Μη - Μεταθετική Κρυπτογραφία επί Ομάδων

Παναγόπουλος Βασίλειος, Α.Μ. 163101

Επιβλέπων Καθηγητής: Βάρσος Δημήτριος

Μεταπτυχιακή Διπλωματική Εργασία
Π.Μ.Σ. - Θεωρητικά Μαθηματικά, Τμήμα Μαθηματικών

ΕΘΝΙΚΟ και ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
Αθήνα 2019

Η εργασία εγκρίθηκε στις 12/09/2019 από την Τριμελή Εξεταστική Επιτροπή
την οποία αποτελούν οι:

1. Βάρσος Δημήτριος, Καθηγητής Τμήματος Μαθηματικών, Ε.Κ.Π.Α.

2. Ράπτης Ευάγγελος, Καθηγητής Τμήματος Μαθηματικών, Ε.Κ.Π.Α.

3. Συκιώτης Μιχαήλ, Επίκουρος Καθηγητής Τμήματος Μαθηματικών, Ε.Κ.Π.Α.

Η εργασία είναι αφιερωμένη
στην οικογένειά μου

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ.Βάρσο Δημήτριο για την καθοδήγηση και τη βοήθεια που μου παρείχε τόσο κατά τη μελέτη του αντικειμένου όσο και κατά τη συγγραφή της εργασίας. Επιπλέον, αξίζει να γίνει ιδιαίτερη αναφορά στο χρόνο που αφιέρωσε καθώς και στο γενικότερο ζήλο τον οποίο επέδειξε καθόλη τη διάρκεια της συνεργασίας μας. Ευχαριστώ επίσης τα υπόλοιπα μέλη της επιτροπής, κκ.Ράπτη Ευάγγελο και Συκιώτη Μιχαήλ.

Περιεχόμενα

Πρόλογος

Η Κρυπτογραφία είναι ένας ιδιαίτερα σημαντικός κλάδος της επιστήμης, ο οποίος βρίσκεται σε άνθιση σε παγκόσμιο επίπεδο. Αυτή ακριβώς η άνθιση οφείλεται στις υπηρεσίες τις οποίες παρέχει στις σύγχρονες κοινωνίες. Ποιες, όμως, είναι αυτές οι υπηρεσίες;

Καθημερινά ερχόμαστε σε επαφή με σύγχρονες τεχνολογίες, με την πιο διαδεδομένη να είναι το διαδίκτυο. Σε αυτό, βλέπουμε διαρκώς όρους όπως: $username$, κωδικός, PIN, πιστοποιητικό ασφαλείας κλπ. Όλες αυτές οι έννοιες είναι απλά εφαρμογές των λεγόμενων πρωτοκόλλων κρυπτογράφησης. Ποια είναι λοιπόν η χρησιμότητα αυτών των πρωτοκόλλων; Η εργασία η οποία επιτελούν είναι το να μας εγγυώνται ασφάλεια σε διάφορες εργασίες που εκτελούμε.

• Για παράδειγμα, όταν επισκεπτόμαστε μία ιστοσελίδα, είναι πολύ σημαντικό να γνωρίζουμε ότι αυτή η ιστοσελίδα είναι πράγματι αυτή που φαίνεται να είναι και όχι κάποια άλλη. Αυτή η λειτουργία ίσως φανεί ανούσια εκ πρώτης όψεως, όμως καταλαβαίνει κανείς τη σημασία όταν επισκεφθεί την ιστοσελίδα μίας τράπεζας όπου και ενδέχεται να διατηρεί ηλεκτρονικό τραπεζικό λογαριασμό.

• Κάθε φορά που συνδεόμαστε σε κάποιο λογαριασμό που ενδεχομένως διατηρούμε (τραπεζικό, $e-mail$ κλπ.) θέλουμε να είμαστε οι μόνοι που να μπορούμε να το κάνουμε.

• Κάθε πληροφορία που μεταβιβάζεται από τον υπολογιστή μας με προορισμό κάποιο δέκτη, περνάει αναγκαστικά από $servers$ οι οποίοι απλά την αποθηκεύουν χωρίς να εξασφαλίζουν όμως και την ιδιωτικότητά της απέναντι σε μη εξουσιοδοτημένα άτομα. Έτσι, τα πρωτόκολλα φροντίζουν αρχικά να κρυπτογραφήσουν αυτήν την πληροφορία και στη συνέχεια να βεβαιωθούν για την

ταυτότητα του δέκτη προκειμένου να ολοκληρωθεί η μεταφορά δεδομένων.

Στην παρούσα εργασία, θα δούμε κάποια σημαντικά πρωτόκολλα. Θα αναλύσουμε τη λειτουργία τους καθώς και τις μαθηματικές ιδιότητες επάνω στις οποίας εδράζεται η ασφάλειά τους. Φυσικά, θα δούμε και μεθόδους με τις οποίες μπορεί να επιτεθεί κανείς προκειμένου να υποκλέψει πληροφορίες - η διαδικασία είναι γνωστή ως 'κρυπτανάλυση' . Η μελέτη μας θα ξεκινήσει με ένα εισαγωγικό κεφάλαιο το οποίο παρέχει το απαραίτητο αλγεβρικό υπόβαθρο καθώς και διάφορα άλλα προαπαιτούμενα.

Η ορολογία που χρησιμοποιούμε έχει ως εξής: οι νόμιμοι συναλλασσόμενοι ονομάζονται Αλίκη και Βασίλης (στην ξενόγλωσση βιβλιογραφία $Alice$ και Bob) ενώ ο υποκλοπέας ονομάζεται Εύα (αντίστοιχα Eve).

Τέλος, θα αναφέρουμε ότι η παρούσα εργασία έχει αποκλειστικά βιβλιογραφικό χαρακτήρα, δηλαδή βασίζεται εξ ολοκλήρου σε πηγές. Τα τμήματα της εργασίας τα οποία δεν έχουν επισημανθεί με παραπομπή προέρχονται ουσιαστικά απευθείας από το κείμενο του βιβλίου $Group - based\ Cryptography$ των $Myasnikov$, $Shpilrain$ και $Ushakov$.

Παναγόπουλος Βασίλειος
Αθήνα, Σεπτέμβριος 2019

Περίληψη

Σε αυτήν την εργασία, μελετάμε το αντικείμενο της μη-μεταθετικής κρυπτογραφίας επί ομάδων και το ενδιαφέρον μας είναι εστιασμένο κυρίως σε πρωτόκολλα ανταλλαγής κλειδιού και ταυτοποίησης.

Στο πρώτο κεφάλαιο εισάγουμε βασικά στοιχεία σχετικά με τη θεωρία ομάδων, όπως είναι οι ελεύθερες ομάδες και οι παραστάσεις ομάδων, καθώς επίσης και τα πιο συνηθισμένα προβλήματα του αντικειμένου τα οποία αποτελούν τον συνδετικό κρίκο ανάμεσα στη θεωρία ομάδων και την κρυπτογραφία.

Στο δεύτερο κεφάλαιο μελετάμε μερικά από τα πιο γνωστά πρωτόκολλα ανταλλαγής κλειδιού και ταυτοποίησης. Αυτή η μελέτη περιλαμβάνει όχι μόνο την αλγοριθμική πλευρά των προαναφερθέντων πρωτοκόλλων αλλά επίσης και τα θέματα που αφορούν την ασφάλειά τους.

Στο τρίτο κεφάλαιο παρουσιάζουμε συγκεκριμένα είδη ομάδων τα οποία μπορούν να χρησιμοποιηθούν ως πλατφόρμες σε ποικίλα πρωτόκολλα και αναλύουμε τα ιδιαίτερα χαρακτηριστικά τους.

Στο τέταρτο κεφάλαιο, το οποίο είναι και το πιο σημαντικό μέρος της εργασίας, διεξάγουμε μια σε βάθος μελέτη του πρωτοκόλλου *Shpilrain - Zapata*.

Abstract

In this thesis, we study the subject of non-commutative cryptography over groups and our interest is mainly focused on key-exchanging and identification protocols.

In chapter one, we introduce basic elements concerning group theory, such as free groups and group presentations, as well as the most common problems of the subject which are a direct link between group theory and cryptography.

In chapter two, we study some of the most well known key-exchanging and identification protocols. This study includes not only the algorithmic side of the aforementioned subjects, but also the side that concerns security.

In chapter three, we present families of groups that can be used as platforms for various protocols and we also analyse their specific characteristics.

In chapter four, which is the most important part of this thesis, we make an in-depth study of the Shpilrain-Zapata protocol.

Κεφάλαιο 1

Βασικές Έννοιες

1.1 Ελεύθερες Ομάδες

Ορισμός: Έστω X μη κενό σύνολο. Μία ομάδα F λέγεται ελεύθερη επί του X αν έχουμε μία απεικόνιση $s : X \to F$ με την ιδιότητα: για κάθε ομάδα G και για κάθε απεικόνιση $a : X \to G$ υπάρχει ομομορφισμός ομάδων β: $F \to G$ έτσι ώστε να ισχύει ότι β$o s$=α.

Αποδεικνύεται ότι η απεικόνιση s είναι ένα προς ένα.

Θεώρημα: Έστω G ομάδα και X ένα σύνολο γεννητόρων της. Έστω F ελεύθερη επί του X. Τότε ισχύει ότι $G \simeq F/ker\beta$, όπου β είναι ο αντίστοιχος (με βάση τα παραπάνω) ομομορφισμός με πεδίο ορισμού την F και πεδίο τιμών την G.

Από το θεώρημα έπεται ότι κάθε ομάδα μπορεί να γραφεί ως πηλίκο κάποιας ελεύθερης ομάδας.

Όμως, το ερώτημα, το οποίο εύλογα μπορεί να θέσει κανείς, είναι το κατά πόσο υπάρχουν ελεύθερες ομάδες. Θα δείξουμε κατασκευαστικά ότι πράγματι υπάρχουν. Ο λόγος για τον οποίο θα παραθέσουμε την κατασκευή είναι για να βοηθήσει τον αναγνώστη να κατανοήσει καλύτερα έννοιες όπως αλφάβητο, λέξη κλπ.

• Έστω X μη κενό σύνολο. Θα δείξουμε ότι υπάρχει ομάδα F ελεύθερη επί του X.

Έστω X^{-1} ένα σύνολο έτσι ώστε $|X| = |X^{-1}|$ και $X \cap X^{-1} = \emptyset$.

Το σύνολο $X \cup X^{-1}$ ονομάζεται αλφάβητο. Έστω $S = \{x_{i_1}^{e_1} \cdots x_{i_k}^{e_k} | x_{i_j} \in X, e_j = \pm 1\}$ όπου το στοιχείο $x_t^{-1} \in X^{-1}$ είναι ο τυπικός αντίστροφος του x_t, δηλαδή οι αρνητικοί εκθέτες έχουν συμβολικό χαρακτήρα.

Ως πράξη στο S ορίζουμε την παράθεση των λέξεων, δηλαδή αν $u = x_{i_1}^{e_1} \cdots x_{i_k}^{e_k}$ και $v = y_{i_1}^{\epsilon_1} \cdots y_{i_t}^{\epsilon_t}$ είναι δύο στοιχεία του S, τότε $u \cdot v = x_{i_1}^{e_1} \cdots x_{i_k}^{e_k} y_{i_1}^{\epsilon_1} \cdots y_{i_t}^{\epsilon_t}$. Προφανώς, η πράξη είναι προσεταιριστική.

Επίσης, στο S επισυνάπτουμε την κενή λέξη 1.

Στο S θα ορίσουμε μια σχέση ισοδυναμίας ως εξής: $u \sim v$ αν από τη u μεταβαίνουμε στη v εισάγοντας ή διαγράφοντας τμήματα της μορφής $x \cdot x^{-1}$ ή $x^{-1} \cdot x$.

Στο σύνολο $S/\sim = \{[u], u \in S\}$ ορίζουμε μία πράξη ως εξής: $[u][v] = [uv]$. Είναι αρκετά σαφές ότι η πράξη είναι καλά ορισμένη με την έννοια ότι δεν εξαρτάται από τους αντιπροσώπους της κάθε κλάσης. Προφανώς, ισχύει ότι $[x][x^{-1}] = [x^{-1}][x] = [1]$.

Καταλήγουμε στις εξής ιδιότητες:

1. Η πράξη στην $S/\sim$ είναι προσεταιριστική.
2. Η [1] αποτελεί το ουδέτερο στοιχείο της πράξης.
3. Έστω $u \in S$ $u = x_{i_1}^{e_1} \cdots x_{i_k}^{e_k}$. Τότε, η λέξη $u^{-1} = x_{i_k}^{-e_k} \cdots x_{i_1}^{-e_1}$ έχει την ιδιότητα: $[u][u^{-1}] = [u^{-1}][u] = [1]$.

Άρα, το σύνολο $S/\sim$ με την πράξη που ορίσαμε είναι ομάδα.

Ορισμός: Μία λέξη $v \in S$ θα ονομάζεται ανηγμένη αν στη γραφή της δεν εμφανίζονται τμήματα της μορφής $x_{i_j}^{e_j} x_{i_{j+1}}^{e_{j+1}}$ με $x_{i_j} = x_{i_{j+1}}$ και $e_j = -e_{j+1}$.

Προφανώς, σε κάθε κλάση υπάρχει μοναδική ανηγμένη λέξη.

Ορισμός: Μήκος της κλάσης (ή ανηγμένο μήκος) ονομάζεται το μήκος της μοναδικής ανηγμένης λέξης της κλάσης.

Έστω X και $F = S/\sim$ όπως ορίστηκαν παραπάνω, η απεικόνιση $i : X \to F$ με $i(x_i) = [x_i]$, G ομάδα και απεικόνιση $a : X \to G$. Ορίζουμε την απεικόνιση $\beta : F \to G$ ως $\beta([x_i]) = a(x_i)$ για κάθε $x_i \in X$, η οποία προφανώς είναι ομομορφισμός. Τότε, προκύπτει άμεσα ότι η F είναι ελεύθερη ομάδα επί του X καθώς ισχύει η σύνθεση $\beta \circ i = a$. Άρα, αποδείξαμε την ύπαρξη των ελεύθερων ομάδων επί συνόλου.

1.2 Παραστάσεις Ομάδων

Στην προηγούμενη παράγραφο είδαμε ότι κάθε ομάδα μπορεί να γραφεί ως πηλίκο ελεύθερης ομάδας. Πιο συγκεκριμένα, $G \simeq F(X)/ker\beta$.

Από τον ορισμό της, η F είναι πλήρως καθορισμένη από τον πληθικό αριθμό των γεννητόρων της. Αντίστοιχα, η ομάδα $ker\beta$ μπορούμε να πούμε ότι προσδιορίζεται πλήρως από το σύνολο των κανονικών γεννητόρων της, έστω R. Τα στοιχεία του συνόλου R ονομάζονται ορίζουσες σχέσεις της ομάδας G σε σχέση με το X.

Με βάση τα όσα μόλις είπαμε, είναι σαφές ότι μπορούμε να γράψουμε την ομάδα G σε μία μορφή πολύ πρακτική: $G = \langle X|R\rangle$. Αυτή η μορφή ονομάζεται παράσταση της ομάδας G και είναι μοναδική ως προς ισομορφισμό. Αν τα σύνολα X και R είναι πεπερασμένα, τότε η παράσταση ονομάζεται πεπερασμένη. Ανάλογα, μία ομάδα ονομάζεται πεπερασμένα παριστώμενη αν έχει πεπερασμένη παράσταση.

Μερικά κλασσικά παραδείγματα πεπερασμένα παριστώμενων ομάδων είναι όλες οι πεπερασμένα παραγόμενες αβελιανές ομάδες, οι πεπερασμένα παραγόμενες μηδενοδύναμες ομάδες, οι *braid groups* και η ομάδα *Thompson*.

1.3 Τα Κύρια Προβλήματα

Τα προβλήματα τα οποία θα αντιμετωπίσουμε σε αυτήν την εργασία είναι δύο ειδών:

1. Τα προβλήματα απόφασης είναι προβλήματα κατά τα οποία καλούμαστε να απαντήσουμε στο κατά πόσο, δοθείσας ιδιότητας Α και στοιχείου Β, το Β έχει την ιδιότητα Α.
2. Τα προβλήματα έρευνας είναι προβλήματα κατά τα οποία καλούμαστε να βρούμε στοιχεία με την ιδιότητα Γ, δεδομένου ότι τέτοια στοιχεία υπάρχουν.

Στη συνέχεια, θα αναφερθούμε σε συγκεκριμένα προβλήματα τα οποία εμφανίζονται στον κλάδο της κρυπτογραφίας και τα οποία εντάσσονται στις παραπάνω δύο κατηγορίες.

1.3.1 Το Πρόβλημα Λέξης

Το πρόβλημα λέξης είναι το εξής:

• Έστω ότι δίνονται μία αναδρομική παράσταση κάποιας ομάδας G καθώς και ένα στοιχείο $g \in G$. Υπάρχει αλγόριθμος ο οποίος μπορεί να αποφανθεί για το αν ισχύει ότι $g = 1_G$?

Ένα σημαντικό θεώρημα είναι το εξής: Αν μία ομάδα έχει δοθεί με τη μορφή αναδρομικής παράστασης τότε η θετική πλευρά στο παραπάνω πρόβλημα έχει αναδρομική λύση. Επίσης, υπάρχει το εξής αποτέλεσμα:

Πρόταση: Έστω $\langle X|R\rangle$ μία αναδρομική παράσταση μίας ομάδας G. Τότε, το σύνολο των λέξεων $g \in G$ με την ιδιότητα $g = 1_G$ είναι αναδρομικά απαριθμήσιμο.

Για να είναι πιο σαφές το τι ακριβώς εννοούμε με τον όρο 'αναδρομικά απαριθμήσιμο', αναφέρουμε το εξής, προερχόμενο από αντίστοιχο λήμμα της ιστοσελίδας *wikipedia*:

Έστω Σ ένα σύνολο φυσικών αριθμών. Λέμε ότι το Σ είναι αναδρομικά απαριθμήσιμο αν υπάρχει ένας αλγόριθμος ο οποίος να απαριθμεί τα στοιχεία του Σ. Αυτό σημαίνει ότι το αποτέλεσμα του αλγορίθμου θα είναι ακριβώς τα στοιχεία του Σ. Ο αλγόριθμος μπορεί να μην τερματίζει ποτέ.

Το πρόβλημα έρευνας λέξης είναι το εξής: Έστω ότι δίνονται μία αναδρομική παράσταση μιας ομάδας G καθώς και ένα στοιχείο τέτοιο ώστε $g = 1_G$. Να γραφεί το g ως γινόμενο συζυγών - και των αντιστρόφων τους - οριζουσών σχέσεων της ομάδας.

Το πρόβλημα έρευνας λέξης έχει πάντοτε αναδρομική λύση καθώς υπάρχει η δυνατότητα αναδρομικής απαρίθμησης όλων των εμπλεκόμενων στοιχείων βάσει της πρότασης που αναφέραμε.

Πρέπει όμως να αναφέρουμε ότι το πλήθος αυτών των παραγόντων μπορεί να είναι πολύ μεγαλύτερο από το μήκος της ίδιας της λέξης. Μάλιστα, υπάρχουν ομάδες στις οποίες το πρόβλημα λέξης επιλύεται αποτελεσματικά, όπου στοιχεία μήκους n που παριστούν τη μονάδα, μπορούν να έχουν πλήθος παραγόντων (όπως αυτοί αναφέρθηκαν παραπάνω) το οποίο δεν φράσσεται από διαδοχικούς εκθέτες n. Τέλος, θα προσθέσουμε ότι εάν σε μία ομάδα το πρόβλημα λέξης δεν επιλύεται αναδρομικά, τότε το μήκος της απόδειξης που επιβεβαιώνει ότι κάποια λέξη είναι ίση με το μοναδιαίο στοιχείο, δεν είναι φραγμένη από καμία αναδρομική συνάρτηση του μήκους της λέξης.

1.3.2 Το Πρόβλημα Συζυγίας

Το πρόβλημα συζυγίας είναι το εξής: έστω ότι δίνονται αναδρομική παράσταση ομάδας G και στοιχεία $g, h \in G$. Υπάρχει αλγόριθμος ο οποίος μπορεί να αποφανθεί για το αν τα δύο στοιχεία είναι συζυγή?

Σε αυτό το σημείο θα επαναλάβουμε αυτό που είπαμε και για το πρόβλημα λέξης: μπορούμε να απαντήσουμε καταφατικά με αναδρομικό τρόπο καθώς μπορεί κανείς να απαριθμήσει αναδρομικά όλα τα συζυγή ενός στοιχείου.

Το πρόβλημα έρευνας συζυγίας είναι το εξής: έστω ότι δίνονται αναδρομική παράσταση ομάδας G και δύο συζυγή στοιχεία $g, h \in G$. Βρείτε στοιχείο x τέτοιο ώστε $x^{-1}gx = h$.

Και σε αυτήν την περίπτωση η επίλυση είναι αναδρομική, αλλά όπως και στο πρόβλημα έρευνας λέξης, αυτού του είδους η επίλυση μπορεί να γίνει ιδιαίτερα αναποτελεσματική.

1.3.3 Το Πρόβλημα Αποδόμησης

Το πρόβλημα έρευνας αποδόμησης είναι το εξής: έστω ότι δίνονται η αναδρομική παράσταση ομάδας, δύο αναδρομικά παραγόμενες υποομάδες της A, B και δύο στοιχεία $g, h \in G$. Βρείτε δύο στοιχεία $x \in A$, $y \in B$ τέτοια ώστε $x \cdot g \cdot y = h$, δεδομένου ότι υπάρχει ένα τέτοιο ζεύγος.

Γενικά, ζεύγος το οποίο ικανοποιεί το ζητούμενο γινόμενο πάντοτε υπάρχει $(x = 1, y = g^{-1}h)$. Άρα, η ουσία του προβλήματος έγκειται στο να εντοπίσουμε στοιχεία εντός των υποομάδων που μας ενδιαφέρουν. Συνεπώς, από εδώ και στο εξής θα αναφερόμαστε στο πρόβλημα ως 'το πρόβλημα έρευνας αποδόμησης υπό τον περιορισμό επί υποομάδων'.

Η περίπτωση όπου ισχύει ότι A=B, είναι το γνωστό πρόβλημα 'διπλού συμπλόκου'.

1.3.4 Το Πρόβλημα Παραγοντοποίησης

Το πρόβλημα που θα αναφέρουμε σε αυτήν την παράγραφο ναι μεν έχει ιδιαίτερο όνομα αλλά, επί της ουσίας, αποτελεί ειδική περίπτωση του προβλήματος

έρευνας αποδόμησης για $g = 1$.

Το πρόβλημα παραγοντοποίησης είναι το εξής: έστω ότι δίνονται ένα στοιχείο w μιας αναδρομικά παριστώμενης ομάδας G και δύο υποομάδες $A, B \leq G$. Υπάρχει αλγόριθμος ο οποίος μπορεί να αποφανθεί για το αν υπάρχουν στοιχεία $a \in A$ και $b \in B$ τέτοια ώστε $a \cdot b = w$?

Το πρόβλημα έρευνας παραγοντοποίησης είναι το εξής: έστω ότι δίνονται ένα στοιχείο w μιας αναδρομικά παριστώμενης ομάδας G και δύο αναδρομικά παραγόμενες υποομάδες $A, B \leq G$. Βρείτε δύο στοιχεία $a \in A$ και $b \in B$ τέτοια ώστε $a \cdot b = w$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος.

Με βάση τα όσα έχουμε αναφέρει, μπορούμε να πούμε ότι τα διάφορα προβλήματα σχετίζονται μεταξύ τους. Πράγματι, σε αυτό το σημείο θα αναφέρουμε μία πρόταση η οποία διατυπώνει αυτές τις σχέσεις με σαφήνεια.

Πρόταση: Έστω G μία αναδρομικά παριστώμενη ομάδα. Τότε, ισχύουν τα εξής:

1. Αν το πρόβλημα συζυγίας στην G είναι επιλύσιμο, τότε και το πρόβλημα λέξης είναι επιλύσιμο.

2. Αν το πρόβλημα έρευνας συζυγίας στην G είναι επιλύσιμο, τότε το πρόβλημα έρευνας αποδόμησης είναι επιλύσιμο για μετατιθέμενες υποομάδες A, B.

3. Αν το πρόβλημα έρευνας συζυγίας στην G είναι επιλύσιμο, τότε το πρόβλημα έρευνας παραγοντοποίησης είναι επιλύσιμο για μετατιθέμενεες υποομάδες A, B.

1.3.5 Το Πρόβλημα Μέλους

Το πρόβλημα μέλους είναι το εξής: έστω ότι δίνονται μία αναδρομικά παριστώμενη ομάδα G, μία υπομάδα $H \leq G$ η οποία παράγεται από τα στοιχεία $h_1, ..., h_k$ καθώς και ένα στοιχείο $g \in G$. Υπάρχει αλγόριθμος ο οποίος μπορεί να αποφανθεί για το αν ισχύει ότι $g \in H$?

Η καταφατική απάντηση του προβλήματος είναι πάντοτε αναδρομική καθώς μπορεί κανείς να απαριθμήσει αναδρομικά όλα τα στοιχεία μιας υποομάδας παραγόμενης από πεπερασμένα το πλήθος στοιχεία. Σε αυτό το σημείο, θα αναφέρουμε ότι το πρόβλημα μέλους καλείται επίσης και 'γενικευμένο πρόβλημα λέξης'.

Το πρόβλημα έρευνας μέλους είναι το εξής: έστω ότι δίνονται μία αναδρομικά παριστώμενη ομάδα G, μία υπομάδα $H \leq G$ η οποία παράγεται από τα στοιχεία $h_1, ..., h_k$ καθώς και ένα στοιχείο $h \in H$. Βρείτε μία έκφραση του h ως προς τα στοιχεία $h_1, ..., h_k$.

1.3.6 Το Πρόβλημα Ισομορφισμού

Το πρόβλημα ισομορφισμού είναι το εξής: έστω ότι δίνονται δύο πεπερασμένα παριστώμενες υποομάδες G_1, G_2. Υπάρχει αλγόριθμος ο οποίος μπορεί να αποφανθεί για το αν είναι ισόμορφες μεταξύ τους?

Η μέθοδος $Tietze$, την οποία θα αναπτύξουμε παρακάτω, απαριθμεί αναδρομικά όλες τις πεπερασμένα παριστώμενες υποομάδες, τις ισομορφικές με μία πεπερασμένα παριστώμενη. Αυτό υπονοεί ότι η θετική πλευρά του προβλήματος ισομορφισμού είναι αναδρομική. Βέβαια, υπάρχει το ενδεχόμενο σε ορισμένες περιπτώσεις τόσο η θετική όσο και η αρνητική πλευρά του προβλήματος να είναι μη αναδρομικές.

1.4 Η Μέθοδος $Nielsen$

Ας δούμε ποια ακριβώς είναι η μέθοδος $Nielsen$.

