Κολοκυθα Αλεξανδρα

Μαθηματική Κρυπτογραφία

Διπλωματική Εργασία
στα Εφαρμοσμένα Μαθηματικά

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
Τμήμα Μαθηματικών
Αθήνα 2015

Αφιερώνεται
στην οικογένεια μου

Περίληψη

Στην εργασία αυτή μελετάται η κανονική μη-μεταθετική κρυπτογραφία, συγκεκριμένα πρωτόκολλα τα οποία χρησιμοποιούν μη-μεταθετικές (ημί)ομάδες ως πλατφόρμες, καθώς και συγκεκριμένες ομάδες, που μπορεί να χρησιμοποιηθούν ως ομάδες πλατφόρμας κρυπτογραφικών πρωτοκόλλων δημοσίου-κλειδιού.

Αρχικά, αναλύουμε τα πρωτόκολλα που βασίζονται στα προβλήματα συζυγίας (conjugacy problem), αποσύνθεσης (decomposition problem), αναζήτησης παραγόντων (factorization search problem) και ειδικότερα τα πρωτόκολλα των Stickel και Anshel-Anshel-Goldfeld. Αλλά και τις σχέσεις τους ανάμεσα σε δίαφορα προβλήματα. Στην συνέχεια, θα αναλύσουμε τα πρωτόκολλα γνησιότητας που βασίζονται στο πρόβλημα συζυγίας (conjugacy problem), συγκεκριμένα των Diffie-Hellman και των Fiat-Shamir, ένα σχήμα που βασίζεται στο διπλό πρόβλημα συζυγίας, όπως και τις σχέσεις των διαφόρων αυτών προβλήματων.

Ακόμα, αναλύουμε ομάδες (ή κλάσεις ομάδων) που μπορούν να χρησιμοποιηθούν ως ομάδες πλατφόρμας. Για παράδειγμα, τις ομάδες πλεξίδων (ή braid groups), την ομάδα Thompson, τις ομάδες μικρών διαφορών, τις ομάδες Artin. Επιπλεόν, μελετάμε την σημασία των κανονικών μορφών σε μία ομάδα και παρουσιάζουμε κάποιες βασικές, όπως η κανονική μορφή του Garside και του Thompson.

Abstract

The aim of this thesis is to study the canonical non-commutative cryptography, more specific protocols which use non-commutative (semi)groups as platforms, as well as specific groups as possible platforms of cryptographic public-key protocols.

In particular, we analyse the protocols based on the conjugacy problem, decomposition problem, factorization search problem, and more specifically the Stickel's key exchange protocol and the Anshel-Anshel-Goldfeld protocol. In following paragraphs, we analyse the authentication protocols based on the conjugacy problem. More specifically a Diffie-Hellman-like scheme, a Fiat-Shamir-like scheme, a shceme based on the twisted conjugacy problem, and the relations between different problems.

Secondly, several groups (or classes of groups) are examined as possible platforms of cryptographic public-key protocols. For instance, the braid groups, Thompson group, small cancelation groups, Artin group. Additionally, we examine the normal forms importance in a group and we present some basic ones: normal form Garside and Thompson's.

Προλογος

Μία από τις βασικότερες εφαρμογές στην κρυπτογραφία είναι η κρυπτογράφηση και αποκρυπτογράφηση προσωπικών μηνυματων και κειμένων. Ένα σύστημα ανταλλαγής κλειδιών επιτρέπει στους χρήστες να συμφωνήσουν σε ένα κοινό κλειδί το οποίο με τη σειρά του θα τους επιτρέπει να κρυπρογραφούν και να αποκρυπτογραφούν τα μηνύματά τους. Η μυστικότητα του κοινού αυτού κλειδιού είναι το πρωτεύον θέμα σε ένα σύστημα ανταλλαγής κλειδιών.

Το πρώτο πρωτόκολλο ανταλλαγής κλειδιών παρουσιάστηκε από τους Diffie-Hellman το 1976 και ανεξάρτητα από τον Merkle το 1978.

Η ασφάλεια του πρωτοκόλλου των Diffie-Hellman βασίζεται στην δυσκολία του προβλήματος Diffie-Hellman, πάνω στα πεπερασμένα πεδία. Η περιέργεια των μαθηματικών στράφηκε στην αναζήτηση νέων κρυπτογραφικών συστημάτων, που θα βασίζονταν σε δύσκολα μαθηματικά προβλήματα, διαφόρων φύσεων και τομέων.

Από τότε που οι Diffie-Hellman πρότειναν την ιδέα του πρωτοκόλλου συμφωνίας κλειδιών και τα συστήματα δημοσίων κλειδιών, το 1976, έχουν μελετηθεί διάφορα πρωτόκολλα συμφωνίας κλειδιών πάνω σε μεταθετικές βάσεις, τροποποιήσεις δηλαδή ήδη υπαρχόντων συστημάτων και της κρυπτανάλυσής τους (δηλαδή η διεργασία αποκρυπτογράφησης ενός μηνύματος από μη εξουσιοδοτημένο χρήστη).

Στα πιο σύγχρονα χρόνια η ανάπτυξη της κινητής τηλεφωνίας είχε ως αποτέλεσμα την στροφή των ερευνών προς αυτήν την κατεύθυνση. Τα πρωτόκολλα αυθεντικότητας και συμφωνίας κλειδιών είναι τα πιο σημαντικά από την σκοπιά της έρευνας, αφού αποτελούν βασικούς πυλώνες ασφάλειας.

Το 1999 ο Anshel παρουσίασε ένα νέο πρωτόκολλο συμφωνίας κλειδιού που χρησιμοποιούσε μη-μεταθετικες ομάδες, εκμεταλλευόμενος την δυσκολία του Προβλήματος Έρευνας Συζυγίας. Συνεχίζοντας στο ίδιο πνεύμα το 2000 ο Ko και το 2001 ο Cha δημοσίευσαν νέα πρωτόκολλα που, επίσης, λειτουργούσαν πάνω σε μη-μεταθετικές ομάδες. Παρόλα αυτά τα συστήματα είναι ευάλωτα σε κάποιες επιθέσεις.

Στην παρούσα διπλωματική εργασία αναλύουμε διάφορα πρωτόκολλα, που βασίζονται στην κανονική μη-μεταθετική κρυπτογραφία και πιο συγκεκριμένα σε γνωστά προβλήματα, όπως το Πρόβλημα Συζυγίας, το Πρόβλημα Αποσύνθεσης, το Πρόβλημα Αναζήτησης Παραγόντων.

Σε πολλές περιπτώσεις, χρειαζόμαστε να μεταφέρουμε δεδομένα με ασφαλή τρόπο: πληροφορίες πιστωτικών καρτών, προσωπικά δεδομένα κ.τ.λ. Η ιδέα της κρυπτογράφισης δημοσίου κλειδιού, γενικά, είναι η δυνατότητα για δύο μερίες να συμφωνήσουν σε ένα κοινό μυστικό κλειδί, το οποίο μπορούν να χρησιμοποιήσουν για να μεταφέρουν δεδομένα με έναν ασφαλή τρόπο. Βλ[1]

Υπάρχουν πολλά κρυπτογραφίκα συστήματα δημοσίου κλειδιού τα οποία βασίζονται στο *Διακριτό Λογαριθμικό Πρόβλημα*, το οποίο είναι: Να βρούμε το x της εξίσωσης $g^x = \mathrm{h}$, όπου g, h είναι δοσμένα, και στο Πρόβλημα Παραγοντοποίησης, το οποίο είναι να αναλύσεις έναν αριθμό σε πρώτους αριθμούς-παράγοντες: Diffie-Hellman Βλ[2] και RSA. Βλ[3]

Αυτά τα σχήματα χρησιμοποιούνται ακόμα και σήμερα. Πράγμα το οποίο έχει ως αποτέλεσμα διάφορα προβλήματα, όπως:

- **Επιθέσεις σε υποκείμενα προβλήματα αυτών των ισχύοντων κρυπτογραφικών συστημάτων:** Ο RSA και το πρωτόκολλο των Diffie-Hellman μπορούν να σπάσουν σε υπο-εκθετικό (subexponential) χρόνο, ο οποίος είναι πιο γρήγορος από τον εκθετικό, για το μήκος του κλειδίου. Το συνηθισμένο μήκος των κλειδιών ασφαλείας είναι τουλάχιστον 1000 bit. Επιπλέον, το μήκος του κλειδιού θα πρέπει να αυξάνεται κάθε λίγα χρόνια. Πράγμα το οποίο κάνει τον αλγόριθμο αρκετά βαρύ.

- **Κβαντικοί υπολογιστές:** Εάν οι κβαντικοί υπολογιστές χρησιμοποιηθούν αρκετά, τότε ο RSA δεν θα είναι πλέον ασφαλής, εφόσον υπάρχουν οι αλγόριθμοι του Peter Shor που εκτελούνται σε πολυωνυμικό χρόνο. Οι αλγόριθμοι αυτοί λύνουν το Διακριτό Λογαριθμικό Πρόβλημα και το Πρόβλημα Παραγοντοποίησης. Συνεπώς, μπορούν να λύσουν τα προβλήματα στα οποία βασίζονται οι RSA και Diffie-Hellman. Βλ[4]

  Για περισσότερες πληροφορίες μπορούμε να δούμε το [5].

- **Πολλά ασφαλή δεδομένα μεταφέρονται με τον ίδιο τρόπο:** Δεν είναι σωστό το γεγονός ότι η πλειοψηφία των δεδομένων, που θεωρούνται ασφαλή, μεταφέρονται με την ίδια μέθοδο, εάν αυτός ο τρόπος σπάσει πολλά ασφαλή δεδομένα θα αποκαλυφθούν.

Ως εκ τούτου, για να λύσει κάποιος αυτά τα προβλήματα, θα πρέπει να ψάξει για νέα κρυπτογραφικά συστήματα δημοσίου κλειδιού τα οποία από την μία μεριά θα είναι

χρηστικά και από την άλλη θα βασίζονται σε ένα πρόβλημα διαφορετικό απο το Διακριτό Λογαριθμικό Πρόβλημα και το Πρόβλημα Παραγοντοποίησης. Επίσης, το πρόβλημα δεν θα πρέπει να έχει λύση υπο-εκθετικού χρόνου μέσω ενός αλγορίθμου.

Η συνδυαστική θεωρία ομάδων είναι ένα γόνιμο έδαφος για να βρούμε δύσκολα προβλήματα που μπορούν να χρησιμοποιηθούν ως βάσεις για κρυπτογραφικά συστήματα.

Θα ήθελα σε αυτό το σημείο να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κ. Ευάγγελο Ράπτη, για το ενδιαφέρον θέμα της παρούσης διπλωματικής και την παρότρυνσή του να ασχοληθώ με αυτό. Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένεια μου και ιδιαίτερα την αδερφή μου που είναι πάντα δίπλα μου και με στηρίζουν. Τέλος, τους φίλους μου Ντίνο και Ναυσικά, για τα χρόνια που περάσαμε μαζί.

Περιεχόμενα

Κεφάλαιο 1

Κανονική Μη-μεταθετική Κρυπτογραφία

1.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα εξετάσουμε διάφορα κρυπτογραφικά πρωτόκολλα που χρησιμοποιούν μη-μεταθετικές (ημί)ομάδες ως πλατφόρμες ή βάσεις, αλλά ταυτόχρονα δεν ξεκινάνε από το κανονικό παράδειγμα ενός πρωτοκόλλου για το δημόσιο κλειδί, το οποίο είναι βασισμένο σε μονόδρομη συνάρτηση. Σε αυτό το κεφάλαιο περιλαμβάνουμε το πρωτόκολλο Anshel-Anshel-Goldfeld, όπως και πρωτόκολλα που είναι πιο κοντά στο πνεύμα των κλασσικών πρωτοκόλλων που βασίζονται στις μεταθετικές (ημί)ομάδες.

1.2 Πρωτόκολλα που βασίζονται στο πρόβλημα αναζήτησης συζυγίας

Αρχικά, θα αναφέρουμε κάποιους βασικούς ορισμούς. Ξεκινάμε έχοντας μια ομάδα G με επιλύσιμο το πρόβλημα της λέξης (word problem).

Ορισμός 1.1. *Για $w,a \in G$ ο συμβολισμός w^a αντιστοιχεί στο $a^{-1}wa$.*

□

Ορισμός 1.2. *Πρόβλημα Λέξης (Word Problem).*
Για μία δοσμένη, πεπερασμένη ομάδα G, που δίνεται με αναδρομικό τύπο και ένα στοιχείο $w \in G$, θέλουμε να δείξουμε εάν $w = 1$ στην G.

□

Παρατηρούμε από την περιγραφή του Προβλήματος Λέξης ότι αποτελείται από δύο μέρη: *ισχύει* και *δεν ισχύει*. Τα ονομάζουμε μέρη *ναί* και *όχι* αντίστοιχα.

Υπενθυμίζουμε ότι:

Ορισμός 1.3. *Πρόβλημα Απόφασης Συζυγίας (ή conjugacy problem ή conjugacy decision problem).*
Έστω G μια ομάδα. Δίνονται δύο στοιχεία u, $v \in G$. Να εξετάσουμε αν υπάρχει $x \in G$ τέτοιο ώστε $u^x = v$.

□

Ορισμός 1.4. *Πρόβλημα Αναζήτησης Συζυγίας (ή conjugacy search problem ή witness conjugacy problem).*
Δίνονται δύο στοιχεία a, $b \in G$. Για κάποιο $x \in G$ ισχύει ότι $u^x = v$. Να εξετάσουμε αν υπάρχει τουλάχιστον ένα συγκεκριμένο x που να ικανοποιεί την συνθήκη.

□

Ορισμός 1.5. *Συζυγές στοιχείο .*

Δύο στοιχεία u, $v \in G$ λέμε ότι είναι συζυγά μεταξύ τους όταν $v = g^{-1}ug$, για κάποιο $g \in G$. Το συμβολιζουμε $u \sim v$.

□

Το Πρόβλημα Αναζήτησης Συζυγίας (ή conjugacy search problem) παρουσιάζει πολύ μεγάλο ενδιαφέρον στην θεωρία ομάδων. Αντιθέτως, το Πρόβλημα Απόφασης Συζυγίας (ή conjugacy decision problem) είναι ενδιαφέρον από την σκοπιά της θεωρίας πολυπλοκότητας, αλλά όχι της θεωρίας ομάδων.

Πράγματι, αν γνωρίζουμε ότι το u είναι συζυγές (conjugate to) του v, μπορούμε απλά να πάμε στην μορφή u^x και να το συγκρίνουμε με το v κάθε φορά, έως ότου βρούμε ότι ταιριάζουν.

Έδω καταλήγουμε σε κάτι προφανές: Μια ομάδα με επιλύσιμο το Πρόβλημα Συζυγίας (ή αλλίως το conjugacy problem) έχει επίσης επιλύσιμο το Πρόβλημα Λέξης (ή αλλιώς το word problem). Αυτός ο ευθύς αλγόριθμος έχει πολυπλοκότητα $O(2^n)$.

Ορισμός 1.6. *Πολυπλοκότητα Αλγορίθμου.*
Σε έναν αλγόριθμο, ο χρόνος πολυπλοκότητας ή πολυπλοκότητα αλγορλίθμου είναι η ποσότητα χρόνου που χρειάζεται ένας αλγόριθμος, εφόσον του εισάγουμε δεδομένα, για να τρέξει και να βρει αποτέλεσμα.
Συγκεκριμένα, η πολυπλοκότητα χαρακτηρίζεται ασυμπτωτική, όταν τείνει στο άπειρο.

Έαν ολες οι εισαγώμενες μεταβλητές είναι μεγέθους n, τότε ο χρόνος που απαιτείται παίρνει το n με τον μεγαλύτερο εκθέτη, π.χ. $5(n^3) + 3n$ *τοτε* $O(n^3)$.
Γραμμική πολλαπλότητα έχουμε όταν O(n) και εκθετική πολλαπλότητα όταν $O(2^n)$.

□

Επιπλέον, αν δεν είναι γνωστός άλλος αλγόριθμος για το Πρόβλημα Αναζήτησης Συζυγίας (conjugacy search problem) σε μία ομάδα G , είναι λογικό να υποστηρίξουμε ότι η $x \longrightarrow u^x$ είναι μία μονόδρομη συνάρτηση και να κατασκευάσουμε ένα κρυπτογραφικό πρωτόκολλο (δημοσίου κλειδιού).
Ξεκινάμε με ένα απλό πρωτόκολλο που οφείλεται στους Ko, Lee:

1. Δημοσιεύεται ένα στοιχείο $w \in G$.
2. Η Μαριέττα επιλέγει ένα προσωπικό στοιχείο $a \in G$ και στέλνει το w^a στον Μάρκο.
3. Ο Μάρκος διαλέγει ένα προσωπικό στοιχείο $b \in G$ και στέλνει το w^b στην Μαριέττα.
4. Η Μαριέττα υπολογίζει $(w^b)^a = w^{ba}$ και ο Μάρκος υπολογίζει $(w^a)^b = w^{ab}$.

Εάν τα a και b επιλέγονται από ένα σύνολο αντιμεταθετικών στοιχείων της ομάδας G, τότε ab=ba. Επομένως, η Μαριέττα και ο Μάρκος παίρνουν ένα κοινό ιδιωτικό

κλειδί, το $w^{ab} = w^{ba}$. Τυπικά, υπάρχουν δυο δημόσιες υποομάδες A και B της ομάδας G, πράγμα που παίρνουμε από τα πεπερασμένα ζευγάρια που δημιουργούν το ab=ba για a ∈ A, b ∈ B. Το να επιλέξουμε την κατάλληλη ομάδα πλατφόρμας (platform group) για το παραπάνω πρωτόκολλο είναι ένα μηδαμινό θέμα.

Στην συνέχεια παραθέτουμε κάποιες απαραίτητες προυποθέσεις που πρέπει να ικανοποιεί η ομάδα πλατφόρμας:

(Σ0) Η ομάδα πρέπει να είναι γνωστή. Πιο συγκεκριμένα θα πρέπει το Πρόβλημα Αναζήτησης Συζυγίας (conjugacy search problem) στην ομάδα είτε να είναι πολύ καλά μελετημένο είτε να μπορεί να περιοριστεί σε ενα αρκετά γνωστό πρόβλημα (ίσως σε κάποιο άλλο τομέα των μαθηματικών).

Αυτή η συνθήκη, παρόλο που δεν είναι μαθηματική, είναι σημαντική εάν θέλουμε το κρυπτογραφικό αποτέλεσμα να χρησιμοποιείται στην πραγματικότητα. Σημειώνουμε ότι αυτή η συνθήκη μειώνει αρκετά τις υποψήφιες ομάδες.

(Σ1) Το Πρόβλημα Λέξης (word problem) στην G πρέπει να έχει μικρή πολλαπλότητα (O(n) ή O(2^n)) σε έναν αλγόριθμο. Ακόμα καλύτερα, θα μπορούσε τα στοιχεία της G να έχουν αποτελεσματικά υπολογίσιμη ¨κανονική μορφή¨.

Αυτό απαιτείται για την αποτελεσματική επιλογή δημοσίου κλειδιού ή για το στάδιο επαλήθευσης σε ένα πρωτόκολλο γνησιότητας.

(Σ2) Το Πρόβλημα Αναζήτησης Συζυγίας (conjugacy search problem) *δεν* θα πρέπει να έχει λύση υπο-εκθετικού χρόνου (ή subexponential-time solution) από έναν πεπερασμένο αλγόριθμο.

Σε αυτό το σημείο πρέπει να τονίσουμε ότι το να αποδείξουμε πως η ομάδα ικανοποιεί την συνθήκη (Σ2) είναι εξαιρετικά δύσκολο, αλλά όχι αδύνατο. Αυτό, είναι στην πραγματικότητα πρόβλημα χιλίων δολλαρίων.

Η συνθήκη (Σ2) θα πρέπει από εδώ και στο εξής να συνδέεται με τη συνθήκη (Σ0). Η μοναδική απόδειξη ότι η ομάδα G έχει αυτή την ιδιότητα είναι το γεγονός ότι πάρα πολλοί μαθηματικοί μελέτησαν το Πρόβλημα Αναζήτησης Συζυγίας (conjugacy search problem) της G για πολύ καιρό.

(Σ3) Θα πρέπει να υπάρχει κάποιος τρόπος να μεταμφιέζουμε τα στοιχεία της G έτσι ώστε να είναι απίθανο να βρίσκουμε το x από το $x^{-1}wx$ με έναν απλό έλεγχο.

Αυτή η συνθήκη μπορεί να μην είναι αρκετά φορμαλιστική αλλά έχει μεγάλη σημασία για τις εφάρμογες.
Ένας τρόπος για να το πετύχουμε είναι να έχουμε κανονική μορφή (normal form) τα στοιχεία της G.

Το να έχουμε κανονική μορφή για τα στοιχεία μίας ομάδας είναι πολύ χρήσιμο, αφού μας δίνει την δυνατότητα να συγκρίνουμε δύο στοιχεία και να βρούμε λύση για το Πρόβλημα Λέξης.

Εάν δεν έχουμε κανονική μορφή και η ομάδα G δίνεται μέσω γεννητόρων και κάποιων σχέσεων χωρίς περαιτέρω πληροφορίες για τις ιδιότητες της G, τότε θα πρέπει τουλάχιστον αυτές οι σχέσεις να είναι πολύ μικρές.

(Σ4) Η G θα πρέπει να είναι μια ομάδα με υπερ-πολυωνυμική (εκθετική ή μεσαία (intermediate)) ανάπτυξη.

Αυτό σημαίνει ότι ο αριθμός των στοιχείων μήκους n της G θα πρέπει να αυξάνεται γρηγορότερα από ένα οποιαδήποτε πολυώνυμο του n. Ακόμα, όταν χρησιμοποιούμε τον όρο **μήκος στοιχείου** συνήθως εννοούμε το μέγεθος της λέξης που αντιπροσωπεύει ένα στοιχείο της ομάδας. Μπορεί ακόμα να σημαίνει το μήκος κάποιας άλλης περιγραφής, π.χ. πολυπλοκότητα πληροφορίας.

Ορισμός 1.7. *Κανονική μορφή (normal form) των στοιχείων μιας ομάδας G.*

Για να έχουν τα στοιχεία μίας ομάδας G κανονική μορφή (normal form) υπάρχει ένας αλγόριθμος που μετατρέπει οποιαδήποτε είσοδο u_{in}, που είναι μια λέξη στις γεννήτριες της G, σε μία έξοδο u_{out} , που είναι άλλη λέξη στους γεννήτορες της G, έτσι ώστε $u_{in} = u_{out}$ στην ομάδα G, το οποίο είναι δύσκολο να διακρίνεις με απλό έλεγχο.

□

Ορισμός 1.8. *Εκθετική (exponential), Μεσαία (intermediate), υπο-εκθετική (subexponential) ανάπτυξη ομάδας.*

Ας είναι $S = \{s_1, ..., s_k\}$ ένα πεπερασμένο σύνολο που δημιουργείται από στοιχεία της ομάδα $G = \langle S \rangle$. Για κάθε στοιχείο της ομάδας $g \in G$ συμβολίζουμε με $l(g) = l_s(g)$

το μήκος της μικρότερης διάσπασης $g = s_{i_1}^{\pm 1} ... s_{i_l}^{\pm 1}$. *Το σύμβολο* $\gamma_G^S(n)$ *αντιστοιχεί στον αριθμό των στοιχείων* $g \in G$, *τέτοια ώστε* $l(g) \leq n$. *Η συνάρτηση* $\gamma = \gamma_G^S$ *ονομάζεται συνάρτηση ανάπτυξης της ομάδας* G *σε σχέση με το σύνολο* S. *Είναι ξεκάθαρο ό,τι* $\gamma(n) \leq \sum_{i=0}^{n} (2k)^i \leq (2k+1)^n$

Μια συνάρτηση f ονομάζεται εκθετική (exponential) εάν $f(n) \sim e^n$.

Μια συνάρτηση f ονομάζεται υπερ-πολυωνυμική εάν $\lim_{n\to\infty} \frac{\ln \gamma(n)}{\ln n} = \infty$.

Για παράδειγμα, οι $n^e e^n$ *και* $exp(\frac{n}{2} - \sqrt{n} \log n)$ *ονομάζονται εκθετικές (exponential), η συναρτήση* $e^{\frac{n}{\log n}}$ *ονομάζεται υπο-εκθετική (subexponential), ενώ η* n^n *δεν είναι τίποτα απο τα δύο. Ακόμα η* n^n *είναι υπερ-πολυωνυμική (superpolynomial), όπως και η* $e^{\frac{n}{\log n}}$.

Τέλος, η συνάρτηση f λέμε οτι εχει μεσαία ανάπτυξη (intermediate growth) εάν είναι και υπο-εκθετική (subexponential) και υπερ-πολυωνυμική (superpolynomial), για παράδειγμα $n^{\log logn}$, $e^{\sqrt{n}}$ *έχουν μεσαία ανάπτυξη intermediate growth.*

Έστω S *ένα πεπερασμένο σύνολο που δημιουργείται απο στοιχεία της ομάδα* G, *η συνάρτηση ανάπτυξης της είναι η* $\gamma = \gamma_G^S$. *Το όριο* $\lim_{n\to\infty} \frac{\ln \gamma(n)}{n}$ *πάντα υπάρχει. Το όριο αυτό ονομάζεται βαθμός ανάπτυξης της* G.

Κάθε ομάδα G *έχει είτε επο-εκθετική (subexponential) είτε υπερ-πολυωνυμική (exponential) ανάπτυξη.*

Βλ.[6]

□

Υπάρχουν ομάδες που ικανοποιούν τις συνθήκες (Σ1), (Σ4). Είναι πολύ πιθανόν να ικανοποιούν και την (Σ2) και κατά συνέπεια να ικανοποιούν την (Σ3). Υπάρχουν ομάδες που έχουν επιλύσιμο το Πρόβλημα Λέξης (word problem) αλλά άλυτο το Πρόβλημα Συζυγίας (conjugacy problem).

1.3 Πρωτόκολλα βασισμένα στο Πρόβλημα Αποσύνθεσης

Μία από τις συνέπειες του Προβλήματος Αναζήτησης Συζυγίας (conjugacy search problem) είναι το:

Ορισμός 1.9. *Πρόβλημα Αποσύνθεσης (decompostition problem).*
Δίνονται δύο στοιχεία $w, w' \in G$. Θέλουμε να βρούμε δύο στοιχεία x και y που να ανήκουν σε ένα δοσμένο υποσύνολο $A \subseteq G$ και να ικανοποιείται η σχέση $x \cdot w \cdot y = w'$, με δεδομένο ότι ένα τέτοιο ζευγάρι στοιχείων υπάρχει .

□

Στην περίπτωση που το A είναι υποομάδα, το πρόβλημα είναι επίσης γνωστό ως το πρόβλημα των δύο σύμπλοκων (ή double coset problem).

Ορισμός 1.10. *Έστω G μία ομάδα και $H \leq G$. Ορίζουμε αριστερό ένα σύνολο της μορφής $gH = \{gh : h \in H\}$ και δεξιό σύμπλοκο ένα σύνολο της μορφής $Hg = \{hg : h \in H\}$.*

□

Γνωρίζουμε ότι τα αριστερά σύμπλοκα είναι σε αμφιμονοσήμαντη αντιστοιχία με τα δεξιά σύμπλοκα της H.

$$\mathrm{gH} \longleftrightarrow Hg^{-1}$$

Το πλήθος των αριστερών συμπλόκων της H είναι ίσο με το πλήθος των δεξιών συμπλόκων της H. Βλ [7]

Παρατηρούμε οτι πάντα υπάρχουν κάποια x και y που ικανοποιούν την ισότητα $x \cdot w \cdot y = \mathrm{w}'$. Για παράδειγμα εάν πάρουμε $\mathrm{x} = 1$ τότε έχουμε $\mathrm{y} = w^{-1}w'$, οπότε το ζητούμενο είναι να ικανοποιούν την συνθήκη $\mathrm{x}, \mathrm{y} \in \mathrm{A}$. Αυτός είναι και ο λόγος που συνήθως δεν αναφερόμαστε σε αυτό ως το Προβλημα Αποσύνθεσης μίας υποομάδας, διότι πάντα θα είναι υποομάδα η A.

Παρατήρηση 1.11. *Στην παράγραφο 1.7 θα δείξουμε ότι αν κάποιος θέλει να κλέψει το δημόσιο κλειδί από το πρωτόκολλο Ko-Lee ή κάποιο άλλο παρόμοιο πρωτόκολλο δεν θα του αποφέρει κανένα αποτέλεσμα λύνοντας το Πρόβλημα Έρευνας Συζυγίας. Είναι αρκετό να λύσει το Πρόβλημα Αποσύνθεσης.*

Προσέχουμε ότι η συνθήκη $\mathrm{x}, \mathrm{y} \in \mathrm{A}$ μπορεί να μην είναι εύκολο να αποδειχθεί για κάποια υποσύνολα του A.

Το αντίστοιχο πρόβλημα ονομάζεται Πρόβλημα Απόφασης (membership (decision) problem). Κάποιοι ερευνητές ανέφεραν πως αν κάποιος χρησιμοποιήσει ωμή βία, απλά πηγαίνοντας σε κάθε ένα στοιχείο του A την φορά, η παραπάνω συνθήκη θα ικανοποιηθεί αυτόματα. Αυτό, όμως, δεν μπορεί να πραγματοποιηθεί με άλλες πιο πρακτικές μεθόδους.

Επιπλέον, παρατηρούμε ότι το Πρόβλημα Αναζήτησης Συζυγίας είναι μία ειδική περίπτωση του Προβλήματος Αποσύνθεσης, όπου το w′ είναι συζυγές με το w και x=y^{-1}.

Στην συνέχεια δίνουμε μια τυπική περιγραφή του πρωτοκόλλου που βασίζεται στο Πρόβλημα Αποσύνθεσης.
Έχουμε μια δημόσια γνωστή ομάδα G και δύο δημόσιες υποομάδες A, B ⊆ G τα στοιχεία των οποίων θα πρέπει να ικανοποιούν την σχέση ab = ba, για οποιαδήποτε a ∈ A, b ∈ B.

1. Η Μαριέττα διαλέγει τυχαία δύο ιδιωτικά στοιχεία $a_1, a_2 \in$ A. Στην συνέχεια στέλνει το στοιχείο $a_1 w a_2$ στον Μάρκο.

2. Ο Μάρκος διαλέγει τυχαία δύο ιδιωτικά στοιχεία $b_1, b_2 \in \mathbf{B}$. Στην συνέχεια στέλνει το στοιχείο $b_1 w b_2$ στην Μαριέττα.

3. Η Μαριέττα υπολογίζει $K_A = a_1 b_1 w b_2 a_2$ και ο Μάρκος υπολογίζει $K_B = b_2 a_1 w b_1 a_2$. Εφόσον $a_i b_i = b_i a_i$ στην G , έχουν $K_A = K_B =$ K, το οποίο είναι το κοινό μυστικό κλειδί της Μαριέττας και του Μάρκου.

Στην συνέχεια θα ασχοληθούμε με παραλλαγές του παραπάνω πρωτοκόλλου.
‘

1.3.1 Συνεστραμένο (ή Twisted) Πρωτόκολλο

Η ιδέα αυτού του πρωτοκόλλου οφείλεται στους Shpilrain και Ushakov. Ουσιαστικά, ακολούθησαν την ιδέα του παραπάνω πρωτοκόλλου, αλλά με κάποιες τροποποιήσεις. Πράγμα το οποίο τον καθιστά ασφαλέστερο (τουλάχιστον για κάποιες επιλογές της ομάδας πλατφόρμας) στις length based επιθέσεις ή αλλιώς στις επιθέσεις μήκους .

Θεωρούμε μία ομάδα G και δύο γνωστές υποομάδες A,B ≤ G.

1. Η Μαριέττα επιλέγει τυχαία τα στοιχεία $a_1 \in$ A και $b_1 \in$ B. Στην συνέχεια στέλνει το στοιχείο $a_1 w b_1$ στον Μάρκο.

2. Ο Μάρκος επιλέγει τυχαία τα στοιχεία $b_2 \in$ B και $a_2 \in$ A. Στην συνέχεια στέλνει το στοιχείο $b_2 w a_2$ στην Μαριέττα.

3. Η Μαριέττα υπολογίζει $K_A = a_1 b_2 w a_2 b_1 = b_2 a_1 w b_1 a_2$ και ο Μάρκος υπολογίζει $K_B = b_2 a_1 w b_1 a_2$. Εφόσον $a_i b_i = b_i a_i$ στην G , έχουμε οτι $K_A = K_B = K$. Αυτό είναι το μυστικό κοινό κλειδί της Μαριέττας και του Μάρκου.

Όπως παρατηρούμε η ασφάλεια αυτού του πρωτοκόλλου βασίζεται σε μία πιο γενική μορφή του Προβλήματος Αποσύνθεσης.

1.3.2 Απόκρυψη μίας εκ των υποομάδων

Όπως και το συνεστραμένο (Twisted) πρωτόκολλο, έτσι και αυτή η ιδέα οφείλεται στους Shpilrain και Ushakov. Ξεκινώντας θα σκιαγραφήσουμε την ιδέα αυτή.

Έστω μια ομάδα G και ένα στοιχείο που ανήκει σε αυτήν, g ∈ G.

Ορισμός 1.12. *Κεντροποιούσα υποομάδα.*
Ορίζουμε την κεντροποιούσα υποομάδα του g στην G ως το σύνολο των στοιχείων h∈G έτσι ώστε hg=gh και τη συμβολίζουμε ως εξής:

$$C_G(g) = \{g \in G : gh = hg\}$$

Έστω ένα σύνολο $S = \{g_1, g_2, ..., g_k\} \subseteq G$. Ορίζουμε την κεντροποίουσα υποομάδα του συνόλου S στην G , που την συμβολίζουμε ως $C_G(g_1, g_2, ..., g_k)$. Η υποομάδα αυτή είναι η τομή των κεντροποιών υποομάδων $C_G(g_i)$, i=1,...,k. Βλ [7]

□

Δίνεται ένα δημόσιο w ∈ G . Η Μαριέττα επιλέγει ένα προσωπικό $a_1 \in$ G και δημοσιέυει μια υποομάδα B $\subseteq C_G(a_1)$. (Σε αυτό το σημείο υποθέτουμε ότι το B μπορεί να υπολογιστεί έυκολα). Παρόμοια, ο Μάρκος επιλέγει ένα προσωπικό $b_2 \in$ G και δημοσιέυει μια υποομάδα A $\subseteq C_G(b_2)$. Η Μαριέττα τότε επιλέγει $a_2 \in$A και στέλνει

$w_1 = a_1 w a_2$ στον Μάρκο, ενώ ο Μάρκος επιλέγει $b_1 \in$B και στέλνει $w_2 = b_1 w b_2$ στην Μαριέττα.

Αντιμετωπίζουμε, όμως, ένα πρόβλημα: Θέλουμε να βρούμε a_1 και a_2 έτσι ώστε $w_1 = a_1 w a_2$, όπου $a_2 \in$A. Όμως, δεν υπάρχει κάτι πού να μας υποδεικνύει πού να ανήκει το a_1. Για αυτό το λόγο πριν κάποιος πραγματοποιήσει μια επιθέση μήκους, θα πρέπει πρώτα να υπολογίσει τους γεννήτορες της κεντροποιούσας υποομάδας $C_G(B)$ (επειδή $a_1 \in C_G(B)$). Αυτό αποτελεί συνήθως ένα αρκετά δύσκολο πρόβλημα, αφου πρέπει να βρεθεί η τομή των κεντροποιών υποομάδων κάθε μεμονομένου στοιχείου. Η εύρεση των γεννητόρων της τομής των υποομάδων είναι δύσκολο πρόβλημα για τις περισσότερες υποομάδες.

Στην συνέχεια δίνουμε μία επίσημη περιγραφή του πρωτοκόλλου. Ως συνηθως η ομάδα G είναι γνωστή και δημόσια, αφήνουμε και το w$\in$ G να είναι δημόσιο επίσης.

1. Η Μαριέττα επιλέγει ένα στοιχείο $a_1 \in$ G όπως και μια υποομάδα της $C_G(a_1)$ και δημοσιεύει τους γεννήτορες της, το σύνολο A $= \{a_1, ...a_k\}$.

2. Ο Μάρκος επιλέγει ένα στοιχείο $b_2 \in$ G όπως και μια υποομάδα της $C_G(b_2)$ και δημοσιεύει τους γεννήτορες της, το σύνολο B $= \{\beta_1, ..., \beta_m\}$.

