Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
Σχολή Θετικών Επιστημών
Τμήμα Μαθηματικών
Πρόγραμμα Μεταπτυχιακών Σπουδών στα Μαθηματικά
Κατεύθυνση Θεωρητικών Μαθηματικών

Κρυπτοσυστηματα και Αποδειξεις Μηδενικης Γνωσης στη Μεταθετικη και Μη-Μεταθετικη Κρυπτογραφια

Χρήστος Πηλιχός

Διπλωματική Εργασία

Επιβλέπων Καθηγητής: Μπάρδης Νικόλαος
Αναπληρωτής Καθηγητής Σ.Σ.Ε.

Δεκέμβριος 2018

Κρυπτοσυστήματα και Αποδείξεις Μηδενικής Γνώσης στη Μεταθετική και Μη-Μεταθετική Κρυπτογραφία

Χρήστος Πηλιχός
(Α.Μ.: 144301)

12 Δεκεμβρίου 2018

Η παρούσα Διπλωματική Εργασία

εκπονήθηκε στο πλαίσιο των σπουδών

για την απόκτηση του

Μεταπτυχιακού Διπλώματος Ειδίκευσης

στα

Μαθηματικά

που απονέμει το

Τμήμα Μαθηματικών

του

Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών

Εγκρίθηκε την 10η Ιανουαρίου, 2019 από Εξεταστική Επιτροπή

αποτελούμενη από τους:

Ονοματεπώνυμο	**Βαθμίδα**	**Υπογραφή**
1. Νικόλαος Μπάρδης	Αναπληρωτής Καθηγητής (επιβλέπων)	……
2. Δημήτριος Βάρσος	Καθηγητής	……
3. Ευαγγελία Κόττα-Αθανασιάδου	Επίκουρη Καθηγήτρια	……

Αφιερωμένη, στους γονείς μου*.

Χρήστος Πηλιχός,
Ασπρόπυργος 2018.

*και σε ένα ακόμη αγαπημένο μου πρόσωπο εντός της οικογενείας!

Περιεχόμενα

Κατάλογος Κρυπτογραφικών Σχημάτων

Πρόλογος

Όσο η ψηφιοποίηση των ανθρωπίνων αναγκών εξελίσσεται, ολοένα και περισσότερο ανακύπτει η ανάγκη για ασφαλή επικοινωνία. Σίγουρα με τη φυσική παρουσία καθιστά τις διαδικασίες πιο απλές (όπως να σιγοψιθυρίσει ο ένας στο αυτί του άλλου ένα μήνυμα, ή να αποδείξει μέσῳ της φυσικής του παρουσίας κάποιος την ταυτότητά του). Ωστόσο, όταν η επικοινωνία επιτυγχάνεται μέσῳ καλωδίων ή ασύρματων μέσων οι καταστάσεις δυσχεραίνουν τρόπον τινά.

Η Κρυπτογραφία έρχεται να λύσει τον γόρδιο δεσμό της ασφαλούς εξ αποστάσεως επικοινωνίας. Μέθοδοι έχουν αναπτυχθεί ήδη από τη δεκαετία του ΄70. Οι μέθοδοι αυτοί αποτελούν την ‘‘παραδοσιακή’’ Κρυπτογραφία –αυτό που εδώ καλείται Μεταθετική Κρυπτογραφία– που είναι καλά μελετημένη όλα αυτά τα χρόνια και έχει στη βιβλιογραφία της σωρεία αποτελεσμάτων. Παρ΄ όλα ταύτα, ένας πιο σύγχρονος κλάδος της Κρυπτογραφίας φαίνεται να κερδίζει έδαφος και να αποκτάει τη δική του βιβλιογραφία: πρόκειται για τη Μη-Μεταθετική Κρυπτογραφία.

Το σκεπτικό για την εκπόνηση της παρούσης διπλωματικής εργασίας είναι:

- Η λεπτομερής παράθεση αλγορίθμων με σκοπό την εισαγωγή του αναγνώστη στη Μεταθετική [§3.1, §3.2 και §3.3] και Μη-Μεταθετική Κρυπτογραφία [§5.1 και §5.2].
- Η αντιπαραβολή, ανάμεσα στη Μεταθετική και Μη-Μεταθετική Κρυπτογραφία, πτυχών όπως η ομομορφική κρυπτογράφηση [§3.2 με §5.2].
- Η υλοποίηση μερικών από τους παραπάνω αλγορίθμων σε εφαρμογές της καθημερινής ζωής [Κεφάλαια 2, 6 και 7].

Σκοπός της εργασίας

Είναι επιθυμητό όπως παρατεθούν και αναπτυχθούν οι εφαρμογές της Μεταθετικής και Μη-Μεταθετικής Κρυπτογραφίας [το οποίο και γίνεται στα Κεφάλαια 2, 6 και 7]. Οι εν λόγῳ εφαρμογές ανακύπτουν σε ζητήματα στην καθημερινή ζωή (η φράση ‘‘πρόσβαση σε στρατιωτική βάση’’ μπορεί να αποδοθεί και ως ‘‘πρόσβαση στον τραπεζικό λογαριασμό μου για διαδικτυακή συναλλαγή’’).

Η Εργασία θίγει πτυχές της Κρυπτογραφίας όπως (i) Συμμετρική κρυπτογράφηση (§6.3 και §7.1), (ii) Ασύμμετρη μεταθετική κρυπτογράφηση (Κεφάλαιο 3), (iii) Ασύμμετρη μη-μεταθετική κρυπτογραφία (Κεφάλαιο 5) και (iv) Χρήση δίτιμων μετασχηματισμών σε συνδυασμό με συναρτήσεις κατακερματισμού (§6.3).

Διάρθρωση της Εργασίας

Ακολουθεί μία αδρή περιγραφή των Κεφαλαίων που έπονται.

Κεφάλαιο 1

Το 1ο Κεφάλαιο περιέχει τις βασικές μαθηματικές έννοιες που θα απαντηθούν αργότερα. Αναπτύσσει τη θεωρία της αριθμητικής υπολοίπων (χρήσιμη για το Κεφάλαιο 3), όσο και τις ομάδες πλεξίδων (που χρησιμοποιούνται στο Κεφάλαιο 4). Τέλος, περιέχει μία σύντομη περιγραφεί των κλάσεων πολυπλοκότητας που θα απαντηθούν στην Εργασία.

Κεφάλαιο 2

Περιλαμβάνεται η θεμελίωση του ‘‘λεξιλογίου’’ που πρόκειται να χρησιμοποιηθεί στο ρουν της Εργασίας. Αφορά τις βασικές κρυπτογραφικές έννοιες, τις προϋποθέσεις ώστε ένα κρυπτοσύστημα να μπορεί να θεωρηθεί ασφαλές και κλείνει με μία πρώτη νύξη για τις αποδείξεις μηδενικής γνώσης.

Κεφάλαιο 3

Παρουσιάζεται και αναλύεται το κρυπτοσύστημα RSA, το οποίο αποτελεί πρότυπο για τη Μεταθετική Κρυπτογραφία. Επίσης, παρατίθενται τα κρυπτοσυστήματα Paillier και το ελλειπτικό El Gamal.

Κεφάλαιο 4

Εδώ εμπεριέχονται εφαρμογές των κρυπτοσυστημάτων του προηγούμενου Κεφαλαίου. Πιο συγκεκριμένα παρουσιάζεται το σχήμα ψηφιακών υπογραφών το οποίο αποτελεί το ανάλογο της υπογραφής στον αληθινό κόσμο. Επίσης, εμπεριέχονται και αυτοτελή (δηλαδή δεν εκμαιεύονται από κάποιο κρυπτοσύστημα) σχήματα ψηφιακών υπογραφών.

Κεφάλαιο 5

Το Κεφάλαιο αρχίζει με μία εισαγωγή στη Μη-Μεταθετική Κρυπτογραφία παρουσιάζοντας ένα κρυπτοσύστημα (των Shpilrain-Zapata) από τον χώρο. Ύστερα παρουσιάζεται από τη σκοπιά της Μη-Μεταθετικής Κρυπτογραφίας η ομομορφική κρυπτογράφηση και πιο συγκεκριμένα το σχήμα των Grigoriev-Ponomarenko.

Κεφάλαιο 6

Παρατίθεται το σχήμα ταυτοποίησης Fiat-Shamir και η βελτίωσή του Feige-Fiat-Shamir τα οποία αποτελούν απαρχή των σχημάτων ταυτοποίησης. Κατ΄ όπιν πραγματοποιείται μία ανασκόπηση στη χρήση boolean άλγεβρας και πως αυτές μπορούν να παράξουν γρήγορα υλοποιήσιμα σχήματα ταυτοποίησης.

Κεφάλαιο 7

Στο παρών Κεφάλαιο εμπεριέχονται σχήματα πιστοποίησης τα οποία μοιάζουν με τα σχήματα ταυτοποίησης με τη μόνη διαφορά ότι δεν υπάρχει ενδεχόμενος δόλος από ανάμεσα στις εμπλεκόμενες οντότητες.

Κεφάλαιο 8

Η Εργασία κλείνει με τη σύνοψη και την παράθεση πιθανών μελλοντικών εξελίξεων των όσων παρουσιάστηκαν.

Παράρτημα Α΄

Εκτός των επιθέσεων στις μαθηματικές τους ιδιότητες τα κρυπτοσυστήματα υπόκεινται και σε επιθέσεις που αφορούν την υλοποίησή τους. Παρατίθεται η περίπτωση των κρυπτοσυστημάτων που χρησιμοποιούν ελλειπτικές καμπύλες.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Μπάρδη Νικόλαο για τη συνεργασία που είχαμε τόσο στο επίπεδο της διπλωματικής, όσο και σε επίπεδο μαθημάτων. Με την αρωγή του εμβάθυνα σε πτυχές της Κρυπτογραφίας διευρύνοντας έτσι το πεδίο των ενδιαφερόντων μου στον κόσμο της Κρυπτογραφίας.

Είμαι χαρούμενος που δέχθηκαν να είναι στη τριμελή εξεταστική επιτροπή μου οι καθηγητές κος Βάρσος Δημήτριος και κα Μητρούλη Μαριλένα.

Ευχαριστώ επίσης τον καθηγητή του τμήματος Μαθηματικών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών κ. Ράπτη Ευάγγελο (επιβλέποντα στη διπλωματική μου για το Π.Μ.Σ. Λογική, Αλγόριθμοι και Πολυπλοκότητα και Υπολογισιμότητα) για τη μύησή μου στον κόσμο της Μη-Μεταθετικής Κρυπτογραφίας το εαρινό εξάμηνο του ακαδημαϊκού έτους 2013-2014.

Ευχαριστώ επίσης τον καθηγητή του τμήματος Μαθηματικών του Πανεπιστημίου Αιγαίου κ. Νάστου Παναγιώτη (επιβλέποντα στην πτυχιακή μου εργασία) ο οποίος το χειμερινό εξάμηνο του ακαδημαϊκού έτους 2011-2012 μου μετέδωσε τις πρώτες μου γνώσεις για την Κρυπτογραφία.

Τέλος, θα επιθυμούσα να ευχαριστήσω την κα Νταή Άλκηστη, γραμματέα του Π.Μ.Σ. Μαθηματικών με την αρωγή της οποίας υπήρξε καταλητική όσον αφορά τα διαδικαστικά θέματα που αφορούσαν το Π.Μ.Σ..

Κεφάλαιο 1

Μαθηματικό υπόβαθρο

Αναπτύσσονται οι έννοιες οι οποίες πρόκειται να απαντηθούν στα επόμενα Κεφάλαια. Η αριθμητική υπολοίπων και οι ιδιότητές της είναι οι αρχές που διέπουν τον σχεδιασμό των αλγορίθμων στο Κεφάλαιο 3. Οι ομάδες πλεξίδων αποτελούν τη δομή υλοποίησης των αλγορίθμων του Κεφαλαίου 5.

1.1 Αριθμητική υπολοίπων

Η **αριθμητική υπολοίπων** είναι ένα σύστημα αριθμητικής για ακεραίους αριθμούς, οι οποίοι αναδιπλώνονται έως την επίτευξη μιας ορισμένης τιμής, η οποία καλείται **συντελεστής** (πληθυντικός αγγλιστί: moduli).

Σύμβαση. $\mathbb{N} := \{1, 2, \ldots\}$ και $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Σε μια πεπερασμένη ομάδα $\mathcal{G} = \langle G, * \rangle$ ($\#G \lneqq \aleph_0$) η **τάξη της ομάδος** $\mathcal{G}$, ορίζεται ως $\mathrm{ord}(\mathcal{G}) = \#G$ (το πλήθος των στοιχείων του συνόλου G), ενώ η **τάξη ενός στοιχείου** $\alpha \in \mathcal{G}$ ορίζεται ως $\mathrm{ord}_{\mathcal{G}}(\alpha) = \min\left\{t \in \mathbb{N} : a^t \equiv 1 \pmod{\mathrm{ord}(\mathcal{G})}\right\}$.

1.1.1 Ορισμοί και βασικά αποτελέσματα

Για κάθε $n \in \mathbb{N}$, συμβολίζεται

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

όπου τα παραπάνω στοιχεία είναι οι αντιπρόσωποι από τις κλάσεις ισοδυναμίας της σχέσης ισοδυναμίας $\mod n \subseteq \mathcal{P}(\mathbb{Z} \times \mathbb{Z})$, με $a \equiv b \pmod n \iff_{o\rho} n \mid a-b$. Η δομή $\langle \mathbb{Z}_n, +_{\mod n} \rangle$, όπου $a +_{\mod n} b := (a+b) \pmod n$ αποδεικνύεται πως αποτελεί ομάδα.

Επί πλέον, ορίζεται

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n : \mu\kappa\delta(x, n) = 1\}$$

Η δομή $\langle \mathbb{Z}_n^*, \times_{\bmod n} \rangle$, με $a \times_{\bmod n} b := (a \cdot b) \pmod n$ αποδεικνύεται πως είναι ομάδα.

Η εφαρμογή της ισοδυναμίας $\bmod n$ μπορεί να είναι σε οποιαδήποτε φάση των υπολογισμών, όπως υπαγορεύει η

Πρόταση 1.1.1. Έστω $n \in \mathbb{N}$. Ισχύουν τα ακόλουθα:

1. $(a \pmod n) \cdot (b \pmod n) \equiv (ab) \pmod n$ και
2. $\big((a \pmod n) \cdot (b \pmod n)\big) \pmod n \equiv (ab) \pmod n$.

Βασικό αποτέλεσμα στην αριθμητική υπολοίπων αποτελεί το:

Θεώρημα 1.1.2 (Κινέζικο Θεώρημα Υπολοίπων). Έστω $m_1, m_2, \ldots, m_r \in \mathbb{N}$, τέτοιοι ώστε $\big(\forall i, j \in \{1, 2, \ldots, r\}\big)[\mu\kappa\delta(m_i, m_j) = 1]$ και $M = m_1 m_2 \cdots m_r \in \mathbb{N}$. Εάν $\alpha) 1 m, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}$, τότε κάθε ακέραιος που ανήκει στην κλάση

$$\left(\alpha_1\beta_1\frac{M}{m_1} + \alpha_2\beta_2\frac{M}{m_2} + \ldots + \alpha_r\beta_r\frac{M}{m_r}\right) \pmod M$$

είναι λύση του συστήματος

$$x \equiv \alpha_i \pmod{m_i} \qquad\qquad i = 1, 2, \ldots, r$$

όπου $\beta_i \in \mathbb{Z}$ είναι αντίστοιχα οι αντιπρόσωποι των αντιστρόφων κλάσεων συζυγίας των $\frac{M}{m_i} \pmod{m_i}$, για $i = 1, 2, \ldots, r$.

1.1.2 Υπόλοιπα και ρίζες

Ορισμός 1.1.3. Ένα $x \in \mathbb{Z}_{n^2}^*$ καλείται n-**οστό υπόλοιπο modulo** n^2 (n-th residue modulo n^2) εάν $(\exists y \in \mathbb{Z}_{n^2}^*)[x^n \equiv y \mod n^2]$.

Εξ ίσου σημαντική είναι και η δυική έννοια των n-οστών υπολοίπων η οποία είναι η ακόλουθη:

Ορισμός 1.1.4. Ένα $y \in \mathbb{Z}$ καλείται n-**οστή ρίζα υπόλοιπο** n) (n-th root modulo n) εάν ισχύει ότι $(\exists z \in \mathbb{Z}_n)[z \equiv y^n \mod n]$.

Το αποτέλεσμα που συνδέει τις παραπάνω δύο έννοιες είναι η ακόλουθη:

Πρόταση 1.1.5. Έστω $n \in \mathbb{N}$. Κάθε n-οστό υπόλοιπο modulo n^2 έχει ακριβώς n διαφορετικές n-οστές ρίζες, εκ των οποίων *ακριβώς μία* είναι αυστηρά μικρότερη του n.

Σύμβαση. Η μοναδική n-οστή ρίζα modulo n^2 του $z \in \mathbb{Z}$ η οποία είναι αυστηρά μικρότερη του n, συμβολίζεται ως $\sqrt[n]{z} \mod n$.

Ορισμός 1.1.6. Οι n-**οστές ρίζες της μονάδος** είναι τα στοιχεία του συνόλου

$$\left\{u \in \mathbb{Z}_n^* : u^n \equiv 1 \pmod{n}\right\}$$

Ένας τρόπος υπολογισμού των n-οστών ριζών της μονάδος παρέχεται από την κάτωθι:

Πρόταση 1.1.7. Έστω $n \in \mathbb{N}$. Ισχύει ότι

$$\begin{aligned}\left\{u \in \mathbb{Z}_n^* : u^n \equiv 1 \pmod{n}\right\} &= \left\{(1+n)^x \mod n^2 : x \in \mathbb{Z}_n^*\right\} \\ &= \left\{1 + nx \mod n^2 : x \in \mathbb{Z}_n^*\right\} \qquad \text{(Λήμμα 3.2.8)}\end{aligned}$$

Ειδική μνεία χρήζει ο κάτωθι ορισμός μιας και απαντάται κατά του ρουν της Εργασίας.

Ορισμός 1.1.8. Ο $q \in \mathbb{Z}$, καλείται **τετραγωνικό υπόλοιπο modulo** $n \in \mathbb{N}$ (quadratic residue modulo n) εάν $(\exists x \in \mathbb{Z}_n)\left[x \neq 0 \implies x^2 \equiv q \pmod{n}\right]$.

Το γεγονός ότι ο $q \in \mathbb{Z}$ είναι τετραγωνικό υπόλοιπο modulo $n \in \mathbb{N}$ θα συμβολίζεται ως $q \mathscr{R} n$. Σε αντίθετη περίπτωση θα αναγράφεται $q \mathscr{N} n$.

Ορισμός 1.1.9. Έστω ένας πρώτος αριθμός $p \gneqq 2$. Ορίζεται ο **σύμβολο του Legendre** ως

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{εάν } a \mathscr{R} p \text{ και } p \nmid a \\ 0, & \text{εάν } p \mid a \\ -1, & \text{εάν } a \mathscr{N} p \text{ και } p \nmid a \end{cases}$$

για $a \in \mathbb{Z}$.

Το σύμβολο Legendre μπορεί να υπολογισθεί από τον ακόλουθο κλειστό τύπο: $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$ (όπου $a \in \mathbb{Z}$ και ο $p \gneqq 2$ είναι πρώτος αριθμός). Επεκτείνοντας το σύμβολο του Legendre προκύπτει ένας ακόμη χαρακτηρισμός.

Ορισμός 1.1.10. Έστω $m \in 2\mathbb{N} - 1$ (περιττός αριθμός), όπου $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ είναι η ανάλυσή του σε πρώτους παράγοντες (ήτοι οι $p_1, p_2, \ldots, p_k \gneqq 2$ είναι πρώτοι αριθμοί και $a_1, a_2, \ldots, a_k \in \mathbb{N}$). Το **σύμβολο Jacobi** ορίζεται ως

$$J_m(n) := \left(\frac{n}{p_1}\right)^{a_1} \left(\frac{n}{p_2}\right)^{a_2} \cdots \left(\frac{n}{p_k}\right)^{a_k}$$

1.2 Μη αβελιανές ομάδες στην Κρυπτογραφία

Τα κριτήρια επιλογής μιας μη αβελιανής ομάδας $G \equiv (G, *)$ ώστε να χρησιμοποιηθεί ως υπόβαθρο υλοποίησης ενός κρυπτογραφικού πρωτοκόλλου συνοψίζονται στα κάτωθι:

Η G **πρέπει να είναι καλώς μελετημένη**: δηλαδή θα πρέπει να υπάρχει μία επαρκώς ανεπτυγμένη θεωρία (:θεωρήματα, ιδιότητες, (αντι)παραδείγματα).

Το πρόβλημα της λέξης [όρα §2.1.2 θα πρέπει να επιλύεται γρήγορα:] δηλαδή σε χρόνο $\mathcal{O}(n)$, ή $\mathcal{O}(n^2)$ [όρα §1.3.1], όπου $n \in \mathbb{N}$ είναι το μέγεθος της εισόδου του αλγορίθμου.

Θα πρέπει να υπάρχει ένας τρόπος σύγχησης των στοιχείων της G: ήτοι να καθίσταται αδύνατη η ανάκτηση των $x, y \in G$ από το $x * y \in G$.

Χρήσιμο γεγονός αποτελεί η ύπαρξη μεθοδολογίας ώστε να υπολογίζονται *κανονικές μορφές* (ήτοι μονοσήμαντα ορισμένα στοιχεία) των στοιχείων της G.

Η G **θα πρέπει να είναι υπερ-πολυωνυμικού ρυθμού**: ήτοι για κάθε $n \in \mathbb{N}$, το πλήθος των στοιχείων της G μήκους* $n \in \mathbb{N}$ είναι μεγαλύτερο από κάθε πολυώνυμο του n).

Υπάρχουν υλοποιήσεις:

- των πρωτοκόλλων [CKLHC01, Ku06] που χρησιμοποιούν ομάδες πλεξίδων [Ar47, BKL98]·
- του πρωτοκόλλου [GZ85] που χρησιμοποιεί τις ομάδες Grigorchyk,
- του πρωτοκόλλου [SZ06] (όρα Σχήμα 5.1) που χρησιμοποιεί τις ελεύθερες μεταβελιανές ομάδες,
- του πρωτοκόλλου [SU05] που χρησιμοποιεί την ομάδα Thompson F,

όπως και πληθώρα άλλων.

Η περιγραφή των μη αβελιανών ομάδες χρειάζεται (τις περισσότερες φορές) πεπερασμένη πληροφορία (γεννήτορες και σχέσεις μεταξύ αυτών). Ωστόσο, περιέχουν πολύ μεγάλο πλήθος στοιχείων γεγονός που δυσχεραίνει κάθε προσπάθεια εξαντλητικής αναζήτησης, ή γνωστή ως επίθεση ωμής βίας. Επίσης, η πολυπλοκότητα των πράξεων ανάμεσα στα στοιχεία τους αυξάνει το υπολογιστικό φόρτο του αντιπάλου (αλλά και του εγκεκριμένου χρήστη που επιθυμεί να επικοινωνήσει· για τον λόγο αυτό -γνωστής κάποιας μυστικής πληροφορίας- έχουν αναπτυχθεί αλγόριθμοι που διευκολύνουν τους υπολογισμούς).

*Εάν $g \in G$, με $g = x_{i_1} * x_{i_2} * \cdots * x_{i_\ell}$, όπου $i_1, i_2, \ldots, i_\ell \in \{1, 2, \ldots, n\}$ και $\{x_1, x_2, \ldots, x_n\} \subseteq G$ είναι ένα σύνολο γεννητόρων της G, τότε το **μήκος** του $g \in G$ είναι $\ell \in \mathbb{N}$.

1.3 Αλγόριθμοι και πολυπλοκότητα

Ορισμός 1.3.1 (Ασυμπτωτικός συμβολισμός). Έστω οι συναρτήσεις $f, g : \mathbb{R} \to \mathbb{R}$.

1. Η g αποτελεί **ασυμπτωτικό άνω φράγμα** για την f εάν ισχύει ότι
$$(\exists M \in \mathbb{R}_+)(\exists x_0 \in \mathbb{R})(\forall x \in \mathbb{R})\big[x \gneqq x_0 \implies |f(x) \leqslant M \cdot |g(x)|\big]$$
Το γεγονός συμβολίζεται ως $f = \mathcal{O}(g)$.
2. Η f αποτελεί **κυριαρχείται ασυμπτωτικό** από την g εάν ισχύει ότι
$$(\forall M \in \mathbb{R}_+)(\exists x_0 \in \mathbb{R})(\forall x \in \mathbb{R})\big[x \gneqq x_0 \implies |f(x)| \leqslant M \cdot |g(x)|\big]$$
Το γεγονός συμβολίζεται ως $f = o(g)$.
3. Η g αποτελεί **ασυμπτωτικό κάτω φράγμα** για την f εάν ισχύει ότι
$$(\exists M \in \mathbb{R}_+)(\exists x_0 \in \mathbb{R})(\forall x \in \mathbb{R})\big[x \gneqq x_0 \implies M \cdot |g(x)| \leqslant |f(x)|\big]$$
Το γεγονός συμβολίζεται ως $f = \Omega(g)$.

Ορισμός 1.3.2. Μία συνάρτηση $f : \mathbb{N} \longrightarrow \mathbb{R}$ καλείται **αμελητέα** (negligible) **συνάρτηση** εάν $(\forall c \in \mathbb{R})(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})\big[n \geqslant n_0 \implies f(n) \leqslant n^{-c}\big]$.

Συμβολισμός. Το γεγονός ότι μία ποσότητα α *δεν* είναι αμελητέα ως προς την ποσότητα x, θα συμβολίζεται ως $\alpha \gg \mathsf{negl}(x)$.

1.3.1 Μηχανές Turing

Θεωρείται ένα μη-κενό σύνολο Σ το οποίο θα καλείται **αλφάβητο**. Κάθε $L \subseteq \Sigma^*$ καλείται **γλώσσα**.

Το (πιο διαδεδομένο) υπολογιστικό μοντέλο που έχει θεσπιστεί από τις αρχές της δεκαετίας του ΄70 είναι η **μηχανή Turing** (προς τιμήν του εμπνευστή της Alan Turing) και συνίσταται στην εξής διατεταγμένη επτάδα:

$$\langle \Sigma,\ \Gamma,\ Q,\ \delta,\ q_0,\ q_{\text{αποδοχής}},\ q_{\text{απόρριψης}} \rangle$$

Τα ‘‘μηχανικά’’ μέρη της μηχανής Turing είναι:

- Μία ταινία με αρχή και δίχως τέλος η οποία είναι χωρισμένη σε ‘‘θέσεις’’ οι οποίες καλούνται **κυψέλες**.
- Μία κεφαλή ανάγνωσης/εγγραφής η οποία έχει τη δυνατότητα να διασχίζει την ταινία είτε κινούμενη μία κυψέλη προς τ΄ αριστερά (συμβολίζεται ως L), είτε κινούμενη μία κυψέλη προς τα δεξιά (συμβολίζεται ως R).

Τα στοιχεία της μηχανής Turing είναι:

- Το σύνολο Σ είναι το **αλφάβητο της εισόδου**.
- Το σύνολο $\Gamma := \Sigma \cup \{\textvisiblespace\}$ καλείται το **αλφάβητο της ταινίας**. *Μόνον το σύμβολο* $\textvisiblespace$ *επιτρέπεται να εμφανίζεται άπειρες φορές στην ταινία.*
- Το σύνολο Q είναι το **σύνολο καταστάσεων** της μηχανής.
  - Η $q_0 \in Q$ είναι η αρχική κατάσταση της μηχανής Turing, $q_{\text{αποδοχής}} \in Q$ είναι η κατάσταση αποδοχής και $q_{\text{απόρριψης}} \in Q$ είναι η κατάσταση απόρριψης της εισόδου από τη μηχανή.
- Η συνάρτηση δ είναι **συνάρτηση μετάβασης** της μηχανής η οποία μπορεί:
  - να έχει μορφή $\delta : (Q \setminus \{q_{\text{αποδοχής}}, q_{\text{απόρριψης}}\}) \times \Gamma \longrightarrow Q \times \Gamma \times \{L, R\}$ και τότε η μηχανή καλείται **αιτιοκρατική** (deterministic) **μηχανή Turing**.
  - να έχει μορφή $\delta : (Q \setminus \{q_{\text{αποδοχής}}, q_{\text{απόρριψης}}\}) \times \Gamma \longrightarrow \mathcal{P}\big(Q \times \Gamma \times \{L, R\}\big)$ (ως $\mathcal{P}(A)$ συμβολίζεται το δυναμοσύνολο του συνόλου A) και τότε η μηχανή καλείται **αναιτιοκρατική** (non-deterministic) **μηχανή Turing**.

Μία μηχανή Turing ξεκινάει τους υπολογισμούς από την κατάσταση $q_0 \in Q$ και αποτελεί ένα πρόγραμμα οι εντολές του οποίου:

- στην αιτιοκρατική μηχανή Turing είναι της μορφής ''$l :$ **εάν** σ **τότε** $(\sigma'; o; l')$'' με σημασία:
  1. Εάν το σύμβολο που διαβάστηκε είναι το $\sigma \in \Sigma$, τότε η μηχανή
     - (α') αντικαθιστάει το $\sigma \in \Sigma$ με το $\sigma' \in \Sigma$,
     - (β') μετακινεί την κεφαλή κατά $o \in \mathbb{Z}$ θέσεις,
       [εάν $o \in \mathbb{N}$, τότε η μετακίνηση γίνεται προς τα δεξιά, αλλιώς προς τ΄ αριστερά]
     - (γ') εκτελεί την οδηγία με ετικέτα l'.
  2. Αλλιώς, εκτελείται η οδηγία με ετικέτα $l + 1$.
- για την αναιτιοκρατική μηχανή Turing είναι της μορφής

$$l : \textbf{εάν } \sigma \textbf{ τότε επίλεξε μία από τις } \{(\sigma_1; o_1; l_1), \ldots, (\sigma_n; o_n; l_n)\} \tag{1.1}$$

  με σημασία όπως παραπάνω.

Η μηχανή περατώνει τους υπολογισμούς της όταν επιτευχθεί μία από τις καταστάσεις $q_{\text{αποδοχής}}$ ή $q_{\text{απόρριψης}}$.

1.3.2 Κλάσεις χρονικής πολυπλοκότητας

Ένας τρόπος ώστε να αναπαρασταθεί μία αναιτιοκρατική μηχανή Turing είναι μέσω του *δένδρου υπολογισμών* (computation tree) της:

(i) ο υπολογισμός της μηχανής ξεκινάει από τη ρίζα του δένδρου και εκτελείται η εντολή της μορφής (1.1) με ετικέτα $l = 1$·

(ii) κάθε κόμβος του δένδρου
- αντιστοιχεί σε μια εντολή της μορφής (1.1) και
- έχει τόσους απογόνους[†], όσες επιλογές έχει η εντολή της μορφής (1.1) που του αντιστοιχεί·

(iii) οι κόμβοι στους οποίους η μηχανή είναι είτε σε κατάσταση $q_{\text{αποδοχής}}$, είτε σε κατάσταση $q_{\text{απόρριψης}}$ (δηλαδή δεν υπάρχουν άλλες εντολές να εκτελεστούν και η μηχανή έχει σταματήσει τους υπολογισμούς της) καλούνται *φύλλα*.

Χωρίς βλάβη της γενικότητας, μπορεί να θεωρηθεί πως κάθε εντολή της μορφής (1.1) έχει δύο ακριβώς πιθανές επόμενες επιλογές. Έτσι, εάν σε έναν υπολογισμό επιλεγεί η πρώτη επιλογή, το γεγονός θα συμβολίζεται με 0, ενώ εάν επιλεγεί η δεύτερη, θα συμβολίζεται με 1. Άρα, κάθε υπολογισμός της μηχανής είναι ένα πεπερασμένη ακολουθία από 0 και 1, ή αλλιώς ένα στοιχείο του $\{0,1\}^*$. Έστω $y \in \{0,1\}^*$ το μονοπάτι του υπολογισμού που ακολουθεί μία αναιτιοκρατική μηχανή Turing που έχει ως είσοδό της την $x \in \{0,1\}^*$.

Στα παρακάτω, για το κατηγόρημα $R : \{0,1\}^* \times \{0,1\}^* \longrightarrow \{0,1\}$ υποτίθεται ότι:

- εάν $R(x,y) = 1$, τότε η $y \in \{0,1\}^*$ πως έχει πολυωνυμικά λιγότερα δυφία απ' όσα η $x \in \{0,1\}^*$, ήτοι $(\exists k \in \mathbb{N})\left[|y| \leqslant |x|^k\right]$ και
- υπάρχει αιτιοκρατική μηχανή Turing που σε πολυωνυμικό χρόνο υπολογίζει το κατηγόρημα R (ήτοι για κάθε $x,y \in \{0,1\}^*$ εάν $R(x,y) = 1$ ή $R(x,y) = 0$).

Η κλάση NP

Από το

Θεώρημα 1.3.3. Η γλώσσα $L \subseteq \{0,1\}^*$ ανήκει στην κλάση NP εάν και μόνον εάν υπάρχει κατηγόρημα $R : \{0,1\}^* \times \{0,1\}^* \longrightarrow \{0,1\}$ (όπως παραπάνω), ώστε $L = \left\{x \in \{0,1\}^* : (\exists y \in \{0,1\}^*)[R(x,y) = 1]\right\}$.

προκύπτει ότι

$$L \in \mathsf{NP} \iff \exists R \text{ τέτοιο ώστε } \begin{cases} x \in L \implies \exists y\, R(x,y) \\ x \notin L \implies \forall y\, \neg R(x,y) \end{cases}$$

Με άλλα λόγια, NP είναι η κλάση των γλωσσών L για τις οποίες: Εάν $x \in L$ ($x \notin L$), τότε *υπάρχει* (*κάθε*) κλάδος στο δένδρο υπολογισμού της αναιτιοκρατικής μηχανής Turing που αποδεικνύει το γεγονός $x \in L$ ($x \notin L$).

[†]Καινούργιοι κόμβοι οι οποίοι συνδέονται στον κόμβο με μία ακμή.

Η κλάση P

Όντας το ‘‘δένδρο’’ υπολογισμού μιας αιτιοκρατικής μηχανής Turing μονοπάτι (καθ΄ ότι κάθε εντολή του προγράμματός της έχει μία πιθανή επόμενη οδηγία), *κάθε* μονοπάτι υπολογισμού συνηγορεί στο γεγονός προς απόδειξη.

$$L \in \mathsf{P} \iff \exists R \text{ τέτοιο ώστε } \begin{cases} x \in L \implies (\forall y)\big[R(x,y)\big] \\ x \notin L \implies (\forall y)\big[\neg R(x,y)\big] \end{cases}$$

1.3.3 Τύποι αναγωγών

Δύο (εκ των τριών διασημοτέρων) τύποι αναγωγών είναι οι ενθάδε από τον πιο αυστηρό σε κριτήρια προς τον πιο χαλαρό:

Πολλά-προς-ένα αναγωγή πολυωνυμικού χρόνου: από ένα πρόβλημα A στο πρόβλημα B -συμβολίζεται ως $A \leqslant_m^P B$- είναι ένας αλγόριθμος μετασχηματίζει στιγμιότυπα του A σε στιγμιότυπα του B, τοιουτοτρόπως ώστε είτε επιλύοντας το αρχικό στιγμιότυπο (του A), είτε το μετασχηματισμένο στιγμιότυπο (του B), η λύση να είναι η ιδία. Οι εν λόγῳ αναγωγές είναι γνωστές και ως **πολυωνυμικοί μετασχηματισμοί** ή **αναγωγές κατά Karp**.

Αναγωγή Turing πολυωνυμικού χρόνου από ένα πρόβλημα A στο πρόβλημα B -συμβολίζεται ως $A \leqslant_T^P B$- είναι ένας αλγόριθμος ο οποίος:

- καλεί πολυωνυμικό πλήθος φορών μία υπορουτίνα η οποία επιλύει το πρόβλημα B και
- εάν εξαιρεθεί ο χρόνος που χρειάζεται κάθε φορά η υπορουτίνα για το πρόβλημα B, ο αλγόριθμος περατώνεται σε πολυωνυμικό χρόνο.

Οι εν λόγῳ αναγωγές είναι γνωστές και ως **αναγωγές κατά Cook**

Ο λόγος που χρησιμοποιείται το σύμβολο $\leqslant$ στις αναγωγές παραπάνω είναι για να υποδηλώσει πως το πρόβλημα B είναι τουλάχιστον τόσο δύσκολο όσο το πρόβλημα A (αφού με μερικές ερωτήσεις για το B, επιλύεται το A). Οι πιο ευρέως χρησιμοποιούμενες αναγωγές είναι οι ‘‘πολλά-προς-ένα αναγωγές πολυωνυμικού χρόνου’’, οι οποίες εννοούνται κάθε φορά που αναφέρεται στην Εργασία η φράση ‘‘αναγωγή πολυωνυμικού χρόνου’’.

Σε εντελώς αφηρημένο επίπεδο ένα υπολογιστικό πρόβλημα Π μπορεί να θεωρηθεί ως $\Pi \subseteq \{0,1\}^\star$. Ως **στιγμιότυπο** ενός προβλήματος Π είναι κάθε $x \in \Pi$. Ένα **πρόβλημα απόφασης** είναι κάθε υπολογιστικό πρόβλημα του οποίου το σύνολο λύσεων είναι {ΝΑΙ, ΟΧΙ}.

Ορισμός 1.3.4. Το πρόβλημα $C \in$ NP καλείται **NP-πλήρες** (NP-complete) εάν για κάθε πρόβλημα στην κλάση NP υπάρχει αναγωγή πολυωνυμικού χρόνου στο C.

Ορισμός 1.3.5. Ένα πρόβλημα H λέγεται **NP-δύσκολο** (NP-hard) εάν για κάθε πρόβλημα στην κλάση NP υπάρχει αναγωγή πολυωνυμικού χρόνου στο H.

Κεφάλαιο 2

Εισαγωγή στην Κρυπτογραφία

''*Η Κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων*''.
- Ron Rivest (1990)

2.1 Βασικοί ορισμοί

Τα σύγχρονα συστήματα ασφάλειας πληροφοριών σχεδιάζονται με γνώμονα την ικανοποίηση των *κρυπτογραφικών υπηρεσιών*. Πρόκειται για τις διαδικασίες οι οποίες χρησιμοποιούν την Κρυπτογραφία για την αντιμετώπιση απειλών. Μερικές κρυπτογραφικές υπηρεσίες συνίστανται οι κάτωθι:

Εμπιστευτικότητα (Confidentiality): Είναι η προστασία από την μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας από τα δεδομένα που μεταφέρονται κατά την επικοινωνία των οντοτήτων στο πρωτόκολλο.

Αυθεντικότητα (Authentication): όσον αφορά

Χρηστών: Πρόκειται για την εξασφάλιση της γνώσης της ταυτότητας της οντότητας με την οποία συνάπτεται η επικοινωνία.

Δεδομένων: Πρόκειται για την εξασφάλιση της ακρίβειας των μεταφερόμενων πληροφοριών, δηλαδή πως ένα μήνυμα προέρχεται όντως από τον επιθυμητό αποστολέα.

Ακεραιότητα (Integrity): Είναι η προστασία από την μη εξουσιοδοτημένη χρήση των δεδομένων που ανταλλασσονται στο πρωτόκολλο.

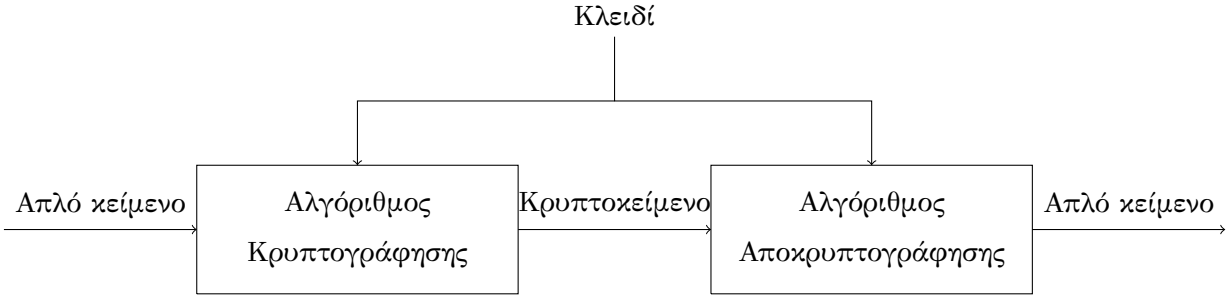
Ορισμός 2.1.1 ([MOV96]). Η **Κρυπτογραφία** είναι η μελέτη των Μαθηματικών τεχνικών οι οποίες σχετίζονται με την ασφάλεια της πληροφορίας, ήτοι με τις έννοιες της εμπιστευτικότητας, της ακεραιότητας των δεδομένων, της αυθεντικοποίησης οντοτήτων και της αυθεντικοποίησης της πηγής των δεδομένων.

Ορισμός 2.1.2. Πρωτόκολλο (επικοινωνίας) είναι ένας κατανεμημένος αλγόριθμος ο οποίος ενέχει τουλάχιστον δύο οντότητες οι οποίες πραγματοποιούν υπολογιστικά βήματα, αλλά και ανταλλάσσουν πληροφορίες αναμεταξύ τους.

Το μήνυμα που πρόκειται να αποσταλλεί καλείται **αρχικό κείμενο** (plain text), ενώ το τροποποιημένο μήνυμα που αποστέλλεται (:κοινοποιείται) καλείται **κρυπτοκείμενο** (cipher text). Ο μεταχηματισμός του απλού κειμένου σε κρυπτοκείμενο καλείται **κρυπτογράφηση**, ενώ η ανάστροφη διαδικασία καλείται **αποκρυπτογράφηση**. Η κρυπτογράφηση καθώς και η αποκρυπτογράφηση όταν λαμβάνουν χώρα χρειάζονται μία επιπλέον ποσότητα πληροφορίας την οποία γνωρίζουν μόνον οι οντότητες που επιθυμούν να επικοινωνήσουν και ονομάζεται **κλειδί**. Η ύπαρξη κλειδιού είναι η βασική διαφοροποίηση της Κρυπτογραφίας από την *Κωδικοποίηση*. Οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης συνιστούν τον **κρυπτογραφικό αλγόριθμο** ή **κρυπταλγόριθμο** (cipher).

Ορισμός 2.1.3. Ένα **κρυπτοσύστημα** είναι μία τριάδα αλγορίθμων $\mathcal{K} = \langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$, όπου $\mathcal{G}$ είναι ο αλγόριθμος δημιουργίας του δημοσίου και του ιδιωτικού κλειδιού για το κρυπτοσύστημα, $\mathcal{E}$ είναι ο αλγόριθμος κρυπτογραφήσεως και $\mathcal{D}$ ο αλγόριθμος αποκρυπτογραφήσεως.

Ορισμός 2.1.4. Ένα κρυπτοσύστημα ονομάζεται **συμμετρικό** εάν οι αλγόριθμοι κρυπτογράφησης και απορκυπτογράφης κάνουν χρήση του ιδίου κλειδιού.

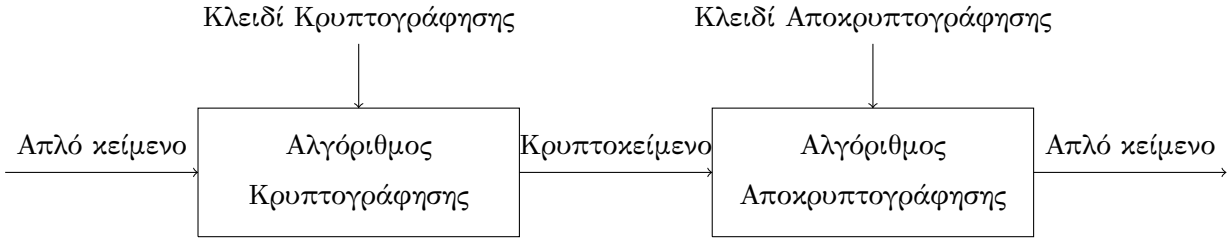


Εμφανείς αδυναμίες ενός συμμετρικού κρυπτοσυστήματος είναι οι κάτωθι:

- Εάν $n \in \mathbb{N}$ οντότητες επιθυμούν ανά 2 να επικοινωνήσουν, τότε
  - κάθε οντότητα θα πρέπει να κατέχει $\binom{n}{2} = \frac{n(n-1)}{2}$ κλειδιά (ένα για κάθε μία άλλη οντότητα με την οποία επιθυμεί να επικοινωνήσει)·
  - χρειάζονται $\binom{n}{2}$ ασφαλείς δίαυλοι επικοινωνίας, ώστε να ανταλλαχθούν τα κλειδιά ανάμεσα στις οντότητες·
  - πρακτικά χρειάζεται κάθε οντότητα να υλοποιήσει με κάθε άλλη οντότητα ένα σχήμα ανταλλαγής κλειδιού.
- Το μέγεθος του κλειδιού είναι μικρότερο από το μέγεθος του απλού κειμένου, κάτι που κάνει το κλειδί ευάλωτο σε μια μετάδοση.
- Το κλειδί έχει περιορισμένη περίοδο ζωής και γι αυτό πρέπει να ανανεώνεται περιοδικα.

Ορισμός 2.1.5. Ένα **σχήμα ανταλλαγής κλειδιού** είναι ένα πρωτόκολλο το οποίο επιτρέπει στις εμπλεκόμενες οντότητες να καταλήξουν σε ένα κοινό κλειδί.

Ορισμός 2.1.6. Ένα κρυπτοσύστημα ονομάζεται **ασύμμετρο** εάν οι αλγόριθμοι κρυπτογράφησης και απορκυπτογράφης κάνουν χρήση ξεχωριστού κλειδιού.



Σε ένα ασύμμετρο κρυπτοσύστημα η δημιουργία των κλειδιών είναι ευθύνη του παραλήπτη μηνυμάτων. Το *κλειδί κρυπτογράφησης* καλείται **δημόσιο κλειδί** καθώς ο παραλήπτης το αποστέλλει σε κάθε ενδιαφερόμενη οντότητα που επιθυμεί να συνάψει επικοινωνία μαζί του. Το *κλειδί αποκρυπτογράφησης* καλείται **ιδιωτικό κλειδί** καθ' όσον φυλάττεται κρυφό αφού αποτελεί τη μυστική πληροφορία η οποία αντιστρέφει τη διαδικασία της κρυπτογράφησης. Σε αντιδιαστολή, στα συμμετρικά κρυπτοσυστήματα, το κλειδί κρυπτογράφησης συμπίπτει με το κλειδί αποκρυπτογράφησης και για αυτό το λόγο δεν κοινοποιείται.

Ορισμός 2.1.7. Θεωρείται ένα κρυπτοσύστημα $\mathcal{K} = \langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$. Έστω $\mathcal{M}$ ο χώρος των απλών κειμένων (όλα τα πιθανά απλά κείμενα) και $\mathcal{C}$ ο χώρος των κρυπτοκειμένων (όλα τα πιθανά κρυπτοκείμενα). Το $\mathcal{K}$ καλείται

- **αιτιοκρατικό** (deterministic) εάν $\mathcal{E} : \mathcal{M} \longrightarrow \mathcal{C}$ και $\mathcal{D} : \mathcal{C} \longrightarrow \mathcal{M}$.
- **πιθανοκρατικό** (probabilistic) εάν $\mathcal{E} : \mathcal{M} \times \mathsf{R} \longrightarrow \mathcal{C}$ και $\mathcal{D} : \mathcal{C} \longrightarrow \mathcal{M}$, όπου R είναι ο χώρος μιας παραμέτρου η οποία επιλέγεται τυχαία.

Επίσης, $\big(\forall \mathsf{T} \in \{\mathcal{M}, \mathcal{M} \times \mathsf{R}\}\big)(\forall \mathrm{x} \in \mathsf{T})\big[\mathcal{D}(\mathcal{E}(\mathrm{x})) = \mathrm{x}\big]$ (ορθότητα κρυπτοσυστήματος).

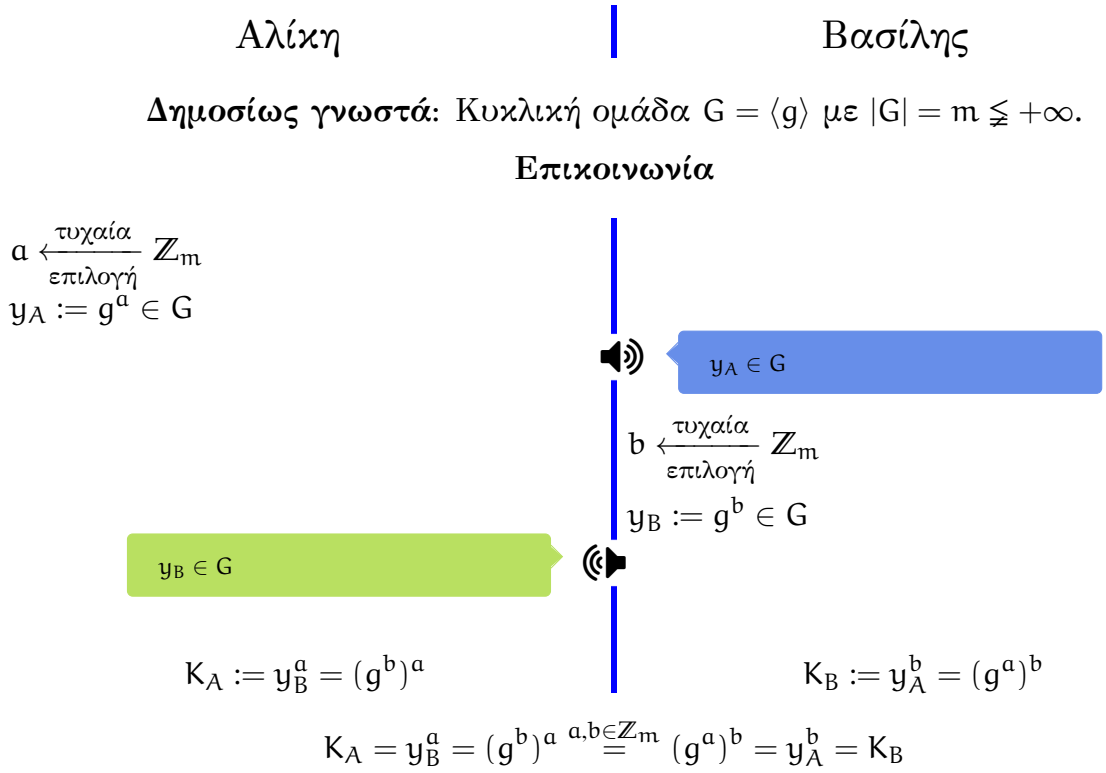
Ορισμός 2.1.8. Ένα **κρυπτογραφικό πρωτόκολλο** είναι ένα πρωτόκολλο επικοινωνίας το οποίο χρησιμοποιεί τεχνικές και μηχανισμούς κρυπτογράφησης.

Παράδειγμα 2.1.9. Μερικά κρυπτογραφικά πρωτόκολλα είναι:

1. Όρα §3.1.7 το σχήμα PGP.
2. Δύο οντότητες:
   (α′) Συμφωνούν σε κοινό κλειδί μέσω ενός σχήματος ανταλλαγής κλειδιού.
   (β′) Ανταλλάζουν μηνύματα με ένα συμμετρικό κρυπτοσύστημα. ⊣

2.1.1 Μεταθετική Κρυπτογραφία

Το 1976 οι Whitefield Diffie και Martin Hellman στο [DH76] εισήγαγαν έναν ρηξικέλευθο τρόπο επικοινωνίας ανάμεσα σε δύο οντότητες. Μέχρι τότε η επικοινωνία δύο οντοτήτων βασιζόταν σε μία προσυμφωνημένη πληροφορία (κλειδί) η οποία δίπε την επικοινωνία. Πλέον, οι οντότητες είναι σε θέση να ανταλλάξουν την κοινό κλειδί επικοινωνίας τους δίχως κάποια πρότερη συνεννόηση.



Σχήμα 2.1: Σχήμα ανταλλαγής κλειδιού Diffie-Hellman

Η ασφάλεια του Σχήματος 2.1 στηρίζεται στο υπολογιστικό πρόβλημα Diffie-Hellman το οποίο συνίσταται στο ακόλουθο:

Το πρόβλημα CDH: Δεδομένων μίας κυκλικής ομάδας $G = \langle g \rangle$, με $|G| = m \lneqq +\infty$ και των $g^a, g^b \in G$, για άγνωστα $a, b \in \mathbb{Z}_m$, να υπολογισθεί το $g^{ab} \in G$.

Σε μια προσπάθεια ώστε να καταταχθεί το πρόβλημα CDH, όσον αφορά την υπολογιστική του πολυπλοκότητα, αντιπαρατίθεται με:

Το πρόβλημα DLOG: Έστω μια κυκλική ομάδα $G = \langle g \rangle$, με $|G| = m \lneqq +\infty$ και $y \in G$. Να βρεθεί $x \in \mathbb{Z}_m$, τέτοιο ώστε $g^x = y$.

Στην πράξη είναι $G = \mathbb{Z}_n$, $n \in \mathbb{N}$. Δεν υπάρχει απόδειξη πως το πρόβλημα είναι υπολογιστικά ανεπίλυτο. Ο καλύτερος αλγόριθμος επίλυσης του προβλήματος DLOG απαιτεί πλήθος υπολογιστικών βημάτων υπερ-πολυωνυμικό ($:o(n^c)$, για κάθε $c \in \mathbb{N}$) ως προς το μέγεθος του στοιχείου $y \in G$ παραπάνω -υποθέτοντας πως η ομάδα έχει επιλεγεί *επαρκώς* πολυπληθής.

Πρόταση 2.1.10. Ισχύει ότι $\texttt{CDH} \preceq \texttt{DLOG}$.

Απόδειξη. Δεδομένων των $g, g^a, g^b \in G = \langle g \rangle$, για άγνωστα $a, b \in \mathbb{Z}_m$, επιλύοντας το πρόβλημα του διακριτού λογαρίθμου για το $g^b \in G$, ο αντίπαλος αποκτάει γνώση του $b \in \mathbb{Z}_m$. Πλέον, υπολογίζεται $(g^a)^b = g^{ab} \in G$ ήτοι το ζητούμενο. □

2.1.2 Μη-Μεταθετική Κρυπτογραφία

Ο Max Dehn ήδη από το 1911 -στην εργασία του [De11]- είχε γνωστοποιήσει πως κύριο μέρος της έρευνάς του ήταν τα ακόλουθα υπολογιστικά προβλήματα:

Το πρόβλημα της λέξης: Δοθείσης μιας ομάδας $G = \langle X \mid R \rangle$ κι ενός $w \in G$, ισχύει ότι το $w \in G$, κάνοντας χρήση των σχέσεων R, ανάγεται στο 1_G;

Το πρόβλημα της συζυγίας: Δοθείσης μιας ομάδας $G = \langle X \mid R \rangle$ και $x, y \in G$, να βρεθεί $z \in G$, τέτοιο ώστε $y = z^{-1}xz$, δεδομένου ότι υπάρχει τέτοιο στοιχείο.

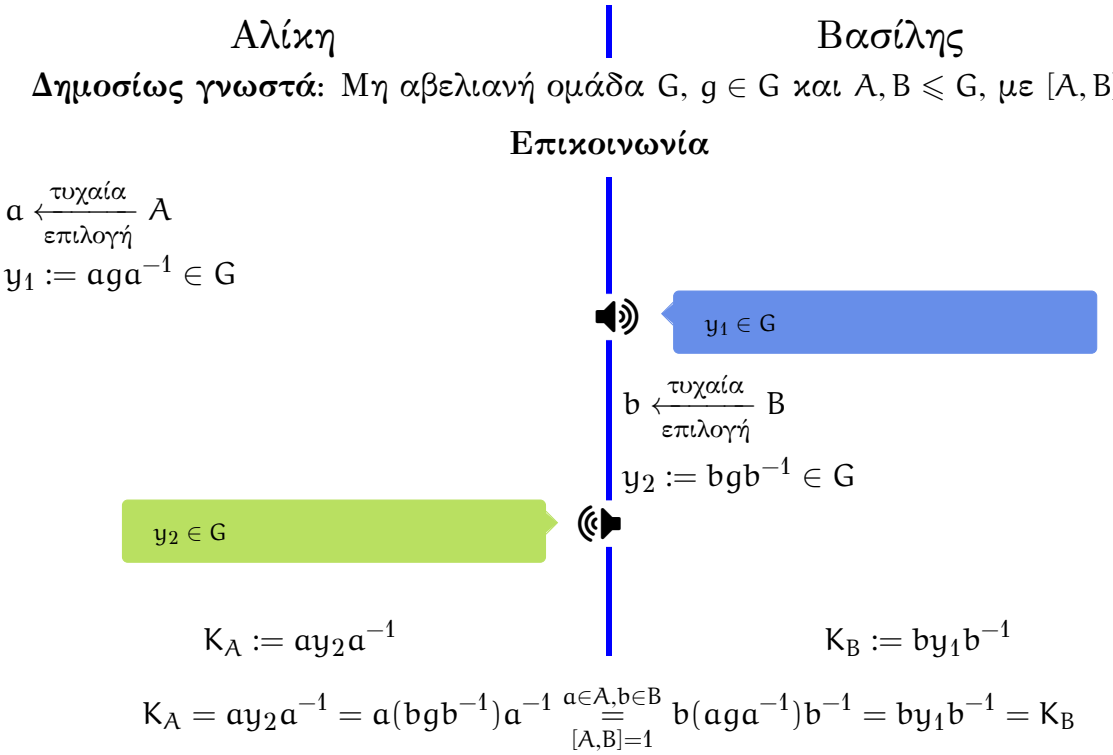
Το πρόβλημα ισομορφισμού ομάδων: Δεδομένων δύο πεπερασμένα παραστάσιμων ομάδων G_1, G_2, υπάρχει ισομορφισμός $G_1 \xrightarrow{\simeq} G_2$;

Τα παραπάνω είναι μερικά από τα υπολογιστικά προβλήματα στα οποία στηρίζεται η ασφάλεια των κρυπτοσυστημάτων στην Μη-Μεταθετική Κρυπτογραφία.

Όσον αφορά το πρόβλημα της λέξης, ο Max Dehn το 1912 στην εργασία του [De12] έδωσε έναν αλγόριθμο ο οποίος επιλύει το πρόβλημα για μία κατηγορία ομάδων (εκείνες που ικανοποιούν τη συνθήκη μικρών ακυρώσεων $C'(1/6)$). Οι Pyotr Nobikov το 1955 στην εργασία του [No55] και William Boone, το 1958, στην εργασία του [Bo58] απέδειξαν ξεχωριστά πως δεν υπάρχει εν γένει αλγόριθμος για το πρόβλημα της λέξης σε πεπερασμένα παριστάσμενες ομάδες.

Οι Ki Hyoung Ko, Sang Ji Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang και Choonsik Park το 2000 στο [CKLHC01] πρότειναν ένα πρωτόκολλο ανταλλαγής κλειδιού εμπνευσμένοι* το πρόβλημα της συζυγίας.

*Όπως αποδεικνύουν οι Vladimir Shpilrain και Alexander Ushakov το 2006 στο [CSP06], η επίλυση του προβλήματος της συζυγίας αποτελεί μη-ικανή προϋπόθεση για την ανάκτηση του κοινού κλειδιού, καθώς αρκεί να επιλυθεί το πρόβλημα της ανάλυσης και το πρόβλημα του μέλους.



Σχήμα 2.2: Σχήμα ανταλλαγής κλειδιού Ko-Lee et al.

Ένα ακόμη διάσημο πρόβλημα της Μη-Μεταθετικής Κρυπτογραφίας είναι:

Το πρόβλημα της ανάλυσης: Θεωρείται μία ομάδα $(G, *)$ και $A \subseteq G$. Δεδομένων των $x, y \in G$, να βρεθεί ένα ζεύγος $(a, b) \in A \times A$, τέτοιο ώστε $y = a * x * b$, δεδομένου πως υπάρχει τουλάχιστον ένα τέτοιο ζεύγος.

Μία προφανής λύση είναι το ζεύγος $(y * x^{-1}, 1_G)$ και τότε $y = (y * x^{-1}) * x * 1_G$, ωστόσο δεν είναι γνωστόν ότι $y * x^{-1}, 1_G \in A \subseteq G$. Η επαλήθευση του ''ανήκειν'' μπορεί να αποτελέσει δύσκολο πρόβλημα (:το πρόβλημα του μέλους της §5.1.1). Για $b = a^{-1} \in G$ και $A = G$ προκύπτει το πρόβλημα της συζυγίας.

Πρώτοι οι Vladimir Shpilrain και Alexander Ushakov το 2005 στο [SU05] στήριξαν την ασφάλεια ενός κρυπτοσυστήματος στο πρόβλημα της ανάλυσης χρησιμοποιώντας ιδιότητες που πληρούν κάποιες υποομάδες (οι *κεντροποιούσες υποομάδες*) μιας μη-αβελιανής ομάδας. Άλλα κρυπτογραφικά πρωτόκολλα τα οποία στηρίζουν την ασφάλειά τους στο πρόβλημα της ανάλυσης είναι: Stickel [Sti05] (μια ανάλυση της ασφάλειάς του: [Sh08]· μια παραλλαγή του με χρήση τροπικών αλγεβρών: [GS13], πάλι από τους Shpilrain-Ushakov [SU06], Yeşem Kurt [Ku06]. Ωστόσο, υπάρχουν κρυπτοσυστήματα που απεδείχθεισαν ανασφαλή, όπως των Xiaofeng Wang, Chen Xu, Guo Li, Hanling Lin [WXLLW14] (έσπασε από τον Vitaly Roman'kov [Rom14]), των Joan-Josep Climent, Pedro R. Navarro και Leandro Tortosa [CNT11] (που έσπασαν οι Abdel A. Kamal και Amr M. Youssef [KY12]).

2.2 Συναρτήσεις κατακερματισμού

Ορισμός 2.2.1. Έστω $n \in \mathbb{N}$. Η **απόσταση Hamming** των $a = (x_1, \ldots, x_n) \in \{0,1\}^n$ και $b = (y_1, \ldots, y_n) \in \{0,1\}^n$ ορίζεται ως $d(a,b) := \#\{i \in \{1,\ldots,n\} : x_i \neq y_i\}$.

Ορισμός 2.2.2. Μία **συναρτηση κατακερματισμού** (ή **συνάρτηση σύνοψης** - hash function) είναι μία συνάρτηση της μορφής $\mathcal{H} : \{0,1\}^* \longrightarrow \{0,1\}^k$, για κάποιο γνωστό και σταθερό $k \in \mathbb{N}$.

Η ιδανική συνάρτηση κατακερματισμού $\mathcal{H} : A \longrightarrow B$ θα πρέπει να πληροί τις ακόλουθες ιδιότητες:

Αιτιοκρατική: $(\forall x \in A)(\exists! y \in B)[\mathcal{H}(x) = y]$.

Αποτελεσματική: Είναι υπολογιστικά εύκολο να βρεθούν οι τιμές.

Αντίσταση πρώτου ορίσματος: Δεδομένου ενός $y \in B$, είναι υπολογιστικά δύσκολο να βρεθεί $x \in A$, τέτοιο ώστε $\mathcal{H}(x) = y$.

Αντίσταση δεύτερου ορίσματος: Δεδομένου ενός $x \in A$ είναι υπολογιστικά δύσκολο να βρεθεί $x' \in A \setminus \{x\}$, τέτοιο ώστε $\mathcal{H}(x) = \mathcal{H}(x')$.

Αποφυγή συγκρούσεων: Είναι υπολογιστικά δύσκολο να βρεθούν $x, x' \in A$, τέτοια ώστε $\mathcal{H}(x) = \mathcal{H}(x')$.

Ελευθερία συσχετισμού: Είναι υπολογιστικά δύσκολο να βρεθούν $x, x' \in A$, με μικρή απόσταση Hamming, ώστε τα $\mathcal{H}(x), \mathcal{H}(x') \in B$ να έχουν επίσης μικρή απόσταση Hamming.

Ωστόσο, στην πράξη, οι ως άνω ιδιότητες δεν δύνανται όπως ικανοποιηθούν ταυτοχρόνως. Για το λόγο αυτόν η συνάρτηση κατακερματισμού $\mathcal{H} : A \longrightarrow B$ υλοποιείται ως **τυχαίο μαντείο** (random oracle) με τον εξής τρόπο: Για κάθε στιγμιότυπο $n \in \mathbb{N}$ (:το πλήθος των φορών που έχει κληθεί η $\mathcal{H} : A \longrightarrow B$) και ερώτημα $x \in A$, ορίζεται

$$\big(\text{History}[n+1],\, \mathcal{H}(x)\big) := \begin{cases} \big((x,r),\, r \xleftarrow{r} B\big), & \text{εάν } n = 0 \\ \big(\text{History}[n], y\big), & \text{εάν } n \neq 0 \text{ και} \\ & \qquad (\exists y \in B)\big[(x,y) \in \text{History}[n]\big] \\ \big(\text{History}[n] \cup (x,r),\, r \xleftarrow{r} B\big), & \text{αλλιώς} \end{cases}$$

Με άλλα λόγια η συνάρτηση διατηρεί πίνακα ιστορικού των απαντήσεών της -τον History[n]. Εάν υπάρχει εγγραφή για τον ερώτημα που της τίθεται στον πίνακα προτέρων απαντήσεών της, τότε αποκρίνεται την ίδια απάντηση που είχε δώσει στα παρελθόν. Σε κάθε άλλη περίπτωση επιστρέφει ένα τυχαίο στοιχείο του πεδίου τιμών B.

Παράδειγμα 2.2.3. Έστω το μήνυμα

- $x :=$ "`Hello world`"

Χρησιμοποιώντας τον κώδικα `ASCII` στην δυαδική του γραφή:

$$\begin{aligned} \texttt{0} \rightsquigarrow 00110000, \quad \ldots, \quad \texttt{9} \rightsquigarrow 00111001, \quad \texttt{A} \rightsquigarrow 01000001, \quad \ldots, \quad \texttt{Z} \rightsquigarrow 01011010, \\ \texttt{␣} \rightsquigarrow 00100000, \quad \texttt{a} \rightsquigarrow 01100001, \quad \ldots, \quad \texttt{z} \rightsquigarrow 01111010 \end{aligned}$$

υπολογίζεται η δυαδική αναπαράστασή $x_2 \in \{0,1\}^*$ του μηνύματος προς αποστολή $x \in \{0,\ldots,9,A,\ldots,Z,a,\ldots,z,\texttt{␣}\}^*$. Τώρα (για να καταστούν ευανάγνωστα τα αποτελέσματα αναπαριστώνται στο 16δικό σύστημα αριθμήσεως):

$$\begin{aligned} \mathsf{SHA\text{-}1}(x_2) &= \texttt{7b502c3a1f48c8609ae212cdfb639dee39673f5e} \\ \mathsf{SHA\text{-}224}(x_2) &= \texttt{ac230f15fcae7f77d8f76e99adf45864a1c6f800655da78dea956112} \end{aligned}$$

Ωστόσο, ακολουθώντας την παραπάνω διαδικασία για το μήνυμα

- $x' :=$ "`hello world`"

προκύπτει

$$\begin{aligned} \mathsf{SHA\text{-}1}(x_2') &= \texttt{2aae6c35c94fcfb415dbe95f408b9ce91ee846ed} \\ \mathsf{SHA\text{-}224}(x_2') &= \texttt{2f05477fc24bb4faefd86517156dafdecec45b8ad3cf2522a563582b} \end{aligned}$$

κάτι εντελώς ασυσχέτιστο με τις κωδικοποιήσεις του μηνύματος x. ⊣

2.3 Μοντέλα ασφαλείας

Ορισμός 2.3.1. Μία (**πιθανοτική**) **δειγματοληψία** (probability ensemble) είναι μία συλλογή κατανομών $\mathcal{D} := \{\mathbf{D}_n\}_{n\in\mathbb{N}}$. Μία **στατιστική δοκιμή** (statistical test) $\mathcal{A}$ για μία δειγματοληψία $\mathcal{D} = \{\mathbf{D}_n\}_{n\in\mathbb{N}}$ είναι ένας αλγόριθμος ο οποίος λαμβάνει ως είσοδο στοιχεία της $\mathbf{D}_n$ και δίδει αποτέλεσμα $\{0,1\}$, για κάθε $n \in \mathbb{N}$.

Θα δημιουργήσουμε ''παίγνια'' (στατιστικές δοκιμές) των οποίων η πιθανότητα επιτυχούς έκβασης είναι η πιθανότητα επιτυχής επίθεσης ενός αντιπάλου σε ένα κρυπτοσύστημα.

