\mathcal{A}$ ο $\mathcal{B}$ αποφασίζει ότι $w \in \mathbb{G}_q$, διαφορετικά αποφασίζει ότι $w \in \mathbb{G}$, Λόγω της τυχαίας επιλογής του w ισχύει ότι $\mathbf{Pr}[w \in \mathbb{G}] = \mathbf{Pr}[w \in \mathbb{G}_q] = \frac{1}{2}$. Επομένως έχουμε

$$\begin{aligned} Adv_{\mathcal{A}} - Adv_{\mathcal{A},H_1} &= \mathbf{Pr}[b' = b \mid w \in \mathbb{G}_q] - \mathbf{Pr}[b' = b \mid w \in \mathbb{G}] = \\ &= \frac{\mathbf{Pr}[b' = b \wedge w \in \mathbb{G}_q]}{\mathbf{Pr}[w \in \mathbb{G}_q]} - \frac{\mathbf{Pr}[b' = b \wedge w \in \mathbb{G}]}{\mathbf{Pr}[w \in \mathbb{G}]} = \\ &= 2 \cdot \mathbf{Pr}[b' = b \wedge w \in \mathbb{G}_q] - 2 \cdot \mathbf{Pr}[b' = b \wedge w \in \mathbb{G}] = 2Adv_{\mathcal{B}}^{\mathrm{SDP}}, \end{aligned}$$

όπου το $Adv_{\mathcal{B}}^{\mathrm{SDP}}$ είναι εξ υποθέσεως αμελητέο.

Ισχυρισμός 2: $Adv_{\mathcal{A},H_1} = 0$.

Θα δείξουμε ότι μία υπογραφή πρόκλησης $\sigma = (\sigma_1, \sigma_2, \sigma_3, c_1, \ldots, c_l, \pi_1, \ldots, \pi_l)$ δεν παρέχει καμία πληροφορία για την ταυτότητα $ID_{b'} = \langle \kappa_1 \ldots \kappa_l \rangle$ που επέλεξε ο προκαλών στο παίγνιο H_1, όταν το h είναι τυχαία επιλεγμένο από την $\mathbb{G}$. Πράγματι, ο υπολογισμός των $\sigma_1 = g^{\alpha} \cdot c^{s+s_1} \cdot V^{s_2}$, $\sigma_2 = g^{-s-s_1}$ και $\sigma_3 = g^{-s_2}$ εξαρτάται μόνο από τη δυσκολία εύρεσης των $\alpha, s + s_1, s_2$. Εξάλλου, ένα ζεύγος τιμών (c_i, π_i) μπορεί να προκύψει ισοπίθανα είτε για $\kappa_i = 0$ είτε για $\kappa_i = 1$, δηλαδή

$$\forall i \in [l] : \exists \tau_0, \tau_1 : (\kappa_i, t_i) = (0, \tau_0) \vee (\kappa_i, t_i) = (1, \tau_1) \quad \text{και} \quad c_i = h^{\tau_0} = u_i \cdot h^{\tau_1}.$$

Αντίστοιχα έχουμε

$$\pi_i \mid_{\kappa_i = 0} = (u_i^{-1} \cdot h^{\tau_0})^{\tau_0} = (u_i^{-1} \cdot u_i \cdot h^{\tau_1})^{\tau_0} = h^{\tau_0 \tau_1} = (u_i \cdot h^{\tau_1})^{\tau_1} = \pi_i \mid_{\kappa_i = 1},$$

επομένως τελικά η σ είναι στατιστικά ανεξάρτητη της $ID_{b'}$. Παρατηρούμε την ομοιότητα με την κατάσταση τέλειας απόκρυψης - τέλειας WI στο GSPS.

Η απόδειξη θεωρήματος έπεται άμεσα από τους Ισχυρισμούς 1 και 2.

$\dashv$

Θεώρημα 4.3.3. *Εάν το* **HiSS** *έχει ασφάλεια EUF-CMA, τότε το BW06 έχει πλήρη ανιχνευσιμότητα.*

Απόδειξη. Έστω αντίπαλος $\mathcal{A}$ που κερδίζει το παίγνιο ανιχνευσιμότητας στο μοντέλο BMW03 και $Adv_{\mathcal{A}}^{trace} = \epsilon$. Κατασκευάζουμε αλγόριθμο $\mathcal{B}$ που κερδίζει το παίγνιο EUF-CMA για το **HiSS** με το ίδιο πλεονέκτημα.

Εφόσον ο $\mathcal{A}$ διαθέτει το $gmsk = q$, υποθέτουμε ότι ο $\mathcal{B}$ γνωρίζει την παραγοντοποίηση του $n = pq$. Ο $\mathcal{B}$ λαμβάνει δημόσιες παραμέτρους του **HiSS** από τις υποομάδες p τάξης $\mathbb{G}_p, \mathbb{G}_{T_p}$ των $\mathbb{G}, \mathbb{G}_T$ αντίστοιχα

$$params' = (p, G, G_T, e, \hat{g}, \hat{u}', \hat{u}_1, \ldots, \hat{u}_l, \hat{v}', \hat{v}_1, \ldots, \hat{v}_m, \hat{A}) \in \mathbb{G}_p^{l+m+3} \times \mathbb{G}_{T_p}.$$

Στη συνέχεια επιλέγει τυχαίους γεννήτορες $(f, h, \gamma', \gamma_1, \ldots, \gamma_l, \delta', \delta_1, \ldots, \delta_m)$ της $\mathbb{G}_q^{l+m+4}$ και $\beta \in \mathbb{Z}_q$ και αποστέλει στον $\mathcal{A}$ τις δημόσιες παραμέτρους του BW06

$$\begin{aligned} params = (n, G, G_T, e, g = \hat{g}f, h, u' = \hat{u}'\gamma', u_1 = \hat{u}_1\gamma_1, \ldots, u_l = \hat{u}_l\gamma_l, v' = \hat{v}'\delta', \\ v_1 = \hat{v}_1\delta_1, \ldots, v_m = \hat{v}_m\delta_m, A = \hat{A} \cdot e(f, f)^{\beta}) \in \mathbb{G} \times \mathbb{G}_q \times \mathbb{G}^{l+m+2} \times \mathbb{G}_T, \end{aligned}$$

μαζί με το κλειδί $gmsk = q$.

Εάν ο $\mathcal{A}$ ζητήσει από τον $\mathcal{B}$ το ιδιωτικό κλειδί χρήστη ταυτότητας $ID = \langle \kappa_1 \cdots \kappa_l \rangle$, ο $\mathcal{B}$ ζητά από τον προκαλούντα υπογραφή πρώτου επιπέδου για μήνυμα ID και λαμβάνει $\hat{K}_{ID} = (\hat{K}_1, \hat{K}_2)$. Έπειτα επιλέγει τυχαίο $r \in \mathbb{Z}_q$ και αποστέλλει ως απάντηση στον $\mathcal{A}$ το καλώς ορισμένο κλειδί

$$K_{ID} = (K_1 = \hat{K}_1 \cdot f^{\beta} \cdot (\gamma' \prod_{i=1}^{l} \gamma_i^{\kappa_i})^r, \quad K_2 = \hat{K}_2 \cdot f^{-r}, \quad K_3 = h^{-r}).$$

Εάν ο $\mathcal{A}$ ζητήσει από τον $\mathcal{B}$ υπογραφή για μήνυμα $M = \langle \mu_1 \cdots \mu_m \rangle$ από το χρήστη $ID = \langle \kappa_1 \ldots \kappa_l \rangle$, τότε αυτός επιλέγει τυχαία $t_1, \ldots, t_l \in \mathbb{Z}_n$, υπολογίζει τα $t = \sum_{i=1}^{l} t_i, \tilde{c}_i = u_i^{\kappa_i} h^{t_i}, \tilde{\pi}_i = (u_i^{2\kappa_i - 1} h^{t_i})^{t_i}$ και ζητά από τον προκαλούντα υπογραφή δευτέρου επιπέδου για μήνυμα $ID||M$ λαμβάνοντας $\hat{\sigma} = (\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3)$. Στη συνέχεια επιλέγει τυχαία $r_1, r_2 \in \mathbb{Z}_q$, δημιουργεί τις

$$\tilde{\sigma}_1 = \hat{\sigma}_1 \cdot f^{\beta} \cdot (\gamma' \prod_{i=1}^{l} \gamma_i^{\kappa_i})^{r_1} \cdot (\delta' \prod_{j=1}^{m} \delta_j^{\mu_j})^{r_2} \cdot h^{r_1 t}, \quad \tilde{\sigma}_2 = \hat{\sigma}_2 \cdot f^{-r_1}, \quad \tilde{\sigma}_3 = \hat{\sigma}_3 \cdot f^{-r_2},$$

και αποστέλλει στον $\mathcal{A}$ την υπογραφή $\tilde{\sigma} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \tilde{\sigma}_3, \tilde{c}_1, \ldots, \tilde{c}_l, \tilde{\pi}_1, \ldots, \tilde{\pi}_l)$.

Ο $\mathcal{A}$ επιστρέφει πλαστογραφημένη υπογραφή $\sigma^* = (\sigma_1, \sigma_2, \sigma_3, c_1, \ldots, c_l, \pi_1, \ldots, \pi_l)$ σε μήνυμα $M^* = \langle \mu_1' \cdots \mu_m' \rangle$. Ο $\mathcal{B}$ ελέγχει πρωτίστως την εγκυρότητα της σ, και εάν αυτό συμβαίνει προχωρά στην ανίχνευση της ταυτότητας $ID' = \langle \kappa_1' \cdots \kappa_l' \rangle$, σύμφωνα με την (4.1). Εάν τα $ID^*, \langle ID^*, M^* \rangle$ δεν είχαν τεθεί ως ερωτήματα εξαγωγής κλειδιού και υπογραφής αντίστοιχα, τότε ο $\mathcal{A}$ κερδίζει το παίγνιο ανιχνευσιμότητας,

οπότε ο $\mathcal{B}$ παράγει πλαστογραφημένη υπογραφή ως εξής: από την ορθότητα των NIZK αποδείξεων c_i, π_i ισχύει ότι είτε $c_i \in \mathbb{G}_q$ ή $c_i u_i^{-1} \in \mathbb{G}_q$. Επομένως, για κάποιο $r'_i \in \mathbb{Z}_q$ ισχύει ότι $c_i = u_i^{\kappa'_i} f^{r'_i}$ και άρα για κάποιο $r' \in \mathbb{Z}_q$

$$c = u' \prod_{i=1}^{l} c_i = (\hat{u} \prod_{i=1}^{l} \hat{u}_i^{\kappa'_i}) \cdot f^{r'}.$$

Έστω $\lambda \in \mathbb{Z}_n : \lambda \equiv 0 \bmod (q) \wedge \lambda \equiv 1 \bmod (p)$. Τότε

$$e(\sigma_1^\lambda, g) \cdot e(\sigma_2^\lambda, \hat{u} \prod_{i=1}^{l} \hat{u}_i^{\kappa_i}) \cdot e(\sigma_3, \hat{v} \prod_{j=1}^{m} \hat{v}_j^{\mu'_j}) = A^\lambda = e(\hat{g}, \hat{g})^{\alpha\lambda} \cdot e(f, f)^{\beta\alpha} = e(\hat{g}, \hat{g})^\alpha = \hat{A},$$

δηλαδή η $\sigma^* = (\sigma_1^\lambda, \sigma_2^\lambda, \sigma_3^\lambda)$ είναι μία έγκυρη πλαστογραφημένη υπογραφή του $ID^* || M^*$ στο **HiSS**.

⊣

Το σχήμα ομαδικών υπογραφών BW06 επιτρέπει επεκτάσεις που αφορούν διαδικάσιες επαλήθευσης στίβας, ανάκλησης, εξουσιοδότησης, υπογραφής μηνυμάτων μήκους $> m$ καθώς και εκούσιας μερικής αποκάλυψης της ταυτότητας ενός μέλους. Αναφέρουμε τέλος πως η βασική διαφορά του σχήματος BW06 με το BW07 είναι ότι στο τελευταίο η ταυτότητα του μέλους αποκρύπτεται, ολόκληρη και όχι ανά bit, σε μία NIZK απόδειξη. Έτσι επιτυγχάνονται υπογραφές σταθερού μεγέθους ανεξαρτητα του μήκους της ταυτότητας του υπογράφοντος. Η ασφάλεια του σχήματος BW07 στηρίζεται στις υποθέσεις CDH, SDP και της δυσκολίας του παρακάτω καινούριου προβλήματος, που αποδεικνύεται ευκολότερο του q-SDH.

Κρυφό Πρόβλημα q-SDH$(\mathbb{G}_p)$ (*Hidden q-SDH* - q-HSDH$(\mathbb{G}_p)$): δεδομένων γεννητόρων $g, h, g^\omega \in \mathbb{G}_p$ και $q-1$ διαφορετικών τριάδων $(g^{1/(\omega+c_i)}, g^{c_i}, h^{c_i})$, όπου $c_i \in \mathbb{Z}_p$ να υπολογιστεί τριάδα $(g^{1/(\omega+c)}, g^c, h^c)$, διάφορη των προηγούμενων.

4.4 Οι ομαδικές υπογραφές του Groth

Μία από τις πρώτες άμεσες εφαρμογές του GSPS ήταν το σχήμα ομαδικών υπογραφών του J.Groth [Gro07] στο μοντέλο BSZ05, βελτιώνοντας έτσι κατά πολύ το μήκος των υπογραφών Gro06 που είχε παρουσιάσει νωρίτερα. Οι υπογραφές Gro07 έχουν μέγεθος $\approx$ 2kB για ασφάλεια 128-bit, το οποίο είναι μεν μεγάλο σε σχέση με αυτά των [BBS04], [ACHdM05], [BW07], αλλά και αρκετά λογικό συγκριτικά με τη θεωρητική ασφάλεια που παρέχεται.

Για την πλήρη μελέτη του σχήματος Gro07 είναι απαραίτητα τα ακόλουθα εργαλεία και υποθέσεις:

- Σχήμα υπογραφών *μίας χρήσης* (*ome-time signatures*) **OTS** = ($\text{Setup}_{\text{OTS}}$, Sign_{OTS}, $\text{Verify}_{\text{OTS}}$) με ασφάλεια SEUF-WCMA, όπως το weak-BB (βλ. §2.8).

- Γεννήτρια $\mathcal{H}$ οικογένειας συναρτήσεων hash $H : \{0,1\}^* \longrightarrow \{0,1\}^{l(k)}$ με δυσκολία εύρεσης συγκρούσεων, όπου $2^{l(k)} < p$.

- Το σχήμα κρυπτογράφησης *με ετικέτες* (*tag-based encryption*) του [Kil06] :

  Setup(1^k)**:** $(p, \mathbb{G}, \mathbb{G}_T, e, g)$ όπου e Τύπου 1 και $\mathbb{G}, \mathbb{G}_T$ τάξης p, p πρώτος και $\langle g \rangle = \mathbb{G}$. Το δημόσιο κλειδί pk συνίσταται από τα τυχαία $(F, H, K, L) \in \mathbb{G}^4$, ενώ το ιδιωτικό κλειδί είναι το $sk = (\phi, \eta)$ ώστε $F = g^{\phi}, H = g^{\eta}$.

  Encrypt(pk, M, t)**:** επιλέγονται τυχαία $r, s \in \mathbb{Z}_p$ και υπολογίζεται το κρυπτοκείμενο

  $$C = (\Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5) = (F^r, H^s, g^{r+s} \cdot M, (g^t \cdot K)^r, (g^t \cdot L)^s).$$

  Decrypt(sk, C, t)**:** η ανάκτηση του μηνύματος M γίνεται υπολογίζοντας

  $$M = \Psi_3 \cdot \Psi_1^{-\phi} \cdot \Psi_2^{-\eta}.$$

  Σε ένα σχήμα κρυπτογράφησης με ετικέτες η κρυπτογράφηση και η αποκρυπτογράφηση πραγματοποιούνται με τη χρήση μίας ετικέτας t. Στο Kil06 η εγκυρότητα ενός κρυπτοκειμένου C ελέγχεται δημόσια μέσω της διαδικασίας

  $$\text{ValidCiphertext}(pk, t, C) := e(F, \Psi_4) \stackrel{?}{=} e(\Psi_1, g^t \cdot K) \wedge e(H, \Psi_5) \stackrel{?}{=} e(\Psi_2, g^t \cdot L).$$

  Για τις ανάγκες του Gro07 αρκεί να γνωρίζουμε ότι το ασθενέστερο επίπεδο ασφάλειας του Kil06, όπου ο αντίπαλος οφείλει να επιλέξει εκ των προτέρων την τιμή της ετικέτας που θα προκληθεί, η *ασθενής CCA-ασφάλεια υπό επιλεγμένη ετικέτα* (*selective-tag weakly CCA-security*) επιτυγχάνεται με την υπόθεση DLin [Kil06 Theorem 2].

- Το σχήμα *πιστοποιημένων υπογραφών* (certified signatures) **CertDS**:

  Setup(1^k)**:** για γεννήτρια $\mathcal{G}$ έχουμε $gk = (p, \mathbb{G}, \mathbb{G}_T, e, g) \leftarrow \mathcal{G}(1^k)$.

  CertKey(gk)**:** $f, h, z \stackrel{\$}{\leftarrow} \mathbb{G}; T \leftarrow e(f, z); (ak, ck) := ((gk, f, h, T), (ak, z))$.

  $\langle$**User**(gk, ak), **Issuer**$(gk, ck)\rangle$**:** $(x, v) \leftarrow \langle User, Issuer\rangle(gk); r \stackrel{\$}{\leftarrow} \mathbb{Z}_p$.

  Έξοδος χρήστη: $(vk = v, sk = x, cert = (a, b) = (f^{-r}, (v \cdot h)^r \cdot z))$.

  Έξοδος διανομέα: $(vk, cert)$.

  Sign(sk, M)**:** εάν $sk \neq -M$ τότε $\sigma := g^{\frac{1}{sk+M}}$ αλλιώς $\perp$.

  Verify$(gk, ak, vk, cert, M, \sigma)$**:** επίστρεψε 1 ανν

  $$e(a, v \cdot h) \cdot e(f, b) = T \wedge e(\sigma, v \cdot g^M) = e(g, g).$$

Σε ένα σχήμα πιστοποιημένων υπογραφών, κάθε υπογραφή συνοδεύεται και από μία βοηθητική πληροφορία για τη γνησιότητα του υπογράφοντος, $cert$, που καλείται πιστοποιητικό. Η διαδικασία επαλήθευσης της γνησιότητας του πιστοποιητικού γίνεται ανεξάρτητα από την επαλήθευση της εγκυρότητας της υπογραφής. Για αυτό το λόγο το σχήμα προβλέπει τη δημιουργία δημόσιου κλειδιού επαλήθευσης πιστοποιητικών ak και ιδιωτικού κλειδιού πιστοποίησης για το διανομέα ck. Τα κλειδιά και το πιστοποιητικό κάθε χρήστη δημιουργούνται μέσω ενός διαλογικού πρωτοκόλλου $\langle User, Issuer\rangle$, όπου οι απόψεις και των δύο πλευρών μπορούν να προσομοιωθούν [Gro07 §4.1].

Ένα σχήμα πιστοποιημένων υπογραφών είναι *ασφαλές*

1. ένας αντίπαλος $\mathcal{A}$ που εκτελεί τους υπολογισμούς

$$(St, ak) \leftarrow \mathcal{A}; (vk, sk, cert) \leftarrow \langle User(gk, ak), \mathcal{A}(St)\rangle$$

   και θέτει ερωτήματα υπογραφής M_i δεν μπορεί να εξάγει έγκυρη τριάδα $(cert', M, \sigma)$ για $M \neq M_i$ (υπαρξιακή μη πλαστογράφηση) και

2. ένας αντίπαλος, ο οποίος μπορεί προσαρμοστικά να εκκινεί διαδικασίες παραγωγής νέων κλειδιών παίζοντας το ρόλο του χρήστη, δεν μπορεί τελικά να παράγει κλειδί επαλήθευσης vk που δεν δημιουργήθηκε από πρότερο διάλογό του με το διανομέα και έγκυρη τριάδα $(cert, M, \sigma)$, με μη αμελητέα πιθανότητα (*unfakeability*).

Το **CertDS** αποδεικνύεται EUF-WCMA ασφαλές υπό την υπόθεση q-SDH και τη νέα υποθέση q-U που ορίζεται παρακάτω [Gro07 Theorem 2].

- Η υπόθεση q-U ορίζεται ειδικά για την ασφάλεια του **CertDS**. Για γεννήτρια παραμέτρων $\mathcal{G}$, πολυώνυμο q και κάθε αντίπαλο $\mathcal{A}_k$ ζητάμε η πιθανότητα

$$\begin{aligned}&\mathbf{Pr}[(p, \mathbb{G}, \mathbb{G}_T, e, g) \leftarrow \mathcal{G}(1^k);\ x_1, r_1, \ldots, x_{q(k)}, r_{q(k)} \leftarrow \mathbb{Z}_p\\ &\quad f, h, z \xleftarrow{\$} \mathbb{G};\ T \leftarrow e(f, z);\ a_i \leftarrow f^{-r_i};\ b_i \leftarrow h^{r_i} \cdot g^{x_i r_i} \cdot z;\\ &\quad (V, A, B, M, S) \leftarrow \mathcal{A}(p, \mathbb{G}, \mathbb{G}_T, e, g, x_1, r_1, a_1, b_1 \ldots, x_{q(k)}, r_{q(k)}, a_{q(k)}, b_{q(k)}) :\\ &\quad V \notin \{g^{x_1}, \ldots, g^{x_{q(k)}}\} \wedge e(A, h \cdot V)e(f, B) = T \wedge e(S, V \cdot g^M) = e(g, g)]\end{aligned}$$

  να είναι αμελητέα. Η υπόθεση q-U αποδεικνύεται ότι ισχύει για generic αλγορίθμους [Gro07 Theorem 1].