3. Η Μαριέττα επιλέγει ένα τυχαίο στοιχείο $a_2 \in \langle \beta_1, ..., \beta_m \rangle$ και στέλνει $P_A = a_1 w a_2$ στον Μάρκο.

4. Ο Μάρκος επιλέγει ένα τυχαίο στοιχείο $b_1 \in \langle a_1, ..., a_k \rangle$ και στέλνει $P_B = b_1 w b_2$ στην Μαριέττα.

5. Η Μαριέττα υπολογίζει $K_A = a_1 P_B a_2$.

6. Ο Μάρκος υπολογίζει $K_B = b_1 P_A b_2$.
   Εφόσον γνωρίζουμε ότι ισχύει $a_1 b_1 = b_1 a_1$ και $a_2 b_2 = b_2 a_2$ έχουμε καταλήξει στο K $= K_A = K_B$, το οποίο είναι το κοινό ιδιωτικό κλειδί.

‘

1.3.3 Τριπλό Πρόβλημα Αποσύνθεσης

Σε αυτήν την παράγραφο παρουσιαζεται το πρωτόκολλο ανταλλαγής κλειδιού που βασίζεται στο Τριπλό Πρόβλημα Αποσύνθεσης, το οποίο οφείλεται στην Kurt. Αυτή η

μέθοδος χρησιμοποιεί μη-μεταθετικές ομάδες και είναι σχεδιασμένη έτσι ώστε να αντιμετωπίζει τις αδυναμίες των προηγούμεων πρωτοκόλλων, συγκεκριμένα το πρωτόκολλο των Diffie-Hellman-like.

Η βελτίωση αυτή αφείλεται στο γεγονός ότι η σχέση μεταξύ δημοσίου και ιδιωτικού κλειδιού δεν είναι πλέον μόνο γραμμική. Συγκεκριμένα, κάποιος θα πρέπει να λύσει και τετραγωνικές σχέσεις και γραμμικές, ώστε να βρεί το κλειδί που δουλεύει.

Το Τριπλό Πρόβλημα Αποσύνθεσης (triple decomposition problem) είναι μια μορφή του Προβλήματος Αποσύνθεσης.

Ορισμός 1.13. *Τριπλό Πρόβλημα Αποσύνθεσης (triple decomposition problem). Ένα γνωστό στοιχείο παραγοντοποιείται σε γινόμενο τριών άγνωστων παραγόντων.*

□

Υπενθυμίζουμε ότι στο σύνηθες Πρόβλημα Αποσύνθεσης ενα γνωστό στοιχείο παραγοντοποιείται σε γινόμενο τριών παραγόντων, όπου οι δύο είναι άγνωστοι και ο ένας (ο μεσαίος) είναι γνωστός.

Στο πρωτόκολλο της Kurt το ιδιωτικό κλειδί έχει τρία στοιχεία. Η ιδέα είναι να κρύψουμε καθένα από αυτά πολλαπλασιάζοντάς τα με τυχαία στοιχεία που ανήκουν σε μια γνωστή ομάδα. Το σημαντικό σημείο είναι ότι ένα από τα στοιχεία αυτά πολλαπλασιάζεται κι από αριστερά κι από δεξιά.

Στην συνέχεια θα περιγράψουμε το πρωτόκολλο.

Ορισμός 1.14. *Ημιομάδα και Μονοειδές.*

Έστω A ένα σύνολο διάφορο του κενού και εφοδιασμένο με μία εσωτερική πράξη $*$ *, δηλαδή* $* : A \times A \longrightarrow A$*. Τότε η δομή (A,*$*) καλείται:*

1. *ημιομάδα, αν η πράξη είναι προσεταιριστική, δηλαδή αν ισχύει*

$$a * (b * c) = a * b * c \ , \forall \ a, \ b \ , \ c \in A$$

2. *μονοειδές , αν είναι ημιομάδα και επιπλέον η πράξη έχει ουδέτερο στοιχείο. Δηλαδη αν υπάρχει στοιχείο του A, το οποίο το συμβολίζουμε με e και καλούμε ουδέτερο στοιχείο, τέτοιο ώστε*

$$a * e = e * a = a$$

Ορισμός 1.15. *Έστω G μονοειδές. Χρησιμοποιούμε τον συμβολισμό [A , B] = 1 για δύο υποσύνολα A , B του G όταν ab = ba , ∀ a ∈ A , b ∈ B.*

□

Το Πρωτόκολλο

Υπάρχει μία δημόσια ομάδα πλατφόρμας (ή μονοειδές) G που είναι μη-μεταθετική και δύο σύνολα από υποσύνολα του G, έστω A = $\{A_1, A_2, A_3, X_1, X_2\}$ και B = $\{B_1, B_2, B_3, Y_1, Y_2\}$ που ικανοποιούν τις δύο εξής συνθήκες : (Βλ[8])

- **(Συνθήκη Αντιστρεψιμότητας)** Τα στοιχεία X_1, X_2, Y_1, Y_2 είναι αντιστρέψιμα.
- **(Συνθήκες Μεταθετικότητας)** $[A_2 , Y_1] = 1$, $[A_3 , Y_2] = 1$, $[B_1 , X_1] = 1$, $[B_2 , X_2] = 1$.

Ρύθμιση του ιδιωτικού και του δημόσιου κλειδιού

Υποθέτουμε ότι έχουμε ένα μονοειδές G και τα υποσύνολα A = $\{A_1, A_2, A_3, X_1, X_2\}$ και B = $\{B_1, B_2, B_3, Y_1, Y_2\}$, τα οποία ικανοποιούν τις παραπάνω συνθήκες. Η Μαριέττα και ο Μάρκος ακολουθούν τα παρακάτω βήματα.

1. Η Μαριέττα και ο Μάρκος συμφωνούν στο ποιός θα χρησιμοποιήσει το κάθε υποσύνολο. Υποθέτουμε ότι η Μαριέττα θα χρησιμοποιήσει το A και ο Μάρκος το B.

2. Η Μαριέττα επιλέγει τυχαία τα στοιχεία $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$, $x_1 \in X_1$, $x_2 \in X_2$ και υπολογίζει

$$\mathrm{u} = a_1x_1,\ \mathrm{v} = x_1^{-1}a_2x_2 \text{ και } \mathrm{w} = x_2^{-1}a_3.$$

   Το ιδιωτικό κλειδί της είναι (a_1, a_2, a_3) και το δημόσιο κλειδί της είναι (u, v, w).

3. Ο Μάρκος επιλέγει τυχαία τα στοιχεία $b_1 \in B_1$, $b_2 \in B_2$, $b_3 \in B_3$, $y_1 \in Y_1$, $y_2 \in Y_2$ και υπολογίζει

$$\mathrm{p} = b_1y_1,\ \mathrm{q} = y_1^{-1}b_2y_2 \text{ και } \mathrm{r} = y_2^{-1}b_3.$$

   Το ιδιωτικό κλειδί του είναι (b_1, b_2, b_3) και το δημόσιο κλειδί του είναι (p, q, r).

Ανταλλαγή κλειδιού

Για να συμφωνήσουν σε ένα κλειδί η Μαριέττα και ο Μάρκος κάνουν τα εξής:

1. Η Μαριέττα στέλνει στον Μάρκο το δημόσιο κλειδί της (u, v, w).

2. Ο Μάρκος στέλνει στην Μαριέττα το δημόσιο κλειδί του (p, q, r).

3. Η Μαριέττα υπολογίζει

   $a_1 p a_2 q a_3 r = a_1(b_1 y_1) a_2 (y_1^{-1} b_2 y_2) a_3 (y_2^{-1} b_3) = a_1 b_1 a_2 b_2 a_3 b_3 = K_A.$

4. Ο Μάρκος υπολογίζει

   $u b_1 v b_2 w b_3 = (a_1 x_1) b_1 (x_1^{-1} a_2 x_2) b_2 (x_2^{-1}) a_3 b_3 = a_1 b_1 a_2 b_2 a_3 b_3 = K_B.$

   Επομένως, $K_A = K_B =$ K είναι το κοινό μυστικό κλειδί της Μαριέττας και του Μάρκου.

Η ιδέα είναι να κρύψουμε το ιδιωτικό κλειδί πολλαπλασιάζοντας κάθε παράγοντα με κάποια στοιχεία που ανήκουν στο μονοειδές. Αυτά τα στοιχεία επιλέγονται από υποσύνολα που ικανοποιούν τις συνθήκες που αναφέραμε παραπάνω, έτσι ώστε και οι δύο μεριές να καταλήξουν στο ίδιο κλειδί. Παρατηρούμε σε αυτό το σημείο ότι δεν υπάρχουν συνθήκες που πρέπει να ικανοποιούν τα υποσύνολα A_1 και B_3. Εάν δεν υπάρχει πρόβλημα στην ασφάλεια τότε μπορεί να επιλέγονται με συγκεκριμένο τρόπο, προκειμένου το σύστημα να γίνει πιο πρακτικό (για παράδειγμα τα κλειδιά να έχουν πιο μικρό μήκος).

Η Ασφάλεια

Κάποιες επιλογές για τα υποσύνολα στο παραπάνω πρωτόκολλο έχουν ως αποτέλεσμα τον άμεσο υπολογισμό του κοινού κλειδιού από τα ιδιωτικά. Εάν αποφύγουμε αυτές τις περιπτώσεις τότε ο μόνος τρόπος να γίνει επίθεση στο σύστημα είναι να ασχοληθούν με εξισώσεις που αφορούν το δημόσιο και το ιδιωτικό κλειδί, δηλαδή να λύσουν τις ακόλουθες εξισώσεις:

$$a_1 x_1 = \mathrm{u}$$
$$x_1^{-1} a_2 x_2 = \mathrm{v}$$
$$x_2^{-1} a_3 = \mathrm{w}$$

για a_1, x_1, a_2, x_2, a_3 που ικανοποιούν τις συνθήκες αντιστρεψιμότητας και μεταθετικότητας. Αυτές οι συνθήκες συναντιούνται εάν είναι βέβαιο ότι τα x_1, a_2, x_2, a_3 ανήκουν στα X_1, A_2, X_2, A_3 αντίστοιχα. Επομένως, το πρόβλημα είναι να αναλύσουμε τα v και w σε στοιχεία των αντίστοιχων υποσυνόλων, ώστε αν αντιστρέψουμε το τελευταίο στοιχείο του v αυτό να είναι το πρώτο του w. Σε αυτό το σημείο σημειώνουμε πως επειδή δεν υπάρχουν περιορισμοί για το a_1 , εφόσον το x_1 βρεθεί, το u μπορεί να αναλυθεί στο a_1x_1 , και παίρνουμε $a_1 = \mathrm{u}\ x_1^{-1}$. Βλ[8].

Για να λύσουμε την δεύτερη εξίσωση απαιτείται το v να αναλυθεί σε τρία στοιχεία, ενώ για την τρίτη απαιτείται το w να αναλυθεί σε δυο. Η βασική διαφορά αυτού του πρωτοκόλλου σε σχέση με τα προηγούμενα, που βασίζονται πάνω σε μη-μεταθετική άλγεβρα, είναι ότι κάποιος θα πρέπει να αντιμετωπίσει δευτεροβάθμιες σχέσεις που με διάσπαση γίνεται το Τριπλό Πρόβλημα Αποσύνθεσης. Σε αυτό το σημείο το πρόβλημα μπορεί να οριστεί ως :

Ορισμός 1.16. *Έστω G ένα μη-μεταθετικό μονοειδές και X, Y, A υποσύνολα του G , όπου τα στοιχεία των X και Y είναι αντιστέψιμα και ικανοποιούν τις συνθήκες μεταθεσιμότητας. Το Τριπλό Πρόβλημα Αποσύνθεσης (triple decomposition problem) στο G αφορά την εύρεση των $x \in G$, $a \in A$ και $y \in Y$ με δεδομένο ότι $u = xay \in G$.*

□

Η ασφάλεια του συστήματος στηρίζεται στο Τριπλό Πρόβλημα Αποσύνθεσης. Εξαρτάται, δηλαδή, από την ομάδα που θα έχουμε ως πλατφόρμα και την επιλογή των υποσυνόλων. Σε αυτό το σημείο πρέπει να τονιστεί ότι όταν λέμε πως λύσαμε ένα πρόβλημα, δεν εννοούμε πως βρήκαμε το ιδιωτικό κλειδί σε κάποια συγκεκριμένη πλατφόρμα. Ανάλογα με την πλατφόρμα μπορούμε να σχεδιάσουμε-μετατρέψουμε το σύστημα σε ένα με διαφορετική δομή, όπου υπάρχουν τα εργαλεία για να αντιμετωπίσουμε τέτοιες εξισώσεις.

Παρακάτω θα αναλύσουμε τις περιπτώσεις στις οποίες το κοινό κλειδί μπορεί να υπολογιστεί από το δημόσιο κλειδί αμέσως. Επομένως, αυτές οι περιπτώσεις θα πρέπει να αποφεύγονται όταν θέλουμε να έχουμε ένα αξιοπιστό πρωτόκολλο.

Περιπτώσεις που πρέπει να αποφεύγονται

Θα αναφέρουμε περιπτώσεις όπου το κοινό κλειδί μπορεί να υπολογιστεί χωρίς να χρειαστεί να λυθεί το σύστημα των δευτεροβάθμιων που αναφέρθηκε παραπάνω και για

αυτό τον λόγο θα πρέπει να αποφεύγονται. Είναι προφανείς περιπτώσεις που δεν θα πρέπει να χρησιμοποιούνται σε οποιαδήποτε πλατφόρμα. (Βλ[8])

Οι περιπτώσεις που θα αναφερθούν παρακάτω επιτρέπουν τον άμεσο υπολογισμό του κοινού κλειδιού από τα δημόσια κλειδιά.

1. Εάν $[X_1 , Y_1] = 1$, $[X_2 , Y_1] = 1$, $[X_2 , Y_2] = 1$, τότε το κοινό κλειδί μπορεί να υπολογιστεί από το δημόσιο κλειδί, εάν :

$$(a_1x_1)(b_1y_1)(x_1^{-1}a_2x_2)(y_1^{-1}b_2y_2)(x_2a_3)(y_2a_3) = \text{upvqwr}.$$

2. Εάν $[A_2 , B_1] = 1$, $[A_3 , B_2] = 1$, $[A_3 , B_1] = 1$ τότε το κοινό κλειδί μπορεί να υπολογιστεί απο το δημόσιο κλειδί εάν:

$$(a_1a_2a_3)\ (b_1b_2b_3) = \text{uvwpqr}.$$

3. Για να μπορέσουμε να στηριχθούμε στην δεύτερη εξίσωση ($x_1^{-1}a_2x_2 = \text{v}$) σε ένα σύστημα πρέπει να εξασφαλίσουμε ό,τι η τρίτη εξίσωση έχει αρκετές λύσεις.

   Στην περίπτωση που υπάρχουν λίγες λύσεις της τρίτης εξίσωσης, η ασφάλεια του συστήματος στηρίζεται στο να αναλύσουμε ένα στοιχείο σε δύο στοιχεία : Πρώτα αναλύουμε το w σε $x_2^{-1}a_3$, στην συνέχεια αντικαθιστούμε το x_2^{-1} στην δεύτερη εξίσωση και τέλος αναλύουμε το vx_2^{-1} στο $x_1^{-1}a_2$.

   Μία άλλη περίπτωση που πρέπει να αποφεύγεται, ώστε να έχουμε ένα καλό πρόβλημα διάσπασης είναι η επόμενη :

4. Εάν $[A_2 , B_1] = 1$ και $[X_2 , B_1] = 1$ ή $[A_3 , B_2] = 1$ και $[A_3 , Y_1] = 1$, τότε η ασφάλεια του συστήματος βασίζεται στην δυσκολία της ανάλυσης ενός στοιχείου σε δύο στοιχεία.

Όταν $[A_2 , B_1] = 1$, το κοινό κλειδί είναι το $a_1a_2b_1b_2a_3b_3$. Πολλαπλασιάζοντας τα δύο πρώτα στοιχεία του δημόσιου κλειδιού της Μαριέττας, παίρνουμε την εξίσωση $a_1a_2x_2 = \text{uv}$. Πρέπει να ελέγξουμε, αν με την κοινή ύπαρξη του a_1a_2 στο κοινό κλειδί και στην παραπάνω εξίσωση δημιουργούνται τρωτά σημεία. Πρέπει να ερευνήσουμε εάν και πότε η ανάλυση του uv στο ax_2 , με $\text{a} \in \text{G}$, $x_2 \in X_2$ αρκεί για να υπολογίσουμε το κοινό κλειδί. Θα ελέγξουμε αν :

$$apqa_3r = \text{κοινό κλειδί.}$$

Αντικαθιστώντας pq $= b_1b_2y_2$ απο αριστερά στην παραπάνω εξίσωση και στην συνέχεια χρησιμοποιώντας $[A_3\ ,\ Y_2] = 1$ και a $= uvx_2^{-1}$ για την δεύτερη εξίσωση και $a_3 = x_2w$ απο δεξιά παίρνουμε :

$$a(b_1b_2y_2)a_3y_2^{-1}b_3 = (uvx_2^{-1})(b_1b_2)a_3b_3 = (uvx_2^{-1})(b_1b_2)x_2wb_3$$

Σημειώνουμε ότι το κοινό κλειδί είναι το $ub_1vb_2wb_3$. Η τελευταία εξίσωση επάνω ισούται με το κοινό κλειδί, εάν $[X_2\ ,\ B_1] = 1$, επειδή τότε έχουμε $vb_1 = b_1v$.

1.4 Πρωτόκολλο βασίσμένο στο Πρόβλημα Αναζήτησης Παραγόντων

Σε αυτή την παράγραφο περιγράφουμε ένα πρωτόκολλο το οποίο βασίζεται στο Πρόβλημα Αναζήτησης Παραγόντων (factorization search problem).

Ορισμός 1.17. *Πρόβλημα Αναζήτησης Παραγόντων (factorization search problem). Δίνεται ένα στοιχείο w της ομάδας G και δύο υποομάδες A,B $\leq$ G.*
Θέλουμε να βρούμε δύο οποιαδήποτε στοιχεία a $\in$ A και b $\in$ B που θα ικανοποιούν την σχέση : a $\cdot$ b = w.

□

Όπως και προηγουμένως, υπάρχει μια δημόσια ομάδα G και δύο δημόσιες υποομάδες A,B $\leq$ G, όπου ισχύει ab = ba ,$\forall$ a $\in$ A, b $\in$ B.

1. Η Μαριέττα επιλέγει τυχαία δύο κρυφά στοιχεία $a_1 \in$ A, $b_1 \in$ B. Στην συνέχεια στέλνει στον Μάρκο το στοιχείο a_1b_1.

2. Ο Μάρκος επιλέγει τυχαία δύο κρυφά στοιχεία $a_2 \in$ A, $b_2 \in$ B. Στην συνέχεια στέλνει στην Μαριέττα το στοιχείο a_2b_2.

3. Η Μαριέττα υπολογίζει :

$$K_A = b_1(a_2b_2)a_1 = a_2b_1a_1b_2 = a_2a_1b_1b_2$$

Ο Μάρκος υπολογίζει :

$$K_B = a_2(a_1b_1)b_2 = a_2a_1b_1b_2.$$

Επομένως, το $K_A = K_B = K$ είναι το κοινό μυστικό κλειδί της Μαριέττας και του Μάρκου.

Σε αυτό το σημείο παρατηρούμε ότι η αντίπαλος, έστω ότι ονομάζεται Εύα, η οποία γνωρίζει τα στοιχεία a_1b_1 και a_2b_2 , μπορεί να υπολογίσει το

$$(a_1b_1)\ (a_2b_2) = a_1b_1a_2b_2 = a_1a_2b_1b_2 \text{ και } (a_2b_2)\ (a_1b_1) = a_2a_1b_2b_1,$$

αλλά κανένα απο αυτά τα γινόμενα δεν είναι ίσα με το K, εάν $a_1a_2 \neq a_2a_1$ και $b_1b_2 \neq b_2b_1$.

Στην συνέχεια ορίζουμε το Πρόβλημα Απόφασης Παραγόντων (*desicion* factorization problem) :

Ορισμός 1.18. *Πρόβλημα Απόφασης Παραγόντων (desicion factorization problem).*
Δίνεται ένα στοιχείο w μιας ομάδας G και δύο υποομάδες A,B ≤ G.
Θέλουμε να βρούμε έαν υπάρχουν ή όχι δύο στοιχεία a ∈ A και b ∈ B, τέτοια ώστε w = a · b.

□

Αυτό φαίνεται να είναι ένα νέο και ασήμαντο πρόβλημα της θεωρίας ομάδων. Για αυτό δίνει ένα παράδειγμα ενός θεωρητικού προβλήματος της θεωρίας ομάδων που αφορά την κρυπτογραφία.

1.5 Πρωτόκολλο ανταλλαγής κλειδιού του Stickel

Το πρωτόκολλο του Stickel είναι εμπνευσμένο από το γνωστό πρωτόκολλο των Diffie-Hellman. Η επιλογή της πλατφόρμας (ομάδας αντιστρέψιμων πινάκων σε πεπερασμένο πεδίο) που έκανε ο Stickel καθιστά το πρωτόκολλο ευάλωτο σε επιθέσεις γραμμικής άλγεβρας με μεγάλη επιτυχία ανάκτησης του κοινού μυστικού κλειδιού. Ακόμη, για έναν αντίπαλο η απόκτηση του κοινού μυστικού κλειδιού δεν είναι δυσκολότερη από

την επίλυση του Προβλήματος Αναζήτησης Αποσύνθεσης (decomposition search problem).
Ωστόσο, μια ελάχιστη βελτίωση (όπως το να χρησιμοποιήσουμε μη-αντιστρέψιμους πίνακες αντί για αντιστρέψιμους) κάνει το πρωτόκολλο λιγότερο ευάλωτο, τουλάχιστον όσον αφορά σε επιθέσεις γραμμικής άλγεβρας. Συνεπώς το πρωτόκολλο αυτό έχει αρκετές δυνατότητες.
Το σημαντικότερο, όμως, όλων όσων θα αποδειχθούν είναι πως στην απόκτηση του κοινού μυστικού κλειδιού στο σχήμα του Stickel, ο αντίπαλος δεν θα έχει να λύσει κάποιο διακριτό λογαριθμικό πρόβλημα, αλλά το εμφανώς πιο εύκολο Πρόβλημα Αναζήτησης Αποσύνθεσης πάνω σε μια πλατφόρμα (ημι)ομάδα G :

Ορισμός 1.19. *Πρόβλημα Αναζήτησης Αποσύνθεσης (decomposition search problem).*

Σε μία γνωστή (ημι)ομάδα G, έχουμε δύο υποομάδες A,B ≤ G και δύο στοιχεία u,w ∈ G. Να εξετάσουμε αν υπάρχουν δύο στοιχεία x ∈ A και y ∈ B που ικανοποιούν την σχέση : x · w · y = u , υπό την προυπόθεση πως ένα τουλάχιστον τέτοιο ζευγάρι στοιχείων υπάρχει.

□

Έστω G μία δημόσια μη-αβελιανή πεπερασμένη ομάδα και δύο δημόσια στοιχεία a,b ∈ G τέτοια ώστε : ab ≠ ba. Στην συνέχεια παρουσιάζουμε το πρωτόκολλο. Έστω ότι τα N,M είναι τα άνω όρια των a,b, αντίστοιχα.

1. Η Μαριέττα επιλέγει δύο τυχαίους φυσικούς αριθμούς n < N , m < M και στέλνει το u = $a^n b^m$ στον Μάρκο.

2. Ο Μάρκος επιλέγει δύο τυχαίους φυσικούς αριθμούς r < N , s < M και στέλνει το v = $a^r b^s$ στην Μαρίεττα $a^n v b^m = a^{n+r} b^{m+s}$.

3. Ο Μάρκος υπολογίζει $K_B = a^r u b^s = a^{n+r} b^{m+s}$.
   Επομένως, η Μαριέττα και ο Μάρκος καταλήγουν με το ίδιο στοιχείο της ομάδας K = $K_A = K_B$, το οποίο είναι το κοινό μυστικό κλειδί.

Όταν ασχολούμαστε με λεπτομέρειες της εκτέλεσης, συνήθως προτιμούμε την παρακάτω πιο γενική μορφή απο το παραπάνω πρωτόκολλο.
Έστω w ∈ G, δημόσιο.

1. Η Μαριέττα επιλέγει δύο τυχαίους φυσικούς αριθμούς n < N , m < M και ένα στοιχείο c_1 που ανήκει στο κέντρο της ομάδας G, και στέλνει το u = $c_1 a^n w b^m$ στον Μάρκο.

2. Ο Μάρκος επιλέγει δύο τυχαίους φυσικούς αριθμούς r < N , s < M και ένα στοιχείο c_2 που ανήκει στο κέντρο της ομάδας G, και στέλνει το v = $c_2 a^r w b^s$ στην Μαρίεττα.

3. Η Μαριέττα υπολογίζει $K_A = c_1 a^n v b^m = c_1 c_2 a^{n+r} b^{m+s}$.

4. Ο Μάρκος υπολογίζει $K_B = c_2 a^r u b^s = c_1 c_2 a^{n+r} b^{m+s}$.
   Επομένως, η Μαριέττα και ο Μάρκος καταλήγουν με το ίδιο στοιχείο της ομάδας K = $K_A = K_B$.

Παρατηρούμε πως για να λειτουργήσει αυτό το πρωτόκολλο, δεν χρειάζεται απαραίτητα η G να είναι ομάδα. Θα έχει το ίδιο αποτελεσμα ακόμη και αν ήταν ημιομάδα, ίσως μάλιστα και καλύτερο.

Παλαιότερα είχε προταθεί ως πλατφόρμα η ομάδα των αντιστρεψιμων k × k πινάκων σε πεπερασμένο πεδίο F_{2^t}. Θα δείξουμε ότι αυτή η επιλογή καθιστά το πρωτόκολλο ευάλωτο σε επιθέσεις γραμμικής άλγεβρας. Πρώτα, όμως, θα ασχοληθούμε με μία γενική προσέγγιση επίθεσης στο πρωτόκολλο του Stickel. Τονίζουμε ότι αυτή η γενική προσέγγιση λειτουργεί εάν η G είναι μια οποιαδήποτε ημιομάδα.

Υπενθυμίζουμε ότι η Μαριέττα στέλνει u = $c_1 a^n v b^m$ στον Μάρκο.

Η πρώτη μας παρατήρηση αφορά την αντίπαλο Εύα. Για να πάρει το κοινό μυστικό κλειδί K στο τέλος, είναι σημαντικό για την αντίπαλο Εύα να βρεί κάποια στοιχεία x, y ∈ G τέτοια ώστε xa = ax, yb = by, u = xwy. Όντως, εάν έχει βρεί τέτοια x,y η Εύα μπορεί να χρησιμοποιήσει το v = $c_2 a^r u b^s$ του Μάρκου για να υπολογίσει :

$$x\ v\ y = x c_2 a^r w b^s y = c_2 a^r x w y b^s = c_2 a^r u b^s = K.$$

Αυτό σημαίνει ότι το να πολλαπλασιάζουμε με το c_i δεν μειώνει την ασφάλεια του πρωτοκόλλου. Ακόμα πιο σημάντικο είναι πως δεν είναι απαραίτητο η Εύα να ανακτήσει

κάποιο εκθέτη n , m , r , s, αλλά μπορεί απλά να λύσει ένα σύστημα εξισώσεων xa = ax , yb = by , u = xwy , όπου τα a , b , u , w είναι γνωστά και τα x , y είναι άγνωστα στοιχεία της πλατφόρμας (ημι)ομάδας G. Αυτό μας δείχνει ότι στην πραγματικότητα το πρωτόκολλο του Stickel αποκλίνει πολύ περισσότερο από αυτό των Diffie-Hellman. Επιπλέον, το να λύσουμε το σύστημα εξισώσεων στην ομάδα G ουσιαστικά δεν είναι τίποτα παραπάνω από το να λύσουμε το Πρόβλημα Αναζήτησης Αποσύνθεσης.
Οι υποομάδες A,B είναι κεντροποιούσες υποομάδες των στοιχείων a και b, αντίστοιχα. Αυτό το ζευγάρι είναι υποομάδα της G, εάν η G είναι ομάδα.

Μέχρι τώρα, καμία συγκεκριμένη (ημι)ομάδα δεν έχει αναγνωρισθεί ως η πλατφορμα που παρέχει την μεγαλύτερη ασφάλεια σε ένα πρωτόκολλο βασισμένο στο πρόβλημα αναζήτησης διάσπασης. Φαίνεται πως οι ημιομάδες πινάκων πάνω σε συγκεκριμένους δακτυλίους μπορούν γενικά να γίνουν αρκετά καλές ομάδες πλατφόρμας. Ο Stickel, επίσης, χρησιμοποιούσε πίνακες, αλλά οι επιλογές του δεν ήταν αρκετά καλές. Επίσης, το σχήμα του Stickel είναι τόσο σίγουρο όσο η δυσκολία του Προβλήματος Αναζήτησης Αποσύνθεσης. Ο λόγος είναι πως υπάρχουν τρόποι να επιτεθεί κανείς στο σχήμα χωρίς να κάνει επίθεση στο σχετικό Πρόβλημα Αναζήτησης Αποσύνθεσης.

Για παράδειγμα, ο Sramka έκανε μια επίθεση στοχεύοντας την ανάκτηση ενός από τους εκθέτες n , m , r , s στο πρωτόκολλο του Stickel. Η επίθεση που θα περιγράψουμε παρακάτω είναι πιο αποτελεσματική απο αυτή του Sramka, αλλά από την άλλη στοχεύει την ανάκτηση μόνο του κοινού μυστικού κλειδιού. Αντιθέτως, ο Sramka στοχευεί την ανάκτηση του ιδιωτικού κλειδιού.

1.5.1 Επίθεση Γραμμικής Άλγεβρας

Σε αυτή την υπο-ενότητα θα εστιάσουμε σε μία συγκεκριμένη ομάδα πλατφόρμας G η οποία προτείνεται από τον Stickel. Η ομάδα G είναι μια ομάδα αντιστρέψιμων k×k πινάκων πάνω σε ένα πεπερασμένο πεδίο F_{2^t}, όπου k = 31. Η παράμετρος l δεν είχε προσδιοριστεί προηγουμένως, αλλά μπορούμε να υποθέσουμε ότι $2 \leq l \leq k$. Η επιλογή των πινάκων a, b, w δεν είναι τόσο σημαντική για την επίθεσή μας. Αντιθέτως, αυτό που είναι σημαντικό είναι τα a, b να είναι αντιστρέψιμα. Παρατηρούμε όμως, ότι η επιλογή των a, b (πιο συγκεκριμένα το γεγονός ότι οι είσοδοι αυτών των πινάκων είναι είτε 0 είτε 1) κάνει το σχήμα πιο αδύναμο.

Υπενθυμίζουμε πως για την Εύα αρκεί να βρεί μία τουλάχιστον λύση του συστήματος εξισώσεων xa = ax , yb = by , u = xwy, όπου a , b , u ,w είναι γνωστά και τα x , y είναι άγνωστοι k×k πινάκων πάνω στο πεπερασμένο πεδίο F_{2^t}. Κάθε μία από τις δύο πρώτες εξισώσεις του συστήματος μπορεί να μετατραπεί σε ένα σύστημα k^2 γραμμικών εξισώσεων για τις (άγνωστες) εισόδους των πινάκων x και y. Όμως, η εξίσωση u = xwy δεν μετατρέπεται σε σύστημα γραμμικών εξισώσεων για τις εισόδους, επειδή περιέχει γινόμενο δύο άγνωστων πινάκων.

Επομένως, πρέπει να κάνουμε την εξής διαδικασία : να πολλαπλασιάσουμε και τα δύο μέλη της εξίσωσης u = xwy με το x^{-1} από αριστερά (σε αυτό το σημείο είναι που χρησιμοποιούμε ότι το x αντιστρέφεται) για να πάρουμε :

$$x^{-1}\mathrm{u} = \mathrm{wy}.$$

Εφόσον, xa = ax, εάν και μόνο αν $x^{-1}a = ax^{-1}$, συμβολίζουμε $x_1 = x^{-1}$ και το αντικαθιστούμε στο σύστημα (που αναφέραμε στην προηγούμενη παράγραφο) έχοντας έτσι:

$$x_1 a = a x_1 \text{ , } \mathrm{yb} = \mathrm{by} \text{ , } x_1\mathrm{u} = \mathrm{wy}.$$

Επομένως, παίρνουμε ότι κάθε εξίσωση αυτού του συστήματος μετατρέπεται σε ένα σύστημα k^2 γραμμικών εξισώσεων για τις (άγνωστες) εισόδους των πινάκων x_1 και y. Επιπλέον, έχουμε ένα σύνολο $3n^2$ γραμμικών εξισώσεων με $2k^2$ αγνώστους. Σημειώνουμε σε αυτό το σημείο ότι μια λύση του τελευταίου συστήματος θα αποφέρει το κοινό κλειδί K εάν και μόνο εάν το x_1 είναι αντιστρέψιμο, επειδή K = xvy και το x = x_1^{-1}.

Εφόσον το u είναι γνωστός αντιστρέψιμος πίνακας, μπορούμε να πολλαπλασιάσουμε τα δύο μέλη της εξίσωσης x_1u = wy με u^{-1} απο δεξιά, για να πάρουμε $x_1 = \mathrm{wy}u^{-1}$. Στην συνέχεια, εξαλείφουμε το x_1 από το σύστημα:

$$\mathrm{wy}u^{-1}\mathrm{a} = \mathrm{awy}u^{-1} \text{ , } \mathrm{yb} = \mathrm{by}.$$

Σε αυτό το σημείο έχουμε μόνο έναν άγνωστο πίνακα y, οπότε έχουμε $2k^2$ γραμμικές εξισώσεις για k^2 εισόδους του y. Έτσι, έχουμε ένα υπερ-ορισμένο σύστημα γραμμικών εξισώσεων (ταυτόχρονα, θυμόμαστε ότι στο πρωτόκολλο του Stickel πήραμε k = 31, οπότε $k^2 = 961$).

Ορισμός 1.20. *ανηγμένη κλιμακωτή μορφή ενός πίνακα (reduced row echelon). Ένας πίνακας λέμε ότι βρίσκεται στην ανηγμένη κλιμακωτή μορφή του (reduced row echelon) όταν ικανοποιεί τις εξής ιδιότητες:*

1. *Το πρώτο μη-μηδενικό στοιχείο κάθε γραμμής, που ονομάζεται κύρια είσοδος, είναι μονάδα.*

2. *Κάθε κύρια είσοδος βρίσκεται σε μία στήλη δεξιά της κύριας εισόδου της προηγούμενης γραμμής.*

3. *Σειρές που έχουν μόνο μηδενικά στοιχεία βρίσκονται κάτω από τις υπόλοιπες σειρές.*

4. *Η κύρια είσοδος κάθε γραμμής είναι η μοναδική μη-μηδενική είσοδος αυτής της στήλης.*

□

Παράδειγμα 1.21. *Ο πίνακας*

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

έχει ανηγμένη κλιμακωτή μορφή μορφή reduced row echelon.

□

Γνωρίζουμε ό,τι το σύστημα αυτό θα πρέπει να έχει τουλάχιστον μία μη τετριμμένη (μη μηδενικη) λύση, για αυτόν τον λόγο εάν πάρουμε τον πίνακα του συστήματος στην ανηγμένη κλιμακωτή μορφή του θα υπάρχει τουλάχιστον μία ελεύθερη μεταβλητή. Αντίθετα, εφόσον το σύστημα είναι ύπερ-ορισμενο, μπορούμε να περιμένουμε ότι ο αριθμός των ελεύθερων μεταβλητών δεν θα είναι τόσο μεγάλος, έτσι ώστε να είναι εφικτό να εξετάσουμε τις πιθανές τιμές των ελεύθερων μεταβλητών κάθε φορά, μέχρι να βρούμε κάποιες τιμές που να αποφέρουν έναν αντιστρέψιμο πίνακα y. Σε αυτό το σημείο υπενθυμίζουμε ότι οι είσοδοι του y είναι είτε 0 είτε 1, αυτή είναι μια επιπλέον αδυναμία του σχήματος του Stickel που αναφέραμε προηγουμένως. Σημειώνουμε ότι το να ελέγξουμε την αντιστρεψιμότητα ενός δοσμένου πίνακα είναι εύκολο επειδή είναι ισοδύναμο με το να μετατρέψουμε έναν πίνακα στην ανηγμένη κλιμακωτή μορφή του. Στην πραγματικότητα, σε όλες τις απόπειρές μας υπήρξε μόνο μία ελεύθερη μεταβλητή, έτσι το τελευταίο βήμα (να ελέγξουμε την αντιστρεψιμότητα) δεν ήταν απαραίτητο επειδή εάν υπάρχει μια μοναδική μη-μηδενική λύση του παραπάνω συστήματος, τότε ο

πίνακας y θα είναι αντιστρέψιμος.