Ορισμός 2.3.2. Έστω μία στατιστική δοκιμή $\mathcal{A}$ για μία δειγματοληψία $\mathcal{D}$. Η **στατιστική απόσταση** των κατανομών $\mathbf{D}_i, \mathbf{D}_j \in \mathcal{D}$ ως προς την στατιστική δοκιμή $\mathcal{A}$ είναι:

$$\Delta_{\mathcal{A}}[X,Y] := \left| \underset{X\leftarrow\mathbf{D}_i}{\mathsf{Prob}}\left[\mathcal{A}(X)=1\right] - \underset{Y\leftarrow\mathbf{D}_j}{\mathsf{Prob}}\left[\mathcal{A}(Y)=1\right] \right| \tag{2.1}$$

Η πιθανότητα επιτυχίας ενός αντιπάλου που διεξάγει επίθεση σ΄ ένα κρυπτοσυστήματος θα καλείται *πλεονέκτημα* (advantage). Συνήθως, στην εξίσωση (2.1) η κατανομή $\mathbf{D}_{\mathrm{i}}$ θα είναι η ομοιόμορφη και η κατανομή $\mathbf{D}_{\mathrm{j}}$ θα είναι ο χώρος απ΄ όπου η γνώση κάποιου στοιχείου του καθιστά την αποκρυπτογράφηση εφικτή.

Συμβολισμός. Παρακάτω ως $\mathscr{A}^{\mathcal{O}_2(\cdot)}$ κι ως $\mathscr{C}^{\mathcal{O}_1(\cdot)}$ συμβολίζεται το γεγονός ότι ο αντίπαλος $\mathscr{A}$ και ο προκαλών $\mathscr{C}$ έχει πρόσβαση στο μαντείο $\mathcal{O}_1(\cdot)$ και $\mathcal{O}_2(\cdot)$ αντίστοιχα, όπου για $s \in \{0,1\}$:

- είτε $\mathcal{O}_s(\cdot) = \mathcal{D}_{sk}(\cdot)$: η πρόσβαση στον αλγόριθμο κρυπτογράφησης $\mathcal{D}_{sk}(\cdot)$ ο οποίος μπορεί να αποκρυπτογραφήσει κρυπτοκείμενα της επιλογής του αντιπάλου ή του προκαλούντος -πλην του κρυπτογραφήματος που δημιούργησε ο προκαλών·
- είτε $\mathcal{O}_s(\cdot) = \varepsilon$: η άρνηση οποιαδήποτε βοήθειας στην οντότητα,

2.3.1 Ασφάλεια μη-διακριτότητας

Σ΄ ένα παίγνιο μη-διακριτότητας $\mathrm{Game}_{\mathsf{IND\text{-}ATK\text{-}b}}$: (1) Οι $\mathscr{A}$ και $\mathscr{C}$ επικοινωνούν και ανταλλάσσουν μηνύματα. (2) Ο $\mathscr{A}$ παράγει δύο μηνύματα m_0, m_1. (3) Ο $\mathscr{C}$ αποστέλλει στον $\mathscr{A}$ την *πρόκληση* $c_b := \mathcal{E}(m_b)$. (4) Ο $\mathscr{A}$ με γνώμονα το c_b και κάποιες άλλες πληροφορίες aux που συνέλεξε υπολογίζει ένα $b' \in \{0,1\}$ στην προσπάθειά του να ‘‘μαντέψει’’ το $b \in \{0,1\}$. (5) Ο $\mathscr{A}$ κερδίζει εάν $b' = b$, γεγονός που συμβολίζεται ως ‘‘$\mathrm{Game}_{\mathsf{IND\text{-}ATK\text{-}b}} = 1$’’.

Ορισμός 2.3.3. Έστω ένα κρυπτοσύστημα $\langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$ και $(\mathcal{C}, \mathcal{A})$ ένα σύστημα προκαλούντος και αντιπάλου. Για $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$ και $\lambda \in \mathbb{N}$, έστω

$$\mathrm{Adv}_{\mathsf{IND\text{-}ATK}}(\lambda) := \left|\mathsf{Prob}[\mathrm{Game}_{\mathsf{IND\text{-}ATK\text{-}1}}(\lambda) = 1] - \mathsf{Prob}[\mathrm{Game}_{\mathsf{IND\text{-}ATK\text{-}0}}(\lambda) = 1]\right|$$

όπου $b \in \{0,1\}$,

$\mathrm{Game}_{\mathsf{IND\text{-}ATK\text{-}b}}(\lambda)$:
$(pk, sk) \leftarrow \mathcal{G}(1^\lambda)$; $(m_0, m_1, \mathsf{aux}) \leftarrow \mathscr{C}^{\mathcal{O}_1(\cdot)}(pk)$, με $|m_0| = |m_1|$;
$c_b \leftarrow \mathcal{E}_{pk}(m_b)$; $b' \leftarrow \mathscr{A}^{\mathcal{O}_2(\cdot)}(m_0, m_1, c_b, \mathsf{aux})$; **επίστρεψε** b';

κι

- αν $\mathsf{ATK} = \mathsf{CPA}$, τότε $\mathcal{O}_1(\cdot) = \varepsilon$ και $\mathcal{O}_2(\cdot) = \varepsilon$.
- αν $\mathsf{ATK} = \mathsf{CCA1}$, τότε $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ και $\mathcal{O}_2(\cdot) = \varepsilon$.
- αν $\mathsf{ATK} = \mathsf{CCA2}$, τότε $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ και $\mathcal{O}_2(\cdot) = \mathcal{D}_{sk}(\cdot)$.

Ορισμός 2.3.4. Ένα κρυπτοσύστημα $\langle \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$ καλείται **IND-ATK ασφαλές**, όπου $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$ και $\lambda \in \mathbb{N}$, εάν $\mathrm{Adv}_{\mathsf{IND\text{-}ATK}}(\lambda) \leqslant \mathrm{negl}(\lambda)$.

2.3.2 Ασφάλεια μη-ελατότητας

Ορισμός 2.3.5. Ένας αλγόριθμος κρυπτογράφησης $\mathcal{E} : \mathcal{M} \longrightarrow \mathcal{C}$ καλείται **ελατός** (ή **εύπλαστος**, malleable) εάν δεδομένου ενός κρυπτοκειμένου $c \in \mathcal{C}$, αυτό μπορεί να παραλλαχθεί σε ένα έτερο κρυπτοκείμενο $d \equiv d(c) \in \mathcal{C}$, το οποίο αποκρυπτογραφείται σε κάποιο επιθυμητό απλό κείμενο $m' \in \mathcal{M}$, δηλαδή $d = \mathcal{E}(m')$.

Παράδειγμα 2.3.6. Έστω ότι η πραγματοποίηση μιας τραπεζικής συναλλαγής χρησιμοποιεί έναν ελατό αλγόριθμο κρυπτογράφησης $\mathcal{E}$. Η συναλλαγή είναι:

ΜΕΤΑΦΟΡΑ €0000100.00 ΣΤΟΝ ΛΟΓΑΡΙΑΣΜΟ #1100.

Γνωρίζοντας ότι πρόκειται για μεταφορά χρημάτων σε λογαριασμό, μπορεί κάποιος παρεμβαίνοντας στο κρυπτογράφημα του παραπάνω μηνύματος να το τροποποιήσει ώστε να η τελική αποκρυπτογράφηση να υπαγορεύει:

ΜΕΤΑΦΟΡΑ €1000000.00 ΣΤΟΝ ΛΟΓΑΡΙΑΣΜΟ #2237. ⊣

Έστω $(\mathscr{C}, \mathscr{A})$ ένα σύστημα προκαλούντος και αντιπάλου. (1) Ο προκαλών $\mathscr{C}$ έχοντας γνώση ενός δημοσίου κλειδιού, δημιουργεί έναν χώρο απλών κειμένων $\mathcal{M}$, απ' όπου αντλεί δύο μηνύματα $m_0, m_1 \in \mathcal{M}$, ιδίου μήκους. (2) Ο αντίπαλος $\mathscr{A}$ λαμβάνει την κρυπτογράφηση c ενός εκ των m_0, m_1. (3) Ο αντίπαλος δημιουργεί μία διμερή σχέση R κι ένα διάνυσμα κρυπτοκειμένων $\mathbf{y}$, το οποίο σε καμμία συντεταγμένη του δεν περιέχει το c_b. (4) Ο αντίπαλος κερδίζει εάν ισχύει η σχέση $R(x_b, \mathbf{x})$, όπου το m_b, $b \in \{0, 1\}$, είναι το κείμενο που αντιστοιχεί στο c και το διάνυσμα $\mathbf{x}$ περιέχει σε κάθε συντεταγμένη του την αποκρυπτογράφηση της αντίστοιχης συντεταγμένης του διανύσματος $\mathbf{y}$.

Ορισμός 2.3.7. Έστω ένα κρυπτοσύστημα $\langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$ και $(\mathscr{C}, \mathscr{A})$ ένα σύστημα προκαλούντος και αντιπάλου. Για $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$ και $\lambda \in \mathbb{N}$, έστω

$$\mathrm{Adv}_{\mathsf{NM\text{-}ATK}}(\lambda) := \left| \mathsf{Prob}[\mathrm{Game}_{\mathsf{NM\text{-}ATK\text{-}1}}(\lambda) = 1] - \mathsf{Prob}[\mathrm{Game}_{\mathsf{NM\text{-}ATK\text{-}0}}(\lambda) = 1] \right|$$

όπου $b \in \{0, 1\}$,

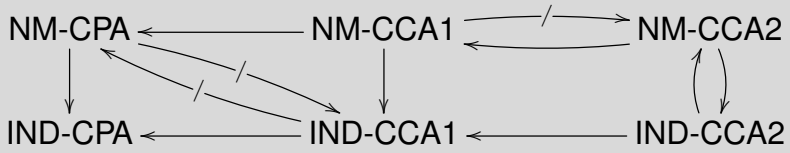
$\mathrm{Game}_{\mathsf{NM\text{-}ATK\text{-}b}}(\lambda)$:
$(pk, sk) \leftarrow \mathcal{G}(1^\lambda)$; $(\mathcal{M}, \mathsf{aux}) \leftarrow \mathscr{C}^{\mathcal{O}_1(\cdot)}(pk)$; $m_0, m_1 \leftarrow \mathcal{M}$, με $|m_0| = |m_1|$;
$c \leftarrow \mathcal{E}_{pk}(m_1)$; $(R, \mathbf{y}) \leftarrow \mathscr{A}^{\mathcal{O}_2(\cdot)}(\mathcal{M}, c, \mathsf{aux})$;
εάν $(c \notin \mathbf{y} \wedge R(m_b, \mathbf{x}))$ **τότε επίστρεψε** 1; **αλλιώς επίστρεψε** 0;

κι

- αν $\mathsf{ATK} = \mathsf{CPA}$, τότε $\mathcal{O}_1(\cdot) = \varepsilon$ και $\mathcal{O}_2(\cdot) = \varepsilon$.
- αν $\mathsf{ATK} = \mathsf{CCA1}$, τότε $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ και $\mathcal{O}_2(\cdot) = \varepsilon$.
- αν $\mathsf{ATK} = \mathsf{CCA2}$, τότε $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ και $\mathcal{O}_2(\cdot) = \mathcal{D}_{sk}(\cdot)$.

Ορισμός 2.3.8. Ένα κρυπτοσύστημα $\langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$ καλείται **NM-ATK ασφαλές**, όπου $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$ και $\lambda \in \mathbb{N}$, εάν $\mathrm{Adv}_{\mathsf{NM\text{-}ATK}}(\lambda) \leqslant \mathrm{negl}(\lambda)$.

Οι επιθέσεις Type-Atk, για $\mathsf{Type} \in \{\mathsf{IND}, \mathsf{NM}\}$ και $\mathsf{Atk} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$ συσχετίζονται (όπως περιγράφεται στο [BDPR98]) ως εξής:



※ Τα βέλη συμβολίζουν συνεπαγωγή ($A \to B$: υπάρχει απόδειξη πως ένα κρυπτοσύστημα που πληροί την έννοια A, τότε πληροί και την B).

※ Τα διεγραμμένα βέλη δηλώνουν διαχωρισμό ($A \nrightarrow B$: μπορεί να κατασκευασθεί κρυπτοσύστημα που πληροί την έννοια A, αλλά όχι την B).

2.4 Αποδείξεις μηδενικής γνώσης

Η ανάγκη για υψηλό επίπεδο ασφάλειας μεταξύ (i) της επικοινωνίας των χρηστών και μεταξύ (ii) πολλών χρηστών προς ένα σύστημα, ανέπτυξε σύγχρονα συστήματα ταυτοποίησης και αυθεντικοποίησης (πιστοποίησης). Το πρόβλημα που ανακύπτει είναι το εξής: Η οντότητα A (ο **αποδεικνύων** (*prover*)) ζητάει την οντότητα B (ο **επιβεβαιωτής** (*verifier*)) πρόσβαση σε ένα αγαθό ή υπηρεσία. Για να επιτραπεί η πρόσβαση, η αρμοδιότητα του B είναι να επαληθεύσει πως ο A κατέχει μία πληροφορία *δίχως ο A να την αποκαλύψει*.

2.4.1 Ιστορική αναδρομή

Οι αποδείξεις μηδενικής γνώσης εισηγήθηκαν από τους Shafi Goldwasser, Silvio Micali και Charles Rackoff στο [GMR85] και αποτελούν μία εκλεπτυσμένη τεχνική που περιορίζει τη ανταλλασσόμενη πληροφορία από τον αποδεικνύων A στον επιβεβαιωτή B σε ένα κρυπτογραφικό πρωτόκολλο. Όπως είχαν ορισθεί αρχικώς ο δεν ήταν ακριβώς αποδείξεις *μηδενικής* γνώσης. Ο B προκαλούσε τον A να αποδείξει ή να διαψεύσει εάν ένα στιγμιότυπο I ανήκει σε μια NP γλώσσα L. Ο αποδεικνύων A απεκάλυπτε στον επιβεβαιωτή B ένα δυφίο (0 ή 1, αναλόγως εάν το I ήταν στιγμιότυπο της L ή όχι). Συνεπώς, υπήρχε μεταφορά πληροφορίας.

Την ίδια περίοδο οι Zvi Galil, Stuart Haber και Moti Yung στο [GHY85] προσπαθούν κάτι διαφορετικό. Ορίζουν την έννοια του ‘‘αποτελέσματος μηδιαχωρίσιμων πρωτοκόλλων’’ ως εξής: ο A στέλνει μία πλήρη απόδειξη ότι το I

ανήκει/δεν ανήκει στη γλώσσα L. Ο B που γνωρίζει εκ των προτέρων την απάντηση επαληθεύει την απόδειξη που έλαβε από τον A. Ο (παθητικός) ωτακουστής δεν είναι σε θέση ούτε να επέμβει στο πρωτόκολλο, ούτε να μεσολαβήσει στην επικοινωνία ανάμεσα στους A και B. Άρα, δεν μπορεί (όντας η γλώσσα L της κλάσης NP) να αποφανθεί (σε αιτιοκρατικό πολυωνυμικό χρόνο) εάν η πληροφορία που κατέχει είναι μία απόδειξη ή μία διάψευση.

Οι Uriel Feige, Amos Fiat και Adi Shamir στο [FFS87] προσπάθησαν να αποκρύψουν και αυτήν την πληροφορία. Αυτό καθίσταται εφικτό αντικαθιστώντας τη ''γνώση'' (ήτοι το δυφίο), με τη ''γνώση της γνώσης'' (δηλαδή ο A μπορεί να πείσει τον B πως κατέχει τη γνώση του δυφίου δίχως να το του το φανερώσει). Έτσι ο B δεν λαμβάνει καμμία πληροφορία για το I, την L, ή την συσχέτισή τους.

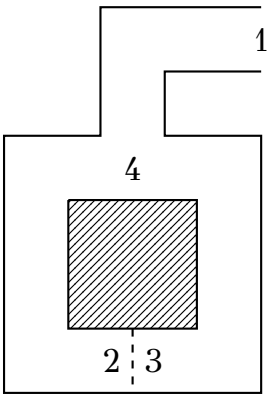
2.4.2 Παράδειγμα: Η μαγική σπηλιά

Ο Βασίλης και η Αλίκη επισκέπτονται τη μαγική σπηλιά. Η σπηλιά εκτείνεται εις βάθος. Έχει μία είσοδο και κατ 'οπιν διαχωρίζεται σε δύο διαδρόμους οι οποίοι καταλήγουν στην ίδια πόρτα. Μόνον όποιος κατέχει το μυστικό κλειδί μπορεί να ανοίξει την πόρτα και να κάνει τον γύρο της σπηλιάς. Ο Βασίλης διάκειται πως έχει το μυστικό κλειδί, αλλά δεν επιθυμεί να το δώσει στην Αλίκη, ώστε εκείνη να πάει και να δοκιμάσει εάν ανοίγει την πόρτα. Έτσι:

(i) Η Αλίκη στέκεται στην είσοδο της σπηλιάς (σημείο 1), ενώ ο Βασίλης εισέρχεται στην σπηλιά, χωρίς η Αλίκη να μπορεί να διακρίνει ποιον δρόμο ακολούθησε ο Βασίλης.

(ii) Όταν ο Βασίλης φτάνει στην μαγική πόρτα (είτε στο σημείο 2, είτε στο σημείο 3) η Αλίκη προχωράει στην διακλάδωση των δύο μονοπατιών (σημείο 4).

(iii) Η Αλίκη καλεί τον Βασίλη να εμφανισθεί είτε από το δεξιό διάδρομο, είτε από τον αριστερό.



Επαναλαμβάνοντας την ίδια διαδικασία αρκετές φορές, η Αλίκη πείθεται πως ο Βασίλης κατέχει το μυστικό κλειδί.

Για περισσότερα παραδείγματα όρα στο [QGAB89].

Μέρος Ι

Κρυπτοσυστήματα

Η ασφάλεια κάθε κρυπτογραφικού πρωτοκόλλου στηρίζεται στη δυσκολία εύρεση λύσεων κάποιων μαθηματικών προβλημάτων. Με άλλα λόγια χρησιμοποιούνται συναρτήσεις $Y = F(X)$ οι οποίες είναι εύκολο να υπολογισθούν, ωστόσο η αντίστροφή τους $X = \Phi(Y)$ -η εύρεση ενός X, ώστε $Y = F(X)$- αποτελεί δύσκολο πρόβλημα, το οποίο κανείς το επιλύει μόνον απαριθμώντας όλα τα δυνατά X.

Το πλεονέκτημα να στηριχθεί η ασφάλεια ενός κρυπτογραφικού σχήματος στο δυσεπίλυτο ενός προβλήματος της Θεωρίας Ομάδων είναι πως επιτρέπουν την ασύμμετρη κρυπτογραφία. Η γενική αρχή που διέπει τα προβλήματα δίτιμης άλγεβρας (συμμετρικοί αλγόριθμοι και μονόδρομες συναρτήσεις -one way functions- ή συναρτήσεις κατακερματισμού -hash functions) καθώς και τα προβλήματα της Θεωρίας Αριθμών είναι: *Λόγῳ της πληθώρας των στοιχείων που αποτιμώνται στο ίδιο στοιχείο (ήτοι* $(\exists X_1, X_2)[X_1 \neq X_2 \wedge F(X_1) = F(X_2)]$*) κάποιες τιμές μπορούν να χρησιμοποιηθούν ως κλειδιά κρυπτογράφησης και κάποιες άλλες ως κλειδιά αποκρυπτογράφησης.* Στους δίτιμους μετασχηματισμούς ωστόσο, δεν είναι εφικτή ακόμη η ασύμμετρη κρυπτογράφηση (και υπάρχει μεγάλη έρευνα ώστε να πραγματοποιηθεί ασύμμετρη κρυπτογράφηση με χρήση αλγεβρών Boole), βασική αρχή της μοντέρνας Κρυπτογραφίας και του σχεδιασμού σχημάτων υπογραφών και ταυτοποίησης. Ένας παράγοντας που συμβάλλει στον περιορισμό των δίτιμων μετασχηματισμών είναι η μοναδικότητά του.

Το πλεονέκτημα να στηριχθεί η ασφάλεια ενός κρυπτογραφικού σχήματος στο δυσεπίλυτο αλγεβρικών εκφράσεων είναι πως τα εν λόγῳ σχήματα είναι υλοποιήσιμα σε συσκευές περιορισμένων υπολογιστικών πόρων (μνήμη, ενέργεια, ταχύτητα και μέγεθος επεξεργαστών). Οι πράξεις γίνονται στο δυαδικό σύστημα και είναι ευκόλως υλοποιήσιμες από ηλεκτρονικές συσκευές. Από την άλλην τα σχήματα που στηρίζονται στο δυσεπίλυτο προβλημάτων από τη Θεωρία Ομάδων χρησιμοποιούν αριθμητικές πράξεις, οι οποίες (ακόμη κι αν συμβαίνουν σε κάποια αριθμητική υπολοίπων) είναι δύσκολο να υλοποιηθούν λόγῳ του μεγέθους των δεδομένων τους [οι υπολογισμοί μεγάλων αριθμών για το κρυπτοσύστημα RSA -όρα Σχήμα 3.1- ξεπερνούν εύκολα τις δυνατότητες ενός υπολογιστού τσέπης].

Οι δίτιμοι μετασχηματισμοί που εμφανίζονται στην §6.4 και στην §7.1 αποτελούν μία καινοτομία, συνδυασμού τυπικών πρωτοκόλλων ασφαλής επικοινωνίας χρηστών με σύστημα κάνοντας χρήση αποδοτικών συμμετρικών αλγορίθμων και συναρτήσεων κατακερματισμού. Οι συναρτήσεις κατακερματισμού χρησιμοποιούν μετασχηματισμούς στις δυαδικές αναπαραστάσεις των δεδομένων που καλούνται να υπολογίσουν. Το Πρότυπο Κρυπτογράφησης Δεδομένων (DES) το οποίο αποτέλεσε για σχεδόν 25 χρόνια το πρότυπο κρυπτογραφικό σχήμα [Νοέμβριος 1976 έως 26 Μαΐου 2002 οπότε και υιοθετήθηκε το Προηγμένο Κρυπτογραφικό Πρότυπο (AES)] καθώς και από αλγορίθμους μονόδρομων μετασχηματισμών.

Κεφάλαιο 3

Μεταθετική Κρυπτογραφία

Η Μεταθετική Κρυπτογραφία αποτελεί τον πιο διαδεδομένο κλάδο της Κρυπτογραφίας. Πρόκειται για τους αλγορίθμους που έχουν την πιο ευρεία εφαρμογή στην καθημερινή ζωή. Εδώ επιχειρείται μία πρώτη παρουσίαση κάποιων πτυχών της Μεταθετικής Κρυπτογραφίας.

3.1 Το κρυπτοσύστημα RSA

Ήδη από το 1976 οι Whitefiled Diffie, Martin Hellman και Ralph Merkle είχαν διατυπώσει την ιδέα του ασύμμετρου κρυπτοσυστήματος, ωστόσο, η ιδέα δεν τύγχανε μιας κατάλληλης μονοσήμαντης συνάρτησης. Το 1978 στο [RSA78] προτάθηκε από τους Ron Rivest, Adi Shamir και Leonard Adleman πρότειναν το πρώτο κρυπτοσύστημα δημοσίου κλειδιού. Στην άλλη πλευρά του Ατλαντικού, το 1975, τρεις άγγλοι, οι James Henry Ellis, Clifford Christopher Cocks και Malcolm John Williamson ήδη είχαν ανακαλύψει σπουδαίες πτυχές της Κρυπτογραφίας (αλγόριθμοι ανταλλαγής κλειδιού). Ωστόσο, τα επιτεύγματά τους διατηρήθηκαν μυστικά, έως το 1997 όταν αποχαρακτηρίστηκαν από απόρρητα.

3.1.1 e-οστές ρίζες στο $\mathbb{Z}_n^*$

Ορισμός 3.1.1. Η **συνάρτηση** φ **του Euler** $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ ορίζεται ως

$$\varphi(n) := \#\{k \in \mathbb{Z}_n : \mu\kappa\delta(k, n) = 1\}$$

Συνεπώς, η $\varphi(n)$ εκφράζει το *πλήθος των σχετικά πρώτων αριθμών με το* $n \in \mathbb{N}$. Μία άλλη οπτική είναι πως εκφράζει *το πλήθος των αντιστρέψιμων στοιχείων στο* $\mathbb{Z}_n$, ήτοι $\varphi(n) = \#\{k \in \mathbb{Z}_n : (\exists \ell \in \mathbb{Z}_n)\big[k\ell \equiv 1 \pmod{n}\big]\}$.

Πρόταση 3.1.2 (Ιδιότητες της συνάρτησης φ του Euler). Ισχύουν τα κάτωθι:

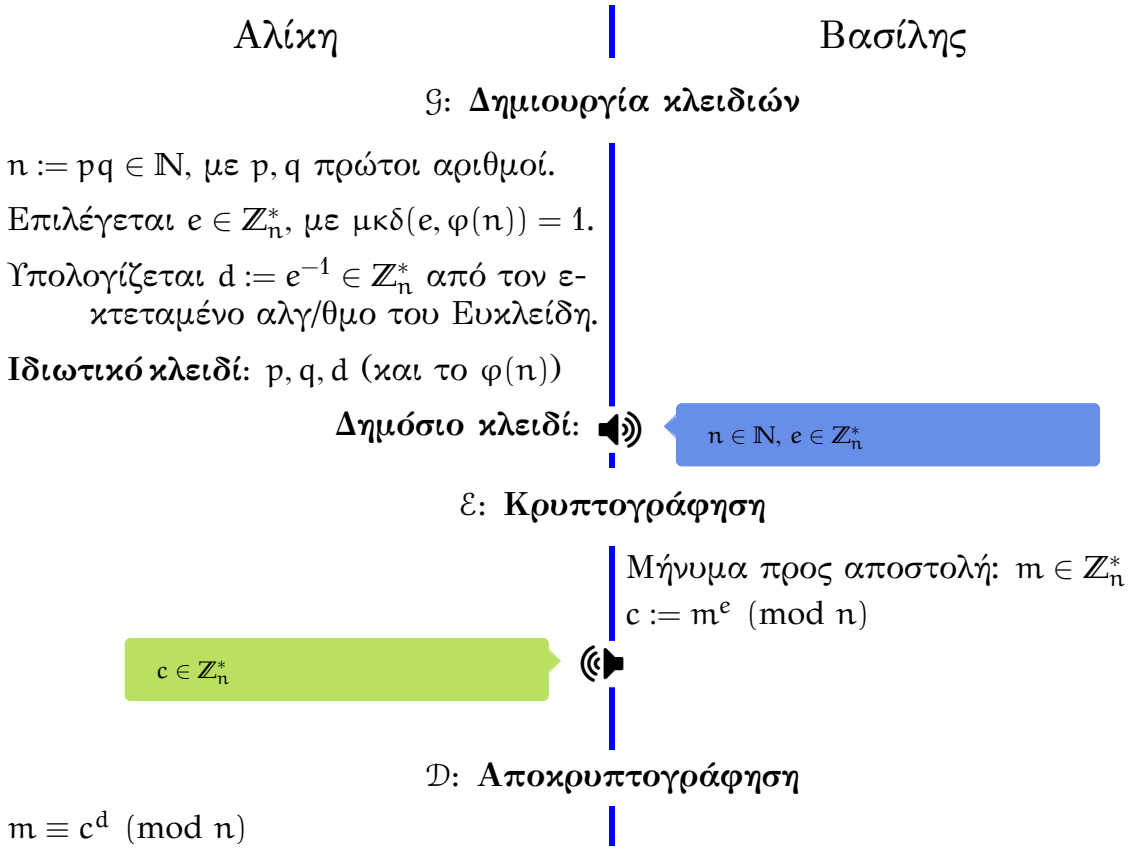
1. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, για κάθε πρώτο αριθμό $p \in \mathbb{N}$ και κάθε $\alpha \in \mathbb{N}$.
2. $(\forall m, n \in \mathbb{N})\big[\mu\kappa\delta(m,n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)\big]$.

Απόδειξη. 1. Ως ο $p \in \mathbb{N}$ πρώτος αριθμός, τότε $(\forall m \in \mathbb{Z}_{p^\alpha})\big[\mu\kappa\delta(p^\alpha, m) \in \{1, p, p^2, \ldots, p^\alpha\}\big]$. Εάν $\mu\kappa\delta(p^\alpha, m) \neq 1$, τότε το $m \in \mathbb{Z}_{p^\alpha}$ δεν είναι πολλαπλάσιο του $p \in \mathbb{N}$. Τα πολλαπλάσια του $p \in \mathbb{N}$ που ανήκουν στο $\mathbb{Z}_{p^\alpha}$ είναι: $1p, 2p, \ldots, p^{\alpha-1}p = p^\alpha$, ήτοι $p^{\alpha-1} \in \mathbb{N}$ σε πλήθος. Άρα, οι υπόλοιποι $p^\alpha - p^{\alpha-1} \in \mathbb{N}$ αριθμοί του $\mathbb{Z}_{p^\alpha}$ είναι σχετικά πρώτοι με τον $p \in \mathbb{N}$.

2. Γενίκευση του: $(\forall m, n \in \mathbb{N})[\mu\kappa\delta(m,n) = 1 \implies \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n]$. □

3.1.2 Υλοποίηση

Ο αλγόριθμος RSA συνιστάει ένα κρυπτοσύστημα που επιτρέπει σε δύο οντότητες να ανταλλάζουν μηνύματα δίχως κάποια πρότερη συνεννόηση.



Σχήμα 3.1: Το κρυπτοσύστημα RSA

Απόδειξη (Ορθότητας κρυπτοσυστήματος RSA). Έστω $e, d \in \mathbb{Z}_n^*$ με $\mu\kappa\delta\big(e, \varphi(n)\big) = 1$ και $ed \equiv 1 \pmod{\varphi(n)}$. Αφού $\mu\kappa\delta(e, \varphi(n)) = 1$, τότε $(\exists k \in \mathbb{Z})[ed = 1 + k\varphi(n)]$. Για $m \in \mathbb{Z}_n$ είναι: $D\big(E(m)\big) = \big(E(m)\big)^d = (m^e)^d = m^{ed} = m^{1+k\varphi(n)} \equiv m \pmod{n}$. □

Από την Πρόταση 3.1.2, εάν $n = p_1^{e_1} \cdots p_j^{e_j}$ είναι η ανάλυσή σε πρώτους παράγοντες ενός $n \in \mathbb{N}$, τότε $\varphi(n) = \varphi(p_1^{e_1} \cdots p_j^{e_j}) \overset{2.}{=} \varphi(p_1^{e_1}) \cdots \varphi(p_j^{e_j}) \overset{1.}{=} \prod_{i=1}^{j} (p_i^{e_i} - p_i^{e_i - 1})$. Ειδικά στο Σχήμα 3.1 είναι $j = 2$ και $e_1 = e_2 = 1$, άρα $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.

Παράδειγμα 3.1.3. Μια πραγμάτωση του RSA είναι η εξής:

Αλίκη (Δημιουργία κλειδιών): Έστω $p = 13$ και $q = 11$. Άρα, $n = 13 \cdot 11 = 143$ και $\varphi(143) = (13 - 1) \cdot (11 - 1) = 12 \cdot 10 = 120$. Επιλέγεται ένας αριθμός που να μην είναι πολλαπλάσιο του $\varphi(143)$· έστω $e = 7$ και ο εκτεταμένος αλγόριθμος του Ευκλείδου δίδει:

i	υπόλοιπο r_i	πηλίκο q_{i-1}	$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$	$t_i = t_{i-2} - q_{i-1} t_{i-1}$
0	120		1	0
1	7		0	1
2	1	17	$1 - 17 \cdot 0 = 1$	$0 - 17 \cdot 1 = -17$

Επαλήθευση: $1 = 1 \cdot 120 + (-17) \cdot 7$. Άρα, $d = -17 \equiv 103 \pmod{120}$.

Αλίκη: Κρατάει μυστικά τα $p = 13$, $q = 11$ και $d = 103$.

Δημοσιοποιεί τα $n = 143$ και $e = 7$.

Βασίλης: Επιθυμεί να στείλει στην Αλίκη το μήνυμα `ATHENS`. Χρησιμοποιεί (για παράδειγμα) την αντιστοιχία `ASCII`, όπου `A`=65, `B`=66, ..., `Y`=89, `Z`=90 και ␣=43. Έτσι `ATHENS` $\rightsquigarrow$ 65 84 72 69 78 83, ήτοι το αλφαριθμητικό μετατρέπεται σε αριθμητικό. Το αριθμητικό αποτέλεσμα χωρίζεται σε μέρη μήκους μικρότερο του $n = 143$ το καθ' ένα, έστω 65-84-72-69-78-83 (ήτοι μήκους 2 το κάθε μέρος). Κάθε σε κάθε μέρος δρα η συνάρτηση κρυπτογράφησης $E_{143,7}(m) := m^7 \pmod{143}$ κι έτσι

$$65^7 \pmod{143} = 65, \quad 84^7 \pmod{143} = 72, \quad 72^7 \pmod{143} = 19,$$
$$69^7 \pmod{143} = 108, \quad 78^7 \pmod{143} = 78, \quad 83^7 \pmod{143} = 8.$$

Ο Βασίλης αποστέλλει στην Αλίκη το αριθμητικό: 65-72-19-108-78-8.

Αλίκη: Εφαρμόζοντας τη συνάρτηση $D_{143,103}(c) := c^{103} \pmod{143}$ κάθε μέρος του κρυπτοκειμένου δίδει το αντίστοιχο μέρος του απλού κειμένου. ⊣

3.1.2.Α΄ Η συνάρτηση Carmichael

Ορισμός 3.1.4. Ορίζεται η **συνάρτηση Carmichael** του $n \in \mathbb{N}$ ως

$$\lambda(n) := \min\{m \in \mathbb{N} : (\forall \alpha \in \mathbb{Z}_n)\big[\mu\kappa\delta(\alpha, n) = 1 \implies (\alpha^m \equiv 1 \pmod{n})\big]\}$$

Στο Σχήμα 3.1:

- αντί του $\varphi(n)$ υπολογίζεται το $\lambda(n) = \epsilon\kappa\pi(\lambda(p), \lambda(q)) = \epsilon\kappa\pi(p-1,\, q-1)$·
- η απαίτηση ‘‘$1 \leqslant e \leqslant \varphi(n)$, ώστε $\mu\kappa\delta(e, \varphi(n)) = 1$’’ αντικαθίσταται με την ‘‘$1 \leqslant e \leqslant \lambda(n)$, ώστε $\mu\kappa\delta(e, \lambda(n)) = 1$’’ και τέλος
- για τον εκθέτη αποκρυπτογράφησης πλέον ισχύει ότι $ed \equiv 1 \pmod{\lambda(n)}$ (αντί του πρότερου $ed \equiv 1 \mod \varphi(n)$)·

Η χρήση της συνάρτησης λ του Carmichael αντί της συνάρτησης φ του Euler μειώνει το μέγεθος των αριθμών που χρησιμοποιούνται στο Σχήμα 3.1, αφού:

Πρόταση 3.1.5. $(\forall n \in \mathbb{N})\big[\lambda(n) \mid \varphi(n)\big]$.

Απόδειξη (σκιαγράφηση). Ο αριθμός $\varphi(n) \in \mathbb{N}$ αποτελεί τη τάξη της (πολλαπλασιαστικής) ομάδος $\mathbb{Z}_n^*$. Ο αριθμός $\lambda(n) \in \mathbb{N}$ αποτελεί τον εκθέτη* την ομάδος $\mathbb{Z}_n^*$. Από τη Θεωρία Ομάδων είναι γνωστόν ότι ο εκθέτης μιας πεπερασμένης αβελιανής ομάδας, διαιρεί τη τάξη της ομάδας. □

3.1.2.Β΄ Επιλογή παραμέτρων

Ορισμός 3.1.6. Ορίζεται το **βάρος Hamming** της $w := \alpha_\ell \alpha_{\ell-1} \cdots \alpha_1 \alpha_0 \in \{0,1\}^*$ ως $\mathrm{hw}(w) = \#\{\alpha_i \in \{0,1\} : a_i \neq 0\}$. Εάν $w \in \{0,1,\ldots,9\}^*$, τότε το βάρος Hamming μετράει το πλήθος των μη-μηδενικών ψηφίων στο δεκαδικό ανάπτυγμα του w.

Επιλογή των πρώτων αριθμών $p, q \in \mathbb{N}$:

- Από το Θεώρημα Πρώτων Αριθμών, υπάρχουν περίπου $\frac{2^d}{d} - \frac{2^{d-1}}{d-1}$ πρώτοι αριθμοί των $d \in \mathbb{N}$ δυφίων.
- Η διαφορά $|p - q|$ δεν θα πρέπει να είναι ούτε μικρή, ούτε μεγάλη.
- Ο $\mu\kappa\delta(p-1,\, q-1) \in \mathbb{N}$ δεν θα πρέπει να είναι μεγάλος.
- Οι $p-1 \in \mathbb{N}$ και $q-1 \in \mathbb{N}$ πρέπει να έχουν μεγάλους πρώτους παράγοντες.
- Οι πρώτοι αριθμοί $p, q \in \mathbb{N}$ πρέπει να είναι **ασφαλείς** (ήτοι οι $\frac{p-1}{2}, \frac{q-1}{2} \in \mathbb{N}$ να είναι επίσης πρώτοι αριθμοί).

*Ως **εκθέτης** μιας ομάδος ορίζεται το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων της ομάδος. Εν περιπτώσει όπου κάτι τέτοιο δεν καθίσταται εφικτό ο δείκτης ορίζεται ως $+\infty$.

Η επιλογή του εκθέτη κρυπτογράφησης $e \in \mathbb{Z}_n^*$**:**

- Ο αλγόριθμος Επαναλαμβανόμενου Τετραγωνισμού υπολογίζει το $x^e \pmod n$ με $\log_2 e + \mathrm{hw}(e)$ πολλαπλασιασμούς. Για $e \in \{3, 17, 65537\}$ ο αλγόριθμος δεν πραγματοποιεί αρκετούς πολλαπλασιασμούς.
- Η επιλογή $e = 3$ έχει αποδειχθεί από τον Dan Boneh το 1999 στο [Bo99] ως μη αξιόπιστη σε μερικές εφαρμογές [όρα §3.1.4.Β΄].
- Θα πρέπει να αποτελείται από μικρό πλήθος δυφίων (bits) και να διαθέτει μικρό βάρος Hamming –όπως ο $e = 2^{16} - 1 = 65537$.

Η επιλογή του εκθέτη αποκρυπτογράφησης $d \in \mathbb{Z}_n^*$**:**

Δεν πρέπει να είναι πολύ μικρή [όρα §3.1.4.Γ΄].

3.1.3 Ασφάλεια

3.1.3.Α΄ Σημαντική ασφάλεια

Έστω πως ο αντίπαλος κατέχει το κρυπτοκείμενο $c \in \mathbb{Z}_n$ και επί πλέον είναι σε θέση να γνωρίζει το θέμα ενός μηνύματος $m \in \mathbb{Z}_n$, αλλά όχι το ίδιο το μήνυμα $m \in \mathbb{Z}_n$ και αμφιταλαντεύεται ανάμεσα στα

$$m_0 := f(\text{``}\texttt{BUY IEEE}\text{''}) \qquad\qquad m_1 := f(\text{``}\texttt{SELL IEEE}\text{''})$$

όπου $f : \{A, B, C, \ldots, Y, Z, \sqcup\}^* \longrightarrow \mathbb{Z}_n$.

Ισχυρισμός. Το κρυπτοσύστημα RSA δεν είναι IND-CPA ασφαλές.

Απόδειξη (Ισχυρισμού). Όντας το κρυπτοσύστημα αιτιοκρατικό, ο αντίπαλος μπορεί να υπολογίσει τα $c_0 := m_0^e \pmod n$ και $c_1 := m_1^e \pmod n$ και να τα συγκρίνει με το $c \in \mathbb{Z}_n$. □

Ισχυρισμός. Το κρυπτοσύστημα RSA δεν είναι IND-CCA ασφαλές.

Απόδειξη (Ισχυρισμού). Ο αντίπαλος είναι σε θέση να αποκρυπτογραφεί μηνύματα της επιλογής του εκτός από το $c \in \mathbb{Z}_n$ που τον ενδιαφέρει. Γνωρίζει όμως ότι $c := m_b^e \pmod n$ είτε για $b = 0$, είτε για $b = 1$, δίχως να ξέρει το $b \in \{0, 1\}$.

1: Επιλέγει $x \in \mathbb{Z}_n$.

2: Αποκρυπτογραφεί το $c' := c_b x^e \pmod n$ και ανακτάει το κείμενο $m' \in \mathbb{Z}_n$.

3: Τώρα $m_b = \frac{m'}{x}$ (αφού $(\frac{m'}{x})^e = \frac{c'}{x^e} \equiv c_b \pmod n = m_b^e \pmod n$).

4: Αποφαίνεται πιο από τα $m_0, m_1 \in \mathbb{Z}_n$ είναι το $m_b \in \mathbb{Z}_n$. □

3.1.3.Β΄ Επίθεση στην ισοτιμία

Μέχρι τώρα είδαμε έμμεσους τρόπους παραβίασης του κρυπτοσυστήματος RSA. Το πρόβλημα στο οποίο το κρυπτοσύστημα στηρίζει την ασφάλειά του είναι:

Το πρόβλημα RSA$[n, e]$: Έστω $n = pq \in \mathbb{N}$, για κάποιους πρώτους αριθμούς $p, q \in \mathbb{N}$, $e \in \mathbb{Z}_n^*$, με $\mu\kappa\delta(e, \varphi(n)) = 1$ και $c \in \mathbb{Z}_n$. Να βρεθεί το σύνολο

$$\{m \in \mathbb{Z}_n : c \equiv m^e \pmod n\} \qquad (e\text{-οστές ρίζες υπόλοιπο } n)$$

δίχως οι πρώτοι αριθμοί $p, q \in \mathbb{N}$ να είναι γνωστοί.

Η πεποίθηση πως η αντιστροφή της $E_{n,e} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, με $E_{n,e} := x^e \pmod n$, είναι δύσκολη δίχως τη γνώση των $(p, q, d) \in \mathbb{N} \times \mathbb{Z} \times \mathbb{Z}_n^*$ καλείται **υπόθεση RSA**.

Το πρόβλημα RSA_KINV$[n, e]$: Έστω $n = pq \in \mathbb{N}$, για κάποιους πρώτους αριθμούς $p, q \in \mathbb{N}$, $e \in \mathbb{Z}_n^*$, με $\mu\kappa\delta(e, \varphi(n)) = 1$ και $c \in \mathbb{Z}_n$. Να βρεθεί η τιμή $e^{-1} \bmod \varphi(n)$, δίχως οι πρώτοι αριθμοί $p, q \in \mathbb{N}$ να είναι γνωστοί.

Θεώρημα 3.1.7. Ισχύει ότι RSA$[n, e] \preceq$ RSA_KINV$[n, e]$.

Απόδειξη. Εάν από το RSA_KINV$[n, e]$ βρεθεί $d := e^{-1} \pmod{\varphi(n)}$, τότε για το $c := m^e \bmod n$, προκύπτει $c^d = (m^e)^d = m^{ed} = m^{1+k\varphi(n)} \equiv m \pmod n$. □

Το πρόβλημα COMPUTE$[\varphi(n)]$: Έστω $n = pq \in \mathbb{N}$, για κάποιους πρώτους αριθμούς $p, q \in \mathbb{N}$ και $\varphi(n) \in \mathbb{N}$. Να βρεθούν οι πρώτοι αριθμοί $p, q \in \mathbb{N}$.

Το πρόβλημα FACT$[n]$: Έστω $n = pq \in \mathbb{N}$, για κάποιους πρώτους αριθμούς. Να βρεθούν οι πρώτοι αριθμοί $p, q \in \mathbb{N}$.

Θεώρημα 3.1.8. Ισχύει ότι COMPUTE$[\varphi(n)] \equiv$ FACT$[n]$.

Απόδειξη. Εάν ο $\varphi(n) \in \mathbb{N}$ ήταν γνωστή ποσότητα, τότε προκύπτει η εξίσωσης

$$\left.\begin{array}{r} n = pq \implies q = n/p \\ \varphi(n) = (p-1)(q-1) \end{array}\right\} \implies p^2 - (n - \varphi(n) + 1)p + n = 0 \qquad (3.1)$$

οι λύσεις της είναι οι πρώτοι παράγοντες του $p, q \in \mathbb{N}$ $n \in \mathbb{N}$. Άρα, ο υπολογισμός του $\varphi(n) \in \mathbb{N}$ είναι ισοδύναμος με την παραγοντοποίηση του $n \in \mathbb{N}$. □

Θεώρημα 3.1.9. Ισχύει ότι RSA_KINV$[n, e] \equiv$ FACT$[n]$

Απόδειξη. Αποδεικνύονται οι ακόλουθες αναγωγές:

RSA_KINV$[n, e] \preceq$ FACT$[n]$: Εάν είναι γνωστή η παραγοντοποίηση του $n \in \mathbb{N}$, τότε είναι γνωστό και το $\varphi(n) \in \mathbb{N}$ και με χρήση το εκτεταμένου αλγορίθμου του Ευκλείδου στα $e \in \mathbb{Z}_n^*$ και $\varphi(n) \in \mathbb{N}$, όπου $\mu\kappa\delta(e, \varphi(n)) = 1$ μπορεί να υπολογιστεί ο εκθέτης αποκρυπτογράφησης $d \in \mathbb{Z}_n^*$.

$\texttt{RSA\_KINV}[n, e] \succeq \texttt{FACT}[n]$: Θεωρούνται γνωστά: η ισοτιμία $n \in \mathbb{N}$, ο εκθέτης κρυπτογράφησης $e \in \mathbb{Z}_n^*$ και από το πρόβλημα $\texttt{RSA\_KINV}[n, e]$ παρέχεται και ο εκθέτης αποκρυπτογράφησης $d \in \mathbb{Z}_n^*$. Η βασική ιδέα είναι η εξής:

> Εύρεση ενός $x \in \mathbb{Z}_n^*$, με $x \not\equiv 1 \pmod n$, αλλά $x^2 \equiv 1 \pmod n$ (ήτοι μιας μη-τετριμμένης τετραγωνική ρίζας της μονάδος) και τότε οι $\mu\kappa\delta(x+1, n) \in \mathbb{N}$ και $\mu\kappa\delta(x-1, n) \in \mathbb{N}$ αποτελούν μη-τετριμμένους παράγοντες της ισοτιμίας $n \in \mathbb{N}$.

Όντας $ed \equiv 1 \pmod{\varphi(n)}$, έπεται πως $ab - 1 \equiv 0 \pmod{\varphi(n)}$. Διαιρείται ο αριθμός $ed - 1 \in \mathbb{N}$ με το 2, όσες φορές αυτό καθίσταται δυνατόν, έτσι $ed - 1 = 2^s r$, για $s \in \mathbb{N}_0$ και $r \in 2\mathbb{N}_0 + 1$

Ισχυρισμός. $(\forall w \in \mathbb{Z}_n^*)\big[w^{(2^s)r} \equiv 1 \mod n\big]$.

> *Απόδειξη (Ισχυρισμού).* $ed \equiv 1 \pmod{\varphi(n)} \Longrightarrow (\exists k \in \mathbb{Z})[ed = 1 + k\varphi(n)]$. Τώρα, $w^{(2^s)r} = w^{ed-1} = w^{k\varphi(n)} \equiv 1 \mod n$. ♠

Άρα, εάν $v := w^{(2^{s-1})r} \not\equiv \pm 1 \pmod n$, τότε οι $\mu\kappa\delta(v+1, n)$ και $\mu\kappa\delta(v-1, n)$ είναι μη-τετριμμένοι παράγοντες της ισοτιμίας $n \in \mathbb{N}$. □

Άρα: $\texttt{RSA}[n, e] \preceq \texttt{RSA\_KINV}[n, e] \equiv \texttt{FACT}[n] \equiv \texttt{COMPUTE}[\varphi(n)]$. Οι Burt Kaliski και Ron Rivest το 2003 στο [KR03] απέδειξαν πως το $\texttt{RSA}[n, e]$ φαντάζει ευκολότερο του $\texttt{FACT}[n]$.

Τυχαία τετράγωνα

Μία ακόμη επίθεση έγκειται στην εύρεση $x, y \in \mathbb{N}$, ώστε $x \equiv \pm y \pmod n$ και $x^2 \not\equiv y^2 \pmod n$ και τότε θα είναι $n \mid (x-y)(x+y)$, αλλά $n \nmid (x-y)$ και $n \nmid (x+y)$. Συνεπώς, είτε ο $\mu\kappa\delta(x-y, n) \in \mathbb{N}$, είτε ο $\mu\kappa\delta(x+y, n) \in \mathbb{N}$ είναι μη-τετριμμένος παράγοντας της ισοτιμίας $n \in \mathbb{N}$. Για την εύρεση των $x, y \in \mathbb{N}$ όπως παραπάνω παρέχεται ο αλγόριθμος των τυχαίων τετραγώνων του John Dixon [Dix81].

Αλγόριθμοι του Pollard

Υπάρχουν επιθέσεις που στοχεύουν στην παραγοντοποίηση της ισοτιμίας $n \in \mathbb{N}$, όπως οι αλγόριθμοι $p - 1$ και ρ του Pollard [Po74, Po74].

3.1.4 Επιθέσεις

3.1.4.Α΄ Επίθεση σε κοινή ισοτιμία

Έστω πως μία έμπιστη αρχή (στις Αποδείξεις Μηδενικής Γνώσης καλείται: *κέντρο*) επιθυμεί να χρησιμοποιήσει την ίδια ισοτιμία $n = pq \in \mathbb{N}$ για όλους

τους χρήστες της. Έτσι κοινοποιεί τα δημόσια κλειδιά τους $\{e_i\}$ και διανέμει προσωπικά σε κάθε χρήστη i τον εκθέτη $d_i \in \mathbb{Z}_n^*$ αποκρυπτογράφησης που θα χρησιμοποιεί.

Ισχυρισμός. Κάθε χρήστης μπορεί να υπολογίσει σε αιτιοκρατικό τετραγωνικό χρόνο τον μυστικό εκθέτη αποκρυπτογράφησης ενός άλλου χρήστη, *δίχως να παραγοντοποιήσει την ισοτιμία* $n \in \mathbb{N}$.

Πράγματι, έστω δύο χρήστες A, B του δικτύου. Ο B μπορεί να υπολογίσει το $d_A \in \mathbb{Z}_n^*$ ως εξής: $e_b d_b \equiv 1 \pmod{\varphi(n)} \implies (\exists k \in \mathbb{Z})\big[e_b d_b - 1 = k\varphi(n)\big]$. Έστω

$$\alpha := \max\{\gamma \in \mathbb{Z} : \gamma \mid (e_B d_B - 1) \text{ και } \mu\kappa\delta(\gamma, e_A) = 1\}, \qquad t := \tfrac{e_B d_B - 1}{\alpha}$$

Για τον υπολογισμό της τιμής του α, τίθενται:

$$g_i := \begin{cases} e_B d_B - 1, & \text{εάν } i = 0 \\ \frac{g_{i-1}}{h_{i-1}}, & \text{αλλιώς} \end{cases} \qquad h_i := \mu\kappa\delta(g_i, e_A)$$

και πραγματοποιούνται υπολογισμοί έως ότου $h_{i_0} = 1$ ($\implies \alpha = g_{i_0}$), για κάποιο $i_0 \in \mathbb{N}$ (εάν $h_i \geqslant 2$, τότε $g_{i+1} \leqslant \frac{1}{2} g_i$ κι άρα βρίσκεται κάποιο $i_0 \in \mathbb{N}$, με $h_{i_0} = 1$, σε πολυωνυμικό χρόνο). Όντας $\mu\kappa\delta(a, e_A) = 1$, από το εκτεταμένο αλγόριθμο του Ευκλείδου προκύπτει πως $(\exists x, y \in \mathbb{Z})[x\alpha + y e_A = 1]$. Τελικώς, $y e_A \equiv 1 \pmod{\varphi(n)}$, διότι $\varphi(n) \mid \alpha$ μιας και $\alpha t = k\varphi(n)$ και $\mu\kappa\delta(t, \varphi(n)) = 1$. Έτσι, η τιμή $y \pmod n$ μπορεί να χρησιμοποιηθεί αντί της $d_A \in \mathbb{Z}_n^*$.

3.1.4.Β΄ Επίθεση σε μικρό εκθέτη κρυπτογράφησης

Όπως αναφέρθηκε και στην §3.1.2, η επιλογή μικρού εκθέτη κρυπτογράφησης $e \in \mathbb{Z}_n^*$ μπορεί να αποβεί μοιραία σε μερικές περιπτώσεις. Έστω, λοιπόν, ότι

- $e = 3$.

και ανακύπτει η ανάγκη για την αποστολή του μηνύματος $m = 105$ σε τρεις διαφορετικές οντότητες. Επιλέγονται οι ισοτιμίες $n_1 = 377, n_2 = 391$ και $n_3 = 589$, οι οποίες είναι ανά δύο πρώτοι αριθμοί, μία για κάθε παραλήπτη. Συνεπώς,

$$c_1 := 102^3 \pmod{377} \equiv 330 \qquad c_2 := 102^3 \pmod{391} \equiv 34$$
$$c_3 := 102^3 \pmod{589} \equiv 419$$

Ο αντίπαλος επιθυμεί να επιλύσει το σύστημα

$$\Big\{c_1 \equiv 330 \pmod{377}, \qquad c_2 \equiv \pmod{391}, \qquad c_3 \equiv 419 \pmod{589}\Big\}$$

Εξ υποθέσεως $(\forall i,j=1,2,3)[i\neq j \implies \mu\kappa\delta(n_i,n_j)=1]$. Έτσι η λύση του παραπάνω συστήματος παρέχεται από το Κινέζικο Θεώρημα Υπολοίπων, όπου ένας τύπος για την εύρεση της κοινής ισοτιμία είναι ο εξής:

$$c = c_1(n_2\cdot n_3)\left[(n_2\cdot n_3)^{-1}\right]_{n_1} + c_2(n_1\cdot n_3)\left[(n_1\cdot n_3)^{-1}\right]_{n_2} + c_3(n_1\cdot n_2)\left[(n_1\cdot n_2)^{-1}\right]_{n_3}$$

Ως $\left[a^{-1}\right]_b$ συμβολίζεται ο πολλαπλασιαστικός αντίστροφος του $a\in\mathbb{Z}_b^*$ στο $\mathbb{Z}_b^*$ (ο οποίος εδώ είναι καλώς ορισμένος, όντας οι $n_1,n_2,n_3\in\mathbb{N}$ ανά δύο πρώτοι αριθμοί). Θεωρείται $t_i = c_i(n_j\cdot n_k)\left[(n_j\cdot n_k)^{-1}\right]_{n_i}$, για $i\in\{1,2,3\}$, $j\in\{1,2,3\}\setminus\{i\}$ και $k\in\{1,2,3\}\setminus\{i,j\}$ κι υπολογίζονται

$$\begin{aligned} t_1 &= 330(391\cdot 589)\left[(391\cdot 589)^{-1}\right]_{377} = 24471571740\\ t_2 &= 34(377\cdot 589)\left[(377\cdot 589)^{-1}\right]_{391} = 505836734\\ t_3 &= 419(377\cdot 391)\left[(377\cdot 391)^{-1}\right]_{589} = 35452267942 \end{aligned}$$

$\therefore c = t_1+t_2+t_3 \pmod{n_1n_2n_3} = 1061208$. Πλέον $\sqrt[3]{c} = \sqrt[3]{1061208} = 102 = m$.

Η επιλογή $e=3$ δεν αποτελεί κάποια εγγενή παθογένεια. Η επίθεση επιτυγχάνει και για μεγαλύτερες τιμές του $e\in\mathbb{N}$, αρκεί (ώστε να μπορέσει να εφαρμοσθεί το Κινέζικο Θεώρημα Υπολοίπων) να υπάρχουν τουλάχιστον e παραλήπτες.

3.1.4.Γ′ Επίθεση σε μικρό εκθέτη αποκρυπτογράφησης

Ορισμός 3.1.10. Ένα **πεπερασμένο συνεχές κλάσμα** είναι ένας πραγματικός αριθμός της μορφής

$$[a_0;a_1,\ldots,a_{n-1},a_n] = a_0 + \cfrac{1}{a_1+\cfrac{1}{a_2+\cdots+a_{n-1}+\cfrac{1}{a_n}}} \qquad \text{όπου } a_0\in\mathbb{R},\ a_1,\ldots,a_n\in\mathbb{R}_+^*$$

Ο $c_k := [a_0;a_1,\ldots,a_k]\in\mathbb{Q}$, $k=0,1,\ldots,n$ ονομάζεται k-**οστός συγκλίνων** του x.

Έστω $n=pq\in\mathbb{N}$, για κάποιους πρώτους αριθμούς $p,q\in\mathbb{N}$ κι έστω ότι ο εκθέτης κρυπτογράφησης $e\in\mathbb{Z}_n^*$ επελέγει αρκετά μεγάλος, τότε ο εκθέτης αποκρυπτογράφησης $d\in\mathbb{Z}_n^*$ θα είναι αρκετά μικρός. Ο Michael Weiner το 1990 στο [Wei90] απέδειξε πως είναι δυνατόν να ανακτηθεί ο $d\in\mathbb{Z}_n^*$ όταν:

- $d \lneqq \frac{1}{3}\sqrt[4]{n}$.

Θεώρημα 3.1.11. Έστω $x\in\mathbb{R}$, $a\in\mathbb{Z}$ και $b\in\mathbb{N}$. Εάν $|x-\frac{a}{b}|\lneqq\frac{1}{2b^2}$, τότε το $\frac{a}{b}\in\mathbb{Q}$ εμφανίζεται στην προσέγγιση με συνεχή κλάσματα.

Ισχύει[†] ότι $\left|{}^{e}/_{n} - {}^{k}/_{d}\right| \lneqq \frac{1}{2d^2}$. Από το Θεώρημα 3.1.11 το κλάσμα $\frac{k}{d} \in \mathbb{Q}$ (το οποίο είναι απλό, όντας $ed = 1 + k\varphi(n)$) εμφανίζεται στην προσέγγιση του $\frac{e}{n} \in \mathbb{Q}$ με συνεχή κλάσματα. Πλέον, ο αντίπαλος μπορεί να βρει το $d \in \mathbb{Z}_n^*$ κρυπτογραφώντας ένα μήνυμα της επιλογής του $m \in \mathbb{Z}_n$ με χρήση του $e \in \mathbb{Z}_n^*$ και δοκιμάζοντας κάθε έναν από τους παρονομαστές της προσέγγισης, έως ότου προκύψει το αρχικό μήνυμα $m \in \mathbb{Z}_n$.

Αντί της συνάρτησης φ του Euler, θα χρησιμοποιηθεί η συνάρτηση λ του Carmichael [όρα §3.1.2.Α΄]. Αναπτύσσεται ο εξής συλλογισμός

$$ed = 1 \pmod{\epsilon\kappa\pi(p-1,\, q-1)} \implies (\exists K \in \mathbb{Z})[ed = K \cdot \epsilon\kappa\pi(p-1,\, q-1) + 1]$$

Τώρα $ab = \mu\kappa\delta(a,b) \cdot \epsilon\kappa\pi(a,b)$. Για $G := \mu\kappa\delta(p-1,\, q-1)$ προκύπτει:

$$\implies ed = \frac{K}{G}(p-1)(q-1) + 1$$

Απλοποιώντας το κλάσμα ${}^{K}/_{G}$, έστω $k := \frac{K}{\mu\kappa\delta(K,G)}$ και $g := \frac{G}{\mu\kappa\delta(K,G)}$, τότε:

$$\implies ed = \frac{k}{g}(p-1)(q-1) + 1 \implies \frac{e}{pq} = \frac{k}{dg}(1-\delta)$$

όπου $\delta = \dfrac{p+q-1-{}^{g}/_{k}}{pq}$. Έτσι η τιμή $\dfrac{e}{pq} = \dfrac{e}{n}$ (η οποία υπολογίζεται από το δημόσιο κλειδί) είναι κατά λίγο μικρότερη της ${}^{k}/_{dg}$.

Παράδειγμα 3.1.12. Έστω πως σε μια εκτέλεση του RSA το δημόσιο κλειδί έγκειται στο $(n, e) := (90581, 17993)$. Η παρακάτω επίθεση θα δώσει έναν μικρό $d \in \mathbb{Z}_n^*$ (για την ακρίβεια $d \lneqq \frac{1}{3}\sqrt[4]{n} \simeq 5,7828$), τέτοιο ώστε $ed \equiv 1 \pmod{n}$. Μερικοί υπολογισμοί δίνουν: ${}^{e}/_{n} = \frac{17993}{90581} = [0; 5, 29, 4, 1, 3, 2, 4, 3]$. Μία προσέγγιση του ${}^{k}/_{d}$ δίδεται από τους πρώτους συγκλίνοντες[‡] του ${}^{e}/_{n}$ οι οποίοι είναι:

$$\frac{k}{d} = 0,\ \frac{1}{5},\ \frac{29}{146},\ \frac{117}{589},\ \frac{146}{735},\ \frac{555}{2794},\ \frac{1256}{6323},\ \frac{5579}{28086},\ \frac{17993}{90851}$$

Με δοκιμές προκύπτει πως ο $c_1 = {}^{1}/_{5}$, δηλαδή $k = 1$ και $d = 5$ (και $e = 17993$), παραγοντοποιεί το $n \in \mathbb{N}$ μιας και: $\varphi(n) = \frac{ed-1}{k} = \frac{17993 \cdot 5 - 1}{1} = 89964$. Από την εξίσωση (3.1) για $e = 17993$ και $n = 90581$ προκύπτει το πολυώνυμο $p^2 - 618p + 90581 = 0$, οι ρίζες του οποίου είναι $p = 379$ και $q = 239$, όπου $379 \cdot 239 = 90581 = n$ κι άρα ευρέθει η παραγοντοποίηση του $n \in \mathbb{N}$. ⊣

[†] Συνάγεται από το γεγονός ότι $n - \varphi(n) \lneqq 3\sqrt{n}$ και ότι $ed = 1 + k\varphi(n) \implies k \lneqq d$.

[‡] Για $x = [a_0; a_1, \ldots, a_n] \in \mathbb{Q}$, τότε $c_k = {}^{p_k}/_{q_k} \in \mathbb{Q}$, $k = 0, \ldots, n$, όπου

$$p_k := \begin{cases} a_0, & \text{εάν } k = 1 \\ a_1 a_0 + 1, & \text{εάν } k = 2 \\ a_k p_{k-1} + p_{k-2}, & \text{εάν } k \geqslant 3 \end{cases} \qquad q_k := \begin{cases} 1, & \text{εάν } k = 1 \\ a_1, & \text{εάν } k = 2 \\ a_k q_{k-1} + q_{k-2}, & \text{εάν } k \geqslant 3 \end{cases}$$

Μία πιο εξεζητημένη ανάλυση είναι αυτή των Dan Boneh και Glenn Durfee το 2000 στο [BD00], όπου αντί για $n^{0.25}(=\sqrt[4]{n})$ επιτυγχάνουν να υπολογίσουν τον εκθέτη αποκρυπτογράφησης $d \in \mathbb{Z}_n^*$, όταν $d \lneqq n^{0.292}$.

Η επιλογή μικρού εκθέτη αποκρυπτογράφησης, καθιστά το κρυπτοσύστημα ευάλωτο σε επιθέσεις εξαντλητικής αναζήτησης.

3.1.5 Ανάκτηση μερικής πληροφορίας

Ενδέχεται να διαρρέει κάποια πληροφορία για το απλό κείμενο, η οποία καλείται **μερική πληροφορία**. Παραδείγματα μερικής πληροφορίας αποτελούν τα εξής:

Η γνώση του τελευταίου δυφίου του μηνύματος $m \in \mathbb{Z}_n$, γεγονός που υλοποιείται από τη συνάρτηση $\text{parity}_{n,e}(E_{n,e}(m)) = \begin{cases} 1, \text{ εάν } m \equiv 1 \pmod 2 \\ 0, \text{ εάν } m \equiv 0 \pmod 2 \end{cases}$.

Η γνώση εάν $0 \leqslant m \leqslant n/2$ **ή εάν** $n/2 \lneqq m \lneqq n-1$, γεγονός που υλοποιείται από τη συνάρτηση $\text{loc}_{n,e}(E_{n,e}(m)) = \begin{cases} 0, \text{ εάν } m \leqslant n/2 \\ 1, \text{ εάν } m > n/2 \end{cases}$.

Η διρρέουσα μερική πληροφορία μπορεί να χρησιμοποιηθεί ώστε να ανακτηθεί το αρχικό μήνυμα. Η απόδειξη ότι ένα κρυπτογραφικό πρωτόκολλο δεν διαρρέει πληροφορία, η διαρροή συνδέεται με κάποιο υπολογιστικά δύσκολο πρόβλημα.

Αποδεικνύεται στο [GMT82] πως τα να ανακτήσει ένας αντίπαλος το απλό κείμενο στο Σχήμα 3.1 είναι ισοδύναμο με τον υπολογσμό της συνάρτησης $\text{parity}_{n,e}$ το οποίο είναι ισοδύναμο με τον υπολογισμό της συνάρτησης $\text{loc}_{n,e}$. Μία εκ των παραπάνω (διπλών) συνεπαγωγών υλοποιείται μέσω:

Αλγόριθμος 3.1.13 OracleRSADecr$((n,e),c)$: Αποκρυπτ/φηση με χρήση $\text{loc}_{n,e}$

Είσοδος: Το δημόσιο κλειδί $(n,e) \in \mathbb{N} \times \mathbb{Z}_n^*$ κι ένα κρυπτοκείμενο $c \in \mathbb{Z}_n$.
Δεδομένα: Αποδοτική αλγοριθμική υλοποίηση της συνάρτησης $\text{loc}_{n,e}$.
΄Εξοδος: Το απλό κείμενο $m \in \mathbb{Z}_n$ που αντιστοιχεί στο κρυπτοκείμενο $c \in \mathbb{Z}_n$.

1: $k \leftarrow \lfloor \log_2 n \rfloor$; $c_0 \leftarrow c$; $low \leftarrow 0$; $hi \leftarrow n$;
2: **για** $(i = 0, 1, \ldots, k)$ **επανάλαβε**
3: $\quad mid \leftarrow (hi + low)/2$;
4: $\quad$ **εάν** $(\text{loc}_{n,e}(c_i) = 1)$ **τότε**
5: $\quad\quad low \leftarrow mid$;
6: $\quad$ **αλλιώς**
7: $\quad\quad hi \leftarrow mid$;
8: $\quad$ **τέλος εάν**
9: $\quad c_{i+1} \leftarrow (c_i \cdot E_{n,e}(2)) \mod n$;
10: **τέλος για**
11: **επίστρεψε** $\lfloor hi \rfloor$;

Παράδειγμα 3.1.14. Για δημόσιο κλειδί του RSA $(n, e) = (1457, 779)$ και κρυπτοκείμενο $c = 722 \in \mathbb{Z}_{1457}$, είναι $\lfloor \log_2 n \rfloor = 10$. Έστω

$i =$	0	1	2	3	4	5	6	7	8	9	10
$\mathrm{loc}_{1457,779}(c_i) =$	1	0	1	0	1	1	1	1	1	0	0

Με τα παραπάνω δεδομένα, ο αλγόριθμος 3.1.13 δίδει:

$i =$	αρχικ/ση	0	1	...	5	...	9	10
$\mathrm{low} =$	0.00	728.50	728.50	$\cdots$	956.16	$\cdots$	998.84	998.84
$\mathrm{hi} =$	1457.00	1457.00	1092.75	$\cdots$	1001.69	$\cdots$	1000.26	999.55
$\mathrm{mid} =$	728.50	1092.75	910.62	$\cdots$	978.92	$\cdots$	999.55	999.55

κι άρα $m = \lfloor \mathrm{hi} \rfloor = \lfloor 999.55 \rfloor = 999$. ⊣

3.1.6 Βελτιώσεις

Συμβολισμός. Έστω $\alpha, \beta \in \{0,1\}^s$, $\gamma \in \{0,1\}^t$, για $s, t \in \mathbb{N}$. Ως $\alpha \oplus \beta$ συμβολίζεται η πράξη της *αποκλειστικής διάζευξης* ανάμεσα στις α, β. Ως $\alpha \parallel \gamma$ συμβολίζεται η *συγκόλληση* ακολουθιών.

Το 1985 στο [BR94] προτάθηκε από τους Mihir Bellare και Phillip Rogaway, ένα πιο αποτελεσματικό σχήμα κρυπτογράφησης ονόματι OAEP (Optimal Asymmetric Encryption Padding) το οποίο χρησιμοποιεί τη τεχνική του παραγεμίσματος και συναρτήσεις κατακερματισμού:

- Έστω $n := k - k_0 - k_1$ όπου $k, k_0, k_1 \in \mathbb{N}$.
  - Το $k_0 \in \mathbb{N}$ είναι επιλεγμένο ώστε ένας αντίπαλος να μην έχει υπολογιστική δύναμη που να ξεπερνάει τα 2^{k_0} βήματα.
- Στο Σχήμα 3.1:
  - Θεωρούνται δύο δημοσίως γνωστές συναρτήσεις κατακερματισμού, η $\mathcal{G} : \{0,1\}^{k_0} \longrightarrow \{0,1\}^{n+k_1}$ και η $\mathcal{H} : \{0,1\}^{n+k_1} \longrightarrow \{0,1\}^{k_0}$.
  - Ο χώρος των απλών κειμένων είναι ο $\mathbb{Z}_n^* \subseteq \{0,1\}^k$.