- Σύστημα απόδειξης Groth-Sahai $(\mathcal{K}, \mathcal{P}, \mathcal{V}, \mathcal{X})$, όπου ο $\mathcal{K}$ με είσοδο $(p, \mathbb{G}, \mathbb{G}_T, e, g)$ παράγει $CRS = (F, H, U, V, W, U', V', W') \in \mathbb{G}^8$ και κλειδί xk, και ο $\mathcal{X}$ είναι εξαγωγέας γνώσης των μαρτύρων $x_1, \ldots, x_n \in \mathbb{G}$ για την απόδειξη που παράγει ο $\mathcal{P}$.

Ένα στοιχείο $x \in \mathbb{G}$ δεσμεύεται στο $(c_1, c_2, c_3) = (F^r \cdot U^t, H^s \cdot V^t, g^{r+s} \cdot W^t \cdot x)$ για τυχαία $r, s, t \in \mathbb{Z}_p$. Ο $\mathcal{K}$ παράγει $U = F^R, V = H^S, W = g^{R+S}$ και $xk = (\phi, \eta)$ ώστε $F = g^\phi, H = g^\eta$, επομένως έχουμε $x = c_3 \cdot c_1^{-\phi} \cdot c_2^{-\eta}$. Σε ένα προσομοιωμένο CRS επιλέγονται $U = F^R, V = H^S, W = g^T$, όπου $T \neq R + S$.

Μία μεταβλητή $\delta \in \mathbb{Z}_p$ δεσμεύεται στο $(d_1, d_2, d_3) = (F^r \cdot (U')^\delta, H^s \cdot (V')^\delta, g^{r+s} \cdot (W')^\delta)$ για τυχαία $r, s \in \mathbb{Z}_p$. Ο $\mathcal{K}$ παράγει $U' = F^R, V' = H^S, W' = g^T$, όπου $T \neq R + S$. Σε ένα προσομοιωμένο CRS επιλέγονται $U' = F^R, V' = H^S, W' = g^{R+S}$ και trapdoor πληροφορία $tk = (R, S)$ ώστε ο προσομοιωτής να μπορεί να «ανοίξει» μία δέσμευση (F^r, H^s, g^{r+s}) στο 0, σε οποιαδήποτε τιμή δ ως $(F^{r-R\delta} \cdot (U')^\delta, H^{s-S\delta} \cdot (V')^\delta, g^{r+s-(R+S)\delta} \cdot (W')^\delta)$.

Τα προσομοιωμένα CRS είναι μη διακρίσιμα από τα πραγματικά υπό την υπόθεση DLin. Αν ξαναγράψουμε τις δεσμεύσεις, θεωρώντας για ευκολία σύγκρισης την $\mathbb{G}$ προσθετική έχουμε ότι

$$c = (\mathcal{O}, \mathcal{O}, x) + [r](F, \mathcal{O}, g) + [s](\mathcal{O}, H, g) + [t](U, V, W)$$
$$d = [\delta](U', V', W') + [r](F, \mathcal{O}, g) + [s](\mathcal{O}, H, g),$$

παρατηρούμε ότι πρόκειται για τις ρυθμίσεις του στιγμιότυπου DLin. Επομένως οι αποδείξεις του Gro07 παράγονται λαμβάνοντας ως συνήθως $\iota(Z) = (\mathcal{O}, \mathcal{O}, Z)$ και $\iota'(z) = [z](U', V', W')$, για $Z \in \mathbb{G}$ και $z \in \mathbb{Z}_p$.

Με τη βοήθεια των παραπάνω κατασκευάζουμε το σχήμα ομαδικών υπογραφών Gro07 από τους εξής αλγόριθμους:

GKey(1^k)**:** $gk \leftarrow \mathcal{G}(1^k)$; Hash $\leftarrow \mathcal{H}(1^k)$; $((f, h, T), z) \leftarrow$ CertKey(gk);
$(CRS, xk) \leftarrow \mathcal{K}(gk)$; $K, L \xleftarrow{\$} \mathbb{G}$; $(F, H, \cdots) \leftarrow Parse(CRS)$;
$pk := (F, H, K, L)$; $(gpk, ik, ok) := ((gk, H, f, h, T, CRS, pk), z, xk)$.

Join – Issue(χρήστης $i : gpk$, διανομέας $: gpk, ik$)**:**
$((v_i, x_i, a_i, b_i), (v_i, a_i, b_i)) \leftarrow \langle User, Issuer \rangle$
Χρήστης: εάν $e(a_i, hv_i)e(f, b_i) = T$ τίθενται $reg[i] := v_i; gsk[i] := (x_i, a_i, b_i)$.

GSign$(gpk, gsk[i], M)$**:** η υπογραφή μηνύματος M από το μέλος i παράγεται εξάγοντας αρχικά $(vk_{\text{ots}}, sk_{\text{ots}}) \leftarrow \text{Setup}_{\text{OTS}}(1^k)$ και στη συνέχεια

Ενόσω$(\text{Hash}(vk_{\text{ots}}) \neq x_i)$
1. $\rho \xleftarrow{\$} \mathbb{Z}_n$; $a = a_i \cdot f^{-r}$; $b = b_i \cdot (h \cdot v_i)^\rho$.
2. $\sigma^{1/(x_i + \text{Hash}(vk_{\text{ots}}))}$.
3. $\pi \leftarrow \mathcal{P}_{\text{NIWI}}(gpk, a, H(vk_{\text{ots}}), (b, v_i, \sigma))$.
4. $y \leftarrow \text{Encrypt}(pk, \text{Hash}(vk_{\text{ots}}), \sigma)$.
5. $\psi \leftarrow \mathcal{P}_{\text{NIZK}}(CRS, (gpk, y, \pi), (r, s, t))$.

6. $\sigma_{\text{ots}} \leftarrow \text{Sign}_{\text{OTS}}(sk_{\text{ots}}, vk_{\text{ots}}, M, a, \pi, y, \psi)$.
Τελικώς επιστρέφεται η υπογραφή $\Sigma := (vk_{ots}, a, \pi, y, \psi, \sigma_{\text{ots}})$.

GVer(gpk, M, Σ)**:** η εγκυρότητα της Σ επαληθέυεται ανν ικανοποιούνται οι

$$\text{Verify}_{\text{OTS}}((vk_{\text{ots}}, M, a, \pi, y, \psi), \sigma_{\text{ots}}) = 1, \text{ValidCiphertext}(pk, \text{Hash}(vk_{\text{ots}}), y) = 1,$$
$$\mathcal{V}_{\text{NIWI}}(CRS, (gpk, a, \text{Hash}(vk_{\text{ots}})), \pi) = 1, \mathcal{V}_{\text{NIZK}}(CRS, (gpk, \pi, y), \psi) = 1.$$

Open(gpk, ok, M, Σ)**:** $(b, v, \sigma) \leftarrow \mathcal{X}(xk, CRS, (gpk, a, \text{Hash}(vk_{\text{ots}})), \pi)$.
Εάν υπάρχει i ώστε $v = v_i$ επίστρεψε (i, σ) αλλιώς επίστρεψε $(0, \sigma)$.

Judge$(gpk, i, reg[i], M, \Sigma, \tau)$**:** η απόδειξη σ γίνεται αποδεκτή ανν

$$i \neq 0 \wedge e(\tau, y_i g^{\text{Hash}(vk_{ds})}) = e(g, g).$$

Σε κάθε εγγραφή νέου μέλους, εκτελείται το διαλογικό πρωτόκολλο του σχήματος **CertDS** και δημιουργούνται κλειδί επαλήθευσης v_i και ιδιωτικό κλειδί x_i για υπογραφές weak-BB, και το πιστοποιητικό (a_i, b_i). Για τη δημιουργία μίας ομαδικής υπογραφής παράγεται έγκυρο ζεύγος κλειδιών $(sk_{\text{ots}}, vk_{\text{ots}})$ για το **OTS**, όπου τα M, vk_{ots} υπογράφονται μέσω των sk_{ds}, x_i αντίστοιχα. Η CPA-πλήρης ανωνυμία επιτυγχάνεται με τη χρήση NIWI απόδειξης γνώσης μίας πιστοποιημένης υπογραφής σ για το vk_{ds}, ενώ για την πλήρη ανωνυμία επιστρατεύεται το κρυπτοσύστημα Kil06, κρυπτογραφώντας την σ με το $\text{Hash}(vk_{\text{ots}})$ ως ετικέτα και παρέχεται NIZK απόδειξη ότι η κρυπτογραφημένη υπογραφή είναι η ίδια που χρησιμοποιήθηκε στην NIWI απόδειξη.

Η NIWI απόδειξη, δηλώνει ότι υπάρχει πιστοποιημένη υπογραφή (a, b, v, σ) για το vk_{ots}, μέσω των εξισώσεων γινομένου-ζεύγματος

$$e(a, h \cdot y) \cdot e(f, b) = T, \quad e(\sigma, v \cdot g^{\text{Hash}(vk_{\text{ots}})}) = e(g, g). \tag{4.2}$$

με μεταβλητές (b, v, σ). Οι τρεις αντίστοιχες δεσμεύσεις και οι δύο αποδείξεις που παράγονται αποτελούνται συνολικά από $3{\cdot}3{+}2{\cdot}9{=}27$ στοιχεία της $\mathbb{G}$. Το a θεωρείται σταθερά, αφού μπορούμε να επιλέξουμε το ρ ώστε το a να μην αποκαλύπτει την ταυτότητα του μέλους.

Στην NIZK απόδειξη, επιχειρούμε να δείξουμε ότι ένα κρυπτοκείμενο της μορφής

$$C = (\Psi_1, \ldots, \Psi_5) = (F^{r_y}, H^{s_y}, g^{r_y+s_y}\sigma, (g^{\text{Hash}(vk_{\text{ots}})} \cdot K)^{r_y}, (g^{\text{Hash}(vk_{\text{ots}})} \cdot L)^{s_y})$$

και μία δέσμευση της μορφής

$$c = (c_1, c_2, c_3) = (F^{r_c} \cdot U^t, H^{s_c} \cdot V^t, g^{r_c+s_c} \cdot W^t \cdot \sigma)$$

αντιστοιχούν στην ίδια τιμή. Θέτοντας $r = r_c - r_y$ και $s = s_c - s_y$ αρκεί να δείξουμε ότι ικανοποιείται η τετράδα εξισώσεων με μεταβλητές ϕ, r, s, t

$$\phi = 1, \quad (c_1^{-1} \cdot \Psi_1)^{\phi} \cdot F^r \cdot U^t = 1, \quad (c_2^{-1} \cdot \Psi_2)^{\phi} \cdot H^s \cdot V^t = 1, \quad (c_3^{-1} \cdot \Psi_3)^{\phi} \cdot g^{r+s} \cdot W^t = 1.$$

Παρατηρούμε ότι ένας προσομοιωτής εξάγει τετριμμένο μάρτυρα $\phi = 1$ για την πρώτη εξίσωση και $\phi = r = s = t = 0$ για τις τρεις τελευταίες εξισώσεις βαθμωτού πολλαπλασιασμού (εδώ αντίστοιχα υψώσεων σε δύναμη). Στη συνέχεια κατασκευάζει απόδειξη αποτελούμενη από τέσσερις δεσμεύσεις για τις ϕ, r, s, t, όπου για τη ϕ μπορούμε απλώς να ορίσουμε ως δέσμευση την τριάδα (U', V', W'), ελέγχοντας έτσι εύκολα την ικανοποιησιμότητα της πρώτης εξίσωσης. Καθώς για το στιγμιότυπο DLin χρειάζονται τρία στοιχεία της $\mathbb{G}$ για κάθε μία από τις άλλες τρεις δεσμεύσεις και κάθε εξίσωση απαιτεί δύο στοιχεία, το συνολικό κόστος είναι τελικά 15 στοιχεία της $\mathbb{G}$.

Το συνολικό μέγεθος μίας ομαδικής υπογραφής $\Sigma = (vk_{ds}, a, \pi, y, \psi, \sigma_{ds})$ είναι 1+1+27+5+15+1=50 στοιχεία της $\mathbb{G}$. Η πληρότητα του Gr07 είναι άμεση συνέπεια της πληρότητας των σχημάτων και των αποδείξεων που περιλαμβάνει. Η ασφάλεια του Gr07 στο μοντέλο BSZ05 αποδεικνύεται στα τρία επόμενα θεωρήματα.

Θεώρημα 4.4.1. *Εάν ισχύει η υπόθεση DLin, η Hash έχει αμελητέα πιθανότητα εύρεσης συγκρούσεων και το* **OTS** *έχει ασφάλεια EUF-WCMA, τότε το Gr07 έχει ανωνυμία.*

Απόδειξη. Λόγω της ασφάλειας EUF-WCMA του **OTS**, υποθέτουμε ότι το v_{ots} δεν χρησιμοποιείται σε ερωτήματα $\text{Open}(\cdot, \cdot)$. Λόγω της αμελητέας πιθανότητας εύρεσης συγκρούσεων της Hash υποθέτουμε επίσης ότι το $\text{Hash}(vk_{\text{ots}})$ δε συμπίπτει με καμία υπογραφή που τέθηκε ως ερώτημα στο $\text{Open}(\cdot, \cdot)$.

Αλλάζουμε τον τρόπο παραγωγής δημόσιου κλειδιού στο Kil06 θέτοντας $K = g^{\kappa}$, $L = g^{\lambda}$ και αποθηκεύοντας τα κ, λ. Σε περίπτωση που το μαντείο $\text{Open}(\cdot, \cdot)$ δεχθεί έγκυρη ομαδική υπογραφή, μπορούμε να αποκρυπτογραφήσουμε το C μέσω των κ, λ, λαμβάνοντας υπογραφή σ. Από τον έλεγχο επαλήθευσης κρυπτοκειμένων του Kil06 και την τέλεια ορθότητα της NIZK απόδειξης ψ προκύπτει ότι είναι η ίδια υπογραφή σ που επιστρέφει ο εξαγωγέας γνώσης της NIWI απόδειξης π. Στη συνέχεια ελέγχεται εάν στο αρχείο εγγραφών υπάρχει i ώστε $e(\sigma, v_i \cdot g^{\text{Hash}(vk_{\text{ots}})}) = e(g, g)$, οπότε επιστρέφουμε (i, σ) αλλιώς επιστρέφουμε $(0, \sigma)$. Η μοναδικότητα της λύσης v_i της πρότερης εξίσωσης εγγυάται την ταύτισή της με την v που επιστρέφει ο εξαγωγέας γνώσης. Η τέλεια ορθότητα της π και η ψ εγγυώνται ότι με τα παραπάνω βήματα μπορούμε να τροποποιήσουμε το μαντείο $\text{Open}(\cdot, \cdot)$ ώστε να μην χρειάζεται το μυστικό κλειδί xk του ανιχνευτή. Επομένως μπορούμε να προσομοιώσουμε το CRS επιτυγχάνοντας τέλεια WI και ZK. Η τέλεια WI συνεπάγεται ότι η π δεν αποκαλύπτει καμία πληροφορία για το ποιας ταυτότητας ιδιωτικό κλειδί $gsk[i_b]$ επιλέχθηκε κατά την δημιουργία της υπογραφής πρόκλησης.

Θεωρούμε τώρα αντίπαλο $\mathcal{A}$ για το παίγνιο ανωνυμίας και κατασκευάζουμε αντίπαλο $\mathcal{B}$ για το Kil06. Ο $\mathcal{B}$ λαμβάνει δημόσιο κλειδί $pk = (F, H, K, L)$ και με τη βοήθεια των F, H, gk προσομοιώνει CRS τέλειας WI αλλά και μηδενικής γνώσης. Ως

εκ τούτου παράγει καλώς κλειδί gpk και μπορεί να προσομοιώσει τα μαντεία AddU, SndToU, SndToI, CrptU, USK, Wreg, Open που αντιστοιχούν στις δυνατότητες του $\mathcal{A}$[1].

Ο $\mathcal{B}$ επιλέγει ζεύγος κλειδιών $(vk_{\text{ots}}, sk_{\text{ots}})$ για το **OTS**, και δηλώνει στον προκαλούντα ως ετικέτα το $\text{Hash}(vk_{\text{ots}})$. Εκτελεί το παίγνιο ανωνυμίας όπως περιγράφτηκε πιο πάνω και τελικά λαμβάνει από τον $\mathcal{A}$ ταυτότητες i_0, i_1 και μήνυμα M. Υπολογίζει υπογραφές $\sigma_{i_0}, \sigma_{i_1}$ του μηνύματος $\text{Hash}(vk_{\text{ots}})$ για τους i_0, i_1 αντίστοιχα και τις αποστέλλει στον προκαλούντα ως κείμενα πρόκλησης, λαμβάνοντας κρυπτοκείμενο C. Με βάση το C και τις τέλειες WI και ZK αποδείξεις που εξασφαλίζει το προσομοιωμένο CRS παράγει ομαδική υπογραφή Σ, την οποία αποστέλλει ως πρόκληση στον $\mathcal{A}$. Εάν ο $\mathcal{A}$ διακρίνει την ταυτότητα του υπογράφοντος της Σ, τότε από την απάντηση του $\mathcal{A}$ ο $\mathcal{B}$ διακρίνει το κείμενο που αντιστοιχεί στο C, κάτι που είναι αδύνατο υποθέτοντας την DLin.

⊣

Θεώρημα 4.4.2. *Εάν ισχύει η υπόθεση q-SDH, η Hash έχει αμελητέα πιθανότητα εύρεσης συγκρούσεων και το* **OTS** *έχει ασφάλεια EUF-WCMA, τότε το Gro07 έχει αντίσταση σε σκευωρία.*

Απόδειξη. Από την SEUF-WCMA ασφάλεια του **OTS** έπεται ότι ένας αντίπαλος $\mathcal{A}$ για το παίγνιο σκευωρίας έχει αμελητέα πιθανότητα να παράγει ζεύγος (M, Σ) με vk_{ots} που έχει ήδη χρησιμοποιηθεί από το μαντείο GSign. Εξάλλου η δυσκολία εύρεσης συγκρούσεων της Hash εξασφαλίζει ότι μπορούμε να παραβλέψουμε την περίπτωση η τιμή $\text{Hash}(vk_{\text{ots}})$ να συμπίπτει με κάποιο vk'_{ots} που έχει χρησιμοποιηθεί από το μαντείο GSign. Επομένως η σκευωρία εναντίον κάποιου χρήστη i ανάγεται στην εύρεση έγκυρης πιστοποιημένης υπογραφής σ για τιμή $\text{Hash}(vk_{\text{ots}})$ που ο i δεν έχει προηγουμένως υπογράψει, εμπίπτοντας έτσι στα πλαίσια της ασφάλειας EUF-WCMA.

Έστω $q(k)$ το πλήθος των εγγεγραμμένων χρηστών που δημιουργούνται από ερωτήματα SndToU του $\mathcal{A}$. Η πιθανότητα να μαντέψουμε πριν την εκκίνηση του παιγνίου σκευωρίας το μέλος i που ο $\mathcal{A}$ διαλέγει να παγιδεύσει είναι $1/q(k)$. Καθώς όμως πρωτόκολλο παραγωγής κλειδιών του **CertDS** μπορεί να προσομοιωθεί με αμελητέα πιθανότητα σφάλματος, η πλαστογράφηση μίας πιστοποιημένης υπογραφής εκ μέρους του i ανάγεται στην πλαστογράφηση υπογραφής weak-BB $\sigma = g^{1/(x_i + \text{Hash}(vk_{ds}))}$, η οποία είναι αμελητέα λόγω της (S)EUF-WCMA ασφάλειας των εν λόγω υπογραφών.

⊣

[1] Στο [Gro07], οι λειτουργίες των AddU, SndToU, SndToI, CrptU, USK, Wreg καλύπτονται από αυτές των JoinCorrupt, JoinExposedUser.

Θεώρημα 4.4.3. *Εάν ισχύει η q-U, τότε το Gr07 έχει ανιχνευσιμότητα.*

Απόδειξη. Από την ορθότητα της π, μία έγκυρη ομαδική υπογραφή Σ συνεπάγεται την ύπαρξη έγκυρης πιστοποιημένης υπογραφής σ του $\mathrm{Hash}(vk_{\mathrm{ots}})$, την οποία εξάγουμε με τη βοήθεια του κλειδιού του ανιχνευτή xk. Από την επαλήθευση γνησιότητας του **CertDS**, η σ αποδίδεται σε κάποιο χρήστη με $reg[i] = v_i$. Η τέλεια ορθότητα της π εξασφαλίζει ότι η εξαγόμενη σ είναι όντως έγκυρη υπογραφή με κλειδί επαλήθευσης v_i. Συνεπώς ένας αντίπαλος δεν μπορεί να παράγει έγκυρες υπογραφές, η οποίες δεν γίνονται αποδεκτές από τον Judge.