Συνεπώς, η πιο προφανής υπόθεση για να βελτιώσουμε το πρωτόκολλο του Stickel είναι, όπως αναφέραμε και προηγουμένως, να χρησιμοποιήσουμε μη-μεταθετικά στοιχεία a, b, w. Συνεπάγεται ότι η πλατφόρμα θα πρέπει να είναι μία ημιομάδα με μη-μεταθετικά στοιχεία. Εάν είναι να χρησιμοποιήσουμε πίνακες τότε είναι λογικό να χρησιμοποιήσουμε την υποομάδα όλων των k × k πινάκων πάνω σε ένα πεπερασμένο δακτύλιο (όχι απαραίτητα πεδίο). Μία τέτοια ημιομάδα τυπικά έχει πολλά μη αντιστρέψιμα στοιχεία, έτσι θα είναι εύκολο να επιλέξουμε a, b, w που να είναι μη αντιστρέψιμα. Σε αυτήν την περίπτωση η επίθεση γραμμικής άλγεβρας δεν θα δουλέψει. Ένα ακόμη πλεονέκτημα του να μην πάρουμε αντιστρέψιμους πίνακες είναι ότι κάποιος μπορεί να χρησιμοποιήσει όχι μόνο τις δυνάμεις a^j ενός δοσμένου δημόσιου πίνακα στο πρωτόκολλο του Stickel, αλλά εκφράσεις της μορφής $\sum_{i=1}^{p} c_i \cdot a^i$, όπου c_i είναι σταθερές.

Βέβαια, δεν χρειάζεται να περιοριστούμε στην χρήση πίνακων στο πρωτόκολλο του Stickel, αλλά όπως εξηγήσαμε και παραπάνω, με μία αφηρημένη (ημι)ομάδα πλατφόρμας G, το σχήμα του Stickel θα σπάσει εάν το σχετικό Πρόβλημα Έρευνας Αποσύνθεσης λυθεί, και ως τώρα καμία αφηρημένη (ημι)ομάδα δεν αντιστέκεται στις γνωστές επιθέσεις πάνω στο Πρόβλημα Έρευνας Αποσύνθεσης.

1.6 Πρωτόκολλο Anshel-Anshel-Goldfeld

Σε αυτή την παράγραφο θα περιγράψουμε ένα πρωτόκολλο καθιέρωσης κλειδιού το οποίο ξεχωρίζει από τα υπόλοιπα διότι δεν χρησιμοποιεί κάποιες μεταθετικές ή μη-μεταθετικές υποομάδες μίας δοσμένης ομάδας πλατφόρμας και μπορεί, στην πραγματικότητα, να χρησιμοποιήσει μη-αβελιανές ομάδες με αποτελεσματικά επιλύσιμο το Πρόβλημα Λέξης ως πλατφόρμα. Το πρωτόκολλο αυτό κάνει την διαφορά και δίνει μεγάλο πλεονέκτημα σε σχέση με άλλα πρωτόκολλα.

Έχουμε μία ομάδα G και τα στοιχεία $a_1, ..., a_k, b_1, ..., b_m \in$ G , δημόσια και τα δυο αντίστοιχα.

1. Η Μαριέττα επιλέγει ένα ιδιωτικό x ∈ G ως λέξη έτσι ώστε x = x$(a_1, ..., a_k)$ και στέλνει το $b_1^x, ..., b_m^x$ στον Μάρκο.

2. Ο Μάρκος επιλέγει ένα ιδιωτικό y ∈ G ως λέξη έτσι ώστε x = x($b_1, ..., b_m$) και στέλνει το $a_1^y, ..., a_k^y$ στην Μαριέττα.

3. Η Μαριέττα υπολογίζει x(a_1^y, ..., a_k^y) = $x^y = y^{-1}xy$.
   Ο Μάρκος υπολογίζει y(b_1^x, ..., b_m^x) = $y^x = x^{-1}yx$.
   Τότε η Μαριέττα και ο Μάρκος καταλήγουν με ένα κοινό μυστικό κλειδί K = $x^{-1}y^{-1}xy$ (το οποίο ονομάζεται μεταθέτης του x και y) : η Μαριέττα πολλαπλασιάζει το $y^{-1}xy$ με το x^{-1} από αριστερά, ενώ ο Μάρκος πολλαπλασιάζει το $x^{-1}yx$ με το y^{-1} από αριστερά, στην συνέχεια αντιστρέφει το αποτέλεσμα και καταλήγει στο: $(y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy$.

Μπορεί να φαίνεται ότι λύνοντας το Πρόβλημα Αναζήτησης Συζυγίας για το b_1^x , ... , b_m^x ; a_1^y , ... , a_k^y στην ομάδα G θα επέτρεπε σε έναν αντίπαλο να πάρει το μυστικό κλειδί K. Όμως, εάν κοιτάξουμε το Βήμα (3) του πρωτοκόλλου, παρατηρούμε πως ο αντίπαλος θα έπρεπε να γνωρίζει είτε το x είτε το y, όχι όμως απλά σαν μία λέξη από τους γεννήτορες της ομάδας G, αλλά σαν μία λέξη που παράγεται από τα a_1 , ... , a_k (και αντίστοιχα σαν μία λέξη που παράγεται από τα b_1 , ... , b_m). Διαφορετικά, δεν θα μπορούσε να υπολογίσει, ας πούμε, το x^y από τα a_1^y , ... , a_k^y. Πράγμα το οποίο σημαίνει ότι ο αντίπαλος θα πρέπει να λύσει το Πρόβλημα Αναζήτησης Μελών (membership search problem).

Ορισμός 1.22. *Πρόβλημα Αναζήτησης Μελών.*
Δίνονται στοιχεία x, a_1, ... , a_k μίας ομάδας G και θέλουμε να βρούμε μία έκφραση (εάν υπάρχει) του x ως μία λέξη που παράγεται από τα a_1 , ... , a_k.

□

Θα ορίσουμε αναλυτικότερα τις ομάδες πλεξίδων στο Κεφάλαιο 2. Βλ. 2.1.1.

Αξίζει να αναφέρουμε ότι το Πρόβλημα Αναζήτησης Μελών χρησιμοποιείται για να καθορίσει εάν ένα δοσμένο στοιχείο x ∈ G ανήκει σε κάποια υποομάδα του G που παράγεται από τα δοσμένα a_1,...,a_k ή όχι. Αυτό το πρόβλημα είναι αρκετά δύσκολο σε πολλές ομάδες. Για παράδειγμα, το Πρόβλημα Αναζήτησης Μελών σε μία ομάδα πλεξίδων B_n είναι αλγοριθμικά άλυτο, εάν n ≥ 6, επειδή μία τέτοια ομάδα πλεξίδων περιέχει υποομάδες ισόμορφες με το $F_2 \times F_2$ (που θα μπορούσε να είναι, για παράδειγμα, η υποομάδα που παράγεται από τα $\sigma_1^2, \sigma_2^2, \sigma_4^2$και σ_5^2, όπου το F_2 είναι μια ελεύθερη ομάδα

δεύτερης τάξης). Σε αυτή την ομάδα $F_2 \times F_2$, το Πρόβλημα Αναζήτησης Μελων είναι αλγοριθμικά άλυτο, όπως προκύπτει από ένα παλιό αποτέλεσμα της Mihailova.

Επίσης, σημειώνουμε ότι εάν ένας αντίπαλος βρει, ας πούμε, κάποιο $\acute{x} \in$ G τέτοιο ώστε $b_1^x = b_1^{\acute{x}}$,...,$b_m^x = b_m^{\acute{x}}$, δεν είναι βέβαιο ότι $\acute{x} =$ x στην G. Ισχύει, όμως, ότι εάν $\acute{x} = c_b x$, όπου $c_b b_i = b_i c_b$ για όλα τα i (που στην συγκεκριμένη περίπτωση λέμε ό,τι το c_b είναι κεντροποιητής του b_i), τότε $b_i^x = b_i^{\acute{x}}$ για όλα τα i. Για αυτόν το λόγο ισχύει $b^x = b^{\acute{x}}$ για οποιοδήποτε στοιχείο b της υποομάδας που παράγεται από τα b_1 ,..., b_m, συγκεκριμένα $y^x = y^{\acute{x}}$. Τώρα το πρόβλημα είναι πως εάν το $\acute{x}$ (και ομοίως το $\acute{y}$) δεν ανήκει στην υποομάδα A που παράγεται από τα a_1,...,a_k (αντιστοίχως στην υποομάδα B που παράγεται από τα b_1,...,b_m), τότε υπάρχει πιθανότητα ο αντίπαλος να μην αποκτήσει το σωστό κοινό μυστικό κλειδί K. Από την άλλη, εάν το $\acute{x}$ (και ομοίως το $\acute{y}$) δεν ανήκουν στην υποομάδα A (αντίστοιχα στην B), τότε υπάρχει πιθανότητα ο αντίπαλος να αποκτήσει το σωστό K, παρόλο που το δικό του $\acute{x}$ και $\acute{y}$ μπορεί να είναι διαφορετικά από τα x και y, αντίστοιχα. Πράγματι, εάν $\acute{x} = c_b x$, $\acute{y} = c_a y$, όπου το c_b είναι κέντρο του B και c_a είναι κέντρο του A, τότε

$$(\acute{x})^{-1}(\acute{y})^{-1}\acute{x}\acute{y} = (c_b x)^{-1}(c_a y)^{-1} c_b x c_a y = x^{-1}c_b^{-1}y^{-1}c_a^{-1}c_b x c_a y = x^{-1}y^{-1}xy = \mathrm{K}$$

Επειδή το c_b μετατρέπεται στο y και στο c_a (σημειώνουμε σε αυτό το σημείο ό,τι το c_a ανήκει στην υποομάδα B, άρα μπορούμε να υποθέσουμε ότι $\acute{y} = c_a y \in$ G, και ομοίως c_b ανήκει στο A) και το c_a μετατρέπεται στο x.

Τονίζουμε ότι ο αντίπαλος καταλήγει να έχει το σωστό κλειδί K (δηλαδή το $\mathrm{K} = (\acute{x})^{-1}(\acute{y})^{-1}\acute{x}\acute{y} = x^{-1}y^{-1}xy$), *εάν και μόνο αν* το c_b μετατρέπεται στο c_a. Ο μόνος πιθανός τρόπος για να το εξασφαλίσουμε, είναι να έχουμε $\acute{x} \in$ A και $\acute{y} \in$ B. Φαίνεται, λοιπόν, πως δεν υπάρχει τρόπος ο αντίπαλος να βεβαιωθεί ότι έχει το σωστό κλειδί.

Γι΄ αυτόν το λόγο, φαίνεται πως εάν ο αντίπαλος επιλέξει να λύσει το Πρόβλημα Αναζήτησης Συγυζίας στην ομάδα G, για να ανακτήσει τα x και y, στην συνέχεια θα έρθει αντιμέτωπος με το Πρόβλημα Αναζήτησης Μελών, που μπορεί να είναι αλγοριθμικά άλυτο σε μία δοσμένη ομάδα. Καταλήγουμε, λοιπόν, στο συμπέρασμα ότι ο αντίπαλος ουσιαστικά πρέπει να λύσει μία πιο δύσκολη μορφή του Προβλήματος Αναζήτησης Συζυγίας:

Δίνονται μία ομάδα G, μία υποομάδα $\mathrm{A} \leq$ G και δύο στοιχεία g, h $\in$ G. Να εξετάσουμε αν υπάρχει x $\in$ A τέτοιο ώστε $\mathrm{h} = x^{-1}gx$, με δεδομένο ότι τουλάχιστον ένα τέτοιο x υπάρχει.

Τελικά, σημειώνουμε ότι όσα έχουμε αναφέρει παραπάνω δεν επηρεάζουν κάποιες επιθέσεις στο πρωτόκολλο των Anshel-Anshel-Goldfeld. Ο λόγος είναι πως οι επιθέσεις αυτές, που χρησιμοποιούν αλγορίθμους που λειτουργούν με «γειτονική έρευνα» (neighborhood search) σε ένα κείμενο θεωρίας ομάδων, μπορεί να αναφερθούν και ως επιθέσεις μήκους. Είναι στοχοθετημένες στο να βρίσκουν μία λύση μίας δοσμένης εξίσωσης (ή συστήματος εξισώσεων) ως λέξη δοσμένων στοιχείων. Ακόμα και αν βρεθεί ένας γρήγορος (πολυωνυμικού χρόνου) αλγόριθμος, για να λυθεί το Πρόβλημα Αναζήτησης Συζυγίας στις ομάδες πλεξίδας, αυτό δεν θα είναι αρκετό για να σπάσει το πρωτόκολλο των Anshel-Anshel-Goldfeld με ντετερμινιστική επίθεση.

1.7 Πρωτόκολλα Πιστοποίησης Αυθεντικότητας βασισμένα στο Πρόβλημα Συζυγίας

Η κρυπτογραφία που βασίζεται στις ομάδες προσέλκυσε μεγάλο ενδιαφέρον μετά τις ευρέσεις των πρωτοκόλλων ανταλλαγής κλειδιών των Anshel-Anshel-Goldfeld και των Ko-Lee από το 1999. Έκτοτε, πλήθος νέων κρυπτογραφικών πρωτοκόλλων έχουν δημοσιευθεί και αναλυθεί, συμπεριλαμβανομένων των πρωτοκόλλων πιστοποίησης αυθεντικότητας δημόσιων κλειδιών που βασίζονται σε μη-πεπερασμένα σύνολα.

Η βασική λειτουργία ενός πρωτοκόλλου πιστοποίησης αυθεντικότητας είναι να επιτρέπει σε έναν νόμιμο χρήστη (την Μαριέττα) να αποδείξει την ταυτότητα της, μέσω ενός μη ασφαλούς καναλιού σε έναν διακομιστή (Μάρκος) χρησιμοποιώντας το ιδιωτικό κλειδί της χωρίς να δίνει πληροφορίες για αυτό. Η Μαριέττα συχνά αναφέρεται ως prover και ο Μάρκος ως verifier.

Υπάρχουν πολλές γενικές διαθέσιμες προτάσεις, οι οποίες χρησιμοποιούν μη αβελιανές ομάδες. Οι περισσότερες από αυτές είναι άμεσες προσαρμογές πρωτοκόλλων ανταλλαγής κλειδιών, όπως είναι το πρωτόκολλο ανταλλαγής κλειδιού Ko-Lee.

1.7.1 Πρωτόκολλο Diffie-Hellman-like

Το πρωτόκολλο Diffie-Hellman-like που αφορά την πιστοποίηση αυθεντικότητας έχει σχεδιαστεί για να επιτρέπει σε ένα σύνολο ανθρώπων να επικοινωνούν μέσω ενός μη ασφαλούς καναλιού ή ανοιχτού δικτύου με ένα κοινό μυστικό κλειδί που μπορεί αργότερα να χρησιμοποιηθεί, για να επιτευχθούν διάφοροι κρυπτογραφικοί στόχοι, όπως είναι

η εμπιστευτικότητα της πολλαπλής διανομής μηνυμάτων ή η ακεραιότητα πολλαπλής διανομής αρχείων. Σε αυτή την περίπτωση η ομάδα των ανθρώπων θεωρείται στατικό μέγεθος. Αρχικά, θα συμφωνήσουν σε μία συνομιλία, στο τέλος της οποίας θα έχουν καθιερώσει ένα κλειδί. Σε αυτή την παράγραφο θα ασχοληθούμε με ένα ζευγάρι ανθρώπων που ανήκουν σε αυτή την ομάδα.

Τα τελευταία χρόνια, έχουν εκδοθεί πολλές διατριβές, προκειμένου να επεκτείνουν το γνωστό πρωτόκολλο Diffie-Hellman για περισσότερους από δύο ανθρώπους. Τα πρωτόκολλα αυτά έχουν ποικίλα εκτελεστικά χαρακτηριστικά, αλλά δεν είναι επιστημονικά τεκμηριωμένα, δείχνοντας απλά ότι πετυχαίνουν τον στόχο τους.

Ξεκινάμε.

Έστω μία ομάδα G και A,B $\leq$ G δύο μεταθετικές υποομάδες της G, δηλαδή ab = ba για οποιοδήποτε a $\in$ A και b $\in$ B.

Το προσωπικό κλειδί της Μαριέττας είναι ένα στοιχείο s $\in$ A. Το δημόσιο κλειδί της Μαριέττας είναι το ζευγάρι (w,t), όπου το w είναι ένα αυθαίρετο στοιχείο της G και t = s^{-1}ws.

Το πρωτόκολλο Diffie-Hellman-like:

1. Ο Μάρκος επιλέγει το r $\in$ B και στέλνει το w′ = r^{-1}wr στην Μαριέττα.

2. Η Μαριέττα στέλνει την απάντηση της, το w′′ = s^{-1}w′r στον Μάρκο.

3. Ο Μάρκος ελέγχει εάν w′′ = r^{-1}tr.

Μία σωστή απάντηση του prover στο Βήμα 2. οδηγεί στην αποδοχή από τον verifier, εφόσον λόγω του σχεδιασμού του πρωτοκόλλου τα στοιχεία r και s μετατίθενται. Εκ τούτου ικανοποιείται η ισότητα:

$$\mathrm{w}'' = s^{-1}\mathrm{w}'\,\mathrm{s} = s^{-1}r^{-1}\mathrm{wrs} = r^{-1}s^{-1}\mathrm{wsr} = r^{-1}\mathrm{tr}$$

Ο εισβολέας (η Εύα) η οποία θέλει να αναγνωρισθεί ως Μαριέττα από το Μάρκο, μπορεί να κάνει τα ακόλουθα:

- **Υπολογισμός προσωπικού κλειδιού της Μαριέττας**, s: Λύνοντας το Πρόβλημα Αναζήτησης Συζυγίας που σχετίζεται με την υποομάδα A ή λύνοντας το Πρόβλημα Αποσύνθεσης για ένα ζευγάρι (w,t) που σχετίζεται με την υποομάδα A, υπολογίζει τα στοιχεία $s_1, s_2 \in$ A τέτοια ώστε t = $s_1 w s_2$. Είναι ασήμαντο να ελέγξουμε ότι για ένα τέτοιο ζευγάρι (s_1, s_2) η ισότητα s_1w′s_2 = w′′

ικανοποιείται πάντα ως εκ τούτου το ζευγάρι (s_1, s_2) λειτουργεί ως το προσωπικό κλειδί της Μαριέττας, s.

- **Υπολογισμός προσωρινού κλειδιού του Μάρκου**, r: Λύνοντας το Πρόβλημα Αναζήτησης Συζυγίας που σχετίζεται με την υποομάδα B ή λύνοντας το Πρόβλημα Αποσύνθεσης για ένα ζευγάρι (w,w′) που σχετίζεται με την υποομάδα B και κάνοντας την παραπάνω διαδικασία, για να επιτεθεί στο προσωπικό κλειδί της Μαριέττας.

Η υπολογιστική δυσκολία αυτών των προβλημάτων εξαρτάται από τις συγκεκριμένες υποομάδες A και B.

Παρατήρηση 1.23. *Αυτό το πρωτόκολλο μπορεί πολύ απλά να μετατραπεί, έτσι ώστε να βασίζεται στο Πρόβλημα Αποσύνθεσης. Πράγματι, υποθέτουμε ότι* A_1, A_2, B_1, B_2 *είναι υποομάδες της ομάδας* G*, τέτοιες ώστε* $[\ A_1\ ,\ B_1\ ] = 1$ *και* $[\ A_2\ ,\ B_2\ ] = 1$*. Το προσωπικό κλειδί της Μαριέττας είναι το ζευγάρι* $(a_1, a_2) \in A_1 \times A_2$ *και το δικό της δημόσιο κλειδί είναι το ζευγάρι* $(w,t) \in G \times G$*, όπου το* w *είναι ένα αυθαίρετο στοιχείο της* G *και* $t = a_1 w a_2$*. Τώρα η διαδικασία τροποποιείται ως εξής:*

- *Ο Μάρκος επιλέγει στοιχεία* $b_1 \in B_1, b_2 \in B_2$ *και στέλνει το* $w' = b_1 w b_2$ *στην Μαριέττα.*
- *Η Μαριέττα στέλνει την απάντηση* $w'' = a_1 w' a_2$ *στον Μάρκο.*
- *Ο Μάρκος ελέγχει εάν* $w'' = b_1 t b_2$*.*

Αυτή η μορφή οφείλεται στους Lal και Chaturwedi. Φαίνεται ότι το Πρόβλημα Αναζήτησης Συζυγίας δεν μπορεί να χρησιμοποιηθεί, για να επιτεθεί κάποιος σε αυτή την μορφή του πρωτοκόλλου.

‘

1.7.2 Πρωτόκολλο Fiat-Shamir-like

Μία άλλη πρόταση ενός πρωτοκόλλου πιστοποίησης αυθεντικότητας βασισμένο σε ομάδες οφείλεται στον Sibert. Αυτό το σχήμα είναι θυμίζει το σχήμα των Fiat-Shamir, το οποίο περιλαμβάνει την επανάληψη ενός βήματος πολλές φορές. Μία από τις βασικές διαφορές σε σχέση με το πρωτόκολλο Diffie-Hellman-like που περιγράψαμε παραπάνω, είναι ότι δεν υπάρχει ανάγκη να διαλέξουμε μεταθετικές υποομάδες A και B.

Θυμίζουμε ότι οποιαδήποτε *διαδραστική απόδειξη του συστήματος γνώσεων* αποτελείται από πολλές επαναλήψεις τυχοποιημένων πρωτοκόλλων για δύο άτομα. Σε ένα από αυτά ο prover επιθυμεί να πείσει το άλλο μέλος, τον verifier για την εγκυρότητα ενός συγκεκριμένου ισχυρισμού. Κάθε τέτοια διαδραστική απόδειξη πρέπει να ικανοποιεί τις συνθήκες *πληρότητας* και *εγκυρότητας*:

- *Πληρότητα*: Εάν ο ισχυρισμός είναι αληθής, θα πρέπει ο verifier να τον δεχτεί με μεγάλη πιθανότητα.
- *Εγκυρότητα*: Εάν ο ισχυρισμός είναι ψευδής, τότε ο verifier τον απορρίπτει με μεγάλη πιθανότητα

Εάν ο prover δεν εμπιστεύεται τον verifier και δεν θέλει να εκθέσει κάποια προσωπική πληροφορία κατά την διαδικασία χορήγησης της απόδειξης ταυτότητας, τότε η ακόλουθη ιδιότητα γίνεται πολύ σημαντική:

Ορισμός 1.24. *Μηδενική Γνώση (Zero-Knowledge).*
Εκτός από την εγκυρότητα των ισχυρισμών του prover, καμία άλλη πληροφορία δεν αποκαλύπτεται κατά την διαδικασία της απόδειξης.

Έστω G μια μη-μεταθετική ομάδα που ονομάζεται *ομάδα πλατφόρμας* και μ ένα μέτρο πιθανότητας στην G (Βλ[9]). Το ιδιωτικό κλειδί του prover, δηλαδή της Μαριέττας, είναι ένα στοιχείο s ∈ G. Το δημόσιο κλειδί είναι το ζευγάρι (w, t), όπου το w είναι ένα τυχαίο στοιχείο της ομάδας G, που ονομάζεται , και $t = s^{-1}ws$ είναι συζυγές του w από το s. Επιπλέον, υποθέτουμε ότι H είναι μία μονόδρομη hash συνάρτηση από την G στο $\{0,1\}^N$. Το πρωτόκολλο λειτουργεί ως εξής:

1. Η Μαριέττα επιλέγει ένα τυχαίο στοιχείο r ∈ G, σύμφωνα με το μέτρο πιθανότητας μ και στέλνει το $x = H(r^{-1}tr)$, που ονομάζεται *δέσμευση*, στον verifier, δηλαδή στον Μάρκο.
2. Ο Μάρκος επιλέγει ένα τυχαίο bit c και το στέλνει στην Μαριέττα.
   - Εάν το c = 0, τότε η Μαριέττα στέλνει y = r στον Μάρκο. Ο Μάρκος ελέγχει αν ικανοποιείται η ισότητα $x = H(r^{-1}tr)$.
   - Εάν το c = 1, τότε η Μαριέττα στέλνει y = sr στον Μάρκο. Ο Μάρκος ελέγχει αν ικανοποιείται η ισότητα $x = H(r^{-1}wr)$.

Είναι ασήμαντο να ελέγξουμε αν η σωστή απάντηση της Μαριέττας (prover) στο Βήμα 2. οδηγεί σε αποδοχή από τον Μάρκο (verifier). Λιγότερο εμφανές είναι για ποιό λόγο μία τέτοια συμφωνία (με ένα τυχαίο bit) χρειάζεται. Μπορεί να φαίνεται ότι η Μαριέττα θα μπορούσε απλά να αποκαλύψει ότι y = sr , χωρίς να αποκαλύψει το μυστικό s, και παρόλα αυτά επιτρέπει στον Μάρκο να επαληθεύσει την ισότητα x = y^{-1}wy.

Σε αυτό το σημείο, η αντίπαλος Εύα, η οποία θέλει να παραστήσει την Μαριέττα, μπορεί απλά να πάρει ένα τυχαίο στοιχείο u και να στείλει x = u^{-1}wu στον Μάρκο. Τότε το u θα παίξει τον ίδιο ρόλο με το y = sr για τις ανάγκες της επαλήθευσης.

Παρομοίως, εάν η Εύα ήξερε σίγουρα ότι η Μαριέττα θα έστελνε y = r για τις ανάγκες της επαλήθευσης, θα μπορούσε να χρησιμοποιήσει ένα τυχαίο στοιχείο u αντί του r. Αυτά μας δείχνουν ότι το παραπάνω πρωτόκολλο πιστοποίησης αυθεντικότητας θα πρέπει να τρέξει πολλές φορές για να είναι αξιόπιστο, διότι αν τρέξει μία φορά, η Εύα θα μπορέσει επιτυχώς να παραστήσει ότι είναι η Μαριέττα με πιθανότητα 1/2. Ύστερα από k φορές, η πιθανότητα μειώνεται στην $\frac{1}{2^k}$

Αυτή η διαδικασία επαναλαμβάνεται k φορές , για να βεβαιωθεί το σφάλμα της εγκυρότητας, δηλαδή η πιθανότητα η ψεύτικη Μαριέττα (prover) να πείσει το Μάρκο (verifier) με ένα ψευδή ισχυρισμό της τάξης 2^{-k}. Αυτή θεωρείται αμελητέα, εάν το k είναι μεγάλο, ας πούμε k ≥ 100. Το πρωτόκολλο αυτό ικανοποιεί και τις δύο συνθήκες, της πληρότητας και της εγκυρότητας.

Ασφάλεια Πρωτοκόλλου

Σημειώνουμε ότι ένας εισβολέας, η Εύα, μπορεί να υπολογίσει το μυστικό κλειδί s ή οποιαδήποτε στοιχείο s ′ ∈ G, τέτοιο ώστε t = $(\acute{x})^{-1}$ws′ . Εάν η Εύα μπορεί να λύσει το Πρόβλημα Αναζήτησης Συζυγίας για την G, τότε μπορεί να αναγνωρισθεί ως prover, δηλαδή ως Μαριέττα. Επιπλέον, η υπολογιστική δυσκολία του Προβλήματος Αναζήτησης Συζυγίας για την G είναι αναγκαία για την ασφάλεια αυτού του πρωτοκόλλου.

Αρχικά, προτάθηκε η χρήση των ομάδων πλεξίδων B_n ως ομάδα πλατφόρμας, επειδή δεν υπήρχε αποτελεσματική λύση στο Πρόβλημα Αναζήτησης Συζυγίας για γνωστές B_n. Αυτό πυροδότησε πολλές έρευνες γύρω από τις ομάδες πλεξίδες. Ως αποτέλεσμα των πρόσφατων εξελίξεων, υπάρχει η άποψη ότι το Πρόβλημα Αναζήτησης Συζυγίας για B_n μπορεί να λυθεί σε πολυωνυμικό χρόνο. Αν αυτό είναι αληθές, τότε το πρω-

τόκολλο πιστοποίησης αυθεντικότητας του Sibert. δηλαδή αυτό που μελετάμε σε αυτή την παράγραφο, δεν είναι ασφαλές για τις B_n. Παρόλα αυτά, το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί με διαφορετικές ομάδες πλατφόρμας και για αυτόν το λόγο είναι σημαντικό να έχουμε εργαλεία για την ανάλυση αυτών των τύπων για τις γενικές μορφές του πρωτοκόλλου του Sibert. Δεν είναι απαραίτητο να λύσουμε το Πρόβλημα Αναζήτησης Συζυγίας για την G, για να σπάσει το σχήμα. Ωστόσο, κάποιος μπορεί να αναλύσει την ιδιότητα Μηδενικής Γνώσης του πρωτοκόλλου χρησιμοποιώντας ιδέες από την θεωρία πιθανοτήτων και να δείξει ότι το πρωτόκολλο δεν είναι ασφαλές υπό μία ασθενή υπόθεση ύπαρξης μίας συνάρτησης αποτελεσματικά υπολογίσιμου μήκους στην ομάδα πλατφόρμας G. Ακόμα και για ομάδες που δεν έχουν συναρτήσεις αποτελεσματικά υπολογίσιμου μήκους, όπως είναι οι B_n, μία λογική προσέγγιση μπορεί να λειτουργήσει το ίδιο αποτελεσματικά.

Έστω μ το μέτρο πιθανότητας στην ομάδα πλατφόρμας G. Καλούμε το *μ αριστερά-αμετάβλητο* εάν για κάθε $\mathrm{A} \subseteq \mathrm{G}$ και $\mathrm{g} \in \mathrm{G}$ η ισότητα $\mu(\mathrm{A}) = \mu(\mathrm{gA})$ διατηρείται.

Ορισμός 1.25. *Έστω G μία ομάδα. Εάν το Πρόβλημα Αναζήτησης Συζυγίας για την G είναι υπολογιστικά δύσκολο (δηλαδή δεν μπορεί να υπολογιστεί από μία πιθανολογική, πολυωνυμικού χρόνου μηχανή Turing) και το μ είναι ένα αριστερά-αμετάβλητο μέτρο πιθανότητας στην G, τότε το παραπάνω πρωτόκολλο είναι ένα διαδραστικό μηδενικής γνώσης σύστημα απόδειξης.*

Προφανώς, δεν υπάρχουν αριστερά-αμετάβλητα μέτρα πιθανότητας στις ομάδες πλεξίδες, που χρησιμοποιούνται ως ομάδες πλατφόρμας στο πρωτόκολλο. Γι΄ αυτόν τον λόγο το πρωτόκολλο αυτό δεν μπορεί να είναι ένα τέλειο μηδενικής γνώσης σύστημα απόδειξης όταν χρησιμοποιεί μία άπειρη ομάδα, όπως η B_n.

1.7.3 Πρωτόκολλο βασισμένο στο Συνεστραμένο Πρόβλημα Συζυγίας

Το πρωτόκολλο πιστοποίησης αυθεντικότητας που περιγράψαμε στην προηγούμενη παράγραφο μπορεί να μετατραπεί, έτσι ώστε να στηρίζεται στο Πρόβλημα Αποσύνθεσης με παρόμοιο τρόπο όπως είχε γίνει στην παράγραφο 1.7.1. Αυτό το σχήμα επιτρέπει μια ακόμα πιο ενδιαφέρουσα τροποποίηση. Έστω ϕ ένας τυχαίος ενδομορφισμός (δηλαδή ομομορφισμός στον εαυτό του) της ομάδας πλατφόρμας G. Υποθέτουμε ότι ϕ είναι δημοσίως γνωστό και μπορεί να είναι μέρος του δημοσίου κλειδιού της Μαριέττας. Το

ιδιωτικό κλειδί της Μαριέττας είναι ένα στοιχείο s ∈ G και το δημόσιο κλειδί της είναι το ζευγάρι (w,t) , όπου το w είναι ένα τυχαίο στοιχείο της G και $t = s^{-1}w\phi(s)$. Το πρωτόκολλο πιστοποίησης αυθεντικότητας λειτουργεί ως εξής:

1. Η Μαριέττα επιλέγει ένα στοιχείο r ∈ G και στέλνει το στοιχείο $x = r^{-1}t\phi(r)$, το οποίο ονομάζεται δέσμευση (commitment), στον Μάρκο.

2. Ο Μάρκος επιλέγει ένα τυχαίο bit c και το στέλνει στην Μαριέττα.

   - Εάν c = 0, τότε η Μαριέττα στέλνει y = r στον Μάρκο και ο Μάρκος ελέγχει, αν η ισότητα $x = y^{-1}t\phi(y)$ ικανοποιείται.
   - Εάν c = 1, τότε η Μαριέττα στέλνει y = sr στον Μάρκο και ο Μάρκος ελέγχει, αν η ισότητα $x = y^{-1}w\phi(y)$ ικανοποιείται.

Ξανά, μία σωστή απάντηση της Μαριέττας (prover) στο Βήμα 2, οδηγεί στην αποδοχή από τον Μάρκο (verifier).

Για να σπάσουμε το πρωτόκολλο, είναι αρκετό να βρούμε ένα οποιοδήποτε στοιχείο $\acute{s} \in G$, τέτοιο ώστε $t = \acute{s}^{-1}w\phi(\acute{s})$ το οποίο είναι για παράδειγμα το πρόβλημα που είναι γνωστό ως Συνεστραμένο (Twisted) Πρόβλημα Συζυγίας:

Ορισμός 1.26. *Συνεστραμένο Πρόβλημα Συζυγίας.*
Έστω G μια ομάδα. Για οποιοδήποτε $\phi \in Aut(G)$ και ένα ζευγάρι στοιχείων $(w,t) \in G$ να εξετάσουμε αν υπάρχει ένας συνεστραμμένος συζεύκτης για τα w και t. Δηλαδή, ένα στοιχείο $s \in G$, τέτοιο ώστε $t = s^{-1}w\phi(s)$, δεδομένου ότι ένα τέτοιο s υπάρχει.

□

Η μορφή απόφασης αυτού του προβλήματος είναι ένα νέο αλγοριθμικό πρόβλημα στην θεωρία ομάδων. Δεν είναι τόσο ασήμαντο για τις ελευθέρες ομάδες. Μία άλλη τάξη ομάδων είναι η τάξη των πολυκυκλικών-πεπερασμένων ομάδων.

Κλείνοντας αυτή την παράγραφο, αξίζει να αναφέρουμε ότι δείξαμε δύο γενικούς τρόπους χρήσης της ιδέα των Fiat-Shamir. Συγκεκριμένα, το πρωτόκολλο πιστοποίησης αυθεντικότητας που βασίζεται στην ιδέα των Fiat-Shamir μπορεί να κανονιστεί, έτσι ώστε η πλαστογραφία να γίνει NP-hard.

Παρατήρηση 1.27. *Υπάρχουν άπειρες ομάδες στις οποίες η συνάρτηση απόστασης $d(\cdot,\cdot)$ μπορούν να υπολογιστούν πολύ δύσκολα. Η ομάδα πλεξίδας B_∞ είναι ένα παράδειγμα μίας τέτοιας ομάδας. Ο υπολογισμός της συνάρτησης απόστασης στην B_∞ είναι γνωστό ότι είναι NP-hard, Βλ.[10]. Τέτοιες ομάδες χρειάζονται ειδική μεταχείριση.*

Επιπλέον, υπάρχουν άπειρες ομάδες για τις οποίες η συνάρτηση απόστασης $d(\cdot,\cdot)$ δεν είναι υπολογίσιμη.

□

1.8 Σχέσεις μεταξύ διαφορετικών προβλημάτων

Σε αυτή την παράγραφο, θα αναλύσουμε τις σχέσεις μεταξύ βαθύτερων προβλημάτων σε κάποια πρωτόκολλα που αναφέραμε και αναλύσαμε στις προηγούμενες παραγράφους.