Έστω μία ελεύθερη ομάδα $F = F_n$ πεπερασμένης διάστασης με σύνολο ελεύθερων γεννητόρων το $X = \{x_1, ..., x_n\}$. Έστω $Y = \{y_1, ..., y_m\}$ ένα τυχαίο

πεπερασμένο σύνολο στοιχείων της ομάδας F. Θεωρούμε τους εξής στοιχειώδεις μετασχηματισμούς οι οποίοι μπορούν να εφαρμοστούν στο Y:

1. Το y_i αντικαθίσταται είτε από το $y_i y_j$ είτε από το $y_j y_i$ για $j \neq i$.
2. Το y_i αντικαθίσταται από το y_i^{-1}.
3. Το y_i αντικαθίσταται από κάποιο y_j και συγχρόνως το y_j αντικαθίσταται από το y_i.
4. Σε περίπτωση που ισχύει $y_i = 1$, διαγράφεται το στοιχείο.

Κάθε πεπερασμένο σύνολο ανηγμένων λέξεων του F_n μπορεί μέσω μιας πεπερασμένης ακολουθίας μετασχηματισμών $Nielsen$ να μετατραπεί σε $Nielsen$ - ανηγμένο σύνολο $U = \{u_1, ..., u_k\}$, δηλαδή σε ένα σύνολο στο οποίο κάθε τριάδα $\upsilon_1, \upsilon_2, \upsilon_3$ της μορφής $u_i^{\pm 1}$ έχει τις εξής τρεις ιδιότητες:

- $\upsilon_1 \neq 1$
- $\upsilon_1\upsilon_2 \neq 1 \Longrightarrow |\upsilon_1\upsilon_2| \geq |\upsilon_1|, |\upsilon_2|$
- $\upsilon_1\upsilon_2 \neq 1$ και $\upsilon_2\upsilon_3 \neq 1 \Longrightarrow |\upsilon_1\upsilon_2\upsilon_3| > |\upsilon_1| - |\upsilon_2| + |\upsilon_3|$

Αποδεικνύεται ότι η υποομάδα της F_n η οποία παράγεται από το U είναι ελεύθερη και έχει βάση την U.

Λέμε ότι δύο σύνολα είναι $Nielsen$ ισοδύναμα εάν μπορούμε να μεταβούμε από το ένα στο άλλο εφαρμόζοντας μια ακολουθία από τους μετασχηματισμούς 1. - 4. Επίσης, έχει αποδειχθεί από τον $Nielsen$ ότι δύο σύνολα παράγουν την ίδια ομάδα αν και μόνο αν είναι $Nielsen$ ισοδύναμα.

1.5 Η Μέθοδος *Schreier*

Σε αυτήν την παράγραφο θα παρουσιάσουμε τη μέθοδο για την περίπτωση των

ελεύθερων ομάδων. Ωστόσο μπορεί να εφαρμοστεί χωρίς προβλήματα και για κάθε τυχαία ομάδα.

Έστω H μία υποομάδα της F. Μία συνάρτηση αντιπροσώπων δεξιών συμπλόκων για την F (επί των γεννητόρων x_i) $modulo\ H$ είναι μία αντιστοιχία λέξεων $w = w(x_1, x_2, ...) \to w' = w'(x_1, x_2, ...)$ όπου τα στοιχεία w' σχηματίζουν ένα σύστημα αντιπροσώπων των δεξιών συμπλόκων $modulo\ H$, με το στοιχείο $w' = w'(x_1, x_2, ...)$ να είναι ο αντιπρόσωπος του συμπλόκου όπου ανήκει το στοιχείο $w = w(x_1, x_2, ...)$. Έτσι, προκύπτουν τα εξής:

Θεώρημα: Έστω μία συνάρτηση αντιπροσώπων δεξιών συμπλόκων για την $F\ modulo\ H$, $w \to w'$. Τότε, η H παράγεται από τις λέξεις: $ux_i \cdot [(ux_i)']^{-1}$, όπου u είναι ένας τυχαίος αντιπρόσωπος και x_i ένας γεννήτορας της H.

• Το σύστημα αντιπροσώπων ονομάζεται σύστημα $Schreier$.

Αποδεικνύεται ότι υπάρχει πάντοτε τέτοιο σύστημα. Επίσης, υπάρχει ένα ελάχιστο σύστημα $Schreier$, ένα σύστημα δηλαδή όπου κάθε αντιπρόσωπος έχει μήκος που δεν ξεπερνάει αυτό της κάθε λέξης την οποία αντιπροσωπεύει. Για να κλείσουμε την παράγραφο, θα αναφέρουμε ένα ιδιαίτερα σημαντικό αποτέλεσμα.

Θεώρημα ($Nielsen$ - $Schreier$): Κάθε μη τετριμμένη υποομάδα ελεύθερης ομάδας είναι ελεύθερη.

1.6 Η Μέθοδος *Tietze*

Σε αυτήν την παράγραφο θα αναλύσουμε τους στοιχειώδεις μετασχηματισμούς $Tietze$, οι οποίοι έχουν το χαρακτηριστικό ότι διατηρούν τους ισομορφισμούς. Εφαρμόζονται σε ομάδες οι οποίες είναι εκφρασμένες με γεννήτορες και ορίζουσες σχέσεις. Τους εισήγαγε ο $Tietze$ με σκοπό να επιλύσει το πρόβλημα ισομορφισμού.

Έστω $G = \langle x_1, x_2, ... | r_1, r_2, ... \rangle$ η παράσταση της ομάδας $G = F/R$, όπου F είναι η ελεύθερη ομάδα που παράγουν τα $x_1, x_2, ...$ και R είναι η κανονική

θήκη την οποία παράγουν οι ορίζουσες σχέσεις $r_1, r_2, ...$ Οι στοιχειώδεις μετασχηματισμοί είναι οι εξής:

(T1) - Εισαγωγή νέου γεννήτορα: Αντικαθιστούμε την παράσταση $\langle x_1, x_2, ...|r_1, r_2, ...\rangle$ με την $\langle y, x_1, x_2, ...|ys^{-1}, r_1, r_2, ...\rangle$, όπου $s = s(x_1, x_2, ...)$ είναι ένα τυχαίο στοιχείο επί των γεννητόρων.

(T2) - Αφαίρεση ενός γεννήτορα: Αντικαθιστούμε την παράσταση της μορφής $\langle y, x_1, x_2, ...|ys^{-1}, r_1, r_2, ...\rangle$, όπου τα στοιχεία $s, r_1, r_2, ...$ ανήκουν στην ομάδα που παράγουν τα στοιχεία $x_1, x_2, ...$, με την παράσταση $\langle x_1, x_2, ...|r_1, r_2, ...\rangle$.

(T3) - Εφαρμογή ενός αυτομορφισμού: Εφαρμόζουμε έναν αυτομορφισμό της ελεύθερης ομάδας που παράγεται από τα $x_1, x_2, ...$ τόσο στους γεννήτορες $x_1, x_2, ...$ όσο στις ορίζουσες σχέσεις $r_1, r_2, ...$

(T4) - Αλλαγή οριζουσών σχέσεων: Αντικαθιστούμε το σύνολο $r_1, r_2, ...$ των οριζουσών σχέσεων με ένα άλλο σύνολο, έστω $r'_1, r'_2, ...$, το οποίο να παράγει την ίδια κανονική θήκη.

Στη συνέχεια, θα αναφέρουμε ένα ιδιαίτερα σημαντικό θεώρημα το οποίο οφείλεται στον ίδιον τον $Tietze$.

Θεώρημα: Δύο ομάδες είναι ισομορφικές αν και μόνο αν μπορεί κανείς να μεταβεί από την παράσταση της μίας στην παράσταση της άλλης με μία ακολουθία από μετασχηματισμούς (T1) - (T4).

Στην περίπτωση που οι υπό εξέταση ομάδες είναι πεπερασμένα παριστώμενες, τότε η ακολουθία των μετασχηματισμών μετάβασης είναι πεπερασμένη.

Σε επόμενο κεφάλαιο, οι μετασχηματισμοί $Tietze$ θα φανούν ιδιαίτερα χρήσιμοι. Πιο συγκεκριμένα, θα τους χρησιμοποιήσουμε σε ένα πρωτόκολλο όπου θα είναι αναγκαία η 'παραλλαγή' γεννητόρων και οριζουσών σχέσεων.

1.7 Κανονικές Μορφές

Οι κανονικές μορφές είναι βασικοί μηχανισμοί απόκρυψης στοιχείων σε πρωτόκολλα κρυπτογράφησης. Οι κανονικές μορφές πρέπει να έχουν δύο βασικές ιδιότητες. Η πρώτη είναι ότι κάθε στοιχείο πρέπει να έχει μοναδική κανονική μορφή. Η δεύτερη είναι ότι σε περίπτωση που δύο στοιχεία έχουν την ίδια κανονική μορφή, τότε θα πρέπει να εξισώνονται ως προς κάποια οπτική.

Το να έχουν τα στοιχεία μίας ομάδας περισσότερες της μίας κανονικές μορφές είναι κάτι που μπορεί να εκθέσει καταστάσεις σε κίνδυνο. Πράγματι, είναι πιθανό η μία κανονική μορφή να αποκαλύπτει αυτό που η άλλη προσπαθεί να αποκρύψει.

1.8 Πολυπλοκότητα

Η πολυπλοκότητα χρόνου [1] αφορά το χρόνο που πρέπει να δαπανηθεί για να εκτελεστεί ένας αλγόριθμος και συμβολίζεται με Ο. Στην παρούσα εργασία θα δούμε συμβολισμούς της μορφής $O(n), O(nlogn), O(2^n)$ κλπ, όπου το n εκφράζει το μέγεθος της εισροής σε μονάδες ή ψηφία.

Υπάρχουν διάφορα είδη πολυπλοκότητας και οι ονομασίες τους προέρχονται από τη μορφή του περιεχομένου της παρένθεσης στον Ο - συμβολισμό.

Τα πιο συνήθη είδη είναι τα εξής:

1. $O(n)$: γραμμική πολυπλοκότητα
2. $O(n^a)$ για a>1: πολυωνυμική πολυπλοκότητα
3. $O(n^2)$: πολυπλοκότητα τετραγωνικού χρόνου
4. $O(logn)$: πολυπλοκότητα λογαριθμικού χρόνου
5. $2^{n^{O(1)}}$: πολυπλοκότητα εκθετικού χρόνου

Κεφάλαιο 2

Βασικά Πρωτόκολλα

Σε αυτό το κεφάλαιο θα αναφέρουμε κάποια σημαντικά πρωτόκολλα κρυπτογράφησης, τα οποία αρχικά ενδεχομένως να φανούν κάπως απλοϊκά, αλλά στην πραγματικότητα οι ιδέες που έθεσαν στο τραπέζι του διαλόγου αποτελούν θεμέλιο για ολόκληρο τον κλάδο της κρυπτογραφίας.
Η απλοϊκή, τουλάχιστον αρχικά, μορφή τους εξυπηρετεί και στο ότι βοηθά τον αναγνώστη να εισχωρήσει ομάλα στη συγκεκριμένη επιστήμη.
Μετά την παρουσίαση των πρωτοκόλλων κρυπτογράφησης, θα δούμε και μερικά πρωτόκολλα πιστοποίησης όπου και θα γίνει αντιληπτή η πολύ στενή σχέση ανάμεσα στα δύο είδη.

Τα σχήματα τα οποία θα αναφέρουμε στη συνέχεια, γενικά, ανήκουν στη λεγόμενη μη μεταθετική κρυπτογραφία δημοσίου κλειδιού. Τα περισσότερα από αυτά βασίζονται στα προβλήματα έρευνας, τα οποία προβλήματα αποτελούν παραλλαγές των λεγόμενων προβλημάτων απόφασης. Τα πρωτόκολλα που βασίζονται στα προβλήματα έρευνας, γενικά μπορούμε να πούμε πως ανήκουν στην κατηγορία των πρωτοκόλλων δημοσίου κλειδιού, βασισμένων σε συναρτήσεις μιας κατεύθυνσης, δηλαδή σε συναρτήσεις των οποίων οι αντίστροφες συναρτήσεις υπολογίζονται ιδιαίτερα δύσκολα.

Θα ξεκινήσουμε αναφέροντας κάποια σχήματα τα οποία βασίζονται σε μη μεταθετικές (ημι)ομάδες.

2.1 Η Εγκαθίδρυση Κλειδιού $Diffie-Hellman$

Το συγκεκριμένο σχήμα αποτέλεσε την εκκίνηση του κλάδου και η βασική της ιδέα αποτελεί βασικότατο εργαλείο μέχρι και σήμερα. Ας δούμε ποια είναι τα βήματά του:

1. Η Αλίκη και ο Βασίλης συμφωνούν σε μία πεπερασμένη κυκλική ομάδα G και σε έναν γεννήτορα g.

2. Η Αλίκη επιλέγει έναν τυχαίο φυσικό αριθμό a και στέλνει στο Βασίλη το στοιχείο g^a.

3. Ο Βασίλης επιλέγει ένα τυχαίο φυσικό αριθμό b και στέλνει στην Αλίκη το στοιχείο g^b.

4. Η Αλίκη υπολογίζει $K_A = (g^b)^a = g^{ba}$.

5. Ο Βασίλης υπολογίζει $K_B = (g^a)^b = g^{ab}$.

Έτσι, οι δύο συναλλασσόμενοι καταφέρνουν να εγκαθιδρύσουν ένα κοινό μυστικό κλειδί K, καθώς είναι προφανές ότι $K = K_A = K_B$

Το πρωτόκολλο θεωρείται ασφαλές εάν η ομάδα και ο γεννήτορας έχουν επιλεγεί κατάλληλα. Η Εύα, προκειμένου να επιτύχει παραβίαση, θα πρέπει να επιλύσει το λεγόμενο πρόβλημα $Diffie - Hellman$. Δηλαδή, πρέπει να καταφέρει να εκμαιεύσει το στοιχείο g^{ab}, το οποίο είναι το μυστικό κλειδί, από τα στοιχεία g^a και g^b. Για κατάλληλες παραμέτρους, αυτό θεωρείται δύσκολο. Αυτές οι παράμετροι, επί της ουσίας, είναι οι ομάδες εντός των οποίων το πρόβλημα των διακριτών λογαρίθμων είναι δύσκολα επιλύσιμο και η ύψωση σε εκθέτη αποτελεσματική. Τα πιο γνωστά παραδείγματα είναι η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$ και η ομάδα των σημείων τα οποία ορίζονται από ελλειπτική καμπύλη πάνω από πεπερασμένο σώμα [2].

Για να ολοκληρώσουμε την ανάλυση του πρωτοκόλλου, θα αναφερθούμε και στην επίθεση ωμής δύναμης την οποία μπορεί να εφαρμόσει η Εύα. Θα μπορούσε να υπολογίσει όλες τις δυνάμεις του g μία προς μία και στη συνέχεια να ελέγξει αν υπάρχει αντιστοιχία με τη μετάδοση που έχει στα χέρια της. Αυτή η διαδικασία θα απαιτούσε $O(|g|)$ το πλήθος πολλαπλασιασμούς, όπου $|g|$ είναι η τάξη του στοιχείου. Όμως, σε πρακτικό επίπεδο, η τάξη του g είναι συνήθως

στο επίπεδο του 10^{300} και, ως εκ τούτου, το συγκεκριμένο πλάνο επίθεσης δεν είναι υλοποιήσιμο.

Σε αυτό το σημείο, θα μπορούσε να αναρωτηθεί κανείς μήπως αντιμετωπίζουν υπολογιστικό πρόβλημα και οι νόμιμοι συμμετέχοντες στο σχήμα. Κάτι τέτοιο όμως δεν ισχύει καθώς υπάρχει ένα υπολογιστικό τεχνάσμα το οποίο διευκολύνει το έργο τους: το ονομάζουμε αλγόριθμο $square - and - multiply$ και βασίζεται στην αναπαράσταση της δύναμης μέσω δυνάμεων του αριθμού 2. Έτσι, σύμφωνα με αυτόν τον αλγόριθμο, ο υπολογισμός απαίτει $O(log_2 a)$ πολλαπλασιασμούς, κάτι που υπολογιστικά είναι πολύ πιο εφικτό.

2.2 Το κρυπτοσύστημα *ElGamal*

Το κρυπτοσύστημα $ElGamal$ είναι ένα πρωτόκολλο δημοσίου κλειδιού, το οποίο βασίζεται στο σχήμα $Diffie - Hellman$. Το συγκεκριμένο κρυπτοσύστημα χρησιμοποιείται σε ποικίλα συστήματα και αποτελεί τη βάση και για ένα σύστημα υπογραφής. Ας δούμε τα βήματα του σχήματος:

1. Η Αλίκη και ο Βασίλης συμφωνούν σε μία πεπερασμένη κυκλική ομάδα G και σε έναν γεννήτορα g της G.

2. Η Αλίκη επιλέγει έναν τυχαίο φυσικό αριθμό a και κοινοποιεί το στοιχείο $c = g^a$.

3. Ο Βασίλης, ο οποίος θέλει να στείλει ένα μήνυμα $m \in G$ στην Αλίκη, επιλέγει έναν τυχαίο φυσικό αριθμό b και μεταδίδει δύο στοιχεία, τα $m \cdot c^b$ και g^b στην Αλίκη. Ας σημειωθεί ότι $c^b = g^{ab}$.

4. Η Αλίκη ανακτά το m με τον εξής υπολογισμό: $m = (m \cdot c^b) \cdot ((g^b)^a)^{-1}$.

Ένα σημαντικό προσόν του σχήματος είναι ο πιθανοθεωρητικός χαρακτήρας του, με την έννοια ότι το m μπορεί να κρυπτογραφηθεί από πολλά διαφορετικά στοιχεία.

2.3 Πιστοποίηση

Σε αυτό το σημείο θα αναφερθούμε σε έναν πολύ σημαντικό κλάδο, ο οποίος είναι πολύ συγγενικός με την κρυπτογράφηση και με την οποία μάλιστα μοιράζεται κοινές τεχνικές. Πρόκειται για την πιστοποίηση ($authentication$) χρήστη.

Σε πολλές περιπτώσεις, και κυρίως στο χώρο του διαδικτύου, είναι πολύ σημαντικό για λόγους ασφαλείας, να γνωρίζει κανείς με ποιον επικοινωνεί ή ακόμα και συναλλάσσεται. Έτσι, ο συγκεκριμένος κλάδος μας προμηθεύει με εργαλεία και μεθόδους που μπορούν να μας εγγυηθούν τα παραπάνω.

Γενικά, μπορούμε να πούμε πως πολλά πρωτόκολλα εγκαθίδρυσης κλειδιού μπορούν να μετατραπούν σε σχήματα πιστοποίησης. Εμείς, θα δούμε την διαδικασία η οποία βασίζεται στο $Diffie - Hellman$.

Ας υποθέσουμε ότι η Αλίκη θέλει να επιβεβαιώσει στον Βασίλη την ταυτότητά της. Αυτό γίνεται με το να τον πληροφορήσει πως έχει γνώση για κάποιο μυστικό χωρίς όμως να αποκαλύψει το ίδιο το μυστικό (και εκθέσει καταστάσεις δημοσίως). Αυτού του είδους τα μοντέλα ονομάζονται αποδείξεις ταυτότητας μηδενικής γνώσης.

1. Η Αλίκη κοινοποιεί μία πεπερασμένη κυκλική ομάδα G καθώς και έναν γεννήτορα g της ομάδας. Στη συνέχεια, επιλέγει έναν τυχαίο φυσικό αριθμό a και κοινοποιεί το g^a.

2. Ο Βασίλης επιλέγει έναν τυχαίο φυσικό αριθμό b και, στη συνέχεια, στέλνει ως δοκιμασία το g^b στην Αλίκη.

3. Η Αλίκη απαντάει με την απόδειξη $P = (g^b)^a = g^{ba}$.

4. Ο Βασίλης ελέγχει εάν πράγματι ισχύει ότι $(g^a)^b = P$.

Άρα, ο Βασίλης πλέον έχει εγκαθιδρύσει ένα δίαυλο επικοινωνίας ο οποίος βασίζεται στην επιλογή α της Αλίκης. Η ουσία του όλου ζητήματος έγκειται στο ότι η Αλίκη μπορεί να επιβεβαιώνει την ταυτότητά της χωρίς να την αποκαλύπτει.

Το σχήμα που μόλις περιγράψαμε είναι η πιο απλή και ενδεχομένως αυτονόητη μορφή. Τώρα, θα διατυπώσουμε ένα ακόμα σύστημα πιστοποίησης το οποίο βασίζεται στο πρωτόκολλο $Diffie - Hellman$.

Και σε αυτήν την περίπτωση, η κατάσταση είναι η ίδια. Η Αλίκη θέλει να επιβεβαιώσει την ταυτότητά της στο Βασίλη μέσω ενός μη ασφαλούς διαύλου επικοινωνίας, χωρίς να αποκαλύψει στοιχεία. Ας δούμε ποιος ακριβώς είναι ο αλγόριθμος:

Έστω G μία ομάδα και A,B $\leq G$ δύο μετατιθέμενες ομάδες, δηλαδή δύο ομάδες οι οποίες έχουν την ιδιότητα: $a \cdot b = b \cdot a$ για $a \in A$, $b \in B$. Το ιδιωτικό κλειδί της Αλίκης είναι ένα στοιχείο $s \in A$. Το δημόσιο κλειδί της είναι ένα ζεύγος (w, t), όπου το w είναι ένα αυθαίρετο στοιχείο της G και $t = s^{-1}ws$.

1. Ο Βασίλης επιλέγει ένα στοιχείο $r \in B$ και στέλνει ως δοκιμασία το $w' = r^{-1}wr$ στην Αλίκη.

2. Η Αλίκη απαντάει στο Βασίλη με το $w'' = s^{-1}w's$.

3. Ο Βασίλης ελέγχει εάν ισχύει $w'' = r^{-1}tr$.

Ο υπολογισμός του Βασίλη βασίζεται στο εξής: $w'' = s^{-1}w's = s^{-1}r^{-1}wrs = r^{-1}s^{-1}wsr = r^{-1}tr$.

Ας δούμε τώρα με ποιους τρόπους μπορεί η Εύα να επιτεθεί, δηλαδή να παρουσιαστεί στο Βασίλη ως η Αλίκη:

- Μπορεί να υπολογίσει το ιδιωτικό κλειδί της Αλίκης, με το να λύσει το πρόβλημα έρευνας συζυγίας, το σχετικό με την υποομάδα A, ή με το να λύσει το πρόβλημα αποδόμησης για το ζεύγος (w, t), πάντα εντός της A, δηλαδή να υπολογίσει στοιχεία $s_1, s_2 \in A$ τέτοια ώστε $t = s_1ws_2$. Είναι προφανές ότι αν βρεθεί ένα τέτοιο ζεύγος, τότε θα ικανοποιεί τη σχέση $s_1w's_2 = w''$. Συνεπώς, το (s_1, s_2) μπορεί να χρησιμοποιηθεί στη θέση του ιδιωτικού κλειδιού της Αλίκης.

- Επίσης, μπορεί να υπολογίσει το κλειδί r του Βασίλη. Αυτό μπορεί να το επιτύχει με το να επιλύσει το πρόβλημα έρευνας συζυγίας στην υποομάδα B ή με το να επιλύσει το πρόβλημα αποδόμησης για ένα ζεύγος (w_1, w_2) στη B και να το χρησιμοποιήσει όπως παραπάνω προκειμένου να επιτεθεί στο ιδιωτικό κλειδί της Αλίκης.

Σημειώνουμε πως η δυσκολία για το κάθε πρόβλημα έχει να κάνει με την επιλογή της κάθε υποομάδας και άρα δεν είναι απαραίτητα η ίδια και για τις δύο.

Θα αναφέρουμε μία τροποποίηση του σχήματος προκειμένου να βασιστεί στο πρόβλημα αποδόμησης.
Έστω οι υποομάδες A_1, A_2, B_1, B_2 της G τέτοιες ώστε $[A_1, B_1] = 1$ και $[A_2, B_2] = 1$, δηλαδή είναι ανά δύο μετατιθέμενες. Το ιδιωτικό κλειδί της Αλίκης είναι ένα ζεύγος $(a_1, a_2) \in A_1 \times A_2$ και το δημόσιο κλειδί της είναι ένα ζεύγος $(w, t) \in G \times G$, όπου το w είναι ένα αυθαίρετο στοιχείο της G και $t = a_1 w a_2$. Ο αλγόριθμος έχει ως εξής:

1. Ο Βασίλης επιλέγει δύο στοιχεία $b_1 \in B_1$ και $b_2 \in B_2$ και στέλνει τη δοκιμασία $w' = b_1 w b_2$ στην Αλίκη.

2. Η Αλίκη αποστέλλει την απάντηση $w'' = a_1 w' a_2$ στο Βασίλη.

3. Ο Βασίλης ελέγχει εάν ισχύει η σχέση: $w'' = b_1 t b_2$.

Εμείς απλά θα αναφέρουμε ότι το πρωτόκολλο οφείλεται στους Lal και $Chaturwedi$ και, από ότι φαίνεται, δεν μπορεί να χρησιμοποιηθεί το πρόβλημα έρευνας συζυγίας ως μέθοδος επίθεσης σε συτήν την παραλλαγή του σχήματος.

Για να ολοκληρώσουμε τη μελέτη μας στα πρωτόκολλα πιστοποίησης, θα αναφέρουμε και ένα τελευταίο, το $Fiat - Shamir$.

Το Πρωτόκολλο Πιστοποίησης $Fiat - Shamir$

Η βασική διαφορά αυτού του σχήματος με τα προηγούμενα εντοπίζεται στο ότι εδώ δεν χρειάζεται να επιλέξουμε μετατιθέμενες υποομάδες. Ας δούμε τι ακριβώς συμβαίνει:
Το ιδιωτικό κλειδί της Αλίκης είναι ένα τυχαίο στοιχείο $s \in G$ και το δημόσιο κλειδί της είναι ένα ζεύγος (w, t), όπου το w είναι στοιχείο της ομάδας G και $t = s^{-1} w s$.

1. Η Αλίκη επιλέγει ένα τυχαίο στοιχείο $r \in G$. Στη συνέχεια, αποστέλλει στο Βασίλη το στοιχείο $x = r^{-1} t r$, το οποίο ονομάζεται δέσμευση.

2. Ο Βασίλης επιλέγει ένα τυχαίο ψηφίο c του δυαδικού συστήματος και το αποστέλλει στην Αλίκη.

3. Η Αλίκη πράττει ως εξής:

   - Αν $c = 0$, τότε η Αλίκη στέλνει το $y = r$ στο Βασίλη και εκείνος, με τη σειρά του, ελέγχει εάν ισχύει η ισότητα $x = y^{-1}ty$.
   - Αν $c = 1$, τότε η Αλίκη στέλνει το $y = sr$ στο Βασίλη και εκείνος στη συνέχεια, ελέγχει εάν ισχύει η ισότητα $x = y^{-1}wy$.

Είναι σαφές ότι μια σωστή απάντηση της Αλίκης στο τρίτο βήμα, οδηγεί σε αποδοχή από το Βασίλη.
Όμως, οφείλουμε να εξηγήσουμε το λόγο ύπαρξης του τυχαίου στοιχείου c. Θα μπορούσε να αναρωτηθεί κανείς: γιατί η Αλίκη δεν περιορίζεται στη μετάδοση του $y = sr$ αφού δεν αποκαλύπτει το ιδιωτικό της κλειδί και παράλληλα δίνει τη δυνατότητα στο Βασίλη να υπολογίσει το $x = y^{-1}wy$?