⊣

4.5 Οι ομαδικές υπογραφές των Liang-Cao-Shao-Lin

Ακολουθώντας τη μεθοδολογία των [BW06], [BW07], [Gro07], οι X.Liang κ.ά. [LCSL07] κατασκεύασαν ένα σχήμα ομαδικών υπογραφών με σταθερά μήκη δημόσιων παραμέτρων και υπογραφών, μικρότερα των προαναφερθέντων σχημάτων και απλούστερο υπολογιστικά. Εντούτοις, η ασφάλειά του ακολουθεί τα πρότυπα των σχημάτων Boyen-Waters (CPA-πλήρης ανωνυμία στο μοντέλο BMW03), επομένως μπορεί να θεωρηθεί περισσότερο σαν εξέλιξη των σχημάτων BW06, BW07, αφού ο βασικός λόγος της υπολογιστικής επιβάρυνσης του Gro07 είναι η επίτευξη ασφάλειας στο μοντέλο BSZ05.

Οι LCSL07 χτίζονται πάνω σε σχήμα ιεραρχικών υπογραφών δύο επιπέδων που βασίζεται στις υπογραφές BB. Οι αλγόριθμοι που συνιστούν το σχήμα LCSL07 είναι οι εξής:

Setup(1^k)**:** Δημιουργούνται παράμετροι $(n = pq, \mathbb{G}, \mathbb{G}_T, e, g, u, h)$ όπου g, u γεννήτορες της $\mathbb{G}$ και h γεννήτορας της $\mathbb{G}_q$, και hash συνάρτηση $H : \{0,1\}^m \longrightarrow \mathbb{Z}_n$, όπου m το μήκος μηνυμάτων. Επιλέγεται τυχαίο $z \in \mathbb{Z}_n^*$. Οι δημόσιες παράμετροι, το μυστικό κλειδί και το κλειδί του GM είναι αντίστοιχα

$$params = (g, h, Z = g^z, u) \in \mathbb{G} \times \mathbb{G}_q \times \mathbb{G} \times \mathbb{G}, \quad msk = z, \quad gmsk = q,$$

Join$(params, msk, ID)$**:** Το ιδιωτικό κλειδί μέλους $ID \in \{0,1\}^l$ είναι το

$$K_{ID} = (K_1, K_2) = (s_{ID}, g^{1/(z+s_{ID})}),$$

όπου το s_{ID} είναι προσωπικό επιλέγεται τυχαία στο $\mathbb{Z}_n^*$.

Sign$(params, ID, K_{ID}, M)$**:** πρώτα υπολογίζεται υπογραφή δύο επιπέδων

$$\rho = (\rho_1, \rho_2, \rho_3) = (g^{K_1}, K_2, u^{\frac{1}{K_1 + H(M)}}),$$

η οποία λόγω του αμετάβλητου των ρ_1, ρ_2 δεν παρέχει ανωνυμία στον υπογράφοντα. Για αυτό το λόγο επιλέγονται τυχαία $t_1, t_2, t_3 \in \mathbb{Z}_n$ και υπολογίζονται οι

$$\sigma_1 = \rho_1 h^{t_1},\ \sigma_2 = \rho_2 h^{t_2},\ \sigma_3 = \rho_3 h^{t_3},\ \pi_1 = \rho_2^{t_1}(Z\rho_1)^{t_2} h^{t_1 t_2},\ \pi_2 = \rho_3^{t_1}(g^{H(M)}\rho_1)^{t_3} h^{t_1 t_3}$$

και τελικά εξάγεται η υπογραφή

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \pi_1, \pi_2) \in \mathbb{G}^5.$$

Verify$(params, ID, K_{ID})$**:** Η σ γίνεται αποδεκτή ανν

$$e(\sigma_1 \cdot Z, \sigma_2) \cdot e(g,g)^{-1} \stackrel{?}{=} e(\pi_1, h) \wedge e(\sigma_1 \cdot g^{H(M)}, \sigma_3) \cdot e(g,u)^{-1} \stackrel{?}{=} e(\pi_2, h).$$

Open$(params, gmsk)$**:** Η ανίχνευση του υπογράφοντος της σ γίνεται ελέγχοντας

$$(\sigma_1)^q = (g^{s_{ID}} \cdot h^{t_1})^q \stackrel{?}{=} (g^{s_{ID}})^q \cdot (g^{K_1})^q$$

και εντοπίζοντας την ταυτότητα που αντιστοιχεί στην τιμή $(g^{K_1})^q$ σε μία ιδιωτική λίστα προϋπολογισμένων $(g^{K_1})^q$ όλων των χρηστών.

Η καλή κατασκεύη του K_{ID} επαληθεύεται εύκολα με τον έλεγχο $e(Zg^{K_1}, K_2) \stackrel{?}{=} e(g,g)$. Η υπογραφή αποτελείται από 5 στοιχεία της $\mathbb{G}$, κατά ένα μικρότερη μίας υπογραφής BW07, ενώ η ανίχνευση μιας ταυτότητας είναι γραμμικά εξαρτώμενη από το πλήθος των μελών της ομάδας. Οι δεσμεύσεις $\sigma_1, \sigma_2, \sigma_3$, των ρ_1, ρ_2, ρ_3 υπολογίζονται σύμφωνα με τις ρυθμίσεις του στιγμιότυπου SDP, οπότε οι π_1, π_2 αποτελούν αποδείξεις της επαληθευσιμότητας των εξισώσεων γινομένου ζεύγματος

$$e(\rho_1 Z, \rho_2) = e(g,g), \quad \text{και} \quad e(\rho_1 g^{H(M)}, \rho_3) = e(g,u).$$

Η ασφάλεια του LCSL07 στηρίζεται στις υποθέσεις SDP, q-SDH και στη νέα υπόθεση q-MOMSDH, για την οποία παραπέμπουμε στο ([LCSL07 §2.2]).

4.6 Οι BU-VLR ομαδικές υπογραφές των Libert-Vergnaud

Όπως έχει ήδη αναφερθεί, οι VLR-ομαδικές υπογραφές BS04 χαρακτηρίζονται από τη μη διατήρηση του ασύνδετου των υπογραφών που έχουν δημιουργηθεί από ένα διεγραμμένο μέλος. Τις περισσότερες φορές όμως, όταν ένα μέλος αποχωρεί εκούσια από την ομάδα, πρέπει να διατηρείται η ιδιωτικότητα των κειμένων που έχει ήδη υπογράψει. Για να είναι δυνατή επομένως η χρήση των VLR-ομαδικών υπογραφών σε τέτοιες περιπτώσεις πρέπει να εμπλουτιστούν με μία διαδικασία που εξασφαλίζει το *αναδρομικό ασύνδετο* (*backward unlikability - BU*) των υπογραφών. Οι πρώτες BU-VLR-ομαδικές υπογραφές στην κρυπτογραφία ζευγμάτων χτίστηκαν

πάνω στις υπογραφές BS04 από τους T.Nakanishi και N.Funabiki [NF05] και έκτοτε εμφανίστηκαν διάφορα βελτιωμένα σχήματα στο ROM [ZL06], [NF07], [WL10] . Η πρώτη υλοποίηση στο standard μοντέλο έγινε από τους B.Libert και D.Vergnaud [NF05] με την κατάλληλη προσαρμογή της μεθοδολογίας του [NF05] ώστε να συναντηθούν οι προϋποθέσεις των NIZK αποδείξεων Groth-Sahai.

Σε ένα σχήμα BU-VLR-ομαδικών υπογραφών η γεννήτρια κλειδιών εφοδιάζεται και με μία παράμετρο T που δηλώνει το πλήθος χρονικών περιόδων. Η λίστα τεκμηρίων ανάκλησης grt περιέχει τεκμήρια $grt[i][j]$ για κάθε χρήστη i κατά την περίοδο j και ενημερώνεται από τον GM στην αρχή κάθε περιόδου. Οι αλγόριθμοι υπογραφής και επαλήθευσης λαμβάνουν υπόψη την περίοδο j και άρα η ανίχνευση μίας υπογραφής από τον GM γίνεται με την επαναληπτική εκτέλεση του αλγορίθμου επαλήθευσης αντλώντας τεκμήρια από τη λίστα $\mathrm{RL}_j = \{grt[i][j], \ldots, grt[N][j]\}$, όπου N το πλήθος των μελών της ομάδας.

Η κατασκευή του LV09 στηρίζεται στις ρυθμίσεις του στιγμιότυπου DLin. Θεωρούμε επομένως το συμμετρικό πίνακα

$$F : \mathbb{G}^3 \times \mathbb{G}^3 \longrightarrow \mathbb{G}_T^9, \quad F(\bar{X}, \bar{Y}) = \tilde{F}(\bar{X}, \bar{Y})^{\frac{1}{2}} \cdot \tilde{F}(\bar{Y}, \bar{X})^{\frac{1}{2}},$$

όπου $\tilde{F}$ είναι η συνάρτηση που απεικονίζει το $(\bar{X}, \bar{Y})$ στον 3×3 πίνακα $(e(X_i, Y_j))$. Για κάθε $x \in \mathbb{G}$ έχουμε $\iota(x) = (1, 1, x)$ και για κάθε $z \in \mathbb{Z}$ ορίζουμε ως $\iota_T(z)$ τον 3×3 πίνακα που έχει τιμή z στη θέση (3,3) και 1 αλλού. Θεωρούμε επίσης την απεικόνιση $E : \mathbb{G} \times \mathbb{G}^3 \longrightarrow \mathbb{G}_T^3$ με $E(h, \bar{g}) = (e(h, g_1), e(h, g_2), (e, g_3))$.

Οι αλγόριθμοι που συνιστούν το LV09 είναι οι εξής:

Keygen$(1^k, N, T)$: Επιλέγονται $(p, \mathbb{G}, \mathbb{G}_T, e)$ και τυχαία $g, h_1, \ldots, h_T, u \in \mathbb{G}_p$, $\alpha, \omega \in \mathbb{Z}_p^*$ και $\bar{v} = (v_0, \ldots, v_n) \in \mathbb{G}^{n+1}$, όπου $n \in poly(k)$. Θέτουμε $A = e(g, g)^\alpha$, $\Omega = g^\omega$. Επιλέγονται επίσης $\alpha_1, \alpha_2 \in \mathbb{Z}_p^*$, $\xi_1, \xi_2 \in \mathbb{Z}_p$ και υπολογίζονται τα $g_1 = g^{\alpha_1}, g_2 = g^{\alpha_2}$ και $\bar{g}_1 = (g_1, 1, g), \bar{g}_2 = (1, g_2, g), \bar{g}_3 = \bar{g}_1^{\xi_1} \cdot \bar{g}_2^{\xi_2}$, όπως το CRS στο παράδειγμα DLin. Τέλος, επιλέγεται Hash συνάρτηση $H : \{0,1\}^* \longrightarrow \{0,1\}^n$. Τα κλειδιά ορίζονται ως

$$gpk = (g, h_1, \ldots, h_T, A, \Omega, u, \bar{v}, \bar{g}_1, \bar{g}_2, \bar{g}_3, H), \quad gmsk = (\alpha, \omega, \alpha_1, \alpha_2)$$
$$gsk[i] = (K_1, K_2, K_3) = ((g^\alpha)^{1/(\omega+s_i)}, g^{s_i}, u^{s_i}), \quad grt[i][j] = h_j^{s_i},$$

όπου s_i είναι μη δημόσια τιμή που χαρακτηρίζει το μέλος i (βλ. [BW07]).

Sign$(gpk, gsk[i], j, M)$: Το i υπολογίζει αρχικά $H(j||M) = \langle m_1 \cdots m_n \rangle$ και εκτελεί τα ακόλουθα βήματα:

1. Επίλέγει τυχαία $\delta, r \in \mathbb{Z}_p^*$ και ορίζει τα

$$T_1 = g^\delta, \quad T_2 = e(h_j, K_2)^\delta, \quad F(m) = v_0 \cdot \textstyle\prod_{t=1}^n v_t^{m_t}$$
$$\theta_1 = K_1, \quad \theta_2 = K_2, \quad \theta_3 = K_3 \cdot F(m)^r, \quad \theta_4 = g^r, \quad \theta_5 = h_j^\delta.$$

2. Δεσμεύει τα θ_i επιλέγοντας τυχαία $r_i, s_i, t_i \in \mathbb{Z}_p^*$ στις τιμές

$$\bar{\sigma}_i = (1, 1, \theta_i) \odot \bar{g}_1^{r_i} \odot \bar{g}_2^{s_i} \odot \bar{g}_3^{t_i},$$

όπου $\odot$ ο κατά σημείο πολλαπλασιασμός μεταξύ διανυσμάτων ή πινάκων ίδιων διαστάσεων.

3. Κατασκευάζει NIWI αποδείξεις $\pi_1 = (\bar{\pi}_{1,1}, \bar{\pi}_{1,2}, \bar{\pi}_{1,3})$ και $\pi_2 = (\pi_{2,1}, \pi_{2,2}, \pi_{2,3})$ για την επαληθευσιμότητα των GS εξισώσεων με μεταβλητές $\theta_1, \theta_2, \theta_3, \theta_4$

$$e(\theta_1, \Omega \cdot \theta_2) = A \quad \text{και} \quad e(\theta_3, g) = e(u, \theta_2) \cdot e(F(m), \theta_4).$$

Η π_1 αντιστοιχεί σε εξίσωση γινομένου ζεύγματος και αποτελείται από 3×3 στοιχεία της $\mathbb{G}$, ενώ η π_2 αντιστοιχεί σε ειδική γραμμική εξίσωση 3 στοιχεία.

4. Κατασκευάζει NIZK αποδείξεις για την επαληθευσιμότητα των GS εξισώσεων με μεταβλητές θ_2, θ_5

$$e(\theta_2, \theta_5) = T_2 \quad \text{και} \quad e(g, \theta_5) = e(h_j, T_1).$$

Η απόδειξη της πρώτης εξίσωσης είναι η $\pi_1 = (\bar{\pi}_{3,1}, \bar{\pi}_{3,2}, \bar{\pi}_{3,3})$. Για την δεύτερη εξίσωση εισάγεται τεχνητή μεταβλητή θ_6 (βλ. §3.4) και ζητούνται NIZK αποδείξεις για τις εξισώσεις $e(g, \theta_5) = e(\theta_6, T_1)$ και $\theta_6 = h_j$. Επομένως υπολογίζεται η δέσμευση $\bar{\sigma}_6 = \iota(h_j) \odot \bar{g}_1^{r_6} \odot \bar{g}_2^{s_6} \odot \bar{g}_3^{t_6}$ και οι αποδείξεις $\pi_4 = (\pi_{4,1}, \pi_{4,2}, \pi_{4,3})$, $\pi_5 = (\pi_{5,1}, \pi_{5,2}, \pi_{5,3})$ επαληθευσιμότητας των

$$e(g, \theta_5) = e(\theta_6, T_1) \quad \text{και} \quad e(\theta_6, g) = e(h_j, g).$$

Τελικώς η υπογραφή είναι η $\sigma = (T_1, T_2, \bar{\sigma}_1, \ldots, \bar{\sigma}_6, \pi_1, \ldots, \pi_5)$.

Verify$(j, M, \sigma, gpk, \mathrm{RL}_j)$: η σ γίνεται αποδεκτή ανν

1. Επαληθεύονται οι παρακάτω ισότητες:

   (i). $F(\bar{\sigma}_1, \iota(\Omega) \cdot \bar{\sigma}_2) = \iota_T(A) \odot F(\bar{g}_1, \bar{\pi}_{1,1}) \odot F(\bar{g}_2, \bar{\pi}_{1,2}) \odot F(\bar{g}_3, \bar{\pi}_{1,3})$.

   (ii). $E(g, \bar{\sigma}_3) = E(u, \bar{\sigma}_2) \odot E(F(m), \bar{\sigma}_4) \odot E(\pi_{2,1}, \bar{g}_1) \odot E(\pi_{2,2}, \bar{g}_2) \odot E(\pi_{2,3}, \bar{g}_3)$.

   (iii). $F(\bar{\sigma}_2, \bar{\sigma}_5) = \iota_T(T_2) \odot F(\bar{g}_1, \bar{\pi}_{3,1}) \odot F(\bar{g}_2, \bar{\pi}_{3,2}) \odot F(\bar{g}_3, \bar{\pi}_{3,3})$.

   (iv). $E(T_1, \bar{\sigma}_6) = E(g, \bar{\sigma}_5) \odot E(\pi_{4,1}, \bar{g}_1) \odot E(\pi_{4,2}, \bar{g}_2) \odot E(\pi_{4,3}, \bar{g}_3)$.

   (v). $E(T_1, \bar{\sigma}_6) = E(h_j, \iota(g)) \odot E(\pi_{5,1}, \bar{g}_1) \odot E(\pi_{5,2}, \bar{g}_2) \odot E(\pi_{5,3}, \bar{g}_3)$.

2. Ο υπογράφων δεν έχει ανακληθεί κατά την περίοδο j, δηλαδή:

$$\text{για κάθε } grt[i][j] = h_j^{s_i} \in \mathrm{RL}_j : T_2 \neq e(h_j^{s_i}, T_1).$$

Το LV09, έχει σταθερό μήκος υπογραφών αποτελούμενων από 46 στοιχεία της $\mathbb{G}$ και 1 της $\mathbb{G}_T$. Εντούτοις, είναι επιφορτισμένο με μεγάλο πλήθος υπολογισμών ζεύγματος και ιδιαίτερα κατά την επαλήθευση. Επιπλέον, το μέγεθος του δημόσιου κλειδιού εξαρτάται γραμμικά από το πλήθος των περιόδων T, αν και οι B.Libert και D.Vergnaud πρότεινουν στην ίδια εργασία μια παραλλαγή του αρχικού σχήματος με μήκος δημόσιου κλειδιού ανεξάρτητο του T. Σε γενικές γραμμές πάντως το LV09 υστερεί πρακτικά σε σχέση με σχήματα BU-VLR-ομαδικών υπογραφών στο ROM, τα νεότερα των οποίων επιταχύνουν σημαντικά την επαλήθευση με νέες τεχνικές γρήγορου ελέγχου ανάκλησης [CL10], [BP11].

Το μοντέλο ασφάλειας των BU-VLR-ομαδικών υπογραφών προσαρμόζεται φυσικά στην ιδιότητα αναδρομικού ασυδέτου υπογραφών. Επομένως ορίζονται οι

BU-ανωνυμία: ο αντίπαλος $\mathcal{A}$, χωρίς να διαθέτει τα $\mathrm{grt}, gsk[1 \cdots N]$, εκτελεί προσαρμοστικά πριν και μετά την πρόκληση ερωτήματα υπογραφής, εξαγωγής ιδιωτικού κλειδιού και τεκμηρίων ανάκλησης για χρονικές περιόδους της επιθυμίας του. Διαλέγει να προκληθεί σε ταυτότητες δύο χρηστών που είναι εκείνη την περίοδο ενεργοί.

Ανιχνευσιμότητα: ο $\mathcal{A}$ διαθέτει το grt αλλά όχι το $gsk[1 \cdots N]$ εκτελεί προσαρμοστικά πριν και μετά την πρόκληση ερωτήματα υπογραφής και εξαγωγής ιδιωτικού κλειδιού. Στο τέλος κερδίζει εάν εξάγει $(\sigma, M, j, \mathrm{RL}_j^*)$ ώστε η σ να γίνεται αποδεκτή, η ανίχνευσή της με αναζήτηση στα $grt[i][j], \ldots, grt[N][j]$ είτε να αποτυγχάνει είτε να εντοπίζει χρήστη εκτός του συνόλου ανακληθέντων χρηστών RL_j^* και επιπλέον να μην αποκτάται από ερωτήματα υπογραφής του M.

Το LV09 αποδεικνύεται ασφαλές με μία ελαφρώς ασθενεστέρη απαίτηση ανιχνευσιμότητας [LV09 §3.2], δεδομένων των υποθέσεων DLin, q-HSDH και της δυσκολίας του παρακάτω νέου προβλήματος, που αποδεικνύεται εύκολα του BDDH και δυσκολότερο του DDH:

Τριμερές Πρόβλημα Απόφασης Diffie-Hellman (*Decision Tripartite Diffie-Hellman - DTDH*)($\mathbb{G}$)**:** δεδομένων (g, g^a, g^b, g^c, η), όπου g γεννήτορας της $\mathbb{G}$ τάξης p, να αποφασιστεί εάν $\eta = g^{abc}$.