Θα ξεκινήσουμε με το Πρόβλημα Αναζήτησης Συζυγίας (ΠΑΣ), το οποίο χρησιμοποιήθηκε στην παράγραφο 1.2. Μία πιο ακριβής ονομασία για αυτό το πρόβλημα θα ήταν το *περιορισμένο στις υποομάδες* Πρόβλημα Αναζήτησης Συζυγίας:

Ορισμός 1.28. *Περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας. Δίνονται δύο στοιχεία w,h της ομάδας G, μία υποομάδα $A \leq G$ και η πληροφορία ότι $w^a = h$ για κάποιο $a \in A$. Θέλουμε να βρούμε τουλάχιστον ένα τέτοιο στοιχείο a.*

□

Σε σχέση με το πρωτόκολλο των Ko-Lee που περιγράψαμε στην παράγραφο 1.2, ένας από τα μέλη, η Μαριέττα, μεταδίδει το w^a για κάποιο ιδιωτικό $\mathrm{a} \in \mathrm{A}$ και το άλλο μέλος, ο Μάρκος, θα μεταδώσει το w^b για κάποιο ιδιωτικό $\mathrm{b} \in \mathrm{B}$, όπου οι υποομάδες A και B είναι μεταθετικές, ισχύει δηλαδή $\mathrm{ab} = \mathrm{ba}$ για οποιοδήποτε $\mathrm{a} \in \mathrm{A}$ και $\mathrm{b} \in \mathrm{B}$.

Τώρα, υποθέτουμε ότι ο αντίπαλος βρίσκει $a_1, a_2 \in \mathrm{A}$, τέτοια ώστε $a_1 w a_2 = a^{-1}\mathrm{wa}$ και $b_1, b_2 \in \mathrm{B}$, τέτοια ώστε $b_1 w b_2 = b^{-1}\mathrm{wb}$. Τότε, ο αντίπαλος παίρνει:

$$a_1 b_1 w b_2 a_2 = a_1 b^{-1} w b a_2 = b^{-1} a_1 w a_2 b = b^{-1} a^{-1}\mathrm{wab} = \mathrm{K}$$

το κοινό μυστικό κλειδί.

Τονίζουμε ότι αυτά τα a_1, a_2 και b_1, b_2 δεν έχουν καμία σχέση με τα στοιχεία που διάλεξε αρχικά η Μαριέττα ή ο Μάρκος, πράγμα το οποίο απλουστεύει την έρευνα σημαντικά. Επίσης, πρέπει να τονίσουμε ότι είναι αρκετό για τον αντίπαλο να βρει μόνο ένα ζευγάρι, ας πούμε το $a_1, a_2 \in \mathrm{A}$, για να πάρει το κοινό μυστικό κλειδί:

$$a_1(b^{-1} w b) a_2 = b^{-1} a_1 w a_2 b = b^{-1} a^{-1} w a b = \mathrm{K}.$$

Συνοπτικά, για να πάρει το μυστικό κλειδί K, ο αντίπαλος δεν χρειάζεται να λύσει το περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας, αλλά είναι αρκετό να λύσει το εμφανώς ευκολότερο περιορισμένο στις υποομάδες Πρόβλημα Αποσύνθεσης:

Ορισμός 1.29. *Περιορισμένο στις υποομάδες Πρόβλημα Αποσύνθεσης.*
Δίνονται δύο στοιχεία w και w′ της ομάδας G. Θέλουμε να βρούμε κάποια στοιχεία a_1 και a_2 που θα ανήκουν σε μια δοσμένη υποομάδα $A \leq G$ και ικανοποιούν το $a_1 \cdot w \cdot a_2 = w'$, δεδομένου ότι τουλάχιστον ένα τέτοιο ζευγάρι στοιχείων υπάρχει.

□

Παρατηρούμε ότι το πρωτόκολλο που οφείλεται στους Shpilrain και Ushakov βασίζεται σε μία κάπως πιο γενική μεταβλητή του Προβλήματος Αναζήτησης Αποσύνθεσης, όπου υπάρχουν δύο διαφορετικές υποομάδες:

Ορισμός 1.30. *Πρόβλημα Αναζήτησης Αποσύνθεσης.*
Δίνονται δύο στοιχεία w και w′ της ομάδας G και δύο υποομάδες $A,B \leq G$. Θέλουμε να βρούμε δύο οποιαδήποτε στοιχεία $a \in A$ και $b \in B$ που να ικανοποιούν το $a \cdot w \cdot b = w'$, δεδομένου ότι τουλάχιστον ένα τέτοιο ζευγάρι στοιχείων υπάρχει.

□

Τότε, ένα ακόμα τέχνασμα μειώνει το Πρόβλημα Αναζήτησης Αποσύνθεσης σε μία ειδική περίπτωση, όπου το w = 1. Δηλαδή, δεδομένου ότι $a \cdot w \cdot b =$ w′, πολλαπλασιάζουμε από αριστερά με το στοιχείο w^{-1} (που είναι το αντίστροφο του δημόσιου στοιχείου w), για να πάρουμε:

$$\mathrm{w}' = w^{-1}a \cdot w \cdot b = (w^{-1}a \cdot w) \cdot b.$$

Επομένως, αν συμβολίσουμε με A^w την υποομάδα που είναι συζυγής με την A από το στοιχείο w, το πρόβλημα για τον αντίπαλο είναι τώρα ένα Πρόβλημα Αναζήτησης Παραγόντων:

Ορισμός 1.31. *Πρόβλημα Αναζήτησης Παραγόντων.*
Δίνονται ένα στοιχείο w′ μιας ομάδας G και δύο υποομάδες $A^w,B \leq G$. Θέλουμε να βρούμε δύο οποιαδήποτε στοιχεία και που θα ικανοποιούν την σχέση $a \cdot b = w'$, δεδομένου ότι ένα τέτοιο ζευγάρι στοιχείων υπάρχει.

□

Από το αρχικό πρωτόκολλο Ko-Lee, κάποιος έχει A = B. Αυτό έχει ως αποτέλεσμα την παρακάτω ενδιαφέρουσα παρατήρηση: Εάν σε αυτό το πρωτόκολλο η A είναι μία

κανονική υποομάδα της G, τότε $A^w = \mathrm{A}$, και το παραπάνω πρόβλημα γίνεται: δίνονται $\mathrm{w}' \in \mathrm{A}$, θέλουμε να βρούμε δύο οποιαδήποτε στοιχεία $a_1, a_2 \in \mathrm{A}$ τέτοια ώστε $\mathrm{w}' = a_1 a_2$. Αυτό το πρόβλημα είναι εύκολο: εδώ το a_1 θα μπορούσε να είναι ένα οποιοδήποτε στοιχείο από την A και τότε $a_2 = a_1^{-1}\mathrm{w}'$.

Για αυτό τον λόγο, για την επιλογή της ομάδας πλατφόρμας G και των δύο μεταθετικών υποομάδων για ένα πρωτόκολλο (όπως περιγράφηκαν στις παραγράφους 1.2 και 1.3) θα πρέπει να αποφευχθούν οι κανονικές υποομάδες. Αυτό, συγκεκριμένα, σημαίνει ότι το να παρουσιάζουμε τις μεταθετικές υποομάδες ως ευθείς παράγοντες δεν είναι σωστό από την σκοπιά της ασφάλειας.

Στον αντίποδα, υπάρχουν οι αντί-κανονικές (malnormal) υποομάδες.

Ορισμός 1.32. *Αντί-κανονική υποομάδα.*
Μία υποομάδα $A \leq G$ ονομάζεται αντί-κανονική (malnormal) υποομάδα της G, εάν για οποιοδήποτε $g \in G$, $A^g \cap A = \{1\}$.

□

Παρατηρούμε ότι εάν στο αρχικό πρωτόκολλο των Ko-Lee η A είναι αντί-κανονική (malnormal) υποομάδα της G, τότε το Πρόβλημα Αναζήτησης Αποσύνθεσης που αντιστοιχεί σε αυτό το πρωτόκολλο έχει μία μοναδική λύση, εάν $\mathrm{w} \notin \mathrm{A}$. Πράγματι, αν υποθέσουμε ότι $\mathrm{w}' = a_1 \cdot w \cdot a_1' = a_2 \cdot w \cdot a_2'$, όπου $a_1 \neq a_2$ τότε: $a_2^{-1} a_1 \mathrm{w} = \mathrm{w}\, a_2' \acute{a}_1^{-1}$ άρα $w^{-1} a_2^{-1} a_1 \mathrm{w} = a_2' \acute{a}_1^{-1}$. Εφόσον η A είναι αντί-κανονική (malnormal) υποομάδα της G, το στοιχείο στα αριστερά δεν ανήκει στην A, ενώ αυτό στα δεξιά ανήκει, δηλαδή υπάρχει αντίφαση. Αυτό το επιχείρημα δείχνει ότι στην πραγματικότητα αν ισχύει $A^g \cap \mathrm{A} = \{1\}$ για αυτό το συγκεκριμένο w, τότε το αντίστοιχο Πρόβλημα Αναζήτησης Αποσύνθεσης έχει μοναδική λύση.

Τελικά, παρουσιάζουμε ένα ακόμα τέχνασμα που περιορίζει, σε κάποιο βαθμό, το Πρόβλημα Αναζήτησης Αποσύνθεσης στο Περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας. Το ίδιο τέχνασμα περιορίζει και το Πρόβλημα Αναζήτησης Παραγόντων στο Περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας. Υποθέτουμε ότι μας δίνουν $\mathrm{w}' = \mathrm{awb}$ και χρειαζόμαστε να ανακτήσουμε τα $\mathrm{a} \in \mathrm{A}$ και $\mathrm{b} \in \mathrm{B}$, όπου A και B είναι δύο μεταθετικές υποομάδες της ομάδας G.

Επιλέγουμε ένα οποιοδήποτε $b_1 \in \mathrm{B}$ και υπολογίζουμε:

$$[\mathrm{awb}, b_1] = b^{-1} w^{-1} a^{-1} b_1^{-1} a w b b_1 = b^{-1} w^{-1} b_1^{-1} w b b_1 = (b_1^{-1})^{wb}\, b_1 = ((b_1^{-1})^w)^b b_1.$$

Εφόσον γνωρίζουμε το b_1, μπορούμε να πολλαπλασιάσουμε το αποτέλεσμα με το awb, b_1^{-1} από δεξιά και να πάρουμε το $\mathrm{w}'' = ((b_1^{-1})^w)^b$. Τώρα το πρόβλημα γίνεται: ανακτούμε το b ∈ B από το γνωστά $\mathrm{w}'' = ((b_1^{-1})^w)^b$ και $\mathrm{w}' = (b_1^{-1})^w$. Αυτό πρόκειται για το Περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας. Αν το λύσει κάποιος, μπορεί να ανακτήσει τα a και b ∈ B.

Ομοίως, για να ανακτήσουμε ένα a ∈ A, κάποιος μπορεί να επιλέξει ένα οποιοδήποτε στοιχείο $a_1 \in$ A και να υπολογίσει:

$$[(awb)^{-1}, a_1^{-1}] = \mathrm{awb}a_1b^{-1}w^{-1}a^{-1}a_1^{-1} = \mathrm{aw}a_1w^{-1}a^{-1}a_1^{-1} = a_1^{w^{-1}a^{-1}}a_1^{-1}$$

Πολλαπλασιάζουμε το αποτέλεσμα με το a_1 από δεξιά για να πάρουμε $\mathrm{w}' = a_1^{w^{-1}a^{-1}}$, και το πρόβλημα γίνεται: ανακτούμε το a ∈ A από το γνωστό $\mathrm{w}' = a_1^{w^{-1}a^{-1}}$ και $a_1^{w^{-1}}$.

Έχουμε σημειώσει ότι, εφόσον μία λύση του Περιορισμένου στις υποομάδες Προβληματος Αναζήτησης Συζυγίας δεν είναι πάντα μοναδική, το να λύσουμε τις παραπάνω δύο περιπτώσεις αυτού του προβλήματος μπορεί να μην δώσει απαραίτητα την σωστή λύση του αρχικού-γνήσιου Προβλήματος Αποσύνθεσης. Παρόλα αυτά, δύο οποιεσδήποτε λύσεις, ας τις ονομάσουμε b′ και b′′, του πρώτου Προβλήματος Αναζήτησης Συζυγίας διαφέρουν κατά ένα στοιχείο του κεντροποιητή $(b_1^{-1})^w$, και αυτός ο κεντροποιητής είναι απίθανο να έχει μη μηδενική τομή με το B.

Ένας παρόμοιος υπολογισμός μας δείχνει ότι το ίδιο τέχνασμα περιορίζει επίσης το Πρόβλημα Αναζήτησης Παραγόντων στο Περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας. Υποθέτουμε ότι δίνονται w = ab και θέλουμε να ανακτήσουμε το a ∈ A και το b ∈ B, όπου A και B είναι δύο μεταθετικές υποομάδες της ομάδας G. Διαλέγουμε ένα οποιοδήποτε $b_1 \in$ B και υπολογίζουμε:

$$[ab, b_1] = b^{-1}a^{-1}b_1^{-1}abb_1 = (b_1^{-1})^b b_1$$

Εφόσον γνωρίζουμε το b_1, μπορούμε να πολλαπλασιάσουμε το αποτέλεσμα με το b_1^{-1} από δεξιά, για να πάρουμε το αποτέλεσμα. Αυτό είναι το Περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας. Αν το λύσει κάποιος, μπορεί να ανακτήσει τα a, b ∈ B.

Το ίδιο τέχνασμα, στην πραγματικότητα, μπορεί να χρησιμοποιηθεί για να επιτεθούμε στο ίδιο το Περιορισμένο στις υποομάδες Πρόβλημα Αναζήτησης Συζυγίας. Υποθέτουμε ότι μας έχουν δοθεί $\mathrm{w}' = a^{-1}\mathrm{w}a$ και χρειαζόμαστε να ανακτήσουμε το a ∈ A. Διαλέγουμε ένα b από την κεντροποιούσα υποομάδα του A, τυπικά υπάρχει μία δημόσια υποομάδα B που τα στοιχεία της μεταθέτονται με αυτά της A, τότε απλά επιλέγουμε ένα b ∈ B. Στην συνέχεια υπολογίζουμε:

$$[\mathrm{w}',\mathrm{b}] = [a^{-1}\mathrm{w}\alpha,\mathrm{b}] = a^{-1}w^{-1}ab^{-1}a^{-1}wab = a^{-1}w^{-1}b^{-1}\mathrm{w}\alpha\mathrm{b} = (b^{-w})^{a}b$$

Πολλαπλασιάζουμε το αποτέλεσμα με το b^{-1} από δεξιά, για να πάρουμε το $(b^{-w})^{a}$. Έτσι το πρόβλημα τώρα είναι να ανακτήσουμε το $\mathrm{a} \in \mathrm{A}$ από το $(b^{-w})^{a}$ και το b^{-w}. Αυτό το πρόβλημα μπορεί να είναι ευκολότερο απο το αρχικό-γνήσιο πρόβλημα, επειδή υπάρχει ευελιξία στην επιλογή του $\mathrm{b} \in \mathrm{B}$. Συγκεκριμένα, μία εφικτή επίθεση, μπορεί να είναι να επιλέξει αρκετά διαφορετικά και να προσπαθήσει να λύσει το παραπάνω Πρόβλημα Αναζήτησης Συζυγίας για κάθε ένα $\mathrm{b} \in \mathrm{B}$, ενώ παράλληλα θα χρησιμοποιήσει κάποια γενική μέθοδο, για παράδειγμα την επίθεση μήκους. Είναι πιθανό αυτή η επίθεση να είναι επιτυχής για τουλάχιστον ένα από τα bs.

Κεφάλαιο 2

Ομάδες Πλατφόρμας

Στην παράγραφο 1.2 περιγράψαμε κάποιες συνθήκες που θα πρέπει να ικανοποιεί μία ομάδα πλατφόρμας ενός πρωτοκόλλου που βασίζεται στο Πρόβλημα Αναζήτησης Συζυγίας. Στην πραγματικότητα, οι περισσότερες από αυτές τις συνθήκες εφαρμόζονται σε ομάδες πλατφόρμας οποιουδήποτε *κανονικού* (δηλαδή, που βασίζεται σε μονόδρομη συνάρτηση) κρυπτογραφικού πρωτοκόλλου, έτσι τις συνοψίζουμε παρακάτω:

Σ0. Η ομάδα θα πρέπει να είναι γνωστή (ή τουλάχιστον πολύ καλά μελετημένη ή και τα δύο ταυτόχρονα).

Σ1. Το Πρόβλημα Λέξης στην G θα πρέπει να έχει γρήγορη (γραμμικού ή τετραγωνικού χρόνου) λύση από έναν αλγόριθμο. Ακόμα καλύτερα, θα πρέπει να υπάρχει μία επαρκής *κανονική μορφή* των στοιχείων της G.

Σ2. Θα πρέπει να υπάρχει τρόπος να μεταμφιέζουμε τα στοιχεία της G, έτσι ώστε να είναι αδύνατο να ανακτήσει κάποιος, ας πούμε, τα x και y από το γινόμενο xy απλά με έλεγχο. Ξανά, μία επαρκής υπολογίσιμη κανονική μορφή θα ήταν χρήσιμη.

Εάν δεν υπάρχει κανονική μορφή, έστω ότι η G δίνεται από τους γεννήτορες και κάποιες σχέσεις, χωρίς παραπάνω πληροφορίες για τις ιδιότητες της G τότε τουλάχιστον κάποιες από αυτές τις σχέσεις θα πρέπει να είναι μικρές.

Σ3. Η G θα πρέπει να είναι μία ομάδα με υπερ-πολυωνυμική ανάπτυξη (δηλαδή εκθετική ή μεσαία). Αυτό σημαίνει ότι το πλήθος των στοιχείων που έχουν μήκος n στην G θα πρέπει να αναπτύσονται γρηγορότερα από ένα πολυώνυμο του n. Πράγμα το οποίο χρειάζεται, για να αποτρευτούν επιθέσεις εξάντλησης για το

κλειδί. Με τον όρο *μήκος κλειδιού*, τυπικά εννοούμε το μήκος μίας λέξης που αντιπροσωπεύει ένα στοιχείο της ομάδας, αλλά πιο γενικά, είναι το μήκος μίας περιγραφής.

Σε αυτό το κεφάλαιο θα εξετάσουμε διάφορες ομάδες (ή τάξεις ομάδων) ως πιθανές πλατφόρμες κρυπτογραφικών πρωτοκόλλων δημοσίου κλειδιού.

2.1 Ομάδες Πλεξίδων

Οι ομάδες πλεξίδων, που ορίστηκαν από τον Artin, είναι μία πολύ ενδιαφέρουσα ομάδα με πολλές πτυχές: σε πολλούς διαφορετικούς επιστημονικούς κλάδους υπάρχει το Πρόβλημα Λέξης της (για να καθορίσει αν δύο στοιχεία είναι ίσα ή όχι σε μία ομάδα). Είναι εύκολο να λυθεί, αλλά κάποια άλλα προβλήματα (όπως είναι το Προβλημα Συζυγίας ή Πρόβλημα Αποσύνθεσης) είναι πιο δύσκολα να λυθούν.

Βασισμένα στην ομάδα πλεξίδων και τα προβλήματα της, δύο κρυπτογραφικά συστήματα παρουσιάστηκαν μία δεκαετία μετά: από τους Anshel-Anshel-Goldfeld, Ko, Lee, Cheon, Han, Kang και Park. Αυτά τα κρυπτογραφικά συστήματα πυροδότησαν μια μεγάλη συζήτηση για τις δυνατότητες της κρυπτογραφίας πάνω στις ομάδες πλεξίδων, αλλά και στις ομάδες γενικότερα.

Ένα ενδιαφέρον σημείο το οποίο αξίζει να αναφέρουμε είναι το Πρόβλημα Συζυγίας στις ομάδες πλεξίδων, το οποίο είχε προσελκύσει το ενδιαφέρον των ερευνητών, πολύ πριν προταθούν τα κρυπτογραφικά συστήματα που βασίζονται στις ομάδες πλεξίδες. Αφού προτάθηκαν τα κρυπτογραφικά αυτά συστήματα, δόθηκαν κάποιες πιθανολογικές λύσεις, αλλά έδωσαν μεγάλη ώθηση στις προσπάθειες να λυθεί θεωρητικά το Πρόβλημα Συζυγίας σε πολυωνυμικό χρόνο.

Η δυνητική χρήση των ομάδων πλεξίδων στην κρυπτογραφία οδήγησε σε επιπλέον προτάσεις κρυπτογραφικών συστημάτων που βασίζονται στα εμφανώς δύσκολα προβλήματα των ομάδων πλεξίδων και σε άλλες ομάδες, όπως του Thompson.

Οι φήμες λένε ότι οι συγγραφείς που εφηύραν το πρωτόκολλο αυτό, προσέγγισαν την Joan Birman ζητώντας της να προτείνει «καλές» μη αβελιανές ομάδες που θα μπορούσαν να χρησιμοποιηθούν ως πλατφόρμα. Χωρίς έκπληξη, η απάντησή της ήταν οι « ομάδες πλεξίδων». Ύστερα από κάποιο αρχικό ενθουσιασμό (που είχε ως αποτέλεσμα την ονομασία αυτού του κλάδου ως «κρυπτογραφία ομάδων πλεξίδων»), φάνηκε ότι το Πρόβλημα Αναζήτησης Συζυγίας στις ομάδες πλεξίδων μπορεί να μην παρείχε ένα

επαρκές επίπεδο ασφαλείας, εκτός εάν τα κλειδιά επιλέγονταν από κάποια μικρά υποσύνολα της ομάδας (που θα πρέπει να οριστούν). Αυτό με το οποίο θα ασχοληθούμε παρακάτω είναι να αναλύσουμε τα πλεονεκτήματα και τα μειονεκτήματα των ομάδων πλεξίδων και να δώσουμε κάποιο θεωρητικό υπόβαθρο.

Είναι γεγονός ότι οι αφηρημένες ομάδες, αντίθετα από τους αριθμούς, δεν είναι κάτι που μαθαίνουμε από την αρχή. Γι΄ αυτό τον λόγο, υπάρχει ένα εμφανές πρόβλημα επικοινωνίας που εμπλέκεται στην προώθηση ενός κρυπτογραφικού προιόντος που χρησιμοποιεί, με κάποιο τρόπο, αφηρημένες ομάδες. Οι ομάδες πλεξίδων παρουσιάζουν ένα προτέρημα, διότι, για να μπορέσουμε να εξηγήσουμε τι είναι, μπορούμε να τις παρουσιάσουμε και σχηματικά. Το γεγονός ότι οι ομάδες πλεξίδων χρησιμοποιούνται σε πολλούς τομείς των μαθηματικών (και της φυσικής) βοηθάει, εφόσον δίνει περισσότερη αξιοπιστία στην δυσκολία του σχετικού προβλήματος.

Θυμόμαστε, για παράδειγμα, πως η εμπιστοσύνη στην ασφάλεια του κρυπτογραφικού συστήματος RSA βασίζεται στις, διαρκείς προσπάθειες χιλιάδων ανθρώπων, όπως είναι και οι μεγάλοι μαθηματικοί Euler και Gauss, για την γρήγορη παραγοντοποίηση ακεραίων. Η ιστορία των ομάδων πλεξίδων ξεκινάει το 1927, όπου ξανά πολλές εκατοντάδες ανθρώπων, συμπεριλαμβανομένων αρκετών υποσχόμενων μαθηματικών όπως Artin, Birman, Thurston, V.F.R. Jones, δούλευαν πάνω σε διάφορες εκδοχές των ομάδων αυτών, όπως και αλγοριθμικές.

Αντιθέτως, από την άποψη της ασφάλειας, το γεγονός ότι οι ομάδες πλεξίδων εμπλέκονται σε τόσες διαφορετικές επιστήμες μπορεί να είναι μειονέκτημα, επειδή οι διαφορετικές επιστήμες και τομείς δίνουν περισσότερα εργαλεία, για να λυθεί το πρόβλημα. Επιπλέον, οι ομάδες πλεξίδων αποδείχθηκαν γραμμικές, πράγμα το οποίο τις καθιστά ευάλωτες σε επιθέσεις γραμμικής άλγεβρας. Αυτό από μόνο του είναι σοβαρό πρόβλημα ασφαλείας.

Όπως είπαμε παραπάνω, οι ομάδες πλεξίδων εμφανίζονται σε πολλούς τομείς των μαθηματικών και έχουν πολλούς ορισμούς. Θα ξεκινήσουμε με μία παρουσίαση των ομάδων πλεξίδων από τους γεννήτορες και τις σχέσεις τους.

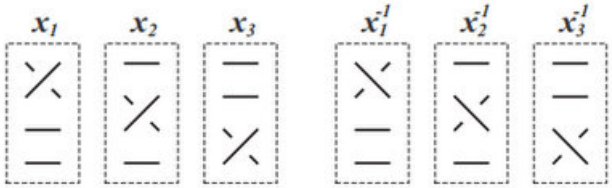
2.1.1 Παρουσίαση της Ομάδας Πλεξίδων

Υπενθυμίζουμε:

Ορισμός 2.1. *Γεννήτορες μιας ομάδας.*
Είναι δυνατό τα στοιχεία μιας ομάδας να παράγονται από ορισμένα στοιχεία χρησιμο-

ποιώντας τις δυνάμεις και τα γινόμενα αυτών. Τα στοιχεία αυτά, των οποίων το πλήθος είναι το μικρότερο δυνατό λέμε ότι αποτελούν γεννήτορες της ομάδας.

□



Οι γεννήτορες της B_4 και οι αντίστροφοί τους.

Σε αυτή την παράγραφο θα παρουσιάσουμε τις ομάδες πλεξίδες. Φανταζόμαστε δύο ράβδους, οριζόντιες, παράλληλες μεταξύ τους, με το επίπεδο που ορίζουν να είναι κάθετο στο έδαφος. Σε κάθε μία τους υπάρχουν τοποθετημένοι n γάντζοι-σημεία, τα $A_1, ...A_n$ στην πάνω και τα $B_1, ...B_n$ στην κάτω, έτσι ώστε:

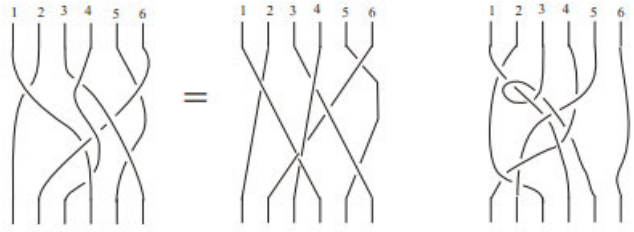
$$\mid A_{i+1} - A_i \mid = \mathrm{c} = \mid B_{i+1} - B_i \mid,$$

$\forall$ i με $0 \leq$ i $\leq$ n-1, και έτσι ώστε το A_1 να βρίσκεται ακριβώς πάνω από το B_1. Φανταστείτε τώρα n κλωστές, με το ένα άκρο τους δεμένο σε κάποιον απο τους A_i και τον άλλο σε κάποιο από τους B_i. Δεν θέλουμε οι κλωστές να μπλέκονται με τον εαυτό τους ούτε να δημιουργούν *κόμπους*. Μπορούμε να απαιτήσουμε τα παρακάτω χαρακτηριστικά:

- Καθένας από τους A_i και B_i έχει δεμένη ακριβώς μία κλωστή.
- Κάθε επίπεδο κάθετο στο επίπεδο των ράβδων, παράλληλο σε αυτές και διερχόμενο ανάμεσά τους, τέμνει κάθε κλωστή σε ακριβώς ένα σημείο.

Ένας τέτοιος σχηματισμός θα ονομάζεται **πλεξίδα σε n κλωστές** ή διαφορετικά **n-πλεξίδα** ή **trivial πλεξίδα**.

Αν δύο πλεξίδες μπορούν να δημιουργηθούν η μία από την άλλη με απλή μετακίνηση ή με αυξομείωση του μήκους των κλωστων, δηλαδή χωρίς να σπάσει ή να λυθεί μία από αυτές, θα τις θεωρούμε ίδιες και δεν θα κάνουμε καμία διάκριση μεταξύ τους.

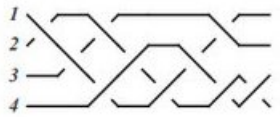


Τα δύο πρώτα σχέδια απεικονίζουν δύο 6-πλεξίδες, ίδιες μεταξύ τους, ενώ το τρίτο δεν είναι πλεξίδα.

Παραστατικά, εάν βάλουμε κάτω και στην σειρά δύο ράβδους τις u και v έτσι ώστε το τέλος της u να είναι η αρχή της v, παίρνουμε μία πλεξίδα που την συμβολίζουμε ως uv, δηλαδή το αποτέλεσμα είναι μία αλληλουχία n κλωστών.

Ορισμός 2.2. *Έστω μία n-πλεξίδα A. Θα λέμε ότι δύο κλωστές διασταυρώνονται θετικά στην A, αν αυτή που έρχεται από δεξιά περνά πάνω από αυτήν που έρχεται από αριστερά. Διαφορετικά, λέμε ότι διασταυρώνονται αρνητικά.*

□



Μία 4-πλεξίδα.

Μία από τις ιδιότητες των πλεξίδων, είναι ότι μπορούμε να ορίσουμε μία πράξη πολλαπλασιασμού ανάμεσα σε δύο πλεξίδες με τον ίδιο αριθμό κλωστών: τοποθετώντας την πρώτη πάνω από την δεύτερη, ξεγαντζώνουμε και ενώνουμε τα ελεύθερα άκρα. Αυτό που προέκυψε είναι επίσης πλεξίδα σε n κλωστές. Παρατηρούμε ότι η πράξη αυτή δεν είναι αντιμεταθετική.

Άλλη μία ιδιότητα των πλεξίδων είναι ότι για κάθε n, το σύνολο των πλεξίδων σε n κλωστές αποτελεί ομάδα με πράξη τον πολλαπλασιασμό, όπως ορίσαμε παραπάνω. Υπάρχει η μοναδιαία πλεξίδα e_n που αποτελείται από n παράλληλες κατακόρυφες κλωστές. Ακόμα, μπορούμε να σχηματίσουμε την αντίστροφη κάθε πλεξίδας, ανακλώντας την αρχική ως προς την κάτω ράβδο. Τέλος, η πράξη είναι κλειστή και προσεταιριστική. Η απόδειξη των παραπάνων είναι γεωμετρική. Θα συμβολίσουμε την ομάδα των πλεξίδων σε n κλωστές με B_n.

Θα ασχοληθούμε τώρα με την αλγεβρική αναπαράσταση των πλεξίδων. Έστω n ∈ N. Ορίζουμε (n-1) n-πλεξίδες τις $x_1, ...x_{n-1}$ τις οποίες θα ονομάσουμε **στοιχειώδεις n-πλεξίδες**, ως εξής:

Η x_i είναι η n-πλεξίδα πανομοιότυπη με την ταυτοτική, με μοναδική διαφορά ότι η κλωστή που ξεκινά από το A_i καταλήγει στο B_{i+1}, ενώ αυτή που ξεκινά από το A_{i+1} καταλήγει στο B_i και διασταυρώνονται θετικά.

Κάθε n-πλεξίδα μπορεί να αναπαρασταθεί ως σύνθεση στοιχειωδών n-πλεξίδων και των αντιστρόφων τους.

Προκύπτουν οι παρακάτω ταυτότητες:

1. Τετριμμένες σχέσεις:

$$x_i x_i^{-1} = x_i^{-1} x_i = 1 \text{ και } x_i \cdot \mathbf{1} = \mathbf{1} \cdot x_i = x_i$$

για i = 1,2,..., n-1

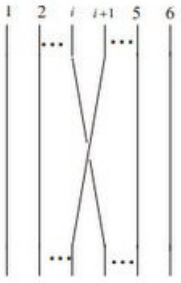
2. Ασθενής αντιμεταθετικότητα:

$$x_i x_j = x_j x_i \text{ όταν } \mid i - j \mid \geq 2 \text{ , i = 1,2,...,n-1}$$

3. Σχέσεις πλεξίδων:

$$x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$$

για i = 1,2,..., n-2



Η s_i στην B_6.

Μπορούμε να πούμε ότι τα για x_i , για για i = 1,2,..., n-1 αποτελούν ένα σύνολο γεννητόρων της B_n, δηλαδή το σύνολο $\{x_1, ..., x_{n-1}\}$ παράγει την B_n.

Ο Artin χρησιμοποιήσε τον εξής συμβολισμό :

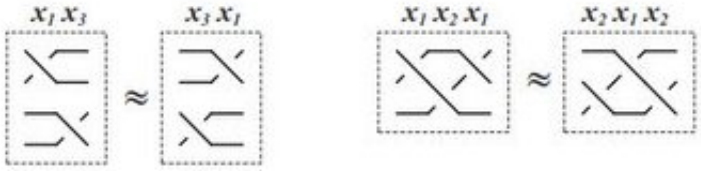
$$B_n = \langle x_1, ...x_{n-1} \mid x_i x_j x_i = x_j x_i x_j \text{ εάν } \mid i - j \mid = 1 \text{ και } x_i x_j = x_j x_i \text{ εάν } \mid i - j \mid > 1 \rangle$$

Με αυτή την περιγραφή μπορεί κανείς εύκολα να δει ότι η B_n έχει άπειρα στοιχεία. Για παράδειγμα, μπορούμε να πολλαπλασιάζουμε συνεχώς με το x_1 και να παίρνουμε πάντα κάτι διαφορετικό, αφού $x_1^i \neq x_1^j$ όταν i ≠ j.

Ορισμός 2.3. *Η B_n είναι ελεύθερης στρέψης (torsion free), αν δεν έχει κανένα στοιχείο στρέψης, δηλαδή δεν υπάρχει κάποιο άλλο στοιχείο g εκτός από το e (την ταυτοτική πλεξίδα), τέτοιο ώστε να ισχύει $g^m = e$ για κάποιο $m \in N$*

□

Επομένως, είναι δυνατό να χρησιμοποιηθεί η B_n ως ομάδα πλατφόρμας για τα πρωτόκολλα που αναφέραμε στις παραγράφους 1.2 και 1.3. Για παράδειγμα, το πρωτόκολλο των Ko, Lee και άλλων χρησιμοποίησε τις ακόλουθες δύο εναλασσόμενες υποομάδες: LB_n που παράγονται από τα $x_1, ...x_{\frac{n}{2}-1}$ και το UB_n που παράγονται από τα $x_{\frac{n}{2}+1}, ...x_{n-1}$.



Τυπικές σχέσεις στις πλεξίδες.

Θα ξανεξετάσουμε τις ιδιότητες (Σ1)-(Σ3) που αναφέραμε στην εισαγωγή αυτού του κεφαλαίου. Υπάρχει πολύ μεγάλη βιβλιογραφία σχετικά με το Πρόβλημα Λέξης και το Πρόβλημα Αναζήτησης Συζυγίας για τις ομάδες πλεξίδων. Οι αρχικές λύσεις και των δύο προβλημάτων, που οφείλονται ουσιαστικά στον Garside, μπορούν να βρεθούν στο μονόγραμμα της Birman. Πολλοί άλλοι αλγόριθμοι προτάθηκαν έκτοτε, οι περισσότεροι από τους οποίους είναι αρκετά αποτελεσματικοί. Ο καλύτερος αυτή τη στιγμή αλγόριθμος για το Πρόβλημα Λέξης έχει τετραγωνική πολυπλοκότητα, δηλαδή O(n^2), όπου n το μήκος της εισαγώμενης λέξης. Επιπλέον, ξεχωρίζουμε τον αλγόριθμο του Dehornoy για το Πρόβλημα Λέξης, του οποίου η πολυπλοκότητα είναι άγνωστη ακόμα και σήμερα. Παρόλα αυτά, φαίνεται ότι δουλεύει πολύ γρήγορα σε πρακτικές εκτελέσεις, πράγμα το οποίο προτείνει ότι η γενική πολυπλοκότητα αυτού του αλγορίθμου μπορεί να είναι γραμμικού χρόνου. Σημειώνουμε ότι υπάρχουν αλγόριθμοι με γενική πολυπλοκότητα που είναι γραμμικού χρόνου για το Πρόβλημα Λέξης στις ομάδες πλεξίδες, που βασίζονται στους ελέγχους πηλίκων. Παρόλα αυτά, αυτοί οι αλγόριθμοι, λόγω του σχεδιασμού τους δίνουν γρηγορότερα αποτελέσματα, εάν η απάντηση είναι *όχι*, δηλαδή

εάν η εισαγώμενη λέξη δεν είναι ίση με το 1 στην B_n. Αντιθέτως, ο αλγόριθμος του Dehornoy δίνει γρήγορα και την απάντηση *ναι*, τουλάχιστον τις περισσότερες φορές. Ωστόσο, δεν έχει βρεθεί ακόμα θεωρητικά το υπο-εκθετικό άνω φράγμα του χρόνου πολυπλοκότητας του αλγορίθμου του Dehornoy.