Η αλήθεια είναι ότι αν δεν υπήρχε το τυχαίο στοιχείο, η Εύα θα μπορούσε κάλλιστα να μεταδώσει το στοιχείο $x = u^{-1}wu$, όπου u είναι ένα αυθαίρετο στοιχείο της ομάδας. Έτσι, το u ΄παίζει΄ το ρόλο του sr. Εντελώς αντίστοιχα, αν το πρωτόκολλο απαιτούσε από την Αλίκη μόνο τη μετάδοση του r, θα μπορούσε η Αλίκη να μεταδώσει ένα οποιοδήποτε στοιχείο στη θέση του r.
Αυτές οι σκέψεις δείχνουν ότι το πρωτόκολλο πρέπει να εκτελείται αρκετές φορές προκειμένου να εξασφαλίζεται μεγαλύτερη αξιοπιστία. Πιο συγκεκριμένα, για κάθε επανάληψη, η Εύα έχει πιθανότητα σωστής 'αναπαράστασης' της Αλίκης ίση με $1/2$. Αν επαναλάβουμε τη διαδικασία n φορές, τότε η πιθανότητά της μειώνεται στο $1/2^n$.
Για να ολοκληρώσουμε την ανάλυση του πρωτοκόλλου θα αναφέρουμε ότι η ουσία του όλου σχήματος έγκειται στη δυσκολία επίλυσης του προβλήματος έρευνας συζυγίας στην ομάδα καθώς και ότι δεν μπορεί να επιστρατευθεί το πρόβλημα έρευνας αποδόμησης στο συγκεκριμένο πρωτόκολλο εξαιτίας της φύσης των στοιχείων τα οποία λαμβάνει ο Βασίλης.

Όπως αναφέραμε μία τροποποίηση του σχήματος πιστοποίησης που βασίζεται στο $Diffie - Hellman$, έτσι θα κάνουμε το ίδιο και για το $Fiat - Shamir$. Αυτό γίνεται για να βασίσουμε το σχήμα στο πρόβλημα αποδόμησης. Επίσης, σε αυτήν την τροποποίηση δίνεται η ευκαιρία να εισάγουμε μία νέα τεχνική: Έστω φ ένας αυθαίρετος ενδομορφισμός της ομάδας G. Θεωρούμε τον φ γνωστό δημοσίως και άρα μπορεί να θεωρηθεί μέρος του δημοσίου κλειδιού της Αλίκης.

Το ιδιωτικό κλειδί της Αλίκης είναι ένα στοιχείο $s \in G$ και το δημόσιο κλειδί

της είναι ένα ζεύγος (w, t), όπου w είναι ένα αυθαίρετο στοιχείο της ομάδας και $t = s^{-1}w\varphi(s)$. Το πρωτόκολλο έχει ως εξής:

1. Η Αλίκη επιλέγει ένα τυχαίο $r \in G$ και στέλνει στο Βασίλη τη δέσμευση $x = r^{-1}t\varphi(r)$.

2. Ο Βασίλης επιλέγει ένα τυχαίο στοιχείο c του δυαδικού συστήματος και το στέλνει στην Αλίκη.

3. Η Αλίκη πράττει ως εξής:

   - Αν $c = 0$ τότε η Αλίκη στέλνει το στοιχείο $y = r$ και ο Βασίλης ελέγχει αν ισχύει η σχέση $x = y^{-1}t\varphi(y)$.
   - Αν $c = 1$ τότε η Αλίκη στέλνει το στοιχείο $y = sr$ και ο Βασίλης ελέγχει αν ισχύει η σχέση $x = y^{-1}w\varphi(y)$.

Όπως και προηγουμένως, η σωστή απάντηση στο τρίτο βήμα οδηγεί σε επιβεβαίωση της ταυτότητας.
Για να επιτεθεί κανείς στο πρωτόκολλο, αρκεί να βρει στοιχείο $s' \in G$ τέτοιο ώστε $t = s'^{-1}w\varphi(s')$. Αυτό είναι μια εκδοχή του λεγόμενου προβλήματος (έρευνας) ανεστραμμένης συζυγίας. Θα το διατυπώσουμε για να είναι πιο σαφές το τι ακριβώς εννοούμε:

Έστω G μία ομάδα. Για κάθε $\varphi \in Aut(G)$ και για κάθε ζεύγος w, t στοιχείων της G, βρείτε έναν ανεστραμμένο συζυγή για το w και το t, δηλαδή ένα στοιχείο $s \in G$ τέτοιο ώστε $t = s^{-1}w\varphi(s)$, δεδομένης της ύπαρξης τέτοιου στοιχείου.

Μπορούμε να πούμε πως το συγκεκριμένο πρόβλημα είναι σχετικά καινούριο για τον ευρύτερο κλάδο της θεωρίας ομάδων και είναι μη τετριμμένο ακόμη και για ελεύθερες ομάδες. Για να αποκτήσουμε μία εικόνα, θα αναφέρουμε μία έρευνα που έχει γίνει πάνω στο συγκεκριμένο θέμα. Η έρευνα αυτή έγινε από τους $Bogopolski, Martino, Maslakova$ και $Ventura$ [3]:

Θα ξεκινήσουμε με έναν ορισμό: $Free - by - cyclic$ ονομάζεται μία ομάδα G η οποία έχει μία ελεύθερη κανονική υποομάδα F με κυκλικό πηλίκο $C = G/F$. Αν η F μπορεί να επιλεγεί πεπερασμένα παραγόμενη, τότε η G ονομάζεται $[f.g.free] - by - cyclic$ ομάδα.

Το πιο σημαντικό αποτέλεσμα της εργασίας είναι το εξής:

Θεώρημα 1: Το πρόβλημα συζυγίας στις $[f.g.free] - by - cyclic$ ομάδες είναι επιλύσιμο.

Προκειμένου να αποδειχθεί το Θεώρημα 1, το οποίο είναι και ο στόχος της εργασίας, χρησιμοποιήθηκαν τα εξής αποτελέσματα:

Θεώρημα 2: Υπάρχει αλγόριθμος ο οποίος αποφαίνεται ότι υπάρχει ένα πεπερασμένο σύνολο γεννητόρων της υποομάδας σταθερού σημείου αυτομορφισμού μιας ελεύθερης ομάδας πεπερασμένης διάστασης.

Σε αυτό το σημείο θα αναφέρουμε ότι υποομάδα σταθερού σημείου αυτομορφισμού f ονομάζεται το εξής σύνολο: $G^f = \{g \in G | f(g) = g\}$.

Θεώρημα 3: Έστω πεπερασμένα παραγόμενη ελεύθερη ομάδα F, δύο στοιχεία της u, y και ένας αυτομορφισμός φ. Είναι αποφασίσιμο το αν υπάρχει ακέραιος k τέτοιος ώστε το $u\varphi^k$ να είναι συζυγές του y. Επιπλέον, αν υπάρχει τέτοιο k, τότε μπορεί να υπολογιστεί.

Πρόταση 4: Έστω F μία πεπερασμένα παραγόμενη ελεύθερη ομάδα. Αν το πρόβλημα ανεστραμένης συζυγίας είναι επιλύσιμο εντός της, τότε και το κανονικό πρόβλημα συζυγίας είναι επιλύσιμο.

Θεώρημα 5: Έστω F μία πεπερασμένα παραγόμενη ελεύθερη ομάδα. Τότε το πρόβλημα ανεστραμένης συζυγίας εντός της είναι επιλύσιμο.

Βέβαια, όπως καταλαβαίνει κανείς, το θεώρημα το οποίο αφορά αμεσότερα το πρωτόκολλό μας είναι το 5.

Για να ολοκληρώσουμε τη συζήτηση που αφορά τα σχήματα $Fiat-Shamir$, θα πούμε ότι έχει δειχθεί πως είναι δυνατόν να κατασκευαστούν παραλλαγές στις οποίες η πλαστοπροσωπία είναι δυσκολίας μη ντετερμινιστικού πολυωνυμικού χρόνου.

2.4 Το Πρωτόκολλο *Anshel−Anshel−Goldfeld*

Το συγκεκριμένο πρωτόκολλο ανήκει στον κλάδο που ονομάζουμε μη μεταθετική κτυπρογραφία καθώς δεν κάνει χρήση της μεταθετικής ιδιότητας ούτε με τη μορφή αβελιανών (υπό)ομάδων αλλά ούτε με τη μορφή μετατιθέμενων υποομάδων. Μπορούμε να πούμε πως ως πλατφόρμα μπορεί να χρησιμοποιηθεί οποιαδήποτε μη αβελιανή ομάδα εντός της οποίας επιλύεται αποτελεσματικά το πρόβλημα λέξης. Προφανώς, αυτό είναι ένα σημαντικό πλεονέκτημα. Προτού προχωρήσουμε σε περιγραφή, ας εξηγήσουμε έναν συμβολισμό: $g^x = x^{-1}gx$, όπου g, x είναι στοιχεία κάποιας ομάδας. Ας δούμε αναλυτικά το σχήμα:

Έστω G μια ομάδα και έστω τα στοιχεία $a_1, ..., a_k, b_1, ..., b_m \in G$. Όλα αυτά είναι κοινοποιημένα δημοσίως.

1. Η Αλίκη επιλέγει ως ιδιωτικό κλειδί ένα στοιχείο $x \in G$, τέτοιο ώστε $x = x(a_1, ..., a_k)$. Στέλνει στο Βασίλη τα στοιχεία $b_1^x, ..., b_m^x$.

2. Ο Βασίλης επιλέγει ως ιδιωτικό κλειδί ένα στοιχείο $y \in G$, τέτοιο ώστε $y = y(b_1, ..., b_m)$. Στέλνει στην Αλίκη τα στοχεία $a_1^y, ..., a_k^y$.

3. Η Αλίκη κάνει τον υπολογισμό $x(a_1^y, ..., a_k^y) = x^y = y^{-1}xy$, και ο Βασίλης τον $y(b_1^x, ..., b_m^x) = y^x = x^{-1}yx$. Έχοντας κάνει αυτόν τον υπολογισμό μπορούν εύκολα να καταλήξουν σε κοινό κλειδί. Πράγματι, η Αλίκη πολλαπλασιάζει το αποτέλεσμά της από αριστερά με το x^{-1} και, αντίστοιχα, ο Βασίλης πολλαπλασιάζει το δικό του αποτέλεσμα από αριστερά με το στοιχείο y^{-1} και στη συνέχεια υπολογίζει το αντίστροφό του.

Προκειμένου η Εύα να επιτεθεί πρέπει να επιλύσει το πρόβλημα έρευνας συζυγίας για όλα τα $a_1^y, ..., a_k^y, b_1^x, ..., b_m^x$. Σε αυτό το σημείο θα επισημάνουμε το εξής: ακόμα και αν η Εύα κατορθώσει να ανακαλύψει το στοιχείο x εκφρασμένο ως προς τους γεννήτορες της ομάδας, και πάλι δεν είναι σε θέση να ανακαλύψει το κοινό κλειδί. Πράγματι, αφενός μεν δεν μπορεί να υπολογίσει την παράσταση y^x, καθώς αγνοεί το στοιχείο y, αφετέρου δε δεν μπορεί να αξιοποιήσει την γνώση των δημοσίων στοιχείων $a_1^y, ..., a_k^y$ καθώς το x δεν είναι εκφρασμένο ως προς τους όρους $a_1, ..., a_k$ αλλά ως προς τους γεννήτορες της ομάδας. Έτσι, αδυνατεί να υπολογίσει το x^y. Ουσιαστικά, σε αυτήν την περίπτωση, η Εύα καλείται να επιλύσει ένα ιδιαίτερο πρόβλημα το οποίο ονομάζεται πρόβλημα έρευνας μέλους:

Έστω στοιχεία $x, a_1, ..., a_k$ της ομάδας G. Βρείτε έκφραση (εάν υπάρχει) του x ως λέξη των $a_1, ..., a_k$.

Επεξηγούμε σε αυτό το σημείο ότι το πρόβλημα απόφασης μέλους έχει να κάνει με το αν το στοιχείο x της ομάδας G ανήκει ή όχι στην υποομάδα που παράγουν τα στοιχεία $a_1, ..., a_k$.

Εμείς απλά θα αναφέρουμε ότι το συγκεκριμένο πρόβλημα φαίνεται πως είναι ιδιαίτερα δύσκολο για πολλές ομάδες. Για παράδειγμα, το πρόβλημα απόφασης μέλους για μία *braid group* B_n είναι αλγοριθμικά μη επιλύσιμο για $n \geq 6$, καθώς μια τέτοια *braid group* περιέχει υποομάδες ισομορφικές με το $F_2 \times F_2$, όπου F_2 είναι η ελεύθερη ομάδα τάξης 2. Η $K.A.Mihailova$ στην εργασία της με τίτλο $The\ occurrence\ problem\ for\ direct\ products\ of\ groups$ έδειξε ότι στην $F_2 \times F_2$ το συγκεκριμένο πρόβλημα είναι αλγοριθμικά μη επιλύσιμο.

Σε αυτό το σημείο θα αναλύσουμε μία μέθοδο επίθεσης:

Έστω ότι η Εύα καταφέρνει να βρει στοιχείο $x' \in G$ τέτοιο ώστε $b_1^x = b_1^{x'}, ..., b_m^x = b_m^{x'}$. Αυτό το στοιχείο ναι μεν έχει την επιθυμητή ιδιότητα της συζυγίας αλλά δεν είναι καθόλου σίγουρο ότι θα ισχύει η ισότητα $x = x'$. Για παράδειγμα, εάν ισχύει ότι $x' = c_b x$, όπου $c_b b_i = b_i c_b$ για κάθε i, τότε $b_i^x = b_i^{x'}$ για κάθε i. Συνεπώς, θα ισχύει ότι $b^x = b^{x'}$ για κάθε στοιχείο b που ανήκει στην υποομάδα που παράγουν τα $b_1, ..., b_m$. Πιο συγκεκριμένα, εφόσον το y ανήκει σε αυτήν την υποομάδα, θα ισχύει ότι $y^{x'} = y^x$.
Όμως τώρα προκύπτει ένα άλλο πρόβλημα. Ακόμα και αν η Εύα βρει ένα τέτοιο x', υπάρχει περίπτωση αυτό το στοιχείο να μην ανήκει καν στην υποομάδα A την παραγόμενη από τα $a_1, ..., a_k$. Άρα είναι πιθανό η Εύα να μην αποκτήσει τελικά το σωστό κοινό κλειδί K. Όλα αυτά φυσικά ισχύουν και για την ανάλογη διεργασία που αφορά το αντίστοιχο y' και την αντίστοιχη υποομάδα B. Αν όμως, τα x', y' ανήκουν στις A και B αντιστοίχως, τότε ο επιτιθέμενος υπάρχει περίπτωση να μπορεί να αποκομίσει το σωστό κλειδί K. Πράγματι, αν $x' = c_b x$ και $y' = c_a y$, όπου c_b ανήκει στην κεντροποιούσα της B και c_a ανήκει στην κεντροποιούσα της A. Τότε, οι υπολογισμοί έχουν ως εξής:

$(x')^{-1}(y')^{-1}x'y' = (c_b x)^{-1}(c_a y)^{-1}c_b x c_a y = x^{-1}{c_b}^{-1}y^{-1}{c_a}^{-1}c_b x c_a y = x^{-1}y^{-1}xy =$
$=$K.
Θα σημειώσουμε ότι $c_b \in A$ και $c_b \in C_G(B)$ καθώς επίσης και ότι $c_a \in B$ και $c_a \in C_G(A)$. Άρα, τα στοιχεία c_a, c_b μετατίθενται μεταξύ τους.

Όπως γίνεται κατανοητό από όσα είπαμε, είναι κομβικό το ότι τα c_a, c_b έχουν τις ιδιότητες τις οποίες αναφέραμε και ότι $x \in A$, $y \in B$. Συνεπώς, αν Η Εύα προσπαθήσει να επιλύσει το πρόβλημα έρευνας συζυγίας, θα πρέπει να αντιμετωπίσει είτε το πρόβλημα έρευνας μέλους είτε το πρόβλημα απόφασης μέλους, με το δεύτερο να είναι με αυξημένη πιθανότητα αλγοριθμικά μη επιλύσιμο στα πλαίσια κάποιας δωθήσας ομάδας. Για να γίνει πιο σαφές το τι ακριβώς εννοούμε με τα διάφορα ονόματα προβλημάτων τα οποία χρησιμοποιήσαμε, απλά θα αναφέρουμε ότι επί της ουσίας η Εύα καλείται να επιλύσει μία πιο σύνθετη εκδοχή του προβλήματος έρευνας συζυγίας:

Έστω ομάδα G, μία υποομάδα Α της G και δύο στοιχεία $g, h \in G$. Βρείτε $x \in A$ τέτοιο ώστε $h = x^{-1}gx$, δεδομένου ότι υπάρχει τέτοιο.

Εν κατακλείδι, το νόημα των όσων είπαμε για τον συγκεκριμένο τύπο επίθεσης είναι ότι ακόμα και αν βρεθεί ένα γρήγορος (πολυωνυμικός) ντετερμινιστικός αλγόριθμος ο οποίος να επιλύει το πρόβλημα έρευνας συζυγίας σε *braid groups*, και πάλι αυτό δεν θα είναι αρκετό για να εξουδετερώσει το πρωτόκολλο χρησιμοποιώντας μία ντετερμινιστική επίθεση. (Σημείωση: Ένας αλγόριθμος καλείται ντετερμινιστικός αν κάθε φορά που εκτελείται δίνει το ίδιο αποτέλεσμα για δεδομένη εισροή.)

Παραπάνω αναφερθήκαμε σε κάποια σημαντικά πλεονεκτήματα του πρωτοκόλλου. Σε αυτό το τελικό τμήμα θα αναφερθούμε και σε κάποιες αδυναμίες.

Θα ξεκινήσουμε χρησιμοποιώντας πληροφορίες προερχόμενες από μία εργασία των $D.Garber$, $S.Kaplan$, $M.Teicher$, $B.Tsaban$ και $U.Vishne$ [4]. Είναι σαφές πως θα επικεντρωθούμε στα ουσιαστικά σημεία της εργασίας χωρίς να γινόμαστε εξαντλητικοί.

Έστω μία ομάδα G. Μία εξίσωση της G με μεταβλητές X_i, $i \in \mathbb{N}$ έχει τη μορφή:

$$X_{k_1}^{\sigma_1} X_{k_2}^{\sigma_2} \cdots X_{k_n}^{\sigma_n} = b, \tag{1}$$

με $k_1, ..., k_n \in \mathbb{N}$, $\sigma_1, ..., \sigma_n \in \{-1, 1\}$ και b δοθέν στοιχείο.

Έστω ότι έχουμε ένα σύστημα εξισώσεων τύπου (1). Πολλές φορές είναι δυ-

νατόν να τροποποιήσουμε το σύστημα με χρήση αλγεβρικών μεθόδων και να προκύψει σύστημα εξισώσεων όπου όλες εκ των οποίων έχουν την ίδια κύρια μεταβλητή. Έτσι, όλες οι εξισώσεις έχουν τη μορφή:

$$XW_i = b_i, \tag{2}$$

όπου X είναι μία από τις μεταβλητές που εμφανίζονταν στο αρχικό σύστημα. Ο στόχος μας είναι να βρούμε αυτήν την κύρια μεταβλητή X στο σύστημα (2). Αν επιτύχουμε, τότε μπορούμε να επαναλάβουμε τη διαδικασία προκειμένου να βρούμε όλες τις μεταβλητές του αρχικού συστήματος. Σε όσα θα ακολουθήσουν, εστιάζουμε την προσοχή μας σε συστήματα τύπου (2).

Θα ξεκινήσουμε περιγράφοντας έναν αλγόριθμο:

Έστω μία ομάδα G, η οποία παράγεται από τα στοιχεία $a_1, ..., a_m$, έστω μία συνάρτηση μήκους $l : G \to \mathbb{R}^+$ και έστω ότι έχει δοθεί σύστημα εξισώσεων της μορφής (2), $i = 1, ..., k$. Έστω $X \in G$, το οποίο έχει μια ελάχιστη μορφή ως: $X = a_{j_1}^{\sigma_1} a_{j_2}^{\sigma_2} \cdots a_{j_n}^{\sigma_n}$.

Ο αλγόριθμος που θα περιγράψουμε δημιουργεί μία διατεταγμένη λίστα από M ακολουθίες μήκους n, τέτοια ώστε, με σημαντική πιθανότητα, η ακολουθία $((j_1, \sigma_1), (j_2, \sigma_2), ..., (j_n, \sigma_n))$, η οποία κωδικοποιεί το X, να εμφανίζεται στη λίστα και μάλιστα τείνει να είναι το πρώτο της μέλος.
Ο αλγόριθμος απασχολεί μνήμη περίπου της τάξης του $M \cdot n$, όπου το M συνήθως επιλέγεται με βάση τους περιορισμούς του υπολογιστή.

Βήμα 1: Για κάθε $j = 1, 2, ..., m$ και $\sigma \in \{-1, 1\}$ υπολογίστε $a_j^{-\sigma} b_i = a_j^{-\sigma} XW_i$, για κάθε $i = 1, ..., k$ και δώστε στο (j, σ) την τιμή $\sum_{i=1}^{k} l(a_j^{-\sigma} b_i)$. Κρατείστε στη μνήμη τα M το πλήθος στοιχεία (j, σ) με τις μικρότερες τιμές.

Βήμα s>1: Για κάθε ακολουθία $((j_1, \sigma_1), ..., (j_{s-1}, \sigma_{s-1}))$ από τις M ακολουθίες που υπάρχουν στη μνήμη, για κάθε $j_s = 1, ..., m$ και κάθε $\sigma_s \in \{-1, 1\}$, υπολογίστε το άθροισμα των μηκών των στοιχείων

$$a_{j_s}^{-\sigma_s}(a_{j_{s-1}}^{-\sigma_{s-1}} \cdots a_{j_1}^{-\sigma_1} b_i) = a_{j_s}^{-\sigma_s} a_{j_{s-1}}^{-\sigma_{s-1}} \cdots a_{j_1}^{-\sigma_1} XW_i,$$

για $i = 1, ..., k$ και αποδώστε το τελικό αποτέλεσμα στην ακολουθία

$((j_1, \sigma_1), ..., (j_s, \sigma_s))$. Κρατείστε στη μνήμη τις M το πλήθος ακολουθίες με τις μικρότερες τιμές.

Τώρα, θα περιγράψουμε το πώς τερματίζει ο αλγόριθμος. Αν είναι γνωστό ότι το X μπορεί να γραφεί ως το γινόμενο το πολύ n γεννητόρων τότε ο αλγόριθμος θα πρέπει να τερματίζει μετά το βήμα n. Υπενθυμίζουμε ότι κάθε ζεύγος της μορφής (j_i, σ_i) επί της ουσίας κωδικοποιεί έναν γεννήτορα του X. Σε διαφορετική περίπτωση, η κατάσταση γίνεται πιο σύνθετη. Στη γενική περίπτωση, μπορούμε να σταματήσουμε τη διαδικασία όταν το άθροισμα των M τιμών αυξάνεται αντί να μειώνεται. Ωστόσο, σε πολλές περιπτώσεις ο τερματισμός του αλγορίθμου μπορεί να γίνει με πολύ πιο αποτελεσματικό τρόπο.

Στην περίπτωση των παραμετρικών εξισώσεων, στις εξισώσεις δηλαδή στις οποίες εμφανίζονται και γνωστές παράμετροι, αν μερικές από τις λέξεις W_i ξεκινούν με τη γνωστή παράμετρο P_i, τότε η απόφαση για το πότε θα σταματήσουμε μπορεί να ληφθεί πολύ πιο αποτελεσματικά: αν σε κάποιο βήμα το X έχει απαλοιφθεί από την εξίσωση, τότε γνωρίζουμε τις λέξεις W_i. Για να το ελέγξουμε, για κάθε μία από τις M επιλογές για το X, υπολογίζουμε τις λέξεις W_i και ελέγχουμε αν το άθροισμα των μηκών $l(P_i^{-1}W_i)$ είναι σημαντικά μικρότερο από αυτό των μηκών $l(W_i)$. Αυτή η διεργασία μας επιτρέπει να αποφανθούμε με σημαντική πιθανότητα για το πιο στοιχείο από τα M υποψήφια για το X είναι το σωστό.

Σε αυτό το σημείο, θα προχωρήσουμε στη μελέτη του προβλήματος συζυγίας, το οποίο μας αφορά και πιο άμεσα.
Η μεθοδολογία που περιγράψαμε για τις παραμετρικές εξισώσεις μπορεί να εφαρμοστεί και σε περιπτώσεις συστημάτων, τα οποία αποτελούνται μόνο από μία εξίσωση. Στην περίπτωση του παραμετρικού προβλήματος συζυγίας, δηλαδή όταν δίνονται τα XPX^{-1} και P και ζητείται η τιμή του X, ο αλγόριθμος μπορεί να τροποποιηθεί και να γίνει πολύ πιο αποτελεσματικός, αν σε κάθε βήμα s απαλοίφουμε τον γεννήτορα $a_{j_s}^{\sigma_s}$ και από τις δύο πλευρές του στοιχείου, προφανώς χρησιμοποιώντας και το αντίστροφό του.

Ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός ότι αν γνωρίζουμε το n εκ των προτέρων, δηλαδή αν γνωρίζουμε το μήκος του X ως προς τους γεννήτορες, τότε ο αρχικός αλγόριθμος λειτουργεί ακόμα και αν δεν γνωρίζουμε το στοιχείο P.

Ένα ακόμα παράδειγμα το οποίο είναι σημαντικό διότι εμφανίζεται πολύ συ-

χνά στα πρωτόκολλα, είναι το πρόβλημα μέλους ομάδας.

Έστω G μία πεπερασμένα παραγόμενη υποομάδα μιας μεγαλύτερης ομάδας L. Το πρόβλημα διατυπώνεται ως εξής: αν $g \in L$, τότε g ανήκει ή όχι στην G? Σε αυτήν την περίπτωση, απλώς εκτελούμε τον αλγόριθμο στο g χρησιμοποιώντας τους γεννήτορες της G και μετά από κάθε βήμα ελέγχουμε αν το g εχει κωδικοποιηθεί από κάποια ακολουθία από τις M. Μάλιστα, αυτή η μέθοδος μας παρέχει έναν πιθανοθεωρητικό τρόπο να εκφράσουμε το g ως γινόμενο των γεννητόρων της G.

Τέλος, για να ολοκληρώσουμε τη μελέτη της συγκεκριμένης έρευνας, θα αναφέρουμε κάποια στατιστικά στοιχεία, τα οποία προέκυψαν από πειράματα, προκειμένου να επιβεβαιώσουμε την εγκυρότητα των όσων αναφέραμε.