4.7 Οι Scalable Ομαδικές Υπογραφές με Μηχανισμό Ανάκλησης των Libert-Peters-Yung

Σε ένα σχήμα ομαδικών υπογραφών με ανάκληση, ο συνδυασμός ενός γρήγορου μηχανισμού ανάκλησης με τη μη γραμμική εξάρτηση των υπόλοιπων διαδικασιών του σχήματος από το πλήθος είτε των μελών της ομάδας N είτε των διαγραφόμενων μελών R, δεν υπήρξε μέχρι πολύ πρόσφατα επιτυχής. Σε ομάδες μεγάλου πλήθους,

είναι αναγκαίο να συνυπάρχουν όσο το δυνατόν περισσότερες *scalable*, δηλαδή σταθερού ή πολυλογαριθμικού, μεγέθους παράμετροι (κλειδιά, πιστοποιητικά, μήκος υπογραφής) και υπολογιστικού κόστους λειτουργίες (υπογραφή, επαλήθευση). Η εφαρμογή δυναμικών συσσωρευτών CL02 στο ACJT00 επιφέρει σταθερό κόστος υπογραφής και επαλήθευσης αλλά απαιτεί τακτή ενημέρωση των πιστοποιητικών των μελών μέσω $O(R)$ υψώσεων σε δύναμη (modular exponentiations - ME), ενώ στις υπογραφές BBS04 με μηχανισμό ανάκλησης είναι απαραίτητη η ενημέρωση των κλειδιών των ενεργών μελών μετά από κάθε ανάκληση. Οι VLR-ομαδικές υπογραφές BS04 και οι BU-VLR προεκτάσεις τους [NF05], [ZL06], [LV09] χαρακτηρίζονται από επαλήθευση γραμμικά εξαρτημένη από το πλήθος των τεκμηρίων ανάκλησης.

Σε νεότερες προσπάθειες, σημαντική βελτίωση αποτέλεσε το σχήμα των T.Nakanishi κ.ά. [NFHF09], με σταθερό κόστος υπογραφής και επαλήθευσης και χωρίς να χρειάζεται τα μέλη να ανανεώνουν τα ιδιωτικά τους κλειδιά. Το αντίτιμο σε αυτό το κέρδος είναι ότι το μέγεθος του ομαδικού δημόσιου κλειδιού είναι $O(N)$ ή $O(\sqrt{N})$ για μεγαλύτερες σταθερές κόστους υπογραφής και επαλήθευσης. Από μία άλλη σκοπιά, οι J.Camenisch, M.Kohlweiss C.Soriente [CKS09] κατασκεύασαν ένα νέο συσσωρευτή για ζεύγματα, τον οποίο εφάρμοσαν παραλλλαγμένα οι C.Fan, R.Hsu και M.Manulis [FHM11] σε ένα σχήμα ομαδικών υπογραφών με σταθερό μήκος υπογραφής και κόστος υπογραφής και επαλήθευσης, όπου όμως σε κάθε ανάκληση ο GM πρέπει να δημοσιεύει $O(N)$ ενημερωμένες τιμές. Τα BU-VLR σχήματα των [CL10], [BP11] παρόλο διαθέτουν μηχανισμό ανάκλησης αρκετά ταχύτερο των [NF05], [ZL06], [LV09] δεν αποφεύγουν τη γραμμική εξάρτηση κατά τη διαδικασία επαλήθευσης.

Λύση στο δύσκολο πρόβλημα κατασκευής scalable ομαδικών υπογραφών με μηχανισμό ανάκλησης παρουσίασαν στο EUROCRYPT 2012 οι B.Libert, T.Peters και M.Yung [LPY12a] . Το σχήμα τους αποδεικνύεται ασφαλές στο standard μοντέλο με τη χρήση του GSPS, πράγμα που καθιστά την επιτυχία τους σπουδαιότερη καθώς όλα τα προαναφερθέντα σχήματα εκτός του LV09 λειτουργούν στο ROM. Οι ομαδικές υπογραφές LPY12 διαθέτουν νέες τεχνικές ανάκλησης που στηρίζονται σε ιδέες από το χώρο της broadband κρυπτογράφησης. Επειδή η κατασκευή του σχήματος είναι περίπλοκη, περιγράφουμε πρώτα προσεκτικά καθεμία από τις συνιστώσες του.

Υπογραφές διατήρησης δομής AHO10. Όπως έχουμε αναφέρει, οι υπογραφές διατήρησης δομής [AFG+10], είναι ένα νέο εργαλείο που βασίζεται στις ιδιότητες του GSPS και ορίζονται ως οι υπογραφές που τα κλειδιά επαλήθευσης, τα μηνύματα και οι υπογραφές είναι στοιχεία ομάδας ζεύγματος και η επαλήθευση είναι μία σύζευξη εξισώσεων γινομένου-ζεύγματος. Στο σχήμα υπογραφών διατήρησης

δομής του [AHO10], επιτυγχάνονται υπογραφές σταθερού μήκους σε μία κίνηση σε προεπιλεγμένου πλήθους n μηνυμάτων όπως δίνεται παρακάτω :

Setup(1^k)**:** παράγονται οι παράμετροι $params = (p, \mathbb{G}, \mathbb{G}_T, e, g)$.

Keygen$(params, n)$**:** επιλέγονται γεννήτορες $G_r, H_r \in \mathbb{G}$, $\alpha_a, \alpha_b, \gamma_z, \delta_z \in \mathbb{Z}_p$ και $\gamma_i, \delta_i \in \mathbb{Z}_p$, $i \in [n]$. Υπολογίζονται τα $A = e(G_r, g^{\alpha_a}), B = e(H_r, g^{\alpha_b})$, $G_z = G_r^{\gamma_z}, H_z = H_r^{\delta_z}$ και $G_i = G_r^{\gamma_i}, H_i = H_r^{\delta_i}$, $i \in [n]$. Το ιδιωτικό και δημόσιο κλειδί είναι τα

$$sk = (\alpha_a, \alpha_b, \gamma_z, \delta_z, \{\gamma_i, \delta_i\}_{i=1}^n) \quad \text{και} \quad pk = (G_r, H_r, G_z, H_z, \{G_i, H_i\}_{i=1}^n, A, B).$$

Sign$(sk, (M_1, \ldots, M_n))$**:** επιλέγονται τυχαία $\zeta, \rho, \tau, \nu, \omega \in \mathbb{Z}_p$ και υπολογίζονται τα $\theta_1 = g^{\zeta}$ καθώς και τα

$$\theta_2 = g^{\rho - \gamma_z \zeta} \cdot \prod_{i=1}^{n} M_i^{-\gamma_i}, \quad \theta_3 = G_r^{\tau}, \quad \theta_4 = g^{(\alpha_a - \rho)/\tau},$$

$$\theta_5 = g^{\nu - \delta_z \zeta} \cdot \prod_{i=1}^{n} M_i^{-\delta_i}, \quad \theta_6 = H_r^{\omega}, \quad \theta_7 = g^{(\alpha_b - \nu)/\omega}.$$

Τελικώς η υπογραφή είναι η $\sigma = (\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, \theta_7)$.

Verify$(pk, (M_1, \ldots, M_n), \sigma)$**:** η σ γίνεται αποδεκτή ανν

$$A = e(G_z, \theta_1) \cdot e(G_r, \theta_2) \cdot e(\theta_3, \theta_4) \cdot \prod_{i=1}^{n} e(G_i, M_i),$$

$$B = e(H_z, \theta_1) \cdot e(H_r, \theta_5) \cdot e(\theta_6, \theta_7) \cdot \prod_{i=1}^{n} e(H_i, M_i).$$

Το AHO10 αποδεικνύεται EUF-CMA ασφαλές δεδομένης της δυσκολίας του εξής προβλήματος:

Πρόβλημα q-Ταυτόχρονου Προσαρμόσιμου Ζεύγματος (*q-Simultaneous Flexible Pairing Problem - q-SFP*)$(\mathbb{G})$**:** δεδομένων $(g_z, h_z, g_r, h_r, a, \tilde{a}, b, \tilde{b}) \in \mathbb{G}^8$ και $q \in \text{poly}(k)$ επτάδων $(z_j, r_j, s_j, t_j, u_j, v_j, w_j) \in \mathbb{G}^7$ ώστε

$$e(a, \tilde{a}) = e(g_z, z_j) \cdot e(g_r, r_j) \cdot e(s_j, t_j) \quad \text{και} \quad e(b, \tilde{b}) = e(h_z, z_j) \cdot e(h_r, u_j) \cdot e(v_j, w_j),$$

να βρεθεί νέα επτάδα (z, r, s, t, u, v, w) που να ικανοποιεί τις παραπάνω εξισώσεις και επίσης να ισχύει ότι $z \notin \{1_{\mathbb{G}}, z_1, \ldots, z_q\}$.

Στα [A+10 §5], [AHO10 §4.4] προτείνεται μία απλή randomization τεχνική με σκοπό τη δημιουργία διαφορετικής υπογραφής $\sigma' = \{\theta_i'\}_{i=1}^7$ στο $(M_1, \ldots, M_n)$, όπου $\theta_1' = \theta$ και οι $\{\theta_i'\}_{i=2}^7$ κατανέμονται ομοιόμορφα στο σύνολο των τιμών που ικανοποιούν τις ισότητες $e(G_r, \theta_2') \cdot e(\theta_3', \theta_4') = e(G_r, \theta_2) \cdot e(\theta_3, \theta_4)$ και $e(H_r, \theta_5') \cdot$

$e(\theta'_6, \theta'_7) = e(H_r, \theta_5) \cdot e(\theta_6, \theta_7)$. Επομένως τα $\theta'_3, \theta'_4, \theta'_6, \theta'_7$ είναι ανεξάρτητα των τιμών $(M_1, \ldots, M_n), \theta'_1, \theta'_2, \theta'_5$ και μπορούν να αποκαλυφθούν όσο οι τελευταίες έχουν δεσμευτεί. Τη διαδικασία παραγωγής της $\sigma' = \{\theta'_i\}_{i=1}^7$ τη γράφουμε ως $\{\theta'_i\}_{i=1}^7 \leftarrow \text{ReRand}(pk, \sigma)$.

Το πλαίσιο broadcast κρυπτογράφησης NNL01. Σε ένα σχήμα broadcast κρυπτογράφησης, δεδομένα όπως ήχος και εικόνα μεταδίδονται ασφαλώς μέσα από ανασφαλές κανάλι, σε πιθανώς δυναμικής φύσης σύνολο νόμιμων χρηστών. Μία καινοτόμος μεθοδολογία κατασκευής με συμμετρικά κλειδιά ήταν το πλαίσιο *Subset-Cover* των D.Naor, M.Naor J.Lotspiech [NNL01]: καθένας από τους $N = 2^l$ νόμιμους χρήστες αντιστοιχεί σε ένα φύλλο πλήρους δυαδικού δένδρου T βάθους l, ενώ σε κάθε κορυφή του T αντιστοιχεί ένα μυστικό κλειδί. Εάν $\mathcal{N}$ είναι το σύνολο των χρηστών και $\mathcal{R} \subset \mathcal{N}$ είναι το σύνολο των διεγραμμένων χρηστών, σκοπός του πλαισίου NNL01 είναι η διαμέριση του συνόλου των ενεργών χρηστών $\mathcal{N}\backslash\mathcal{R}$ σε m σύνολα $S_1, \ldots, S_m$. Από τα διάφορα στιγμιότυπα της μεθοδολογίας Subset-Cover, παραθέτουμε για συντομία μόνο τη μέθοδο *διαφοράς υποσυνόλου* (*subset difference - SD*), αν και στο [LPY12a] επισημαίνεται ότι μπορούν να εφαρμοστούν και άλλα στιγμιότυπα με ανάλογο συμβιβασμό στην επίδοση των επιμέρους λειτουργιών του σχήματος ομαδικών υπογραφών.

Στη μέθοδο SD καλούμε T_{x_j} το υποδένδρο του T με ρίζα την κορυφή x_j. Το σύνολο $\mathcal{N}\backslash\mathcal{R}$ διαμερίζεται στα υποσύνολα $S_{k_1,u_1}, \ldots, S_{k_m,u_m}$, όπου κάθε S_{k_i,u_i} καθορίζεται από την κορυφή x_{k_i} και μίας εκ των απογόνων της, x_{u_i}, που καλούνται *πρωτεύουσα* και *δευτερεύουσα* ρίζα του S_{k_i,u_i}, και αποτελείται απο τα φύλλα του $T_{x_{k_i}}$ που δεν ανήκουν στο T_{u_i}. Αποδεικνύεται ότι το μέγιστο πλήθος υποσυνόλων ειναι $m = 2R - 1$, όπου $R = |\mathcal{R}|$ [NNL01 Lemma 3]. Σε κάθε S_{k_i,u_i} ανατίθεται *μερικό* κλειδί P_{k_i,u_i} για τον υπολογισμό του συμμετρικού κλειδιού K_{k_i,u_i} και μερικά κλειδιά P_{k_i,u_d} για κάθε απόγονο x_{u_d} της x_{u_i}. Ένα P_{k_i,u_d} υπολογίζεται δύσκολα δίχως τη γνώση ενός μερικού κλειδιού P_{k_i,u_j} προγόνου x_{u_j} της x_{u_d}. Έστω v_i το φύλλο που αντιστοιχεί στο χρήστη i, $\epsilon = x_0, x_1, \ldots, x_l = v_i$ το μονοπάτι από τη ρίζα του T ως τη v_i, και copath_{x_j} το σύνολο όλων των αδελφών των ενδιάμεσων κορυφών του μονοπατιού $x_j, \ldots, v_i$ για κάθε T_{x_j}. Ο i παράγει τα κλειδιά όλων των S_{k_i,u_i} που ανήκει, αποθηκεύοντας τα $O(l^2)$ πλήθους μερικά κλειδιά $P_{x_j,w}$ για κάθε $w \in \text{copath}_{x_j}$, αφού ανήκει στο υποσύνολο με πρωτεύουσα ρίζα x_j και δευτερεύουσα ρίζα w.

Η broadcast κρυπτογράφηση δημόσιου κλειδιού DF02. Στο [DF02], οι Y. Dodis και N.Fazio πρότειναν μία επέκταση της μεθόδου SD για broadcast κρυπτογράφηση δημοσίου κλειδιού με τη βοήθεια σχημάτων ιεραρχικής κρυπτογράφησης

βάσει ταυτοτήτων (HIBE) (βλ. §2.5). Κάθε κορυφή w του T βάθους $\leqslant l$ έχει ετικέτα $\langle w\rangle$ η οποία ορίζεται αναδρομικά ως ϵ για τη ρίζα του T και $\langle w\rangle||0$, $\langle w\rangle||1$ για το αριστερό και το δεξί παιδί της w αντίστοιχα. Κατά την κρυπτογράφηση, για κάθε S_{k_i,u_i} με πρωτεύουσα ρίζα x_{k_i} και δευτερεύουσα ρίζα x_{u_i}, η ετικέτα $\langle x_{u_i}\rangle$ δαβάζεται ως $\langle x_{k_i}\rangle||u_{i,l_{i,1}}\cdots u_{i,l_{i,2}}$, όπου $u_{i,j}\in\{0,1\}$ για $j\in\{l_{i,1},\ldots,l_{i,2}\}$. Στη συνέχεια υπολογίζεται κρυπτοκείμενο για την ταυτότητα $(\langle x_{u_i}\rangle, u_{i,l_{i,1}},\ldots,u_{i,l_{i,2}})$ επιπέδου $l_{i,2}-l_{i,1}+2$. Εάν $\epsilon=x_0,x_1,\ldots,x_l=v_i$ όπως πριν, για κάθε υποδένδρο T_{x_j} και $w\in \mathrm{copath}_{x_j}$, ο χρήστης i λαμβάνει HIBE ιδιωτικό κλειδί για ταυτότητα $\langle x_j\rangle, w_{l_1},\ldots,w_{l_2}$ με καθορισμένο τρόπο καθώς υπάρχουν $l_1,l_2\in\{1,\ldots,l\}$ ώστε $\langle w\rangle||w_{l_1}\cdots w_{l_2}$. Επομένως ο i μπορεί να αποκρυπτογραφήσει κάθε κρυπτοκείμενο που αποστέλλεται σε υποσύνολο του $\mathcal{N}\backslash\mathcal{R}$ που ανήκει αποθηκεύοντας $O(\log^2 N)$ HIBE ιδιωτικά κλειδιά.

Το HIBE σχήμα BBG05. Για λόγους που θα δοθούν παρακάτω, το HIBE σχήμα που θα χρησιμοποιηθεί στις ομαδικές υπογραφές LPY12 είναι αυτό των D.Boneh, X.Boyen και E.Goh [BBG05], με σταθερού μήκους κρυπτοκείμενα. Το BBG05 l επιπέδων αποτελείται από τις εξής αλγορίθμους:

Setup$(1^k, l)$**:** Επιλέγονται δημόσιες παράμετροι $(p,\mathbb{G},\mathbb{G}_T,e)$ ως συνήθως και τυχαία $\alpha\in\mathbb{Z}_p$, g,g_2, $h_0,h_1,\ldots,h_l\in\mathbb{G}$. Το κύριο δημόσιο και ιδιωτικό κλειδί είναι

$$mpk_{\mathrm{BBG}}=(p,\mathbb{G},\mathbb{G}_T,e,g,g_1=g^\alpha,g_2,\{h_i\}_{i=0}^l),\quad msk_{\mathrm{BBG}}=g_2^\alpha.$$

Keygen$(msk_{\mathrm{BBG}}, ID=(I_1,\ldots,I_n))$**:** το ιδιωτικό κλειδί για την ταυτότητα $ID\in\mathbb{Z}_p^n$ στο επίπεδο n υπολογίζεται επιλέγοντας τυχαίο $r\in\mathbb{Z}_p$ ως

$$d_{ID}=(D_1,D_2,K_{n+1},\ldots,K_l)=(g_2^\alpha\cdot(h_0\cdot\prod_{i=1}^n h_i^{I_i})^r, g^r, h_{n+1}^r,\ldots,h_l^r)\in\mathbb{G}^{l-n+2}.$$

Extract$(d_{ID}, ID'=(I_1,\ldots,I_{n+1}))$**:** το κλειδί για την ταυτότητα ID' στο επίπεδο $n+1$ υπολογίζεται δεδομένου του d_{ID} επιλέγοντας τυχαίο $r'\in\mathbb{Z}_p$ ως

$$\begin{aligned}d_{ID'}&=(D_1',D_2',K_{n+2}',\ldots,K_l')=\\&=(D_1\cdot K_{n+1}^{I_{n+1}}\cdot(h_0\cdot\prod_{i=1}^{n+1}h_i^{I_i})^{r'}, D_2\cdot g^{r'}, K_{n+2}\cdot h_{n+2}^{r'},\ldots,K_l\cdot h_l^{r'})\in\mathbb{G}^{l-n+1}.\end{aligned}$$

Encrypt$(mpk_{\mathrm{BBG}}, ID=(I_1,\ldots,I_n), M)$**:** Για $M\in\mathbb{G}$ επιλέγεται $s\in\mathbb{Z}_p$ και υπολογίζεται το κρυπτοκείμενο

$$C=(C_0,C_1,C_2)=(M\cdot e(g_1,g_2)^s, g^s, (h_0\cdot\prod_{i=1}^n h_i^{I_i})^s).$$

Decrypt$(mpk_{\mathrm{BBG}}, d_{ID}, C)$**:** Ανακτάται το μήνυμα

$$M=C_0\cdot e(C_1,D_1)^{-1}\cdot e(C_2,D_2).$$

Ένα ιδιωτικό κλειδί d_{ID} χωρίζεται στο κλειδί αποκρυπτογράφησης (D_1, D_2) και τα μεταβατικά κλειδιά $(K_{n+1}, \ldots, K_l)$. Στις υπογραφές LPY12, το $d_{ID'}$ παράγεται χωρίς την τυχαιότητα που προσφέρει η επιλογή του r', δηλαδή

$$d_{ID'} = (D_1', D_2', K_{n+2}', \ldots, K_l') = (g_2^{\alpha} \cdot (h_0 \cdot \prod_{i=1}^{n+1} h_i^{I_i})^r, g^r, h_{n+2}^r, \ldots, h_l^r) \in \mathbb{G}^{l-n+1}.$$

Με αυτόν τρόπο, κλειδιά που αντιστοιχούν σε απογόνους της ID, μοιράζονται την ίδια παράμετρο g^r. Η ασφάλεια του LPY12 δεν επηρεάζεται διότι κάθε μέλος που ανήκει στο σύνολο $S_(k_i, u_i)$ αποκτά κλειδί για την ταυτότητα $(\langle x_{k_i} \rangle, u_{i,l_{i,1}}, \ldots, u_{i,l_{i,2}})$ το οποίο παράγεται εκ νέου, δηλαδή από νέο τυχαίο r, κατά την εγγραφή του.

Οι ομαδικές υπογραφές LPY12. Το μοντέλο κατασκευής και ασφάλειας που ακολουθείται συνδυάζει τη μορφή του KY04 με τη δυνατότητα διαχωρισμού των αρχών του BSZ05, επαυξημένο με τον αλγόριθμο Revoke, ο οποίος με είσοδο τα gpk και σύνολο μελών προς διαγραφή $\mathcal{R}_t \subset St_{users}$, επιτρέπει στον GM να επιστρέφει μία ανανεωμένη λίστα ανάκλησης RL_t για την περίοδο t. Αντίστοιχα ορίζεται μαντείο Q_{revoke} που σε ερώτημα $i \in St_{users}$ επιστρέφει στον αντίπαλο ανανεωμένη λίστα RL_t για νέα περίοδο t που περιέχει τον i.

