Αλγοριθμοι στη Θεωρια Ομαδων

Χρήστος Πηλιχός

Διπλωματική Εργασία

Επιβλέπων Καθηγητής: Ευάγγελος Ράπτης

μΠλ∀

Πανεπιστήμιο Αθηνών Τμήμα Μαθηματικών, Τμήμα Μεθοδολογίας, Ιστορίας και Θεωρίας της Επιστήμης, Τμήμα Πληροφορικής και Τηλεπικοινωνιών **Εθνικό Μετσόβειο Πολυτεχνείο** Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών, Σχολή Ηλεκτρολόγων Μηχανικών και Υπολογιστών **Πανεπιστήμιο Πατρών** Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής

Αλγόριθμοι στη Θεωρία Ομάδων

Χρήστος Πηλιχός
(Α.Μ.: 201206)

15 Νοεμβρίου 2017

Η παρούσα Διπλωματική Εργασία

εκπονήθηκε στα πλαίσια των σπουδών

για την απόκτηση του

Μεταπτυχιακού Διπλώματος Ειδίκευσης

στη

Λογική και Θεωρία Αλγορίθμων και Υπολογισμού

που απονέμει το

Τμήμα Μαθηματικών

του

Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών

Εγκρίθηκε την 13η Νοεμβρίου, 2017 από Εξεταστική Επιτροπή

αποτελούμενη από τους:

Ονοματεπώνυμο	**Βαθμίδα**	**Υπογραφή**
1. Ευάγγελος Ράπτης	Καθηγητής	……
2. Ελευθέριος Κυρούσης	Καθηγητής	……
3. Αριστείδης Παγουρτζής	Αναπληρωτής Καθηγητής	……

Αφιερωμένη, στους γονείς μου.

Χρήστος Πηλιχός,
Ασπρόπυργος 2017.

Περιεχόμενα

Κατάλογος Κρυπτογραφικών Σχημάτων

Κατάλογος Αλγορίθμων

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντά μου κ. Ευάγγελο Ράπτη τόσο για την μύησή μου στον κόσμο της Μη-Μεταθετικής Κρυπτογραφίας, όσο και για την εμπιστοσύνη που μου έδειξε στην εκπόνηση της παρούσας διπλωματικής εργασίας. Ευχαριστώ επίσης τα υπόλοιπα μέλη της τριμελούς επιτροπής κκ. Αριστείδη Παγουρτζή (που υπήρξε διδάσκων μου σε πολλά αλγοριθμικά μαθήματα) και Ελευθέριο Κυρούση (για τον μαθηματική αυστηρότητα των λεγομένων μου).

Τον επιβλέποντά στην προπτυχιακή μου εργασία κ. Παναγιώτη Νάστου, που με μύησε στον κόσμο της Κρυπτογραφίας.

Όλους εκείνους στάθηκαν δίπλα μου και που μέσα από συζητήσεις και με τις παροτρύνσεις τους ολοκλήρωσα την διπλωματική μου εργασία.

Πρόλογος

Από την αρχαιότητα ήδη αναζητούνταν τρόποι ώστε να μεταδίδονται πληροφορίες μόνον σε συγκεκριμένα άτομα. Οι τρόποι αυτοί περιορίζονταν είτε σε αριθμητικές ολισθήσεις (ο αλγόριθμος του Καίσαρα), είτε σε τεχνάσματα (όπως το γράψιμο ενός μηνύματος σε μια κορδέλα τυλιγμένη σε μία ράβδο καταλλήλου μεγέθους). Ωστόσο, τα περισσότερα περιελάμβαναν ένα είδος προσυνεννόησης (κατά πόσο έχει γίνει ολίσθηση; πόσο είναι το διαμέτρημα της ράβδου;). Ακόμη και το απόλυτα ασφαλές σημειωματάριο-μιας-χρήσης που χρησιμοποιήθηκε κατά την διάρκεια του Β΄ Παγκοσμίου Πολέμου απαιτούσε την συνάντηση των εμπλεκομένων οντοτήτων πριν την έναρξη της επικοινωνίας τους.

Ξέχωρα από όλες τις προσπάθειες της αρχαιότητας δεσπόζει εκείνη ενός βασιλιά, ο οποίος έγραψε στο ξυρισμένο κεφάλι ενός αυλικού του ένα μήνυμα κι όταν φύτρωσαν εκ νέου τα μαλλιά του αυλικού, τον έστειλε στον παραλήπτη του μηνύματος (έναν έτερο βασιλέα). Εάν και ευφυής τρόπος, είναι καθόλα αδόκιμος, μιας και συνήθως η κρυπτογραφημένη πληροφορία πρέπει να φθάσει άμεσα στον παραλήπτη της.

Η Θεωρία Ομάδων εξομάλυνε κατά πολύ την όλη κατάσταση, επιτρέποντας σε οντότητες, δίχως κάποια ιδιαίτερη προσυνεννόηση, με (δημόσια) ανταλλαγή δεδομένων, να καταλήγουν στην ίδια πληροφορία αμφότεροι. Ωστόσο, πάλι οι εμπλεκόμενες πράξεις ήταν οι συνήθεις αριθμητικές που απαντώνται στην καθημερινότητα (ασφαλώς σε αρκετά ανώτερο επίπεδο δυσκολίας/πολυπλοκότητας). Έτσι, το ενδιαφέρον στράφηκε σε πιο αφηρημένες δομές ομάδων. Εκεί, η αφαιρετική φύση τους απέκρυπτε από μόνη της πληροφορίες για τα ανταλλασσόμενα στοιχεία. Έτσι γεννάται η Μη-Μεταθετική Κρυπτογραφία.

Σκοπός της Εργασίας είναι ενασχόληση και η ανάλυσή τους εις βάθος κάποιων εφαρμογών της Μη-Μεταθετικής Κρυπτογραφίας. Πέραν του πρώτου της Κεφαλαίου, που παραθέτει βασικές έννοιες και ορισμούς ώστε να γίνονται εύληπτα όσα θα ακολουθήσουν μετέπειτα, η Εργασία χωρίζεται σε 3 βασικά μέρη:

Μέρος Ι: Κρυπτοσυστήματα εμπνευσμένα από το πρόβλημα της λέξης. Απαρχή της Μη-μεταθετικής Κρυπτογραφίας αποτελεί το κρυπτογραφικό σχήμα των Wagner-Magyarik. Κατόπιν το Μέρος συνεχίζει με το σχήμα των Garzon-Zalcstein, αλλά και μια πολύ μεταγενέστερη και ιδιάζουσα ιδέα κρυπτογράφησης με χρήση λογικών κυκλωμάτων. Τέλος, περιλαμβάνεται και μία άλλη εφαρμογή της Κρυπτογραφίας που αφορά στην ανταλλαγή πληροφορίας από περισσότερες των δύο οντοτήτων.

Μέρος ΙΙ : Κρυπτοσυστήματα βασισμένα στο πρόβλημα της συζυγίας. Το μέρος περιλαμβάνει τα δύο πιο επιφανή κρυπτογραφικά σχήματα που αφορούν το πρόβλημα της συζυγίας : εκείνο των Ko-Lee-Cheon-Han-Kang-Park (το οποίο εξάγεται απευθείας από το πρόβλημα) και το πιο εξεζητημένο των Anshel-Anshel-Goldfeld (καθώς και τη γενίκευσή του). Αμφότερα τα σχήματα έχουν πληθώρα αναφορών που εξετάζουν την κρυπτογραφική τους ασφάλεια, αλλά και προτάσεων που τα καθιστούν περισσότερο αξιόπιστα. Το Μέρος ολοκληρώνεται με μία διαφορετική –πιο διεξοδική– ματιά στα Σχήματα.

Μέρος ΙΙΙ : Κρυπτοσυστήματα βασισμένα στο πρόβλημα της αναλύσεως. Κατόπιν της ενασχόλησης με τα παραπάνω αλγοριθμικά προβλήματα, το ενδιαφέρον στράφηκε σε ένα ευρύτερο πρόβλημα, εκείνο της αναλύσεως. Η προσπάθεια του E. Stickel άφησε περιθώρια βελτίωσής της (πολυωνυμική εκδοχή του πρωτοκόλλου), καθώς και αποτέλεσε πρόσφορο έδαφος το οποίο αξιοποιήθηκε σε πιο αφηρημένες δομές (τροπική εκδοχή). Τα σχήματα των Shpilrain-Ushakov και Y. Kurt και η ασφάλειά τους κλείνουν το τρίτο και τελευταίο Μέρος της Εργασίας.

Τέλος, να σημειωθεί πως ο παραπάνω διάχωρισμός δεν εξαντλεί τον κόσμο της Μημεταθετικής Κρυπτογραφίας. Υπάρχουν κι άλλα προβλήματα (επί παραδείγματι το πρόβλημα του μέλους) και ιδιότητες των ομάδων (για παράδειγμα η ομομορφική κρυπτογράφηση) που προσφέρονται για τη δημιουργία αλγορίθμων κρυπτογράφησης και αποκρυπτογράφησης.

Χρήστος Πηλιχός
Ασπρόπυργος, 2 Οκτωβρίου, 2017

Κεφάλαιο 1

Μια εισαγωγή...

Διερευνόντας διάφορες πτυχές από την Κρυπτογραφία και την Θεωρία Ομάδων, το παρών Κεφάλαιο αποτελεί μια προσπάθεια σταχυολόγησης βασικών εννοιών που θα αποτελέσουν βασικά συστατικά σε κάθε Κεφάλαιο που έπεται. Πιο αναλυτικά, αρχικώς διακρίνονται δύο μεγάλοι τομείς για την Κρυπτογραφια: η Μεταθετική και η Μη-μεταθετική Κρυπτογραφία (η Εργασία ασχολείται με τον τελευταίο). Ύστερα, εισάγονται δύο θέματα από την Θεωρία Ομάδων: οι Ελεύθερες Ομάδες και οι Ομάδες Πλεξίδων.

1.1 ...στην Κρυπτογραφία

Η Κρυπτογραφία αποτελεί κλάδο των Μαθηματικών. Πραγματεύεται τον μετασχηματισμό δεδομένων προκειμένου το περιεχόμενο αυτών [RfC2828]:

1. Να είναι σε μια μη κατανοητή μορφή,
2. Να μην είναι δυνατόν να υποστεί μη ανιχνεύσιμη αλλοίωση,
3. Να εμποδιστεί η μη εξουσιοδοτημένη χρήση.

Ο Ron Rivest έδωσε έναν πιο βελτιωμένο ορισμό της Κρυπτογραφίας:

> "Η Κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων."
>
> [Ron Rivest, 1990]

Διάσημες εφαρμογές της Κρυπτογραφίας συνθέτουν κρυπτογραφικά σχήματα. Ακολούθως, σταχυολογούνται μόνο μερικές από αυτές τις εφαρμογές:

Ανταλλαγή κλειδιού: Πρόκειται για έναν αλγόριθμο ο οποίος επιτρέπει σε οντότητες –δίχως πρότερη συνεννόηση– να συμφωνήσουν (ανταλλάξουν) σε ένα *κοινό κλειδί* το οποίο θα διέπει την μελλοντική τους επικοινωνία με χρήση κρυπτοσυστημάτων.

Κρυπτοσυστήματα: Πρόκειται για διαδικασίες οι οποίες επιτρέπουν την *μετατροπή* απλού κειμένου σε μη κατανοητή μορφή και *τ' ανάστροφο* (με χρήση κάποιας ιδιωτικής πληροφορίας). Τα κρυπτοσυστήματα διαχωρίζονται σε:

Αλγόριθμοι συμμετρικού κλειδιού: Η διαδικασία της κρυπτογράφησης καθώς και της αποκρυπτογράφησης χρησιμοποιεί την ίδια πληροφορία (μυστικό κλειδί). Μπορεί να χρησιμοποιηθεί είτε κοινό κλειδί, είτε ένα κλειδί για την μία διαδικασία και ένα παρόμοιό του (με χρήση κάποιου μετασχηματισμού) για την άλλη διαδικασία.

Αλγόριθμοι ασύμμετρου κλειδιού: Τα κλειδιά που χρησιμοποιούνται για τις διαδικασίες της κρυπτογράφησης και αποκρυπτογράφησης είναι διαφορετικά και ιδιωτικά (δηλαδή είναι γνωστά μόνον σε μία οντότητα).

Αλγόριθμοι ροής (stream): Το κείμενο χωρίζεται σε μέρη και κρυπτογραφείται εκ των υστέρων. Συνήθως τέτοιοι αλγόριθμοι συνοδεύονται από μία γεννήτρια ψευδοτυχαίων στοιχείων η οποία παράγει μία ακολουθία στοιχείων που χρησιμεύει ως κλειδί. Το i-οστό στοιχείο κάθε μέρους κρυπτογραφείται με το i-οστό στοιχείο του κλειδιού.

Πιστοποίηση: Πρόκειται για την προσκόμιση διαβεβαίωσης μιας οντότητας έναντι μιας άλλης, στο ότι η πρότερη *κατέχει* την λύση κάποιας «προκλήσεως» (challenge), *δίχως να αποκαλυφθεί* ποια είναι η ακριβής λύση.

Τέλος, υπάρχουν κι άλλες διάσημες εφαρμογές όπως το μοίρασμα μυστικού (βλ. §4.3) και η πιστοποίηση υπογραφής (βλ. §4.3.3.Α').

Υπάρχουν δύο μεγάλοι κλάδοι στους οποίους χωρίζεται η Κρυπτογραφία:

Μεταθετική Κρυπτογραφία Μη-Μεταθετική Κρυπτογραφία

Η Μεταθετική Κρυπτογραφία είναι η πιο κοινώς διαδεδομένη αφού κάνει χρήση αριθμητικών πράξεων. Διάσημα κρυπτοσυστήματα αποτελούν εκείνα των Rivest-Shamir-Adleman [RSA78], του El Gamal [EG85], των Goldwasser-Micali [GM84], του Paillier [Pai99] καθώς και το σχήμα ανταλλαγής κλειδιού των Diffie-Hellman [DH76].

1.1.1 Μη-μεταθετική Κρυπτογραφία

Το 1911 ο Max Dehn στην εργασία του [De11] εισήγαγε τα εξής προβλήματα:

Το πρόβλημα της λέξης. Για μια ομάδα G και $w \in G$, ισχύει ότι $w = 1_G$ στην G;

[Για τις ομάδες πλεξίδων (βλ. §1.3) παρέχονται λύσεις του προβλήματος από τους Artin [Ar45], Garside-Thurston [Ga69, ECHLPT92], Birman-Ko-Lee [BKL98] και Dehornoy [Deh97].]

Το γενικευμένο πρόβλημα της λέξης. Για μια ομάδα G, $w \in G$ και $H \leqslant G$, ισχύει ότι $w \in H$;

[Το πρόβλημα επιλύεται στις κυκλικές υποομάδες της B_n, όπου ως λέξη [βλ. §1.2] ο γεννήτορας έχει άθροισμα εκθετών ίσον με 0.]

Το πρόβλημα της συζυγίας. Στην ομάδα G, έστω $w, u \in G$. Υπάρχει $x \in G$, τέτοιο ώστε $u = x^{-1}wx$;

[Ο Garside στο [Ga69] απέδειξε πως το πρόβλημα επιλύεται στις ομάδες πλεξίδων.]

Το πρόβλημα της μικρότερης λέξης. Έστω μια ομάδα G και $w \in G$. Να βρεθεί το στοιχείο μικρότερου μήκους του συνόλου $\{u \in G : u \sim w\} \subseteq G$ (βλ. σχέση (1.1)).

[Το 1991 οι M. S. Paterson και A. A. Razborov στο [PR1991] έδειξαν πως για τις ομάδες πλεξίδων το πρόβλημα είναι τουλάχιστον NP-πλήρες. Άρα, ένας αιτιοκρατικός πολυωνυμικός αλγόριθμος για το πρόβλημα της μικρότερης λέξης θα έδινε $P = NP$.]

Οι γενικές απατήσεις που χρειάζεται να ικανοποιεί η μη-μεταθετική ομάδα G, ώστε κάθε ένα από τα πρωτόκολλα που ακολουθούν στην Εργασία να καθίσταται ασφαλές είναι:

(O0) Η ομάδα πρέπει να είναι γνωστή (ή καλώς μελετημένη, ή αμφότερα).

(O1) Το πρόβλημα της λέξης πρέπει να έχει ταχύ (γραμμικής ή τετραγωνικής πολυπλοκότητας) αιτιοκρατικό αλγόριθμο επίλυσης.

- Πιο συγκεκριμένα να υπολογίζονται γρήγορα οι "κανονικές μορφές" των στοιχείων της ομάδας.

(O2) Θα πρέπει να υπάρχει ένας αποτελεσματικός τρόπος σύγχησης των στοιχείων· έτσι θα είναι αδύνατη η ανάκτηση των $x, y \in G$ από το γινόμενό τους $xy \in G$.

[Πάλι αρκεί να υπολογίζονται γρήγορα οι "κανονικές μορφές" των στοιχείων.]

(O3) Το μέγεθος των στοιχείων της G θα πρέπει να μεγαλώνει με εκθετικό ρυθμό.

[δηλαδή το πλήθος των στοιχείων που απαιτούν n στοιχεία της G ώστε να γραφούν, να μεγαλώνει εκθετικά σε σχέση με το n].

Παρατήρηση 1.1. *Παρακάτω σε όποιο κρυπτογραφικό πρωτόκολλο προτείνεται μία ομάδα ως βάση του πρωτοκόλλου, η ομάδα αυτή ικανοποιεί τις συνθήκες **(O0)**–**(O3)**· ειδικότερα, οι ομάδες πλεξίδων (βλ. §1.3).*

1.2 ...στις Ελεύθερες Ομάδες

1.2.1 Ορισμοί

► Θεωρείται ένα τυχόν σύνολο $X \neq \varnothing$.

Εδώ η φύση των συμβόλων που περιέχει το εν λόγω σύνολο είναι αδιάφορη. Η **κενή ακολουθία** –ήτοι η ακολουθία που δεν περιέχει κανένα σύμβολο– θα συμβολίζεται ως ε.

Ορισμός 1.2. Το **άστρο του Kleene του** X –συμβολίζεται ως $X^\star$– ορίζεται ως

$$X^\star := \bigcup_{n\in\mathbb{N}_0} V_n$$

όπου

$$V_0 := \{\varepsilon\}, \quad V_1 := X, \quad \ldots, \quad V_{n+1} := \big\{(w,x) \in X^n \times X : w \in X_n \wedge x \in X\big\}, \quad \ldots,$$

δηλαδή είναι το σύνολο των πεπερασμένου μήκους συμβολοσειρών από στοιχεία του X.

Συμβολισμός. *Έστω $n \in \mathbb{N}$ και x μία ακολουθία στοιχείων του X. Το γεγονός ότι η x έχει μήκος ακριβώς n, συμβολίζεται ως $x \in \{0,1\}^n$, εάν δε το μήκος της είναι το πολύ n, τότε θα συμβολίζεται ως $x \in \{0,1\}^{\leqslant n}$. Επιπλέον $X^* := \{f : \mathbb{N} \to X\}$.*

Στο σύνολο X αντιστοιχίζεται το σύνολο X^{-1} όπου $(\forall x \in X)(\exists! y \in X^{-1})[xy = \varepsilon = yx]$ (απόρροια της οποίας είναι πως $|X| = |X^{-1}|$.) Τα στοιχεία του συνόλου X^{-1} δεν είναι επ' ουδενί τυχαία. Σε κάθε στοιχείο $x \in X$ έχει αντιστοιχιθεί ένα και μοναδικό στοιχείο $y \in X^{-1}$ το οποίο διαδραματίζει το ρόλο του αντιστρόφου (όπως στις ομάδες) και γι αυτό το λόγο –εφεξής– θα συμβολίζεται ως x^{-1}.

► Θα συμβολίζεται $S_X := (X \cup X^{-1})^\star$.

Ορισμός 1.3. Λέξη καλείται κάθε στοιχείο του συνόλου S_X. **Υπολέξη** της $w \in S_X$ καλείται κάθε υπακολουθία της w.

Για λόγους πρακτικότητας οι λέξεις θα πάψουν να συμβολίζονται με τον κλασσικό συμβολισμό των ακολουθιών (ή των διατεταγμένων ζευγών αν προτιμάτε) και εφεξής θα παραλείπονται οι παρενθέσεις και τα κόμματα. Έτσι μια λέξη θα γράφεται με απλή παράθεση των συμβόλων της, το ένα πλάι στ' άλλο.

Στο S_X ορίζεται η σχέση ισοδύναμίας $\sim \in \mathcal{P}(S_X \times S_X)$ ως ακολούθως:

$$w_1 \sim w_2 \iff \left\{\begin{array}{c}\text{υπάρχει ακολουθία λέξεων } w_1 = u_1, u_2, \ldots u_\tau = w_2 \text{ τέτοια ώστε}\\ \text{κάθε } u_i \ (2 \leqslant i \leqslant \tau) \text{ να λαμβάνεται από το } u_{i-1} \text{ με διαγραφή ή}\\ \text{παρεμβολή μιας λέξης της μορφής } xx^{-1} \text{ ή } x^{-1}x, \text{ για κάποιο } x \in X\end{array}\right] \tag{1.1}$$

Ορισμός 1.4. Ανηγμένη λέξη καλείται κάθε λέξη που *δεν* περιέχει εμφανίσεις της ε, ή υπολέξεις της μορφής xx^{-1}, ή της μορφής $x^{-1}x$, για κάθε $x \in X$.

Συνεπώς, (κατά φυσιολογικό τρόπο) το σύνολο $X \neq \varnothing$ καλείται **αλφάβητο**.

Ορισμός 1.5. Η **ελεύθερη ομάδα** F_X **που παράγεται από το σύνολο** X ορίζεται ως $F_X := S_X/_\sim$, ήτοι το σύνολο όλων των κλάσεων ισοδυναμίας της σχέσης $\sim \in \mathcal{P}(S_X \times S_X)$.

Ο όρος *ομάδα* εμπεριέχει και

- μία πράξη: Στην εν λόγῳ περίπτωση είναι η (εποφαινόμενη)
$$[w_1][w_2] = [w_1 w_2] \qquad (w_1, w_2 \in S_X)$$
- ένα μοναδικό ουδέτερο στοιχείο: Η κενή ακολουθία ε έχει το ρόλο αυτόν.
- μοναδικό αντίστροφο για κάθε στοιχείο: Εάν $w = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \cdots x_{i_\rho}^{\delta_\rho}$, τότε
$$[w]^{-1} = \left[x_{i_\rho}^{-\delta_\rho} \cdots x_{i_2}^{-\delta_2} x_{i_1}^{-\delta_1}\right]$$

1.2.2 Ελεύθερα γινόμενα

► Θεωρείται G_α, $\alpha \in J$, μια οικογένεια ομάδων (με το J είναι ένα σύνολο δεικτών).

Μια **λέξη μήκους** $n \in \mathbb{N}$ στο **αλφάβητο** $\bigsqcup_{\alpha\in J} G_\alpha$ (ξένη ένωση των ομάδων) είναι μια πεπερασμένη ακολουθία $(g_1, g_2, \ldots, g_n) \in G_{\alpha_1} \times \cdots \times G_{\alpha_n}$, με $\alpha_1, \ldots, \alpha_n \in J$. Μία στοιχειώδης αναγωγή σε μια λέξη $(g_1, \ldots, g_n) \in G_{\alpha_1} \times \cdots \times G_{\alpha_n}$, $\alpha_1, \ldots, \alpha_n \in J$, καλείται μία από τις κάτωθι "δράσεις":

$$(g_1, \ldots, g_i, g_{i+1}, \ldots, g_n) \longmapsto (g_1, \ldots, g_i \cdot g_{i+1}, \ldots, g_n) \qquad (\text{εάν } \alpha_i = \alpha_{i+1})$$

και

$$(g_1, \ldots, g_{i-1}, 1_{G_{\alpha_i}}, g_{i+1}, \ldots, g_n) \longmapsto (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$$

Μια λέξη θα καλείται **ανηγμένη** εάν δεν μπορεί να εφαρμοσθεί καμμία στοιχειώδης αναγωγή.

Έστω W να είναι το σύνολο όλων των ανηγμένων λέξεων στο αλφάβητο $\bigsqcup_{\alpha\in J} G_\alpha$ και $\mathcal{P}(W)$ να είναι η ομάδα μεταθέσεων W. Για κάθε $\alpha \in J$ και $g \in G_\alpha$ ορίζεται η μετάθεση $\mathcal{L}_g^\alpha \in \mathcal{P}(W)$ ως ακολούθως:

$$\mathcal{L}_g^\alpha(\varnothing) := (g)$$

$$\mathcal{L}_g^\alpha(g_1, \ldots, g_n) := \begin{cases} (g_1, \ldots, g_n), & \text{εάν } g = 1_\alpha \\ (g, g_1, \ldots, g_n), & \text{εάν } g \neq 1_\alpha \wedge \alpha \neq \alpha_1 \\ (gg_1, \ldots, g_n), & \text{εάν } g \neq 1_\alpha \wedge \alpha = \alpha_1 \wedge gg_1 \neq 1_\alpha \\ (g_2, \ldots, g_n), & \text{εάν } g \neq 1_\alpha \wedge \alpha = \alpha_! \wedge gg_1 = 1_\alpha \end{cases}$$

Λήμμα 1.6. *Η απεικόνιση* $i_\alpha : G_\alpha \longrightarrow \mathcal{P}(W)$, *με* $i_\alpha(g) := \mathcal{L}^\alpha_g(g)$, *είναι μονομορφισμός.*

Απόδειξη. Έστω $\alpha \in J$.

$[\![H\, i_\alpha : G_\alpha \to \mathcal{P}(W)$ *είναι ομομορφισμός*$]\!]$: Πράγματι, διακρίνοντας κάθε μία από τις περιπτώσεις του ορισμού της μεταθέσεως $\mathcal{L}^\alpha_g$ έπεται πως

$$(\forall g, h \in G_\alpha)\left[\mathcal{L}^\alpha_{gh} = \mathcal{L}^\alpha_g \circ \mathcal{L}^\alpha_h\right]$$

το οποίο είναι το ζητούμενο.

$[\![H\, i_\alpha : G_\alpha \to \mathcal{P}(W)$ *είναι 1-1*$]\!]$: Έστω $g \in G_\alpha \setminus \{1_\alpha\}$, τότε $i_\alpha(g)(\varnothing) = \mathcal{L}^\alpha_g(\varnothing) = (g)$. Συνεπώς, $\mathcal{L}^\alpha_g \neq \mathrm{id}_W$ κι άρα η $i_\alpha : G_\alpha \to \mathcal{P}(W)$ είναι 1-1. □

Συμβολισμός. Έστω μια ομάδα G και $S \subseteq G$. Ως $\mathrm{gp}(S)$ θα συμβολίζεται η υποομάδα που παράγεται από το S, δηλαδή η μικρότερη δυνατή ομάδα που περιέχει το *σύνολο* S.

Ορισμός 1.7. Το **ελεύθερο γινόμενο** των ομάδων G_α, $\alpha \in J$, είναι η υποομάδα της $\mathcal{P}(W)$ που παράγεται από τις υποομάδες $i_\alpha(G_\alpha)$, $\alpha \in J$, και συμβολίζεται με $*_{\alpha\in J} G_\alpha$, δηλαδή

$$\underset{\alpha\in J}{*} G_\alpha =_{o\rho} \mathrm{gp}\left(\left\{i_\alpha(G_\alpha) : \alpha \in J\right\}\right) \leqslant \mathcal{P}(W)$$

Οι ομάδες $\{G_\alpha : \alpha \in J\}$ καλούνται (**ελεύθεροι**) **παράγοντες** του ελευθέρου γινομένου.

Μερικές (βασικές) ιδιότητες του ελεύθερου γινομένου είναι οι ακόλουθες:

Λήμμα 1.8. *Έστω* $\{G_\alpha\}_{\alpha\in J}$ *μια συλλογή ομάδων. Η ανηγμένη μορφή κάθε στοιχείου* $g \in *_{\alpha\in J} G_\alpha$ *είναι μοναδική.*

Απόδειξη. Αφού (εξ ορισμού) $*_{\alpha\in J} G_\alpha = \mathrm{gp}\left(\left\{i_\alpha(G_\alpha) : \alpha \in J\right\}\right)$, κάθε $g \in *_{\alpha\in J} G_\alpha$ γράφεται ως γινόμενο στοιχείων των $i_\alpha(G_\alpha)$, $\alpha \in J$. Έστω

$$i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_k}(g_k) = g = i_{\beta_1}(h_1)i_{\beta_2}(h_2)\cdots i_{\beta_m}(h_m)$$

δύο ανηγμένες μορφές του $1 \neq g \in *_{\alpha\in J} G_\alpha$, τότε

$$\begin{aligned} g(\varnothing) &= i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_k}(g_k)(\varnothing) \\ &= (\mathcal{L}^{\alpha_1}_{g_1} \circ \mathcal{L}^{\alpha_2}_{g_2} \circ \cdots \circ \mathcal{L}^{\alpha_k}_{g_k})(\varnothing) \\ &= (g_1, g_2, \ldots, g_k) \end{aligned} \qquad \begin{aligned} g(\varnothing) &= i_{\beta_1}(h_1)i_{\beta_2}(h_2)\cdots i_{\beta_m}(h_m)(\varnothing) \\ &= (\mathcal{L}^{\beta_1}_{h_1} \circ \mathcal{L}^{\beta_2}_{h_2} \circ \cdots \circ \mathcal{L}^{\beta_m}_{h_m})(\varnothing) \\ &= (h_1, h_2, \ldots, h_m) \end{aligned}$$

Έπεται ότι $k = m$ και $(\forall i = 1, 2, \ldots, k)[\alpha_i = \beta_i \wedge g_i = h_i]$. □

Λήμμα 1.9. *Έστω* $\{G_\alpha\}_{\alpha\in J}$ *μια συλλογή ομάδων. Αν το στοιχείο*

$$\underset{\alpha\in J}{*} G_\alpha \ni g = i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_k}(g_k), \qquad \mu\varepsilon\ k \in \mathbb{N}$$

είναι σε ανηγμένη μορφή, τότε $g \neq 1$.

Απόδειξη. Πράγματι, $g(\varnothing) = (g_1, g_2, \ldots, g_m) \in W$ κι άρα $g \neq 1 = \mathrm{id}_W$. □

Λήμμα 1.10. *Η απεικόνιση* $\phi : *_{\alpha\in J} G_\alpha \longrightarrow W$, *με*

$$\phi(g) = \begin{cases} (g_1, g_2, \ldots, g_k), & \text{εάν } g \neq 1 \text{ και } g = i_{\alpha_1}(g_1)\cdots i_{\alpha_k}(g_k) \\ & \text{είναι η ανηγμένη μορφή του } g \\ \varnothing, & \text{εάν } g = 1 \end{cases}$$

είναι 1-1 και επί. Έτσι είναι δυνατόν αντί των στοιχείων του ελευθέρου γινομένου $*_{\alpha\in J} G_\alpha$, *να γίνεται λόγος για ανηγμένες λέξεις στο* $\bigsqcup_{\alpha\in J} G_\alpha$.

Ορισμός 1.11. Έστω ένα σύνολο $X \neq \varnothing$. Για κάθε $\alpha \in X$ θεωρείται η άπειρη κυκλική ομάδα $\langle\alpha\rangle := \{\alpha^i : i \in \mathbb{Z}\}$ που παράγεται από το α. Η **ελεύθερη ομάδα επί του** X είναι το ελεύθερο γινόμενο των ομάδων $\langle\alpha\rangle$, $\alpha \in X$, και συμβολίζεται με $F(X)$, ήτοι

$$F(X) =_{o\rho} \mathop{*}_{\alpha\in X} \langle\alpha\rangle$$

Ορίζεται, επίσης, $F(\varnothing) := \{1\}$. Το σύνολο X καλείται **βάση** της $F(X)$ και ο πληθάριθμος $|X|$ **διάσταση** της $F(X)$.

Το ακόλουθο αποτέλεσμα δίδει τη μορφή των στοιχείων της ελευθέρας ομάδος.

Πρόταση 1.12. Έστω μια ομάδα G και $X \subseteq G$. Τα ακόλουθα είναι ισοδύναμα:

1. Η G είναι ελεύθερη ομάδα με βάση το X [σύμφωνα με τον Ορισμό 1.11].
2. Κάθε $g \in G \setminus \{1\}$ μπορεί να γραφεί κατά μοναδικό τρόπο ως

   $$g = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \cdots x_{i_k}^{\delta_k}$$

   με $k \in \mathbb{N}$, $(\forall \sigma = 1, \ldots, k)\left[1 \neq x_{i_\sigma} \in X \wedge \delta_\sigma \in \mathbb{Z}_+\right]$ & $(\forall \sigma = 1, \ldots, k-1)[x_{i_\sigma} \neq x_{i_{\sigma+1}}]$.
3. Η G παράγεται από το σύνολο X και το 1_G δεν μπορεί να γραφεί ως $x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \cdots x_{i_k}^{\delta_k}$, για $k \in \mathbb{N}$, $(\forall \sigma = 1, \ldots, k)[1 \neq x_{i_\sigma} \in X \wedge \delta_\sigma \in \mathbb{Z}_+^*]$ και $(\forall \sigma = 1, \ldots, k-1)[x_{i_\sigma} \neq x_{\sigma+1}]$.

Απόδειξη. Η απόδειξη απορρέει από τα Λήμματα 1.8, 1.9 και 1.10. □

Συμβολισμός. Έστω ένα σύνολο X. Ορίζεται η συνάρτηση $\partial : X \times F(X) \to \mathbb{N}_0$ ως εξής:

$$\partial_a(w) \equiv \partial(a, w) := \begin{cases} 0, & \text{εάν } w = \varepsilon \\ \delta + \partial_a(w'), & \text{εάν } w = a^\delta w', \text{ για } \delta \in \mathbb{Z} \text{ και } w' \in F(X) \\ \partial_a(w'), & \text{εάν } w = b^\delta w', \text{ για } \delta \in \mathbb{Z},\ w' \in F(X) \text{ και } b \neq a \end{cases}$$

Κατ' επέκτασην ορίζεται $\partial_{a,b}(w) := \partial_a(w) + \partial_b(w)$ και ούτο καθ' εξής.... Επίσης, ορίζεται $|\cdot| : F(X) \longrightarrow \mathbb{N}_0$, με $|w| := \sum_{\alpha\in X} \partial_\alpha(w) < +\infty$.

Τέλος, ένα σημαντικό αποτέλεσμα είναι το εξής:

Θεώρημα 1.13 (Κανονική συνθήκη)**.** Έστω ένα σύνολο X και $F(X)$ η ελεύθερη ομάδα επί του X. Για κάθε ομάδα H και κάθε απεικόνιση $\phi : X \to H$ υπάρχει μοναδικός ομομορφισμός $\Phi : F(X) \to H$ που επεκτείνει την ϕ.

Απόρροια του παραπάνω αποτελέσματος είναι η ακόλουθη

Πρόταση 1.14. Η διάσταση μιας ελεύθερης ομάδας είναι καλώς ορισμένη, ήτοι δύο ελεύθερες ομάδες είναι ισόμορφες εάν και μόνον εάν οι διαστάσεις τους συμφωνούν.

1.2.3 Παραστάσεις ομάδων

Ορισμός 1.15. Μια ομάδα G έχει **παράσταση** την $\langle X \mid R \rangle$, όπου $R \subseteq F(X)$, εάν

$$G = F(X) \Big/ \mathrm{gp}\left(\left\{wrw^{-1} \in F(X) : w \in F(X) \wedge r \in R^{\pm 1}\right\}\right)$$

Το X καλείται **σύνολο γεννητόρων** της G και το R καλείται **σύνολο σχέσεων** και τα στοιχεία του **συσχετιστές**.

Συμβολισμός. Δεδομένης μιας ομάδας G, θα γίνεται αναφορά στο σύνολο των γεννητόρων της με τον συμβολισμό $\mathscr{X}(G)$, ενώ στο σύνολο σχέσεών της με τον συμβολισμό $\mathscr{R}(G)$.

Αντίστροφα, έστω ένα σύνολο $X \neq \varnothing$. Θεωρείται η ελεύθερη ομάδα $F(X)$ επί του X και για $R \subseteq F(X)$ ορίζεται

$$\langle X \mid R \rangle =_{\mathrm{op}} F(X) \Big/ \mathrm{gp}\left(\left\{wrw^{-1} \in F(X) : w \in F(X) \wedge r \in R^{\pm 1}\right\}\right)$$

Ορισμός 1.16. Η $G = \langle X \mid R \rangle$ καλείται **πεπερασμένα παραγόμενη** εάν $|X| < +\infty$, ενώ καλείται **πεπερασμένα παριστάμενη** εάν $|X|, |R| < +\infty$.

Δύο σημαντικά αποτελέσματα –οι αποδείξεις των οποίων στηρίζονται στο ανάλογο του Θεωρήματος 1.13 για τις ελεύθερες ομάδες– είναι τα εξής:

Πρόταση 1.17. Κάθε ομάδα G έχει μια παράσταση.

Θεώρημα 1.18 (von Duck)**.** Έστω $G = \langle X \mid R \rangle$ και H μια άλλη ομάδα. Κάθε απεικόνιση $\phi : X \to H$, με $(\forall r \in R)[\phi(r) = 1_G]$, μπορεί να επεκταθεί σε ομομορφισμό $\overline{\phi} : G \to H$.

Παράδειγμα 1.19. Έστω $n \in \mathbb{N}$.

1. $\mathbb{Z}_n = \langle x \mid x^n = 1 \rangle = \mathbb{Z}/n\mathbb{Z}$.
2. Εάν $G_1 = \langle X_1 \mid R_1 \rangle$ και $G_2 = \langle X_2 \mid R_2 \rangle$, τότε $G_1 * G_2 = \langle X_1 \sqcup X_2 \mid R_1 \sqcup R_2 \rangle$.

. . . και με χρήση του Θεωρήματος 1.18 (von Duck) προκύπτουν τα ακόλουθα:

3. $D_n = \langle \rho, \varepsilon \mid \rho^n = \varepsilon^2 = \varepsilon\rho\varepsilon^{-1}\rho = 1 \rangle$.
4. $\mathbb{Z}^n = \langle x_1, x_2, \ldots, x_n \mid (\forall i, j = 1, 2, \ldots, n)[x_i x_j = x_j x_i] \rangle$.
5. $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle \alpha, \beta \mid \alpha^2 = \beta^2 = \alpha\beta\alpha^{-1}\beta^{-1} = 1 \rangle$. ⊣

1.3 . . . στις Ομάδες Πλεξίδων

Οι ομάδες πλεξίδων (braid groups) εισήχθησαν από τον Artin.

1.3.1 Παραστάσεις των Ομάδων Πλεξίδων

1.3.1.Α΄ Η παράσταση του Artin

Ορισμός 1.20 (Artin, [Ar47])**.** Για $n \in \mathbb{N} \setminus \{1\}$, η **ομάδα n-πλεξίδων** ορίζεται ως

$$B_n := \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & |i-j| \geqslant 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & i = 1, 2, \ldots, n-2 \end{array} \right\rangle$$

Η ως άνω παράσταση καλείται **παράσταση του Artin** και οι γεννήτορές της **γεννήτορες του Artin**.

Ένα στοιχείο της B_n θα καλείται **n-πλεξίδα**. Η ταυτοτική συνάρτηση στο $\{\sigma_1, \ldots, \sigma_{n-1}\}$ εμβαπτίζει την B_n στην B_{n+1}, άρα μία n-πλεξίδα, μπορεί να θεωρηθεί ως $(n+1)$-πλεξίδα. Κατ' επέκτασην ορίζεται και το όριο B_∞.

Ισχύει ότι $B_2 \simeq \mathbb{Z}$ (όντας η B_2 κυκλική και άπειρη) και για $n \geqslant 3$ η B_n δεν είναι αντιμεταθετική και $\mathcal{Z}(B_n) \simeq \mathbb{Z}$.

1.3.1.Β΄ Οπτικοποίηση

Μία n-πλεξίδα λαμβάνεται τοποθετώντας παράλληλα n κομμάτια σχοινιού πεπερασμένου μήκους και καθώς εκτείνονται θα τέμνονται (:περνώντας το ένα πάνω από το άλλο, ή το ένα κάτω από το άλλο) δίχως να αλλάζει η κατεύθυνσή τους. Εδώ τα σχοινιά θα τοποθετούνται οριζόντια και η αρίθμηση θα αρχίζει από το υψηλότερο.

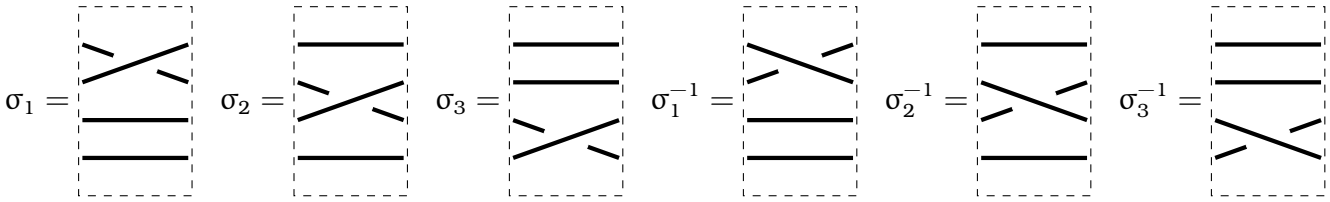
Έστω οι πλεξίδες $\alpha, \nu \in B_n$.

⟦*Το γινόμενο* $\alpha\nu$ *υπολογίζεται*⟧ ενώνοντας το τέλος του i-οστού σχοινιού της α με την αρχή του i-στού σχοινιού της ν, για κάθε $i = 1, 2, \ldots, n$.

⟦*Το ταυτοτικό στοιχείο* ε⟧ ορίζεται ως η πλεξίδα της οποίας κανένα σχοινί της δεν τέμνεται με κάποιο άλλο.

⟦*Το αντίστροφο* α^{-1} *υπολογίζεται*⟧ περνώντας από κάτω κάθε σχοινί που περνάει από πάνω στην α και τ' ανάστροφο.

Σχηματικά για την B_4 η εικόνα είναι:



Σχήμα 1.1: Οι Artin γεννήτορες της B_4 και τ' αντίστροφά τους

Πλέον, από τα σχήματα, είναι προφανές ότι για κάθε $i, j = 1, 2, \ldots, n-1$:

- εάν $|i-j| > 1$, τότε $\sigma_i\sigma_j = \sigma_j\sigma_1$ και

  [Η πλεξίδα σ_i δεν επηρεάζει τα σχοινιά της σ_{i+1}, ούτε επίσης και η σ_{i+1} της σ_i.]

- εάν $i \leqslant n-2$, τότε $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$.

Μία τομή δύο σχοινιών σε μια πλεξίδα καλείται **θετική** εάν το σχοινί που βρίσκεται από επάνω έχει θετική κλίση, ειδάλλως καλείται **αρνητική**. Εμβαπτίζοντας τις πλεξίδες στον $\mathbb{R}^3$ ανακύπτει το

Πρόβλημα της ισοτοπίας των πλεξίδων. Δεδομένων των πλεξίδων $\alpha, \nu \in B_n$ είναι δυνατόν να μετακινηθούν τα σχοινιά της πλεξίδας α (δίχως να αλλάξουν τα τελικά τους σημεία, ούτε να να μετακινηθούν διασταυρώνοντας το ένα με το άλλο) ώστε να προκύψει η πλεξίδα ν;

το οποίο ουσιαστικά αποτελεί το πρόβλημα της λέξης για την ομάδα B_n.

1.3.1.Γ΄ Η παράσταση των Birman-Ko-Lee

Η διαφορά των γεννητόρων στην παράσταση των Birman-Ko-Lee [BKL98] με εκείνους στην παράσταση του Artin είναι πως περιέχουν αυθαίρετες δισταυρώσεις (i, j) αντί των διαστραυρώσεων $(i, i+1)$ των γεννητόρων του Artin.