Τα πειράματα έγιναν σε υποομάδες της *braid group* B_N, $N = 8$, αριθμός αρκετά μεγάλος ώστε η ομάδα να μην είναι τετριμμένη και συγχρόνως όχι ιδιαίτερα μεγάλη προκειμένου να μπορούν να διεξαχθούν τα πειράματα. Η εργασία έγινε πάνω σε πεπερασμένα παραγόμενες υποομάδες οι οποίες είχαν επιλεγεί τυχαία. Στο πείραμα όπου εξετάστηκε η αποτελεσματικότητα του αλγορίθμου, οι παράμετροι (m, n, k, l, M) είχαν ως εξής:

1. m ήταν το πλήθος των γεννητόρων της υποομάδος, με τιμές 2, 4 ή 8.
2. n ήταν το πλήθος των γεννητόρων της ομάδας οι οποίοι πολλαπλασιάστηκαν έτσι ώστε να προκύψει το X, με τιμές 16, 32 ή 64.
3. k ήταν το πλήθος των δοσμένων εξισώσεων τύπου (2), με τιμές 1, 2, 4 ή 8.
4. l ήταν το πλήθος των γεννητόρων της ομάδας οι οποίοι πολλαπλασιάστηκαν έτσι ώστε να προκύψουν οι λέξεις W_i στις εξισώσεις της μορφής (2), με τιμές 4 ή 8
5. M ήταν η διαθέσιμη μνήμη, με τιμές 2, 4, 8, 16, 32, 64, 128, 256 ή 512.

Άρα, συνολικά, πρόκειται για ένα πείραμα 648 λιστών παραμέτρων το οποίο επαναλήφθηκε 16 φορές.

Στο 83% των πειραμάτων, το X βρισκόταν στη λίστα των M υποψηφίων για το ίδιο το X. Στο 75% των πειραμάτων, βρισκόταν μάλιστα στην πρώτη θέση

της λίστας. Συγκεκριμμένα, για M=512, η πιθανότητα το X να καταλήξει να βρίσκεται στις θέσεις 1, 2 και 3 είναι 0,83, 0,08 και 0,03 αντίστοιχα.

Τα πειράματα που αφορούν το πρόβλημα μέλους έγιναν με τιμές $k = 1$, $m = 4$ ή 8 και M=512. Σε αυτά τα πειράματα δινόταν ένα μοναδικό στοιχείο της μορφής XW και το ζητούμενο ήταν να βρεθεί αναπαράσταση του X ως προς τους δοσμένους γεννήτορες - πρόκειται, δηλαδή, για μια γενικευμένη περίπτωση του κλασσικού προβλήματος. Η επιτυχία ήταν της τάξης του 0,98.

Για να ολοκληρώσουμε τη μελέτη της συγκεκριμένης εργασίας, θα πρέπει να αναλύσουμε τα αποτελέσματά της.

Όπως προκύπτει άμεσα από τα πειραματικά δεδομένα, παρόλο που το πρωτόκολλο $Anshel - Anshel - Goldfeld$ βασίζεται στη δυσκολία του προβλήματος συζυγίας σε τυχαίες υποομάδες των *braid groups* και στη δυσκολία του προβλήματος μέλους, είναι εκτεθειμένο σε τέτοιου είδους επίθεση. Πιο συγκεκριμένα, τα πειράματα εκτελέστηκαν για μικρές τιμές μνήμης και προκύπτει ότι αν τις αυξήσουμε, τότε αυξάνονται σημαντικά και οι πιθανότητες επιτυχίας της επίθεσης. Εν κατακλείδι, φαίνεται πως για να 'θωρακιστεί' αυτό το πρωτόκολλο, καθώς και όλα όσα είναι εκτεθειμένα με τον ίδιο τρόπο, από αυτού του είδους την επίθεση, θα πρέπει να αυξηθούν σε τέτοιο βαθμό οι παράμετροι εργασίας έτσι ώστε να έχουν ως κατάληξη τη μη λειτουργικότητα του συστήματος. Για να γίνει αυτό πιο σαφές, απλά θα αναφέρουμε πως η αύξηση του δείκτη N σε μία *braid group* μειώνει αισθητά την αποτελεσματικότητα της επίθεσης.

Κεφάλαιο 3

Ομάδες - Πλατφόρμες

Στην συγκεκριμένη παράγραφο θα ασχοληθούμε με το πιο βασικό μέρος ενός πρωτοκόλλου, δηλαδή με την ομάδα πάνω στην οποία εργαζόμαστε ή, όπως αλλιώς λέμε, την ομάδα - πλατφόρμα. Έχοντας ήδη αναφέρει ορισμένα πρωτόκολλα κάθως επίσης και τους τρόπους με τους οποίους μπορεί κανείς να τους επιτεθεί, μπορούμε πλέον να θέσουμε όρους ως προς την επιλογή ομάδας.

Γενικά, μπορούμε να πούμε ότι για τις ομάδες των πρωτοκόλλων, τα οποία βασίζονται στο πρόβλημα έρευνας συζυγίας, απαιτείται η ικανοποίηση ορισμένων προϋποθέσεων. Αυτές οι προϋποθέσεις, σε γενικές γραμμές, πρέπει να πληρούνται σε κάθε κανονικό κρυπτογραφικό πρωτόκολλο, δηλαδή σε κάθε σχήμα το οποίο βασίζεται σε συνάρτηση μίας κατεύθυνσης. Ας δούμε ποιες ακριβώς είναι αυτές:

(ΠΡ1): Η ομάδα πρέπει να είναι γνωστή και καλά μελετημένη.

(ΠΡ2): Το πρόβλημα λέξης μέσα στην ομάδα πρέπει να έχει γρήγορη λύση από κάποιον ντετερμινιστικό αλγόριθμο. Λέγοντας 'γρήγορη λύση' εννοούμε γραμμικού ή τετραγωνικού χρόνου. Ακόμα καλύτερα, μια αποτελεσματικά υπολογίσιμη 'κανονική μορφή' για τα στοιχεία της ομάδας.

(ΠΡ3): Θα πρέπει να υπάρχει τρόπος να 'παραλλάσσονται' τα στοιχεία της ομάδας, έτσι ώστε να μην είναι δυνατό να αναγνωριστούν, για παράδειγμα, τα x, y από γνωστό γινόμενο xy απλά μέσω παρατήρησης. Επισημαίνουμε ξανά τη χρησιμότητα ύπαρξης αποτελεσματικά υπολογίσιμης κανονικής μορφής. Στην

περίπτωση που δεν υπάρχει κανονική μορφή, με την έννοια ότι η ομάδα μας έχει δοθεί με τη μορφή παράστασης και χωρίς επιπρόσθετες πληροφορίες για ιδιότητες, τότε θα πρέπει τουλάχιστον κάποιες από τις ορίζουσες σχέσεις να έχουν πολύ μικρό μήκος.

(ΠΡ4): Η ομάδα πρέπει να υπερ-πολυωνυμικής (εκθετικής ή μέσης) ανάπτυξης, δηλαδή πρέπει το πλήθος των στοιχείων μήκους n της ομάδας να αυξάνεται ταχύτερα από κάθε πολυώνυμο του n. Αυτό είναι απαραίτητο προκειμένου να είναι ασφαλές το πρωτόκολλο απέναντι σε επιθέσεις πλήρους εξάντλησης του χώρου του κλειδιού. Σε αυτό το σημείο θα αναφέρουμε ότι μέσης επέκτασης ονομάζονται οι ομάδες οι οποίες δεν είναι ούτε πολυωνυμικής ούτε εκθετικής επέκτασης. Την ύπαρξή τους απέδειξε ο $O.Grigorchuk$ το 1983.

(ΠΡ5): Σε πρωτόκολλα στα οποία γίνεται χρήση είτε μεταθετικότητας είτε προβλημάτων συζυγίας ή αποδόμησης είναι σημαντικό να αποφεύγονται κανονικές υποομάδες.

Στη συνέχεια, θα αναφέρουμε κάποια είδη ομάδων, ορισμένα έχουν αναφερθεί ήδη και αλλά θα τα συναντήσουμε αργότερα, τα οποία έχουν έντονη παρουσία σε διάφορα πρωτόκολλα.

3.1 *Braid Groups*

Τις *braid groups* τις είδαμε στη συζήτηση που κάναμε για το πρωτόκολλο $Anshel - Anshel - Goldfeld$. Αρχικά, είχαν επιλεχθεί καθώς θεωρήθηκαν καταλλήλες ως μη αβελιανές ομάδες, ωστόσο στη συνέχεια φάνηκε πως ίσως δεν παρείχαν επαρκές επίπεδο ασφαλείας (είδαμε στοιχεία και γι΄ αυτό). Τώρα, θα δούμε διάφορα πλεονεκτήματα και μειονεκτήμα τους.

Ένα βασικό μειονέκτημά τους είναι ότι εμφανίζονται σε πολλά προβλήματα και ποικίλες περιοχές της άλγεβρας. Αυτό σημαίνει πως είναι δυνατό κάποιος επίδοξος κρυπταναλυτής να αντλήσει εργαλεία από διάφορες πηγές.

Σε αυτό το σημείο, είναι χρήσιμο να ορίσουμε και τυπικά τις *braid groups*.

Δεν θα αναφερθούμε στην αλγεβρική παράστασή τους και θα δώσουμε απευθείας τον ορισμό τους:

$B_n = \langle x_1, ..., x_{n-1} | x_i x_j x_i = x_j x_i x_j$ αν $|i-j| = 1$, $x_i x_j = x_j x_i$ αν $|i-j| > 1 \rangle$.

Θα εξετάσουμε το κατά πόσο οι *braid groups* πληρούν τις προϋποθέσεις που θέσαμε για τις ομάδες - πλατφόρμες. Αρχικά, όπως ήδη έχουμε αναφέρει, είναι ιδιαίτερα γνωστές και έχουν μελετηθεί αρκετά. Επιπλέον, τα προβλήματα λέξης και συζυγίας έχουν μελετηθεί σε πολύ σημαντικό βαθμό. Μάλιστα, υπάρχει ντετερμινιστικός αλγόριθμος για το πρόβλημα λέξης ο οποίος έχει πολυπλοκότητα τετραγωνικού χρόνου ως προς το μήκος της λέξης εισαγωγής. Επίσης, για το συγκεκριμένο πρόβλημα, υπάρχουν αλγόριθμοι με πολυπλοκότητα γραμμικού χρόνου στη γενική τους περίπτωση. Ωστόσο, αυτοί οι αλγόριθμοι δίνουν γρήγορη απάντηση μόνο για την αρνητική εκδοχή του προβλήματος λέξης, κατά την οποία δηλαδή το στοιχείο είναι διάφορο του μοναδιαίου της *braid group*. Αντίθετα, ο αλγόριθμος του *Doherty* δίνει γρήγορη απάντηση και για τη θετική περίπτωση, όμως γι΄ αυτόν δεν έχει βρεθεί υποεκθετικό άνω φράγμα για την πολυπλοκότητά του.

Το πρόβλημα συζυγίας στις *braid groups* διαχρονικά βρίσκεται στο επίκεντρο πολλών ερευνών και πρόσφατα έχει υπάρξει ιδιαίτερη δραστηριότητα όσον αφορά την χειρότερη εκδοχή πολυπλοκότητας. Ωστόσο, είναι ακόμα ανοικτό το αν υπάρχει λύση πολυωνυμικού χρόνου για τα προβλήματα έρευνας και απόφασης συζυγίας. Είναι ανοικτό ακόμα και το αν το πρόβλημα συζυγίας ανήκει στην κλάση πολυπλοκότητας μη - ντετερμινιστικού πολυωνυμικού χρόνου (ασθενέστερο του προηγούμενου).

Όσον αφορά την (ΠΡ3), υπάρχουν ποικίλες κανονικές μορφές για τα στοιχεία των *braid groups*, οι οποίες μπορούν να χρησιμοποιηθούν και ως μηχανισμοί απόκρυψης. Ωστόσο, αυτή η ποικιλία στις κανονικές μορφές εγκυμονεί κινδύνους, με την έννοια ότι μία μορφή μπορεί να αποκαλύψει αυτό που προσπαθεί μία άλλη να αποκρύψει. Μάλιστα, αυτό το μειονέκτημα έχει ήδη αξιοποιηθεί σε σχήμα κρυπτανάλυσης.

Τέλος, σχετικά με την (ΠΡ4), αναφέρουμε ότι για $n \geq 2$, όλες οι *braid groups* B_n εχουν εκθετική επέκταση.

3.2 Η Ομάδα *Thompson*

Αρχικά, θα αναφέρουμε ότι οι ομάδες *Thompson*, F, απαντώνται σε πολλούς κλάδους των μαθηματικών όπως την άλγεβρα, τη γεωμετρία και την ανάλυση. Ως εκ τούτου είναι και αυτές καλά μελετημένες και άρα, πληρούν την (ΠΡ1). Επίσης, είναι άπειρες και μη αβελιανές και, επομένως, ελκυστικές στο να χρησιμοποιηθούν ως πλατφόρμες για πρωτόκολλα.

Αρχικά, θα αναφέρουμε μία άπειρη (και κομψή) παράσταση της ομάδας η οποία, όπως θα δούμε στη συνέχεια, μας επιτρέπει να κατασκευάσουμε μία πολύ βολική κανονική μορφή:

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

Ας δούμε τώρα ποια ακριβώς είναι η λεγόμενη 'κλασσική' κανονική μορφή των στοιχείων της ομάδας *Thompson*.

Ως κανονική μορφή ενός στοιχείου αυτής της ομάδας ορίζεται μία λέξη της μορφής:

$$x_{i_1} \cdots x_{i_s} x_{j_t}^{-1} \cdots x_{j_1}^{-1},$$

ετσι ώστε να πληρούνται τα εξής δύο κριτήρια:

(ΚΜ1): $i_1 \leq \cdots \leq i_s$ και $j_1 \leq \cdots \leq j_t$.
(ΚΜ2): αν εμφανίζονται τα x_i και x_i^{-1}, τότε εμφανίζεται είτε το x_{i+1} είτε το x_{i+1}^{-1} επίσης.

Ακόμη, λέμε ότι μία λέξη είναι ημικανονικής μορφής αν έχει τη μορφή που αναφέραμε παραπάνω και πληρεί μόνο το (ΚΜ1).

Σε αυτό το σημείο. θα αναφέρουμε απλά ότι υπάρχει αλγόριθμος ο οποίος σε πρώτο χρόνο απλοποιεί μια τυχαία λέξη, φέρνοντάς την σε ημικανονική μορφή και, στη συνέχεια, την εκφράζει σε κανονική. Έχει δειχθεί ότι ο χρόνος υπολογισμού της κανονικής μορφής ενός τυχαίου στοιχείου της ομάδας *Thompson* είναι $O(|w|log|w|)$.

Όσον αφορά τις ιδιότητες της ομάδας $Thompson$, γνωρίζουμε ότι έχουν εκθετική επέκταση [5], δηλαδή αναφερόμαστε στην (ΠΡ4).

Για να κλείσουμε τη συγκεκριμένη υποπαράγραφο, θα αναφέρουμε ότι έχει προταθεί μία αποτελεσματική επίθεση στο πρόβλημα (έρευνας) αποδόμησης και αυτό οφείλεται στο ότι η ταυτόχρονη παρουσία δύο κανονικών μορφών για τα στοιχεία της ίδιας ομάδας μπορεί να είναι πηγή κινδύνου - η μία ενδέχεται να αποκαλύπτει αυτό που προσπαθεί η άλλη να κρύψει. Ανάλογη αναφορά είχαμε κάνει και στην υποπαράγραφο που αφορούσε τις $braid\ groups$.

3.3 *Small Cancellation Groups*

Για να οριστούν οι $Small\ Cancellation\ Groups$ χρειάζεται να εισάγουμε πρώτα κάποιες έννοιες.

Έστω $F(X)$ η ελεύθερη ομάδα η οποία παράγεται από το αλφάβητο
$X = \{x_i | i \in I\}$, όπου I είναι ένα συνολο δεικτών.
Μία λέξη $w(x_1, ..., x_n) = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_n}^{\epsilon_n}$, όπου $\epsilon_k \in \{-1, 1\}$ και τα x_{i_k} δεν είναι απαραίτητα διακεκριμένα, στην $F(X)$ ονομάζεται ανηγμένη X - λέξη αν έχει την ιδιότητα: $x_{i_k}^{\epsilon_k} \neq x_{i_{k+1}}^{-\epsilon_{k+1}}$ για $1 \leq k \leq n-1$.
Επιπλέον, η λέξη $w(x_1, ..., x_n)$ λέγεται κυκλικά ανηγμένη αν είναι ανηγμένη και $x_{i_1}^{\epsilon_1} \neq x_{i_n}^{-\epsilon_n}$.
Ένα σύνολο R, το οποίο περιέχει κυκλικά ανηγμένες λέξεις της $F(X)$, ονομάζεται συμμετρικοποιημένο αν είναι κλειστό ως προς τις κυκλικές μεταθέσεις και τις αντιστροφές των στοιχείων του.

Εστω η ομάδα $G = \langle X | R \rangle$. Μία μη κενή λέξη $u \in F(X)$ ονομάζεται τμήμα εάν υπάρχουν δύο διακεκριμένες ορίζουσες σχέσεις $r_1, r_2 \in R$ τέτοιες ώστε $r_1 = uv_1$ και $r_2 = uv_2$ για κάποια $v_1, v_2 \in F(X)$ και χωρίς να υπάρχει καμία διαγραφή μεταξύ των u και v_1 ή των u και v_2. Η ομάδα G ανήκει στην κλάση $C(p)$ εάν κανένα στοιχείο του R δεν είναι γινόμενο λιγότερων των p τμημάτων. Επίσης, η ομάδα ανήκει στην κλάση $C'(\lambda)$ εάν για κάθε $r \in R$ τέτοιο ώστε $r = uv$ με u τμήμα, ισχύει ότι $|u| < \lambda |r|$.

Εάν η $G = \langle X|R\rangle$ ανήκει στην κλάση $C(p)$ (αντίστοιχα στην $C'(\lambda)$)τότε λέμε ότι ικανοποιεί την $C(p)$ *small cancellation condition* (αντίστοιχα την $C'(\lambda)$ *small cancellation condition*).

3.3.1 Ο Αλγόριθμος του *Dehn*

Εάν η G ανήκει στην κλάση $C'(1/6)$, τότε ο αλγόριθμος του *Dehn* λύνει αποτελεσματικά το πρόβλημα λέξης εντός της ομάδας. Άρα, ικανοποιείται η (ΠΡ2). Εφόσον γίνεται αναφορά σε αυτόν σε πρωτόκολλο το οποίο θα αναλυθεί αργότερα, θα τον περιγράψουμε αναλυτικά:

1. Σε μία εισρέουσα μη κενή λέξη w αναζητείστε ένα 'μεγάλο' μέρος κάποιας ορίζουσας σχέσης (δηλαδή, μέρος του οποίου το μήκος να είναι μεγαλύτερο από το μισό μήκος της ορίζουσας σχέσης). Εάν δεν υπάρχει τέτοιο μέρος επιστρέψτε το μήνυμα '$w \neq 1$ στην G'.

2. Εάν τέτοιο τμήμα, έστω u, πράγματι υπάρχει, τότε ισχύει ότι $r = uv$ για κάποιο $r \in R$, όπου το μήκος του v είναι μικρότερο από αυτό του u. Τότε, αντικαταστείστε το στοιχείο u με το v^{-1} εντός της w. Το μήκος της νέας λέξης w' είναι μικρότερο από αυτό της w. Εάν $w' = 1$, τότε επιστρέψτε το μήνυμα '$w = 1$ στην G'.

3. Εάν $w' \neq 1$, τότε επαναλάβετε το βήμα 1 για w'.

Εφόσον το μήκος του w μειώνεται με κάθε επανάληψη, είναι σαφές ότι ο αλγόριθμος τερματίζει σε πεπερασμένα το πλήθος βήματα. Η πολυπλοκότητά του είναι τετραγωνικού χρόνου ως προς το μήκος της λέξης εισροής.

3.4 Επιλύσιμες Ομάδες

Ορισμός: Έστω F_n μία ελεύθερη ομάδα διάστασης n. Η σχετικά ελεύθερη ομάδα F_n/F_n'' ονομάζεται ελεύθερη μετα-αβελιανή ομάδα διάστασης n και συμβολίζεται με M_n.

(Υπενθυμίζουμε ότι $G' = [G, G]$ και άρα $G'' = [G', G']$. Με $[G, G]$ συμβολίζουμε την ομάδα που παράγεται από τα στοιχεία $[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$, με $g_1, g_2 \in G$.)

Είναι σημαντικό να αναφέρουμε σε αυτό το σημείο ότι υπάρχει αλγόριθμος πολυπλοκότητας το πολύ τετραγωνικού χρόνου ως προς το μήκος της λέξης εισροής, ο οποίος επιλύει το πρόβλημα λέξης στην M_n.

Για τα στοιχεία της M_n υπάρχουν μία κανονική (καλώς ορισμένη) και μία ημικανονική (όχι καλώς ορισμένη) μορφή. Συνεπώς, η ημικανονική μορφή για $n>2$ δεν είναι μοναδική και γι΄ αυτόν το λόγο δεν μπορεί να χρησιμοποιηθεί ως κοινό κλειδί σε πρωτόκολλα. Ο υπολογισμός της απαιτεί τετραγωνικό χρόνο ως προς το μήκος της λέξης εισροής και είναι χρήσιμη για τις διαβιβάσεις (μετατρέπεται εύκολα σε λέξη).

Εφόσον η ημικανονική μορφή δεν μπορεί να αξιοποιηθεί στα πλαίσια πρωτοκόλλων, εισάγεται μία κανονική μορφή - ένας 2×2 πίνακας - η οποία είναι μοναδική και υπολογίζεται αποτελεσματικά (τετραγωνικός χρόνος ως προς το μήκος της λέξης εισροής). Ως μειονέκτημα μπορούμε να αναφέρουμε το γεγονός ότι δεν μετατρέπεται εύκολα σε λέξη.

Αυτή η κανονική μορφή προέρχεται από τη γνωστή εμφύτευση $Magnus\ embedding$. Δεν θα αναφέρουμε περισσότερα γι΄ αυτήν την εμφύτευση, καθώς η μελέτη της ξεφεύγει από τα πλαίσια της εργασίας.

3.5 Η Ομάδα *Grigorchuk*

Η ομάδα *Grigorchuk*, την οποία συμβολίζουμε με Γ, εμφανίζεται σε πολλά προβλήματα που αφορούν τη θεωρία ομάδων και πρόσφατα προτάθηκε και ως πλατφόρμα για συγκεκριμένο πρωτόκολλο κρυπτογράφησης. Για να μπορέσουμε να ορίσουμε την ομάδα, θα πρέπει πρώτα να αναφέρουμε κάποια στοιχεία.

Έστω το άπειρο δυαδικό δέντρο με ρίζα το οποίο συμβολίζουμε με $\mathcal{T}$. Το σύνολο Τ των κορυφών του είναι το σύνολο των δυαδικών ακολουθιών. Για να είναι πιο σαφές τι ακριβώς εννοούμε με τον όρο 'δυαδικό δέντρο με ρίζα', θα αναφέρουμε τα εξής:
Το δέντρο εκκινεί από ένα σημείο το οποίο ονομάζεται ρίζα και συμβολίζεται με ε. Στη συνέχεια, εξετάζοντας με τη σειρά τους όρους μίας δυαδικής ακολουθίας, κατευθυνόμαστε σε δεξί κλάδο αν το ψηφίο είναι το 1 και σε αριστερό αν είναι το 0.

Τώρα, μπορούμε να ξεκινήσουμε τη μελέτη.

Επίπεδα ενός δυαδικού δέντρου $\mathcal{T}$ ονομάζουμε τα σύνολα κορυφών
$L_k = \{b_1...b_k | b_i \in \{0,1\}\}$.

Οι αυτομορφισμοί φ του $\mathcal{T}$ αφήνουν σταθερή τη ρίζα του δέντρου και μεταθέτουν τις κορυφές διατηρώντας τις μεταξύ τους συνδέσεις, με την έννοια ότι αν οι κορυφές u_1 και u_2 συνδέονται με μία ακμή, τότε θα συμβαίνει το ίδιο και για τις κορυφές $\varphi(u_1)$ και $\varphi(u_2)$.
Σε αυτό το σημείο θα θεωρήσουμε έναν συγκεκριμένο αυτομορφισμό, τον α, ο οποίος έχει την ιδιότητα: $\alpha(b_1, b_2, ..., b_n)=(1-b_1, b_2, ..., b_n)$. Επίσης, τα στοιχεία της ομάδας $Aut(\mathcal{T})$ τα οποία αφήνουν αμετάβλητα τα στοιχεία του επιπέδου 1, συμβολίζονται με $St(1)$.

Ως ομάδα *Grigorchuk* Γ ορίζουμε την υποομάδα της $Aut(\mathcal{T})$, την παραγόμενη από τα 4 στοιχεία: α, β, γ, δ. Το στοιχείο α είναι όπως το ορίσαμε παραπάνω. Τα υπόλοιπα 3 ορίζονται αναδρομικά ως εξής:

$\beta(b_1, b_2, ..., b_n) = \{(b_1, 1-b_2, b_3, ..., b_n)$ αν $b_1 = 0$, $(b_1, \gamma(b_2, ..., b_n))$ αν $b_1 = 1\}$

$\gamma(b_1, b_2, ..., b_n) = \{(b_1, 1-b_2, b_3, ..., b_n)$ αν $b_1 = 0$, $(b_1, \delta(b_2, ..., b_n))$ αν $b_1 = 1\}$

$\delta(b_1, b_2, ..., b_n) = \{(b_1, b_2, b_3, ..., b_n)$ αν $b_1 = 0$, $(b_1,\beta(b_2, ..., b_n))$ αν $b_1 = 1\}$

Είναι σαφές πως όλες αυτές οι απεικονίσεις είναι αυτομορφισμοί της ομάδας $\mathcal{T}$ ενώ παράλληλα είναι και στοιχεία του $St(1)$. Το παρακάτω παράδειγμα αποσαφηνίζει τον αναδρομικό ορισμό των στοιχείων:

$\beta(1, 1, 1, 0, 1) = (1,\gamma(1, 1, 0, 1)) = (1, 1,\delta(1, 0, 1)) = (1, 1, 1,\beta(0, 1) = (1, 1, 1, 0, 0).$

Σε αυτό το σημείο θα διατυπώσουμε τα σημαντικότερα αποτελέσματα που αφορούν την ομάδα $Grigorchuk$:

• Υπάρχει αλγόριθμος, τον οποίο δεν θα περιγράψουμε στη σύντομη αναφορά μας, ο οποίος επιλύει το πρόβλημα ταυτότητας (ή λέξης) στην ομάδα $Grigorchuk$, σε χρόνο $O(|w|log|w|)$.

• Υπάρχει κανονική μορφή ρ_w της λέξης $w \in \Gamma$, η οποία είναι ένα πεπερασμένο δυαδικό δέντρο με κορυφές οι οποίες χαρακτηρίζονται από τα στοιχεία της Γ {1, α, β, γ, δ}.

• Δύο λέξεις $u = u(\alpha,\beta,\gamma,\delta)$ και $v = v(\alpha,\beta,\gamma,\delta)$ αντιπροσωπεύουν το ίδιο στοιχείο της Γ αν και μόνο αν ρ_u=ρ_v.