Δημιουργία κλειδιών: Όπως στο Σχήμα 3.1.

Κρυπτογράφηση: Ο Βασίλης επιθυμεί να αποστείλει το μήνυμα x μήκους το πολύ $k - 320$ δυφίων. Επιλέγει τυχαία ένα $r \in \{0,1\}^{k_0}$, θεωρεί

$$m := \big[(x \parallel 0^{k_1}) \oplus \mathcal{G}(r)\big] \parallel \Big[r \oplus \mathcal{H}\big((x \parallel 0^{k_1}) \oplus \mathcal{G}(r)\big)\Big]$$

και κρυπτογραφεί όπως στο Σχήμα 3.1.

Αποκρυπτογράφηση: Η Αλίκη:

(α′) Ανακτά το m από το κρυπτοκείμενο όπως στο Σχήμα 3.1.

Έστω X, Y ο αριθμός με 2δική αναπαράσταση τα αριστερότερα $n - k_0$ δυφία, τα δεξιότερα k_0 δυφία αντίστοιχα του m.

(β′) Ανακτά το $r = Y \oplus \mathcal{H}(X)$.

(γ′) Ανακτά το $x \parallel 0^{k_1} = X \oplus \mathcal{G}(r)$ και απορρίπτει τα k_1 τελευταία δυφία.

Το OAEP έχει αποδειχθεί ασφαλές έναντι των επιθέσεων CCA. Οι Ronald Cramer και Victor Shoup το 1998 στο [CS98] πρότειναν το OAEP+ μία παραλλαγή του OAEP βασισμένη στο κρυπτοσύστημα El Gamal [EG85].

3.1.7 Σύνοψη

Πλεονεκτήματα RSA: Είναι το ευκολότερο σε κατανόηση και το δημοφιλέστερο όλων των παρομοίων του. Το ιδιωτικό κλειδί δεν μεταδίδεται.

Μειονεκτήματα RSA: Χρειάζονται πράξεις που δεν μπορούν να υλοποιηθούν σε κοινούς υπολογιστές, καθώς απαιτείται μεγάλος αριθμός υπολογιστικών πόρων. Η πολυπλοκότητα των πράξεων το καθιστά το RSA υπολογιστικά πιο αργό (100 ή και 1000 φορές) σε σχέση με το Προηγμένο Σύστημα Κρυπτογράφησης (AES), το οποίο υλοποιείται αποδοτικά σε όλες τις πλατφόρμες υπολογιστών (64, 128, 256, 1024, 2048 δυφίων).

Στην πράξη όμως ένας συνδυασμός των δύο είναι πιο αποδοτικός:

1. Η Αλίκη:
   (α′) Κρυπτογραφεί το μήνυμα προς αποστολή με χρήση του DES με τυχαίο κλειδί.
   (β′) Κρυπτογραφεί το παραπάνω τυχαίο κλειδί μέσῳ του RSA, κάνοντας χρήση του δημοσίου κλειδιού του Βασίλη.
   (γ′) Αποστέλει αμφότερα τα παραπάνω στον Βασίλη.
2. Ο Βασίλης:
   (α′) Αποκρυπτογραφεί το κλειδί που έλαβε μέσῳ του RSA κάνοντας χρήση του ιδιωτικού του κλειδιού και ανακτάει το τυχαίο κλειδί που χρησιμοποίησε η Αλίκη.
   (β′) Αποκρυπτογραφεί το κρυπτοκείμενο που έλαβε κάνοντας χρήση του DES με κλειδί το ανέκτησε παραπάνω.

Η παραπάνω τεχνική καλείται **PGP** (Pretty Good Privacy) και αναπτύχθηκε το 1991 από τον Philip Zimmermann (όρα επίσης [Zi99]).

3.2 Ομομορφική κρυπτογραφία: Paillier

Το κρυπτοσύστημα Paillier αναπτύχθηκε από τον Pascal Paillier στο [Pai99] το 1999. Η ασφάλεια του κρυπτοσυστήματος βασίζεται στην υπόθεση DCRA [όρα §3.2.4.Β΄] η οποία αποτελεί την πεποίθηση πως το πρόβλημα υπολογισμού των n-οστών υπολειμματικων κλάσεων είναι υπολογιστικά δύσκολο.

Συμβολισμός. Θεωρείται $\mathcal{R} := \{pq \in \mathbb{N} : \text{οι } p, q \in \mathbb{N} \text{ είναι πρώτοι αριθμοί}\}$.

3.2.1 Ομομορφική κρυπτογράφηση

Ορισμός 3.2.1. Έστω ένα κρυπτοσύστημα $\mathcal{K} = \langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$ και $\langle M, * \rangle, \langle C, \star \rangle$ ο χώρος των απλών κειμένων και των κρυπτοκειμένων αντιστοίχως καθείς εφοδιασμένος με μία (δική του) πράξη. Το (αιτιοκρατικό/πιθανοκρατικό) κρυπτοσύστημα $\mathcal{K}$ λέγεται πως έχει την ιδιότητα της **μερικής ομομορφικής κρυπτογράφησης** εάν

$$(\forall x_1, x_2 \in M)\big[\mathcal{E}(x_1) \star \mathcal{E}(x_2) = \mathcal{E}(x_1 * x_2)\big]$$

Επίσης θα λέγεται πως το $\mathcal{K}$ παρουσιάζει $*$**-στική ομομορφική ιδιότητα**.

Κάποια μερικώς ομομορφικά κρυπτοσυστήματα είναι: το κρυπτοσύστημα RSA της §3.1.2 (που παρουσιάζει πολλαπλασιαστική υπόλοιπο n ομομορφική ιδιότητα), το κρυπτοσύστημα των Shafi Goldwasser και Silvio Micali [GM82] (που παρουσιάζει προσθετική υπόλοιπο 2 ομομορφική ιδιότητα) και σαφώς το Σχήμα 3.2.

Πλήρης ομομορφική κρυπτογράφηση

Έστω πως σε ένα κρυπτοσύστημα $\mathcal{K} := \langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$ ο χώρος του απλού κειμένου και ο χώρος των κρυπτοκειμένων έχουν τη μορφή δακτυλίου, δηλαδή είναι $(M, *_M, \divideontimes_M)$ και $(C, *_C, \divideontimes_C)$ αντίστοιχα. Το $\mathcal{K}$ λέγεται πως πληροί την ιδιότητα της **πλήρους ομομορφικής κρυπτογράφησης** εάν *διατηρεί τη δομή δακτυλίου*:

$$(\forall m_1, m_2 \in M)\big[\mathcal{E}(m_1) *_C \mathcal{E}(m_2) = \mathcal{E}(m_1 *_M m_2) \text{ και } \mathcal{E}(m_1) \divideontimes_C \mathcal{E}(m_2) = \mathcal{E}(m_1 \divideontimes_M m_2)\big]$$

Τα πλήρως ομομορφικά κρυπτοσυστήματα αποτελούν ισχυρά εργαλεία (ισχυρότερα από τα μερικώς ομομορφικά κρυπτοσυστήματα). Μπορούν να χρησιμοποιηθούν στην κατασκευή προγραμματων που επιλύουν λογικά κυκλώματα: η είσοδος είναι κρυπτογραφημένες αληθοτιμές και η έξοδός η κρυπτογραφημένη επίλυση του κυκλώματος.

Μια πιο λεπτομερής μελέτη για τα πλήρη ομομορφικά κρυπτοσυστήματα καθώς κι ένα πλήρες ομομορφικό σχήμα περιέχονται στο [Li10].

3.2.2 n-οστές υπολλειματικές κλάσεις

Κρυπτογράφηση

Έστω $n \in \mathcal{R}$. Για κάθε $g \in \mathbb{Z}^*_{n^2}$, ορίζεται η συνάρτηση

$$\mathcal{F}_g(m,r) : \mathbb{Z}_n \times \mathbb{Z}^*_n \longrightarrow \mathbb{Z}^*_{n^2} \qquad \mathcal{F}_g(m,r) := g^m \cdot r^n \pmod{n^2} \qquad (g \in \mathbb{Z}^*_{n^2})$$

Το κρυπτοκείμενο που αντιστοιχεί στο απλό κείμενο $m \in \mathbb{Z}_n$, συνίσταται στο $c := \mathcal{F}_g(m,r) = g^m \cdot r^n \pmod{n^2}$, για κάποιο τυχαία επιλεγμένο $r \in \mathbb{Z}^*_n$.

Συμβολισμός. Εάν $I \subseteq \mathbb{N}$ είναι ένα σύνολο δεικτών, η ξένη ένωση μιας οικογενείας συνόλων $\{A_i\}_{i\in I}$, ορίζεται ως $\biguplus_{i\in I} A_i := \bigcup_{i\in I} (\{i\} \times A_i)$.

Ορισμός 3.2.2. Για κάθε $n \in \mathcal{R}$, ορίζονται

$$\mathcal{B}_\alpha := \{x \in \mathbb{Z}^*_{n^2} : \mathrm{ord}_{\mathbb{Z}^*_{n^2}}(x) = n \cdot \alpha\} \subseteq \mathbb{Z}^*_{n^2} \qquad \mathcal{B} := \biguplus_{\alpha=1}^{\lambda(n)} \mathcal{B}_\alpha$$

όπου $\lambda : \mathbb{N} \longrightarrow \mathbb{N}$ είναι η συνάρτηση λ του Carmichael [όρα Ορισμό 3.1.4].

Ορισμός 3.2.3. Έστω $n \in \mathcal{R}$ και $g \in \mathcal{B}$. Ορίζεται η n-**οστή υπολειμματική κλάση του** $w \in \mathbb{Z}^*_{n^2}$ **ως προς** $g \in \mathcal{B}$ (n-th residuosity class of w with respect of g) $[\![w]\!]_g$ ως το μοναδικό $x \in \mathbb{Z}_n$ το οποίο ικανοποιεί το κατηγόρημα:

$$C(x,g,w) \Longleftrightarrow_{\mathrm{o}\rho} (\exists y \in \mathbb{Z}^*_n)[\mathcal{F}_g(x,y) = w] \tag{3.2}$$

Το πρόβλημα που στηρίζεται η ασφάλεια του κρυπτοσυστήματος Paillier είναι

Το πρόβλημα CLASS$[n,g]$: Δεδομένων $n \in \mathcal{R}$, $w \in \mathbb{Z}^*_{n^2}$ και $g \in \mathcal{B}$, να υπολογισθεί η κλάση $[\![w]\!]_g$.

Λήμμα 3.2.4 ([Pai99]). *Το πρόβλημα* CLASS$[n,g]$ *είναι τυχαιοκρατικά αυτο-αναγώγιμο υπεράνω των στοιχείων του* $\mathcal{B}$, *δηλαδή* $(\forall n \in \mathcal{R})(\forall g_1, g_2 \in \mathcal{B})\big[\textit{CLASS}[n,g_1] \equiv \textit{CLASS}[n,g_2]\big]$.

Πόρισμα 3.2.5. *Ισχύει ότι* $(\forall n \in \mathcal{R})(\forall g_1, g_2 \in \mathcal{B})\big[[\![g_1]\!]_{g_2} \equiv [\![g_2]\!]^{-1}_{g_1} \pmod{n}\big]$

Απόδειξη. Για $w = g_1$, το Λήμμα 3.2.4 δίδει ότι $1 = [\![g_1]\!]_{g_1} \equiv [\![g_1]\!]_{g_2} \cdot [\![g_2]\!]_{g_1} \pmod{n}$, δηλαδή $[\![g_1]\!]_{g_2} \equiv [\![g_2]\!]^{-1}_{g_1} \pmod{n}$. □

Ένα ακόμη πόρισμα του Λήμματος 3.2.4 είναι ότι το η πολυπλοκότητα του προβλήματος CLASS$[n,g]$, δεν εξαρτάται από την επιλογή του $g \in \mathcal{B}$ και συνεπώς αυτό μπορεί να παραλειφθεί. Έτσι ορίζεται, πλέον,

Το πρόβλημα CLASS$[n]$: Δεδομένων $n \in \mathcal{R}$, $w \in \mathbb{Z}^*_{n^2}$ και $g \in \mathcal{B}$, να βρεθεί η $[\![w]\!]_g$.

Αποκρυπτογράφηση

Εν αρχή, δεδομένου ενός $n \in \mathbb{Z}^*$, ορίζεται η συνάρτηση

$$L : \mathbb{Z} \longrightarrow \mathbb{Z} \qquad\qquad L(u) := \frac{u-1}{n}$$

όπου $\frac{a}{b}$ είναι η συνήθης διαίρεση (ακεραίων) του $a \in \mathbb{Z}$ με το $b \in \mathbb{Z}$.

Πρόταση 3.2.6. Έστω $\mathcal{S}_n := \{u \in \mathbb{Z}^*_{n^2} : u \equiv 1 \mod n^2\}$. Η $L : \mathcal{S}_n \longrightarrow \mathbb{Z}$ είναι καλώς ορισμένη.

Απόδειξη. Για $u \in \mathcal{S}_n$, είναι $u \in [0, n^2) \cap \mathbb{N}_0$ και $u = mn + 1$, για κάποιο $m \in [0, n) \cap \mathbb{N}_0$. Επομένως,

$$\forall u \in \mathcal{S}_n : \quad L(u) = \frac{u-1}{n} \overset{u \in \mathcal{S}_n}{=} \frac{(mn+1)-1}{n} = m \in [0, n) \cap \mathbb{N}_0 \subseteq \mathbb{Z}$$

Άρα, $L(u) \in \mathbb{Z}_n$ και η $L : \mathbb{Z} \longrightarrow \mathbb{Z}$ είναι καλώς ορισμένη. □

Τα παρακάτω αποτελέσματα χρησιμεύουν στην απόδειξη της Λήμματος 3.2.10:

Πρόταση 3.2.7. Για κάθε $n \in \mathcal{R}$ και κάθε $w \in \mathbb{Z}^*_{n^2}$, ισχύουν ότι

(α') $w^{\lambda(n)} \equiv 1 \mod n$

(β') $w^{n\lambda(n)} \equiv 1 \mod n^2$

όπου $\lambda : \mathbb{N} \longrightarrow \mathbb{N}$ είναι η συνάρτηση Carmichael [όρα Ορισμό 3.1.4].

Λήμμα 3.2.8. *Ισχύει ότι* $(\forall n \in \mathcal{R})(\forall x \in \mathbb{N})\big[(\alpha + n)^x \equiv \alpha^n + n\alpha^{n-1}x \mod n^2\big]$.

Απόδειξη. $(\alpha + n)^x = \sum_{k=0}^{x} \binom{x}{k} n^k = 1 + n\alpha^{n-1}x + \Omega(n^2)$. □

Λήμμα 3.2.9. *Ισχύει ότι* $(\forall n \in \mathcal{R})[1 + n \in \mathcal{B}]$.

Απόδειξη. Από το Λήμμα 3.2.8 ισχύει ότι $(1+n)^x \equiv 1 + nx \mod n^2$ κι άρα το $1 + n$ είναι n-οστή ρίζα της μονάδος κι άρα $\mathrm{ord}_{\mathbb{Z}^*_{n^2}}(1 + n) = n$. □

Λήμμα 3.2.10. *Ισχύει ότι* $(\forall n \in \mathcal{R})(\forall w \in \mathbb{Z}^*_{n^2})\big[L(w^\lambda \bmod n^2) = \lambda \cdot [\![w]\!]_{1+n} \bmod n\big]$, *όπου* $\lambda \equiv \lambda(n) = \epsilon\kappa\pi(p-1, q-1)$.

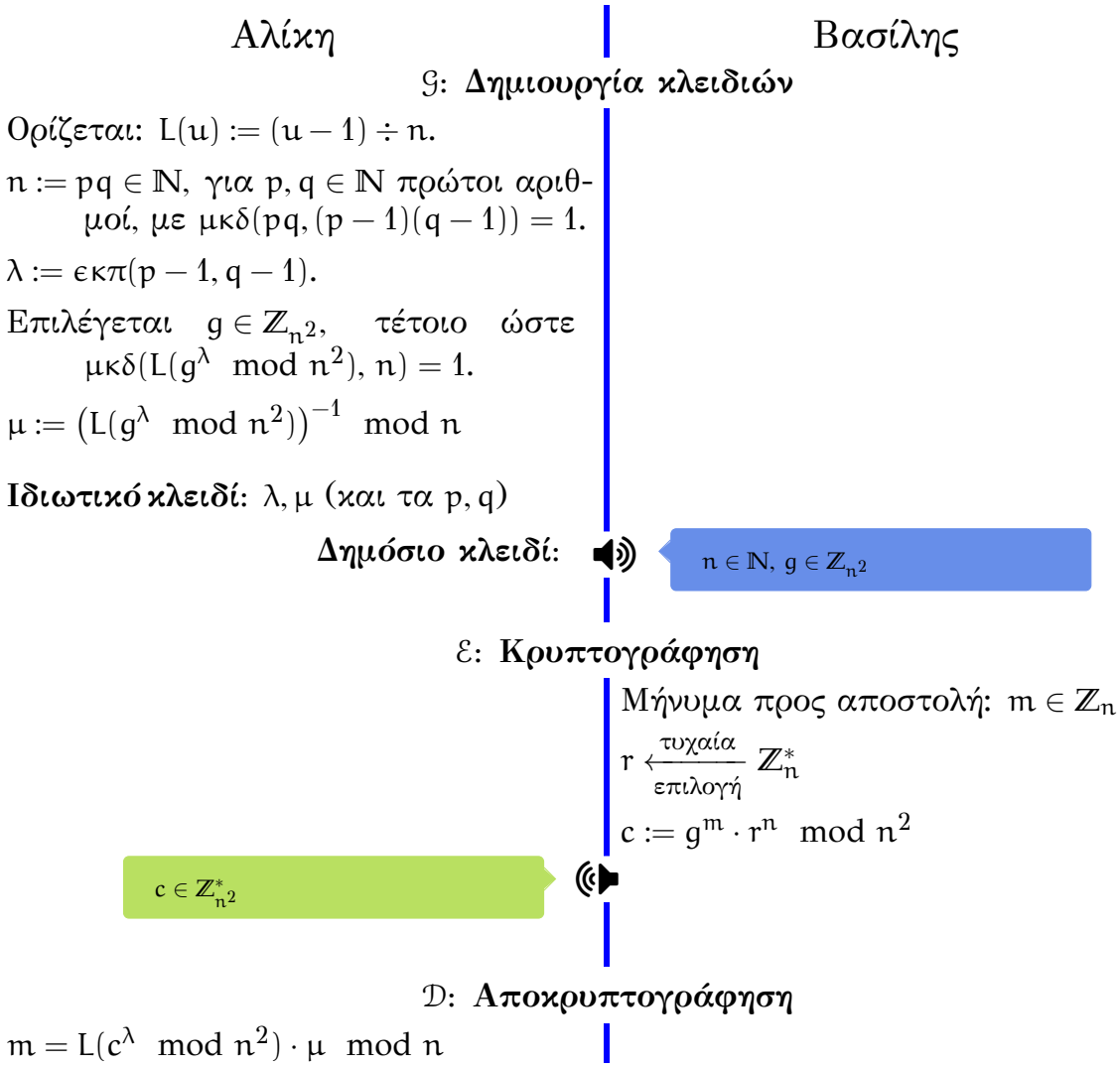
Απόδειξη. Από το Λήμμα 3.2.9 είναι $1 + n \in \mathcal{B}$. Για την υπολειμματική κλάση $[\![w]\!]_{1+n}$ ισχύει $(\exists \alpha \in \mathbb{Z}_n)(\exists \beta \in \mathbb{Z}^*_n)[w = (1+n)^\alpha \cdot \beta^n \mod n^2]$. Άρα, $\alpha = [\![w]\!]_{1+n}$.

$$w^\lambda = (1+n)^{\alpha\lambda} \cdot \beta^{n\lambda} \overset{\text{Πρόταση 3.2.7-}(\beta')}{=} (1+n)^{\alpha\lambda} \overset{\text{Λήμμα 3.2.8}}{\equiv} 1 + \alpha\lambda n \mod n^2$$

Τελικά, $L(w^\lambda \bmod n^2) = \frac{(1+\alpha\lambda n)-1}{n} = \alpha\lambda = \lambda \cdot [\![w]\!]_{1+n}$. □

3.2.3 Υλοποίηση

Το κρυπτοσύστημα Paillier είναι ένα τυχαιοκρατικό, ασύμμετρου κλειδιού κρυπτοσύστημα ανάμεσα σε δύο οντότητες δίχως κάποια πρότερη συνεννόηση.



Σχήμα 3.2: Το κρυπτοσύστημα Paillier

Θεώρημα 3.2.11 (Ορθότητα του κρυπτοσυστήματος Paillier). *Έστω $n = pq \in \mathcal{R}$, $g \in \mathbb{Z}_{n^2}$, με $\mu\kappa\delta\big(L(g^\lambda \mod n^2), n\big) = 1$, καθώς και οι συναρτήσεις*

$$\mathcal{E}_g : \mathbb{Z}_n \times \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_{n^2}^* \qquad \mathcal{E}_g(m, r) := \mathcal{F}_g(m, r) = g^m \cdot r^n \pmod{n^2}$$

$$\mathcal{D}_{p,q,g} : \mathbb{Z}_{n^2}^* \longrightarrow \mathbb{Z}_n \qquad \mathcal{D}_{p,q,g}(c) := \frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \pmod{n}$$

για $L(u) = \frac{u-1}{n}$ και $\lambda \equiv \lambda(n) = \epsilon\kappa\pi(p-1, q-1)$, τότε $(\forall m \in \mathbb{Z}_n)[\mathcal{D}_{p,q,g}(\mathcal{E}_g(m)) = m]$.

Απόδειξη. Δεδομένου ότι $\mathcal{R} \ni n = pq$, $g \in \mathbb{Z}_{n^2}$, με $\mu\kappa\delta\big(L(g^\lambda \mod n^2), n\big) = 1$, και $c = \mathcal{E}_g(m, r) \in \mathbb{Z}^*_{n^2}$, για $m \in \mathbb{Z}_n$ και $r \in \mathbb{Z}^*_n$, ισχύει ότι

$$\mathcal{D}_{p,q,g}(c) = \frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \overset{\text{Λήμμα 3.2.10}}{=} \frac{\lambda \cdot [\![c]\!]_{1+n}}{\lambda \cdot [\![g]\!]_{1+n}} = \frac{[\![c]\!]_{1+n}}{[\![g]\!]_{1+n}} =$$

$$= [\![c]\!]_{1+n} \cdot [\![g]\!]^{-1}_{1+n} \overset{\text{Πόρισμα 3.2.5}}{=} [\![c]\!]_{1+n} \cdot [\![1+n]\!]_g \overset{\text{Λήμμα 3.2.4}}{=} [\![c]\!]_g = m$$

με τη τελευταία ισότητα να ισχύει διότι $c = \mathcal{E}_g(m, r) = g^m \cdot r^n \pmod{n^2}$. □

3.2.3.Α΄ Παράμετροι υλοποίησης

Για $\lceil \log_2 p \rceil \approx \lceil \log_2 q \rceil$ (οι $p, q \in \mathbb{N}$ αναπαριστώνται από παρόμοιο πλήθος δυφίων), τότε προκύπτει μία πιο απλοποιημένη εκδοχή του κρυπτοσυστήματος Paillier για $g := n + 1$, $\lambda := \varphi(n)$ και $\mu := (\varphi(n))^{-1}$, με $\varphi(n) = (p-1)(q-1)$.

Αλγόριθμος παραγωγής κλειδιών $\mathcal{G}$: Η απαίτηση $\mu\kappa\delta(n, \lambda(n)) = 1$ τίθεται ώστε οι πρώτοι $p, q \in \mathbb{N}$ να μην είναι παραπλήσιου πλήθους δυφίων. Το στοιχείο βάσης $g \in \mathcal{B}$ μπορεί να επιλεγεί ως $g = 2$, ή κάποιον άλλον μικρό αριθμό, ή τυχαία από το $\{x \in \mathbb{Z}^*_{n^2} : n \mid \mathrm{ord}_{\mathbb{Z}^*_{n^2}}(x)\}$.

Αλγόριθμος κρυπτογράφησης $\mathcal{E}$: Υπολογίζοντας εξ αρχής τη τιμή $r^n \pmod{n^2}$ (ή $g^{nr} \pmod{n^2}$ για την παραλλαγή) μειώνεται το κόστος υλοποίησης.

Αλγόριθμος αποκρυπτογράφησης $\mathcal{D}$: Υπολογίζοντας το $\mu := L(u)$, για $c^h \in \mathcal{S}_n$ με $h \in \{\lambda, \alpha\}$ εκ των προτέρων μειώνει την υπολογιστική πολυπλοκότητα του Σχήματος. Ο υπολογισμός είναι χαμηλού κόστους: απαιτεί έναν πολλαπλασιασμό modulo $2^{|n|}$, αφού πρώτα υπολογισθεί το $n^{-1} \mod 2^{|n|}$.

Ένας άλλος τρόπος αποκρυπτογράφησης χρησιμοποιεί το Κινέζικο Θεώρημα Υπολοίπων: Έστω $y \in \{p, q\}$. Ορίζεται $L_y : \mathcal{S}_y \longrightarrow \mathbb{Z}$, με $L_y(u) := \frac{u-1}{y}$, όπου $\mathcal{S}_y := \{x \in \mathbb{Z}_{y^2} : x \equiv 1 \pmod{y}\}$. Τώρα $m = K\Theta\Upsilon(m_p, m_q) \mod pq$, όπου $m_y := \dfrac{L_y(c^{y-1} \mod y^2)}{\big[L_y(g^{y-1} \mod y^2)\big]^{-1} \mod y} \mod y$.

3.2.3.Β΄ Ομομορφική ιδιότητα

Θεωρούνται οι αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης του Σχήματος 3.2 ως $\textsc{Enc}\left(\langle n, g\rangle, m\right) := \mathcal{F}_g(m, r)$ και $\textsc{Dec}\left(\langle \lambda, \mu\rangle, c\right) := [\![c]\!]_g$ αντίστοιχα.

Λήμμα 3.2.12 (Προσθετική ομομορφική ιδιότητα). *Το κρυπτοσύστημα Paillier παρουσιάζει* $+_{\mathrm{mod}\, n}$ *(προσθετική υπόλοιπο* n*) ομομορφική ιδιότητα, δηλαδή*

$$(\forall m_1, m_2 \in \mathbb{Z}_n)\Big[\,\mathrm{Enc}\left(\langle n, g\rangle, m_1\right) \times_{\mathrm{mod}\, n^2} \mathrm{Enc}\left(\langle n, g\rangle, m_2\right) = \mathrm{Enc}\left(\langle n, g\rangle, m_1 +_{\mathrm{mod}\, n} m_2\right)\Big]$$

Απόδειξη. Έστω $r_1, r_2 \in \mathbb{Z}_n^*$, τότε

$$\begin{aligned}
\mathrm{Enc}\left(\langle n, g\rangle, m_1\right) \times_{\mathrm{mod}\, n^2} \mathrm{Enc}\left(\langle n, g\rangle, m_2\right) &\iff (g^{m_1} \cdot r_1^n \mod n^2) \cdot (g^{m_2} \cdot r^{n_2} \mod n^2) \mod n^2 \\
&\iff (g^{m_1} \cdot r_1^n) \cdot (g^{m_2} \cdot r_2^n) \mod n^2 \\
&\iff g^{m_1 +_{\mathrm{mod}\, n} m_2} \cdot (r_1 +_{\mathrm{mod}\, n^2} r_2)^n \mod n^2 \\
&\iff \mathrm{Enc}\left(\langle n, g\rangle, m_1 +_{\mathrm{mod}\, n} m_2\right) \qquad \square
\end{aligned}$$

Λήμμα 3.2.13 (Πολλαπλασιαστική ομομορφική ιδιότητα). *Το κρυπτοσύστημα Paillier παρουσιάζει* $\times_{\mathrm{mod}\, n}$ *(πολλαπλασιασμός υπόλοιπο* n*) ομομορφική ιδιότητα, δηλαδή*

$$(\forall m_1, m_2 \in \mathbb{Z}_n)\Big[\left[\,\mathrm{Enc}\left(\langle n, g\rangle, m_1\right)\right]^{m_2} = \mathrm{Enc}\left(\langle n, g\rangle, m_1 \cdot m_2 \mod n\right) = \left[\,\mathrm{Enc}\left(\langle n, g\rangle, m_2\right)\right]^{m_1}\Big]$$

Απόδειξη. Ισχύει ότι

$$\begin{aligned}
\left[\,\textsc{Enc}\left(\langle n, g\rangle, m_1\right)\right]^{m_2} &= (g^{m_1} \cdot r^n)^{m_2} \mod n^2 = \\
&= g^{m_1 m_2} \cdot (r^{m_2})^n \mod n^2 = \textsc{Enc}\left(\langle n, g\rangle, m_1 \cdot m_2 \mod n\right)
\end{aligned}$$

Επίσης,

$$\begin{aligned}
\left[\,\textsc{Enc}\left(\langle n, g\rangle, m_2\right)\right]^{m_1} &= (g^{m_2} \cdot r^n)^{m_1} \mod n^2 = \\
&= g^{m_1 m_2} \cdot (r^{m_1})^n \mod n^2 = \textsc{Enc}\left(\langle n, g\rangle, m_1 \cdot m_2 \mod n\right) \qquad \square
\end{aligned}$$

Πρόταση 3.2.14 (Ιδιότητα της αυτο-τύφλωσης). Κάθε κρυπτοκείμενο $c \in \mathbb{Z}_{n^2}^*$ μπορεί να παραλλαχθεί σε ένα έτερο (έγκυρο) κρυπτοκείμενο $c' \in \mathbb{Z}_{n^2}^*$ και αμφότερα να αποκρυπτογραφούνται στο ίδιο απλό κείμενο $m \in \mathbb{Z}_n$. Ακριβέστερα:

$$\textsc{Dec}\left(\langle \lambda, \mu\rangle, \textsc{Enc}\left(\langle n, g\rangle, m\right)\right) = m = \textsc{Dec}\left(\langle \lambda, \mu\rangle, \textsc{Enc}\left(\langle n, g\rangle, m\right) \cdot r^n \mod n^2\right)$$

Απόδειξη. Έστω $c := \textsc{Enc}\left(\langle n, g\rangle, m\right)$ και $c' := \textsc{Enc}\left(\langle n, g\rangle, m\right) \cdot r^n \bmod n^2$.

- $\textsc{Dec}\left(\langle \lambda, \mu\rangle, c\right) = m$, λόγω του Θεωρήματος 3.2.11 (ορθότητα το κρυπτοσυστήματος Paillier).
- $c' = \textsc{Enc}\left(\langle n, g\rangle, m\right) \cdot r^n \bmod n^2 = (g^m \cdot s^n) \cdot r^n \bmod n^2 = g^m \cdot (s \cdot r)^n \bmod n^2$, το οποίο είναι έγκυρο κρυπτοκείμενο. Από το Θεώρημα 3.2.11, προκύπτει ότι $\textsc{Dec}\left(\langle \lambda, \mu\rangle, c'\right) = [\![c']\!]_g = m \mod n$. $\square$

3.2.4 Ασφάλεια

Η σχέση του προβλήματος $\texttt{CLASS}[n]$, $n \in \mathcal{R}$ επάνω στο οποίο στηρίχθηκε η ανάλυση για το κρυπτοσύστημα Paillier, ως προς άλλα γνωστά ανοικτά προβλήματα, πρόκειται να συνάγει την ασφάλεια του σχήματος.

Κατ΄ αρχάς, ένα εγγενές ιδίωμα του κρυπτοσυστήματος Paillier αποτελεί το γεγονός ότι είναι ελατός [όρα Ορισμό 2.3.5]. Ακόμη γενικότερα, ισχύει το

Λήμμα 3.2.15. *Κάθε μερικώς ομομορφικό κρυπτοσύστημα είναι ελατό.*

Απόδειξη. Προφανές, από τους Ορισμούς 3.2.1 και 2.3.5. □

3.2.4.Α΄ Συσχετίσεις πολυπλοκότητας

Θεώρημα 3.2.16. Ισχύει ότι $(\forall n \in \mathcal{R})\big[\texttt{CLASS}[n] \preceq \texttt{FACT}[n]\big]$.

Απόδειξη. {Βήμα 1}: Δεδομένου ενός αλγορίθμου για το πρόβλημα $\texttt{FACT}[n]$, η παραγοντοποίηση του $n \in \mathcal{R}$, σε $n = pq$ καθίσταται γνωστή και κατ΄ επέκτασην είναι δυνατόν να βρεθεί η τιμή $\lambda \equiv \lambda(n) := \epsilon\kappa\pi(p-1, q-1)$.

{Βήμα 2}: Όντας (δημοσίως) γνωστά τα $n \in \mathcal{R}$, $g \in \mathcal{B}$ και πλέον και το $\lambda \in \mathbb{N}$, από το Θεώρημα 3.2.11 (Ορθότητα του κρυπτοσυστήματος Paillier) υπολογίζεται η κλάση $[\![g^m \cdot r^n \bmod n^2]\!]_g$ (ήτοι το κρυπτογραφημένο μήνυμα). □

Κατά συνέπεια, για $n \in \mathcal{R}$, το πρόβλημα $\texttt{CLASS}[n]$ δεν είναι δυσκολότερο από την παραγοντοποίηση του $n \in \mathcal{R}$, δηλαδή το πρόβλημα $\texttt{FACT}[n]$.

Θεώρημα 3.2.17. Ισχύει ότι $(\forall n \in \mathcal{R})\big[\texttt{CLASS}[n] \preceq \texttt{RSA}[n, n]\big]$.

Απόδειξη. Έστω πως παρέχεται ένας αλγόριθμος, ο οποίος επιλύει το πρόβλημα $\texttt{RSA}[n, n]$, για $n \in \mathcal{R}$. Δεδομένου ότι

1. $(\forall g_1, g_2 \in \mathcal{B})\big[\texttt{CLASS}[n, g_1] \equiv \texttt{CLASS}[n, g_2]\big]$ [όρα Λήμμα 3.2.4] και
2. $1 + n \in \mathcal{B}$ [όρα Λήμμα 3.2.9]

αρκεί να δειχθεί ότι

- $\texttt{CLASS}[n, n+1] \preceq \texttt{RSA}[n, n]$.

Προς τούτο,

(α') $[\![w]\!]_{1+n} \overset{(3.2)}{\iff} (\exists x \in \mathbb{Z}_n)(\exists y \in \mathbb{Z}_n^*)[w = (1+n)^x \cdot y^n \mod n^2]$.

(β') $(1+n)^x \equiv 1 \mod n$ [όρα Λήμμα 3.2.8]

Συνεπώς, $w \equiv y^n \mod n$, το οποίο $y \in \mathbb{Z}_n^*$ καθίσταται γνωστόν επιλύοντας το πρόβλημα $\texttt{RSA}[n, n]$. Τελικώς, $wy^{-n} \overset{(\alpha')}{=} (1+n)^x \mod n^2 \overset{\text{Λήμμα } 3.2.8}{=} 1 + xn \mod n^2$, απ΄ όπου επιλύοντας, προκύπτει το $x = [\![w]\!]_{1+n}$. □

Άρα, το πρόβλημα $\texttt{CLASS}[n]$ δεν είναι δυσκολότερο του προβλήματος $\texttt{RSA}[n, n]$.

3.2.4.Β΄ DCRA ασφάλεια

Αρχικά εισάγεται

Το πρόβλημα CR[n]: Δεδομένου ενός $n \in \mathcal{R}$, να υπολογισθεί το σύνολο των n-οστών υπολοίπων modulo n, ήτοι το $\left\{z \in \mathbb{Z} : (\exists y \in \mathbb{Z}^*_{n^2})[z \equiv y^n \mod n^2]\right\}$.

Η υπόθεση στην οποία πρόκειται να στηριχθεί η απόδειξη ασφαλείας είναι η:

Υπόθεση DCRA: Δεν υπάρχει αλγόριθμος πολυωνυμικού χρόνου για τον διαχωρισμό των n-οστών υπολοίπων modulo n, από τα μη n-οστά υπόλοιπα modulo n.

γνωστή ως **Υπόθεση Απόφασης Συνθέτων Υπολοίπων** (Decisional Composite Residuosity Assumption, DCRA) και εκφράζει (την πεποίθηση) πως το πρόβλημα CR[n] είναι δυσεπίλυτο. Η εκδοχή απόφασης του προβλήματος CLASS[n] είναι:

Το πρόβλημα D-CLASS[n]: Δεδομένων των $n \in \mathcal{R}$, $w \in \mathbb{Z}^*_{n^2}$, $x \in \mathbb{Z}_n$ και $g \in \mathcal{B}$, ισχύει ότι $x = [\![w]\!]_g$;

Λήμμα 3.2.18 ([Pai99], Λήμμα 2). *Για κάθε $n \in \mathcal{R}$, ισχύουν τα κάτωθι:*

(α) $[\![w]\!]_g = 0$ *εάν και μόνον εάν το* $w \in \mathbb{Z}^*_{n^2}$ *είναι ένα* n*-οστό υπόλοιπο modulo* n^2.

(β) Ισχύει ότι $(\forall g \in \mathcal{B})(\forall w_1, w_2 \in \mathbb{Z}^*_{n^2})\left[[\![w_1 \times_{\mathrm{mod}\, n^2} w_2]\!]_g = [\![w_1]\!]_g +_{\mathrm{mod}\, n} [\![w_2]\!]_g\right]$.

Θεώρημα 3.2.19. Ισχύει ότι $(\forall n \in \mathcal{R})\left[\mathrm{CR}[n] \equiv \mathrm{D\text{-}CLASS}[n]\right]$.

Απόδειξη. (D-CLASS[n] $\preceq$ CR[n]): Έστω $\mathcal{O}^{\mathrm{CR}}$ ο αλγόριθμος ο οποίος επιλύει το πρόβλημα CR[n], $g \in \mathcal{B}$ και $w \in \mathbb{Z}^*_{n^2}$. Ο αλγόριθμος λειτουργεί ως εξής:

$$\mathcal{O}^{\mathrm{CR}}(w \cdot g^{-x}) = \begin{cases} 1, & \text{εάν } (\exists r \in \mathbb{Z}^*_n)[w \cdot g^{-x} \equiv r^n \mod n^2] \\ 0, & \text{αλλιώς} \end{cases}$$

Επομένως, εάν $\mathcal{O}^{\mathrm{CR}}(w \cdot g^{-x}) = 1$, τότε

$$\left.\begin{array}{l} [\![w \cdot g^{-x}]\!]_g \overset{\text{Λήμμα 3.2.18-}(\alpha')}{=} 0 \\ [\![w \cdot g^{-x}]\!]_g \overset{\text{Λήμμα 3.2.18-}(\beta')}{=} [\![w]\!]_g + [\![g^{-x}]\!]_g \mod n = [\![w]\!]_g - x \mod n \end{array}\right\} \Longrightarrow$$
$$\Longrightarrow 0 = [\![w \cdot g^{-x}]\!]_g \equiv [\![w]\!]_g - x \mod n \Longrightarrow [\![w]\!]_g \equiv x \mod n$$

δηλαδή το πρόβλημα CLASS[n] (κι άρα και το D-CLASS[n]) επιλύθηκε.

($\texttt{CR}[n] \preceq \texttt{D-CLASS}[n]$): Έστω $\mathcal{O}^{\text{D-Class}}$ ένας αλγόριθμος ο οποίος επιλύει το πρόβλημα $\texttt{D-CLASS}[n]$, $w \in \mathbb{Z}^*_{n^2}$ καθώς κι ένα (τυχαίο) $g \in \mathcal{B}$ (μία πιθανή επιλογή είναι το $1 + n \in \mathcal{B}$). Ο αλγόριθμος λειτουργεί ως εξής:

$$\mathcal{O}^{\text{D-Class}}(g, w, 0) = \begin{cases} 1, & \text{εάν } [\![w]\!]_g = 0 \\ 0, & \text{αλλιώς} \end{cases}$$

Εάν $\mathcal{O}^{\text{D-Class}}(g, w, 0) = 1$, τότε $w = g^0 \cdot r^n \mod n^2 = r^n \mod n^2$ κι άρα το $w \in \mathbb{Z}^*_{n^2}$ είναι n-οστό υπόλοιπο modulo n^2.

Εάν $\mathcal{O}^{\text{D-Class}}(g, w, 0) = 0$, τότε $(\exists y \in \mathbb{Z}_n)\big[(y^n \not\equiv 1 \mod n^2) \Rightarrow (w = g^y \cdot r^n \mod n^2)\big]$ κι άρα το $w \in \mathbb{Z}^*_{n^2}$ *δεν* είναι n-οστό υπόλοιπο modulo n^2.

Άρα, για κάθε $w \in \mathbb{Z}^*_{n^2}$, η απάντηση του αλγορίθμου $\mathcal{O}^{\text{D-Class}}(g, w, 0)$ επιλύει το πρόβλημα $\texttt{CR}[n]$. □

Ισχύει ότι $\texttt{D-CLASS}[n] \preceq \texttt{CLASS}[n]$ (πιο εύκολα επαληθεύεται εάν ένα στοιχείο αποτελεί λύση, παρά να βρεθεί η λύση ενός προβλήματος). Τελικώς:

$$\texttt{CR}[n] \equiv \texttt{D-CLASS}[n] \preceq \texttt{CLASS}[n] \preceq \texttt{RSA}[n, n] \preceq \texttt{FACT}[n]$$

Από την υπολογιστική ισοδυναμία $\texttt{CR}[n] \equiv \texttt{D-CLASS}[n]$, η υπόθεση DCRA επάγει πως το πρόβλημα $\texttt{D-CLASS}[n]$ είναι δυσεπίλυτο. Η δυσκολία, οδηγεί στον:

Ορισμός 3.2.20. Έστω $n \in \mathcal{R}$, $\ell = \lceil \log_2 n \rceil$ και $g \in \mathcal{B}$. Ένα κρυπτοσύστημα καλείται **DCRA ασφαλές** εάν για το τυχαία επιλεγμένο $w \in \mathbb{Z}^*_{n^2}$, ισχύει πως

$$(\forall \text{ PPT } \mathcal{A})\Big[\big|\, \mathsf{Prob}[\mathcal{A}(n, g, w, x) = 1] - \mathsf{Prob}[\mathcal{A}(n, g, w, [\![w]\!]_g] = 1\big| = \mathsf{negl}(\ell)\Big]$$

όπου το ακρωνύμιο PPT σημαίνει *πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου*.

3.2.4.Γ΄ Απόδειξη ασφαλείας

Αποδεικνύοντας τη σημαντική ασφάλεια του κρυπτοσυστήματος Paillier, τότε το κρυπτοσύστημα καθίσταται και IND-CPA ασφαλές, από τα κάτωθι Θεωρήματα:

Θεώρημα 3.2.21. Ισχύει ότι:

$$\text{IND-CPA ασφάλεια} \iff \text{σημαντικά ασφαλές ως προς CPA}$$

Θεώρημα 3.2.22. Το κρυπτοσύστημα Paillier είναι σημαντικά ασφαλές σε επιθέσεις επιλεγμένου απλού κειμένου (CPA) εάν και μόνον εάν είναι DCRA ασφαλές.

Απόδειξη. Θα αποδειχθεί η αντιθετοαναστροφή του ζητουμένου, δηλαδή ότι: ''¬Paillier σημαντικά ασφαλές $\iff$ ¬DCRA ασφαλές''. Στα παρακάτω, η παράμετρος $\ell \in \mathbb{N}$ θα συμβολίζει το μήκος της εισόδου του εκάστοτε αλγορίθμου. Προς τούτο θεωρούνται οι εξής αλγόριθμοι: Είναι $n \in \mathcal{R}$ και $g \in \mathcal{B}$.

- $\mathcal{A}(m_0, m_1, c, n, g)$: Ο $\mathcal{A}$ επιστρέφει $b \in \{0,1\}$ εικάζοντας πως το $c \in \mathbb{Z}^*_{n^2}$ είναι το κρυπτοκείμενο του $m_b \in \mathbb{Z}_n$ (δηλαδή $[\![c]\!]_g = m_b$).
- $\mathcal{B}(n, g, w, x)$: Ο $\mathcal{B}$ με μη-αμελητέα πιθανότητα επιστρέφει 1 εάν $x = [\![w]\!]_g$ και 0 αλλιώς, για $x \in \mathbb{Z}^*_{n^2}$ και $x \in \mathbb{Z}_n$.

(Paillier όχι σημαντικά ασφαλές $\Rightarrow$ Paillier όχι DCRA ασφαλές): Έστω ότι το κρυπτοσύστημα Paillier δεν είναι σημαντικά ασφαλές. Έπεται ότι υπάρχει ένας πιθανοτικός πολυωνυμικού χρόνου αντίπαλος $\mathcal{A}$, για τον οποίον ισχύει ότι:

(i) $m_0, m_1 \in \mathbb{Z}_n$, $c \in \mathbb{Z}^*_{n^2}$, $n \in \mathcal{R}$ και $g \in \mathcal{B}$.

(ii) $\mathcal{A}(m_0, m_1, c, n, g) = b \in \{0,1\}$, όπου ο $\mathcal{A}$ *εικάζει* πως το $c \in \mathbb{Z}^*_{n^2}$ είναι το κρυπτογράφημα του m_b.

(iii) $\mathsf{Prob}[\mathrm{Game}^{\mathcal{A}}_{\mathsf{IND\text{-}CPA}}(1^\ell) = 1] > 1/2 + \alpha$, για $\alpha \equiv \alpha(\ell) \gg \mathsf{negl}(\ell)$.

Σκοπός είναι να δημιουργηθεί ένας πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου $\mathcal{B}$, ο οποίος να καταρρίπτει τον Ορισμό 3.2.20: Με χρήση του αλγορίθμου $\mathcal{A}$, ο $\mathcal{B}$ επιλύει το πρόβλημα D-CLASS$[n]$ με μη-αμελητέα πιθανότητα.

Αλγόριθμος 3.2.23 $\mathcal{B}(n, g, w, x)$: Εξαγωγή πληροφορίας από το κρυπτοσύστημα Paillier με μη-αμελητέα πιθανότητα

1: $g \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathcal{B}$;
2: $r \leftarrow w \cdot g^{-x} \mod n^2$;
3: $c \leftarrow g^{m_b} \cdot r \mod n^2$;
4: $b \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{0,1\}$;
5: **εάν** $(b = \mathcal{A}(m_0, m_1, c, n, g))$ **τότε**
6: **επίστρεψε** 1;
7: **αλλιώς**
8: **επίστρεψε** 0;
9: **τέλος εάν**

Επομένως, εάν $x = [\![w]\!]_g$, τότε $r = g^{[\![w]\!]_g} \cdot s^n \cdot g^{-[\![w]\!]_g} \mod n^2 = s^n \mod n^2$, δηλαδή το $r \in \mathbb{Z}^*_{n^2}$ είναι ένα n-οστό υπόλοιπο modulo n κι άρα το $c = g^{m_b} \cdot r \mod n^2 = g^{m_b} \cdot s^n \mod n^2$ είναι μία έγκυρη κρυπτογράφηση του $m_b \in \mathbb{Z}_n$. Η πιθανότητα ο $\mathcal{A}$ να αποφανθεί θετικώς (να επιστρέψει 1) ισούται με την πιθανότητα ο $\mathcal{B}$ να

μάντεψε σωστά το απλό κείμενο $m_b \in \mathbb{Z}_n$ στο οποίο αντιστοιχεί το $c \in \mathbb{Z}^*_{n^2}$:

$$\mathsf{Prob}[\mathcal{B}(n, w, [\![w]\!]_g) = 1] = \mathsf{Prob}[\mathrm{Game}^{\mathcal{A}}_{\mathsf{IND\text{-}CPA}}(1^\ell) = 1] > 1/2 + \alpha$$

Εάν $x \neq [\![w]\!]_g$, τότε το $r = w \cdot g^{-x} \bmod n^2$ είναι ένα τυχαίο στοιχείο του $\mathbb{Z}^*_{n^2}$. Άρα, $r = g^\varepsilon \cdot s^n \bmod n^2$, για κάποιο $\varepsilon \in \mathbb{Z}_n$ ομοιόμορφα κατανεμημένο στο $\mathbb{Z}_n$ και $c = g^{m_b} \cdot (g^\varepsilon \cdot s^n) \bmod n^2 = g^{m_b+\varepsilon} \cdot s^n \bmod n^2$, όπου πλέον το $m_b \in \mathbb{Z}_n$ έχει κρυφτεί, λόγῳ της προσαρτήσεως (padding) του (αγνώστου, όντας τυχαίο) $\varepsilon \in \mathbb{Z}_n$. Κατ' επέκταση, ο $\mathcal{A}$ δεν μπορεί παρά να αποφασίσει (πλήρως) στη τύχη για την προέλευση του $w \in \mathbb{Z}^*_{n^2}$ κι άρα

$$\mathsf{Prob}[\mathcal{B}(n, w, x) = 1] = 1/2$$

για το τυχαία επιλεγμένο $x \in \mathbb{Z}_n$. Τελικά

$$\left|\mathsf{Prob}[\mathcal{B}(n, w, [\![w]\!]_g) = 1] - \mathsf{Prob}\mathcal{B}(n, w, x) = 1\right| > 1/2 + \alpha - 1/2 = \alpha \gg \mathsf{negl}(\ell)$$

κι άρα ο $\mathcal{B}$ επιλύει σε πολυωνυμικό χρόνο την υπόθεση DCRA με μη-αμελητέα πιθανότητα.

(Paillier όχι DCRA ασφαλές $\Rightarrow$ Paillier όχι σημαντικά ασφαλές): Έστω ότι υπάρχει πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου $\mathcal{B}(n, g, w, x)$ ο οποίος επιλύει το πρόβλημα D-CLASS$[n]$ και για τον οποίον ισχύουν:

> $\mathsf{Prob}[\mathcal{B}(n, g, w, [\![w]\!]_g) = 1] - \mathsf{Prob}[n, g, w, x = 1] > \beta$, για $\beta \equiv \beta(\ell) \gg \mathsf{negl}(\ell)$
> (χωρίς βλάβη της γενικότητας, δεν λογίζεται η απόλυτη τιμή της διαφοράς· ομοίως κι αν $\mathsf{Prob}[n, g, w, x = 1] - \mathsf{Prob}[\mathcal{B}(n, g, w, [\![w]\!]_g) = 1] > \beta$).

Σκοπός είναι για τυχαία επιλεγμένα $m_0, m_1 \in \mathbb{Z}_n$, $b \in \{0, 1\}$ και $c = \textsc{Enc}\big(\langle n, g\rangle, m_b\big)$, να δημιουργηθεί ένα πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου που να βρίσκει το $b \in \{0, 1\}$ με μη-αμελητέα πιθανότητα.

Ο αλγόριθμος $\mathcal{A}$ βασίζεται πλήρως στη γνώμη του αλγορίθμου $\mathcal{B}$: Γνωρίζοντας ο $\mathcal{A}$ πιο απλό κείμενο έδωσε στον $\mathcal{B}$, απλώς επιστρέφει την εικασία του $\mathcal{B}$. Τώρα,

$$\begin{aligned}
\mathsf{Prob}\big[\mathcal{A}(m_0, m_1, c, n, g = 1\big] &= \mathsf{Prob}\big[\mathcal{B}(n, g, c, m_1) = 1 \mid [\![c]\!]_g = m_1\big] \cdot \mathsf{Prob}\big[[\![c]\!]_g = m_1\big] + \\
&\quad + \mathsf{Prob}\big[\mathcal{B}(n, g, c, m_1) = 0 \mid [\![c]\!]_g \neq m_1\big] \cdot \mathsf{Prob}\big[[\![c]\!]_g \neq m_1\big] \\
&= \frac{1}{2}\Big[\mathsf{Prob}[\mathcal{B}(n, g, w, [\![w]\!]_g) = 1] + \big(1 - \mathsf{Prob}[\mathcal{B}(n, g, w, x) = 1]\big)\Big] \\
&= \frac{1}{2} + \frac{1}{2}\Big(\mathsf{Prob}[\mathcal{B}(n, g, w, [\![w]\!]_g) = 1] - \mathsf{Prob}[\mathcal{B}(n, g, w, x)] = 1\Big) \\
&\gneqq \frac{1}{2} + \frac{1}{2}\beta \gg \mathsf{negl}(\ell)
\end{aligned}$$

κι άρα ο $\mathcal{A}$ εικάζει με μη-αμελητέα πιθανότητα την προέλευση του $c \in \mathbb{Z}^*_{n^2}$. □

3.2.5 Βελτίωση: Σχεδόν τετραγωνική αποκρυπτογράφηση

Η διαδικασία της αποκρυπτογράφησης στο κρυπτοσύστημα Paillier μπορεί να επιτευχθεί σε σχεδόν τετραγωνική πολυπλοκότητα, ακριβέστερα σε $\mathcal{O}\big((\lceil \log_2 n \rceil)^{2+\epsilon}\big)$ πράξεις δυφίων. Η ιδέα είναι να περιοριστεί ο χώρος των κρυπτοκειμένων από το $\mathbb{Z}^*_{n^2}$ σε μια κυκλική υποομάδα του. Στο Σχήμα 3.2 αρκεί η Αλίκη να κάνει τις εξής μετατροπές στον αλγόριθμο παραγωγής κλειδιών $\mathcal{G}$:

- $g \in \mathcal{B}_\alpha$, για $1 \leqslant \alpha \leqslant \lambda$ (αντί του ''$g \in \mathbb{Z}_{n^2}$, με $\mu\kappa\delta\big(L(g^\lambda \mod n^2), n\big) = 1$''),
- $\mu := \big(L(g^\alpha \mod n^2)\big)^{-1} \mod n$.

και στον αλγόριθμο αποκρυπτογράφησης $\mathcal{D}$: $m = L(c^\alpha \mod n^2) \cdot \mu \mod n$ (αντί του ''$m = L(c^\lambda \mod n^2) \cdot \mu \mod n$'').

Παρατήρηση 3.2.24. *1. Το $\lambda := \epsilon\kappa\pi(p-1, q-1)$ να είναι πολλαπλάσιο κάποιου πρώτου αριθμού με πλήθος δυφίων $\geqslant 160$.*

2. Πλέον, το ιδιωτικό κλειδί είναι το $\alpha \in \{1, 2, \ldots, \lambda(n)\}$. Η ορθότητα του Σχήματος έγκειται στο γεγονός ότι $(\forall w \in \langle g \rangle)\left[\llbracket w \rrbracket_g = \dfrac{L(w^\alpha \mod n^2)}{L(g^\alpha \mod n^2)} \mod n\right]$ το οποίο αποδεικνύεται κατά παρόμοιο τρόπο όπως και το Θεώρημα 3.2.11 (Ορθότητα του κρυπτοσυστήματος Paillier).

Χρονική πολυπλοκότητα: Συμβολίζεται $|\cdot| := \lceil \log_2(\cdot) \rceil$. Η πιο κοστοβόρα πράξη του παραπάνω Σχήματος είναι η $c \longmapsto c^\alpha \pmod{n^2}$, η οποία κι έχει πολυπλοκότητα $\mathcal{O}\big(|n|^2|\alpha|\big)$ (σε αντιδιαστολή με την $\mathcal{O}\big(|n|^3\big)$ του Σχήματος 3.2). Εάν επιλεχθεί $g \in \mathcal{B}_\alpha$, έτσι ώστε $|\alpha| = \Omega\big(|n|^\epsilon\big)$, για $\epsilon > 0$, τότε προκύπτει η επιθυμητή πολυπλοκότητα των $\mathcal{O}\big(|n|^{2+\epsilon}\big)$ πράξεων δυφίων. ⊣

Η ασφάλεια του κρυπτοσυστήματος πλέον επαφίεται στο δυσεπίλυτο του προβλήματος του μερικού διακριτού λογαρίθμου και της εκδοχής απόφασής του:

Το πρόβλημα PDL$[n, g]$: Έστω $n \in \mathcal{R}$, $g \in \mathcal{B}_\alpha$, για $1 \leqslant \alpha \leqslant \lambda$ και $w \in \langle g \rangle$. Να υπολογισθεί η κλάση $\llbracket w \rrbracket_g$.

Το πρόβλημα D-PDL$[n, g]$: Έστω $n \in \mathcal{R}$, $g \in \mathcal{B}_\alpha$, για $1 \leqslant \alpha \leqslant \lambda$, $w \in \langle g \rangle$ και $x \in \mathbb{Z}_n$. Ισχύει ότι $\llbracket w \rrbracket_g = x$;

Θεώρημα 3.2.25. Έστω $n \in \mathcal{R}$ και $g \in \mathcal{B}_\alpha$, με $1 \leqslant \alpha \leqslant \lambda$. Το παραπάνω Σχήμα

- είναι μονόδρομο εάν και μόνον εάν το πρόβλημα PDL$[n, g]$ είναι υπολογιστικά δύσκολο.
- είναι σημαντικά ασφαλές εάν και μόνον εάν το πρόβλημα D-PDL$[n, g]$ είναι υπολογιστικά δύσκολο.

Από τα παραπάνω προκύπτει ότι PDL$[n, g] \preceq$ CLASS$[n]$ και D-PDL$[n, g] \preceq$ CR$[n]$.

3.2.6 Σύνοψη

Αφ΄ ενός ένα μερικώς ομομορφικό κρυπτοσύστημα ως ελατό να φαντάζει ευάλωτο, ωστόσο η ομομορφική ιδιότητα είναι επιθυμητή σε κάποιες περιπτώσεις.

Εφαρμογές

Έπονται δύο τρόποι αξιοποίησης των ιδιοτήτων του κρυπτοσυστήματος Paillier:

Ηλεκτρονική ψηφοφορία: Έστω πως $m \in \mathbb{N}$ ψηφοφόροι καλούνται να ψηφίσουν για μία πρόταση είτε 1 (υπέρ), είτε 0 (κατά). Κάθε ψηφοφόρος κρυπτογραφεί την απόφασή του με χρήση του κρυπτοσυστήματος Paillier και την αποστέλλει. Η διεξάγουσα αρχή υπολογίζει το γινόμενο των κρυπτογραφημένων m ψήφων και αποκρυπτογραφόντας το παράγει μία τιμή $n \in \mathbb{N}$, η οποία αποτελεί το άθροισμα όλων των θετικών ψήφων [χάριν στο Λήμμα 3.2.12 (προσθετική ομομορφική ιδιότητα)]. Πλέον, η διεξάγουσα αρχή γνωρίζει πως υπάρχουν $n \in \{0, \ldots, m\}$ ψήφοι υπέρ της πρότασης και $m - n \in \{0, \ldots, m\}$ ψήφοι κατά. Η τυχαία παράμετρος $r \in \mathbb{Z}_n^*$ διασφαλίζει πως δύο όμοιες ψήφοι (2 υπέρ, ή 2 κατά) θα κρυπτογραφηθούν στο ίδιο στοιχείο του $\mathbb{Z}_n$ με αμελητέα πιθανότητα.

Ηλεκτρονική πληρωμή: Έστω πως ανακύπτει η ανάγκη για πληρωμή μέσω διαδικτύο κι έστω πως ο αγοραστής δεν επιθυμεί να αποκαλύψει τον αριθμό της πιστωτικής του κάρτας (κι άρα τη ταυτότητά του) στον πωλητή. Το κρυπτοσύστημα Paillier λόγω της Πρόταση 3.2.14 (Ιδιότητα της αυτοτύφλωσης) δίδει τη δυνατότητα διασφάλισης της ανωνυμίας του αγοραστή.

3.3 Κρυπτογραφία Ελλειπτικών Καμπυλών

Στις αρχές του $18^{ου}$ αιώνα, ένας Ιταλός Μαθηματικός ονόματι Giulio Fagano ανακάλυψε τα *ελλειπτικά ολοκληρώματα* στην προσπάθειά του να υπολογίσει το μήκος τόξου σε ελλείψεις [Bro00]. Τα εν λόγω ολοκληρώματα ήταν της μορφής:

$$I(x) = \int_c^x R\left(t, \sqrt{P(t)}\right) dt$$

για κάποια σταθερά $c \in \mathbb{R}$, μία ρητή συνάρτηση $R : \mathbb{R} \longrightarrow \mathbb{R}$ και $P \in \mathbb{R}[t]$, με $\deg P \in \{2, 3\}$ όπου οι ρίζες του δεν επαναλαμβάνονται. Άρα, για να βρεθεί το μήκος τόξου επάνω σε μία έλλειψη, αρκεί να υπολογίσει το παραπάνω ολοκλήρωμα. Έτσι, οι καμπύλες της μορφής $y^2 = x^3 + ax^2 + bx + c$ προέκυψε να είναι το μαθηματικό αντικείμενο που σήμερα αποκαλείται *ελλειπτικές καμπύλες* [Rao7].

3.3.1 Θεωρία Ελλειπτικών Καμπυλών

3.3.1.Α΄ Ελλειπτικές καμπύλες υπεράνω σωμάτων

Ένα **πεπερασμένο σώμα** (ή **σώμα Galois**) είναι ένα σώμα με πεπερασμένο πλήθος στοιχείων (:τάξη). Είναι γνωστό ότι:

- Κάθε πεπερασμένο σώμα έχει πλήθος στοιχείων έναν πρώτο αριθμό ή δύναμη ενός πρώτου αριθμού.
- Για κάθε $n \in \mathbb{N}$ και κάθε πρώτο αριθμό $p \in \mathbb{N}$, υπάρχει μοναδικό -ως προς ισομορφισμό- σώμα με p^n στοιχεία.

Ως $GF(p^r)$ συμβολίζεται το σώμα τάξεως $p^r \in \mathbb{N}$, για κάποιον πρώτο αριθμό $p \in \mathbb{N}$ και $r \in \mathbb{N}$. Τα απλούστερα παραδείγματα πεπερασμένων σωμάτων είναι τα σώματα τάξεως έναν πρώτο αριθμό $p \in \mathbb{N}$, συμβολίζονται ως $GF(p)$, ή $\mathbb{F}_p$, ή $\mathbb{Z}/p\mathbb{Z}$ και αντί των στοιχείων τους χρησιμοποιούνται οι αριθμοί $0, 1, \ldots, p-1$.

Έστω $\mathbb{F} \in \{\mathbb{R}\} \cup \{GF(p^r) : p \in \mathbb{N}$ πρώτος αριθμός και $r \in \mathbb{N}\}$.

Ορισμός 3.3.1. Η **ελλειπτική καμπύλη** $\mathcal{E}(\mathbb{F})$ **υπεράνω του σώματος** $\mathbb{F}$ ορίζεται ως $\mathcal{E}(\mathbb{F}) := \{(x, y) \in \mathbb{F} \times \mathbb{F} : p(x, y) = q(x)\} \cup \{\mathbf{O}_\infty\}$ όπου $p \in \mathbb{F}[x, y]$, $q \in \mathbb{F}[x]$ και:

- Εάν $\text{char}(\mathbb{F}) \notin \{2, 3\}$, τότε $p(x, y) = y^2$ και $q(x) = x^3 + ax + b$. Το $q \in \mathbb{F}[x]$ δεν έχει πολλαπλές ρίζες, ήτοι $4a^3 + 27b^2 \neq 0$. Η συνθήκη $y^2 = x^3 + ax + b$ ονομάζεται **βραχεία, κανονική μορφή Weierstrass**.
- Εάν $\text{char}(\mathbb{F}) = 2$, τότε είτε θεωρείται $p(x, y) = y^2 + cy$, είτε $p(x, y) = y^2 + xy$. Σε αμφότερες τις περιπτώσεις είναι $q(x) = x^3 + ax + b$.
- Εάν $\text{char}(\mathbb{F}) = 3$, τότε $p(x, y) = y^2$ και $q(x) = x^3 + ax^2 + bx + c$, με το $q \in \mathbb{F}[x]$ να μην έχει πολλαπλές ρίζες [ήτοι έχει μη-μηδενική διακρίνουσα].

Το $\mathbf{O}_\infty$ ονομάζεται ‘‘σημείο στο άπειρο’’.

Κανονική μορφή ελλειπτικών καμπυλών

Η πιο διαδεδομένη κανονική μορφή (από την οποία με χρήση μετασχηματισμών συνάγονται[§] οι εξισώσεις κάθε περίπτωσης του Ορισμού 3.3.1) είναι η εξής:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{(μακρά, κανονική μορφή Weierstrass)}$$

με $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$ και διακρίνουσα $\Delta \neq 0$, όπου

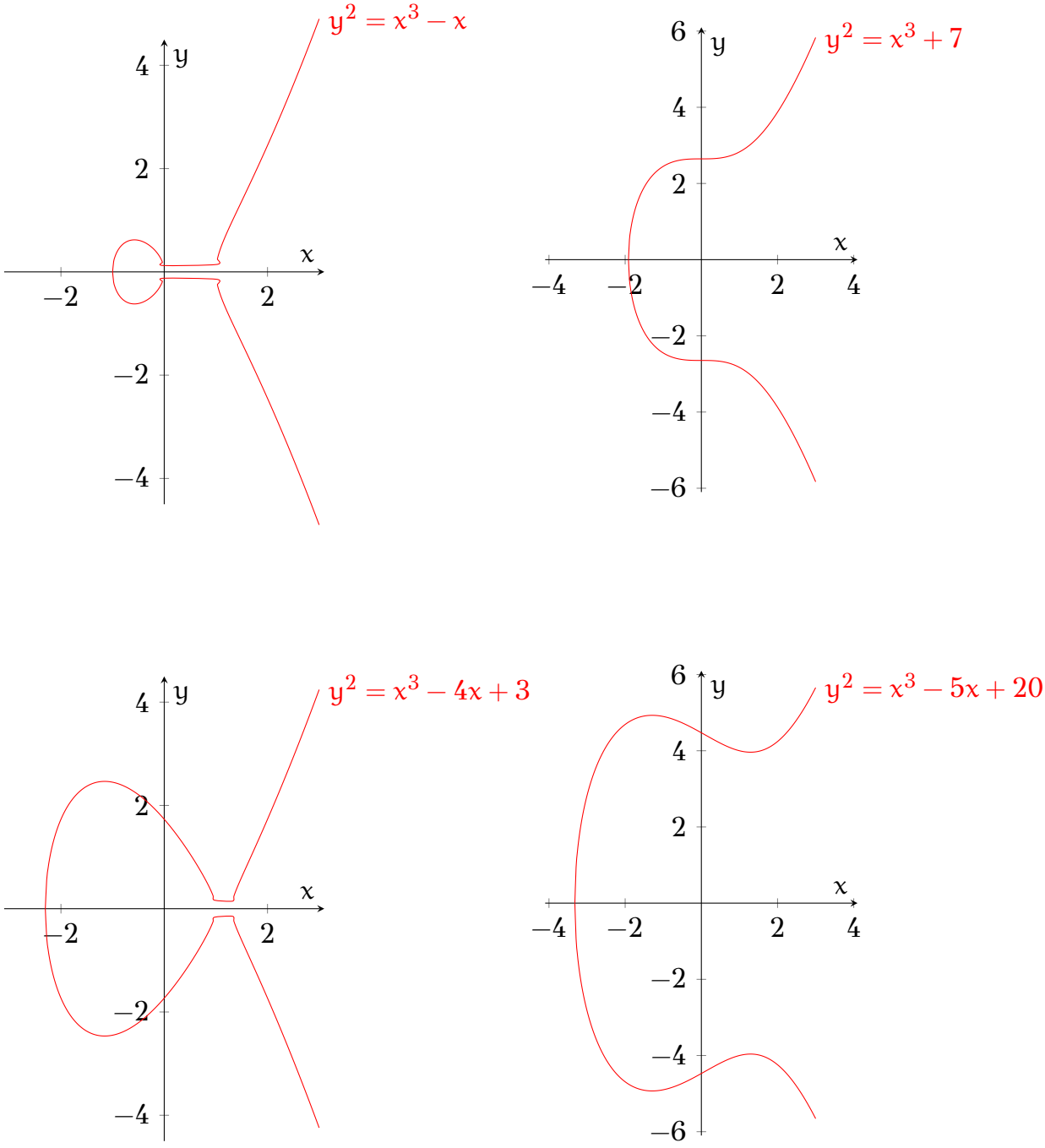
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

για $b_2 := a_1^2 + 4a_4$, $b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$, $b_4 := 2a_4 + a_1a_3$ και $b_6 := a_3^2 + 4a_6$. Εάν $\text{char}(\mathbb{F}) \notin \{2, 3\}$, τότε $\Delta = -16(4a_4^3 + 27a_6)$.

[§] Έστω $\mathbb{K}$, με $\text{char}(\mathbb{K}) \notin \{2, 3\}$. Στην μακρά κανονική μορφή Weierstrass

1. εφαρμόζεται (όντας $\text{char}(\mathbb{K}) \neq 2$) ο μετασχηματισμός $y \longmapsto y - \frac{1}{2}(a_1x + a_3)$ και
2. στο αποτέλεσμα εφαρμόζεται (διότι $\text{char}(\mathbb{K}) \neq 3$) ο μετασχηματισμός $x \longmapsto x - \frac{1}{3}b_2$

και τότε προκύπτει η βραχεία, κανονική μορφή Weierstrass.