Πρόταση 1.21 (Birman-Ko-Lee, [BKL98])**.** Έστω $n \in \mathbb{N}$, και $t, s \in \mathbb{N}$, με $1 \leqslant s < t \leqslant n$, τότε ορίζεται

$$a_{ts} := (\sigma_{t-1}\sigma_{t-2}\cdots\sigma_{s+1})\sigma_s(\sigma_{s+1}^{-1}\cdots\sigma_{t-2}^{-1}\sigma_{t-1}^{-1}) \in B_n$$

[Διαισθητικά, η $a_{ts} \in B_n$ είναι η πλεξίδα όπου τα νήματα t και s έχουν εναλλαχθεί ώστε να περνούν υπεράνω όλων των νημάτων $t+1$ έως $s-1$.] τότε

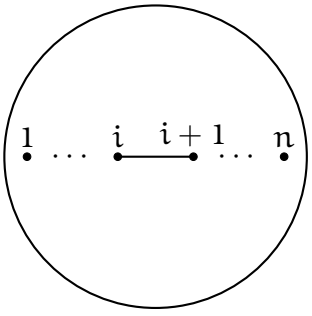
$$B_n = \left\langle \{a_{ts} \in B_n : 1 \leqslant s < t \leqslant n\} \;\middle|\; \begin{array}{c} (\forall q, r, s, t = 1, \ldots, n)\big[([s,t] \cap [q,r] = \varnothing) \implies a_{ts}a_{rq} = a_{rq}a_{ts}\big] \\ (\forall r, s, t = 1, \ldots, n)[r < s < t \implies a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr}] \end{array} \right\rangle$$

1.3.1.Δ΄ Η διαφορά των δύο παραστάσεων

Παρατήρηση 1.22. *Κατ΄ αρχάς ισχύει ότι* $a_{t+1,t} = \sigma_t$*, για κάθε* $t = 1, \ldots, n-1$.

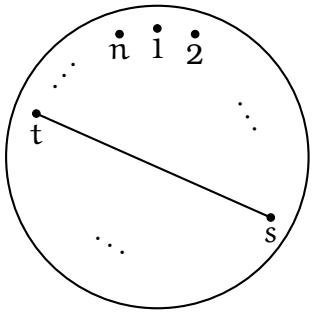
Η διαφοροποίηση των δύο παραστάσεων μπορεί να οπτικοποιηθεί ως ακολούθως: Θεωρείται ο $D_n \subseteq \mathbb{C}^2$, ήτοι ο κλειστός δίσκος κέντρου 0, με n σταθερά και διακριτά σημεία.

Στην παράσταση του Artin τα σημεία τοποθετούνται στην ευθεία των πραγματικών αριθμών συμμετρικά ως προς το κέντρο των αξόνων. Ο γεννήτορας $\sigma_i \in B_n$ συνδέει το σημείο i με το σημείο $i+1$ κατά μήκος της πραγματικής γραμμής.



Σχήμα 1.2: Ο Artin γεννήτορας $\sigma_i \in B_n$, για $1 \leqslant i \leqslant n-1$

Στην παράσταση των Birman-Ko-Lee τα σημεία σχηματίζουν ένα n-γωνο. Ο γεννήτορας $a_{ts} \in B_n$ συνδέει τα σημεία t και s μέσῳ της αντίστοιχης χορδής του n-γώνου.



Σχήμα 1.3: Ο Birman-Ko-Lee γεννήτορας $a_{ts} \in B_n$, για $1 \leqslant s < t \leqslant n$

1.3.2 Κανονικές μορφές των πλεξίδων

1.3.2.Α΄ Η κανονική μορφή του Garside

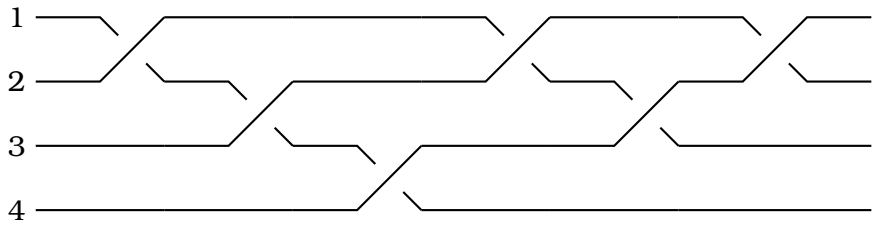
Η κανονική μορφή του Garside εισηγήθηκε από τον ίδιον τον F. Garside στην εργασία του [Ga69]· άλλες παραλλαγές της εμπεριέχονται στις [Ad84, Del72, EM94, ECHLPT92, Th88].

Μία πλεξίδα καλείται **θετική** εάν μπορεί να γραφεί ως γινόμενο γεννητόρων του Artin με θετικές δυνάμεις. Το σύνολο των θετικών n-πλεξίδων συμβολίζεται ως B_n^+ και εφοδιασμένο με την συγκόλληση πλεξίδων συνιστά ένα μονοειδές [βλ. Ορισμό 2.2].

Η **θεμελιώδης n-πλεξίδα** ορίζεται ως η πλεξίδα

$$\Delta_n := (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1\sigma_2)\sigma_1 \in B_n$$

Γεωμετρικά η μορφή της θεμελιώδους πλεξίδας θα είναι κάπως έτσι:



Σχήμα 1.4: Η θεμελιώδης πλεξίδα $\Delta_4 = (\sigma_1\sigma_2\sigma_3)(\sigma_1\sigma_2)\sigma_1$

Πρόταση 1.23 (Ιδιότητες Δ_n)**.** Για κάθε $n \in \mathbb{N}$ ισχύουν τα επόμενα:

1. $(\forall i = 1, \ldots, n-1)(\exists A, B \in B_n^+)[\Delta_n = \sigma_i A = B\sigma_i]$.
2. $(\forall i = 1, \ldots, n-1)[\Delta_n^{-1}\sigma_i\Delta_n = \sigma_{n-i}]$.
3. $\mathcal{Z}(B_n) = \mathrm{gp}\,(\Delta_n^2)$.

Θεωρείται μια μερική διάταξη στις n-πλεξίδες ως ακολούθως:

$$A \preceq B \iff_{o\rho} (\exists C \in B_n^+)[B = AC]$$

ήτοι η πλεξίδα $A \in B_n$ είναι αρχικό τμήμα της $B \in B_n$.

Πρόταση 1.24 (Ιδιότητες $\preceq$)**.** Για κάθε $n \in \mathbb{N}$ ισχύουν τα κάτωθι:

1. $(\forall B \in B_n)[B \in B_n^+ \iff \varepsilon \preceq B]$.
2. $(\forall A, B \in B_n)[A \preceq B \iff B^{-1} \preceq A^{-1}]$.

Μία $P \in B_n$ λέγεται **πλεξίδα μετάθεσης** (ή **απλή πλεξίδα**) εάν $\varepsilon \preceq P \preceq \Delta_n$· η ονομασία οφείλεται στον επιμορφισμό $B_n \longrightarrow S_n$, όπου για $\pi \in S_n$, ο $\pi(i) \in \{1, \ldots, n\}$ συμβολίζει τη θέση που κατέχει στην αρχή της πλεξίδας το σχοινί που στο τέλος της πλεξίδα βρίσκεται στην i-οστή θέση. Συνεπώς, υπάρχουν $n!$ διακεκριμένες απλές πλεξίδες. Γεωμετρικά, μία n-πλεξίδα μετάθεσης είναι μία n-πλεξίδα της οποίας κάθε δύο σχοινία της τέμνονται θετικά *τουλάχιστον* μία φορά.

Δεδομένης μιας πλεξίδας μετάθεσης $P \in B_n$, ορίζεται το **αρχικό σύνολο** $S(P)$ και το **τελικό σύνολο** $F(P)$ ως ακόλουθα:

$$S(P) := \left\{ i \in \{1, \ldots, n-1\} : (\exists Q \in B_n^+)[P = \sigma_i Q] \right\}$$
$$F(P) := \left\{ i \in \{1, \ldots, n-1\} : (\exists Q \in B_n^+)[P = Q\sigma_i] \right\}$$

Επί παραδείγματι, $S(\Delta_n) = F(\Delta_n) = \{1, \ldots, n-1\}$.

Η ακολουθία $\{P_i\}_{i=1}^k$ είναι μία **αριστερά βαρύνουσα ανάλυση** μιας θετικής πλεξίδας $A \in B_n^+$ εάν

1. $A = P_1 P_2 \cdots P_k$.
2. Οι $P_1, \ldots, P_k$ είναι πλεξίδες μετάθεσης.
3. $S(P_{i+1}) \subset F(P_i)$, $i = 1, \ldots, k-1$, ήτοι οποιαδήποτε προσθήκη ενός γεννήτορα από την P_{i+1} στην P_i, θα μετέτρεπε την P_i σε πλεξίδα που δεν είναι πλεξίδα μετάθεσης.

Οι πλεξίδες μετάθεσης που αντιστοιχούν στην ταυτοτική μετάθεση καλούνται **γνήσιες**, το σύνολο των οποίων συμβολίζεται ως PB_n.

Συνεπώς, προκύπτει η εξής βραχεία ακριβής ακολουθία: $1 \to PB_n \rightarrowtail B_n \twoheadrightarrow S_n \to 1$.

Θεώρημα 1.25 (Κανονική μορφή Garside)**.** Για κάθε $w \in B_n$, υπάρχει μοναδική έκφραση

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

όπου το $r \in \mathbb{Z}$ είναι μεγιστικό, οι $P_1, \ldots, P_k$ είναι πλεξίδες μεταθέσεων και ιδιαιτέρως $P_k \neq \varepsilon$ και η $P_1 P_2 \cdots P_k$ είναι μία αριστερά βαρύνουσα ανάλυση.

Η μεθοδολογία ώστε μια $w \in B_n$ να περιέλεθει σε κανονική μορφή Garside είναι η κάτωθι:

(1) Κάθε εμφάνιση του σ_i^{-1}, $i = 1, \ldots, n-1$, στην w αντικαθίσταται από την $\Delta_n^{-1} B_i$, όπου η B_i είναι μια πλεξίδα μετάθεσης.

(2) Κάθε εμφάνιση της Δ_n μετακινείται στην αρχή με χρήση της Πρότασης 1.23-2.. Επομένως, $w = \Delta_n^{r'} A$, όπου $A \in B_n^+$.

(3) Γραφή της $A \in B_n$ σε αριστερά βαρύνουσα ανάλυση:
1: $A = Q_1 Q_2 \cdots Q_j$, όπου οι $Q_1, Q_2, \ldots, Q_j$ είναι πλεξίδες μετάθεσης;
2: **επανάλαβε**
3: $i \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{s \in \{1, \ldots, j\} : S(Q_{s+1}) \not\subseteq F(Q_s)\}$;
4: $k \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{k \in S(Q_{i+1}) \setminus F(Q_i)\}$;
5: Με χρήση των $\mathscr{R}(B_n)$ μεταφορά του σ_k από την Q_{i+1} στην Q_i;
6: $A = Q_1 Q_2 \cdots Q_i' Q_{i+1}' \cdots Q_j$;
7: **έως ότου** $((\forall p = 1, \ldots, j-1)[S(Q_{p+1}) \subseteq F(Q_p)])$

Παράδειγμα 1.26. Έστω η $w = \sigma_1 \sigma_3^{-1} \sigma_2 \in B_4$.

(1) Αντικατάσταση του σ_3^{-1} με $\Delta_4^{-1} \sigma_3 \sigma_2 \sigma_1 \sigma_3 \sigma_2$, οπότε $w = \sigma_1 \cdot \Delta_4^{-1} \sigma_3 \sigma_2 \sigma_1 \sigma_3 \sigma_2 \cdot \sigma_2$.

(2) Μετακίνηση στα αριστερά της Δ_4 [Πρόταση 1.23-2.], άρα $w = \Delta_4^{-1} \cdot \sigma_3 \sigma_3 \sigma_2 \sigma_1 \sigma_3 \sigma_2 \sigma_2$.

(3) Ανάλυση του θετικού μέρους σε αριστερά βαρύνουσα ανάλυση, οπότε προκύπτει ότι $w = \Delta_4^{-1} \cdot \sigma_2 \sigma_1 \sigma_3 \sigma_2 \sigma_1 \cdot \sigma_1 \sigma_2$. ⊣

Θεώρημα 1.27 ([ECHLPT92, §9.5])**.** Δεδομένης της Artin παράστασης, υπάρχει αιτιοκρατικός αλγόριθμος που για κάθε $w \in B_n$ υπολογίζει την Garside κανονική μορφή σε χρόνο $\mathcal{O}\big(|w|^2 n \log_2 n\big)$.

Παρόμοια, μπορεί κανείς να ορίσει και την *δεξιά βαρύνουσα ανάλυση*.

Ορισμός 1.28. Έστω $w \in B_n$, τότε ορίζονται

$$\inf(w) := \max\{r \in \mathbb{Z} : \Delta_n^r \preceq w\} \qquad \sup(w) := \min\{s \in \mathbb{Z} : w \preceq \Delta_n^s\}$$

και το **θεσμικό μήκος** $\operatorname{len}(w) := \sup(w) - \inf(w)$.

Εάν $w = \Delta_n^m P_1 P_2 \cdots P_k$ είναι η Garside κανονική μορφή της $w \in B_n$, τότε $\inf(w) = m$ και $\sup(w) = m + k$.

Ορισμός 1.29. Το **σύνολο κορυφής** (summit set) της $x \in B_n$ ορίζεται ως
$\mathrm{SS}(x) := \{w^{-1} x w \in B_n : w \in B_n \wedge \inf(w^{-1} x w)$ μεγιστικό$\}$
και το **σύνολο υπερ-κορυφής** (super summit set) της $x \in B_n$ ως
$\mathrm{SSS}(x) := \{w^{-1} x w \in B_n : w \in B_n \wedge \inf(w^{-1} x w)$ μεγιστικό $\wedge \sup(w^{-1} x w)$ ελαχιστικό$\}$

1.3.2.Β΄ Η κανονική μορφή των Birman-Ko-Lee

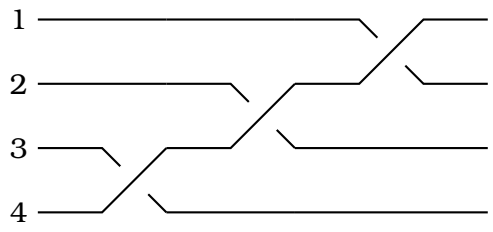
Οι J. Birman, K. Ko και S. Lee της προτείνουν μια κανονική μορφή βασιζόμενοι στην παράστασή τους.

Ορίζουν μια νέα θεμελιώδη πλεξίδα:

$$\delta_n = a_{n,n-1}a_{n-1,n-2}\cdots a_{2,1}$$

ή σε δεδομένα γεννητόρων Artin: $\delta_n = \sigma_{n-1}\sigma_{n-2}\cdots\sigma_1$.

Γεωμετρικά, η μορφή της νεοεισαχθήσης θεμελιώδους πλεξίδας θα είναι κάπως έτσι



Σχήμα 1.5: Η θεμελιώδης πλεξίδα $\delta_4 = a_{43}a_{32}a_{21} = \sigma_3\sigma_2\sigma_1$

Θεώρημα 1.30. Για κάθε $n \in \mathbb{N}$ ισχύουν τα ακόλουθα:

1. $\Delta_n^2 = \delta_n^n$.
2. Με τους ορισμούς προσαρμοσμένους στην Birman-Ko-Lee παράσταση, ισχύει η αντίστοιχη της Πρότασης 1.23:

   (α΄) $(\forall s,t \in \mathbb{N})(\exists A,B \in B_n^+)[1 \leqslant s < t \leqslant n \implies a_{ts}A = Ba_{ts}]$.

   (β΄) $(\forall s,t \in \mathbb{N})[1 \leqslant s < t < n \implies a_{ts}\delta_n = \delta_n a_{t+1,s+1}]$.

   (γ΄) $\mathcal{Z}(B_n) = \mathrm{gp}\,(\delta_n^n)$.

Παρόμοια με την Garside κανονική μορφή κάθε $w \in B_n$ έχει μοναδική γραφή ως

$$w = \delta_n^j A_1 A_2 \cdots A_k$$

όπου $A_1A_2\cdots A_k \in B_n^+$, το $j \in \mathbb{Z}$ μεγιστικό και το $k \in \mathbb{N}_0$ ελαχιστικό ως προς όλες τις γραφές, επίσης $A_1,\ldots,A_n \in B_n^+$ και καθορίζονται μοναδικά από τις αντίστοιχες μεταθέσεις τους (βλ. [BKL98, Λήμμα 3.1]).

Ορίζεται η σχέση μερικής διάταξης

$$v \sqsubseteq w \iff_{o\rho} (\exists a,b \in B_n^+)[w = avb]$$

Μία πλεξίδα $w \in B_n$ καλείται **θεσμικός παράγοντας**[*] (canonical factor) εάν $\varepsilon \sqsubseteq w \sqsubseteq \delta_n$. Υπάρχουν $C_n = \dfrac{(2n)!}{n!(n+1)!}$ (αριθμός Catalan) διακεκριμένοι θεσμικοί παράγοντες (βλ. [BKL98, Λήμμα 3.5]).

Παρατήρηση 1.31. *Όντας $C_n \ll n!$ μερικές φορές είναι υπολογιστικά ευκολότερο να εργάζεται κανείς με την Birman-Ko-Lee παράσταση.*

Η μεθοδολογία ώστε μία $w \in B_n$ να περιέλθει σε Birman-Ko-Lee κανονική μορφή είναι:

(α') Κάθε εμφάνιση a_{ts}^{-1}, με $1 \leqslant s < t \leqslant n$, αντικαθίσταται από $\delta_n^{-1} A \in B_n$, για $A \in B_n^+$.

(β') Μετακίνηση όλων των δ_n στα αριστερά της λέξης.

(γ') Μετατροπή της θετικής λέξης που προκύπτει σε αριστερά βαρύνουσα ανάλυση θεσμικών παραγόντων.

Θεώρημα 1.32. Θεωρώντας την Birman-Ko-Lee παράσταση, υπάρχει αιτιοκρατικός αλγόριθμος που βρίσκει την Birman-Ko-Lee κανονική μορφή κάθε $w \in B_n$ σε χρόνο $\mathcal{O}\big(|w|^2 n\big)$.

Παρατήρηση 1.33. *Οι έννοιες* $\inf(w), \sup(w), \mathrm{SS}(w), \mathrm{SSS}(w)$ *και* $\mathrm{len}(w)$, *για* $w \in B_n$, *ορίζονται και στην Birman-Ko-Lee παράσταση αντικαθιστώντας την μερική διάταξη $\preceq$ με την $\sqsubseteq$ και την Garside κανονική μορφή με την Birman-Ko-Lee κανονική μορφή.*

1.3.3 Η αναπαράσταση του Burau

Ορισμός 1.34. Έστω μια ομάδα $(G, *)$. Η απεικόνιση $\rho : G \longrightarrow GL(n, V)$ καλείται **αναπαράσταση** εάν ισχύει ότι $(\forall g, h \in G)[\rho(g*h) = \rho(g) \times \rho(h)]$, όπου ως $\times$ συμβολίζεται πολλαπλασιασμός πινάκων, για κάποιο $n \in \mathbb{N}$ και κάποιον διανυσματικό χώρο V.

Η αναπαράσταση του Burau απεικονίζει την ομάδα πλεξίδων B_n στην $GL(n-1, \mathbb{Z}\big[t^{\pm 1}\big])$ των $(n-1) \times (n-1)$ πινάκων με πολυώνυμα Laurent[†] με ακεραίους συντελεστές. Η απεικόνιση έχει ως εξής: Ο γεννήτορας $\sigma_i \in B_n$ απεικονίζεται στον $(n-1)\times(n-1)$ πίνακα που προκύπτει από τον ταυτοτικό πίνακα έχοντας αντικαταστήσει το στοιχείο $(i, i+1)$ με τον "υποπίνακα" $\left[\begin{smallmatrix} 1-t & t \\ 1 & 0 \end{smallmatrix}\right]$.

$$\rho_n : B_n \longrightarrow GL(n-1, \mathbb{Z}\big[t^{\pm 1}\big]), \qquad \sigma_i \overset{\rho_n}{\longmapsto} \left(\begin{array}{c|c|c} I_{i-1} & 0 & 0 \\ \hline 0 & \begin{smallmatrix} 1-t & t \\ 1 & 0 \end{smallmatrix} & 0 \\ \hline 0 & 0 & I_{n-i-1} \end{array}\right)$$

όπου $I_k \in GL(k, \mathbb{Z}\big[t^{\pm 1}\big])$ είναι ο ταυτοτικός $k \times k$ πίνακας, ενώ τα μηδενικά παραπάνω συμβολίζουν τον μηδενικό πίνακα (καταλλήλου μεγέθους κάθε φορά).

[*] Πρόκειται για την αντίστοιχη της έννοιας της απλής πλεξίδας στους γεννήτορες Artin.

[†] Έστω ένα σώμα $\mathbb{F}$. Τα πολυώνυμα Laurent μιας μεταβλητής X έχουν τη μορφή $\sum_{k \in \mathbb{Z}} p_k X^k$ και σχηματίζουν έναν δακτύλιο που συμβολίζεται ως $\mathbb{F}[X^{\pm 1}]$.

Μέρος Ι

Κρυπτοσυστήματα εμπνευσμένα από το πρόβλημα της λέξης

Ήδη από το 1911 ο Max Dehn -στην εργασία του [De11]- είχε γνωστοποιήσει πως κύριο μέρος της έρευνάς του [μαζί με δύο ακόμη προβλήματα: της συζυγίας (βλ. Μέρος II της Εργασίας) και του Ισομορφισμού (βλ. παρακάτω)] αποτελεί

Το πρόβλημα της λέξης (εκδοχή απόφασης). Δοθείσης μιας ομάδας $G = \langle X \mid R \rangle$ κι ενός $w \in G$, ισχύει ότι $w \sim_R \varepsilon$;

Προφανώς, το πρόβλημα έγκειται στην εύρεση ενός αλγορίθμου, ο οποίος αποφαίνεται του ερωτήματος σε κάποιο λογικό χρονικό πλαίσιο. Έναν αλγόριθμο απέδωσε ο ίδιος ο Max Dehn για τις ομάδες που ικανοποιούν τη συνθήκη μικρών ακυρώσεων $C'(1/6)$ (βλ. Ορισμό 4.19) στην εργασία του [De12].

Ο Pyotr Nobikov το 1955 -στην εργασία του [No55]- αποφάνθηκε πως εν γένει δεν υπάρχει αλγόριθμος που να αποφαίνεται το πρόβλημα της λέξης στην πεπερασμένα παριστάμενη ομάδα G. Μία ακόμη απόδειξη παρέχεται από τον William Boone, το 1958, στην εργασία του [Bo58].

Καθίσταται σαφές πως το πρόβλημα χωρίζεται σε δύο μέρη: το καταφατικό (ισχύει ότι $w \sim_G \varepsilon$;) και το αρνητικό (ή όχι;). Ένα πρώτο αποτέλεσμα υπαγορεύει πως υπάρχει αλγοριθμική ημιαναδρομική διαδικασία για το καταφατικό μέρος του προβλήματος.

Πρόταση 1.35. Έστω η αναδρομικά παραστάσιμη ομάδα $G = \langle X \mid R \rangle$. Το σύνολο

$$\{g \in G \mid g \sim_G \varepsilon\}$$

είναι αναδρομικά αριθμήσιμο.

Δεν υπάρχει κάποια ιδιαιτερότητα ως προς την επιλογή του μοναδιαίου στοιχείου της ομάδος. Θα μπορούσε να εξετασθεί η ισότητα των στοιχείων της ομάδος ως προς οποιοδήποτε συγκεκριμένο στοιχείο (της ομάδος). Έτσι ένα ειδικότερο του προβλήματος της λέξεως προκύπτει να είναι

Το μεμονωμένο πρόβλημα της λέξης. Έστω μία ομάδα $G = \langle X \mid R \rangle$ κι ένα δεδομένο $w \in G$. Ισχύει για το αυθαίρετο $t \in G$ ότι $t \sim_G w$ ή όχι;

Τέλος, για λόγους πληρότητα, παρατίθεται ενθάδε

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

το οποίο επίσης παρέχει κρυπτογραφικές μεθόδους και το οποίο εν γένει δεν επιδέχεται αλγορίθμου που να το επιλύει σε κάθε ομάδα.

Κεφάλαιο 2

Το σχήμα ανταλλαγής κλειδιού των Wagner-Magyarik

Απαρχή των πρωτοκόλλων της μη-μεταθετικής Κρυπτογραφίας αποτελεί το σχήμα των Neil R. Wagner και Robert Magyarik –που εισάγεται στην εργασία τους [WM85]– σκοπός του οποίου είναι η ανταλλαγή ενός μυστικού κωδικού (κλειδιού) ανάμεσα σε δύο οντότητες. Πέραν του πρωτοκόλλου, περιέχονται και οι προτεινόμενες παράμετροι ασφαλείας του σχήματος, όπως αυτές παρέχονται από τους εισηγητές του. Η δεύτερη Ενότητα αποδομεί το σχήμα μιας και καταφέρνει να αντλήσει πληροφορία για το μυστικό κλειδί, ενώ η τρίτη Ενότητα έρχεται να αποδώσει ξανά δύναμη στο πρωτόκολλο λόγῳ μιας απλής παρατήρησης.

2.1 Το πρωτόκολλο των Wagner-Magyarik

- Έστω μια ομάδα $G = \langle X \mid R \rangle$.

Στην ελεύθερη ομάδα $F(X)$, θεωρούνται οι ακόλουθοι κανόνες:

(K1) Διαγραφή μιας υπολέξης της μορφής xx^{-1}, ή $x^{-1}x$, για κάποιο $x \in X$.

(K2) Εισαγωγή μιας υπολέξης της μορφής xx^{-1}, ή $x^{-1}x$, για κάποιο $x \in X$, οπουδήποτε στη λέξη.

(K3) Διαγραφή μιας υπολέξης της μορφής $r \in R$, ή της μορφής $r^{-1} \in R$.

(K4) Εισαγωγή μιας υπολέξης της μορφής $r \in R$, ή $r^{-1} \in R$, οπουδήποτε στη λέξη.

Συμβολισμός. $x \sim_G y \iff_{o\rho} \left[\begin{array}{c} \text{υπάρχει ακολουθία } w_0, \ldots, w_n \in F(X), \text{ ώστε } w_0 = x, \\ w_n = y, \text{ με το } w_i \in F(X) \text{ προκύπτει από το } w_{i-1} \in F(X) \text{ με} \\ \text{εφαρμογή κάποιου κανόνα (K1)—(K4) στην } G \ (i = 1, \ldots, n) \end{array} \right]$.

Αλίκη	Βασίλης

Αρχικά δεδομένα για την επακόλουθη επικοινωνία

Ομάδα $G = \langle X \mid R \rangle$ με δύσκολο πρόβλημα της λέξης και $S \subseteq F(X)$ τέτοιο ώστε η ομάδα $H = \langle X \mid R \cup S \rangle$ να έχει εύκολο πρόβλημα της λέξης. Επιπλέον, $w_0, w_1 \in F(X)$, με $w_0 \not\sim_H w_1$ (κι άρα και $w_0 \not\sim_G w_1$).	$K = b_1 b_2 \ldots b_n \in \{0,1\}^n$, όπου $n \in \mathbb{N}$.

Επικοινωνία

Ιδιωτικό κλειδί: $S \subseteq F(X)$.

Δημόσιο κλειδί: $G = \langle X \mid R \rangle$ και $w_0, w_1 \in F(X)$

Για $k = 1, 2, \ldots, n$ επανάλαβε:

$y_k \in F(X)$

$w_i \sim_G y_k$, όπου $b_k = i \in \{0,1\}$, με εφαρμογή τυχαίου πλήθους φορών σε τυχαία σημεία της w_i, κάποιου κανόνα (K1)–(K4) (όχι κατ' ανάγκη του ιδίου κάθε φορά).

$$b_k = \begin{cases} 0, & \text{εάν } y_k w_0^{-1} \sim_H 1 \\ 1, & \text{εάν } y_k w_1^{-1} \sim_H 1 \end{cases}$$

Σχήμα 2.1: Το σχήμα ανταλλαγής κλειδιού Wagner-Magyarik

Το σχήμα μπορεί να γενικευθεί και στο αυθαίρετο αλφάβητο Σ ως εξής: Θεωρείται το σύνολο $W(\Sigma) = \{w_\sigma \in F(X) : \sigma \in \Sigma\}$, όπου $(\forall \sigma, \tau \in \Sigma)[\sigma \neq \tau \implies w_\sigma \not\sim_G w_\tau]$. Το δημόσιο κλειδί πλέον είναι το $\{\langle X \mid R \rangle, W(\Sigma)\}$. Για την κρυπτογράφηση του γράμματος $\sigma \in \Sigma$ χρησιμοποιείται η λέξη $w_\sigma \in W(\Sigma)$. [Άνωθεν -προφανώς- είναι $\Sigma = \{0,1\}$.]

Στις πεπερασμένα παραγόμενες ομάδες η πολυπλοκότητα του προβλήματος της λέξης έγκειται στην ομάδα και όχι στην επιλογή της παράστασης. Με άλλα λόγια εάν η ομάδα $\langle X \mid R \rangle$, όπου $|X| < +\infty$, έχει επιλύσιμο πρόβλημα της λέξης, τότε θα έχει επιλύσιμο πρόβλημα της λέξης για κάθε σύνολο γεννητόρων Y, με $|Y| < +\infty$· η πολυπλοκότητα του προβλήματος αλλάζει γραμμικά ανάμεσα στις διαφορετικές παραστάσεις (βλ. [MO85]).

2.1.1 Εικασίες ασφαλείας

Στο [WM85] οι εισηγητές του σχήματος απαριθμούν τις κάτωθι επιθέσεις*:

⟦*Να βρεθεί αποτελεσματικός αλγόριθμος ο οποίος επιλύει το πρόβλημα της λέξης στην* G⟧:
Με έναν τέτοιον αλγόριθμο, κανείς αποφασίζει με ποια εκ των w_0 ή w_1 είναι ισοδύναμη με την w. Ο Gilles Brassard αναφέρει πως υπάρχει πάντοτε ένας απλός, αλλά απρόσιτος, αλγόριθμος ο οποίος κάνει αυτή τη δουλειά:

> "Σε πεπερασμένο χρονικό διάστημα να δοκιμαστούν όσο το δυνατόν περισσότερες εφαρμογές των κανόνων (K1)—(K4) στις w_0, w_1 με σκοπό να παραχθεί η w."

Οι εισηγητές ελπίζουν πως με κατάλληλη επιλογή της ομάδος G, επιθέσεις σαν και την παραπάνω θα καθίστανται αδύνατες.

⟦*Να βρεθεί* $T \subseteq F(X)$ *ώστε η* $K = \langle X \mid R \cup T \rangle$ *να έχει επιλύσιμο πρόβλημα της λέξης και* $w_0 \not\sim_K w_1$⟧: Δεν χρειάζεται να είναι $T \cap S \neq \varnothing$ (όπου $S \subseteq F(X)$ είναι το μυστικό κλειδί). Οι εισηγητές ισχυρίζονται πως με τις επιλογές που προτείνουν (βλ. §2.1.2) τέτοιες επιθέσεις αποκλείονται.

⟦*Να δοκιμαστεί κάθε δυνατό* $S \subseteq F(X)$ *μέχρι να αποκρυπτογραφηθεί το κρυπτοκείμενο*⟧:
Μία τέτοια επίθεση θα επιτύγχανε· για το λόγο αυτό δείχνει πως η κρυπτανάλυση έγκειται σε αναιτιοκρατικές κλάσεις πολυπλοκότητας (οι εισηγητές κάνουν αναφορά για την κλάση NP, ωστόσο στην πραγματικότητα πρόκειται για χαμηλότερη κλάση, βλ. §2.2.1). Επιπλέον, δεν υπάρχουν ενδείξεις για το μήκος του μικρότερου κλειδιού που μπορεί να χρησιμοποιηθεί για αποκρυπτογράφηση. Επίσης, με κατάλληλη επιλογή της ομάδας G, ενδέχεται να υπάρχουν άπειρα πιθανά υποψήφια κλειδιά, γεγονός που μειώνει την πιθανότητα ευστοχίας της εξαντλητικής αναζήτησης.

⟦*Επίθεση με γνωστό κείμενο*⟧: δηλαδή ένα γνωστό κείμενο έχει κρυπτογραφηθεί με όλα τα πιθανά κλειδιά έχοντας παράξει έτσι γνώση για τη συμπεριφορά του σχήματος. Μια τέτοια επίθεση είναι σχεδόν απίθανη, αφού

(α′) ακόμη και με το σωστό κλειδί, το κρυπτοκείμενο δεν μπορεί να παρέχει καμμία πληροφορία [αφού έγκειται στον αποστολέα το πόσο θα *αποκρύψει* την w_i, $i \in \{0, 1\}$ με την εφαρμογή των κανόνων (K1)—(K4)]·

(β′) ο χώρος των πιθανών κλειδιών ενδέχεται να είναι άπειρος.

---

*οι οποίες υπολείπονται αποδείξεων και γι αυτό και τιτλοφορούνται ως *εικασίες*.

2.1.2 Πειραματικά δεδομένα

Μορφή του μυστικού κλειδιού. Γενική πεποίθηση είναι η επιλογή του μυστικού κλειδιού S, να είναι τέτοια ώστε $r \sim_H \varepsilon$, όπου $H = \langle X \mid R \cup S \rangle$. Για τον λόγο αυτό οι εισηγητές προτείνουν τα στοιχεία $s \in S$ να έχουν τις ακόλουθες μορφές:

(S1) Διαγραφή ενός γεννήτορα: $s = x$, για κάποιο $x \in X$.
[Άρα, θα είναι $x = \varepsilon$ στην H, δηλαδή κάθε εμφάνιση του x απαλείφεται.]

(S2) Ταύτιση δύο γεννητόρων: $s = xy^{-1}$ (ή $s = xy$), για κάποια $x, y \in X$.
[Άρα, θα είναι $xy^{-1} = \varepsilon$ (ή $xy = \varepsilon$) στην H, δηλαδή $x = y$ (αντίστοιχα $x = y^{-1}$)].

(S3) Αντιμετάθεση δύο γεννητόρων: $s = xyx^{-1}y^{-1}$, για κάποια $x, y \in X$.
[Άρα, θα είναι $xy = yx$ στην H.]

Η χρήση των παραπάνω κανόνων θα απλοποιούσε τις λέξεις του R. Κατά βάση τα σύνολα $R, S \subseteq F(X)$ θα επιλεχθούν κατά τέτοιον τρόπο ώστε κάθε $r \in R$ αν συγκολληθεί με κάθε $s \in S$ να προκύπτει η κενή λέξη ε. Κατόπιν όλων των παραπάνω η ομάδα H θα είναι μια ομάδα με σχέσεις μόνον της μορφής (S3), ωστόσο θα πρέπει να διατηρηθεί ότι $w_0 \not\sim_H w_1$.

Έτσι λοιπόν προκύπτει επιπροσθέτως η εξής επίθεση:

$[\![$*Να βρεθούν* $s_j = \varepsilon$, $j \in J$, *των τύπων (S1)–(S3) ώστε* $(\forall r \in R)[r \sim_H \varepsilon]$ *και* $w_0 \not\sim_H w_1]\!]$: Η αποφυγή μιας τέτοιας επίθεσης είναι η επιλογή των w_0, w_1 να γίνει κατά τέτοιο τρόπο ώστε για τις "περισσότερες" επιλογές των s_j, $j \in J$, να προκύπτει πως $w_0 \sim_H w_1$.

Προς αποφυγήν της παραπάνω επίθεσης, συνίσταται ώστε το σύνολο των σχέσεων $R \subseteq F(X)$ να επιλέγεται κατά τέτοιο τρόπο, ώστε για τις *περισσότερες* επιλογές ενός $S \subseteq F(X)$, ώστε $(\forall r \in R)[r \sim_H \varepsilon]$, όπου $H = \langle G \mid R \cup S \rangle$, να έπεται και ότι $w_0 \sim_H \varepsilon$ και $w_1 \sim_H \varepsilon$. Κάτι τέτοιο καθίσταται εφικτό επιτρέποντας μόνον για ένα $Y \subseteq X$, με $|Y| \ll |X|$, να ισχύει ότι $(\forall y, z \in Y)[zy \neq yz]$.

Μορφή του δημοσίου κλειδιού. Σύμφωνα με το ως άνω σκεπτικό οι εισηγητές καταλήγουν στο ότι κάθε $r \in R$, θα πρέπει να είναι μιας εκ των κάτωθι μορφών:

(R1) $x_i x_j x_k x_l x_i^{-1} x_k^{-1} x_j^{-1} x_l^{-1}$,

(R2) $x_i x_j x_k x_i^{-1} x_j^{-1} x_k^{-1}$,

(R3) $x_i x_j x_k x_i^{-1} x_k^{-1} x_j^{-1}$,

όπου $x_i, x_j, x_k, x_l \in X \cup X^{-1}$.

Οι εισηγητές ενισχύουν τη δύναμη του σχήματος μ' ένα

Παράδειγμα 2.1. Έστω ομάδα $G = \langle X \mid R \rangle$, $x_3x_6x_1x_2 \in F(X)$ και $x_1x_2x_3x_4x_5x_6 \in R$, τότε $x_1x_2x_3x_4x_5x_6 \in R \iff x_1x_2x_3x_4x_5x_6 = \varepsilon \iff x_3x_4x_5 = x_2^{-1}x_1^{-1}x_6^{-1}$ και θεωρώντας τον αντίστροφο κάθε μέλους $x_5^{-1}x_4^{-1}x_3^{-1} = x_6x_1x_2$. Άρα, $x_3x_6x_1x_2 \sim_G x_3x_5^{-1}x_4^{-1}x_3^{-1}$. ⊣

το οποίο καταδεικνύει τη δύναμη του συνόλου σχέσεων $R \subseteq F(X)$ αφού κάθε συσχετιστής μήκους n μπορεί να γραφεί με $2n^2$ τρόπους αναδιάτασσοντας κυκλικά τα γραμμάτά του.

Σύγχηση του κρυπτοκειμένου. Η τελείως τυχαία εφαρμογή των συσχετιστών στις λέξεις είναι ανεπιθύμητη, καθώς θα πρέπει το μέγεθος του παραγόμενου κρυπτοκεκιμένου να κυμαίνεται σε κάποια λογικά όρια. Επιπλέον, δεν είναι επιθυμητό μία ύστερη εφαρμογή ενός συσχετιστή να ακυρώνει κάποια πρότερη εφαρμογή. Γι αυτό διατηρείται μία (εικονική) στοίβα η οποία αποσοβεί τέτοιες ακυρώσεις. Η στρατηγική είναι η εξής:

1: **επανάλαβε**
2: Επιλογή μιας θέσης της λέξης w_i, $b_k = i$, κι ενός $r \in R$ στη τύχη.
3: Προσπάθεια εφαρμογής του συσχετιστού $r \in R$ κοντά στην επιλεγμένη θέση.
4: **έως ότου** (κάθε γράμμα της αρχικής λέξης να έχει αντικατασταθεί)

2.2 Κρυπτανάλυση

2.2.1 Κριτική

Οι Jean-Camille Birget, Σπύρος Μαγκλιβέρας και Michal Sramka στην κριτική τους για το σχήμα ανταλλαγής κλειδιού των Wagner-Magyarik που εμπεριέχεται στο [BMS06] διακρίνουν τα εξής ελαττωματικά σημεία:

Ερώτημα: Πώς επιλέγονται κατάλληλες παραστάσεις $\langle X \mid R \rangle$ και $\langle X \mid R \cup S \rangle$, καθώς και πως κατασκευάζεται ο αλγόριθμος για το πρόβλημα της λέξης στην $\langle X \mid R \cup S \rangle$;

Απάντηση: Η §2.1.2 παρέχει μια απάντηση, ωστόσο μη-ικανοποιητική. Είναι ανοικτό πρόβλημα εάν η μεθοδολογία που παρουσιάζεται δημιουργεί ομάδες με δύσκολα επιλύσιμο πρόβλημα της λέξης. Η επιλογή ενός $R \subseteq F(X)$ ώστε η ομάδα $\langle X \mid R \rangle$ να έχει δύσκολα επιλύσιμο πρόβλημα της λέξης είναι από μόνο του δύσκολο πρόβλημα.

Ερώτημα: Πώς επιλέγονται κατάλληλες $w_0, w_1 \in F(X)$;

Απάντηση: Ανοικτό ερώτημα.

Ερώτημα: Σύμφωνα με ποιο πρότυπο γίνεται εφαρμογή και πότε κρίνεται επαρκής η εφαρμογή των κανόνων (K1)—(K4);

Απάντηση: Η §2.1.2 περιέχει μια μερική, μη-ικανοποιητική απάντηση. Εν γένει το ερώτημα παραμένει ανοικτό.

Ερώτημα: Πόσο ασφαλές είναι το σχήμα;

Απάντηση: Στο [WM85] γίνεται λόγος –σε θεωρητικό υπόβαθρο– για την ασφάλεια του σχήματος· εδώ παρουσιάζεται στην §2.1.1. Ωστόσο, η §2.2.2 δίνει την απάντηση.

Ερώτημα: Πώς διαχειρίζονται τα εναλλακτικά κλειδιά; [δηλαδή τα $T \subseteq F(X)$, τέτοια ώστε η $K = \langle X \mid R \cup T \rangle$ έχει εύκολα επιλύσιμο πρόβλημα της λέξης και $w_0 \not\sim_K w_1$.]

Απάντηση: Κάθε ομομορφική εικόνα της $\langle X \mid R \rangle$ με εύκολα επιλύσιμο πρόβλημα της λέξης η οποία δεν καθιστά τις $w_0, w_1 \in F(X)$ ισοδύναμες μπορεί να χρησιμοποιηθεί για αποκρυπτογράφηση. Συνεπώς αυξάνεται η πολυπλοκότητα απόδειξης ασφαλείας του σχήματος καθώς θα πρέπει επιπλέον να δειχθεί πως το

> "Να βρεθεί μια ομομορφική εικόνα της $\langle X \mid R \rangle$ που διατηρεί μη ισοδύναμα τα $w_0, w_1 \in F(X)$ κι έχει εύκολα επιλύσιμο πρόβλημα της λέξης"

είναι δύσκολο πρόβλημα.

Ωστόσο, η αδυναμία του συστήματος κρύβεται στην εσφαλμένη πεποίθηση πως η ασφάλεια στηρίζεται στη δυσκολία της επίλυσης του προβλήματος της λέξης, ενώ στην πραγματικότητα στηρίζεται στο πιο (αδύναμο) *υποσχετικό* πρόβλημα

Το πρόβλημα επιλογής της λέξης. Έστω μια ομάδα G και $w, w_0, w_1 \in F(X)$. *Είναι γνωστόν ότι είτε* $ww_0^{-1} = 1_G$, *είτε* $ww_1^{-1} = 1_G$. Ισχύει ότι $ww_0^{-1} = 1_G$;

Η σημαντική διαφορά με το κλασσικό πρόβλημα της λέξεως είναι πως το παραπάνω ενέχει μία αρχική συνθήκη, δηλαδή είναι γνωστό εκ των προτέρων πως η w ισούται με μία εκ των w_0, w_1. Οι αλγόριθμοι για υποσχετικά προβλήματα λαμβάνουν πάντοτε υπόψιν τους την αρχική συνθήκη· έτσι εάν τους δοθεί μία είσοδος που δεν ικανοποιεί την αρχική συνθήκη είτε δεν τερματίζουν, είτε δεν δίδουν σωστή απάντηση. Το πρόβλημα επιλογής της λέξης στην ομάδα G είναι

- πάντοτε επιλύσιμο εάν η G είναι πεπερασμένα παριστάμενη·
- ανήκει στην κλάση $\mathsf{NP} \cap \mathsf{coNP} \subseteq \mathsf{NP}$ (η πεποίθηση είναι πως είναι γνήσιος εγκλεισμός) εάν το πρόβλημα της λέξης στην ομάδα G ανήκει είτε στην κλάση NP, είτε στην coNP.