Βασική ιδέα είναι ένα broadcast κρυπτοκείμενο να αποτελέσει λίστα ανάκλησης για το σχήμα. Σε δυναμική ομάδα maximum μεγέθους 2^l, κάθε μέλος εγγράφεται έχοντας αντιστοιχηθεί σε φύλλο δένδρου T βάθους l και με πιστοποιητικό που περιλαμβάνει τα $O(l^2)$ HIBE ιδιωτικά κλειδιά. Σε κάθε περίοδο t, ο GM παράγει ενημερωμένη RL_t που αποτελείται από $O(R)$ κρυπτοκείμενα, το καθένα υπογεγραμμένο μέσω υπογραφής AHO10. Το μέλος i αποδεικνύει ότι δεν έχει ανακληθεί δεσμεύοντας ένα κρυπτοκείμενο C_j της RL_t και αποδεικνύοντας ότι κατέχει κλειδί που αποκρυπτογραφεί το C_j. Επίσης πείθει τον επαληθευτή ότι $C_j \in \mathrm{RL}_t$ παρέχοντας γνώση υπογραφής για το C_j. Η ανωνυμία του i διατηρείται εάν το HIBE σχήμα που χρησιμοποιείται έχει σταθερού μήκους κρυπτοκείμενα, ειδάλλως το μήκος του κρυπτοκειμένου μπορεί να αποκάλυπτε σημαντική πληροφορία για τη θέση του i στο δένδρο.

Η ανωνυμία και η αντίσταση σε σκευωρία του σχήματος εξασφαλίζεται με τη χρήση NIZK τεχνικών των [Gro06], [Gro07], ενώ για την αποφυγή εσφαλμένης αναγνώρισης απαιτείται το HIBE σχήμα να είναι ασφαλές κατά μία ειδική έννοια: κανένας αντίπαλος που προεπιλέγει την ταυτότητα πρόκλησης ID και λαμβάνει το μυστικό κλειδί msk της PKG, το δημόσιο κλειδί κρυπτογράφησης mpk καθώς και το ιδιωτικό κλειδί d_{ID} της ID, δεν μπορεί να παράγει ιδιωτικό κλειδί ταυτότητας $ID' \neq ID$ τηρώντας την τυχαιότητα που επιλέχτηκε κατά τον αλγόριθμο παραγωγής ιδιωτικών κλειδιών. Η ιδιότητα αυτή ονομάζεται *ευρωστία κλειδιού* (*key-robustness*) και πληρούται από το HIBE σχήμα BBG05 υπό την υπόθεση CDH.

Το σχήμα ομαδικών υπογραφών LPY12 συνίσταται από τους εξής αλγορίθμους:

Setup$(1^k, N = 2^l)$**:** Επιλέγονται ως συνήθως $(p, \mathbb{G}, \mathbb{G}_T, e, g)$ και παράγονται δύο ζεύγη κλειδιών για υπογραφές AHO10

$$sk_{\text{AHO}}^{(d)} = (\alpha_a^{(d)}, \alpha_b^{(d)}, \gamma_z^{(d)}, \delta_z^{(d)}, \{\gamma_i^{(d)}, \delta_i^{(d)}\}_{i=1}^2) \quad \text{και}$$

$$pk_{\text{AHO}}^{(d)} = (G_r^{(d)}, H_r^{(d)}, G_z^{(d)}, H_z^{(d)}, \{G_i^{(d)}, H_i^{(d)}\}_{i=1}^2, A^{(d)}, B^{(d)}), \quad d \in \{0,1\}.$$

Όπως στο LV09, επιλέγονται τυχαία $\beta_1, \beta_2, \xi_1, \xi_2 \in \mathbb{Z}_p^*$ και υπολογίζονται τα $f_1 = g^{\beta_1}, f_2 = g^{\beta_2}$. Τελικά έχουμε το CRS $\mathbf{f} = (\bar{f}_1, \bar{f}_2, \bar{f}_3)$, όπου $\bar{f}_1 = (f_1, 1, g)$, $\bar{f}_2 = (1, f_2, g)$, $\bar{f}_3 = \bar{f}_1^{\xi_1} \cdot \bar{f}_2^{\xi_2}$. Επιλέγονται επίσης $U, V \in \mathbb{G}$ που μαζί με τα f_1, f_2, g θα αποτελέσουν δημόσιο κλειδί κρυπτογράφησης. Παράγεται κύριο δημόσιο κλειδί $mpk_{\text{BBG}} = (\{h_i\}_{i=0}^l)$ του BBG05 (αγνοούμε τα g_1, g_2). Επιλέγονται συνάρτηση κωδικοποίησης $\mathcal{H} : \bigcup_{i=0}^l \{0,1\}^i \longrightarrow \mathbb{Z}_p^*$ [2] και SEUF-CMA σχήμα υπογραφών μίας χρήσης $\mathbf{OTS} = (\mathcal{G}, \mathcal{S}, \mathcal{V})$, όπως οι υπογραφές BB.

Θέτουμε ως ιδιωτικά κλειδιά του GM και της *αρχής ανίχνευσης* (*opening authority - OA*) τα $gmsk = (sk_{\text{AHO}}^{(0)}, sk_{\text{AHO}}^{(1)})$ και $oask = (\beta_1, \beta_2)$ και ως ομαδικό δημόσιο κλειδί το $gpk = (g, pk_{\text{AHO}}^{(0)}, pk_{\text{AHO}}^{(1)}, mpk_{\text{BBG}}, \mathbf{f}, (U, V), \mathcal{H}, \mathbf{OTS})$.

Join$^{\text{GM},i}$**:** Εκτελείται το διαλογικό πρωτόκολλο $\langle J_{\text{user}}, J_{\text{GM}}(St, gmsk)\rangle(1^k, gpk)$:

1. Ο J_{user} επιλέγει τυχαίο $x \in \mathbb{Z}_p$ και αποστέλλει την τιμή $X = g^x$.
2. Εάν η X εμφανίζεται σε κάποιο $\text{transcript}_j \in St_{trans}$, ο J_{GM} σταματά και επιστρέφει $\perp$. Διαφορετικά, αντιστοιχεί στον i φύλλο v_i του T με ετικέτα $\langle v_i\rangle = v_{i,1}, \ldots, v_{i,l} \in \{0,1\}^l$. Έστω $\epsilon = x_0, x_1, \ldots, x_l = v_i$ το μονοπάτι από τη ρίζα του T ως τη v_i. Για $j = 0, \ldots, l$:
   i. Εάν T_{x_j} και copath_{x_j} όπως ορίστηκαν πριν, τότε για κάθε $w \in \text{copath}_{x_j}$ $\langle w\rangle = \langle x_j\rangle || w_{l_1} \cdots w_{l_2}$, αφού η x_j είναι πρόγονος της w. Επιλέγεται επομένως τυχαίο $r \in \mathbb{Z}_p$ και υπολογίζεται το HIBE ιδιωτικό κλειδί

$$\begin{aligned} d_w &= (D_{w,1}, D_{w,2}, K_{w,l_2-l_1+3}, \ldots, K_{w,l}) = \\ &= ((h_0 \cdot h_1^{\mathcal{H}(\langle x_j\rangle)} \cdot h_2^{\mathcal{H}(w_{l_1})} \cdots h_{l_2-l_1+2}^{\mathcal{H}(w_{l_2})})^r, g^r, h_{l_2-l_1+3}^r, \ldots, h_l^r), \end{aligned}$$

   για την ταυτότητα $(\mathcal{H}(\langle x_j\rangle), \mathcal{H}(w_{l_1}), \ldots, \mathcal{H}(w_{l_2})) \in (\mathbb{Z}_p^*)^{l_2-l_1+2}$.
   ii. Με τη χρήση του $sk_{\text{AHO}}^{(0)}$ παράγεται υπογραφή AHO10 $\sigma_w = (\theta_{w,1}, \ldots, \theta_{w,7})$ για το μήνυμα $(X, D_{w,2})$ που δεσμεύει το d_w με την τιμή X που ταυτοποιεί τον i.

   Ο J_{GM} αποστέλλει την ετικέτα $\langle v_i\rangle$ και τα ιδιωτικά κλειδιά $\{\{d_w\}_{w \in \text{copath}_{x_j}}\}_{j=0}^l$.

[2] Μία τέτοια συνάρτηση κατασκευάζεται εύκολα εάν $|\bigcup_{i=0}^l \{0,1\}^i| = 2^{l+1} - 1 < p - 1$ και «απομηδενίζει» τις ταυτότητες.

3. Ο J_{user} επαληθεύει την εγκυρότητα των d_w και εάν αυτό συμβαίνει, αποστέλλει μία συνηθισμένη υπογραφή $sign_i = \text{Sign}(usk[i], X||\{\{d_w\}_{w\in\text{copath}_{x_j}}\}_{j=0}^{l})$.

4. Εάν $\text{Verify}(upk[i], X||\{\{d_w\}_{w\in\text{copath}_{x_j}}\}_{j=0}^{l}, sign_i)$=0, ο J_{GM} απορρίπτει. Διαφορετικά, επιστρέφει τις υπογραφές $\{\{\sigma_w\}_{w\in\text{copath}_{x_j}}\}_{j=0}^{l}$ και αποθηκεύει την επικοινωνία του με τον J_{user}.

5. Ο J_{user} ορίζει ως πιστοποιητικό του i το $cert_i = (\langle v_i\rangle, \{\{d_w, \sigma_w\}_{w\in\text{copath}_{x_j}}\}_{j=0}^{l})$. Ως μυστική τιμή του i επιλέγεται η $sec_i = x$.

Revoke$(gpk, gmsk, t, \mathcal{R}_t)$**:** Εφαρμόζουμε την μέθοδο SD και βρίσκουμε διαμέριση $S_{k_1,u_1}, \ldots, S_{k_m,u_m}$ του $\{1,\ldots,N\}\backslash\mathcal{R}_t$, όπου $m \leqslant 2\cdot|\mathcal{R}_t| - 1$. Για $i = 0,\ldots,m$:

i. Σύμφωνα με το DF02, έχουμε ότι $\langle x_{u_i}\rangle = \langle x_{k_i}\rangle||u_{i,l_{i,1}}\cdots u_{i,l_{i,2}}$, όπου $u_{i,j} \in \{0,1\}$ για $j \in \{l_{i,1},\ldots,l_{i,2}\}$. Κωδικοποιούμε το υποσύνολο S_{k_i,u_i} ως το στοιχείο

$$C_i = h_0 \cdot h_1^{\mathcal{H}(\langle x_{k_i}\rangle)} \cdot h_2^{\mathcal{H}(u_{i,l_{i,1}})} \cdots h_{l_{i,2}-l_{i,1}+2}^{\mathcal{H}(u_{i,l_{i,2}})} \in \mathbb{G}.$$

ii. Το C_i καθιστάται γνήσιο αφού δεσμευτεί με την περίοδο $t \in \mathbb{Z}_p$, με την παραγωγή υπογραφής AHO10 $\Theta_i = (\Theta_{i,1},\ldots,\Theta_{i,7})$ του μηνύματος (C_i, g^t) υπό το κλειδί $sk_{\text{AHO}}^{(1)}$.

Ο GM επιστρέφει την ανανεωμένη λίστα $RL_t = (t, \mathcal{R}_t, \{\langle x_{k_i}\rangle, \langle x_{u_i}\rangle, (C_i, \Theta_i)\}_{i=1}^{m})$.

Sign$(gpk, t, RL_t, cert_i, sec_i, M)$**:** Εάν $i \in \mathcal{R}_t$ τότε επιστρέφουμε $\perp$. Διαφορετικά:

1. Δημιουργείται ζεύγος κλειδιών $(sk, vk) \leftarrow \mathcal{G}(1^k)$.

2. Με τη χρήση της RL_t εντοπίζεται S_{k_j,u_j} που περιέχει το φύλλο v_i και έστω x_{k_j}, x_{u_j} οι πρωτεύουσα και δευτερεύουσα ρίζα του αντίστοιχα. Εφόσον $\langle x_{u_j}\rangle = \langle x_{k_j}\rangle||u_{j,l_1}\cdots u_{j,l_2}$ για κάποια $l_1 < l_2 \leqslant l$ και $v_i \notin T_{x_{u_j}}$, υπάρχει ελάχιστο l_1' ώστε το $\langle x_{k_j}\rangle||u_{j,l_1}\cdots u_{j,l_1'}$ να είναι πρόθεμα του $\langle x_{u_j}\rangle$ αλλά όχι του $\langle v_i\rangle$. Τότε το σύνολο $\{d_w\}_{w\in\text{copath}_{x_{k_j}}}$ περιέχει κλειδί d_w ώστε

$$d_w = ((h_0 \cdot h_1^{\mathcal{H}(\langle x_{k_j}\rangle)} \cdot h_2^{\mathcal{H}(u_{j,l_1})} \cdots h_{l_1'-l_1+2}^{\mathcal{H}(u_{j,l_1'})})^r, g^r, h_{l_1'-l_1+3}, \ldots, h_l^r).$$

Επομένως, ο υπογράφων i μπορεί να εξάγει HIBE κλειδί αποκρυπτογράφησης

$$\begin{aligned}(D_{j,1}, D_{j,2}) &= ((h_0 \cdot h_1^{\mathcal{H}(\langle x_{k_i}\rangle)} \cdot h_2^{\mathcal{H}(u_{i,l_1})} \cdots h_{l_1'-l_1+2}^{\mathcal{H}(u_{i,l_1'})} \cdots h_{l_2-l_1+2}^{\mathcal{H}(u_{i,l_2})})^r, g^r)\\ &= ((h_0 \cdot h_1^{\mathcal{H}(\langle x_{k_i}\rangle)} \cdot h_2^{\mathcal{H}(u_{i,l_1})} \cdots h_{l_2-l_1+2}^{\mathcal{H}(u_{i,l_2})})^r, g^r).\end{aligned}$$

3. Ο i αποδεικνύει ότι μπορεί να αποκρυπτογραφήσει το C_j υπολογίζοντας τη νέα υπογραφή $\{\Theta'_{j,k}\}_{k=1}^{7} \leftarrow \text{ReRand}(pk_{\text{AHO}}^{(1)}, \Theta_j)$ και τις GS δεσμεύσεις com_{C_j}, $com_{\Theta'_{j,1}}, com_{\Theta'_{j,2}}, com_{\Theta'_{j,5}}$ για τις τιμές $C_j, \Theta'_{j,1}, \Theta'_{j,2}, \Theta'_{j,5}$ βάσει του στιγμιότυπου DLin. Θεωρώντας τις $\Theta'_{j,3}, \Theta'_{j,4}, \Theta'_{j,6}, \Theta'_{j,7}$ κατασκευάζει απόδειξη π_{C_j}

της εγκυρότητας του κρυπτοκειμένου C_j κατά την περίοδο t μέσω της επαληθευσιμότητας των γραμμικών εξισώσεων

$$A^{(1)} \cdot e(\Theta'_{j,3}, \Theta'_{j,4})^{-1} \cdot e(G_2^{(1)}, g^t)^{-1} = e(G_z^{(1)}, \Theta'_{j,1}) \cdot e(G_r^{(1)}, \Theta'_{j,2}) \cdot e(G_1^{(1)}, C_j),$$

$$B^{(1)} \cdot e(\Theta'_{j,6}, \Theta'_{j,7})^{-1} \cdot e(H_2^{(1)}, g^t)^{-1} = e(H_z^{(1)}, \Theta'_{j,1}) \cdot e(H_r^{(1)}, \Theta'_{j,5}) \cdot e(H_1^{(1)}, C_j).$$

Έπειτα παράγει δεσμεύσεις $com_{D_{j,1}}, com_{D_{j,2}}$ για τα $D_{j,1}, D_{j,2}$ και απόδειξη π_{D_j} για την επαληθευσιμότητα της τετραγωνικής εξίσωσης $e(D_{j,1}, g) = e(C_j, D_{j,2})$. Οι π_{C_j} και π_{D_j} αποτελούνται συνολικά από 2·3+9=15 στοιχεία.

4. Από την υπογραφή AHO10 $\sigma_j = (\theta_{j,1}, \ldots, \theta_{j,7})$ του μηνύματος $(X, D_{j,2})$ υπό το κλειδί $sk_{\text{AHO}}^{(0)}$ υπολογίζονται οι $\{\theta'_{j,k}\}_{k=1}^{7} \leftarrow \text{ReRand}(pk_{\text{AHO}}^{(0)}, \sigma_j)$, οι GS δεσμεύσεις $com_{\theta'_{j,1}}, com_{\theta'_{j,2}}, com_{\theta'_{j,5}}$ για τις τιμές $\theta'_{j,1}, \theta'_{j,2}, \theta'_{j,5}$ και η δέσμευση com_X για τη X. Παράγεται απόδειξη π_{σ_j} για την επαληθευσιμότητα των γραμμικών εξισώσεων

$$A^{(0)} \cdot e(\theta'_{j,3}, \theta'_{j,4})^{-1} = e(G_z^{(0)}, \theta'_{j,1}) \cdot e(G_r^{(0)}, \theta'_{j,2}) \cdot e(G_1^{(0)}, X) \cdot e(G_2^{(0)}, D_{j,2}),$$

$$B^{(0)} \cdot e(\theta'_{j,6}, \theta'_{j,7})^{-1} = e(H_z^{(0)}, \theta'_{j,1}) \cdot e(H_r^{(0)}, \theta'_{j,5}) \cdot e(H_1^{(0)}, X) \cdot e(H_2^{(0)}, D_{j,2}).$$

Η π_{σ_j} αποτελείται από 2·3=6 στοιχεία.

5. Έστω ότι $vk \in \mathbb{Z}_p$ μέσω κατάλληλης συνάρτησης hash. Επιλέγονται τυχαία $z_1, z_2 \in \mathbb{Z}_p$ και με ετικέτα το vk υπολογίζεται κρυπτοκείμενο Kil06 (βλ. §4.4)

$$(\Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5) = (f^{z_1}, f^{z_2}, X \cdot g^{z_1+z_2}, (g^{vk} \cdot U)^{z_1}, (g^{vk} \cdot V)^{z_2}).$$

6. Παράγεται NIZK απόδειξη ότι οι $com_X = (1, 1, X) \odot \bar{f}_1^{\phi_{X,1}} \odot \bar{f}_2^{\phi_{X,2}} \odot \bar{f}_3^{\phi_{X,3}}$ και οι (Ψ_1, Ψ_2, Ψ_3) αντιστοιχούν στην ίδια τιμή X, όπως στην κατασκευή των Gro07. Γράφοντας $\bar{f}_3 = (f_{3,1}, f_{3,2}, f_{3,3})$ έχουμε ότι

$$com_X \odot (\Psi_1, \Psi_2, \Psi_3)^{-1} = (f_1^{\tau_1} \cdot f_{3,1}^{\tau_3}, f_2^{\tau_2} \cdot f_{3,2}^{\tau_3}, g^{\tau_1+\tau_2} \cdot f_{3,3}^{\tau_3}), \tag{4.3}$$

όπου $\tau_1 = \phi_{X,1} - z_1, \tau_1 = \phi_{X,2} - z_2, \tau_3 = \phi_{X,3}$. Ο i δεσμεύει τις τ_1, τ_2, τ_3 υπολογίζοντας $com_{\tau_k} = ((1, 1, g) \odot \bar{f}_3)^{\tau_k} \odot \bar{f}_1^{\phi_{\tau_k,1}} \odot \bar{f}_2^{\phi_{\tau_k,2}})$, για $k = 1, 2, 3$, όπου τα $\phi_{\tau_k,2}, \phi_{\tau_k,2}$ επιλέγονται τυχαία. Επίσης, παράγει αποδείξεις $\{\pi_{eq,k}\}_{k=1}^{3}$ ότι οι τ_1, τ_2, τ_3 ικανοποιούν τις τρεις γραμμικές εξισώσεις που προκύπτουν από την (4.3), αποτελούμενες η καθεμία από 2 στοιχεία.

7. Υπολογίζονται weak-BB υπογραφή $\sigma_{vk} = g^{1/(x+vk)}$, η αντίστοιχη δέσμευση $com_{\sigma_{vk}}$ και η NIWI απόδειξη $\pi_{\sigma_{vk}}$ ότι οι σ_{vk}, X ικανοποιούν την τετραγωνική εξίσωση $e(\sigma_{vk}, X \cdot g^{vk}) = e(g, g)$. Η $\pi_{\sigma_{vk}}$ αποτελείται επομένως από 9 στοιχεία.

8. Υπολογίζεται η $\sigma_{\text{OTS}} = \mathcal{S}(sk, (M, RL_t, \Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Omega, \mathbf{com}, \mathbf{\Pi}))$, όπου $\Omega = \{\Theta'_{j,k}, \theta'_{j,k}\}_{k=1}^{7}$, $\mathbf{\Pi} = (\pi_{C_j}.\pi_{D_j}, \pi_{\sigma_j}, \{\pi_{eg,k}\}_{k\in\{1,2,3\}}, \pi_{\sigma_{vk}})$ και

$$\mathbf{com} = (com_{C_j}, \{com_{D_{j,k}}\}_{k\in\{1,2\}}, com_X, \{com_{\Theta'_{j,k}}\}_{k\in\{1,2,5\}}, \{com_{\theta'_{j,k}}\}_{k\in\{1,2,5\}}, \{com_{\tau_k}\}_{k\in\{1,2,3\}}, com_{\sigma_{vk}}).$$

Τελικώς επιστρέφεται η υπογραφή $\sigma = (vk, \Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Omega, \mathbf{com}, \mathbf{\Pi}, \sigma_{\text{OTS}})$.