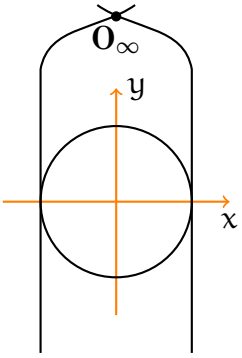


Σχήμα 3.3: Ελλειπτικές καμπύλες υπεράνω του $\mathbb{R}$

Το σημείο στο άπειρο

Έστω $S := \{(X,Y,Z) \in \mathbb{R}^3 : (X,Y,Z) \neq (0,0,0)\}$. Ορίζεται μία σχέση ισοδυναμίας υπεράνω των στοιχείων του S, ως:

$$(X,Y,Z) \sim (A,B,C) \Leftrightarrow_{\text{ορ}} (\exists \lambda \in \mathbb{Z})[X = \lambda A \wedge Y = \lambda B \wedge Z = \lambda C] \quad (3.3)$$



Η κλάση ισοδυναμίας $[\![(X,Y,Z)]\!]_\sim$ του $(X,Y,Z) \in S$ καλείται **προβολικό σημείο**. Το σύνολο $\mathbb{P} := \{[\![(X,Y,Z)]\!]_\sim \subseteq \mathbb{R}^3 : (X,Y,Z) \in S\}$ καλείται **προβολικό επίπεδο**. Εάν $(X,Y,Z) \in S$, με $Z \neq 0$, τότε $(\exists!(x,y,1) \in S)\big[(X,Y,Z) \in [\![(x,y,1)]\!]_\sim\big]$ (είναι $x := X/Z$ και $y := Y/Z$). Συνεπώς,

$$\begin{aligned}\mathbb{P} &= \{[\![(X,Y,Z)]\!]_\sim \subseteq \mathbb{R}^3 : (X,Y,Z) \in S \text{ και } Z \neq 0\} \cup \{[\![(X,Y,0)]\!]_\sim \subseteq \mathbb{R}^3 : (X,Y,0) \in S\} \\ &= \{(x,y) \in \mathbb{R}^2 : (X,Y,Z) \in [\![(x,y,1)]\!]_\sim \text{ για } (X,Y,Z) \in S \text{ με } Z \neq 0\} \cup \\ &\quad \cup \{[\![(X,Y,0)]\!]_\sim \subseteq \mathbb{R}^3 : (X,Y,0) \in S\}\end{aligned}$$

Τα μεν πρώτα σημεία ($(X,Y,Z) \in S$ με $Z \neq 0$) βρίσκονται πάνω στο συγγενές (affine) επίπεδο (:χώρος διάστασης 2). Τα μεν επόμενα ($(X,Y,0) \in S$) σε μια ευθεία την αποκαλούμενη ''επ΄ άπειρον ευθεία''. Ως *σημείο στο άπειρο* ορίζεται το προβολικό σημείο $[\![(0,1,0)]\!]_\sim$, ήτοι η τομή του άξονα $y'y$ με την επ΄ άπειρον ευθεία. Στις εφαρμογές πολλές φορές είναι βολικό να θεωρείται $\mathbf{O}_\infty = (0,0)$.

Γεωμετρική ερμηνεία πρόσθεσης δύο σημείων

Έστω ένα σώμα $\mathbb{K}$ και μία ελλειπτική καμπύλη $\mathcal{E}(\mathbb{K})$ και $P,Q \in \mathcal{E}$. Ορίζεται:

1. Εάν $P = \mathbf{O}_\infty$, τότε $\boxminus P := \mathbf{O}_\infty$ και $P \boxplus Q = Q$.
   [Το $\mathbf{O}_\infty$ θεωρείται ως ουδέτερο στοιχείο στην πρόσθεση $\boxplus : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$.]

Εφ εξής θεωρείται πως $P \neq \mathbf{O}_\infty \neq Q$.

2. Το $\boxminus P$ ορίζεται να είναι το σημείο (επί της $\mathcal{E}$) με ίδια τετμημένη και αντίθετη τεταγμένη σε σχέση με το P.
3. Εάν τα $P,Q \in \mathcal{E}$ έχουν διαφορετικές τετμημένες, τότε η ευθεία $\ell = \overline{PQ}$ η οποία διέρχεται από τα $P,Q \in \mathcal{E}$ τέμνει την $\mathcal{E}$ σε ακριβώς ένα σημείο, έστω $R \in \mathcal{E}$. Ορίζεται $P \boxplus Q := \boxminus R$.
4. Εάν $Q = \boxminus P$, τότε $P \boxplus Q := \mathbf{O}_\infty$.
5. Εάν $P = Q$, τότε ορίζεται $P \boxplus Q := \boxminus R$, όπου
   (α΄) εάν το $P \in \mathcal{E}$ είναι σημείο καμπής ορίζεται $R := P$·
   (β΄) διαφορετικά η εφαπτομένη στο $P \in \mathcal{E}$ θα τέμνει την $\mathcal{E}$ σε ακριβώς ένα σημείο, έστω $R \in \mathcal{E}$.

Ο λόγος που θεωρείται το σημείο $\boxminus R$ αντί του R παραπάνω είναι ο ακόλουθος: έστω ότι $P \boxplus Q = R$, τότε ισχύει ότι $P \boxplus R = Q$ και ότι $Q \boxplus R = P$ κι άρα $P = Q = R = \mathbf{O}_\infty$ και η πράξη $\boxplus : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$ δεν είναι καλώς ορισμένη.

Η μονοσήμαντη κατασκευή του σημείου $P \boxplus Q$ από τα P, Q στηρίζεται στο

Θεώρημα 3.3.2 (Bezout). Το πλήθος των κοινών σημείων δύο καμπυλών στο επίπεδο, οι οποίες δεν τέμνονται σε άπειρα σημεία, δεν υπερβαίνει το γινόμενο των βαθμών τους, με την ισότητα να ισχύει εάν συνυπολογισθούν και τα σημεία στο άπειρο και εκείνα με μιγαδικές συντεταγμένες.

Θεώρημα 3.3.3. Έστω ένα σώμα $\mathbb{K}$ και μία ελλειπτική καμπύλη $\mathcal{E}(\mathbb{K})$, με μακρά κανονική μορφή Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, για $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. Έστω $P = (x_1, y_1) \in \mathcal{E}$, $Q = (x_2, y_2)$ και $P \boxplus Q = (x_3, y_3)$. Το αποτέλεσμα $P \boxplus Q$ υπολογίζεται ως εξής:

(i) Ορίζεται $\boxminus P := (x, -y - a_1x - a_3)$.

(ii) Εάν $x_1 = x_2$ και $y_1 + y_2 + a_1x_2 + a_3 = 0$ (περίπτωση $Q = \boxminus P$), τότε $P \boxplus Q = \mathbf{O}_\infty$.

(iii) Εάν $y_1 + y_2 + a_1x_2 + a_3 \neq 0$, τότε

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \qquad y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

όπου

(α') Εάν $x_1 \neq x_2$ (περίπτωση $P \neq \pm Q$), τότε $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ και $\nu = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$ (η εξίσωση $y = \lambda x + \nu$ διέρχεται από τα διακριτά σημεία $P, Q \in \mathcal{E}$).

(β') Εάν $x_1 = x_2$ (περίπτωση $P = Q$), τότε $\lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$ και $\nu = \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$ (η εξίσωση $y = \lambda x + \nu$ είναι η εφαπτομένη ευθεία στο σημείο $P \in \mathcal{E}$).

Η δομή $G(\mathcal{E}) := (\mathcal{E}, \boxplus)$ συνιστά αβελιανή[¶] ομάδα.

Για την απόδειξη του παραπάνω όρα [Si8$_5$]. Ούσα η $(\mathcal{E}, \boxplus)$ αβελιανή, υιοθετούνται άπαντες οι συμβολισμοί και οι έννοιες από τη Θεωρία Ομάδων που αφορούν τις αβελιανές ομάδες.

Έστω $k \in \mathbb{Z}$ και $P \in \mathcal{E}(\mathbb{K})$ για ένα τυχαίο σώμα $\mathbb{K}$. Η πράξη του **βαθμωτού πολλαπλασιασμού** $\boxdot : \mathbb{Z} \times \mathcal{E} \longrightarrow \mathcal{E}$ είναι η επαναλμβανομενη πρόσθεση $|k| \in \mathbb{N}_0$ αντιτύπων του P (εάν $k \geqslant 0$), ή του $\boxminus P$ (εάν $k < 0$).

Το παραπάνω Θεώρημα απαντάται ξανά στην §3.3.1.Γ′ όπου εκεί έχει προσαρμοσθεί στην περίσταση όπου $\mathbb{K} = \mathbb{F}_p$, για κάποιον πρώτο αριθμό $p \in \mathbb{N}$.

[¶]Μιας και η ευθεία (εφαπτομένη) που έχει φορέα το $\vec{PQ}$ (το $P = Q$) συμπίπτει σχηματικά με την ευθεία (εφαπτομένη) που έχει φορέα το $\vec{QP}$ (το $Q = P$).

3.3.1.Β΄ Ελλειπτικές καμπύλες υπεράνω πεπερασμένων σωμάτων

Για τη συνέχεια του Κεφαλαίου θα θεωρούνται καμπύλες της μορφής

$$\begin{aligned}\mathcal{E} = \{(x,y) \in \mathrm{GF}(p) : y^2 = x^3 + ax + b \pmod p,\ a,b \in \mathrm{GF}(p),\\ 4a^3 + 27b^2 \not\equiv 0 \pmod p\} \cup \{\mathbf{O}_\infty\}\end{aligned} \tag{3.4}$$

για κάποιον πρώτο αριθμό $p \in \mathbb{N}$ οι οποίες θα συμβολίζονται ως $\mathcal{E}(\mathrm{GF}(p))$.

Ορισμός 3.3.4. Το πλήθος των στοιχείων μιας ελλειπτική καμπύλης $\mathcal{E}$ υπεράνω ενός (τυχαίου) σώματος $\mathbb{K}$ καλείται **τάξη** της $\mathcal{E}$ και συμβολίζεται ως $\#\mathcal{E}$.

Η καμπύλη (3.4) έχει $\#\mathcal{E} \leqslant 2p + 1 \in \mathbb{N}$ σημεία μιας και:

- $\mathbf{O}_\infty \in \mathcal{E}$ και
- υπάρχουν $p \in \mathbb{N}$ επιλογές για το $x \in \mathrm{GF}(p)$ και για κάθε μία εξ αυτών υπάρχουν το πολύ 2 επιλογές για το $y \in \mathrm{GF}(p)$ που ικανοποιούν την (3.4).

Ένα φράγμα όσον αφορά το πλήθος των σημείων της ελλειπτικής καμπύλης (3.4) παρέχεται από το

Θεώρημα 3.3.5 (Hasse). Έστω $p \in \mathbb{N}$ ένας πρώτος αριθμός. Για κάθε ελλειπτική καμπύλη $\mathcal{E}(\mathrm{GF}(p))$ το πλήθος των σημείων αυτής $\#\mathcal{E}$ έχει ως εξής:

$$p + 1 - 2\sqrt{p} \leqslant \#\mathcal{E} \leqslant p + 1 + 2\sqrt{p}$$

Ορισμός 3.3.6. Έστω μία ελλειπτική καμπύλη $\mathcal{E}$ της μορφής (3.4). Ο αριθμός $t \in \mathbb{Z}$, με $\#\mathcal{E} = p + 1 - t$ καλείται **ίχνος του Frobenius**.

- Εάν $t = 1$, τότε η καμπύλη καλείται **μη-ομαλή** (anomalus).
- Εάν $p \mid t$, τότε η καμπύλη καλείται **υπεριδιάζουσα** (supersingular).

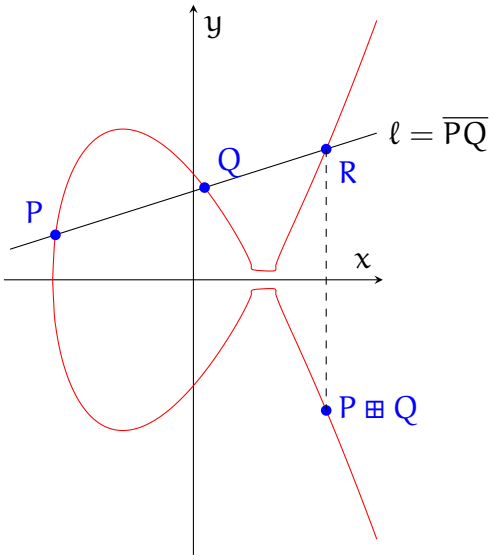
Οι μη-ομαλές και υπεριδιάζουσες ελλειπτικές καμπύλες αποφεύγονται στο να χρησιμοποιούνται σε κρυπτογραφικές εφαρμογές [όρα §3.3.3].

Ο ακριβής αριθμός των σημείων μιας ελλειπτικής καμπύλης δίδεται από τον αλγόριθμο του Schoof, ο οποίος έχει χρονική πολυπλοκότητα $\mathcal{O}((\log_2 p)^8)$. Εφ όσον, λοιπόν, δύναται να υπολογισθεί ο $\#\mathcal{E}$ ανακύπτει η ανάγκη ώστε να μελετηθεί εις βάθος η $\mathrm{G}(\mathcal{E})$. Πιο συγκεκριμένα θα ήταν θεμιτό να βρεθεί μία ‘‘μεγάλης τάξης’’ κυκλική υποομάδα της $\mathrm{G}(\mathcal{E})$.

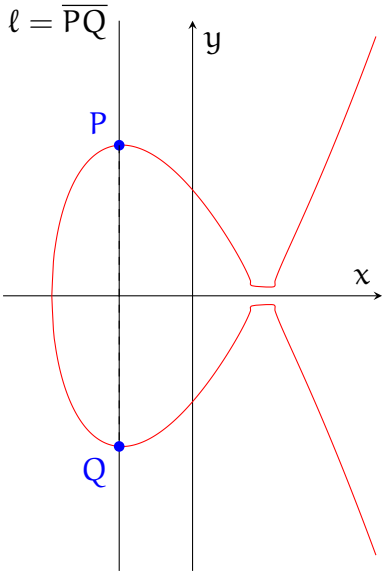
Η τάξη $q \in \mathbb{N}$ μιας υποομάδας της $\mathrm{G}(\mathcal{E})$ η οποία έχει ως γεννήτορα το σημείο $P \in \mathrm{G}(\mathcal{E})$ -η υποομάδα συμβολίζεται ως $\langle P \rangle$- υπολογίζεται ως εξής:

1. Υπολογισμός της $\#\mathcal{E}$ με χρήση του αλγορίθμου του Schoof [Sch8_5, Sch$_{95}$].
2. $q = \min\{m \in \mathbb{Z} : m \mid \#\mathcal{E} \text{ και } m \boxdot P = \mathbf{O}_\infty\}$.

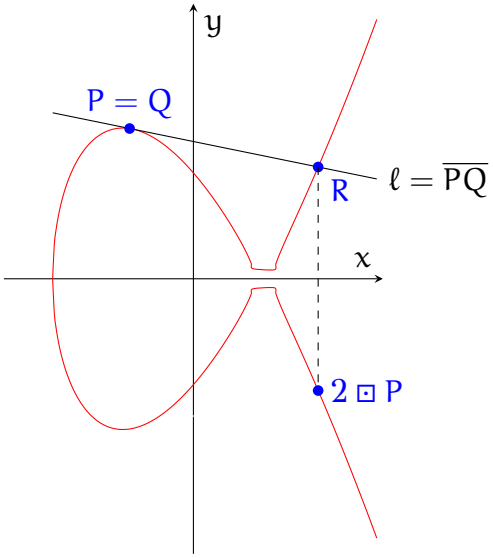
Θεώρημα 3.3.7 (Θεώρημα Lagrange). Έστω $\mathcal{E}$ μία ελλειπτική καμπύλη υπεράνω ενός πεπερασμένου σώματος. Ισχύει ότι $(\forall P \in \mathcal{E})[\mathrm{ord}(P) \mid \#\mathcal{E}]$.



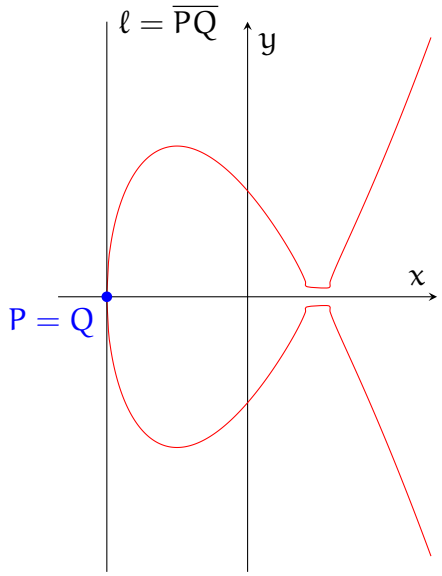
(α΄) Περίπτωση: $P \neq Q$ και $x_1 \neq x_2$



(β΄) Περίπτωση: $P \neq Q$ και $x_1 = x_2$



(γ΄) Περίπτωση: $P = Q$ και $y_1 = y_2 \neq 0$



(δ΄) Περίπτωση: $P = Q$ και $y_1 = y_2 = 0$

Σχήμα 3.4: Οι περιπτώσεις για την πρόσθεση των σημείων $P = (x_1, y_1) \in \mathcal{E}$ και $Q = (x_2, y_2) \in \mathcal{E}$

3.3.1.Γ΄ Ελλειπτικές καμπύλες στην Κρυπτογραφία

Στις κρυπτογραφικές εφαρμογές (όπως αυτές της §3.3.2) γίνεται χρήση των εξής:

- **Μη-υπεριδιάζουσες ελλειπτικές καμπύλες υπεράνω του σώματος** $\mathrm{GF}(p)$, **με** $p \in \mathbb{N}$ **να είναι πρώτος αριθμός με** $p \geqslant 3$ **και** $\mathrm{char}(\mathrm{GF}(p)) \notin \{2, 3\}$.
  [Ο τύπος τους δίδεται από την βραχεία, κανονική μορφή Weierstrass: $y^2 = x^3 + ax + b$, για $a, b \in \mathrm{GF}(p)$ με διακρίνουσα $\Delta = -16(4a^3 + 27b^2) \neq 0$.]
- **Μη-υπεριδιάζουσες ελλειπτικές καμπύλες υπεράνω του** $\mathrm{GF}(2^k)$, **με** $k \in \mathbb{N}$.
  [Όντας $\mathrm{char}(\mathrm{GF}(2^k)) = 2$, ο τύπος τους δίδεται την εξίσωση με μορφή: $y^2 + xy = x^3 + ax^2 + b$, για $a, b \in \mathrm{GF}(2^k)$ με διακρίνουσα $\Delta = b \neq 0$.]
- **Ελλειπτικές καμπύλες Koblitz.**
  [Πρόκειται για μη-ομαλές ελλειπτικές καμπύλες υπεράνω του $\mathrm{GF}(2^k)$, για $k \in \mathbb{N}$, με το τύπο: $y^2 + xy = x^3 + ax^2 + b$, για $a, b \in \mathrm{GF}(2^k)$.]

Οι ελλειπτικές καμπύλες υπεράνω των σωμάτων $\mathrm{GF}(2^k)$, $k \in \mathbb{N}$, χρησιμοποιούνται σε ψηφιακές τεχνολογίες (οι πράξεις γίνονται στο δυαδικό σύστημα).

Αναπαράσταση ενός μηνύματος με χρήση ελλειπτικών καμπυλών

Στην ελλειπτική καμπύλη $\mathcal{E}(\mathbb{F}_p)$, για $p \in \mathbb{N}$ πρώτο αριθμό, με βραχεία, κανονική μορφή Weierstrass: $y^2 = x^2 + Ax + B$, για $A, B \in \mathbb{F}_p$, έστω το μήνυμα προς αποστολή $m \in \{0, 1, 2, \ldots, \frac{p}{100}\}$. Ακολουθείται η εξής μεθοδολογία:

1: **επιλογή** k; /* Αρκεί $k = 2$ */
2: **για** $(i = 0, 1, \ldots, 10^k - 1)$
3: $\quad x_i \leftarrow 10^k m + i$;
4: $\quad s_i \leftarrow x_i^3 + Ax_i + B$;
5: $\quad$ **εάν** $((\exists y_i \in \mathbb{N})[s_i = y_i^2])$ **τότε**
6: $\quad\quad$ **επίστρεψε** $P := (x_i, y_i)$; **έξοδος**;
7: $\quad$ **τέλος εάν**
8: **τέλος για**
9: **τύπωσε** ‘‘Επίλεξε άλλη καμπύλη!’’;

Μία συνθήκη ώστε να $(\exists y_i \in \mathbb{N})[y_i^2 = s_j]$ είναι η συνθήκη: $s_j^{(p-1)} \equiv 1 \pmod{p}$. Για τον υπολογισμό της $\sqrt{s_i}$ μπορεί να χρησιμοποιηθεί ο αλγόριθμος των Shanks-Tonelli [Sha73, Di]. Για την ανάκτηση του $m \in \{0, 1, \ldots, p/100\}$, δεδομένου του $P = (x, y) \in \mathcal{E}$ αρκεί να υπολογισθεί η ποσότητα $\left\lfloor \frac{x}{10^k} \right\rfloor$. Η τεταγμένη $y \in \mathbb{F}_p^\times$ αποτελεί τυχαίο στοιχείο του $\mathbb{F}_p^\times$ και για $p > 2$ όντας το σώμα $\mathbb{F}_p^\times$ κυκλική ομάδα τάξης $p \in \mathbb{N}$ η πιθανότητα ένα s_i να είναι τετράγωνο κάποιου αριθμού είναι $\approx 1/2$. Άρα, η πιθανότητα ώστε ο αλγόριθμος να επιστρέψει ένα σημείο $P \in \mathcal{E}$ είναι $1 - 2^{-10^k}$.

Πράξεις σημείων ελλειπτικής καμπύλης $\mathcal{E}(\mathbb{F}_p)$

Έστω μία μη-υπεριδιάζουσα ελλειπτική καμπύλη $\mathcal{E}(\mathbb{F}_p)$, για κάποιον πρώτο αριθμό $p \in \mathbb{N}$, με $\mathrm{char}(\mathrm{GF}(p)) > 3$ και βραχεία κανονική μορφή Weierstrass: $y^2 = x^3 + ax + b$, για $a, b \in \mathbb{F}_p$. Θεωρούνται τα σημεία $P := (x_1, y_1) \in \mathcal{E}$, $Q := (x_2, y_2) \in \mathcal{E}$

- Εάν $x_1 \neq x_2$ ή $P = Q$ με $y_1 (= y_2) \neq 0$, τότε $P \boxplus Q = (x_3, y_3)$, όπου $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $x_3 = \lambda^2 - x_1 - x_2$ και $y_3 = \lambda(x_1 - x_3) - y_1$.
- Αλλιώς (είτε $x_1 = x_2 \wedge y_1 \neq y_2$, είτε $P = Q \wedge y_1 (= y_2) = 0$) $P \boxplus Q = \mathbf{O}_\infty$ (καθ' όσον η ευθεία που διέρχεται από τα P, Q είναι παράλληλη στην άξονα $y'y$).

Αλγόριθμος 3.3.8 DOUBLE_AND_ADD_ALWAYS$(b_{\ell-1}, \ldots, b_0), P)$: Βαθ/τός πολ/μός

Είσοδος: $(b_{\ell-1}, \ldots, b_1, b_0) \in \{0,1\}^\ell$ και $P \in \mathcal{E}$.
Έξοδος: $\left(\sum_{i=0}^{\ell-1} b_i 2^i\right) \boxdot P \in \mathcal{E}$.

1: $Q_0 \leftarrow Q_1 \leftarrow \mathbf{O}_\infty$;
2: **εάν** $(b_0 = 1)$ **τότε**
3: $\quad Q_0 \leftarrow P$;
4: **τέλος εάν**
5: **για** $(i = 0, 1, \ldots, \ell - 1)$
6: $\quad Q_0 \leftarrow 2 \boxdot Q_0$; $\quad Q_1 \leftarrow Q_0 \boxplus P$; $\quad Q_0 \leftarrow 2 \boxdot Q_{d_i}$;
7: **τέλος για**
8: **επίστρεψε** Q_0;

3.3.2 Υλοποιήσεις

Ορισμός 3.3.9. Έστω ένας πρώτος αριθμός $p \in \mathbb{N}$. Οι **παράμετροι τομέα** (domain parameters) της ελλειπτικής καμπύλης $\mathcal{E}(\mathbb{F}_p)$ είναι η εξάδα:

$$(p, a, b, P, n, h) \in \mathbb{N} \times \mathrm{GF}(p) \times \mathrm{GF}(p) \times \mathcal{E} \times \mathbb{N} \times \mathbb{N}$$

όπου

- $p \in \mathbb{N}$ είναι η τάξη του σώματος $\mathrm{GF}(p)$,
- $a, b \in \mathrm{GF}(p)$ είναι οι συντελεστές της βραχείας, κανονικής μορφής Weierstrass της $\mathcal{E}$,
- $P \in \mathcal{E}$ το **σημείο βάσης**,
- $n = \mathrm{ord}(P)$ είναι η τάξη του σημείου βάσης $P \in \mathcal{E}$,
- $h := {}^{\#\mathcal{E}}/_n$ ο **συμπαράγοντας** (cofactor) [από το Θεώρημα 3.3.5: $h \in \mathbb{N}$].

Το 1985 προτάθηκε από τους Neal Koblitz (στο [Ko87]) και Victor Miller (στο [Mi86]) το **Πρόβλημα Διακριτού Λογαρίθμου σε Ελλειπτικές Καμπύλες**:

Το πρόβλημα ECDLP: Γνωστών των παραμέτρων τομέα της ελλειπτικής καμπύλης $\mathcal{E}(\mathrm{GF}(p))$ και $Q \in \langle P \rangle$ να βρεθεί $k \in \mathbb{Z}_n$, με $Q = k \boxdot P$.

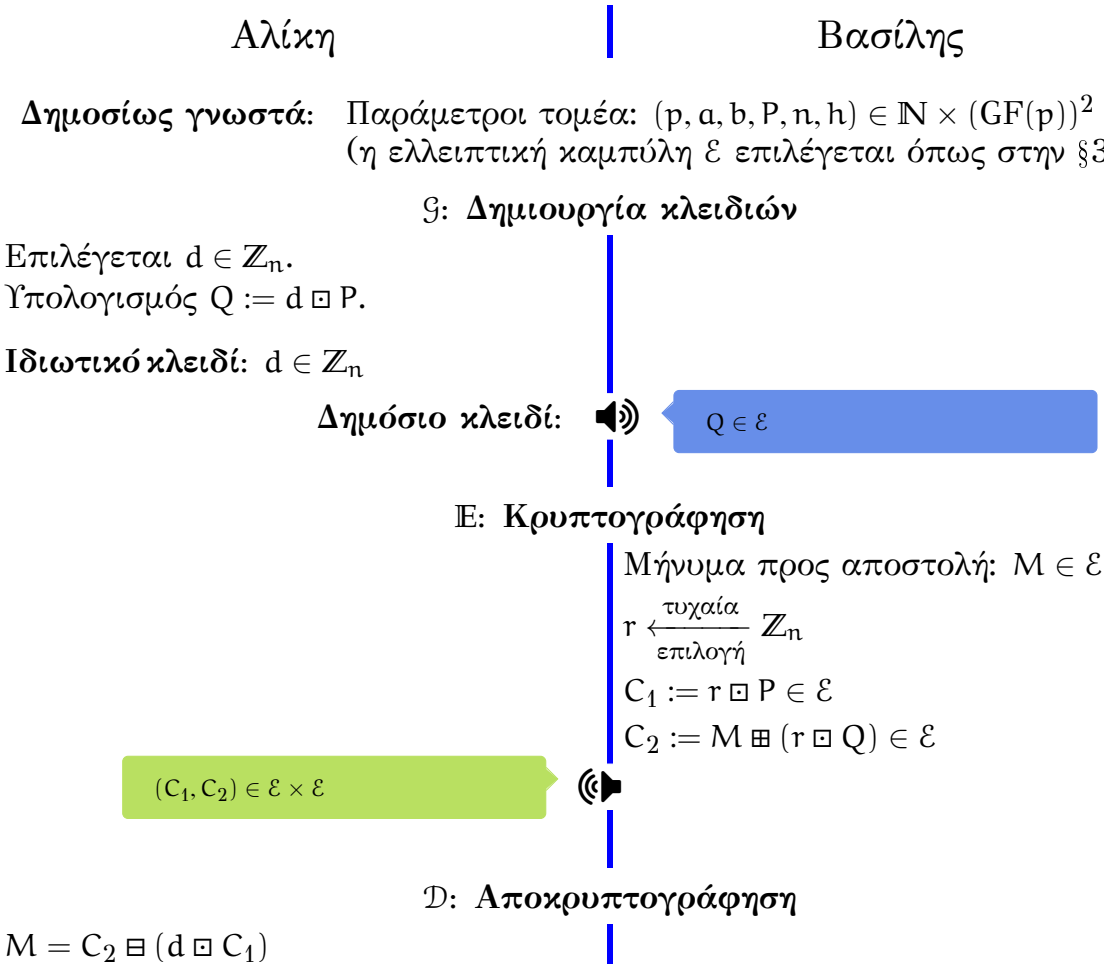
Ελλειπτικό πρωτόκολλο Diffie-Hellman

Το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman [όρα Σχήμα ;;] μπορεί αντί να υπολογίζει στοιχεία εντός μιας κυκλικής ομάδας, να κάνει χρήση βαθμωτού πολλαπλασιασμού σε στοιχεία μιας ελλειπτικής καμπύλης. Έτσι το υποκείμενο πρόβλημα που καλείται να επιλύσει ο αντίπαλος είναι:

Το πρόβλημα ECDHP: Δεδομένων των παραμέτρων τομέα της ελλειπτικής καμπύλης $\mathcal{E}(\mathrm{GF}(p))$ και $a \boxdot P, b \boxdot P \in \mathcal{E}$, με $a, b \in \mathbb{Z}_n$, να βρεθεί το $(ab) \boxdot P \in \mathcal{E}$.

3.3.2.Α΄ Ελλειπτικό κρυπτοσύστημα El Gamal

Το ανάλογο του κρυπτοσυστήματος που προτάθηκε από τον Taher El Gamal στο [EG85] το 1985 για τις ελλειπτικές καμπύλες είναι το ακόλουθο σχήμα, το οποίο στηρίζει την ασφάλειά του στο πρόβλημα ECDLP:



Σχήμα 3.5: Το ελλειπτικό κρυπτοσύστημα El Gamal

Λήμμα 3.3.10 (Ορθότητα ελλειπτικού κρυπτοσυστήματος El Gamal). *Στο Σχήμα 3.5 ισχύει ότι* $(\forall M \in \mathcal{E})[\mathcal{D}(\mathbb{E}(M)) = M]$.

Απόδειξη. Είναι $d \boxdot C_1 = d \boxdot (r \boxdot P) \overset{d,r\in\mathbb{Z}_n}{=} r \boxdot (d \boxdot P) = r \boxdot Q$. Κατά συνέπεια, $C_2 \boxminus d \boxdot C_1 = \big[M \boxplus (r \boxdot Q)\big] \boxminus d \boxdot C_1 = \big[M \boxplus (r \boxdot Q)\big] \boxminus r \boxdot Q = M \in \mathcal{E}$. □

3.3.3 Ασφάλεια

Εξετάζεται η ασφάλεια των σχημάτων σε ελλειπτικές καμπύλες, τόσο έναντι σε ευθείες επιθέσεις στις παραμέτρους τους.

Επίθεση MOV

Η επίθεση MOV οφείλεται στους Albert Menezes, Tatsuaki Okamoto και Scott Vanstone από το 1993 και περιέχεται στο [MOV93]. Η ιδέα της επίθεσης είναι:

> Το ECDLP για την ελλειπτική καμπύλη $\mathcal{E}$ υπεράνω του σώματος $\mathbb{F}_p$ να αναχθεί στο DLP στο σώμα $\mathbb{F}_{p^\ell}$, όπου $\ell = \min\{m \in \mathbb{N} : p^m \equiv 1 \pmod{\#\mathcal{E}}\}$.

Ζευγάρωμα Weil

Έστω $\mathcal{E}$ μία ελλειπτική καμπύλη υπεράνω του σώματος $\mathbb{K}$. Θεωρείται $n \in \mathbb{N}$, ώστε εάν $\mathrm{char}(K) > 0$, τότε $\mu\kappa\delta\big(n, \mathrm{char}(\mathbb{K})\big) = 1$. Για το ζευγάρωμα Weil

$$e : \mathcal{E}[n] \times \mathcal{E}[n] \longrightarrow \{x \in \overline{\mathbb{K}} : x^n = 1\}$$

όπου $\mathcal{E}[n] := \{T \in \mathcal{E} : n \boxdot T = \mathbf{O}_\infty\}$ ισχύει ότι

- $\big(\forall P, Q \in \mathcal{E}[n]\big)(\forall r, s \in \mathbb{N})\big[e(rP, sQ) = (e(P, Q))^{rs}\big]$.
- $(\forall S \in \mathcal{E})[e(S, T) = 1] \implies T = \mathbf{O}_\infty$ και $(\forall T \in \mathcal{E})[e(S, T) = 1] \implies S = \mathbf{O}_\infty$.

ήτοι είναι n-οστή ρίζα της μονάδος και μη-εκφυλισμένη διγραμμική μορφή.

Αλγόριθμος 3.3.11 MOV_Attk: Αναγωγή του ECDLP στο DLP

Δεδομένα: Ελλειπτική καμπύλη $\mathcal{E}$ υπεράνω του $\mathbb{F}_p$ και $P, Q \in \mathcal{E}$.

1: $s \leftarrow 0$;
2: **επανάλαβε**
3: $\quad S_i \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathcal{E}$ θεωρημένη υπεράνω του $\mathbb{F}_{p^\ell}$;
4: $\quad M_i \leftarrow \mathrm{ord}(S_i)$; $\quad d_i \leftarrow \mu\kappa\delta(M_i, \#\mathcal{E})$; $\quad T_i \leftarrow (M_i/d_i)S_i$;
5: $\quad u_i \leftarrow e(P, T_i)$; $\quad w_i \leftarrow e(Q, T_i)$;
6: $\quad k_i \leftarrow \mathtt{DLP}(u, w)$ στο $\mathbb{F}^\times_{p^\ell}$ /* Ισχύει ότι $u_i^{k_i} = w_i$ στο $\mathbb{F}_{p^\ell}$, με $k_i \in \mathbb{Z}_n$ */
7: $\quad s \leftarrow s + 1$;
8: **έως ότου** $(\epsilon\kappa\pi(d_1, d_2, \ldots, d_s) = \#\mathcal{E})$
9: **εύρεση** $k \in \mathbb{Z}_{\#\mathcal{E}}$ **τέτοιο ώστε** $(\forall i = 1, 2, \ldots, s)\big[k \equiv k_i \pmod{d_i}\big]$;

Απόδειξη (ορθότητας του Αλγορίθμου 3.3.11). Κατ' αρχάς $\mathrm{ord}(T_i) = d_i \mid N$ κι άρα $T_i \in \mathcal{E}[\#\mathcal{E}]$. Έστω $w_i = e(S_i, T_i)$, για κάποιο τυχαίο $S_i \in \mathcal{E}$ θεωρημένη υπεράνω του $\mathbb{F}_{p^\ell}$. Τώρα, έστω $\zeta \in \{u_i, w_i\}$ και $R \in \{P, Q\}$ με $R = P$ εάν $\zeta = u_i$ και $R = Q$ εάν $\zeta = w_i$. Υπολογίζεται:

$$\zeta^{d_i} = (e(R, T_i))^{d_i} = e(R, d_i \boxdot T_i) = e(R, M_i S_i) = e(R, \mathbf{O}_\infty) = 1 \tag{3.5}$$

Άρα, $u_i, w_i \in \{x \in \mathbb{F} : x^{d_i} = 1\}$. Επομένως, έχει νόημα να επιλυθεί το πρόβλημα του διακριτού λογαρίθμου για τα u_i, w_i στο $\mathbb{F}_{p^\ell}$ και να δώσει $k_i \in \mathbb{Z}_n$, με $u_i^{k_i} = w_i$.

Τώρα, έστω ότι $Q = k \boxdot P$ κι έστω $l_i \in \mathbb{Z}$, με $k \equiv l_i \pmod{d_i}$. Έπεται ότι

$$w = e(Q, T_i) = e(k \boxdot P, T_i) = (e(P, T_i))^k = u^k \implies u^k = w$$

Επίσης,

$$u^{d_i} \overset{(3.5)}{=} 1 \implies u^{l_i} \equiv w \pmod{d_i} \implies l_i \equiv k_i \pmod{d_i}$$

Όντας $k \equiv l_i \pmod{d_i}$ και $l_i \equiv k_i \pmod{d_i}$, άρα και $k \equiv k_i \pmod{d_i}$. □

Η επίθεση είναι αποτελεσματική όταν ο $\ell \in \mathbb{N}$ προκύπτει να είναι μικρός αριθμός. Συνήθως $\ell \approx p$ κι άρα η παραπάνω αναγωγή δεν διευκολύνει και πολύ τη λύση του προβλήματος.

Επί πλέον των προαναφερθέντων, μία παρόμοια επίθεση αποτελεί εκείνη των Hans-Georg Rück και Gerhard Frey από το 1994 στο [RF94].

Επίθεση σε μη-ομαλές καμπύλες

Η Atsuko Miyaji στο [Mi92] το 1993 πρότεινε τη χρήση μη-ομαλών ελλειπτικών καμπυλών καθ' ότι είναι ανθεκτικές στις επιθέσεις MOV. Ωστόσο το πρόβλημα ECDLP υπεράνω μιας ελλειπτικής καμπύλης $\mathcal{E}$ με $\#\mathcal{E}$ υπεράνω του σώματος $\mathbb{F}_q$, όπου ο $q \in \mathbb{N}$ είναι πρώτος αριθμός, μπορεί να αναχθεί στο πρόβλημα DLP στην προσθετική ομάδα $\mathbb{F}_q^+$ των ακεραίων υπόλοιπο $q \in \mathbb{N}$. Αυτό συμβαίνει διότι η ομάδα $G(\mathcal{E})$ είναι κυκλική τάξη έναν πρώτο αριθμό (τον $q \in \mathbb{N}$) και κατά συνέπεια είναι ισόμορφη με την προσθετική ομάδα $\mathbb{F}_q^+$. Οι Kiyomichi Araki και Takakazu Satoh το 1998 στο [AS98], ο Nigel Smart το 1999 στο [Sm99] και ο Igor Semaev το 1998 στο [Se98] έδειξαν πως ο ισομορφισμός $\Psi : G(\mathcal{E}) \longrightarrow \mathbb{F}_q^+$ μπορεί να υπολογισθεί με αποτελεσματικό τρόπο.

Η μέθοδος ελαχίστου βήματος - μεγίστου βήματος

Ο αλγόριθμος οφείλεται στον Daniel Shanks, το 1971, και περιέχεται στο [Sha71]. Ωστόσο, το 1994 ο Vasili Il'ich Nechaev στο [Ne94] αναφέρει πως ο αλγόριθμος ήταν γνωστός στον Alexander Osipovich Gel'fond ήδη από το 1962. Ο αλγόριθμος έχει χρονική πολυπλοκότητα και χωρική πολυπλοκότητα τάξης $\mathcal{O}(\sqrt{\#\mathcal{E}})$.

Τυχαίοι περίπατοι

Θεωρείται το γράφημα Cayley της ομάδας $G(\mathcal{E})$, μία τυχαία συνάρτηση $f : \mathcal{E} \longrightarrow \mathcal{E}$ κι ένα σημείο $P_0 \in \mathcal{E}$. Ένας **περίπατος** από το $P_0 \in \mathcal{E}$ ορίζεται ως P_0, $P_1 := f(P_0)$, $P_2 := f(P_1)$, $P_3 := f(P_2)$, ... Όντας η $f : \mathcal{E} \longrightarrow \mathcal{E}$ συνάρτηση, εάν $P_\lambda = P_\rho$, για κάποια $\lambda, \rho \in \mathbb{N}$, με $\rho > \lambda$, τότε ο περίπατος χωρίζεται σε δύο μέρη:

- στη διαδρομή $P_0, P_1, \ldots, P_\lambda$ και
- στον κύκλο $P_\lambda, P_{\lambda+1}, \ldots, P_{\rho-1}, P_\rho = P_\lambda$.

Στο παραπάνω γεγονός οφείλει το όνομά της η μέθοδος ρ του Pollard, ο οποίος για να επιλύσει το ECDLP ακολουθεί την εξής μεθοδολογία:

1: Διαμέριση των σημείων της $\mathcal{E}(GF(p))$ στα $S_1, S_2, S_3 \subseteq \mathcal{E}$, ώστε $\mathbf{O}_\infty \notin S_2$.

2: $R_0 \leftarrow P$; $\quad a_0 \leftarrow 1$; $\quad b_0 \leftarrow 0$;.

3: Για κάθε $i = 0, 1, 2, \ldots$ όρισε $R_i = (a_i \boxdot P) \boxplus (b_i \boxdot Q)$ όπου

$$a_{i+1} = \begin{cases} a_i, & \text{εάν } R_i \in S_1 \\ 2a_i \pmod{\#\mathcal{E}}, & \text{εάν } R_i \in S_2 \\ a_i + 1, & \text{εάν } R_i \in S_3 \end{cases} \quad b_{i+1} = \begin{cases} b_i + 1, & \text{εάν } R_i \in S_1 \\ 2b_i \pmod{\#\mathcal{E}}, & \text{εάν } R_i \in S_2 \\ b_i, & \text{εάν } R_i \in S_3 \end{cases} \tag{3.6}$$

4: Επανάλαβε τα παραπάνω βήματα έως ότου βρεθεί $m \in \mathbb{N}$ με $R_m = R_{2m}$.

5: Όντας $(a_m \boxdot P) \boxplus (b_m \boxdot Q) = R_m = R_{2m} = (a_{2m} \boxdot P) \boxplus (b_{2m} \boxdot Q)$, τότε είναι $Q = k \boxdot P$, όπου $k = \dfrac{a_{2m} - a_m}{b_m - b_{2m}} \pmod{\#\mathcal{E}}$.

Ο αλγόριθμος ακολουθεί τον τυχαίο περίπατο:

$$f : \mathcal{E} \longrightarrow \mathcal{E} \qquad R_i = f(R_i) := \begin{cases} Q \boxplus R_i, & \text{εάν } R_i \in S_1 \\ 2 \boxdot R_i, & \text{εάν } R_i \in S_2 \\ P \boxplus R_i, & \text{εάν } R_i \in S_3 \end{cases}$$

και επιλύει το πρόβλημα ECDLP σε $\mathcal{O}(\sqrt{\#\mathcal{E}})$ πράξεις ελλειπτικών καμπυλών.

Παράδειγμα 3.3.12. Θα εφαρμοσθεί ο αλγόριθμος ρ του Pollard στην ελλειπτική καμπύλη $\mathcal{E}(\mathbb{F}_{47}) : y^2 = x^3 + 34x + 10$, για $P = (30, 26) \in \mathcal{E}$ και $Q = (35, 41) \in \mathcal{E}$.

(α΄) Έστω η διαμέριση των σημείων της $y^2 = x^3 + 34x + 10$:

$$S_1 := \{(x, y) \in \mathcal{E}(\mathbb{F}_{47}) : 0 \leqslant y \lneqq 15\} \quad S_2 := \{(x, y) \in \mathcal{E}(\mathbb{F}_{47}) : 15 \leqslant y \lneqq 30\}$$
$$S_3 := \{(x, y) \in \mathcal{E}(\mathbb{F}_{47}) : 0 \leqslant y \lneqq 15\}$$

με $|S_1| = 13$, $|S_2| = 16$ και $|S_3| = 12$. Άρα, $|S_1| \approx |S_2| \approx |S_3|$ κι άρα αποτελεί αποδεκτή διαμέριση για να εφαρμοσθεί ο αλγόριθμος. Επίσης $\#\mathcal{E} = 41$.

(β′) Τίθενται: $R_0 := P = (30, 26) \in \mathcal{E}(\mathbb{F}_{47})$, $a_0 := 1$ και $b_0 := 0$.

(γ′) Εφαρμόζοντας τους ορισμούς (3.6) υπολογίζονται τα ζεύγη:

$$\begin{aligned}
(R_1, R_2) &= \big((30, 26), (14, 9)\big), & (R_2, R_4) &= \big((14, 9), (28, 42)\big),\\
(R_3, R_6) &= \big((20, 18), (30, 12)\big), & (R_4, R_8) &= \big((28, 42), (30, 21)\big),\\
(R_5, R_{10}) &= \big((6, 17), (30, 21)\big), & (R_6, R_{12}) &= \big((30, 21), (30, 21)\big).
\end{aligned}$$

Βρέθηκε ότι $R_6 = R_{12}$, για $a_6 = 10$, $b_6 = 8$, $a_{12} = 5$ και $b_{12} = 23$.

(δ′) Πλέον, $Q = k \boxdot P$, για $k = \dfrac{a_{12} - a_6}{b_6 - b_{12}} = \dfrac{5 - 10}{8 - 23} = \dfrac{-5}{-15} = 3^{-1} \equiv 14 \pmod{41}$. ⊣

Με χρήση τυχαίων περιπάτων η μέθοδος ελαχίστου βήματος – μεγίστου βήματος επιδέχεται βελτιώσεων όσον αφορά τη χωρική της πολυπλοκότητα: (i) είτε με χρήση των αλγορίθμων ρ και λ του Pollard, (ii) είτε στη μέθοδο εντοπισμού κύκλων του Floyd [όρα [Kn98, σ.4]], (iii) είτε όπως πρότεινε ο D. C. Terr το 2000 στο [Te00].

Η μέθοδος Pohlig και Hellman

Οι Stephen Pohlig και Martin Hellman το 1978 στο [PH78] παρατήρησαν ότι για την επίλυση του ECDLP σε μια ελλειπτική καμπύλη $\mathcal{E}$ με $\#\mathcal{E} = \prod_{i=1}^{s} p_i^{e_i}$ (η ανάλυση σε πρώτους παράγοντες της $\#\mathcal{E} \in \mathbb{N}$), αρκεί να επιλυθεί το ECDLP σε ελλειπτικές καμπύλες με τάξη $p_i \in \mathbb{N}$, για κάθε $i = 1, 2, \ldots, s$.

Έστω η ελλειπτική καμπύλη $\mathcal{E}(\mathrm{GF}(p))$, για κάποιον πρώτο αριθμό $p \in \mathbb{N}$. Εάν $Q = k \boxdot P$, για $n = \mathrm{ord}(P)$, $k \in \mathbb{Z}_n$ και $P, Q \in \mathcal{E}$, τότε επιλύοντας το πρόβλημα DLP για την $\mathcal{E}(\mathrm{GF}(p_i^{e_i}))$, για κάθε $i = 1, 2, \ldots, s$, θα προκύψουν $k_1, \ldots, k_s \in \mathbb{Z}$, με $(\forall i = 1, 2, \ldots, s)\big[k_i \equiv k \pmod{p_i^{e_i}}\big]$. Το Κινέζικο Θεώρημα Υπολοίπων διασφαλίζει την ύπαρξη μοναδικής λύσης $k \in \mathbb{Z}$ για το σύστημα

$$k \equiv k_1 \pmod{p_1^{e_1}}, \qquad k \equiv k_2 \pmod{p_2^{e_2}}, \qquad \ldots, \qquad k \equiv k_s \pmod{p_s^{e_s}}$$

που είναι και το ζητούμενο.

Πολυπλοκότητα της μεθόδου: Εάν $\#\mathcal{E} = \prod_{i=1}^{s} m_i^{k_i}$, τότε η μέθοδος χρειάζεται

$$\mathcal{O}\left(\sum_{i=1}^{s} e_i\big(\log n + \sqrt{p_i}\big)\right)$$

πράξεις ελλειπτικών καμπυλών, σύμφωνα με το [Mo06]. ⊣

Πρότυπα για την επιλογή της ελλειπτικής καμπύλης

Για την αποφυγή των παραπάνω επιθέσεων υπάρχουν κάποια πρότυπα στην επιλογή της ελλειπτικής καμπύλης στα πρωτόκολλα της §3.3.2:

Ορισμός 3.3.13. Η τάξη $\#\mathcal{E}$ μιας ελλειπτικής καμπύλης $\mathcal{E}$ υπεράνω ενός σώματος $\mathrm{GF}(p)$, για κάποιον πρώτο αριθμό $p \in \mathbb{N}$, καλείται **κατάλληλη** (suitable) εάν

1. Η $\#\mathcal{E}$ περιέχει πρώτο παράγοντα έναν μεγάλο (συνήθως μεγαλύτερο του 2^{160}) πρώτο αριθμό.
2. $m \neq p$.
3. $\big(\forall k \in \{1, 2, \ldots, 20\}\big)\big[p^k \equiv 1 \pmod{\#\mathcal{E}}\big]$.

Στον Ορισμό 3.3.13: η πρώτη συνθήκη θωρακίζει τον αλγόριθμο από την επίθεση Pohlig-Hellman, η δεύτερη καθιστά αναποτελεσματικές τις επιθέσεις σε μη-ομαλές καμπύλες και η τρίτη διασφαλίζει την προστασία απέναντι των επιθέσεων MOV. Η ισχύουσα υπολογιστική ικανότητα απαιτεί χρήση κλειδιών τουλάχιστον 160 δυφίων και προς τούτο ο περιορισμός στην πρώτη συνθήκη.

3.3.4 Βελτιώσεις

3.3.4.Α΄ Συμπίεση σημείων ελλειπτικής καμπύλης

Η μετάδοση ενός σημείου $P = (x, y)$ μιας ελλειπτικής καμπύλης $\mathcal{E}(\mathbb{K})$ χρειάζεται $\lceil \log_2 x \rceil + \lceil \log_2 y \rceil \in \mathbb{N}$ δυφία (όσα χρειάζεται η αναπαράσταση των $x, y \in \mathbb{K}$). Συμπιέζοντας το σημείο κατάλληλα θα χρειάζεται μόνον $\lceil \log_2 x \rceil + 1$ δυφία.

Περίπτωση $\mathrm{GF}(p)$, **με** $p \geqslant 3$

Έστω $p \in \mathbb{N}$ ένας περιττός πρώτος αριθμός. Η ελλειπτική καμπύλη $\mathcal{E}(\mathrm{GF}(p))$ χει βραχεία, κανονική μορφή Weierstrass:

$$\mathcal{E}: \; y^2 = x^3 + ax + b$$

για $a, b \in \mathrm{GF}(p)$. Δεδομένου ενός $x \in \mathrm{GF}(p)$, έπεται ότι ο υπολογισμός της $\sqrt{y}$, μπορεί να δώσει ως αποτέλεσμα είτε το $y \in \mathrm{GF}(p)$, είτε το $-y \in \mathrm{GF}(p)$. Όντας ο $p \in \mathbb{N}$ περιττός (πρώτος) αριθμός προκύπτει πως η μία λύση θα είναι άρτια, ενώ η άλλη περιττή. Συνεπώς:

1: $P_{\mathrm{comp}} := (x,\ y \mod 2)$;

Για την αποσυμπίεση του $P_{comp} = (x, i) \in GF(p) \times \{0, 1\}$: Οι οντότητες συμφωνούν πως εάν $b = 0$, τότε επιλέγεται η άρτια ρίζα του $z \in \mathbb{Z}_p$, αλλιώς επιλέγεται η περιττή ρίζα του $z \in \mathbb{Z}_p$.

1: $z \leftarrow x^3 + ax + b \mod p$;
2: **εάν** $(\left(\frac{z}{p}\right) = -1)$ **τότε**
3: **επίστρεψε** ''αποτυχία''; /* z όχι τετραγωνικό υπόλοιπο modulo p */
4: **αλλιώς**
5: $y \leftarrow z^{1/2} \mod p$; /* Με χρήση του αλγορίθμου Shanks-Tonelli */
6: **εάν** $(y \equiv i \mod 2)$ **τότε**
7: **επίστρεψε** (x, y);
8: **αλλιώς**
9: **επίστρεψε** $(x, p - y)$;
10: **τέλος εάν**
11: **τέλος εάν**

Περίπτωση $GL(2^r)$

Μία ελλειπτική καμπύλη $\mathcal{E}(GF(2^r))$ έχει μακρά, κανονική μορφή Weierstrass:

$$y^2 + xy + x^3 + a_2x^2 + a_6 \tag{3.7}$$

για $a_2, a_6 \in GF(2^r)$ και $a_6 \neq 0$. Οι πράξεις στα σημεία $P = (x_1, y_1) \in \mathcal{E}(GF(2^r))$ και $Q = (x_2, y_2) \in \mathcal{E}(GF(2^r))$ έχουν ως εξής:

- $P \boxplus \mathbf{O}_\infty = P$.
- $\boxminus P = (x, x + y)$.
- Εάν $P, Q \neq \mathbf{O}_\infty$ και $P \neq \boxminus Q$, τότε $P \boxplus Q = (x_3, y_3)$, όπου

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + x_1 + x_2 + a_2 \\ y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 \end{aligned} \qquad \text{για } \lambda = \begin{cases} (y_1 + y_2)/(x_1 + x_2), & \text{εάν } P \neq Q \\ x_1 + y_1/x_1, & \text{εάν } P = Q \end{cases}$$

Για τις αλγοριθμικές κατασκευές υποτίθεται ότι $x \neq 0$, ειδ' άλλως (εάν $x = 0$), τότε $P = \boxminus P$. Θεωρώντας $z := y/x$ στην (3.7), προκύπτει η

$$z^2 + z = x + a_2 + \frac{a_6}{x^2} \tag{3.8}$$

Ορισμός 3.3.14. Η συνάρτηση **ίχνους** $tr : GF(2^r) \to \{0, 1\}$ ορίζεται $tr(\alpha) := \sum_{i=0}^{r-1} \alpha^{2^i}$.

Οι δύο λύσεις της εξίσωσης (3.8) έχουν ίχνος 0 η μία και 1 η άλλη. Συνεπώς:

1: $P_{bin\_comp} := (x, tr(y/x))$;

Η αποσυμπίεση του σημείου $P_{\text{bin\_comp}}(x, i) \in GF(2^r) \times \{0, 1\}$ έχει ως εξής:

1: $(z_1, z_2) \leftarrow$ **επίλυση**"$z^2 + z = x + a_2$";
2: **εάν** $(\text{tr}(z_1) = i)$ **τότε**
3: **επίστρεψε** (x, xz_1);
4: **αλλιώς**
5: **επίστρεψε** (x, xz_2);
6: **τέλος εάν**

3.3.4.Β΄ Αποδοτικότερες υλοποιήσεις πράξεων σε ελλειπτικές καμπύλες

Χρήση προβολικών συντεταγμένων

Γενικεύοντας τη σχέση (3.3) στο τυχαίο σώμα $\mathbb{K}$, προκύπτει η εξής σχέση ισοδυναμίας υπεράνω του συνόλου $\mathbb{K}^3 \setminus \{(0_\mathbb{K}, 0_\mathbb{K}, 0_\mathbb{K})\}$:

$$(X, Y, Z) \sim (A, B, C) \Longleftrightarrow_{o\rho} (\exists \lambda \in \mathbb{K})(\exists c, d, e \in \mathbb{Z})[X = \lambda^c A \wedge Y = \lambda^d B \wedge Z = \lambda^e C]$$

Οι κλάσεις ισοδυναμίας $[\![(X, Y, Z)]\!]_\sim$, $X, Y, Z \in \mathbb{K}$, συνθέτουν το προβολικό επίπεδο $\mathbb{P} = \{[\![(X, Y, Z)]\!]_\sim \subseteq \mathbb{K}^3\} = \{[\![(X, Y, Z)]\!]_\sim \subseteq \mathbb{K}^3 : Z \neq 0_\mathbb{K}\} \cup \{[\![(X, Y, 0)]\!]_\sim \subseteq \mathbb{K}^3\}$. Ο δεύτερος όρος της παραπάνω ένωσης καλείται *ευθεία στο άπειρο*. Ο πρώτος όρος της ένωσης δύναται να ταυτιστεί με το συγγενές επίπεδο (:συγγενής (affine) χώρος διάστασης 2) $A^2_\mathbb{K}$ μέσω του μετασχηματισμού

$$A^2_\mathbb{K} \longrightarrow \mathbb{P} \qquad \{\, x \longmapsto X/Z^c \quad y \longmapsto Y/Z^d \,\}$$

Για $c = d = 1$ προκύπτουν οι *συνήθεις προβολικές συντεταγμένες*. Για $c = 2$ και $d = 1$ προκύπτουν οι Jacobi προβολικές συντεταγμένες, ενώ για $c = 1$ και $d = 2$ προκύπτουν οι Lopez-Dahlab προβολικές συντεταγμένες.

Έστω μια ελλειπτική καμπύλη $\mathcal{E}$ υπεράνω του $GF(p)$, για $\text{char}(GF(p)) > 3$, της οποίας η βραχεία, κανονική μορφή Weierstrass είναι η $y^2 = x^3 + ax + b$, για $a, b \in GF(p)$. Η ελλειπτική καμπύλη $\mathcal{E}$ με χρήση προβολικών συντεταγμένων, έχει ως βραχεία, κανονική μορφή Weierstrass την:

$$\mathcal{E} : Y^2 = \begin{cases} X^3 Z^{2d-3c} + aXZ^{2d-c} + bZ^{2d}, & \text{εάν } 2d > 3c \\ Z^{2d-3c}(X^3 + aXZ^{2c} + bZ^{3c}), & \text{αλλιώς} \end{cases}$$

Για τις τυπικές προβολικές συντεταγμένες είναι $c = d = 1$ κι άρα η $\mathcal{E}$ έχει βραχεία, κανονική μορφή Weierstrass: $Y^2Z = X^3 + aXZ^2 + bZ^3$.

Έστω $(X_1, Y_1, Z_1), (X_2, Y_2, Z_2) \in \mathbb{P}$, τότε

- $(X_1, Y_1, Z_1) \boxplus (X_2, Y_2, Z_2) = \big(VT,\ U(V^2V_2 - T) - V^3U_2,\ V^3W\big)$, με $U := Y_2Z_1 - Y_1Z_2$, $V := X_2Z_1 - X_1Z_2$, $W := Z_1Z_2$ και $T := U^2W - V^3 - 2V^2X_1Z_2$.
- $2 \boxdot (X, Y, Z) := \big(2HS,\ W(4T - H) - 8Y^2S^2,\ 8S^3\big)$, όπου $W := aZ^2 + 3X^2$, $S := YZ$, $T := XYS$ και $H := W^2 + 8B$.

Βαθμωτός πολλαπλασιασμός

Μία μέθοδος η οποία χρησιμοποιεί λιγότερες πράξεις υπεράνω ελλειπτικών καμπυλών είναι η *μέθοδος (σταθερό/μεταβλητού) παραθύρου* [HMV04]. Η βασική ιδέα της μεθόδου μεταβλητού παραθύρου έχει ως εξής:

1. Ο αλγόριθμος δέχεται ως είσοδο το βαθμωτό μέγεθος $d \in \mathbb{N}$, το σημείο $P \in \mathcal{E}(GF(p))$ και το μέγιστο μέγεθος που δύναται να φθάσει το παράθυρο $w \in \mathbb{N}$ [για τις καμπύλες NIST‖ (:καμπύλες $\mathcal{E}(\mathbb{F}_p)$ για κάποιον ψευδοπρώτο του Mersenne $p \in \mathbb{N}$, όπως $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ ή $p = 2^{521} - 1$) αρκεί $w = 4$].
2. Υπολογίζονται τα σημεία $P_d := d \boxdot P$, για $i = 1, 3, 5, 7, 9, \ldots, 2^w - 1$.
3. Σε κάθε επανάληψη ο αλγόριθμος επεξεργάζεται τμήματα της μορφής $100\ldots001$ (:παράθυρο) της δυαδικής αναπαράστασης του βαθμωτού $k \in \mathbb{N}$.
   - Εάν $k = 25_{10} = 11001_2$, τότε ο αλγόριθμος θα πραγματευθεί τα τμήματα (παράθυρα) 1 (μεγέθους 1) και 1001 (μεγέθους 4), υπό την προϋπόθεση ότι έχει τεθεί $w \geqslant 4$.
   - Η ανίχνευση των παραθύρων ξεκινάει από τα δυφία που αντιστοιχούν σε μεγαλύτερες δυνάμεις του 2.

Η μέθοδος σταθερού παραθύρου επεξεργάζεται τμήματα σταθερού μήκους της δυαδικής αναπαράστασης του $k \in \mathbb{N}$. Υστερεί, ωστόσο, σε ταχύτητα από τη μέθοδο μεταβλητού παραθύρου.

3.3.4.Γ′ Περιπτώσεις υλοποίησης πρωτοκόλλων ελλειπτικών καμπυλών

Στις υλοποιήσεις θεωρούνται προβολικές συντεταγμένες.

Περίπτωση 1: Χρησιμοποιείται συνδυασμός της μεθόδου Double And Add Always [Αλγόριθμος 3.3.8] και τύφλωσης βαθμωτού [scalar blinding - όρα §Α′.2].
Ο χρόνος παραγωγής της υπογραφής αυξάνεται, λόγῳ των ψεύτικων πράξεων που χρησιμοποιεί η μέθοδος Double And Add Always. Η υλοποίηση είναι ανθεκτική έναντι σε απλές παράπλευρες επιθέσεις. Ωστόσο, είναι τρωτή έναντι στις doubling attacks [FV03].

Περίπτωση 2: Χρησιμοποιείται συνδυασμός της μεθόδου Double And Add Always [Αλγόριθμος 3.3.8] και της μεθόδου μεταβλητού παραθύρου [Αλγόριθμος ;;]. Το μυστικό βαθμωτό τυφλώνεται [scalar blinding - όρα §Α′.2] στους υπολογισμούς που συμμετέχει.
Η εν λόγῳ υλοποίηση είναι ανθεκτική έναντι σε απλή/διαφορική ανάλυση ισχύος. Στη μέθοδο παραθύρου, κάθε παράθυρο (εάν επιλεγεί μεγέθους

‖ National Institue of Standards and Technology

4 δυφίων) έχει 16 επιλογές (δύο για κάθε δυφίο του) ή σε δεκαδική αναπαράσταση το παράθυρο αναπαριστάει έναν αριθμό από το 0 έως το 15. Για να μην ξεχωρίζει ο πολλαπλασιασμός με το 0, υπεισέρχεται η μέθοδος Double And Add Always στην μέθοδο μεταβλητού παραθύρου.

Περίπτωση 3: Χρήση της μεθόδου Montgomery Ladder [Αλγόριθμος Α΄.1.1] και της μεθόδου τυχαίας τύφλωσης του βαθμωτού [random scalar blinding - όρα §Α΄.2].
Δεν χρησιμοποιούνται ψεύτικες πράξεις. Η τύφλωση του βαθμωτού έχει ως εξής: Επιλέγεται τυχαίο $s \in \mathbb{N}$ και υπολογίζονται τα $s \boxdot P$ και $(k - s) \boxdot P$. Επιστρέφεται το $Q = (s \boxdot P) \boxminus ((s - k) \boxdot P) = k \boxdot P$.
Αποτελεί αρκετά κοστοβόρα υλοποίηση, όμως είναι η ασφαλέστερη. Ο διαχωρισμός του βαθμωτού διπλασιάζει τον χρόνο υπολογισμού, αλλά είναι ασφαλής τακτική έναντι σε επιθέσεις διαφορικής ανάλυσης ισχύος. Η Montgomery Ladder καθιστά την υλοποίηση ασφαλή έναντι σε επιθέσεις απλής ανάλυσης ισχύος, μιας και κάθε δυφίου του βαθμωτού μεταχειρίζεται το ίδιο· επίσης είναι ασφαλής έναντι στη C-Safe error επίθεση.

3.3.5 Σύνοψη

Οι ελλειπτικές καμπύλες χρήζουν αντικείμενο μελέτης της Θεωρίας Αριθμών και της Αλγεβρικής Γεωμετρίας για πάνω από δύο αιώνες. Καταστάλαγμα αυτού του ενδιαφέροντος είναι η παραγωγή αρκετών αποτελεσμάτων γύρω από τη Θεωρία των Ελλειπτικών Καμπυλών. Ωστόσο, τα τελευταία είκοσι χρόνια οι ελλειπτικές καμπύλες βρίσκουν και εφαρμογή στην Κρυπτογραφία. Αυτό συμβαίνει καθ΄ όσον μπορούν να αναπαραστήσουν τα σημεία του $\mathbb{Z}_p$ –για κάποιον πρώτο αριθμό $p \in \mathbb{N}$– με πολύ μεγάλη επιτυχία αφού:

- Παράγουν εύκολα κυκλικές ομάδες.
- Το ανάλογο του προβλήματος του διακριτού λογαρίθμου αποτελεί ένα υπολογιστικά δύσκολο πρόβλημα.

Συνέπεια των παραπάνω είναι η χρήση λιγότερων δυφίων στα κλειδιά των πρωτοκόλλων. Παρ΄ όλο που το μαθηματικό υπόβαθρο για τη μελέτη των ελλειπτικών καμπυλών είναι υψηλό, η κατανόησή τους μπορεί να επιτευχθεί παραλείποντας τις ‘‘δύσβατες’’ λεπτομέρειες των σχετικών αποτελεσμάτων.

Όλες οι βελτιώσεις της §3.3.4 οδηγούν στη δέσμευση λίγων υπολογιστικών πόρων στην υλοποίηση των κρυπτογραφικών σχημάτων υπεράνω των ελλειπτικών καμπυλών. Οι υπολογισμοί καθώς και το μέγεθος των πληροφοριών που συμμετέχουν στα πρωτόκολλα μειώνεται καθιστώντας τις εν λόγω υλοποιήσει αποδοτικότερες σε σχέση με τις παραδοσιακές πράξεις σε μεγάλους αριθμούς.

Κεφάλαιο 4

Σχήματα Υπογραφών

Μια ψηφιακή υπογραφή αποτελεί την βασική κρυπτογραφική αρχή η οποία δημιουργήθηκε ως ισοδύναμο στο ψηφιακό κόσμο της χειρόγραφης υπογραφής.

Ορισμός 4.0.1. Ένα **σχήμα ψηφιακών υπογραφών** (ή απλούστερα *σχήμα υπογραφών*) αποτελείται από μία τριάδα αλγορίθμων $\langle \textsc{Gen}, \textsc{Sign}, \textsc{Verify} \rangle$, όπου:

Ο αλγόριθμος κλειδιού Gen: δέχεται ως είσοδο μία παράμετρο ασφαλείας και παράγει ως έξοδο ένα ζεύγος $(\mathrm{vk}, \mathrm{sk})$. Το vk καλείται **κλειδί επαλήθευσης** ή *δημόσιο κλειδί* και το sk **κλειδί υπογραφής** ή *μυστικό κλειδί*.

Ο αλγόριθμος υπογραφής Sign: δέχεται ως είσοδο μία παράμετρο ασφαλείας, το κλειδί υπογραφής sk και ένα μήνυμα M και παράγει ως έξοδο την υπογραφή σ.

Ο αλγόριθμος επαλήθευσης Verify: δέχεται ως είσοδο το κλειδί επαλήθευσης vk, μία υπογραφή σ κι ένα μήνυμα M. Ο αλγόριθμος επιστρέφει 1 ή 0 αντιστοίχως εάν η υπογραφή σ είναι έγκυρη ή όχι.

Με άλλα λόγια, κάθε οντότητα κατέχει μία μυστική πληροφορία, την sk, με την οποία υπογράφει *μοναδικά* κάθε μήνυμα M (παράγοντας την υπογραφή σ), καθώς και μία δημοσίως γνωστή πληροφορία vk. Κάθε συνδιαλεγόμενο μέλος μπορεί να επαληθεύσει την υπογραφή με τη χρήση του vk. Μόνον κάποιος γνώστης της πληροφορίας sk μπορεί να υπογράψει το μήνυμα, ωστόσο κάθε ενδιαφερόμενος μπορεί να επαληθεύσει το γνήσιο της υπογραφής χρησιμοποιώντας την (δημοσίως γνωστή) πληροφορία vk.

Οι αλγόριθμοι Gen και Sign είναι πιθανοκρατικοί (διενεργούν τυχαίες επιλογές) αλγόριθμοι πολυωνυμικού χρόνου, ενώ ο αλγόριθμος Verify είναι αιτιοκρατικός (ντετερμινιστικός) αλγόριθμος πολυωνυμικού χρόνου.