2.2.2 Επίθεση αντίδρασης

Πρόκειται για μια επίθεση αντίδρασης (reaction attack). Οι πρώτες τέτοιες επιθέσεις απαντώνται από τους Chris Hall, Ian Goldberg και Bruce Schneider στο [HGS99] οι οποίοι κατάφεραν να αποκρυπτογραφήσουν και να εξάγουν το μυστικό κλειδί στα σχήματα των McEllie και Ajtai-Dwork. Το 2002 οι María Isabel González Vasco και Rainer Steinwandt δημοσίευσαν την παρούσα επίθεση αντίδρασης στην εργασία τους [VS02].

Σκοπός της επίθεσης είναι η εύρεση ενός συνόλου

$$\overline{S} = \{a \in A \mid a \sim_H \varepsilon\}$$

απ' όπου μπορεί να εξαχθεί ένα σύνολο $\overline{\mathcal{S}}$, ώστε η $\langle X \mid \overline{\mathcal{S}} \rangle$ είναι μία παράσταση της $H = \langle X \mid R \cup S \rangle$ (ή κάποιου άλλου πηλίκου της που είναι έγκυρο μυστικό κλειδί —2^{η} Επίθεση της §2.2.2).

2.2.2.Α΄ Υποθέσεις εργασίας

(ΥΕ1) $w_0 w_1 \not\sim_H w_1 w_0$.

(ΥΕ2) Ένα μαντείο $\mathfrak{O} : F(X) \longrightarrow \{0, 1\}$, με $\mathfrak{O}(w) = \begin{cases} 1, & \text{εάν } w \sim_H w_1 \vee w \sim_H w_2 \\ 0, & \text{αλλιώς} \end{cases}$.

(ΥΕ3) Ένα $A \subseteq F(X)$, όπου η εξαντλητική αναζήτηση γίνεται σε αποτελεσματικό χρόνο.

Για την εύρεση του συνόλου $\overline{S}$ είναι διαθέσιμος ο ακόλουθος αλγόριθμος:

Αλγόριθμος 2.1 RA(A): Αλγόριθμος συσχετιστών.

Είσοδος: Ένα σύνολο $A \subseteq F(X)$, όπου $G = \langle X \mid R \rangle$.
Δεδομένα: Οι υποθέσεις εργασίας (ΥΕ1), (ΥΕ2) και (ΥΕ3).
Έξοδος: $\overline{S} = \{a \in A \mid a \sim_H \varepsilon\} \subseteq A$.

```
1: S̄ ← ∅;
2: για κάθε a ∈ A
3:    εάν ((𝔒(aw₀) = 1) ∧ (𝔒(w₀a) = 1)) τότε
4:       S̄ ← S̄ ∪ {a};
5:    τέλος εάν
6: τέλος για
7: επίστρεψε S̄;
```

Ορθότητα του Αλγορίθμου 2.1: Γίνονται αποδεκτές οι υποθέσεις εργασίας (ΥΕ1), (ΥΕ2) και (ΥΕ3) και διακρίνονται οι ακόλουθες περιπτώσεις:

- Εάν είτε $\mathfrak{O}(aw_0) = 0$, είτε $\mathfrak{O}(w_0a) = 0$, τότε προφανώς $a \notin \overline{S}$.
- Αλλιώς είναι $\mathfrak{O}(aw_0) = \mathfrak{O}(w_0a) = 1$, κι έστω ότι $a \notin \overline{S}$, τότε

$$\mathfrak{O}(aw_0) = 1 \implies \begin{cases} \text{είτε } aw_0 \sim_H w_0 \implies a \in \overline{S} \text{ (άτοπο εξ υποθέσεως)} \\ \text{είτε } aw_0 \sim_H w_1 \implies w_0aw_0 \sim_H w_0w_1 \end{cases} \tag{2.1}$$

$$\mathfrak{O}(w_0a) = 1 \implies \begin{cases} \text{είτε } w_0a \sim_H w_0 \implies a \in \overline{S} \text{ (άτοπο εξ υποθέσεως)} \\ \text{είτε } w_0a \sim_H w_1 \implies w_0aw_0 \sim_H w_1w_0 \end{cases} \tag{2.2}$$

Άρα, $w_0w_1 \overset{(2.1)}{\sim_H} w_0aw_0 \overset{(2.2)}{\sim_H} w_1w_0 \implies w_0w_1 \sim_H w_1w_0$, άτοπο εκ της (ΥΕ1). ⊣

2.2.2.Β΄ Υλοποίηση

Έστω το δημόσιο κλειδί για το πρωτόκολλο Wagner-Magyarik

$$\begin{cases} G = \langle X \mid R \rangle \\ w_0, w_1 \in F(X) \end{cases}$$

(όπου η ομάδα $G = \langle X \mid R \rangle$ έχει δύσκολα επιλύσιμο πρόβλημα της λέξης) καθώς και το ιδιωτικό κλειδί

$$S \subseteq F(X)$$

(όπου η ομάδα $H = \langle X \mid R \cup S \rangle$ έχει εύκολα επιλύσιμο πρόβλημα της λέξης). Υποτίθεται πως η υλοποίησή του ακολουθεί τα πρότυπα της §2.1.2.

- Εντοπισμός των συσχετιστών τύπου (R1):

$$\begin{aligned} \overline{S}_1 &:= \mathtt{RA}(X) \\ &\equiv \{x \in X : x \sim_H \varepsilon\} \end{aligned}$$

  ήτοι το σύνολο γεννητόρων που διαγράφονται στην H.

- Εντοπισμός των συσχετιστών τύπου (R2):

$$\begin{aligned} \overline{S}_2 &:= \mathtt{RA}\big(X \setminus \overline{S}_1\big) \\ &\equiv \big\{x_i x_j^{-1} \in F\big(X \setminus \overline{S}_1\big) : i \neq j \wedge x_i \sim_H x_j\big\} \end{aligned}$$

  (με $\left|\overline{S}_2\right| \leqslant |X|^2$) ήτοι το σύνολο γεννητόρων που συμπίπτουν στην H.

- Εντοπισμός των συσχετιστών τύπου (R3):

$$\begin{aligned}\overline{S}_3 &:= \mathrm{RA}(X \setminus (\overline{S}_1 \cup \overline{S}_2)) \\ &\equiv \left\{x_i x_j x_i^{-1} x_j^{-1} \in F(X \setminus (\overline{S}_1 \cup \overline{S}_2)) : i \neq j \wedge x_i x_j \sim_H x_j x_i\right\}\end{aligned}$$

  (με $\left|\overline{S}_3\right| \leqslant |X|^2$) δηλαδή το σύνολο γεννητόρων που αντιμετατίθενται στην H.

Η παράσταση $\langle X \mid \overline{S}_1 \cup \overline{S}_2 \cup \overline{S}_3\rangle$ είναι μία (άλλη) παράσταση της $H = \langle X \mid R \cup S\rangle$.

2.3 Αναθεώρηση

Το 2005 οι Françoise Levy-dit-Vehel και L Perret αναφέρουν στην εργασία τους [LP05] πως η επίθεση αντίδρασης της §2.2.2 επιτυγχάνει λόγῳ του σκεπτικού της §2.1.2.

Ορισμός 2.2. Ένα **μονοειδές** είναι ένα σύνολο G εφοδιασμένο με μια διμελή προσεταιριστική πράξη $* : G \times G \to G$ και $(\exists! e \in G)(\forall x \in G)[x * e = e * x]$ (ταυτοτικό στοιχείο).

Οι N. Wagner και M. Magyarik εξαρχής παρατητρούν πως η χρήση μονοειδών δεν προσθέτει κάποια υπολογιστικη πολυπλοκότητα στο κρυπτοσύστημά τους. Την παρατήρηση αυτή, ωστόσο, οι F. Levy-dit-Vehel και L. Perret την χρησιμοποιούν για την αποσόβηση επιθέσεων αντίδρασης [βλ. §2.2.2].

► Έστω ένα πεπερασμένο αλφάβητο $\Delta = \{x_1, x_2, \ldots, x_n\}$.

Συμβολισμός. Για την παρούσα Ενότητα μόνον, ως Δ^* θα συμβολίζεται το ελεύθερο μονοδειδές που παράγεται από το σύνολο Δ.

Ορισμός 2.3. Έστω $R \subseteq \Delta^* \times \Delta^*$.

1. Ορίζεται η σχέση $\leftrightarrow_R \subseteq \Delta^* \times \Delta^*$ ως

   $u \leftrightarrow_S v \iff_{\text{ορ}} (\exists x, y \in \Delta^*)(\exists (\ell, r) \in R)\left[(u = x\ell y \wedge v = xry) \vee (u = xry \wedge v = x\ell y)\right]$

2. Η **Thue συνάφεια** που παράγεται από το R επί του Δ^*, συμβολίζεται με $\overset{*}{\leftrightarrow}_R$ και ορίζεται να είναι η ανακλαστική και μεταβατική κλειστότητα της σχέσης $\leftrightarrow_R$.

3. Ορίζεται $(\Delta, R) := {}^{\Delta}\!/_{\overset{*}{\leftrightarrow}_R}$.

4. Έστω $\theta \subseteq \Delta \times \Delta$ μία διμελής, ανακλαστική και μεταβατική σχέση στο Δ. Σε κάθε $w \in \Delta^*$, κάθε υπολέξη $ab \in \Delta^2$ της w, με $(a, b) \in \theta$, μπορεί να αντικατασταθεί από την υπολέξη $ba \in \Delta^2$. Το γεγονός πως μία $v \in \Delta^*$ που προκύπτει από την $u \in \Delta^*$ με εφαρμογή τις προαναφερθήσης διαδικασίας συμβολίζεται ως $u \equiv_\theta v$.

Έτσι, με την καινούργια ορολογία, ανακύπτει

Το πρόβλημα της λέξης στο μονοειδές (Δ, R)**.** Δοσμένων $u, v \in \Delta^*$ ισχύει ότι $u \overset{*}{\leftrightarrow}_R v$;

Η εκδοχή του σχήματος ανταλλαγής κλειδιού Wagner-Magyarik για τα μονοειδή είναι:

Αλίκη. Δημόσιο κλειδί: Μονοειδές (Δ, R), $|R| < +\infty$ και $w_0, w_1 \in \Delta^*$, με $w_0 \overset{*}{\not\leftrightarrow} w_1$.
Ιδιωτικό κλειδί: $S \subseteq \Delta^* \times \Delta^*$, τέτοιο ώστε το (Δ, S) έχει τις ιδιότητες

$$(\forall u, v \in \Delta^*)\big[u \overset{*}{\leftrightarrow}_R v \implies u \overset{*}{\leftrightarrow}_S v\big] \qquad\qquad w_0 \overset{*}{\not\leftrightarrow}_S w_1$$

Βασίλης. Κρυπτογραφεί το $b \in \{0, 1\}$ επιλέγοντας μία $w \in \Delta^*$, με $w \overset{*}{\leftrightarrow}_R w_b$.

Αλίκη. Αποκρυπτογραφεί την $w_b \in \Delta^*$ στο μονοειδές (Δ, S) και ανακτάει το $b \in \{0, 1\}$.

Η μορφή του ιδιωτικού κλειδιού $S \subseteq \Delta^* \times \Delta^*$ θα είναι $S = S_1 \cup S_2 \cup S_3$, όπου

$$S_1 \equiv S_1(K) := \big\{(x, \varepsilon) \in \Delta^* \times \Delta^* : x \in K\big\}, \quad S_2 \equiv S_2(M) := \big\{(x, y) \in \Delta^* \times \Delta^* : x, y \in M\big\},$$
$$S_3 \equiv S_3(N) := \big\{(xy, yx) \in \Delta^* \times \Delta^* : x, y \in N\big\}$$

για κάποια $K, M, N \subseteq X$, δηλαδή όπως ακριβώς είχε προταθεί στο αρχικό πρωτόκολλο των Wagner-Magyarik, με τη μόνη διαφορά πως εδώ γίνεται χρήση μονοειδών και τα αντίστροφα στοιχεία *δεν* είναι καλώς ορισμένα, γεγονός που προσθέτει δύναμη στο πρωτόκολλο.

Σε κάθε προσπάθεια παρείφρησης στο πρωτόκολλο, (η εκδοχή απόφασης του προβλήματος που) ανακύπτει (είναι)

Το πρόβλημα Wagner-Magyarik (εκδοχή απόφασης, $\mathtt{WM}_d$). Στο αλφάβητο Δ, θεωρείται το Thue σύστημα $R \subseteq F(\Delta) \times F(\Delta)$ καθώς και $w_0, w_1 \in F(\Delta)$, με $w_0 \overset{*}{\not\leftrightarrow}_R w_1$. Υπάρχει $S \subseteq F(\Delta) \times F(\Delta)$ της μορφής $S = S_1 \cup S_2 \cup S_3$ (τα S_1, S_2, S_3 όπως παραπάνω), τέτοιο ώστε $(\forall x, y \in \Delta^*)\big[x \overset{*}{\leftrightarrow}_R y \implies x \overset{*}{\leftrightarrow}_S y\big]$ και $w_0 \overset{*}{\not\leftrightarrow}_S w_1$;

Ένα *συναφές* πρόβλημα είναι

Το πρόβλημα TMMI[†] (εκδοχή απόφασης, $\mathtt{TMMI}_d$). Στο αλφάβητο Δ, θεωρείται το Thue σύστημα $T \subseteq \Delta^* \times \Delta^*$ καθώς και $y_0, y_1 \in \Delta^*$. Υπάρχει ένα αλφάβητο Σ, ένας μητετριμμένος μορφισμός (ερμηνείας) $g : \Delta^* \longrightarrow \Sigma^*$ και μία σχέση (συγχρονισμού) θ στο Σ, ώστε $g(y_0) \not\equiv_\theta g(y_1)$, $(\forall d \in \Delta)[g(d) \in \Sigma \vee g(d) = \varepsilon]$, $(\exists d \in \Delta)[g(d) \in \Sigma]$ και $\big(\forall u, v \in \Delta^*\big)\big[u \overset{*}{\leftrightarrow}_T v \implies g(u) \equiv_\theta g(v)\big]$;

Θεώρημα 2.4 ([LP05, Πόρισμα 2]). 1. Το $\mathtt{WM}_d$ είναι NP-πλήρες πρόβλημα.

[Υπάρχει πολυωνυμική αναγωγή πολλά-προς-ένα από το SAT στο $\mathtt{TMMI}_d$. Επίσης, υπάρχει πολυωνυμική αναγωγή πολλά-προς-ένα από το $\mathtt{TMMI}_d$ στο $\mathtt{WM}_d$.]

2. Το (υπολογιστικό) πρόβλημα Wagner-Magyarik (που συνίσταται στον προσδιορισμό του συνόλου $S \subseteq \Delta^* \times \Delta^*$ από την εκδοχή απόφασης) είναι NP-δύσκολο πρόβλημα.

[Η εκδοχή απόφασης ενός προβλήματος πάντοτε είναι δυσκολότερη από την υπολογιστική του εκδοχή.]

[†]Thue Monoid Morphism Interpretation

Κεφάλαιο 3

Ένα σχήμα ανταλλαγής κλειδιού βασισμένο στις ομάδες Grigorchyk

Η επόμενη προσπάθεια να στηριχθεί ένα σχήμα ανταλλαγής κλειδιού στο πρόβλημα της λέξης είναι αυτή των Garzon-Zalcstein στο [GZ85], το 1985. Στην εργασία τους χρησιμοποιούν τη δυσκολία επίλυσης του προβλήματος της λέξης εν προκειμένῳ να διαχωρίσουν κλάσεις υπολογιστικής πολυπλοκότητας. Το Κεφάλαιο αρχίζει με μια εισαγωγή στις ομάδες Grigorchyk και αναφορά των ιδιοτήτων τους που θα χρησιμοποιηθούν. Ύστερα παρουσιάζεται το σχήμα των Garzon-Zalcstein και κατόπιν η επίθεση που καθιστά το σχήμα ανασφαλές.

3.1 Οι ομάδες Grigorchyk

3.1.1 Θεωρία Γραφημάτων

Μερικοί βασικοί (και χρήσιμοι στο ρουν της Εργασίας) ορισμοί:

Κατευθυνόμενο γράφημα είναι μια δομή $\Gamma = (V, E)$, όπου V ένα σύνολο και $E \subseteq V \times V$.

Μονοπάτι μήκους $n \in \mathbb{N}_0$ είναι μια διατεταγμένη n-άδα $(v_0, v_1, \ldots, v_n) \in V^{n+1}$, όπου $(\forall i = 1, 2, \ldots, n)\left[(v_{i-1}, v_i) \in E\right]$ και $(\forall i, j = 1, 2, \ldots, n)[i \neq j \implies v_i \neq v_j]$.

Κύκλος μήκους $n \in \mathbb{N}$ είναι ένα μονοπάτι $(v_1, v_2, \ldots, v_n) \in V^n$, όπου $v_1 = v_n$.

Δένδρο είναι ένα γράφημα $T = (V, E)$ που δεν περιέχει κύκλους (μήκους $n = 1, \ldots, |V|$).

Απόγονος της κορυφής $v \in V$ καλείται κάθε κορυφή $w \in \left\{y \in V : (v, y) \in E\right\}$.

Πρόγονος την κορυφής $v \in V$ καλείται κάθε κορυφή $w \in \left\{x \in V : (x, v) \in E\right\}$.

Ρίζα ενός δένδρου $T = (V, E)$ καλείται η (μόνη) κορυφή με $\{(x, v) \in E : x \in V\} = \varnothing$.

Πλήρες δυαδικό δένδρο $T = (V, E)$ καλείται ένα δένδρο με ρίζα, κάθε κορυφή του οποίου έχει *ακριβώς* δύο απογόνους.

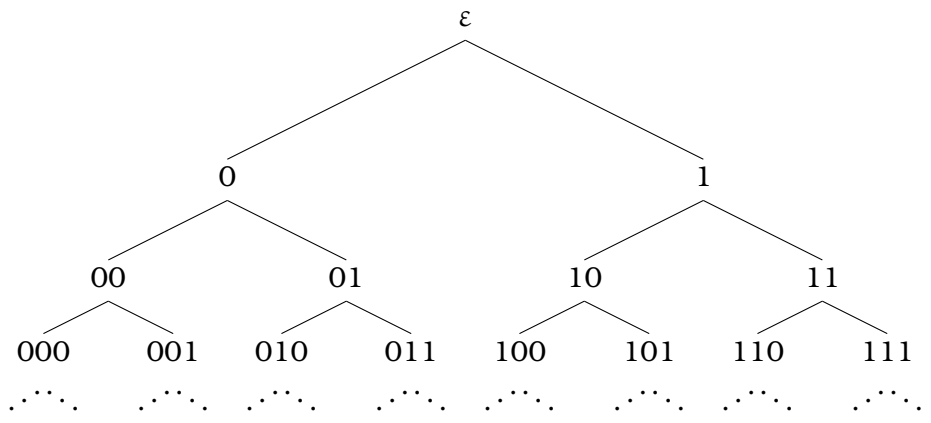
n**-οστό επίπεδο ενός δυαδικού δένδρου** καλείται το σύνολο όλων των μονοπατιών μήκους $n \in \mathbb{N}_0$ με πρώτη κορυφή τους τη ρίζα του δένδρου.

Άπειρο γράφημα/(2δικό)δένδρο καλείται κάθε γράφημα/(2δικό)δένδρο, με $|V| = +\infty$.

n**-οστό,** $n \in \mathbb{N}_0$**, επίπεδο του 2δικού δένδρου** T ορίζεται ως $\{(\varepsilon, x) \in T : x \in \{0,1\}^n\}$.

3.1.2 Η κατασκευή των ομάδων Grigorchyk

Θεωρείται το πλήρες άπειρο δυαδικό δένδρο $\mathcal{T}$ με ρίζα ε. Έστω $\mathcal{Y}$ το σύνολο όλων των μονοπατιών με απαρχή τη ρίζα ε. Κάθε στοιχείο $\gamma \in \mathcal{Y}$ μπορεί να αναπαρασταθεί μέσω μιας δυαδικής ακολουθίας $(\gamma_n)_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$, όπου ως 0 θα υποδηλώνεται η μετάβαση στον αριστερό απόγονο της τρέχουσας κορυφής κι ως 1 η μετάβαση στον δεξιό απόγονο της τρέχουσας κορυφής. Με άλλα λόγια, κάθε 0 υποδηλώνει μια αριστερή στροφή στο μονοπάτι και κάθε 1 υποδηλώνει μια δεξιά στροφή. Παρακάτω, διακρίνονται τα 3 πρώτα επίπεδα του απείρου πλήρους δυαδικού δένδρου με ρίζα



Έστω μια τριαδική ακολουθία $\chi = (\chi_n)_{n\in\mathbb{N}} \in \{0,1,2\}^{\mathbb{N}}$. Η **ομάδα Grigorchyk** G_χ είναι η ομάδα των μεταθέσεων των στοιχείων του $\mathcal{Y}$ η οποία παράγεται από τους εξής 4 αυτομορφισμούς $a, b_\chi, c_\chi, d_\chi \in \operatorname{Aut}\mathcal{T}$, η δράση* των οποίων καθορίζεται ακολούθως:

Ο αυτομορφισμός a δρα στην $(\gamma_1, \gamma_2, \ldots) \in \mathcal{Y}$ ανακλώντας την πρώτη στροφή, ήτοι

$$a(\gamma_1, \gamma_2, \ldots) = (1 - \gamma_1, \gamma_2, \ldots)$$

*$\operatorname{Aut}\mathcal{T} \times \{0,1,2\}^{\mathbb{N}} \longrightarrow \{0,1,2\}^{\mathbb{N}}$. μιας και ο εναλλακτικός ορισμός της G_χ είναι ο εξής: Η ομάδα G_χ είναι η υποομάδα της $\operatorname{Aut}\mathcal{T}$, η οποία παράγεται από τους $a, b_\chi, c_\chi, d_\chi$ (όπως αυτοί περιγράφονται παρακάτω.

Θεωρούνται τρεις ακολουθίες $U = (u_n)_{n\in\mathbb{N}}, V = (v_n)_{n\in\mathbb{N}}, W = (w_n)_{n\in\mathbb{N}} \in \{A, T\}^{\mathbb{N}}$ –όπου A σημαίνει "ανάκλαση" (της στροφής) και T σημαίνει "ταυτοτική" (:διατήρηση της στροφής ως έχει)– ως εξής:

$$\text{εάν } \chi_n = 0, \text{ τότε } \left\{\begin{array}{r} u_n = E \\ v_n = E \\ w_n = T \end{array}\right|, \quad \text{εάν } \chi_n = 1, \text{ τότε } \left\{\begin{array}{r} u_n = E \\ v_n = T \\ w_n = E \end{array}\right|, \quad \text{εάν } \chi_n = 2, \text{ τότε } \left\{\begin{array}{r} u_n = T \\ v_n = E \\ w_n = E \end{array}\right|$$

για κάθε $n \in \mathbb{N}$. Ο αυτομορφισμός b_χ δρα στην $(\gamma_1, \gamma_2, \ldots) \in \mathcal{Y}$ ως εξής:

$$b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots) = \left\{\begin{array}{r} (\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots), \quad \text{εάν } u_i = E \\ (\gamma_1, \ldots, \gamma_{i+1}, \ldots), \quad \text{αλλιώς} \end{array}\right.$$
$$(\text{όπου } i = \min\{j \in \mathbb{N} : \gamma_j = 0\})$$

(ή $v_i = E$, ή $w_i = E$ εάν στη θέση του b_χ είναι ο c_χ, ή ο d_χ αντιστοίχως). Με άλλα λόγια οι αυτομορφισμοί b_χ, c_χ, d_χ αφήνουν αναλλοίωτες τις στροφές $\gamma_1, \gamma_2, \ldots, \gamma_i$, όπου $i \in \mathbb{N}$ είναι η πρώτη αριστερή στροφή της ακολουθίας και ανακλούν τη στροφή γ_{i+1} εάν $u_i = E$, $v_i = E$, $w_i = E$ αντίστοιχα· σε κάθε άλλη περίπτωση η ακολουθία παραμένει αμετάβλητη.

Παράδειγμα 3.1. Έστω $\chi = \overline{012} = 012012012\ldots$, τότε

$i =$	1	2	3	4	5	6	7	8	9	…
$\chi =$	0	1	2	0	1	2	0	1	2	…
$U =$	E	E	T	E	E	T	E	E	T	…
$V =$	E	T	E	E	T	E	E	T	E	…
$W =$	T	E	E	T	E	E	T	E	E	…

Συνεπώς,

$$\begin{aligned} a(1,1,1,0,1,\ldots) &= (0,1,1,0,1,\ldots) \\ b_\chi(1,1,1,0,1,\ldots) = c_\chi(1,1,1,0,1,\ldots) &= (1,1,1,0,0,\ldots) \qquad (\text{αφού } u_4 = v_4 = E) \\ d_\chi(1,1,1,0,1,\ldots) &= (1,1,1,0,1,\ldots) \qquad (\text{αφού } w_4 = T) \end{aligned}$$

Εδώ συγκεκριμένα ισχύει ότι

- $(\forall \gamma \in \mathcal{Y})\big[[\min\{j \in \mathbb{N} : \gamma_j = 0\} \equiv 0 \mod 3] \implies b_\chi\gamma = \gamma\big]$·
- $(\forall \gamma \in \mathcal{Y})\big[[\min\{j \in \mathbb{N} : \gamma_j = 0\} \equiv 2 \mod 3] \implies c_\chi\gamma = \gamma\big]$·
- $(\forall \gamma \in \mathcal{Y})\big[[\min\{j \in \mathbb{N} : \gamma_j = 0\} \equiv 1 \mod 3] \implies d_\chi\gamma = \gamma\big]$·

λόγῳ της περιοδικότητας της $\chi \in \{0,1,2\}^{\mathbb{N}}$ (και κατ' επέκτασιν των $U, V, W \in \{T, E\}^{\mathbb{N}}$). ⊣

Λήμμα 3.2. *Έστω* $\chi \in \{0,1,2\}^{\mathbb{N}}$, *τότε ισχύουν τα εξής:*

(α΄) $a^2 = b_\chi^2 = c_\chi^2 = d_\chi^2 = 1_{G_\chi}$, *όπου* $(\forall \gamma \in \mathcal{Y})[1_{G_\chi}\gamma = \gamma]$.

(β΄) $b_\chi c_\chi = c_\chi b_\chi = d_\chi$, $b_\chi d_\chi = d_\chi b_\chi = c_\chi$ *και* $c_\chi d_\chi = d_\chi c_\chi = b_\chi$.

Απόδειξη. Θεωρείται μία $\gamma = (\gamma_1, \gamma_2, \ldots) \in \mathcal{Y}$ κι έστω ότι $i := \min\{j \in \mathbb{N} : \gamma_j = 0\}$ (:η πρώτη αριστερή στροφή της $\gamma \in \mathcal{Y}$).

(α΄) Κατ' αρχάς $a^2(\gamma_1, \gamma_2, \ldots) = \alpha(1-\gamma_1, \gamma_2, \ldots) = (1-(1-\gamma_1), \gamma_2, \ldots) = \gamma$. Εάν $u_i = E$, τότε

$$b_\chi^2(\gamma_1, \gamma_2, \ldots) = b_\chi\big(b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{u_i=E}{=} b_\chi(\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots)$$
$$\overset{u_i=E}{=} (\gamma_1, \ldots, \gamma_i, 1-(1-\gamma_{i+1}), \ldots) = (\gamma_1, \ldots, \gamma_{i+1}, \ldots).$$

Εάν δε $u_i = T$, τότε

$$b_\chi^2(\gamma_1, \gamma_2, \ldots) = b_\chi\big(b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{u_i=T}{=} b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots) \overset{u_i=T}{=} (\gamma_1, \ldots, \gamma_{i+1}, \ldots).$$

Παρόμοια είναι και η περιπτωσιολογία των $v_i \in \{T, E\}$ και $w_i \in \{T, E\}$ για τις δράσεις των c_χ και d_χ αντιστοίχως.

(β΄) Για το γεγονός $b_\chi c_\chi = c_\chi b_\chi = d_\chi$ διακρίνεται η κάτωθι περιπτωσιολογία:

- Εάν $\chi_i = 0$, τότε $u_i = v_i = E$ και $w_i = T$, άρα

$$b_\chi\big(c_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{v_i=E}{=} b_\chi(\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots) \overset{u_i=E}{=} (\gamma_1, \ldots, 1-(1-\gamma_{i+1}), \ldots) = \gamma$$
$$c_\chi\big(b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{u_i=E}{=} c_\chi(\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots) \overset{v_i=E}{=} (\gamma_1, \ldots, 1-(1-\gamma_{i+1}), \ldots) = \gamma$$
$$d_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots) \overset{w_i=T}{=} \gamma$$

- Εάν $\chi_i = 1$, τότε $u_i = w_i = E$ και $v_i = T$, άρα

$$b_\chi\big(c_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{v_i=T}{=} b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots) \overset{u_i=E}{=} (\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots)$$
$$c_\chi\big(b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{u_i=E}{=} c_\chi(\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots) \overset{v_i=T}{=} (\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots)$$
$$d_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots) \overset{w_i=T}{=} (\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots)$$

- Εάν $\chi_i = 2$, τότε $v_i = w_i = E$ και $u_i = T$, άρα

$$b_\chi\big(c_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{v_i=E}{=} b_\chi(\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots) \overset{u_i=T}{=} (\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots)$$
$$c_\chi\big(b_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots)\big) \overset{u_i=T}{=} c_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots) \overset{v_i=E}{=} (\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots)$$
$$d_\chi(\gamma_1, \ldots, \gamma_{i+1}, \ldots) \overset{w_i=E}{=} (\gamma_1, \ldots, 1-\gamma_{i+1}, \ldots)$$

Ανάλογη είναι και η περιπτωσιολογία για τις υπόλοιπες σχέσεις. □

3.1.3 Ιδιότητες των ομάδων Grigorchyk

Μερικές παρατηρήσεις για την ομάδα G_χ:

- Το σύνολο γεννητόρων μπορεί να περιοριστεί στο $\{a, b_\chi, c_\chi\}$.

  [Από το Λήμμα 3.2-(β') ισχύει ότι $d_\chi = b_\chi c_\chi$.]

- Η G_χ είναι πηλίκο της $\mathbb{Z}_2 * (\mathbb{Z}_2 \times \mathbb{Z}_2)$.

  [Εκπορεύεται από το γεγονός ότι το σύνολο $\{a, b_\chi, c_\chi\}$ παράγει την G_χ και πως η απεικόνιση $G_\chi \longrightarrow \mathbb{Z}_2 * (\mathbb{Z}_2 \times \mathbb{Z}_2)$, με

  $$a \longmapsto \Big([1]_2, \big([0]_2, [0]_2\big)\Big), \quad b_\chi \longmapsto \Big([0]_2, \big([1]_2, [0]_2\big)\Big), \quad c_\chi \longmapsto \Big([0]_2, \big([0]_2, [1]_2\big)\Big)$$

  αποτελεί επιμορφισμό (ήτοι κάθε γεννήτορας της G_χ στέλνεται στον γεννήτορα του εκάστοτε παράγοντα του γινομένου $\mathbb{Z}_2 * (\mathbb{Z}_2 \times \mathbb{Z}_2)$· εδώ $[x]_2 = \{2k + x \in \mathbb{Z} : k \in \mathbb{Z}\}$).]

- Από το Λήμμα 3.2 επάγεται ότι

  $$w \in G_\chi \iff \left\{ \begin{array}{l} w = 1_{G_\chi} \veebar w \in \{b_\chi, c_\chi, d_\chi\} \\ \qquad\qquad \veebar \left\{ \begin{array}{l} \big(\exists u_0, \ldots, u_{n+1} \in \{1_{G_\chi}, b_\chi, c_\chi, d_\chi\}\big) \\ \qquad \big[(u_1, \ldots, u_n \neq 1_{G_\chi}) \wedge (w = w_0 a w_1 \cdots w_n a w_{n+1})\big] \end{array} \right\} \end{array} \right.$$

- $\big(\forall r \in R(G_\chi)\big)[\partial_a(r) \equiv 0 \mod 2]$.

  [Γεωμετρικά, ο $a \in \operatorname{Aut} \mathcal{T}$ εναλλάσσει το αριστερό υποδένδρο (με ρίζα το 0) με το δεξιό υποδένδρο (με ρίζα το 1).]

Ορισμός 3.3. Έστω $\chi \in \{0, 1, 2\}^{\mathbb{N}}$. Κάθε λέξη της μορφής

$$u_0 a u_1 a u_2 \cdots u_n a u_{n+1} \in G_\chi \tag{3.1}$$

με $u_0, u_1, \ldots, u_n, u_{n+1} \in \{1_{G_\chi}, b_\chi, c_\chi, d_\chi\}$, με $u_1, \ldots, u_n \neq 1_{G_\chi}$, θα καλείται **ανηγμένη**.

Θεώρημα 3.4 ([Grig85], Πόρισμα 3.2 και Θεώρημα 6.2)**.** Θεωρείται μία $\chi \in \{0, 1, 2\}^{\mathbb{N}}$. Η ομάδα G_χ είναι άπειρη και προσεγγιστικά πεπερασμένη[†]. Επιπλέον, εάν τουλάχιστον 2 εκ των 0, 1, 2 επαναλαμβάνονται άπειρες φορές στην χ, τότε η G_χ

1. είναι απείρως παριστάμενη·

   [δηλαδή $G_\chi = \langle a, b_\chi, c_\chi, d_\chi \mid R \rangle$, με το $R \subseteq F\big(\{a, b_\chi, c_\chi, d_\chi\}\big)$ να είναι άπειρο]

2. έχει υπο-εκθετικό ρυθμό ανάπτυξης.

   [δηλαδή εάν $\#(n) := \Big|\{u_0 \cdots u_k \in G_\chi : u_0, \ldots, u_k \in \{a, b_\chi, c_\chi d_\chi\} \wedge k \leqslant n\}\Big|$, τότε $(\forall k \in \mathbb{R}_+^*)\big[\#(n) = o(k^n)\big]$]

[†][Εξ ορισμού] Για κάθε $w \in G_\chi$, υπάρχει πεπερασμένη ομάδα K και ομομορφισμός $\phi : G \to K$, με $\phi(w) \neq 1_K$. Αποδεικνύεται πως αυτό είναι ισοδύναμο με το ότι $\bigcap \{N \lhd G_\chi : |G_\chi : N| < +\infty\} = \{1_{G_\chi}\}$

Θεωρείται η μετάθεση $\sigma : \{0,1,2\}^{\mathbb{N}} \longrightarrow \{0,1,2,\}^{\mathbb{N}}$, με $(\chi_n)_{n\in\mathbb{N}} \overset{\sigma}{\longmapsto} (\chi_{n+1})_{n\in\mathbb{N}}$. Ορίζεται $G_1 := G_\chi$ και $G_{n+1} := G_{\sigma^n(\chi)}$, $n \in \mathbb{N}$. Οι γεννήτορές της ομάδος G_n θα συμβολίζονται ως a, b_n, c_n, d_n (ήτοι $\zeta_{n+1} = \zeta_{\sigma^n(\chi)}$, για $\zeta \in \{b,c,d\}$). Για κάθε $n \in \mathbb{N}_0$ θεωρείται η

$$H_n := \{w \in G_n : \partial_a(w) \equiv 0 \mod 2\} \leqslant G_n$$

Προφανώς:

- $|G_n : H_n| = 2$.
  [$G_n = H_n \cup aH_n$, με $aH_n = \{w \in G_n : \partial_a(w) \equiv 1 \mod 2\}$ και $H_n \cap aH_n = \varnothing$.]
- $H_n = \langle b_n,\ c_n,\ d_n,\ ab_na,\ ac_na,\ ad_na\rangle$.
  [Κατ' αρχάς το ∂_a σε κάθε έναν από τους παραπάνω όρους είναι άρτιο και η συγκόλλησή τους μπορεί να παράξει λέξεις μόνον με άρτιο ∂_a.]

Για κάθε $n \in \mathbb{N}$, περιορίζοντας τη δράση της H_n στο δεξιό και αριστερό υποδένδρο του $\mathcal{T}$ –ήτοι στα υποδένδρα του $\mathcal{T}$ με ρίζα το 0 και το 1 αντίστοιχα– επάγονται δύο ομομορφισμοί $\phi_0^{(n)}, \phi_1^{(n)} : H_n \longrightarrow G_{n+1}$ τέτοιοι ώστε:

(α') $w = 1_{H_n}$ εάν και μόνον εάν $\left(\phi_0^{(n)}(w),\ \phi_1^{(n)}(w)\right) = (1_{G_{n+1}}, 1_{G_{n+1}})$ και

(β') $\left|\phi_0^{(n)}(w)\right|, \left|\phi_1^{(n)}(w)\right| \leqslant \lceil w/2 \rceil$

και η δράση των οποίων περιγράφεται από τον ακόλουθο πίνακα:

	b_n	c_n	d_n	ab_na	ac_na	ad_na
$\phi_0^{(n)}$	$\overline{u}_n$	$\overline{v}_n$	$\overline{w}_n$	b_{n+1}	c_{n+1}	d_{n+1}
$\phi_1^{(n)}$	b_{n+1}	c_{n+1}	d_{n+1}	$\overline{u}_n$	$\overline{v}_n$	$\overline{w}_n$

Πίνακας 3.1: Η δράση των ομομορφισμών $\phi_0^{(n)}, \phi_1^{(n)}$. Εδώ είναι $\overline{u}_n = \begin{cases} a, \text{ αν } u_n = E \\ 1_{G_{n+1}}, \text{ αν } u_n = T \end{cases}$ (και αντίστοιχα για τα $\overline{v}_n, \overline{w}_n$)

3.2 Το πρωτόκολλο των Garzon-Zalcstein

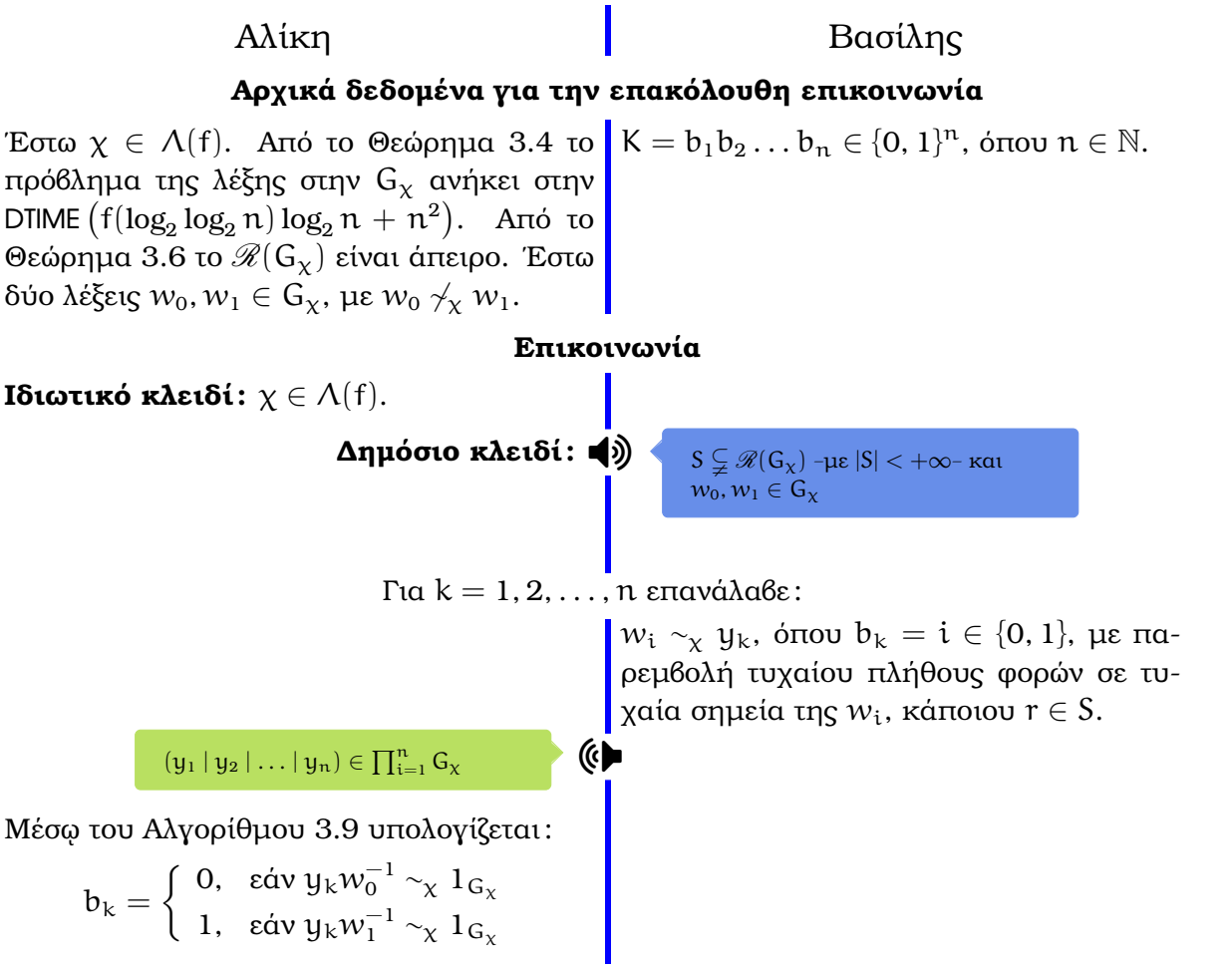
Ορισμός 3.5 ([GZ85], Ορισμός 3.1)**.** Έστω $f : \mathbb{N} \to \mathbb{N}$ μία μη-φθίνουσα συνάρτηση και μία ακολουθία $\chi = (\chi_j)_{j\in\mathbb{N}} \in \{0,1,2\}^{\mathbb{N}}$. Θα ισχύει ότι $\chi \in \mathsf{DTIME}(f)$ εάν υπάρχει αιτιοκρατική μηχανή Turing που υπολογίζει το $\chi_j \in \{0,1,2\}$ σε χρόνο $\mathcal{O}(f(n))$, όπου $n = \lceil \log_2 j \rceil + 1$ το πλήθος των δυφίων (bit) του δείκτη της θέσης. [Ανάλογοι ορισμοί υφίστανται και για χωρικές και για αναιτιοκρατικές κλάσεις πολυπλοκότητος.]

Συμβολισμός. $\Lambda(f) := \{\chi \in \{0,1,2\}^{\mathbb{N}} : \chi \in \mathsf{DTIME}(f)$, ακριβώς δύο ψηφία εμφανίζονται άπειρες φορές$\}$.

Συμβολισμός. $u \sim_\chi v \iff_{\text{ορ}} \left\{ \begin{array}{c} \text{υπάρχει ακολουθία } w_0, w_1, \ldots, w_n \in G_\chi \text{ ώστε } w_0 = u, \\ w_n = v \text{ και το } w_i \text{ προκύπτει από το } u_{i-1} \text{ με παρεμβολή} \\ \text{ή διαγραφή όρων του συνόλου } \mathscr{R}(G_\chi) \ (i = 1, \ldots, n). \end{array} \right]$.

Θεώρημα 3.6 ([GZ85], Θεώρημα 3.2)**.** Έστω $\chi \in \{0,1,2\}^{\mathbb{N}}$ και $f : \mathbb{N} \to \mathbb{N}$ μία μη-φθίνουσα συνάρτηση.

1. Εάν $\chi \in \mathsf{DSPACE}(f)$, τότε το πρόβλημα της λέξης στην ομάδα G_χ ανήκει στην κλάση $\mathsf{DSPACE}\big(\log_2 n + f(\log_2 \log_2 n)\big)$. Αντίστοιχα για $\chi \in \mathsf{NSPACE}(f)$.
2. Εάν $\chi \in \mathsf{DTIME}(f)$, τότε το πρόβλημα της λέξης στην ομάδα G_χ ανήκει στην κλάση $\mathsf{DTIME}\big(f(\log_2 \log_2 n)\log_2 n + n^2\big)$. Αντίστοιχα για $\chi \in \mathsf{NTIME}(f)$.