• Υπάρχει αλγόριθμος ο οποίος για κάθε λέξη $w = w(\alpha,\beta,\gamma,\delta)$ υπολογίζει την αντίστοιχη κανονική μορφή ρ_w σε χρόνο $O(|w|log_2|w|)$.

3.6 Ομάδες Πινάκων

Για το τέλος του κεφαλαίου αφήσαμε τις ομάδες πινάκων πάνω σε πεπερασμένους μεταθετικούς δακτυλίους διότι διαθέτουν χαρακτηριστικά που φαίνεται να τις καθιστούν την καλύτερη επιλογή για το ρόλο της πλατφόρμας πρωτοκόλλων όπως αυτά που έχουμε ήδη περιγράψει.

Το βασικό πλεονέκτημα είναι η μη μεταθετικότητα του πολλαπλασιασμού των

πινάκων η οποία όμως συνδυάζεται με τη μεταθετικότητα των εγγραφών τους. Έτσι, εξασφαλίζεται η αποτελεσματική απόκρυψη των στοιχείων της ομάδας (ΠΡ3). Όσον αφορά την παραλλαγή των στοιχείων, έχουμε δει ότι ουσιαστικά αυτό εξασφαλίζεται από τις κανονικές μορφές που εισάγουμε κατά περίπτωση. Το πλεονέκτημα με τους πίνακες είναι ότι αποτελούν κανονικές μορφές από μόνοι τους εξαιτίας του τρόπου γραφής τους, χωρίς να χρειάζονται επιπλέον υπολογισμοί. Μάλιστα, ήδη έχουμε δει παράδειγμα κανονικής μορφής κατά το οποίο αντιστοιχούνται στοιχεία κάποιας ομάδας με πίνακες.

Ο λόγος για τον οποίο προτιμείται ο δακτύλιος να είναι πεπερασμένος έχει να κάνει με το ότι έτσι εξασφαλίζεται καλύτερη απόκρυψη. Πράγματι, η περιοδικότητα του δακτυλίου εξασφαλίζει πολλαπλούς τρόπους γραφής για το κάθε στοιχείο. Άρα, η περιοδικότητα σε συνδυασμό με τη μεταθετικότητα προσδίδουν στην ομάδα σημαντική δυναμική ως προς τους μηχανισμούς απόκρυψης στοιχείων. Και, επαναλαμβάνουμε, ότι η μεταθετικότητα των στοιχείων του πίνακα συνδυάζεται με την αντιμεταθετικότητα των ίδιων των πινάκων δίνοντας μας έτσι ένα ιδιαίτερα αποτελεσματικό μείγμα.

Σε αυτό το σημείο θα αναφέρουμε ορισμένα πρακτικά παραδείγματα, δηλαδή θα μελετήσουμε περιπτώσεις πεπερασμένων μεταθετικών δακτυλίων.

Η πιο απλή επιλογή θα ήταν ο $\mathbb{Z}_n$. Οι πίνακες επί του συγκεκριμένου δακτυλίου μπορούν να χρησιμοποιηθούν ως πλατφόρμες για το πρωτόκολλο ανταλλαγής κλειδιού $Diffie-Hellman$ με προφανές μειονέκτημα, όμως, το ότι θα πρέπει το n να είναι ιδιαίτερα μεγάλο προκειμένου να εξασφαλιστεί ένας επαρκώς μεγάλος χώρος κλειδιού. Πάντως, για τη συγκεκριμένη περίπτωση, θα αναφέρουμε ότι έχει γίνει ουσιαστικά ελάχιστη έρευνα σχετικά με τον αν είναι πιο αποδοτική η ομάδα πινάκων επί του $\mathbb{Z}_n$ από τον ίδιο τον $\mathbb{Z}_n$ σε θέματα ασφαλείας.

Μία άλλη επιλογή είναι ο $R = F_p[x]/(f(x))$, όπου F_p είναι το σώμα p στοιχείων, $F_p[x]$ ο αντίστοιχος πολυωνυμικός δακτύλιος και $(f(x))$ το ιδεώδες το οποίο παράγεται από το ανάγωγο πολυώνυμο $f(x)$ βαθμού n. Ο δακτύλιος R είναι ισομορφικός με το σώμα F_{p^n}, αλλά η εμφάνιση του R ως πηλίκο παρέχει ένα μεγάλο χώρο κλειδιού ενώ παράλληλα διατηρεί όλες τις βασικές παραμέτρους ιδιαίτερα μικρές. Ένα τέτοιο σώμα χρησιμοποιήθηκε από τους $Tillich$ και $Zemor$ με παραμέτρους $p = 2$ και $100<n<200$. Οι πίνακες που χρησιμοποίησαν άνηκαν στην ομάδα $SL_2(R)$. Οι δύο ερευνητές δημιούργησαν μια $hash\ function$, δηλαδή μία συνάρτηση μίας κατεύθυνσης η οποία αντιστοιχίζει

δεδομένα σε ακολουθίες στοιχείων. Ωστόσο, πρέπει να αναφέρουμε πως μετά από χρόνια ερευνών, καταρρίφθηκε η ιδιότητα *collision resistance* η οποία είναι απαραίτητη προϋπόθεση για κάθε *hash function* που χρησιμοποιείται στον κλάδο της κρυπτογραφίας [6][7].

Η ίδια ιδέα θα μπορούσε να βελτιωθεί με τη χρήση του δακτυλίου των *truncated* πολυωνύμων επί του $\mathbb{Z}_n$. *Truncated* πολυώνυμα, ή πιο σωστά N-*truncated* πολυώνυμα μιας μεταβλητής, είναι εκφράσεις της μορφής $\sum_{k=0}^{N} a_k x^k$ με τη συνήθη πρόσθεση και πολλαπλασιασμό τέτοιον ώστε $x^i \cdot x^j = x^{(i+j)mod(N+1)}$. Ουσιαστικά, βρίσκεται στο ίδιο μήκος κύματος με το δακτύλιο R που αναφέραμε παραπάνω, μόνο που εδώ αντί για το ανάγωγο πολυώνυμο $f(x)$ χρησιμοποιείται το πολύ πιο απλό $x^{(N+1)}$. Αυτό έχει ως αποτέλεσμα το ότι ο R παύει να είναι σώμα και το ότι οι υπολογισμοί εντός του γίνονται αρκετά αποτελεσματικά. Επίσης, με 'μικρό κόστος' επιτυγχάνεται μεγάλος χώρος κλειδιού. Για παράδειγμα, για $n = 100$ και $N = 20$, προκύπτουν $100^{21} = 10^{42}$ $N-truncated$ πολυώνυμα. Έτσι, μπορούν να προκύψουν 10^{168} το πλήθος 2×2 πίνακες σε αυτόν το δακτύλιο.

Κεφάλαιο 4

Το Πρωτόκολλο *Shpilrain - Zapata*

4.1 Εισαγωγή

Το κεντρικό θέμα αυτής της ενότητας έχει να κάνει με το πρωτόκολλο $Shpilrain-Zapata$ το οποίο βασίζεται στο πρόβλημα λέξης σε περιβάλλον ομάδων. Η ιδέα της χρήσης του συγκεκριμένου προβλήματος σε πρωτόκολλα εμφανίζεται, ουσιαστικά για πρώτη φορά, στο πρωτόκολλο δημοσίου κλειδιού $Wagner - Magyarik$ το 1985. Οι δημιουργοί του είχαν πιστεί πως είχαν κατασκευάσει ένα δυνατό εργαλείο κρυπτογράφησης βασισμένο στο πρόβλημα λέξης. Ωστόσο, όπως αποδείχθηκε στη συνέχεια από τους $Gonzales - Vasco/Steinwandt$ και τους $Baumslag/Myasnikov/Shpilrain$ το συγκεκριμένο σύστημα όχι μόνο δεν ήταν ασφαλές αλλά επί της ουσίας δεν βασιζόταν καν στο πρόβλημα λέξης αλλά στο πρόβλημα επιλογής λέξης. Συνεπώς, προκειμένου να ακοκτήσει ο αναγνώστης σφαιρική γνώση επί του θέματος, θα ήταν καλό να ξεκινήσουμε την ενότητα με αναφορά σε αυτήν την πρωτόλεια προσπάθεια [8].

4.2 Το Πρωτόκολλο των $Wagner - Magyarik$

Έστω X ένα πεπερασμένο σύνολο γεννητόρων και R, S πεπερασμένα σύνολα οριζουσών σχέσεων τέτοια ώστε να πληρούνται οι εξής προϋποθέσεις:
Για την ομάδα $G = \langle X|R\rangle$ το πρόβλημα λέξης επιλύεται δύσκολα, ενώ για την ομάδα $H = \langle X|R \cup S\rangle$ επιλύεται εύκολα.
Η Αλίκη χρησιμοποιεί το σύνολο S ως ιδιωτικό κλειδί, ενώ η ομάδα G μαζί

με δύο επιλεγμένες λέξεις W_0 και W_1, οι οποίες δεν είναι ισοδύναμες στην H, αποτελούν το δημόσιο κλειδί.
Ας υποθέσουμε ότι ο Βασίλης θέλει να στείλει στην Αλίκη το δικό του ιδιωτικό κλειδί, το οποίο είναι μια δυαδική ακολουθία. Τότε σύμφωνα με το πρωτόκολλο θα ακολουθήσει την εξής διαδικασία:
Για να κρυπτογραφήσει το ψηφίο i, θα επιλέξει τη λέξη W_i και θα εφαρμόσει σε αυτήν μετασχηματισμούς $Tietze$ με τυχαίο τρόπο, δημιουργώντας εν τέλει μια καινούρια λέξη: την W, την οποία και αποστέλλει.
Η Αλίκη προκειμένου να αποκρυπτογραφήσει, καλείται να ελέγξει κατά πόσο το γινόμενο WW_i^{-1} ισούται με 1 εντός της H. Ουσιαστικά το σχήμα βασίζεται στην ευκολία επίλυσης του προβλήματος λέξης στην H (για την Αλίκη) και στην αντίστοιχη δυσκολία στην G (για την Εύα).

Στην εισαγωγή της ενότητας αναφέραμε ότι το πρόβλημα που επιστρατεύεται δεν είναι αυτό της λέξης αλλά της επιλογής λέξης. Η διαφορά συνίσταται στο εξής: το πρόβλημα επιλογής λέξης ενέχει την αρχική συνθήκη ότι το W ισούται με κάποιο από τα W_i. Δυστυχώς, για τη συγκεκριμένη περίπτωση αποδείχθηκε ότι το πρόβλημα επιλογής λέξης είναι αναδρομικά επιλύσιμο για κάθε αναδρομικά παριστώμενη ομάδα και άρα δεν μπορεί να χρησιμοποιηθεί.

4.3 Το Πρωτόκολλο των $Shpilrain - Zapata$

Ο $Vladimir\ Shpilrain$ οπως είδαμε ήταν ανάμεσα σε αυτούς που κατέδειξαν τα προβλήματα του πρωτοκόλλου $Wagner - Magyarik$. Στη συνέχεια, σε συνεργασία με τον $Gabriel\ Zapata$, ανέπτυξαν ένα καινούριο πρωτόκολλο βασισμένο στις ίδιες ιδέες (δυσκολία επίλυσης του προβλήματος λέξης) το οποίο όμως αντιμετώπισε τις αδυναμίες που είχαν εντοπιστεί. Πριν ξεκινήσουμε την επί της ουσίας μελέτη, ας δούμε επακριβώς τη λειτουργία του:

1. Θεωρούμε ένα κοινοποιημένο σύνολο παραστάσεων εντός των οποίων επιλύεται εύκολα το πρόβλημα λέξης.

2. Η Αλίκη επιλέγει τυχαία μια τέτοια παράσταση, έστω Γ, και την επεξεργάζεται μέσω των μετασχηματισμών $Tietze$.
   Προκύπτει η παράσταση Γ′.
   Η Αλίκη αφαιρεί κάποιες ορίζουσες σχέσεις από την Γ′ δημιουργώντας μια καινούρια παράσταση $\hat{\Gamma}$, την οποία και κοινοποιεί.

3. Ο Βασίλης έχει ένα ιδιωτικό κλειδί στη μορφή δυαδικής ακολουθίας.
   Αν ένα ψηφίο ισούται με 1, το αντικαθιστά με στοιχείο ίσο με τη μονάδα της ομάδας $\hat{\Gamma}$.
   Αν ένα ψηφίο ισούται με 0, το αντικαθιστά με οποιοδήποτε στοιχείο διάφορο της μονάδας.
   Στη συνέχεια, μεταδίδει την τελική μορφή.

4. Η Αλίκη παραλαμβάνει τα στοιχεία και τα αντιμετωπίζει ως στοιχεία της Γ'.
   Μέσω του ισομορφισμού που έχει προκύψει από τους μετασχηματισμούς *Tietze*, τα μετατρέπει σε στοιχεία της Γ.
   Τέλος, επιλύει το πρόβλημα λέξης στη Γ.

Τώρα, θα προχωρήσουμε στην ιδιαίτερη ανάλυση του καθενός από τα παραπάνω τέσσερα βήματα του πρωτοκόλλου.

4.3.1 Το Σύνολο των Παραστάσεων

Για το πρώτο βήμα του πρωτοκόλλου η ανάλυση που μπορεί να γίνει είναι υπαρξιακού χαρακτήρα, δηλαδή το κάτα πόσο είναι εγγυημένη η μη τετριμμένη ύπαρξη ομάδων εντός των οποίων να επιλύεται αποτελεσματικά το πρόβλημα λέξης. Όπως προκύπτει από την έρευνα που έχει γίνει για το συγκεκριμένο σχήμα, η αποτελεσματικότητα μεταφράζεται ως τετραγωνικός χρόνος ως προς το μήκος της λέξης. Όσον αφορά στην ουσία του θέματος, είναι γνωστά διάφορα είδη πεπερασμένα παριστώμενων ομάδων με επιλύσιμο πρόβλημα λέξης. Πιο συγκεκριμένα, μία *generic* πεπερασμένα παριστώμενη ομάδα είναι και *small cancellation group*. Τέλος, ισχύει ότι στις *small cancellation groups* (κλάση $C'(1/6)$) το πρόβλημα λέξης επιλύεται, βάση του αλγορίθμου *Dehn*, και - υπό τις κατάλληλες προϋποθέσεις - αποτελεσματικά. Περισσότερα θα δούμε στο μέρος μου ακολουθεί.

4.3.2 Η Επιλογή της Αλίκης

Ήδη έχουμε κάνει μια εισαγωγική συζήτηση για το θέμα των κατάλληλων ομάδων. Όπως γίνεται εύκολα κατανοητό, προκειμένου η Αλίκη να επιλέγει παραστάσεις με αποτελεσματικό τρόπο ως προς τους στόχους της επιλυσιμότητας, θα πρέπει να μπουν κάποιοι περιορισμοί. Πρώτα και κυριότερα, το σύνολο

των παραστάσεων θα είναι η κλάση των *small cancellation groups*. Σε αυτό το σημείο θα υπενθυμίσουμε κάποιους ορισμούς, απαραίτητους για τη συνέχεια, και θα επαναλάβουμε κάποια ήδη γνωστά πράγματα για τις ελεύθερες ομάδες:

1. Έστω $X = \{x_i | i \in I\}$ το σύνολο που παράγει την ελεύθερη ομάδα $F(X)$. Κάθε λέξη $W = W(x_1, x_2, ..., x_n)$ θα έχει τη μορφή $W = {x_{i_1}}^{e_1} * * * {x_{i_n}}^{e_n}$, όπου $e_i \in \{-1, +1\}$, όπου τα x_{i_j} δεν είναι κατ΄ ανάγκη διακεκριμένα.
   Μία λέξη ονομάζεται ανηγμένη αν ισχύει ότι ${x_{i_k}}^{e_k} \neq x_{i_{k+1}}^{-e_{k+1}}$ για κάθε $1 \leq i_k \leq n-1$.

2. Μία λέξη ονομάζεται κυκλικά ανηγμένη αν είναι ανηγμένη και επιπλέον έχει την ιδιότητα ${x_{i_1}}^{e_1} \neq {x_{i_n}}^{-e_n}$.

3. Ένα σύνολο S που περιέχει κυκλικά ανηγμένες λέξεις της $F(X)$ ονομάζεται συμμετροποιημένο αν είναι κλειστό ως προς τις κυκλικές μεταθέσεις και τις συζυγίες των στοιχείων του.

4. Έστω ομάδα G με παράσταση $\langle X|R\rangle$. Μία μη κενή λεξη $u \in F(X)$ καλείται τμήμα αν υπάρχουν δύο διακεκριμένες ορίζουσες σχέσεις $r_1, r_2 \in R$ τέτοιες ώστε $r_1 = us_1$ και $r_2 = us_2$ με $s_1, s_2 \in F(X)$ και χωρίς να εμφανίζονται διαγραφές γεννητόρων ανάμεσα είτε στα u και s_1 είτε στα u και s_2.

5. Τέλος, λέμε ότι μία ομάδα ανήκει στην κλάση $C(p)$ εάν καμία ορίζουσα σχέση δεν είναι γινόμενο λιγότερων από p τμήματα. Επίσης, λέμε ότι μια ομάδα G ανήκει στην κλάση $C'(\lambda)$ εάν για κάθε $r \in R$ τέτοιο ώστε $r = us$ με u: κομμάτι, ισχύει ότι $\mid u \mid < \lambda \mid r \mid$.

Πιο συγκεκριμένα, εάν η G ανήκει στην κλάση $C'(1/6)$ τότε ο αλγόριθμος του *Dehn* επιλύει αποτελεσματικά το πρόβλημα λέξης εντός της G. Αυτό, όπως αναφέραμε και παραπάνω, μεταφράζεται ως τετραγωνικός χρόνος ως προς το μήκος της λέξης.
Τελικά, αυτό που έχει να κάνει η Αλίκη προκειμένου να επιλέξει τυχαία μια *random cancellation group* είναι να διαλέξει μερικές τυχαίες λέξεις και να ελέγξει κατά πόσο το αντίστοιχο συμμετροποιημένο σύνολο ανήκει στην κλάση $C'(1/6)$ έτσι ώστε να επιτύχει την αποτελεσματική επίλυση.

Για να κλείσουμε το θέμα της επιλογής ομάδας - πλατφόρμας και για να τονίσουμε τον πρακτικό χαρακτήρα που έχουμε προσπαθήσει να προσδώσουμε στην ανάλυση του πρωτοκόλλου, θα αναφέρουμε κάποιες παραμέτρους με τις οποίες μπορεί να εργαστεί αποδοτικά η Αλίκη για την 'παραγωγή' της κατάλληλης αναπαράστασης Γ:

1. Η Αλίκη επιλέγει έναν ακέραιο k τέτοιο ώστε $10 \leq k \leq 20$. Η παράσταση που θα κατασκευάσει θα παράγεται από k γεννήτορες: x_1,x_2,.....,x_k.

2. Στη συνέχεια θα επιλέξει m, $10 \leq m \leq 30$, το πλήθος τυχαίες λέξεις οι οποίες παράγονται από τους παραπάνω γεννήτορες και θα λειτουργήσουν ως ορίζουσες σχέσεις. Εάν l_i είναι το μήκος της τυχαίας λέξης r_i, τότε θα πρέπει να ισχύει $L_1 \leq l_i \leq L_2$ με προτεινόμενες τιμές: $L_1 = 12$, $L_2 = 20$.

3. Όταν ολοκληρώσει τη διαδικασία κατασκευής της παράστασης $\hat{\Gamma}$ όπως την είχαμε προσδιορίσει στον ορισμό του πρωτοκόλλου, προσθέστει μία ακόμα ορίζουσα σχέση: την $x'_i = \prod_{j=1}^{M} [x'_i, w_j]$ όπου x'_i είναι ένας τυχαίος γεννήτορας της $\hat{\Gamma}$ και w_j τυχαία στοιχεία μήκους 1 ή 2 στους γεννήτορες $x'_1, x'_2, ...$ με τον συμβολισμό των αγκυλών να παραπέμπει στους μεταθέτες, δηλαδή: $[a, b] = a^{-1}b^{-1}ab$. Στη συνέχεια, υπολογίζει την αντίστροφη εικόνα της ορίζουσας σχέσης εντός της Γ και την προσθέτει στις ορίζουσες σχέσεις αυτής. Έτσι, η Γ καταλήγει να έχει k γεννήτορες και $m + 1$ ορίζουσες σχέσεις. Ο λόγος που προσθέσαμε αυτό το στοιχείο στην $\hat{\Gamma}$ αφορά την ενίσχυση του σχήματος απέναντι σε ένα συγκεκριμένο είδος επιθέσεων, τις αποκαλούμενες επιθέσεις πηλίκων. Θα μιλήσουμε αναλυτικότερα γι' αυτές παρακάτω.

4. Τέλος, ελέγχει κατά πόσο η παράσταση της Γ ικανοποιεί τη συνθήκη $C'(1/6)$ (αυτό επιτυγχάνεται με πολύ μεγάλη πιθανότητα). Αν αυτό δεν γίνει, επαναλαμβάνει τη διαδικασία.

Μετασχηματισμοί *Tietze*

Σε γενικές γραμμές αναλύσαμε τα πάντα όσον αφορά τις ενέργειες της Αλίκης. Αναφέραμε ότι η (ισομορφική) παράσταση Γ′ προκύπτει από την παράσταση Γ. Είπαμε ότι αυτό γίνεται μέσω των μετασχηματισμών *Tietze* και καλό είναι σε

αυτό το σημείο να τους επαναλάβουμε:

(T1): Εισάγουμε νέο γεννήτορα. Δηλαδή αντικαθιστούμε την αρχική μορφή $\langle x_1, x_2, ...|r_1, r_2, ...\rangle$ με την $\langle y, x_1, x_2, ...|ys^{-1}, r_1, r_2, ...\rangle$, όπου το s είναι μια λέξη των γεννητόρων $x_1, x_2, ...$

(T2): Ακυρώνουμε έναν γεννήτορα. Πρόκειται για το αντίστροφο της προηγούμενης διαδικασίας. Αν δηλαδή έχουμε μια μορφή $\langle y, x_1, x_2, ...|q, r_1, r_2, ...\rangle$, όπου το q είναι της μορφής ys^{-1} και τα $s, r_1, r_2, ...$ είναι στοιχεία της ομάδος που παράγεται από τα $x_1, x_2, ...$, την αντικαθιστούμε από μια παράσταση της μορφής $\langle x_1, x_2, ...|r_1, r_2, ...\rangle$.

(T3): Εφαρμόζουμε αυτομορφισμό. Δηλαδή, εφαρμόζουμε έναν αυτομορφισμό της ελεύθερης ομάδος, της παραγόμενης από τα $x_1, x_2, ...$ τόσο στους γεννήτορες $x_1, x_2, ...$ όσο και σε όλες τις ορίζουσες σχέσεις $r_1, r_2, ...$

(T4): Αλλάζουμε τις ορίζουσες σχέσεις. Δηλαδή, αντικαθιστούμε το σύνολο των οριζουσών σχέσεων με ένα άλλο σύνολο το οποίο έχει την ίδια κανονική θήκη με το αρχικό - αυτό σημαίνει ότι παράγουν την ίδια κανονική υποομάδα.

Ο *Heinrich Franz Friedrich Tietze* απέδειξε ότι δύο ομάδες είναι ισομορφικές αν και μόνο αν μπορεί να μεταβεί κανείς από τη μία παράσταση στην άλλη εφαρμόζοντας μια ακολουθία από τους μετασχηματισμούς του. Δηλαδή, κάθε ισομορφισμός είναι μια σύνθεση τέτοιων μετασχηματισμών. Άρα, επί της ουσίας, οι μετασχηματισμοί *Tietze* αντιπροσωπεύουν τους πιο στοιχειώδεις ισομορφισμούς που μπορούν να εφαρμοστούν. Το σημαντικό στοιχείο τους είναι ότι κάθε μετασχηματισμός είναι εύκολα αντιστρέψιμος και άρα η Αλίκη διευκολύνεται ιδιαίτερα στο υπολογισμό των αντιστρόφων ισομορφισμών μεταξύ των Γ και Γ'.

Οι τρεις πρώτοι μετασχηματισμοί είναι σαφείς ως προς την εκτελεσή τους. Ωστόσο, ο τέταρτος μπορούμε να πούμε πως δεν καθορίζεται με σαφήνεια. Γι' αυτό το λόγο θα ηταν πολύ βολίκο αν μπορούσαμε να προσδιορίσουμε κάποια αναδρομική διαδικασία:
• (T_4') : Στο σύνολο των οριζουσών σχέσεων αντικαθιστούμε το r_i με ένα από

τα r_i^{-1}, $r_i r_j$, $r_i r_j^{-1}$, $r_j r_i$, $r_j r_i^{-1}$, $x_k^{-1} r_i x_k$, $x_k r_i x_k^{-1}$, όπου $j \neq i$ και το k τυχαίος ακέραιος.

Για να κλείσουμε τη συζήτηση που αφορά την Αλίκη, θα αναφέρουμε κάποιες απλές τεχνικές που μπορεί αυτή να επιστρατεύσει έτσι ώστε να βελτιώσει το επίπεδο ασφαλείας του πρωτοκόλλου.

- Άπαξ και επιλέξει παράσταση, έστω Γ, μία εύστοχη κίνηση θα ήταν να εφαρμόσει διαδοχικούς μετασχηματισμούς (T_4') προκειμένου να αλλοιώσει την εμφάνιση της Γ. Αυτή η μέθοδος δεν αυξάνει την πολυπλοκότητα του τελικού ισομορφισμού (οι μετασχηματισμοί (T_4') επάγουν όλοι τους την ταυτοτική απεικόνιση) και έχει το χαρακτηριστικό ότι είναι πολύ πιθανό να καταργεί την ενδεχόμενη *small cancellation group* ιδιότητα της Γ. Αργότερα θα δούμε πώς αυτό το χαρακτηριστικό μπορεί να φανεί πολύ χρήσιμο στην ασφάλεια του σχήματος.

- Στην προηγούμενη τεχνική είδαμε την ιδέα του να μετασχηματίζουμε τη μορφή μιας παράστασης. Τώρα θα δούμε μία ακόμα που κινείται στο ίδιο μήκος κύματος. Η Αλίκη μπορεί να πάρει το ελεύθερο γινόμενο της ομάδας που έχει επιλέξει με την τετριμμένη. Πρακτικά, για να κατασκευάσει αυτό το γινόμενο αρκεί να προσθέσει νέους γεννήτορες, έστω $z_1, ..., z_q$, και νέες ορίζουσες σχέσεις $s_1(z_1, .., z_q), ..., s_t(z_1, ..., z_q)$ έτσι ώστε η παράσταση $\langle z_1, ..., z_q | s_1, ..., s_t \rangle$ να απεικονίζει την τετριμμένη ομάδα. Στη συνέχεια, μπορεί να εφαρμόσει διαδοχικά μετασχηματισμούς (T_3) και (T_4') προκειμένου να αναμίξει τις παλιές και τις καινούριες ορίζουσες σχέσεις.