Σε ένα σχήμα ψηφιακών υπογραφών, ένας **πλαστογράφος ψηφιακών υπογραφών** (digital signature forgery) είναι ένας αντίπαλος ο οποίος, δίχως να ξέρει το κλειδί υπογραφής sk, μπορεί και δημιουργεί μία έγκυρη υπογραφή σ για ένα μήνυμα m, ήτοι $\textsc{Verify}(\mathrm{vk}, (\mathrm{m}, \sigma)) = 1$, το οποίο μήνυμα δεν έχει υπογραφεί πρότερα από τον αλγόριθμο $\textsc{Sign}(\mathrm{sk}, \mathrm{m})$. Αναλόγως της δυναμικής διακρίνονται:

Υπαρξιακός πλαστογράφος (existential forgery): Ο αντίπαλος δημιουργεί τουλάχιστον ένα ζεύγος μηνύματος-υπογραφής (m, σ), δίχως η σ να έχει παραχθεί πρότινως από τον αλγόριθμο $\textsc{Sign}(\mathrm{sk}, \mathrm{m})$. Δεν γίνεται μνεία για το νόημα του μηνύματος m· μπορεί να μην έχει νόημα, ο στόχος είναι να ικανοποιείται το γεγονός ότι $\textsc{Verify}(\mathrm{vk}, (\mathrm{m}, \sigma)) = 1$.
[Όρα Παράδειγμα 4.2.1 και για την αντιμετώπισή του όρα την §4.2.1.]

Επιλεκτικός πλαστογράφος (selective forgery): Ο αντίπαλος εργάζεται ώστε να παράξει έγκυρη υπογραφή σ για ένα δεδομένο μήνυμα m. Το μήνυμα είναι προκαθορισμένο εξ αρχής και ενδέχεται να πληροί κάποιες μαθηματικές ιδιότητες που αφορούν τον αλγόριθμο υπογραφής.

Καθολικός πλαστογράφος (universal forgery): Ο αντίπαλος είναι σε θέση να δημιουργεί έγκυρες υπογραφές σ, για *οποιοδήποτε* μήνυμα m. Τα μηνύματα τυγχάνουν της επιλογής του αντιπάλου, μπορεί να είναι τυχαία επιλεγμένα ή να έχουν τεθεί ως πρόκληση (σε κάποιο παίγνιο ασφαλείας).

Ορισμός 4.0.2. Το **άστρο Kleene** του συνόλου $\mathrm{X} \neq \varnothing$ ορίζεται ως $\mathrm{X}^\star := \bigcup_{\mathrm{n} \in \mathbb{N}_0} \mathrm{V}_\mathrm{n}$, όπου $\mathrm{V}_0 := \{\varepsilon\}$, $\mathrm{V}_1 := \mathrm{X} \cup \{\varepsilon\}, \ldots, \mathrm{V}_{\mathrm{n}+1} := \big\{(w, \mathrm{x}) : w \in \mathrm{X}_\mathrm{n} \wedge \mathrm{x} \in \mathrm{X}\big\}$, … και ε είναι το *μοναδικό* στοιχείο του $\mathrm{X}^\star$ το οποίο δεν περιέχει σύμβολα (στοιχεία του X) και προς τούτο καλείται **κενή ακολουθία**.

4.1 Η απαρχή όλων: η ιδέα του Shamir

Έστω S το αλφάβητο του μηνύματος. Το σχήμα υπογραφών που προτάθηκε από τον Adi Shamir το 1978 στο [Sh78] έγκειται στην επαλήθευση της ισοτιμίας:

$$\mathrm{s}^e \equiv \mathrm{i} \cdot \mathrm{t}^{\mathrm{f}(\mathrm{t},\mathrm{m})} \pmod{\mathrm{n}} \tag{4.1}$$

όπου παραπάνω:

- το $\mathrm{m} \in \mathrm{S}^\star$ είναι το μήνυμα προς υπογραφή,
- το $(\mathrm{s}, \mathrm{t}) \in \mathbb{Z}_\mathrm{n} \times \mathbb{Z}_\mathrm{n}$ είναι η υπογραφή,
- ο $\mathrm{i} \in \mathbb{N}$ προκύπτει (εφαρμόζοντας μια μονόδρομη συνάρτηση) από το αλφαριθμητικό που καθορίζεται από τα στοιχεία του χρήστη,
- ο $\mathrm{n} \in \mathbb{N}$ είναι το γινόμενο δύο μεγάλων πρώτων αριθμών,
- ο $e \in \mathbb{N}$ είναι ένας μεγάλος πρώτος αριθμός, ώστε $\mu\kappa\delta\big(e, \varphi(\mathrm{n})\big) = 1$ και
- η συνάρτηση $\mathrm{f} : \mathbb{Z}_\mathrm{n} \times \mathrm{S}^\star \longrightarrow \mathbb{N}$ είναι μία μονόδρομη συνάρτηση.

Η ευθύνη του κέντρου: Το κέντρο φροντίζει να προμηθεύει τους χρήστες του με έξυπνες κάρτες οι οποίες περιέχουν:

- την ισοτιμία $n \in \mathbb{N}$,
- το $e \in \mathbb{N}$ (ο εκθέτης κρυπτογράφησης),
- μία αλγοριθμική υλοποίηση της συνάρτησης $f : \mathbb{Z}_n \times S^\star \longrightarrow \mathbb{N}$ και
- το $i \in \mathbb{N}$ (διαφορετικό σε κάθε χρήστη) από το οποίο συνάγεται το μυστικό κλειδί του κατόχου της, $g \in \mathbb{N}$, όπου $g^e \equiv i \pmod n$.

Η ασφάλεια του σχήματος στηρίζεται στην

Υπόθεση RSA: Για $n \in \mathcal{R}$, $x \in \mathbb{Z}_n$ και $e \in \mathbb{Z}^*_{\varphi(n)}$ είναι υπολογιστικά δύσκολο να αντιστραφεί η συνάρτηση $E(x) := x^e \pmod n$.

Ο αλγόριθμος κλειδιού Shamir_Gen(i) υπολογίζει το $g \in \mathbb{N}$, ώστε $g^e \equiv i \pmod n$ (ένας υπολογισμός που απαιτεί τη γνώση της παραγοντοποίησης του $n \in \mathbb{N}$, γνώση που μόνον το κέντρο κατέχει).

Ο αλγόριθμος επαλήθευσης Shamir_Verify$(i, (s,t), m)$ επαληθεύει την ισοτιμία (4.1). Εν περιπτώσει όπου η $(s,t) \in \mathbb{Z}_n \times \mathbb{Z}_n$ είναι μία έγκυρη υπογραφή (ήτοι έχει παραχθεί από τον αλγόριθμο 4.1.1) ο υπολογισμός δίδει:

$$s^e \pmod n = \left(g \cdot r^{f(t,m)}\right)^e \pmod n = g^e \cdot r^{e \cdot f(t,m)} \pmod n =$$
$$= g^e \cdot \left(r^e\right)^{f(t,m)} \pmod n = i \cdot t^{f(t,m)} \pmod n$$

Τέλος, ο αλγόριθμος Shamir_Sign(g,m) δημιουργεί μία υπογραφή η οποία αφού επαληθεύει την ισοτιμία (4.1), πείθει τον επιβεβαιωτή πως ο αποδεικνύων πράγματι κατέχει τη γνώση της μυστικής πληροφορίας $g \in \mathbb{N}$.

Αλγόριθμος 4.1.1 Shamir_Sign(g,m): Δημιουργία υπογραφής Shamir.

Δεδομένα: Ισοτιμία $n \in \mathbb{N}$, εκθέτης κρυπτογράφησης $e \in \mathbb{N}$, μονόδρομη συνάρτηση $f : \mathbb{Z}_n \times S^\star \to \mathbb{N}$.
Είσοδος: Η μυστική πληροφορία $g \in \mathbb{N}$ και το μήνυμα προς υπογραφή $m \in S^\star$.
΄Εξοδος: Υπογραφή $(s,t) \in \mathbb{Z}_n \times \mathbb{Z}_n$ για το μήνυμα $m \in S^\star$.

1: $r \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathbb{N}$;
2: $t \leftarrow r^e \mod n$;
3: $s \leftarrow g \cdot r^{f(t,m)} \mod n$; /* $\text{μκδ}\left(e, \varphi(n)\right) = 1$ */
4: **επίστρεψε** (s,t);

Σχόλια για τον αλγόριθμο 4.1.1:

1. Η συνθήκη $\mu\kappa\delta\big(e, \varphi(n)\big) = 1$ διασφαλίζει την ύπαρξη των $g, s \in \mathbb{N}$ ως e-οστών ριζών των $i, s^e \in \mathbb{N}$ αντιστοίχως.

2. Η πληροφορία $g \in \mathbb{N}$ αποκρύπτεται χάριν στη τυχαιότητα του $r \in \mathbb{N}$ (άρα δεν θα πρέπει να επαναχρησιμοποιείται ή να αποκαλύπτεται).

Παρατήρηση 4.1.2 (Σημειώσεις ασφάλειας υπογραφής Shamir).

(α) Κάθε μήνυμα $m \in S^\star$ ενδέχεται να έχει πληθώρα δυνατόν υπογραφών $(s, t) \in \mathbb{N} \times \mathbb{N}$. Ωστόσο, η πυκνότητά τους είναι τόσο μικρή που μία τυχαία αναζήτηση καταλήγει αδύνατη.

(β) Σταθεροποιώντας είτε το $s \in \mathbb{N}$, είτε το $t \in \mathbb{N}$, η εύρεση της μιας έγκυρης υπογραφής $(s, t) \in \mathbb{N} \times \mathbb{N}$ ανάγεται στο πρόβλημα εξαγωγής e-οστών ριζών.

(γ) Εάν οποιαδήποτε από τις δύο εμφανίσεις του $t \in \mathbb{N}$ στην ισοτιμία (4.1) απαλλοιφεί (επί παραδείγματι αντικατασταθεί με μία σταθερά), τότε η ασφάλεια του συστήματος εξασθενεί.

(δ) Εάν $\mu\kappa\delta\big(f(t, m), e\big) = c \gneqq 1$, τότε υπάρχει δυνατότητα να εξαχθούν c-οστές ρίζες του $i \in \mathbb{N}$, μέσῳ της εξίσωσης (4.1). Συνεπώς,

- *ο $e \in \mathbb{N}$ πρέπει να επιλεγεί αρκετά μεγάλος πρώτος αριθμός και*
- *η $f : \mathbb{Z}_n \times S^\star \longrightarrow \mathbb{N}$ επαρκώς ισχυρή μονόδρομη συνάρτηση*

ώστε να αποφευχθεί περίπτωση ανωτέρω.

Σύνοψη

Το σχήμα στην ουσία είναι ένα κρυπτοσύστημα ασύμμετρου κλειδιού. Η διαφορά έγκειται στο ότι αντί να παράγονται τυχαία τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης, ο χρήστης επιλέγει ως κλειδί κρυπτογράφησης (δημόσιο κλειδί), ένα αλφαριθμητικό το οποίο τον καθορίζει μοναδικά.

Με χρήση της ορολογίας του Ορισμού 4.0.1 είναι κανένας από τους άνωθεν αλγορίθμους δεν χρησιμοποιεί κάποια παράμετρο ασφαλείας, $vk := i$, $sk := g$ (όπου $g^e \equiv i \mod n$) και $\sigma := (s, t)$.

4.2 Υπογραφές RSA

Έστω $\mathcal{E}_K(m)$ και $\mathcal{D}_K(c)$ η συνάρτηση κρυπτογράφησης/αποκρυπτογράφησης αντίστοιχα, όπου K είναι το ζεύγος δημοσίου-ιδιωτικού κλειδιού, $m \in \mathscr{M}$ και $c \in \mathscr{C}$, για $\mathscr{M}$ τον χώρο των απλών κειμένων και $\mathscr{C}$ τον χώρο των κρυπτοκειμένων. Η ορθότητα κάθε κρυπτοσυστήματος) υπαγορεύει:

$$(\forall m \in \mathscr{M})\big[\mathcal{D}_K(\mathcal{E}_K(m)) = m\big]$$

Εάν δε, ισχύει και ότι $\mathscr{M} = \mathscr{C}$, τότε ισχύει και η σχέση

$$(\forall m \in \mathscr{M})\big[\mathcal{E}_K(\mathcal{D}(m)) = m\big]$$

Το κρυπτοσύστημα RSA [Σχήμα 3.1] εμπίπτει στην ως άνω οριζομένη περίπτωση, αφού $\mathscr{M} = \mathscr{C} = \mathbb{Z}_n$. *Αντιστρέφοντας το ρόλο του ιδιωτικού με αυτόν του δημοσίου κλειδιού προκύπτει το* ***σχήμα υπογραφών RSA.***

Ο αλγόριθμος RSA_Gen(p, q) είναι ακριβώς ο αλγόριθμος παραγωγής κλειδιών του κρυπτοσυστήματος RSA: Δέχεται δύο πρώτους αριθμούς $p, q \in \mathbb{N}$ και υπολογίζει τις ποσότητες $n = pq \in \mathcal{R}$ και $\varphi(n) \in \mathbb{N}$. Κατ' όπιν επιστρέφει το ιδιωτικό κλειδί $(p, q, d) \in \mathbb{N}^2 \times \mathbb{Z}_n^*$ και το δημόσιο κλειδί $(n, e) \in \mathcal{R} \times \mathbb{Z}_n^*$, τα οποία πληρούν τα εξής: $\mu\kappa\delta(e, \varphi(n)) = 1$ και $de \equiv 1 \pmod{\varphi(n)}$.

Ο αλγόριθμος RSA_Sign$((p, q, d), m)$ δέχεται ως είσοδό του το ιδιωτικό κλειδί $(p, q, d) \in \mathbb{N}^2 \times \mathbb{Z}_n^*$ και το μήνυμα προς υπογραφή $m \in \mathbb{Z}_n$ κι έχει ως έξοδό του το $c := m^d \pmod{n}$.

Ο αλγόριθμος RSA_Verify$((n, e), c, m)$ έχει ως είσοδό του το δημόσιο κλειδί $(n, e) \in \mathcal{R} \times \mathbb{Z}_n^*$, ένα κρυπτοκείμενο $c \in \mathbb{Z}_n$ και το μήνυμα προς επαλήθευση $m \in \mathbb{Z}_n$. Αποδέχεται την υπογραφή $c \in \mathbb{Z}_n$ εάν $m \equiv c^d \pmod{n}$.

Η υπογραφή RSA είναι πολύ εύκολο να παραχθεί (αφού απαιτείται μια μικρή τροποποίηση του κρυπτοσυστήματος RSA) και συνάμα πολύ εύκολο να να πλαστογραφηθεί. Έπονται δύο επιθέσεις που επιτυγχάνουν στην υπογραφή RSA:

Επίθεση χωρίς μήνυμα (no message attack): Έστω $\sigma \in \mathbb{Z}_n$ η υπογραφή και αναζητείται μήνυμα $m \in \mathbb{Z}_n$ το οποίο να έχει ως έγκυρη υπογραφή του την $\sigma \in \mathbb{Z}_n$. Γνωρίζοντας το δημόσιο κλειδί $(n, e) \in R \times \mathbb{Z}_n^*$, είναι δυνατόν να υπολογισθεί η ποσότητα $m := \sigma^e \pmod{n}$. Πλέον, η υπογραφή $\sigma \in \mathbb{Z}_n$ αποτελεί έγκυρη (αλλά πλαστογραφημένη) υπογραφή για το μήνυμα $m \in \mathbb{Z}_n$, καθ' ότι $m^d = (\sigma^e)^d = \sigma^{ed} \equiv \sigma \pmod{\varphi(n)}$. Η επίθεση έχει νόημα καθώς ήθισται το μήνυμα προς επαλήθευση $m \in \mathbb{Z}_n$ να μην έχει κάποιο νόημα (ενδέχεται να είναι το κλειδί κάποιου συμμετρικού κρυπτοσυστήματος).

Επίθεση επιλεγμένου απλού κειμένου (chosen plaintext attack): Όντας το κρυπτοσύστημα RSA ελατό* εάν $s_1, s_2 \in \mathbb{Z}_n$ είναι δύο έγκυρες υπογραφές για

*... αφού πληροί την ομομορφική ιδιότητα: $(\forall m_1, m_2 \in \mathscr{M})\big[\mathcal{E}_K(m_1 \cdot m_2) = \mathcal{E}(m_1) * \mathcal{E}(m_2)\big]$.

τα μηνύματα $m_1, m_2 \in \mathbb{Z}_n$ αντίστοιχα, τότε η υπογραφή $s_1 s_2 \pmod n$ αποτελεί έγκυρη υπογραφή για το μήνυμα $m_1 m_2 \pmod n$.

Παράδειγμα 4.2.1. Έστω $p = 3$, $q = 11$ ($\Longrightarrow n = 3 \cdot 11 = 33$ και $\varphi(33) = 20$), $e = 3$, $d = 7$ και οι διαθέσιμες υπογραφές $(m_1, s_1) = (4, 16)$ και $(m_2, s_2) = (6, 30)$.

Για το μήνυμα

$$m' = m_1 m_2 \pmod n = 4 \cdot 6 \pmod{33} = 24$$

υπολογίζεται

$$s' = s_1 s_2 \pmod n = 16 \cdot 30 \pmod{33} = 18$$

Η $s' = 18$ αποτελεί έγκυρη υπογραφή για το μήνυμα $m' = 24$ καθ' όσον $(m')^d = 24^7 = 4586471424 \equiv 18 \pmod{33}$. ⊣

Για την αντιμετώπιση των παραπάνω επιθέσεων έχουν προταθεί πληθώρα μέτρων. Ένα από αυτά είναι η ακόλουθη έννοια:

Ορισμός 4.2.2. Μία **συνάρτηση πλεονάζουσας πληροφορίας** (redundancy function) είναι μία δημοσίως γνωστή, αντιστρέψιμη προβολή από τον χώρο των απλών κειμένων σε έναν υπόχωρο με συγκεκριμένες ιδιότητες.

Παράδειγμα 4.2.3. Μία συνάρτηση πλεονάζουσας πληροφορίας είναι μία συνάρτηση η οποία κάθε 8 δυφία απλού κειμένου παρεμβάλει την ακολουθία 10101. ⊣

4.2.1 RSA-Full Domain Hash

Μία άλλη λύση για την θωράκιση έναντι των επιθέσεων χωρίς μήνυμα και των επιθέσεων επιλεγμένου απλού κειμένου, είναι το σχήμα υπογραφών RSA-FDH (Full Domain Hash) το οποίο επεκτείνει το δημόσιο κλειδί $(n, e) \in \mathcal{R} \times \mathbb{Z}_n^*$ στο $(n, e; \mathcal{H})$, όπου $\mathcal{H} : \{0,1\}^\star \longrightarrow \mathbb{Z}_n^*$ είναι μία συνάρτηση κατακερματισμού. Πλέον, αντί του $m \in \mathbb{Z}_n$, στο σχήμα υπογραφών RSA θα χρησιμοποιείται το $\mathcal{H}(m) \in \mathbb{Z}_n^*$.

Θεωρούνται $n \in \mathcal{R}$ και $e \in \mathbb{Z}_{\varphi(n)}^*$. Έστω $\mathcal{A}$ να είναι ένας αντίπαλος πολυωνυμικού χρόνου ο οποίος -έχοντας πρόσβαση σε ένα τυχαίο μαντείο- μπορεί να πλαστογραφήσει υπογραφές του σχήματος RSA-FDH (με τις παραμέτρους n και e). Χρησιμοποιώντας τον αντίπαλο $\mathcal{A}$ θα κατασκευασθεί ένας αντίπαλος πολυωνυμικού χρόνου $\mathcal{B}$ ο οποίος θα επιλύει το πρόβλημα $\mathtt{RSA}[n, e]$. Συνεπώς,

- Ο $\mathcal{B}$ γνωρίζει: $n \in \mathcal{R}$, $e \in \mathbb{Z}_{\varphi(n)}^*$ και $y \in \mathbb{Z}_n^*$.
- Ο $\mathcal{B}$ αναζητεί: $x \in \mathbb{Z}_n$, τέτοιο ώστε $x^e \equiv y \pmod n$.

Η ακριβής ασφάλεια του σχήματος υπογραφών RSA-FDH

Αποδεικνύεται [BR96, Coo0] ότι εάν υπάρχει αλγόριθμος ο οποίος επιλύει το πρόβλημα $\mathtt{RSA}[n, e]$, $n \in \mathbb{R}$ και $e \in \mathbb{Z}^*_{\varphi(n)}$, σε χρόνο $t' \in \mathbb{N}$, με πιθανότητα $\epsilon' \in [0, 1]$, τότε το σχήμα υπογραφών RSA-FDH μπορεί να παραβιαστεί σε χρόνο

$$t = t' - (q_{\text{hash}} + q_{\text{sig}} + 1) \cdot \mathcal{O}(k^3)$$

με πιθανότητα

$$\epsilon = \left(1 + \frac{1}{q_{\text{sig}} + 1}\right)^{-q_{\text{sig}}-1} \cdot q_{\text{sig}} \cdot \epsilon'$$

όπου $k \in \mathbb{N}$ είναι μία παράμετρος ασφαλείας που αφορά τον αλγόριθμο παραγωγής κλειδιών $\text{RSA\_Gen}(1^k)$ αλγόριθμος έχει υπολογίσει το πολύ q_{hash} τιμές της συνάρτησης κατακερματισμού $\mathcal{H} : \{0,1\}^\star \longrightarrow \mathbb{Z}^*_n$ κι το πολύ q_{sig} υπογραφές του σχήματος RSA-FDH.

Οι Mihil Bellare και Phillip Rogaway το 1996 στο [BR96] πρότειναν την πιθανοκρατική εκδοχή του σχήματος RSA-FDH η οποία καλείται PSS (Probabilistic Signature Scheme). Αντί της υπογραφής $(m, \mathcal{H}(m))$ αποστέλλεται

$$0 \parallel w \parallel r_* \parallel g_2(w)$$

όπου έχουν επιλεχθεί $k, k_0, k_1 \in \mathbb{N}$, τέτοια ώστε $k_0 + k_1 \leqslant k - 1$ (για παράδειγμα: $k = 1024$ και $k_0 = k_1 = 128$)· ως $\parallel$ συμβολίζεται η παράθεση δυαδικών ακολουθιών και

- το $r \in \{0,1\}^{k_0}$ είναι η τυχαία παράμετρος,
- $w := h(m \parallel r)$ και
- $r_* := g_1(w)$

όπου παραπάνω έχουν χρησιμοποιηθεί οι εξής συναρτήσεις κατακερματισμού $h : \{0,1\}^\star \longrightarrow \{0,1\}^{k_1}$ και $g : \{0,1\}^{k_1} \longrightarrow \{0,1\}^{k-k_1-1}$ καθώς και οι συναρτήσεις $g_1 : \{0,1\}^{k_1} \longrightarrow \{0,1\}^{k_0}$ η οποία επιστρέφει τα πρώτα k_0 δυφία του ορίσματός της και η $g_2 : \{0,1\}^{k_1} \longrightarrow \{0,1\}^{k-k_0-k_1-1}$ η οποία επιστρέφει τα τελευταία $k-k_0-k_1-1$ δυφία του ορίσματός της.

Η ακριβής ασφάλεια του σχήματος PSS είναι

$$\begin{aligned} t(k) &= t'(k) - \left[q_{\text{sig}}(k) + q_{\text{hash}}(k) + 1\right] \cdot k_0 \cdot \Theta(k^3) \\ \epsilon(k) &= \epsilon'(k) + \left[3(q_{\text{sig}}(k) + q_{\text{hash}}(k))^2\right] \cdot (2^{-k_0} + 2^{-k_1}) \end{aligned}$$

όπου $t' \in \mathbb{N}$ είναι ο χρόνος που χρειάζεται ένας αντίπαλος να επιλύσει το πρόβλημα $\mathtt{RSA}[n, e]$ με πιθανότητα επιτυχίας $\epsilon' \in [0, 1]$.

4.3 Το σχήμα υπογραφών Fiat-Shamir

Στο σχήμα ταυτοποίησης Fiat-Shamir [όρα §6.1] ο ρόλος του επαληθευτή (τερματικό) είναι αφ΄ ενός παθητικός, αφ΄ ετέρου μείζονος σημασίας:

> Ο τυχαία επιλεγμένος $(e_{ij}) \in \mathbb{M}_{t\times k}(\mathbb{Z}_2)$, δεν περιέχει κάποια ιδιαίτερη πληροφορία, ωστόσο η αδυναμία του χρήστη να προβλέψει τον πίνακα, αποτρέπει την πλαστογράφηση.

Στο σχήμα υπογραφών τον παθητικό (αλλά κρίσιμο) ρόλο έχει μία δημόσια συνάρτηση κατακερματισμού απ΄ όπου δημιουργείται ο τυχαίος $(e_{ij}) \in \mathbb{M}_{t\times k}(\mathbb{Z}_2)$.

Αλγόριθμος 4.3.1 FS_Sign(I, m): Δημιουργία υπογραφής Fiat-Shamir

---

Είσοδος: Αναγνωριστικό αλφαριθμητικό I και μήνυμα m.
Δεδομένα: Ισοτιμία $n \in \mathbb{N}$. Συνάρτηση κατακερματισμού $f : \{0,1\}^\star \longrightarrow [0, n)$.
΄Εξοδος: Υπογραφή $\left((e_{ij})_{\substack{i=1,\dots,t\\ j=1,\dots,k}}, (y_i)_{i=1,\dots t}\right) \in \mathbb{M}_{t\times k}(\mathbb{Z}_2) \times \mathbb{Z}_n^t$.

1: $r_1, r_2, \dots, r_t \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathbb{Z}_n$;
2: **για** $(i = 1, 2, \dots, t)$
3: $\quad x_i \leftarrow r_i^2 \mod n$;
4: **τέλος για**
5: $(b_0, b_1, \dots, b_{\lceil \log_2 n\rceil - 1})_2 \leftarrow f(m, x_1, \dots, x_t)$; /* 2δική αν/ση του $f(m, x_1, \dots, x_t)$ */
6: **για** $(i = 1, 2, \dots, t)$
7: $\quad$ **για** $(j = 1, 2, \dots, k)$
8: $\quad\quad e_{ij} \leftarrow b_{(i-1)k+j-1}$; /* Τα πρώτα kt δυφία του $f(m, x_1, \dots, x_t)$ */
9: $\quad$ **τέλος για**
10: $\quad y_i \leftarrow r_i \prod_{j=1}^{k} s_j^{e_{ij}} \mod n$;
11: **τέλος για**
12: **επίστρεψε** $\left((e_{ij})_{\substack{i=1,\dots,t\\ j=1,\dots,k}}, (y_i)_{i=1,\dots,t}\right)$;

Λήμμα 4.3.2. *Για το μήνυμα* m, *η υπογραφή* $\left((e_{ij})_{\substack{i=1,\dots,t\\ j=1,\dots,k}}, (y_i)_{i=1,\dots t}\right) \in \mathbb{M}_{t\times k}(\mathbb{Z}_2)\times\mathbb{Z}_n^t$ *που παράγει το αλγόριθμος* FS_Sign(I, m) *επιλέγεται ομοιόμορφα ανάμεσα από τις έγκυρες υπογραφές για το μήνυμα* m.

Απόδειξη. Δοσμένης μιας υπογραφής μπορούν να υπολογισθούν τα $r_1^2, \dots, r_t^2 \in \mathbb{Z}_n$ από την εξίσωση (4.2). Υπάρχουν δύο δυνατές επιλογές για κάθε $r_1, \dots, r_t \in \mathbb{Z}_n$. Συνεπώς, υπάρχουν 2^t διαθέσιμες επιλογές για το $(r_1, \dots, r_t) \in \mathbb{Z}_n^t$. Ούσα η επιλογή των $r_1, \dots, r_t \in \mathbb{Z}_n$ τυχούσα, τότε η υπογραφή επιλέγεται ομοιόμορφα από το σύνολο των έγκυρων υπογραφών για το μήνυμα. □

Αλγόριθμος 4.3.3 FS_VERIFY$\Big(((e_{ij})_{i=1,\ldots,t,\, j=1,\ldots,k}, (y_i)_{i=1,\ldots,t}), I, m\Big)$: Επαλήθευση υπογραφής Fiat-Shamir

Είσοδος: Υπογραφή $\Big((e_{ij})_{\substack{i=1,\ldots,t\\ j=1,\ldots,k}}, (y_i)_{i=1,\ldots,t}\Big) \in \mathbb{M}_{t\times k}(\mathbb{Z}_2) \times \mathbb{Z}_n^t$. Αναγνωριστικό αλφαριθμητικό I. Μήνυμα m.
Δεδομένα: Ισοτιμία $n \in \mathbb{N}$. Συνάρτηση κατακερματισμού $f : \{0,1\}^\star \longrightarrow [0,n)$.
΄Εξοδος: Αποδοχή/Απόρριψη της υπογραφής.

για $(j = 1, 2, \ldots, k)$
  $v_j \leftarrow f(I, j)$
τέλος για
για $(i = 1, 2, \ldots, t)$
  $z_i \leftarrow y_i^2 \prod_{j=1}^{k} v_j^{e_{ij}}$;
τέλος για
$(c_0, c_1, \ldots, c_{\lceil \log_2 n\rceil - 1})_2 \leftarrow f(m, z_1, \ldots, z_t)$; /* 2δική αν/ση του $f(m, x_1, \ldots, x_t)$ */
για $(i = 1, 2, \ldots, t)$
  για $(j = 1, 2, \ldots, k)$
    εάν $(c_{(i-1)k+j-1} \neq e_{ij})$ **τότε**
      επίστρεψε ''απόρριψη'';
    τέλος εάν
  τέλος για
τέλος για
επίστρεψε ''αποδοχή'';

Απόδειξη (Ορθότητας του σχήματος υπογραφής Fiat-Shamir). Για κάθε $i = 1, 2, \ldots, t$, εξ ορισμού, ισχύει ότι

$$z_i = y_i^2 \prod_{j=1}^{t} v_j^{e_{ij}} = \left(r_i \prod_{k=1}^{t} s_k^{e_{ik}}\right)^2 \prod_{j=1}^{t} v_j^{e_{ij}} = r_i^2 \prod_{j=1}^{t} (s_j^2 v_j)^{e_{ij}} = r_i^2 \equiv x_i \pmod{n} \quad (4.2)$$

Κατά συνέπεια, είναι $f(m, z_1, \ldots, z_t) = f(m, x_1, \ldots, x_t)$. □

Ασφάλεια του σχήματος υπογραφών Fiat-Shamir

Ο αλγόριθμος AL: ΄Εστω ένας πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου ο οποίος με είσοδος την ισοτιμία $n \in \mathbb{N}$, τα $v_j := f(I, j) \in \mathbb{Z}_n$ και τις έγκυρες υπογραφές των μηνυμάτων $m_1, m_2, \ldots$ της επιλογής του και παράγει μία έγκυρη υπογραφή για κάποιο άλλο μήνυμα m_0.

Λήμμα 4.3.4 ([FS86]). *Εάν η πολυπλοκότητα του προβλήματος της παραγοντοποίησης της ισοτιμίας* $n \in \mathbb{N}$ *και το μέγεθος* $2^{kt} \in \mathbb{N}$ *μεγαλώνουν με ρυθμό* $o(n^c)$*, τότε ο αλγόριθμος* AL *δεν μπορεί να πλαστογραφήσει υπογραφές του σχήματος υπογραφών Fiat-Shamir, το οποίο κάνει χρήση τυχαίων συναρτήσεων* $f : \{0,1\}^\star \longrightarrow [0,n)$*.*

Λήμμα 4.3.5 ([FS86]). *Εάν αλγόριθμος* AL *μπορεί να επιτύχει πλαστογράφηση στο σχήμα υπογραφών Fiat-Shamir σε χρόνο* $T \in \mathbb{N}$ *με πιθανότητα* $(1+\varepsilon)T2^{-kt}$*, για μια τυχαία συνάρτηση* $f : \{0,1\}^\star \longrightarrow [0,n)$*, τότε μπορεί να παραγοντοποιήσει την ισοτιμία* $n \in \mathbb{N}$ *με μη-αμελητέα πιθανότητα σε χρόνο* $T^2 2^{kt}$*.*

Παρατήρηση 4.3.6. *Η παράλληλη εκτέλεση του σχήματος υπογραφών Fiat-Shamir δεν είναι μηδενικής γνώσης για λόγω επιλογής του ορισμού της μηδενικής γνώσης.*

Παράμετροι ασφαλείας του σχήματος υπογραφών Fiat-Shamir: Υλοποιώντας το σχήμα $k \in \mathbb{N}$ φορές, ο πλαστογράφος μπορεί να επιτύχει εάν σε όλους τους γύρους μάντεψε σωστά από όλες τις πιθανές 2^{kt} επιλογές. Επιλέγοντας $k = 9$ (γύροι) και $t = 8$ (το πλήθος των $r_i \in \mathbb{Z}_n$), τότε ο αντίπαλος μπορεί να επιτύχει στην πλαστογράφησή του με πιθανότητα $2^{-kt} = 2^{-72}$. Το ιδιωτικό κλειδί μπορεί να αποθηκευθεί σε μία μνήμη 576 byte, ενώ η υπογραφή απαιτεί 521 byte.

Πολυπλοκότητα του σχήματος υπογραφών Fiat-Shamir: Ο μέσος όρος των πολλαπλασιασμών στο $\mathbb{Z}_n$ ανέρχεται σε $\frac{1}{2}t(k+2)$ ($\overset{k=9}{\underset{t=8}{=}} 44$).

4.4 Ψηφιακές Υπογραφές με χρήση Ελλειπτικών Καμπυλών (ECDSA)

Κατ΄ αρχάς, για την αλγοριθμική υλοποίηση των ψηφιακών υπογραφών με χρήση ελλειπτικών καμπυλών, οι παράμετροι τομέα [όρα 3.3.9] συνίστανται στην εξής εξάδα $(p, a, b, P, q, h) \in \mathbb{N} \times \mathbb{F}_p^2 \times \mathcal{E} \times \mathbb{N}^2$.

Εδώ συγκεκριμένα είναι:

- Για τον πρώτο αριθμό $p \in \mathbb{N}$ ισχύει ότι $(2^{80}+1) \lneqq p$.
- $\mathrm{ord}(P) = q$, για κάποιον πρώτο αριθμό $q \in \mathbb{N}$, τέτοιον ώστε $q \mid \#\mathcal{E}$.
- Ως συνάρτηση κατακερματισμού $\mathcal{H}(\cdot)$ να χρησιμοποιηθεί κάποια από τις συναρτήσεις SHA-i, $i \in \{0,1,2,3\}$.

Αλγόριθμος 4.4.1 ECDSA_Gen(): Δημιουργία κλειδιού υπογραφής ECDSA.

Δεδομένα: Παράμετροι τομέα $(p, a, b, P, q, h) \in \mathbb{N} \times \mathbb{F}_p^2 \times \mathcal{E} \times \mathbb{N}^2$.
Έξοδος: Το ιδιωτικό κλειδί $d \in \mathbb{Z}_n$ και το δημόσιο κλειδί $Q = d \boxdot P \in \mathcal{E}$.

1: $d \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathbb{Z}_q$; /* $q = \text{ord}(P)$ */
2: **επίστρεψε** $(d, Q) := (d, d \boxdot P)$;

Ορισμός 4.4.2. Στον Αλγόριθμο 4.4.1 (ECDSA_Gen) ο τυχαιοκρατικός παράγοντας $d \in \mathbb{Z}_q$ καλείται **ιδιωτικό κλειδί**. Το $Q = d \boxdot P \in \mathcal{E}(\mathbb{F}_p)$ καλείται **δημόσιο κλειδί**.

Αλγόριθμος 4.4.3 ECDSA_Sign(d, M): Δημιουργία υπογραφής ECDSA.

Δεδομένα: Παράμετροι τομέα $(p, a, b, P, q, h) \in \mathbb{N} \times \mathbb{F}_p^2 \times \mathcal{E} \times \mathbb{N}^2$. Συνάρτηση κατακερματισμού $\mathcal{H} : \mathcal{E} \longrightarrow \{0,1\}^k$. Συνάρτηση $\mathcal{B}_\ell : \mathcal{E} \longrightarrow \mathbb{N}$, όπου $\mathcal{B}_\ell(M)$ είναι ο φυσικός αριθμός που έχει ως δυαδική αναπαράσταση τα αριστερότερα ℓ δυφία του $\mathcal{H}(M)$.
Είσοδος: Το μυστικό κλειδί d και το μήνυμα προς υπογραφή $M \in \mathcal{E}$.
Έξοδος: Υπογραφή $(r, s) \in \mathbb{Z}_q \times \mathbb{Z}_q$ για το μήνυμα $M \in \mathcal{E}$.

1: **επανάλαβε**
2: **επανάλαβε**
3: $k \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathbb{Z}_q$; /* $q = \text{ord}(P)$ */
4: $(x_1, y_1) \leftarrow k \boxdot P$;
5: $r \leftarrow \lfloor x_1 \rfloor \mod q$;
6: **έως ότου** $(r \neq 0)$;
7: $s \leftarrow k^{-1}(\mathcal{B}_\ell(M) + dr) \mod q$;
8: **έως ότου** $(s \neq 0)$;
9: **επίστρεψε** $\sigma := (r, s)$;

Ορισμός 4.4.4. Στον Αλγόριθμο 4.4.3 (ECDSA_Sign) ο τυχαιοκρατικός παράγοντας $k \in \mathbb{Z}_q$ καλείται **εφήμερο κλειδί**.

Αλγόριθμος 4.4.5 ECDSA_Verify $\big((r,s),Q,M\big)$: Επαλήθευση υπογραφής ECDSA.

Δεδομένα: Παράμετροι τομέα $(p,a,b,P,q,h) \in \mathbb{N}\times\mathbb{F}_p^2\times\mathcal{E}\times\mathbb{N}^2$. Συνάρτηση κατακερματισμού $\mathcal{H}:\mathcal{E}\longrightarrow\{0,1\}^k$. Συνάρτηση $\mathcal{B}_\ell:\mathcal{E}\longrightarrow\mathbb{N}$, όπου $\mathcal{B}_\ell(M)$ είναι ο φυσικός αριθμός που έχει ως δυαδική αναπαράσταση τα αριστερότερα ℓ δυφία της δυαδικής αναπαράστασης του $\mathcal{H}(M)$.
Είσοδος: Υπογραφή $(r,s)\in\mathbb{N}\times\mathbb{N}$, δημόσιο κλειδί $Q\in\mathcal{E}$, μήνυμα $m\in\mathcal{E}$.
Έξοδος: Αποδοχή/Απόρριψη της υπογραφής $(r,s)\in\mathbb{N}\times\mathbb{N}$ για το μήνυμα $m\in\mathcal{E}$.

1: **εάν** $((r\notin\mathbb{Z}_q)\bigvee(s\notin\mathbb{Z}_q))$ **τότε**
2: **επίστρεψε** ''απόρριψη''
3: **τέλος εάν**
4: $u_1\leftarrow s^{-1}\mathcal{B}_\ell(M) \mod q$; $u_2\leftarrow s^{-1}r \mod q$;
5: $X\leftarrow(u_1\boxdot P)\boxplus(u_2\boxdot Q)$;
6: **εάν** $(X=\mathbf{O}_\infty)$ **τότε**
7: **επίστρεψε** ''απόρριψη'';
8: **τέλος εάν**
9: $(x_1,y_1)\leftarrow X$;
10: $v\leftarrow\lfloor x_1\rfloor \mod q$;
11: **εάν** $(v=r)$ **τότε**
12: **επίστρεψε** ''αποδοχή'';
13: **αλλιώς**
14: **επίστρεψε** ''απόρριψη'';
15: **τέλος εάν**

Απόδειξη (Ορθότητας του σχήματος υπογραφών ECDSA). Έστω πως από τις εκτελέσεις των αλγορίθμων προκύπτουν τα εξής αποτελέσματα:

$$(d,Q)\leftarrow\text{ECDSA\_Gen}() \qquad (r,s)\leftarrow\text{ECDSA\_Sign}(d,M)$$

όπου οι παράμετροι τομέα είναι οι: $(p,a,b,P,q,h)\in\mathbb{N}\times\mathbb{F}_p^2\times\mathcal{E}\times\mathbb{N}^2$. Τώρα,

$$\begin{aligned}
X &= (u_1\boxdot P)\boxplus(u_2\boxdot Q) && \text{(Αλγόριθμος ECDSA_Verify, γραμμή 5)}\\
&= (u_1\boxdot P)\boxplus((u_2 d)\boxdot P)) && \text{(Αλγόριθμος ECDSA_Gen, γραμμή 2)}\\
&= (u_1+u_2 d)\boxdot P\\
&= (s^{-1}\mathcal{B}_\ell(M)+s^{-1}rd)\boxdot P && \text{(Αλγόριθμος ECDSA_Verify, γραμμή 4)}\\
&= \big(s^{-1}(\mathcal{B}_\ell(M)+rd)\big)\boxdot P\\
&= \Big(\big((\mathcal{B}_\ell(M)+dr)^{-1}k\big)(\mathcal{B}_\ell(M)+rd)\Big)\boxdot P && \text{(Αλγόριθμος ECDSA_Sign, γραμμή 7)}\\
&= k\boxdot P
\end{aligned}$$

Συνεπώς, το σημείο $X\in\mathcal{E}$ που υπολογίζει ο αλγόριθμος ECDSA_Verify είναι το σημείο $k\boxdot P\in\mathcal{E}$ το οποίο υπολόγισε ο αλγόριθμος ECDSA_Sign. □

Σημειώσεις ασφάλειας ECDSA

Για απλοποίηση στους συλλογισμούς, θεωρείται $\ell = \infty$, όπου $\mathcal{B}_\infty \equiv \mathcal{H}$.

► Για τη συνάρτηση κατακερματισμού $\mathcal{H} : \mathcal{E} \longrightarrow \{0,1\}^k$:

- Εάν η $\mathcal{H} : \mathcal{E} \longrightarrow \{0,1\}^k$ αντιστρέφεται εύκολα (δηλαδή δεν είναι pre-image resistant), τότε ο αντίπαλος

  (α′) επιλέγει αυθαίρετα ένα $l \in \mathbb{Z}$ και υπολογίζει $Q \boxplus (l \boxdot P) = (x, y) \in \mathcal{E}$, και θέτει $r := x \pmod q$·

  (β′) κατ΄ όπιν υπολογίζει $e := rl \pmod q$ και

  (γ′) βρίσκει (όντας η $\mathcal{H} : \mathcal{E} \longrightarrow \{0,1\}^k$ μη pre-image resistant) ένα μήνυμα $M \in \mathcal{E}$, τέτοιο ώστε $e = \mathcal{H}(M)$.

  Το ζεύγος $(r, r) \in \mathbb{Z}_q^2$ αποτελεί έγκυρη υπογραφή για το μήνυμα $\mathcal{H}(M)$.

- Εάν η $\mathcal{H} : \mathcal{E} \longrightarrow \{0,1\}^k$ δεν αποσοβεί στις συγκρούσεις (ήτοι δεν είναι colission resistant), τότε ο αντίπαλος

  (i) βρίσκει δύο μηνύματα $M, M' \in \mathcal{E}$, τέτοια ώστε $\mathcal{H}(M) = \mathcal{H}(M')$

  (ii) και εν συνεχεία ζητάει να λάβει μία έγκυρη υπογραφή $\sigma \in \mathbb{Z}_q^2$ για το μήνυμα $M \in \mathcal{E}$.

  Η υπογραφή $\sigma \in \mathbb{Z}_q^2$ είναι έγκυρη και για το μήνυμα $M' \in \mathcal{E}$.

► Για τους ελέγχους στους αλγορίθμους υπογραφής και επαλήθευσης:

- Ο αλγόριθμος ECDSA_Sign(d, M) απαιτεί όπως $r \not\equiv 0 \pmod q$. Έστω πως παραλείπεται ο εν λόγῳ έλεγχος. Επιλέγονται

  – το σώμα $\mathbb{F}_p$, για κάποιον πρώτο αριθμό $p \in \mathbb{N}$,

  – η ελλειπτική καμπύλη $\mathcal{E}(\mathbb{F}_p) : y^3 = x^2 + ax + b$, με $a, b \in \mathbb{F}_p$, όπου το $b \in \mathbb{F}_p$ είναι τετραγωνικό υπόλοιπο modulo p και

  – ως σημείο βάσης το $P = (0, \sqrt{b})$ (η επιλογή της τετμημένης να ισούται με 0 μικραίνει το μέγεθος των παραμέτρων τομέα).

  Πλέον, ο επιτιθέμενος μπορεί να υπογράψει κάθε μήνυμα της επιλογής του $M \in \mathcal{E}$, χρησιμοποιώντας ως υπογραφή την $\sigma = (0, \mathcal{H}(M))$.

- Ο αλγόριθμος ECDSA_Verify$\big((r, s), Q, M\big)$ στην αρχή πραγματοποιεί τον έλεγχο: $r, s \overset{?}{\in} \mathbb{Z}_q$. Οι έλεγχοι μπορούν να υλοποιηθούν αποδοτικά και η απουσία τους έχει οδηγήσει στη διεξαγωγή επιθέσεων σε παρόμοια σχήματα υπογραφών.

► Για το εφήμερο κλειδί:

- Το εφήμερο κλειδί πρέπει να διατηρείται μυστικό. Εάν το εφήμερο κλειδί $k \in \mathbb{Z}_q$ διαρρεύσει, τότε το ιδιωτικό κλειδί μπορεί να υπολογισθεί ως [Αλγόριθμος ECDSA_Sign, 7η γραμμή]:

$$d = r^{-1}(ks - \mathcal{H}(M)) \pmod q \tag{4.3}$$

- Για μικρό εφήμερο κλειδί, πάλι καθίσταται δυνατή η ανάκτηση του ιδιωτικού κλειδιού [όρα §;;].

- Το εφήμερο κλειδί πρέπει να αλλάζει σε κάθε υπογραφή. Διαφορετικά, έστω οι υπογραφές $(r, s_1), (r, s_2) \in \mathbb{Z}_q^2$ για τα μηνύματα $M_1, M_2 \in \mathcal{E}$ αντίστοιχα, έχουν δημιουργηθεί με το ίδιο εφήμερο κλειδί $k \in \mathbb{Z}_q$. Έχουμε:

$$s_1 \equiv k^{-1}(\mathcal{H}(M_1) + dr) \pmod q \qquad s_2 \equiv k^{-1}(\mathcal{H}(M_2) + dr) \pmod q$$

ή ισοδύναμα

$$ks_1 \equiv \mathcal{H}(M_1) + dr \pmod q \qquad ks_2 \equiv \mathcal{H}(M_2) + dr \pmod q$$

και αφαιρώντας κατά μέλη τις παραπάνω ισοτιμίες προκύπτει ότι

$$k(s_1 - s_2) \equiv \mathcal{H}(M_1) - \mathcal{H}(M_2) \pmod q$$

Εάν $s_1 \not\equiv s_2 \pmod q$ (το οποίο ισχύει κατά πάσα πιθανότητα), τότε

$$k \equiv (s_1 - s_2)^{-1}(\mathcal{H}(M_1) - \mathcal{H}(M_2)) \pmod q$$

Έτσι, γνωρίζοντας ο αντίπαλος το εφήμερο κλειδί, μπορεί να υπολογίσει το ιδιωτικό κλειδί από την ισοτιμία (4.3).

Αιτιοκρατικός ECDSA

► Το 2010 διέρρευσαν τα ιδιωτικά κλειδιά του Sony Playstation 3 καθ΄ ότι χρησιμοποιούνταν υπογραφές της μορφής $(r, s_1), (r, s_2)$ [PS3].

► Τον Αύγουστο του 2013 ελαττωματικές γεννήτριες εφήμερων κλειδιών σε συσκευές Android είχαν ως αποτέλεσμα να χαθούν bitcoins [And13].

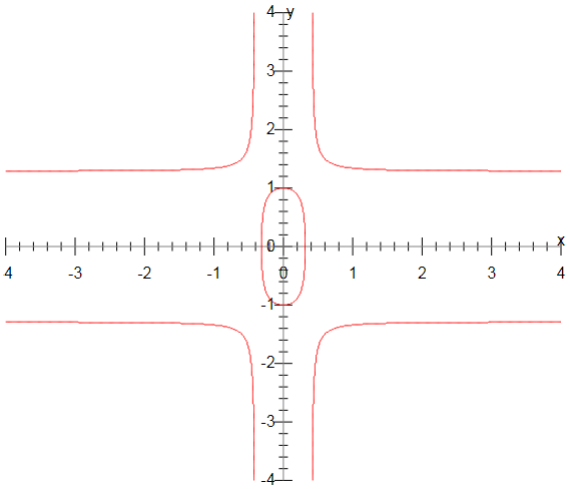
Τα παραπάνω περιστατικά οδήγησαν τον T. Pornin το 2013 στο [Po13] (RfC6979) να δημιουργήσει τον αιτιοκρατικό (deterministic) ECDSA: Το εφήμερο κλειδί επιλέγεται από μία αιτιοκρατική[a] γεννήτρια ψευδοτυχαίων αριθμών, την HMAC-DRBG, η οποία δέχεται ως αρχικοποιήσεις (seeds) της τα $\mathcal{H}(M)$ και το ιδιωτικό κλειδί. Η ασφάλεια του αιτιοκρατικού ECDSA έγκειται στο γεγονός ότι η HMAC-DRBG έχει ψευδοτυχαία συμπεριφορά.

[a] Σε ίδια δεδομένα εισόδου, η γεννήτρια παράγει το ίδιο αποτέλεσμα.

4.4.1 Ψηφιακές υπογραφές σε καμπύλες Edwards (EdDSA)

Ο αλγόριθμος αναπτύχθηκε από τους Daniel Bernstein, Niels Duif, Tanja Lange, Peter Schwabe και Bo-Yin Yang το 2012 στο [EdDSA12] και αποτελεί πρότυπο επικοινωνίας RfC8032.

Ένα σχήμα EdDSA (Edwards-curve Digital Signature Algoritmh) είναι ένα σχήμα που χρησιμοποιεί τις *στρεβλωμένες καμπύλες Edwards*, οι οποίες είναι ελλειπτικές καμπύλες ορισμένες υπεράνω ενός σώματος $\mathbb{K}$, με $\mathrm{char}(\mathbb{K}) \neq 2$ και με βραχεία, κανονική μορφή Weierstrass: $ax^2 + y^2 = 1 + dx^2y^2$.



Σχήμα 4.1: Η στρεβλωμένη καμπύλη Edwards: $10x^2 + y^2 = 1 + 6x^2y^2$

Παρακάτω, υποτίθεται πως $a = 1$ και οι καμπύλες του συγκεκριμένου τύπου ονομάζονται *καμπύλες Edwards*.

Το σχήμα ψηφιακών υπογραφών EdDSA συντίθεται από την επιλογή των εξής παραμέτρων:

$$(p,\ b,\ \mathcal{C},\ \mathcal{H},\ d,\ B,\ \ell, 2^c) \in \mathbb{N}^2 \times (\mathbb{F}_p \to \{0,1\}^{b-1}) \times \mathrm{HashFun} \times \mathbb{F}_p \times \mathcal{E}(\mathbb{F}_p) \times \mathbb{N}^2$$

όπου

- $p \in \mathbb{N}$ πρώτος αριθμός, με $p \equiv 1 \pmod 4$,
- $b \in \mathbb{N}$, όπου $2^{b-1} > p$, έτσι ώστε να μπορούν να αναπαρασταθούν τα σημεία της ελλειπτικής καμπύλης $\mathcal{E}$ και του σώματος $\mathbb{F}_p$ ως συμβολοσειρές των b δυφίων,
- $\mathcal{C} : \mathbb{F}_p \longrightarrow \{0,1\}^{b-1}$ ένας τρόπος κωδικοποίησης των στοιχείων του $\mathbb{F}_p$ σε δυαδικές ακολουθίες μήκους $b-1$ δυφίων,

- $\mathcal{H} : \mathcal{E} \cup \mathbb{F}_p \longrightarrow \{0,1\}^{2b}$,
- $d \in \mathbb{F}_p$, έτσι ώστε $(\nexists z \in \mathbb{F}_p)[z^2 = d]$,
- $\mathcal{E}(\mathbb{F}_p) : -x^2 + y^2 = 1 + dx^2 + y^2$ είναι η βραχεία, κανονική μορφή Weierstrass της ελλειπτικής καμπύλης $\mathcal{E}$,
- $B \in \mathcal{E}(\mathbb{F}_p)$ είναι ένα σημείο της $\mathcal{E}(\mathbb{F}_p)$, το οποίο καλείται **σημείο βάσης**,
- $\ell \in (2^{b-4}, 2^{b-3})$ όπου $\ell = \mathrm{ord}(B)$,
- $2^c \in \mathbb{N}$ είναι η τιμή του συμπαράγοντα της ελλειπτικής καμπύλης, ήτοι $\#\mathcal{E}/\ell = 2^c$, για κάποιο $c \in \mathbb{N}$.

Από τα παραπάνω συνάγεται ότι $\#\mathcal{E} = 2^c\ell$. Επί πλέον θεωρείται η συνάρτηση $\mathcal{B}_s : \mathcal{E} \cup \mathbb{F}_p \longrightarrow \{0,1\}^s$, για $s = 0, 1, \ldots, 2b$, όπου $\mathcal{B}_s(\cdot)$ είναι τα $s \leqslant 2b$ λιγότερο σημαντικά δυφία του $\mathcal{H}(\cdot)$.

Παρατήρηση 4.4.6 (Σημείωση ασφάλειας EdDSA). *Ο αλγόριθμος Pollard ρ θα χρειασθεί $\sqrt{\ell\pi/4}$ πράξεις ελλειπτικών καμπυλών ώστε να επιλύσει το πρόβλημα ECDLP. Συνεπώς, προτείνεται*[†] *όπως $\ell \gtrsim 2^{200}$. Ωστόσο, η επιλογή του $\ell \in \mathbb{N}$ δεσμεύεται από την επιλογή του $p \in \mathbb{N}$, μιας και από το Θεώρημα 3.3.5 (Hasse) ισχύει ότι $|2^c\ell - p - 1| = |\#\mathcal{E} - p - 1| < 2\sqrt{p}$.*

Συμβολισμός. Εάν $P = (x, y) \in \mathcal{E}$, τότε $\underline{P} := (y, x \bmod 2) \in \mathbb{F}_p \times \{0,1\}$.

Αλγόριθμος 4.4.7 EdDSA_Gen(): Αλγόριθμος δημιουργίας κλειδιών EdDSA

Έξοδος: Το ιδιωτικό κλειδί $k \in \{0,1\}^b$ και το δημόσιο κλειδί $\underline{A} \in \mathbb{F}_p \times \{0,1\}$.

1: $k \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{0,1\}^b$;
2: $(h_0, h_1, \ldots, h_{2b-1}) \leftarrow \mathcal{H}(k)$;
3: $a \leftarrow 2^{b-2} + \sum_{i=3}^{b-3} 2^i h_i$; /* Το $a \in \mathbb{Z}$ ειναι πολ/σιο του 8 */
4: $A \leftarrow a \boxdot B$;
5: **επίστρεψε** $(k, \underline{A})$;

Το ιδιωτικό κλειδί $(y, b) \in \mathbb{F}_p \times \{0,1\}$ χρειάζεται b δυφία για να αναπαρασταθεί.

Η συγκόληση (παράθεση) δυαδικών ακολουθιών s_1, s_2 συμβολίζεται ως $s_1 \parallel s_2$. Θεωρείται η συνάρτηση `point-2-str` : $\mathcal{E} \longrightarrow \{0,1\}^\star$, όπου εάν $P = (x, y) \in \mathcal{E}$, τότε `point-2-str`$(P) = s_1 \parallel s_2$, όπου $s_1, s_2 \in \{0,1\}^b$ είναι η δυαδική αναπαράσταση των $x, y \in \mathbb{F}_p$ αντίστοιχα.

[†] `https://safecurves.cr.yp.to/rho.html`

Συμβολισμός. Εάν $T \in \mathbb{F}_p$, τότε $\hat{T} := \mathcal{C}(T) \in \{0,1\}^b$.

Αλγόριθμος 4.4.8 EdDSA_Sign(k, M): Δημιουργία υπογραφής EdDSA

Είσοδος: Το ιδιωτικό κλειδί $k \in \{0,1\}^b$ και το μήνυμα προς υπογραφή $M \in \mathcal{E}$.
Έξοδος: Υπογραφή $(\underline{R}, \hat{S}) \in (\mathbb{F}_p \times \{0,1\}) \times \{0,1\}^b$.

1: $(h_0, h_1, \ldots, h_{2b-1}) \leftarrow \mathcal{H}(k)$;
2: $r \leftarrow \mathcal{H}(h_b \cdots h_{2b-1} \,\|\, \texttt{point-2-str}(M))$;
3: $R \leftarrow r \boxdot B$;
4: $S \leftarrow r + \mathcal{H}\big(\texttt{point-2-str}(\underline{R}) \,\|\, \texttt{point-2-str}(\underline{A}) \,\|\, \texttt{point-2-str}(M)\big)a \mod \ell$;
5: **επίστρεψε** $(\underline{R}, \hat{S})$;

Η ανάκτηση της τετμημένης του $a \boxdot B$ επιτυγχάνεται μέσω του υπολογισμού: $x = (-1)^b \sqrt{\dfrac{y^2 - 1}{dy^2 + 1}}$. Θεωρείται η συνάρτηση $\texttt{str-2-int} : \{0,1\}^\star \longrightarrow \mathbb{N}$, με αποτέλεσμα τον φυσικό αριθμό που έχει δυαδική αναπαράσταση το όρισμά της.

Αλγόριθμος 4.4.9 EdDSA_Verify$(\underline{A}, M, (\underline{R}, \hat{S}))$: Επαλήθευση υπογραφής EdDSA

Είσοδος: Το δημόσιο κλειδί $\underline{A} \in \mathbb{F}_p \times \{0,1\}$, το μήνυμα προς επαλήθευση $M \in \mathcal{E}$ και η υπογραφή $(\underline{R}, \hat{S}) \in (\mathbb{F}_p \times \{0,1\}) \times \{0,1\}^b$.
Έξοδος: Αποδοχή/Απόρριψη της υπογραφής.

1: $A \leftarrow \underline{A}$; $\quad S \leftarrow \hat{S}$;
2: $H \leftarrow \texttt{str-2-int}\Big(\mathcal{H}\big(\texttt{point-2-str}(\underline{R}) \,\|\, \texttt{point-2-str}(\underline{A}) \,\|\, \texttt{point-2-str}(M)\big)\Big)$;
3: **εάν** $((8S) \boxdot B = (8 \boxdot R) \boxplus ((8H) \boxdot A))$ **τότε**
4: **επίστρεψε** ''αποδοχή'';
5: **αλλιώς**
6: **επίστρεψε** ''απόρριψη'';
7: **τέλος εάν**

Απόδειξη (ορθότητας σχήματος EdDSA). Απλουστεύοντας τον συμβολισμό, είναι:

$$\begin{aligned}
(8S) \boxdot B &= (8(r + \mathcal{H}(\underline{R}, \underline{A}, M)a) \boxdot B \qquad \text{(Αλγόριθμος EdDSA_Sign, γραμμή 4)} \\
&= (8 \boxdot (r \boxdot B)) \boxplus \big((8\mathcal{H}(\underline{R}, \underline{A}, M)) \boxdot (a \boxdot B)\big) \\
&= (8 \boxdot (r \boxdot B)) \boxplus \big((8\mathcal{H}(\underline{R}, \underline{A}, M)) \boxdot A\big) \\
&\qquad\qquad \text{(Αλγόριθμος EdDSA_Gen, γραμμή 4: } A = a \boxdot B) \\
&= (8 \boxdot R) \boxplus \big((8\mathcal{H}(\underline{R}, \underline{A}, M)) \boxdot A\big) \\
&\qquad\qquad \text{(Αλγόριθμος EdDSA_Sign, γραμμή 3: } R = r \boxdot B)
\end{aligned}$$

ήτοι η συνθήκη που ελέγχει ο αλγόριθμος EdDSA_Verify στην 3η του γραμμή. □

Το EdDSA σχήμα υπογραφών Ed25519-SHA-512

Επιλέγονται οι παράμετροι ως ακολούθως:

- $p = 2^{255} - 19$ (ο οποίος είναι πρώτος αριθμός),
- $b = 256$,
- η κωδικοποίηση μικρού-μέσου[α] (little-median) του $\{0, 1, \ldots, 2^{255} - 20\}$,
- $\mathcal{H} = \mathsf{SHA\text{-}512}$,
- $d = -\frac{121665}{121666}$ κι άρα[β] $\mathcal{E}(\mathbb{F}_{2^{255}-19}) : -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$,
- $B = (x, 4/5) \in \mathcal{E}(\mathbb{F}_{2^{255}-19})$ όπου $x \equiv 0 \pmod 2$ και
- $\ell \in \mathbb{N}$ ένας πρώτος μήκους 253 δυφίων.

[α] Η *κωδικοποίηση μικρού-μέσου* του $n \in \mathbb{N}$ είναι η $(h_0, h_1, \ldots, h_s) \in \{0,1\}^\star$ (όπου $s = \lceil \log_2 n \rceil$), με $n = \sum_{i=1}^{s} h_i 2^i$ (κι όχι $n = \sum_{i=1}^{s} h_i 2^{s-i}$· δηλαδή τα δυφία αποθηκεύονται με ''ανάποδη'' σειρά).

[β] Θεωρώντας τον μετασχηματισμό $\left\{ x \longmapsto \frac{u}{v}\sqrt{-486664}, \quad y \longmapsto \frac{u-1}{u+1} \right\}$ η ελλειπτική καμπύλη $\mathcal{E}(\mathbb{F}_{2^{255}-19})$ είναι ισοδύναμη με την καμπύλη Montgomery: Ed25519.

4.5 Το σχήμα υπογραφών Paillier

4.5.1 Παραλλαγή του Paillier με μονόδρομες μεταθέσεις καταπακτής

Ορισμός 4.5.1. Έστω X, Y δύο σύνολα, $\mathcal{U}$ μία κατανομή και $e, d \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathcal{U}$. Μία συνάρτηση $f_e : X \longrightarrow Y$ καλείται

- **μονόδρομη** εάν $(\forall \text{ PPT } \mathcal{A})\big[\,\mathsf{Prob}[\mathcal{A}(e, f_e(x)) = x' \wedge f_e(x) = f_e(x')\big] = \mathsf{negl}\left(\lceil \log_2 e \rceil\right)$.
- **συνάρτηση καταπακτής** εάν $(\exists \text{ DPT } \mathcal{T})\big[\mathcal{T}(d, f_e(x)) = x' \wedge f_e(x) = f_e(x')\big]$.
- **μετάθεση** εάν είναι 1–1 και επί.

Πρόταση 4.5.2 ([Pai99, Λήμμα 1]). Έστω $n \in \mathcal{R}$. Εάν $g \in \mathbb{Z}^*_{n^2}$, με $\mathrm{ord}_{\mathbb{Z}^*_{n^2}}(g) = kn$, $k \in \mathbb{N}$, τότε η συνάρτηση

$$\mathcal{F}_g : \mathbb{Z}_n \times \mathbb{Z}^*_n \longrightarrow \mathbb{Z}^*_{n^2} \qquad \mathcal{F}_g(m, r) := g^m \cdot r^n \pmod{n^2}$$

είναι 1–1 και επί.

Έτσι προκύπτει ένα νέο κρυπτοσύστημα (αλγόριθμοι 4.5.3 και 4.5.4).

Αλγόριθμος 4.5.3 Enc1TP$(\langle n, g\rangle, m)$:Υπολογισμός 1δρομης μετάθεσης καταπακτής

Είσοδος: Το δημόσιο κλειδί του Paillier $\langle n, g\rangle \in \mathcal{R} \times \mathbb{Z}_{n^2}$ και το μήνυμα $m \in \mathbb{Z}^*_{n^2}$.
Έξοδος: Το κρυπτοκείμενο $c \in \mathbb{Z}^*_{n^2}$ που αντιστοιχεί στο $m \in \mathbb{Z}^*_{n^2}$.

1: $m_1 \leftarrow m \mod n$; $m_2 \leftarrow m \operatorname{div} n$; /* $m = m_1 + n \cdot m_2$ */
2: **επίστρεψε** $c := g^{m_1} \cdot m_2^n \mod n^2$; /* $c = \mathcal{F}_g(m_1, m_2)$ */

Όπως και στο αρχικό σχήμα του κρυπτοσυστήματος Paillier, η κρυφή πληροφορία που καθιστά εύκολη την αντιστροφή της μονόδρομης μετάθεσης καταπακτής, είναι η παραγοντοποίηση του $n \in \mathcal{R}$.

Αλγόριθμος 4.5.4 Dec1TP$(\langle \lambda, \mu\rangle, c)$:Αντιστροφή 1δρομης μετάθεσης καταπακτής

Είσοδος: Το ιδιωτικό κλειδί $\langle \lambda, \mu\rangle \in \mathbb{N} \times \mathbb{Z}_n$ και το κρυπτοκείμενο $c \in \mathbb{Z}^*_{n^2}$.
Έξοδος: Το απλό κείμενο $m \in \mathbb{Z}_n$ που αντιστοιχεί στο κρυπτοκείμενο $c \in \mathbb{Z}^*_{n^2}$.

1: **όρισε** $L(u-1) \div n$;
2: $m_1 \leftarrow L(c^\lambda \mod n^2) \cdot \mu \bmod n$; /* $\mu := \left(L(g^\lambda \mod n^2)\right)^{-1} \mod n$ */
3: $d \leftarrow c \cdot g^{-m_1} \mod n$; $m_2 \leftarrow d^{(n^{-1} \bmod \lambda)} \mod n$;
4: **επίστρεψε** $m := m_1 + n \cdot m_2$;

Απόδειξη (ορθότητας του σχήματος μονόδρομης μετάθεσης καταπακτής). Έστω το στοιχείο $c := \mathcal{F}_g(m_1, m_2) \in \mathbb{Z}^*_{n^2}$, για $m_1 \in \mathbb{Z}_n$ και $m_2 \in \mathbb{Z}^*_n$.

(α′) Από την ορθότητα του Σχήματος 3.2 έπεται: $L(c^\lambda \mod n^2) \cdot \mu \bmod n = m_1$.

(β′) Τώρα $d = c \cdot g^{-m_1} \mod n = (g^{m_1} \cdot m_2^n) \cdot g^{-m_1} \mod n = m_2^n \mod n$ και

$$d^{(n^{-1} \bmod \lambda)} = (m_2^n)^{(n^{-1} \bmod \lambda)} =^{\ddagger} m_2^{(1 \bmod \lambda)} = (m_2^\alpha)^\lambda \overset{\text{Πρόταση 3.2.7-(α′)}}{\equiv} m_2 \mod n$$

□

Θεώρημα 4.5.5 ([Pai99, Θεώρημα 6]). Το κρυπτοσύστημα που συνιστούν οι αλγόριθμοι 4.5.3 και 4.5.4 είναι μονόδρομο σχήμα εάν και μόνον εάν το πρόβλημα RSA$[n, n]$, για $n \in \mathcal{R}$, είναι δύσκολο να επιλυθεί.

4.5.2 Υλοποίηση υπογραφών

Ο αλγόριθμος Paillier_Gen(p, q) είναι ο αλγόριθμος δημιουργίας κλειδιών του κρυπτοσυστήματος Paillier [όρα Σχήμα 3.2].

$^\ddagger 1 \mod \lambda \iff (\exists \alpha \in \mathbb{Z})[1 = \alpha\lambda]$.

Αλγόριθμος 4.5.6 PAILLIER_SIGN$\big(\langle n, g\rangle, \langle \lambda, \mu\rangle, m\big)$: Δημιουργία υπογραφής Paillier

Είσοδος: Το δημόσιο και ιδιωτικό κλειδί $\langle n, g\rangle \in \mathcal{R} \times \mathcal{B}$ και $\langle \lambda, \mu\rangle \in \mathbb{N} \times \mathbb{Z}_n$ του κρυπτοσυστήματος Paillier και το μήνυμα προς υπογραφή $m \in \mathbb{Z}_n$.
Δεδομένα: Συνάρτηση κατακερματισμού $\mathcal{H} : \mathbb{N} \longrightarrow \mathbb{Z}^*_{n^2}$.
Έξοδος: Υπογραφή $(s_1, s_2) \in \mathbb{Z}_n \times \mathbb{Z}_n$ για το μήνυμα $m \in \mathbb{Z}_n$.

1: **όρισε** $L(u) := (u - 1) \div n$; /* $\lambda := \text{εκπ}(p - 1, q - 1)$ */
2: $s_1 \leftarrow L\big((\mathcal{H}(m))^{\lambda} \mod n^2\big) \cdot \mu \mod n$; /* $\mu := \big(L(g^{\lambda} \mod n^2)\big)^{-1} \mod n$ */
3: $s_2 \leftarrow \big(\mathcal{H}(m) \cdot g^{-s_1}\big)^{(n^{-1} \mod \lambda)} \mod n$;
4: **επίστρεψε** (s_1, s_2);

Ο αλγόριθμος PAILLIER_VERIFY$\big(\langle n, g\rangle, \mathcal{H}(m), \langle s_1, s_2\rangle\big)$ ελέγχει την ισοτιμία:

$$\mathcal{H}(m) \stackrel{?}{\equiv} \mathcal{F}_g(s_1, s_2) = g^{s_1} \cdot s_2^n \pmod{n^2}$$

όπου $n \in \mathcal{R}$, $\mathcal{H}(m) \in \mathbb{Z}^*_{n^2}$, $g \in \mathcal{B}$ και $\sigma := (s_1, s_2) \in \mathbb{Z}_n \times \mathbb{Z}_n$.