Σχήμα 3.1: Το σχήμα ανταλλαγής κλειδιού Garzon-Zalcstein

Μερικές παρατηρήσεις:

- Εάν $f = \mathcal{O}\left(2^{2^{n+1}-n}\right)$, τότε το πρόβλημα της λέξης στην G_χ ανήκει στην $\mathsf{DTIME}(n^2)$.
- Έστω πως επιλέγονται δύο λέξεις $x, y \in G_\chi$, με $|x|, |y| \leqslant n^r$ για $r \in \mathbb{R}_+^*$, στη τύχη. Η πιθανότητα ώστε $x \sim_\chi y$ είναι υποεκθετικά μικρή. Συνεπώς, το σχήμα μπορεί να υλοποιηθεί σε "λογικό" χρόνο.

  [Έστω $B[n] := \left\{\{y \in G_\chi : x \sim_\chi y\} \subseteq G_\chi : x \in G_x \wedge (\exists r \in \mathbb{R}_+^*)\left[|x| \leqslant n^r\right]\right\}$, τότε για τη συνάρτηση αύξησης μεγέθους των στοιχείων $\rho : \mathbb{N} \to \mathbb{N}$ της G_χ είναι $\rho(n) = \left|B[n]\right|$. Συνεπώς, $\mathsf{Prob}\left[w \sim_\chi 1_{G_\chi} \wedge w \in B[n]\right] = 1/\rho(n)$. Έχοντας η G_χ υποεκθετικό ρυθμό αύξησης [Θεώρημα 3.4], το ζητούμενο έπεται.]

3.2.1 Εικασίες ασφαλείας

Οι εισηγητές στηρίζουν τη δύναμη του σχήματος στα εξής σημεία:

(1) Η πληροφορία $\{w_0, w_1, S\}$ δεν επαρκεί για τον προσδιορισμό της ομάδος G_χ.

[Κατ' αρχάς η G_χ, $\chi \in \Lambda(f)$, είναι απείρως παριστάμενη [Θεώρημα 3.4]. Έτσι, κανένα πεπερασμένο σύνολο γεννητόρων και λέξεων w_0, w_1 δεν προσδιορίζουν πλήρως την G_χ. Ακόμη κι αν βρεθεί ομάδα $K = \langle x, y, z, u \mid S\rangle$, με $w_0 \not\sim w_1$ στην K. Επεκτείνοντας την K ώστε να προκύψει κάποια G_ξ, $\xi \in \Lambda(f)$, ενδέχεται να προκύψει:

- $w_0 \sim_\xi w_1$ λόγῳ του απείρου πλήθους των πιθανών ανεξάρτητων συσχετιστών.
- δύσκολα επιλύσιμο πρόβλημα της λέξης στην G_ξ.]

(2) Δεν απαιτείται κάποια ομάδα αριθμών ως υπόβαθρο του σχήματος. Δεν γίνεται χρήση ομομορφικής κρυπτογράφησης.

[Χρήση των παραπάνω θα παρείχε κρυπταναλυτικά εργαλεία. Έτσι το σχήμα καθίσταται ασφαλέστερο του RSA στις εν λόγῳ επιθέσεις.]

(3) Επειδή απαιτείται πεπερασμένο πλήθος ($\leqslant \left\lceil \log_2 |w| \right\rceil$ [Θεώρημα 3.10]) ψηφίων της $\chi \in \Lambda(f)$ έπεται πως υπάρχουν πολυωνυμικά πολλά υποψήφια κλειδιά αποκρυπτογράφησης. Όμως δεν είναι εύκολο να εξακριβωθεί εάν ένα τέτοιο κλειδί είναι το σωστό καθότι η πραγματική ακολουθία $\chi \in \Lambda(f)$ δεν καθορίζεται μοναδικά. Έτσι πρέπει να χρησιμοποιηθεί επιλεγμένο γνωστό κρυπτοκείμενο ώστε να καθορισθεί πιο από τα υποψήφια κλειδιά είναι το σωστό· επίθεση που αποτυγχάνει από τη φύση του προβλήματος της λέξης: μία επιτυχημένη αποκρυπτογράφηση δεν εγγυάται πως έχει βρεθεί το σωστό κλειδί.

(4) Μόνον πεπερασμένο πλήθος ψηφίων της ακολουθίας $\chi \in \Lambda(f)$ απαιτούνται για την αποκρυπτογράφηση. Άρα, το δημόσιο κλειδί δύναται να αλλάξει –δίχως να αλλάξει το ιδιωτικό– αλλάζοντας τις $w_0, w_1 \in G_\chi$, το $S \subseteq \mathscr{R}(G_\chi)$ και/ή κάποια ψηφία της χ.

3.3 Κρυπτανάλυση

Σύμβαση. *Για λόγους απλοποίησης των υπολογισμών, εφεξής, δεν θα λαμβάνεται υπόψιν η υπολογιστική πολυπλοκότητα της ακολουθίας* $\chi \in \{0,1,2\}^{\mathbb{N}}$.

Κατ' αρχάς μία βασική

Παρατήρηση 3.7. *Πρέπει* $\partial_a(w_0) \equiv \partial_a(w_1) \mod 2$ *(αμφότερα περιττά, ή άρτια).*

Έστω πως δεν είναι κι έστω ότι $\partial_a(w_0) = 2m$ και $\partial_a(w_1) = 2n+1$, για $m, n \in \mathbb{N}$. Ισχύει ότι $\big(\forall r \in \mathscr{R}(G_\chi)\big)[\partial_a(r) \equiv 0 \mod 2]$, δηλαδή η εισαγωγή συσχετιστών αυξάνει κατά άρτιο πλήθος τις εμφανίσεις του γεννήτορα $a \in G_\chi$. Έτσι εάν $w_* \in G_\chi$ είναι το κρυπτοκείμενο, τότε $w_* = \begin{cases} w_0 & \text{εάν } \partial_a(w_*) \equiv 0 \mod 2 \\ w_1 & \text{αλλιώς} \end{cases}$, δηλαδή αποκρυπτογραφήθηκε.

Θεώρημα 3.8. Θεωρούνται μία $\chi \in \{0,1,2\}^{\mathbb{N}}$, ένα $n \in \mathbb{N}$ καθώς και μία ανηγμένη λέξη $w \in G_n$, όπου το $\partial_a(w)$ είναι άρτιο. Εάν $\partial_a(w) < \partial_{b_n,c_n,d_n}(w)$ (αντιστοίχως $>$, $=$), τότε $\phi_0^{(n)}(w), \phi_1^{(n)}(w) \leqslant \lceil |w|/2 \rceil$ (αντιστοίχως $\lfloor |w|/2 \rfloor$, $|w|/2$).

Απόδειξη. Όντας η w ανηγμένη στην G_n, τότε θα είναι της μορφής (3.1), ήτοι

$$w = u_0\, a * a * \cdots * a\, u_k$$

όπου $* \in \{b_n, c_n, d_n\}$, $u_0, u_k \in \{1_{G_n}, b_n, c_n, d_n\}$. Όντας $\partial_a(w) < \partial_{b_n,c_n,d_n}(w)$, τα $|w|-1$ πρώτα στοιχεία της w μπορεί να διαμερισθούν σε τετράδες της μορφής $*\,a*a$ (κι αν $* = u_0$, τότε ενδέχεται και $u_0 = 1_{G_\chi}$) και να περισσέψει το u_k. Ισχύει ότι

$$\phi_0^{(n)}(*\,a*a) = \phi_0^{(n)}(*)\phi_0^{(n)}(a*a) \qquad \phi_1^{(n)}(a*a) = \phi_1^{(n)}(*)\phi_1^{(n)}(a*a)$$

($\phi_0^{(n)}, \phi_1^{(n)}$ ομομορφισμοί)

$$\in \{a\bullet, \bullet\} \qquad \in \{\bullet a, \bullet\} \qquad \text{(Πίνακας 3.1)}$$

όπου $\bullet \in \{b_{n+1}, c_{n+1}, d_{n+1}\}$. Εάν $u_0 = 1_{G_n}$, τότε

$$\phi_0^{(n)}(1_{G_n}\, a*a) = \phi_0(a*a) \qquad \phi_1^{(n)}(1_{G_n}\, a*a) = \phi_1^{(n)}(a*a)$$

$$\in \{\bullet\} \qquad \in \{a, 1_{G_n}\} \qquad \text{(Πίνακας 3.1)}$$

δηλαδή οι $\phi_0^{(n)}, \phi_1^{(n)}$ απεικονίζουν λέξεις μήκους 4 σε λέξεις μήκους το πολύ 2. Τέλος,

$$\phi_i^{(n)}(u_k) \in \begin{cases} \{1_{G_{n+1}}\}, & \text{εάν } u_k = 1_{G_n} \text{ (αφού ο } \phi_i^{(n)} : H_n \to G_{n+1} \text{ είναι ομομορφισμός)} \\ \{\bullet\}, & \text{εάν } u_k \in \{b_n, c_n, d_n\} \text{ και } i = 0 \\ \{1_{G_{n+1}}, a\}, & \text{εάν } u_k \in \{b_n, c_n, d_n\} \text{ και } i = 1 \end{cases}$$

δηλαδή οι $\phi_0^{(n)}, \phi_1^{(n)}$ απεικονίζουν λέξεις μήκους 1 σε λέξεις μήκους 1.

Υπάρχουν $\dfrac{\partial(w)-1}{4}$ τετράδες στην w, άρα

$$\left|\phi_i^{(n)}(w)\right| \leqslant 2\frac{|w|-1}{4}+1 = \frac{|w|-1}{2}+1 = \frac{|w|+1}{2} = \left\lceil\frac{|w|}{2}\right\rceil \qquad (i=0,1)$$

Η απόδειξη για τα ενδεχόμενα $>, =$ είναι παρόμοια. □

Αλγόριθμος 3.9 `WPSA`(χ, w): Αλγόριθμος Επίλυσης του Προβλήματος της Λέξης.

Είσοδος: $\chi \in \{0,1,2\}^{\mathbb{N}}$ και $w \in G_\chi$.

Δεδομένα: Η δράση των ομομορφισμών $\phi_0^{(n)}, \phi_1^{(n)} : H_n \to G_{n+1}$, όπως περιγράφεται στον πίνακα 3.1.

Έξοδος: 1 εάν $w = 1_{G_\chi}$, 0 αλλιώς.

1: **εάν** $(\partial_a \not\equiv 0 \mod 2)$ **τότε**
2: **επίστρεψε** 0;
3: **τέλος εάν**
4: $w_r \rightsquigarrow w$; /* Αναγωγή στην ανηγμένη μορφή της w (βλ. μορφή (3.1)) */
/* Οριακές Συνθήκες */
5: **εάν** $(w = 1_{G_\chi})$ **τότε**
6: **επίστρεψε** 1; /* Οριακή συνθήκη: Φύλλο του δένδρου $= 1_{G_\chi}$ */
7: **αλλιώς εάν** $(w \in \{b_\chi, c_\chi, d_\chi\})$ **τότε**
8: **επίστρεψε** 0; /* Οριακή συνθήκη: Φύλλο του δένδρου $\neq 1_{G_\chi}$ */
9: **τέλος εάν**
/* Διαίρει και Βασίλευε */
10: **εάν** $\Big(\texttt{WPSA}\big(\sigma(\chi),\, \phi_0\big(\sigma(\chi), w_r\big)\big),\ \texttt{WPSA}\big(\sigma(\chi),\, \phi_1\big(\sigma(\chi), w_r\big)\big)\Big) = (1,1)$ **τότε**
11: **επίστρεψε** 1;
12: **αλλιώς**
13: **επίστρεψε** 0;
14: **τέλος εάν**

Πολυπλοκότητα του Αλγορίθμου 3.9: Κάθε λέξη w αναλύεται σε δύο υπολέξεις $\phi_0^{(n)}(w)$ και $\phi_1^{(n)}$, με $\left|\phi_0^{(n)}(w)\right|, \left|\phi_0^{(n)}(w)\right| \leqslant \lceil |w|/2 \rceil$ [Θεώρημα 3.8], άρα ο αλγόριθμος καλείται να επιλύσει δύο προβλήματα τάξης μεγέθους το πολύ το ήμισυ του αρχικού. Η εφαρμογή των ομομορφισμών $\phi_0^{(n)}, \phi_1^{(n)} : H_n \longrightarrow G_{n+1}$ απαιτεί την γνώση όλων των γραμμάτων της λέξης w, έτσι είναι γραμμικού υπολογιστικού κόστους. Συνεπώς,

$$T\big(|w|\big) = 2T\big(|w|/2\big) + \mathcal{O}\big(|w|\big)$$

απ' όπου προκύπτει πως η πολυπλοκότητα του Αλγορίθμου 3.9 είναι $\mathcal{O}(|w| \log_2 |w|)$.⊣

Συμβολισμός. Έστω $\chi \in \{0,1,2\}^{\mathbb{N}}$ και $w \in G_\chi$. Θα συμβολίζεται

- ως M_w^χ ο ακριβής αριθμός των αρχικών ψηφίων που χρειάζεται ο $\texttt{WPSA}(\chi, w)$ (Αλγόριθμος 3.9) να περατωθεί. Ισχύει ότι $M_w^\chi \leqslant \left\lceil \log_2 |w| \right\rceil$ [Θεώρημα 3.10].
- ως $\Omega_w := \left\{\chi \in \{0,1,2\}^{\mathbb{N}} \mid w \sim_\chi 1_{G_\chi}\right\}$.
- ως $M_w := \min\{M_w^\chi \in \mathbb{N} \mid \chi \in \Omega_w\}$.

Θεώρημα 3.10. Έστω $\chi \in \{0,1,2\}^{\mathbb{N}}$ και $w \in G_\omega$. $M_w^\chi \leqslant \left\lceil \log_2 |w| \right\rceil$. Επίσης M_w^χ είναι και το ύψος του δυαδικού δένδρου που κατασκευάζει ο Αλγόριθμος 3.9.

Απόδειξη. Κατά τη δράση των ομομορφισμών $\phi_0^{(i)}, \phi_1^{(i)} : H_i \longrightarrow G_{i+1}$ απαιτείται γνώση του i-οστού ψηφίου της χ. Έστω $n \in \mathbb{N}$ το πλήθος των επιπέδων του δυαδικού δένδρου που κατασκευάζει ο Αλγόριθμος 3.9. Το n επιτυγχάνεται όταν ο αλγόριθμος έχει δημιουργήσει ένα δυαδικό δένδρο ύψους n με τετριμμένα φύλλα. Έστω ότι υπάρχουν n επίπεδα, τότε:

⟦*1ο επίπεδο*⟧: Από το Θεώρημα 3.8 οι λέξεις που προκύπτουν είναι το πολύ μήκους $\left\lceil |w|/2 \right\rceil$ και κάθε μία έχει άρτιο πλήθος εμφανίσεων του γεννήτορα $a \in G_\chi$, ειδ' άλλως ο αλγόριθμος τερματίζει νωρίτερα του n.

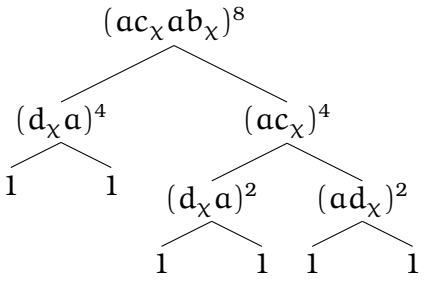
⟦*2ο επίπεδο*⟧: Από το Θεώρημα 3.8 οι λέξεις που προκύπτουν είναι το πολύ μήκους $\left\lceil \left\lceil |w|/2 \right\rceil /2 \right\rceil = \left\lceil |w|/2^2 \right\rceil$ και κάθε μία έχει άρτιο πλήθος εμφανίσεων του γεννήτορα a, ειδ' άλλως ο αλγόριθμος τερματίζει νωρίτερα του n.

$\vdots$

⟦n-*οστό* επίπεδο⟧: Από το Θεώρημα 3.8, οι λέξεις που προκύπτουν είναι το πολύ μήκους $\left\lceil \left\lceil |w|/2^{n-1} \right\rceil /2 \right\rceil = \left\lceil |w|/2^n \right\rceil = 1$, αφού ο αλγόριθμος τερματίζει. Συνεπώς, $\left\lceil |w|/2 \right\rceil = 1 \implies |w| < 2^n \implies \log_2 |w| < n \implies n = \left\lceil \log_2 |w| \right\rceil$. □

Παράδειγμα 3.11. Το παρακάτω

$$\texttt{WPSA}\left(\overline{012},\, (ac_\chi ab_\chi)^8\right) =$$



είναι το δένδρο που σχηματίζει ο Αλγόριθμος 3.9. Στο επίπεδο $n \in \mathbb{N}_0$ ο αριστερός (αντ. δεξιός) απόγονος προκύπτει με την εφαρμογή του ομομορφισμού $\phi_0^{(n+1)}$ (αντ. $\phi_1^{(n+1)}$) στον πρόγονο. Επαληθεύεται ότι $M^\chi_{(ac_\chi ab_\chi)^8} = 3 \leqslant 5 = \log_2 32 = \log_2 \left|(ac_\chi ab_\chi)^8\right|$ ⊣

Θεώρημα 3.12. Δοσμένης μιας λέξεως $w \in G_\chi$, υπάρχει αλγόριθμος που για κάθε ακολουθία του Ω_w –εάν υπάρχουν– εμφανίζει τα M_w^χ πρώτα ψηφία της.

Απόδειξη. Ο αλγόριθμος είναι ο

Αλγόριθμος 3.13 `ISSA`(w): Αλγόριθμος εύρεσης Αρχικών Τμημάτων Ακολουθιών.

Είσοδος: $w \in G_\chi$

Δεδομένα: Η δράση των ομομορφισμών $\phi_0^{(n)}, \phi_1^{(n)} : H_n \to G_{n+1}$, όπως περιγράφεται στον πίνακα 3.1.

Έξοδος: Τα M_w^χ πρώτα ψηφία κάθε ακολουθίας του Ω_w.

```
1: i ← 2; χ[1] ← 0; ξ ←(τυχαία επιλογή)− {0,1,2}^ℕ; χ ← (χ[1], ξ); Q[1] ← {w};/* Αρχικοποιήσεις */
2: όσο (χ[1] ≠ 3) επανάλαβε
3:    WPSA_res ← WPSA((χ[1],...,χ[i−1],ξ), w);
4:    εάν ((∃F ∈ Q[i−1])[∂_a(F) ≢ 0 mod 2] ∨ [WPSA_res = 1]) τότε
5:       χ[i−1] ← χ[i−1] + 1;
6:       εάν (WPSA_res = 1) τότε εκτύπωσε χ[1],...,χ[i−1];
7:    αλλιώς εάν (χ[i−1] = 3) τότε
8:       χ[i−2] ← χ[i−2] + 1;
9:       i ← i−1; /* "Διαγραφή" τρέχοντος όρου-Μετάβαση στον προηγούμενο "γύρο" */
10:   αλλιώς
11:      χ[i] ← 0; Q[i] ← {φ_0^(i)(F), φ_1^(i)(F) ∈ G_i : F ∈ Q[i−1]};
12:      i ← i+1;                          /* Μετάβαση στον επόμενο "γύρο" */
13:   τέλος εάν
14: τέλος όσο
```

και τερματίζει όταν $\chi_1 = 3$.

Κάθε εκτύπωσης έχει προηγηθεί μια επιτυχής έκβαση του Αλγορίθμου 3.9. Έτσι εμφανίζονται οι M_w^χ πρώτοι όροι μιας $\chi \in \Omega_w$. Εάν $\Omega_w = \varnothing$, τότε $\chi_1 = 3$ –διότι $(\forall j \in \{0,1,2\})[\text{WPSA\_res} \equiv \texttt{WPSA}((j,\xi), w) \neq 1]$– χωρίς εκτυπώσιμα αποτελέσματα. □

Ένα υπολογιστικό φράγμα για τον Αλγόριθμο 3.13: Ο Αλγόριθμος 3.13 εμφανίζει αποτελέσματα σε "λογικά πλαίσια" –και για μεγάλες τιμές του $|w|$– αφού τυπώνει το πολύ $3^{\lceil \log_2 |w| \rceil} \leqslant |w|^{\log_2 3} \leqslant |w|^2$ ακολουθίες [$|\{0,1,2\}| = 3$ και Θεώρημα 3.10]. ⊣

3.3.1 Επίθεση μετά υλοποιήσεως

Έστω $n \in \mathbb{N}$ η παράμετρος ασφαλείας και έστω ότι το δημόσιο κλειδί συνίσταται στο $r_1, r_2, \ldots, r_n \in R(G_\chi)$ και $w_0, w_1 \in G_\chi$. Σκοπός είναι η εύρεση (αρχικού τμήματος) της ακολουθίας $\chi \in \{0,1,2\}^\mathbb{N}$ (και τότε θα είναι $r_1 = \ldots = r_n = 1_{G_\chi}$ και $w_0 \not\sim_\chi w_1$ στην G_χ).

> Έστω $n = 3$ και θεωρούνται οι συσχετιστές $r_1 = (ab)^4$, $r_2 = (abab)^8$, $r_3 = (bada)^8$ καθώς και οι λέξεις $w_0 = (bacabacacaca)^2 bacab$ και $w_1 = acacacabacabacacaca$.

Με εφαρμογή του Αλγορίθμου 3.13 στη λέξη $u := w_0^{-1}w_1$, προκύπτουν τα M_u^χ πρώτα στοιχεία κάθε ακολουθίας $\chi \in \Omega_u$. Αυτές πρόκειται να συνθέσουν τη λίστα των **μη-αποδεκτών αρχικών τμημάτων** ακολουθιών. Οι ακολουθίες είναι μη αποδεκτές καθότι

$$(\forall \chi \in \Omega_u)(\forall w \in G_\chi)\big(\forall i \in \{0,1\}\big)\big[\big((w_* \sim_\chi w_0) \vee (w_* \sim_\chi w_1)\big) \implies w_* w_i^{-1} = 1_{G_\chi}\big]$$

αφού

$$w_* w_i^{-1} = \begin{cases} w_* w_0^{-1} \ (\text{για } i = 0) \sim_\chi \begin{cases} w_0 w_0^{-1} & (\text{εάν } w_* \sim_\chi w_0) \quad = 1_{G_\chi} \\ w_1 w_0^{-1} = u \ (\text{εάν } w_* \sim_\chi w_1) & \sim_\chi 1_{G_\chi} \ (\text{αφού } \chi \in \Omega_u) \end{cases} \\ w_* w_1^{-1} \ (\text{για } i = 1) \sim_\chi \begin{cases} w_0 w_1^{-1} = u \ (\text{εάν } w_* \sim_\chi w_0) & \sim_\chi 1_{G_\chi} \ (\text{αφού } \chi \in \Omega_u) \\ w_1 w_1^{-1} & (\text{εάν } w_0 \sim_\chi w_1) \quad = 1_{G_\chi} \end{cases} \end{cases}$$

ήτοι δεν υπάρχει διάκριση των w_0, w_1. Εάν είναι $\Omega_u = \varnothing$, τότε η λίστα είναι κενή.

Εφαρμόζοντας τον Αλγόριθμο 3.13 στη λέξη $w_0^{-1}w_1$ προκύπτει η λίστα των *μη-αποδεκτών* αρχικών τμημάτων για την ακολουθία χ:

1. 01
2. 1
3. 21

Κατόπιν γίνεται εφαρμογή του Αλγορίθμου 3.13 σε κάθε στοιχείο $r_1, \ldots, r_n$ (ώστε να βρεθούν τα αρχικά τμήματα των ακολουθιών που καθιστούν τετριμμένο (:συσχετιστή) το κάθε r_i, $i = 1, 2, \ldots, n$). Εν συνεχεία συναληθεύονται τα αρχικά τμήματα που προκύπτουν, ώστε να συνθέσουν τη λίστα των **υποψηφίων αρχικών τμημάτων** ακολουθιών· η οποία είναι μη-κενή, καθότι περιέχει αρχικό τμήμα της ακολουθίας του μυστικού κλειδιού.

Εφαρμόζοντας τον Αλγόριθμο 3.13 σε κάθε ένα από τα r_1, r_2, r_3 προκύπτουν για τον καθένα μία λίστα με αρχικά υποψήφια τμήματα για την ακολουθία χ:

$\texttt{ISSA}(r_1) =$	2							
$\texttt{ISSA}(r_2) =$	012	021	101	11	121	202	212	22
$\texttt{ISSA}(r_3) =$	00	010	020	102	120	202	212	22

και συναληθεύοντας όλα τα παραπάνω αρχικά τμήματα, προκύπτει πως η λίστα με τα *υποψήφια* αρχικά τμήματα της ακολουθίας χ είναι η:

1. 202
2. 212
3. 22

Εξετάζονται ένα προς ένα τα στοιχεία της λίστας υποψηφίων αρχικών τμημάτων ακολουθιών και αποδέχονται/απορρίπτονται σύμφωνα με την ακόλουθη περιπτωσιολογία: Έστω p το πλήθος των ψηφίων του τρέχοντος στοιχείου προς εξέταση.

Περίπτωση 1: Εάν υπάρχει (τουλάχιστον) στοιχείο της λίστας μη-αποδεκτών αρχικών τμημάτων με περισσότερα των p στοιχεία και τα p πρώτα ψηφία συμπίπτουν με τα p ψηφία του εξεταζόμενου –εν περιπτώσει που υπάρχουν πολλά στοιχεία, επιλέγεται το μικρότερο σε μήκος· έστω μήκους k, το υποψήφιο αρχικό τμήμα καθίσταται αποδεκτό με την αυθαίρετη προσθήκη ψηφίων, προσέχοντας πως τα πρώτα $k - p$ πρώτα αυθαίρετα ψηφία να μην συμπίπτουν με τα $k - p$ τελευταία ψηφία του αρχικού τμήματος που έχει επιλεχθεί για αντιπαράθεση από τη λίστα των μη-αποδεκτών αρχικών τμημάτων.

Περίπτωση 2: Εάν υπάρχει στοιχείο της λίστας μη-αποδεκτών αρχικών τμημάτων με $k \leqslant p$ στοιχεία και τα ψηφία αυτά συμπίπτουν με τα k αρχικά ψηφία του εξεταζόμενου υποψηφίου, τότε το υποψήφιο αρχικό τμήμα απορρίπτεται.

Περίπτωση 3: Εάν η λίστα μη-αποδεκτών αρχικών τμημάτων ακολουθιών είναι κενή, ή δεν συμβαίνει καμμία από τις παραπάνω περιπτώσεις, τότε το υποψήφιο αρχικό τμήμα καθίσταται αποδεκτό.

> Ο υποψήφιος 212 εμπίπτει στην Περίπτωση 2 παραπάνω και δι αυτό απορρίπτεται. Οι αποψήφιοι 202 και 22 εμπίπτουν στην Περίπτωση 3 και δι αυτό καθίστανται αποδεκτοί· και με τη συμπλήρωση στο τέλος με αυθαίρετα επιλεγμένων στοιχείων του συνόλου $\{0, 1, 2\}$ μετατρέπονται σε κλειδιά κατάλληλα προς *απο*κρυπτογράφηση.

Έστω ξ το αρχικό τμήμα της ακολουθίας που προκύπτει ύστερα απ' όλα τα παραπάνω. Εάν $w_* \in G_\chi$ είναι το κρυπτοκείμενο, τότε ισχύει ότι

$$\texttt{WPSA}\big(\xi, \{0,1,2\}^{\mathbb{N}}\big),\, w_* w_i^{-1}) = \begin{cases} 1, & \text{εάν } w_* \sim_\chi w_i \text{ στην } G_\chi \\ 0, & \text{αλλιώς} \end{cases} \qquad (i = 0, 1)$$

αφού οι $\chi, \xi \in \{0, 1, 2\}^{\mathbb{N}}$ συμφωνούν στα πρώτα M_{w_*} ψηφία τους.

Κεφάλαιο 4

Λέξεων επόμενα. . .

Την κατακλείδα του ταξιδιού στον κόσμο του προβλήματος της λέξης την συνθέτουν μερικά πιο εξεζητημένα σχήματα ανταλλαγής κλειδιού: των Birget-Μαγκλιβέρα-Sramka και των Shpilrain-Zapata. Παρουσιάζεται επίσης μια άλλη δυνατότητα της Μη-Μεταθετικής Κρυπτογραφίας: το μοίρασμα του μυστικού. Η έννοια απαντάται αρχικά στην Μεταθετική Κρυπτογραφία, από τον Adi Shamir στο [Sh79]. Τέλος, προτείνονται κάποιες (ημι)ομάδες [πέραν των ομάδων πλεξίδων] για τα σχήματα του Κεφαλαίου.

4.1 Ένα σχήμα ανταλλαγής κλειδιού με κυκλώματα

4.1.1 Λογικά κυκλώματα και η ομάδα gp $\left(G_{3,1}^{\mathrm{mod}\,3}(0,1;\#)\cup\{\kappa_{321}\}\right)$

Ορισμός 4.1. Στο κατευθυνόμενο γράφημα (V,E) ορίζονται $\mathrm{In}(v):=\{u\in V:(u,v)\in E\}$, $\mathrm{indeg}(v):=\left|\mathrm{In}(v)\right|$, $\mathrm{Out}(v):=\{u\in V:(v,u)\in E\}$ $\mathrm{outdeg}(v):=\left|\mathrm{Out}(v)\right|$, για κάθε $v\in V$.

Ορισμός 4.2. Ως **κύκλωμα** ορίζεται το κατευθυνόμενο γράφημα $\Gamma=(V,E)$, όπου

- $I:=\{v\in V:\mathrm{indeg}(v)=0\}$, με $|I|=m\in\mathbb{N}$ (η **είσοδος** του κυκλώματος)·
- $E:=\{v\in V:\mathrm{outdeg}(v)=0\}$, με $|E|=n\in\mathbb{N}$ (η **έξοδος** του κυκλώματος)·
- κάθε $v\in I$ φέρει μία (αυθαίρετα επιλεγμένη) ετικέτα, ως εξής: $(v,b)\in V\times\{0,1\}$·
- κάθε $v\in V\smallsetminus I$ έχει δύο ετικέτες: $(v,g,b)\in V\times\{\textsc{Και},\textsc{Η},\textsc{Οχι},\Delta\textsc{ιαχ}\}\times\{0,1\}$, όπου για $\mathrm{In}(v)=\{(x_i,g_i,b_i):1\leqslant i\leqslant\mathrm{indeg}(v)\}$, $\mathrm{Out}(v)=\{(y_j,g_j,b_j):1\leqslant j\leqslant\mathrm{outdeg}(v)\}$
  - και $g=\textsc{Και}$, τότε $\mathrm{indeg}(v)=2$ και $b=\left\lfloor(x_1+x_2)/2\right\rfloor$.
  - και $g=\textsc{Η}$, τότε $\mathrm{indeg}(v)=2$ και $b=\left\lceil(x_1+x_2)/2\right\rceil$.
  - και $g=\textsc{Οχι}$, τότε $\mathrm{indeg}(v)=1$ και $b=1-x_1$.
  - και $g=\Delta\textsc{ιαχ}$, τότε $\mathrm{indeg}(v)=1$, $\mathrm{outdeg}(v)=2$ και $b=y_1=y_2=x_1$.

► *Στο σχεδιασμό κυκλωμάτων η "πύλη" `fork` εκφράζει την διάσπαση ενός καλωδίου σε δύο τα οποία μεταφέρουν την ίδια πληροφορία με το αρχικό.*

Το γράμμα #

Κάθε κύκλωμα υπολογίζει μία (λογική) συνάρτηση $f : \{0,1\}^m \to \{0,1\}^n$, η οποία μπορεί να θεωρηθεί κι ως (μερική) συνάρτηση με αυθαίρετα μεγάλη είσοδο

$$\{0,1\}^* \longrightarrow \{0,1\}^* \qquad x_0x_1\cdots x_{m-1}w \longmapsto f(x_0,x_1,\ldots,x_{m-1})w \qquad \text{(για κάθε } w \in \{0,1\}^*\text{)}$$

Έτσι εισάγεται το σύμβολο "#" που σηματοδοτεί το πέρας των εισόδων του κυκλώματος.

Το στοιχείο κ_{321}

► *Στον σχεδιασμό κυκλωμάτων πολλές φορές τα καλώδια τέμνονται (δίχως αν αλληλεπιδρούν) γεγονός που εδώ θα απεικονισθεί μέσω μεταθέσεων των φυσικών αριθμών (αφού πλεον η είσοδος του κυκλώματος είναι στοιχείου του* $\{0,1\}^*$.

Ορισμός 4.3. Έστω ένα σύνολο X και μία ομάδα $(G,*)$. Η **(αριστερή) δράση της** G **στο** X ορίζεται ως μία απεικόνιση $\cdot : G \times X \to X$, τέτοια ώστε $(\forall x \in X)[1_G \cdot x = x]$ και $(\forall x \in X)(\forall g_1, g_2 \in G)\big[(g_1 * g_2)\cdot x = g_1 \cdot (g_2 \cdot x)\big]$. Εάν επιπλέον, ισχύει ότι

- $(\forall g,h \in G)\big[g \neq h \implies (\exists x \in X)[g\cdot x \neq h \cdot x]\big]$, τότε η δράση καλείται **πιστή**.
- $(\forall x,y \in G)(\exists g \in G)[g\cdot x = y]$, τότε η δράση καλείται **μεταβατική**.

Η σειρά των κορυφών της εισόδου έχει σημασία, έτσι είναι επιθυμητή η αναδιάταξη των κορυφών εισόδου, μέσω της δράσης $\mathrm{Sym}(\{0,\ldots,m-1\}) \times \{0,1\}^* \longrightarrow \{0,1\}^*$.

Επί παραδείγματι θα είναι

$$(m-1 \mid 0 \mid \cdots \mid m-2)x_0x_1\cdots x_{m-1}\#w \longmapsto x_1\cdots x_{m-1}x_0\#w$$

για $w \in \{0,1\}^*$.

Για τον παραπάνω λόγο ορίζονται οι μεταθέσεις

$$\begin{aligned}
\gamma_0 &:= \ldots\ldots (3n \mid 3n+1 \mid 3n+2)\ \ldots\ (3 \mid 4 \mid 5)\,(0 \mid 1 \mid 2)\\
\gamma_1 &:= \ldots\ldots (3n+1 \mid 3n+2 \mid 3(n+1))\ \ldots\ (4 \mid 5 \mid 6)\,(1 \mid 2 \mid 3)\,(0)\\
\gamma_2 &:= \ldots\ldots (3n+2 \mid 3(n+1) \mid 3(n+1)+1)\ \ldots\ (5 \mid 6 \mid 7)\,(2 \mid 3 \mid 4)\,(1)\,(0)\\
\gamma_3 &:= \ldots\ldots (3n \mid 3n+1 \mid 3n+2)\ \ldots\ (3 \mid 4 \mid 5)\,(2)\,(1)\,(0)
\end{aligned}$$

Έτσι, $\kappa_i(x_0x_1\dots x_m\#w) = y_0y_1\dots y_m\#w$, όπου $y_{\gamma_i(k)} = x_k$, ή ισοδύναμα $y_k = x_{\gamma_i^{-1}(k)}$, για $k = 0, 1, \dots, m$, $i = 0, 1, 2, 3$ και $w \in \{0, 1, \#\}$. Από τα προηγούμενα, η εν λόγῳ δράση ορίζεται καλώς εάν $m \equiv i \mod 3$. Εν πάσει άλλη περιπτώσει, υποτίθεται πως τα "περισσευόμενα" (ένα ή δύο) δυφία παραμένουν στη θέση τους.

Για $x = x_0 \dots x_i \dots x_m \in \{0, 1\}^*$, $m \in \mathbb{N}$ ορίζονται

- Εάν $m = 3n + 2$, τότε $\kappa_j(xr\#) := x_{\gamma_j^{-1}(0)} \dots x_{\gamma_j^{-1}(i)} \dots x_{\gamma_j^{-1}(3n+2)} r\#$, για $j \in \{0, 3\}$.
- Εάν $m = 3(n + 1)$, τότε $\kappa_1(xr\#) := x_{\gamma_1^{-1}(0)} \dots x_{\gamma_1^{-1}(i)} \dots x_{\gamma_1^{-1}(3(n+1))} r\#$.
- Εάν $m = 3(n + 1) + 1$, τότε $\kappa_2(xr\#) := x_{\gamma_2^{-1}(0)} \dots x_{\gamma_2^{-1}(i)} \dots x_{\gamma_2^{-1}(3(n+1)+1)} r\#$.

όπου $r \in \{0, 1\}^{\leqslant 2}$. Ειδικότερα, $\kappa_{321}(\cdot) \equiv \kappa_3(\kappa_2(\kappa_1(\cdot)))$.

Η ομάδα $G_{3,1}^{\mathrm{mod}\,3}(0, 1; \#)$

Ορισμός 4.4. Έστω ένα σύνολο A, με $|A| \in \mathbb{N} \setminus \{1\}$. Παρακάτω ως $\cdot : A^\star \times A^\star \longrightarrow A^\star$ θα συμβολίζεται η παράθεση λέξεων.

1. (α′) Το $u \in A^\star$ καλείται **πρόθεμα** του $v \in A^\star$ εάν $(\exists w \in A^\star)[v = uw]$.

   (β′) Το $P \subseteq A^\star$ είναι **προθεματικός κώδικας υπεράνω του** A εάν κανένα στοιχείο του P δεν είναι πρόθεμα κάποιου άλλου στοιχείου του P.

   (γ′) Ένας προθεματικός κώδικας καλείται **μεγιστικός** εάν δεν είναι γνήσιο υποσύνολο κάποιου άλλου προθεματικού κώδικα.

2. Το $R \subseteq A^\star$ καλείται **δεξιό ιδεώδες του** $A^\star$ εάν

$$R \cdot A^\star := \{r \cdot a \in A^\star : r \in R \wedge a \in A^\star\} \subseteq R$$

3. (α′) Ένας **ισομορφισμός δεξιών ιδεωδών** του $A^\star$ είναι μία 1-1 και επί απεικόνιση $\varphi : R_1 \longrightarrow R_2$, όπου τα $R_1, R_2 \subseteq A^\star$ είναι δεξιά ιδεώδη κι επίσης ισχύει ότι $(\forall u \in R_1)(\forall x \in A^\star)\big[\varphi(u) \cdot x = \varphi(u \cdot x)\big]$.

   (β′) Ο ισομορφισμός δεξιών ιδεωδών $\varphi : R_1 \longrightarrow R_2$ λέγεται **μεγιστικός** εάν δεν υπάρχει ισομορφισμός δεξιών ιδεωδών $\Phi : J_1 \longrightarrow J_2$, με $J_1 \supsetneq R_1$, $J_2 \supsetneq R_2$ και $\Phi \restriction R_1 \equiv \varphi$.

   - Εάν $\varphi : R_1 \longrightarrow R_2$ είναι ένας ισομορφισμός δεξιών ιδεωδών του $A^\star$, τότε ως $\max\varphi$ συμβολίζεται ο μεγιστικός ισομορφισμός δεξιών ιδεωδών, όπου $\max\varphi \restriction R_1 \equiv \varphi$.

4. Το δεξιό ιδεώδες $R \subseteq A^\star$ καλείται **ουσιώδες** (essential) εάν $R \cap I \neq \varnothing$, για κάθε δεξιό ιδεώδες $I \subseteq A^\star$.

5. Το δεξιό ιδεώδες $R \subseteq A^\star$ καλείται **πεπερασμένα παραγόμενο** εάν ο προθεματικός κώδικας που του αντιστοιχεί* είναι πεπερασμένος.

Ορισμός 4.5 ([Bir06 Ορισμός 3.2 και 4.4])**.** Έστω ένα σύνολο A, με $|A| = N \in \mathbb{N} \setminus \{1\}$. Η **ομάδα Thompson-Higman** $G_{N,1}$ έχει ως στοιχεία όλους τους μεγιστικούς ισομορφισμούς ανάμεσα σε πεπερασμένα παραγόμενα ουσιώδη δεξιά ιδεώδη του $A^\star$ και πράξη την $(\varphi, \psi) \longmapsto \max(\varphi \circ \psi)$ (η σύνθεση των μερικών ισομορφισμών δεξιών ιδεωδών του $A^\star$) $\varphi, \psi \in G_{N,1}$. Κατ' επέκταση, ορίζεται η (υπο)ομάδα (της $G_{3,1}$),

$$G_{3,1}^{\bmod 3}(0,1;\#) := \Big\{\Phi \in G_{3,1} : \Phi\big(\{0,1\}^*\big) \subseteq \{0,1\}^*,\ \Phi^{-1}\big(\{0,1\}^*\big) \subseteq \{0,1\}^* \\ \text{οι } \Phi^{\pm 1}\big|_{\{0,1\}^*} \text{ είναι ολικές συναρτήσεις και } (\forall x \in \{0,1\}^*)[\Phi^{\pm 1}(x\#) \in \{0,1\}^*\#] \\ \text{για όποια } x \in \{0,1\}^* \text{ ορίζεται η } \Phi(x) \text{ ισχύει } \big|\Phi(x)\big| \equiv |x| \mod 3\Big\}$$

Παρατήρηση 4.6. *Η ομάδα* $G_{2,1}$ *είναι η ομάδα Thompson* V.

Ορισμός 4.7. Θεωρείται ένα σύνολο A, με $|A| \in \mathbb{N} \setminus \{1\}$. Έστω $\varphi : P_1 \cdot A^\star \longrightarrow P_2 \cdot A^\star$ ένας ισομορφισμός δεξιών ιδεωδών του $A^\star$, όπου τα $P_1, P_2 \subseteq A^\star$ είναι προθεματικοί κώδικες.

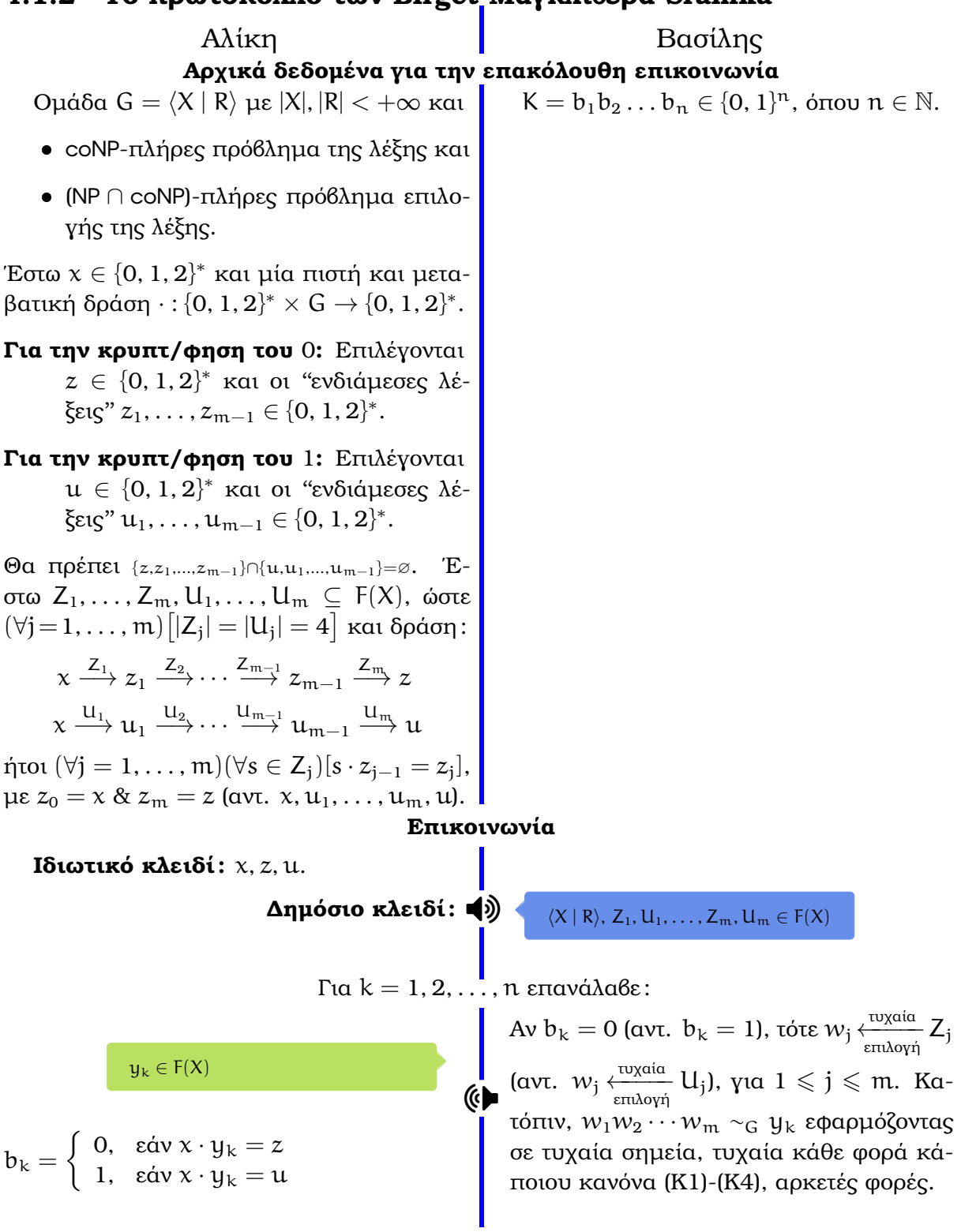
- Ο μεγιστικός προθεματικός κώδικας $P_1 \subseteq A^\star$ καλείται **πεδίο κώδικα** (domain code) του $\varphi : P_1 \cdot A^\star \longrightarrow P_2 \cdot A^\star$.
- Ο μεγιστικός προθεματικός κώδικας $P_2 \subseteq A^\star$ καλείται **εικόνα κώδικα** (image code ή range code) του $\varphi : P_1 \cdot A^\star \longrightarrow P_2 \cdot A^\star$.