Verify$(gpk, t, RL_t, \sigma, M)$**:** για την επαλήθευση της σ εκτελούνται τα βήματα:

1. Εάν $\mathcal{V}(vk, (M, RL_t, \Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Omega, \mathbf{com}, \mathbf{\Pi}), \sigma_{\text{OTS}}) = 0$, επίστρεψε 0.
2. (Έλεγχος Kil06) Εάν $e(\Psi_1, g^{vk} \cdot U) \neq e(f_1, \Psi_4)$ ή $e(\Psi_2, g^{vk} \cdot V) \neq e(f_2, \Psi_5)$, επίστρεψε 0.
3. Εάν επαληθεύονται όλες οι αποδείξεις, επίστρεψε 1. Διαφορετικά, επίστρεψε 0.

Open$(gpk, t, RL_t, \sigma, M, oask, St)$**:** δεδομένου του $oask = (\beta_1, \beta_2)$, εάν Verify$(gpk, t, RL_t, \sigma, M) = 0$, επίστρεψε $\perp$. Διαφορετικά, αποκρυπτογραφείται το κρυπτοκείμενο Kil06 ως $\tilde{X} = \Psi_3 \cdot \Psi_1^{-1/\beta_1} \cdot \Psi_2^{-1/\beta_2}$. Εάν στη βάση δεδομένων St_{trans} βρεθεί καταχώρηση $\langle i, \text{transcript}_i = (X, \{\{d_w, \sigma_w\}_{w\in\text{copath}_{x_j}}\}_{j=0}^{l}, sign_i)\rangle$ ώστε $X = \tilde{X}$, τότε επίστρεψε i. Διαφορετικά, επίστρεψε $\perp$.

Η λίστα ανάκλησης RL_t περιέχει για κάθε $i \in [m]$, 8 στοιχεία της $\mathbb{G}$ και τις ετικέτες των κορυφών που ορίζουν το S_{k_i,u_i} (μεγέθους $2{\cdot}\log(N)$). Χρειάζονται $O(\log^3(N))$ στοιχεία για την αποθήκευση του πιστοποιητικού ενός μέλους. Τα $\mathbf{com}, \mathbf{\Pi}$ αποτελούνται από 42 και 36 στοιχεία αντίστοιχα ενώ αν χρησιμοποιηθούν οι υπογραφές μίας χρήσης του [Gro06 §5.1] η σ αποτελείται συνολικά από 96 στοιχεία, δηλαδή ≈6kB για ασφάλεια 128-bit. Το κόστος επαλήθευσης είναι σταθερό, ενώ για τη δημιουργία μίας υπογραφής η κύρια επιβάρυνση είναι η εκτέλεση $\log(N)$ ΜΕ κατά την παραγωγή του HIBE ιδωτικού κλειδιού στο βήμα 2. Εντούτοις, το βήμα 2 αρκεί να εκτελεστεί μόνο μία φορά για κάθε περίοδο t, κατά τη δημιουργία της πρώτης υπογραφής σε αυτήν την περίοδο. Σημειώνουμε πως με τη χρήση μιας διαφορετικής subset cover μεθόδου διαμέρισης του συνόλου των ενεργών μελών (complete subtree - CS), κερδίζουμε σταθερό μήκος ομαδικού δημόσιου κλειδιού και κόστους υπογραφής και πιστοποιητικά $O(\log(N))$ πλήθους στοιχείων, με επιβάρυνση στο μέγεθος της λίστας ανάκλησης κατά πολλαπλασιαστικό παράγοντα $O(\log(N/R))$. Το σχήμα LPY12 αποδεικνύεται ασφαλές απέναντι σε επιθέσεις ανωνυμίας, σκευωρίας και εσφαλμένης αναγνώρισης υπό τις υποθέσεις DLin, q_b-SDH και q-SFP αντίστοιχα για συγκεκριμένα q_b, q [LPY12b Theorems 1,2&3]. Ενδεικτικά, αποδεικνύουμε την ασφάλεια σε επιθέσεις εσφαλμένης αναγνώρισης.

Θεώρημα 4.7.1. *Το σχήμα LPY12 είναι ασφαλές απέναντι σε επιθέσεις εσφαλμένης αναγνώρισης υπό την υπόθεση q-SFP για* $q = \max\{l^2 \cdot q_a, q_r^2\}$*, όπου* q_a *το*

πλήθος των ερωτημάτων δημιουργίας ελεγχόμενων μελών στο $\mathrm{Q}_{\mathcal{A}-\mathrm{join}}$ *και* q_r *το πλήθος των ερωτημάτων ανάκλησης στο* $\mathrm{Q}_{\mathrm{revoke}}$.

Απόδειξη. Στο παίγνιο εσφαλμένης αναγνώρισης ο αντίπαλος $\mathcal{A}$ εκτός από ερωτήματα στα $\mathrm{Q}_{\mathcal{A}-\mathrm{join}}$, $\mathrm{Q}_{\mathrm{revoke}}$ μπορεί να θέσει ερωτήματα απόκτησης των κλειδιών gpk και $oask$ και ανάγνωσης των δεδομένων της διεπιφάνειας $\mathfrak{I}$, εκτός των $gpk, gpmsk$, $oask$ στα μαντεία $\mathrm{Q}_{\mathrm{pub}}$, $\mathrm{Q}_{\mathrm{keyOA}}$ και $\mathrm{Q}_{\mathrm{read}}$ αντίστοιχα. Τελικώς επιστρέφει ζεύγος (M^*, σ^*) και κερδίζει εάν

1. $\mathrm{Verify}(gpk, t*, RL_{t*}, \sigma^*, M^*) = 1$ και
2. $\mathrm{Open}(gpk, t*, RL_{t*}, \sigma^*, M^*, oask, St^*) = i \notin U^{\mathcal{A}} \backslash \mathcal{R}_{t*}$,

όπου τα $RL_{t*}, St^*, \mathcal{R}_{t*}$ λαμβάνονται για τη νεά περίοδο t^* με το πέρας των ερωτημάτων. Ο ορισμός επεκτείνει αυτόν του μοντέλου KU04, αφού ο $\mathcal{A}$ κερδίζει ακόμα και όταν η σ^* ανιχνεύεται προς ελεγχόμενο μέλος που διαγράφτηκε κατά τη διάρκεια της περιόδου t^*.

Έστω $\sigma^* = (vk^*, \Psi_1^*, \Psi_2^*, \Psi_3^*, \Psi_4^*, \Psi_{*5}, \Omega_*, \mathbf{com}_*, \mathbf{\Pi}, \sigma_{OTS}^*)$. Ανάλογα με τα περιεχόμενα των $com_C^*, com_{D_1}^*, com_{D_2}^*, com_X^*, \{com_{\Theta'_{j,k}}^*\}_{k\in\{1,2,5\}}, \{com_{\theta'_{j,k}}^*\}_{k\in\{1,2,5\}}$ διακρίνουμε τις εξής περιπτώσεις:

Πλαστογραφήσεις τύπου I: η δέσμευση com_C^* περιέχει $C^* \in \mathbb{G}$ ώστε το ζεύγος (C^*, g^{t^*}) να μην υπογράφτηκε μετά τη δημιουργία της RL_{t*}.

Πλαστογραφήσεις τύπου II: η δέσμευση com_C^* περιέχει έγκυρο HIBE κρυπτοκείμενο C^* για την περίοδο t^* και έστω $C^* = C_j^*$, $j \in [m]$, όπου τα $\{C_1^*, \ldots, C_m^*\}$ περιέχονται στην RL_{t*}. Η εκτέλεση του Open είτε εξάγει νέα τιμή X^* ή εντοπίζει διεγραμμένο μέλος $i \in U^{\mathcal{A}} \cap \mathcal{R}_{t*}$, παρόλο που η σ^* ως έγκυρη πείθει ότι το (D_1^*, D_2^*) αποκρυπτογραφεί το C_j^* και ότι οι $\{com_{\theta'_{j,k}}^*\}_{k=1}^7$ συνιστούν έγκυρη υπογραφή του (X^*, D_2^*). Διακρίνουμε τις εξής περιπτώσεις:

1. Το (X^*, D_2^*) δεν υπογράφτηκε από τον J_{GM} σε καμία εκτέλεση του πρωτοκόλλου Join. Επομένως είτε η X^* δεν εμφανίζεται στο St_{trans} ή το μέλος $i \in U^{\mathcal{A}} \cap \mathcal{R}_{t*}$ συμπίπτει με ενεργό μέλος $i' \in U^{\mathcal{A}}$ του οποίου το φύλλο $v_{i'}$ ανήκει στο S_{k_j,u_j}. Καθώς το C_j^* κρυπτογραφεί το S_{k_j,u_j}, έπεται ότι το i πλαστογράφησε υπογραφή AHO10 για το μήνυμα (X^*, D_2^*).
2. Το (X^*, D_2^*) υπογράφτηκε από τον J_{GM} σε κάποια εκτέλεση του πρωτοκόλλου Join. Τότε επικαλούμαστε την ευρωστία κλειδιού που χαρακτηρίζει το σχήμα HIBE. Το i έχει ανακληθεί κατά την περίοδο t^*, άρα το κλειδί αποκρυπτογράφησης (D_1^*, D_2^*) δε δόθηκε ως μέλος του πιστοποιητικού του i. Εφόσον όμως το (X^*, D_2^*) υπογράφτηκε από τον J_{GM}, ο i πρέπει να απέκτησε από τον J_{GM} κλειδί (D_1, D_2^*), όπου $(D_1 \neq D_1^*)$, για ταυτότητα διαφορετική από αυτή που αντιστοιχεί στο S_{k_j,u_j}.

Είναι φανερό ότι πλαστογραφήσεις τύπου I και II.1 συνεπάγονται την πλαστογράφηση υπογραφής AHO10. Για την περίπτωση πλαστογραφήσεων τύπου II.2 έχουμε τον ακόλουθο ισχυρισμό:

Ισχυρισμός: *Εάν το LPY12 επιδέχεται επιθέσεις τύπου II.2, τότε το BBG05 δεν έχει ευρωστία κλειδιού.*

Η απόδειξη του παραπάνω ισχυρισμού στηρίζεται στο [LPY12b Lemma 2].

Σε κάθε ερώτημα προς το $\mathrm{Q}_{\mathcal{A}-\mathrm{join}}$ δημιουργούνται l^2 υπογραφές AHO10 ενώ στο i-οστό ερώτημα προς το $\mathrm{Q}_{\mathrm{revoke}}$ δημιουργούνται $\leqslant 2 \cdot (|\mathcal{R}_{t_0}| + i - 1) - 1$ υπογραφές AHO10, όπου $\mathcal{R}_{t_0}$ το σύνολο των διεγραμμένων μελών πριν την εκκίνηση των ερωτημάτων ανάκλησης. Υποθέτοντας ότι $|\mathcal{R}_{t_0}| < q_r$ λαμβάνουμε το φράγμα $q = \max\{l^2 \cdot q_a, q_r^2\}$. Η υπόθεση q-SFP συνεπάγεται την υπόθεση CDH που με τη σειρά της, όπως αναφέραμε, συνεπάγεται την ευρωστία κλειδιού του BBG05 [LPY12b Lemma 1]. Το γεγονός αυτό σε συνδυασμό με τον ισχυρισμό ολοκληρώνει την απόδειξη του θεωρήματος.

⊣

4.8 Σύνοψη Κεφαλαίου - Περαιτέρω Σχήματα Ομαδικών Υπογραφών

Παρουσιάσαμε αναλυτικά τα μοντέλα σύνταξης και ασφάλειας για σχήματα ομαδικών υπογραφών BMW03, KY04, BSZ05, καλύπτοντας τη στατική και δυναμική περίπτωση, και τη σύνταξη ένος σχήματος ανιχνεύσιμων υπογραφών [KTY04]. Αναφέραμε την έννοια του δυναμικού συσσωρευτή [CL02] και τη σημασία του στην κατασκευή ομαδικών υπογραφών με αποτελεσματικό μηχανισμό ανάκλησης. Μελετήσαμε αρχικά τα πολύ επιδραστικά σχήματα BBS04 και BS04 που προκύπτουν από σχετικά ZK-πρωτόκολλα με μετατροπή σε NIZK σχήματα στο ROM μέσω τεχνικών Fiat-Shamir. Στη συνέχεια επικεντρωθήκαμε σε σχήματα ομαδικών υπογραφών στο standard μοντέλο. Ειδικότερα, αναλύσαμε το σχήμα BW06 που μαζί με τα Gr06, BW07 μπορεί να εκληφθεί ως προπομπός των σχημάτων ομαδικών υπογραφών που είναι εφαρμογές στιγμιοτύπων του GSPS. Από τα τελευταία, επιλέξαμε να δείξουμε τα σχήματα Gro07, LCSL07, τις BU-VLR-ομαδικές υπογραφές LV09 και τις πολύ πρόσφατες scalable ομαδικές υπογραφές με μηχανισμό ανάκλησης LPY12.

Πέραν αυτών που αναφέρθηκαν κατά την πρόοδο του κεφαλαίου, ορισμένα αξιοσημείωτα σχήματα στο standard μοντέλο από την κρυπτογραφία ζευγμάτων είναι οι VLR-ομαδικές υπογραφές βάσει ταυτοτήτων των L.Ibraimi κ.ά. [INHJ10], οι ομαδικές υπογραφές με *πλήρη forward ασφάλεια* των B.Libert M.Yung [LY10]

και οι *unique* ομαδικές υπογραφές των M.Franklin και H.Zhang [FZ12], όπου δύο υπογραφές στο ίδιο μήνυμα από την ίδιο χρήστη έχουν ένα σημαντικό κοινό μέρος. Όσον αφορά επεκτάσεις της έννοιας των ομαδικών υπογραφών, έχουμε τις ομαδικές υπογραφές με διαβάθμιση της ανωνυμίας των μελών από τους X.Boyen και C.Delerablée [BD08] και τις ανιχνεύσιμες υπογραφές των B.Libert και M.Yung [LY09]. Το εύρος των σχημάτων με ασφάλεια στο ROM είναι πολύ μεγαλύτερο. Μία πρώτου επιπέδου αναφορά στη βιβλιογραφία περιλαμβάνει τα [KY05], [DP06], [Kha07].

4.9 Εφαρμογές - Συμπεράσματα

Γενικό συμπέρασμα είναι πως μέχρι σήμερα, από όσον γνωρίζουμε, δεν έχει εμφανιστεί κάποιο σχήμα ομαδικών υπογραφών που να αποτελεί σε κάθε περίπτωση την απόλυτα ισορροπημένη επιλογή. Ακόμα και με την προσθήκη του συστήματος απόδειξης Groth-Sahai ως εργαλείο, τα σχήματα που αποφεύγουν τη χρήση τυχαίων μαντείων και ως εκ τούτου επιτυγχάνουν υψηλότερη θεωρητική ασφάλεια, φαίνεται να υστερούν σε λειτουργικότητα. Εάν μάλιστα ληφθεί υπόψη και η αποτελεσματική ανάκληση των μελών, οι επιλογές περιορίζονται ακόμα περισσότερο.

Τα παραπάνω δε σημαίνουν βέβαια ότι οι ομαδικές υπογραφές από την κρυπτογραφία ζευγμάτων δε βρίσκουν εφαρμογή, απλώς ότι επιβάλλεται κάθε φορά να τεθούν σε προτεραιότητα οι ιδιότητες που μας ενδιαφέρουν. Στα αναπτυσσόμενα δίκτυα κυκλοφορίας οχημάτων (*vehivular ad hoc networks -VANETs*), οι ομαδικές υπογραφές BBS04 μπορούν να χρησιμοποιηθούν για την επικοινωνία μεταξύ των οχήματων-μελών της ad hoc κατασκευασμένης ομάδας, χωρίς να αποκαλύπτονται προσωπικά δεδομένα όπως η πινακίδα ή η θέση του οχήματος [LSHS07], [SSBP09]. Τα VANETs είναι δίκτυα που απαιτούν υπολογιστική ταχύτητα και έτσι οι σύντομες υπογραφές BBS04 προτιμήθηκαν αρχικά σε σχέση με κάποιο ασφαλέστερο αλλά δυσλειτουργικό σχήμα, αν και τεχνικές δυσκολίες όπως η διαχείριση των οχημάτων που εγκαταλείπουν την ομάδα και του τρόπου επιλογής του GM καθιστούν μέχρι στιγμής επιφυλακτικούς τους σχεδιαστές VANET πρωτοκόλλων στη χρήση ομαδικών υπογραφών. Οι υπογραφές BBS04 και BS04 αποτελούν επίσης βασικά δομικά στοιχεία σε σχήματα *άμεσης ανώνυμης επικύρωσης* (*direct anonymous attestation - DAA*), μία κατηγορία υπογραφών που επιτρέπει την πιστοποίηση γνησιότητας hardware στα πλαίσια των απαιτήσεων του Trusted Computing Group. Τα νέα αυτά σχήματα [BL09], [Che10], μαζί και με άλλα σχήματα DAA από την κρυπτογραφία ζευγμάτων και ελλειπτικών καμπυλών, έχοντας μικρότερα μήκη κλειδιών και υπογραφής, φιλοδοξούν να αντικαταστήσουν το standard σχήμα ISO/IEC 11889 που βασιζεται στην ισχυρή υπόθεση RSA. BU-VLR-ομαδικές υπογραφές, όπως οι NF05, εχούν προταθεί σε πρωτόκολλα αυθεντικοποίησης για ασύρματα

δίκτυα [FNH+06], [HBC+11]. Ιδιότητες παρεμφερείς με των ομαδικών υπογραφών συναντούμε σε σχήματα e-cash τόσο στο ROM [CHL05], όσο και στο standard μοντέλο [FPV09].

Σε εφαρμογές που στοχεύουν σε ομάδες μικρότερης κλίμακας, η χρήση ενός σχήματος στο standard μοντέλο είναι πιο εφικτή. Πολλές φορές μπορεί να επιβάλλεται εάν η θεωρητική ασφάλεια είναι το κύριο ζητούμενο. Για παράδειγμα, σε έναν μειοδοτικό διαγωνισμό για την ανάθεση ενός έργου, οι ενδιαφερόμενες εταιρείες απαρτίζουν μία ομάδα, πιθανότατα χωρίς αμοιβαία εμπιστοσύνη, και οι προσφορές τους μπορούν να υπογράφονται ανώνυμα. Σε αυτήν την περίπτωση, η πλήρης ανώνυμία του σχήματος Gro07 αντισταθμίζει τη βραδύτητά του. Στο χώρο μίας εταιρείας, ο διευθύνων σύμβουλος ενός τμήματος μπορεί να εκτελέσει συγκεντρωτικά το ρόλο του GM και του διανομέα ιδιωτικών κλειδιών, όπως στο μοντέλο BMW03 και ειδικότερα τις υπογραφές BW06, BW07. Το ίδιο ισχύει και για όποια εφαρμογή η ιεραρχία είναι προκαθορισμένη από τις ιδιότητες των χρηστών του σχήματος. Σε μία άλλη κατηγορία υλοποιήσεων, οι X.Liang κ.ά. [LLC+11] χρησιμοποιούν τις υπογραφές LCSL07 για την κατασκευή σχήματος κλήσεων επείγουσας ιατρικής βοήθειας με προστασία των προσωπικών δεδομένων των ασθενών.

Την τελευταία δεκαετία, οι μελετητές έχουν εντρυφήσει στην μοντελοποίηση πολλών ειδών ομαδικών υπογραφών και της ανάλογης ασφάλειάς τους. Το εύρος που εμφανίζει η αντίστοιχη βιβλιογραφία έχει ήδη θέσει ισχυρές βάσεις για περαιτέρω έρευνα στον τομέα. Ως εκ τούτου, δημιουργείται η εντύπωση πως για να ισχυροποιηθεί σημαντικά η θέση των ομαδικών υπογραφών στην κρυπτογραφία ζευγμάτων και γενικότερα στην ασύμμετρη κρυπτογραφία, χρειάζεται μία πιο γενική θεώρηση των παραμέτρων που καθορίζουν την αποδοτικότητα και την αξιοπιστία τους. Οι τεχνικές broadband κρυπτογράφησης που εφαρμόστηκαν στο μηχανισμό ανάκλησης των υπογραφών LPY12 είναι σίγουρα ένα βήμα προς αυτή την κατεύθυνση. Σε πρώτο βαθμό είναι αναγκαίο να αναζητηθούν σχήματα των οποίων η ασφάλεια βασίζεται αποκλειστικά σε ευρέως αποδεκτές υποθέσεις (π.χ. CDH, CBDH, Dlin q-SDH), αντί να εκμαιεύεται από διαρκώς νέες και ισχυρότερες των καθιερωμένων. Επίσης, να επινοηθούν καινούρια στιγμιότυπα του GSPS για ασύμμετρα ζεύγματα, που να περιορίζουν το πλήθος των υπολογισμών ζεύγματος που απαιτούνται στα στιγμιότυπα SXDH και SDlin, ώστε να βελτιωθούν οι επιδόσεις σχημάτων στο standard μοντέλο, και κυρίως οι σταθερές κόστους. Είναι προφανές πως ένα νέο μη διαλογικό σύστημα απόδειξης, το οποίο θα είναι αποδοτικότερο του GSPS, θα δώσει τεράστια ώθηση. Ακόμα και έτσι όμως, ο βασικότερος λόγος δυστοκίας δεν είναι άλλος από το θεμελιώδες ζήτημα του χρόνου υπολογισμού των ζευγμάτων. Πιθανόν η λύση να δοθεί σύντομα μέσω μεθόδων παράλληλου υπολογισμού όπως στο ROM [AKMRH11] (βλ. §1.5). Σίγουρα πάντως, μέχρι αυτό να συμβεί, ο θεω-

ρητικός σχεδιασμός λειτουργικών και ασφαλών σχημάτων ομαδικών υπογραφών με όσο το δυνατόν λιγότερους επίπονους υπολογισμούς θα έχει προετοιμάσει το έδαφος για την εδραίωση αυτού του πολύ ενδιαφέροντος εργαλείου στον κόσμο των εφαρμογών.