Το Πρόβλημα Συζυγίας για τις ομάδες πλεξίδων είχε και έχει πολύ ενδιαφέρον. Πρόσφατα, έχει γίνει εκτεταμένη έρευνα σχετικά με την (στην χειρότερη περίπτωση) πολυπλοκότητα αυτού του προβλήματος. Έχει γίνει αξιοσημείωτη πρόοδος που οφείλεται στις έρευνες των Birman, Gonzales-Meneses, Gebhardt, E. Lee, S. J. Lee και άλλων. Παρόλα αυτά, παραμένει ανοικτό το πρόβλημα: αν το Πρόβλημα Απόφασης ή Αναζήτησης Συζυγίας στις ομάδες πλεξίδων μπορεί να λυθεί σε πολυωνυμικό χρόνο από έναν αλγόριθμο. Το ασθενές πρόβλημα: αν το Πρόβλημα Συζυγίας στις ομάδες πλεξίδων είναι της τάξης πολυπλοκότητας NP, είναι ακόμα ανοικτό.

Εάν πάρουμε την συνθήκη (Σ2), παρατηρούμε ότι υπάρχουν πολλές κανονικές μορφές για στοιχεία των ομάδων πλεξίδων που είναι γνωστές και πρόκειται για φυσικούς μηχανισμούς απόκρυψης. Όμως, εδώ πρέπει να προειδοποιήσουμε ότι η παρουσία πολλών διαφορετικών κανονικών μορφών μπορεί να είναι πιθανό πρόβλημα ασφαλείας, επειδή μία κανονική μορφή μπορεί να αποκαλύψει τι προσπαθεί να κρύψει μία άλλη. Στην πραγματικότητα, αυτή η παρατήρηση έχει ήδη χρησιμοποιηθεί για την κρυπτανάλυση ενός πρωτοκόλλου που βασίζεται στις ομάδες πλεξίδων: το να μετατρέψεις την κανονική μορφή Garside στην κανονική μορφή Dehornoy καθιστά την αντίστοιχη μεταβίβαση πιο ευάλλωτη σε κάποιες επιθέσεις.

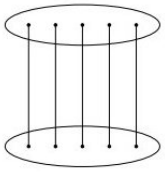
Τέλος, σχετικά με την συνθήκη (Σ3) παρατηρούμε ότι όλες οι ομάδες πλεξίδων B_n έχουν εκθετική ανάπτυξη εάν $\mathrm{n} \geq 2$. Για $\mathrm{n} \geq 3$ αμέσως έπεται το γεγονός ότι η B_n έχει ελεύθερες υποομάδες. Για παράδειγμα τα x_1^2 και x_2^2 παράγουν μία ελεύθερη υποομάδα.

2.1.2 Μέθοδος Dehornoy χωρίς χερούλι

Θυμίζουμε ότι με τον όρο *κανονική μορφή* ενός στοιχείου της ομάδας εννοούμε την μοναδική παρουσίασή του σε κάθε στοιχείο της ομάδας. Είναι πολύ χρήσιμο τα στοιχεία να έχουν μία κανονική μορφή μέσα στην ομάδα. Αυτό μας επιτρέπει να συγκρίνουμε δύο στοιχεία, γεγονός που δίνει λύση για το Πρόβλημα Λέξης.

Παράδειγμα 2.4. *Δίνεται μία πλεξίδα w. Ισχύει $w \equiv \epsilon$; Δηλαδή, το w αντιπροσωπεύει την μονάδα πλεξίδας ϵ;*

□



Η μονάδα πλεξίδας ε $\in B_5$.

Εφόσον η B_n είναι ομάδα, τα παραπάνω πρόβλημα είναι ισοδύναμο με το:

Παράδειγμα 2.5. *Δίνονται δύο πλεξίδες w, w΄. Ισχύει $w \equiv w'$; Δηλαδή, τα w και w΄ αντιπροσωπεύουν την ίδια πλεξίδα;*

□

Η απάντηση είναι ναι, η w ≡ w΄ είναι ισοδύναμη με w^{-1} w΄ ≡ ε, όπου w^{-1} είναι η λέξη που αποκτάμε από την w, αν αντιστρέψουμε την σειρά των γραμμάτων και ανταλλάξουμε τα σ_i και σ_i^{-1} παντού. Βλ[11].

Ορισμός 2.6. *Μία λέξη στις ομάδες πλεξίδων ονομάζεται x_i-**handle** όταν είναι της μορφής $x_i^e v x_i^{-1}$, όπου το $e = \pm 1$ και η v είναι μία λέξη που δεν περιέχει γράμματα της μορφής $x_k^{\pm 1}$, με $k <$ n-1 ή $k > i$ και επιπλέον είτε το x_{i+1} είτε το x_{i+1}^{-1} δεν εμφανίζονται στο v.*

□

Ορισμός 2.7. *Έστω ότι u είναι μία x_i-handle, $u = x_i^e v x_i^{-e}$. Ορίζουμε red(u) να είναι η λέξη που προκύπτει από τη u αντικαθιστώντας κάθε γράμμα με $x_{i+1}^{\pm 1}$ και αφήνοντας τα υπόλοιπα γράμματα απαράλλαχτα. Αν w και w΄ είναι δύο λέξεις στις πλεξίδες, λέμε ότι η w΄ έχει προέλθει από την w με handle-αναγωγή (reduction), αν μπορούμε να μετατρέψουμε την w στην w΄ αντικαθιστώντας διαδοχικά κάποια handle u με τις αντίστοιχες λέξεις red(u).*

□

Με βάση αυτούς τους ορισμούς αποδεικνύεται η ακόλουθη πρόταση:

Θεώρημα 2.8. *Έστω μία λέξη w στις πλεξίδες, μήκους l. Τότε η w είναι ίση με την κενή λέξη e (δηλαδή την ταυτοτική πλεξίδα), αν και μόνο αν η w αναγάγεται στην e, αν και μόνο αν κάθε ακολουθία αναγωγών που ξεκινούν με την w καταλήγουν στην e. Επιπλέον, κάθε ακολουθία αναγωγών που ξεκινά από την w τερματίζει το αργότερο σε εκθετικό χρόνο.*

□

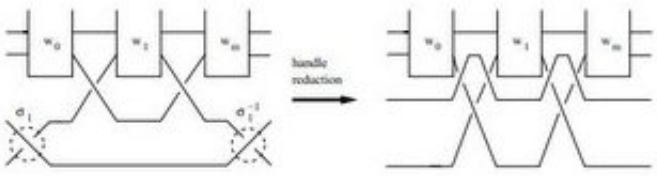
Έτσι, μία λέξη είναι ίση με την κενή, αν και μόνο αν ανάγεται στην κενή.

Η πρόταση δίνει ένα κακό άνω φράγμα, αλλά στην πράξη οι αλγόριθμοι που έχουν προταθεί για την υλοποίηση της αναγωγής δίνουν πολύ καλά αποτελέσματα.

Η διαδικασία *handle-αναγωγή* προτάθηκε από τον Dehornoy και παρατηρούμε ότι πρόκειται για μία επέκταση της διαδικασίας handle-αναγωγής για τις ελεύθερες ομάδες. Η διαδικασία handle-αναγωγής αποτελείται από την επαναλαμβανόμενη διαγραφή όλων των μοτίβων της μορφής $\mathrm{x}x^{-1}$ ή $x^{-1}\mathrm{x}$. Ξεκινάμε με μία αυθαίρετη λέξη w μήκους m, χωρίς να έχει σημασία πώς έγιναν οι μειώσεις. Κάποιος θα τελειώσει το πολύ στα $\frac{m}{2}$ βήματα με μία μοναδική μειωμένη λέξη, που δεν περιέχει $\mathrm{x}x^{-1}$ ή $x^{-1}\mathrm{x}$.

Οι ελεύθερες μειώσεις είναι δυνατές για οποιαδήποτε παρουσίαση μίας ομάδας και ιδιαίτερα για την B_n. Για παράδειγμα, η λέξη $x_1x_2x_1x_2^{-1}x_1^{-1}x_2^{-1}$ αντιπροσωπεύει μία μονάδα λέξης, αλλά οι ελεύθερες μειώσεις δεν μπορούν να την μειώσουν άλλο.

Η διαδικασία handle-αναγωγής γενικεύει τις ελεύθερες μειώσεις και περιλαμβάνει όχι μόνο μοτίβα της μορφής $\mathrm{x}x^{-1}$ ή $x^{-1}\mathrm{x}$, αλλά και πιο γενικά μοτίβα της μορφής $x_1...x_i^{-1}$ ή $x_1^{-1}...x_i$.



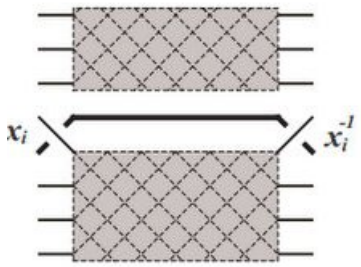
Ένα παράδειγμα μίας handle-αναγωγής (για την σ_1). Οι δύο κυκλωμένες διασταυρώσεις στην αριστερή εικόνα είναι η αρχή και το τέλος της αναγωγής.

Ορισμός 2.9. *Ένα x_i-handle $x_i^{-e}wx_i^e$, όπου $w = w(x_1, ..., x_{i-2}, x_{i+1}, ..., x_n$ ονομάζεται επιτρεπτό (permitted), εάν η w δεν περιέχει x_{i+1}-handles. Λέμε ότι η λέξη της πλεξίδας υ'λαμβάνεται απο την λέξη πλεξίδας v με ένα βήμα handle-αναγωγής, εάν κάποια υπολέξη της v είναι ένα επιτρεπτό x_i-handle $x_i^{-e}wx_i^e$ και υ'λαμβάνεται από την v, αν εφαρμοστούν οι ακόλουθες αντικαταστάσεις για όλα τα γράμματα σε ένα handle $x_i^{-e}wx_i^e$:*

$$x_j^{\pm 1} \longrightarrow \begin{cases} 0 & \epsilon\acute{\alpha}\nu \quad j = i \\ x_{i+1}^e x_i^{\pm 1} x_{i+1}^e & \epsilon\acute{\alpha}\nu \quad j = i+1 \\ x_j^{\pm 1} & \epsilon\acute{\alpha}\nu \quad j > i+1, j < i \end{cases}$$

□

Σε αυτό το σχήμα έχουμε:



Μία αναγωγή.

Ορισμός 2.10. *Λέμε ότι η λέξη πλεξίδας v΄λαμβάνεται από την λέξη πλεξίδας v από m βήματα handle-αναγωγή, εάν υπάρχει μία αλληλουχία m+1 λέξεων $v = v_0, v_1, ..., v_m = v'$ όπου κάθε μία από αυτές έχει ληφθεί από την προηγούμενη με ενός βήματος handle-αναγωγή. Μία λέξη πλεξίδας καλείται handle free ή handle ελεύθερη, εάν δεν περιέχει καμία handle.*

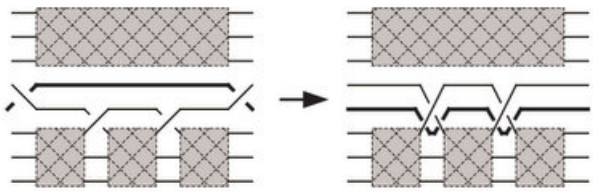
□

Η βασική ουσία της handle-αναγωγής αναφέρεται στο παρακάτω θεώρημα:

Θεώρημα 2.11. *Έστω v μία λέξη της ομάδας πλεξίδων. Ισχύουν τα ακόλουθα:*

- *Οποιαδήποτε ακολουθία handle-αναγωγών που εφαρμόζονται για την v τελικά θα σταματήσουν και θα παράγουν μία handle free ή handle ελεύθερη λέξη πλεξίδα v΄ (που γενικά εξαρτάται από μία συγκεκριμένη αλληλουχία αναγωγών), αντιπροσωπεύοντας το ίδιο στοιχείο της ομάδας πλεξίδων, όπως η v.*
- *Η λέξη v αντιπροσωπεύει την ταυτότητα μίας ομάδας πλεξίδων, αν και μόνο αν οποιαδήποτε αλληλουχία handle-αναγωγής εφαρμοστεί στην v παράγεται η trivial λέξη.*

□



Μία handle-αναγωγή ενός βήματος ενός επιτρεπτού $x_i - handle$.

Παρατήρηση 2.12. ***Εκτιμήση Πολυπλοκότητας :*** *Παρόλο που η διαδικασία της handle-αναγωγής στην πράξη είναι πολύ αποτελεσματική και τις περισσότερες φορές λειτουργεί σε γραμμικό χρόνο βάσει του μήκους της λέξης της ομάδας πλεξίδων, δεν υπάρχει καλή εκτίμηση της πολυπλοκότητας.*

□

2.1.3 Κανονική Μορφή Garside

Η κανονική μορφή του Garside προέρχεται από την έρευνα και την δουλειά του Garside. Πολλές παραλλαγές έχουν μελετηθεί σε πολλές ανεξάρτητες μελέτες.

Ορισμός 2.13. *Απλά στοιχεία.*

Έστω μια ομάδα μεταθέσεων S_n. Για κάθε μετάθεση $s \in S_n$ θεωρούμε την κοντύτερη θετική πλεξίδα ξ_s, έτσι ώστε $\pi(\xi_s) = s$. Τα στοιχεία:

$$S = \{\xi_s \mid s \in S_n\}$$

καλούνται ***απλά στοιχεία****.*

□

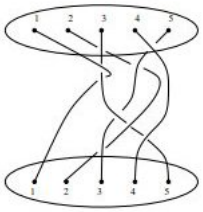
Ορισμός 2.14. *Για τις μεταθέσεις s και t λέμε ότι ένα απλό στοιχείο ξ_s είναι μικρότερο από το ξ_t (ή ότι το ξ_s είναι ένας αριστερός διαιρέτης του ξ_t), αν υπάρχει $r \in S_n$ τέτοιο ώστε $\xi_t = \xi_s\xi_r$ και το συμβολίζουμε με $\xi_s < \xi_t$.*

□

Τα στοιχεία της B_n μπορούν να ερμηνευτούν ως γεωμετρικές πλεξίδες σε n κλωστές. Κάθε πλεξίδα μπορεί να συνδεθεί με το επίπεδο διάγραμμα που παίρνουμε αν ενώσουμε τα στοιχειώδη σχεδιαγράμματα της εικόνας που αντιστοιχούν σε επιτυχημένα γράμματα.

Οι γεωμετρικοί Artin γεννήτορες.

Φαίνεται ότι ένα διάγραμμα πλεξίδας απορρέι από μία εικόνα τριών-διαστάσεων που αποτελείται από n ασύνδετες καμπύλες που συνδέουν τα σημεία (1, 0, 0), ..., (n, 0, 0) με τα σημεία (1, 0, 1), ..., (n, 0, 1) στον $\mathbb{R}^3$.



Ένα παράδειγμα μίας πλεξίδας στην B_5.

Τότε οι σχέσεις με τις οποίες ορίσαμε στον συμβολισμό του Artin έχουν την εξής ιδιότητα: μετακινούν συνεχώς τις καμπύλες χωρίς να αλλάζουν τα άκρα, που είναι το τέλος τους, και δεν τις αφήνουν να τμηθούν. Συνεπώς, το Πρόβλημα Λέξης για τις ομάδες πλεξίδων με τον συμβολισμό του Artin είναι επίσης ένα Πρόβλημα Ομάδων Πλεξίδων.

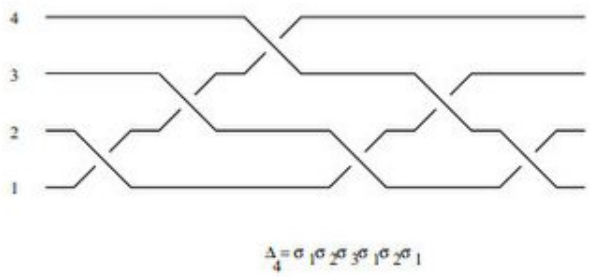
Ξεκινάμε με τον ορισμό της *θετικής πλεξίδας*, η οποία είναι μία πλεξίδα που μπορεί να γραφτεί ως γινόμενο θετικών δυνάμεων των γεννητόρων του Artin.

Χρησιμοποιούμε τον συμβολισμό B_n^+ για να δηλώσουμε το σύνολο όλων των θετικών πλεξίδων. Αυτό το σύνολο έχει την δομή ενός μονοειδούς με πράξη την αλληλουχία πλεξίδων.

Ένα σημαντικό παράδειγμα θετικών πλεξίδων, το οποίο παίζει κεντρικό ρόλο στην κανονική μορφή του Garside, είναι η $\Delta_n \in B_n$:

$$\Delta_n = (\sigma_1 ... \sigma_{n-1})\ (\sigma_1 ... \sigma_{n-2})\ ...\ \sigma_1$$

Γεωμετρικά, η Δ_n είναι πλεξίδα σε n-κλωστές, όπου δύο οποιεσδήποτε κλωστές διασταυρώνονται θετικά ακριβώς μία φορά.



Η θεμελιώδης πλεξίδα Δ_4.

Η θεμελιώδης πλεξίδα έχει κάποιες σημαντικές ιδιότητες:

1. Για οποιοδήποτε γεννήτορα σ_i, μπορούμε να γράψουμε $\Delta_n = \sigma_i$ A = B σ_i , όπου A, B θετικές πλεξίδες.

2. Για οποιοδήποτε γεννήτορα σ_i, ισχύουν τα ακόλουθα:

$$\tau(\sigma_i\ ) = \Delta_n^{-1}\sigma_i\Delta_n = \sigma_{n-i}$$

3. Η Δ_n^2 είναι ο γεννήτορας του κέντρου της B_n.

Στην συνέχεια, θα παρουσιάσουμε τις *πλεξίδες μετάθεσης*. Μπορεί να οριστεί μερική σειρά στα στοιχεία της B_n: Για A, B $\in B_n$ λέμε ότι η A είναι μία **προκαθόριση** της B εάν B = AC για κάποια C $\in B_n^+$ και την συμβολίζουμε με A $\preceq$ B. Βασικές ιδιότητες είναι οι ακόλουθες:

- B $\in B_n^+ \Leftrightarrow \varepsilon \preceq$ B
- A $\preceq$ B $\Leftrightarrow B^{-1} \preceq A^{-1}$

Η P $\in B_n$ είναι **πλεξίδα μετάθεσης** (ή απλή πλεξίδα), εάν ικανοποιεί την $\varepsilon \preceq$ P $\preceq \Delta_n$. Η ονομασία της προέρχεται από το γεγονός της ύπαρξης αμφιμονοσήμαντης αντιστοιχίας ανάμεσα στο σύνολο των πλεξίδων μεταθέσεων της B_n με την συμμετρική ομάδα S_n (υπάρχει μία φυσική *χαρτογράφηση* από την B_n στην S_n, που ορίζεται αν στείλουμε το i στο τέλος της κλωστής η οποία ξεκινά από την θέση i). Επομένως, έχουμε n! πλεξίδες μεταθέσεων. Βλ[11].

Γεωμετρικά, η πλεξίδα μετάθεσης είναι μία πλεξίδα σε n-κλωστές, όπου δύο οποιεσδήποτε κλωστές διασταυρώνονται θετικά το πολύ μία φορά.

Δίνεται μία πλεξίδα μετάθεσης P, μπορούμε να ορίσουμε το **σύνολο εκκίνησης** S(P) και το **σύνολο τερματισμού** F(P):

$$\mathrm{S(P)} = \{\ i \mid P = \sigma_i P' \text{ για κάποια } \mathrm{P}' \in B_n^+\ \}$$
$$\mathrm{F(P)} = \{\ i \mid P = P'\,\sigma_i \text{ για κάποια } \mathrm{P}' \in B_n^+\ \}$$

Το σύνολο εκκίνησης είναι οι δείκτες των γεννητόρων οι οποίοι μπορούν να ξεκινήσουν μία παρουσίαση της P. Αντίστοιχα ορίζεται το σύνολο τερματισμού. Για παράδειγμα, $\mathrm{S}(\Delta_n) = \mathrm{F}(\Delta_n) = \{1, ..., \text{n-1}\}$.

Ορισμός 2.15. *Μία αριστερή αποσύνθεση της θετικά πλεξίδας $A \in B_n^+$ σε μία ακολουθία πλεξίδων μεταθέσεων είναι:*

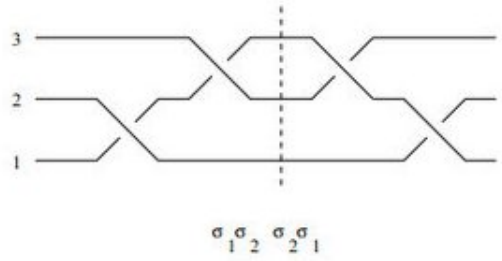
$$A = P_1 P_2 ... P_k$$

όπου τα P_i είναι πλεξίδες μεταθέσεων, και $S(P_{i+1}) \subset F(P_i)$.

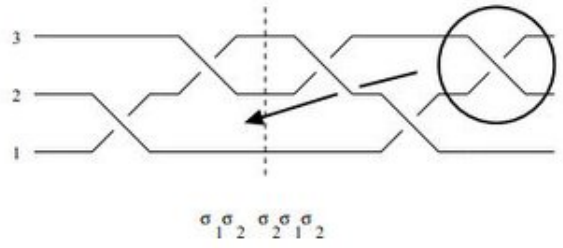
□

Οποιαδήποτε προσθήκη σε έναν γεννήτορα από την P_{i+1} στην P_i θα μετατρέψει την P_i σε πλεξίδα η οποία όμως δεν είναι πλεξίδα μετάθεσης.

Παράδειγμα 2.16. *Η ακόλουθη πλεξίδα είναι αριστερής αποσύνθεσης:*



Η ακόλουθη πλεξίδα δεν είναι αριστερής αποσύνθεσης, λόγω της κυκλωμένης διασταύρωσης που μπορεί να μετακινηθεί στην πρώτη πλεξίδα μετάθεσης:



□

Τώρα, παρουσιάζεται με την αλγεβρική μορφή:

$$\sigma_1\sigma_2 \cdot \sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2 \cdot \sigma_1\sigma_2\sigma_1 = \sigma_1\sigma_2\sigma_2 \cdot \sigma_2\sigma_1$$

Το ακόλουθο θεώρημα παρουσίαζει την **μορφή του Garside** ή *αριστερή κανονική μορφή* και δηλώνει την μοναδικότητά της:

Θεώρημα 2.17. *Κανονική μορφή του Garside. Για κάθε πλεξίδα $w \in B_n$, υπάρχει μία μοναδική μορφή-παρουσίαση:*

$$w = \Delta_n^r P_1 P_2 ... P_k$$

όπου $r \in \mathbb{Z}$ είναι το ανώτατο όριο, P_i είναι οι πλεξίδες μεταθέσεων, $P_k \neq \varepsilon$ και $P_1P_2...P_k$ είναι μία αριστερή αποσύνθεση.

□

Για να μετατρέψουμε μία δοσμένη πλεξίδα w στην κανονική μορφή της (κανονική μορφή του Garside), πρέπει να εκτελέσουμε τα παρακάτω βήματα:

1. Για οποιαδήποτε αρνητική δύναμη κάποιου γεννήτορα, αντικαθιστούμε την σ_i^{-1} με $\Delta_n^{-1}B_i$, όπου B_i είναι μία πλεξίδα μεταθέσεων.

2. Μετακινούμε οποιαδήποτε εμφάνιση της Δ_n στα αριστερά, χρησιμοποιώντας την σχέση: $\Delta_n^{-1}\sigma_i\Delta_n = \tau(\sigma_i) = \sigma_{n-i}$. Έτσι, παίρνουμε w = $\Delta_n^r A$, όπου η A είναι θετική πλεξίδα.

3. Γράφουμε την A ως αριστερή αποσύνθεση πλεξίδων μεταθέσεων. Ο τρόπος για να το κάνουμε αυτό είναι: Παίρνουμε την A και την σπάμε σε πλεξίδες μεταθέσεων, δηλαδή παίρνουμε τις μακρύτερες πιθανές ακολουθίες γεννητόρων, που είναι ακόμα πλεξίδες μεταθέσεων. Έτσι παίρνουμε: A = $Q_1Q_2...Q_j$, όπου κάθε Q_i είναι μία πλεξίδα μετάθεσης. Για κάθε i, υπολογίζουμε το σύνολο τερματισμού F(Q_i) και το σύνολο εκκίνησης S(Q_{i+1}). Στην περίπτωση που το σύνολο εκκίνησης δεν περιέχεται στο σύνολο τερματισμού, παίρνουμε ένα γεννήτορα $\sigma_i \in S(Q_{i+1})\backslash F(Q_i)$ και χρησιμοποιώντας τις σχέσεις της ομάδας πλεξίδων τον μετακινούμε από το Q_{i+1} στο Q_i. Τότε παίρνουμε την αποσύνθεση A = $Q_1Q_2...Q_i'$ Q_{i+1}' $...Q_j$. Συνεχίζουμε την διαδικασία έως ότου έχουμε S(Q_{i+1}) $\subseteq$ F(Q_i) για κάθε i. Τότε έχουμε μία αριστερή αποσύνθεση, όπως χρειαζόμασταν.

Παράδειγμα 2.18. *Ας παρουσίασουμε την ομάδα πλεξίδας $w = \sigma_1\sigma_3^{-1}\sigma_2 \in B_4$. Θέλουμε να την φέρουμε στην κανονική Garside μορφή της.*

Αρχικά θα πρέπει να αντικαταστήσουμε το σ_3^{-1} με το $\Delta_4^{-1}\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2$, έτσι ώστε να πάρουμε:

$$w = \sigma_1 \cdot \Delta_4^{-1}\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2 \cdot \sigma_2$$

Τώρα, μεταφέρουμε την Δ_4 *στα αριστερά:*

$$w = \Delta_4^{-1}\sigma_3\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2\sigma_2$$

Αποσυνθέτοντας το θετικό μέρος σε μία αριστερή αποσύνθεση έχουμε:

$$w = \Delta_4^{-1} \cdot \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2$$

□

Η πολυπλοκότητα της μετατροπής μίας λέξης στην κανονική Garside μορφή της με σεβασμό στην παρουσίαση-μορφή του Artin είναι O($\mid W \mid^2 nlogn$), όπου $\mid W \mid$ είναι το μήκος της λέξης στην B_n.

Με αντίστοιχο τρόπο ορίζουμε την δεξιά κανονική μορφή. Μία *δεξιά αποσύνθεση* μίας θετικής πλεξίδας $A \in B_n^+$ σε μία ακολουθία πλεξίδων μεταθέσεων είναι:

$$A = P_k...P_2P_1$$

όπου P_i είναι πλεξίδες μεταθέσεων και $F(Q_{i+1})\ S(Q_i)$. Οποιαδήποτε προσθήκη σε έναν γεννήτορα από την P_{i+1} στην P_i θα μετατρέψει την P_i σε πλεξίδα, η οποία όμως δεν είναι πλεξίδα μετάθεσης.

Στην συνέχεια ακολουθεί το θεώρημα της δεξιάς κανονικής μορφής και της μοναδικότητας:

Θεώρημα 2.19. *Για κάθε πλεξίδα* $w \in B_n$*, υπάρχει μία μοναδική μορφή-παρουσίαση:*

$$w = P_k....P_2P_1\Delta_n^r$$

όπου $r \in \mathbb{Z}$ *είναι το ανώτατο όριο,* P_i *είναι οι πλεξίδες μεταθέσεων και* $P_k...P_2P_1$ *είναι μία δεξιά αποσύνθεση.*

□

Τώρα ορίζουμε το infimum και το supremum μίας πλεξίδας w:

Για w $\in B_n$, θέτουμε inf(w) = max $\{r : \Delta_n^r \preceq w\}$ και sup(w) = min $\{s : w \preceq \Delta_n^s\}$

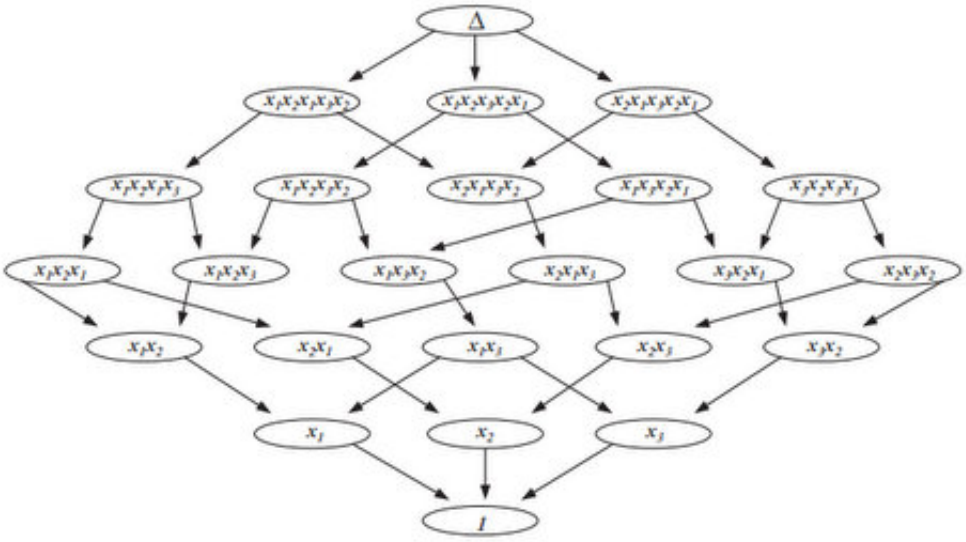
Παρατηρούμε ότι εάν w $= \Delta_n^m P_1 P_2 .. P_k$ είναι η κανονική Garside μορφή της w, τότε inf(w) = m, sup(w) = m+k.

Ένας άλλος τρόπος μελέτης της κανονικής Garside μορφής είναι:

Υπάρχουν δύο ειδικές απλές πλεξίδες του B_n: η τετριμμένη πλεξίδα που είναι το μικρότερο στοιχείο του S και η ημι-ανεστραμμένη πλεξίδα $\Delta = \xi_{(n,n-1,...,2,1)}$, η οποία είναι το μεγαλύτερο στοιχείο του S. Το σύνολο των απλών πλεξίδων της τάξης $<$ από αυτήν που ορίστηκε παραπάνω, έχει τη δομή πλέγματος με ΜΚΔ (gcd) και ΕΚΠ (lcm) που ορίζονται ως εξής:

$$\text{ΜΚΔ}(\xi_s, \xi_t) = \gcd(\xi_s, \xi_t) = \max\{\xi_r \mid \xi_r < \xi_s \text{ και } \xi_r < \xi_t\}$$
$$\text{ΕΚΠ}(\xi_s, \xi_t) = \text{lcm}(\xi_s, \xi_t) = \min\{\xi_r \mid \xi_s < \xi_r \text{ και } \xi_t < \xi_r\}$$

Παρατηρούμε ότι αφού το S περιέχει και το ελαχιστικό στοιχείο και μεγιστικό οι gcd και lcm είναι καλά ορισμένες.



Απλά στοιχεία της B_4.

Ορισμός 2.20. ***Η αριστερή κανονική μορφή μίας πλεξίδας*** *$a \in B_n$ του Garside είναι ένα ζευγάρι $(p,(s_1,...,s_l))$, όπου $p \in \mathbb{Z}$ και $s_1,...,s_l$ μία ακολουθία μεταθέσεων στο $S_n - \{1,\Delta\}$ που ικανοποιεί την παρακάτω ιδιότητα: για κάθε i = 1,...,l-1,*

$$\xi_1 = gcd(\xi_{s_i^{-1}\Delta}, \xi_{s_{i+1}})$$

□

Η κανονική μορφή (p, $(s_1, ..., s_l)$), αναπαριστά το παρακάτω στοιχείο της B_n:

$$\xi_{\Delta}^{p} \cdot \xi_{s_1} \cdot ... \cdot \xi_{s_n}$$

Παρατήρηση 2.21. *Εκτίμηση Πολυπλοκότητας.*
Υπάρχει ένας αλγόριθμος που για οποιαδήποτε λέξη πλεξίδας $w = w(x_1, ...x_{n-1})$ υπολογίζει την κανονική μορφή της αντίστοιχης πλεξίδας. Επιπλέον, η χρονική πολυπλοκότητα του αλγορίθμου είναι $O(n^2 \mid w \mid^2)$.

□

2.2 Ομάδα Thompson

Όταν κάποια κρυπτογραφικά συστήματα που βασίζονταν σε ομάδες πλεξίδες δέχτηκαν επίθεση, ήταν φυσικό οι μελετητές να ψάξουν για διαφορετικές ομάδες, με την ελπίδα ότι ένα παρόμοιο κρυπτογραφικό σύστημα με διαφορετική ομάδα θα είναι πιο ασφαλές και πιο επιτυχημένο. Η ομάδα Thompson ήταν μία φυσική υποψήφια για την θέση της ζητούμενης ομάδας: υπάρχει μία κανονική μορφή που μπορεί να υπολογιστεί εύκολα, αλλά το Πρόβλημα Αποσύνθεσης φαίνεται δύσκολο. Πάνω σε αυτή τη βάση οι Shpilrain και Ushakov πρότειναν ένα κρυπτογραφικό σύστημα.

Η ομάδα Thompson F είναι γνωστή σε πολλούς τομείς των μαθηματικων, συμπεριλαμβανομένων της άλγεβρας, της γεωμετρίας και της ανάλυσης. Η ομάδα είναι άπειρη μη-αβελιανή. Για εμάς, είναι σημαντικό ότι η ομάδα Thompson F έχει την ακόλουθη πολύ όμορφη αναπαράσταση:

$$\mathrm{F} = \langle x_0, x_1, x_2, ... \mid x_i^{-1} x_k x_i = x_{k+1} \text{ (k>i)} \rangle$$

Αυτή η αναπαράσταση είναι άπειρη. Ακόμη, υπάρχουν πεπερασμένες αναπαραστάσεις αυτής της ομάδας. Για παράδειγμα:

$$\mathrm{F} = \langle x_0, x_1, x_2, x_3, x_4 \mid x_i^{-1} x_k x_i = x_{k+1} \text{ (k>i , k<4)} \rangle$$

Όμως, η άπειρη αναπαράσταση πιο πάνω επιτρέπει μια κατάλληλη κανονική μορφή, οπότε εδώ θα χρησιμοποιήσουμε αυτή. Η κλασική κανονική μορφή για ένα στοιχείο της ομάδας Thompson είναι μια λέξη της μορφής:

$$x_{i_1}, ...x_i, x_{j_t}^{-1}, ..., x_{j_1}^{-1}$$

η οποία ικανοποεί τις επόμενες δύο συνθήκες:

(NF1) $i_1 \leq ... \leq i_s$ και $j_1 \leq ... \leq j_t$.

(NF2) Εάν συμβαίνουν και το x_i και το x_i^{-1}, τότε συμβαίνει επίσης είτε το x_{i+1} είτε το x_{i+1}^{-1}.

Ορισμός 2.22. *Ημικανονική μορφή.*

Λέμε ότι η λέξη w είναι σε ***ημικανονική μορφή****, αν έχει την κλασσική κανονική μορφή της ομάδας Thompson και ικανοποιεί την συνθήκη (NF1).*

□

Έχουμε αναφέρει ότι η κανονική μορφή μιας δεδομένης λέξης w στην ομάδα Thompson F μπορεί να υπολογιστεί σε χρόνο O($\mid w \mid \log \mid w \mid$).

Ένα άλλο πλεονέκτημα των πρωτοκόλλων που βασίζονται σε συμβολικούς υπολογισμούς, έναντι σε αυτούς που βασίζονται σε υπολογισμούς με αριθμούς, είναι η πιθανότητα να παράγεις μία τυχαία λέξη με ένα σύμβολο την φορά. Για παράδειγμα, στον RSA, κάποιος χρησιμοποιεί τυχαίους πρώτους αριθμούς που προφανώς δεν μπορουν να δημιουργηθούν με ένα ψηφίο την φορά.