Ορισμός 4.8 ([Bir06, Ορισμός 3.2])**.** Ο μεγιστικός μερικός ισομορφισμός δεξιών ιδεωδών του $\{0,1,\#\}^\star$) $\Phi_f \in G_{3,1}^{\bmod 3}(0,1;\#)$ **προσομοιάζει** (simulates) τη λογική συνάρτηση $f : \{0,1\}^m \longrightarrow \{0,1\}^n$, για $m, n \in \mathbb{N}$, εάν

1. το πεδίο και η εικόνα κώδικα του Φ_f είναι υποσύνολα του $\{0,1\}\{0,1\}^* \cup \{0,1\}^*\#$.
2. $\Phi_f\big(0\{0,1\}^m\big) \subseteq 0^{1+i(n)}\{0,1\}^{n+m}$, έτσι ώστε
$$\Phi_f(0x_1 \dots x_m) = 0^{1+i(n)} f(x_1, \dots, x_m) x_1 \dots x_m$$
όπου $i(n) \in \{0,1,2\}$, με $i(n) \equiv -(1+n) \mod 3$ (δηλαδή η συνάρτηση $i(n)$ διατηρεί τα μήκη modulo 3).
3. - $\Phi_f^{\pm 1}\big(\{0,1\}^*\big) \subseteq \{0,1\}^*$ και $\Phi_f^{\pm 1}\big(\{0,1\}^*\#\big) \subseteq \{0,1\}^*\#$.
   - $\Phi_f\big(0\{0,1\}^*\big) \subseteq 0\{0,1\}^*$ και $\Phi_f^{-1}\big(1\{0,1\}^*\big) \subseteq 1\{0,1\}^*$.

*Το σύνολο των δεξιών ιδεωδών του $A^\star$ είναι σε 1-1 αντιστοιχία με το σύνολο των προθεματικών κωδικών υπεράνω του A.

4.1.2 Το πρωτόκολλο των Birget-Μαγκλιβέρα-Sramka



Σχήμα 4.1: Το σχήμα ανταλλαγής κλειδιού Birget-Μαγκλιβέρα-Sramka

Η αποκρυπτογράφηση στηρίζεται στο γεγονός ότι:

Γεγονός. Εάν $g_0, g_1 \in \mathrm{gp}\left(G_{3,1}^{\mathrm{mod}\,3}(0,1;\#) \cup \{\kappa_{321}\}\right)$, με $g_0 \neq g_1$ και $|g_0|, |g_1| \leqslant n$, τότε υπάρχει $z \in \{0,1,2\}^*$, με $|z| \in \mathcal{O}(n)$ και $(z)g_0 \neq (z)g_1$.

4.1.2.Α΄ Σχεδιαστικές παράμετροι

- $n = 100$ ή $n = 200$.
- $m = 100$ ή $m = 200$.
- $n \leqslant |x|, |z|, |u| \leqslant 2n$.
- $(\forall i = 1, \ldots, m-1)[n/2 \leqslant |z_i|, |u_i| \leqslant 4n]$.

Αλγόριθμος 4.9 Δημιουργία των συστημάτων $(Z_1, \ldots, Z_m)$ και $(U_1, \ldots, U_m)$.

για $(j = 1, \ldots, m)$
  για $(k = 1, \ldots, |Z_j|)$
    /* Τα κυκλώματα των $(z_j, z_{j+1}) \in Z_j \times Z_{j+1}$ και $(u_j, u_{j+1}) \in U_j \times U_{j+1}$ θα πρέπει να είναι όσο το δυνατόν παρόμοια, κι αν $u_j \neq z_j$, τότε μπορεί να χρησιμοποιηθεί το ίδιο κύκλωμα. Παρακάτω είναι $z_{j+1} = z$ και $u_{j+1} = u$ */
    Σχεδιάζεται ένα λογικό κύκλωμα που απεικονίζει την $z_j \in Z_j$ στην $z_{j+1} \in Z_{j+1}$;
    Παρόμοια για το ζεύγος $(u_j, u_{j+1}) \in U_j \times U_{j+1}$;
    Κάνοντας χρήση της αντιστοιχίας των λογικών κυκλωμάτων με τα στοιχεία της $G_{3,1}$, προκύπτουν τα στοιχεία της G που προσομοιάζουν τα εν λόγῳ κυκλώματα;
  τέλος για
τέλος για

Σύγχηση κρυπτοκειμένου. Έστω $w \in Z_1 \times \cdots \times Z_m$ (αντ. $w \in U_1 \times \cdots \times U_m$), με $|w| \leqslant n$. Θεωρείται η "συμμετροποιημένη παράσταση" $G_s = \langle X \mid R_s \rangle$ της $G = \langle X \mid R \rangle$, όπου $R_s := R^{\pm 1} \cup \{$όλες οι κυκλικές μεταθέσεις των στοιχείων του $R^{\pm 1}\}$. Θεωρείται το σύστημα μεταβάσεων (rewriting system):

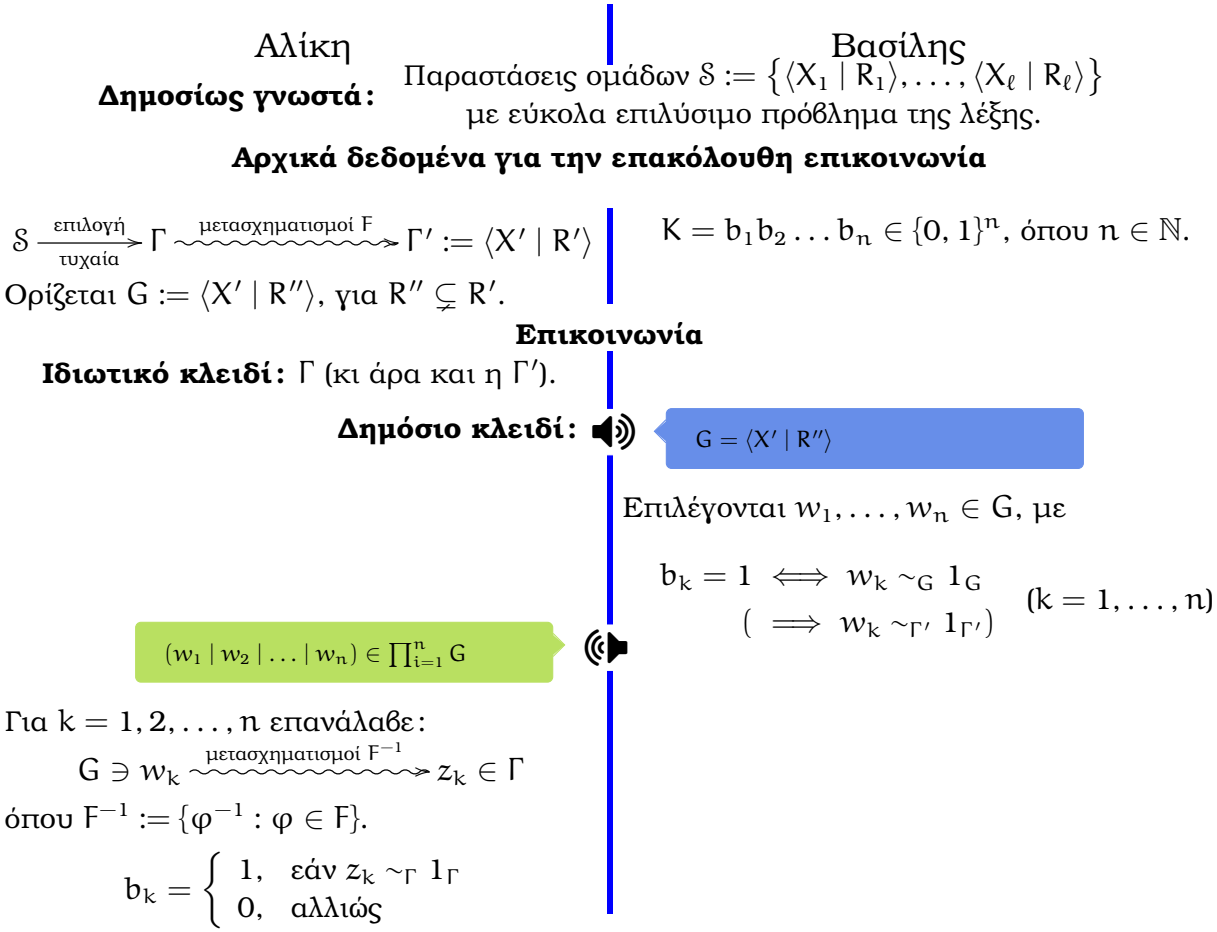
$$\mathcal{R} := \left\{(u \longrightarrow v) \in F(X) \times F(X) : u^{-1}v \in R_s\right\} \cup \left\{(xx^{-1} \longleftrightarrow \varepsilon) \in F(X) \times F(X) : x \in X^{\pm 1}\right\}$$

Η διακδικάσία σύγχησης της w έχει ως εξής:

επανάλαβε
  για $(i = 1, 2, \ldots, n)$
    $j \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{1, \ldots, |w|\}$; $r = (u \longrightarrow v) \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathcal{R}$;
    εάν (μπορεί να εφαρμοσθεί ο κανόνας r στη θέση j της w) **τότε**
      $w = aub \xrightarrow{\mathcal{R}:\,(u \to v)} avb$, με $a, b \in F(X)$ και $|a| = j - 1$;
      $w \leftarrow avb$;
    τέλος εάν
  τέλος για
έως ότου (κάθε στοιχείο της αρχικής λέξης να έχει αντικατασταθεί)

4.2 Το πρωτόκολλο των Shpilrain-Zapata

Το πρωτόκολλο δημοσιεύθηκε στο [SZ09] και φέρεται ως το πρώτο μη-σπασμένο σχήμα ανταλλαγής κλειδού που στηρίζεται στο πρόβλημα της λέξης.



Σχήμα 4.2: Το σχήμα ανταλλαγής κλειδιού Shpilrain-Zapata

Μερικές παρατηρήσεις:

- Ο Βασίλης φαίνεται να έχει δύσκολο έργο, καθώς καλείται να επιλέξει στοιχεία ώστε $w \sim_G 1_G$ και $w \not\sim_G 1_G$ χωρίς να ξέρει την αρχική παράσταση Γ (ενδέχεται η Γ να περιέχει συσχετιστές ώστε $w \not\sim_G 1_G$, αλλά $w \sim_\Gamma 1$.)
- Τα κρυπτογραφημένα στοιχεία δεν πρέπει να παρέχουν καμμία πληροφορία για το δυφίο από το οποίο προέρχονται. Επομένως, ο Βασίλης πρέπει να είναι σε θέση ώστε να δημιουργεί *φαινομενικά τυχαίες* λέξεις w, ώστε $w \sim_G 1_G$. Για το λόγο αυτό οι εισηγητές προτείνουν στο [SZ09] μία μέθοδο "ανακατέματος".

Αλγόριθμος 4.10 Δημιουργία "τυχαίων" λέξεων σε πεπερασμένα παριστάμενες ομάδες.

Δεδομένα: Το δημόσιο κλειδί της Αλίκης $G = \langle X' \mid R'' \rangle$.
διαδικασία Ανακάτεμα(w, p)
για $(\ell = 1, 2, \ldots, p)$
  Εισαγωγή σχεδόν $2p/k$ λέξεων της μορφής $x'(x')^{-1}$ ή $(x')^{-1}x'$, για $x' \in X'$, σε τυχαία σημεία της u, όπου $k = |X'|$;
  Εξετάζοντας την u από το τέλος της προς την αρχή για κάθε υπολέξη $x \in F(X')$, με $|x| = 2$, της u, τέτοια ώστε $axb \in R''$, αντικαθίσταται από την $a^{-1}b^{-1} \in F(X')$.
  Απαλοιφή κάθε υπολέξης της $u \in F(X')$ της μορφής $x'(x')^{-1}$ ή $(x')^{-1}x'$, για $x' \in X'$;
τέλος για
τέλος διαδικασίας Ανακάτεμα

πρόγραμμα Δημιουργία_ταυτοτικών_λέξεων /* Δημιουργία $u \in G$, με $u \sim_G 1_G$ */
$u \leftarrow s_1 s_2 \cdots s_p \in F(X')$, όπου $|u| = p \geqslant 10 \cdot |R''|$ και

$$s_1, \ldots, s_p \in \left\{ w^{-1} r w \in G : r \in (R'')^{\pm 1},\ |r| \in \{3, 4\},\ w \in F(X'),\ |w| \in \{0, 1, 2\} \right\};$$

κάλεσε Ανακάτεμα(u, p);
$u \leftarrow (x')^{-1}u^{-1}x'u$ για κάποιο $x' \in X'$;
κάλεσε Ανακάτεμα$(u, |u|/2)$;
επίστρεψε u;
τέλος προγράμματος Δημιουργία_ταυτοτικών_λέξεων

πρόγραμμα Δημιουργία_μη-ταυτοτικών_λέξεων /* Δημιουργία $u \in G$, με $u \not\sim_G 1_G$ */
Επιλέγεται $u \equiv u(x'_1, x'_2, x'_3, \ldots) = (x'_{j_1})^{\delta_1}(x'_{j_2})^{\delta_2} \cdots (x'_{j_t})^{\delta_t} \in F(X')$;
$u \leftarrow (x'_{j_1})^{\zeta_1}(x'_{j_2})^{\zeta_2} \cdots (x'_{j_t})^{\zeta_t}$, ώστε $\zeta_1 + \zeta_2 + \ldots + \zeta_t = 0$;
$u \leftarrow (x')^{-1}u^{-1}x'u$, για κάποιο $x' \in X'$;
κάλεσε Ανακάτεμα$(u, |u|/2)$;
επίστρεψε u;
τέλος προγράμματος Δημιουργία_μη-ταυτοτικών_λέξεων

Πυκνότητα των $w \not\sim_\Gamma 1$: *Εάν $G = \langle X \mid R \rangle$, τότε $G = F(X)/R$. Για άπειρη G, η ασυμπτωτική συχνότητα της R στην $F(X)$ είναι* $\rho_{F(X)}(R) := \lim\limits_{n \to +\infty} \dfrac{\left|\{x \in R : |x| \leqslant n\}\right|}{\left|\{x \in F(X) : |x| \leqslant n\}\right|} = 0.$

Όντας η G άπειρη, έπεται ότι $\lim\limits_{n \to +\infty} \Pr\left[w \equiv w(X) \neq 1 \wedge |w| = n\right] \approx 1$. *Ωστόσο, είναι αδύνατον να επιλεχθεί άπειρο μήκος για την παράσταση των κρυπτογραφημένων δυφίων! Επομένως, για πιο απτά μήκη, περί 100-200, γεννάται το ερώτημα*

$$\text{Αν } \Gamma = \langle X \mid R \rangle \text{ είναι το ιδιωτικό κλειδί της Αλίκης, πόσο γρήγορα } \rho_{F(X)}(R) \longrightarrow 0;$$

Η απάντηση είναι οι μη-υπαγόμενες ομάδες (non-amenable groups).

4.2.1 Μετασχηματισμοί Tietze

Για τη διάχυση της παράστασης Γ στην Γ', αλλά και για τη σύνθεση της Γ από την Γ' μια καλή προτίμηση μετασχηματισμών που διατηρούν τους ισομορφισμούς είναι:

Ορισμός 4.11. Οι **μετασχηματισμοί Tietze** ορίζονται τα εξής τέσσερα σχήματα υπεράνω παραστάσεων ομάδων:

(T1) *Εισαγωγή ενός καινούργιου γεννήτορα* $y \notin \{x_1, x_2, \ldots\}$*:*

$$\Gamma = \langle x_1, x_2, \ldots \mid r_1, r_2, \ldots \rangle \overset{\text{(T1)}}{\rightsquigarrow} \Gamma' = \langle y, x_1, x_2, \ldots \mid ys^{-1}, r_1, r_2, \ldots \rangle$$

όπου $s \in F(x_1, x_2, \ldots)$.

(T2) *Αφαίρεση ενός γεννήτορα:* Εάν $s \in F(x_1, x_2, \ldots)$, τότε

$$\Gamma = \langle y, x_1, x_2, \ldots \mid ys^{-1}, r_1, r_2, \ldots \rangle \overset{\text{(T2)}}{\rightsquigarrow} \Gamma' = \langle x_1, x_2, \ldots \mid r_1, r_2, \ldots \rangle$$

(T3) *Εφαρμογή αυτομορφισμού:* Για τον αυτομορφισμό[†], $\varphi : \{x_1, x_2, \ldots\} \to \{x_1, x_2, \ldots\}$,

$$\Gamma = \langle x_1, x_2, \ldots \mid r_1, r_2, \ldots \rangle \overset{\text{(T3)}}{\rightsquigarrow} \Gamma' = \langle x_1, x_2, \ldots \mid \varphi(r_1), \varphi(r_2), \ldots \rangle$$

(T4) *Αλλαγή του συνόλου των συσχετιστών:* Εάν $\Gamma = \langle x_1, x_2, \ldots \mid r_1, r_2, \ldots \rangle$, τότε μπορεί το σύνολο $r_1, r_2, \ldots$ να αντικατασταθεί από το $r'_1, r'_2, \ldots$ το οποία να έχει την ίδια συζυγή κλειστότητα με το αρχικό.

Για τους μετασχηματισμούς **(T1)**—**(T3)** είναι εύκολο να βρεθεί ρητός ισομορφισμός καθώς και ο αντίστροφός του. Για τον **(T4)** ο εμπλεκόμενος ισομορφισμός είναι ο ταυτοτικός· συνεπώς, είναι επιθυμητή η δημιουργία μιας αναδρομικής διαδικασίας για τον **(T4)**:

(T4′) Εάν $\Gamma = \langle x_1, x_2, \ldots \mid r_1, r_2, \ldots \rangle$, μερικά r_i μπορούν να αντικατασταθούν από κάποιο

$$r_i^{-1}, \quad r_i r_j, \quad r_i r_j^{-1}, \quad r_j r_i, \quad r_j r_i^{-1}, \quad x_k^{-1} r_i x_k, \quad x_k r_i x_k^{-1} \quad (\text{για } j \neq i \text{ και τυχόν } k)$$

4.2.2 Επίθεση ισομορφισμού

Πρόκειται για μια επίθεση "ωμής βίας" που απαιτεί τεράστια υπολογιστική ικανότητα από το μέρος τους αντιπάλου (γι αυτό και παραμένει σε θεωρητικό πλαίσιο).

Επίθεση ισομορφισμού: *Η Εύα μπορεί να επαυξήσει την δημοσίως γνωστή παράσταση* G*, ώστε να προκύψει μία ισόμορφη της* Γ *παράσταση.*

Πιο συγκεκριμένα, η Εύα μπορεί να προσθέτει ένα στοιχείο κάθε φορά στην παράσταση G παίρνοντας την G_+ και να επαληθεύει εάν $(\exists \Gamma_i \in \mathcal{S})[G_+ \simeq \Gamma_i]$.

[†]Μία αμφιρριπτική (1-1 και επί) συνάρτηση από ένα μαθηματικό αντικείμενο, στον εαυτό του.

Μια θεμελιώδης έννοια από την Θεωρία Πολυπλοκότητας είναι η:

Ορισμός 4.12. Ένα υποσύνολο των φυσικών αριθμών καλείται **αναδρομικό** εάν υπάρχει αλγόριθμος που υπολογίζει την χαρακτηριστική του συνάρτηση.

Η επίθεση ισομορφισμών είναι θεωρητικά εφικτή, επειδή

(I) η συλλογή $\mathcal{S}$ υποτίθεται αναδρομική και

(II) το σύνολο όλων των παραστάσεων των ισόμορφων ομάδων με μία πεπερασμένα παραστάσιμη ομάδα είναι αναδρομικό.

Επαληθεύοντας εάν $G_+ \simeq \Gamma_i$ (γενικώς)

Έστω η επαυξημένη παράσταση G_+ καθώς και μία τυχαία παράσταση Γ_i. Η Εύα για να επαληθεύσει εάν $G_+ \simeq \Gamma_i$, θα πρέπει να ακολουθήσει τα εξής βήματα:

1. Απαριθμεί τις δυνατές απεκονίσεις $f : \mathscr{X}(\Gamma_i) \longrightarrow F\big(\mathscr{X}(G_+)\big)$.
2. Απαριθμεί τις δυνατές απεκονίσεις $g : \mathscr{X}(\Gamma_+) \longrightarrow F\big(\mathscr{X}(\Gamma_i)\big)$.
3. Επαληθεύει εάν κάθε ζεύγος (f, g), με τις f, g όπως παραπάνω, ικανοποιεί ότι:
   (α′) $f \circ g = \mathrm{id}_{\Gamma_i}$.
   (β′) Οι f, g είναι ομομορφισμοί.
   [δηλαδή να ισχύει: $\big(\forall r \in \mathscr{R}(\Gamma_i)\big)[f(r) = 1_{G_+}]$ και $\big(\forall r \in \mathscr{R}(G_+)\big)[g(r) = 1_{\Gamma_i}]$, με τη τελευταία σχέση να επαληθεύεται εύκολα, αφού η $\Gamma_i \in \mathcal{S}$ έχει εύκολα επιλύσιμο πρόβλημα της λέξης.]

Επαληθεύοντας εάν $G_+ \simeq \Gamma_i \in \mathcal{S}$

Έστω η επαυξημένη παράσταση G_+ και μία $\Gamma_i \in \mathcal{S}$. Εν περιπτώσει όπου $\Gamma_i \not\simeq G_+$, τότε πρόκειται για την αρνητική έκβαση του προβλήματος του ισομορφισμού, η οποία δεν είναι αναδρομική. Έτσι, η Εύα καλείται να επαληθεύσει πληθώρα συνδυασμών απεικονίσεων $f : \mathscr{X}(\Gamma_i) \longrightarrow F\big(\mathscr{X}(G_+)\big)$ και $g : \mathscr{X}(\Gamma_+) \longrightarrow F\big(\mathscr{X}(\Gamma_i)\big)$ (όπως παραπάνω) εσαεί. Συνεπώς, σε κάθε της προσπάθεια καταλαμβάνει κάποια υπολογιστική μνήμη. Συνεχίζοντας (εσαεί) τις προσπάθειες, σύντομα θα έχει εξαντλήσει όλους τους πόρους της μνήμης της, αφού ο πληθάριθμος του συνόλου $\big\{\langle \mathscr{X}(G) \mid S\rangle : \mathscr{R}(G) \subseteq S \text{ και } |\sum_{s\in S}|s| \leqslant \sum_{r\in\mathscr{R}(\Gamma_i)|}|r|\big\}$ αυξάνει εκθετικά σε σχέση με το $\sum_{r\in\mathscr{R}(\Gamma_i)}|r|$ (:**μέγεθος της παράστασης**). Για παράδειγμα, $\Big|\big\{\langle Y \mid S\rangle : |Y| = 6 \wedge \sum_{s\in S}|s| \leqslant 100\big\}\Big| \geqslant 10^{100}$.

Να σημειωθεί πως υπάρχουν και εξυπνότεροι τρόποι ώστε να δημιουργηθεί η G_+, ωστόσο η παραπάνω συζήτηση είχε σκοπό να πείσει τον αναγνώστη πως ακόμη κι έτσι, θα χρειάζονταν πάλι απεριοριόριστοι πόροι μνήμης.

4.2.3 Επίθεση πηλίκου

Ένας τρόπος ώστε η Εύα να προσπαθήσει να ανακτήσει τα μηδενικά δυφία από τις κρυπτογραφημένες τους λέξεις, παρέχεται από την

Επίθεση πηλίκου: *Η Εύα προσθέτει πεπερασμένο πλήθος ή άπειρους συσχετιστές στην παράσταση* G *ώστε να δημιουργήσει μία ομάδα στην οποία το πρόβλημα της λέξεως είναι επιλύσιμο (βασικά ώστε να μπορεί να το επιλύσει η Εύα).*

Ορισμός 4.13. Έστω μία ομάδα G. Η G καλείται **αβελιανή** εάν $(\forall a, b \in G)\big\{[a, b] = 1\big\}$. Η G καλείται **μεταβελιανή** εάν $(\forall a, b, c, d \in G)\Big\{\big[[a, b], [c, d]\big] = 1\Big\}$. Η G καλείται **μηδενοδυναμική**[‡] **κλάσης** $c \geqslant 1$ εάν $(\forall y_1, y_2, \ldots, y_{c+1} \in G)\big\{[y_1, y_2, \ldots, y_{c+1}] = 1\big\}$. Παραπάνω είναι $[\alpha_1, \ldots, \alpha_{n+1}] = \begin{cases} \alpha_1^{-1}\alpha_2^{-1}\alpha_1\alpha_2, & \text{εάν } n = 1 \\ \big[[\alpha_1, \ldots, \alpha_n], \alpha_{n+1}\big], & \text{εάν } n > 1 \end{cases}$.

- Το έργο της Εύας ευκολύνεται εάν προσπαθήσει να βρει υπόλοιπα σε αβελιανές ή ευρύτερα σε μηδενοδυναμικές ομάδες.

Επί παραδείγματι, εάν η ομάδα G είναι

- πηλίκο αβελιανών ομάδων, τότε αρκεί να προστεθεί πεπερασμένο πλήθος συσχετιστών της μορφής $[x_i', x_j']$, για κάθε ζεύγος (i, j).
- πηλίκο μηδενοδύναμων ομάδων, τότε θα πρέπει να προστεθούν (πεπερασμένα πολλοί) συσχετιστές της μορφής $[x_{i_1}', x_{i_2}', \ldots, x_{i_{c+1}}']$, για κάποιο c.

Ορισμός 4.14. Έστω F μία ελεύθερη ομάδα. Μία **ελεύθερη μεταβελιανή ομάδα** είναι η ομάδα πηλίκο $F\Big/\big[[F, F], [F, F]\big]$, όπου η $\big[[F, F], [F, F]\big]$ καλείται η **δεύτερη υποομάδα αντιμεταθετών** (second commutator group).

Πρόταση 4.15. Κάθε ελεύθερη μεταβελιανή ομάδα είναι απείρως παριστάμενη.

Ωστόσο, για τα μεταβελιανά πηλίκα, θα πρέπει, από την Πρόταση 4.15, να προστεθούν άπειροι το πλήθος συσχετιστές. Παρ' όλα ταύτα δεν χρειάζεται όλη η άπειρη πληροφορία: *Αρκεί να θεωρηθεί η* G *ως εκλέπτυνση μιας μεταβελιανής ομάδος και να εφαρμοσθεί ο αλγόριθμος που επιλύει το πρόβλημα της λέξης ο οποίος είναι ο ίδιος για όλες τις πεπερασμένες μεταβελιανές ομάδες.*

[‡]Απόδοση στα ελληνικά του όρου nilpotent από το *Αγγλοελληνικόν λεξικόν των Θεωρητικών και Εφηρμοσμένων Μαθηματικών*, έκδοσις Τεχνικού Επιμελητηρίου της Ελλάδος, Μεμάς Κολαΐτης Αθήναι, 1976.

Η επίθεση πηλίκου αφορά και τις μηδενοδυναμικές και τις μεταβελιανές ομάδες, έτσι:

- Η Αλίκη προσθέτει έναν συσχετιστή της μορφής $x'_i = \prod_{j=1}^{M} [x'_i, w_j]$ στην G.
- Ο Βασίλης επιλέγει μία λέξη της μορφής $w = [x'_i, u]$ όταν θέλει να κρυπτογραφήσει ένα δυφίο 0, με $w \not\sim_G 1_G$ και κατ' επέκτασην $w \not\sim_{\Gamma'} 1_{\Gamma'}$.

Πράγματι, μια μεταβελιανή επίθεση πηλίκου σε στοιχεία της μορφής $[x'_i, u]$ δεν δουλεύει καθώς το συγκεκριμένο στοιχείο ανήκει στην δεύτερη υποομάδα αντιμεταθετών της ομάδας G, αφού $x'_i = \prod_{j=1}^{M} [x'_i, w_j]$ και άρα το x'_i ανήκει στην υποομάδα αντιμεταθετών της G. Επιπροσθέτως, επειδή $[x'_i, u] = \left[\prod_{j=1}^{M} [x'_i, w_j], u\right] = \left[\prod_{k=1}^{M} \left[\prod_{j=1}^{M} [x'_i, w_j], w_k\right], u\right]$ και αναδρομικά ούτο καθ' εξής, αποτυγχάνουν και οι επιθέσεις μηδενοδυναμικών πηλίκων.

4.2.4 Προτεινόμενες παράμετροι

Έστω $\langle x_1, \ldots, x_k \mid r_1, \ldots, r_m \rangle \in \mathcal{S}$. Προτείνονται:

- $10 \leqslant k \leqslant 20$.
- $10 \leqslant m \leqslant 30$ και $(\forall i = 1, 2, \ldots, m)[12 \leqslant |r_i| \leqslant 20]$.
- Για το σημείο $\Gamma \overset{\text{μετασχηματισμοί } F}{\rightsquigarrow} \Gamma'$ συνιστάται:
  1: εφαρμογή μετασχηματισμών Tietze **(T4′)** για να «ανακατευθεί» η παράσταση Γ·
  2: εφαρμογή $s_1 \in \mathbb{N}$ φορών του μετασχηματισμού Tietze **(T1)** (με το μήκος των γεννητόρων να πληροί τα παραπάνω φράγματα)· και
  3: εφαρμογή $s_2 \in \mathbb{N}$ φορών του μετασχηματισμού Tietze **(T2)**.

  Δεν υπάρχει πρόβλεψη για τα $s_1, s_2 \in \mathbb{N}$, ωστόσο προτείνεται $s_1 + s_2 \geqslant 50$, διότι τότε περί το 30% των συσχετιστών θα έχουν μήκος 4. Από το υπόλοιπο 70% θα απορριφθούν τόσοι συσχετιστές, ώστε οι μισοί συσχετιστές της Γ′ να έχουν μήκος 4.
- Για την αποφυγή επιθέσεων πηλίκου (§4.2.3), θεωρείται

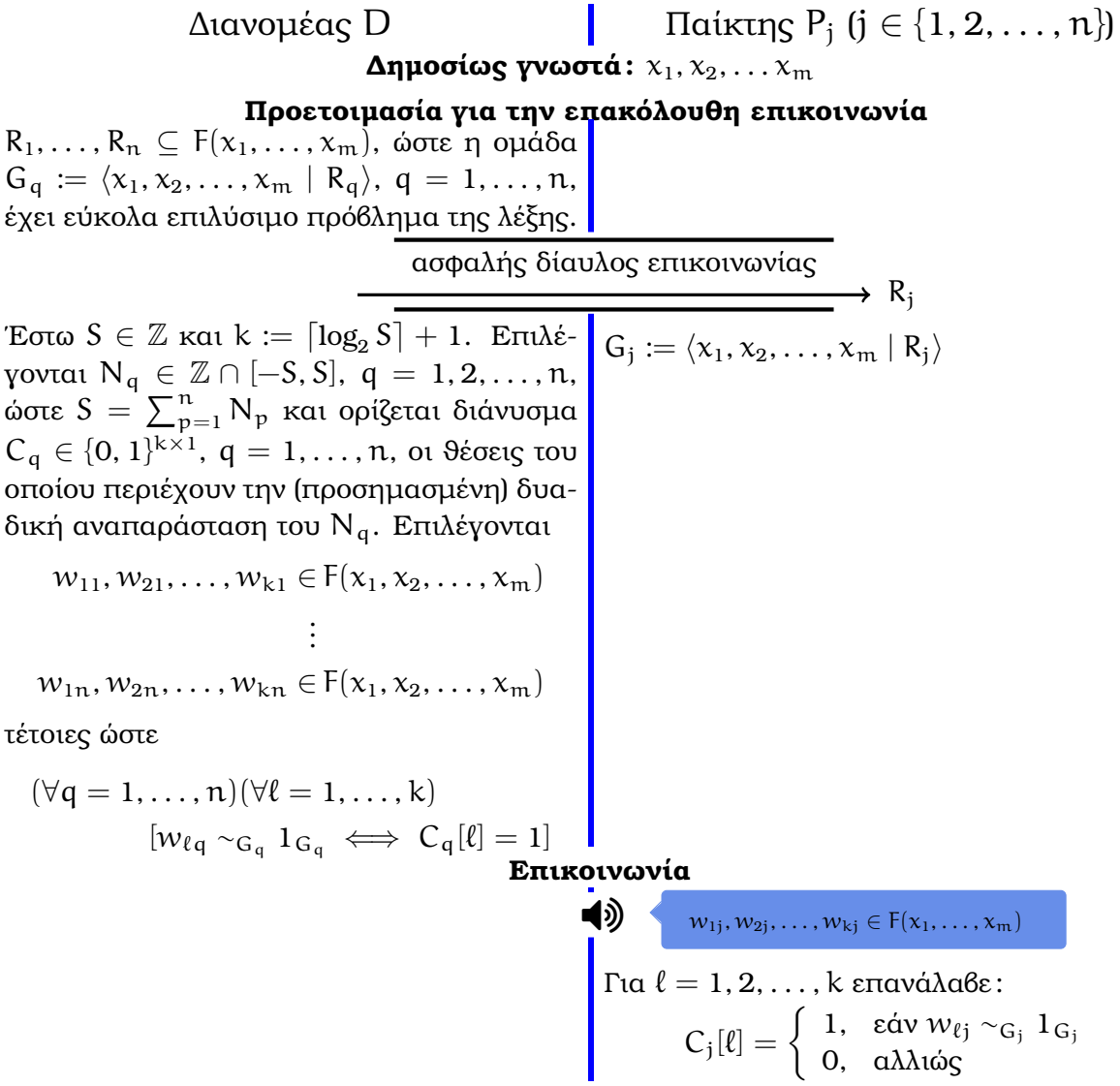
$$\mathscr{R}(G) = R'' \cup \left\{ x'_i = \prod_{j=1}^{M} x'_i w_j (x'_i)^{-1} w_j^{-1} \right\}$$

  για κάποιον τυχαία επιλεγμένο $x'_i \in X' = \mathscr{X}(\Gamma')$ και τυχαίες $w_1, \ldots, w_M \in F(X')$, με $|w_1|, \ldots, |w_M| \in \{1, 2\}$. Προτείνεται $M = 10$. Στην εφαρμογή των αντιστρόφων μετασχηματισμών η εικόνα του επιπλέον συσχετιστή θα συμπεριληφθεί στην Γ, έτσι θα είναι $\left|\mathscr{X}(\Gamma)\right| = |X|$ και $\left|\mathscr{R}(\Gamma)\right| = |R| + 1$, όπου αρχικά ήταν $\Gamma = \langle X \mid R \rangle$.
- Εάν η Γ′ ικανοποιεί τη συνθήκη μικρών ακυρώσεων $C'(1/6)$ (βλ. Ορισμό 4.19· θα την πληροί με μεγάλη πιθανότητα), τότε καθίσταται αποδεκτή. Ειδάλλως, επαναλαμβάνεται η διαδικασία εξ αρχής.

4.3 Μοίρασμα μυστικού

Σ' ένα σχήμα μοιράσματος μυστικού ένα σύνολο $n \in \mathbb{N}$ παικτών κατέχει μέρος του κοινού μυστικού S. Σ' ένα σχήμα με (t, n)-κατώφλι, το μυστικό S αποκαλύπτεται μόνον όταν ένα συγκεκριμένο πλήθος $t \leqslant n$ παικτών κοινοποιήσει την μυστική πληροφορία που κατέχει.

4.3.1 Ένα σχήμα μοιράσματος μυστικού με (n, n)-κατώφλι



Όταν συγκεντρωθούν και οι n παίκτες, τότε $S = \sum_{q=1}^{n} (-1)^{C_q[1]} \sum_{\ell=1}^{k-1} C_q[k - \ell + 1] 2^{\ell - 1}$.

Σχήμα 4.3: Μοίρασμα μυστικού με (n, n)-κατώφλι

4.3.2 Ένα σχήμα μοιράσματος μυστικού με (t, n)-κατώφλι

Διανομέας D	Παίκτης P_j ($j \in \{1, 2, \ldots, n\}$)
Δημοσίως γνωστά: $x_1, x_2, \ldots x_m$	
Προετοιμασία για την επακόλουθη επικοινωνία	
$R_1, \ldots, R_n \subseteq F(x_1, \ldots, x_m)$, ώστε η ομάδα $G_q := \langle x_1, x_2, \ldots, x_m \mid R_q \rangle$, $q = 1, \ldots, n$, έχει εύκολα επιλύσιμο πρόβλημα της λέξης.	
ασφαλής δίαυλος επικοινωνίας $\longrightarrow R_j$	
Έστω $S \in \mathbb{Z}_p$, για κάποιον πρώτο αριθμό $p \in \mathbb{N}$, με $p > t$, και $k := \lceil \log_2 S \rceil$. Επιλέγεται πολυώνυμο $f \in \mathbb{Z}_p(X)$, με $\deg f = t - 1, \qquad f(0) = S.$ Ορίζονται τα διανύσματα $C_q \in \{0,1\}^{k \times 1}$, για $q = 1, \ldots, n$, ώστε οι θέσεις του καθενός να περιέχουν την δυαδική αναπαράσταση του $f(q) \in \mathbb{Z}_p$. Επιλέγονται $w_{11}, w_{21}, \ldots, w_{k1} \in F(x_1, x_2, \ldots, x_m)$ $\vdots$ $w_{1n}, w_{2n}, \ldots, w_{kn} \in F(x_1, x_2, \ldots, x_m)$ τέτοιες ώστε $(\forall q = 1, \ldots, n)(\forall \ell = 1, \ldots, k)$ $[w_{\ell q} \sim_{G_q} 1_{G_q} \iff C_q[\ell] = 1]$	$G_j := \langle x_1, x_2, \ldots, x_m \mid R_j \rangle$
Επικοινωνία	
	$(j, w_{1j}, \ldots, w_{kj}) \in \in \{1, \ldots, n\} \times \left(F(x_1, \ldots, x_m)\right)^k$
	Για $\ell = 1, 2, \ldots, k$ επανάλαβε: $C_j[\ell] = \begin{cases} 1, & \text{εάν } w_{\ell j} \sim_{G_j} 1_{G_j} \\ 0, & \text{αλλιώς} \end{cases}$

Όταν συγκεντρωθούν $t \leqslant n$ παίκτες, τότε το κοινό μυστικό S ανακτάται με το μέθοδο των συντελεστών Lagrange από τα ζεύγη $\left\{\left(j,\ (-1)^{C_j[1]} \sum_{\ell=1}^{k-1} C_j[k+1-\ell] 2^{\ell-1}\right)\right\}_{j=1,\ldots,t}$.

Σχήμα 4.4: Μοίρασμα μυστικού με (t, n)-κατώφλι

4.3.2.Α΄ Συντελεστές Lagrange

Θεωρείται το πολυώνυμο

$$f(X) = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \ldots + \alpha_{t-1} X^{t-1} \in \mathbb{Z}_p[X]$$

για $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{t-1} \in \mathbb{Z}_p$, δια κάποιον πρώτο αριθμό $p \in \mathbb{N}$, $p > t$, $\alpha_{t-1} \neq 0$ και κάποιο $t \in \mathbb{N}$. Έστω επίσης t διακεκριμένα[§] ζεύγη τιμών

$$\big(z_1, p(z_1)\big),\ \big(z_2, p(z_2)\big),\ \big(z_3, p(z_3)\big),\ \ldots,\ \big(z_t, p(z_t)\big)$$

όπου, όπως και πριν, $(\forall i \in \mathbb{N})[0 < i \leqslant t \implies z_i \neq 0]$, αλλιώς ο παίκτης με $z_i = 0$ κατέχει το κοινό μυστικό S.

Η ανάκτηση του μυστικού στηρίζεται στο εξής:

Γεγονός. Έστω ένα πολυώνυμο f με $\deg(f) = t - 1$, τότε το f ορίζεται μοναδικά από t *διακεκριμένα* ζεύγη τιμών $\big(z_i, p(z_i)\big) \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Ως **συντελεστές Lagrange** ορίζονται οι ακόλουθοι λόγοι:

$$\ell_j(x) := \prod_{\substack{1 \leqslant m \leqslant t \\ m \neq j}} \frac{x - x_m}{x_j - x_m} \qquad \text{για κάθε } j = 1, 2, \ldots, t$$

[Επί παραδείγματι, εάν $t = 3$, τότε $\ell_1(x) = \frac{x-x_2}{x_1-x_2} \cdot \frac{x-x_3}{x_1-x_3}$, $\ell_2(x) = \frac{x-x_1}{x_2-x_1} \cdot \frac{x-x_3}{x_2-x_3}$ και $\ell_3(x) = \frac{x-x_1}{x_3-x_1} \cdot \frac{x-x_2}{x_3-x_2}$.] Θέτοντας,

$$\begin{aligned} g(x) &:= \sum_{i=1}^{t} \big(\ell_i(x) \cdot f(z_i)\big) \\ &= \ell_1(x) \cdot p(z_1) + \ell_2(x) \cdot p(z_2) + \ldots + \ell_t(x) \cdot p(z_t) \end{aligned}$$

προκύπτει πως $g = f$. Τώρα πλέον, $S = \alpha_0 = g(0)$.

Συγκεκριμένα, για το Σχήμα 4.4 είναι

$$S = f(0) = g(0) = \sum_{i \in I} \big(\ell_i(0) \cdot f(i)\big) = \sum_{i \in I} f(i) \prod_{\substack{j \in I \\ j \neq i}} \frac{-j}{i-j},\ \text{ για } I \subseteq \{1, \ldots, n\} \text{ και } |I| = t$$

δηλαδή το κοινό μυστικό $S \in \mathbb{Z}_p$ είναι γραμμικός συνδυασμός των ιδιωτικών μυστικών $f(1), \ldots, f(n)$, με κοινώς γνωστούς συντελεστές $\ell_1(0), \ldots, \ell_n(0)$.

[§] $(\forall i, j = 1, 2, \ldots, t)[i \neq j \implies z_i \neq z_j]$ γι αυτό και η υπόθεση $p > t$.