Σε αυτό το σημείο είναι χρήσιμο να πούμε κάποια πράγματα σχετικά με το καθόλου απλό ζήτημα των παραστάσεων της τεριμμένης ομάδας [9].

Έστω F η ελεύθερη ομάδα με *rank* $n \geq 2$ και $X = \{x_1, ..., x_n\}$ το σύνολο των γεννητόρων της και έστω $Y = \{y_1, ..., y_m\}$ ενα τυχαίο πεπερασμένο σύνολο με στοιχεία από την F. Θεωρούμε τους εξής μετασχηματισμούς επί του Y:

$(AC1)$: Αντικαθιστούμε το y_i με το $y_i y_j$ με $j \neq i$.
$(AC2)$: Αντικαθιστούμε το y_i με το y_i^{-1}.
$(AC3)$: Αντικαθιστούμε το y_i με το $g y_i g^{-1}$ για κάποιο $g \in F$.

Λέμε ότι δύο σύνολα Y και $\widetilde{Y}$ είναι $Andrews$ - $Curtis$ ισοδύναμα εάν το ένα μπορεί να προκύψει από το αλλό εφαρμόζοντας μια ακολουθία από τους παραπάνω μετασχηματισμούς.
Με $\langle Y\rangle^F$ θα συμβολίσουμε την κανονική θήκη ενός συνόλου Y εντός της F.

• Η εικασία των $Andrews$ - $Curtis$: Έστω $Y = \{y_1, ..., y_n\}$ ενα σύνολο της F. Τότε $\langle Y\rangle^F = F$ αν και μόνο αν το Y είναι AC ισοδύναμο με το $X = \{x_1, ..., x_n\}$.

Με βάση αυτήν την εικασία, μπορούμε να διατυπώσουμε κάτι που αφορά άμεσα τα όσα πραγματευόμαστε σε όλη αυτήν την ενότητα:

• Κάθε ισορροπημένη παράσταση, δηλαδή κάθε παράσταση όπου το (πεπερασμένο) πλήθος των γεννητόρων είναι ίδιο με αυτό των οριζουσών σχέσεων, της τετριμμένης ομάδας μπορεί να μετατραπεί στην τυπική, $\langle x_1, ..., x_n|x_1, ..., x_n\rangle$, μέσω μιας ακολουθίας των μετασχηματισμών που αναφέραμε.

Λέμε ότι μία ομάδα G ικανοποιεί την ιδιότητα ACP_k, $k \in \mathbb{N}$, των $Andrews$ - $Curtis$ αν για κάθε δύο σύνολα $U, V \in G^k$ ισχύει η εξής ισοδυναμία:

$$\langle U\rangle^G = \langle V\rangle^G = G \iff U \sim V$$

Έτσι, διατυπώνεται η ακόλουθη σημαντική ερώτηση:

• Ισχύει ότι για κάθε ομάδα G υπάρχει ακέραιος k_0 τέτοιος ώστε η G να ικανοποιεί την ACP_k για κάθε $k{>}k_0$;

Έχει δειχθεί ότι η ερώτηση αυτή έχει θετική απάντηση για κάποιες ομάδες. Επίσης, παρά την γενική αντίληψη ότι η εικασία $Andrews$ - $Curtis$ δεν ισχύει, δεν έχουν βρεθεί έγκυρα αντιπαραδείγματα, πέρα από κάποιες προτάσεις συγκεκριμένων ομάδων που ενδέχεται να μπορούν να επιτελέσουν τέτοιο ρόλο.

Όλη αυτή η συζήτηση που κάναμε για τις ιδέες των $Andrews$ και $Curtis$ ενέχει ιδιαίτερη σημασία αν σκεφτεί κανείς πως μόλις αποκτήσαμε ένα δυνατό εργαλείο για την κατασκευή πολυπλοκότερων της στοιχειώδους (ισορροπημένων) παραστάσεων. Δηλαδή, η Αλίκη μπορεί να εκκινήσει τη διαδικασία με την παράσταση $\langle x_1, ..., x_n|x_1, ..., x_n\rangle$ και στη συνέχεια να εφαρμόσει ακολουθία μετασχηματισμών $AC(1) - AC(3)$ πετυχαίνοντας έτσι το επιθυμητό αποτέλεσμα.

Για να κλείσουμε την -ενδεχομένως μεγάλη- παρένθεση που κάναμε αναφέροντας τα των $Andrews$ - $Curtis$, θα διατυπώσουμε ένα θεώρημα πρακτικού χαρακτήρα.

• Θεώρημα: Κάθε παράσταση με την παρακάτω μορφή προσδιορίζει την τετριμμένη ομάδα: $\langle x, y, z | x = z[y^{-1}, x^{-1}, z], y = x[y^{-1}, x^{-1}, z^{-1}][z^{-1}, x], w\rangle$, όπου w είναι μία λέξη στο αλφάβητο των x, y, z της οποίας το άθροισμα εκθετών ισούται με ± 1.

Επανερχόμενοι στις τεχνικές που μπορεί να χρησιμοποιήσει η Αλίκη για τους μετασχηματισμούς της παράστασης Γ παρατηρούμε πως όλα όσα αναφέραμε για τις παραστάσεις της τετριμμένης ομάδας έχουν να κάνουν με ισορροπημένα παραδείγματα. Στην πραγματικότητα η Αλίκη θα μπορούσε να προσθέσει τυχαίες ορίζουσες σχέσεις προκειμένου να αποκρύψει ακόμα καλύτερα τις προθέσεις της και να μπερδέψει την Εύα.

Το τελευταίο τέχνασμα που θα συζητήσουμε αφορά το μήκος των λέξεων που αποτελούν τις ορίζουσες σχέσεις της ομάδας. Η Αλίκη μπορεί να αντικαταστήσει την παράστασή της με μία ισόμορφη, της οποίας όμως οι περισσότερες ορίζουσες σχέσεις θα έχουν μήκος το πολύ 4. Η κεντρική ιδέα είναι ότι οι μικρές λέξεις είναι πιο εύκολα διαχειρίσιμες ως προς τους μετασχηματισμούς. Ας δούμε όμως ποια είναι ακριβώς η διαδικασία:
Έστω ότι εκκινούμε με μία παράσταση $\langle x_1, ..., x_k | r_1, ..., r_m\rangle$ και έστω $r_1 = x_i x_j u$ με $1 \leq i, j \leq k$. Τότε θα εφαρμόσουμε μετασχηματισμό T(1), δηλαδή θα προσθέσουμε επιπλέον γεννήτορα x_{k+1} και ορίζουσα σχέση $r_{m+1} = x_{k+1}^{-1} x_i x_j$. Έτσι προκύπτει η ισόμορφη παράσταση $\langle x_1, ..., x_k, x_{k+1} | r_1, ..., r_m, r_{m+1}\rangle$. Στη συνέχεια, θα αντικαταστήσουμε το r_1 με $r_1' = x_{k+1} u$ παίρνοντας έτσι την ισόμορφη $\langle x_1, ..., x_k, x_{k+1} | r_1', ..., r_m, r_{m+1}\rangle$ και πετυχαίνοντας έτσι τη μείωση του μήκους r_1 κατά 1. Συνεχίζοντας αναλόγως, τελικά θα προκύψει μια παράσταση στην οποία πολλές ορίζουσες σχέσεις θα έχουν μήκος το πολύ 3 ενώ πρακτικά το μόνο που έχουμε να κάνουμε είναι το να προσθέτουμε επιπλέον γεννήτορες. Ουσιαστικά στοχεύουμε για μήκος 3 ή 4, αριθμοί που είναι επαρκείς για την 'παραχάραξη' των λέξεων που θέλουμε να επιτύχουμε, ενώ παράλληλα δεν θα θέλαμε μικρότερα μήκη γιατί αυτό θα καθιστούσε τις μορφές των λέξεων απλούστερες. Αν στο τέλος της διαδικασίας εντοπίσουμε ορίζουσες σχέσεις

με μεγαλύτερο μήκος, τότε αυτές μπορούμε απλά να τις διαγράψουμε ολοκληρώνοντας έτσι το τελικό βήμα της Αλίκης, μεταβαίνοντας δηλαδή από το Γ′στο $\hat{\Gamma}$.

4.3.3 Η Επιλογή του Βασίλη

Στις προηγούμενες ενότητες του κεφαλαίου συζητήσαμε τις ενέργειες και τις λεπτομέρειες που αφορούν τα δύο πρώτα βήματα του πρωτοκόλλου. Σε αυτήν την ενότητα θα αναλύσουμε το τρίτο βήμα καθώς και τα διάφορα ζητήματα που προκύπτουν. Για να είμαστε πιο σαφείς, θα μιλήσουμε για τις ενέργειες του Βασίλη.
Για αρχή, θα υπενθυμίσουμε τη διαδικασία του βήματος: Ο Βασίλης χρησιμοποιεί μια δυαδική ακολουθία ως ιδιωτικό κλειδί. Εάν ένα ψηφίο ισούται με 1, θα μεταδώσει στη θέση του ένα στοιχείο το οποίο θα ισούται με το μοναδιαίο της ομάδας $\hat{\Gamma}$. Εάν το ένα ψηφίο ισούται με 0, θα μεταδώσει ένα στοιχείο διάφορο του μοναδιαίου εντός της $\hat{\Gamma}$.
Οι πρώτες εύλογες απορίες που εγείρονται αφορούν τον τρόπο κατασκευής των στοιχείων που θα επιτελέσουν τους παραπάνω ρόλους.
Θα ξεκινήσουμε με την περίπτωση του 1: Εδώ ο Βασίλης καλείται να μεταδώσει μια λέξη με την προϋπόθεση ότι αυτή θα εμφανίζεται όσο το δυνατόν πιο τυχαία έτσι ώστε να μην αποκαλύπτει την ιδιαίτερη ταυτότητα του στοιχείου που κρυπτογραφείται. Αυτή η ιδέα ονομάζεται 'σημασιολογική ασφάλεια'. Πιο συγκεκριμένα, πάντα μιλώντας διαισθητικά, ένα σύστημα θεωρείται σημασιολογικά ασφαλές αν κανένας πολυωνυμικά περιορισμένος αντίπαλος δεν μπορεί να αποσπάσει πληροφορίες για το αυθεντικό - μη κρυπτογραφημένο κείμενο από την κρυπτογραφημένη μορφή του. Σε αυτό το σημείο θα εισάγουμε και μία ακόμα έννοια για να γίνει πιο σφαιρικά κατανοητή η σημασιολογική ασφάλεια. Αδιακριτότητα ονομάζεται η ανικανότητα του αντιπάλου να ταυτοποιήσει ένα κείμενο, μεταξύ δύο αυθεντικών κειμένων, δοθείσης μιας κρυπτογραφημένης μορφής. Οι *Bagherzandi*, *Mohajeri* και *Salmasizadeh* απέδειξαν κάποιου είδους ισοδυναμία ανάμεσα στις δύο έννοιες [10] - περισσότερες λεπτομέρειες δεν εξυπηρετούν τους σκοπούς της εργασίας μας.
Ο Βασίλης, έχοντας τα παραπάνω υπόψην του, κατασκευάζει μια λέξη χρησιμοποιώντας τις ορίζουσες σχέσεις και τα συζυγή τους. Η κεντρική ιδέα είναι να μετασχηματίσει το μοναδιαίο στοιχείο της ομάδας με τέτοιο τρόπο ώστε να μην εμφανίζονται μεγάλα τμήματα αποτελούμενα από ορίζουσες σχέσεις στη γραφή

της λέξης. Έστω u αυτή η λέξη. Η διαδικασία προκειμένου να το επιτύχει ονομάζεται $shuffling$ δηλαδή ανάδευση και πράγματοποιείται πάντα με τα δεδομένα ότι ο Βασίλης δεν γνωρίζει καμία ιδιότητα της ομάδας $\hat{\Gamma}$ πέρα από το ότι οι περισσότερες ορίζουσες σχέσεις της είναι μήκους 3 ή 4.

1. Ο Βασίλης κατασκυάζει τη λέξη $u = s_1 * * * s_p$, όπου s_i ανήκει στο σύνολο των οριζουσών σχέσεων μήκους 3 ή 4, των αντιστρόφων τους και των συζυγών τους ως προς λέξεις μήκους 1 ή 2. Θα πρέπει ο αριθμός p να είναι μεγαλύτερος του δεκαπλασίου του πλήθους των οριζουσών σχέσεων.

2. Στη συνέχεια εισάγει $2p/k$ το πλήθος εκφράσεις της μορφής $x'_j(x'_j)^{-1}$ ή $(x'_j)^{-1}x'_j$ σε τυχαία σημεία της λέξης u, όπου k είναι το πλήθος των γεννητόρων x'_i της $\hat{\Gamma}$.

3. Σαρώνει τη λέξη από τα αριστερά προς τα δεξιά ψάχνοντας για υπολέξεις μήκους 2 που να είναι μέρη οριζουσών σχέσεων μήκους 3 ή 4. Όποτε εντοπίζει μία τέτοια την αντικαθιστά ως εξής: έστω ότι η υπολέξη είναι η $x'_1x'_2$ και ισχύει ότι $\hat{r}_i = x'_1x'_2x'_3x'_4$ για κάποια ορίζουσα σχέση $\hat{r}_i$. Τότε αντικαθιστά την υπολέξη με την $(x'_4)^{-1}(x'_3)^{-1}$. Εάν η υπολέξη είναι η $x'_2x'_3$ αντικαθιστά με την $(x'_1)^{-1}(x'_4)^{-1}$. Στην περίπτωση που έχει περισσότερες της μίας επιλογές, επιλέγει τυχαία μία από αυτές.

4. Αν μετά το τρίτο βήμα εξακολουθούν να υπάρχουν υπολέξεις της μορφής $x'_i(x'_i)^{-1}$ και $(x'_i)^{-1}x'_i$, τις διαγράφει.

Ολόκληρη η παραπάνω διαδικασία θα πρέπει να επαναληφθεί τουλάχιστον p φορές προκειμένου να επιτευχθεί καλή "παραχάραξη" της λέξης και για να είμαστε σαφείς, στην προκειμένη περίπτωση ως παραχάραξη αναφέρουμε την μη εμφάνιση οριζουσών σχέσεων μήκους 3 ή 4 στη γραφή της u.
Όταν ο Βασίλης ολοκληρώσει τα παραπάνω, θέτει $w = [x'_i, u]$ και επαναλαμβάνει τη διαδικασία για το w, $|w|/2$ φορές όπου το x'_i είναι ο γεννήτορας που είχε χρησιμοποιήσει αντίστοιχα η Αλίκη στην κατακευή της $\hat{\Gamma}$ κατά τα δικά της βήματα. Αξίζει να κάνουμε δύο παρατηρήσεις. Πρώτον, η λέξη w είναι η μονάδα της ομάδας $\hat{\Gamma}$, άρα και της Γ' και φυσικά και της Γ. Δεύτερον, χρησιμοποιούμε στοιχείο της μορφής του w ετσι ώστε να προστατευθούμε από ένα συγκεκριμένο είδος επιθέσεων που θα δούμε παρακάτω: τις επιθέσεις πηλίκων.

Όσα αναφέρθηκαν παραπάνω αφορούν τη διαδικασία μετάδοσης της μονάδας.

Ιδιαίτερη σημασία όμως έχει και η περίπτωση που ο Βασίλης θέλει να μεταδώσει μη μοναδιαίο στοιχείο. Όπως θα δούμε, προκειμένου να επιτευχθεί ο στόχος, θα χρησιμοποιηθούν και στοιχεία πιθανοτήτων.

Η βασική ιδέα είναι ότι αν επιλέξει κανείς μία τυχαία λέξη με σχετικά μεγάλο μήκος, τότε η πιθανότητα να είναι διάφορη του μοναδιαίου στοιχείου της ομάδας είναι πρακτικά ίση με 1 [11].
Διατυπωμένο ομαδοθεωρητικά το πρόβλημα έχει ως εξής: Δεδομένου ότι κάθε ομάδα G είναι το πηλίκο μιας ελεύθερης ομάδας F προς την αντίστοιχη ομάδα R την οποία παράγει κάποιο σύνολο οριζουσών σχέσεων, ποια είναι η πιθανότητα το τυχαίο στοιχείο (λέξη) της F να μην ανήκει στην R;

• Ορισμός (ασυμπτωτικής πυκνότητας): Έστω X ένα πεπερασμένο αλφάβητο με τουλάχιστον δύο στοιχεία και έστω $(X^*)^k$ το σύνολο των $k-$άδων λέξεων της X. Το μήκος μιας $k-$άδας $w_1, w_2, ...w_k$ ορίζεται ως το άθροισμα των μηκών των w_i. Έστω S ένα υποσύνολο του $(X^*)^k$. Για κάθε $n \geq 0$, ως B_n ορίζουμε το σύνολο όλων των $k-$άδων του $(X^*)^k$ με μήκος το πολύ n.

Ορίζουμε την ασυμπτωτική πυκνότητα $p(S)$ του S στο $(X^*)^k$ ως το όριο

$$p(S) := \limsup_{n\to\infty} p_n(S), \text{ όπου } p_n(S) := \frac{|S\cap B_n|}{|B_n|}$$

Εάν το όριο $\lim_{n\to\infty} p_n(S)$ υπάρχει, ορίζουμε $\widehat{p}(S) := p(S)$

Άρα, έχουμε ότι $\widehat{p}(S) = \lim_{n\to\infty} p_n(S)$.

Για να ολοκληρώσουμε αυτήν τη μικρή παρένθεση ορισμών, θα αναφέρουμε πως όταν καλούμε ένα σύνολο $S \subseteq (X^*)^k$ γενικό, εννοούμε ότι έχει την ιδιότητα: $\widehat{p}(S) = 1$.

Συνεπώς, το νόημα των όσων είπαμε παραπάνω συνοψίζεται στο ότι πρέπει

να προκύπτει ότι: $p(R) = \limsup_{n\to\infty} \frac{\#\{u \in R :| u |\leq n\}}{\#\{u \in F :| u |\leq n\}} = 0,$

όπου οι απόλυτες τιμές υποδηλώνουν, όπως πάντα, το λεξικογραφικό μήκος των λέξεων.

Ο $Wolfgang\ Woess$ στην εργασία του με τίτλο $Cogrowth\ of\ groups\ and\ simple\ random\ walks$ αποδεικνύει ότι εάν η ομάδα $G = F/R$ είναι άπειρη, τότε ισχύει ότι $p(R) = 0$.
Εφόσον εργαζόμαστε σε άπειρες ομάδες, το νόημα που προκύπτει από τα όρια που αναφέραμε παραπάνω είναι ότι η πιθανότητα μία τυχαία λέξη μήκους n να είναι διάφορη του μοναδιαίου στοιχείου της G τείνει στο 1 καθώς το n τείνει στο άπειρο. Βέβαια, επειδή καλούμαστε να αντιμετωπίσουμε το πρόβλημα σε πρακτικό και όχι θεωρητικό επίπεδο, ένα ρεαλιστικό μήκος για μια τυχαία λέξη είναι της τάξης 100 με 200.
Συνεπώς, το επόμενο ερώτημα που οφείλουμε να απαντήσουμε αφορά το πόσο γρήγορα επέρχεται η ζητούμενη σύκλιση για τις λέξεις που αναφέραμε. Ο $Woess$, στην εργασία που ήδη αναφέραμε, καταλήγει στο ότι στις $non-amenable$ ομάδες επιτυγχάνεται η σύγκλιση με εκθετική ταχύτητα. Ο ορισμός των $non-amenable$ ομάδων ξεφεύγει από τους σκοπούς της εργασίας μας και γι΄ αυτό το λόγο θα αρκεστούμε στο να αναφέρουμε πως οι $small\ cancellation\ groups$, με τις οποίες εργαζόμαστε στο συγκεκριμένο πρωτόκολλο, είναι $non-amenable$.

Σε αυτό το σημείο δεν πρέπει να ξεχνάμε ότι ο Βασίλης δεν εργάζεται στην ίδια ομάδα με την Αλίκη. Άρα, υπάρχει ο κίνδυνος μια μη μοναδιαία λέξη του Βασίλη, δηλαδή της ομάδος $\widehat{\Gamma}$, να μετατραπεί σε μοναδιαία της Γ' μέσω του φυσικού επιμορφισμού. Στην πραγματικότητα, αυτός ο κίνδυνος δεν υπάρχει καθώς, κατα πρώτον, όλες οι ομάδες που εμφανίζονται είναι $small\ cancellation$ και κατά δεύτερον, η τυχαία επιλογή στοιχείου στην $\widehat{\Gamma}$ μεταφράζεται σε τυχαία επιλογή στοιχείου στην Γ'. Συνεπώς, όλα όσα αναφέραμε παραπάνω περί σύγκλισης, ισχύουν αυτούσια στη Γ'.

Επομένως, τώρα δεν μένει παρά να δούμε ποιες είναι οι ενέργειες του Βασίλη προτού μεταδώσει το μη μοναδιαίο στοιχείο:

Αρχικά, επιλέγει μία τυχαία λέξη από την παράγωγο υποομάδα της ελεύθερης ομάδας, η οποία ελεύθερη ομάδα παράγεται από τα $x'_1, x'_2, ...$ Αυτό επιτυγχάνεται επιλέγοντας μια τυχαία λέξη υ της ελεύθερης ομάδας και ισορροπώντας στη συνέχεια τους εκθέτες του κάθε γεννήτορα της ελεύθερης ομάδας, δηλαδή φροντίζουμε ώστε το άθροισμα των εκθετών κάθε γεννήτορα να είναι 0. Έτσι, προκύπτει η λέξη u της οποίας το μήκος πρέπει να είναι της ίδιας τάξης με αυτά των λέξεων που αντιπροσωπεύουν το μαναδιαίο στοιχείο. Πράγματι, εφόσον

η ομάδα F/F', όπου F η ελεύθερη ομάδα που αναφέραμε και F' η αντίστοιχη παράγωγος, είναι αβελιανή, προκύπτει ότι όλοι οι όροι $x'_1/F', x'_2/F', ...$ της λέξης u/F' μετατίθενται και ακριβώς επειδή αυτή είναι ισορροπημένη προκύπτει το μοναδιαίο στοιχείο της ομάδας F/F'. Άρα, όντως η λέξη u ανήκει στην παράγωγο υποομάδα.
Στη συνέχεια, ο Βασίλης θέτει $w = [x'_i, u]$, οπου το x'_i είναι το αντίστοιχο στοιχείο που είχε χρησιμοποιήσει η Αλίκη στην κατασκευή της ορίζουσας σχέσης την οποία και είχε προσθέσει. Επισημαίνουμε ότι $w = [x'_i, u] \neq 1_{\widehat{\Gamma}}$ καθώς αν αυτό δεν ίσχυε θα έπρεπε το στοιχείο u να είναι δύναμη του x'_i, πράγμα που από τη δομή του αποκλείεται. Τέλος, εφαρμόζει ανάδευση των ειδών (2) - (4), όπως τους είχαμε αναφέρει παραπάνω, περίπου $|w|/2$ φορές.

Άρα, στην κατεύθυνση της σημασιολογικής ασφάλειας συμβάλλουν τόσο το μήκος της λέξης u όσο και η φύση του στοιχείου $w = [x'_i, u]$ το οποίο έχει αυτή τη μορφή έτσι ώστε ναι μεν να διατηρεί τον τυχαίο χαρακτήρα του αλλά και να μην είναι αναγνωρίσιμο σε σχέση με τη γραφή του μοναδιαίου στοιχείου. Γι' αυτόν ακριβώς το λόγο άλλωστε τα δύο στοιχεία (μοναδιαίο και τυχαίο) έχουν οριστεί και υποστεί επεξεργασία ($shuffling$) με τον ίδιο τρόπο.

Ωστόσο, αξίζει να σημειωθεί πως δεν έχει υπάρξει συνεπής απόδειξη που να πιστοποιεί ότι πράγματι, το μοναδιαίο στοιχείο είναι μη αναγνωρίσιμο σε σχέση με το τυχαίο. Βέβαια, αυτή η ανεπάρκεια καλύπτεται από το ότι διάφορα πειράματα που έχουν πραγματοποιηθεί με τη βοήθεια υπολογιστών έχουν δείξει πως όταν εργαζόμαστε με ομάδες ($\widehat{\Gamma}$) των οποίων οι ορίζουσες σχέσεις είναι μήκους το πολύ 4, τότε οι λέξεις που αντιπροσωπεύουν το $1_{\widehat{\Gamma}}$, και οι οποίες έχουν προκύψει μέσα από τις διαδικασίες που έχουμε περιγράψει παραπάνω, έχουν ίδια συχνότητα εμφάνισης για υπολέξεις μήκους 1, 2 ή 3 δείχνοντας ότι είναι πιθανό ο στόχος μας να έχει επιτευχθεί, δηλαδή η λέξη να μοιάζει όσο το δυνατόν περισσότερο με τυχαία. Για να είναι πιο σαφές τι ακριβώς εννοούμε με τη συχνότητα εμφάνισης, υπενθυμίζουμε ότι η ανάδευση κατά τη διαδικασία 'παραχάραξης' του $1_{\widehat{\Gamma}}$ είχε ως στόχο την εξάλειψη οριζουσών σχέσεων μήκους 3 ή 4 στη γραφή του.

4.3.4 Επιθέσεις στο Πρωτόκολλο *Shpilrain – Zapata*

Σε αυτό το κεφάλαιο αναλύσαμε το πρωτόκολλο καθώς και τους τρόπους με τους οποίους μπορεί να γίνει αποτελεσματικά η εφαρμογή του. Ωστόσο, ακριβώς αυτή η αποτελεσματικότητα καθώς, σε τελική ανάλυση, και το ίδιο το πρωτόκολλο εξαρτάται σε τεράστιο βαθμό από την ασφάλεια που μας παρέχει. Ήδη στην ανάλυση των τεχνικών που κάναμε παραπάνω, έγιναν νύξεις σχετικά με διάφορα είδη επιθέσεων που μπορούν να μας απειλήσουν. Σε αυτήν την υποπαράγραφο θα αναλύσουμε κάποιες μορφές επιθέσεων και έτσι θα μπορέσουμε να αντιλυφθούμε σε μεγαλύτερο βάθος το νόημα του πρωτοκόλλου.

Η Επίθεση Ισομορφισμού

Η πρώτη και πιο τετριμμένη μορφή επίθεσης είναι η επίθεση ισομορφισμού, η οποία μπορεί και να χαρακτηριστεί και ως επίθεση 'ωμής βίας'. Από την ανάλυση που θα κάνουμε θα γίνει σαφής και ο λόγος για τον οποίο πήρε αυτήν την ονομασία.

Αρχικά, υπενθυμίζουμε πως το σύνολο των ομάδων από το οποίο επιλέγει η Αλίκη τη Γ ως βάση για το πρωτόκολλο, είναι γνωστό δημοσίως. Επίσης, δημόσια είναι και η $\widehat{\Gamma}$. Η τακτική της Εύας είναι να προσθέτει ορίζουσες σχέσεις στην παράσταη της $\widehat{\Gamma}$ με την ελπίδα να την αντιστοιχίσει ισομορφικά με κάποια ομάδα από το δημόσιο σύνολο που αναφέραμε.
Σε θεωρητικό επίπεδο κάτι τέτοιο είναι κατορθωτό μιας και είναι αναδρομικώς ορισμένο τόσο το σύνολο των ομάδων όσο και το σύνολο των πεπερασμένων παραστάσεων των ισομορφικών με δοθείσα παράσταση.