Το Πρωτόκολλο

Έστω F είναι μία ομάδα Thompson, που δίνεται από την συνηθισμένη άπειρη μορφή και ακόμα s $\in \mathbb{R}$ ένας θετικός ακέραιος. Ορίζουμε τα σύνολα A_s και B_s παρακάτω. Το σύνολο A_s αποτελείται από στοιχεία που η κανονική μορφή τους έχει την εξής μορφή:

$$x_{i_1}...x_{i_m}x_{j_m}^{-1}...x_{j_1}^{-1}$$

τα θετικά και αρνητικά μέρη έχουν το ίδιο μήκος m, και

$$i_k \text{ - k} < \text{s και } j_k \text{ - k} < \text{s για κάθε k} = 1,....,\text{s (3)}$$

Το σύνολο B_s αποτελείται από στοιχεία που αναπαριστάνται από λέξεις με γεννήτορες $x_{s+1}, x_{s+2}, ...$ Προφάνως, B_s είναι υποομάδα της F.

Πρόταση 2.23. *Έστω $a \in A_s$ και $b \in B_s$. Τότε στην ομάδα F ισχύει $ab = ba$.*

Απόδειξη: Έστω α = $x_{i_1}...x_{i_m}x_{j_m}^{-1}...x_{j_1}^{-1}$ και b = $x_{k_1}^{\epsilon_1}...x_{k_l}^{\epsilon_l}$, όπου $k_q >$ s για κάθε q = 1,...,l. Με επαγωγή στο l και m είναι εύκολο να δείξουμε ότι στην ομάδα F ισχύει:

$$\text{b} = \text{b} = x_{i_1}...x_{i_m}\delta_m(b)x_{j_m}^{-1}...x_{j_1}^{-1}$$

όπου δ_M είναι χειριστής που αυξάνει τους δείκτες όλων των γεννητόρων του M. Οπότε αποδείχθηκε. Βλ[12]

□

Πρόταση 2.24. *Έστω $s \geq 2$ ένας ακέραιος. Το σύνολο A_s είναι υποομάδα της F που παράγεται από $x_0x_1^{-1}, ..., x_0x_s^{-1}$.*

Απόδειξη: Το σύνολο A_s περίεχει την ταυτότητα και ισχύει ότι $A_s = A_s^{-1}$. Για να δείξουμε ότι το A_s είναι κλειστό ως προς τον πολλαπλασίασμο, παίρνουμε δύο τυχαίες κανονικές μορφές της A_s:

$$\text{u} = x_{i_1}...x_{i_m}x_{j_m}^{-1}...x_{j_1}^{-1}$$

και

$$\text{v} = x_{p_1}...x_{p_l}x_{q_l}^{-1}...x_{q_1}^{-1}$$

και δείχνουμε ότι η κανονική μορφή uv ανήκει στην A_s. Πρώτα, σημειώνουμε ότι εφόσον το πλήθος των αρνητικών και θετικών αριθμών στο uv είναι το ίδιο, τα μήκη των θετικών και αρνητικών αριθμών στην κανονική μορφή της uv είναι επίσης τα ίδια. Έτσι, μας απομένει να δείξουμε ότι η συνθήκη (3) των δεικτών στην κανονική μορφή της uv ικανοποιείται. Στην συνέχεια, σκιαγραφούμε την απόδειξη της ιδιότητας.

Θεωρούμε ότι η υπο-λέξη στην μέση του γινομένου uv γράφεται ως εξής:

$$\text{uv} = x_{i_1}...x_{i_m}(x_{j_m}^{-1}...x_{j_i}^{-1}x_{p_1}...x_{p_l})x_{q_l}^{-1}...x_{q_1}^{-1}$$

και βρίσκουμε μία ημικανονική μορφή για αυτό, χρησιμοποιώντας τις σχέσεις της F (περισσότερα θετικά γράμματα στα αριστερά και αρνητικά γράμματα στα δεξιά ξεκινώντας από την μέση της υπο-λέξης). Δηλώνουμε την αποκτημένη λέξη με w. Η λέξη w είναι το γινόμενο μίας αρνητικής και μίας θετικής λέξης: w = pn. Με επαγωγή στο l+m κάποιος μπορεί να δείξει ότι και το p και το n ικανοποιούν την συνθήκη (3).

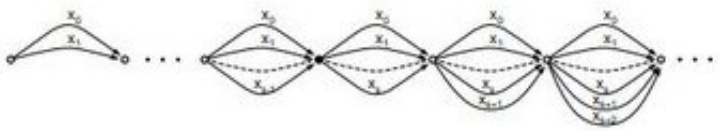
Στην συνέχεια, βρίσκουμε κανονικές μορφές για τις λέξεις p και n χρησιμοποιώντας τις σχέσεις της F (για την p μετακινούμε τα γράμματα με τους μικρότερους δείκτες στα δεξιά των γραμμάτων με μεγαλύτερους δείκτες). Με επαγωγή στο πλήθος των

χειριστών που εκτελούνται, κάποιος μπορεί να δείξει ότι οι αποκτημένες λέξεις p′ και n′ ικανοποιούν την συνθήκη (3). Για αυτόν τον λόγο, η λέξη w′ = p′n′ είναι μία ημικανονική μορφή της λέξης uv που ικανοποιεί την συνθήκη (3).

Τέλος, αφαιρούμε εκείνα τα ζευγάρια των γεννητόρων, στην w′, που έρχονται σε αντίθεση με την ιδιότητα (NF2). Επίσης, με επαγωγή στο πλήθος των ζευγαριών αυτών, κάποιος μπορεί να δείξει ότι το αποτέλεσμα θα ικανοποιεί την συνθήκη (3). Γι′ αυτόν το λόγο η uv ανήκει στην A_s, η A_s είναι κλειστή ως προς τον πολλαπλασιασμό και έτσι η A_s είναι υποομάδα.

Τώρα θα δείξουμε ότι το σύνολο των λέξεων $\{x_0x_1^{-1}, ..., x_0x_s^{-1}\}$ παράγει την υποομάδα A_s. Τα στοιχεία $\{x_0x_1^{-1}, ..., x_0x_s^{-1}\}$ προφανώς ανήκουν στην A_s. Για να δείξουμε ότι $A_s \leq \langle x_0x_1^{-1}, ..., x_0x_s^{-1}\rangle$, κατασκευάζουμε το γράφημα του Schreier των $\langle x_0x_1^{-1}, ..., x_0x_s^{-1}\rangle$ και βλέπουμε ότι οποιαδήποτε λέξη της A_s ανήκει στην υποομάδα στα δεξιά.

□



Το γράφημα του Schreier της υποομάδας $H = \langle x_0x_1^{-1}, ..., x_0x_s^{-1}\rangle$. Η μάυρη τελεία συμβολίζει το αντίστοιχο αριστερό σύμπλοκο της H.

Παράμετροι και δημιουργία κλειδιού

Στην πρακτική ανταλλαγή κλειδιών προτείνουμε να επιλεγεί μία από τις παρακάτω παραμέτρους. Βλ[12]

(1) Επιλέγουμε (τυχαία και ανεπίσημα) την παράμετρο s από το διάστημα [3,8] και την παράμετρο M από το σύνολο $\{256, 258, ..., 318, 320\}$.

(2) Επιλέγουμε την λέξη-βάση w ως ένα γινόμενο των γεννητόρων

$$S_W = \{x_0, x_1, ..., x_{s+2}\}$$

και των αντιστρόφων τους. Αυτό γίνεται ως εξής: Ξεκινάμε με την κενή λέξη v_0. Όταν έχουμε μία τρέχουσα λέξη v_i, την πολλαπλασιάζουμε από δεξιά με ένα γεννήτορα από το $S_B^{\pm 1}$ και υπολογίζουμε την κανονική μορφή του γινομένου. Η λέξη που αποκτάμε την συμβολίζουμε ως v_{i+1}. Συνεχίζουμε την διαδικασία μέχρι η αποκτημένη λέξη v_{i+1} να έχει μήκος M.

(3) Επιλέγουμε a_1 και a_2 ως γινόμενα λέξεων από την

$$S_A = \{x_0 x_1^{-1}, ..., x_0 x_s^{-1}\}$$

και των αντιστρόφων τους. Αυτό γίνεται ομοίως, όπως κάναμε παραπάνω για την w. Ξεκινάμε με την κενή λέξη u_0. Έστω u_i να είναι η τρέχουσα κατασκευασμένη λέξη μήκους μικρότερου του M. Πολλαπλασιάζουμε την u_i από δεξιά με μία τυχαία επιλεγμένη λέξη από την $S_A^{\pm 1}$ και υπολογίζουμε την κανονική μορφή του γινομένου. Συμβολίζουμε την αποκτημένη κανονική μορφή με u_{i+1}. Συνεχίζουμε την διαδικασία μέχρι η αποκτημένη λέξη u_{i+1} να έχει μήκος M.

(4) Επιλέγουμε b_1 και b_2 ως γινόμενα λέξεων από την

$$S_B = \{x_{s+1}, x_{s+2}, ..., x_{2s}\}$$

και των αντιστρόφων τους. Αυτό γίνεται όμοια, όπως κάναμε παραπάνω για την w. Ξεκινάμε με την κενή λέξη v_0. Έστω v_i η τρέχουσα κατασκευασμένη λέξη μήκους μικρότερου του M. Πολλαπλασιάζουμε την v_i από δεξιά με μία τυχαία επιλεγμένη λέξη απο την $S_B^{\pm 1}$ και υπολογίζουμε την κανονική μορφή του γινομένου. Συμβολίζουμε την αποκτημένη κανονική μορφή με v_{i+1}. Συνεχίζουμε την διαδικασία μέχρι η αποκτημένη λέξη v_{i+1} να έχει μήκος M.

□

Σε αυτό το σημείο, οφείλουμε να τονίσουμε ότι $\mid A_s(M) \mid \geq \sqrt{2}^M$.

Οι παράμετροι παραπάνω επιλέχθηκαν, έτσι ώστε να αποτρέχουν την επίθεση μήκους. Σημειώνουμε ότι για την ομάδα Thompson μία επίθεση μήκους μπορεί να είναι απειλή. Εφόσον οι ιδέες πίσω από τις επιθέσεις μήκους δεν αναλύονται σχεδόν ποτέ, παρακάτω παρουσιάζουμε έναν τυπικό αλγόριθμο που εκτελεί μία τέτοια επίθεση (*Αλγόριθμος 1*).

Ορίζουμε ένα κατευθυνόμενο επισημασμένο γράφημα $\Gamma = (\mathrm{V}(\Gamma), \mathrm{E}(\Gamma))$ ως εξής:

- Το σύνολο των κορυφών $\mathrm{V}(\Gamma)$ αντιστοιχεί στο σύνολο όλων των στοιχείων της ομάδας F.
- Το σύνολο των ακμών $\mathrm{E}(\Gamma)$ περιέχει ακμές $v_1 \overset{(w_1,w_2)}{\longrightarrow} v_2$, έτσι ώστε $v_2 = w_1 v_1 w_2$ στην ομάδα F, με δύο ειδών επιγραφές:

1. $(w_1,1)$, όπου $w_1 \in S_A^{\pm 1}$.
2. $(1,w_2)$, όπου $w_2 \in S_B^{\pm 1}$.

Για ένα στοιχείο w ∈ F συμβολίζουμε με Γ_w την συνδεδεμένη συνιστώσα του Γ που περιέχει το w. Από την περιγραφή του πρωτοκόλλου έπεται ότι το w και το στοιχείο $w' = a_1 w b_1$ που μεταδίδεται από την Μαριέττα στον Μάρκο ανήκουν στο $\Gamma_w = \Gamma_{\acute{w}}$. Το σπάσιμο του κλειδιού της Μαριέττας είναι ισοδύναμο με την εύρεση μίας ετικέτας ενός μονοπατιού από το w στο w′ στο Γ_w.

Για να δοκιμάσουμε το πρωτόκολλο, εκτελούμε μία σειρά πειραμάτων. Παράγουμε τυχαία κλειδιά (όπως περιγράψαμε παραπάνω) και τρέχουμε τον *Αλγόριθμο 1* για αυτά τα κλειδιά, ο οποίος παρουσιάζεται παρακάτω. Ο *Αλγόριθμος 1* συνεχίζει να κατασκευάζει Γ_w και $\Gamma_{\acute{w}}$ μέχρι να βρεθεί ένα κοινό στοιχείο. Τα σύνολα $S_w = S_{\acute{w}}$ στον αλγόριθμο συσσωρεύουν κατασκευασμένα μέρη των γραφημάτων Γ_w και $\Gamma_{\acute{w}}$. Τα σύνολα $M_w \subset S_w$ και $M_{\acute{w}} \subset S_{\acute{w}}$ ονομάζονται τα σύνολα των μαρκαρισμένων κορυφών και χρησιμοποιούνται για να ξεχωρίσει κορυφές που έχουν εκπονηθεί.

Αλγόριθμος 1 (Επίθεση μήκους)
INPUT. Η γνήσια δημόσια λέξη w και η λέξη w′ που μεταδίδονται από την Μαριέττα.
OUTPUT. Ένα ζευγάρι των λέξεων $x_1 \in S_A, x_2 \in S_B$ τέτοια ώστε $w' = x_1 w x_2$.
ΕΚΚΙΝΗΣΗ. Θέτουμε $S_w = \{w\}$, $S_{\acute{w}} = \{\acute{w}\}$, $M_w = \emptyset$, $M_{\acute{w}} = \emptyset$.
ΥΠΟΛΟΓΙΣΜΟΙ.

Α. Βρίσκουμε μία συντομότερη λέξη u ∈ $S_w \setminus M_w$.

Β. Πολλαπλασιάζουμε την u με τα στοιχεία $S_A^{\pm 1}$ από αριστερά και με τα στοιχεία $S_B^{\pm 1}$ από δεξιά και προσθέτουμε κάθε αποτέλεσμα στο S_w με τις άκρες μαρκαρισμένες αντίστοιχα.

Γ. Προσθέτουμε το u στο M_w.

Δ. Εκτελούμε τα βήματα Α-Γ, με τα $S_{\acute{w}}$ και $M_{\acute{w}}$ να αντικαταστούν τα S_w και M_w, αντίστοιχα.

Ε. Εάν $S_w \cap S_{\acute{w}} = \emptyset$, τότε πάμε στο βήμα Α.

ΣΤ. Εάν υπάρχει $\bar{w} \in S_w \cap S_{\acute{w}}$ τότε βρίσκουμε μία διαδρομή στο S_w από το w στο $\bar{w}$ και μία διαδρομή στο $S_{\acute{w}}$ από το $\bar{w}$ στο w′. Ενώνουμε αυτά τα δύο και παίρνουμε την επιγραφή του αποτελέσματος.

Εκτελούμε μία σειρά δοκιμών αυτής της επίθεσης μήκους, σε κάθε δοκιμή αφήνουμε το πρόγραμμα να τρέξει, μπορεί και όλη νύχτα. Κανένα πρόγραμμα δεν έχει αποτέλεσμα, δηλαδή η τάξη επιτυχίας της επίθεσης μήκους στις δοκιμές μας είναι 0.

Θέτουμε $\rho(\mathrm{w})$ την κανονική μορφή της $\mathrm{w} \in \mathrm{F}$. Αυτή είναι μοναδική για κάθε στοιχείο της F. Θυμόμαστε ότι μία λέξη w έχει ημικανονική μορφή, εάν έχει την κλασική κανονική μορφή της ομάδας Thompson και ικανοποιεί την συνθήκη (NF1). Η ημικανονική μορφή δεν είναι μοναδική. Ως συνήθως, για μία λέξη w στο αλφάβητο X συμβολίζουμε με $\bar{w}$ την αντίστοιχα ελεύθερα μειωμένη λέξη.

Όπως αναφέραμε παραπάνω, η κανονική μορφή ενός στοιχείου της ομάδας Thompson μπορεί να υπολογιστεί σε δύο βήματα:

1. Υπολογίζουμε την ημικανονική μορφή.

2. Αφαιρούμε εκείνα τα ζευγάρια των γεννητόρων στην w′ που έρχονται σε αντίθεση με την ιδιότητα (NF2).

Το πρώτο ζευγάρι μπορούμε να το βρούμε (Λήμμα 1) χρησιμοποιώντας το ακόλουθο σύστημα επαναγραφής (για όλα τα ζευγάρια (i,k) τέτοια ώστε i<k) :

$$x_k x_i \to x_i x_{k+1}$$

$$x_k^{-1} x_i \to x_i x_{k+1}^{-1}$$

$$x_i^{-1} x_k \to x_{k+1} x_i^{-1}$$

$$x_i^{-1} x_k^{-1} \to x_{k+1}^{-1} x_i^{-1}$$

Επιπλέον, για όλα τα $\mathrm{i} \in \mathbb{N}$

$$x_i^{-1} x_i \to 1$$

Συμβολίζουμε το σύστημα κανόνων με το $\Re$. Το επόμενο Λήμμα είναι προφανές.

Λήμμα 2.25. *Το $\Re$ τελειώνει με μία ημικανονική μορφή. Επιπλέον, μία λέξη είναι σε ημικανονική μορφή, αν και μόνο αν είναι $\Re$-μειωμένη.*

□

Ας μελετήσουμε πιο προσεκτικά το $\Re$. Αυτό είναι παρόμοιο με το να διαλέξουμε μία λίστα αριθμών, αλλά με δύο διαφορές: οι δείκτες των γεννητόρων μπορεί να αυξηθούν, και κάποιοι γεννήτορες μπορεί να εξαφανιστούν.

Σύμφωνα με το Λήμμα 1, για μία οποιαδήποτε λέξη w με γεννήτορες της F, το τελικό αποτέλεσμα των επαναγραφών μέσω του $\Re$ είναι μία ημικανονική μορφή. Για αυτό τον λόγο, για να υπολογίσουμε μία ημικανονική μορφή, εκτελούμε επαναγραφές μεσω του $\Re$. Αυτό επιτυγχάνεται με έναν ειδικό τρόπο στον Αλγόριθμο 3, έτσι ώστε να εξασφαλίζεται η καλύτερη απόδοση. Για μεγαλύτερη ευκολία, παρουσιάζουμε την παραμετρική συνάρτηση $\delta_\epsilon, \epsilon \in \mathbb{Z}$ που ορίζεται στο σύνολο όλων των λέξεων από το αλφάβητο $\{x_0^{\pm 1}, x_1^{\pm 1}, ...\}$ με:

$$x_i^{\pm 1} \overset{\delta_\epsilon}{\mapsto} x_{i+\epsilon}^{\pm 1}.$$

Η συνάρτηση μπορεί να μην οριστεί για κάποια αρνητικά ϵ σε κάποια δοσμένη λέξη w $= \mathrm{w}(x_{i_1}^{\pm 1}, x_{i_2}^{\pm 1}, ...,$ αλλά όταν χρησιμοποιείται, υποθέτουμε ότι η συνάρτηση δεν ορίζεται.

Συγχώνευση Ημικανονικών Μορφών

Θεωρούμε πρώτα την περίπτωση όπου η λέξη w είναι γινόμενο των w_1 και w_2 που δίνονται σε ημικανονική μορφή. Έστω $w_1 = p_1 n_1$ και $w_2 = p_2 n_2$, όπου p_i, n_i (i = 1, 2) είναι τα θετικά και τα αρνητικά μέρη του w_i. Είναι φανερό ότι κάποιος μπορεί να κανονίσει την διαδικασία επανάγραψης για τα $p_1 n_1 p_2 n_2 \in \Re$ με τον εξής τρόπο:

1. Ξαναγράγουμε την υπο-λέξη $n_1 p_1$ της w σε μία ημικανονική μορφή $\acute{p_2}\acute{n_1}$. Συμβολίζουμε με $\mathrm{w}' = p_1 \acute{p_2} \acute{n_1} n_2$ το αποτέλεσμα.

2. Ξαναγράγουμε την θετική υπο-λέξη $p_1 \acute{p_2}$ της w′ σε μία ημικανονική μορφή p. Συμβολίζουμε με $\mathrm{w}'' = \mathrm{p}\acute{n_1} n_2$ το αποτέλεσμα.

3. Ξαναγράγουμε την αρνητική υπο-λέξη $\acute{n_1} n_2$ της w′ σε μία ημικανονική μορφή n. Συμβολίζουμε με $\mathrm{w}''' = \mathrm{pn}$ το αποτέλεσμα.

Η λέξη $\mathrm{w}''' = \mathrm{pn}$ είναι φανερό ότι είναι σε ημικανονική μορφή και $\mathrm{w} =_F \mathrm{w}'''$. Αυτή η διαδικασία μπορεί να απεικονιστεί ως εξής:

$$p_1 \underbrace{n_1 p_2} n_2$$

$$\Downarrow$$

$$\underbrace{p_1 p_2'}\ \underbrace{n_1' n_2}$$

$$\Downarrow$$

pn

Ο επόμενος αλγόριθμος εκτελεί το πρώτο βήμα επαναγραφής από το παραπάνω σχήμα και με το ακόλουθο Λήμμα μπορούμε να ισχυριστούμε ότι εκτελεί σωστά το πρώτο βήμα σε γραμμικό χρόνο.

Αλγόριθμος 2 (Ημικανονική μορφή γινομένου μίας θετικής και μίας αρνητικής ημικανονικής μορφής)

SIGNATURE. w = Merge$_{-,+}$(n, p, ϵ_1, ϵ_2).

INPUT. Οι ημικανονικές μορφές n και p (όπου n = $x_{j_t}^{-1}...x_{j_1}^{-1}$ και p = $x_{i_1}...x_{i_s}$ και οι αριθμοί $\epsilon_1, \epsilon_2 \in \mathbb{Z}$.

OUTPUT. Η ημικανονική μορφή της w τέτοια ώστε w $=_F \delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p)$.

ΥΠΟΛΟΓΙΣΜΟΙ.

Α. Εάν s = 0 ή t = 0, τότε έχουμε αποτέλεσμα ένα γινόμενο np.

Β. Εάν $j_1 + \epsilon_1 = i_1 + \epsilon_2$, τότε:

1. Υπολογίζουμε w = Merge$_{-,+}(x_{j_t}^{-1}...x_{j_2}^{-1}, x_{i_2}, ..., x_{i_s}, \epsilon_1, \epsilon_2)$.
2. Αποτέλεσμα: w.

Γ. Εάν $j_1 + \epsilon_1 < i_1 + \epsilon_2$, τότε:

1. Υπολογίζουμε w = Merge$_{-,+}(x_{j_t}^{-1}...x_{j_2}^{-1}, x_{i_1}, ..., x_{i_s}, \epsilon_1, \epsilon_2 + 1)$.
2. Αποτέλεσμα: w$x_{j_1+\epsilon_1}^{-1}$.

Δ. Εάν $j_1 + \epsilon_1 > i_1 + \epsilon_2$, τότε:

1. Υπολογίζουμε w = Merge$_{-,+}(x_{j_t}^{-1}...x_{j_1}^{-1}, x_{i_2}, ..., x_{i_s}, \epsilon_1 + 1, \epsilon_2)$.
2. Αποτέλεσμα: $x_{i_1+\epsilon_2}$w.

Λήμμα 2.26. *Για οποιεσδήποτε κανονικές μορφές n και p (n = $x_{j_t}^{-1}...x_{j_1}^{-1}$ και p = $x_{i_1}...x_{i_s}$) και αριθμούς $\epsilon_1, \epsilon_2 \in \mathbb{Z}$, η έξοδος w = Merge$_{-,+}$(n, p, ϵ_1, ϵ_2) του Αλγόριθμου 2 είναι ημικανονική μορφή για $\delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p)$. Επιπλέον, ο χρόνος πολυπλοκότητας που απαιτείται, για να υπολογιστεί το w, είναι φραγμένος από το C(| n | + | p |) για κάποια σταθερά C.*

Απόδειξη. Εφόσον σε κάθε επανάληψη η σταθερά C εκτελεί στοιχειώδη βήματα και σε κάθε μετέπειτα επανάληψη το άθροισμα $\mid n \mid + \mid p \mid$ μειώνεται κατά ένα, τότε ο χρόνος πολυπλοκότητας του Αλγορίθμου 2 είναι γραμμικός.

Αποδεικνύουμε την ορθότητα του Αλγορίθμου 2 με επαγωγή στο $\mid n \mid + \mid p \mid$. Υποθέτουμε ότι $\mid n \mid + \mid p \mid = 0$. Τότε στο βήμα Α. παίρνουμε την έξοδο $\mathrm{w} = \mathrm{np}$, η οποία είναι μία κενή λέξη. Σαφώς, κάθε w είναι μία ημικανονική μορφή του np, οπότε θέσαμε την βάση της επαγωγής.

Υποθέτουμε ότι $\mid n \mid + \mid p \mid = \mathrm{N}+1$ και ότι για οποιαδήποτε λέξη μικρότερη αυτής ισχύει η βάση. Διακρίνουμε τέσσερις περιπτώσεις. Εάν $\mid n \mid = 0$ ή $\mid p \mid = 0$ τότε μία απο αυτές τις λέξεις είναι μηδαμινή και προφανώς το γινόμενο np είναι μία σωστή έξοδος για αυτή την περίπτωση. Εάν $j_1+\epsilon_1 = i_1+\epsilon_2$, τότε $x_{j_1+\epsilon_1}^{-1}x_{i_1+\epsilon_2}$ ακυρώνεται μέσα στο γινόμενο $\delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p)$. Άρα έχουμε τελειώσει με την υπόθεση της επαγωγής.

Εάν $j_1 + \epsilon_1 < i_1 + \epsilon_2$, τότε το $j_1 + \epsilon_1$ είναι το μικρότερο εύρημα (index) στην $\delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p)$ και για αυτό τον λόγο, χρησιμοποιώντας το $\Re$, η λέξη $\delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p)$ μπορεί να γραφτεί με τον ακόλουθο τρόπο:

$$\delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p) = x_{j_t+\epsilon_1}^{-1}...x_{j_2+\epsilon_1}^{-1}x_{j_1+\epsilon_1}^{-1}x_{i_1+\epsilon_1}...x_{i_s+\epsilon_2} \xrightarrow{\Re} x_{j_t+\epsilon_1}^{-1}...x_{j_2+\epsilon_1}^{-1}x_{i_1+\epsilon_1+1}...x_{i_s+\epsilon_2+1}x_{j_i+\epsilon_1}^{-1}$$

Σημειώνουμε ότι εφόσον $j_1 + \epsilon_1$ είναι το μικρότερο εύρημα (index) στην $\delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p)$, στην $\mathrm{w} = \mathrm{Merge}_{-,+}(x_{j_t}^{-1}...x_{j_2}^{-1}, x_{i_2}...x_{i_s}, \epsilon_1, \epsilon_2)$ δεν είναι μικρότερο από το $j_1+\epsilon_1$. Με την βάση της επαγωγής, το w είναι μία ημικανονική μορφή για το $\delta_{\epsilon_1}(x_{j_t}^{-1}...x_{j_2}^{-1})\delta_{\epsilon_2}(x_{i_2}...x_{i_s})$. Για αυτό τον λόγο $wx_{j_1+\epsilon_2+1}^{-1} =_F \delta_{\epsilon_1}(n)\delta_{\epsilon_2}(p)$ το οποίο είναι και μία ημικανονική μορφή.

Η τελευταία περίπτωση όπου $j_1 + \epsilon_1 > i_1 + \epsilon_2$, αντιμετωπίζεται αναλόγως.

□

Χρησιμοποιώντας ιδέες από τον Αλγόριθμο 2, κάποιος μπορεί εύκολα να εφαρμόσει έναν αλγόριθμο, για να συγχωνεύσει τις θετικές λέξεις και έναν άλλο για τις αρνητικές, έτσι ώστε προτάσεις, όπως το Λήμμα 2.24, να ισχύουν. Θα συμβολίζουμε αυτούς τους δύο αλγόριθμους με $\mathrm{Merge}_{-,-}(n_1, n_2, \epsilon_1, \epsilon_2)$ και $\mathrm{Merge}_{+,+}(p_1, p_2, \epsilon_1, \epsilon_2)$ αντίστοιχα. Επομένως, ο υπολογισμός της ημικανονικής μορφής ενός γινομένου δύο τυχαίων ημικανονικών μορφών έχει την παρακάτω μορφή.

Αλγόριθμος 3 (Ημικανονική μορφή ενός γινομένου ημικανονικών μορφών)
SIGNATURE. $\mathrm{w} = \mathrm{Merge}(w_1, w_2)$.
INPUT. Οι ημικανονικές μορφές w_1 και w_2.

OUTPUT. Η ημικανονική μορφή της w τέτοια ώστε w $=_F w_1 w_2$.
ΥΠΟΛΟΓΙΣΜΟΙ.

Α. Γράφουμε το w_i ως γινόμενο μίας θετικής και μίας αρνητικής λέξης ($w_1 = p_1 n_1$ και $w_2 = p_2 n_2$).

Β. Υπολογίζουμε $\mathrm{w}' = \mathrm{Merge}_{-,+}(n_1, p_2, 0, 0)$ και το γράφουμε ως γινόμενο μίας θετικής και μίας αρνητικής λέξης $\mathrm{w}' = p_2' n_1'$.

Γ. Υπολογίζουμε $\mathrm{w}'' = \mathrm{Merge}_{+,+}(p_1, p_2', 0, 0)$.

Δ. Υπολογίζουμε $\mathrm{w}''' = \mathrm{Merge}_{-,-}(n_1', n_2, 0, 0)$.

Ε. Έχουμε έξοδο $\mathrm{w}'' \mathrm{w}'''$.

Λήμμα 2.27. *Για ένα οποιοδήποτε ζευγάρι ημικανονικών μορφών w_1 και w_2 η λέξη $w = Merge(w_1, w_2)$ είναι μία ημικανονική μορφή του γινομένου $w_1 w_2$. Επιπλέον, ο χρόνος πολυπλοκότητας του υπολογισμού της w είναι φραγμένος από το $C(\mid n \mid + \mid p \mid)$ για κάποια σταθερά C.*

□

Υπολογισμός Ημικανονικής Μορφής

Αλγόριθμος 4 (Ημικανονική Μορφή)
SIGNATURE. u = ΗμικανονικήΜορφή(w).
INPUT. Μία λέξη w γραμμένη σε γεννήτορες της F.
OUTPUT. Μια ημικανονική μορφή u τέτοια ώστε u = w στην F.
ΥΠΟΛΟΓΙΣΜΟΙ.

Α. Εάν $\mid w \mid \leq 1$, τότε η έξοδος είναι w.

Β. Θέτουμε την w ως γινόμενο $w_1 w_2$, τέτοιο ώστε $\mid w_1 \mid - \mid w_2 \mid \leq 1$.

Γ. Αναδρομικά υπολογίζουμε $u_1 =$ ΗμικανονικήΜορφή(w_1) και $u_2 =$ ΗμικανονικήΜορφή(w_2).

Δ. Έστω u = Merge(u_1, u_2).

Ε. Έξοδος u.

Λήμμα 2.28. *Έστω w μία λέξη σε γεννήτορες της F. Η έξοδος του Αλγόριθμου 4 στην w είναι μία ημικανονική μορφή της w. Το πλήθος των λειτουργιών που απαιτούνται από τον Αλγόριθμο 4 να τερματίσει είναι O(C| w | log | w |), όπου η C είναι μία σταθερά ανεξάρτητη της w.*

Απόδειξη. Η πρώτη δήλωση μπορεί να αποδειχθεί με επαγωγή για το μήκος της w. Η βάση της επαγωγής σε αυτή την περίπτωση είναι, όταν $\mid w \mid = 1$. Σε αυτή την περίπτωση η w είναι ήδη σε ημικανονική μορφή και η έξοδος είναι σωστή. Το βήμα της επαγωγής αποδείχθηκε στο Λημμα 2.25.

Για να αποδείξουμε την δεύτερη δήλωση, συμβολίζουμε με T(n) το πλήθος των βημάτων που απαιτούνται απο τον Αλγόριθμο 4, για να τερματίσει σε ένα αποτέλεσμα του μήκους της n. Τότε προφανώς:

$$\mathrm{T(n)} = 2\mathrm{T}(\tfrac{n}{2}) + \mathrm{C}{\cdot}n,$$

όπου το τελευταίο $C \cdot n$ είναι η πολυπλοκότητα της συγχώνευσης δύο ημικανονικών μορφών με το άθροισμα των μηκών το πολύ $\mid n \mid$.

□

Υπολογισμός Κανονικής Μορφής

Το επόμενο Λήμμα δείχνει πως ένα ζευγάρι γεννητόρων που έρχεται σε αντίθεση με την ιδιότητα (NF2) μπορεί να αφαιρεθεί και πως όλα αυτά τα ζευγάρια μπορούν να βρεθούν.

Λήμμα 2.29. *Έστω $w = x_{i_1}...x_{i_s}x_{j_t}^{-1}...x_{j_1}^{-1}$ η ημικανονική μορφή και $(x_{i_a}, x_{i_b}^{-1})$ το ζευγάρι γεννητόρων στην w που έρχεται σε αντίθεση με την ιδιότητα (NF2), όπου a και b είναι τα μέγιστα με αυτή την ιδιότητα. Έστω*

$$w' = x_{i_1}...x_{i_{a-1}}\delta_{-1}(x_{i_{a+1}}...x_{i_s}x_{j_t}^{-1}...x_{j_b+1}^{-1})x_{j_b-1}^{-1}...x_{j_1}$$

Τότε το w′ είναι σε ημικανονική μορφή και ισχύει $w{=_F}w'$. Επιπλέον, εάν $(x_{i_c}, x_{j_d}^{-1})$ είναι το ζευγάρι γεννητόρων στην w′ που έρχονται σε αντίθεση με την ιδιότητα (NF2) (όπου a και b είναι τα μέγιστα με αυτή την ιδιότητα), τότε $c < a$ και $d < b$.

Απόδειξη. Από τον ορισμό της (NF2) και των ημικανονικών μορφών έπεται ότι όλοι οι δείκτες στο $x_{i_{a+1}}...x_{i_s}x_{j_t}^{-1}...x_{j_b+1}^{-1}$ είναι μεγαλύτεροι του $i_a + 1$ και για αυτό τον λόγο οι δείκτες στο $\delta_{-1}(x_{i_{a+1}}...x_{i_s}x_{j_t}^{-1}...x_{j_b+1}^{-1})$ είναι μεγαλύτεροι του i_a. Τώρα είναι φανερό

ότι η w′ είναι μία ημικανονική μορφή. Συνεπώς αν κάνουμε επαναγράφες αντίθετες των επαναγραφών στο $\Re$, παίρνουμε την λέξη w′ από την λέξη w. Άρα, w$=_F$ w′ .

Υπάρχουν δύο πιθανές περιπτώσεις: είτε c > a και d > b είτε c < a και d < b. Χρειάζεται να δείξουμε ότι η πρώτη περίπτωση είναι απίθανη. Υποθέτουμε c > a και d > b. Παρατηρούμε ότι εάν $(x_{i_a}, x_{i_b}^{-1})$ είναι ένα ζευγάρι γεννητόρων που έρχεται σε αντίθεση με την ιδιότητα (NF2), τότε το $(x_{i_a+\epsilon}, x_{i_b+\epsilon}^{-1})$ έρχεται σε αντίθεση με την ιδιότητα (NF2) στην $\delta_\epsilon(w)$. Επομένως, οι ανισότητες c > a και d > b έρχονται σε αντίθεση με την επιλογή των a και b.

□

Με την βοήθεια του Λήμματος 2.27 μπορούμε να ξεκινήσουμε την εύρεση των ζευγαριών που έρχονται σε αντίθεση με την ιδιότητα (NF2) σε ημικανονική μορφή αρχίζοντας από την μέση της λέξης. Ο επόμενος αλγόριθμος εκτελεί αυτή την ιδέα. Ο Αλγόριθμος έχει δύο μέρη. Το πρώτο μέρος βρίσκει όλα αυτά τα ζευγάρια ξεκινώντας από την μέση μίας δοσμένης w. Το δεύτερο μέρος εφαρμόζει το $\delta\epsilon$ στα τμήματα όπου απαιτείται.

Ένα αξιοσημείωτο χαρακτηριστικό του Αλγόριθμου 5 είναι ότι δεν εφαρμόζει τον χειριστή δ_{-1} κατευθείαν (όπως στο Λήμμα 2.27), όταν βρίσκει ένα κακό ζευγάρι. Αντίθετα, κρατάει την πληροφορία για το πως θα πρέπει να αλλάξουν οι δείκτες αργότερα. Αυτή η πληροφορία είναι συσσωρευμένη σε δύο προτάσεις, μία για την θετική υπολέξη της w και μία για την αρνητική λέξη της w. Το μέγεθος της πρότασης S_1 (ή της S_2) ισούται με το μήκος μία βοηθητικής λέξης w_1 (ή w_2). Επομένως στο βήμα B. το x_a (ή το x_b) ορίζεται αν και μόνο αν το ϵ_1 (ή αντίστοιχα το ϵ_2) ορίζεται.