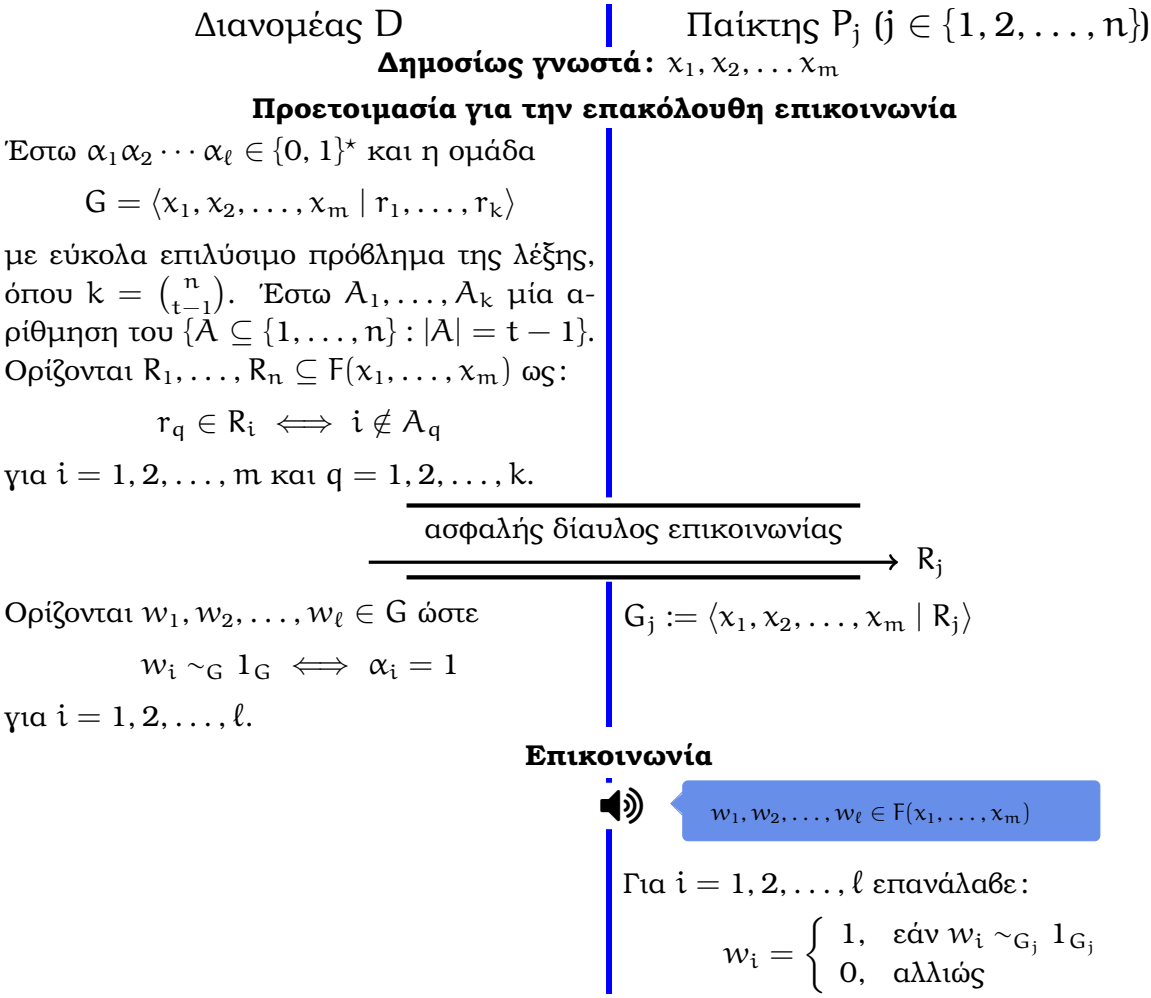
Παρατήρηση 4.16. *Εάν* $t \geqslant 3$*, τότε η αποκάλυψη του κοινού μυστικού* $S \in \mathbb{Z}_p$ *μπορεί να συμβεί χωρίς κάθε παίκτης να αποκαλύψει το προσωπικό του μυστικό —βλ. §4.3.4.*

Παρατήρηση 4.17. *Το σχήμα αποτίμηση-παρεμβολή είναι αρκετά σύνηθες*

$$\boxed{f(X) = \alpha_0 + \alpha_1 X + \ldots + \alpha_{t-1} X^{t-1}} \underset{\text{Παρεμβολή}}{\overset{\text{Αποτίμηση}}{\rightleftarrows}} \boxed{\big(z_1, f(z_1)\big),\ \ldots,\ \big(z_t, f(z_t)\big)}$$

κι έχει πληθώρα εφαρμογών (παραδείγματος χάριν: ταχύς μετασχηματισμός Fourier).

4.3.3 Ένα σχήμα μοιράσματος μυστικού με χρήση ομάδων



Σχήμα 4.5: Σχήμα μοιράσματος μυστικού με χρήση ομάδων

Μερικές παρατηρήσεις:

(I) Η συνθήκη $(\forall i = 1, \dots, k)(\forall q = 1, \dots, n)[r_q \in R_i \iff i \notin A_q]$ εξασφαλίζει πως

$$(\forall i = 1, 2, \dots, k)\big[\big|\{q \in \mathbb{N} : r_i \notin R_q\}\big| = t - 1\big]$$

Άρα,

(α′) $(\forall i = 1, \dots, k)\big(\forall I \subseteq \{1, \dots, n\}\big)\big[|I| = t \implies r_i \in \bigcup_{q \in I} R_q\big]$, ενώ

(β′) $\big(\forall I \subseteq \{1, \dots, n\}\big)(\exists s \in \{1, \dots, k\})\big[|I| = t \implies r_s \in \bigcup_{q \in I} R_q\big]$.

(II) Οι λέξεις $w \in \{w \in \{w_1, \dots, w_\ell\} : w \sim_G 1_G\}$ θα πρέπει να περιέχουν τους περισσοτέρους εκ των συσχετιστών $r_1, \dots, r_k \in F(x_1, \dots, x_m)$. Επιπλέον, κάθε $r_q \in F(x_1, \dots, x_m)$, $q = 1, \dots, k$ θα πρέπει να έχει χρησιμοποιηθεί στην κατασκευή κάποιας $w_i \in F(x_1, \dots, x_m)$, $i = 1, \dots, \ell$.

4.3.3.Α′ Ένα σχήμα υπογραφών

Όλα τα σχήματα της Ενότητας είναι πρωτόκολλα κρυπτογράφησης *δυφίο προς δυφίο*, ήτοι:

- Εάν $\alpha \in \{0, 1\}^\star$ η ακολουθία προς κρυπτογράφηση, τότε

$$1 \longmapsto w \in \{x \in G : x \sim_G 1_G\} \qquad 0 \longmapsto w' \in \{y \in G : y \not\sim_G 1_G\}$$

Το μυστικό που πρόκειται να μοιρασθεί χρειάζεται (δημιουργείται) στο τελευταίο βήμα.

Ο παραπάνω λόγος μπορεί να μετατρέψει το σχήμα σε ένα *σχήμα υπογραφών*. Πράγματι, έστω το μήνυμα προς αποστολή $\alpha = \alpha_1 \dots \alpha_\ell \in \{0, 1\}^\star$ και $s = s_1 \dots s_p \in \{0, 1\}^\star$ μία προαποφασισμένη κοινώς γνωστή (σε όλους τους παίκτες P_i) ακολουθία. Πριν την μετάδοση:

> Ορίζονται τα $w_1, \dots w_{\ell+p} \in G$ ως εξής:
>
> $$w_i = 1_G \iff \alpha_i = 1 \qquad (i = 1, \dots, \ell)$$
> $$w_k = 1_G \iff s_k = 1 \qquad (k = 1, \dots, p)$$
>
> οι οποίες υπόκεινται στην Παρατήρηση (II) παραπάνω.

Πλέον, οποιοδήποτε σύνολο αποτελούμενο από t εκ των συνολικά n παικτών μπορεί να επαληθεύσει πως πράγματι το μήνυμα α προέρχεται από τον διανομέα D. Ο έλεγχος μπορεί να συμβεί απλώς ελέγχοντας εάν η υπογραφή s του D εμπεριέχεται στο μήνυμα α.

Παρατήρηση 4.18. *Εάν είναι γνωστόν εκ των προτέρων σε ποιο σημείο του μηνύματος βρίσκεται η υπογραφή s (έστω στο τέλος), τότε είναι δυνατόν και λιγότεροι από t παίκτες να ανακτήσουν όλους τους συσχετιστές $r_1, \dots, r_m$. Επομένως, συνιστάται η υπογραφή s να εμπεριέχεται σε κάποιο τυχαίο σημείο του μηνύματος α, δηλαδή να μεταδοθεί το στοιχείο $\beta s \gamma$, όπου $\beta, \gamma \in \{0, 1\}^\star \setminus \{\varepsilon\}$ και $\alpha = \beta\gamma$.*

4.3.4 Έμπιστη ανάκτηση του κοινού μυστικού

Όλα τα πρωτόκολλα μοιράσματος του μυστικού όπως ορίσθηκαν στην παρούσα Ενότητα δεν είναι ασφαλή έναντι σε έναν ενεργητικό αντίπαλο —έστω την Μάλλορυ. Πράγματι, έστω πως η στρατηγική που ακολουθείται ώστε οι t παίκτες να ανακτήσουν το μυστικό είναι:

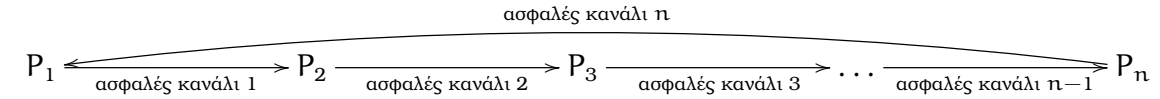
- Κάθε παίκτης P_i κοινοποιεί στους υπολοίπους το μέρος του μυστικού s_i που κατέχει.

Εάν η Μάλλορυ είναι μία από τους παίκτες, έστω ο παίκτης P_j, τότε μπορεί αντί του πραγματικού μέρους του μυστικού που κατέχει s_j, να κοινοποιήσει ένα $s'_j \neq s_j$. Έτσι όντας οι υπόλοιποι παίκτες P_i, για $i \neq j$, έντιμοι κοινοποιώντας τα πραγματικά s_i, τότε

$$s_j + \sum_{\substack{i=1 \\ i\neq j}}^{t} s_i = S \neq s'_j + \sum_{\substack{i=1 \\ i\neq j}}^{t} s_i$$

Επομένως, η *άμεση* κοινοποίηση του μέρους του μυστικού που κατέχει κάθε παίκτης *δεν* είναι και τόσο ασφαλής. Για το πρωτόκολλο της §4.3.1, έστω η διαδικασία —από το [GS]:

Υπενθυμίζεται πως ο παίκτης P_i, για $i = 1, \ldots, n$, κατέχει το μέρος $C_i \in \{0,1\}^{k\times 1}$ του μυστικού $S \in \mathbb{N}$ και χρειάζονται και οι $n \in \mathbb{N}$ παίκτες ώστε να ανακτηθεί το S. Έστω ότι



Ο παίκτης P_1**:** εκκινεί τη διαδικασία επιλέγοντας μία στήλη $A_1 \in \mathbb{N}^{k\times 1}$ με τυχαία στοιχεία. Κατόπιν στέλνει στον παίκτη P_2, το $A_1 + C_1$.

Ο παίκτης P_i**,** $i = 2, \ldots, n-1$**:** επιλέγει μία στήλη $A_i \in \mathbb{N}^{k\times 1}$ με τυχαία στοιχεία.

1. Λαμβάνει από τον παίκτη P_{i-1} το άθροισμα $\sum_{m=1}^{i-1}(A_m + C_m)$.
2. Στέλνει στον παίκτη P_{i+1} το άθροισμα $(A_i + C_i) + \sum_{m=1}^{i-1}(A_m + C_m)$.

Ο παίκτης P_n**:** επιλέγει μία στήλη $A_n \in \mathbb{N}^{1\times k}$ αποτελούμενη από τυχαία στοιχεία. Κατόπιν στέλνει στον παίκτη P_1, το $A_n + C_n + \sum_{m=1}^{n-1}(A_m + C_m)$.

Πλέον, ο παίκτης P_1 έχει στην κατοχή του το $C := \sum_{m=1}^{n}(A_m + C_m) = \sum_{m=1}^{n} A_m + \sum_{m=1}^{n} C_m$.

Ο παίκτης P_1**:** κοινοποιεί το $C - A_1 = \sum_{m=1}^{n} C_m + \sum_{m=2}^{n} A_m$ στους $P_2, \ldots, P_n$.

[Έτσι δεν αποκαλύπτεται στον P_2 (που γνωρίζει το $A_1 + C_1$) το A_1, άρα ούτε το C_1.]

Κάθε παίκτης P_i**,** $2 \leqslant i \leqslant n$**:** αφαιρεί το προσωπικό του A_i από το $C - A_1$ ενώπιον όλων. Όταν όλοι οι παίκτες έχουν αφαιρέσει τα προσωπικά τους A_i, τότε προκύπτει το κοινό μυστικό $S = \sum_{m=1}^{n} C_m$.

Η παραπάνω διαδικασία διασφαλίζει τα μυστικά $C_1, \ldots, C_n$ των παικτών. Ωστόσο, η διασφάλιση αυτή προϋποθέτει $t \geqslant 3$.

Ανοικτό Ερώτημα. Δεδομένου ότι απαιτούνται δύο συμμετέχοντες για την αποκάλυψη του κοινού μυστικού (ήτοι $t = 2$) —ο καθείς έχει ως μυστικό του το σημείο $\big(x_i, f(x_i)\big)$, $i = 1, 2$, στο επίπεδο— είναι δυνατόν να ανακτηθεί το κοινό μυστικό S με τρόπο ώστε να μην αποκαλύψει ο ένας παίκτης στον άλλον το μυστικό του σημείο;

Να σημειωθεί ότι:

- Το πρωτόκολλο της §4.3.1 που επιλέχθηκε δεν διαδραμάτισε κάποιον καθοριστικό ρόλο (απλώς έπρεπε να συγκεκριμενοποιηθεί ο χώρος στον οποίον ανήκαν τα στοιχεία). Η διαδικασία εφαρμόζεται και στα υπόλοιπα σχήματα μοιράσματος μυστικού (των §4.3.2 και §4.3.3).
- Παρ' ότι $C_i \in \{0, 1\}^{k\times 1}$ και $A_i \in \mathbb{N}^{k\times 1}$, η πρόσθεση $N_i + C_i$ είναι η συνήθης πρόσθεση μεταξύ διανυσμάτων φυσικών αριθμών.
  - Θα ήταν δυνατόν και $A_i \in \{0, 1\}^{k\times 1}$ και τότε η πράξη θα ήταν η πρόσθεση modulo 2 κι άρα $A_i + C_i \in \{0, 1\}^{(k+1)\times 1}$ (αφού το άθροισμα δύο αριθμών k δυφίων έχει το πολύ $k + 1$ δυφία). Για τον ίδιο λόγο $\{0, 1\}^{(k+n)\times 1} \ni \sum_{k=1}^{n} (A_k + C_k)$.

4.4 Ομάδες με εύκολα επιλύσιμο πρόβλημα λέξης

Ομάδες μικρών ακυρώσεων

Ορισμός 4.19. Έστω μια ομάδα $G = \langle X \mid R\rangle$.

1. Η $u \in F(X)\setminus\{\varepsilon\}$ είναι **κομμάτι** αν $(\exists r_1, r_2 \in R)\big(\exists v_1, v_2 \in F(X)\big)[r_1 = uv_1 \wedge r_2 = uv_2]$, με τις uv_1, uv_2 να είναι ανηγμένες.
2. $G \in C'(\lambda)$, $0 < \lambda < 1$, εάν πληροί την *μετρική συνθήκη μικρών ακυρώσεων*: Για κάθε $r \in R$, με $r = uv$, η $u \in F(X) \setminus \{\varepsilon\}$ είναι κομμάτι, με $|u| < \lambda|r|$.
3. $G \in C(p)$, $p \in \mathbb{N}$, εάν κάθε $r \in R$ είναι γινόμενο τουλάχιστον p κομματιών.
4. $G \in T(q)$, $q \in \mathbb{N}\setminus\{1, 2\}$ για κάθε $t \in \mathbb{N}\cap[3, q)$ και κάθε $r_1, \ldots, r_t \in R$, με $r_1 \neq r_2^{-1}$, $\ldots, r_t \neq r_1^{-1}$, τουλάχιστον ένα εκ των $r_1r_2, \ldots, r_tr_1$ είναι ελεύθερα ανηγμένο.

Λήμμα 4.20. *Έστω μια ομάδα* G. *Εάν η* G *είναι πεπερασμένα παριστάμενη και*

- $G \in \{C'(1/4)\text{-}T(4),\ C(6),\ C(4)\text{-}T(4),\ C(3)\text{-}T(3)\}$ *ή*
- $G \in C'(1/6)$ *[τη λύση παρέχει ο αλγόριθμος του Dehn]*

τότε η G *έχει εύκολα επιλύσιμο πρόβλημα της λέξης.*

Προσεγγιστικά πεπερασμένες ομάδες

Ορισμός 4.21. Μία ομάδα G καλείται **προσεγγιστικά πεπερασμένη** (residually finite) εάν για κάθε $g \in G$, με $g \neq 1_G$, υπάρχει ένας ομομορφισμός h από την G σε κάποια πεπερασμένη ομάδα ώστε $h(g) \neq 1$.

Θεώρημα 4.22 (McKinsey, [McK$_{43}$])**.** Το πρόβλημα της λέξεως επιλύεται στις πεπερασμένα παραστάσιμες, προσεγγιστικά πεπερασμένες ομάδες.

Λήμμα 4.23. *Οι ελεύθερες ομάδες είναι προσεγγιστικά πεπερασμένες.*

Απόδειξη. Θεωρείται η ελεύθερη ομάδα G, με $\mathscr{X}(G) = \{x_1, x_2, \ldots, x_m\}$ και η ανηγμένη $1_G \neq w = x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \cdots x_{i_n}^{\delta_n} \in G$, με $\delta_i \in \{\pm 1\}$. Η συνάρτηση $f : \{x_{i_1}^{\delta_1}, \ldots, x_{i_n}^{\delta_n}\} \longrightarrow S_{n+1}$, με

$$f(x_{i_k}^{\delta_k}) = \begin{cases} \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n+1 \\ ? & \cdots & k+1 & ? & \cdots & ? \end{pmatrix}, & \text{εάν } \delta_k = 1 \\ \\ \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n+1 \\ ? & \cdots & ? & k & \cdots & ? \end{pmatrix}, & \text{εάν } \delta_k = -1 \end{cases}$$

είναι καλώς ορισμένη και επεκτείνεται στην $\overline{f}$, όπου οι θέσεις των ? αντικαθίστανται από αριθμούς εκ του συνόλου $\{1, \ldots, n+1\}$, ώστε να διατηρείται η μετάθεση. Τελικά, $\varphi(x_{i_1}^{\delta_1} x_{i_2}^{\delta_2} \cdots x_{i_n}^{\delta_n}) = \overline{f}(x_{i_n})^{\delta_n} \circ \cdots \circ \overline{f}(x_{i_2})^{\delta_2} \circ \overline{f}(x_{i_1})^{\delta_1}$. □

Γραμμικές ομάδες

Ορισμός 4.24. Μία ομάδα καλείται **γραμμική** (linear) εάν είναι ισόμορφη με μία υποομάδα της $GL_n(\mathbb{F})$, για κάποιο σώμα $\mathbb{F}$.

Θεώρημα 4.25 (Malcev, [Ma$_{40}$])**.** Κάθε πεπερασμένα παραγόμενη γραμμική ομάδα είναι προσεγγιστικά πεπερασμένη.

Παράδειγμα 4.26. Το σύνολο $M_n(R)$ των $n \times n$ πινάκων υπεράνω ενός δακτυλίου R, εφοδιασμένο με πρόσθεση και πολλαπλασιασμό πινάκων είναι γραμμική ομάδα. ⊣

Λήμμα 4.27 (C. Druţu, M. Sapir, [DS$_{04}$])**.** *Η ομάδα* $H = \langle a, b, t \mid tat^{-1} = a^k, tbt^{-1} = b^l \rangle$ *είναι γραμμική εάν και μόνον εάν* $k, l \notin \{-1, 1\}$.

το οποίο προκύπτει ως πόρισμα από την

Πρόταση 4.28 (Wehrfritz, [We$_{73}$])**.** Η ομάδα $H = \langle a, b, t \mid tat^{-1} = a^k, tbt^{-1} = b^l \rangle$, για $k, l \notin \{-1, 1\}$ δεν είναι γραμμική.

Αξιοσημείωτη είναι και η πρώτη *μη γραμμική, προσεγγιστικά πεπερασμένη* ομάδα:

Λήμμα 4.29 (C. Druţu, M. Sapir, [DS$_{04}$])**.** *Η ομάδα* $\langle a, t \mid t^2 a t^{-2} = a^2 \rangle$ *δεν είναι γραμμική, αλλά είναι προσεγγιστικά πεπερασμένη.*

Μέρος ΙΙ

Κρυπτοσυστήματα βασισμένα στο πρόβλημα της συζυγίας

Υστερα σειρά έχει ένα ακόμη πρόβλημα της Θεωρία Ομάδων, το οποίο έχει εφαρμογή στην Μη-Μεταθετική Κρυπτογραφία. Πρόκειται για

Το πρόβλημα της συζυγίας. Θεωρείται μια ομάδα G. Δοθέντων $g, h \in G$ να βρεθεί ένα $x \in G$ τέτοιο ώστε $h = x^{-1}gx$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο στοιχείο.

Κατά φυσιολογικό τρόπο το πρόβλημα αποδίδει το πρώτο πρωτόκολλο του Μέρους· πρόκτειται για το [KLCHKP00] (Κεφάλαιο 5).

Μερικές ειδικότερες υποθέσεις από το [Sh04] για την επιλογή της ομάδας G που χρησιμοποείται στα πρωτόκολλα του Μέρους, αποτελούν οι παρακάτω:

(Συζ0) Η G πρέπει να είναι καλώς μελετημένη.

[Με άλλα λόγια θα πρέπει να είναι γνωστή η φύση του προβλήματος της συζυγίας στην ομάδα, ή τουλάχιστον να μπορεί να αναχθεί σε κάποιο άλλο γνωστό πρόβλημα.]

(Συζ1) Το πρόβλημα της λέξης στην G πρέπει να είναι εύκολα επιλύσιμο.

[Με άλλα λόγια να υπάρχει αλγόριθμος γραμμικής/τετραγωνικής πολυπλοκότητας που να το επιλύει. Ο λόγος είναι ο ταχύς υπολογισμός των κανονικών μορφών των στοιχείων της G.]

(Συζ2) Το πρόβλημα της συζυγίας στην G πρέπει να είναι δύσκολα επιλύσιμο.

[Με άλλα λόγια να μην υπάρχει υπο-εκθετικός αλγόριθμος που να το επιλύει. Η απόδειξη της παρούσης ιδιότητας είναι αρκετά δύσκολο πρόβλημα· αποτελεί -κυριολεκτικά- πρόβλημα του ενός εκατομμυρίου δολαρίων, βλ. [CMI].]

(Συζ3) Θα πρέπει να είναι δυνατόν να εφαρμοσθεί σύγχυση στα στοιχεία της G.

[Έτσι γίνεται αδύνατη η ανάκτηση του $x \in G$, απλά παρατηρώντας το $x^{-1}wx \in G$.]

(Συζ4) Η G θα πρέπει να έχει εκθετικό ρυθμό αύξησης.

[Με άλλα λόγια το πλήθος των στοιχείων (λεξικογραφικού) μήκους n να είναι μεγαλύτερο από κάθε δυνατό πολυώνυμο του n. Έτσι αποφεύγονται τυχούσες εξαντλητικές επιθέσεις στα πιθανά κλειδιά.]

Σύμβαση. *Κάθε στοιχείο που μεταδίδουν οι οντότητες στα πρωτόκολλα του Μέρους είναι στην κανονική του μορφή.*

Μία γενίκευση του προβλήματος της συζυγίας είναι

Το πρόβλημα ανάλυσης συζυγίας. Θεωρείται μια ομάδα G, $H \leqslant G$ και $x, bxb^{-1} \in G$, για κάποιο (μυστικό) $b \in H$. Να βρεθούν $a', a'' \in H$, τέτοια ώστε $a'xa'' = bxb^{-1}$.

Κεφάλαιο 5

Τα πρωτόκολλα των Ko-Lee-Cheon-Han-Kang-Park

Ως φυσική απόρροια του προβλήματος της συζυγίας, παρέχεται το πρωτόκολλο ανταλλαγής κλειδιού των Ko-Lee-Cheon-Han-Kang-Park [βλ. Σχήμα 5.1], το πρώτο κατά σειρά στην παρούσα Εργασία που στηρίζεται στις ομάδες πλεξίδων. Κατόπιν, το πρωτόκολλο ανάγεται σε κρυπτοσύστημα [βλ. Σχήμα 5.2] και παρατίθενται τα τεχνικά χαρακτηριστικά και η ανθεκτικότητά του σε κάποιες κρυπταναλυτικές επιθέσεις. Επιπλέον εξετάζεται η γενίκευση του πρωτοκόλου από τους Cha-Ko-Lee-Han-Cheon [βλ. Σχήμα 5.3] και πως, περιοριζόμενοι σε θετικές πλεξίδες, καθίσταται δυνατή η άντληση πληροφορίας.

5.1 Μία μονόδρομη συνάρτηση

Με τον όρο "μονόδρομη (one-way) συνάρτηση" νοείται μία υπολογιστικά εύκολη διαδικασία, της οποίας η αντίστροφη διαδικασία είναι υπολογιστικά δύσκολη. Θεωρούνται οι $UB_r, LB_s \leqslant B_{r+s}$ ως εξής: Ανακαλώντας την γεωμετρική ερμηνεία των πλεξίδων [βλ. §1.3.1.Β΄]

- η μεν UB_r ενεργεί μόνον στα πάνω (upper) r σχοινιά και
- η δε LB_s ενεργεί μόνον στα κάτω (lower) s σχοινιά.

Συνεπώς, ισχύει $(\forall a \in UB_r)(\forall b \in LB_s)[ab = ba]$. Είναι πρόδηλο πως $UB_r \simeq B_r$.

Θεωρείται η συνάρτηση

$$f : UB_r \times B_{r+s} \longrightarrow B_{r+s} \times B_{r+s} \qquad (a, x) \overset{f}{\longmapsto} (axa^{-1}, x) \tag{5.1}$$

η οποία αποτελεί μονόδρομη συνάρτηση αφού αφενώς οι πράξεις στις ομάδες πλεξίδων γίνονται σε ικανοποιητικό χρόνο, αφετέρου κάθε γνωστή αλγοριθμική προσπάθεια αντιστροφής της συνάρτησης απαιτεί εκθετικό χρόνο.

Εδραζόμενοι στην δύναμη της συνάρτησης (5.1) ανακύπτει

Το πρόβλημα KLCHKP**.** Δοθέντων των $r, s \in \mathbb{N}$ και $x, axa^{-1}, bxb^{-1} \in B_{r+s}$, για κάποια (μυστικά) $a \in UB_r$ και $b \in LB_s$, να υπολογισθεί το $abxa^{-1}b^{-1} \in B_{r+s}$.

το οποίο πρόκειται να αποτελέσει τη βάση για την κρυπτογραφική ασφάλεια του πρωτοκόλλου της §5.2. Με άλλα λόγια, αρκεί να βρεθεί το (μυστικό)

- $a \in UB_r$ και τότε θα είναι $a(bxb^{-1})a^{-1} = abxa^{-1}b^{-1}$, ή
- $b \in LB_s$ και τότε θα είναι $b(axa^{-1})b^{-1} = abxa^{-1}b^{-1}$

αφού $a \in UB_r$ και $b \in LB_s$.

Το πρόβλημα KLCHKP επάγεται από (:είναι τουλάχιστον τόσο δύσκολα επιλύσιμο όσο)

Το πρόβλημα της ανάλυσης συζυγίας. Έστω μια ομάδα G, $H \leqslant G$ και $x, bxb^{-1} \in G$, για κάποιο (μυστικό) $b \in H$. Να βρεθούν $a', a'' \in H$, τέτοια ώστε $a'xa'' = bxb^{-1}$.

το οποίο αποτελεί μία γενίκευση του προβλήματος της συζυγίας.

Πρόνοια, θα πρέπει να ληφθεί, ώστε το $x \in B_{r+s}$ να είναι αρκούντως "περίπλοκο", ήτοι να αποφεύονται παθογενείς περιπτώσεις όπου

$$(\exists x_1 \in UB_r)(\exists x_2 \in LB_s)(\exists z \in B_{r+s})\big[([UB_r, z] = [LB_s, z] = 1) \wedge (x = x_1x_2z)\big] \qquad (5.2)$$

όπου $[S, z] = 1$ είναι η συντομογραφία της σχέσης $(\forall s \in S)[sz = zs]$, για $S \in \{UB_r, LB_s\}$. Στις περιπτώσεις της σχέσης (5.2) ισχύει ότι

$$abxa^{-1}b^{-1} \overset{\text{εξ. (5.2)}}{=} ab(x_1x_2z)a^{-1}b^{-1} \underset{[LB_s,z]=1}{\overset{[UB_r,z]=1}{=}} ab(x_1x_2)a^{-1}b^{-1}z =$$

$$\underset{a^{-1}\in UB_r}{\overset{x_2\in LB_s}{=}} abx_1a^{-1}x_2b^{-1}z \underset{b\in LB_s}{\overset{x_1\in UB_r}{=}} ax_1ba^{-1}x_2b^{-1}z \underset{b\in LB_s}{\overset{a^{-1}\in UB_r}{=}} (ax_1a^{-1})(bx_2b^{-1})z$$

ήτοι το $abxa^{-1}b^{-1} \in B_{r+s}$ ανακτάται από τα γνωστά $axa^{-1}, bxb^{-1}, x^{-1} \in B_{r+s}$, αφού

$$\begin{aligned}
(axa^{-1})x^{=1}(bxb^{-1}) &= (ax_1x_2za^{-1})(x_1x_2z)^{-1}(bx_1x_2zb^{-1}) && \text{(εξίσωση (5.2))}\\
&= (ax_1a^{-1}x_2z)(z^{-1}x_2^{-1}x_1^{-1})(bx_1x_2zb^{-1})\\
&&& (a \in UB_r,\ [UB_r, z] = 1 \text{ και } x_2 \in LB_e)\\
&= (ax_1a^{-1}x_2z)(z^{-1}x_2^{-1}x_1^{-1})(x_1bx_2b^{-1}z)\\
&&& (x_1 \in UB_r,\ b, b^{-1} \in LB_s \text{ και } [LB_s, z] = 1)\\
&= (ax_1a^{-1})(bx_2b^{-1})z
\end{aligned}$$

Οι Roger Fenn, Dale Rolfsen και Jun Zhu στην εργασία τους [FRZ96] αναφέρουν πως επιλέγοντας στην τύχη η πιθανότητα μια πλεξίδα $x \in B_{r+s}$ να ικανοποιεί την συνθήκη (5.2) είναι αρκούντως μικρή, περί $\left(\dfrac{r!\,s!}{(r+s)!}\right)^{\text{len}(x)}$.

Παρατήρηση 5.1. *Έστω* $n = r+s$. *Υπενθυμίζεται πως υπάρχει επιμορφισμός* $\rho : B_n \twoheadrightarrow S_n$ *[βλ. §1.3.2.Α']. Για την αποφυγή εξαγωγής πληροφορίας για τις* $\rho(a), \rho(b) \in S_n$ *μελετώντας τις* $\rho(x), \rho(axa^{-1}), \rho(bxb^{-1}) \in S_n$, *θα πρέπει τα* $a \in UB_r$ *και* $b \in LB_s$, *να είναι γνήσιες πλεξίδες, δηλαδή να ισχύει* $\rho(a) = \rho(b) = id_{S_n}$.

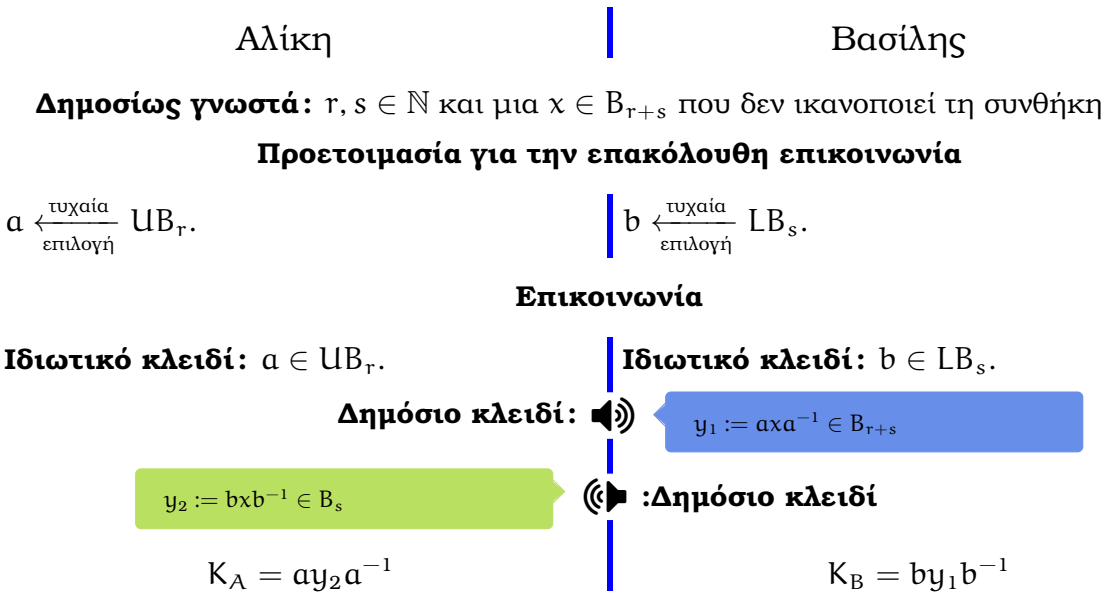
5.2 Το σχήμα ανταλλαγής κλειδιού των Ko-Lee-Cheon-Han-Kang-Park

Ως το πρώτο Σχήμα της Εργασίας το οποίο στηρίζεται σε πλεξίδες, ανακύπτει το ερώτημα πόσο υπολογιστικά εύχρηστο (από άποψη υπολογισμών) είναι. Προς τούτο παρατίθεται το

Θεώρημα 5.2 ([ECHLPT92, KLCHKP00])**.** Έστω $n \in \mathbb{N}$. Θεωρούνται οι $x, y \in B_n$ σε Garside κανονική μορφή, όπου $\text{len}(x) = p$ και $\text{len}(y) = q$.

1. Ο υπολογισμός της Garside κανονικής μορφής της $xy \in B_n$ απαιτεί χρόνο $\mathcal{O}(pqn \log_2 n)$.
2. Ο υπολογισμός της Garside κανονικής μορφής της $x^{-1} \in B_n$ απαιτεί χρόνο $\mathcal{O}(pn)$.

Υπενθυμίζεται πως ο υπολογισμός της Garside κανονικής μορφής της $w \in B_n$ απαιτεί χρόνο $\mathcal{O}(|w|^2 n \log_2 n)$ [Θεώρημα 1.27].



$$K_A = ay_2a^{-1} = a(bxb^{-1})a^{-1} = b(axa^{-1})b^{-1} = by_1b^{-1} = K_B$$

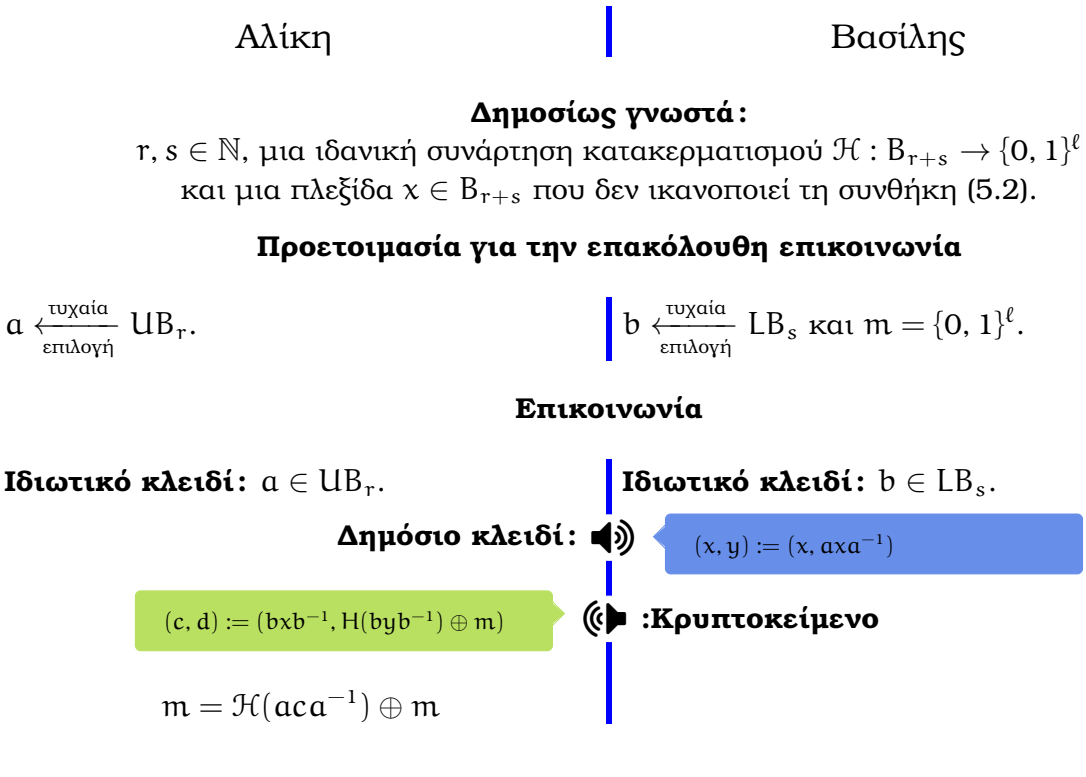
με τη μεσαία ισότητα να ισχύει διότι $a \in UB_r$, $b \in LB_s$ και $(\forall s \in UB_r)(\forall t \in LB_s)[st = ts]$.

Σχήμα 5.1: Το σχήμα ανταλλαγής κλειδιού Ko-Lee-Cheon-Han-Kang-Park

5.3 Το κρυπτοσύστημα των Ko-Lee-Cheon-Han-Kang-Park

Μία συνάρτηση καλείται **συνάρτηση κατακερματισμού** (hash function) εάν μπορεί να απεικονίζει δεδομένα αυθαίρετα μεγάλου μεγέθους σε δεδομένα συγκεκριμένου μεγέθους. Μία συνάρτηση κατακερματισμού λεγεται **ιδανική** εάν επιπλέον είναι ενριπτική*.

Χρησιμοποιώντας το Σχήμα 5.1 οι Ki Hyoung Ko, Sang Ji Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang και Choonsik Park προτείνουν το κάτωθι κρυπτοσύστημα:



Σχήμα 5.2: Το κρυπτοσύστημα Ko-Lee-Cheon-Han-Kang-Park

Ορθότητα της αποκρυπτογράφησης: Ισχύει

$$\begin{aligned}\mathcal{H}(aca^{-1}) \oplus d &= \mathcal{H}\big(a(byb^{-1})a^{-1}\big) \oplus \mathcal{H}(byb^{-1}) \oplus m \\ &= \mathcal{H}(byb^{-1}) \oplus \mathcal{H}(byb^{-1}) \oplus m \\ &= m\end{aligned}$$

όπου η ισότητα $aca^{-1} = byb^{-1}$ ισχύει από το Σχήμα 5.2. Η πράξη $\oplus$ είναι η πρόσθεση υπόλοιπο 2 δυφίο-προς-δυφίο.

*ένα-προς-ένα

5.3.1 Σχεδιαστικά χαρακτηριστικά

Συμβολισμός. Ως $\|x\|$ θα συμβολίζεται το πληθος των δυφίων που χρειάζονται για να αναπαραστασθεί η πλεξίδα $x \in B_n$.

Στα στοιχεία του Σχήματος 5.2, χωρίς βλάβη της γενικότητος, έστω ότι $r = s = n/2$ καθώς και $\mathrm{len}(a) = \mathrm{len}(b) = \mathrm{len}(x) = p \in \mathbb{N}$. Ισχύουν τα παρακάτω:

1) Εάν $w \in B_n$, με Garside κανονική μορφή $w = \Delta_n^k P_1 P_2 \cdots P_p$, τότε $\|w\| = pn \log_2 n$.

   - Οι $P_1, \ldots, P_p$ είναι πλεξίδες μετάθεσεις και μία ματάθεση μπορεί να ανιτστοιχηθεί σε κάποιον αριθμό $\mathbb{N}_0 \cap [0, \ldots, n!)$.
   - $n! = \Theta\big(\exp(n \log_2 n)\big) = \Theta(pn \log_2 n)$.

2) $2p \leqslant \mathrm{len}(bxb^{-1}), \mathrm{len}(abya^{-1}b^{-1}) \leqslant 3p$.

   - Γενικώς, $(\forall y_1, y_2 \in B_n)[\mathrm{len}(y_1 y_2) \leqslant \mathrm{len}(y_1) + \mathrm{len}(y_2)]$.
   - Ειδικώς, $(\forall y_1 \in UB_r)(\forall y_2 \in LB_s)\big[\mathrm{len}(y_1 y_2) \leqslant \max\{\mathrm{len}(y_1), \mathrm{len}(y_2)\}\big]$.

   Συνεπώς, $\mathrm{len}(bxb^{-1}), \mathrm{len}(abya^{-1}b^{-1}) \leqslant 3p$. Για ειδικές επιλογές των a, b, x προκύπτει το κάτω φράγμα.

3) $\|a\| = \Theta(\frac{1}{2} pn \log_2 n)$.

   - $\|a\| = pr \log_2 r$ [λόγῳ του 1)].
   - $pr \log_2 r = \Theta(p \frac{n}{2} \log_2 \frac{n}{2}) = \Theta(\frac{1}{2} pn \log_2 n)$.

4) $\|bxb^{-1}\| = 3pn \log_2 n$.

   [Λόγῳ του 1) και του αναλόγου του 3) για το $b \in LB_s$.]

5) $\big\|(bxb^{-1}, \mathcal{H}(byb^{-1}) \oplus m)\big\| = 3pn \log_2 n + pn \log_2 n = 4pn \log_2 n$.

   - $\mathrm{len}(abxa^{-1}b^{-1}) \overset{2)}{=} \max\{\mathrm{len}(a), \mathrm{len}(b), \mathrm{len}(x), \mathrm{len}(a), \mathrm{len}(a^{-1}), \mathrm{len}(b^{-1})\} = p$.
   - Από το [KLCHKP00, Θεώρημα 3] το πλήθος των n-πλεξίδων με $2p$ θεσμικούς παράγοντες είναι τουλάχιστον εκθετικό ως προς το

$$\log_2 \left(\left\lfloor \tfrac{n-1}{2} \right\rfloor !\right)^{2p} = 2p \log_2 \left(\left\lfloor \tfrac{n-1}{2} \right\rfloor !\right) = \Theta(2p \log_2 (\tfrac{n}{2}!)) = \Theta(2p \tfrac{n}{2} \log_2 \tfrac{n}{2}) = \Theta(pn \log_2 n)$$

   - $\big\|\mathcal{H}(abxa^{-1}b^{-1})\big\| = pn \log_2 n$ [αφού $abxa^{-1}b^{-1} \in B_n$ και από το 1)].

6) Η διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης απαιτούν $\mathcal{O}(p^2 n \log_2 n)$ χρόνο [λόγῳ του Θεωρήματος 5.2].

7) Μία επίθεση ωμής βίας (:εξαντλητικής αναζήτησης) στο Σχήμα 5.2, ώστε να ανακτηθεί το $a \in UB_r$ από το $axa^{-1} \in B_n$ (αντίστοιχα του $b \in LB_s$ από το $byb^{-1} \in B_n$) ενέχει $(r!)^p = (\frac{n}{2}!)^p = \Theta\big(\exp(\frac{1}{2} pn \log_2 n)\big)$ ενδεχόμενα [βλ. και §5.3.2.Α'].

8) Το μήκος του κρυπτογραφημένου μηνύματος είναι τετραπλάσιο του αρχικού μηνύματος [λόγῳ των 1) και 5)].