Βιβλιογραφία

[Ζάχ07] Ζάχος, Ε.: *Σημειώσεις στη Θεωρία Αριθμών και την Κρυπτογραφία*, 2007.

[ACHdM05] Ateniese, G., J. Camenisch, S. Hohenberger, και B. de Medeiros: *Practical group signatures without random oracles.* IACR Cryptology ePrint Archive, 2005:385, 2005.

[ACJT00] Ateniese, G., J. Camenisch, M. Joye, και G. Tsudik: *A practical and provably secure coalition-resistant group signature scheme.* Στο *Advances in Cryptology - CRYPTO 2000, Proceedings*, τόμος 1880 του *Lecture Notes in Computer Science*, σελίδες 255–270. Springer, 2000.

[AFG+10] Abe, M., G. Fuchsbauer, J. Groth, K. Haralambiev, και M. Ohkubo: *Structure-preserving signatures and commitments to group elements.* Στο *Advances in Cryptology - CRYPTO 2010, Proceedings*, τόμος 6223 του *Lecture Notes in Computer Science*, σελίδες 209–236. Springer, 2010.

[AHO10] Abe, M., K. Haralambiev, και M. Ohkubo: *Signing on elements in bilinear groups for modular protocol design.* IACR Cryptology ePrint Archive, 2010:133, 2010.

[AKL+11] Aranha, D. F., K. Karabina, P. Longa, C. H. Gebotys, και J. López: *Faster explicit formulas for computing pairings over ordinary curves.* Στο *Advances in Cryptology - EUROCRYPT 2011, Proceedings*, τόμος 6632 του *Lecture Notes in Computer Science*, σελίδες 48–68. Springer, 2011.

[AKMRH11] Aranha, D. F., E. Knapp, A. Menezes, και F. Rodríguez-Henríquez: *Parallelizing the Weil and Tate pairings.* Στο *Cryptography and Coding - 13th IMA International Conference, IMACC 2011, Proceedings*, τόμος 7089 του *Lecture Notes in Computer Science*, σελίδες 275–295. Springer, 2011.

[ARP02] Al-Riyami, S. S. και K. G. Paterson: *Tripartite authenticated key agreement protocols from pairings.* IACR Cryptology ePrint Archive, 2002:35, 2002.

[ARP03] Al-Riyami, S. S. και K. G. Paterson: *Certificateless public key cryptography.* IACR Cryptology ePrint Archive, 2003:126, 2003.

[ARP05] Al-Riyami, S. S. και K. G. Paterson: *CBE from CL-PKE: A generic construction and efficient schemes.* Στο *Public Key Cryptography - PKC 2005, Proceedings*, τόμος 3386 του *Lecture Notes in Computer Science*, σελίδες 398–415. Springer, 2005.

[AST01] Ateniese, G., D. Song, και G. Tsudik: *Quasi-efficient revocation of group signatures.* IACR Cryptology ePrint Archive, 2001:101, 2001.

[BB04a] Boneh, D. και X. Boyen: *Efficient selective-ID secure identity-based encryption without random oracles.* Στο *Advances in Cryptology - EUROCRYPT 2004, Proceedings*, τόμος 3027 του *Lecture Notes in Computer Science*, σελίδες 223–238. Springer, 2004.

[BB04b] Boneh, D. και X. Boyen: *Secure identity based encryption without random oracles.* Στο *Advances in Cryptology - CRYPTO 2004, Proceedings*, τόμος 3152 του *Lecture Notes in Computer Science*, σελίδες 443–459. Springer, 2004.

[BB04c] Boneh, D. και X. Boyen: *Short signatures without random oracles.* Στο *Advances in Cryptology - EUROCRYPT 2004, Proceedings*, τόμος 3027 του *Lecture Notes in Computer Science*, σελίδες 56–73. Springer, 2004.

[BBG05] Boneh, D., X. Boyen, και E. J. Goh: *Hierarchical identity based encryption with constant size ciphertext.* IACR Cryptology ePrint Archive, 2005:15, 2005.

[BBS04] Boneh, D., X. Boyen, και H. Shacham: *Short group signatures.* Στο *Advances in Cryptology - CRYPTO 2004, Proceedings*, τόμος 3152 του *Lecture Notes in Computer Science*, σελίδες 41–55. Springer, 2004.

[BCC+09] Belenkiy, M., J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, και H. Shacham: *Randomizable proofs and delegatable anonymous credentials.* Στο *Advances in Cryptology - CRYPTO 2009, 2009. Proceedings*, τόμος 5677 του *Lecture Notes in Computer Science*, σελίδες 108–125. Springer, 2009.

[BCKL08] Belenkiy, M., M. Chase, M. Kohlweiss, και A. Lysyanskaya: *P-signatures and noninteractive anonymous credentials.* Στο *Theory of Cryptography - TCC 2008*, τόμος 4948 του *Lecture Notes in Computer Science*, σελίδες 356–374. Springer, 2008.

[BCKL09] Belenkiy, M., M. Chase, M. Kohlweiss, και A. Lysyanskaya: *Compact E-Cash and simulatable VRFs revisited.* Στο *Pairing-Based Cryptography - PAIRING 2009, Proceedings*, τόμος 5671 του *Lecture Notes in Computer Science*, σελίδες 114–131. Springer, 2009.

[BD08] Boyen, X. και C. Delerablée: *Expressive subgroup signatures.* Στο *Security and Cryptography for Networks, 6th International Conference - SCN 2008, Proceedings*, τόμος 5229 του *Lecture Notes in Computer Science*, σελίδες 185–200. Springer, 2008.

[BDPR98] Bellare, M., A. Desai, D. Pointcheval, και P. Rogaway: *Relations among notions of security for public-key encryption schemes.* Στο *Advances in Cryptology - CRYPTO 1998, Proceedings*, τόμος 1462 του *Lecture Notes in Computer Science*, σελίδες 26–45. Springer, 1998.

[BEF03] Brown, E., E. Errthum, και D. Fu: *Weil pairing vs. Tate pairing in IBE systems.* Technical Report, 2003.

[BF01] Boneh, D. και M. K. Franklin: *Identity-based encryption from the Weil pairing.* Στο *Advances in Cryptology - CRYPTO 2001, Proceedings*, τόμος 2139 του *Lecture Notes in Computer Science*, σελίδες 213–229. Springer, 2001.

[BF03] Boneh, D. και M. K. Franklin: *Identity-based encryption from the Weil pairing.* SIAM Journal of Computing, 32(3):586–615, 2003.

[BF08] Barbosa, M. και P. Farshim: *Certificateless signcryption.* Στο *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008*, σελίδες 369–372. ACM, 2008.

[BFI+10] Blazy, O., G. Fuchsbauer, M. Izabachène, A. Jambert, H. Sibert, και D. Vergnaud: *Batch Groth-Sahai.* IACR Cryptology ePrint Archive, 2010:40, 2010.

[BFM88] Blum, M., P. Feldman, και S. Micali: *Non-interactive zero-knowledge and its applications (extended abstract).* Στο *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, σελίδες 103–112. ACM, 1988.

[BGDM+10] Beuchat, J. L., J. E. González-Díaz, S. Mitsunari, E. Okamoto, F. Rodríguez-Henríquez, και T. Teruya: *High-speed software implementation of the optimal Ate pairing over Barreto-Naehrig curves.* Στο *Pairing-Based Cryptography - Pairing 2010, Proceedings*, τόμος 6487 του *Lecture Notes in Computer Science*, σελίδες 21–39. Springer, 2010.

[BGhS04] Barreto, P. S. L. M., S. D. Galbraith, C. O. hEigeartaigh, και M. Scott: *Efficient pairing computation on supersingular Abelian varieties.* IACR Cryptology ePrint Archive, 2004:375, 2004.

[BGLS03] Boneh, D., C. Gentry, B. Lynn, και H. Shacham: *Aggregate and verifiably encrypted signatures from bilinear maps.* Στο *Advances in Cryptology - EUROCRYPT 2003, Proceedings*, τόμος 2656 του *Lecture Notes in Computer Science*, σελίδες 416–432. Springer, 2003.

[BGN05] Boneh, D., E. J. Goh, και K. Nissim: *Evaluating 2-DNF formulas on ciphertexts.* Στο *Theory of Cryptography, Second Theory of Cryptography Conference - TCC 2005, Proceedings*, τόμος 3378 του *Lecture Notes in Computer Science*, σελίδες 325–341. Springer, 2005.

[BGR98] Bellare, M., J. A. Garay, και T. Rabin: *Fast batch verification for modular exponentiation and digital signatures.* Στο *Advances in Cryptology - EUROCRYPT 1998, Proceedings*, τόμος 1403 του *Lecture Notes in Computer Science*, σελίδες 236–250. Springer, 1998.

[BK98] Balasubramanian, R. και N. Koblitz: *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone algorithm.* Journal of Cryptology, 11(2):141–145, 1998.

[BKLS02] Barreto, P. S. L. M., H. Y. Kim, B. Lynn, και M. Scott: *Efficient algorithms for pairing-based cryptosystems.* Στο *Advances in Cryptology - CRYPTO 2002, Proceedings*, τόμος 2442 του *Lecture Notes in Computer Science*, σελίδες 354–368. Springer, 2002.

[BL09] Brickell, E. και J. Li: *Enhanced privacy ID from bilinear pairing.* IACR Cryptology ePrint Archive, 2009:95, 2009.

[BLS01] Boneh, D., B. Lynn, και H. Shacham: *Short signatures from the Weil pairing.* Στο *Advances in Cryptology - ASIACRYPT 2001, Proceedings*, τόμος 2248 του *Lecture Notes in Computer Science*, σελίδες 514–532. Springer, 2001.

[BLS03a] Barreto, P. S. L. M., B. Lynn, και M. Scott: *On the selection of pairing-friendly groups.* IACR Cryptology ePrint Archive, 2003:86, 2003.

[BLS03b] Barretto, P. S. L. M., B. Lynn, και M. Scott: *Constructing elliptic curves with prescribed embedding degrees.* Στο *Proceedings of the Third Workshop on Security in Communications Networks, SCN 2002*, τόμος 2576 του *Lecture Notes in Computer Science*, σελίδες 257–267. Springer-Verlag, 2003.

[BLS03c] Boneh, D., B. Lynn, και H. Shacham: *Short signatures from the Weil pairing*, 2003. Διορθωμένη έκδοση του [BLS01].

[BMW03] Bellare, M., D. Micciancio, και B. Warinschi: *Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions.* Στο *Advances in Cryptology - EUROCRYPT 2003, Proceedings*, τόμος 2656 του *Lecture Notes in Computer Science*, σελίδες 614–629. Springer, 2003.

[BN05] Barreto, P. S. L. M. και M. Naehrig: *Pairing-friendly elliptic curves of prime order.* IACR Cryptology ePrint Archive, 2005:133, 2005.

[BNN06] Bellare, M., C. Namprempre, και G. Neven: *Unrestricted aggregate signatures.* IACR Cryptology ePrint Archive, 2006:285, 2006.

[Bol02] Boldyreva, A.: *Efficient threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman-group signature scheme.* IACR Cryptology ePrint Archive, 2002:118, 2002.

[BP11] Bringer, J. και A. Patey: *Backward unlinkability for a VLR group signature scheme with efficient revocation check.* IACR Cryptology ePrint Archive, 2011:376, 2011.

[BR93] Bellare, M. και P. Rogaway: *Random oracles are practical: A paradigm for designing efficient protocols.* Στο *Proceedings of the 1st ACM Conference on Computer and Communications Security - CCS 93*, σελίδες 62–73. ACM, 1993.

[Bri03] Brickell, E.: *An efficient protocol for anonymously providing assurance of the container of a private key.* Υποβεβλημένο στο the Trusted Computing Group, 2003.

[BS01] Bresson, E. και J. Stern: *Efficient revocation in group signatures.* Στο *Public Key Cryptography - PKC 2001, Proceedings*, τόμος 1992 του *Lecture Notes in Computer Science*, σελίδες 190–206. Springer, 2001.

[BS04] Boneh, D. και H. Shacham: *Group signatures with verifier-local revocation.* Στο *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004*, σελίδες 168–177. ACM, 2004.

[BSMP91] Blum, M., A. De Santis, S. Micali, και G. Persiano: *Noninteractive zero-knowledge.* SIAM Journal of Computing, 20(6):1084–1118, 1991.

[BSS99] Blake, I., G. Seroussi, και N. P. Smart: *Elliptic Curves in Cryptography.* Cambridge University Press, 1999.

[BSS05] Blake, I., G. Seroussi, και N. P. Smart: *Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.

[BSW11] Boyle, E., G. Segev, και D. Wichs: *Fully leakage-resilient signatures*. Στο *Advances in Cryptology - EUROCRYPT 2011, Proceedings*, τόμος 6632 του *Lecture Notes in Computer Science*, σελίδες 89–108. Springer, 2011.

[BSZ05] Bellare, M., H. Shi, και C. Zhang: *Foundations of group signatures: The case of dynamic groups*. Στο *Topics in Cryptology - CT-RSA 2005, Proceedings*, τόμος 3376 του *Lecture Notes in Computer Science*, σελίδες 136–153. Springer, 2005.

[BW06] Boyen, X. και B. Waters: *Compact group signatures without random oracles*. Στο *Advances in Cryptology - EUROCRYPT 2006, Proceedings*, τόμος 4004 του *Lecture Notes in Computer Science*, σελίδες 427–444. Springer, 2006.

[BW07] Boyen, X. και B. Waters: *Full-domain subgroup hiding and constant-size group signatures*. Στο *Public Key Cryptography - PKC 2007, Proceedings*, τόμος 4450 του *Lecture Notes in Computer Science*, σελίδες 1–15. Springer, 2007.

[CC03] Cha, J. C. και J. H. Cheon: *An identity-based signature from gap Diffie-Hellman groups*. Στο *Public Key Cryptography - PKC 2003, Proceedings*, τόμος 2567 του *Lecture Notes in Computer Science*, σελίδες 18–30. Springer, 2003.

[CGH98] Canetti, R., O. Goldreich, και S. Halevi: *The random oracle methodology, revisited (preliminary version)*. Στο *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing - STOC 1998*, σελίδες 209–218. ACM, 1998.

[Che10] Chen, L.: *A DAA scheme requiring less TPM resources*. IACR Cryptology ePrint Archive, 2010:8, 2010.

[CHK03] Canetti, R., S. Halevi, και J. Katz: *A forward-secure public-key encryption scheme*. Στο *Advances in Cryptology - EUROCRYPT 2003, Proceedings*, τόμος 2656 του *Lecture Notes in Computer Science*, σελίδες 255–271. Springer, 2003.

[CHL05] Camenisch, J., S. Hohenberger, και A. Lysyanskaya: *Compact E-Cash*. Στο *Advances in Cryptology - EUROCRYPT 2005, Proceedings*, τόμος 3494 του *Lecture Notes in Computer Science*, σελίδες 302–321. Springer, 2005.

[CHSS02] Chen, L., K. Harrison, D. Soldera, και N. P. Smart: *Applications of multiple trust authorities in pairing based cryptosystems.* Στο *Infrastructure Security, International Conference - InfraSec 2002, Proceedings*, τόμος 2437 του *Lecture Notes in Computer Science*, σελίδες 260–275. Springer, 2002.

[CKS09] Camenisch, J., M. Kohlweiss, και C. Soriente: *An accumulator based on bilinear maps and efficient revocation for anonymous credentials.* Στο *Public Key Cryptography - PKC 2009, Proceedings*, τόμος 5443 του *Lecture Notes in Computer Science*, σελίδες 481–500. Springer, 2009.

[CL02] Camenisch, J. και A. Lysyanskaya: *Dynamic accumulators and application to efficient revocation of anonymous credentials.* Στο *Advances in Cryptology - CRYPTO 2002, Proceedings*, τόμος 2442 του *Lecture Notes in Computer Science*, σελίδες 61–76. Springer, 2002.

[CL04] Camenisch, J. και A. Lysyanskaya: *Signature schemes and anonymous credentials from bilinear maps.* Στο *Advances in Cryptology - CRYPTO 2004, Proceedings*, τόμος 3152 του *Lecture Notes in Computer Science*, σελίδες 56–72. Springer, 2004.

[CL10] Chen, L. και J. Li: *VLR group signatures with indisputable exculpability and efficient revocation.* Στο *Proceedings of SocialCom/PASSAT 2010*, σελίδες 727–734. IEEE Computer Society, 2010.

[Coc01] Cocks, C.: *An identity based encryption scheme based on quadratic residues.* Στο *Cryptography and Coding, 8th IMA International Conference, Proceedings*, τόμος 2260 του *Lecture Notes in Computer Science*, σελίδες 360–363. Springer, 2001.

[CP94] Chen, L. και T. P. Pedersen: *New group signature schemes (extended abstract).* Στο *Advances in Cryptology - EUROCRYPT 1994, Proceedings*, τόμος 950 του *Lecture Notes in Computer Science*, σελίδες 171–181. Springer, 1994.

[CvH91] Chaum, D. και E. van Heyst: *Group signatures.* Στο *Advances in Cryptology - EUROCRYPT 1991, Proceedings*, τόμος 547 του *Lecture Notes in Computer Science*, σελίδες 257–265. Springer, 1991.

[DCC05] Duan, P., S. Cui, και C.W. Chan: *Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems.* Preprint, Cryptology ePrint Archive, 2005:342, 2005.

[DE02] Dupont, R. και A. Enge: *Practical non-interactive key distribution based on pairings.* IACR Cryptology ePrint Archive, 2002:136, 2002.

[DEM02] Dupont, R., A. Enge, και F. Morain: *Building curves with arbitrary small MOV degree over finite prime fields.* IACR Cryptology ePrint Archive, 2002:94, 2002.

[DF02] Dodis, Y. και N. Fazio: *Public key broadcast encryption for stateless receivers.* Στο *Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop - DRM 2002*, τόμος 2696 του *Lecture Notes in Computer Science*, σελίδες 61–80. Springer, 2002.

[DNS98] Dwork, C., M. Naor, και A. Sahai: *Concurrent zero-knowledge.* Στο *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing - STOC 1998*, σελίδες 409–418. ACM, 1998.

[DP06] Delerablée, C. και D. Pointcheval: *Dynamic fully anonymous short group signatures.* Στο *Progressin Cryptology - VIETCRYPT 2006, Revised Selected Papers*, τόμος 4341 του *Lecture Notes in Computer Science*, σελίδες 193–210. Springer, 2006.

[FFS88] Feige, U., A. Fiat, και A. Shamir: *Zero-knowledge proofs of identity.* Journal of Cryptology, 1(2):77–94, 1988.

[FGHP09] Ferrara, A. L., M. Green, S. Hohenberger, και M. Ø. Pedersen: *Practical short signature batch verification.* Στο *Topics in Cryptology - CT-RSA 2009, Proceedings*, τόμος 5473 του *Lecture Notes in Computer Science*, σελίδες 309–324. Springer, 2009.

[FHM11] Fan, C. I, R. H. Hsu, και M. Manulis: *Group signature with constant revocation costs for signers and verifiers.* Στο *Cryptology and Network Security, 10th International Conference - CANS 2011, Proceedings*, τόμος 7092 του *Lecture Notes in Computer Science*, σελίδες 214–233. Springer, 2011.

[FLS90] Feige, U., D. Lapidot, και A. Shamir: *Multiple non-interactive zero knowledge proofs based on a single random string (extended abstract).* Στο *31st Annual Symposium on Foundations of Computer Science - FOCS 1990, Volume I*, σελίδες 308–317. IEEE Computer Society, 1990.

[FMR99] Frey, G., M. Müller, και H. G. Rück: *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems.* IEEE Transactions on Information Theory, 45(5):1717–1719, 1999.

[FNH+06] Funabiki, N., T. Nakanishi, H.Takahashi, K. Miki, και J. Kawashima: *A proposal of anonymous IEEE802.1X authentication protocol for wireless networks.* IEEE Workshop on Secure Network Protocols, σελίδες 26–31, 2006.

[FO99] Fujisaki, E. και T. Okamoto: *Secure integration of asymmetric and symmetric encryption schemes.* Στο *Advances in Cryptology - CRYPTO 1999 Proceedings*, τόμος 1666 του *Lecture Notes in Computer Science*, σελίδες 537–554. Springer, 1999.