Αλγόριθμος 5 (Αφαίρεση κακών ζευγαριών από μία ημικανονική μορφή)

SIGNATURE. w = EraseBadPairs(u).

INPUT. Μία ημικανονική μορφή u $= x_{i_1}...x_{i_s}x_{j_t}^{-1}...x_{j_1}^{-1}$.

OUTPUT. Μια λέξη w η οποία είναι η κανονική μορφή της u.

INITIALIZATION. Έστω $\delta = 0, \delta_1 = 0, \delta_2 = 0, w_1 = 1, w_2 = 1$. Έστω $u_1 = x_{i_1}...x_{i_s}$ και $u_2 = x_{j_t}^{-1}...x_{j_1}^{-1}$ το θετικό και το αρνητικό μέρος της u, αντίστοιχα. Επιπλέον, θέτουμε δύο μηδενικές προτάσεις S_1 και S_2.

ΥΠΟΛΟΓΙΣΜΟΙ.

A. Έχουμε $u_1 = x_{i_1}...x_{i_s}$ και $u_2 = x_{j_t}^{-1}...x_{j_1}^{-1}$.

Β. Έχουμε x_a να είναι το ακρο-αριστερά γράμμα της w_1, x_b ως το άκρο-δεξιά γράμμα της w_2 και ϵ_i (i = 1, 2) το πάνω στοιχείο της S_i, δηλαδή το τελευταίο στοιχείο που μπήκε εκεί. Αν μία από αυτές τις τιμές δεν υπάρχει, (επειδή για παράδειγμα η S_i είναι κενή), τότε η αντίστοιχη μεταβλητή δεν ορίζεται.

1. Εάν s > 0 και (ή t $= 0$ ή $i_s > j_t$), τότε:
   α) πολλαπλασιάζουμε την w_1 από αριστερά με την x_{i_s}(δηλαδή $w_1 \longleftarrow x_{i_s}w_1$).
   β) αφαιρούμε το x_{i_s} από την u_1.
   γ) βάζουμε 0 στην S_1.
   δ) πάμε στο βήμα 5.
2. Εάν t > 0 και (ή s $= 0$ ή $i_s < j_t$), τότε:
   α) πολλαπλασιάζουμε την w_2 από δεξιά με την $x_{j_t}^{-1}$ (δηλαδή $w_2 \longleftarrow w_2x_{j_t}^{-1}$).
   β) αφαιρούμε το $x_{j_t}^{-1}$ από την u_2.
   γ) βάζουμε 0 στην S_2.
   δ) πάμε στο βήμα 5.
3. Εάν $i_s = j_t$ και (οι αριθμοί $a - \epsilon_1$ και $b - \epsilon_2$ (αυτοί που έχουν οριστεί δεν είναι ίσοι με το i_s ή $i_s + 1$)), τότε:
   α) αφαιρούμε την x_{i_s} από την u_1.
   β) αφαιρούμε το $x_{j_t}^{-1}$ από την u_2.
   γ) εάν η S_1 δεν είναι κενή, αυξάνουμε το πάνω στοιχείο της S_1.
   δ) εάν η S_2 δεν είναι κενή, αυξάνουμε το πάνω στοιχείο της S_2.
   στ) πάμε στο βήμα 5.
4. Εάν τα 1-3 δεν μπορούν να εφαρμοστούν (όταν $i_s = j_t$ και (ένας από τους αριθμούς $a - \epsilon_1, b - \epsilon_2$ ορίζεται και είναι ίσος με είτε το i_s είτε το $i_s + 1$)), τότε:
   α) πολλαπλασιάζουμε την w_1 από αριστερά με το x_{i_s}(δηλαδή $w_1 \longleftarrow x_{i_s}w_1$).
   β) πολλαπλασιάζουμε την w_2 από δεξιά με το $x_{j_j}^{-1}$(δηλαδή $w_2 \longleftarrow w_2x_{j_t}^{-1}$).
   γ) αφαιρούμε την x_{i_s} από την u_1.
   δ) αφαιρούμε το $x_{j_t}^{-1}$ από την u_2.
   στ) βάζουμε 0 στην S_1.

ζ) βάζουμε 0 στην S_2.

η) πάμε στο βήμα 5.

5. Εάν S_1 και S_2 δεν είναι κενές, τότε πάμε στο βήμα 1.

Γ. Εφόσον η (w_1) δεν είναι κενή:

1. παίρνουμε το x_1 ως το πρώτο γράμμα της w_1 (δηλαδή $w_1 = x_{i_1}\dot{w_1}$).
2. παίρνουμε c από την κορυφή της S_1 και το προσθέτουμε στο δ_1 (δηλαδή $\delta_1 \longleftarrow \delta_1 + c$).
3. πολλαπλασιάζουμε το u_1 από δεξιά με το $x_{i_1} - \delta_1$ (δηλαδή $u_1 \longleftarrow u_1 x_{i_1} - \delta_1$).
4. αφαιρούμε το x_{i_1} από την w_1.

Δ. Εφόσον η (w_2) δεν είναι κενή:

1. παίρνουμε το x_{j_1} ως το τελευταίο γράμμα της w_2 (δηλαδή $w_2 = w_1' \dot{x}_{j_1}^{-1}$).
2. παίρνουμε c από την κορυφή της S_2 και το προσθέτουμε στο δ_2 (δηλαδή $\delta_2 \longleftarrow \delta_2 + c$).
3. πολλαπλασιάζουμε το u_2 από αριστερά με το $x_{j_1-\delta_2}^{-1}$ (δηλαδή $u_2 \longleftarrow x_{j_1-\delta_2}^{-1} u_2$).
4. αφαιρούμε το $x_{j_1}^{-1}$ από την w_2.

Ε. Έξοδος $u_1 u_2$.

Πρόταση 2.30. *Η έξοδος του Αλγόριθμου 5 είναι η κανονική μορφή w μίας ημικανονικής μορφής u. Το πλήθος των λειτουργιών που απαιτούνται, για να τερματίσει ο Αλγόριθμος 5, είναι γραμμένες από το $D\cdot \mid u \mid$, όπου D είναι μία σταθερά ανεξάρτητη της u.*

Απόδειξη: Απο το Λήμμα 2.27 έπεται το πρώτο μέλος της πρότασης. Η εκτίμηση του χρόνου είναι προφανής από τον Αλγόριθμο, εφόσον οι λέξεις u_1, u_2 υποβάλλονται σε επεξεργασία γράμμα ανά γράμμα, και κανένα γράμμα δεν επεξεργάζεται δύο φορές.

□

Επομένως, έχουμε το βασικό συμπέρασμα για αυτή την παράγραφο:

Θεώρημα 2.31. *Σε μία ομάδα Thompson F, η κανονική μορφή μίας δοσμένης λέξης w μπορεί να υπολογιστεί σε χρόνο $O(\mid w \mid log \mid w \mid)$.*

Τέλος, παρατηρούμε ότι πιο πρόσφατα, ο Matucci δημοσίευσε μία αποτελεσματική επίθεση στο Πρόβλημα (Αναζήτησης) Αποσύνθεσης στην ομάδα Thompson F, που βασίζεται σε μία ερμηνεία των ομάδων Thompson ως ομάδα διατηρούμενου-προσανατολισμού γραμμικά-τμηματικών ομομορφισμών του διαστήματος μονάδας. Το συμπέρασμα εδώ, όπως και στις ομάδες πλεξίδων, είναι ότι η ύπαρξη δίαφορων (κανονικών) μορφών των στοιχείων μίας ομάδας μπορεί να είναι πιθανό πρόβλημα ασφάλειας επειδή μία (κανονική) μορφή μπορεί να αποκαλύψει τι προσπαθεί να κρύψει η άλλη.

2.3 Ομάδες Πινάκων

Σε αυτή την παράγραφο προτείνουμε τις ομάδες πινάκων επί πεπερασμένων μεταθετικών δακτυλίων από τις καλύτερες πλατφόρμες για κανονικά κρυπτογραφικά πρωτόκολλα, διότι αυτές οι ομάδες έχουν πολλαπλά οφέλη υπό την έννοια ότι μπορεί ο πολλαπλασιασμός πινάκων είναι μη μεταθετικός αλλά οι καταχωρήσεις πινάκων προέρχονται από μεταθετικό δακτύλιο, παρέχοντας έτσι έναν καλό μηχανισμό απόκρυψης. Επιπλέον, οι ομάδες πινάκων έχουν το πλεονέκτημα να παρουσιάζουν τα στοιχεία τους σε μία «φυσική» κανονική μορφή.

Ο λόγος που θέλουμε ο βασικός δακτύλιος να είναι πεπερασμένος, είναι ότι οι πεπερασμένοι δακτύλιοι R είναι περιοδικοί. **Περιοδικός δακτύλιος** σημαίνει ότι για κάθε u ∈ R υπάρχουν θετικοί ακέραιοι m,k τέτοιοι που $u^m = u^k$. Η περιοδικότητα είναι καλή για την διάχυση, επειδή αυξάνει το *δυναμικό σύστημα*. Τα δυναμικά συστήματα με έναν μεγάλο αριθμό μελών συνήθως επιδεικνύουν πολυ πολύπλοκη συμπεριφορά, οπότε είναι αρκετό να αναφέρουμε το περιβοήτο (3x+1) πρόβλημα.

Τονίζουμε ιδιαίτερα ότι

ΜΕΤΑΘΕΤΙΚΟΤΗΤΑ και *ΠΕΡΙΟΔΙΚΟΤΗΤΑ*

είναι δύο εργαλεία μεγάλης σημασίας που βοηθάνε στην απόκρυψη των παραγόντων ενός γινομένου. Όμως, η σημαντικότητα τους για την ασφάλεια της κρυπτογραφίας δεν μπορεί γενικά να υπερεκτιμηθεί. Για καλύτερη ασφάλεια, την ίδια στιγμή, η μεταθετικότητα μπορεί να ενισχυθεί από τη μή μεταθετικότητα. Οπότε η

ΜΕΤΑΘΕΤΙΚΟΤΗΤΑ υπό την ενίσχυση της *ΜΗ-ΜΕΤΑΘΕΤΙΚΟΤΗΤΑΣ*

είναι ένα άλλο σημαντικό συστατικό για την ασφάλεια της κρυπτογραφίας. Αποτρέπει τον επιτιθέμενο με χρησιμοποίηση προφανών σχέσεων να ανακτήσει τους παράγοντες του γινομένου, όπως ab = ba.

Τέλος, θα αναφερθούμε σε παραδείγματα πεπερασμένων δακτυλίων που θα μπορούσαν να χρησιμοποιηθούν ως βασικοί δακτύλιοι στις ομάδες πινάκων στην κρυπτογραφία. Ο πιο απλός θα ήταν ο δακτύλιος $\mathbb{Z}_n$: οι πίνακες πάνω στον $\mathbb{Z}_n$ μπορούν να χρησιμοποιηθούν ως πλατφόρμα στο γνήσιο πρωτόκολλο ανταλλαγής κλειδιού των Diffie-Hellman, αλλά ένα προφανές μειονέκτημα αυτού του δακτυλίου είναι ότι το n θα πρέπει να είναι πολύ μεγάλο για να παρέχει έναν ικανοποιητικά μεγάλο χώρο κλειδιού. Σημειώνουμε ότι έχει γίνει πολύ λίγη έρευνα σχετικά με την σύγκριση των ομάδων πινάκων πάνω από τον $\mathbb{Z}_n$ σε σχέση με τον ίδιο τον $\mathbb{Z}_n$, όσον αφορά στην ασφάλεια, όταν χρησιμοποιούνται ως πλατφόρμα για το γνήσιο πρωτόκολλο ανταλλαγής κλειδιού των Diffie-Hellman.

Μία άλλη πιθανότητα είναι να χρησιμοποιήσουμε τον $\mathrm{R} = \mathbf{F}_p[x]/(f(x))$. Εδώ, $\mathbf{F}_p$ είναι το πεδίο με p στοιχεία, το $\mathbf{F}_p[x]$ είναι ο δακτύλιος των πολυωνύμων πάνω στον $\mathbf{F}_p$, και (f(x)) είναι το ιδεώδες του $\mathbf{F}_p$ που παράγεται από ένα πολυώνυμο f(x) βαθμού n. Αυτός ο δακτύλιος είναι ισομορφικός στο πεδίο $\mathbf{F}_{p^n}$, αλλά η αναπαράσταση του R ως ένα πεδίο πηλίκου επιτρέπει σε κάποιον να πάρει ένα μεγάλο χώρο κλειδιού, ενώ διατηρεί όλες τις βασικές παραμέτρους. Σημειώνουμε ότι ένας τέτοιος δακτύλιος έχει χρησιμοποιηθεί από τους Tillich-Zémor κατά την κατασκευή μίας hash συνάρτησης. Στον δακτύλιο χρησιμοποίησαν $\mathrm{p} = 2$ και n είναι ένας πρώτος αριθμός, έτσι ώστε $100 < \mathrm{n} < 200$. Οι πίνακες που θεώρησαν ανήκουν στην ομάδα $SL_2(\mathrm{R})$.

Μία βελτίωση της ίδιας ιδέας είναι να χρησιμοποιήσουμε τον δακτύλιο των *περικομμένων πολυωνύμων* πάνω στον $\mathbb{Z}_n$. Τα *περικομμένα πολυωνύμα* ή τα *N-περικομμένα πολυωνύμα*, έχουν την μορφή $\sum_{k=0}^{N} a_k x^k$ με την γνωστή πρόσθεση και πολλαπλασιασμό και τον κανόνα $x^i \cdot x^j = x^{(i+j)mod(N+1)}$. Όπως και στον δακτύλιο R στην προηγούμενη παράγραφο, αυτός ο δακτύλιος είναι ένα πηλίκο πολυωνύμων ενός ιδεώδους, αλλά αυτό το ιδεώδες (που παράγεται από το πολυώνυμο x^{N+1}) είναι αρκετά απλό και οι υπολογισμοί στον αντίστοιχο δακτύλιο πηλίκου είναι αρκετά αποτελεσματικοί. Επίσης, ένας μεγάλος χώρος κλειδιού παρέχεται εδώ με χαμηλό κόστος. Για παράδειγμα, με $\mathrm{n} = 100$, $\mathrm{N} = 20$, υπάρχουν $100^{21} = 10^{42}$ *N-περικομμένα πολυωνύμα*. Δηλαδή, υπάρχουν πάνω από 10^{160} πίνακες 2×2 πάνω σε αυτό τον δακτύλιο.

2.4 Ομάδες μικρών διαγραφών

Σε αυτή την παράγραφο προτείνονται οι ομάδες μικρών διαγραφών ως πλατφόρμες ενός κρυπτογραφικού συστήματος.

Ορισμός 2.32. *Ομάδες μικρών διαγραφών.*

Οι ***ομάδες μικρών διαγραφών*** *έχουν σχέσεις (relators) που ικανοποιούν μία μετρική συνθήκη. Πιο συγκεκριμένα, έστω F(X) μια ελεύθερη ομάδα με βάση* $X = \{x_i \mid i \in I\}$*, όπου I ένα σύνολο ευρετήριο. Έστω* $\epsilon_k \in \{\pm 1\}$ *όπου* $1 \leq k \leq n$*. Μία λέξη:*

$$w(x_1, ..., x_n) = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$$

όπου F(X) με όλα τα x_{i_k} *όχι απαραιτήτως διακριτά, είναι μια* ***μειωμένη X-λέξη*** *(reduced X-word), αν* $x_{i_k}^{\epsilon_k} \neq x_{i_{k+1}}^{-\epsilon_{k+1}}$*,για* $1 \leq k - 1 \leq n$*. Επιπλέον, η λέξη* $w(x_1, ..., x_n)$ *είναι* ***κυκλικά μειωμένη*** *(cyclically reduced), αν είναι μία μειωμένη X-λέξη και* $x_{i_1}^{\epsilon_1} \neq x_{i_n}^{-\epsilon_n}$*. Ένα σύνολο R που περιέχει κυκλικά μειωμένες λέξεις από το F(X) είναι* ***συμμετρικό*** *(symmetrized) αν είναι κλειστό ως προς τις κυκλικές μεταθέσεις και στο να δέχεται αντιστρόφους.*

□

Ορισμός 2.33. *Έστω G μια ομάδα με αναπαράσταση* $\langle X, R \rangle$*. Μία μη κενή λέξη u* $\in F(X)$ *καλείται piece αν υπάρχουν δύο διαφορετικές σχέσεις (relators)* $r_1, r_2 \in R$ *της G , τέτοιες ώστε* $r_1 = uv_1$ *και* $r_2 = uv_2$ *για κάποια* $v_1, v_2 \in F(X)$ *και με καμία απαλοιφή μεταξύ των u και* v_1 *ή μεταξύ των u και* v_2*.*

□

Μία ομάδα G ανήκει στη τάξη C(p), αν κανένα στοιχείο του R δεν είναι γινόμενο λιγότερο από p pieces.

Επίσης η ομάδα G ανήκει στη τάξη C(λ) αν για κάθε r ∈ R τέτοιο ώστε r = uv και u είναι ένα piece ισχύει: $\mid u \mid < \lambda \mid r \mid$.

2.4.1 Αλγόριθμος Dehn

Αν η G ανήκει στη κλάση $C(\frac{1}{6})$, τότε ο αλγόριθμος Dehn λύνει το Πρόβλημα Λέξης αποτελεσματικά. Ο αλγόριθμος αυτός είναι πολύ απλός:

1. Σε μία (μη κενή) λέξη εισόδου w, αναζητούμε για ένα μεγάλο piece της σχέσης (relator) R (δηλαδή ένα piece του οποίου το μήκος είναι περισσότερο από το μισό του μήκους ολόκληρης της σχέσης (relator)). Αν δεν υπάρχει τέτοιο piece, τότε παίρνουμε στην έξοδο w≠1 στην G.

2. Εάν ένα τέτοιο piece, ας το πούμε u, δεν υπάρχει, τότε r = uv για κάποιο r∈ R, όπου το μήκος της v είναι μικρότερο της u. Τότε αντικαθιστούμε τη u με τη v^{-1} στην w. Το μήκος της λέξης w′ του αποτελέσματος είναι μικρότερο από εκείνο της w. Αν w′ = 1, τότε παίρνουμε στην έξοδο w = 1 στην G.

3. Εάν το w′ ≠ 1, τότε επαναλαμβάνουμε από Βήμα 1. με w:= w′.

Αφού το μήκος της w μειώνεται μετά από κάθε loop, αυτός ο αλγόριθμος θα τερματίσει μετά από έναν πεπερασμένο αριθμό βημάτων. Έχει πολυπλοκότητα τετραγωνικού χρόνου ως προς το μήκος της λέξης εισόδου w. Τέλος, σημειώνουμε ότι μια γενικά πεπερασμένως αναπαραστάσιμη ομάδα αποτελεί μία ομάδα μικρών διαγραφών.

Παράδειγμα 2.34. *Έστω* $\langle x_1, x_2, x_3; x_1^2x_2x_3^2x_2^{-1} = 1, x_2^2x_3x_1^2x_3^{-1} = 1\rangle$ *να είναι μία παρουσίαση της ομάδας G. Τώρα,* $x_1^{\pm 2}, x_2^{\pm 1}, x_2^{\pm 2}, x_3^{\pm 1}, x_3^{\pm 2}, (x_2x_3)^{\pm 1}, (x_2x_3^{-1})^{\pm 1}$ *είναι κομμάτια της G και κάθε σχέση (relator) είναι ένα γινόμενο τεσσάρων κομματιών από τα παραπάνω. Για αυτό η ομάδα G ανήκει στην κλάση των C(4) ομάδων. Παρόλα αυτά η G δεν ανήκει στην κλάση των C′(1/6): Για i = 1, 2, 3 τα κομμάτια* $x_i^{\pm 1}$*, ικανοποιούν την ιδιότητα* $| x_i^{\pm 1} | = \frac{1}{6} | x_1x_2x_3x_4^2x_2^{-1} |$ *και* $| x_i^{\pm 1} | = \frac{1}{6} | x_2^2x_3x_1x_4x_3^{-1} |$.

□

Η λύση στο Πρόβλημα Συζυγίας είναι άσχετο με την εκτέλεση του κρυπτογραφικού πρωτοκόλλου αξιοποιώντας την υπολογιστική δυσκολία του Προβλήματος Αναζήτησης Συζυγίας. Παρόλα αυτά, παρέχονται λογικές αποδείξεις ενός δυνητικά δύσκολου υπολογιστικά Προβλήματος Αναζήτησης Συζυγίας εάν δεν υπάρχει γνωστός πολυωνυμικός χρόνος αλγορίθμου για το Πρόβλημα Συζυγίας.

Για μία τάξη ομάδων μικρών διαγραφών που κατέχουν την ιδιότητα του μη γνωστού πολυωνυμικού χρόνου αλγορίθμου για το Πρόβλημα Συζυγίας, χρειαζόμαστε μία ακόμη συνθήκη. Μία ομάδα G με πεπερασμένη παρουσίαση της μορφή της $\langle X; R\rangle$ ανήκει στην κλάση T(q) για έναν φυσικό αριθμό q εάν για οποιαδήποτε πρόταση $r_1, ..., r_n \in R$, με $3 \leq n < q$ και $r_i \neq r_{i+1}^{-1}$, τουλάχιστον ένα απο τα γινόμενα $r_1r_2, ..., r_{n-1}r_n, r_nr_1$ είναι κυκλικά μειωμένη χωρίς διαγραφή. Βλ[13].

Ορισμός 2.35. *Μία ομάδα G με πεπερασμένη παρουσίαση της μορφή της* $\langle X; R\rangle$ *λέγεται* ***ομάδα μικρών διαγραφών τύπου C(p)-T(p)****, εάν ανήκει στις τάξεις C(p) και T(p).*

□

Το Πρόβλημα της Λέξης είναι επιλύσιμο στην τάξη των ομάδων μικρών διαγραφών του τύπου C(4)-T(4). Εάν οι υπερβολικές ομάδες $C'(1/6)$ αποφευχθούν, τότε, γενικά, δεν υπάρχει γνωστός πολυωνυμικός χρόνος αλγορίθμου για τη λύση του Προβλήματος Αναζήτησης Συζυγίας για τις ομάδες σε αυτήν την τάξη (ενώ το Πρόβλημα Συζυγίας είναι επιλύσιμο).

Επομένως, σε αυτή την τάξη, οι νόμιμες οντότητες μπορούν να διαλέξουν μία τυχαία ομάδα και να εκτελέσουν ένα αλγεβρικό κρυπτογραφικό πρωτόκολλο δημοσίου κλειδιού που στηρίζεται στην δυσκολία του Προβλήματος Αναζήτησης Συζυγίας ή ενός ακόμη πιο δύσκολου προβλήματος.

Παράδειγμα 2.36. *Θεωρούμε την ομάδα G με την εξής παρουσίαση*

$$\langle x_1, x_2, x_3; x_1^2 x_2 x_3^2 x_2^{-1}, x_2^2 x_3 x_1^2 x_3^{-1} \rangle$$

για κάποια r_1, r_2, r_3, έτσι ώστε κάποιο από αυτά να μην είναι ο αντίστροφος του άλλου, από το συμμετρικό σύνολο $\{x_1^2 x_2 x_3^2 x_2^{-1}, x_2^2 x_3 x_1^2 x_3^{-1}\}$ και καμία διαγραφή να μην είναι εφικτή σε τουλάχιστον μία από τις λέξεις $r_1 r_2, r_2 r_3, r_3 r_1$. Για αυτό τον λόγο η G ανήκει στην τάξη των T(4) και C(4) ομάδων, αλλά όχι στην $C'(1/6)$ ομάδων.

□

2.5 Επιλύσιμες Ομάδες

Ας θυμηθούμε τους παρακάτω ορισμούς:

Ορισμός 2.37.

- *Μία ομάδα G καλείται* ***αβελιανή*** *αν $[a, b] = 1$ για κάθε a,b όπου με $[a, b]$ συμβολίζουμε $a^{-1}b^{-1}ab$.*

  Αυτό μπορεί να γενικευτεί κατά διάφορους τρόπους.

- *Μία ομάδα G καλείται* ***μεταβελιανή*** *αν $[[x, y], [z, t]] = 1$ για κάθε x, y, z, $t \in G$.*

- *Μία ομάδα G καλείται* ***μηδενοδύναμη της τάξης*** *$c \in 1$ αν $[y_1, y_2, ..., y_{c+1}] = 1$ για κάθε $y_1, y_2, ..., y_{c+1} \in G$, όπου $[y_1, y_2, y_3] = [[y_1, y_2], y_3]$κλπ.*

- *Η* ***αντιμεταθετική υποομάδα*** *της G είναι η ομάδα $G' = [G, G]$ που παράγεται από όλους τους αντιμεταθέτες δηλαδή, από εκφράσεις της μορφής $[u, v] = u^{-1}v^{-1}uv$, όπου u,v $\in G$.*

□

Επιπλέον, μπορούμε να καθορίσουμε, τον k-οστό όρο της *κατώτερης κεντρικής σειράς* της G: $\gamma_1(G) = G, \gamma_2(G) = [G, G], \gamma_k(G) = [\gamma_{k-1}(G), G]$. Σημειώνουμε ότι κάποιο έχει $a([u, v]) = [a(u), a(v)]$ για κάθε ενδομορφισμό a στην G. Επομένως, η $\gamma_k(G)$ είναι μία πλήρως αμετάβλητη υποομάδα της G, για κάθε $k \leq 1$, και έτσι:

$$G'' = [G', G']$$

Θα ασχοληθούμε ιδιαίτερα με τις ελεύθερες μεταβελιανές ομάδες αφού οι ομάδες αυτές χρησιμοποιούνται ως πλατφόρμες στα κρυπτογραφικά πρωτόκολλα.

- Έστω F_n μία ελεύθερη ομάδα τάξης n. Η σχετικά ελεύθερη ομάδα $F_n/{F_n}''$ καλείται **ελεύθερη μεταβελιανή ομάδα** τάξης n, την οποία συμβολίζουμε με M_n.

2.5.1 Κανονικές Μορφές Στις Ελεύθερες Μεταβελιανές Ομάδες

Σε αυτήν την ενότητα θα περιγράψουμε την κανονική και την ημικανονική μορφή των στοιχείων μιας ελεύθερης μεταβελιανής ομάδας M_n. Η ημικανονική μορφή είναι καλή για τις μεταδόσεις, γιατί είναι εύκολα μετατρέψιμη πίσω στη λέξη που αντιπροσωπεύει το μεταδιδόμενο στοιχείο. Συνεπώς, αυτή η μορφή δεν είναι μοναδική εάν $n > 2$ (για αυτό την ονομάζουμε ημικανονική). Έτσι δε μπορεί να χρησιμοποιηθεί ως κοινό μυστικό από την Μαριέττα και τον Μάρκο σε ένα κρυπτογραφικό πρωτόκολλο. Για το λόγο αυτό, μπορεί να χρησιμοποιηθεί η κανονική μορφή (ένας πίνακας 2×2).

Έστω $u \in M_n$. Με u_{ab} συμβολίζουμε τον αβελιανισμό του u δηλ. την εικόνα του u ως προς τον επιμορφισμό $a : M_n \longrightarrow M_n/[M_n, M_n]$. Σημειώνουμε ότι μπορούμε να προσδιορίσουμε το $M_n/[M_n, M_n]$ με το $F_n/[F_n, F_n]$. Στην ουσία το u_{ab} είναι ένα στοιχείο από την ομάδα παραγόντων της F_n, αλλά ωστόσο χρησιμοποιούμε επίσης τον ίδιο συμβολισμό u_{ab} για κάθε λέξη με γεννήτορες x_i (δηλ. ένα στοιχείο από το περιβάλλον της ελεύθερης ομάδας F_n) που αναπαριστά το u_{ab} όταν δεν είναι διφορούμενη.

Για u, v $\in M_n$, με u^v συμβολίζουμε την έκφραση $v^{-1}uv$. Διαφορετικά, λέμε ότι τα u και v είναι συζυγή. Αν $u \in [M_n, M_n]$ τότε μπορεί να επεκταθεί στο δακτύλιο $\mathbb{Z}(M_n/[M_n, M_n])$ τον οποίο θα συμβολίζουμε με $\mathbb{Z}A_n$. (Εδώ $A_n = M_n/[M_n, M_n]$ είναι ελεύθερη αβελιανή ομάδα τάξης n).

Έστω W $\in \mathbb{Z}A_n$ της μορφής $W = \sum a_i v_i$, όπου $a_i \in \mathbb{Z}$ και $v_i \in A_n$. Τότε συμβολίζουμε με u^W το γινόμενο $\prod (u^{a_i})^{v_i}$. Αυτό το γινόμενο είναι καλά ορισμένο, αφού κάθε δύο στοιχεία του $[M_n, M_n]$ αντιμετατίθενται στο M_n.

Τώρα έστω u $\in M_n$. Τότε το υ μπορεί να γραφεί στη παρακάτω ημικανονική μορφή:

$$\mathrm{u} = u_{ab} \prod_{i<j} ([x_i, x_j])^{W_{ij}}$$

όπου $W_{ij} \in \mathbb{Z}A_n$. Για να φτάσουμε σε αυτήν την μορφή, χρησιμοποιούμε τη διαδικασία συλλογής που βασίζεται στις παρακάτω ταυτότητες (θυμόμαστε ότι $[x, y] = x^{-1}y^{-1}xy$):

$$[y, x] = [x, y]^{-1},$$

$$xy = yx[x, y],$$

$$(xy)^{-1} = y^{-1}([y, x])^{y^{-1}x^{-1}}x,$$

$$x^{-1}y = y([y, x])^{y^{-1}x^{-1}}x^{-1},$$

$$[x, y]z = z([x, y])^z$$

Η διαδικασία συλλογής είναι απλή:

1. Χρησιμοποιώντας τις παραπάνω ταυτότητες, πηγαίνουμε από τα αριστερά προς τα δεξιά κατά μήκος της λέξης u συλλέγοντας όλες τις μη-μεταθετικές εμφανίσεις του x_1 στα αριστερά (που σημαίνει ότι δε νοιαζόμαστε για τις εμφανίσεις $[x_1, x_j]$ ή $[x_j, x_1]$ που δημιουργούνται κατά την πρόοδο της διαδικασίας). Επαναλαμβάνουμε με $x_2, x_3, ...$ Στο τέλος της διαδικασίας, η u θα έχει τη μορφή $\mathrm{u} = u_{ab} \cdot c$, όπου c $\in [M_n, M_n]$ είναι το γινόμενο εκφράσεων της μορφής $[x_i, x_j]^g, g \in M_n$.

2. Αφού δύο οποιαδήποτε στοιχεία του $[M_n, M_n]$ μετατίθενται στο $[M_n]$, μπορεί κάποιος εύκολα να ανασυγκροτήσει τις εκφράσεις $([x_i, x_j])^g$ έτσι που η u να πάρει τη μορφή:

$$\mathrm{u} = u_{ab} \cdot \prod_{i<j} ([x_i, x_j])^{W_{ij}} \text{ ,όπου } W_{ij} \in \mathbb{Z}A_n.$$

Αυτή η διαδικασία παίρνει τετραγωνικό χρόνο όσον αφορά στο μήκος του u.

Το να μετατρέψουμε την ημικανονική μορφή σε λέξη είναι τετριμμένο, καθότι η u είναι ήδη λέξη. Το μόνο πρόβλημα με τη ημικανονική μορφή είναι ότι δεν είναι

μοναδική, αν n > 2 κι επομένως δε μπορεί να χρησιμοποιηθεί ως κοινό μυστικό κλειδί της Μαριέττας και του Μάρκου.

(Για n > 2 χρησιμοποιούμε τη κανονική μορφή που είναι μοναδική, αποτελεσματικά υπολογίσιμη (σε τετραγωνικό χρόνο όσον αφορά το μήκος της u), αλλά όχι και τόσο εύκολα μετατρέψιμη πίσω στη λέξη).

Στην συνέχεια, θα παρουσιάσουμε τις *Παραγώγους του Fox*, οι οποίες είναι μη-μεταθετικά ανάλογες με τις συνηθισμένες παραγώγους του Leibniz.

Ορισμός 2.38. *Παράγωγος του Fox. Έστω $\mathbb{Z}F$ να είναι η ομάδα δακτυλίου μίας ελεύθερης ομάδας F που παράγεται από τα $x_1, x_2, ...$ Μία παράγωγος του Fox του x_i είναι ένας χάρτης $\partial_{x_i} : \mathbb{Z}F \longrightarrow \mathbb{Z}F$ έτσι ώστε $\partial_{x_i}(x_j) = \delta_{ij}$ και $\partial_{x_i}(vw) = \partial_{x_i}(v) + v \cdot \partial_{x_i}(w)$ για κάποια $v, w \in F$. Αυτός ο χάρτης μπορεί να επεκταθεί σε όλο το $\mathbb{Z}F$ μέσω γραμμικότητας.*

□

Παράδειγμα 2.39. *Έστω $g \in F$ και 1 να είναι η ταυτότητα του F. Εφόσον $\partial(1) = \partial(1) + \partial(1)$, έπεται ότι $\partial(1) = 0$. Για αυτό τον λόγο $\partial(gg^{-1}) = \partial(g) + g\partial(g^{-1}) = 0$, άρα συνεπάγεται $\partial(g^{-1}) = -g^{-1}\partial(g)$.*

□

Παράδειγμα 2.40. *Έστω x και y να είναι οι γεννήτορες της ελεύθερης ομάδας F(x,y). Τότε:*

$$\partial_x([x,y]) = \partial_x(x^{-1}y^{-1}xy)$$

$$= \partial_x(x^{-1}) + x^{-1}\partial_x(y^{-1}) + x^{-1}y^{-1}\partial_x(x) + x^{-1}y^{-1}x\partial_x(y)$$

$$= -x^{-1} + x^{-1}y^{-1} = x^{-1}y^{-1}(1-y).$$

$$\partial_y([x,y]) = \partial_y(x^{-1}) + x^{-1}\partial_y(y^{-1}) + x^{-1}y^{-1}\partial_y(x) + x^{-1}y^{-1}x\partial_y(y)$$

$$= -x^{-1}y^{-1} + x^{-1}y^{-1}x$$

$$= -x^{-1}y^{-1}(1-x)$$

□

Με F_{ab} συμβολίζουμε τον αβελιανισμό μίας ελεύθερης ομάδας F, δηλαδή την ομάδα παράγοντα F/F' . Έστω $\alpha : F \longrightarrow F_{ab}$ να είναι ο φυσικός επιμορφισμός. Μπορούμε να περιμένουμε ότι ο χάρτης $\alpha : \mathbb{Z}F \longrightarrow \mathbb{Z}F_{ab}$ να είναι γραμμικός.

Πρόταση 2.41. *Έστω $w \in F_n$. Τότε $w \in F_n''$ αν και μόνο αν $\alpha(\partial_{x_i}(w)) = 0$ για κάθε γεννήτορα x_i του F_n.*

□

Αυτή η πρόταση έχει ως αποτέλεσμα ένα απλό αλγόριθμο που μπορεί να λύσει το Πρόβλημα Λέξης σε μία ελεύθερη μεταβελιανή ομάδα M_n: δίνεται μία λέξη w $\in M_n$ με σχετικά ελεύθερους γεννήτορες x_i. Η w μπορεί να θεωρηθεί ως ένα στοιχείο της ελεύθερης ομάδας F_n με το ίδιο σύνολο ελεύθερων γεννητόρων. Μπορούμε να υπολογίσουμε το $\partial_{x_i}(w)$ για κάθε x_i και να ελέγξουμε αν όλα είναι αβελιανά με το 0. Το τελευταίο είναι άμεσο αποτέλεσμα εφόσον το Πρόβλημα της Λέξης σε μία ελεύθερη αβελιανή ομάδα F_{ab} είναι εύκολα επιλύσιμο.