5.3.2 Κρυπτανάλυση

5.3.2.Α΄ Επίθεση ωμής βίας

Επίθεση ωμής βίας (εκδοχή Α΄):
Δεδομένων των $x, axa^{-1} \in B_n$, να βρεθεί το $a \in UB_r$.

Στην θεωρία είναι $a \in UB_r$, στην πράξη όμως η Εύα θα μπορούσε απλά να απαριθμήσει όλες τις πιθανές κανονικές μορφές $w = \Delta_r^u P_1 \cdots P_p \in UB_r$, για κάποιο $p \in \mathbb{N}$ —ανάλογο της υπολογιστικης της δύναμης— και να επαληθεύει κάθε φορά εάν $w = axa^{-1}$. Εκ του [KLCHKP00, Θεώρημα 3] υπάρχουν $\left(\frac{r-1}{2}!\right)^p$ διαφορετικοί συναδυασμοί. Όμως, για $r = 45$, και $p = 2$, τότε $\left(\frac{r-1}{2}!\right)^p = (22!)^2 > 2^{139}$ και μια τέτοια αναζήτηση είναι άνευ χρηστικότητας.

Ωστόσο, ενδέχεται να

- $(\exists a' \in UB_r)[a' \neq a \wedge a'x(a')^{-1} = axa^{-1}]$.

Εν τοιαύτη περιπτώσει:

- $a'x(a')^{-1} = axa^{-1} \iff a^{-1}a'x = xa^{-1}a' \iff a^{-1}a' \in C_G(x)$ και
- $a, a' \in UB_r \implies a^{-1}a' \in UB_r$ (όντας $UB_r \leqslant B_{r+s}$).

Επίθεση ωμής βίας (εκδοχή Β΄):
Να βρεθεί $a' \in UB_r$, τέτοιο ώστε $a^{-1}a' \in C_G(x) \cap UB_r$.

Για ειδικές επιλογές του $x \in B_n$ και συγκεκριμένο θεσμικό μήκος, δύναται να ισχύει $\left|C_G(x) \cap UB_r\right| \ll \left|UB_r\right|$ κι έτσι θα είναι δύσκολη η εύρεση ενός $a' \in UB_r$, όπως παραπάνω.

Μια άλλη εκδοχή έχει ως εξής:

- $a'x(a')^{-1} = axa^{-1} \iff x^{-1}a^{-1}a'x(a')^{-1} = a^{-1} \iff x^{-1}a^{-1}a'x = a^{-1}a'$.
- $a, a' \in UB_r \implies a^{-1}a' \in UB_r$ (όντας $UB_r \leqslant B_{r+s}$).

Επίθεση ωμής βίας (εκδοχή Γ΄):
Να βρεθεί $a' \in UB_r$, τέτοιο ώστε $x^{-1}a^{-1}a'x \in UB_r$.

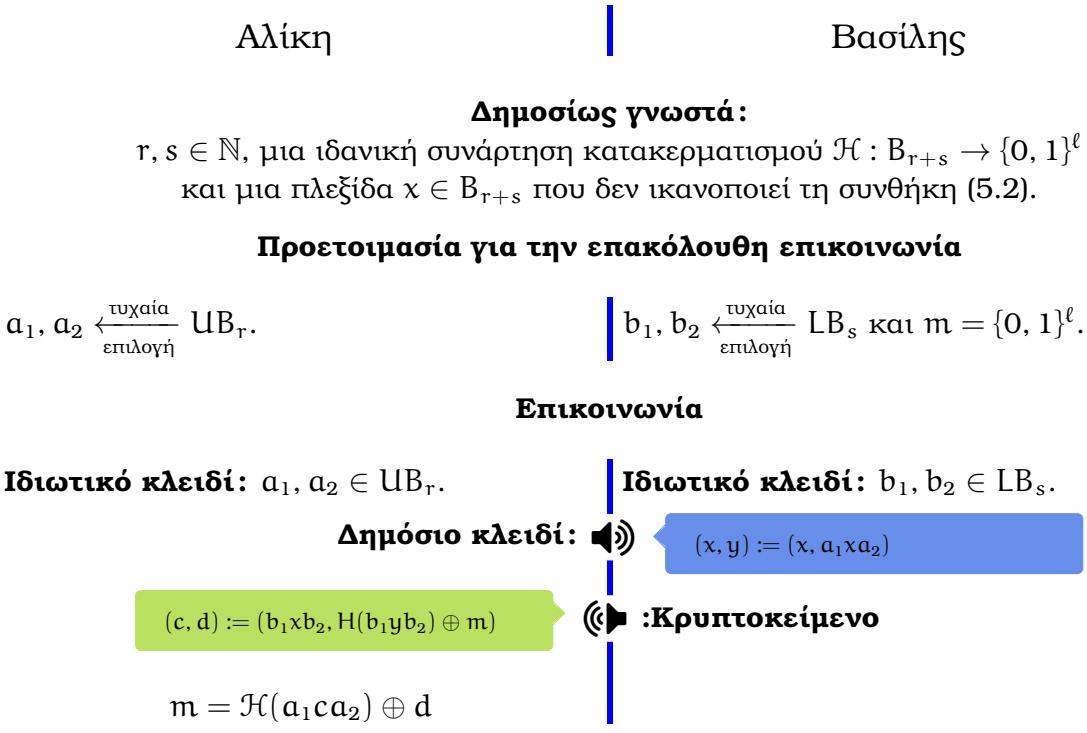
η επίτευξη της οποίας συνδέεται με την επίλυση του προβλήματος ανάλυσης της συζυγίας.

5.3.2.Β΄ Επίθεση με χρήση συνόλων υπερ-κορυφής

Οι F. Garside στην [Ga69], W. Thurston στην [ECHLPT92], E. El-Rifai και H. Morton στην [EM94] και J. Birman, K. Ko και S. Lee στην [BKL98] παρέχουν αλγορίθμου για την εύρεση ενός $a \in B_{r+s}$ (όχι στο UB_r όπως ζητείται). Συνεπώς, η δοκιμή μιας τέτοιας επίθεσης θα αποτύγχανε.

5.4 Το κρυπτοσύστημα των Cha-Ko-Lee-Han-Cheon

Οι Jae Choon Cha, Ki Hyoung Ko, Sang Ji Lee, Jae Woo Han και Jung Hee Cheon προτείνουν στην εργασία του [CKLHC01] την ακόλουθη γενίκευση του Σχήματος 5.2:



Σχήμα 5.3: Το κρυπτοσύστημα Cha-Ko-Lee-Han-Cheon

Σύνδεση με το Σχήμα 5.2. Θέτοντας $a_2 = a_1^{-1}$ και $b_2 = b_1^{-1}$, προκύπτει το Σχήμα 5.2.

Σημειώνεται πως για το δημόσιο κλειδί $(x, a_1 x a_2) \in B_n \times B_n$, ενδέχεται να υπάρχουν πολλά ψευδο-κλειδά, ήτοι να $(\exists z_1, z_2 \in UB_r)[z_1 \neq a_1 \wedge z_2 \neq a_2 \wedge z_1 x z_2 = a_1 x a_2]$. Κάθε τέτοιο ψευδο-κλειδί μπορεί να αποκρυπτογραφήσει επιτυχώς το κρυπτοκείμενο. [Η §5.4.1 βρίσκει ψευδοκλειδιά στις θετικές πλεξίδες.]

Το υποκείμενο πρόβλημα στο οποίο στηρίζεται η ασφάλεια του Σχήματος 5.3 είναι

Το πρόβλημα BPKE[§]**.** Δοθέντων $x, y \in B_n$ να βρεθεί ένα ζεύγος $(a_1, a_2) \in UB_r \times UB_r$, τέτοια ώστε $y = a_1 x a_2$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος.

5.4.1 Σπάσιμο του κρυπτοσυστήματος για θετικές πλεξίδες

Θεωρείται το ανάλογο του BPKE προβλήματος στις θετικές πλεξίδες:

Το πρόβλημα BPKE_+**.** Δοθέντων $x, y \in B_n^+$ να βρεθεί ένα ζεύγος $(a_1, a_2) \in UB_r^+ \times UB_r^+$, τέτοιο ώστε $y = a_1 x a_2$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος.

Σύμβαση. Στα παρακάτω $m = r = s$, όπου $m := \lfloor n/2 \rfloor$.

Ως $\rho_n : B_s \longrightarrow GL(s, \mathbb{Z}[t^{\pm 1}])$ συμβολίζεται η αναπαράσταση του Burau [βλ. §1.3.3].

Υπολογισμός των $\rho_m(a_1), \rho_m(a_2) \in GL(m, \mathbb{Z}[t^{\pm 1}])$ **από το** $(x, a_1 x a_2) \in B_n^+ \times B_n^+$**.**

Έστω $(x, y) \in B_n^+ \times B_n^+$, με $y = a_1 x a_2$, για $a_1, a_2 \in UB_m^+$. Υπάρχει $(A_1', A_2') \in GL(m, \mathbb{Z}[t^{\pm 1}])$, ώστε

(i) Για $i = 1, 2$, υπάρχει $A_i' = \begin{bmatrix} A_i & 0 \\ 0 & I_{n-m} \end{bmatrix} \in GL(m, \mathbb{Z}[t^{\pm 1}])$, με $A_i \in GL\left(m, \mathbb{Z}[t]\right)$.

(ii) $\rho_n(y) = A_1' \rho_n(x) A_2'$.

Θεωρώντας

$$\rho_n(x) = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix} \qquad\qquad \rho_n(y) = \begin{bmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{bmatrix}$$

όπου $X_1, Y_1 \in \mathbb{M}_m\big(\mathbb{Z}[t]\big)$, $X_2, Y_2 \in \mathbb{M}_{m,n-m}\big(\mathbb{Z}[t]\big)$, $X_3, Y_3 \in \mathbb{M}_{n-m,m}\big(\mathbb{Z}[t]\big)$ καθώς και $X_4, Y_4 \in \mathbb{M}_{n-m}\big(\mathbb{Z}[t]\big)$, τότε λόγω του γεγονότος ότι $\rho_n(y) = A_1' \rho_n(x) A_2'$ προκύπτει το σύστημα εξισώσεων

$$\begin{aligned} Y_1 &= A_1 X_1 A_2 & \qquad Y_4 &= X_4 \\ Y_2 &= A_1 X_2 & \qquad Y_3 &= X_3 A_2 \end{aligned} \tag{5.3}$$

Θεωρώντας τις εξισώσεις (5.3), εάν τουλάχιστον εις εκ των X_2, X_3 είναι πλήρους τάξεως, τότε οι $A_1, A_2 \in GL\left(m, \mathbb{Z}[t]\right)$ καθορίζονται μοναδικώς.

Συγκεκριμένα εάν $m = n/2 \in \mathbb{N}$, τότε ισχύει

$$\operatorname{rank}(X_i) = m \iff \mathbb{Z}[t] \ni \det(X_i) \neq 0$$

[§]Braid group Public Key Encryption scheme

Επίσης,

- αποδεικνύεται πως εάν υπάρχει $t_0 \in \mathbb{Z}$, τέτοιο ώστε $\operatorname{rank}(X_i\big|_{t=t_0}) = m$, τότε $\operatorname{rank}(X_i) = m$, όπου $i \in \{1, 2\}$.
- πειραματικά επαληθεύεται πως όσο αυξάνει το $|x| \in \mathbb{N}$, αυξάνει και η πιθανότητα ώστε $\max\{\operatorname{rank}(X_i) \in \mathbb{N} : i = 1, 2\} = m$.

Έστω –χωρίς βλάβη της γενικότητος– ότι $\operatorname{rank}(X_3) = m$. Για $A_2 = (a_2^{ij}) \in \mathbb{M}_{m,n-m}\big(\mathbb{Z}[t]\big)$, έπεται πως $(\forall i = 1, \dots, m)(\forall j = 1, \dots, n-m)\big[a_2^{ij} \in \mathbb{Z}[t]\big]$. Ισχύει ότι

$$\max\left\{ \deg a_2^{ij} \in \mathbb{N}_0 : \begin{matrix} i = 1, \dots, m, \\ j = 1, \dots, n-m \end{matrix} \right\} \leqslant |a_2| \leqslant \sup(a_2)\frac{m(m-1)}{2} \leqslant \frac{sm(m-1)}{2}$$

όπου $m = \lfloor n/2 \rfloor$ και το s είναι το άνω φράγμα του $\sup(a_2)$ στην UB_m.

Παρατήρηση 5.3. *Για την ακρίβεια είναι* $|a_2| = -(t_0)^{-1}\log\big(\det(A_2\big|_{t=t_0})\big)$, *μιας και ισχύει πως* $(\forall j = 1, \dots, n-1)[\det(\rho_m(\sigma_j)) = -t]$.

Κατόπιν, εκτελούνται τα ακόλουθα βήματα:

1: $Q \leftarrow \varnothing$;
2: **για κάθε** $(t_0 \in \{z \in \mathbb{Z} : \operatorname{rank}(X_3\big|_{t=t_0}) = m\})$
3: Υπολογισμός των $X_3\big|_{t=t_0}$ και $Y_3\big|_{t=t_0}$;
4: Υπολογισμός του $A_2\big|_{t=t_0}$ χρησιμοποιώντας την απαλοιφή Gauss-Jordan;
5: $Q \leftarrow Q \cup \{(t_0, A_2\big|_{t=t_0})\}$;
6: **τέλος για**
7: Υπολογισμός του A_2 με χρήση παρεμβολής κατά Lagrange στην Q;

[Η επανάληψη εκτελείται $|a_2|+1$ φορές. Η απαλοιφή Gauss-Jordan απαιτεί χρόνο $\mathcal{O}(m^2)$, ενώ η παρεμβολή Lagrange χρόνο $\mathcal{O}(m^2|a_2|^2)$. Συνολικά, η παραπάνω διαδικασία απαιτεί $(|a_2|+1)\mathcal{O}(m^3) + \mathcal{O}(m^2|a_2|^2) = \mathcal{O}(m^2|a_2|^2)$ χρόνο –δεδομένου ότι $|a_2| > m$.]

Υπολογισμός του $a \in UB_m$ **από την** $\rho_m(a) \in \mathrm{GL}(m, \mathbb{Z}\big[t^{\pm 1}\big])$

Δεδομένου ενός $\rho_m(a) \in \mathrm{GL}(m, \mathbb{Z}\big[t^{\pm 1}\big])$, για κάποιο $a \in UB_m^+$, με $|a| = l$, σκοπός της Υποενότητας είναι η εύρεση ενός αλγορίθμου ο οποίος θα επιστρέφει μία ακολουθία $\big(A[1], \dots, A[l]\big) \in \{1, \dots, n-1\}^l$, τέτοια ώστε $a = \sigma_{A[1]} \cdots \sigma_{A[l]}$ (ως λέξη των Artin γεννητόρων).

Στα παρακάτω συμβολίζεται:

- ως $\rho_m(a)_{i,j} \in \mathbb{Z}[t]$ το στοιχείο στη θέση (i, j) του $\rho_m(a) \in \mathrm{GL}(m, \mathbb{Z}\big[t^{\pm 1}\big])$.
- ως $\rho_m(a)_{\bullet,j} \in \mathbb{Z}[t]$ η στήλη j του $\rho_m(a) \in \mathrm{GL}(m, \mathbb{Z}\big[t^{\pm 1}\big])$.

Έστω $M = \max\{\deg(\rho_m(a)_{i,j}) \in \mathbb{N}_0 : i,j = 1,2,\dots,n\}$. Ορίζεται

$$c'\big(\rho_m(a)\big) := \min\Big\{j \in \{1,\dots,m-1\} : \rho_m(a)_{\bullet,j+1} \in t\mathbb{Z}[t] \text{ και } \max\{\rho_m(a)_{i,j} \in \mathbb{N}_0 : i = 1,\dots,m\} = M\Big\}$$

Στην εργασία τους [LePa03], οι Eokyung Lee και Hong Park παρέχουν τον εξής:

Αλγόριθμος 5.4 Ανάκτηση της $a \in UB_m^+$ από τον $\rho_m(a) \in GL(m, \mathbb{Z}[t^{\pm 1}])$.

Είσοδος: $\rho_m(a) \in GL(m, \mathbb{Z}[t^{\pm 1}])$.
Έξοδος: $z \in UB_m^+$, τέτοιο ώστε $\rho_m(z) = \rho_m(a)$.

για ($i = l$ **έως** 1 **με βήμα** -1)
  $j \leftarrow c'\big(\rho_m(a)\big)$;
  εάν (δεν υπάρχει τέτοιο $j \in \{1,\dots,m\}$) **τότε**
    έξοδος από την επανάληψη;
  τέλος εάν
  $A[i] \leftarrow j$; /* Απομνημόνευση του σ_j */
  $\rho_m(a) \leftarrow \rho_m(a)\rho_m(\sigma_j)^{-1}$; /* Διαγραφή του σ_j */
τέλος για
επίστρεψε $\sigma_{A[i+1]} \cdots \sigma_{A[l]}$;

Η απόδειξη ορθότητας του Αλγορίθμου 5.4 καθώς και ένας πιο εξεζητημένος αλγόριθμος που ανακτά την $x \in UB_m^+$ από τον $\rho_m(a) \in GL(m, \mathbb{Z}[t^{\pm 1}])$ περιέχονται στην [LePa03].

Ανάκτηση του ιδιωτικού κλειδιού επιλύοντας το BPKE$_+$

Έστω $x, y \in B_n^+$ το δημόσιο κλειδί και $a_1, a_2 \in UB_r^+$ το ιδιωτικό κλειδί στο Σχήμα 5.3, ήτοι $y = a_1 x a_2$. Το $\inf(x) \in \mathbb{Z}$ είναι υπολογίσιμο, άρα έστω ένα $u \in 2\mathbb{Z}$, ώστε $x' := \Delta_n^u x \in B_n^+$. Υπολογίσιμα είναι και τα $\inf(a_1), \inf(a_2) \in \mathbb{Z}$, κι έστω $\nu = \inf\{\inf(a_1), \inf(a_2)\}$. (Κάτωθι ως Δ_L νοείται η θεμελιώδης πλεξίδα στην (υπο)ομάδα UB_r, όμως επειδή $UB_r \simeq B_r$, είναι $\Delta_L \equiv \Delta_r$.)

⟦Για $\nu < 0$⟧: Έστω $y' := \Delta_L^{-\nu}\Delta_n^u y \Delta_L^{-\nu} \in B_n$. Ισχύει ότι $\Delta_n^{-\nu} a_1, a_2 \Delta_n^{-\nu} \in UB_r$ (εξ ορισμού του $\nu \in \mathbb{Z}$). Άρα, δεδομένων των $x', y' \in B_n^+$, αρκεί να βρεθούν $P_1, P_2 \in UB_r^+$, τέτοια ώστε $y' = P_1 x' P_2$. Πράγματι, επιλύοντας το BPKE$_+$ για τα $x', y' \in B_n^+$, παρέχονται $P_1, P_2 \in UB_r^+$, με $y' = P_1 x' P_2$. Ορίζονται $z_1 := \Delta_L^\nu P_1$ και $z_2 := P_2 \Delta_L^\nu$. Επομένως, $z_1, z_2 \in UB_r$ και $z_1 x z_2 = (\Delta_L^\nu P_1) x (P_2 \Delta_L^\nu) = \Delta_n^{-u}\Delta_L^\nu P_1 x P_2 \Delta_L^\nu = \Delta_n^{-u}\Delta_L^\nu y' \Delta_L^\nu = y$. Συνεπώς, το ζεύγος $(z_1, z_2) \in UB_r^+ \times UB_r^+$ υποκαθιστά καθόλα το ιδιωτικό κλειδί $(a_1, a_2) \in UB_r^+ \times UB_r^+$.

⟦Για $\nu \geqslant 0$⟧: Έστω $y' := \Delta_n^u y$. Με παρόμοιο τρόπο όπως παραπάνω, προκύπτει το εναλλακτικό ιδιωτικό κλειδί $(z_1, z_2) \in UB_r^+ \times UB_r^+$.

Κεφάλαιο 6

Τα πρωτόκολλα των Anshel-Anshel-Goldfeld

Ένα πιο εξεζητημένο σχήμα ανταλλαγής κλειδιού σε σχέση με εκείνο των Ko, Lee και λοιπών είναι αυτό των Iris Anshel, Michael Anshel και Dorian Goldfeld που δημοσιεύεται στο [AAG99].

6.1 Ένα θεωρητικό πρωτόκολλο

Έστω μία πεντάδα $(\mathbf{U}, \mathbf{V}, \beta, \gamma_1, \gamma_2)$, όπου

- Τα $(\mathbf{U}, *)$, $(\mathbf{V}, \cdot)$ είναι μονοειδή.
- Οι συναρτήσεις

$$\beta : \mathbf{U} \times \mathbf{U} \longrightarrow \mathbf{V}, \qquad \gamma_1, \gamma_2 : \mathbf{U} \times \mathbf{V} \longrightarrow \mathbf{V}$$

ικανοποιούν τις εξής ιδιότητες:

(i) $(\forall x, y_1, y_2 \in \mathbf{U})\big[\beta(x,\ y_1 * y_2) = \beta(x,\ y_1) \cdot \beta(x, y_2)\big]$.

(ii) $(\forall x, y \in \mathbf{U})\big[\gamma_1(x,\ \beta(y, x)) = \gamma_2(y,\ \beta(x, y))\big]$.

(iii) Δεδομένων των $y_1, y_2, \ldots, y_k \in \mathbf{U}$ και $\beta(x, y_1), \beta(x, y_2), \ldots, \beta(x, y_k) \in \mathbf{V}$, είναι υπολογιστικά δύσκολο να βρεθεί το $x \in \mathbf{U}$.

Έτσι προκύπτει το εξής σχήμα:

Δημοσίως γνωστά: Υπομονοειδή $S_A, S_B \subseteq U$, τα οποία παράγονται από τα σύνολα $\{s_1, \ldots, s_m\}$ και $\{t_1, \ldots, t_n\}$ αντίστοιχα.

Κλειδιά:

της Αλίκης:

Ιδιωτικό: $a = s_{i_1}^{\delta_1} * \ldots * a_{i_k}^{\delta_k} \in S_A$.

Δημόσιο: $\big(\beta(a, t_1), \ldots, \beta(a, t_n)\big)$.

του Βασίλη:

Ιδιωτικό: $b = t_{j_1}^{\zeta_1} * \ldots * t_{j_r}^{\zeta_r} \in S_B$.

Δημόσιο: $\big(\beta(b, s_1), \ldots, \beta(b, s_m)\big)$.

Υπολογισμοί:

της Αλίκης:

$$K_A := \gamma_1\big(a, \beta(b, s_{i_1})^{\delta_1} \cdot \ldots \cdot \beta(b, s_{i_k})^{\delta_k}\big) \overset{\text{(i)}}{=} \gamma_1\big(a, \beta(b, s_{i_1}^{\delta_1} * \ldots * s_{i_k}^{\delta_k})\big) = \gamma_1\big(a, \beta(b, a)\big)$$

του Βασίλη:

$$K_B := \gamma_2\big(b, \beta(a, t_{j_1})^{\zeta_1} \cdot \ldots \cdot \beta(a, t_{j_r})^{\zeta_r}\big) \overset{\text{(i)}}{=} \gamma_2\big(b, \beta(a, t_{j_1}^{\zeta_1} * \ldots * t_{j_r}^{\zeta_r})\big) = \gamma_2\big(b, \beta(a, b)\big)$$

Κοινό κλειδί: $K = \gamma_1\big(a,\ \beta(b, a)\big) \overset{\text{(ii)}}{=} \gamma_2\big(b,\ \beta(a, b)\big)$.

Η ασφάλεια του σχήματος εδράζεται στην ιδιότητα (iii) παραπάνω.

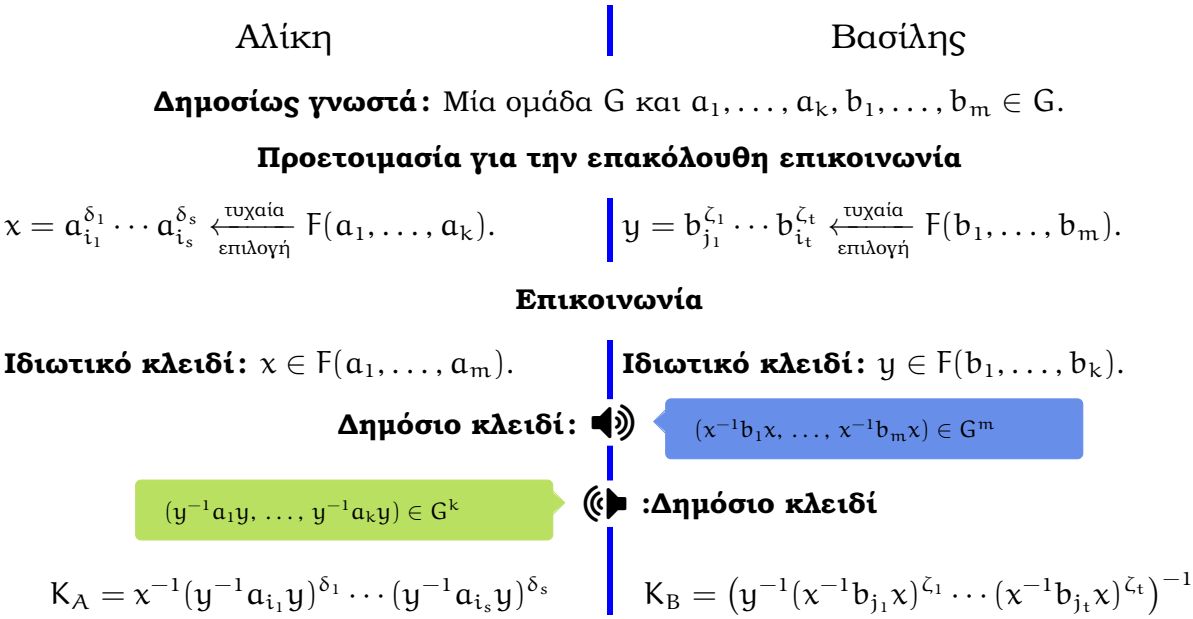
6.2 Το πρωτόκολλο των Anshel-Anshel-Goldfeld

Θεωρώντας στο σχήμα της §6.1

- $\mathbf{U} = \mathbf{V} = G$, για μια ομάδα G και
- $\beta, \gamma_1, \gamma_2 : G \times G \longrightarrow G$, με

$$\beta(x, y) := x^{-1}yx, \qquad \gamma_1(u, v) := u^{-1}v, \qquad \gamma_2(u, v) := v^{-1}u$$

προκύπτει το κλασσικό πρωτόκολλο των Anshel-Anshel-Goldfeld.



$$\begin{aligned} K_A &= x^{-1}(y^{-1}a_{i_1}y)^{\delta_1} \cdots (y^{-1}a_{i_s}y)^{\delta_s} = \\ &= x^{-1}(y^{-1}a_{i_1}^{\delta_1}y) \cdots (y^{-1}a_{i_s}^{\delta_s}y) = x^{-1}y^{-1}a_{i_1}^{\delta_1} \cdots a_{i_s}^{\delta_s}y = x^{-1}y^{-1}xy \end{aligned}$$

και

$$\begin{aligned} K_B &= \left(y^{-1}(x^{-1}b_{j_1}x)^{\zeta_1} \cdots (x^{-1}b_{j_t}x)^{\zeta_t}\right)^{-1} = \left(y^{-1}(x^{-1}b_{j_1}^{\zeta_1}x) \cdots (x^{-1}b_{j_t}^{\zeta_t}x)\right)^{-1} \\ &= \left(y^{-1}x^{-1}b_{j_1}^{\zeta_1} \cdots b_{j_t}^{\zeta_t}x)\right)^{-1} = \left(y^{-1}x^{-1}yx\right)^{-1} = x^{-1}y^{-1}xy \end{aligned}$$

Σχήμα 6.1: Το σχήμα ανταλλαγής κλειδιού Anshel-Anshel-Goldfeld

Στο τέλος του πρωτοκόλλου οι οντότητες καταλήγουν σε μια (συνήθως διαφορετική) μορφή του $K \in G$. Εάν υπάρχει αλγόριθμος που να υπολογίζει εύκολα τις κανονικές μορφές των στοιχείων της G, τότε αυτός εφαρμόζεται. Ωστόσο, υπάρχουν ομάδες με αργό αλγόριθμος υπολογισμού κανονικών μορφών, αλλά με γρήγορο αλγόριθμο επιλύσεως του προβλήματος της λέξης. Εν τοιαύτη περιπτώσει ο Βασίλης μπορεί να στείλει μία άλλη μορφή του K_B στην Αλίκη, ή ένα στοιχείο που δεν σχετίζεται με το K_B κι εκείνη να επαληθεύσει επιλύοντας το πρόβλημα της λέξης στην G εάν στάλθηκε το K ή όχι. Σε καταφατική απάντηση σημειώνεται το δυφίο 1, ειδάλλως σημειώνεται το 0. Επαναλαμβάνοντας την άνωθεν διαδικασία $\ell \in \mathbb{N}$ φορές, συμφωνούν σε κοινή μορφή κλειδιού.

Η δυσκολία στην παρείσφρηση στο Σχήμα 6.1 φαινομενικά* εκφέρεται από

Το πρόβλημα της πολλαπλής ταυτόχρονης συζυγίας. Δεδομένων μιας ομάδας G και $x_1, \ldots, x_n, a^{-1}x_1a, \ldots, a^{-1}x_na$, για κάποιο (μυστικό) $a \in G$, να βρεθεί το $a \in G$.

*Για την αποσαφήνιση βλ. §7.2.

6.3 Το πρωτόκολλο των Anshel-Anshel-Fisher-Goldfeld

6.3.1 Η χρωματισμένη αναπαράσταση Burau

Η **ανηγμένη αναπαράσταση Burau** ορίζεται ως η απεικόνιση

$$\rho_n : B_n \longrightarrow GL(n-1, \mathbb{Z}\left[t^{\pm 1}\right]), \qquad \rho_n(\sigma_i) := C_i(t)$$

όπου

$$C_1(t) = \left(\begin{array}{cc|c} -t & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & I_{n-3} \end{array}\right) \quad C_i(t) = \left(\begin{array}{c|ccc|c} I_{i-2} & & 0 & & 0 \\ \hline & 1 & 0 & 0 & \\ 0 & t & -t & 1 & 0 \\ & 0 & 0 & 1 & \\ \hline 0 & & 0 & & I_{n-i-2} \end{array}\right) \quad C_{n-1}(t) = \left(\begin{array}{c|cc} I_{n-3} & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & t & -t \end{array}\right)$$

όπου παραπάνω είναι $2 \leqslant i \leqslant n-2$.

Ισχύει ότι

$$\begin{aligned} C_i(t)C_j(t) &= C_j(t)C_i(t), && |i-j| \geqslant 2 \\ C_i(t)C_{i+1}(t)C_i(t) &= C_{i+1}(t)C_i(t)C_{i+1}(t), && i = 1, 2, \ldots, n-2 \end{aligned}$$

κι άρα η $\rho : B_n \longrightarrow GL(n-1\mathbb{Z}\left[t^{\pm 1}\right])$ είναι ομομορφισμός ομάδων.

Επιπλέον,

$$C_1^{-1}(t) = \left(\begin{array}{cc|c} -1/t & 1/t & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & I_{n-3} \end{array}\right) \qquad C_{n-1}^{-1}(t) = \left(\begin{array}{c|cc} I_{n-3} & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 1/t & -1/t \end{array}\right)$$

$$C_i^{-1}(t) = \left(\begin{array}{c|ccc|c} I_{i-2} & & 0 & & 0 \\ \hline & 1 & 0 & 0 & \\ 0 & 1 & -1/t & 1/t & 0 \\ & 0 & 0 & 1 & \\ \hline 0 & & 0 & & I_{n-i-2} \end{array}\right) \qquad \text{(για } 2 \leqslant i \leqslant n-2\text{)}$$

Παράδειγμα 6.1. Στην B_3 ισχύει ότι

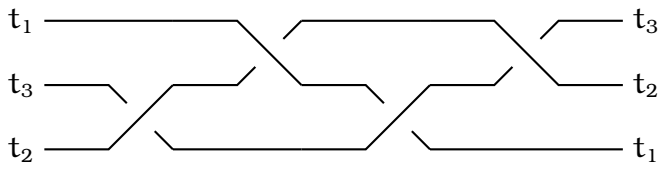
$$\begin{aligned} \rho_3(\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2) &= \rho_3(\sigma_1^{-1})\rho_3(\sigma_2)\rho_3(\sigma_1^{-1})\rho_3(\sigma_2) \\ &\qquad \text{(όντας η } \rho_3 : B_3 \longrightarrow GL(2, \mathbb{Z}\left[t^{\pm 1}\right]) \text{ ομομορφισμός)} \\ &= \begin{pmatrix} -1/t & 1/t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ t & -t \end{pmatrix}\begin{pmatrix} -1/t & 1/t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ t & -t \end{pmatrix} \\ &= \begin{pmatrix} 1/t^2 - 2/t - t + 1 & -1/t + t - 1 \\ -t^2 + t - 1 & t^2 - t \end{pmatrix} \end{aligned}$$

⊣

Φέρνοντας κατά νου την οπτικοποίηση των n-πλεξίδων [βλ. §1.3.1.Β΄] επισυνάπτονται ετικέτες στα σχοινιά της n-πλεξίδας ως εξής:

> η ετικέτα t_j, $1 \leqslant j \leqslant n$ επισυναπτεται στο σχοινί που βρίσκεται στη θέση $n-j-1$ (απαριθμώντας από το ανώτερο) στο *τέλος* (στο δεξιό μέρος) της n-πλεξίδας.

Τοποθετώντας ετικέτες στην 3-πλεξίδα του Σχήματος 6.1 προκύπτει:



Σχήμα 6.2: Η πλεξίδα $\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2 \in B_3$ με ετικέτες

Ορισμός 6.2. Έστω $w \in B_n$, όπου $w = \sigma_{i_1}^{\delta_1}\sigma_{i_2}^{\delta_2}\cdots\sigma_{i_k}^{\delta_k}$, με $\delta_1, \delta_2, \ldots, \delta_k \in \{\pm 1\}$. Ως t_{j_r} νοείται η ετικέτα του σχοινιού που διέρχεται από κάτω στην r-οστή τομή (μετρώντας από τ΄ αριστερά προς τα δεξιά της πλεξίδας). Ο **χρωματισμένος πίνακας Burau** $M_\alpha(t_1, \ldots, t_n) \in \mathrm{GL}(n-1, \mathbb{Z}\big[t_1^{\pm 1}, \ldots, t_n^{\pm 1}\big])$ της $w \in B_n$ ορίζεται ως

$$M_w(t_1, \ldots, t_n) := \prod_{r=1}^{k} \big(C_{i_r}(t_{j_r})\big)^{\delta_r}$$

όπου ο $C_{i_r}(t_{j_r}) \in \mathbb{Z}\big[t_{j_r}^{\pm 1}\big]$, $r = 1, 2, \ldots, k$ είναι ο πίνακας της ανηγμένης αναπαράστασης Burau.

Παράδειγμα 6.3. Στην B_3 ισχύει ότι

$$\begin{aligned} M_{\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2}(t_1, t_2, t_3) &= C_1(t_3)^{-1}\, C_2(t_2)\, C_1(t_1)^{-1}\, C_2(t_3) \qquad \text{(βλ. Σχήμα 6.2)} \\ &= \begin{pmatrix} -t_3^{-1} & t_3^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t_2 & -t_2 \end{pmatrix} \begin{pmatrix} -t_1^{-1} & t_1^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t_3 & -t_3 \end{pmatrix} \\ &= \begin{pmatrix} -1/t_1 - t_2 + t_2/t_1 + \frac{1}{t_1 t_3} - t_2/t_1 t_3 & 1/t_1 + t_2 - t_2/t_1 \\ -t_2/t_1 - t_2 t_3 + t_2 t_3/t_1 & t_2 t_3 - t_2 t_3/t_1 \end{pmatrix} \end{aligned}$$

(αντιπαραβολή με το Παράδειγμα 6.1.) ⊣

Ορισμός 6.4. Η **χρωματισμένη ομάδα Burau** ορίζεται ως η δομή $\mathrm{CB}_n \equiv (\mathrm{CB}_n, *)$, όπου

- $\mathrm{CB}_n := \mathrm{S}_n \times \mathrm{GL}(n-1, \mathbb{Z}\big[t_1^{\pm 1}, \ldots, t_n^{\pm 1}\big])$
- $* : \mathrm{CB}_n \times \mathrm{CB}_n \longrightarrow \mathrm{CB}_n$, με $(\alpha_1, M_1) * (\alpha_2, M_2) := (\alpha_1\alpha_2, (\alpha_2^{-1} \cdot M_1)M_2)$

για τη δράση $\cdot : \mathrm{S}_n \times \mathrm{CB}_n \longrightarrow \mathrm{CB}_n$, με

$$\alpha \cdot \big(f_{ij}(t_1, \ldots, t_n)\big)_{1 \leqslant i,j \leqslant n-1} := \big(f_{ij}(t_{\alpha(1)}, \ldots, t_{\alpha(n)})\big)_{1 \leqslant i,j \leqslant n-1}$$

Από τον Ορισμό συνάγεται για την CB_n ότι

(i) Το $(\mathrm{id}_{\mathrm{S}_n},\ \mathrm{I}_{n-1})$ είναι το ταυτοτικό στοιχείο της CB_n.

(ii) $(\alpha,\ M)^{-1} = (\alpha^{-1},\ \alpha^{-1} \cdot M)$.

Ορισμός 6.5. Η **χρωματισμένη αναπαράσταση Burau** θεωρείται ως η απεικόνιση

$$\begin{aligned} \mathfrak{c} \equiv \mathfrak{c}_n : \mathrm{B}_n &\longrightarrow \mathrm{CB}_n \\ \sigma_i \xrightarrow{\mathfrak{c}} &\big((i,\ i+1),\ \mathrm{C}_i(t_{i+1})\big) \qquad (\text{για } i = 1, 2, \ldots, n-2) \end{aligned}$$

Λήμμα 6.6. *Η χρωματισμένη αναπαράσταση Burau:*

1. *είναι ομομορφισμός ομάδων (ικανοποιεί του συσχετιστές της* B_n*) και*
2. $(\forall \alpha \in \mathrm{B}_n)\big[\mathfrak{c}(a) = (\pi_\alpha,\ M_\alpha)\big]$, *όπου η* $\pi_a \in \mathrm{S}_n$ *είναι επαγόμενη μετάθεση και ο* $M_a \in \mathrm{GL}(n-1, \mathbb{Z}\big[t_1^{\pm 1}, \ldots, t_n^{\pm 1}\big])$ *είναι ο πίνακας που παρέχεται από τον Ορισμό 6.2.*

6.3.2 Το σχήμα ανταλλαγής κλειδιού των Anshel-Anshel-Fisher-Goldfeld

Έστω

- ένας (μικρός) πρώτος αριθμός $p \in \mathbb{N}$ και
- $\mathcal{K}_{n,p} := \mathrm{S}_n \times \mathrm{GL}(n-1,\ \mathbb{F}_p)$ (ο χώρος των πιθανών κλειδιών).

Ορισμός 6.7. Θεωρούνται τα αντιστρέψιμα $\tau_1, \ldots, \tau_n \in \mathbb{F}_p$, για τα οποία ισχύει ότι $(\forall i, j = 1, 2, \ldots, n)[i \neq j \implies \tau_i \neq \tau_j]$. Ορίζεται

$$\mathbb{E} \equiv \mathbb{E}_{p,\tau_1,\ldots,\tau_n} : \mathrm{B}_n \longrightarrow \mathcal{K}_{n,p} \qquad \mathbb{E}(a) := \big(\pi_a,\ M_a(\tau_1, \ldots, \tau_n) \mod p\big)$$

όπου ως $M_a(\tau_1, \ldots, \tau_n) \mod p$ νοείται ως η εφαρμογή της πράξης $\mathrm{mod}\ p$ σε κάθε στοιχείο του $M_a(\tau_1, \ldots, \tau_n) \in \mathrm{GL}(n-1, \mathbb{F}_p)$.

Πρόταση 6.8 ([AAFG01])**.** Θεωρούνται $\alpha \in \mathrm{B}_n$ και $\tau_1, \ldots, \tau_n \in \mathbb{F}_p$ αντιστρέψιμα και διακεκριμένα. Υπάρχει αλγόριθμος που υπολογίζει το $\mathbb{E}_{p,\tau_1,\ldots,\tau_n}(\alpha) \in \mathcal{K}_{n,p}$ σε χρόνο $\mathcal{O}(n|\alpha|(\log_2 p)^2)$.

Αλίκη	Βασίλης

Δημοσίως γνωστά:
$G = B_n$, για $p > n > 6$, $a_1, \ldots, a_k, b_1, \ldots, b_m \in G = B_n$ (στο Σχήμα 6.1)
και (επιπλέον των υποθέσεων του Σχήματος 6.1) $\tau_1, \ldots, \tau_n \in \mathbb{F}_p$.

Προετοιμασία για την επακόλουθη επικοινωνία
Όπως στο Σχήμα 6.1

Επικοινωνία
Όπως στο Σχήμα 6.1, με το επιπλέον βήμα ότι

Εάν $K'_A \in B_n$ είναι το κλειδί της Αλίκης από το Σχήμα 6.1, τότε	Εάν $K'_B \in B_n$ είναι το κλειδί του Βασίλη από το Σχήμα 6.1, τότε
$K_A = \mathbb{E}(K'_A) = \big(\pi_{K_A},\, M_{K_A}(\tau_1, \ldots, \tau_n)\big) \in \mathcal{K}_{n,p}$	$K_B = \mathbb{E}(K'_B) = \big(\pi_{K_B},\, M_{K_B}(\tau_1, \ldots, \tau_n)\big) \in \mathcal{K}_{n,p}$

Σχήμα 6.3: Το σχήμα ανταλλαγής κλειδιού Anshel-Anshel-Fisher-Goldfeld

6.3.2.Α΄ Προτεινόμενες παράμετροι

Οι κάτωθι παράμετροι παρέχονται από την [AAFG01]:

- Για τον πρώτο αριθμό $p \in \mathbb{N}$ ο μόνος περιορισμός είναι ότι $p > n$, ώστε να μπορούν να επιλεχθούν τα διακεκριμένα και αντιστρέψιμα στοιχεία $\tau_1, \ldots, \tau_n \in \mathbb{F}_p$. Μια καλή επιλογή είναι $p < 1000$.

- $n = 80$ και $k = m = 20$.

- $(\forall i = 1, 2, \ldots, k)\big(\exists r \in \{5, 6, \ldots, 10\}\big)\big(\exists z_1, \ldots, z_r \in \{\pm 1\}\big)\big[\alpha_i = \sigma_{i_1}^{z_1} \cdots \sigma_{i_r}^{z_r}\big]$.
  $(\forall j = 1, 2, \ldots, m)\big(\exists s \in \{5, 6, \ldots, 10\}\big)\big(\exists d_1, \ldots, d_s \in \{\pm 1\}\big)\big[\beta_j = \sigma_{j_1}^{d_1} \cdots \sigma_{j_s}^{d_s}\big]$.

- $x = \prod_{k=1}^{100} \beta_{j_k}^{\zeta_k}$ και $y = \prod_{k=1}^{100} \alpha_{i_k}^{\delta_k}$, όπου $\zeta_1, \delta_1, \ldots, \zeta_{100}, \delta_{100} \in \{\pm 1\}$.

6.4 Κρυπτανάλυση

Παρ' ότι που το Σχήμα 6.3 αποτελεί γενίκευση του Σχήματος 6.1 ωστόσο αποδεικνύεται πως δεν παρέχει περισσότερη ασφάλεια. Για το λόγο αυτό η κρυπτανάλυση αμφοτέρων των σχημάτων πραγματεύεται ταυτόχρονα στην παρούσα Ενότητα, δηλαδή οι ακόλουθοι συλλογισμοί αφορούν και τα δύο σχήματα.