[FPV09] Fuchsbauer, G., D. Pointcheval, και D. Vergnaud: *Transferable constant-size fair E-Cash.* Στο *Cryptology and Network Security, 8th International Conference - CANS 2009, Proceedings*, τόμος 5888 του *Lecture Notes in Computer Science*, σελίδες 226–247. Springer, 2009.

[FR94] Frey, G. και H. G. Rück: *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves.* Mathematics of Computation, 62(206):865–874, 1994.

[FS86] Fiat, A. και A. Shamir: *How to prove yourself: Practical solutions to identification and signature problems.* Στο *Advances in Cryptology - CRYPTO 1986, Proceedings*, τόμος 263 του *Lecture Notes in Computer Science*, σελίδες 186–194. Springer, 1986.

[FS90] Feige, U. και A. Shamir: *Witness indistinguishable and witness hiding protocols.* Στο *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing - STOC 1990*, σελίδες 416–426. ACM, 1990.

[FST06] Freeman, D., M. Scott, και E. Teske: *A taxonomy of pairing-friendly elliptic curves.* IACR Cryptology ePrint Archive, 2006:372, 2006.

[FZ12] Franklin, M. K. και H. Zhang: *Unique group signatures.* IACR Cryptology ePrint Archive, 2012:204, 2012.

[Gal01] Galbraith, S. D.: *Supersingular curves in cryptography.* Στο *Advances in Cryptology - ASIACRYPT 2001, Proceedings*, τόμος 2248 του *Lecture Notes in Computer Science*, σελίδες 495–513. Springer, 2001.

[GB08] Goldwasser, S. και M. Bellare: *Lecture notes on cryptography*, 2008.

[Gen06] Gentry, C.: *Practical identity-based encryption without random oracles.* Στο *Advances in Cryptology - EUROCRYPT 2006, Proceedings*, τόμος 4004 του *Lecture Notes in Computer Science*, σελίδες 445–464. Springer, 2006.

[GHO+07] Granger, R., F. Hess, R. Oyono, N. Thériault, και F. Vercauteren: *Ate pairing on hyperelliptic curves.* Στο *Advances in Cryptology - EUROCRYPT 2007, Proceedings*, τόμος 4515 του *Lecture Notes in Computer Science*, σελίδες 430–447. Springer, 2007.

[GHS02] Galbraith, S. D., K. Harrison, και D. Soldera: *Implementing the Tate pairing.* Στο *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Proceedings*, τόμος 2369 του *Lecture Notes in Computer Science*, σελίδες 324–337. Springer, 2002.

[GHV07] Galbraith, S. D., F. Hess, και F. Vercauteren: *Hyperelliptic pairings.* Στο *Pairing-Based Cryptography - PAIRING 2007, Proceedings*, τόμος 4575 του *Lecture Notes in Computer Science*, σελίδες 108–131. Springer, 2007.

[GK96] Goldreich, O. και H. Krawczyk: *On the composition of zero-knowledge proof systems.* SIAM Journal of the Computing, 25(1):169–192, 1996.

[GMR85] Goldwasser, S., S. Micali, και C. Rackoff: *The knowledge complexity of interactive proof-systems (extended abstract).* Στο *Proceedings of the 17th Annual ACM Symposium on Theory of Computing - STOC 1985*, σελίδες 291–304. ACM, 1985.

[GMW86] Goldreich, O., S. Micali, και A. Wigderson: *Proofs that yield nothing but their validity and a methodology of cryptographic protocol design (extended abstract).* Στο *27th Annual Symposium on Foundations of Computer Science - FOCS 1986*, σελίδες 174–187. IEEE Computer Society, 1986.

[GO94] Goldreich, O. και Y. Oren: *Definitions and properties of zero-knowledge proof systems.* Journal of Cryptology, 7(1):1–32, 1994.

[Gol01] Goldreich, O.: *The Foundations of Cryptography - Volume 1: Basic Tools.* Cambridge University Press, 2001, ISBN 0-521-83084-2.

[GOS06a] Groth, J., R. Ostrovsky, και A. Sahai: *Non-interactive Zaps and new techniques for NIZK.* Στο *Advances in Cryptology - CRYPTO 2006, Proceedings*, τόμος 4117 του *Lecture Notes in Computer Science*, σελίδες 97–111. Springer, 2006.

[GOS06b] Groth, J., R. Ostrovsky, και A. Sahai: *Perfect non-interactive zero knowledge for NP.* Στο *Advances in Cryptology - EUROCRYPT 2006, Proceedings*, τόμος 4004 του *Lecture Notes in Computer Science*, σελίδες 339–358. Springer, 2006.

[GPS08] Galbraith, S. D., K. G. Paterson, και N. P. Smart: *Pairings for cryptographers.* Discrete Applied Mathematics, 156(16):3113–3121, 2008.

[Gro06] Groth, J.: *Simulation-sound NIZK proofs for a practical language and constant size group signatures.* Στο *Advances in Cryptology - ASIACRYPT 2006, Proceedings*, σελίδες 444–459, 2006.

[Gro07] Groth, J.: *Fully anonymous group signatures without random oracles.* IACR Cryptology ePrint Archive, 2007:186, 2007.

[GS02] Gentry, C. και A. Silverberg: *Hierarchical ID-based cryptography.* Στο *Advances in Cryptology - ASIACRYPT 2002, Proceedings*, τόμος 2501 του *Lecture Notes in Computer Science*, σελίδες 548–566. Springer, 2002.

[GS07] Groth, J. και A. Sahai: *Efficient non-interactive proof systems for bilinear groups.* IACR Cryptology ePrint Archive, 2007:155, 2007.

[GS08] Groth, J. και A. Sahai: *Efficient non-interactive proof systems for bilinear groups.* Στο *Advances in Cryptology - EUROCRYPT 2008, Proceedings*, τόμος 4965 του *Lecture Notes in Computer Science*, σελίδες 415–432. Springer, 2008.

[GSW09] Ghadafi, E., N. P. Smart, και B. Warinschi: *Groth-Sahai proofs revisited.* IACR Cryptology ePrint Archive, 2009:599, 2009.

[GV11] Guillevic, A. και D. Vergnaud: *Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions.* IACR Cryptology ePrint Archive, 2011:604, 2011.

[HBC+11] He, D., J. Bu, S. Chan, C. Chen, και M. Yin: *Privacy-preserving universal authentication protocol for wireless communications.* IEEE Transactions on Wireless Communications, 10(2):431–436, 2011.

[Hes02] Hess, F.: *Exponent group signature schemes and efficient identity based signature schemes based on pairings.* IACR Cryptology ePrint Archive, 2002:12, 2002.

[Hes04] Hess, F.: *A note on the Tate pairing of curves over finite fields.* Archiv der Mathematik, 82(1):28–32, 2004.

[Hes08] Hess, F.: *Pairing lattices.* IACR Cryptology ePrint Archive, 2008:125, 2008.

[HMS08] Hankerson, D., A. Menezes, και M. Scott: *Software implementation of pairings.* Identity-Based Cryptography, 2:188–206, 2008.

[HSV06] Hess, F., N. P. Smart, και F. Vercauteren: *The Eta pairing revisited.* IACR Cryptology ePrint Archive, 2006:110, 2006.

[INHJ10] Ibraimi, L., S. Nikova, P. Hartel, και W. Joker: *An identity-based group signature with membership revocation in the standard model.* CTIT technical report series, University of Twente, 2010.

[Jou00] Joux, A.: *A one round protocol for tripartite Diffie-Hellman.* Στο *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, 2000, Proceedings*, τόμος 1838 του *Lecture Notes in Computer Science*, σελίδες 385–394. Springer, 2000.

[Kha07] Khader, D.: *Attribute based group signatures.* IACR Cryptology ePrint Archive, 2007:159, 2007.

[Kil06] Kiltz, E.: *Chosen-ciphertext security from tag-based encryption.* Στο *Theory of Cryptography, Third Theory of Cryptography Conference - TCC 2006, Proceedings*, τόμος 3876 του *Lecture Notes in Computer Science*, σελίδες 581–600. Springer, 2006.

[Kim07] Kiming, I.: *Elliptic Curves: various supplements*, 2007. Σημειώσεις διαλέξεων.

[KT08] Kawazoe, M. και T. Takahashi: *Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$.* Στο *Pairing-Based Cryptography - PAIRING 2008, Proceedings*, τόμος 5209 του *Lecture Notes in Computer Science*, σελίδες 164–177. Springer, 2008.

[KTY04] Kiayias, A., Y. Tsiounis, και M. Yung: *Traceable signatures.* Στο *Advances in Cryptology - EUROCRYPT 2004, Proceedings*, τόμος 3027 του *Lecture Notes in Computer Science*, σελίδες 571–589. Springer, 2004.

[Kun05] Kunz, E.: *Introduction to Plane Algebraic Curves.* Birkhäuser, 2005.

[KY04] Kiayias, A. και M. Yung: *Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders.* IACR Cryptology ePrint Archive, 2004:76, 2004.

[KY05] Kiayias, A. και M. Yung: *Group signatures with efficient concurrent join.* IACR Cryptology ePrint Archive, 2005:345, 2005.

[LCSL07] Liang, X., Z. Cao, J. Shao, και H. Lin: *Short group signature without random oracles.* IACR Cryptology ePrint Archive, 2007:450, 2007.

[LLC+11] Liang, X., R. Lu, L. Chen, X. Lin, και X. Shen: *PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks.* Journal of Communications and Networks, 13(2):102–112, 2011.

[LLP08] Lee, E., H. S. Lee, και C. M. Park: *Efficient and generalized pairing computation on Abelian varieties.* IACR Cryptology ePrint Archive, 2008:40, 2008.

[LPY12a] Libert, B., T. Peters, και M. Yung: *Scalable group signatures with revocation.* Στο *Advances in Cryptology - EUROCRYPT 2012, Proceedings*, τόμος 7237 του *Lecture Notes in Computer Science*, σελίδες 609–627. Springer, 2012.

[LPY12b] Libert, B., T. Peters, και M. Yung: *Scalable group signatures with revocation.* Διαθέσιμο στο http://perso.uclouvain.be/benoit.libert/rgsig-full-version.pdf, 2012.

[LQ03] Libert, B. και J. J. Quisquater: *Identity based undeniable signatures.* IACR Cryptology ePrint Archive, 2003:206, 2003.

[LQ04] Libert, B. και J. J. Quisquater: *Efficient signcryption with key privacy from gap Diffie-Hellman groups.* Στο *Public Key Cryptography - PKC 2004*, τόμος 2947 του *Lecture Notes in Computer Science*, σελίδες 187–200. Springer, 2004.

[LQ06] Libert, B. και J. J. Quisquater: *On constructing certificateless cryptosystems from identity based encryption.* Στο *Public Key Cryptography - PKC 2006, Proceedings*, τόμος 3958 του *Lecture Notes in Computer Science*, σελίδες 474–490. Springer, 2006.

[LSHS07] Lin, X., X. Sun, P. H. Ho, και X. Shen: *GSIS: A secure and privacy-preserving protocol for vehicular communications.* IEEE Transactions on Vehicular Technology, 56(6):3442–3456, 2007.

[LV09] Libert, B. και D. Vergnaud: *Group signatures with verifier-local revocation and backward unlinkability in the standard model.* Στο *Proceedings of Cryptology and Network Security, 8th International Conference - CANS 2009*, τόμος 5888 του *Lecture Notes in Computer Science*, σελίδες 498–517. Springer, 2009.

[LY09] Libert, B. και M. Yung: *Efficient traceable signatures in the standard model.* Στο *Pairing-Based Cryptography - PAIRING 2009, Proceedings*, τόμος 5671 του *Lecture Notes in Computer Science*, σελίδες 187–205. Springer, 2009.

[LY10] Libert, B. και M. Yung: *Dynamic fully forward-secure group signatures.* Στο *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security - ASIACCS 2010*, σελίδες 70–81. ACM, 2010.

[Lyn02] Lynn, B.: *Authenticated identity-based encryption.* IACR Cryptology ePrint Archive, 2002:072, 2002.

[Men93] Menezes, A. J.: *Elliptic Curve Public Key Cryptosystems.* Kluwer Academic Publishers, 1993.

[Mil86] Miller, V.: *Short programs for functions on curves.* Unpublished manuscript, 1986.

[MKHO07] Matsuda, S., N. Kanayama, F. Hess, και E. Okamoto: *Optimised versions of the Ate and twisted Ate pairings.* IACR Cryptology ePrint Archive, 2007:13, 2007.

[MNT01] Miyaji, A., M. Nakabayashi, και S. Takano: *New explicit conditions of elliptic curve traces for FR-reduction.* IEICE Transformations on Fundamentals, E84-A(5):1234–1243, 2001.

[MOV93] Menezes, A., T. Okamoto, και S. A. Vanstone: *Reducing elliptic curve logarithms to logarithms in a finite field.* IEEE Transactions on Information Theory, 39(5):1639–1646, 1993.

[MPB03] Mont, M. C., S. Pearson, και P. Bramhall: *Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services.* Στο *14th International Workshop on Database and Expert Systems Applications -DEXA 2003*, σελίδες 377–382. IEEE Computer Society, 2003.

[MSK02] Mitsunari, S., R. Sakai, και Masao Kasahara: *A new traitor tracing.* IEICE Transactions on Fundamentals, E85-A(2):481–484, 2002.

[MTVY10] Malkin, T., I. Teranishi, Y. Vahlis, και M. Yung: *Signatures resilient to continual leakage on memory and computation.* IACR Cryptology ePrint Archive, 2010:522, 2010.

[NF05] Nakanishi, T. και N. Funabiki: *Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps.* Στο *Advances in Cryptology - ASIACRYPT 2005, Proceedings*, τόμος 3788 του *Lecture Notes in Computer Science*, σελίδες 533–548. Springer, 2005.

[NF07] Nakanishi, T. και N. Funabiki: *A short verifier-local revocation group signature scheme with backward unlinkability.* IEICE Transactions, 90-A(9):1793–1802, 2007.

[NFHF09] Nakanishi, T., H. Fujii, Y. Hira, και N. Funabiki: *Revocable group signature schemes with constant costs for signing and verifying.* Στο *Public Key Cryptography - PKC 2009, Proceedings*, τόμος 5443 του *Lecture Notes in Computer Science*, σελίδες 463–480. Springer, 2009.

[NNL01] Naor, D., M. Naor, και J. Lotspiech: *Revocation and tracing schemes for stateless receivers.* Στο *Advances in Cryptology - CRYPTO 2001, Proceedings*, τόμος 2139 του *Lecture Notes in Computer Science*, σελίδες 41–62. Springer, 2001.

[NNS10] Naehrig, M., R. Niederhagen, και P. Schwabe: *New software speed records for cryptographic pairings.* Στο *Progress in Cryptology - LATINCRYPT 2010, Proceedings*, τόμος 6212 του *Lecture Notes in Computer Science*, σελίδες 109–123. Springer, 2010.

[NY90] Naor, M. και M. Yung: *Public-key cryptosystems provably secure against chosen ciphertext attacks.* Στο *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing - STOC 1990*, σελίδες 427–437. ACM, 1990.

[OP01] Okamoto, T. και D. Pointcheval: *The gap-problems: A new class of problems for the security of cryptographic schemes.* Στο *Public Key Cryptography - PKC 2001, Proceedings*, τόμος 1992 του *Lecture Notes in Computer Science*, σελίδες 104–118. Springer, 2001.

[Pas03] Pass, R.: *On deniability in the common reference string and random oracle model.* Στο *Advances in Cryptology - CRYPTO 2003, Proceedings*, τόμος 2729 του *Lecture Notes in Computer Science*, σελίδες 316–337. Springer, 2003.

[Pat02a] Paterson, K. G.: *Cryptography from pairings: a snapshot of current research.* Information Security Technical Repor, 7(2):41–54, 2002.

[Pat02b] Paterson, K. G.: *ID-based signatures from pairings on elliptic curves.* IACR Cryptology ePrint Archive, 2002:4, 2002.

[PKO09] Phong, L. T., K. Kurosawa, και W. Ogata: *Provably secure convertible undeniable signatures with unambiguity.* IACR Cryptology ePrint Archive, 2009:394, 2009.

[SBWP03] Steinfeld, R., L. Bull, H. Wang, και J. Pieprzyk: *Universal designated-verifier signatures.* IACR Cryptology ePrint Archive, 2003:192, 2003.

[Sco02] Scott, M.: *http://www.computing.dcu.ie/∼mike/tate.html*, 2002.

[Sha85] Shamir, A.: *Identity-based cryptosystems and signature schemes.* Στο *Advances in Cryptology - CRYPTO 1984, Proceedings*, τόμος 196 του *Lecture Notes in Computer Science*, σελίδες 47–53. Springer, 1985.

[Sha92] Shamir, A.: *IP = PSPACE.* Journal of the ACM, 39(4):869–877, 1992.

[Sil86] Silverman, J. H.: *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[Sma02] Smart, N. P.: *An identity based authenticated key agreement protocol based on the Weil pairing.* Electronics Letters, 38:630–632, 2002.

[SOK00] Sakai, R., K. Ohgishi, και M. Kasahara: *Cryptosystems based on pairing.* Στο *2000 Symposium on Cryptography and Information Security - SCIS 2000*, 2000.

[SOK01] Sakai, R., K. Ohgishi, και M. Kasahara: *Cryptosystems based on pairing over elliptic curve.* Στο *2001 Symposium on Cryptography and Information Security - SCIS 2001*, 2001.

[Son01] Song, D. X.: *Practical forward secure group signature schemes.* Στο *Proceedings of the 8th ACM Conference on Computer and Communications Security - CCS 2001*, σελίδες 225–234. ACM, 2001.

[SSBP09] Studer, A., E. Shi, F. Bai, και A. Perrig: *TACKing together efficient authentication, revocation, and privacy in VANETs.* Στο *Proceedings of SECON 2009*, σελίδες 1–9. IEEE, 2009.

[Ste94] Stepanov, S. A.: *Arithmetic of Algebraic Curves.* Consultants Bureau, 1994.

[Sti06] Stinson, D. R.: *Cryptography: Theory and Practice.* Chapman and Hall/CRC Press, 2006.

[SW05] Sahai, A. και B. Waters: *Fuzzy identity-based encryption.* Στο *Advances in Cryptology - EUROCRYPT 2005, Proceedings*, τόμος 3494 του *Lecture Notes in Computer Science*, σελίδες 457–473. Springer, 2005.

[Tat57] Tate, J.: *WC-groups over p-adic Fields.* Séminaire Bourbaki, exposé 156, Secretariat mathématique, Paris, 1957.

[Ver01] Verheul, E. R.: *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems.* Στο *Advances in Cryptology - EUROCRYPT 2001, Proceedings*, τόμος 2045 του *Lecture Notes in Computer Science*, σελίδες 195–210. Springer, 2001.

[Ver04] Verheul, E. R.: *Evidence that xtr is more secure than supersingular elliptic curve cryptosystems.* Journal of Cryptology, 17(4):277–296, 2004.

[Ver10] Vercauteren, F.: *Optimal pairings.* IEEE Transactions on Information Theory, 56(1):455–461, 2010.

[Wat05] Waters, B.: *Efficient identity-based encryption without random oracles.* Στο *Advances in Cryptology - EUROCRYPT 2005, Proceedings*, τόμος 3494 του *Lecture Notes in Computer Science*, σελίδες 114–127. Springer, 2005.

[Wee09] Wee, H.: *Zero knowledge in the random oracle model, revisited.* Στο *Advances in Cryptology - ASIACRYPT 2009, Proceedings*, τόμος 5912 του *Lecture Notes in Computer Science*, σελίδες 417–434. Springer, 2009.

[WL10] Wei, L. και J. Liu: *Shorter verifier-local revocation group signature with backward unlinkability.* Στο *Pairing-Based Cryptography - PAIRING 2010, Proceedings*, τόμος 6487 του *Lecture Notes in Computer Science*, σελίδες 136–146. Springer, 2010.

[WSI03] Watanabe, Y., J. Shikata, και H. Imai: *Equivalence between semantic security and indistinguishability against chosen ciphertext attacks.* Στο *Public Key Cryptography - PKC 2003, Proceedings*, τόμος 2567 του *Lecture Notes in Computer Science*, σελίδες 71–84. Springer, 2003.

[YL04] Yum, D. H. και P. J. Lee: *Generic construction of certificateless encryption.* Στο *Computational Science and Its Applications - ICCSA 2004, Proceedings, Part I*, τόμος 3043 του *Lecture Notes in Computer Science*, σελίδες 802–811. Springer, 2004.

[ZL06] Zhou, S. και D. Lin: *Shorter verifier-local revocation group signatures from bilinear maps.* IACR Cryptology ePrint Archive, 2006:286, 2006.

[ZSNL03] Zhang, F., R. Safavi-Naini, και C. Y. Lin: *New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairing.* IACR Cryptology ePrint Archive, 2003:104, 2003.

[ZWXF06] Zhang, Z., D. S. Wong, J. Xu, και D. Feng: *Certificateless public-key signature: Security model and efficient construction.* Στο *Applied Cryptography and Network Security, 4th International Conference - ACNS 2006, Proceedings*, τόμος 3989 του *Lecture Notes in Computer Science*, σελίδες 293–308. Springer, 2006.

[ZZH07] Zhao, C., F. Zhang, και J. Huang: *A note on the Ate pairing.* Preprint, Cryptology ePrint Archive, 2007:247, 2007.