Αυτός ο αλγόριθμος δεν είναι μόνο εύκολος, αλλά είναι και αποτελεσματικός:

Πρόταση 2.42. *Ο Αλγόριθμος που επιλύει το Πρόβλημα της Λέξης στην M_n που βασίζεται στην Πρόταση 2.35 έχει το πολύ τετραγωνικό χρόνο πολυπλοκότητας σε σχέση με το μήκος της εισαγώμενης λέξης.*

Απόδειξη:

Έστω w $\in F_n$ και με το $\mid w \mid = m$ συμβολιζουμε το συνηθισμένο μήκος της λέξης w. Ο υπολογισμός της $\partial_{x_i}(w)$, για κάποιους γεννήτορες x_i, έχει ως αποτέλεσμα το πολύ m αθροίσματα σε μία ελεύθερη ομάδα δακτυλίου $\mathbb{Z}F_n$. Επομένως, ο υπολογισμός της ∂_x έχει το πολύ γραμμικό χρόνο πολυπλοκότητας. Τότε, το να αποφασίσουμε αν ο αβελιανισμός της $\partial_{x_i}(w)$ είναι 0, ανέρχεται στην συλλογή των αθροισμάτων της μορφής $c \cdot h_i$, όπου $c \in \mathbb{Z}, h_i \in F_n$ τέτοια ώστε όλα τα h_i να έχουν τον ίδιο αβελιανισμό. Αυτό επιτυγχάνεται μέσω της επαναγραφής κάθε h_i στην μορφή $x_1^{\alpha_1}x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n} \cdot u_i$, όπου $u_i \in F_n'$. Εφόσον τα h_i έχουν μήκος $\leq m$ και το πλήθος των h_i είναι το πολύ m, αυτό το μέρος του αλγορίθμου χρειάζεται $O(m^2)$, πράγμα με το οποίο τελειώνει η απόδειξη.

□

Τέλος, περιγράφουμε την κανονική μορφή των u $\in M_n$ που βασίζεται στις παραγώγους του Fox.

Για κάποιο στοιχείο u $\in M_n$ μίας ελεύθερης αβελιανής ομάδας, η κανονική του μορφή είναι ένας 2×2 πίνακας με τις ακόλουθες εισόδους:

1. Η είσοδος στην κάτω αριστερά γωνία είναι 0.

2. Η είσοδος στην κάτω δεξιά γωνία είναι 1.

3. Η είσοδος στην πάνω αριστερά γωνία είναι ο αβελιανισμός της u, έτσι είναι ένα στοιχείο της ελεύθερης αβελιανής ομάδας $M_n/[M_n, M_n]$.

4. Η είσοδος στην πάνω δεξιά γωνία είναι το πιο σημαντικό. Είναι ένα διάνυσμα n αβελιανισμένων μερικών παραγώγων του Fox της λέξης u.

Σημειώνουμε ότι η ελεύθερη αβελιανή ομάδα $M_n/[M_n, M_n]$ επιδρά πάνω στα διανύσματα αβελιανισμένων παραγώγων του Fox μέσω της πράξης του πολλαπλασιασμού. Αυτό κάνει το σύνολο των κανονικών μορφών υπό την πράξη του πολλαπλασιασμού, ομάδα. Επιπλεόν, η αναπαράσταση των στοιχείων της M_n με την κανονική τους μορφή είναι έμπιστη, βασικά έχουμε την ενσωμάτωση των M_n σε μία ομάδα πινάκων, αυτή καλείται ενσωμάτωση Magnus.

2.6 Ομάδες Artin

Οι ομάδες Artin μπορούν να χρησιμοποιηθούν ως πλατφόρμες στα κρυπτογραφικά πρωτόκολλα. Έστω G(Γ) μία ομάδα με αναπαράσταση:

$$\mathrm{G}(\Gamma) = \langle g_1, ..., g_n : r(g_i, g_j) \text{ (για } 1 \leq i, j \leq n \text{ και } i \neq j)\rangle,$$

όπου $n \geq 2$ και $r(g_i, g_j) = 1$ είναι μία σχέση (relator) με δύο γεννήτορες. Αν δίνεται η ομάδα G(Γ), τότε υπάρχει ένα σχετικό γράφημα με ετικέτες και αντιστρόφως. Οι κόμβοι του γραφήματος Γ_G έχουν ως ετικέτες τους γεννήτορες της G_Γ. Κάθε δύο κόμβοι $g_i, g_j \in \Gamma_G$ συνδέονται με ακμή αν υπάρχει μία σχέση $r(g_i, g_j) \in \Gamma_G$ μεταξύ των αντίστοιχων γεννητόρων. Με άλλα λόγια, οι ακμές έχουν ως ετικέτες σχέσεις.

Παράδειγμα 2.43. *Μία ομάδα Artin A(Γ) είναι μία ομάδα με αναπαράσταση:*

$$A(\Gamma) = \langle a_1, ..., a_n : \mu_{ij} = \mu_{ji} \text{ (για } 1 \leq i < j \leq n)\rangle$$

όπου $\mu_{ij} = \alpha_i\alpha_j a_i ... = \mu_{ij}$ άρα $\mu_{ij} = \mu_{ji}$. Οι ομάδες Artin είναι μία γενίκευση των ομάδων πλεξίδων. Για μία ομάδα Artin A(Γ), το σχετικό γράφημα Γ_A με ετικέτες δεν έχει πολλαπλές ακμές ή βρόχους. Οι κόμβοι a_i του Γ_A είναι οι γεννήτορες της ομάδας Artin. Κάθε δύο κόμβοι $a_ia_j \in \Gamma_A$ συνδέονται με ακμή, η οποία έχει ως ετικέτα τον

ακέραιο m_{ij}, που αντιστοιχεί στη σχέση $\mu_{ij} = \mu_{ji}$ (μεταξύ των αντίστοιχων γεννητόρων $a_i a_j \in A(\Gamma)$). Γενικά, οι αυτομορφισμοί (ή ενδομορφισμοί) του γραφήματος Γ_G εισάγουν αυτομορφισμούς (ή ενδομορφισμούς) της ομάδας G_Γ. Έτσι, το γράφημα που σχετίζεται με την G_Γ μας δίνει έναν τρόπο να κατασκευάσουμε μία ημιομάδα ενδομορφισμών της G_Γ η οποία μπορεί να περιέχει ένα μεγάλο πλήθος αντιμεταθετικών στοιχείων.

□

Παράδειγμα 2.44. *Οι σχέσεις της ομάδας πλεξίδων B_n χρησιμοποιούν δύο γεννήτορες. Το αντίστοιχο γράφημα της B_n είναι ένα απλό μονοπάτι και έχει μόνο έναν αυτομορφισμό, εκείνον της $B_n : \sigma_i \longmapsto \sigma_{n-i}$ και ο οποίος συμβαίνει να είναι ένας εσωτερικός αυτομορφισμός της B_n. Για τις άλλες ομάδες G_Γ τα αντίστοιχα γραφήματα είναι πιο περίπλοκα και είναι εύκολο να φτιάξουμε μία μεγάλη ημιομάδα (ή ημιομάδα) $T \subseteq EndG(\Gamma)$ ενδομορφισμών (ή αυτομορφισμών).*

□

Οι ομάδες Artin A(Γ) με την ιδιότητα $\mu_{ij} \geq 4$ ονομάζονται **ομάδες Artin εξαιρετικά μεγάλου τύπου**. Ένα δέντρο Γ_A που αντιστοιχεί σε μία ομάδα Artin εξαιρετικά μεγάλου τύπου, παρέχει μία άμεση διαδικασία κατασκευής ημιομάδας ενδομορφισμών της A(Γ). Πιο αναλυτικά, οι ομάδες Artin εξαιρετικά μεγάλου τύπου δουλεύουν αυτόματα, οπότε το Πρόβλημα Λέξης για ομάδες αυτής της κλάσης μπορούν να λυθεί σε τετραγωνικό χρόνο. Βλ[13].

Ορισμός 2.45. *Ένα αλγεβρικό κρυπτογραφικό σύστημα δημοσίου κλειδιού είναι μία πλειάδα (S, T, f; $\mathcal{H}$, h), που ικανοποιεί τις εξής ιδιότητες:*

1. *Τα S και T υπολογίσιμες αλγεβρικές δομές (π.χ. ημιομάδες).*
2. *Η $f : S \longrightarrow T$ είναι μία δράση, μονόδρομη και καλώς ορισμένη για τις καθορισμένες τιμές του T: δίνεται ένα ιδιωτικό $t \in T$ και ένα δημόσιο $w \in S$, είναι αδύνατο να καθορίσουμε το t από το f(w, t), και για οποιοδήποτε $w' \in S$ τέτοιο ώστε $w' = w$, παίρνουμε f(w′, t) = f(w, t).*
3. *Το $\mathcal{H}$ είναι ένα σύνολο βοηθητικών υπολογίσιμων αλγεβρικών δομών που ορίζονται για συγκεκριμένα πρωτόκολλα (π.χ. δημοσίου κλειδιού).*

4. *Η $h : X \times Y \longrightarrow X$ είναι μία βοηθητική δράση (που ορίζεται για συγκεκριμένα πρωτόκολλα), όπου τα X, Y είναι δύο από τις αλγεβρικές δομές S, T, ή $H \in \mathcal{H}$.*

□

Για να αλλάξουμε την συνηθισμένη μεθοδολογία της σιωπηλής εργασίας απλά μόνο με αυτομορφισμούς της ομάδας G, γενικεύουμε μία δράση f : G × AutG ⟶ G, χρησιμοποιώντας τον προηγούμενο ορισμό, στην καλώς-ορισμένη δράση πάνω σε μία αλγεβρική δομή S που πάει σε μία αλγεβρική δομή N για καθορισμένες τιμές της N.

Για να δηλώσουμε το πλεονέκτημα της έννοιας του αφηρημένου, κατασκευάζουμε ένα κρυπτογραφικό σύστημα δημοσίου κλειδιού, για την εκτέλεση ενός πρωτοκόλλου ανταλλαγής κλειδιού που βασίζεται σε μία γενίκευση το διακριτού λογαριθμικού προβλήματος:

Ορισμός 2.46. *Ανταλλαγή κλειδιού μεταθετικής δράσης (CAKE)*

Επιλέγουμε τις πλατφόρμες S και T για να ορίσουμε μία αλγεβρική ((PKC) = Public Key Cryptography) πλειάδα (S, T, f; $\mathcal{H}$, h), όπου το βοηθητικό σύνολο $\mathcal{H}$ είναι $\{A, B \subseteq T \mid \forall \alpha \in A, \forall \beta \in B : \alpha\beta = \beta\alpha\}$, το πρωτόκολλο ανταλλαγής κλειδιού είναι ένα σύνολο για δύο οντότητες, την Μαριέττα και τον Μάρκο.

Το Πρωτόκολλο:

1. *Η ημιομάδα S, η λέξη $w \in S$ και ένα παράγων σύνολο για κάθε ημιομάδα της $\mathcal{H}$ είναι γνωστές ή δημοσιοποιούνται.*

2. *Η Μαριέττα διαλέγει μία ιδιωτική λέξη $\alpha \in A$ που ικανοποιεί f(w,α) ≠ 1 και στέλνει f(w,α) = wα στον Μάρκο.*

3. *Ο Μάρκος διαλέγει μία ιδιωτική λέξη $\beta \in B$ που ικανοποιεί f(w,β) ≠ 1 και στέλνει f(w,β) = wβ στην Μαριέττα.*

4. *Η Μαριέττα υπολογίζει $f(w\,\beta, \alpha) = w\,\beta\alpha$ και ο Μάρκος υπολογίζει $f(w\,\alpha, \beta) = w\,\alpha\beta$. Και οι δύο ιδρύουν το $w\,\beta\alpha = w\,\alpha\beta$ ως το κοινό μυστικό κλειδί.*

□

Για αυτό τον λόγο μπορούμε να προτείνουμε τις ομάδες Artin εξαιρετικά μεγάλου τύπου ως πλατφόρμες για το CAKE.

Πρωτόκολλο Ανταλλαγής Κλειδιού που βασίζεται στις ομάδες Artin

Δημιουργία κλειδιού:

Επιλέγουμε τυχαία ένα πεπερασμένο δέντρο Γ με l στοιχεία τέτοια ώστε ο βαθμός των ριζών είναι ίσος με 2, και οι βαθμοί όλων των άλλων κορυφών να είναι ανάμεσα στο 2 και σε έναν ακέραιο m, με εξαίρεση τις ακριανές κορυφές που οι βαθμοί τους είναι 1. Σχετίζουμε το δέντρο Γ με μία ομάδα Artin ΑΓ εξαιρετικά μεγάλου τύπου βάζοντας ετικέτες με ένα γράμμα a_i σε κάθε κορυφή του Γ και αριθμώντας τις άκρες με ένα (τυχαίο) $m_{ij} \geq 4$,εάν υπάρχουν δύο αντίστοιχες κορυφές a_i και a_j προσπίπτουσες σε αυτή την άκρη.

Έστω a_k η ρίζα του δέντρου και $\Gamma_0 = \Gamma$ - a_k ένα υπογράφημα που παίρνουμε αν αφαιρέσουμε την ρίζα a_k. Το γράφημα Γ_0 αποτελείται από δύο πεπερασμένα κομματιασμένα υποδέντρα, ας πούμε, Γ_A και Γ_B που είναι συνδεδεμένα με την ρίζα a_k. Οι σχετικές υποομάδες είναι $A\Gamma_A$ και $A\Gamma_B$.

Το σύνολο των γραφημάτων των ενδομορφισμών Γ_A και Γ_B επάγουν το υπομονοειδές των ενδομορφισμών $\mathrm{End}A\Gamma_A \times End A\Gamma_B \subseteq End A\Gamma$ τέτοια ώστε για οποιοδήποτε $\alpha \in End A\Gamma_A$ και $\beta \in End A\Gamma_B$ και για τα α, β ισχύει η αντιμεταθετική ιδιότητα: $\alpha\beta = \beta\alpha$.

Έτσι ώστε και για τα δύο υπομονοείδη να επιδρούν μη τετριμμένα σε μία δημόσια λέξη $\mathrm{w} \in A\Gamma$, η λέξη θα πρέπει να περιέχει κάποια παράγοντα στοιχεία $a_1, ..., a_p \in A\Gamma_A$ και κάποια παράγοντα στοιχεία $b_1, ..., b_q \in A\Gamma_B$, δηλαδή $\mathrm{w} = \mathrm{w}(a_1, ..., a_p, b_1, ..., b_q)$.

Ανταλλαγή κλειδιού μεταθετικής δράσης για ομάδες Artin εξαιρετικά μεγάλου τύπου.

Διαλέγουμε μία τυχαία ομάδα Artin εξαιρετικά μεγάλου τύπου να είναι η πλατφόρμα S για την CAKE πλειάδα (S, T, f; $\mathcal{H}$, h) και ας είναι $\mathrm{T} = \mathrm{End}A\Gamma_A \times End A\Gamma_B$. Ορίζουμε το $\mathcal{H}$ να είναι το σύνολο $\{End A\Gamma_A, End A\Gamma_B\}$. Το πρωτόκολλο αφορά την Μαριέττα και τον Μάρκο.

Το Πρωτόκολλο:

1. Η τυχαία ομάδα ΑΓ, η λέξη $\mathrm{w} = \mathrm{w}(a_1, ..., a_p, b_1, ..., b_q) \in A\Gamma$ και ένα παράγον σύνολο για κάθε στοιχείο του $\mathcal{H}$ είναι δημόσια ή δημοσιοποιούνται.

2. Η Μαριέττα διαλέγει μία ιδιωτική λέξη $\alpha \in End A\Gamma_A$ και στέλνει f(w, α) = w^α στον Μάρκο.

3. Ο Μάρκος διαλέγει μία ιδιωτική λέξη $\beta \in End A\Gamma_B$ και στέλνει f(w, β) = w^β στην Μαριέττα.

4. Η Μαριέττα υπολογίζει f(w^β, α) = $w^{\beta\alpha}$ και ο Μάρκος υπολογίζει f(w^α, β) = $w^{\alpha\beta}$. Η Μαριέττα και ο Μάρκος θέτουν το

$$w^{\beta\alpha} = w^{\alpha\beta}$$

ως το κοινό μυστικό κλειδί.

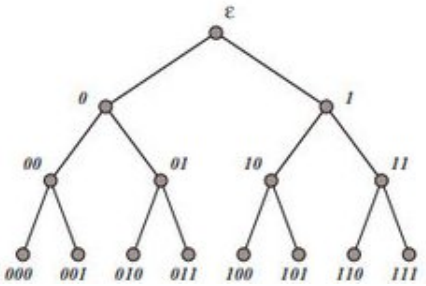
Παρατήρηση 2.47. *Η τυχαία επιλογή της ομάδας ΑΓ, έκανε την παρούσα προσέγγιση πιο δυναμική. Η τάξη των ομάδων Artin εξαιρετικά μεγάλου τύπου φαίνεται να είναι λιγότερο αλγοριθμικά ομογενής σε σχέση, ας πούμε, με την τάξη των ομάδων πλεξίδων. Γενικά, η αλγοριθμική μη-ομοιογένεια μπορεί να διαταράσσει γενικές αλγοριθμικές μεθόδους και ο αντίπαλος να αποκτήσει το ιδιωτικό κλειδί. Για παράδειγμα, ένας τυπικός ενδομορφισμός (όχι αυτομορφισμός) της ΑΓ μπορεί να συγχωνεύσει δύο τερματικές κορυφές (παιδιά) με τον ίδιο πατέρα, εάν μπερδέψει το μήκος της λέξης w. Επομένως, η επίδραση ενός τέτοιου ενδομορφισμού στο μήκος ενός στοιχείου της ομάδας δεν είναι πιο προβλέψιμη, αν γίνουν επιθέσεις μήκους.*

□

2.7 Ομάδες Grigorchuk

Σε αυτή την παράγραφο, ορίζουμε τις γνήσιες ομάδες Grigorchuk Γ. Η ομάδα Γ είναι πολύ σημαντική για πολλά θεωρητικά προβλήματα της θεωρίας ομάδων, όπως είναι η ανάπτυξη ή οι απλά πεπερασμένες ομάδες. Πρόσφατα, θεωρήθηκαν ως πιθανή πλατφόρμα για ένα κρυπτογραφικό σύστημα.

Θα ξεκινήσουμε με την παρουσίαση της ομάδας αυτομορφισμών ενός άπειρου δέντρου. Συμβολίζουμε με $\mathcal{T}$ το δέντρο αυτό. Το σύνολο T των κορυφών του $\mathcal{T}$ είναι το σύνολο των πεπερασμένων δυαδικών προτάσεων.



Ορισμός 2.48. *Επίπεδα δέντρου.*

Το σύνολο των κορυφών $L_k = \{b_1...b_k \mid b_i = 0,1\}$ *με το ίδιο μήκος* k *ονομάζονται επίπεδα (levels) στο δέντρο* $\mathcal{T}$.

□

Ένας αυτομορφισμός ϕ του $\mathcal{T}$ φτιάχνει την ρίζα ε του $\mathcal{T}$ και μεταθέτει τις κορυφές διατηρώντας την συνδεσιμότητα, δηλαδή το εάν οι κορυφές v_1 και v_2 συνδέονται από μία κορυφή του $\mathcal{T}$ τότε να συνδέονται και τα $\phi(v_1)$, $\phi(v_2)$. Είναι εύκολο να παρατηρήσουμε ότι για οποιοδήποτε k ένας αυτομορφισμός ϕ του $\mathcal{T}$ ορίζει μία μετάθεση των κορυφών στο επίπεδο L_k. Η ομάδα των αυτομορφισμών του $\mathcal{T}$ συμβολίζεται με $Aut(\mathcal{T})$.

Θεωρούμε έναν αυτομορφισμό α που έχει ειδικό ρόλο στην $Aut(\mathcal{T})$. Δημιουργεί έναν χάρτη από μία $\{0,1\}$-πρόταση σε μία $\{0,1\}$-πρόταση που αποκτάται με το να αλλάξουμε το πρώτο στοιχείο:

$$\alpha(b_1, b_2, ..., b_n) = (1 - b_1, b_2, ..., b_n).$$

Γεωμετρικά, μπορούμε να δούμε την δράση ενός αυτομορφισμού α, αν ανταλλάξουμε τα δεξιά και τα αριστερά υποδέντρα του $\mathcal{T}$. Συμβολίζουμε με St(1) μία υποομάδα των $Aut(\mathcal{T})$ που σταθεροποιεί τις κορυφές L_1. Η υποομάδα St(1) είναι κανονική του δείκτη 2 στους $Aut(\mathcal{T})$ με αριστερά (και δεξιά) σύμπλοκα (cosets) $\{1, \alpha\}$.

Ορισμός 2.49. *Ομάδα Grigorchuk.*

Η ομάδα Grigorchuk είναι μία υποομάδα των $Aut(\mathcal{T})$ *που παράγεται απο τέσσερα στοιχεία που παραδοσιακά συμβολίζονται με a, b, c, d. Το στοιχείο a το ορίσαμε παραπάνω. Οι άλλοι τρείς αυτομορφισμοί ορίζονται παρακάτω:*

$$\boldsymbol{b}\ (b_1, b_2, ..., b_n) = \begin{cases} (b_1, 1 - b_2, ..., b_n) & \text{εάν} \quad b_i = 0 \\ (b_1, c(b_2, ..., b_n)) & \text{εάν} \quad b_1 = 1 \end{cases}$$

$$\boldsymbol{c}\ (b_1, b_2, ..., b_n) = \begin{cases} (b_1, 1 - b_2, ..., b_n) & \epsilon\acute{\alpha}\nu \quad b_i = 0 \\ (b_1, d(b_2, ..., b_n)) & \epsilon\acute{\alpha}\nu \quad b_1 = 1 \end{cases}$$

$$\boldsymbol{d}\ (b_1, b_2, ..., b_n) = \begin{cases} (b_1, 1 - b_2, ..., b_n) & \epsilon\acute{\alpha}\nu \quad b_i = 0 \\ (b_1, b(b_2, ..., b_n)) & \epsilon\acute{\alpha}\nu \quad b_1 = 1 \end{cases}$$

□

Είναι εύκολο να αποδείξουμε ότι οι ορισμένοι χάρτες ανήκουν στους $Aut(\mathcal{T})$ και ότι τα a, b, c, d ∈ St(1). Το επόμενο παράδειγμα απεικονίζει τον υπολογισμό της εικόνας μίας κορυφής (δυαδική πρόταση):

$$\text{b}(1,\ 1,\ 1,\ 0,\ 1) = (1,\ \text{c}(1,\ 2,\ 0,\ 1)\ ) = (1,\ 1,\ \text{d}(1,\ 0,\ 1)\ ) =$$

$$= (1,\ 1,\ 1,\ \text{b}(0,\ 1)\ ) = (1,\ 1,\ 1,\ 0,\ 0).$$

Λήμμα 2.50. *Οι σχέσεις (relators):*

$$a^2 = b^2 = c^2 = d^2 = 1 \ \kappa\alpha\iota \ bc = cb = d$$

κρατούν τους γεννήτορες της Γ.

□

Λήμμα 2.51. *Η ομάδα* $\Gamma = \langle a, b, c, d\rangle$ *είναι ένα πηλίκο του* $(\mathbb{Z}/2\mathbb{Z}) * ((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}))$.

Απόδειξη: Από το Λήμμα 2.46 έπεται ότι μία υποομάδα $\langle b, c, d\rangle$ είναι ισόμορφη με το $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Επιπλέον, έχουμε την σχέση $a^2 = 1$. Έτσι το να χαρτογραφίσουμε την Γ από το $(\mathbb{Z}/2\mathbb{Z}) * ((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}))$, ουσιαστικά χαρτογραφούμε τον γεννήτορα του πρώτου ελεύθερου παράγοντα στο a και τους αβελιανούς γεννήτορες του δεύτερου ελεύθερου παράγοντα στο b και c, είναι επιμορφισμός.

□

Από το Λήμμα 2.46 έπεται ότι μία οποιαδήποτε λέξη w = w(a, b, c, d) είναι ίση με μία λέξη της μορφής:

$$u_0 a u_1 a u_2 ... u_{k-1} a u_k$$

όπου $u - 0, ..., u_k \in \{b, c, d\}$ και, ίσως, τα $u - 0, ..., u_k$ είναι τετριμμένα.

Ορισμός 2.52. *Μειωμένη λέξη.*

Μία λέξη του τύπου

$$u_0 a u_1 a u_2 ... u_{k-1} a u_k$$

ονομάζεται μειωμένη.

□

Λήμμα 2.53. *Μία λέξη w = w(a, b, c, d) απεικονίζει ένα στοιχείο του St(1), αν και μόνο αν όλο το πλήθος ενός συμβόλου είναι άρτιο (ή όμοιο). Επιπλεόν, η υποομάδα St(1) της Γ παράγεται από έξι στοιχεία* $\{b, c, d, aba, aca, ada\}$.

Απόδειξη: Προκύπτει άμεσα από τον ορισμό των στοιχείων a, b, c και d.

□

Μία λέξη που αντιπροσωπεύει ένα στοιχείο της St(1) μπορεί να γραφτεί ως γινόμενο των γεννητόρων της St(1) με την παρακάτω μορφή:

$$u_0 \cdot (a u_1 a) \cdot u_2 \cdot (a u_3 a) \cdot u_4 \cdot ... \cdot (a u_{k-3} a) \cdot u_{k-2} \cdot (a u_{k-1} a) \cdot u_k$$

όπου $u_0, ..., u_k \in \{b, c, d\}$ και τα u_0, u_k είναι, ίσως, τετριμμένα. Εφόσον οποιοδήποτε στοιχείο ϕ της St(1) συμπεριφέρεται τετριμμένα στο πρώτο επίπεδο του δέντρου $\mathcal{T}$ έπεται ότι το ϕ μπορεί να αναπαραστεί ως ένα ζευγάρι (ϕ_0, ϕ_1), όπου ϕ_0, ϕ_1 είναι αυτομορφισμοί των δεξιών και αριστερών υποδέντρων του $\mathcal{T}$ αντίστοιχα. Είναι εύκολο, λοιπόν, να ελέγξουμε ότι:

$$\text{b} = (\text{a, c}),\ \text{aba} = (\text{c, a}),$$

$$\text{c} = (\text{a, d}),\ \text{aca} = (\text{d, a}),$$

$$\text{d} = (1, \text{b}),\ \text{ada} = (\text{b, } 1),$$

Συμβολίζουμε τις σχέσεις αυτές με (1).

Επιπλέον, εάν u,v $\in$ St(1) και u $= (u_0, u_1)$ και v $= (v_0, v_1)$, τότε:

$$uv = (u_0 v_0, u_1 v_1).$$

Λήμμα 2.54. *Έστω w = w(a, b, c, d)* $\in$ *St(1) μία μειωμένη λέξη και* $w = (w_0, w_1)$. *Τότε:*

$$\mid w_0 \mid, \mid w_1 \mid \leq \frac{|w|+1}{2}.$$

Επιπλέον, εάν η w ξεκινάει με ένα σύμβολο a, τότε $\mid w_0 \mid, \mid w_1 \mid \leq \frac{|w|}{2}$.

Απόδειξη: Οποιαδήποτε λέξη w $\in$ St(1) μπορεί να γραφεί ως γινόμενο. Αν χρησιμοποιήσουμε τον τύπο (1) και τον τύπο $uv = (u_0v_0, u_1v_1)$ τότε είναι εύκολο να ελέγξουμε και τις δύο ανισότητες.

□

Αλγόριθμος 6 (Πρόβλημα Ταυτότητας για την Γ)

INPUT. Μία μειωμένη λέξη w = w(a, b, c, d).

OUTPUT. *Αληθές*, αν η w αντιπροσωπεύει την ταυτότητα της Γ. Διαφορετικά, *Ψευδές*.

ΥΠΟΛΟΓΙΣΜΟΙ.

A. Εάν $\mid w \mid = 0$, τότε η έξοδος είναι *Αληθές*. Εάν $\mid w \mid = 1$, τότε η έξοδος είναι *Ψευδές*.

B. Κυκλικά μεταθέτουμε την w έτσι ώστε να ξεκινά με το σύμβολο α.

Γ. Υπολογίζουμε το αλγεβρικό άθροισμα των δυνάμεων του α στην w. Εάν είναι παράξενο, τότε η έξοδο είναι *Ψευδές*.

Δ. Επαναγράφουμε την w ως γινόμενο των στοιχείων b, c, d, aba, aca, ada και χρησιμοποιούμε τον τύπο (1) για να βρούμε το αντίστοιχο (w_0, w_1).

E. Αναδρομικά ελέγχουμε εάν τα w_0 και w_1 αντιπροσωπεύουν την ταυτότητα της Γ. Τότε η έξοδος είναι *Αληθές*. Διαφορετικά, η έξοδος είναι *Ψευδές*.

Θεώρημα 2.55. *Ο Αλγόριθμος 6 λύνει το Πρόβλημα Ταυτότητας για την ομάδα Grigorchuk Γ σε χρόνο* $O(\mid w \mid log \mid w \mid)$.

Απόδειξη:

Μία λέξη w αντιπροσωπεύει την ταυτότητα της Γ, αν και μόνο αν ανήκει στην St(1) και επιδρά τετριμμένα στο αριστερό και δεξί υποδέντρο της $\mathcal{T}$. Επομένως, ο αλγόριθμος που λύνει το Πρόβλημα Ταυτότητας πρέπει να ξεκινάει με τον έλεγχο: αν w $\in$ St(1). Αν ισχύει, επαναγράφει την w ως γινόμενο των στοιχείων b, c, d, aba, aca, ada. Τότε χρησιμοποιεί τις ισότητες (1), για να υπολογίσει τα στοιχεία (w_0, w_1) περιγράφοντας

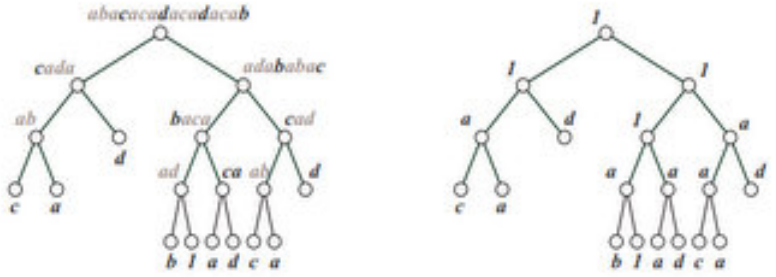
την δράση στα υποδέντρα και ελέγχει εάν αντιπροσωπεύουν τις ταυτότητες. Επομένως, ο Αλγόριθμος 6 λύνει σωστά το Πρόβλημα Ταυτότητας για την Γ.

Για μία λέξη w, ο Αλγόριθμος 6 εκτελεί τα βήματα Α-Δ σε γραμμικό χρόνο O(| w |). Στο Βήμα Ε καταλήγουμε με δύο λέξεις τις w_0 και w_1, όπου κάθε μίας το μήκος είναι λιγότερο από $\frac{|w|}{2}$ και αναδρομικά τρέχει την ίδια διαδικασία για τα w_0 και w_1.

Ο ολικός χρόνος πολυπλοκότητας των Βημάτων Α-Δ για τις λέξεις w_0 και w_1 είναι O(| w_0 |) + O(| w_1 |). Στο βήμα Δ χωρίζουμε τα w_0 και w_1 και αποκτάμε τέσσερις νέες λέξεις. Ο χρόνος πολυπλοκότητας των Βημάτων Α-Δ για αυτές τις λέξεις είναι φραγμένος από το O(| w |) ξανά. Αυτό συνεχίζεται μέχρι να πάρουμε λέξεις μήκους 0 και 1 για τις οποίες ξέρουμε την απάντηση. Εφόσον κάθε φορά χωρίζουμε τις λέξεις σε δύο κομμάτια καθένα απο τα δύο δεν είναι μεγαλύτερο από το μισό της αρχικής λέξης, έπεται ότι σε log_2 | w | βήματα καταλήγουμε σε λέξεις μήκους είτε 0 είτε 1. Για αυτό το λόγο η ολική πολυπλοκότητα τις διαδικασίας είναι φραγμένη από το O(| w | log_2 | w |).

□

Αν κάποιος βασιστεί στον Αλγόριθμο 6 μπορεί να διαμορφώσει την διαδικασία για να κατασκευάσει κανονικές μορφές των στοιχείων της Γ. Η κανονική μορφή ρ_w ενός στοιχείου w ∈ Γ είναι ένα πεπερασμένο δέντρο με ετικέτες, που είναι τα στοιχεία $\{1, a, b, c, d\} \in \Gamma$, στις κορυφές του.



Μία κανονική μορφή των στοιχείων abacacadacadacab. Το δέντρο στα αριστερά απεικονίζει την διαδικασία του υπολογισμού των κανονικων μορφών.

Το δέντρο ρ_w για μία λέξη w = w(a, b, c, d) μπορεί να κατασκευαστεί όπως παρακάτω:

- Χρησιμοποιώντας τον Αλγόριθμο 6 ελέγχουμε αν η w είναι ίση με 1, a, b, c, d

στην Γ. Αν ισχύει, τότε το ρ_w περιέχει μία κορυφή με ετικέτα με το αντίστοιχο σύμβολο.

- Εάν η w δεν είναι ίση με 1, a, b, c, d στην Γ, τότε:
  - Εάν w $\in$ St(1) και w $= (w_0, w_1)$, τότε ρ_w είναι ένα δέντρο με μία ρίζα με ετικέτα το 1, το αριστερό υποδέντρο είναι το ρ_{w_0} και το δεξί υποδέντρο είναι το ρ_{w_1}.
  - Εάν w $\notin$ St(1) και wa $= (w_0, w_1)$, τότε ρ_w είναι ένα δέντρο με μία ρίζα με ετικέτα το a, το αριστερό υποδέντρο είναι το ρ_{w_0} και το δεξί υποδέντρο είναι το ρ_{w_1}.

Πρόταση 2.56. *Έστω $u = u(a, b, c, d)$ και $v = v(a, b, c, d)$. Οι λέξεις u και v απεικονίζουν τα ίδια στοιχεία της Γ αν και μόνο αν $\rho_u = \rho_v$.*

□

Θεώρημα 2.57. *Υπάρχει αλγόριθμος που για οποιαδήποτε λέξη $w = w(a, b, c, d)$ κατασκευάζει την αντίστοιχη κανονική μορφή ρ_w σε χρόνο $O(\mid w \mid log_2 \mid w \mid)$.*

□

Κεφάλαιο 3

Βιβλιογραφία

[1] N. Koblitz and A. Menezes, A survey of public-key cryptosystems, SIAM , εκδόθηκε Review 46 (2004), σελ. 599–634.

[2] W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans , εκδόθηκε Inf. Theory 22 (1976), σελ. 644–654.

[3] R. L. Rivest, A. Shamir, and L. Adleman, On Digital Signatures and Public Key Cryptosystems, Commun , εκδόθηκε Ass. Comp. Mach. 21 (1978), σελ. 120–126.

[4] P.W. Shor, Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer , εκδόθηκε SIAM J. Comp. 26(5) (1997), σελ. 1484–1509.

[5] D. Aharonov, Quantum computation, Annual Review of Computational Physics , εκδόθηκε World Scientific, Volume VI, (Dietrich Stauffer, ed.) (1998), σελ. 259–346.

[6] Groups of Intermediate Growth, an Introduction, Rostislav Grigorchuk and Igor Pak, εκδόθηκε April 4, 2008. σελ. 2-3.

[7] Θεωρία Ομάδων, Α. Πάπιστας, Τμήμα Μαθηματικών, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, εκδοσεις Ζήτης.

[8] Tripartite Key Agreement Protocol using Triple Decomposition Search Problem, T.Isaiyarasi and Dr.K.Sankarasubramanian , εκδόθηκε International

Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.

[9] Mean-Set Attack: Cryptanalysis of Sibert et al. Authentication Protocol, Natalia Mosina and Alexander Ushakov, εκδόθηκε June 25, 2010.

[10] Encyclopedia of Operations Research and Management Science , Saul I. Gass and Carl M. Harris, εκδόθηκε 2001.

[11] Braid Group Cryptography, David Garber, εκδόθηκε στο Lecture notes of Tutorials, June 2007.

[12] Thompson's group and public key cryptography, Vladimir Shpilrain and Alexander Ushakov, εκδόθηκε May 2005.

[13] Combinatorial Group Tgeory and Public Key Cryptography, Vladimir Shpilrain and Gabriel Zapata, εκδόθηκε June 2004.

[14] Anshel, Anshel, and Goldfeld, An algebraic method for public key cryptography, εκδόθηκε (1999), σελ. 287-291.

[15] Anshel, Anshel, Goldfeld, and S. Lemieux, Key Agreement, T he Algebraic EraserTM, and Lightweight Cryptography. Algebraic Methods in Cryptography, Contemporary M athematics 418, εκδόθηκε American Mathematical Society, 2006, σελ. 1-34.

[16] Appel and Schupp, Artin groups and inf inite Coxeter groups, εκδόθηκε Invent.Math. 72 (1983), σελ. 201-220.

[17] Arzhantseva and Olshanskii, Genericity of the class of groups in which subgroups with a lesser number of generators are free, εκδόθηκε (Russian) M at. Zametki 59 (1996), σελ. 489-496.

Ευρετήριο