Πόρισμα 4.5.7 (του Θεωρήματος 4.5.5). *Υλοποιώντας τη συναρτηση κατακερματισμού $\mathcal{H} : \mathbb{N} \longrightarrow \mathbb{Z}^*_{n^2}$ ως τυχαίο μαντείο, ένας αντίπαλος υπαρξιακής πλαστογραφίας (existential forgery adversary) για το σχήμα υπογραφών Paillier ο οποίος επιχειρεί επίθεση επιλεγμενου απλού κειμένου (KPA) έχει αμελητέα πιθανότητα να αντιστρέψει το σχήμα, δεδομένου ότι το πρόβλημα RSA$[n, n]$ είναι υπολογιστικά δύσκολο.*

Κεφάλαιο 5

Μη-μεταθετική Κρυπτογραφία

Ο έτερος κλάδος της Κρυπτογραφίας που θα αναπτυχθεί είναι η Μη-Μεταθετική Κρυπτογραφία. Πρόκειται για ένα τομέα πιο σύγχρονο από εκείνον της Μεταθετικής Κρυπτογραφίας εάν και τα πρώτα ψήγματα υπήρχαν ήδη από τις αρχές του $20^{ου}$ αιώνος.

Συμβολισμοί του Κεφαλαίου

Στο παρόν Κεφάλαιο κάθε ομάδα G που θεωρείται είναι μη αβελιανή κι άρα θα θεωρείται με τον πολλαπλασιαστικό συμβολισμό. Επί πλέον:

- Για $X \subseteq G$, ως $\langle X \rangle$ θα συμβολίζεται η (πολλαπλασιαστική) ομάδα που παράγεται από τα στοιχεία του X.
- Για $x, y \in G$, συμβολίζεται $[x, y] := x^{-1}y^{-1}xy$. Επί πλέον, για $n \geqslant 2$ και $y_1, \ldots, y_{n+1} \in G$, συμβολίζεται $[y_1, \ldots, y_n, y_{n+1}] := \big[[y_1, \ldots, y_n], y_{n+1}\big]$.
- Για $A, B \leqslant G$, ως $[A, B] = 1$, θα συμβολίζεται το γεγονός ότι τα στοιχεία των $A, B \leqslant G$ εναλλάσσονται ζευγητά, ήτοι $(\forall a \in A)(\forall b \in B)[ab = ba]$.
- Εάν η $K \leqslant G$ είναι κανονική υποομάδα της G, συμβολίζεται ως $K \triangleleft G$.

5.1 Το πρόβλημα του μέλους

Το Σχήμα 5.1 αποτελεί ένα κρυπτοσύστημα η ασφάλεια του οποίου στηρίζεται *αποκλειστικά* στη δυσκολία επίλυσης του προβλήματος του μέλους. Ωστόσο,

το πρόβλημα του μέλους ενδέχεται να *ανακύψει* και σε κρυπτοσυστήματα που βασίζονται σε άλλα προβλήματα*.

5.1.1 Το πρόβλημα

Το υποκείμενο πρόβλημα λοιπόν συνίσταται ως ακολούθως:

Το πρόβλημα του μέλους: Θεωρείται μία ομάδα G, $H := \langle h_1, \ldots, h_k \rangle \leqslant G$, με $h_1, \ldots, h_k \in G$ και $h \in H$. Να βρεθούν $e_1, \ldots, e_\ell \in \mathbb{Z}$ και $i_1, \ldots, i_\ell \in \{1, \ldots, k\}$, έτσι ώστε $h = h_{i_1}^{e_1} \cdots h_{i_\ell}^{e_\ell}$.

Την εκδοχή απόφασης του προβλήματος συνθέτει το ακόλουθο:

Το πρόβλημα του μέλους (εκδοχή απόφασης): Θεωρείται μία ομάδα G, $h \in H$ και $H := \langle h_1, \ldots, h_k \rangle \leqslant G$, με $h_1, \ldots, h_k \in G$. Ισχύει ότι $h \overset{?}{\in} H$;

Έστω το κατηγόρημα

$$\mathrm{Mem}(G, H, x) = \begin{cases} 1, & \text{εάν } x \in H \\ 0, & \text{αλλιώς} \end{cases}$$

όπου η G είναι μία ομάδα $H \leqslant G$ και $x \in G$. Μερικές εκδοχές απόφασης από τα προβλήματα που έχουν ήδη παρατεθεί στην Εργασία μπορούν να αναχθούν στον υπολογισμό του κατηγορήματος $\mathrm{Mem}(G, H, x)$:

1. *Η εκδοχή απόφασης του προβλήματος τετραγωνικού υπολοίπου modulo* n^2, για

$$G = \{x \in \mathbb{Z}_n^* \mid J_n(x) = 1\}$$
$$H = \{x^2 \mod n \mid x \in \mathbb{Z}_n^*\}$$

   Είναι η εκδοχή απόφασης του προβλήματος που στηρίζει την ασφάλειά του το κρυπτοσύστημα Goldwasser-Micali [GM82].

2. *Η εκδοχή απόφασης του προβλήματος* $\mathsf{CR}[n]$ [όρα §3.2.4.Β΄], για

$$G = \{g^m y^n \mod n^2 \mid m \in \{0, 1, \ldots, n-1\} \text{ και } y \in \mathbb{Z}_{n^2}^*\}$$
$$H = \{y^n \mod n^2 \mid y \in \mathbb{Z}_{n^2}^*\}$$

   Η υπόθεση DCRA εκφράζει την πεποίθηση πως το πρόβλημα $\mathsf{CR}[n]$ είναι υπολογιστικά δύσκολο και κατ΄ επέκτασην του κρυπτοσύστημα Paillier [όρα §3.2] είναι ασφαλές.

*Σύμφωνα με το [CSP06], ένας αντίπαλος που προσπαθεί να παρεισφρήσει στο Σχήμα 2.2 πρέπει να επιλύσει *και* το πρόβλημα του μέλους, παρ΄ όλο που το Σχήμα 2.2 σχεδιάστηκε ώστε να στηρίζεται στο πρόβλημα της (πολλαπλής) συζυγίας.

3. *Η εκδοχή απόφασης του προβλήματος Diffie-Hellman*: Έστω $C = \langle g \rangle$ η κυκλική ομάδα τάξη έναν πρώτο αριθμό $p \in \mathbb{N}$ και $\alpha, \beta \in \mathbb{Z}_p^*$ (το ιδιωτικό κλειδί της Αλίκης και του Βασίλη αντίστοιχα). Η τετράδα $(g, g^\alpha, g^\beta, \omega) \in C^4$ καλείται **τετράδα Diffie-Hellman** εάν $\omega = (g^\alpha)^\beta$. Έστω $G := C \times C$, $x := (g, g^\alpha) \in G$ και $y := (g^\beta, \omega) \in G$. Προφανώς, η $(g, g^\alpha, g^\beta, \omega) \in C^4$ είναι τετράδα Diffie-Hellman εάν και μόνον εάν $y \in H := \langle x \rangle = \big\langle (g, g^\alpha) \big\rangle \leqslant G$.

$$G = C \times C = \langle g \rangle \times \langle g \rangle$$
$$H = \langle x \rangle = \big\langle (g, g^\alpha) \big\rangle$$

Πρόκειται για την εκδοχή απόφασης του προβλήματος που στηρίζεται η ασφάλεια του σχήματος ανταλλαγής κλειδιού Diffie-Hellman [όρα Σχήμα 2.1].

καθώς και σε άλλα προβλήματα κρυπτοσυστημάτων (όρα [YS01]).

5.1.2 Σχετικώς ελεύθερες ομάδες

Ορισμός 5.1.1. Έστω F μία ελεύθερη ομάδα και $R \triangleleft F$. Η ομάδα πηλίκο F/R καλείται **σχετικώς ελεύθερη** εάν η R είναι πλήρως αναλλοίωτη[†] υποομάδα της F. Εάν δε $F = \langle x_1, \ldots, x_n \rangle$, τότε τα σύμπλοκα $x_1R, \ldots, x_nR \in F/R$ καλούνται **σχετικώς ελεύθεροι γεννήτορες** της F/R.

Μία σχετικώς ελεύθερη ομάδα διάστασης $n \in \mathbb{N}$ συμβολίζεται ως $\mathcal{F}_n$, ήτοι $\mathcal{F}_n = F_n/R$ όπου η $R \triangleleft F_n$ είναι μία πλήρως αναλλοίωτη υποομάδα της F_n.

Θεωρείται η ελεύθερη ομάδα F_n διάστασης $n \in \mathbb{N}$ κι έστω $X = \{x_1, \ldots, x_n\} \subseteq F_n$ το σύνολο των γεννητόρων της. Οι απεικονίσεις $\gamma_j, \beta_{jk} : X \longrightarrow F_n$, για $1 \leqslant i, j, k \leqslant n$, όπου

$$\gamma_j(x_i) := \begin{cases} x_i^{-1}, & \text{εάν } i = j \\ x_i, & \text{αλλιώς} \end{cases} \qquad \beta_{jk}(x_i) := \begin{cases} x_i x_j, & \text{εάν } i = k \\ x_i, & \text{αλλιώς} \end{cases} \tag{5.1}$$

επάγουν[‡] αυτομορφιμούς της F_n, οι οποίοι καλούνται **αυτομορφισμοί Nielsen**.

Με ακριβώς τον ίδιο τρόπο οι αυτομορφισμοί Nielsen μπορούν να ορισθούν υπεράνω οποιασδήποτε σχετικώς ελεύθερης ομάδας $\mathcal{F}_n$, $n \in \mathbb{N}$. Τα στοιχεία της υποομάδας της $\mathrm{Aut}(\mathcal{F}_n)$ που παράγουν οι αυτομορφισμοί Nielsen της $\mathcal{F}_n$, καλούνται **ήμεροι** (tame) **αυτομορφισμοί**.

[†] $\big(\forall \alpha \in \mathrm{End}(F)\big)[\alpha(R) = R]$

[‡] Οι ελεύθερες ομάδες (κι όχι μόνον) πληρούν την ιδιότητα: ''*Μία απεικόνιση ορισμένη σε ένα σύνολο γεννητόρων μπορεί να επεκταθεί σε ολόκληρη την ομάδα*''.

Έστω, τώρα, πως

$$\mathcal{F}_{n+m} = \langle x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m} \mid R \rangle$$

και έστω ένας

$$\varphi \in \mathrm{Aut}(\mathcal{F}_{n+m}) \qquad\qquad x_i \overset{\varphi}{\longmapsto} y_i \equiv y_i(x_1, \ldots, x_{n+m})$$

για $i = 1, 2, \ldots, n+m$.

Επέκταση του $\varphi \in \mathrm{Aut}(\mathcal{F}_{n+m})$ **στο** $\mathcal{F}_{n+m}^{n+m}$: Ο $\varphi \in \mathrm{Aut}(\mathcal{F}_{n+m})$ δρα κατά φυσιολογικό τρόπο στο $\mathcal{F}_{n+m}^{n+m}$ (ευθύ γινόμενο $n+m$ αντιτύπων της $\mathcal{F}_{n+m}$), δηλαδή

$$(x_1, \ldots, x_{n+m}) \overset{\varphi}{\longmapsto} \big(\varphi(x_1), \ldots, \varphi(x_{n+m})\big) = (y_1, \ldots, y_{n+m})$$

όπου $y_i \equiv y_i(x_1, \ldots, x_{n+m}) \in \mathcal{F}_{n+m}$, για $i = 1, \ldots, n+m$, και γενικότερα

$$(u_1, \ldots, u_{n+m}) \overset{\varphi}{\longmapsto} \big(\varphi(u_1), \ldots, \varphi(u_{n+m})\big) = (y_1, \ldots, y_{n+m})$$

όπου $u_i \equiv u_i(x_1, \ldots, x_{n+m}) \in \mathcal{F}_{n+m}$ και $y_i \equiv y_i(x_1, \ldots, x_{n+m}) \in \mathcal{F}_{n+m}$, για $i = 1, \ldots, n+m$.

Περιορισμός του $\varphi \in \mathrm{Aut}(\mathcal{F}_{n+m})$ **στην** $\mathcal{F}_n$: Έστω $\hat{\varphi} : T \longrightarrow \mathcal{F}_{n+m}^{n+m}$, όπου

$$T := \big\{(u_1, \ldots, u_n, 1, \ldots, 1) \in \mathcal{F}_{n+m}^{n+m} : u_i \equiv u_i(x_1, \ldots, x_n),\ i = 1, 2, \ldots, n\big\} \subseteq \mathcal{F}_{n+m}^{n+m}$$

με $T \simeq \mathcal{F}_n^n$ και

$$\hat{\varphi} : T \longrightarrow \mathcal{F}_{n+m}^{n+m} \qquad\qquad (u_1, \ldots, u_n, 1, \ldots, 1) \overset{\hat{\varphi}}{\longmapsto} \big(\hat{y}_1, \ldots, \hat{y}_{n+m}\big) \tag{5.2}$$

όπου $u_i \equiv u_i(x_1, \ldots, x_n) \in \mathcal{F}_n$ και $\hat{y}_i \equiv y_i(u_1, \ldots, u_n, 1, \ldots, 1) \in \mathcal{F}_{n+m}^{n+m}$

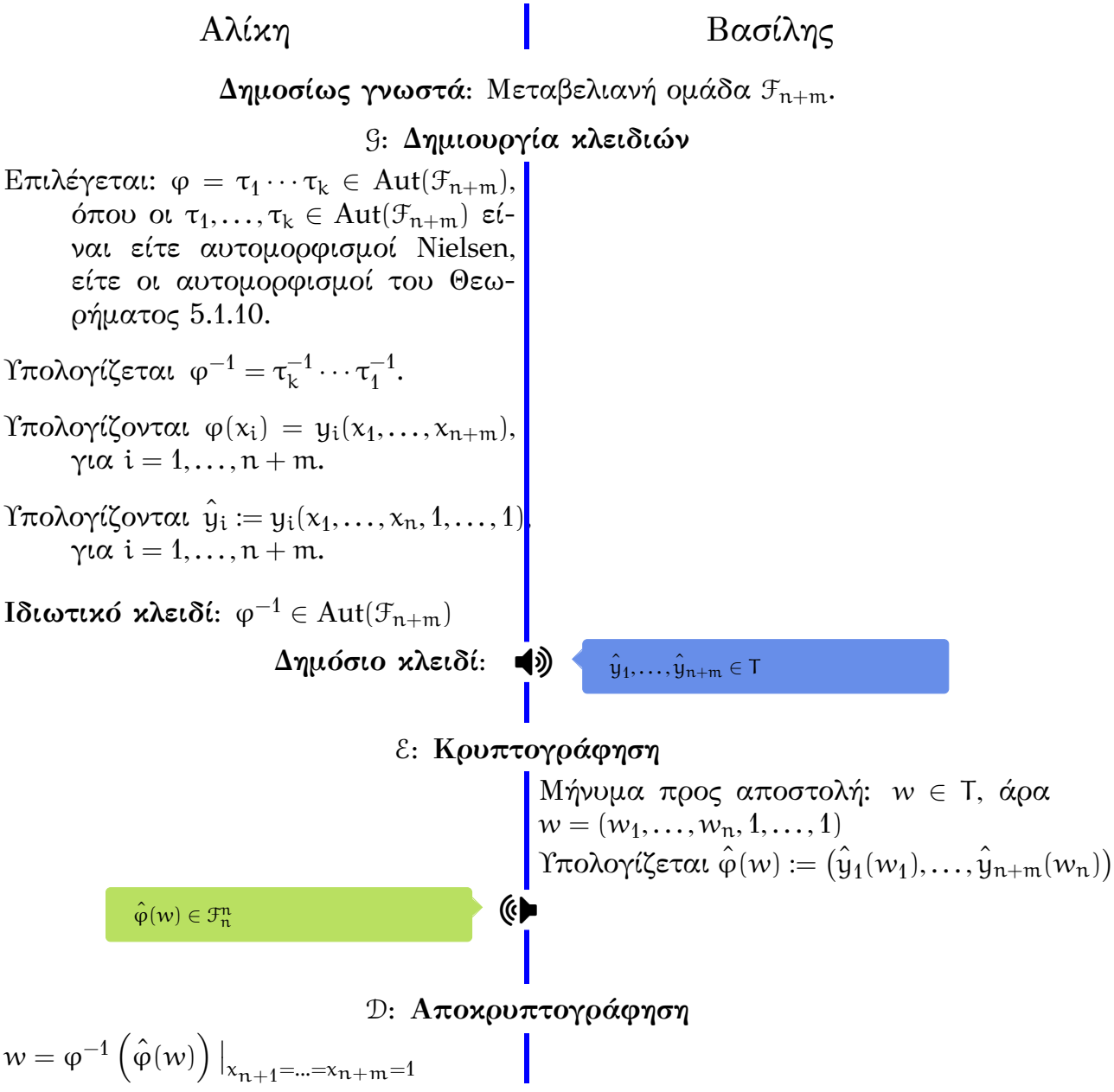
Λήμμα 5.1.2. *Η απεικόνιση* (5.2)*, είναι 1–1.*

Απόδειξη. Όντας $\varphi \in \mathrm{Aut}(\mathcal{F}_{n+m}^{n+m})$, η $\varphi : \mathcal{F}_{n+m}^{n+m} \longrightarrow \mathcal{F}_{n+m}^{n+m}$ είναι και 1–1. Ο περιορισμός μίας 1–1 συνάρτησης, είναι 1–1 συνάρτηση. Άρα, η $\hat{\varphi} : T \longrightarrow \mathcal{F}_{n+m}^{n+m}$ είναι 1–1 ως περιορισμός της 1–1 συνάρτησης $\varphi : \mathcal{F}_{n+m}^{n+m} \longrightarrow \mathcal{F}_{n+m}^{n+m}$. □

Παρατήρηση 5.1.3. *Δεν υπάρχει προφανής τρόπος ώστε δεδομένης της* $\hat{\varphi} : T \to \mathcal{F}_{n+m}^{n+m}$ *να ανακτηθεί ο* $\varphi \in \mathrm{Aut}(\mathcal{F}_{n+m}^{n+m})$ *(δηλαδή* $\varphi\big|_T \equiv \hat{\varphi}$*).*

5.1.3 Το κρυπτοσύστημα Shpilrain-Zapata

Το ακόλουθο κρυπτοσύστημα οφείλεται στους Vladimir Shpilrain και Gabriel Zapata το οποίο δημοσιεύθηκε το 2006 στο [SZ06].



Σχήμα 5.1: Το κρυπτοσύστημα Shpilrain-Zapata

Το Σχήμα 5.1 παρ΄ ότι αποτελεί κρυπτοσύστημα, μπορεί να μετατραπεί σε σχήμα ανταλλαγής κλειδιού για ένα συμμετρικό κρυπτοσύστημα ως εξής:

> Η Αλίκη και ο Βασίλης συμφωνούν πως το μυστικό τους κλειδί θα είναι η κανονική μορφή II της §5.1.4.Β΄.

Παράδειγμα 5.1.4. Έστω $n = 2$, $m = 1$ και $\beta_{jk} \in \mathrm{Aut}(\mathcal{F}_3)$, $1 \leqslant j,k \leqslant 3$, οι αυτομορφισμοί Nielsen υπεράνω της $\mathcal{F}_3$.

Δημιουργία κλειδιού: Η Αλίκη επιλέγει $\varphi := \beta_{23}^2\beta_{12}\beta_{31}\beta_{32}$ και τότε

$$x_1 \overset{\varphi}{\longmapsto} x_1x_3x_2^2 =: y_1(x_1,x_2,x_3), \quad x_2 \overset{\varphi}{\longmapsto} x_2x_1x_3x_2^2 =: y_2(x_1,x_2,x_3),$$
$$x_3 \overset{\varphi}{\longmapsto} x_3x_2^2 =: y_3(x_1,x_2,x_3)$$

και κατ΄ επέκταση, $\hat{y}_1 := y_1(x_1,x_2,1) = x_1x_2^2$, $\hat{y}_2 := y_2(x_1,x_2,1) = x_2x_1x_2^2$ και $\hat{y}_3 := y_3(x_1,x_2,1) = x_2^2$.

Δημόσιο κλειδί: $\hat{y}_1, \hat{y}_2, \hat{y}_3 \in T$.

Ιδιωτικό κλειδί: $\varphi^{-1} = \beta_{32}\beta_{31}\beta_{12}\beta_{23}^{-2} \in \mathrm{Aut}(\mathcal{F}_3)$.

Κρυπτογράφηση: Ο Βασίλης επιθυμεί να αποστείλει στην Αλίκη το μήνυμα $w := \big(u_1(x_1,x_2),\, u_2(x_1,x_2)\big) \in \mathcal{F}_2^2$ στην Αλίκη. Υπολογίζει το κρυπτοκείμενο

$$\hat{\varphi}(w) := \big(\hat{y}_1(u_1,u_2),\, \hat{y}_2(u_1,u_2),\, \hat{y}_3(u_1,u_2)\big) = (u_1u_2^2,\, u_2u_1u_2^2,\, u_2^2) \in T$$

το οποίο και εν τέλει αποστέλλει.

Αποκρυπτογράφηση: Η Αλίκη υπολογίζει $\varphi^{-1}\left(\hat{\varphi}(w)\right)\big|_{x_3=1} = (u_1,u_2)$.

Στην προκειμένη περίπτωση ο αντίπαλος μπορεί να ανακτήσει το μήνυμα $w \in \mathcal{F}_2^2$ ως ακολούθως:

1. Από το δημόσιο κλειδί $(\hat{y}_1,\hat{y}_2,\hat{y}_3) \in T$ υπολογίζει $\hat{y}_1\hat{y}_3^{-1} = x_1$ και $\hat{y}_2\hat{y}_1^{-1} = x_2$.

2. Από το κρυπτοκείμενο $\hat{\varphi}(w) = (v_1,v_2,v_3) \in T$, υπολογίζει $u_1 = v_1v_3^{-1}$ και $u_2 = v_2v_1^{-1}$, δηλαδή το μήνυμα $w = (u_1,u_2)$. ⊣

5.1.4 Ελεύθερες μεταβελιανές ομάδες

Ορισμός 5.1.5. Μία ομάδα G καλείται

- **αβελιανή** εάν $(\forall g, h \in G)\big[[g,h] = 1_G\big]$.
- **μεταβελιανή** εάν $(\forall x, y, z, t \in G)\big[\big[[x,y],[z,t]\big] = 1_G\big]$.
- **μηδενοδύναμη τάξης** $c \in \mathbb{N}$ εάν $(\forall y_1, \ldots, y_{c+1} \in G)\big[[y_1, \ldots, y_{c+1}] = 1_G\big]$.

Θεωρείται μία ομάδα G. Η **παράγωγος υποομάδα** $G' \leqslant G$ της G ορίζεται ως

$$G' := [G,G] = \big\langle [x,y] \in G : x, y \in G \big\rangle$$

Επίσης, ορίζεται η **δεύτερη παράγωγος** της ομάδος G ως $G'' := [G', G']$. Για $n \geqslant 3$ ορίζεται η n-**οστή παράγωγος** της ομάδος G ως $G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$, όπου $G^{(1)} = G'$ και $G^{(2)} = G''$.

Λήμμα 5.1.6. *Σε κάθε ομάδα* G, *η* $G' \leqslant G$ *είναι πλήρως αναλλοίωτη υποομάδα της* G.

Απόδειξη. Έστω $\alpha \in \mathrm{End}(G)$ και $u, v \in G$. Υπολογίζεται

$$\alpha([u,v]) = \alpha(u^{-1}v^{-1}uv) \overset{\alpha \in \mathrm{End}(G)}{=} \alpha(u)^{-1}\alpha(v)^{-1}\alpha(u)\alpha(v) = [\alpha(u), \alpha(v)] \qquad \square$$

Ορισμός 5.1.7. Η **αβελιανοποίηση** μιας ομάδας G συνίσταται στην $G_{ab} := {}^{G}\!/_{G'}$.

Ορίζεται η **κατωτέρα κεντρική σειρά** μιας ομάδος G ως η φθίνουσα σειρά υποομάδων της G:

$$\cdots \triangleleft \gamma_{n+1}(G) \triangleleft \gamma_n(G) \triangleleft \cdots \triangleleft \gamma_2(G) = G' \triangleleft \gamma_1(G) = G$$

η οποία υπακούει στην εξής αναδρομή: $\gamma_1(G) := G, \ldots, \gamma_k(G) := [\gamma_{k-1}(G), G]$.

Λήμμα 5.1.8. *Σε μια ομάδα* G, *η* G'' *και κάθε όρος της κατωτέρας κεντρικής σειράς της* G *είναι πλήρως αναλλοίωτη υποομάδα της* G.

5.1.4.Α΄ Ορισμοί

Ορισμός 5.1.9. Έστω F_n η ελεύθερη ομάδα διάστασης $n \in \mathbb{N}$. Η σχετικώς ελεύθερη ομάδα $M_n := {}^{F_n}\!/_{F_n''}$ καλείται **ελεύθερη μεταβελιανή ομάδα διάστασης** $n \in \mathbb{N}$.

Μία ελεύθερη μεταβελιανή ομάδα είναι προφανώς μεταβελιανή ομάδα.

Η επιλογή ελευθέρων μεταβελιανών ομάδων ικανοποιεί τα εξής επιθυμητά κριτήρια:

(M1) Το πρόβλημα της λέξης είναι εύκολα επιλύσιμο στην M_n.

[Ο Αλγόριθμος 5.1.17 για $w \in M_n$, επιλύει το πρόβλημα της λέξης $w \stackrel{?}{=} 1_{M_n}$ σε $\mathcal{O}(|w|^2 n)$ χρόνο.]

(M2) Η M_n έχει εκθετικό ρυθμό αύξησης.

[Υπάρχουν εκθετικά πολλά (σε σχέση μέγεθος κλειδιού-μέγεθος κλειδοχώρου) κλειδιά· όρα [Mi69].]

(M3) Δεν υπάρχει αλγόριθμος πολυωνυμικού χρόνου που να επιλύει το πρόβλημα του μέλους στην M_n.

[Υπάρχουν αλγόριθμοι οι οποίοι επιλύουν το πρόβλημα του μέλος (εκδοχή απόφασης) στις M_n [όρα [Cou00, Ro880]], ωστόσο κανείς τους δεν είναι πολυωνυμικού χρόνου.]

Οι ελεύθερες μεταβελιανές ομάδες M_n είναι απείρως παριστάμενες για $n \geqslant 2$ [όρα [BST880]], δηλαδή κάθε παράστασή τους $\langle X \mid R \rangle$, το R είναι άπειρο σύνολο, γεγονός που αντίκειται στις μέχρι πρότινος χρησιμοποιούμενες ομάδες.

Για να αποφευχθεί η επίθεση που επιτυγχάνεται στο Παράδειγμα 5.1.4 κατά την επιλογή του $\varphi \in \mathrm{Aut}(\mathcal{F}_{n+m}^{n+m})$ για το Σχήμα 5.1 γίνεται χρήση των ακολούθων συναρτήσεων.

Θεώρημα 5.1.10 ([Sh91]). Έστω $\mathcal{F}_n = F_n \Big/ [R, R]$ και $u \in R$, για μια $R \leqslant F_n$. Εάν $R \leqslant \gamma_3(F_n)$ και $n \geqslant 2$, τότε ο

$$\alpha_{u,j} \in \mathrm{Aut}(\mathcal{F}_n) \qquad \alpha_{u,j}(x_i) := \begin{cases} x_j[x_j, u, x_j], & \text{εάν } i = j \\ x_i, & \text{αλλιώς} \end{cases} \tag{5.3}$$

είναι άγριος (:όχι ήμερος).

Παρατήρηση 5.1.11. *Για το Θεώρημα 5.1.10:*

- $\alpha_{u,j}^{-1}(x_i) = \begin{cases} x_j[x_j, u^{-1}, x_j], & \textit{εάν } i{=}j \\ x_i, & \textit{αλλιώς} \end{cases}$.
- *Όντας (εκ του Ορισμού 5.1.9)* $M_n = F_n \Big/ F_n'' = F_n \Big/ [F_n', F_n']$, *το Θεώρημα 5.1.10 δεν μπορεί να εφαρμοσθεί καθώς* $F_n' \not\leqslant \gamma_3(F_n)$.
  - *Από το [BM85] είναι γνωστόν ότι οι* M_n, *με* $n \neq 3$, *έχουν μόνον ήμερους αυτομορφιμούς.*
  - *Παρ΄ ότι οι αυτομορφισμοί* (5.3) *είναι ήμεροι, είναι δύσκολη η ανάλυσή τους σε σύνθεση αυτομορφισμών Nielsen.*

Επεκτείνοντας το Παράδειγμα 5.1.4 προκύπτει το ακόλουθο:

Παράδειγμα 5.1.12. Έστω $n = 2$ και $m = 1$. Θεωρείται ο

$$\alpha := \alpha_{[x_1,x_2],1} \in \mathrm{Aut}(M_3) \qquad \alpha(x_i) := \begin{cases} x_1[x_1,[x_1,x_2],x_1], & \text{εάν } i = 1 \\ x_i, & \text{αλλιώς} \end{cases}$$

Ορίζεται $\psi := \alpha\varphi \in \mathrm{Aut}(M_3)$, με (από το Παράδειγμα 5.1.4) $\varphi = \beta_{23}^2\beta_{12}\beta_{31}\beta_{32}$. Τώρα,

$$\begin{aligned} x_1 &\overset{\psi}{\longmapsto} z_1(x_1,x_2,x_3) = \alpha(y_1) = x_1[x_1,[x_1,x_2],x_1]x_3x_2^2 \\ x_2 &\overset{\psi}{\longmapsto} z_2(x_1,x_2,x_3) = \alpha(y_2) = x_2x_1[x_1,[x_1,x_2],x_1]x_3x_2^2 \\ x_3 &\overset{\psi}{\longmapsto} z_3(x_1,x_2,x_3) = \alpha(y_3) = x_3x_2^2 \end{aligned}$$

και κατ΄ επέκταση

$$\begin{aligned} \hat{z}_1 &:= z_1(x_1,x_2,1) = x_1[x_1,[x_1,x_2],x_1]x_2^2 \\ \hat{z}_2 &:= z_2(x_1,x_2,1) = x_2x_1[x_1,[x_1,x_2],x_1]x_2^2 \\ \hat{z}_3 &:= z_3(x_1,x_2,1) = x_2^2 \end{aligned}$$

Πλέον,

- Τα x_1, x_2 ως στοιχεία της F_2 δεν ανήκουν στην $\langle \hat{z}_1, \hat{z}_2, \hat{z}_3 \rangle \subseteq F_2$.
- Όντας $\alpha \in \mathrm{Aut}(M_3)$, τα x_1, x_2 ως στοιχεία της $M_3 = {F_3}\big/{F_3''}$ ανήκουν στην $\langle \hat{z}_1, \hat{z}_2, \hat{z}_3 \rangle \subseteq M_3$.

Συνεπώς, ο αντίπαλος ακόμη κι αν βρει τα x_1, x_2 (όπως στο Παράδειγμα 5.1.4) καλείται να επιλύσει το πρόβλημα του μέλους στην $\langle \hat{z}_1, \hat{z}_2, \hat{z}_3 \rangle \subseteq M_3$, το οποίο είναι δυσκολότερο από το πρόβλημα του μέλους στην F_3 (γεγονός που συμβαίνει σε κάθε διάσταση). ⊣

5.1.4.Β΄ Κανονικές μορφές

Ο δακτύλιος ομάδας RG: Έστω R ένας δακτύλιος και G μία (ελεύθερη) ομάδα. Ως RG συμβολίζεται το σύνολο των συναρτήσεων $f : R \longrightarrow G$, με πεπερασμένο φορέα, ήτοι $\#\{x \in R : f(x) \neq 0_G\} \lneq +\infty$. Ένα τυπικό στοιχείο του RG αναγράφεται ως $\sum_{r\in R} a_r g_r$, όπου $a_r \in R$, με $\#\{a_r \in R : a_r \neq 0_R\} \lneq +\infty$, και $g_r \in G$, για $r \in R$.

Συμβολισμός

- Οι γεννήτορες της M_n θα συμβολίζονται απλά ως $x_1, \ldots, x_n$.

Έστω $u, v \in M_n$.

- $u_{ab} := \pi(u)$, όπου $\pi : M_n \longrightarrow {M_n}\Big/{[M_n, M_n]}$ είναι ο κανονικός επιμορφισμός.
- $u^v := v^{-1}uv$.
- $A_n := {M_n}\Big/{[M_n, M_n]}$.
- Έστω ότι $u \in [M_n, M_n] \leqslant M_n$. Η συζυγία επεκτείνεται για $W \in \mathbb{Z}A_n$: Έστω $W \in \mathbb{Z}A_n$, τότε $W = \sum_{i\in\mathbb{Z}} a_i v_i$, για $a_i \in \mathbb{Z}$, όπου $\#\{i \in \mathbb{Z} : a_i \neq 0\} \lneqq +\infty$ και $v_i \in A_n$, για $i \in \mathbb{Z}$. Συμβολίζεται $u^W = \prod (u^{a_i})^{v_i} = \prod (v_i^{-1} u^{a_i} v_i)$.

Κανονική μορφή I

Κάθε $u \in M_n$ μπορεί να περιέλθει στην εξής *κανονική μορφή*:

$$u = u_{ab} \cdot \prod_{\substack{i=1 \\ i<j}}^{n} [x_i, x_j]^{W_{ij}} \tag{5.4}$$

όπου $W_{ij} \in \mathbb{Z}A_n$, για κάθε $i, j \in \{1, 2, \ldots, n\}$, με $i < j$. Η παραπάνω κανονική μορφή μπορεί να υπολογισθεί ως ακολούθως:

1) Χρησιμοποιώντας τις ιδιότητες των μεταθετών:

$$[y, x] = [x, y]^{-1}, \qquad xy^{-1} = y^{-1}[y, x]^{y^{-1}x^{-1}}x, \qquad [x, y]z = z[x, y]^z,$$
$$xy = yx[x, y], \qquad x^{-1}y = y[y, x]^{y^{-1}x^{-1}}x^{-1}$$

   (α′) Μεταφέρονται όλες οι εμφανίσεις ‘‘εκτός-μεταθετών’’ του x_1 στην αρχή (αριστερότερα) της $u \in M_n$ (δηλαδή οι εμφανίσεις του x_1 που δεν συμμετέχουν σε μεταθέτες της μορφής $[x_1, x_j]$ ή $[x_j, x_1]$, $j = 2, 3, \ldots, n$).

   (β′) Επαναλβάνεται η άνωθεν διαδικασία για τους γεννήτορες $x_2, x_3, \ldots, x_n$.

   Στο τέλος της διαδικασίας θα είναι $u = u_{ab} \cdot c$, όπου $c \in [M_n, M_n]$, το οποίο θα είναι γινόμενο στοιχείων της μορφής $[x_i, x_j]^g$, $g \in M_n$.

2) Αφού για κάθε $k, l \in [M_n, M_n]$ ισχύει ότι $kl = lk$ στην M_n, τα στοιχεία του παραπάνω όρου $c \in [M_n, M_n]$ μπορούν να διαταχθούν κατά τρόπον τέτοιον ώστε $u = u_{ab} \cdot \prod_{\substack{i=1 \\ i<j}}^{n} [x_i, x_j]^{W_{ij}}$, για $W_{ij} \in \mathbb{Z}A_n$, $i, j = 1, \ldots, n$, με $i < j$.

Η κανονική μορφή (5.4) είναι εύκολο να υπολογισθεί, ωστόσο για $n \geqq 2$ δεν είναι μοναδική και γι αυτό δεν μπορεί να χρησιμοποιηθεί για να αναπαραστήσει τα στοιχεία που ανταλλάζουν οι οντότητες στο πρωτόκολλο.

Κανονική μορφή II

Ορισμός 5.1.13. Έστω μία ελεύθερη ομάδα F με γεννήτορες τους $x_1, x_2, \ldots$. Η **παράγωγος Fox ως προς τον** x_i ορίζεται ως η απεικόνιση $\partial_{x_i} : \mathbb{Z}F \longrightarrow \mathbb{Z}F$ η οποία ικανοποιεί τις ακόλουθες ιδιότητες:

- $\partial_{x_i}(x_j) = \delta_{ij}$ (η συνάρτηση δέλτα του Kronecker).
- $\partial_{x_i}(uw) = \partial_{x_i}(u) + u \cdot \partial_{x_i}(w)$, για $u, w \in F$.

Παράδειγμα 5.1.14. Θεωρείται F μία ελεύθερη ομάδα και 1 το ταυτοτικό της στοιχείο. Έστω $g \in F$ και x ένας γεννήτορας της F.

$\{\partial(1) = 0\}$: $\partial_x(1) = \partial_x(1) + 1\partial_x(1)\partial_x(1) + \partial_x(1) \implies \partial_x(1) = 0.$

$\{\partial(g^{-1}) = -g^{-1}\partial(g)\}$: $0 = \partial_x(1) = \partial(g^{-1}g) = \partial_x(g^{-1}) + g^{-1}\partial_x(g).$ ⊣

Παράδειγμα 5.1.15. Έστω $F_n = \langle x, y, \ldots \rangle$ η ελεύθερη ομάδα διάστασης $n \geqslant 2$. Λαμβάνοντας υπ' όψιν τα αποτελέσματα του Παραδείγματος 5.1.14 υπολογίζονται:

$$\begin{aligned}\partial_z\big([x,y]\big) = \partial_z(x^{-1}y^{-1}xy) &= \partial_z(x^{-1}) + x^{-1}\partial_z(y^{-1}) + x^{-1}y^{-1}\partial_z(x) + x^{-1}y^{-1}x\partial_z(y)\\ &= -x^{-1}\partial_z(x) + x^{-1}y^{-1}\partial_z(y) + x^{-1}y^{-1}\partial(x) + x^{-1}y^{-1}x\partial_z(x)\end{aligned}$$

- Για $z = x$, προκύπτει $\partial_x\big([x,y]\big) = x^{-1}y^{-1}(1-y)$.
- Για $z = y$, προκύπτει $\partial_y\big([x,y]\big) = -x^{-1}y^{-1}(1-x)$. ⊣

Θεωρείται ο φυσικός επιμορφισμός

$$p : F \longrightarrow F_{ab} \qquad\qquad w \overset{p}{\longmapsto} wF'$$

ο οποίος επεκτείνεται γραμμικά στην απεικόνιση $p : \mathbb{Z}F \longrightarrow \mathbb{Z}F_{ab}$.

Πρόταση 5.1.16 ([Gu87])**.** Έστω $w \in F_n = \langle x_1, \ldots, x_n \rangle$. Ισχύει ότι

$$w \in F_n'' \iff (\forall i = 1, \ldots, n)[p(\partial_{x_i}(w)) = 0]$$

Αλγόριθμος 5.1.17 Solve_WP_$M_n(w)$: Επίλυση του προβλήματος της λέξης στην M_n

Δεδομένα: $x_1F_n'', \ldots, x_nF_n''$ οι σχετικώς ελεύθεροι γεννήτορες της M_n, δηλαδή $F_n = \langle x_1, \ldots, x_n \rangle$ και $M_n = {F_n}\Big/{F_n''} = \langle x_1F_n'', \ldots, x_nF_n'' \rangle$. Ο φυσικός επιμορφισμός $p : \mathbb{Z}F_n \longrightarrow \mathbb{Z}(F_n)_{ab}$

Είσοδος: $w \equiv w(x_1F_n'', \ldots, x_nF_n'') \in M_n$.

Έξοδος: Απόφανση εάν $w \stackrel{?}{=} 1_{M_n}$.

```
1: w ← w(x_1, ..., x_n);      /* Η w θεωρείται υπεράνω των γεννητόρων x_1, ..., x_n */
2: για (i = 1, 2, ..., n)
3:    εάν (p(∂_{x_i}(w)) ≠ 0) τότε
4:       τύπωσε ''w ≠ 1_{M_n}'';                          /* Άρα, w ∉ F_n'' */
5:       έξοδος;
6:    τέλος εάν
7: τέλος για
8: τύπωσε ''w = 1_{M_n}'';                                /* Άρα, w ∈ F_n'' */
```

Εάν λοιπόν $\forall i = 1, \ldots, n)[p(\partial_{x_i}(w)) = 0]$, τότε $w \in F_n''$ κι άρα $w = 1_{M_n}$, διότι $M_n = {F_n}\Big/{F_n''}$. Έτσι εκμαιεύεται ο παρακάτω αλγόριθμος ο οποίος επιλύει το πρόβλημα της λέξης στην M_n.

Πρόταση 5.1.18 ([SZ06]). Ο Αλγόριθμος 5.1.17 έχει το πολύ τετραγωνική πολυπλοκότητα ως προς το μήκος της λέξης που δέχεται ως είσοδο.

Η *κανονική μορφή* του $u \in M_n$ είναι ο 2×2 πίνακας

$$u = \begin{bmatrix} u_{ab} & \left(\partial_{x_1}(p(u)), \ldots, \partial_{x_n}(p(u))\right) \\ 0 & 1 \end{bmatrix} \tag{5.5}$$

η οποία έχει μοναδική γραφή, ωστόσο είναι χρονοβόρα στο να υπολογισθεί. Κατά τον πολλαπλασιασμό δύο κανονικών μορφών (5.4) (πολλαπλασιασμός δύο 2×2 πινάκων), για τον υπολογισμό του άνω δεξιά στοιχείου της προκύπτουσας κανονικής μορφής, θα χρειασθεί ''πολλαπλασιασμός'' στοιχείων της $[M_n, M_n]$ με τα διανύσματα του πίνακα της κανονικής μορφής (5.4). Θεωρώντας πως ο εν λόγω ''πολλαπλασιασμός'' γίνεται κατά συντεταγμένη προκύπτει πως το σύνολο των κανονικών μορφών εφοδιασμένο με τον πολλαπλασιασμό πινάκων -όπως ορίσθηκε μόλις- αποκτάει δομή ομάδας.

Παρατήρηση 5.1.19. *Η αναπαράσταση των στοιχείων της M_n στην κανονική μορφή (5.4) είναι πιστή*[§] *κι άρα προκύπτει η εμβάπτιση της M_n στην ομάδα των πινάκων της μορφής (5.4). Η εν λόγω εμβάπτιση καλείται **εμβάπτιση Magnus** [όρα [Gu87]].*

[§] έχει τετριμμένο πυρήνα

5.1.5 Ασφάλεια

Υπάρχουν δύο τρόποι με τους οποίους ένας αντίπαλος θα μπορούσε να επιτύχει πλήγμα στο Σχήμα 5.1:

Α΄. Γνωρίζοντας το δημόσιο κλειδί $\hat{\varphi}$, να υπολογισθεί ο $\varphi^{-1} \in \mathrm{Aut}(M_{m+n})$.

Β΄. Να επιλυθεί το πρόβλημα του μέλους στην M_{m+n} [όρα Παράδειγμα 5.1.12].

Για την προτέρα επίθεση -όπως αναφέρθηκε και στην Παρατήρηση 5.1.3- δεν υπάρχει κάποια προφανής μέθοδος υπολογισμού. Επομένως, θα αναπτυχθούν επιχειρήματα γύρω από τη δεύτερη επίθεση.

Ο αλγόριθμος 5.1.17 επιλύει το πρόβλημα της λέξης στην ομάδα M_n χρησιμοποιώντας την παράγωγο Fox. Ωστόσο, υπάρχει ένας πιο ‘‘ωμός’’ ώστε να επιλυθεί το πρόβλημα.

Ορισμός 5.1.20. Μία ομάδα G καλείται **προσεγγιστικά πεπερασμένη** (residually finite) εάν για κάθε $g \in G \setminus \{1_G\}$, υπάρχει μία πεπερασμένη ομάδα H_g κι ένας ομομορφισμός $f : G \longrightarrow H_g$, τέτοια ώστε $f(g) \neq 1_{H_g}$.

Εάν μία ομάδα $G = {}^{F}\!/_{R}$ είναι προσεγγιστικά πεπεπερασμένη και πεπερασμένα παριστάμενη, τότε το πρόβλημα της λέξης στην G επιλύεται ως εξής:

1: Έστω $w \in G$ ως λέξη των γεννητόρων της F.

2: Εκτελούνται παράλληλα οι παρακατω αλγόριθμοι:

(α΄) Απαριθμεί όλους τους ομομορφισμούς $f : G \longrightarrow K$ της G και σε εκείνους οι οποίοι έχουν πεπερασμένη εικόνα ελέγχει εάν $f(g) \neq 1_K$.

(β΄) Απαριθμεί όλα τα στοιχεία της $R \lhd F$ και ελέγχει αν κάποιο είναι το w.

Η ως άνω μεθοδολογία είναι επιτυχής, αλλά όχι πρακτικά εφαρμόσιμη.

Ορισμός 5.1.21. Μία ομάδα G καλείται **τοπικώς εκταθείσα προσεγγιστικά πεπερασμένη** (locally extended residually finite) εάν για κάθε υποομάδα της $K \leqslant G$, και $g \in G \setminus K$, υπάρχει πεπερασμένη ομάδα $H_{g,K}$ και ομομορφισμός $f : G \longrightarrow H_{g,K}$, τέτοια ώστε $f(g) \in f[G] \setminus f[K]$.

Ο T. Coulbois το 2000 στο [Cou00] απέδειξε πως οι μεταβελιανές ομάδες είναι τοπικώς εκταθείσες προσεγγιστικά πεπερασμένες ομάδες. Το πρόβλημα της λέξης σε μία τοπικώς εκταθείσα προσεγγιστικά πεπερασμένη ομάδα επιλύεται όπως και στις προσεγγιστικά πεπερασμένες ομάδες. Ωστόσο, ένας τέτοιος αλγόριθμος δεν είναι πρακτικά υλοποιήσιμος.

Ένας άλλος αλγόριθμος προτάθηκε από τον N. S. Romanovskii το 1980 στο [Ro80], όπου -ανάμεσα σε άλλα- υπολογίζει τη βάση Gröbner ενός ιδεώδους του δακτυλίου πολυωνύμων Laurent. Ωστόσο, ακόμη κι αυτός ο αλγόριθμος είναι πρακτικά μη υλοποιήσιμος.

5.1.6 Παράμετροι υλοποίησης

Ομάδα υλοποίησης:

Παρά την ύπαρξη των αλγορίθμων [Cou00, Ro80] για την υλοποίηση του Σχήματος 5.1 προτείνονται οι μεταβελιανές ομάδες $M_r = F_r \Big/ [F'_r, F'_r]$, όπου $r = 30$, και $r = n + m$, με $n = 8$ και $m = 2$.

Επιλογή μυστικού κλειδιού:

Κατά τη δημιουργία του $\varphi := \tau_1 \cdots \tau_k \in \mathrm{Aut}(M_r)$ προτείνεται

- $k = 30$ και
- το σύνολο $\{\tau_1, \ldots, \tau_k\}$ δημιουργείται επιλέγοντας τυχαία από τους ομομορφισμούς Nielsen και τους ομομορφισμούς του Θεωρήματος 5.1.10 όπου
  - με πιθανότητα 90% επιλέγεται ένας αυτομορφισμός Nielsen (5.1) και
  - με πιθανότητα 10% επιλέγεται ένας αυτομορφισμός $a_{u,j} \in \mathrm{Aut}(M_r)$ [όρα (5.3)], για κάποια τυχαία επιλεγμένη $u \in [F_r, F_r]$.

Συνεπώς, σε μια (σχετικώς) ελεύθερη ομάδα διάστασης 10, η επιλογή 30 αυτομορφισμών Nielsen δίδει $100^{30} = 10^{60}$ επιλογές για τον φ. Για να μην είναι ο υπολογισμός του φ αρκετά κοστοβόρος, όσον αφορά τη τυχαία επιλογή $u \in [F_r, F_r]$, για τους αυτομορφισμούς (5.3), τίθεται ο περιορισμός $|u| \leqslant 10$. Έτσι υπάρχουν 10^7 δυνατές επιλογές για την $u \in [F_r, F_r]$.

5.1.7 Σύνοψη

Οι Vladimir Shpilrain και Gabriel Zapata χρησιμοποίησαν το πρόβλημα του μέλους ώστε να στηρίξουν την ασφάλεια του Σχήματος 5.1. Ως ομάδα υλοποίησης του κρυπτοσυστήματος επιλέχθηκε η κλάση των μεταβελιανών ομάδων οι οποίες πεπερασμένα παριστάμενες, εν αντιθέσει με τη συνήθη τακτική επιλογής απείρως παραστάσιμων ομάδων. Οι μεταβελιανές ομάδες έχουν ως προτέρημα ότι το πρόβλημα της λέξης είναι ευκόλως επιλύσιμο καθώς και ότι έχουν εύκολα υπολογίσιμες κανονικές μορφές.

Οι εμπνευστές του Σχήματος 5.1 αναφέρουν πως υπάρχουν ομοιότητες σε φιλοσοφικό επίπεδο όσον αφορά το Σχήμα 5.2, ωστόσο το κρυπτοκείμενο που παράγει το Σχήμα 5.1 δεν αποτελεί ομομορφική [σύμφωνα με τον Ορισμό 5.2.1] εικόνα (ή προεικόνα) του απλού κειμένου από το οποίο προέρχεται. Επίσης,

αναφέρουν πως οι ιδέες για το Σχήμα 5.1 (που εντάσσεται στη Μη-Μεταθετική Κρυπτογραφία) εντοπίζονται στο κρυπτοσύστημα από το [Moh99] (από τη Μεταθετική Κρυπτογραφία· το οποίο χρησιμοποιεί tame αυτομορφισμούς και υλοποιείται στο $\mathrm{GF}(2^m)$, όρα §6.3), το οποίο απεδείχθει ανασφαλές στο [GC00].

5.2 Ομομορφική κρυπτογραφία και λογικά κυκλώματα

Αναλύεται μία διαφορετική -από τον Ορισμό 3.2.1- έννοια για την ομομορφική κρυπτογράφηση.

5.2.1 Ομομορφικά κρυπτοσυστήματα

Ορισμός 5.2.1. Έστω H μία μη τετριμμένη και πεπερασμένη ομάδα, G μία πεπερασμένα παραγόμενη ομάδα και $f : G \twoheadrightarrow H$ ένας επιμορφισμός. Θεωρείται R ένα σύνολο αντιπροσώπων των συμπλόκων του $\ker f$ στην G, A ένα σύνολο και μία απεικόνιση $P : A \longrightarrow G$ τέτοια ώστε $\mathrm{Im}\, P = \ker f$. Η τριάδα $\mathcal{S} = \langle A, P, R\rangle$ καλείται **ομομορφικό κρυπτοσύστημα υπεράνω της** H **ως προς τον** f εάν υπάρχει $N \in \mathbb{N}$ -το οποίο καλείται **μέγεθος** του $\mathcal{S}$-, έτσι ώστε να ικανοποιούνται:

(H1) Τα στοιχεία του συνόλου A είναι λέξεις υπεράνω ενός δεδομένου αλφαβήτου. Η τυχαία επιλογή ενός $a \in A$ με $|a| = N$ μπορεί να επιτευχθεί σε πιθανοτικό χρόνο $N^{\mathcal{O}(1)}$.

(H2) Τα στοιχεία της ομάδας G αναπαριστώνται υπεράνω ενός συγκεκριμένου αλφαβήτου. Ο έλεγχος της ισότητας ανάμεσα σε δύο στοιχεία της G και η πράξη ανάμεσα σε δύο στοιχεία της G απαιτούν χρόνο $N^{\mathcal{O}(1)}$, δεδομένου ότι τα προαναφερθέντα στοιχεία έχουν μήκος του πολύ N.

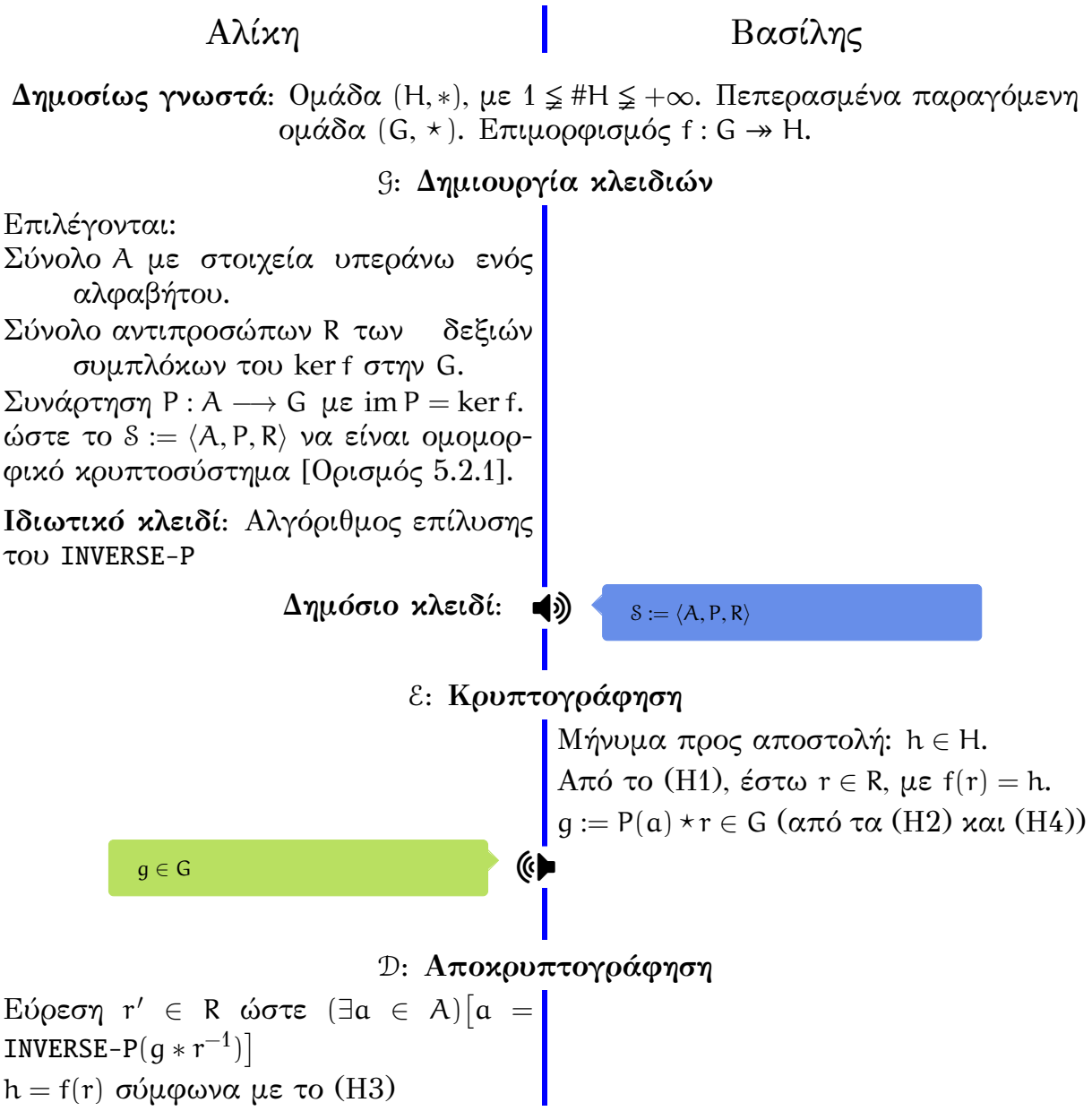
(H3)
- Το σύνολο R αναπαρίσταται ως λίστα στοιχείων.
- Η ομάδα H αναπαρίσταται από τον πίνακα της πράξης της ομάδας.
- Η 1–1 και επί απεικόνιση $R \longrightarrow H$ (η οποία επάγεται από την $f : G \to H$) αναπαρίσταται, και ζεύγη της μορφής $(r, f(r))$.
- $|R| = |H| = \mathcal{O}(1)$.

Για κάθε απεικόνιση $P : A \longrightarrow G$ το πρόβλημα `INVERSE-P`(g) είναι η εξακρίβωση εάν $g \in \mathrm{Im}(P)$ κι αν ναι, τότε επιστρέφεται τυχαία ένα $a \in A$, ώστε $P(a) = g$.

(H4) Η απεικόνιση $P : A \longrightarrow G$ είναι μία συνάρτηση καταπακτής: Για $a \in A$,
- το $P(a) \in G$ υπολογίζεται σε χρόνο $|a|^{\mathcal{O}(1)}$, ενώ
- το πρόβλημα `INVERSE-P`(a) είναι υπολογιστικά δύσκολο.

5.2.2 Υλοποίηση

Στο [GP03] οι Dima Grigoriev και Ilia Ponomarenko προτείνουν το εξής:



Σχήμα 5.2: Το κρυπτοσύστημα των Grigoriev-Ponomarenko

5.2.2.Α΄ Ασφάλεια

Το υποκείμενο υπολογιστικό πρόβλημα στο οποίο θα στηρίχθηκε η ασφάλεια του Σχήματος 5.2 είναι:

Το πρόβλημα FACTOR$[n, m]$: Έστω ότι $n = pq \in \mathcal{R}$ και $m \in \mathbb{N} \setminus \{1\}$, τέτοια ώστε $G_{n,m} \Big/ (\mathbb{Z}_n)^m \simeq (\mathbb{Z}_m, +)$, όπου $G_{n,m} := \left\{g \in \mathbb{Z}_n^* : \mathbf{J}_n(g) \in \{1, (-1)^{m \bmod 2}\}\right\}$. Δεδομένου ότι $m \mid p-1$ και $\mu\kappa\delta(m, q-1) = \mu\kappa\delta(m, 2)$, να βρεθούν οι πρώτοι αριθμοί $p, q \in \mathbb{N}$.

Όσον αφορά την κατασκευή ομομορφικών (σύμφωνα με τον Ορισμό 5.2.1) κρυπτοσυστημάτων που στηρίζονται στο πρόβλημα FACTOR$[n, m]$ ισχύει το παρακάτω

Θεώρημα 5.2.2 ([GP03], Θεώρημα 1.3)**.** Θεωρείται μία μη τετριμμένη και πεπερασμένη ομάδα H και $N \in \mathbb{N}$. Μπορεί να σχεδιασθεί ένα ομομορφικό [ως προς τον Ορισμό 5.2.1] κρυπτοσύστημα $\mathcal{S} \equiv \mathcal{S}(H, N)$, του οποίου το πρόβλημα INVERSE-P να είναι πολυωνυμικού χρόνου πιθανοτικά ισοδύναμο με τα προβλήματα FACTOR$[m, n]$, για κατάλληλο $n = e^{\mathcal{O}(N)}$ και $m \in \mathbb{N}$ το οποίο διατρέχει τους διαιρέτες της $\#H$.

για τις περιπτώσεις όπου:

(α΄) η G είναι πεπερασμένη αβελιανή ομάδα και η H είναι κυκλική ομάδα (όρα [GP03, §2])·

(β΄) η G είναι πεπερασμένο ελεύθερο γινόμενο κάποιων συγκεκριμένων αβελιανών ομάδων και η H είναι τυχούσα (όρα [GP03, §3]).

5.2.3 Λογικά κυκλώματα και αποτελέσματα

Λογικά κυκλώματα

Το $\{\neg, \wedge\}$ (άρνηση, σύζευξη) αποτελούν επαρκές (:κάθε τύπος της Προτασιακής Λογικής μπορεί να εκφρασθεί χρησιμοποιώντας ως πράξεις την άρνηση και τη σύζευξη) σύνολο.

Οπτικοποίηση: Το *λογικό κύκλωμα* είναι ένα κατευθυνόμενο γράφημα $\langle V, E\rangle$, όπου το V είναι ένα σύνολο και $E \subseteq \left\{(u, v) \in V \times V : u \neq v\right\}$. Ορίζονται

$$\mathrm{indeg}(v) := \#\{u \in V : (u, v) \in E\} \qquad \mathrm{outdeg}(v) := \#\{u \in V : (v, u) \in E\}$$

Εάν $e := (u, v) \in E$, τότε η $u \in V$ καλείται **αρχή** της $e \in E$ και η $v \in V$ καλείται **πέρας** της $e \in E$.

- Ως είσοδος του λογικού κυκλώματος επιλέγονται $x_1, \ldots, x_n \in V$, όπου $\mathrm{indeg}(x_i) = 0$, $i = 1, \ldots, n$. Το $n \in \mathbb{N}$ καλείται **μέγεθος** του λογικού κυκλώματος.
- Ως έξοδος του λογικού κυκλώματος επιλέγεται μία κορυφή $y \in V$, όπου $\mathrm{outdeg}(y) = 0$.
- Οι κορυφές $x_1, \ldots, x_n \in V$ φέρουν από μία ετικέτα: $(x_i, b_i) \in V \times \{0, 1\}$ (η ανάθεση των τιμών στο λογικό κύκλωμα).
- Κάθε $v \in V \setminus \{x_1, \ldots, x_n\}$ φέρει 1 ετικέτα: $(v, g, b) \in V \times \{\neg, \wedge\} \times \{0, 1\}$, όπου
  - εάν $g = \neg$, τότε $\mathrm{indeg}(v) = \mathrm{outdeg}(v) = 1$ και $b = 1 - x$, όπου (u, g', x) (ή (u, x) εάν $u \in \{x_1, \ldots, x_n\}$) είναι η ετικέτα της $u \in V$, με $(u, v) \in E$.
  - εάν $g = \wedge$, τότε $\mathrm{indeg}(v) = 2$, $\mathrm{outdeg}(v) = 1$ και $b = x_1 \cdot x_2$, όπου (u_i, g_i, x_i) (ή (u_i, x_i) εάν $u_i \in \{x_1, \ldots, x_n\}$) είναι η ετικέτα της $u_i \in V$, με $(u_i, v) \in E$, για $i = 1, 2$.

Το $\max\{r \in \mathbb{N} : \{v_1, \ldots, v_r\} \subseteq V$ και $(\forall i = 1, \ldots, r-1)[(v_i, v_{i+1}) \in E]\}$ (:μέγιστο μονοπάτι στο γράφημα) καλείται **βάθος** του λογικού κυκλώματος.

Αλγεβρική έκφραση: Ένα *λογικό κύκλωμα* είναι μία συνάρτηση της μορφής $B : \{0, 1\}^n \longrightarrow \{0, 1\}$, η οποία αποτελείται από τη σύνθεση της αλγεβρικής μορφής των λογικών πράξεων $\neg, \wedge$, η οποία είναι

$$\neg x := 1 - x \pmod 2 \qquad x \wedge y := xy \pmod 2 \qquad (x, y \in \{0, 1\})$$

Λογικά κυκλώματα σε ομάδες

Ορισμός 5.2.3. Έστω $B \equiv B(X_1, X_2, \ldots, X_n) : \{0, 1\}^n \longrightarrow \{0, 1\}$ ένα λογικό κύκλωμα και H μία ομάδα. Μία λέξη

$$h_1^{x_{l_1}} h_2^{x_{l_2}} \cdots h_m^{x_{l_m}}, \qquad h_1, h_2, \ldots, h_m \in G, \ \ l_1, l_2, \ldots, l_m \in \{1, 2, \ldots, n\} \tag{5.6}$$

καλείται **προσομοίωση μεγέθους** $m \in \mathbb{N}$ **του** B **στην** H εάν

$$\left(\exists h \in H \setminus \{1_H\}\right)\left(\forall (x_1, x_2, \ldots, x_n) \in \{0, 1\}^n\right)\left[h_1^{x_{l_1}} h_2^{x_{l_2}} \cdots h_m^{x_{l_m}} = h^{B(x_1, x_2, \ldots, x_n)}\right]$$

Επιλύσιμες ομάδες

Έστω μία ομάδα G. Η σειρά

$$\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

καλείται **επιλύσιμη** εάν για κάθε $i = 1, \ldots, n$, το πηλίκο $G_i \big/ G_{i-1}$ είναι αβελιανή ομάδα. Μία ομάδα καλείται **επιλύσιμη** εάν έχει επιλύσιμη σειρά, ειδ' άλλως καλείται **μη-επιλύσιμη**.

Θεώρημα 5.2.4 (Burnside). Μία ομάδα G, με $|G| = p^\alpha q^\beta$, για $p, q \in \mathbb{N}$ πρώτους αριθμούς και $\alpha, \beta \in \mathbb{N}_0$ είναι επιλύσιμη.

Στον αντίποδα, η συμμετρική ομάδα των 5 στοιχείων S_5, η εναλλάσσουσα υποομάδα σε 5 στοιχεία A_5 και η $SL(2, \mathbb{F}_5) := \{A \in \mathbb{M}_{2\times 2}(\mathbb{F}_5) : \det A = 1\}$ είναι μερικές *μη-επιλύσιμες* ομάδες.

Σε όσα έπονται, αντί για μια ''*μη-επιλύσιμη ομάδα*'' H, αρκεί $H = \mathrm{Sym}(5) := \{f : X \longrightarrow X \mid \eta\ f$ είναι 1–1 και επί και $\#X = 5\}$.

Οι David Mix Barrington, Howard Straubing και Denis Therien το 1990 απέδειξαν ότι:

Θεώρημα 5.2.5 ([BST$_{90}$]). Έστω H μια μη-επιλύσιμη ομάδα και B ένα λογικό κύκλωμα. Υπάρχει προσομοίωση (της μορφής (5.6)) του B στην H το μέγεθος τη οποίας είναι εκθετικό ως προς το βάθος του B.

Εν περιπτώσει όπου το βάθος του λογικού κυκλώματος $B : \{0,1\}^n \longrightarrow \{0,1\}$ είναι $\mathcal{O}(\log n)$, τότε το μέγεθος της προσομοίωσης που δίδει το Θεώρημα 5.2.5 είναι $n^{\mathcal{O}(1)}$.

Κρυπτογραφημένη προσομοίωση

Ορισμός 5.2.6. Έστω H μία πεπερασμένη και μη-τετριμμένη ομάδα και G μία πεπερασμένα παραγόμενη ομάδα. Το λογικό κύκλωμα B είναι **κρυπτογραφμένα προσομοιωμένο** (encrypted simulated) **ως προς τον επιμορφισμό** $f : G \twoheadrightarrow H$ εάν

$$(\exists g_1, \ldots, g_m \in G)\big(\exists h \in H \smallsetminus \{1_H\}\big)\big(\forall (x_1, \ldots, x_n) \in \{0,1\}^n\big)\left[f(g_1^{x_{l_1}} \cdots g_m^{x_{l_m}}) = h^{B(x_1,\ldots,x_n)}\right] \tag{5.7}$$

για $l_1, \ldots, l_m \in \{1, \ldots, n\}$ και $m \in \mathbb{N}$.

Κατά συνέπεια, με τη σημειογραφία του Ορισμού 5.2.6 έχοντας μία προσομοίωση της μορφής (5.6) για το λογικό κύκλωμα B στην H, τότε μπορεί να προκύψει μία κρυπτογραφημένη προσομοίωση του B επιλέγοντας τυχαία $g_1, \ldots, g_m \in G$, τέτοια ώστε $f(g_i) = h_i$, για $i = 1, \ldots, m$ [τοιουτοτρόπως η (5.7) επαληθεύεται].

Από τον συνδυασμό των Θεωρημάτων 5.2.2 και 5.2.5 προκύπτει το εξής:

Πόρισμα 5.2.7. *Έστω μία πεπερασμένη και μη-επιλύσιμη ομάδα H. Για κάθε ομομορφικό*[¶] *κρυπτοσύστημα $\mathcal{S}$ μεγέθους $N \in \mathbb{N}$ υπεράνω της H και κάθε λογικό κύκλωμα B βάθους $\mathcal{O}(\log N)$, μπορεί να σχεδιασθεί σε χρόνο $N^{\mathcal{O}(1)}$ μια κρυπτογραφημένη προσομοίωση του B υπεράνω του $\mathcal{S}$.*

Με τους συμβολισμούς του Ορισμού 5.2.6, η έννοια της *κρυπτογραφημένης προσομοίωσης* έγκειται στο γεγονός ότι δοθέντων των $g_1, \ldots, g_m \in G$, $h \in H \setminus \{1_H\}$, και της προσομοιωμένης κρυπτογράφησης (5.7), είναι υπολογιστικά δύσκολο να βρεθεί η τιμή του λογικού κυκλώματος $B : \{0,1\}^n \longrightarrow \{0,1\}$, καθ' ότι κάτι τέτοιο θα προϋπέθετε την γνώση της απάντησης εάν $f(g_1^{x_{l_1}} \cdots g_n^{x_{l_n}}) \overset{(5.7)}{=} h^{B(x_1,\ldots,x_n)} \overset{?}{=} 1_H$ ή ισοδύναμα $g_1^{x_{l_1}} \cdots g_n^{x_{l_m}} \overset{?}{\in} \ker f$ (διότι $B(x_1, \ldots, x_n) \in \{0,1\}$ κι άρα $h^{B(x_1,\ldots,x_n)} = 1_H$, για $B(x_1, \ldots, x_n) = 0$, ειδ' άλλως $h^{B(x_1,\ldots,x_n)} \neq 1_H$).