Σε αυτό το σημείο, είναι χρήσιμο να εξηγήσουμε τι ακριβώς εννοούμε με τον όρο 'αναδρομικώς ορισμένο σύνολο'. Θα το κάνουμε αναλύοντας την αριθμήσιμη εκδοχή του [12]:

Έστω σύνολο $A \subseteq \mathbb{N}^n$. Τότε μπορούμε να θεωρήσουμε το A ως μία χαρακτηριστική συνάρτηση η οποία αντιστοιχίζει τον αριθμό 1 στο στοιχείο x αν αυτό ανήκει στο A και την τιμή 0 αν αυτό δεν ανήκει στο A.
Συνεπώς, αναδρομικώς ορισμένο (ή υπολογίσιμο) μπορεί να ονομαστεί ένα

σύνολο του οποίου η χαρακτηριστική συνάρτηση είναι υπολογίσιμη.
Λέγοντας ύπολογίσιμη συνάρτηση΄ εννούμε πως μπορεί να βρεθεί αλγόριθμος ο οποίος να επιτελεί το έργο της συνάρτησης, με την έννοια ότι σε κάθε είσοδο αποδίδει κάποιο αποτέλεσμα.

Αρα, αντιλαμβάνεται κανείς ότι:
Ένα σύνολο ονομάζεται αναδρομικώς ορισμένο αν και μόνο αν υπάρχει αλγόριθμος ο οποίος, δοθέντος στοιχείου x, να μπορεί να αποφανθεί για το αν το x ανήκει στο σύνολο, υπό την έννοια ότι τερματίζει για οποιαδήποτε είσοδο.

Επιστρέφοντας στην ανάλυση για την επίθεση στο πρωτόκολλο, αναφέρουμε ότι πρακτικά αυτή η μέθοδος δεν μπορεί να εφαρμοστεί καθώς απαιτεί τεράστια ποσότητα πόρων. Ας δούμε όμως πιο αναλυτικά τι ακριβώς συμβαίνει:
Η Εύα γνωρίζει την ομάδα $\hat{\Gamma}$ με την οποία δουλεύει ο Βασίλης. Έτσι, προσθέτει μία ορίζουσα σχέση σε αυτήν την ομάδα και στη συνέχεια ελέγχει κατά πόσο αυτή, ας την ονομάσουμε $\hat{\Gamma}_+$, είναι ισομορφική με κάποια από τη δημόσια ΄δεξαμενή΄ ομάδων. Ο τρόπος με τον οποίο γίνεται αυτός ο έλεγχος είναι ο εξής: έστω ότι η Αλίκη θέλει να εργαστεί με τις $\hat{\Gamma}_+$ και Γ_i. Θα σαρώσει όλες τις απεικονίσεις, μία προς μία, από την Γ_i στην $\hat{\Gamma}_+$ οι οποίες είναι ορισμένες στους γεννήτορες της Γ_i. Ακριβώς η ίδια διαδικασία επαναλαμβάνεται για τις απεικονίσεις από την $\hat{\Gamma}_+$ στην Γ_i. Στη συνέχεια, θα ελέγξει αν η σύνθεση δύο τέτοιων απεικονίσεων έχει ως αποτέλεσμα την ταυτοτική στη Γ_i και φυσικά κατά πόσο οι απεικονίσεις που χρησιμοποιούνται είναι ομομορφισμοί, δηλαδή το κατά πόσο αντιστοιχίζουν τις ορίζουσες σχέσεις με το μοναδιαίο στοιχείο της άλλης ομάδας. Εφόσον πρέπει να ελεγχθεί η ισότητα με την ταυτοτική απεικόνιση, καταλαβαίνει κανείς ότι η επιλυσιμότητα του προβλήματος λέξης εντός της Γ_i απλοποιεί κατά πολύ την κατάσταση. Ωστόσο, στην πραγματικότητα η Εύα ενδιαφέρεται μόνο για το ένα μέρος του προβλήματος λέξης, αυτό που αφορά την καταφατική απάντηση, και η επίλυση στο συγκεκριμένο πρόβλημα είναι πάντοτε αναδρομική.
Ας δούμε όμως πιο συγκεκριμένα τι γίνεται στην - πιο πιθανή - περίπτωση όπου οι δύο ομάδες δεν είναι ισομορφικές: εφόσον η αρνητική απάντηση του προβλήματος της λέξης δεν είναι αναδρομική, η Εύα θα πρέπει να ελέγχει απεικονίσεις επ΄ αόριστον. Για κάθε ομάδα Γ_i θα αναγκάζεται να δεσμεύει πόρους μνήμης. Καθώς όμως το μέγεθος της Γ_i αυξάνεται εκθετικά ως προς το μέγεθος της παράστασης, δηλαδή ως προς το συνολικό μήκος των οριζουσών σχέσεων, η Εύα θα καταλήξει να φτάσει αρκετά γρήγορα τα φυσικά όρια τα οποία εκ των

πραγμάτων υπάρχουν. Για παράδειγμα θα αναφέρουμε ότι το πλήθος των παραστάσεων με 6 γεννήτορες και συνολικό μήκος οριζουσών σχέσεων το πολύ 100, είναι 10^{100}. Η μέθοδος που περιγράψαμε μπορεί να μην είναι η μοναδική ή ούτε καν η πιο ΄έξυπνη΄, ωστόσο είναι αντιπροσωπευτική για τα μεγέθη και τις δυσκολίες που προκύπτουν.

Τέλος, από τη διαδικασία που ακολούθησε η Εύα, μπορούμε να εκμαιεύσουμε μια ακόμα γραμμή άμυνας για το πρωτόκολλό μας: όταν η Αλίκη επιλέξει την ομάδα Γ που θα χρησιμοποιήσει ως βάση για την όλη διαδικασία, μπορεί να προσθέσει στο σύνολο (*pool*) των δημόσιων ομάδων και όλες αυτές τις ομάδες που διαφέρουν από τη Γ ως προς κάποια ή κάποιες ορίζουσες σχέσεις δημιουργώντας έτσι παραλλαγές και δυσχεραίνοντας το έργο της Εύας ως προς τον εντοπισμό ισόμορφων ομάδων. Φυσικά, αυτές οι επιπρόσθετες ομάδες θα πρέπει σε κάθε περίπτωση να πληρούν τις προϋποθέσεις που έχουμε αναφέρει στη σχετική υποπαράγραφο.

Η Επίθεση Πηλίκου

Έχουμε ήδη αναφέρει πως το παραπάνω παράδειγμα επίθεσης ωμής βίας δεν είναι ιδιαίτερα αποτελεσματικό. Σε αυτήν την υποπεράγραφο θα δούμε μια πιο συγκροτημένη προσπάθεια - την επίθεση πηλίκου.

Η πρώτη κίνηση της Εύας είναι να χρησιμοποιήσει το λεγόμενο ΄τεστ πηλίκου΄, όπου θα προσπαθήσει να ανακαλύψει τα μηδενικά στοιχεία στη δυαδική ακολουθία του Βασίλη. Πιο συγκεκριμένα, θα δοκιμάσει να προσθέσει - πεπερασμένες ή και άπειρες (με την αναδρομική μέθοδο) το πλήθος - ορίζουσες σχέσεις στην ομάδα ούτως ώστε να καταφέρει να την ταυτίσει με κάποια ομάδα την οποία γνωρίζει και η οποία έχει επιλύσιμο πρόβλημα λέξης.
Το νόημα είναι να στοχεύσει μόνο σε γνωστά πηλίκα, για παράδειγμα αναφέρουμε τα αβελιανά, όπου προσθέτει ως ορίζουσες σχέσεις όλους τους μεταθέτες της μορφής $[x'_i, x'_j]$ με x'_i, x'_j: γεννήτορες της ομάδας Γ_i, και τα μηδενοδύναμα, όπου προσθέτει τους ίδιους μεταθέτες αλλά ως γεννήτορες και με αυξημένο βάρος αυτή τη φορά. Για την περίπτωση των μετα-αβελιανών ομάδων, δηλαδή όπου ισχύει G': αβελιανή, η Εύα θα χρειαστεί να προσθέσει άπειρες το πλήθος ορίζουσες σχέσεις καθώς γνωρίζουμε ότι η ελεύθερες μετα-αβελιανές ομάδες δεν είναι πεπερασμένα παριστώμενες. Όμως αυτή η εξέλιξη δεν θα την προ-

βληματίσει καθώς δεν χρειάζεται πραγματικά να προσθέσει άπειρα το πλήθος στοιχεία: μπορεί απλά να θεωρήσει την Γ_i ως μια παράσταση στην πολλαπλότητα των μετα-αβελιανών ομάδων και να εφαρμόσει τον σχετικό αλγόριθμο που είναι καθολικός για όλες τις πεπερασμένα παριστώμενες ομάδες μέσα στη συγκεκριμένη πολλαπλότητα.
Τέλος, θα σημειώσουμε ότι αυτό το είδος επίθεσης δεν μπορεί να χρησιμοποιηθεί σε υπερβολικά πηλίκα καθώς δεν υπάρχει μέθοδος προσθήκης συγκεκριμένων γεννητόρων στη $\hat{\Gamma}$, η οποία να διασφαλίζει το ότι η καινούρια ομάδα είναι υπερβολική. Αυτό το γεγονός εμποδίζει την Εύα από το να χρησιμοποιήσει τη λεγόμενη και ιδιαίτερα αποτελεσματική υπερβολική επίθεση πηλίκων. Για να γίνει πιο σαφές το τι ακριβώς εννοούμε θα υπενθυμίσουμε ότι οι πεπερασμένα παριστώμενες *small cancellation groups* (δηλαδή οι ομάδες τις οποίες περιέχει η 'δεξαμενή' μας) είναι ως προς λέξη υπερβολικές με το πρόβλημα λέξης να είναι επιλύσιμο εντός τους μέσω του αλγορίθμου του *Dehn*.

Για να κλείσουμε την υποπαράγραφο, θα αναφερθούμε σε μέτρα άμυνας που ήδη έχουμε πάρει κατά τη μεθοδολογία του πρωτοκόλλου. Γενικά, η επίθεση που μόλις περιγράψαμε επιστρατεύει μηδενοδύναμα ή μετα-αβελιανά πηλίκα της $\hat{\Gamma}$. Γι' αυτόν ακριβώς το λόγο η Αλίκη είχε προσθέσει στην ομάδα της την ορίζουσα σχέση $x'_i = \prod_{j=1}^{M}[x'_i, w_j]$ και ο Βασίλης είχε επιλέξει στοιχείο της μορφής $[x'_i, u]$ όποτε ήθελε να μεταδώσει μη μοναδιαίο στοιχείο. Πράγματι, η επίθεση μετα-αβελιανού πηλίκου σε στοιχείο της μορφής $[x'_i, u]$ δεν θα μπορούσε να λειτουργήσει καθώς αυτό το στοιχείο ανήκει στην ομάδα $(\hat{\Gamma})''$ μιας και το x'_i ανήκει στο $(\hat{\Gamma})'$ μέσω της ορίζουσας σχέσης $x'_i = \prod_{j=1}^{M}[x'_i, w_j]$ και το u είχε οριστεί με τον τρόπο που είχαμε αναφέρει. Επιπλέον, ένα στοιχείο της μορφής $[x'_i, u]$ ανήκει σε κάθε όρο της κατωτέρας κεντρικής σειράς, καθώς $[x'_i, u] = [\prod_{j=1}^{M}[x'_i, w_j], u] = [\prod_{j=1}^{M}[\prod_{j=1}^{M}[x'_i, w_j], w_j], u]$ κλπ. Άρα, με αυτό τον τρόπο είμαστε προστατευμένοι και από τις επιθέσεις μηδενοδύναμου πηλίκου.

4.3.5 Η Επίθεση Εξομοίωσης Κρυπτογράφησης

Σε αυτό το μέρος θα αναπτύξουμε ένα άλλο είδος επίθεσης, τη λεγόμενη επίθεση εξομοίωσης κρυπτογράφησης. Η διαδικασία είναι έχει ως εξής: η Εύα δημιουργεί διαρκώς κλειδιά με τυχαίο τρόπο και στη συνέχεια ελέγχει κατά πόσο η κάθε επιλογή συμπίπτει με την ακολουθία την οποία μεταδίδει ο Βασίλης. Η ελπίδα του επιτιθέμενου είναι αυτό να πραγματοποιηθεί με ΄συντριπτική΄ πιθανότητα. Έτσι, η αποτελεσματικότητα του αλγορίθμου καθορίζει το αν θα επιτραπεί στην Εύα να αποκρυπτογραφήσει.

Ωστόσο, η περιγραφή που μόλις κάναμε αφορά γενικά τη μέθοδο επίθεσης ανεξαρτήτως πρωτοκόλλου. Στην περίπτωση του πρωτοκόλλου *Shpilrain - Zapata* αυτή η συντριπτική πιθανότητα δεν υφίσταται. Ο λόγος που συμβαίνει αυτό έχει να κάνει με το ότι η μέθοδος της νόμιμης αποκρυπτογράφησης της Αλίκης δεν είναι τέλεια, με την έννοια ότι και αυτή βασίζεται στις πιθανότητες.

Ας δούμε όμως ποια ακριβώς είναι η μέθοδος της παράνομης αποκρυπτογράφησης: η Εύα φτιάχνει δύο λίστες. Η πρώτη περιέχει όλες τις λέξεις οι οποίες είναι διάφορες του μοναδιαίου στοιχείου της $\hat{\Gamma}$ και η δεύτερη όλες αυτές οι οποίες είναι ίσες με τη μονάδα. Σε πρακτικό επίπεδο, η πρώτη λίστα δεν έχει κάποια χρησιμότητα μιας και η επιλογή του Βασίλη για το μη μοναδιαίο στοιχείο είναι εντελώς τυχαία και άρα θα έπρεπε να περιέχει ολόκληρη την ελεύθερη ομάδα. Συνεπώς, είναι αρκετό το να αποφανθεί κανείς αν ένα στοιχείο ανήκει στη δεύτερη λίστα ή όχι. Έτσι, ο πυρήνας του προβλήματος είναι το κατά πόσο μπορούμε να απαντήσουμε στην ερώτηση για το αν ένα στοιχείο ανήκει σε μία άπειρη λίστα. Άρα, θα μπορούσε να πει κανείς ότι η Εύα μπορεί να ελέγχει μέχρι κάποιο σημείο και από εκεί και πέρα να υποθέτει ότι η πιθανότητα να είναι σωστή είναι συντριπτικά μεγάλη (κοντά στο 1). Ουσιαστικά, δηλαδή, να πράξει όπως και η Αλίκη. Ωστόσο, κάτι τέτοιο δεν γίνεται μιας και όπως θα δούμε στη συνέχεια, η πιθανότητα με την οποία αποκρυπτογραφεί η Αλίκη μπορεί να γίνει πολύ διαφορετική από αυτήν της Εύας. Ας δούμε πιο συγκεκριμένα τι ακριβώς συμβαίνει:

- Προκειμένου η Αλίκη να αποκρυπτογραφήσει σωστά με συντριπτική πιθανότητα, θα πρέπει η πιθανότητα $P_1(N)$ μια τυχαία λέξη μήκους N να μην είναι το μοναδιαίο στοιχείο της ομάδας, να τείνει στο 1 με αυξημένο ρυθμό καθώς το N τείνει στο άπειρο.

- Προκειμένου η Εύα να αποκρυπτογραφήσει σωστά με συντριπτική πιθανότητα, θα πρέπει η πιθανότητα $P_2(N, f(N))$ μια τυχαία λέξη μήκους N, η οποία είναι το μοναδιαίο στοιχείο, να έχει απόδειξη μήκους μικρότερη ή ίση του $f(N)$ για το ότι πράγματι είναι το μοναδιαίο, να συγκλίνει στο 1 με αυξημένο ρυθμό καθώς το N τείνει στο άπειρο, όπου το $f(N)$ αντιπροσωπεύει την υπολογιστική ικανότητα της Εύας.

Παρατηρούμε ότι οι μορφές που έχουν οι δύο πιθανότητες είναι εντελώς διαφορετικής φύσης. Ήδη έχουμε δει ότι η $P_1(N)$ έχει αναλυθεί επαρκώς και, πράγματι, τείνει στο 1 καθώς το N τείνει στο άπειρο για άπειρες ομάδες.

Αντίθετα, η κατάσταση για την Εύα δεν είναι τόσο απλή μιας και η πιθανότητα $P_2(N, f(N))$, ως συνάρτηση, μπορεί να γίνει ιδιαίτερα πολύπλοκη. Μάλιστα, αυτού του είδους οι συναρτήσεις είναι αντικείμενο ερευνών. Εμείς θα αναφέρουμε ότι είναι πιθανό για κάθε συνάρτηση $f(N)$ να υπάρχουν ομάδες για τις οποίες η σύγκλιση στο 1 δεν συμβαίνει καν.

Σε αυτό το σημείο θα χρησιμοποιήσουμε μία δημοσίευση των $Osin$ και $Shpilrain$ [13]. Σε αυτήν την πηγή εντοπίζουμε μια πρακτική ανάλυση των όσων μόλις περιγράψαμε.

Η ανάλυση που έχουμε κάνει αλλά και που θα κάνουμε βασίζεται στις εξής παραδοχές:

1. Η Εύα δεν έχει υπολογιστικούς περιορισμούς.
2. Η Εύα γνωρίζει τα πάντα σχετικά με τον Βασίλη - αλγόριθμο κρυπτογράφησης και υλικό ($hardware$).
3. Η Εύα δεν γνωρίζει τον αλγόριθμο που χρησιμοποιεί η Αλίκη για τη δημιουργία του δημοσίου κλειδιού.

Θα σημειώσουμε ότι το 1. προφανώς και δεν εμφανίζεται σε πραγματικές συνθήκες αλλά το χρησιμοποιούμε στην εργασία μας προκειμένου να ενισχύσουμε τη θεωρητική της δυναμική.

Πριν προχωρήσουμε σε λεπτομέρειες, πρέπει να διευκρινίσουμε ότι το πρωτόκολλό μας δεν 'υπόσχεται' ασφάλεια από επίθεση εξομοίωσης κρυπτογράφησης στο δημόσιο κλειδί ή στον αλγόριθμο αποκρυπτογράφησης της Αλίκης, αλλά μονάχα από αυτήν η οποία στοχεύει στις μεταδόσεις του Βασίλη.

Επίσης, πρέπει να αναφερθεί ότι σε διάφορες εμπορικές εφαρμογές, όπως οι διαδικτυακές συναλλαγές, θεωρούνται γνωστοί τόσο οι δύο αλγόριθμοι της Αλίκης όσο και ο αλγόριθμος του Βασίλη. Ως εκ τούτου, οι αλγόριθμοι κρυπτογράφησης της Αλίκης θεωρούνται πιο επισφαλείς στις επιθέσεις εξομοίωσης κρυπτογράφησης.

Τώρα θα περιγράψουμε ένα σχήμα το οποίο είναι ασφαλές ενάντια στις επιθέσεις στη μετάδοση του Βασίλη, με βάση πάντα τις τρεις προϋποθέσεις τις οποίες αναφέραμε παραπάνω. Πιο συγκεκριμένα, ο Βασίλης κρυπτογραφεί και αποστέλλει κάθε φορά ένα ψηφίο της ακολουθίας του, και η Αλίκη αποκρυπτογραφεί το κάθε ψηφίο σωστά με πιθανότητα που μπορεί να θεωρηθεί οσοδήποτε κοντά στο 1 θέλουμε αλλά όχι ακριβώς 1. Επίσης, αξίζει να αναφερθεί ότι δεν υπάρχουν απαιτήσεις όσον αφορά τις υπολογιστικές ικανότητες του Βασίλη και μάλιστα, η κρυπτογράφησή του μπορεί να γίνει ακόμα και χειρονακτικά, όπως για παράδειγμα σε ένα πεδίο στρατιωτικών επιχειρήσεων όπου ο επικεφαλής αξιωματικός μπορεί να κάνει την κρυπτογράφησή του με 'χαρτί και μολύβι' και να μεταδόσει το μήνυμά του ακόμα και μέσω τηλεφώνου. Σε αυτήν την περίπτωση, στην οποία ανήκει και το δικό μας πρωτόκολλο, δεν χρειάζεται να είναι γνωστό κανένα από τα στοιχεία που αφορούν την Αλίκη. Πάντως, αυτό που θα περιγράψουμε δεν είναι ιδιαίτερα πρακτικό για εμπορικές εφαρμογές καθώς απαιτεί σημαντική εργασία από την Αλίκη προκειμένου να παραλάβει ακόμα και ένα ψηφίο από τη μετάδοση του Βασίλη. Το σχήμα εχει τα εξής χαρακτηριστικά:

1. Ο Βασίλης κρυπτογραφεί το μυστικό ψηφίο του με μια λέξη από ένα δημόσιο αλφάβητο X.

2. Η Αλίκη αποκρυπτογραφεί τη μετάδοση του Βασίλη σωστά με πιθανότητα αυθαίρετα κοντά στο 1, αλλά όχι ακριβώς 1.

3. Η Εύα δεν έχει κανένα περιορισμό όσον αφορά την ταχύτητα υπολογισμού και τον χώρο αποθήκευσης.

4. Η Εύα γνωρίζει πλήρως τον αλγόριθμο και το υλικό του Βασίλη. Όμως, δεν μπορεί να προβλέψει τους τυχαίους αριθμούς τους οποίους επιλέγει ο Βασίλης και δεν γνωρίζει τον αλγόριθμο δημιουργίας δημοσίου κλειδιού της Αλίκης.

5. Η Εύα δεν μπορεί να αποκρυπτογραφήσει το ψηφίο του Βασίλη με πιθανότητα μεγαλύτερη του 3/4.

Τώρα, θα περιγράψουμε το ίδιο το πρωτόκολλο, σε κάθε επανάληψη του οποίου μεταδίδεται και από ένα ψηφίο. Για κάθε ψηφίο η Αλίκη δημιουργεί και ένα καινούριο δημόσιο κλειδί:

1. Η Αλίκη κοινοποιεί δύο παραστάσεις ομάδων ως εξής:

   $\Gamma_1 = \langle x_1, x_2, ..., x_n | r_1, r_2, ..., r_k \rangle$
   $\Gamma_2 = \langle x_1, x_2, ..., x_n | s_1, s_2, ..., s_m \rangle$
   Μία από αυτές ορίζει την τετριμμένη ομάδα ενώ η άλλη ορίζει μία άπειρη ομάδα και τις οποίες μόνο η Αλίκη μπορεί να διακρίνει. Επίσης, θα πρέπει στην άπειρη ομάδα να μπορεί να επιλυθεί το πρόβλημα λέξης αποτελεσματικά, δηλαδή να μπορεί να αποφανθεί η Αλίκη σχετικά με το αν ένα στοιχείο ισούται με τη μονάδα ή όχι μέσα στη δεδομένη ομάδα. Η επιλογή τέτοιων ομάδων δεν θα πρέπει να μας προβληματίζει, καθώς ήδη έχουμε αναφέρει πως οι *small cancellation groups* εκπληρώνουν την επιθυμία μας.

2. Ο Βασίλης στην περίπτωση που θέλει να μεταδώσει το 1, εργάζεται ως εξής: Μεταδίδει ένα ζεύγος λέξεων (w_1, w_2) από το αλφάβητο $X = x_1, x_2, ..., x_n, x_1^{-1}, x_2^{-1}, ..., x_n^{-1}$, με την πρώτη να έχει επιλεγεί τυχαία ενώ με τη δεύτερη να ισούται με το μοναδιαίο στοιχείο της ομάδας G_2 η οποία ορίζεται από την παράσταση Γ_2.

3. Ο Βασίλης στην περίπτωση που θέλει να μεταδώσει το 0, εργάζεται ως εξής: Μεταδίδει ένα ζεύγος λέξεων με την δεύτερη να έχει επιλεγεί τυχαία και με την πρώτη να ισούται με το μοναδιαίο στοιχείο της ομάδας G_1 η οποία και ορίζεται από την πρώτη παράσταση.

Σε αυτό το σημείο θα προσδιορίσουμε το πώς ακριβώς λειτουργούν οι δύο αλγόριθμοι του Βασίλη:

Για να επιλέξει ένα στοιχείο διάφορο του μοναδιαίου στην ομάδα G_1, απλά επιλέγει μία τυχαία λέξη την οποία χτίζει γράμμα προς γράμμα, διαλέγοντας στοιχεία χωρίς διάκριση από το αλφάβητο X. Το μήκος της λέξης επιλέγεται συναρτήσει της υπολογιστικής του ικανότητας. Στο τέλος, διαγράφει λέξης της μορφής: $x_i x_i^{-1}$

Για να επιλέξει στοιχείο ίσο με τη μονάδα της ομάδας G_i, χρειάζεται να εφαρμόσει τις παρακάτω δύο μεθόδους κατά τυχαιά ακολουθία, ξεκινώντας με την τυχαία λέξη:

1. Εισάγουμε σε τυχαία θέση της λέξης το γινόμενο hh^{-1}, όπου h τυχαία λέξη.

2. Εισάγουμε σε τυχαία θέση της λέξης το τυχαίο συζυγές $g^{-1}r_i g$, όπου r_i είναι μια τυχαία ορίζουσα σχέση της ομάδας.

Όπως και προηγουμένως, θα πρέπει και τώρα ο Βασίλης να διαγράψει όλους τους όρους της μορφής: $x_i x_i^{-1}$. Πάντως, σε κάθε περίπτωση, το σημαντικό είναι οι λέξεις οι οποίες θα προκύψουν από τις δύο μεθόδους να έχουν το ίδιο μήκος και όχι η ίδια η μέθοδος παραγωγής του μοναδιαίου στοιχείου, μιας και μπορεί να αντικατασταθεί και από άλλες χωρίς προβλήματα.

Ας δούμε τώρα τον τρόπο με τον οποίο αυτό το σχήμα εξυπηρετεί την αποκρυπτογράφηση από μέρους της Αλίκης:
Ας υποθέσουμε χωρίς βλάβη της γενικότητας ότι η ομάδα G_1 είναι η τετριμμένη, ενώ η G_2 είναι η άπειρη. Έστω ότι παραλαμβάνει μια μετάδοση του Βασίλη (w_1, w_2) με $w_1 \in G_1$ και $w_2 \in G_2$. Οι περιπτώσεις που μπορούν να εμφανιστούν είναι οι εξής:

- $w_1 = 1_{G_1}$, $w_2 \neq 1_{G_2}$: Τότε η Αλίκη μπορεί να συμπεράνει με πιθανότητα ακριβώς ίση με 1 ότι ο Βασίλης σκοπεύει στο να μεταδώσει το 0.