5.2.4 Εφαρμογές: Δύο διαδραστικά πρωτόκολλα

Ως πρωθύστερο των αποδείξεων μηδενικής γνώσης παρατίθενται τα κάτωθι διαδραστικά πρωτόκολλα που εκμαιεύονται από το Σχήμα 5.2. Θεωρούνται γνωστά: μία πεπερασμένη και μη-τετριμμένη ομάδα H, μία πεπερασμένα παραγόμενη ομάδα G, ένας επιμορφισμός $f : G \twoheadrightarrow H$ κι ένα ομομορφικό κρυπτοσύστημα $\mathcal{S} := \langle A, P, R \rangle$ [όρα Ορισμό 5.2.1].

Παρατήρηση 5.2.8. *Θεωρώντας (λογικά) κυκλώματα βάθους $\mathcal{O}(\log N)$, όπου $N \in \mathbb{N}$ είναι το μέγεθος του ομομορφικού κρυπτοσυστήματος $\mathcal{S}$, τότε οι παρακάτω εκδοχές υλοποιούνται σε χρόνο $N^{\mathcal{O}(1)}$.*

Αποτίμηση ενός κρυπτογραφημένου κυκλώματος:

Το πλαίσιο του πρωτοκόλλου συνίσταται στο εξής:

> Η Αλίκη γνωρίζει ένα λογικό κύκλωμα $B : \{0,1\}^n \longrightarrow \{0,1\}$ το οποίο και θέλει να κρατήσει μυστικό. Ο Βασίλης θέλει να λάβει γνώση της αποτίμησης $B(x_1, \ldots, x_n)$, για κάποιο $(x_1, \ldots, x_n) \in \{0,1\}^n$ το οποίο δεν επιθυμεί να αποκαλύψει.

[¶]υπό το πρίσμα του Ορισμού 5.2.1

Η στιχομυθία ανάμεσα στην Αλίκη και τον Βασίλη έχει ως εξής:

Αλίκη: Αποστέλλει στον Βασίλη μία κρυπτογραφημένη προσομοίωση ως προς τον επιμορφισμό $f : G \twoheadrightarrow H$ της μορφής (5.7), δηλαδή τα $g_1, \ldots, g_m \in G$ και $h \in H$.

Βασίλης: Αποστέλλει στην Αλίκη το $g := g_1^{x_{l_1}} \cdots g_m^{x_{l_m}} \in G$.

Αλίκη: Υπολογίζει και αποστέλλει στον Βασίλη το $f(g) = h^{B(x_1,\ldots,x_n)} \in H$.

Βασίλης: Επαληθεύει στην *πεπερασμένη* ομάδα H εάν $h^{B(x_1,\ldots,x_n)} = f(g) \stackrel{?}{=} h$ (κι άρα $B(x_1, \ldots, x_n) = 1$) ή εάν $h^{B(x_1,\ldots,x_n)} = f(g) \stackrel{?}{=} 1_H$ (κι άρα $B(x_1, \ldots, x_n) = 0$).

Αποτίμηση σε μια κρυπτογραφημένη είσοδο:

Αντί για λογικά κυκλώματα της μορφής $B : \{0,1\}^n \longrightarrow \{0,1\}$, εδώ θεωρούνται κυκλώματα υπεράνω της ομάδος H τα οποία είναι ''συναρτήσεις'' της μορφής $B_H : H^n \longrightarrow H$. Οι πράξεις που λαμβάνουν χώρα στα εν λόγῳ κυκλώματα είναι σύνθεση πράξεων ορισμένων στην H και αντί των τιμών $\{0,1\}$ το κύκλωμα κάνει χρήση των στοιχείων της H.

Το πλαίσιο του πρωτοκόλλου συνίσταται στο εξής:

> Ο Βασίλης έχει γνώση ενός κυκλώματος υπεράνω της H, το οποίο και δεν επιθυμεί να αποκαλύψει. Η Αλίκη επιθυμεί να υπολογίσει τη τιμή $B_H(y_1, \ldots, y_n) \in H$, για κάποιο $(y_1, \ldots, y_n) \in G^n$, το οποίο διατηρεί μυστικό.

Η στιχομυθία έχει ως ακολούθως:

Αλίκη: Αποστέλλει στον Βασίλη το $(z_1, \ldots, z_n) := \big(f(y_1), \ldots, f(y_n)\big) \in H^n$.

Βασίλης: Υπολογίζει την ''ανύψωση'' $f^{-1}(B_H) : G^n \longrightarrow G$ του $B_H : H^n \longrightarrow H$ ως εξής:

- κάθε στοιχείο του $h \in H$ στο B_H αντικαθίσταται από κάποιο $g \in G$, ώστε $f(g) = h$·
- κάθε πράξη στην H αντικαθίσταται από μία πράξη της G.

Αποστέλλει στην Αλίκη το $\big(f^{-1}(B_H)\big)(z_1, \ldots, z_n) \in G$.

Αλίκη: Υπολογίζει το $f\Big(\big(f^{-1}(B_H)\big)(z_1, \ldots, z_n)\Big) = B_H(y_1, \ldots, y_n) \in H$.

5.2.5 Σύνοψη

Οι Dima Grigoriev και Ilia Ponomarenko το 2003 στο [GP03] πρότειναν το Σχήμα 5.2 [το οποίο κάνει χρήση του Ορισμού 5.2.1]. Όπως αναφέρθηκε και στην §3.2.1 τα ομομορφικά κρυπτοσυστήματα -αν και ελατά- έχουν χρησιμότητα στην επίλυση κωδικοποιημένων λογικών κυκλωμάτων [όρα §5.2.4].

Τέλος, να σημειωθεί πως ο Ορισμός 5.2.1 δεν συνάδει με την θεώρηση που αναπτύσσεται στην §3.2.1 γεγονός που συνοψίζεται στην κάτωθι:

Παρατήρηση 5.2.9. *Το κρυπτοσύστημα Paillier [όρα §3.2] με τους συμβολισμούς του Ορισμού 5.2.1 συνίσταται στο* $\mathcal{S} = \langle A, P, R\rangle = \langle \mathbb{Z}^*_{n^2}, P(g) := g^n, R\rangle$, *με* $H = (\mathbb{Z}_n, +)$, $G = \mathbb{Z}^*_{n^2}$ *και* $\ker f = \{g^n \in G : g \in G\}$, *δεν είναι ομομορφικό κατά τον Ορισμό 5.2.1.*

Πράγματι, η συνθήκη (H4) του Ορισμού 5.2.1 δεν πληρείται από το κρυπτοσύστημα Paillier καθ΄ όσον όντας $|G| = |\mathbb{Z}^*_{n^2}| = \varphi(n^2) \leqslant n^2 = |(\mathbb{Z}_n, +)|^2 = |H|^2$, *τότε η συνάρτηση* $P(g) := g^n$ *αντιστρέφεται σε πολυωνυμικό χρόνο ως προς το* $|H|$*).*

Μέρος ΙΙ

Αποδείξεις μηδενικής γνώσης

Στην πράξη, οι χρήστες κάποιου δικτύου επιθυμούν την πρόσβαση σε κάποιο αγαθό ή υπηρεσία.

- Υπάρχει μία ουδέτερη πηγή που απολαμβάνει της εμπιστοσύνης των χρηστών, η οποία καλείται **κέντρο**, και τους προμηθεύει με *έξυπνες κάρτες*.
- Οι έξυπνες κάρτες διαδραματίζουν το ρόλο του αποδεικνύοντος και περιέχουν προσωπικές πληροφορίες του ιδιοκτήτη τους, ικανές για να τους προσδώσουν μοναδικότητα έναντι ενός άλλου χρήστη.
- Το ρόλο του επιβεβαιωτή διαδραματίζουν αυτόνομα (μη-εξαρτώμενα από το κέντρο) τερματικά που υποβάλουν σε δοκιμασίες τις κάρτες εν προκειμένῳ να επιτρέψουν την πρόσβαση στο αγαθό.

Ωστόσο, πρόβλημα δεν αποτελεί μόνον η διασφάλιση πως εγκεκριμένοι χρήστες θα έχουν πρόσβαση στο αγαθό. Επίσης, πρέπει να λαμβάνεται μέριμνα ώστε και ο χρήστης να είναι διασφαλισμένος έναντι οιασδήποτε υποκλοπής των στοιχείων του από έναν αντίπαλο που συνεργάζεται με τον επιβεβαιωτή. Αναλόγως του επιπέδου ασφαλείας διακρίνονται τα εξής σχήματα:

Σχήματα ταυτοποίησης (*identification schemes*): Ο Α μπορεί να αποδείξει στον Β πως πράγματι είναι ο Α, όμως ο Β δεν μπορεί να αποδείξει *σε κανέναν άλλον* πως είναι ο Α. [όρα Κεφάλαιο 6]

Σχήματα υπογραφών (*signature schemes*): Ο Α μπορεί να αποδείξει στον Β πως πράγματι είναι ο Α, όμως ο Β δεν μπορεί να αποδείξει *ούτε καν στον εαυτό του* πως είναι ο Α. [όρα Κεφάλαιο 4]

Σχήματα πιστοποίησης (*authentification schemes*): Ο Α μπορεί να αποδείξει στον Β πως πράγματι είναι ο Α, όμως *κανείς άλλος δεν μπορεί να αποδείξει στο* Β *πως είναι ο* Α. [όρα Κεφάλαιο 7]

Εφαρμογή αποδείξεων μηδενικής γνώσης γίνεται:

- στα διαβατήρια (ώστε να μην αντιγράφονται και να αναπαράγονται από εχθρικές κυβερνήσεις),
- στις πιστωτικές κάρτες (για να μην αντιγράφονται οι αριθμοί τους σε καινούργιες άδειες κάρτες),
- στους κωδικούς Η/Υ (για να αντέχουν ηλεκτρονικές επιθέσεις),
- στις στρατιωτικές εντολών και στα συστήματα ελέγχου (εν περιπτώσει που περιέλθουν σε εχθρική κατοχή).

Κεφάλαιο 6

Σχήματα Ταυτοποίησης

Εφαρμογές εμπορικής ή στρατιωτικής φύσεως απαιτούν τον εντοπισμό των εισβολέων σε πραγματικό χρόνο και την άρνηση της πρόσβασής τους στην παρεχόμενη υπηρεσία. Αυτός είναι ο σκοπός των σχημάτων ταυτοποίησης.

6.1 Το σχήμα ταυτοποίησης Fiat-Shamir

Οι Amos Fiat και Adi Shamir πρότειναν το 1986 στο [FS86] ένα σχήμα ταυτοποίησης καθώς κι ένα σχήμα υπογραφών [όρα §4.3].

6.1.1 Εγκατάσταση του δικτύου

Το κέντρο προβαίνει στις κάτωθι ενέργειες, με την αναγραφόμενη σειρά:

Αρχικές παράμετροι: Επιλέγονται ένα $n \in \mathbb{N}$ ο οποίος είναι γινόμενο δύο μεγάλων πρώτων αριθμών και μία συνάρτηση $f : S^\star \times \mathbb{N} \longrightarrow \mathbb{Z}_n$ η συμπεριφορά της οποίας προσομοιάζει την κανονική κατανομή.

Τα τερματικά: Το κέντρο κατανέμει τα τερματικά του στις υπηρεσίες του εν προκειμένῳ να ταυτοποιούν πως ο αιτών πρόσβαση στις υπηρεσίες του κέντρου, αποτελεί έναν έγκυρο χρήστη. Τα τερματικά:

- εκτελούν πράξεις υπόλοιπο $n \in \mathbb{N}$ και
- περιέχουν αλγοριθμική υλοποίηση της συνάρτησης $f : S^\star \times \mathbb{N} \longrightarrow \mathbb{Z}_n$.

Εγγραφή χρήστη: Όταν μία εγκεκριμένη (μέσῳ ελέγχου φυσικής παρουσίας) οντότητα αιτείται στο κέντρο για την χορήγηση μιας έξυπνης κάρτας, το κέντρο δημιουργεί ένα αλφαριθμητικό $I \in S^\star$ το οποίο περιέχει:

- προσωπικές πληροφορίες του χρήστη (ονοματεπώνυμο, διεύθυνση, αριθμός ταυτότητας, φυσική περιγραφή, αριθμός μητρώου ασφάλισης)
- πληροφορίες κάρτας (ημερομηνία λήξης, επίπεδο πρόσβασης κι άλλα).

Χορήγηση έξυπνης κάρτας: Το κέντρο προμηθεύει τους χρήστες με έξυπνες κάρτες που εκτελούν πράξεις υπόλοιπο $n \in \mathbb{N}$, περιέχουν το αλφαριθμητικό $I \in S^\star$ με τα προσωπικά δεδομένα του χρήστη, $(s_{j_1}, j_1), \ldots, (s_{j_k}, j_k) \in \mathbb{Z}_n \times \mathbb{N}$, όπου τα $j_1, \ldots, j_k \in \mathbb{N}$ είναι διακεκριμένα, με $(\forall s = 1, \ldots, k)[f(I, j_s) \mathscr{R} n]$ και s_{j_k} το πρώτο (στη διάταξη $0 \preceq 1 \preceq \ldots \preceq n-1$) $q \in \mathbb{Z}_n$ με $q^2 \equiv (f(I, j_k))^{-1} \mod n$.

6.1.2 Υλοποίηση του σχήματος

Αποδεικνύων (έξυπνη κάρτα)	Επιβεβαιωτής (τερματικό)
Αρχικά δεδομένα	
Η έξυπνη κάρτα εκτελεί πράξεις υπόλοιπο $n \in \mathbb{N}$, το αλφαριθμητικό $I \in S^\star$, τα ζεύγη $(s_{j_1}, j_1), \ldots, (s_{j_k}, j_k) \in \mathbb{Z}_n \times \mathbb{N}$.	Το τερματικό εκτελεί πράξεις υπόλοιπο $n \in \mathbb{N}$ και μία αλγοριθμική υλοποίηση της συνάρτησης $f : S^\star \times \mathbb{N} \longrightarrow \mathbb{Z}_n$.
Απόδειξη	
Ιδιωτικό κλειδί: $s_{j_1}, \ldots, s_{j_k} \in \mathbb{Z}_n$	
	$I \in S^\star$ και $j_1, \ldots, j_k \in \mathbb{N}$
	για $(\ell = 1, 2, \ldots, k)$ $v_\ell := f(I, j_\ell)$
για $(i = 1, 2, \ldots, t)$ **επανάλαβε:**	
	$e_{i1}, \ldots, e_{ik} \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{0, 1\}$
$(e_{i1}, e_{i2}, \ldots, e_{ik}) \in \{0, 1\}^k$	
$x_i := r_i^2 \mod n$, για $r_i \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathbb{Z}_n$	
$y_i := r_i \prod_{\ell=1}^{k} s_{j_\ell}^{e_{i\ell}} \mod n$	
	$x_i, y_i \in \mathbb{Z}_n$
	εάν $(x_i \not\equiv y_i^2 \prod_{\ell=1}^{k} v_{j_\ell}^{e_{i\ell}} \mod n)$ **τότε**
	επίστρεψε ''άρνηση πρόσβασης'';
	τερματισμός πρωτοκόλλου;
	αλλιώς εάν $(i = t)$ **τότε**
	επίστρεψε ''έγκυρος χρήστης'';
	τερματισμός πρωτοκόλλου;
	τέλος εάν

Σχήμα 6.1: Το σχήμα ταυτοποίησης Fiat-Shamir

Στο Σχήμα 6.1 αποδεικνύων προσπαθεί να πείσει τον επιβεβαιωτή πως κατέχει την γνώση των $s_{j_1}, \ldots, s_{j_k} \in \mathbb{Z}_n$ δίχως να τα αποκαλύψει.

Απόδειξη (Ορθότητας του Σχήματος 6.1). Εξ ορισμού ισχύει ότι

$$y_i^2 \prod_{\ell=1}^{k} v_{j_\ell}^{e_{i\ell}} = \left(r_i \prod_{\ell=1}^{k} s_{j_\ell}^{e_{i\ell}} \right)^2 \prod_{\ell=1}^{k} v_{j_\ell}^{e_{i\ell}} = r_i^2 \prod_{\ell=1}^{k} \left(s_{j_\ell}^2\right)^{e_{i\ell}} \prod_{\ell=1}^{k} v_{j_\ell}^{e_{i\ell}} =$$

$$= x_i \prod_{\ell=1}^{k} \left(s_{j_\ell}^2\right)^{e_{i\ell}} v_{j_\ell}^{e_{i\ell}} = x_i \prod_{\ell=1}^{k} \left(f(I, j_\ell)\right)^{-1} f(I, j_\ell) = x_i \quad \square$$

Δυφίο-προς-δυφίο πολυπλοκότητα του σχήματος ταυτοποίησης 6.1: Θέτοντας $k = 5$ και $t = 4$ ο μέσος αριθμός των πολλαπλασιασμών modulo n είναι $\frac{1}{2}t(k+2) = 14$. Ο αριθμός των δυφίων που ανταλλάσσονται από τις οντότητες κατά την ταυτοποίηση ανέρχεται στα 323 bytes (κι άρα η κάρτα μπορεί να περιέχει μία ROM των 320 byte. Για $k = 18$, $t = 2$ και τα διανύσματα $(e_{i1}, \ldots, e_{ik}) \in \{0,1\}^k$, $i = 1, 2$, έχουν το πολύ τρία 1 (υπάρχουν 988 τέτοια διανύσματα), τότε ο μέσος όρος των πολλαπλασιασμών modulo n είναι $7,8$.

6.1.2.Α΄ Παράμετροι του σχήματος

Παρατήρηση 6.1.1. Η έννοια του κέντρου μπορεί να εξαλειφθεί από το σχήμα ως εξής: Κάθε χρήστης επιλέγει το δικό του $n \in \mathbb{N}$ και το δημοσιοποιεί σε έναν κατάλογο δημοσίων κλειδιών.

- Εάν η συνάρτηση $f : S^\star \times \mathbb{N} \longrightarrow [0, n)$ απέχει από το να είναι (φαινομενικά) τυχαία, μπορεί το αλφαριθμητικό $I \in S^\star$ επιπλέον των στοιχείων που αναγράφονται παραπάνω, να περιέχει στο τέλος του μερικά τυχαία επιλεγμένα στοιχεία του S.
- Πρακτικά, $k \in \{1, \ldots, 18\}$. Όμως, μεγαλύτερες τιμές του $k \in \mathbb{N}$ μπορούν να μειώσουν την χρονική πολυπλοκότητα του σχήματος.
- $\lceil \log_2 n \rceil \geqslant 512$ (ήτοι το $n \in \mathbb{N}$ πρέπει να είναι ένας αριθμός από τουλάχιστον 512 δυφία), μιας και η παραγοντοποίηση ενός τόσο μεγάλου αριθμού φαντάζει δύσκολη για τις σημερινές υπολογιστικές δυνατότητες.
- Ένας αντίπαλος ο οποίος παρακολουθεί πολυωνυμικά πολλές αποδείξεις ανάμεσα σε έναν συγκεκριμένο χρήστη και τον επιβεβαιωτή δεν μπορεί να αποκτήσει κάποιο επί πλέον πλεονέκτημα: Εάν χρησιμοποιήσει τα ίδια $x_i \in \mathbb{Z}_n$ τα οποία έχει καταγράψει, τότε θα είναι σε θέση να επιτύχει πρόσβαση στο δίκτυο μόνον εάν ο επιβεβαιωτής αποστείλει το 0/1-διάνυσμα που είχε αποστείλει όταν ‘‘συνομιλούσε’’ με τον έγκυρο χρήστη. Επειδή κάθε $x_i \in \mathbb{Z}_n$ δεν επαναχρησιμοποιείται από τον έγκυρο χρήστη, ο αντίπαλος θα πρέπει να προβλέψει το διάνυσμα του επιβεβαιωτή. Συνεπώς, η

πιθανότητα επιτυχίας του αντιπάλου παραμένει 2^{-kt} (ανά φορά που υλοποιεί το πρωτόκολλο).

Παρατήρηση 6.1.2. *Η παράλληλη εκδοχή του Σχήματος 6.1 αποτελείται από ένα γύρο:*

(1) Ο αποδεικνύων αποστέλλει όλα τα $x_1, \ldots, x_t \in \mathbb{Z}_n$.
(2) Ο επιβεβαιωτής αποστέλλει όλα τα $0/1$*-διανύσματα που έχει επιλέξει.*
(3) Ο αποδεικνύων αποστέλλει όλα τα $y_1, \ldots, y_t \in \mathbb{Z}_n$.
(4) Ο επιβεβαιωτής επαληθεύει εάν $(\forall i = 1, \ldots, t)\left[x_i \equiv y_i^2 \prod_{\ell=1}^{k} v_{j\ell}^{e_{i\ell}}\right]$.

6.1.2.Β′ Ασφάλεια του σχήματος

Παρατήρηση 6.1.3. *Θεωρείται πως η παραγοντοποίηση της ισοτιμίας* $n = pq \in \mathcal{R}$ *απαιτεί χρόνο* $o(2^{kt})$.

Λήμμα 6.1.4. *Έστω ένας αντίπαλος ο οποίος δεν γνωρίζει τα μυστικά* $s_1, \ldots, s_k \in \mathbb{Z}_n$ *κι ούτε είναι σε θέση να υπολογίσει σε εφικτό χρόνο ουδένα γινόμενο της μορφής* $\prod_{j=1}^{k} v_j^{c_j} \pmod n$, *για* $(c_1, \ldots, c_k) \in \{-1, 0, 1\}^k \setminus \{(0, \ldots, 0)\}$. *Αν ο επαληθευτής ακολουθήσει το Σχήμα 6.1, ο αντίπαλος μπορεί να τον παραπλανήσει με πιθανότητα* 2^{-kt}.

Απόδειξη. Ο αντίπαλος μπορεί να παραπλανήσει τον επιβεβαιωτή προβλέποντας το $(e_{i1}, \ldots, e_{ik}) \in \{0, 1\}^k$ και να αποστείλει

$$x_i = r_i^2 \prod_{j=1}^{k} v_j^{e_{ij}} \pmod n \qquad\qquad y_i = r_i$$

Ωστόσο, η πιθανότητα μιας ορθής πρόβλεψης είναι 2^{-k}. Επαναλαμβάνοντας το πρωτόκολλο $t \in \mathbb{N}$ φορές, η πιθανότητα ώστε να παραπλανηθεί ο επιβεβαιωτής είναι 2^{-kt}.

Για να μπορέσει ο αντίπαλος να είναι αποτελεσματικότερος έναντι του (τίμιου) επιβεβαιωτή θα πρέπει να μπορεί σε κάθε έναν από τους $t \in \mathbb{N}$ γύρους, όταν αποστέλλει το $x_i \in \mathbb{Z}_n$, $i \in \{1, \ldots, k\}$, να μπορεί να επαληθεύσει εάν τα

$$\frac{x_i}{\prod_{j=1}^{k} v_j^{e_{ij}}} \qquad\qquad \frac{x_i}{\prod_{j=1}^{k} v_j^{d_{ij}}}$$

είναι τετραγωνικά υπόλοιπα και να τα υπολογίσει. Έστω πως οι υπολογισμοί δίδουν $y_\alpha, y_\beta \in \mathbb{Z}_n$ αντίστοιχα (παραπάνω είναι $(e_{i1}, \ldots, e_{ik}), (d_{i1}, \ldots, d_{ik}) \in \{0, 1\}^k$). Ο λόγος $y_\alpha / y_\beta \pmod n$ είναι της μορφής $\prod_{j=1}^{k} v_j^{c_j}$ και εξ υποθέσεως ο αντίπαλος δεν είναι σε θέση να τον υπολογίσει σε εφικτό χρόνο.

Συνεπώς, δεν γίνεται ένας αντίπαλος να παραπλανήσει έναν (τίμιο) επιβεβαιωτή με πιθανότητα καλύτερη από 2^{-kt}. □

Λήμμα 6.1.5. *Για δεδομένα* $k \in \mathbb{N}$ *και* $t \in \mathbb{N}$, *το Σχήμα 6.1 αποτελεί απόδειξη μηδενικής γνώσης.*

Απόδειξη (σκιαγράφηση). Κατά τη φάση της απόδειξης στο Σχήμα 6.1 δεν διαρρέεται πληροφορία για τα $s_1, \ldots, s_k \in \mathbb{Z}_n$. Πράγματι, σε κάθε γύρο $i = 1, \ldots, t$ κοινοποιείται το $y_i \in \mathbb{Z}_n$ στο οποίο η οποιαδήποτε διαρρέουσα πληροφορία για τα μυστικά $s_1, \ldots, s_k \in \mathbb{Z}_n$ αποσιωπάται με τον πολλαπλασιασμό με $r_i \in \mathbb{Z}_n$ το οποίο αποτελεί το τετραγωνικό υπόλοιπο ενός τυχαία επιλεγμενου $r_i \in \mathbb{Z}_n$. □

Άρα, το σχήμα 6.1 δεν είναι απροσπέλαστο. Υπάρχει πιθανότητα 2^{-kt} ένας επιτιθέμενος να καταφέρει να αποκτήσει πρόσβαση στο δίκτυο. Κατά συνέπεια το επίπεδο ασφαλείας του σχήματος εξαρτάται από τις παραμέτρους $k, t \in \mathbb{N}$.

- Για $k = 5$ (διαφορετικά τετραγωνικά υπόλοιπα) και $t = 4$ (επαναλήψεις) η παραπάνω πιθανότητα είναι 2^{-20}.
- Για (στρατιωτικούς σκοπούς επιλέγονται) $k = 6$ και $t = 5$ (κι έτσι) η παραπάνω πιθανότητα είναι 2^{-30}.

Συνεπώς, είναι πρακτικά αδύνατον να επιτύχει ο επιτιθέμενος να αποκτήσει πρόσβαση στο σύστημα. Κανείς δεν θα επιχειρούσε να εισέλθει σε στρατιωτική περιοχή έχοντας πιθανότητα 2^{-30} να ξεγελάσει το τερματικό. Ακόμη κι αν ο επιτιθέμενος επιχειρούσε 1000 φορές κάθε ημέρα ώστε να αποκτήσει παράτυπα πρόσβαση στο σύστημα με τον να δημιουργεί πλαστές κάρτες, θα του κόστιζε πάνω από 3000 έτη για να τα καταφέρει.

6.2 Το σχήμα ταυτοποίησης Feige-Fiat-Shamir

Το 1987 οι Uriel Feige, Amos Fiat και Adi Shamir στο [FFS87] πρότειναν ένα σχήμα ταυτοποίησης σύμφωνα μ΄ έναν πιο αυστηρό ορισμό μηδενικής γνώσης.

6.2.1 Εγκατάσταση του δικτύου

Ορισμός 6.2.1. Ο $4r + 3 \in \mathbb{Z}$, $r \in \mathbb{Z}$, καλείται **ακέραιος Blum**.

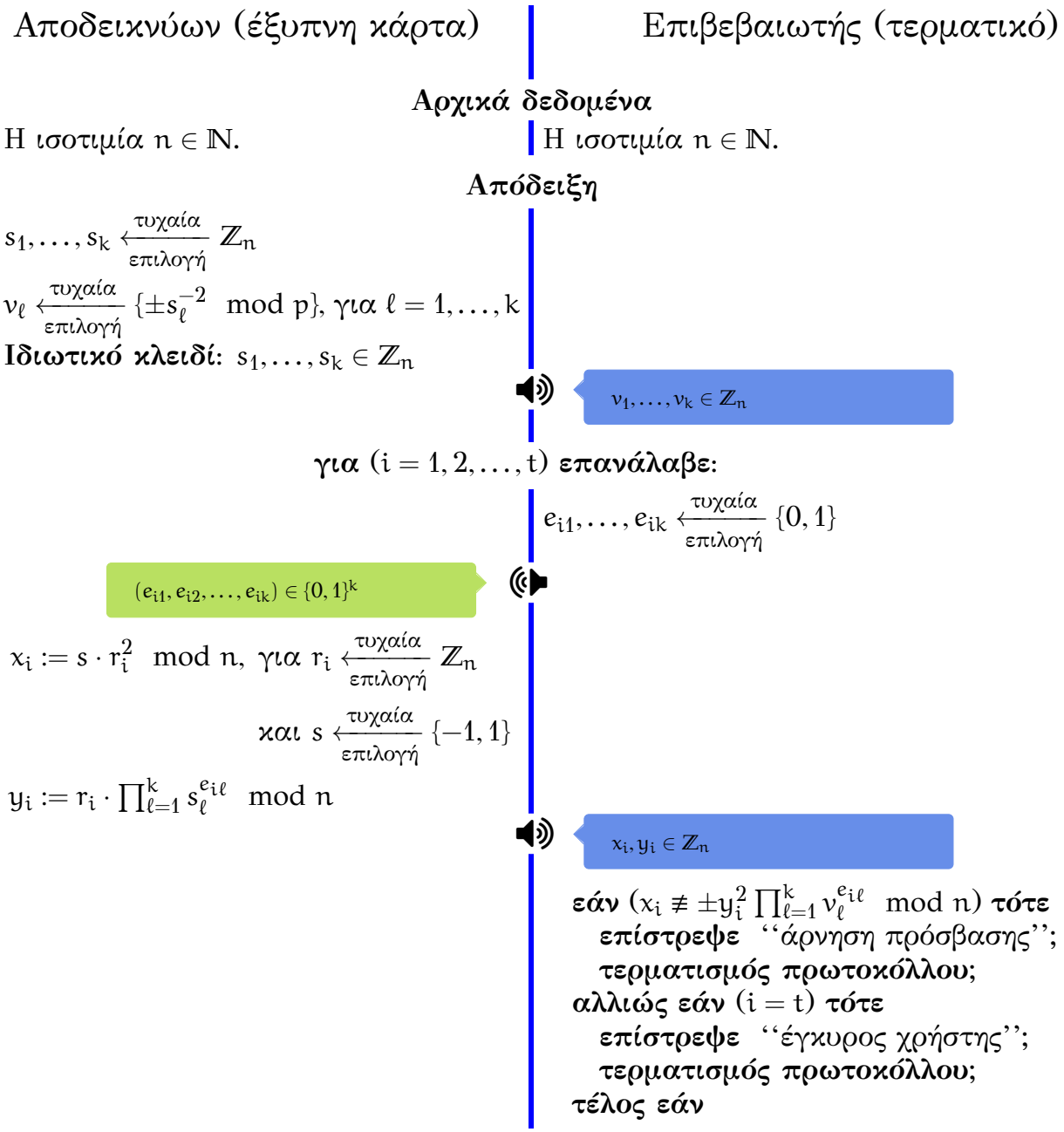
► Ο μοναδικός σκοπός του κέντρου είναι να δημοσιεύσει την ισοτιμία $n \in \mathbb{N}$ η οποία είναι γινόμενο δύο ακεραίων Blum οι οποίοι είναι πρώτοι αριθμοί.

Γνώρισμα ισοτιμιών όπως παραπάνω είναι πως έχει το $-1 \in \mathbb{Z}$ αποτελεί τετραγωνικό υπόλοιπο modulo n, το οποίο έχει σύμβολο Jacobi $\mathbf{J}(-1, n) = +1$.

Σε αντίθεση με το κρυπτοσύστημα RSA [όρα §3.1] όπου για κάθε δύο επικοινωνούσες οντότητες απαιτείται και καινούργια ισοτιμία, εδώ μπορούν όλοι οι χρήστες να γνωρίζουν την μία (κοινή) ισοτιμία $n \in \mathbb{N}$.

6.2.2 Υλοποίηση του σχήματος

Το ενθάδε σχήμα ταυτοποίησης αποτελεί τροποποίηση του Σχήματος 6.1: Εδώ ο αποδεικνύων μπορεί να αποδείξει στον επιβεβαιωτή ότι γνωρίζει εάν ένας συγκεκριμένος αριθμός είναι ή δεν είναι τετραγωνικό υπόλοιπο modulo n δίχως να αποκαλύψει τι ισχύει τελικά (πληροφορία που διέρρεε στο Σχήμα 6.1).



Σχήμα 6.2: Το σχήμα ταυτοποίησης Feige-Fiat-Shamir

Απόδειξη (Ορθότητας του Σχήματος 6.2). Με χρήση των ορισμών προκύπτει:

$$y_i^2 \cdot \prod_{\ell=1}^{k} v_\ell^{e_{i\ell}} = \left(r_i \cdot \prod_{\mu=1}^{k} s_\mu^{e_{i\mu}} \right) \cdot \prod_{\ell=1}^{k} v_\ell^{e_{i\ell}} = r_i^2 \cdot \prod_{\ell=1}^{k} (s_\ell v_\ell)^{e_{i\ell}} = \pm r_i^2 \equiv \pm x_i \pmod{n} \quad \square$$

6.2.3 Ασφάλεια του σχήματος

Οι Uriel Feige, Amos Fiat και Adi Shamir στο [FFS87] πρότειναν έναν πιο αυστηρό ορισμό της μηδενικής γνώσης ο οποίος απλοποιημένα έχει ως εξής:

Ορισμός 6.2.2. Έστω ζεύγος πιθανοτικών μηχανών Turing πολυωνυμικού χρόνου A (ο αποδεικνύων, που αποτελεί έναν έγκυρο χρήστη), $\tilde{B}$ (ο ανέντιμος επιβεβαιωτής, ο οποίος θέλει να παραστήσει αργότερα τον A). Ένα σχήμα αποδεικνύωντος/επιβεβαιωτή είναι **μηδενικής γνώσης** εάν κατ' όπιν της υλοποίησής του από τους $A, \tilde{B}$, ο $\tilde{B}$ μπορεί να αναπαράξει την επικοινωνία του με τον A μέσῳ μιας πιθανοτικής μηχανής Turing πολυωνυμικού χρόνου το αποτέλεσμα της οποίας δείχνει σαν οι αποκρίσεις να επιλέγονται τυχαία.

Με άλλα λόγια, ο ανέντιμος επιβεβαιωτής $\tilde{B}$ ακόμη και μέσῳ της διάδρασης μ' έναν έγκυρο χρήστη A, δεν μπορεί να χρησιμοποιήσει τη διάδραση αυτή ώστε να παραστήσει τον A.

Θεώρημα 6.2.3 ([FFS87], Θεώρημα 3). Έστω $n \in \mathbb{N}$ να είναι γινόμενο δύο ακεραίων Blum οι οποίοι είναι πρώτοι αριθμοί, $k = \mathcal{O}(\log\log n)$ και $t = \mathcal{O}(\log n)$.

(α') Εάν ένας αντίπαλος για το Σχήμα 6.2 μπορεί να ξεγελάσει έναν (τίμιο) επιβεβαιωτή με μη-αμελητέα πιθανότητα, τότε υπάρχει μηχανή Turing η οποία να παράγει τα μυστικά $s_1, \ldots, s_k \in \mathbb{Z}_n$ με συντριπτική πιθανότητα.

(β') Το Σχήμα 6.2 είναι μηδενικής γνώσης [σύμφωνα με τον Ορισμό 6.2.2].

Απόδειξη. (α') Όρα [FFS87, Θεώρημα 3].

(β') Ένας αντίπαλος μπορεί σε κάθε γύρω να ξεγελάσει τον επιβεβαιωτή με πιθανότητα 2^{-k} (προβλέποντας το διάνυσμα $(e_{i1}, \ldots, e_{ik}) \in \{0,1\}^k$). *Υπάρχει* μηχανή Turing η οποία προσομοιώνει την επικοινωνία ανάμεσα στον έντιμο αποδεικνύοντα A και τον ανέντιμο επιβεβαιωτή $\tilde{B}$ σε χρόνο $\mathcal{O}(t \cdot 2^k)$, ο οποίος -από τις υποθέσεις για τα $k, t \in \mathbb{N}$- είναι πολυωνυμικός ως προς το πλήθος των δυφίων του $v_j \in \mathbb{Z}_p$. Επί πλέον, επειδή:

- $(\forall v \in \mathbb{Z}_p)\left[J_p(v) = 1 \implies (\exists s \in \mathbb{Z}_p)[v \cdot s^2 \equiv \pm 1 \mod p]\right]$ και
- ο έλεγχος εάν $J_p(v) \stackrel{?}{=} 1$ γίνεται σε πολυωνυμικό χρόνο

προκύπτει πως το Σχήμα 6.2 είναι απόδειξη μηδενικής γνώσης σύμφωνα με τον Ορισμό 6.2.2. $\square$

6.2.4 Παράλληλη υλοποίηση

Κατά την παράλληλη εκτέλεση του Σχήματος 6.2 -όπως περιγράφεται στην Παρατήρηση 6.1.2- η πληροφορία η οποία μπορεί να αντλήσει ένας ανέντιμος επιβεβαιωτής $\tilde{\mathrm{B}}$ κατ΄ όπιν διαδράσεως με έναν έγκυρο χρήστη A φαίνεται πως είναι πολύ συγκεκριμένη και πως εν τέλει είναι μία γνώση η οποία δεν μπορεί να αξιοποιηθεί από τον $\tilde{\mathrm{B}}$ ώστε να επιτύχει τον στόχο του (να προσποιηθεί τον A).

Ασφάλεια

Ορισμός 6.2.4. Ένα πρωτόκολλο ανάμεσα στις οντότητες A (επιβεβαιωτής) και B (αποδεικνύων) λέγεται πως **αποκαλύπτει μη-μεταφερόμενη πληροφορία** αν:

- όταν αμφότερες οι οντότητες είναι εγκεκριμένοι χρήστες, τότε ο B αποδέχεται τον A με συντριπτική πιθανότητα και
- ένας ανέντιμος επιβεβαιωτής $\tilde{\mathrm{B}}$ κατ΄ όπιν πολυωνυμικά πολλών εκτελέσεων του πρωτοκόλλου με τον A, μπορεί να παραστήσει τον A με αμελητέα πιθανότητα.

Η παράλληλη υλοποίηση, παρ΄ ότι για τεχνικούς λόγους δεν μπορεί να χαρακτηρισθεί ως απόδειξη μηδενικής γνώσης, προσφέρει ένα ικανοποιητικό επίπεδο ασφαλείας. Στο [FFS87] αποδεικνύεται (βασικά κάτι ισχυρότερο από το παρακάτω):

Θεώρημα 6.2.5. Εάν η παραγοντοποίηση της ισοτιμίας $\mathrm{n} \in \mathbb{N}$ αποτελεί υπολογιστικά δύσκολο πρόβλημα, τότε η παράλληλη εκδοχή του σχήματος αυθεντικοποίησης αποκαλύπτει μη-μεταφερόμενη πληροφορία.

Παράμετροι υλοποίησης

Ένας μη εξουσιοδοτημένος χρήσης $\tilde{\mathrm{A}}$, μπορεί να αποκτήσει πρόσβαση στο δίκτυο με πιθανότητα $2^{-\mathrm{kt}}$, όπως προκύπτει από το Θεώρημα 6.2.3-(β΄). Αρκεί να τεθεί $\mathrm{kt} = 20$. Εν τοιαύτη περιπτώσει

> εάν $\tilde{\mathrm{A}}, \tilde{\mathrm{B}}$ είναι ένας ανέντιμος αποδεικνύων και ένας ανέντιμος επιβεβαιωτής οι οποίοι συνεργάζονται ώστε να πείσουν τον (έντιμο) επιβεβαιωτή B πως πρόκειται για τον (έγκυρο) χρήστη A,

τότε ο $\tilde{\mathrm{A}}$ έχει πιθανότητα $\leqslant 2^{-20}$ να πείσει τον B, αφού πρώτα ο $\tilde{\mathrm{B}}$ έχει υλοποιήσει 2^{20} φορές το πρωτόκολλο με τον A, εκτός εάν η παραγοντοποίηση της ισοτιμίας $\mathrm{n} \in \mathbb{N}$ επιτυγχάνεται σε λιγότερα από 2^{100} βήματα (πόρισμα από το Θεώρημα 5 στο [FFS87]).

Για επίπεδο ασφαλείας τάξης 2^{-20}, αρκεί να επιλεγούν $k = 5$ (μυστικοί αριθμοί) και $t = 4$ (γύροι της φάσης της απόδειξης). Ο μέσος όρος των πολλαπλασιασμών modulo n ανά οντότητα ανέρχεται σε $\frac{1}{2}(k+1)t \overset{k=5}{\underset{t=4}{=}} 12$, μέγεθος 1000 φορές μικρότερο από τους πολλαπλασιασμούς modulo n που απαιτεί το σχήμα RSA [όρα §3.1].

6.3 Το σχήμα ταυτοποίησης των Bardis-Markovskyi-Doukas-Drigas υπεράνω του $\mathrm{GF}(2^m)$

Θεώρηση του $\mathrm{GF}(2^m)$ με πολυώνυμα:

Έστω $m \in \mathbb{N}$. Το σώμα Galois $\mathrm{GF}(2^m) \equiv (\mathrm{GF}(2^m), \oplus, \otimes)$:

- $\mathrm{GF}(2^m) = \{f \in \mathbb{Z}_2[x] : \deg(f) \lneqq m\}$,
- η πράξη $\oplus : \mathrm{GF}(2^m) \times \mathrm{GF}(2^m) \longrightarrow \mathrm{GF}(2^m)$ είναι η πρόσθεση πολυωνύμων και η αναγωγή των συντελεστών του αποτελέσματος στο $\mathbb{Z}_2$ και
- η πράξη $\otimes : \mathrm{GF}(2^m) \times \mathrm{GF}(2^m) \longrightarrow \mathrm{GF}(2^m)$ είναι ο πολλαπλασιασμός πολυωνύμων, αναγωγή των συντελεστών του αποτελέσματος στο $\mathbb{Z}_2$ και η διαίρεση (πολυωνύμων) του αποτελέσματος με ένα ανάγωγο πολυώνυμο του $\mathrm{GF}(2^m)$.

Ορισμός 6.3.1. Ένα πολυώνυμο καλείται **ανάγωγο** εάν δεν μπορεί να γραφεί ως γινόμενο πολυωνύμων μικροτέρου βαθμού.

Στο $\mathbb{Z}_2[x]$ πάντοτε είναι εφικτό να βρει κανείς ένα ανάγωγο πολυώνυμο το οποίο είτε θα είναι της μορφής

$$x^m + x^a + 1$$

ή της μορφής

$$x^m + x^a + x^b + x^c + 1$$

για $m, a, b, c \in \mathbb{N}$, με $a, b, c \lneqq m$. Κατ' όπιν σταθεροποιείται το εν λόγω ανάγωγο πολυώνυμο και χρησιμοποιείται ώστε να παράξει το $\mathrm{GF}(2^m)$.

Παρατήρηση 6.3.2. *Διαφορετικά ανάγωγα πολυώνυμα του ιδίου βαθμού δίδουν ισόμορφες εικόνες του* $\mathrm{GF}(2^m)$.

Παράδειγμα 6.3.3. Έστω $m = 8$, $\alpha(x) = x^2+x+1 \in \mathbb{Z}_2[x]$, $\beta(x) = x^3+x+1 \in \mathbb{Z}_2[x]$. Το $p(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ είναι ανάγωγο (κι άρα παράγει το $\mathrm{GF}(2^8)$).

- $\alpha \oplus \beta = (x^2 + x + 1) \oplus (x^3 + x + 1) = x^3 + x^2 + 2x + 2 \pmod 2 \equiv x^3 + x^2$,
- $\alpha \otimes \beta = (x^2 + x + 1) \otimes (x^3 + x + 1) = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1 \pmod{p(x)} = x^5 + x^4 + 1 \pmod{p(x)} = x^5 + x^4 + 1$, όπου η τελευταία ισότητα ισχύει, διότι $\deg(x^5 + x^4 + 1) = 5 < 8 = \deg p(x)$. ⊣

Θεώρηση του $\mathrm{GF}(2^m)$ **με δυαδικές ακολουθίες**:

Συμβολισμός. Εφεξής θεωρούνται:

- η πράξη της *λογικής σύζευξης* $\cdot : \{0,1\}^m \times \{0,1\} \longrightarrow \{0,1\}^m$, όπου $x \cdot 1 = x$ και $x \cdot 0 = 0$·
- η πράξη της *αποκλειστικής διάζευξης* $\oplus : \{0,1\} \times \{0,1\} \longrightarrow \{0,1\}$, όπου $x \oplus y = 1$ εάν $x \neq y$, ειδ΄ άλλως $x \oplus y = 0$, η οποία επεκτείνεται (χρησιμοποιώντας το ίδιο σύμβολο) δυφίο-προς-δυφίο (bitwise) στις δυαδικές ακολουθίες·
- ως b^ν, για $b \in \{0,1\}$ και $\nu \in \mathbb{N}$, αναπαρίσταται η δυαδική ακολουθία αποτελούμενη από ν δυφία b·
- η πράξη της *αριστερής ολίσθησης* $\ll : \{0,1\}^\star \times \mathbb{N}_0 \longrightarrow \{0,1\}^\star$, με $x \ll n := x0^n$ (η $x \in \{0,1\}^\star$ ακολουθούμενη από n μηδενικά δυφία· ισοδυναμεί με πολλαπλασιασμό κατά 2^n του φυσικού με δυαδικό ανάπτυγμα x).

΄Εστω $m \in \mathbb{N}$. Το σώμα Galois $\mathrm{GF}(2^m) \equiv (\mathrm{GF}(2^m), \oplus, \otimes)$:

- $\mathrm{GF}(2^m) = \{0,1\}^m$,
- η πράξη $\oplus : \mathrm{GF}(2^m) \times \mathrm{GF}(2^m) \longrightarrow \mathrm{GF}(2^m)$ είναι η αποκλειστική διάζευξη δυφίο-προς-δυφίο και
- η πράξη $\otimes : \mathrm{GF}(2^m) \times \mathrm{GF}(2^m) \longrightarrow \mathrm{GF}(2^m)$ είναι ο πολλαπλασιασμός δυαδικών ακολουθιών δίχως μεταφορά κρατουμένου.

΄Εστω $m = 8$ και $p, q \in \mathrm{GF}(2^8)$, με $p = 111_2 \in \{0,1\}^8$ και $q = 1011_2 \in \{0,1\}^8$. Οι συνήθεις δυαδικές πράξεις θα έδιδαν:

- $7 + 11 = 111_2 + 1011_2 = 10011_2 = 16$ και
- για το αποτέλεσμα $7 \otimes 5 = 111_2 \otimes 011_2$, έχει κανείς:

$$\begin{array}{rr} & 111 \quad (\text{πολλαπλασιαστέος}) \\ \times & 1011 \quad (\text{πολλαπλασιαστής}) \\ \hline & 111 \quad (=111\ll 0) \\ & 1110 \quad (=111\ll 1) \\ & 00000 \\ + & 111000 \quad (=111\ll 3) \\ \hline \end{array}$$

κι άρα $7 \times 11 = 111_2 \times 1011_2 = 111_2 + 1110_2 + 111000_2 = 10101_2 + 111000_2 = 1001101_2 = 77$ ως αναμενόταν. Εδώ σημειώνεται ο τύπος του πολλαπλασιασμού δυαδικών ακολουθιών $U, (\nu_1\, \nu_2\, \cdots\, \nu_m) \in \{0,1\}^m$:

$$U \times (\nu_1\, \nu_2\, \cdots\, \nu_m)_2 = (U \cdot \nu_1) + \big((U \cdot \nu_2) \ll 1\big) + \ldots + \big((U \cdot \nu_m) \ll (m-1)\big)$$

ήτοι λαμβάνονται υπ΄ όψιν οι ολισθήσεις του πολλαπλασιαστέου όπου το δυφίο του πολλαπλασιαστή ισούται με 1.

Ωστόσο στο σώμα Galois $\mathrm{GF}(2^8)$ οι πράξεις συνίστανται ως εξής:

- *αποκλειστική διάζευξη*: $7 \oplus 5 = 111_2 \oplus 1011_2 = 1100_2 = 12$·
- *πολλαπλασιασμός δίχως τη μεταφορά κρατουμένου:* ο οποίος είναι όπως ο συνήθης (δυαδικός) πολλαπλασιασμός, απλώς κάνει χρήση της αποκλειστικής διάζευξης, δηλαδή $7 \otimes 5 = 111_2 \otimes 1011_2 = 111_2 \oplus 1110_2 \oplus 111000_2 = 1001_2 \oplus 111000_2 = 110001_2 = 49$.

Συνεπώς, ''ξεχνώντας τα κρατούμενα'', για $U, \{v_1, \ldots, v_m\} \in \{0,1\}^m$ ο πολλαπλασιασμός δίχως μεταφορά κρατουμένου ορίζεται ως:

$$U \otimes (v_1\, v_2 \ldots v_m)_2 = (U \cdot v_1) \oplus \big((U \cdot v_2) \ll 1\big) \oplus \cdots \oplus \big((U \cdot v_m) \ll (m-1)\big)$$

Ύψωση σε δύναμη και αριθμητική υπολοίπων στο $\mathrm{GF}(2^m)$:

Παρατήρηση 6.3.4. *Κάθε πολυώνυμο χαρακτηρίζεται από τους συντελεστές του. Έτσι κάθε δυαδική ακολουθία μήκους* m *ορίζει ένα δυαδικό πολυώνυμο βαθμού* $m-1$.

[Επί παραδείγματι $1011_2 \rightsquigarrow x^3 + 0x^2 + x + 1 = x^3 + x + 1$*.]*

Συμβολισμός. Επεκείνεται η πράξη του ''λογικού και'' σε δυαδικές ακολουθίες ως $\cdot : \{0,1\}^s \times \{0,1\}^t \longrightarrow \{0,1\}^{\max\{s,t\}}$ όπου $a \cdot b$ να είναι η δυαδική ακολουθία που αντιστοιχεί στο γινόμενο των πολυωνύμων που αντιστοιχούν στις a, b.

Παρακάτω είναι: $\mathrm{GF}(2^m) = \{f \in \mathbb{Z}_2[x] : \deg(f) \lneqq m\} = \{0,1\}^m = \{0, 1, \ldots, 2^m - 1\}$, $m \in \mathbb{N}$, $A = (a_1\, a_2 \cdots a_\ell)_2, B \in \mathrm{GF}(2^m)$, $\ell \leqslant m$, $E = (e_1\, e_2 \ldots e_s)_2 \in \mathbb{N}$ και $n \in \mathbb{N}$.

Το υπόλοιπο του A ως προς M, συμβολίζεται ως $A \bmod n$ και είναι το αποτέλεσμα $A_p \mod n_p$, όπου τα $A_p, n_p \in \mathbb{Z}_2[x]$ είναι τα πολυώνυμα των αριθμών A, n αντιστοίχως.

Η δύναμη με βάση A και εκθέτη E υπολογίζεται ως συνήθως: προσπελάζονται τα δυφία του εκθέτη από τα δεξιά προς τα αριστερά (στην πράξη ήθισται από τα αριστερά προς τα δεξιά):

1: $R \leftarrow 1$;
2: **για** $(j = \ell$ **έως** 1 **με βήμα** $-1)$
3: **εάν** $(e_j = 1)$ **τότε** $R \leftarrow (R \otimes A) \bmod n$;

κι άρα ο αλγόριθμος χρειάζεται $\mathrm{hw}(E) \in \mathbb{N}$ (βάρος Hamming) πράξεις $\otimes$.

6.3.1 Εφαρμογή του σχήματος ταυτοποίησης των Bardis-Markovskyi-Doukas-Drigas στο Σχήμα 6.2 (FFS)

Ακολουθεί το Σχήμα 6.2 για $k = 1$ πρόκληση του επιβεβαιωτή ανά γύρο, υλοποιημένο στο $\mathrm{GF}(2^m)$ κατά τους N. Bardis, N. Doukas, A. Drigas και Oleksandr Markovskyi το 2012 από το [BMDD12]. Τα δεδομένα στις αγκύλες αποτελούν παράδειγμα υλοποίησης.

Αποδεικνύων	Επιβεβαιωτής

Δημοσίως γνωστά: Υλοποίηση στο $\mathrm{GF}(2^m)$ [έστω $m = 4$] με ισοτιμία $n \in \mathbb{N}$ [έστω $n = 11001_2 = 25$ η οποία αντιστοιχεί στο ανάγωγο υπεράνω του $\mathrm{GF}(2^4)$ πολυώνυμο $x^4 + x^3 + 1$].

Φάση αρχικοποιήσεων

$\theta \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{0,1\}^m$ $[\theta := 4]$

Υπολογισμός $\theta \otimes n \oplus 1 \in \{0,1\}^{2m-1}$
$[4 \otimes 24 \oplus 1 = 101]$

Ανάλυση σε: $\theta \otimes n \oplus 1 = d \otimes s$, για $d, s \in \{0,1\}^m$
$[d \otimes s = 9 \otimes 13 = 101 = \theta \otimes n \oplus 1]$

$\nu := d\big|^2 \bmod n$ και $\nu^{-1} := s\big|^2 \bmod n$
$[\nu = 9 \otimes 9 \bmod 25 = 14$ και $\nu^{-1} = 13 \otimes 13 \bmod 25 = 7]$

Κλειδιά: ιδιωτικό: s, δημόσιο: d

Αποστολή δημοσίου κλειδιού d → Παραλαβή δημοσίου κλειδιού d

Φάση πιστοποίησης

$r \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathbb{N}$ $[r := 10]$

Αποστολή $x := r\big|^2 \bmod n$
$[x := 10 \otimes 10 \ (\mathrm{rem}\ 25) = 11]$ → Παραλαβή του x

Φάση διαπίστευσης (επανάληψη $t \in \mathbb{N}$ φορές)

$e \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{0,1\}$

Παραλαβή πρόκλησης $e \in \{0,1\}$ ← Αποστολή πρόκλησης $e \in \{0,1\}$

εάν $(e = 0)$ **τότε**
  Στείλε r
αλλιώς
  Στείλε $y := r \otimes s \bmod n$
τέλος εάν → Παραλαβή διαπίστευσης

εάν $(e = 0 \wedge d = r\big|^2 \bmod n)$ **τότε**
  έγκυρος χρήστης
αλλιώς εάν$(e = 1 \wedge \wedge d = y\big|^2 \otimes \nu \bmod n)$ **τότε**
  έγκυρος χρήστης
αλλιώς
  άρνηση πρόσβασης
τέλος εάν

Βελτιωμένος αλγόριθμος πολλαπλασιασμού:

Θεώρημα 6.3.5. Για $A \in GF(2^m)$, $m \in \mathbb{N}$, με 2δική αναπαράσταση $(a_1\, a_2 \cdots a_\ell)_2$, $1 \leqslant \ell \leqslant m$, και $E = 2^k$, $k \in \mathbb{N}_0$, ισχύει ότι $A\big|^E = a_1 + a_2 \cdot 2^E + a_3 \cdot 2^{2\cdot E} + \ldots + a_\ell \cdot 2^{(\ell-1)\cdot E}$.

Για $A, B \in GF(2^m)$ και $n \in \mathbb{N}_0$, από το Θεώρημα 6.3.5 εκμαιεύονται τα εξής:

- ο υπολογισμός του $A|^2 \in GF(2^m)$ επιτυγχάνεται παρεμβάλοντας ανάμεσα σε δύο διαδοχικά δυφία της δυαδικής αναπαράστασης του A ένα 0, [επί παραδείγματι $A = 1011_2 \rightsquigarrow A|^2 = \mathbf{1000101}_2$ στο $GF(2^m)$]
- $A|^E \text{ rem } n = (T_1 \cdot a_1) + (T_2 \cdot a_2) + \ldots + (T_\ell \cdot a_\ell)$, όπου $T_i := 2^{(i-1)\cdot E} \text{ rem } n$. [Ο Akram Moustafa το 2014 στο [Mou14] πρότεινε έναν δικό του τρόπο.]

Στο [BMDD12] προτείνεται ένας αποδοτικός αλγόριθμος υπολογισμού τετραγώνου σε αριθμητική υπολοίπων που αφορά την υλοποίηση του Σχήματος 6.2 στο $GF(2^m)$: $A|^2 \otimes B \text{ rem } n = (V_1 \cdot a_1) \oplus (V_2 \cdot a_2) \oplus \cdots \oplus (V_\ell \cdot a_\ell)$, με $V_i := B \cdot 4^{i-1} \text{ rem } n$. Συνεχίζουν γενικεύοντας το παραπάνω και παραθέτουν έναν πιο αποτελεσματικό αλγόριθμο για τον υπολογισμό του $A|^E \otimes B \text{ rem } n$, ο οποίος χρησιμοποιεί 1 έως 4 δυφία (της δυαδικής αναπαράστασης) του E και τις τιμές: $V_i := B \cdot 4^{i-1} \text{ rem } n$, $W_i := B \cdot 16^{i-1} \text{ rem } n$, $U_i = 16^{i-1} \text{ rem } n$ και $Y_i := 256^{i-1} \text{ rem } n$ καταλλήλως.

Παρατήρηση 6.3.6. *Οι υπολογισμοί γίνονται γρηγορότερα, εάν βρεθούν εκ προοιμίου οι τιμές* $T_1, \ldots, T_\ell$, $V_1, \ldots, V_\ell$, *(και* $W_1, \ldots, W_\ell$, $U_1, \ldots, U_\ell$, $Y_1, \ldots, Y_\ell$*).*

6.4 Το σχήμα ταυτοποίησης Stavroulakis σε Boolean άλγεβρες με μονόδρομες συναρτήσεις κατακερματισμού

Θεωρείται μία διαδικασία $F(X)$ όπου:

(α′) η αντίστροφη διαδικασία $\Phi(X)$ της $F(X)$ είναι απεικόνιση πολλά-προς-ένα, ήτοι υπάρχει σύνολο Ω, ώστε $(\forall Q, G \in \Omega)[Q \neq G \implies F(Q) = F(G) = U]$ και

(β′) ο υπολογισμός των κωδικών (:στοιχεία του Ω) απαιτεί κατανάλωση μικρής ποσότητας υπολογιστικών πόρων για εγκεκριμένους χρήστες και για τους εισβολείς απαιτείται μεγάλη υπολογστική ισχύς ώστε να τους υπολογίσουν.

Για τον ορισμό ενός boolean μετασχηματισμού $F : \{0,1\}^n \longrightarrow \{0,1\}^n$ αρκεί να ορισθεί η τιμή $Y = F(X)$, για κάθε $X = \{x_1, x_2, \ldots, x_n\} \in \{0,1\}^n$. Έτσι γράφοντας $F(X) = Y = \{y_1, \ldots, y_n\}$, όπου $y_1, \ldots, y_n \in \{0,1\}$ μπορεί να θεωρηθεί πως υπολογίζεται από μία συνάρτηση $f_i : \{0,1\}^n \longrightarrow \{0,1\}$, ως $y_i = f_i(X)$, για $i = 1, \ldots, n$. Συνεπώς, $F(X) = \{f_1(X), \ldots, f_n(X)\}$ κι άρα για τον ορισμό της $F : \{0,1\}^n \longrightarrow \{0,1\}^n$, αρκεί να ορισθούν οι $f_1, \ldots, f_n : \{0,1\}^n \longrightarrow \{0,1\}$.

Υπάρχουν τρεις τρόποι ώστε να αναπαρασταθεί ένας boolean μετασχηματισμός: 1. με χρήση πινάκων αληθείας, 2. σε αλγεβρική κανονική μορφή και 3. ως

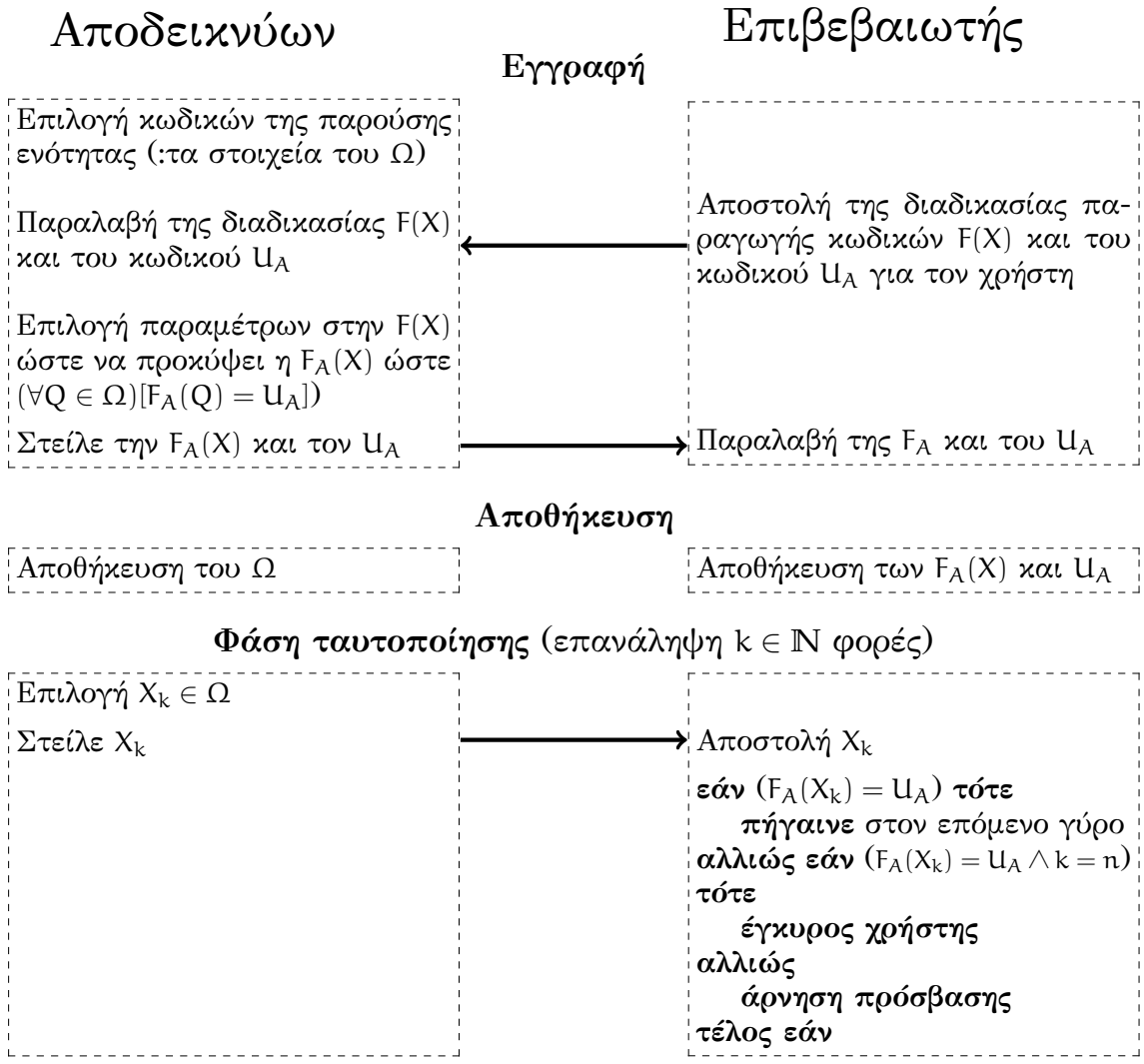
μια διαδικασία (έναν αλγόριθμο που υπολογίζει το Y δεδομένου του X). Σε κρυπτογραφικά θέματα χρησιμοποιείται ο τελευταίος τρόπος αναπαράστασης.

Η δομή υπολογισμού του $F(X)$ έχει ως ακολούθως:

1. η εισόδος των n δυφίων χωρίζεται σε h μέρη μήκους k δυφία έκαστος·
2. τα μέρη υποβάλονται σε γύρους όπου καθείς τους αποτελείται από την εφαρμογή μη-γραμμικών boolean μετασχηματισμών και συνδυασμό των αποτελεσμάτων τους.

Ορίζονται οι μετασχηματισμοί $\varphi_\ell : \{0,1\}^k \to \mathbb{N}$, με $\varphi_\ell(\{d_1, d_2, \ldots, d_k\}) := \sum_{j=1}^{k} d_j 2^{j-1}$, για $\ell = 1, \ldots, h$ (οι δεκαδικοί αριθμοί που αντιστοιχούν στα στοιχεία του $\{0,1\}^k$).

Σε ένα αφαιρετικό επίπεδο, ένα σχήμα ταυτοποίησης δίνεται ως εξής:

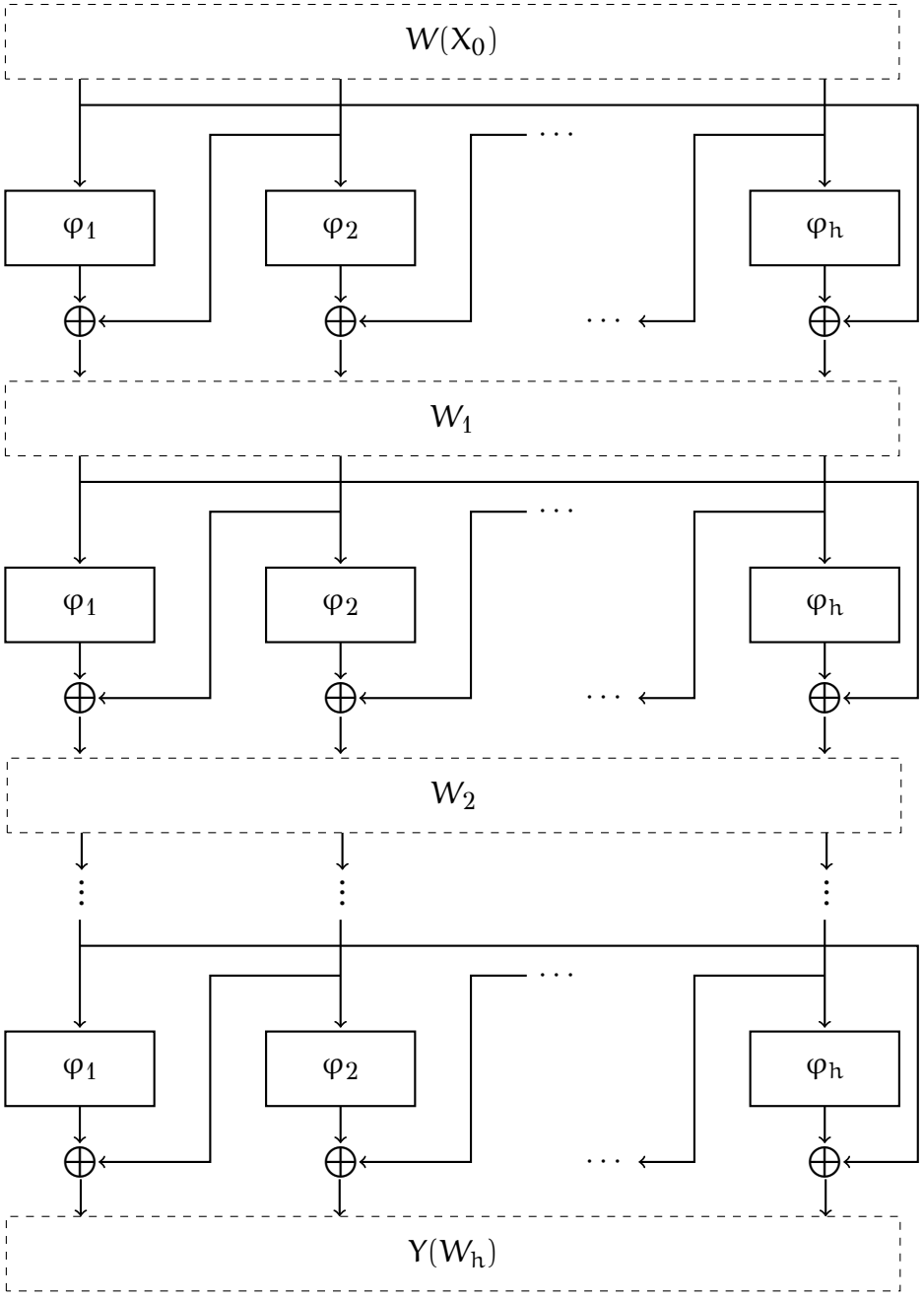


Σχήμα 6.3: Το σχήμα του P. Stavroulakis για ταυτοποίηση με μηδενική γνώση των χρηστών με σύστημα με βάση Boolean μετασχηματισμούς

Δύο μέθοδοι παραγωγής της $F(X)$ και του Ω δίνονται από τους:

- N. Bardis, N. Doukas και O. P. Markovskyi το 2010 στο [BDM10],
- P. Stavroulakis, O. P. Markovskyi, N. Bardis και N. Doukas το 2011 στο [SMBD11].

Οι ως άνω εισηγητές προτείνουν το εξής σχήμα για τη διαδικασία $F(X)$:



Σχήμα 6.4: Διαδικασία σύνθεσης Boolean μονόδρομου μετασχηματισμού

Θεωρείται ως W_q, $q = 0, 1, \ldots, h$, η έξοδος του κάθε γύρου του σχήματος που προηγείται. Ως Z_{qi}, $i = 1, 2, \ldots, h$ συμβολίζεται το τμήμα των δυφίων $(i-1)k+1$ έως και ik της W_q, ήτοι $W_q = (Z_{q1}, Z_{q2}, \ldots, Z_{qh})$. Ο υπολογισμός $Y = F(X)$ αντιστοιχεί στην παραπάνω διαδικασία ως $W_0 = X$ και $W_h = Y$. Οι εξισώσεις που διέπουν την παραπάνω διαδικασία είναι οι εξής:

$$Z_{0,j} = (x_{(i-1)k+1}, x_{(i-1)k+2}, \ldots, x_{ik}) \qquad (i = 1, 2, \ldots, h)$$

$$Z_{qg} = \varphi_j(Z_{q-1,g}) \oplus Z_{q-1,g+1} \qquad (q = 1, 2, \ldots, h,\ g = 1, 2, \ldots, h-1)$$

$$Z_{sh} = \varphi_h(Z_{s-1,h}) \oplus Z_{q-1,1} \qquad (s = 1, 2, \ldots, h)$$

Συνοψίζοντας, για τη δημιουργία ενός σχήματος ταυτοποίησης όπως στο Σχήμα 6.3, πρέπει να συμβούν τα παρακάτω:

(α′) Θεμελίωση του μετασχηματισμού $F : \{0,1\}^n \longrightarrow \{0,1\}^n$ ως πίνακα των boolean μετασχηματισμών $\phi_1, \phi_2, \ldots, \phi_h : \{0,1\}^k \longrightarrow \mathbb{N}$.