- $w_1 = 1_{G_1}$, $w_2 = 1_{G_2}$: Τότε η Αλίκη μπορεί να συμπεράνει ότι ο Βασίλης σκοπεύει στο να μεταδώσει το 1, αλλά όμως η πιθανότητα ακρίβειας της Αλίκης δεν είναι ακριβώς 1. Αυτό οφείλεται στο ότι ο Βασίλης όποτε επιθυμεί να μεταδώσει ένα μη μοναδιαίο στοιχείο από μια ομάδα, τότε απλά επιλέγει ένα με τυχαίο τρόπο. Έτσι, υπάρχει η (υπερβολικά μικρή) πιθανότητα, ο Βασίλης να μεταδώσει ένα μοναδιαίο στοιχείο ενώ στόχευε σε

μη μοναδιαίο. Συνεπώς, υπάρχει μια ελάχιστη πιθανότητα η Αλίκη να καταλήξει σε λανθασμένο συμπέρασμα. Αυτό το ζήτημα το έχουμε αναλύσει λεπτομερώς σε προηγούμενη παράγραφο. Εδώ απλά θα προσθέσουμε ότι για τις περισσότερες ομάδες αυτή η πιθανότητα σφάλματος ε, τείνει στο μηδέν με εκθετική ταχύτητα καθώς το μήκος της w_2 τείνει στο άπειρο.

Φυσικά, για να ολοκληρωθεί η μελέτη ενός σχήματος, οφείλουμε να εξετάσουμε και τις μεθόδους επίθεσης σε αυτό.

Χρησιμοποιώντας τα χαρακτηριστικά 3 και 4 του σχήματος, όπως τα περιγράψαμε παραπάνω, μπορούμε να πούμε ότι η Εύα θα καταφέρει να ταυτοποιήσει τη λέξη που ισούται με το μοναδιαίο στοιχείο στην αντίστοιχη ομάδα, καθώς και τη λέξη (αν υπάρχει) η οποία δεν αντιστοιχεί σε μοναδιαίο. Μην ξεχνάμε ότι η ιδιότητα 3 ουσιαστικά υπονοεί ότι δεν υπάρχει ο περιορισμός της συνάρτησης $f(N)$ που αναφέραμε προηγουμένως. Ο τρόπος με τον οποίο το κάνει είναι η μέθοδος που έχουμε ήδη περιγράψει, η προσομοίωση κρυπτογράφησης. Δηλαδή, η Εύα θα επαναλάβει τους δύο αλγορίθμους του Βασίλη (τους οποίους και γνωρίζει) κατά τυχαίο τρόπο, καταλήγοντας να έχει φτιάξει δύο λίστες στοιχείων: η πρώτη περιέχει τα υποτιθέμενα μη μοναδιαία στοιχεία και η δεύτερη τα μοναδιαία. Όπως έχουμε ήδη επισημάνει, στη λίστα των μη μοναδιαίων στοιχείων, επί της ουσίας εμφανίζονται όλες οι λέξεις του αλφαβήτου - με συντριπτική πιθανότητα - κι αυτό γιατί η μέθοδος με την οποία εργάζεται ο Βασίλης στηρίζεται στην απόλυτη τυχαιότητα. Συνεπώς, δεν έχει νόημα το να ασχοληθεί με αυτήν η Εύα και άρα επικεντρώνεται στην άλλη λίστα η οποία περιέχει τα μοναδιαία στοιχεία της αντίστοιχης ομάδας.
Το βασικό πρόβλημα που αντιμετωπίζει η Εύα σε αυτό το σημείο είναι ότι καλείται να αποφανθεί για το αν ανήκει ή όχι ένα στοιχείο στη λίστα, δεδομένου ότι η λίστα είναι άπειρη. Εδώ, η Εύα επιστρατεύει το χαρακτηριστικό 4. του σχήματος, δηλαδή, εφόσον γνωρίζει τους αλγορίθμους αλλά και τις υπολογιστικές δυνατότητες ($hardware$) του Βασίλη, τότε μπορεί να προσδιορίσει ένα όριο σχετικά με το μήκος της λίστας. Συνεπώς, η Εύα μπορεί πράγματι να καταλήξει σε συμπεράσματα για το αν μια λέξη ισούται με το μοναδιαίο στοιχείο ή όχι. Ας δούμε πιο συγκεκριμένα τι ακριβώς συμβαίνει:

1. $w_1 = 1_{G_1}$ και $w_2 = 1_{G_2}$
2. $w_1 = 1_{G_1}$ και $w_2 \neq 1_{G_2}$

3. $w_1 \neq 1_{G_1}$ και $w_2 = 1_{G_2}$

Θα ξεκινήσουμε την ανάλυση αναφέροντας ότι οι περιπτώσεις 2. και 3. δεν μπορεί να συμβαίνουν συγχρόνως, καθώς έχουμε πει ότι μία από τις δύο ομάδες είναι η τετριμμένη και η άλλη άπειρη. Επομένως, είναι σαφές ότι η περίπτωση 1. εμφανίζεται με πιθανότητα 1/2. Συγκεκριμένα, η περίπτωση 1. πραγματοποιείται είτε όταν ο Βασίλης θέλει να μεταδώσει το 1 και η G_1 είναι η τετριμμένη είτε όταν θέλει να μεταδώσει το 0 και η G_2 είναι η τετριμμένη. Αν πραγματοποιείται η 1. τότε η Εύα δεν μπορεί να αποκρυπτογραφήσει με πιθανότητα γνήσια μεγαλύτερη του 1/2 καθώς δεν γνωρίζει ποια είναι η τετριμμένη ομάδα και άρα δεν μπορεί να αντιληφθεί την πρόθεση του Βασίλη. Ενδεχομένως, η Εύα να μπορούσε να βελτιώσει την πιθανότητά της, αλλά αυτό μπορεί να πραγματοποιηθεί με επίθεση εις βάρος της Αλίκης και όπως έχουμε αναφέρει από την αρχή, θα ασχοληθούμε μόνο με επιθέσεις ενάντια στο Βασίλη. Εμείς απλά θα περιοριστούμε στο να αναφέρουμε ότι, σε αντίθεση με το τι μπορεί να υποδεικνύει η ΄κοινή αντίληψη΄, το να συμπεράνει κανείς αν μια ομάδα είναι η τετριμμένη μπορεί να γίνει μία ιδιαίτερα δύσκολη διαδικασία.
Τώρα θα αναφερθούμε στο πιο σημαντικό μέρος του σχήματος και για το οποίο μέχρι ώρας δεν έχουμε πει τίποτε. Φυσικά αναφερόμαστε στο χαρακτηριστικό 5. Δηλαδή, θα εξηγήσουμε το γιατί η πιθανότητα με την οποία αποκρυπτογραφεί η Εύα το κάθε φηφίο δεν μπορεί να ξεπεράσει το 3/4. Πράγματι, όταν εμφανίζεται η πρώτη περίπτωση, η πιθανότητα σωστής αποκτυπτογράφησης είναι 1, ενώ όταν εμφανίζεται είτε η δεύτερη είτε η τρίτη (δεν μπορεί να συμβαίνουν και οι δύο) τότε η πιθανότητα είναι 1/2. Έτσι, υπολογίζουμε: $(1)\cdot 1/2 + (1/2)\cdot 1/2$. Άρα, πράγματι, η πιθανότητα της Εύας να υποκλέψει σωστά ένα ψηφίο της μετάδοσης του Βασίλη είναι ακριβώς 3/4. Αυτή η πιθανότητα ενδεχομένως να φαίνεται αρκετά μεγάλη, στην πραγματικότητα όμως κάτι τέτοιο δεν ισχύει: αν η μετάδοση του Βασίλη έχει n ψηφία, τότε η πιθανότητα που έχει η Εύα να υποκλέψει σωστά ολόκληρο το μήνυμα είναι $(3/4)^n$. Έτσι, είναι εύκολα αντιληπτό ότι καθώς αυξάνεται το n, η πιθανότητα της Εύας μειώνεται με υψηλό ρυθμό. Για να έχει ο αναγνώστης μια εικόνα για το πόσο γρήγορα μειώνεται, απλά θα αναφέρουμε ότι για τα 16 ψηφία μιας πιστωτικής κάρτας και με πιθανότητα 3/4 για το κάθε ψηφίο, αντιστοιχεί πιθανότητα της τάξης του 10^{-7}. Επομένως, τώρα μπορούμε να αντιληφθούμε πλήρως το λόγο για τον οποίο το σχήμα έχει αυτή τη μορφή και πιο συγκεκριμένα, το λόγο για τον οποίο η Αλίκη χρησιμοποίησε το τέχνασμα των δύο ομάδων. Ουσιαστικά, η Εύα καλείται να αντιμετωπίσει την άγνοια της ως προς το ποια ομάδα είναι η τετριμμένη, ενώ η Αλίκη αντιμετωπίζει μονάχα τον κίνδυνο ο Βασίλης να επιλέξει άθελά του το

μοναδιαίο στοιχείο ομάδας - κινδύνος ο οποίος, όπως έχουμε πει, είναι ιδιαίτερα μικρός.

Για να ολοκληρώσουμε τη μελέτη του πρωτοκόλλου $Shpilrain$ - $Zapata$, οφείλουμε να κάνουμε μια αναφορά και στην επίθεση που μπορεί να εξαπολύσει η Εύα σε βάρος της Αλίκης, μία επίθεση η οποία έχει υψηλές απαιτήσεις όσον αφορά τις υπολογιστικές δυνατότητες της Εύας (υπερεκθετικά μεγαλύτερες από αυτές τις Αλίκης). Πρόκειται για επίθεση εξομοίωσης (και άρα θα πρέπει η Εύα να γνωρίζει τους αλγορίθμους της Αλίκης) που στοχεύει στο δημόσιο κλειδί. Πιο συγκεκριμένα, μπορούμε να πούμε το εξής:

Η Εύα εξομοιώνει τον αλγόριθμο της Αλίκης, παράγοντας δημόσια κλειδιά ξανά και ξανά με τυχαίο τρόπο και κάποια στιγμή, με συντριπτική πιθανότητα, θα πετύχει το στόχο της, δηλαδή θα αποκτήσει το πραγματικό κλειδί.

Αν πετύχει το στόχο της, πλέον θα έχει πλήρη γνώση των ομάδων που χρησιμοποιούνται στο πρωτόκολλο και άρα θα μπορεί να αποκρυπτογραφήσει τη μετάδοση του Βασίλη με την ίδια πιθανότητα με την οποία το κάνει και η Αλίκη.

Βέβαια, ο πραγματικός λόγος για τον οποίο κάνουμε αυτήν τη συζήτηση είναι το να καταλήξουμε σε έναν αλγόριθμο τον οποίο να μπορεί να χρησιμοποιήσει η Αλίκη για να αυξήσει την ασφάλειά της. Ο αλγόριθμος είναι απλός και στοχεύει στο να δημιουργεί υπερεκθετικά πολλές εκδοχές για τον επίδοξο κρυπταναλυτή και έτσι να του δημιουργεί ιδιαίτερα αυξημένες υπολογιστικές απαιτήσεις σε σύγκριση με τις δυνατότητες της Αλίκης.

Ο αλγόριθμος είναι πολύ απλός και ο στόχος του είναι να δημιουργεί παραστάσεις της τετριμμένης ομάδας με διάφορους τρόπους. Είναι γνωστό ότι οι παράστασεις με τον παρακάτω τύπο απεικονίζουν την τετριμμένη ομάδα:

$\langle x, y | x^{-1}y^n x = y^{n+1}, w = 1 \rangle$, όπου $n \geq 1$ και w είναι οποιαδήποτε λέξη των x και y με άθροισμα εκθετών του x ίσο με τη μονάδα.

Ας υποθέσουμε ότι το μήκος k της w είναι ένας επαρκώς μεγάλος ακέραιος ο οποίος επιλέγεται από την Αλίκη. Αυτός ο αριθμός μπορεί να θεωρηθεί ένα μέτρο της πολυπλοκότητας της παράστασης. Σε τεχνικό επίπεδο, μπορούμε να πούμε ότι και το n επηρεάζει την πολυπλοκότητα, αλλά δεν είναι ιδιαίτερα σημαντικό για εμάς και έτσι θα το θεωρούμε αρκετά μικρό και σταθερό σε όσα

θα ακολουθήσουν.

Θα περιγράψουμε έναν αλγόριθμο k βημάτων για την παραγωγή παραστάσεων πολυπλοκότητας $O(k^3)$ οι οποίες αντιπροσωπεύουν την τετριμμένη ομάδα:

1. Στο πρώτο βήμα, η Αλίκη επιλέγει μια παράσταση της μορφής:
   $\langle x_1, y_1 | x_1^{-1} y_1^n x_1 = y_1^{n+1}, w_1 = 1 \rangle$, όπου w_1 είναι τυχαία λέξη των x_1 και y_1 με μήκος k και άθροισμα εκθετών του x_1 ίσο με 1.

2. Στο i-οστό βήμα, με $1<i<k$, η Αλίκη προσθέτει δύο νέους γεννήτορες, x_i και y_i, καθώς και μία καινούρια ορίζουσα σχέση w_i μήκους k και με άθροισμα εκθετών του x_i ίσο με 1. Επίσης, προσθέτει την ορίζουσα σχέση $x_i^{-1} y_i^n x_i = y_i^{n+1}$. Η παράσταση η οποία προκύπτει εξακολουθεί να απεικονίζει την τετριμμένη ομάδα και, πιο συγκεκριμένα, ισχύει $x_i = 1$ και $y_i = 1$. Στη συνέχεια, η Αλίκη αναμειγνύει τους παλιούς γεννήτορες με τους καινούριους προσθέτοντας τα στοιχεία $x_i^{\pm 1}$ και $y_i^{\pm 1}$ σε k τυχαίες θέσεις της κάθε ορίζουσας σχέσης. Η ιδέα είναι να προκύπτουν χονδρικά k γεννήτορες με δείκτη i σε κάθε παλία ορίζουσα σχέση.

3. Στο k-οστό βήμα, η Αλίκη προσθέτει δύο καινούριους γεννήτορες, x_k και y_k, και δύο ορίζουσες σχέσεις, $x_k^{-1} y_k x_k y_k^{-2}$ και w_k, όπου w_k είναι λέξη μικρού μήκους, ας πούμε μεταξύ 3 και 6, η οποία έχει άθροισμα εκθετών του x_k ίσο με 1. Η ομάδα η οποία προκύπτει είναι τετριμμένη και για να γίνει αυτό πιο σαφές αρκεί να επισημάνουμε ότι
   $x_k^{-1} y_k x_k y_k^{-2} = 1 \iff x_k^{-1} y_k x_k = y_k^2$, και το οποίο ικανοποιεί τη μορφή:
   $x^{-1} y^n x = y^{n+1}$
   Άρα, όλοι οι γεννήτορες ισούνται με το μοναδιαίο στοιχείο της ομάδας. Στη συνέχεια, η Αλίκη προσθέτει σε αυτήν την παράσταση χονδρικά άλλες k ορίζουσες σχέσεις, όπου κάθε τέτοια σχέση είναι μια τυχαία λέξη των γεννητόρων $x_1, y_1, x_2, y_2, ..., x_k, y_k$ μήκους 1,2 ή 3. Η μόνη παρέμβαση που κάνει η Αλίκη στην τυχαιότητα των λέξεων είναι ότι φροντίζει έτσι ώστε κάθε γεννήτορας να εμφανίζεται τουλάχιστον σε μία τέτοια λέξη / ορίζουσα σχέση. Στη συνέχεια, η Αλίκη αναμειγνύει τις καινούριες ορίζουσες σχέσεις τόσο μεταξύ τους όσο και με τις ορίζουσες σχέσεις $x_k^{-1} y_k x_k y_k^{-2}$ και w_k, μέσω των παρακάτω μετασχηματισμών:

$r_i \to r_i r_j$, $r_i \to r_i r_j^{-1}$, $r_i \to r_j r_i$, $r_i \to r_j^{-1} r_i$, όπου r_i, r_j είναι διαφορετικές μεταξύ τους ορίζουσες σχέσεις.

Εφαρμόζουμε αυτούς τους μετασχηματισμούς μέχρι όλες οι ορίζουσες σχέσεις να έχουν χονδρικά k εμφανίσεις του κάθε γεννήτορα.

4. Για το τελευταίο βήμα του αλγορίθμου, η Αλίκη επαναβαπτίζει τυχαία όλους τους γεννήτορες προκειμένου να κρύψει την ακολουθία των βημάτων της.

Έτσι, προκύπτει ότι ο αλγόριθμος που μόλις περιγράψαμε έχει πολυπλοκότητα $O(k^3)$. Αυτό έχει ως συνέπεια το ότι η Εύα, προκειμένου να εξομοιώσει πλήρως την τυχαιότητα του αλγορίθμου, θα χρειαζόταν χρόνο της τάξης του $O(k^k)$. Πιο συγκεκριμένα, θα έπρεπε να 'εξερευνήσει' τυχαίες (υπο)λέξεις μήκους k, σε $2k$ το πλήθος γράμματα.

4.3.6 Ανακεφαλαίωση του Πρωτοκόλλου

Το συγκεκριμένο πρωτόκολλο κάλυψε σημαντική έκταση και η περιγραφή και ανάλυσή του πέρασε από διάφορα στάδια. Αυτό μπορεί να έχει ως αποτέλεσμα ναι μεν ο αναγνώστης να κατανόησε το κάθε βήμα ξεχωριστά, αλλά πάντοτε υπάρχει ο κίνδυνος να χάθηκε η γενική εποπτεία για το πώς πορευτήκαμε. Σε αυτήν την τελευταία παράγραφο θα ασχοληθούμε ακριβώς με αυτό - τη γενική επισκόπηση των όσων αναφέραμε.

Στην αρχή αναφερθήκαμε στο πρωτόκολλο *Wagner - Magyarik*. Οι δημιουργοί πίστευαν πως είχαν κατασκευάσει ένα ασφαλές πρωτόκολλο το οποίο βασιζόταν στο πρόβλημα λέξης. Στη συνέχεια, αποδείχθηκε πως, στην πραγματικότητα, βασιζόταν στο πρόβλημα επιλογής λέξης, το οποίο μάλιστα ήταν και ευκόλως επιλύσιμο στις ομάδες οι οποίες επιστρατεύονταν για το συγκεκριμένο πρωτόκολλο.

Έχοντας ως βάση τις ιδέες του παραπάνω πρωτοκόλλου, κατασκευάστηκε ένα νέο πρωτόκολλο, το *Shpilrain - Zapata*, το οποίο διόρθωνε τα κακώς κείμενα. Εμείς αναλύσαμε λεπτομερώς όλα του τα συστατικά στοιχεία: το σύνολο (*pool*)

των παραστάσεων, το πώς η Αλίκη επιλέγει μία και το πώς την μετασχηματίζει για να κατασκευάσει το δημόσιο κλειδί, το πώς κατασκευάζει ο Βασίλης το ιδιωτικό του κλειδί.
Στη συνέχεια, ασχοληθήκαμε με τις επιθέσεις που μπορούν να γίνουν και μέσω αυτών καταλήξαμε σε μερικές βελτιώσεις που μπορούν να εφαρμοστούν.
Αρχικά, είδαμε την επίθεση ισομορφισμού. Η Εύα προσθέτει ορίζουσες σχέσεις στην κοινοποιημένη ομάδα με την ελπίδα να την αντιστοιχίσει με κάποια ομάδα του *pool* και άρα να καταφέρει να βρει με ποια ομάδα εργάζεται η Αλίκη. Όμως, η προσπάθεια αυτή της Εύας απαιτεί τεράστια ποσότητα πόρων και έτσι είναι καταδικασμένη.
Η επόμενη μορφή επίθεσης είναι η επίθεση πηλίκου. Μπορούμε να πούμε πως μοιάζει κάπως με την επίθεση ισομορφισμού, αλλά διαφέρει στο ότι η Εύα δεν στοχεύει στο να ανακαλύψει την ομάδα της Αλίκης. Η Εύα προσπαθεί, με την προσθήκη οριζουσών σχέσεων, να μετατρέψει την ομάδα σε κάποια την οποία να γνωρίζει και η οποία να έχει εύκολα επιλύσιμο πρόβλημα λέξης. Αυτή η επίθεση, όμως, δεν έχει αποτέλεσμα καθώς η Αλίκη εργάζεται πάνω σε συγκεκριμένο είδος ομάδων οι οποίες την αποτρέπουν καθώς επίσης χρησιμοποιεί και μία ΄στοχευμένη΄ ορίζουσα σχέση. Είναι σαφές πως το πρωτόκολλο στήθηκε βασισμένο στα διάφορα είδη επιθέσεων.
Τώρα θα περάσουμε στο τελευταίο είδος επίθεσης το οποίο και επιδρά σημαντικά στη μορφή του σχήματός μας. Πρόκειται για την επίθεση εξομοίωσης κρυπτογράφησης. Εδώ, επί της ουσίας, η Εύα γνωρίζοντας τους αλγορίθμους του Βασίλη τους επαναλαμβάνει και δημιουργεί λίστες με τα στοιχεία που τις προκύπτουν. Όμως, και πάλι η επίθεση δεν αποδίδει καθώς οι πιθανότητες της δεν της εγγυώνται κατά κανένα τρόπο την επιτυχία. Ουσιαστικά, αυτό το έλλειμμα πιθανότητας βασίζεται σε ένα ακόμα τέχνασμα που προσθέτει η Αλίκη στις κινήσεις της: η βασική ιδέα είναι ότι λοξοδρομεί ελαφρώς από τον αρχικό ορισμό του σχήματος, δημοσιεύοντας δύο αντί για μία ομάδες. Έτσι, με τον τρόπο που περιγράψαμε στο κυρίως σώμα του κεφαλαίου, οι πιθανότητες παραβίασης μειώνονται δραματικά.
Τέλος, εισάγουμε ένα καινούριο τύπο επίθεσης, την επίθεση στο δέκτη, η οποία όμως χρησιμοποιεί την ήδη διατυπωμένη μεθοδολογία - πρόκειται για μια ακόμη εκδοχή της επίθεσης εξομοίωσης. Πιο συγκεκριμένα, η Εύα προσπαθεί να καταλάβει ποια ομάδα είναι η τετριμμένη από αυτές που μεταδίδει η Αλίκη (έχουμε ήδη αναφερθεί στο μάταιο της προσπάθειας αποκρυπτογράφησης της μη τετριμμένης ομάδας). Έτσι, εισάγουμε μια ακόμη γραμμή άμυνας η οποία είναι ένας αλγόριθμος ο οποίος καταλήγει να έχει υπερβολικές υπολογιστικές απαιτήσεις από την Εύα και άρα την θέτει 'εκτός μάχης΄.

4.3.7 Μία Γενική Θεώρηση του Πρωτοκόλλου

Σε αυτήν την τελευταία παράγραφο θα αναφέρουμε κάποια γενικά χαρακτηριστικά του πρωτοκόλλου.
Η κρυπτογράφηση του κάθε ψηφίου γίνεται ιδιαίτερα αποτελεσματικά καθώς απαιτείται τετραγωνικός (*quadratic*) χρόνος στο μήκος της μεταδιδόμενης λέξης - το οποίο είναι περίπου 150. Επίσης, η Αλίκη, προκειμένου να αποκρυπτογραφήσει κάθε λέξη, χρειάζεται χρόνο ο οποίος είναι φραγμένος από το $C \cdot |w|$, οπου το C είναι μια σταθερά η οποία εξαρτάται από τον ισομορφισμό που χρησιμοποιεί.
Δεν θα ήταν υπερβολή να πούμε πως η βιωσιμότητα του πρωτοκόλλου, και σε τελευταία ανάλυση και το ίδιο το πρωτόκολλο, βασίζεται αποκλειστικά στη διαφορετική δυναμική που φέρουν η Αλίκη και η Εύα και αυτή η δυναμική καθορίζεται από τους ιδιωτικούς (δηλαδή μη κοινοποιημένους) μετασχηματισμούς μέσω ισομορφισμών οι οποίοι επιστρατεύονται από την Αλίκη.

Για να ολοκληρώσουμε την ανάλυσή μας, οφείλουμε να κάνουμε και μία αναφορά σε ένα μειονέκτημα του σχήματος σε σύγκριση με άλλα ευρέως διαδεδομένα πρωτόκολλα: η κρυπτογράφηση που χρησιμοποιούμε έχει ιδιαίτερα μεγάλο βαθμό επέκτασης, με την έννοια ότι κάθε ψηφίο από τη μετάδοση του Βασίλη κρυπτογραφείται σε λέξη μήκους περίπου 150, αριθμός ο οποίος προκύπτει από πειράματα ηλεκτρονικών υπολογισμών. Αυτό ακριβώς είναι το τίμημα το οποίο καλούμαστε να πληρώσουμε προκειμένου να δεσμεύσουμε πολύ μεγάλη υπολογιστική δύναμη από την Εύα.

Βιβλιογραφία

• *Alexei Myasnikov*, *Vladimir Shpilrain*, *Alexander Ushakov - Group − based Cryptography*, *Birkhauser*

• Δημήτριος Βάρσος - Σημειώσεις Παραδόσεων Θεωρίας Ομάδων

• Χρήστος Πηλιχός - Αλγόριθμοι στη Θεωρία Ομάδων, Μ.Π.Λ.Α.

[1] *Time Complexity*, Λήμμα *Wikipedia*

[2] *Alfred J. Menezes*, *Scott A. Vanstone*, *Paul C. Van Oorschot - Handbook of Applied Cryptography*, *CRC Press*

[3] *O.Bogopolski*, *A.Martino*, *O.Maslakova*, *E.Ventura - Free−by−cyclic groups have solvable conjugacy problem*

[4] *D.Garber*, *S.Kaplan*, *M.Teicher*, *B.Tsaban*, *U.Vishne - Probabilistic solutions of equations in the braid group*

[5] *J.W.Cannon*, *W.J.Floyd*, *W.R.Parry - Introductory Notes on Richard Thompson's Groups*

[6] *Markus Grassl*, *Ivana Ilic*, *Spyros Magliveras*, *Rainer Steinwandt - Cryptanalysis of the Tillich - Zemor hash function*

[7] *Christophe Petit*, *Jean − Jacques Quisquater - Preimages for the Tillich - Zemor hash function*

[8] *Gilbert Baumslag*, *Benjamin Fine*, *Martin Kreuzer*, *Gerhard Rosenberger*

- *A Course in Mathematical Cryptography*, *DE GRUYTER*

[9] *Alexei D. Myasnikov*, *Alexei G. Myasnikov*, *Vladimir Shpilrain* - *On the Andrews - Curtis Equivalence*

[10] *Ali Bagherzandi*, *Javad Mohajeri*, *Mahmoud Salmasizadeh* - *Relations between semantic security and indistinguishability against cpa*, $non-$ *adaptive cca and adaptive cca in comparison based framework*

[11] *Ilya Kapovich*, *Alexei Myasnikov*, *Paul Schupp*, *Vladimir Shpilrain* - $Generic-case$ *complexity*, *decision problems in group theory and random walks*, *Journal of Algebra* - *March* 2002

[12] *S.Cook* - *Recursive and Recursively Enumerable Sets*, *Notes Fall* 2008, *University of Toronto* - *Computer Science*

[13] *D.Osin*, *V.Shpilrain* - *Public key encryption and encryption emulation attacks*, *Conference Paper* 2008