(β′) Επιλογή* του συνόλου κωδικών $\Omega = \{X_1, X_2, \ldots, X_m\}$ για τα οποία θα ισχύει $(\forall Q \in \Omega)[F(Q) = Y]$.

*Αλγόριθμοι για την παραγωγή του Ω εμπεριέχονται στα [BDM10, SMBD11]

Κεφάλαιο 7

Σχήματα Πιστοποίησης

Ο κύριος στόχος ενός σχήματος πιστοποίησης είναι να επιτρέψει σε δύο εγκεκριμένους χρήστες ενός δικτύου να αποδείξουν ο ένας στον άλλον το γνήσιον της ταυτότητός τους, δεδομένου ότι η επικοινωνία τους διαδραματίζεται σε ένα ανασφαλές κανάλι επικοινωνίας. Τα σχήματα πιστοποίησης χρησιμεύουν όταν ο αποδεικνύων A και ο επαληθευτής B συνεργάζονται εναντίον εξωγενών απειλών.

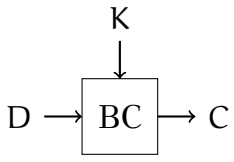
7.1 Το σχήμα πιστοποίησης Bardis-Doukas-Markovskyi

Αλγόριθμος τμήματος (block cipher): είναι ένας αιτιοκρατικός συμμετρικός κρυπταλγόριθμος ο οποίος χωρίζει το απλό κείμενο σε τμήματα (blocks) ιδίου μήκους, τα οποία κρυπτογραφεί με τον ίδιο μετασχηματισμό.

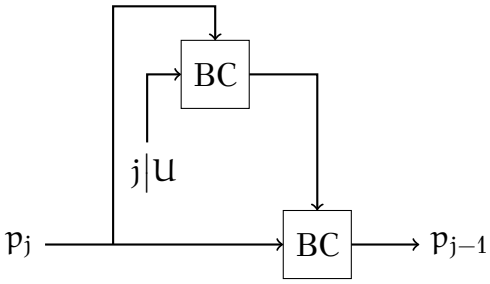
Έστω $\mathcal{E} : \mathscr{M} \times \mathscr{K} \longrightarrow \mathcal{C}$ και $\mathcal{D} : \mathcal{C} \times \mathscr{K} \longrightarrow \mathscr{M}$ οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης ενός αλγορίθμου τμήματος, όπου $\mathscr{M}, \mathcal{C}, \mathscr{K}$ είναι ο χώρος των απλών κειμένων, των κρυπτοκειμένων και των κλειδιών αντίστοιχα. Σημειώστε πως οι αλγόριθμοι τμήματος είναι συμμετρικά σχήματα. Κατά συνέπεια, το κλειδί της κρυπτογράφησης ταυτίζεται με εκείνο της αποκρυπτογράφησης.

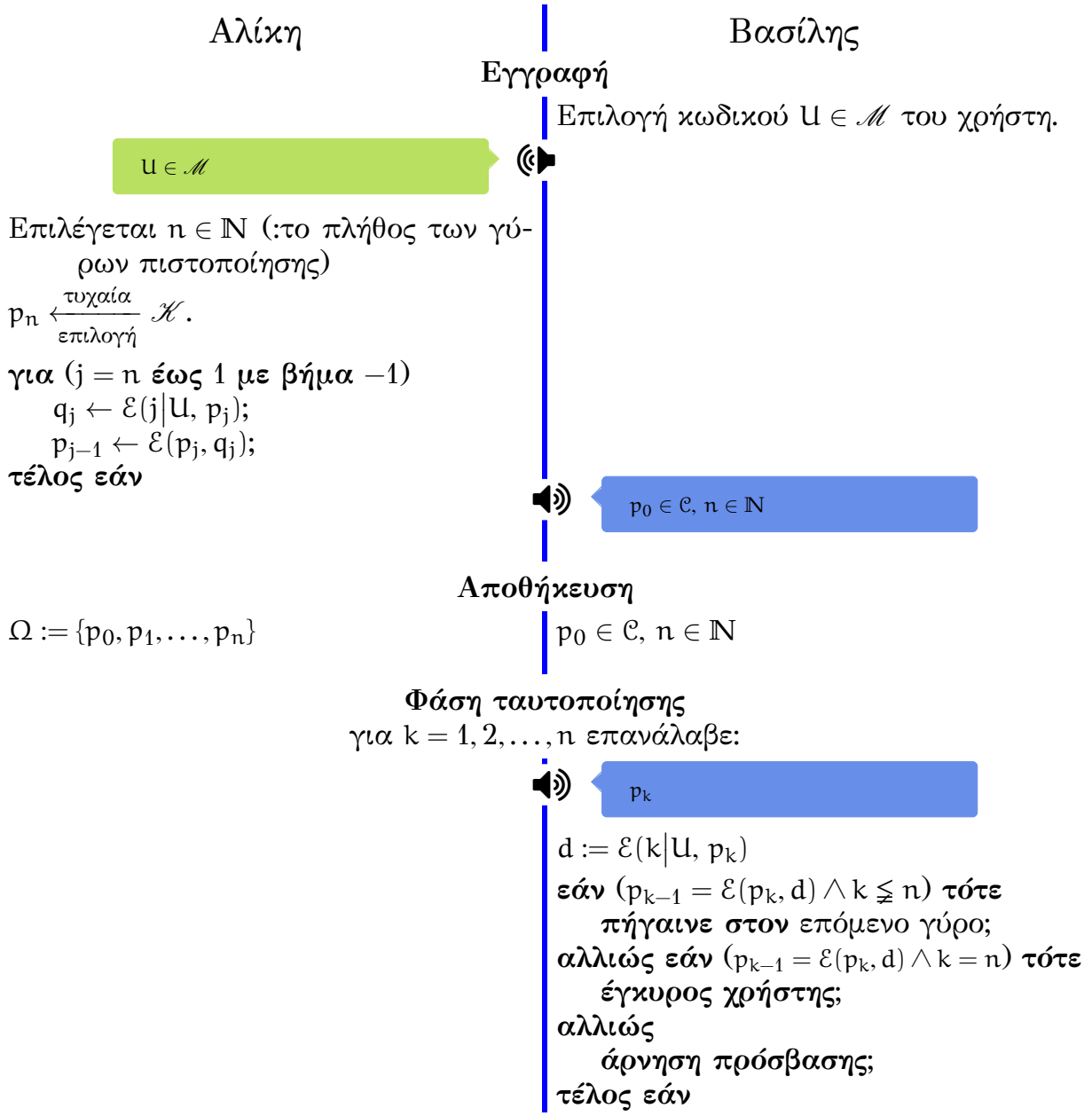
Πιστοί στο Σχήμα 6.3 οι Nikolaos Bardis, Nikolaos Doukas και Oleksandr Markovskyi το 2017 στο [BDM17] προτείνουν τα εξής:

- Η διαδικασία F(X) είναι ένας αμοιβαία συμφωνημένος αλγόριθμος τμήματος BC ο οποίος λαμβάνει το απλό κείμενο D και το κλειδί K και επιστρέφει το κρυπτοκείμενο C. Στο [BDM17] προτείνεται ο αλγόριθμος τμήματος Rijndael (ή αλλιώς: AES).



- Η παραγωγή των κωδικών της συνδερίας $p_n, p_{n-1}, \ldots, p_1, p_0$ -ήτοι τα στοιχεία του Ω- υλοποιείται με την υλοποίηση $n \in \mathbb{N}$ γύρων της διπλανής μορφής όπου ως $j|u$ συμβολίζεται η παράθεση των j, u και ο πρώτος κωδικός p_n έχει επιλεγεί τυχαία.





Σχήμα 7.1: Το σχήμα πιστοποίησης των Bardis-Doukas-Markovskyi

Απόδειξη (Ορθότητας Σχήματος 7.1). Έστω $j \in \{1, 2, \ldots, n\}$. Η Αλίκη έχει υπολογίσει: $p_{j-1} = \mathcal{E}(p_j, q_j) = \mathcal{E}\big(p_j, \mathcal{E}(j\big|U, p_j)\big)$, για $1 \leqslant j \leqslant n$. Ο Βασίλης υπολογίζει $p_{j-1} = \mathcal{E}(p_j, d)$, όπου $d = \mathcal{E}(j\big|U, p'_j)$, όπου p'_j είναι το στοιχείο που έλαβε από την Αλίκη(;). Συνεπώς, ο Βασίλης προχωράει στον επόμενο γύρο εάν το p'_j είναι το αληθινό p_j που χρησιμοποίησε η Αλίκη κατά την εγγραφή. □

7.1.1 Ασφάλεια

Ασφάλεια έναντι εξωτερικών απειλών:

Ένας επιτιθέμενος για το Σχήμα 7.1 (δηλαδή κάποια οντότητα που προσπαθεί να συστηθεί ως Αλίκη στον Βασίλη) πραγματοποιεί την επίθεσή του κατά τη φάση της ταυτοποίησης με στόχο:

- την εύρεση του p_{j-1}, βασιζόμενος στην προϊστορία $p_{j-2}, \ldots, p_0$.

Κατά συνέπεια,

- πρέπει να ευρεθούν λ, μ, τέτοια ώστε $p_{j-1} = \mathcal{E}(\lambda, \mu)$ και $\mu = \mathcal{E}(\alpha, \lambda)$, με το α να είναι άγνωστο.

Μία τέτοια προσπάθεια θα απαιτούσε εξαντλητική αναζήτηση ώστε να βρεθούν οι τιμές α, λ.

> Ο όγκος των δοκιμών της παραπάνω εξαντλητικής αναζήτησης -όπου ως BC είναι ο αλγόριθμος Rijndael με κλειδί 256 δυφίων- είναι $2^{256+L(U)}$, για $L(U)$ να είναι το μήκος του κωδικού U.

Συνεπώς, οι υπολογιστικοί πόροι που χρειάζεται ο υπολογισμός του p_{j-1} είναι οι διπλάσιοι από το να διαρραγεί ο αλγόριθμος BC.

Ασφάλεια έναντι στον ανέντιμο επιβεβαιωτή:

Έστω $j \in \{1, \ldots, n\}$. Ο ανέντιμος Βασίλης επιθυμεί

- στον j-οστό γύρο να μαντέψει τον κωδικό p_j έχοντας γνώση των κωδικών $p_{j-1}, p_{j-2}, \ldots, p_1, p_0, U$ με την πληροφορία $j\big|U$ να είναι άγνωστη.

Μία επιλογή είναι ο υπολογισμός ενός α, ώστε $p_{j-1} = \mathcal{E}(p_j, \mathcal{E}(\alpha, p_j))$ ισοδυναμεί με το σπάσιμο του BC.

Μία άλλη επιλογή είναι η απαρίθμηση όλων των πιθανών τιμών για τον κωδικό p_n και επίλυση μέσω του τύπου $p_{j-1} = \mathcal{E}\big(p_j, \mathcal{E}(p_j, \alpha)\big)$. Μία τέτοια προσπάθεια θα απαιτούσε n-πλάσιους υπολογιστικούς πόρους απ' ότι η παραπάνω επιλογή.

7.1.2 Αποδοτικότητα

Στους επεξεργαστές των H/Υ ένας αριθμός $m \in \mathbb{N}$ δυφίων χωρίζεται σε $d \in \mathbb{N}$ τμήματα με το κάθε τμήμα να αποτελείται από πλήθος δυφιών όσα και η χωριτικότητα του επεξεργαστή. Επί παραδείγματι, για ένα αριθμό $m = 2048$ δυφίων, ένας επεξεργαστής των 64 δυφίων τον διαχωρίζει σε $d = \frac{2048}{64} = 32$ μέρη.

Στο Σχήμα 6.2 (Feige-Fiat-Shamir) κάθε γύρος ταυτοποίησης χρειάζεται τον υπολογισμό $\alpha^2 \cdot \beta \mod n$. Κατά μέσο όρο, η πράξη αυτή απαιτεί χρόνο ανάλογο με

$$d^2 \cdot (t_m + t_a) + m \cdot d \cdot t_a$$

όπου τα $d, m \in \mathbb{N}$ είναι όπως παραπάνω και t_m, t_a είναι ο χρόνος που απαιτείται για την πραγμάτωση ενός πολλαπλασιασμού ή μιας πρόσθεσης/αφαίρεσης αντίστοιχα στον μικροεπεξεργαστή. Λαμβάνοντας υπ΄ όψιν πως στους σύγχρονους επεξεργαστές:

- ο συνήθης πολλαπλασιασμός απαιτεί 10πλάσιο υπολογιστικό κόστος απ΄ όσο μία λογική πράξη και
- η συνήθης πρόσθεση απαιτεί 2πλάσιο υπολογιστικό κόστος απ΄ όσο μια λογική πράξη,

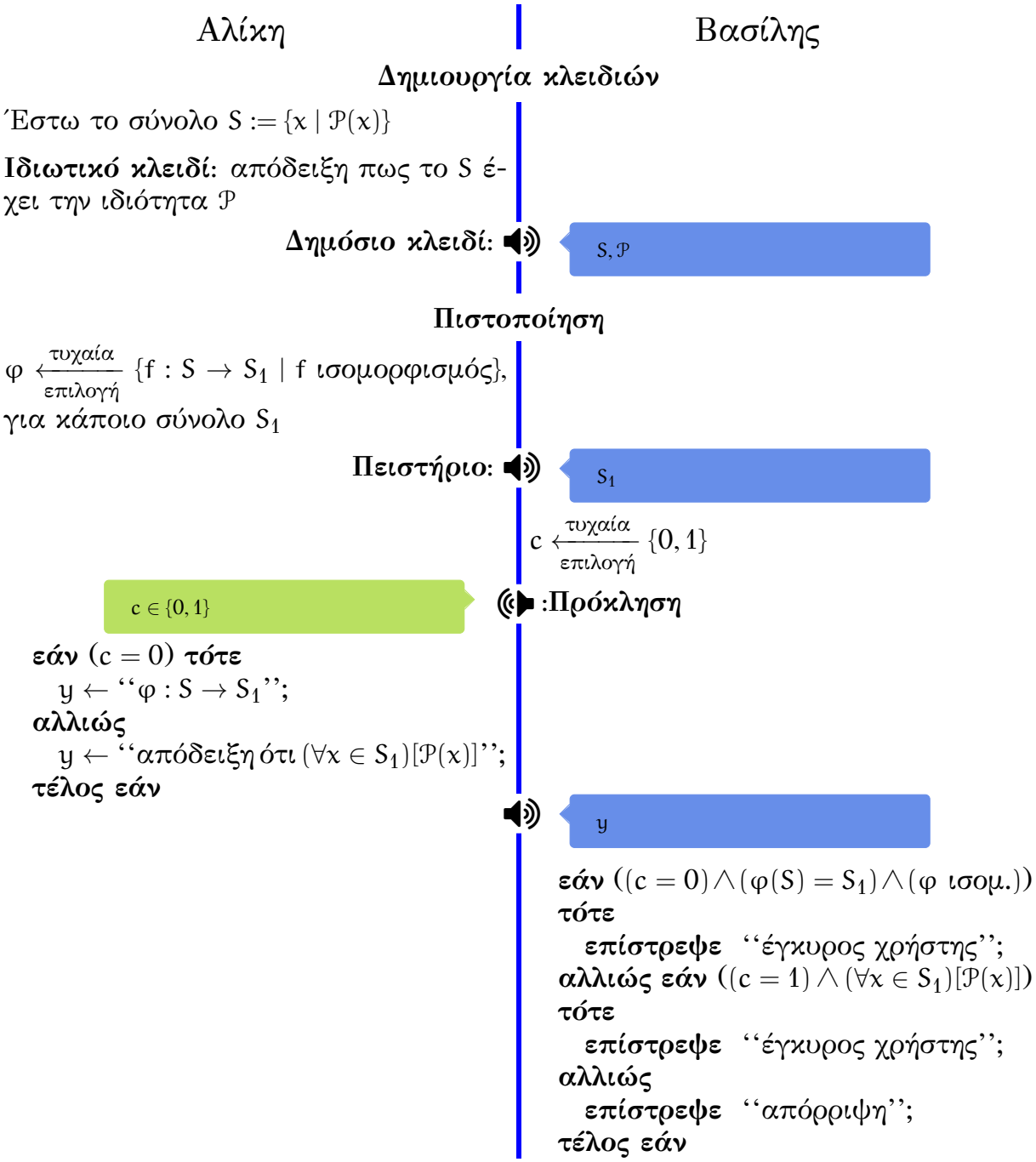
η εφαρμογή -σε έναν αριθμό των $m = 2048$ δυφίων- δύο αλγορίθμων τμήματος είναι κατά 64 φορές γρηγορότερη διαδικασία από εκείνη του υπολογισμού του $\alpha^2 \cdot \beta \mod n$.

Δεδομένου ότι το Σχήμα 6.2 (Feige-Fiat-Shamir) χρειάζεται περί τους 20 γύρους ταυτοποίησης για να επιτύχει ένα ικανοποιητικό επίπεδο ασφαλείας, το Σχήμα 7.1 για $n = 20$ γύρους πιστοποίησης είναι κατά 1280 γρηγορότερο του Σχήματος 6.2.

Το Σχήμα 7.1 προτάθηκε για την γρήγορη πιστοποίηση απομακρυσμένων χρηστών, δίχως να θυσιάζεται το επίπεδο ασφαλείας (χάριν της γρήγορης υλοποίησης).

7.2 Το σχήμα πιστοποίησης Grigoriev-Shpilrain

Το ενθάδε σχήμα οφείλεται στους Dima Grigoriev και Vladimir Sphilrain το 2008 από το [GS08] και αποτελεί γενίκευση του σχήματος Fiat-Shamir [όρα §6.1].



Σχήμα 7.2: Το σχήμα πιστοποίησης Grigoriev-Shpilrain

7.2.1 Ασφάλεια

Η δυνατότητα να βρεθεί μία απόδειξη ώστε δοσμένου ενός συνόλου S, εκείνο πληροί την ιδιότητα $\mathcal{P}$ είναι NP-hard πρόβλημα (όρα επί παραδείγματι [GJ$_{79}$]).

Πρόταση 7.2.1. Έστω πως η φάση πιστοποίησης του Σχήματος 7.2 έχει λάβει χώρα τόσες φορές ώστε και οι δύο τιμές της πρόκλησης να έχουν εμφανισθεί. Ένας αντίπαλος ο οποίος θέλει να συστηθεί ως Αλίκη στον Βασίλη επιτυγχάνει εάν και μόνον εάν μπορεί να αποδείξει πως το σύνολο S πληροί την ιδιότητα $\mathcal{P}$.

Απόδειξη. ($\Longrightarrow$): Έστω πως η Μάλλορυ θέλει να συστηθεί ως Αλίκη στον Βασίλη. Επεμβαίνει στην αρχή της φάσης πιστοποίησης στέλνοντας το δικό της πειστήριο, το σύνολο S_2. Πλέον, πρέπει να είναι έτοιμη για τις δύο προκλήσεις του Βασίλη.

- Εάν η πρόκληση είναι $c = 0$, τότε η Μάλλορυ πρέπει να αποστείλει στον Βασίλη έναν ισομορφισμό $\psi : S \longrightarrow S_2$.
- Εάν η πρόκληση είναι $c = 1$, τότε η Μάλλορυ πρέπει να αποστείλει στον Βασίλη μία απόδειξη του γεγονότος ότι $(\forall x \in S_2)[\mathcal{P}(x)]$.

Όντας η αντιστροφή της $\psi : S \longrightarrow S_2$ γνωστή στην Μάλλορυ, έπεται πως μπορεί να παράξει μια απόδειξη του γεγονότος ότι $(\forall x \in S_2)[\mathcal{P}(x)]$.

($\Longleftarrow$): Μία τέτοια απόδειξη αποτελεί μυστικό κλειδί της Αλίκης. □

Παρατήρηση 7.2.2. *Τα στοιχεία του* $\{f : S \longrightarrow S_1 \mid f$ *ισομορφισμός*$\}$ *πρέπει να είναι υπολογιστικά δύσκολο να αντιστραφούν.*

7.2.2 Υλοποιήσεις

Παρατίθενται δύο προτάσεις των εμπνευστών του Σχήματος 7.2 από το [GS$_{08}$].

7.2.2.Α΄ Χρωματισμός γραφημάτων

Θεωρία Γραφημάτων

Έστω δύο γραφήματα $\Gamma = \langle V, E\rangle$ και $\Gamma' = \langle V', E'\rangle$. Ένας **ισομορφισμός γραφημάτων** είναι μία 1–1 και επί απεικόνιση $\sigma : V \longrightarrow V'$, τέτοια ώστε $(\forall\{u, v\} \in E)[\{\sigma(u), \sigma(v)\} \in E']$. Συμβολίζεται ως $\Gamma_1 \simeq \Gamma_2$.

Ένα γράφημα $\Gamma = \langle V, E\rangle$ είναι k-**χρωματίσιμο**, για $k \in \mathbb{N}$, εάν υπάρχει μία **συνάρτηση χρωματισμού** $\kappa : V \longrightarrow \{1, 2, \ldots, k\}$, ήτοι $(\forall\{u, w\} \in E)\big[\kappa(u) \neq \kappa(w)\big]$. *Η συνάρτηση χρωματισμού δεν χρειάζεται να είναι επί.* Τα στοιχεία του συνόλου $\{1, \ldots, k\}$ αντιστοιχούν στα διαφορετικά χρώματα.

Η υλοποίηση του Σχήματος 7.2 έχει ως εξής:

(0) Το δημόσιο κλειδί της Αλίκης είναι ένα k-χρωματίσιμο γράφημα $\Gamma = \langle V, E\rangle$ και το ιδιωτικό κλειδί είναι η συνάρτηση χρωματισμού $\kappa : V \longrightarrow \{1, \ldots, k\}$.

(1) Η Αλίκη επιλέγει έναν ισομορφισμό $\psi : \Gamma \longrightarrow \Gamma_1$, για κάποιο γράφημα $\Gamma_1 = \langle V', E'\rangle$, και αποστέλλει στον Βασίλη το *πειστήριό* της: το γράφημα Γ_1.

(2) Ο Βασίλης αποστέλλει την *πρόκληση* $c \in \{0, 1\}$ στην Αλίκη.

(3)
- Εάν η πρόκληση είναι $c = 0$, τότε
  (α′) η Αλίκη αποστέλλει τον ισομορφισμό γραφημάτων $\psi : \Gamma \longrightarrow \Gamma_1$.
  (β′) ο Βασίλης επαληθεύει εάν η συνάρτηση $\psi : \Gamma \longrightarrow \Gamma_1$ είναι πράγματι ισομορφισμός γραφημάτων.
- Εάν η πρόκληση είναι $c = 1$, τότε
  (α′) η Αλίκη αποστέλλει μία συνάρτηση χρωματισμού $\mu : V' \longrightarrow \{1, \ldots, k\}$.
  (β′) ο Βασίλης επαληθεύει εάν η συνάρτηση $\mu : V' \longrightarrow \{1, \ldots, k\}$ αποτελεί πράγματι συνάρτηση χρωματισμού.

Η παρούσα εκδοχή στηρίζει την ασφάλειά της στα ακόλουθα:

Το πρόβλημα ισομορφισμού γραφημάτων (εκδοχή απόφασης): Δοσμένων δύο γραφημάτων Γ_1, Γ_2, υπάρχει ισομορφισμός ανάμεσά τους;

Το πρόβλημα είναι NP, αλλά δεν είναι γνωστόν εάν είναι NP-hard.

Το πρόβλημα του k-χρωματισμού γραφήματος (εκδοχή απόφασης): Δοσμένου ενός γραφήματος Γ, είναι αυτό k-χρωματίσιμο;

Το πρόβλημα είναι NP-complete και *κατά μέσο όρο* τα στιγμιότυπά του ανήκουν στην κλάση NP-hard.

Αλγόριθμος δημιουργίας k-χρωματίσιμου γραφήματος: Έστω ένα σύνολο V, με $\#V = n \in \mathbb{N}$.

1: Το $n \in \mathbb{N}$ αναλύεται σε $n_1, \ldots, n_k \in \mathbb{N}_0$, όπου $n = \sum_{i=1}^{k} n_i$.
2: Το σύνολο V διαμερίζεται σε $V_1, \ldots, V_k \subseteq V$ με $(\forall i = 1, \ldots, k)[n_i = \#V_i]$.
3: Το σύνολο των ακμών E δημιουργείται σύμφωνα με τα κριτήρια: Για κάθε $u, w \in V$, με $u \neq w$,
- εάν $(\exists i \in \{1, \ldots, k\})[u, w \in V_i]$, τότε $\{u, w\} \notin E$,
- αλλιώς $\mathsf{Prob}\big[\{u, w\} \in E\big] = 1/2$.

Το γράφημα $\Gamma = \langle V, E\rangle$ που παράγει ο προαναφερθείς αλγόριθμος είναι k-χρωματίσιμο η συνάρτηση χρωματισμού του οποίου είναι η $\kappa : V \longrightarrow \{1, \ldots, k\}$, όπου $(\forall i = 1, \ldots, k)(\forall u \in V_i)[\kappa(u) = i]$.

Πρόταση 7.2.3. Έστω πως η φάση της πιστοποίησης στην παρούσα υλοποίηση του Σχήματος 7.2 έχει επαναληφθεί αρκετές φορές ώστε ο Βασίλης έχει στείλει αμφότερες τις δυνατές τιμές της πρόκλησής του. Ένας αντίπαλος ο οποίος προσπαθεί να συστηθεί ως Αλίκη στον Βασίλη και ο οποίος ξεκινάει να δρα στην αρχή της φάσης της πιστοποίησης, είναι επιτυχής εάν και μόνον εάν μπορεί να βρει έναν k-χρωματισμό στο γράφημα $\Gamma = \langle V, E \rangle$.

Απόδειξη. ($\Longrightarrow$): Έστω πως η Μάλλορυ προσπαθεί να συστηθεί ως Αλίκη στον Βασίλη. Για να το επιτύχει, ξεκινάει να δρα στην αρχή της φάσης πιστοποίησης της παρούσας υλοποίησης του Σχήματος 7.2 και αποστέλλει στον Βασίλη ένα γράφημα $\Gamma_2 = \langle V'', E'' \rangle$ της επιλογής της. Κατά συνέπεια θα πρέπει να αποστείλλει στον Βασίλη ένα πειστήριο, ώστε ανεξαρτήτως της πρόκλησης του Βασίλη, εκείνη θα πρέπει να αποκριθεί αληθώς. Συνεπώς,

- Εάν η πρόκληση είναι $c = 0$, τότε η Μάλλορυ πρέπει να γνωρίζει έναν ισομορφισμό γραφημάτων $\Gamma \simeq \Gamma_2$.
- Εάν η πρόκληση είναι $c = 1$, τότε η Μάλλορυ πρέπει να στείλει μία συνάρτηση χρωματισμού $\nu : V'' \longrightarrow \{1, \ldots, k\}$ για το γράφημα Γ_2, όπου $\Gamma_2 \simeq \Gamma$.

Συνεπώς, η Μάλλορυ θα πρέπει να βρει ένα γράφημα $\Gamma_2 \simeq \Gamma$ (το πρόβλημα του ισομορφισμού γραφημάτων είναι δύσκολο) το οποίο είναι k-χρωματίσιμο (το πρόβλημα του k-χρωματισμού ενός γραφήματος είναι δύσκολο).

($\Longleftarrow$): Αφού η Μάλλορυ μπορώντας να λύσει το πρόβλημα του k-χρωματισμού για το γράφημα Γ, τότε μπορεί να ανακτήσει το μυστικό κλειδί της Αλίκης. □

7.2.2.Β΄ Ενδομορφισμοί ομάδων/δακτυλίων

Η υλοποίηση του Σχήματος 7.2 έχει ως εξής:

(0) Η Αλίκη έχει δημόσιο κλειδί της μία ομάδα (έναν δακτύλιος) G, $g, h \in G$, ώστε $\varphi(g) = h$, για κάποιον $\varphi \in \mathrm{End}(G)$ και ιδιωτικό κλειδί τον $\varphi \in \mathrm{End}(G)$.

(1) Η Αλίκη επιλέγει $\psi \in \mathrm{Aut}(G)$ και στέλνει στον Βασίλη το *πειστήριο*: $\nu := \psi(h)$.

(2) Ο Βασίλης αποστέλλει την *πρόκληση* $c \in \{0, 1\}$ στην Αλίκη.

(3)
- Εάν η πρόκληση είναι $c = 0$, τότε
  (α΄) η Αλίκη αποστέλλει τον $\psi \in \mathrm{Aut}(G)$·
  (β΄) ο Βασίλης ελέγχει αν $\nu \stackrel{?}{=} \psi(h)$ κι αν πράγματι $\psi \stackrel{?}{\in} \mathrm{Aut}(G)$.
- Εάν η πρόκληση είναι $c = 1$, τότε
  (α΄) η Αλίκη αποστέλλει τη σύνθεση $\psi \circ \varphi = \psi(\varphi) \in \mathrm{End}(G)$.
  (β΄) ο Βασίλης ελέγχει αν $(\psi \circ \varphi)(g) = \psi(\varphi(g)) \stackrel{?}{=} \nu$ κι αν $\psi \circ \varphi \stackrel{?}{\in} \mathrm{End}(G)$.

Παρατήρηση 7.2.4. *Έστω μία απεικόνιση* $f : G \longrightarrow G$. *Η απόφανση εάν* $f \overset{?}{\in} \mathrm{End}(G)$ *ή εάν* $f \overset{?}{\in} \mathrm{Aut}(G)$ *εξαρτάται από την επιλογή της ομάδας* G.

- *Εάν για παράδειγμα είναι διαθέσιμη η παράσταση της ομάδας* $G = \langle X \mid R \rangle$, *τότε ισχύει ότι* $f \in \mathrm{End}(G)$ *εάν* $(\forall r \in R)[f(r) = 1_G]$. *Κατά συνέπεια, η* G *θα πρέπει να έχει εύκολα επιλύσιμο πρόβλημα της λέξης.*
- *Για το εάν* $f \overset{?}{\in} \mathrm{Aut}(G)$, *δεν υπάρχει κάποια μεθοδολογία. Ωστόσο, για τις ελεύθερες μεταβελιανές ομάδες τάξης* 2 *[όρα παρακάτω] παρέχεται ένας τρόπος εξακρίβωσης. Εν γένει η Αλίκη θα μπορούσε μαζί με την απάντησή της* y, *στην πρόκληση* $c \in \{0, 1\}$, *να συμπεριλάβει μία απόδειξη πως* $\psi \in \mathrm{Aut}(G)$.

Η παρούσα εκδοχή στηρίζει την ασφάλειά της στο ακόλουθο υπολογιστικό πρόβλημα:

Το πρόβλημα του ενδομορφισμού: Δεδομένης/ου μιας/ενός (ημι)ομάδας/δακτυλίου G και $g, h \in G$, υπάρχει $f \in \mathrm{End}(G)$, έτσι ώστε $f(g) = h$;

Σε κάποιες ομάδες και δακτυλίους το πρόβλημα του ενδομορφισμού είναι ανεπίλυτο καθ' ότι ισοδυναμεί με την επίλυση μιας διοφαντικής εξίσωσης (όρα [Rom77, Rom79]).

Πρόταση 7.2.5. Έστω πως η φάση της πιστοποίησης στην παρούσα υλοποίηση του Σχήματος 7.2 έχει επαναληφθεί αρκετές φορές ώστε ο Βασίλης έχει στείλει αμφότερες τις δυνατές τιμές της πρόκλησής του. Ένας αντίπαλος ο οποίος προσπαθεί να συστηθεί ως Αλίκη στον Βασίλη και ο οποίος ξεκινάει να δρα στην αρχή της φάσης της πιστοποίησης, είναι επιτυχής εάν και μόνον εάν μπορεί βρει $\varphi \in \mathrm{End}(G)$, τέτοιο ώστε $\varphi(g) = h$.

Απόδειξη. ($\Longrightarrow$): Έστω πως η Μάλλορυ προσπαθεί να συστηθεί ως Αλίκη στον Βασίλη. Για να το επιτύχει, ξεκινάει να δρα στην αρχή της φάσης πιστοποίησης της παρούσας υλοποίησης του Σχήματος 7.2 και αποστέλλει στον Βασίλη κάποιο $v' \in G$ της επιλογής της. Κατά συνέπεια θα πρέπει να αποστείλλει στον Βασίλη ένα πειστήριο, ώστε ανεξαρτήτως της πρόκλησης του Βασίλη, εκείνη θα πρέπει να αποκριθεί αληθώς. Συνεπώς,

- Εάν η πρόκληση είναι $c = 0$, τότε η Μάλλορυ πρέπει να γνωρίζει έναν $\psi' \in \mathrm{End}(G)$, τέτοιον ώστε $v' = \psi'(h)$.
- Εάν η πρόκληση είναι $c = 1$, τότε η Μάλλορυ πρέπει να στείλει τη σύνθεση $\psi' \circ \varphi' \in \mathrm{End}(G)$, έτσι ώστε $\varphi' \in \mathrm{Aut}(G)$ και $v' = (\psi' \circ \varphi')(g)$.

Συνεπώς, η Μάλλορυ θα πρέπει επιλύσει (δύο φορές) το πρόβλημα του ενδομορφισμού (μία για τον $\psi' \in \mathrm{End}(G)$ και μία για τον $\psi' \circ \varphi' \in \mathrm{End}(G)$).

($\Longleftarrow$): Προφανές, αφού η Μάλλορυ εάν βρει $f \in \mathrm{End}(G)$, ώστε $f(g) = h$, τότε ο $f \in \mathrm{End}(G)$ μπορεί να χρησιμοποιηθεί αντί του μυστικού κλειδιού της Αλίκης. □

Ομάδα υλοποίησης: Ως ομάδα υλοποίησης προτείνεται η ελεύθερη μεταβελιανή ομάδα τάξης 2, M_2 [όρα Ορισμό 5.1.9]. Ο Vitaly Roman'kov το 1979 στο [Rom79] απέδειξε πως δοσμένης μιας διοφαντικής εξίσωσης E δύναται κατά αποτελεσματικό τρόπο να ευρεθούν $u, w \in M_2$, ώστε για κάθε λύση της E να υπάρχει ένας $f \in \mathrm{End}(M_2)$, όπου $u = f(w)$ και $w = f(u)$. Κατά συνέπεια, υπάρχουν ζεύγη $(u, w) \in M_2 \times M_2$ για τα οποία το πρόβλημα του ενδομορφισμού να είναι NP-hard. Άρα, η παραβίαση της παρούσας υλοποίησης στην ομάδα M_2 του Σχήματος 7.2 αποτελεί NP-hard.

7.2.3 Ένα ακόμη πρωτόκολλο των Grigoriev-Shpilrain

Ορισμός 7.2.6. Η (ημι)ομάδα $(S, *)$ λέγεται πως **δρα** επί του συνόλου X αν υπάρχει απεικόνιση $\bullet : S \times X \longrightarrow X$, τέτοια ώστε

(i) $(\forall s, t \in S)(\forall x \in X)\big[(s * t) \bullet x = s \bullet (t \bullet x)\big]$ και

(ii) $(\forall x \in X)[1_S \bullet x = x]$.

Μία ακόμη παραλλαγή του σχήματος των Fiat-Shamir που προτείνουν οι Dima Grigoriev και Vladimir Shpilrain στο [GS08] είναι η εξής: Έστω πως η ημιομάδα $(S, *)$ δρα επί του συνόλου $X \neq \varnothing$.

(0) Το δημόσιο κλειδί της Αλίκης είναι η ημιομάδα S, το σύνολο X, $x \in X$ και $u := s \bullet x$, για κάποιο τυχαία επιλεγμένο $s \in S$. Το μυστικό της κλειδί είναι το $s \in S$.

(1) Η Αλίκη στέλνει στον Βασίλη το *πειστήριό* της: $v := t \bullet u = t \bullet (s \bullet x) \in X$, για κάποιο τυχαία επιλεγμένο $t \in S$.

(2) Ο Βασίλης αποστέλλει στην Αλίκη την πρόκλησή του $c \in \{0, 1\}$.

(3)
- Εάν η πρόκληση είναι $c = 0$, τότε
  - (α′) η Αλίκη αποστέλλει το $t \in S$ στον Βασίλη·
  - (β′) ο Βασίλης επαληθεύει εάν $v \stackrel{?}{=} t \bullet u$.
- Εάν η πρόκληση είναι $c = 1$, τότε
  - (α′) η Αλίκη αποστέλλει το $ts \in S$ στον Βασίλη·
  - (β′) ο Βασίλης επαληθεύει εάν $v \stackrel{?}{=} (ts) \bullet x = t \bullet (s \bullet x)$.

Παρατήρηση 7.2.7. *Στο [GS08] περιέχονται δύο ακόμη υλοποιήσεις οι οποίες αφορούν το παραπάνω σχήμα πιστοποίησης.*

Μέρος III

Επίλογος

Κεφάλαιο 8

Επίλογος

8.1 Σύνοψη της Εργασίας

Καθώς η υπολογιστική ισχύς αυξάνει, ανακύπτει διαρκώς η ανάγκη για καινούργια πρωτόκολλα κρυπτογράφησης, ή για τροποποίηση των υπαρχόντων, ώστε να ανταπεξέρχονται στις νέες υπολογιστικές ικανότητες.

Μεταθετική Κρυπογραφία

Στη Μεταθετική Κρυπτογραφία στηρίζεται η ασφάλεια της καθημερινότητας. Πρόκειται για αλγορίθμους βαθιά ριζομένους στις καθημερινές συνήθειες (κινητά τηλέφωνα, κωδικοί Η/Υ ή λογαριασμών, συναλλαγές). Όντας πρωτόκολλα τα οποία χειρίζονται αριθμητικές πράξεις, η χρήση μεγαλυτέρων αριθμών δεν αποτελεί λύση καθώς δεν μπορούν να υλοποιηθούν με αποδοτικό τρόπο κάτω από τις σύγχρονες απαιτήσεις των χρηστών και του IoT. Για το λόγο αυτό, αναζητούνται τροποποιήσεις, που επιτρέπουν την αποδοτική υλοποίηση και ταυτόχρονα παρέχουν υψηλό επίπεδο ασφαλείας.

Μη-Μεταθετική Κρυπτογραφία

Η Μη-Μεταθετική Κρυπτογραφία αποτελεί πολλά υποσχόμενο κλάδο της Κρυπτογραφίας με πλήθος συγγραμμάτων κατά τον $21^{ο}$ αιώνα. Παρά το ‘‘νεαρό της ηλικίας της’’, χρησιμοποιεί αποτελέσματα τα οποία είναι γνωστά από τις απαρχές του $20^{ου}$ αιώνα. Αποτελεί ενεργό κλάδο, καθώς στο τομέα της κρυπτανάλυσης πολλές φορές τα προτεινόμενα πρωτόκολλα σπάζουν σε διάστημα ενός έτους από τη δημοσίευσή τους). Πολλές πτυχές της μένουν να διαφωτιστούν

(όπως εάν αντί για ομάδες χρησιμοποιηθούν δακτύλιοι· σε ποιες (μη-αβελιανές) ομάδες τα υπολογιστικά προβλήματα όπου στηρίζονται τα πρωτόκολλα είναι δύσκολο να επιλυθούν· καθώς και άλλες).

Αποδείξεις Μηδενικής γνώσης

Οι αποδείξεις μηδενικής γνώσης απαντώνται παντού στην καθημερινότητα από την επαλήθευση ενός κωδικού στα μέσα κοινωνικής δικτύωσης, μέχρι τη στρατιωτική διαταγή που μεταβιβάζεται σε ένα στράτευμα. Εδώ υπεισέρχεται το ‘‘τίμημα’’ της ασφάλειας έναντι της γρήγορης υλοποίησης. Επί παραδείγματι, δεν είναι επιθυμητό ένα κακόβουλο λογισμικό να μπορεί να αποκτήσει πρόσβαση στα δεδομένα ενός τραπεζικού λογαριασμού που πραγματοποιεί συναλλαγές μέσῳ διαδικτύου. Είναι όμως αμελητέας σημασίας το γεγονός πως ένας αντίπαλος έλαβε -σε εύλογο χρονικό διάσταση- γνώση μιας στρατιωτικής πληροφορίας που αφορά στην άμεση εκτόξευση ενός πυραύλου, δεδομένου ότι ο πύραυλος εκτοξεύθηκε τη στιγμή που εξεδώθει η εντολή. Συνεπώς, αναλόγως των προσδοκιών, κανείς μπορεί να επιλέξει ανάμεσα σε κοστοβόρες υπολογιστικά μαθηματικές πράξεις που παράγουν ασφαλέστερα πρωτόκολλα, ή τις γρηγορότερες πράξεις στο δυαδικό σύστημα που καθιστούν τα πρωτόκολλα περισόττερο ευάλωτα.

8.2 Μελλοντικές οδοί

Επειδή η Μη-Μεταθετική Κρυπτογραφία χρειάζεται εξειδικευμένη γνώση (όπως τις ιδιότητες των ομάδων πλεξίδων για κάποια πρωτόκολλα, ή των μεταβελιανών ομάδων για κάποια άλλα) φαντάζει πιο απόμακρη σε σχέση με την ευχέρεια της υλοποίησης αριθμητικών πράξεων. Ωστόσο, θα ήταν ενδιαφέρον να δοκιμασθούν στην πράξη τα εν λόγω πρωτόκολλα.

Αντί να επαληθεύονται αριθμοί υψωμένοι σε δύναμη, modulo έναν αριθμό γινόμενο δύο πρώτων, θα μπορούσε να εξετάζεται κατά πόσον ένα γράφημα είναι k-χρωματίσιμο. Η Θεωρία Αλγορίθμων και ιδιαίτερα η Θεωρία Δομών Δεδομένων είναι εξελιγμένες σε τέτοιο βαθμό που μπορούν να αναπαραστήσουν με εύλογο όγκο δομές -όπως τα γραφήματα- και να τις ψηφιοποιήσουν στο δυαδικό αλφάβητο.

Ο συνδυασμός Μεταθετικής και Μη-Μεταθετικής Κρυπτογραφίας. Παράδειγμα αποτελεί το πρωτόκολλο των Hilyati Hanin Zazali και Wan Ainun Mior Othman το 2012 στο [ZO12] οι οποίοι σχεδίασαν ένα κρυπτοσύστημα βασισμένο σ΄ ένα πρόβλημα από τη Μη-Μεταθετική Κρυπτογραφία (το πρόβλημα της ανάλύσεως), υλοποιημένο σε δομές της Μεταθετικής Κρυπτογραφίας (ελλειπτικές καμπύλες).

Παράρτημα

Παράρτημα Α΄

Παράπλευρες επιθέσεις σε ελλειπτικές καμπύλες

Η υλοποίηση ενός ασφαλούς κρυπτοσυστήματος, ενδέχεται να μην είναι ασφαλής. Υπάρχουν επιθέσεις που αξιοποιούν μία διαρρέουσα ποσότητα πληροφορίας της υλοποίησης που είχε επιλεγεί και προς τούτο ονομάστηκαν **παράπλευρες επιθέσεις** (Side Channel Attacks - SCA). Είναι αποδοτικές μόνον όταν το κρυπτογραφικό πρωτόκολλο υλοποιείται σε συσκευή η οποία βρίσκεται σε εχθρικό περιβάλλον. Μία σταχυολόγησή τους είναι: 1) Επιθέσεις Χρονισμού (Timing Attacks), 2) Ανάλυση Λαθών (Fault Analysis - FA), 3) Ανάλυση Αποτυχίας, 4) Απλή Ανάλυση Ισχύος (Simple Power Analysis - SPA), 5) Διαφορική Ανάλυση Ισχύος (Differential Power Analysis - DPA), 6) Ανάλυση της ορατής ακτινοβολίας που διαρρέεται από τις οθόνες, 7) Ανάλυσης των διαχεόμενων ακουστικών σημάτων.

Οι παράπλευρες επιθέσεις διακρίνονται σε: (i) Παθητικές (η Απλή/Διαφορική Ανάλυση Ισχύος ή οι Επιθέσεις Χρονισμού) (ii) Ενεργητικές (η Ανάλυση Λαθών).

Α΄.1 Απλή ανάλυση ισχύος

Για την αποφυγή επιθέσεων απλής ανάλυσης ισχύος υπάρχουν οι εξής μέθοδοι.

Η μέθοδος **Double and add always** σε κάθε γύρο πραγματοποιεί ψεύτικες (dummy) προσθέσεις σημείων. Για κάθε δυφίο του βαθμωτού, οι λειτουργίες της πρόσθεσης και του διπλασιασμού εκτελούνται έτσι ώστε οι υπολογιστικές διεργασίες να είναι ανεξάρτητες από το βαθμωτό.

Η μέθοδος **Montgomery Ladder** υλοποιεί τον βαθμωτό πολλαπλασιασμό. Εφαρμόζει τον αλγόριθμο Double_and_Add, αλλά υπολογίζει σταθερά τον ίδιο αριθμό διπλασιασμού και πρόσθεσης σημείων σε ένα σταθερό πρότυπο, ανεξάρτητο από το βαθμωτό και δίχως ψεύτικους (dummy) υπολογισμούς.

Αλγόριθμος Α΄.1.1 MONTGOMERY_LADDER$\big((b_{\ell-1},\ldots,b_1,b_0),P\big)$: Βαθμωτός πολ/μός

Είσοδος: $(b_{\ell-1},\ldots,b_1,b_0)\in\{0,1\}^\ell$ και $P\in\mathcal{E}$.
΄Εξοδος: $\big(\sum_{i=0}^{\ell-1} b_i 2^i\big)\boxdot P\in\mathcal{E}$.

1: $Q_0\leftarrow Q_1\leftarrow \mathbf{O}_\infty$;
2: **εάν** $(b_0=1)$ **τότε**
3: $\quad Q_0\leftarrow P;\qquad Q_1\leftarrow 2\boxdot P$;
4: **τέλος εάν**
5: **για** $(i=0,1,\ldots,\ell-1)$
6: $\quad Q_{1-b_i}\leftarrow Q_0\boxplus Q_1;\qquad Q_{d_i}\leftarrow 2\boxdot Q_{d_i}$;
7: **τέλος για**
8: **επίστρεψε** Q_0;

Σε κάθε φάση του αλγορίθμου παραπάνω είναι $Q_1\boxminus Q_0=P$. Ο P. Montgomery παρατήρησε πως τετμημένη του αθροίσματος δύο σημείων με σταθερή διαφορά μπορεί να υπολογισθεί κάνοντας χρήση μόνον των τετμημένων των σημείων.

Η μέθοδος **Unified Operation** συνδυάζει την πρόσθεση και τον διπλασιασμό σημείων σε μια λειτουργία που εξαλείφει τις διαφορές ανάμεσα στις πράξεις.

Αλγόριθμος Α΄.1.2 UNIFIED_OPERATION$\big((x_1,y_1),(x_2,y_2)\big)$: Άθροισμα σημείων

Είσοδος: Σημεία $(x_1,y_1),(x_2,y_2)\in\mathcal{E}$.
Δεδομένα: $a,b\in\mathbb{K}$ όπου $\mathcal{E}: y^2=x^3+ax+b$
΄Εξοδος: Το άθροισμα $(x_1,y_1)\boxplus(x_2,y_2)\in\mathcal{E}$.

1: $\lambda\leftarrow\dfrac{x_1^2+x_1x_2+x_2^2+a}{y_1+y_2}$;$\qquad\mu\leftarrow y_1-\lambda x_1$;
2: **επίστρεψε** $(\lambda^2-x_1-x_2,\ -\lambda x_3-\mu)$;

Α΄.2 Διαφορική ανάλυση ισχύος

Έστω $\mathcal{E}$ μία ελλειπτική καμπύλη, $P\in\mathcal{E}$, $n=\mathrm{ord}(P)$ και $d\in\mathbb{Z}_n$ το ιδιωτικό κλειδί. Σκοπός είναι να μην υπολογισθεί το ιδιωτικό κλειδί. Προς τούτο:

Τύφλωση Βαθμωτού [Co99]: Αντί του $Q=d\boxdot P\in\mathcal{E}$ στέλνεται το $Q'=d'\boxdot P\in\mathcal{E}$, όπου $d':=d+k\cdot\#\mathcal{E}$, για κάποιο τυχαίο $k\in\mathbb{Z}$ μήκους $n\in\mathbb{N}$ δυφίων. Πλέον: $Q=d'\boxdot P=(d+k\cdot\#\mathcal{E})\boxdot P=(d\boxdot P)\boxplus(k\boxdot(\#\mathcal{E}\boxdot P))\overset{\#\mathcal{E}\boxdot P=\mathbf{O}_\infty}{=}d\boxdot P$.

Τύφλωση Σημείου Βάσης: Αντί του $Q=d\boxdot P$ στέλνεται το $Q'=d\boxdot(P\boxplus R)\in\mathcal{E}$, για τυχαίο $R\in\mathcal{E}$. Το σημείο $d\boxdot R\in\mathcal{E}$ κρατείται μυστική.

Τυχαία Διαμέριση Βαθμωτού [CJRR99, CJ01]: Αντί του $Q=d\boxdot P\in\mathcal{E}$ αποστέλλεται το $Q'=d'\boxdot P\in\mathcal{E}$, όπου $d':=\big(\lfloor d/r\rfloor\big)\cdot r+(d\mod r)$, για κάποιο τυχαίο $r\in\mathbb{N}$. Πλέον: $d'\boxdot P=\big((d\mod r)\boxdot P\big)\boxplus\big(\big(\lfloor d/r\rfloor\big)\boxdot(r\boxdot P)\big)$.

Οι Benoit Feix, Mylene Roussellet και Alexandre Venelli στο [FRV14] το 2014 παρουσιάζουν επιθέσεις που αναιρούν τις παραπάνω τυφλώσεις.

Βιβλιογραφία

[And13] *Android Security Vulnerability*, (2013), διαθέσιμο στον ιστότοπο: `https://bitcoin.org/en/alert/2013-08-11-android`.

[Ar47] E. Artin, *Theory of Braids*, Ann. Math. **48** (1947), ssv.101—126.

[AS98] K. Araki, T. Satoh, *Fermat quotients and the polynomial time discrete* log *algorithm for anomalous elliptic curves*, Comm. MAth. Univ. Sancti Pauli, 47 (1998), σσ.81—91.

[BDM10] N. Bardis, N. Doukas, O. Markovskyi, *Fast Subscriber identification based on the zero knowledge principle for multimedia content distribution*, International Journal of Multimedia Intelligence and Security, Vol. 1, No. 4, (2010), σσ.363—377.

[BDM17] N. Bardis, N. Doukas, O. Markovskyi, *Zero-Knowledge Identification Method Based on Block Ciphers*, 2017 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO), Prague, Czech Republic (2017), σσ.307—311.

[BMDD12] N. Bardis, O. Markovskyi, N. Doukas, F. Drigas, *Fast implementation zero knowledge identification schemes using Galois Fields Arithmetic*, Proceeding of IX. Internatioanl Symposium IEEE on Telecommunications - BIHTEL-2012, October 25-27, Sarajevo, Bosnia and Herzegovina (2012), ISBN: 978-1-4673-4876-8.

[BM85] S. Bachmuth, H. Y. Mochizuki, $\mathrm{Aut}(\mathsf{F}) \longrightarrow \mathrm{Aut}(\mathsf{F}/\mathsf{F}'')$ *is surective for free group* F *of rank* $\geqslant 4$, Trans. Amer. Math. Soc. 292 (1985), σσ.81—101.

[BR94] M. Bellare, P. Rogaway, *Optimal Asymmetric Encryption*, In Advances in Cryptology - EUROCRYPT'94 (1995), σσ.92—111.

[BR96] M. Bellare, P. Rogaway, *The exact security of Digital Signatures - How to Sign with RSA and Rabin*, EUROCRYPT 1996 (1996), σσ.399—416.

[BDPR98] M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, *Relations Among Notions of Security for Public-Key Encryption Schemes*, In Advances in Cryptology - CRYPTO'98, Springer-Verlag, Vol. 1462 (1998), 26—45.

[BKL98] J. Birman, K. Ko, S. Lee, *A new approach to the word problem in braid groups*, Adv. Math. **139** (1998), 322—353.

[Bo99] D. Boneh, *Twenty Years of attacks on the RSA Cryptosystem*, Noticies of the American Mathematical Society, 46(2) (1999), 203—213.

[BD00] D. Boneh, G. Durfee, *Cryptanalysis of RSA with private key* d *less than* $N^{0.292}$, IEEE Transactions on Information Theory 46(4) (2000), σσ.1339—1349.

[Bo58] W. Boone, *The word problem*, Proceedings of the National Academy of Sciences, 44(10), `www.pnas.org/sgi/reprint/44/10/1061.pdf`, (1958), σσ.1061—1065.

[Br00] E. Brown, *Three Fermat trails to elliptic curves*, The College Mathematics Journal, 31(3) (2000), σσ.162—172.

[BST90] D. M. Barrington, H. Staubing, D. Therien, *Non-uniform automata over groups*, Information and Computation, 132 (1990), σσ.89—109.

[BST80] G. Baumslag, R. Strebel, M. W. Thomson, *On the multiplicator of* $F/\gamma_c R$, J. Pure Appl. Algebra 16 (1980), σσ.121—132.

[CJ01] C. Clavier, M. Joye, *Universal exponentiation algorithm a first step towards provable SPA-resistance*, In: Koç. Ç.K., Paar, C. (eds.) Cryptographic Hardware Embedded Systems - CHES 2001, Lecture Notes in Computer Science, vol. 2162, Springer Verlin / Heidelberg (2001), σσ.300—308.

[CJRR99] S. Chari, C. S. Julta, J. R. Rao, P. Rohatgi, *Towards sound approaches to counteract power-analysis attacks*, In: Weiener, M. (ed.) Advances in Cryptology - CRYPTO'99, Lecture Notes on Computer Science, vol. 1666, Springer Berlin / Heidelberg (1999), σσ.398—412.

[CKLHC01] J. C. Cha, K. H. Ko, S. J. Lee, J. W. Han, J. H. Cheon, *An Efficient Implementation of Braid Groups*, ASIACRYPT'01, LNCS **2248** (2001), ssv.144—156.

[CNT11] J.-J. Climent, P. R. Navarro, L. Tortosa, *Key exchange protocols over noncommutative ring. The case* End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$), Proceedings of the 11th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2011) ed. J. Vigo Aguiar (2011), σσ.357—364.

[Co99] J. S. Coron, *Resistance against differential power analysis for elliptic curve cryptosystems*, In: Koç. Ç.K., Paar, C. (eds.) Cryptographic Hardware Embedded Systems - CHES 1999, Lecture Notes in Computer Science, vol. 1717, Springer Verlin / Heidelberg (1999, σσ.292—302.

[Co00] J. S. Coron, *On the Exact Security of Full Domain Hash*, CRYPTO 2000 (2000), σσ.229—235.

[Cou00] T. Coulbois, *Propri t s de Ribes-Zaleskii, produit libre et g n ralisations*, Ph.D. Thesis, Uniiversité de Paris VII (2000).

[CSP06] V. Shpilrain, A. Ushakov, *The conjugacy search problem in public key cryptography: unnessecary and insufficient*, Appl. Algebra Engrg. Comm. Comput. 17 (2006) 285–289.

[CS98] R. Cramer, V. Shoup, *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*, In Hugo Krawczyk, editor, Advances in Cryptology - CRYPTO'98, volume 1462 of Lecture Notes in Computer Science Springer Berlin Heidelberg, (1998), σσ.13—25.

[De11] M. Dehn, *Uber unendliche diskontinuierliche Gruppen*, Math. Annaeln., 71(1) (1911), σσ.116—144.

[De12] M. Dehn, *Transformation der Kurven auf zweinseitigen Flächen*, Math. Annaeln., 72(3) (1912), 413—421.

[DH76] W. Diffie, M. Hellman, *New directions in Cryptography*, IEEE Trans. Inf. Theor., 22(6) (1976), 644—654.

[Di] L. E. Dickson, *History of the Theory of Numbers*, 1, σσ.215—216.

[Dix81] J. D. Dixon, *Asymptotically fast factorization of integers*, Math. Comp. 36(153) (1981), σσ.255—260.

[EdDSA12] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, B.Y. Yang *High-speed high-security signatures*, Journal of Cryptographic Engineering 2(2) (2012), σσ.77—89.

[EG85] T. El Gamal, *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete algorithms*, IEEE Trnsactions on Information Theory 31(4) (1985), σσ.469—472.

[FFS87] U. Feige, A. Fiat, A. Shamir, *Zero Knowledge Proofs of Identity*, STOC '87: Proceedings of the nineteenth annual ACM conference on Theory of computing (1987), σσ.210—217.

[FV03] P. A. Fouque, F. Valette, *The doubling attack - why upwards is better than downwards*, Cryptographic Hardware and Embedded Systems - CHES 2003, (2003), σσ.269—280.

[FRV14] B. Feix, M. Roussellet, A. Venelli, *Side-Chanel Analysis on Blinded Ragular Scalar Multiplications*, INDOCRYPT '14 (2014) σσ.3—20.

[FS86] A. Fiat, A. Shamir, *How To Prove Yourself: Practical Solutions to Identification and Signature Problems*, CRYPTO '86, LNCS 263 (1986) σσ.186—196.

[GHY85] Z. Galil, S. Haber, M. Yung, *A Private Interactive Test of a Boolean Predicate and Minimum-Knowledge Public Key Cryptosystems*, Proceedings FOCS 1985 (1985), σσ.360—371.

[GJ79] M. Garey, J. Johnson, *Computers and Intractability, A Guide to NP-Completeness*, W. H. Freeman (1979).

[GM82] S. Goldwasser, S. Micali, *Probabilistic Encryption*, Proc. of 14th Symposium on Theory of Computing (1982), σσ.365—377.

[GMR85] S. Goldwasser, S. Micali, C. Rackoff, *Knowledge Complexity of Interactive Proof Systems*, Proceedings of STOC 1985 (1985), σσ.291—304.

[GMT82] S. Goldwasser, S. Micali, P. Tong, *Why and how to estabilsh a private code on a public network (extended abstract)*, In 23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, (1982) σσ.134—144.

[GC00] L. Goubin, N. T. Coulbois, *Cryptanalysis of the TTM cryptosystem*, Asiacrypt, Lecture Notes in Comput. Sci. 1976, Springer (2000), 44—57.

[GP03] D. Grigoriev, I. Ponomarenko, *Homomorphic public-key cryptosystems and encrypting boolean circuits*, (2003).

[GS08] D. Grigoriev, V. Shpilrain, *Zero-knowledge authentication schemes from actions on graphs, groups, or rings*, Annals of Pure and Applied Logic 162(3) (2008), σσ.194—200.

[GS13] D. Grigoriev, V. Shpilrain, *Tropical Cryptography* (2013), διαθέσιμο στον ιστότοπο: `http://arxiv.org/abs/1301.1195`.

[Gu87] N. Gupta, *Gree Group Rings*, Contemp. Math. 66, Amer. Math. Soc. (1987).

[GZ85] M. Garzon, Y. Zalcstein, *The compllexity of Grigorchyk groups with Application to Cryptography*, Theoretical Computer Science 88 (1985), Elsevier, σσ.83—98.

[HMV04] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag & Hall/CRC, New York, ISBN 0-387-95273-X (2004).

[Kn98] D. E. Knuth, *The Art of Computer Programming, vol. II: Semi-numerical Algorithms*, third edition, Addison-Wesley (1998).

[Ko87] N. Koblitz, *Elliptic curve cryptosystems*, Math of Comp., 48 (1987) σσ.203—209.

[Ka16] G. Karystianos, *Elliptic Curves Cryptography and its Application to Bitcoin*, Postgraduate program in Logic, Algoritmhs and Computation, thesis for the Master in Science degree (2016).

[KR03] B. Kaliski, R. Rivest, *RSA problem*, ACM SIGKDD, Explorations (2003).

[Ku06] Y. Kurt, *A New Key Exchange Primitive Based on the Triple Decomposition Problem*, IACR Cryptography (2006), διαθέσιμο στον ιστότοπο: `http://eprint.iacr.org/2006/378`.

[KY12] A. A. Kamal, A. M. Youssef, *Cryptanalysis of a key exchange protocol based on the endomorphisms ring* $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, Applicable Algebra in Engineering, Communication and Computing 23(3–4) (2012), σσ.143—149.

[Li10] C. Litsas, *Fully Homomorphic Encryption*, Postgraduate program in Logic, Algoritmhs and Computation, thesis for the Master in Science degree (2010).

[Mi86] V. Miller, *Uses of elliptic curves in Cryptography*, in Advances in Cryptology – Crypto '85, LNCS 218 (Springer) (1986) σσ.417—426.

[Mi69] J. Milnor, *Growth of finitely generated solvable groups*, J. Differential Geometry 2 (1968), σσ.447—449.

[Mi92] A. Miyaji, *Elliptic curves over* $\mathbb{F}_p$ *suitable for cryptosystems*, in Advances in Cryptology – Auscrypt '92, LNCS 218 (Springer) (1993), σσ.479—491.

[MOV93] A. J. Menezes, T. Okamoto, S. A. Vanstone, *Reducing elliptic curve logarithms to a finite field*, IEEE Trans., Info Theory, 39 (1993), σσ.1639—1646.

[MOV96] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography* (1996), CRC Press Book.

[MSU08] A. D. Myasnikov, V. Shpilrain, A. Ushakov, *Group-Based Cryptography*, Advanced Courses in Mathematics, CRM Barcelona (2008), Βιρκηυσερ ἔρλαγ, Βασελ.

[Moh99] T. Moh, *A public key system with signature and master key functions*, Comm. Algebra 27 (1999), 2207—2222.

[Mo06] R. A. Mollin, *An Introduction To Cryptography*, ISBN 978-1-58488-618-1, CRC Press Book (2006).

[Mou14] A. Moustafa, *Fast Exponentiation in Galois Field* GF(2^m) *Using Precomputations*, Contemporary Engineering Sciences, Vol. 7, No. 4 (2014), σσ.193—206.

[Na12] P. Nastou, *Cryptography*, Lecture Notes from University of the Aegean, Department of Mathematics (2012).

[Ne94] V. I. Nechaev, *Complexity of a determinate algorithm for the descrete logarithm*, Mathematical Notes, vol. 55, no. 2, (1994), σσ.165—172.

[No55] P. S. Nobikov, *Algorithmic Unsolvability of the Word Problem in Group Theory* (1958).

[Pai99] P. Paillier, *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*, Advanced in Cryptography, Proceedings of EUROCRYPT '99, Springer-Verlag (1999), σσ.50—61.

[PH78] S. C. Pohlig, M. E. Hellman *An Improved Algorithm for Computing Logarithms over* GF(p) *and its Cryptographic Significance*, IEEE Transactions on Information Theory (24) (1978), 106—110.

[Po74] J. M. Pollard, *Theorems of factorization and primality testing*, Proceedings of the Cambridge Philosophical Society, 76(3) (1974), σσ.521—528.

[Po74] J. M. Pollard, *A Monte Carlo method for factorization*, BIT Numerical Mathematics, 15(3) (1975), σσ.331—334.

[Po13] T. Pornin, *Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithms (ECDSA)*, RfC6979 (2013).

[PS3] *Console Hacking 2010 - PS3 Epic Fail*, (2010), σσ.123—128, διαθέσιμο στον ιστότοπο: https://events.ccc.de/congress/2010/Fahrplan/attachments/1780_27c3_console_hacking_2010.pdf.

[QGAB89] J.-J. Quisquater, L. Guillou, M. Annick, T. Berson, *How to Explain Zero-Knowledge Protocols to Your Children*, Proceedings on Advances in Cryptology - CRYPTO'89, 435, (1989), σσ.628—631.

[Ra07] D. Ravenel, *Elliptic Curves: what they are, why they are called elliptic, and why topologists like them*, Wayne State University Mathematics Colloquium (2007).

[RF94] H. G. Ruck, G. Frey, *A remark concerning* m*-divisibility and the descrete logarithm in the divisor class group of curves*, Mathematics of Computation, 62 (206) (1994), σσ.865—874.

[Rom77] V. A. Roman'kov, *Unsolvability of the problem of endomorphic reducibility in free nilpotent and in free rings*, Algebra and Logic 16 (1977), σσ.310—320.

[Rom79] V. A. Roman'kov, *Equations in free metabelian groups*, Siberian Math. J. 20 (1979), σσ.469—471.

[Rom14] V. A. Roman'kov, *A polynomial time algorithm for the braid double shielded public key cryptosystems*, ArXiv 1412.5277v1 [math.GR] (2014).

[Ro80] N. S. Romanovskii, *The occurence problem for extensions of abelian and nilpotent groups*, Sib. Math. J. 21 (1980), σσ.177—184.

[RSA78] R. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Comm. of the ACM, 21 (1978), σσ.120—126.

[Sch85] R. Schoof, *Elliptic Curves over Finite Fields and and the Computation of square roots* mod p, Mathematics of Computation 44 (1985) σσ.483—495.

[Sch95] R. Schoof, *Counting Points on Elliptic Curves over Finite Fileds*, Journal de Théorie des Nombres de Bordeaux 7 (1995) σσ.219—254.

[Se98] I. A. Semaev, *Evaluation of discrete logarithms on some elliptic curves*, Mathematics of Computation, 67 (1998), σσ.353—356.

[Sh78] A. Shamir, *Identity-Based Cryptosystems and Signature Schemes*, Proceedings of the CRYPTO '84, Lecture Notes in Computer Science no. 196, Springer Verlag (1984).

[Sha71] D. Shanks, *Class number, a theory of factorization and general*, In Proc. Symp. Pure Math. 20, AMS, Providence, R.I. (1971), σσ.415—440.

[Sha73] D. Shanks, *Five Number-theoretic Algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics (1973), σσ.51—70.

[Sh91] V. Shpilrain, *Automorphisms of* F/R' *groups*, Internat. J. Algebra and Comput. 1 (1991), σσ.177—184.

[Sh08] V. Shpilrain, *Cryptanalysis of Stickel's Key Exchange Scheme*, Computer Science in Russia, Lecture Notes on Computer Science 5010, Springer, (2008), σσ.283—288.

[Si85] J. H. Silverman, *The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics*, ISBN 0387962034, Springer (1985).

[Sm99] N. P. Smart, *The discrete logarithm problem on elliptic curves of trace one*, Journal of Cryptology 12 (1999), σσ.193—196.

[SU05] V. Shpilrain, A. Ushakov, *Thompson's group and public key cryptography*, Lecture Notes Comp. Sc. **3531** (2005) 151–164.

[SU06] V. Shpilrain, A. Ushakov, *A New Key Exchange Protocol Based on the Decomposition Problem*, Contemp. Math. 418 (2006) 161–167.

[SZ06] V. Shpilrain, G. Zapata, *Using the subgroup memebership search problem in public key cryptography*, Algebraic Methods in Cryptography, Contemporary Mathematics 418, American Mathematical Society (2006), σσ.169—179.

[SMBD11] P. Stavroulakis, O. Markovskyi,N. Bardis, N. Doukas, *Efficient Zero-Knowledge Identification Based on One Way Boolean Transformations*, GLOBECOM Workshops (GC Wkshps), IEEE (2011), σσ.275—280.

[Sti05] E. Stickel, *A New Method for Exchanging Secret Keys*, In: Proc. of the Third Inernational Conference on Information Technology and Applications (ICITA05) (2005) 426–430.

[Te00] D. C. Terr, *A modification of Shank's baby-step giant-step algorithm*, Mathematics of Computation 69 (2000), σσ.767—773.

[Wei90] Michael J. Weiner, *Cryptanalysis of short RSA secret exponents*, Information Theory, IEEE Transactions on, 36(3) (1990), σσ.553—558.

[WXLLW14] X. Wang, C. Xu, G. Li, H. Lin, W. Wang, *Double shielded Public Key Cryptosystems*, Cryptology ePrint Archive Report 2014/588 (2004), σσ.1—14.

[YS01] A. Yamamura, T. Saito, *Private information retrieval based on the subgrou memebership problem*, In B. Barafharajan (ed.), Sixth Australian Conference on Information Security and Privacy, Vol. 2119 of Lecture Notes in Computer Science, Sydney, Australia, (2001), σσ.206—220.

[Zi99] P. Zimmermeann, *Why I wrote PGP*, Essays on PGP (1999).

[ZO12] H. Zazali, W. Othman, *Key Exchange in Elliptic Curve Cryptography Based on the Decomposition Problem*, Sains Malysiana 41(7), (2012), σσ.907—910.