6.4.1 Επίθεση Γραμμικής Άλγεβρας

Χρησιμοποιώντας αποκλειστικά γνήσεις πλεξίδες, η συνάρτηση $\mathbb{E} : B_n \longrightarrow \mathcal{K}_{n,p}$ γίνεται ομομορφισμός ομάδων. Έτσι η παραβίαση του κρυπτοσυστήματος μπορεί να επιτευχθεί με αλγεβρικές μεθόδους. Παρ' όλο που στην [AAFG01] προτείνονται παράμετροι ώστε να αποφευχθούν τέτοιες επιθέσεις, αποδεικνύονται εν τέλει ανεπαρκείς.

Θεωρείται

Το πρόβλημα της λίστας πολλαπλής ταυτόχρονης συζυγίας. Να βρεθούν όλες οι λύσεις που ικανοποιούν ένα στιγμιότυπο του προβλήματος της πολλαπλής ταυτόχρονης συζυγίας.

Θεώρημα 6.9. Εάν οι επαγόμενες μεταθέσεις των ιδιωτικών κλειδιών του Σχήματος 6.3 είναι γνωστές, τότε προκύπτουν τέσσερα προβλήματα λίστας πολλαπλής ταυτόχρονης συζυγίας στην $GL(n-1,\mathbb{F}_p)$, όπου η συναλήθευση των λύσεών τους δίδει τη συντεταγμένη με τον πίνακα του κοινού μυστικού (κλειδιού).

Απόδειξη (σκιαγράφηση). Από τον ορισμό και της ιδιότητες της χρωματισμένης αναπαράστασης Burau προκύπτει ότι

$$\begin{aligned}\mathfrak{c}(x^{-1}y^{-1}xy) &= (\pi_x, M_x)^{-1}(\pi_y, M_y)^{-1}(\pi_x, M_x)(\pi_y, M_y)\\ &= (\pi_x^{-1}, \pi_x M_x^{-1})(\pi_y^{-1}, \pi_y M_y^{-1})(\pi_x, M_x)(\pi_y, M_y)\\ &= \left(\pi_x^{-1}\pi_y^{-1}\pi_x\pi_y,\ (\pi_y\pi_x^{-1}\pi_y\pi_x M_x^{-1})(\pi_y^{-1}\pi_x^{-1}\pi_y M_y^{-1})(\pi_y^{-1}M_x)M_y\right)\end{aligned}$$

Επομενως, η συνιστώσα του πίνακα του κοινού κλειδιού αποτελείται από τους πίνακες

$$(\pi_y^{-1}\pi_x^{-1}\pi_y\pi_x M_x^{-1}),\qquad (\pi_y^{-1}\pi_x^{-1}\pi_y M_y^{-1}),\qquad (\pi_y^{-1}M_x),\qquad M_y \tag{6.1}$$

αποτιμημένους για $(t_1,\ldots,t_n) = (\tau_1,\ldots,\tau_n) \in \mathbb{F}_p^n$, δηλαδή δεδομένων των π_x, π_y, κατασκευάζεται ένα πρόβλημα λίστας πολλαπλής συζυγίας για κάθε έναν από τους παραπάνω (αποτιμημένους) πίνακες που έχει ως λύση του τον (αποτιμημένο) πίνακα ως εξής: Θεωρείται (για παράδειγμα) ο $X = (\pi_y^{-1}M_x)(\tau_1,\ldots,\tau_n)$ και τότε:

Είσοδος: $\{\alpha_i, x^{-1}\alpha_i x \in GL(n-1,\mathbb{F}_p) : i = 1,2,\ldots,r\}$, $\pi_x, \pi_y \in S_n$, $X \in GL(n-1,\mathbb{F}_p)$.

Δεδομένα: $N \in \mathbb{N}$ (το πλήθος των εξισώσεων του προβληματος).

Έξοδος: $W_j, V_j \in GL(n-1,\mathbb{F}_p)$, $j = 1,\ldots,N$, ώστε $W_jX = XV_j$, για $j = 1,\ldots,N$.

1: **για** $(j = 1,2,\ldots,N)$
2: Επιλέγεται $w = \mathcal{U}(\alpha_1,\ldots,\alpha_r)$ (ομοιόμορφα), ώστε να είναι γνήσια πλεξίδα;
3: $v \leftarrow (x^{-1}\alpha_{i_1}x)^{\delta_1}\cdots(x^{-1}\alpha_{i_s}x)^{\delta_s} = x^{-1}wx$ (γνήσια πλεξίδα), όπου $w = \alpha_{i_1}^{\delta_1}\cdots\alpha_{i_s}^{\delta_s}$;
4: Υπολογίζονται οι M_α, M_c;
5: Ισχύει ότι $(\pi_y^{-1}\pi_x^{-1}M_w)(\pi_y^{-1}M_x) = (\pi_y^{-1}M_x)(\pi_y^{-1}M_v)$;
6: **επίστρεψε** $(W_j, V_j) \leftarrow \left((\pi_y^{-1}\pi_x^{-1}M_\alpha)(\tau_1,\ldots,\tau_n),\ (\pi_y^{-1}M_c)(\tau_1,\ldots,\tau_n)\right)$;
7: **τέλος για**

Η γραμμή 5 παραπάνω προκύπτει από το γεγονός πως $wx = xv$ καθώς και από το ότι $\mathfrak{c}(wx) = (\pi_x,\ (\pi_x^{-1}M_w)M_x)$ και $\mathfrak{c}(xv) = (\pi_x,\ M_xM_v)$. Παρόμοια, προκύπτουν τα αντίστοιχα προβλήματα λίστας πολλαπλής συζυγίας για τους υπολοίπους πίνακες (6.1). □

6.4.2 Επίθεση στο ιδιωτικό κλειδί

Σύμβαση. *Θεωρείται ο εσωτερικός αυτομορφισμός* $\tau : B_n \longrightarrow B_n$, *με* $\tau(w) = \Delta_n^{-1} w \Delta_n$.

Ορισμός 6.10. Η πλεξίδα $\alpha \in B_n^+$ καλείται **ουρά** της $\gamma \in B_n^+$ εάν $(\exists \beta \in B_n)[\gamma = \beta\alpha]$.

Τον κινητήριο μοχλό της επίθεσης αποτελεί το

Λήμμα 6.11 ([EM94]). *Έστω* $v, w \in B_n$, *με* $w = \alpha^{-1}v\alpha$, *για κάποιο* $\alpha \in B_n^+$. *Έστω* $w = \Delta_n^r W_1 \cdots W_s$ *η (Garside) κανονική μορφή της* $w \in B_n$. *Εάν* $\inf(w) < \inf(v)$, *τότε* $(\exists \gamma \in B_n)\big[\inf(\gamma) = \inf(x) \wedge \alpha = \gamma\Delta\tau^r(W_1^{-1})\big]$.

το οποίο και υλοποιείται στον παρακάτω

Αλγόριθμος 6.12 $\texttt{MSCP}\big((v_1, w_1), \ldots, (v_m, w_m)\big)$:Επίλυση πολ/πλής ταυτόχρονης συζυγίας.

Είσοδος: $(v_1, w_1), \ldots, (v_m, w_m) \in B_n^2$, τέτοια ώστε $w_i = xv_ix^{-1}$, $i = 1, 2, \ldots, m$, για κάποιο (μυστικό) $x \in B_n^+$.

Έξοδος: $\big(\alpha,\ (c_1, \ldots, c_m)\big) \in B_n^+ \times B_n^m$, τέτοια ώστε $c_i = \alpha w_i \alpha^{-1}$, για κάθε $i = 1, \ldots, m$.

1: $\alpha \leftarrow \varepsilon$;
2: **για** ($i = 1, 2, \ldots, m$
3: $\quad v_i \leftarrow$ κανονική μορφή της v_i;
4: $\quad w_i \leftarrow$ κανονική μορφή της w_i, η οποία μοιάζει ως εξής:

$$w_i = \Delta_n^{r_i} W_1^{(i)} \cdots W_s^{(i)} \tag{6.2}$$

5: $\quad c_i \leftarrow w_i$;
6: **τέλος για**
7: **όσο** $\big((\exists j \in \{1, \ldots, m\})\big[\inf(c_j) < \inf(v_j)\big]\big)$
8: $\quad j \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \big\{k \in \{1, \ldots, m\} : \inf(w_k) < \inf(v_k)\big\}$;
9: $\quad \gamma \leftarrow \Delta_n\tau^{r_j}\big((W_1^{(j)})^{-1}\big)$; $\quad \alpha \leftarrow \gamma\alpha$;
10: $\quad$ **για** ($i = 1, 2, \ldots, m$)
11: $\quad\quad c_i \leftarrow \gamma c_i \gamma^{-1}$;
12: $\quad\quad c_i \leftarrow$ κανονική μορφή της w_i, όπως στην μορφή (6.2);
13: $\quad$ **τέλος για**
14: **τέλος όσο**
15: **επίστρεψε** $\big(\alpha,\ (c_1, \ldots, c_m)\big)$;

Χρονική πολυπλοκότητα του Αλγορίθμου 6.12. Από την Πρόταση 6.11, το $\gamma \in B_n^+$ αποτελεί ουρά του $x \in B_n^+$. Σε κάθε εκτέλεση του βρόχου **όσο**...**τέλος όσο** το $|\gamma| \in \mathbb{N}$ αυξάνεται, άρα ο βρόχος εκτελείται το πολύ $|x| \in \mathbb{N}$ φορές. Επιπλέον,

- ο πολλαπλασιαμός $\gamma c_i \gamma^{-1}$, για $c_i \in B_n$ και γ μία n-πλεξίδα μετάθεσης, απαιτεί $\mathcal{O}(n|c_i| \log_2 n)$ χρόνο·
- ο πολλαπλασιαμός γa απαιτεί $\mathcal{O}(n|a| \log_2 n)$ χρόνο·
- ο υπολογισμός της Garside κανονικής μορφής μιας $w \in B_n$ απαιτεί $\mathcal{O}\big(|w|^2 n \log_2 n\big)$ χρόνο.

Τελικά, η χρονική πολυπλοκότητα του Αλγορίθμου 6.12 είναι

$$\mathcal{O}\left(n|x| \log_2 n\Big(|x| + \sum_{i=1}^{m} \big(|v_i| + |w_i|\big)\Big)\right)$$

6.4.3 Ευριστική επίλυση του προβλήματος της πολλαπλής ταυτόχρονης συζυγίας

Παρατίθενται τα

Θεώρημα 6.13 ([BKL98, EM94, ECHLPT92], Κυκλικότητας)**.** Έστω $w \in B_n$, με (Garside) κανονική μορφή την $w = \Delta_n^u P_1 \cdots P_k$. Ορίζονται η **κύκλωση** και η **αντικύκλωση** της $w \in B_n$ ως

$$\mathbf{c}(w) := \Delta_m^u P_2 \cdots P_k \tau^u(A_1), \qquad \mathbf{d}(w) := \Delta_n^u \tau^{-u}(P_k) P_1 \cdots P_{k-1}$$

1. Εάν το $\inf(w) \in \mathbb{Z}$ δεν είναι μεγιστικό στην κλάση συζυγίας της $w \in B_n$, τότε $(\exists l \in \mathbb{Z})\big[\inf(\mathbf{c}^l(w)) > \inf(w)\big]$.

2. Εάν το $\sup(w) \in \mathbb{Z}$ δεν είναι ελαχιστικό στην κλάση συζυγίας της $w \in B_n$, τότε $(\exists l \in \mathbb{Z})\big[\sup(\mathbf{d}^l(w)) < \sup(w)\big]$.

3. Η μεγιστική τιμή του $\inf(a) \in \mathbb{Z}$ και η ελαχιστική τιμή του $\sup(a) \in \mathbb{Z}$ μπορούν να επιτευχθούν ταυτοχρόνως. Με άλλα λόγια $\mathrm{SSS}(a) \neq \varnothing$.

Θεώρημα 6.14 ([BKL98, EM94, ECHLPT92], Κυρτότητας)**.** Έστω $w = x^{-1} v x$, με $\inf(v) = \inf(w)$ και $\sup(v) = \sup(w)$. Έστω επίσης $x = H_1 H_2 \cdots H_k$ η κανονική μορφή του $x \in B_n$. Ισχύει ότι

$$\inf(H_1^{-1} v H_1) \geqslant \inf(v) \qquad \sup(H_1^{-1} a H_1) \leqslant \sup(a)$$

Μία πρώτη απόπειρα για την επίλυση του προβλήματος της συζυγίας για τα $v, w \in B_n$ (να βρεθεί $x \in B_n$, ώστε $w = x^{-1}vx$) έχει ως εξής:

> Ισχύει ότι $\inf(v) = \inf(\tau(v))$ και $\sup(v) = \sup(\tau(v))$. Από το Θεώρημα 6.14 (Κυρτότητας) εάν οι $v, w \in B_n$ περιέχονται στο ίδιο σύνολο υπερ-κορυφής –έστω S–, τότε υπάρχει μία πεπερασμένη ακολουθία
>
> $$v = a_0 \longrightarrow a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_k = w$$
>
> όπου για κάθε $i = 1, 2, \ldots, k$ ώστε
>
> - $a_i \in S$ και
> - $a_i = P_i^{-1} a_{i-1} P_i$, για κάποια πλεξίδα μετάθεσης $P_i \in B_n$.

Το πρόβλημα της συζυγίας, τώρα, επιλύεται ως ακόλουθα:

Βήμα Α′: Με εφαρμογή του Θεωρήματος 6.13 (Κυρτότητας) στις $a, c \in B_n$ υπολογίζονται οι $v', w' \in B_n$ αντίστοιχα, όπου $v', w' \in S$.

Βήμα Β′: Για κάθε πλεξίδα μετάθεσης A_α, $\alpha \in S_n$, υπολογίζεται η $A_\alpha v A_\alpha^{-1}$ και συλλέγονται εκείνες, με $\inf(A_\alpha v' A_\alpha) = \inf(w')$ και $\sup(A_\alpha v' A_\alpha) = \sup(w')$.

Το Βήμα Α′ του αλγορίθμου εκτελείται σε πολυωνυμικό χρόνο, ενώ το Βήμα Β′ απαριθμεί όλες τις δυνατές $n!$ μεταθέσεις κι άρα απαιτεί εκθετικό, ως προς το n, χρόνο. Έτσι, ανακύπτει η ανάγκη για την δημιουργία ευριστικών (heuristic) διαδικασιών.

Μία απλή παρατήρηση επεκτείνει το Λήμμα 6.11 στο

Λήμμα 6.15 ([EM94]). *Έστω $v, w \in B_n$, με $w = \alpha^{-1} v \alpha$, για κάποιο $\alpha \in B_n^+$. Έστω $w = \Delta_n^r W_1 \cdots W_s$ η (Garside) κανονική μορφή της $w \in B_n$. Ισχύουν τα ακόλουθα:*

(α′) Εάν $\inf(w) < \inf(v)$, τότε $(\exists \gamma \in B_n)\big[\inf(\gamma) = \inf(x) \wedge \alpha = \gamma \Delta_n \tau^r(W_1^{-1})\big]$.

(β′) Εάν $\sup(w) > \sup(v)$, τότε η W_s είναι ουρά της $\alpha \in B_n^+$.

Απόδειξη. (α′) Πρόκειται για το Λήμμα 6.11.

(β′) Προκύπτει παρατηρώντας πως η αντικύκλωση της $w \in B_n$, προκύπτει από την κύκλωση της $w^{-1} \in B_n$. □

Το Λήμμα υποδεικνύει έναν τρόπο ώστε για κάθε πλεξίδα $w \in B_n$ να βρίσκεται μία πλεξίδα από την κλάση συζυγίας της w με ελαχιστικό θεσμικό μήκος, δηλαδή ένα στοιχείο του συνόλου υπερκορυφής της w, $SSS(w)$ (βλ. Ορισμό 1.29· $\big|SSS(w)\big| < +\infty$· για έναν αλγόριθμο υπολογισμού βλ. [EM94]).

Αλγόριθμος 6.16 $\texttt{HMCP}\big((\nu_1, w_1), \ldots, (\nu_m, w_m)\big)$: Ευριστική επίλυση πολλαπλής ταυτόχρονης συζυγίας.

Είσοδος: $(\nu_1, w_1), \ldots, (\nu_m, w_m) \in B_n^2$, τέτοια ώστε $w_i = x\nu_i x^{-1}$, $i = 1, 2, \ldots, m$, για κάποιο (μυστικό) $x \in B_n^+$, με $\inf x = 0$.

Έξοδος: Είτε $\alpha \in B_n^+$, με $(\forall i = 1, 2, \ldots, m)[w_i = \alpha^{-1}\nu_i\alpha]$, είτε "αποτυχία".

$\alpha \leftarrow \varepsilon$;
για $(i = 1, 2, \ldots, m)$
  $\nu_i \leftarrow$ κανονική μορφή της ν_i;
  $w_i \leftarrow$ κανονική μορφή της w_i, όπου η κανονική μορφή μοιάζει ως εξής:

$$w_i = \Delta_n^{r_i} W_1^{(i)} \cdots W_s^{(i)} \tag{6.3}$$

τέλος για
$\big(\gamma, (w_1, \ldots, w_m)\big) \leftarrow \texttt{MCP}\big((\nu_1, w_1), \ldots, (\nu_m, w_m)\big)$; /* Βλ. Αλγόριθμο 6.12 */
όσο $\big(\big(\exists j \in \{1, \ldots, m\}\big)\big[\sup(w_j) > \sup(\nu_j)\big]\big)$
  $j \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \big\{k \in \{1, \ldots, m\} : \sup(w_k) < \sup(\nu_k)\big\}$;
  $\gamma \leftarrow W_s^{(j)}$; $\alpha \leftarrow \gamma\alpha$;
  για $(i = 1, 2, \ldots, m)$
    $w_i \leftarrow \gamma w_i \gamma^{-1}$;
    $w_i \leftarrow$ κανονική μορφή της w_i, όπως στην μορφή (6.3);
  τέλος για
τέλος όσο
$\mu \leftarrow \textsc{ΜαντεψεΤαυτοχρονηΜεταθεση}\big((\nu_1, w_1), \ldots, (\nu_m, w_m)\big)$;
$\alpha \leftarrow \mu\alpha$;
για κάθε $(i = 1, 2, \ldots, m)$ $w_i \leftarrow \mu w_i \mu^{-1}$;
εάν $((\forall i = 1, 2, \ldots, m)[\nu_i = w_i])$ **τότε**
  επίστρεψε α;
αλλιώς
  επίστρεψε "αποτυχία";
τέλος εάν

Παρατήρηση 6.17. *Η απαίτηση $\alpha \in B_n^+$ είναι στον Αλγόριθμο 6.16 είναι άνευ σημασίας. Πράγματι, εάν $w = x^{-1}\nu x$, για κάποιο $x \in B_n$, με κανονική μορφή $x = \Delta_n^r X_1 \cdots X_s$, τότε όντας $\Delta_n^2 \in \mathcal{Z}(B_n)$ [βλ. Πρόταση 1.23-3.], έπεται πως και $w = y^{-1}\nu y$, όπου $y = \Delta_n^{r \bmod 2} X_1 \cdots X_s \in B_n^+$. Όμως $y, \Delta_n^{-1} y \in B_n^+$, με $\inf(y) = 0 = \inf(\Delta_n^{-1} y)$, κι άρα αρκεί να υλοποιηθεί ο Αλγόριθμος 6.16 με επεκτεταμένη είσοδο*

$$\big\{(\nu_i, w_i), (\Delta_n^{-1}\nu_i, \Delta_n^{-1} w_i) \in B_n^2 : i = 1, 2, \ldots, m\big\}$$

Στην γραμμή 15 του Αλγορίθμου 6.16, η προκύπτουσα $w \in B_n$ έχει θεσμικό μήκος μικρότερο ή ίσο από εκείνο της $v \in B_n$ και έχει προκύψει πως $w = x_0^{-1} v x_0$, όπου $x = x_0 \alpha$. Εξ άλλου, όπως αναφέρθηκε και στην ανάλυση της χρονικής πολυπλοκότητας του Αλγορίθμου 6.12, κάθε βρόχος **όσο**...**τέλος όσο** εκτελείται *το πολύ* $|x|$ φορές, έτσι τόσο ο Αλγόριθμος 6.12, όσο και ο Αλγόριθμος 6.16 ενδέχεται να επιστρέψουν την ουρά $\alpha \in B_n^+$ του $x \in B_n^+$ κι όχι το ζητούμενο —ήτοι το $x \in B_n^+$ ώστε $w_i = x v_i x^{-1}$, για κάθε $i = 1, 2, \ldots, m$. Έτσι η συνάρτηση ΜΑΝΤΕΨΕΤΑΥΤΟΧΡΟΝΗΜΕΤΑΘΕΣΗ προσπαθεί να **μαντέψει** μια $\mu \in B_n^+$, τέτοια ώστε $\pi(\mu) = \pi(x_0)$, όπου $w_i = (\mu x_0)^{-1} v_i (\mu x_0)$, για κάθε $i = 1, 2, \ldots, m$. Ακολούθως, παρατίθεται ο αλγόριθμος για την περίπτωση όπου $m = 1$.

Αλγόριθμος 6.18 Η συνάρτηση ΜΑΝΤΕΨΕΜΕΤΑΘΕΣΗ(v, w)

Είσοδος: $(v, w) \in B_n^2$, με $w = xvx^{-1}$, για κάποιο (μυστικό) $x \in B_n^+$, με $\inf x = 0$.
Έξοδος: $\mu \in B_n^+$, με $\pi(\mu) = \pi(x)$.

1: $\tau \leftarrow \mathrm{id}_{S_n}$;
2: $(\chi_1, \ldots, \chi_n) \leftarrow (\xi_1, \ldots, \xi_n) \leftarrow (\text{false}, \ldots, \text{false})$;
3: **για** ($i = n$ **έως** 1 **με βήμα** -1)
4: $\quad r \leftarrow s \leftarrow i$;
5: $\quad$ **όσο** ($\chi_r = \text{false}$)
6: $\quad\quad \chi_r \leftarrow \text{true}$; $r \leftarrow \pi(v)(r)$; $s \leftarrow \pi(w)(s)$;
7: $\quad\quad$ **εάν** ($r \neq s$) **τότε**
8: $\quad\quad\quad \tau(r) \leftarrow s$;
9: $\quad\quad$ **τέλος εάν**
10: $\quad$ **τέλος όσο**
11: **τέλος για**
12: **για** ($i = n,\ 1,\ -1$)
13: $\quad$ **εάν** ($\xi_i = \text{false}$) **τότε**
14: $\quad\quad \xi_i \leftarrow \text{true}$; $r \leftarrow i$;
15: $\quad\quad$ **όσο** ($\xi_{\tau(r)} = \text{false} \wedge \tau(r) \neq r$)
16: $\quad\quad\quad r \leftarrow \tau(r)$; $\xi_r \leftarrow \text{true}$;
17: $\quad\quad$ **τέλος όσο**
18: $\quad\quad \tau(r) \leftarrow i$;
19: $\quad$ **τέλος εάν**
20: **τέλος για**
21: **επίστρεψε** $\pi^{-1}(\tau)$;

Παρατήρηση 6.19. *Ουδείς εκ των Αλγορίθμων 6.16, 6.18 είναι πιθανοτικός, έτσι η επαναλαμβανόμενη εκτέλεσή τους δεν πρόκειται να καλυτερέψει αποτελέσματα προτέρων εκτελέσεων.*

Μερική συζήτηση για τον Αλγόριθμο 6.18. Στις περιπτώσεις όπου η $\nu \in B_n$ είναι γνήσια πλεξίδα, δηλαδή $\pi(\nu) = \mathrm{id}_{S_n}$, πειραματικά επαληθεύεται πως η $\pi(x_0) \in S_n$ είναι αρκούντως "απλή" μετάθεση ώστε να υπολογισθεί από τον Αλγόριθμο 6.18. Για τις γνήσιες πλεξίδες, μία υποσχόμενη ευριστική διαδικασία είναι η ακόλουθη:

> Εάν $\nu = \Delta_n^a V_1 \cdots V_s$ και $w = \Delta_n^b W_1 \cdots W_t$ είναι οι (Garside) κανονικές μορφές των $\nu \in B_n$ και $w \in B_n$ αντίστοιχα, τότε οι επιλογές $\mu = \pi^{-1}\big(\pi(V_1 W_1^{-1})\big)$, ή $\mu = \pi^{-1}\big(\pi(V_s^{-1} W_t\big)$ έχουν αρκετές πιθανότητες ώστε να είναι οι κατάλληλες. Ακόμη κι αν αυτές αποτύχουν, τότε *μαντεύονται* $\mu = \psi\omega$, για $\psi, \omega \in B_n^+$, όπου εδώ η $\omega \in B_n^+$ είναι η μεγαλύτερη σε πλήθος γεννητόρων κοινή ουρά των παραπάνω προτεινομένων επιλογών.

Κεφάλαιο 7

Το πρόβλημα της συζυγίας: Μη-αναγκαίο και μη-ικανό

Όταν συνελλήφθησαν ως ιδέες τα πρωτόκολλα που παρουσιάστηκαν στο παρών Μέρος της Εργασίας είχαν ως γνώμονα να στηρίξουν την ασφάλειά τους στο πρόβλημα της συζυγίας. Ωστόσο, η αλήθεια που αντιμετωπίζει ο αντίπαλος είναι κατάτι διαφορετική, όπως παρουσιάζεται στο [SU06].

7.1 Μη-αναγκαίο για το πρωτόκολλο Ko-Lee-Cheon-Han-Kang-Park

Υπενθυμίζεται το [KLCHKP00]:

Δημοσίως γνωστά: Ομάδα G, $w \in G$ και $A, B \leqslant G$ με $(\forall a \in A)(\forall b \in B)[ab = ba]$.

Κλειδιά:

της Αλίκης: Ιδιωτικό: $a \in A$. Δημόσιο: $a^{-1}wa \in G$.

του Βασίλη: Ιδιωτικό: $b \in B$. Δημόσιο: $b^{-1}wb \in G$.

Υπολογισμοί:

της Αλίκης: $K_A := a^{-1}(b^{-1}wb)a = a^{-1}b^{-1}wba \in G$.

του Βασίλη: $K_B := b^{-1}(a^{-1}wa)b \overset{\substack{a\in A\\ b\in B}}{=} a^{-1}b^{-1}wba \in G$.

Κοινό κλειδί: $K = b^{-1}a^{-1}wab \in G$.

Έστω πως η Εύα βρίσκει $a_1, a_2, b_1, b_2 \in G$ τέτοια ώστε

$$a_1 w a_2 = a^{-1} w a \qquad\qquad b_1 w b_2 = b^{-1} w b \tag{7.1}$$

και

$$(\forall b \in B)[a_1 b = b a_1 \wedge a_2 b = b a_2] \tag{7.2}$$

τότε προκύπτει ότι $a_1(b_1 w b_2)a_2 \overset{(7.1)}{=} a_1 b^{-1} w b a_2 \underset{b\in B}{\overset{(7.2)}{=}} b^{-1}(a_1 w a_2)b \overset{(7.1)}{=} b^{-1}a^{-1}wab = K$.

Να σημειωθεί πως τα $a_1, a_2, b_1, b_2 \in G$ παραπάνω δεν έχουν να κάνουν με τις προσωπικές επιλογές $a \in A$ και $b \in B$ της Αλίκης και το Βασίλη αντιστοίχως κάτι που κάνει την επίθεση ευκολότερη. Οι απαιτήσεις (7.1) και (7.2) μπορούν να αντικατασταθούν από τις:

$$a_1 w a_2 = a^{-1} w a \tag{7.3}$$

$$a_1, a_2 \in A \tag{7.4}$$

και η επίθεση έχει ως ακολούθως: Δεδομένης της (δημοσίας) μετάδοσης του Βασίλη $b^{-1}wb \in G$ προκύπτει ότι

$$\begin{aligned} a_1(b^{-1}wb)a_2 &= b^{-1}(a_1 w a_2)b && \text{(Συνθήκη (7.3))} \\ &= b^{-1}a^{-1}wab && \text{(Συνθήκη (7.4))} \\ &= K \end{aligned}$$

Συνεπώς, ο αντίπαλος καλείται να λύσει το φαινομενικά* ευκολότερο

Το πρόβλημα της αναλύσεως. Θεωρείται μια ομάδα G. Δοθέντων $w, w' \in G$ και $A \subseteq G$ να βρεθούν $x, y \in A$, τέτοια ώστε $w' = xwy$ δεδομένου ότι τουλάχιστον ένα τέτοιο ζεύγος $(x, y) \in A \times A$ υπάρχει.

Εδώ θα μπορούσε να προταθεί η προφανής λύση $x = 1 \in G$ και $y = w^{-1}w' \in G$. Ωστόσο, κανείς δεν εγγυάται πως $1, w^{-1}w' \in A$ (υπογραμμίζεται πως είναι $A \subseteq G$). Έτσι ανακύπτει το

Πρόβλημα του μέλους (εκδοχή απόφασης). Έστω μια ομάδα G και $u, v_1, \ldots, v_\ell \in G$. Ισχύει ότι $u \in \mathrm{gp}(v_1, \ldots, v_\ell)$;

Παρατήρηση 7.1. *Επί παραδείγματι,* $(\forall n \geqslant 6)(\exists H \leqslant B_n)[H \simeq F_2 \times F_2]$ *(από το [Co94] έστω* $H = \mathrm{gp}(\sigma_1^2, \sigma_2^2, \sigma_4^4, \sigma_5^2) \leqslant B_n$*) όπου* F_2 *είναι η ελευθέρα ομάδα τάξεως* 2 *και γι αυτό η εκδοχή απόφασης του προβλήματος του μέλους είναι αλγοριθμικά ανεπίλυτη όπως υπαγορεύει το [Mih58].*

*Το πρόβλημα της συζυγίας είναι ειδική περίπτωση του προβλήματος της αναλύσεως: Για $A = G$ και $x = y^{-1}$ στο πρόβλημα της αναλύσεως προκύπτει το πρόβλημα της συζυγίας. Συνεπώς, είναι εν γένει δυσκολότερο να επιλυθεί ένα πρόβλημα με ένα βαθμό ελευθερίας (να βρεθεί $x \in G$, ώστε $w' = x^{-1}wx$), παρά να επιλύσει ένα πρόβλημα με δύο βαθμούς ελευθερίας (να βρεθούν $x, y \in G$, ώστε $w' = xwy$).

7.2 Μη-ικανό για το πρωτόκολλο Anshel-Anshel-Goldfeld

Για το πιο εξεζητημένο πρωτόκολλο των Anshel-Anshel-Goldfeld, το οποίο είναι γενικότερο εκείνου των Ko-Lee-Cheon-Han-Kang-Park –με την έννοια του ότι δεν υπάρχουν συγκεκριμένες υποθέσεις για την ομάδα G που χρησιμοποιείται– υπενθυμίζεται το [AAG99]:

Δημοσίως γνωστά: Ομάδα G και $a_1, \ldots, a_k, b_1, \ldots, b_m \in G$.

Κλειδιά:

της Αλίκης:
Ιδιωτικό: $x = a_{i_1}^{\delta_1} \cdots a_{i_s}^{\delta_s} \in G$, με $s \in \mathbb{N}$, $i_1, \ldots, i_s \in \{1, \ldots, k\}$, $\delta_1, \ldots, \delta_s \in \{\pm 1\}$.
Δημόσιο: $x^{-1}b_1x, \ldots, x^{-1}b_mx \in \prod_{n=1}^{m} G$.

του Βασίλη:
Ιδιωτικό: $y = b_{j_1}^{\zeta_1} \cdots b_{j_t}^{\zeta_t} \in G$, με $t \in \mathbb{N}$, $j_1, \ldots, j_t \in \{1, \ldots, m\}$, $\zeta_1, \ldots, \zeta_t \in \{\pm 1\}$.
Δημόσιο: $y^{-1}a_1y, \ldots, y^{-1}a_ky \in \prod_{n=1}^{m} G$.

Υπολογισμοί:

της Αλίκης: $K_A := x^{-1}(y^{-1}a_{i_1}y)^{\delta_1} \cdots (y^{-1}a_{i_s}y)^{\delta_s} = x^{-1}y^{-1}(x_{i_1}^{\delta_1} \cdots x_{i_s}^{\delta_s})y = x^{-1}y^{-1}xy.$

του Βασίλη: $K_B := (y^{-1}(x^{-1}b_{j_1}x)^{\zeta_1} \cdots (x^{-1}b_{j_t}x)^{\zeta_t})^{-1} = \left(y^{-1}x^{-1}(b_{i_1}^{\zeta_1} \cdots b_{i_t}^{\zeta_t})x\right)^{-1} =$
$= \left(y^{-1}x^{-1}yx\right)^{-1} = x^{-1}y^{-1}xy.$

Κοινό κλειδί: $K = x^{-1}y^{-1}xy \in G$.

Η κοινή πεποίθηση για τις ενέργειες της Εύας είναι πως

> Αρκεί να επιλυθεί το πρόβλημα της συζυγίας για τα
>
> $$x^{-1}b_1x, \ldots, x^{-1}b_kx; y^{-1}a_1y, \ldots, y^{-1}a_ky \in G$$
>
> ώστε να ανακτηθούν τα $x, y \in G$.

Όμως, τότε θα είναι $x, y \in F\big(\mathscr{X}(G)\big)$. Κάτι τέτοιο δεν είναι επαρκές, αφού εάν κοιτάξει κανείς το μέρος των υπολογισμών του πρωτοκόλλου, θα πρέπει να είναι γνωστή και η έκφραση των $x, y \in G$ ως λέξεις των $a_1, \ldots, a_k \in G$ και $b_1, \ldots, b_m$ αντιστοίχως. Συνεπώς, η Εύα θα πρέπει επιπλέον να επιλύσει το

Πρόβλημα του μέλους. Θεωρείται μια ομάδα G. Δοθέντων $u, v_1, \ldots, v_\ell \in G$ να βρεθεί (εάν υπάρχει) μία έκφραση του $u \in G$ ως λέξη των $v_1, \ldots, v_\ell$.

Να σημειωθεί πως ακόμη κι αν η Εύα βρει $x' \in G$, με

$$(x')^{-1}b_1x' = x^{-1}b_1x, \qquad \dots \qquad (x')^{-1}b_mx' = x^{-1}b_mx$$

δεν είναι εγγυημένο πως $x' = x$ στην G. Πράγματι, έστω ότι $x' = c_bx \in G$, όπου $(\forall i = 1, \dots, m)[c_bb_i = b_ic_b]$, τότε $(\forall i = 1, \dots, m)[x^{-1}b_ix = (x')^{-1}b_ix]$ κι άρα και $(\forall b \in B)[x^{-1}bx = (x')^{-1}bx']$, όπου $B = gp(b_1, \dots, b_m)$· ειδικά $x^{-1}yx = (x')^{-1}yx'$ (όντας $y \in B$).

- Εάν $x' \notin A$, όπου $A := gp(a_1, \dots, a_m)$, και $y' \notin B$, τότε η Εύα δεν είναι σίγουρο ότι μπορεί να ανακτήσει το K.
- Εάν είτε $x' \in A$, είτε $y' \in B$, τότε η Εύα μπορεί να ανακτήσει το κοινό κλειδί K –ακόμη κι αν $x' \neq x$ και $y' \neq y$ στην G– ως εξής: Έστω $x' \in A$, και $x' = c_bx \in A$, με $c_b \in C_G(b_1, \dots, b_m)$, και $y' = c_ay \in G$, όπου $c_a \in C_G(a_1, \dots, a_k)$, τότε

  $$(x')^{-1}(y')^{-1}x'y' = (c_bx)^{-1}(c_ay)^{-1}(c_bx)(c_ay) = x^{-1}c_b^{-1}y^{-1}c_a^{-1}c_bxc_ay$$

  και επειδή $c_a \in C_G(a_1, \dots, a_m)$ και $c_b \in C_G(b_1, \dots, b_m)$, έπεται ότι

  $$= x^{-1}y^{-1}c_b^{-1}c_a^{-1}c_bc_axy$$

  Όντας $A \ni x' = c_bx$, $x \in A$, προκύπτει ότι $c_b \in A$ κι όντας $c_a \in C_G(a_1, \dots, a_m)$, τότε $c_ac_b = c_bc_a$. Συνεπώς,

  $$= K$$

  Παρόμοια κι αν $y' \in B$.

Έτσι εάν η Εύα επιλέξει να επιλύσει το πρόβλημα της συζυγίας, καταλήγει στο να χρειάζεται να επιλύσει είτε το πρόβλημα του μέλους, είτε την εκδοχή απόφασής του, το οποίο εν γένει είναι δύσκολα επιλύσιμο πρόβλημα [βλ. Παρατήρηση 7.1].

Εναλλακτικά, η Εύα καλείται να επιλύσει ένα αλγοριθμικά πιο δύσκολο πρόβλημα από εκείνο της συζυγίας, το

Πρόβλημα της συζυγίας σε υποομάδες. Θεωρείται μια ομάδα G. Δοθέντων $A \leqslant G$ και $g, h \in G$, να βρεθεί $x \in A$, τέτοιο ώστε $h = x^{-1}gx$, δεδομένου ότι τουλάχιστον ένα τέτοιο στοιχείο υπάρχει.

Μέρος ΙΙΙ

Κρυπτοσυστήματα βασισμένα στο πρόβλημα της αναλύσεως

Κατακλείδα της Εργασίας αποτελεί μία γενίκευση του προβλήματος της συζυγίας –όπως εξάλλου έχει ήδη επισημανθεί· το τελευταίο πρόβλημα που τυγχάνει εκτεταμένης παρουσιάσεως. Ο λόγος για

Το πρόβλημα της αναλύσεως. Θεωρείται μια ομάδα $(G, *)$ και $A \subseteq G$. Δεδομένων $w, w' \in G$ να βρεθεί ένα ζεύγος $(x, y) \in A \times A$, τέτοιο ώστε $w' = x * w * y$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος.

Επισημαίνεται η προφανής λύση $x = w'w^{-1} \in G$ και $y = 1_G \in G$. Ωστόσο δεν είναι γνωστόν εάν ικανοποιείται η απαίτηση ώστε $1_G, w'w^{-1} \in A \subseteq G$. Ο έλεγχος εάν ένα στοιχείο περιέχεται σε μια ομάδα, μπορεί να αποτελέσει δύσκολο πρόβλημα για κατάλληλες επιλογές ομάδων [πρόβλημα του μέλους].

Το πρόβλημα της αναλύσεως παρέχει κατά φυσιολογικό τρόπο το εξής πρωτόκολλο ανταλλαγής κλειδιού:

Αλίκη	Βασίλης
Δημοσίως γνωστά: Ομάδα G, $w \in G$ και $A, B \leqslant G$, με $(\forall a \in A)(\forall b \in B)[ab = ba]$.	
Προετοιμασία για την επακόλουθη επικοινωνία	
$a_1, a_2 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} A$.	$b_1, b_2 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} B$.
Επικοινωνία	
Ιδιωτικό κλειδί: $a_1, a_2 \in B$.	**Ιδιωτικό κλειδί:** $b_1, b_2 \in B$.
Δημόσιο κλειδί:	$u := a_1 w a_2 \in G$
$v := b_1 w b_2 \in G$	**:Δημόσιο κλειδί**
$K_A = a_1 v a_2$	$K_B = b_1 u b_2$

$$K_A = a_1 v a_2 = a_1 (b_1 w b_2) a_2 \overset{[A,B]=1}{=} b_1 (a_1 w a_2) b_2 = b_1 u b_2 = K_B$$

Σχήμα ΑΝ: Το άμεσο σχήμα ανταλλαγής κλειδιού από το πρόβλημα της αναλύσεως

Παραλλαγές του Σχήματος ΑΝ παρέχονται στο Κεφάλαιο 8 και στην §10.1.

Παρατήρηση. *Εν αντιθέσει με την περιορισμένη σε υποομάδες εκδοχή του προβλήματος της συζυγίας, το πρόβλημα της αναλύσεως είναι πάντοτε περιορισμένο σε υποομάδες.*

Κεφάλαιο 8

Ένα πρωτόκολλο βασισμένο στην ομάδα Thompson F

Το κρυπτοσύστημα των Shpilrain-Ushakov που περιέχεται στο [SU05] είναι ένα σχεδόν άμεσα εκμαιευόμενο σύστημα από το πρόβλημα της αναλύσεως. Οι δημιουργοί του -Vladimir Shpilrain και Alexander Ushakov- έχουν προτείνει την ομάδα του Richard Thompson (συγκεκριμένα την F) για την υλοποίηση του κρυπτοσυστήματος. Ακολούθως της παρουσίασης της ομάδας Thompson και του κρυπτοσυστήματος, το Κεφάλαιο κλείνει με το (αλγοριθμικά εύκολα επιλύσιμο) πρόβλημα της εύρεσης των κανονικών μορφών των στοιχείων (μια μορφή διάχυσης των ιδιωτικών κλειδιών των οντοτήτων).

Διαφοροποίηση από το Σχήμα ΑΝ: Στο δημόσιο κλειδί της Αλίκης (αντ. του Βασίλη) $x_1 w y_1 \in G$ (αντ. $x_2 w y_2 \in G$) αντί για $x_1, y_1 \in A$ (αντ. $x_2, y_2 \in B$), είναι $x_i \in A$ και $y_i \in B$, για $i = 1, 2$.

8.1 Η ομάδα Thompson F

Η ομάδα Thompson F είναι μία άπειρη μη-αβελιανή ομάδα με (άπειρη) παράσταση

$$F = \left\langle x_0, x_1, \ldots \mid (\forall i, k \in \mathbb{N}_0)[k > i \implies x_i^{-1} x_k x_i = x_{k+1}] \right\rangle$$

Ωστόσο υπάρχουν και πεπερασμένες παραστάσεις της ομάδος Thompson F, όπως η

$$= \langle A, B \mid [AB^{-1},\ A^{-1}BA] = [AB^{-1},\ A^{-2}BA^2] = 1 \rangle$$

(αρκεί να θέσει κανείς $x_0 := A$ και $x_n := A^{1-n}BA^{n-1}$, για $n \in \mathbb{N}$), ή όπως η

$$= \langle x_0, x_1 \mid x_2 x_1 = x_1 x_3,\ x_3 x_1 = x_1 x_4 \rangle$$

όπου $x_n := x_0^{1-n} x_1 x_0^{n-1}$, για $n \geqslant 2$ ή και η

$$= \langle x_0, x_1 \mid x_2 x_0 = x_0 x_3,\ x_3 x_0 = x_0 x_4 \rangle$$

όπου $x_{n+1} := x_{n-1}^{-1} x_n x_{n-1}$, για κάθε $n \geqslant 2$.

Ορισμός 8.1. Ένα στοιχείο $w \in F$ λέγεται πως είναι σε **κανονική μορφή** εάν

$$w = x_{i_1} \cdots x_{i_s} x_{j_t}^{-1} \cdots x_{j_1}^{-1} \tag{8.1}$$

όπου $s, t \in \mathbb{N}$, $i_1, \ldots, i_s, j_1, \ldots, j_t \in \mathbb{N}$ και ισχύουν οι κάτωθι συνθήκες:

(KM1) $i_1 \leqslant \ldots \leqslant i_s$ και $j_1 \leqslant \ldots \leqslant j_t$.

(KM2) Εάν $w = \cdots x_i \cdots x_i^{-1} \cdots$, τότε είτε υπάρχει εμφάνιση του x_{i+1}, είτε του x_{i+1}^{-1}.

Η κανονική μορφή ενός $w \in F$, θα συμβολίζεται ως $\mathtt{NF}(w)$, λόγῳ του Αλγορίθμου 8.16.

Παρατήρηση 8.2. *Η κανονική μορφή ενός $w \in F$ είναι μοναδική.*

Για τις λέξεις $w \in F$ της μορφής (8.1) το μέρος $x_{i_1} \cdots x_{i_s}$ θα καλείται **θετικό μέρος**, ενώ το $x_{j_t}^{-1} \cdots x_{j_1}^{-1}$ θα καλείται **αρνητικό μέρος**.

Οι πεπερασμένες παραστάσεις δεν προσφέρονται για αποτελεσματικό υπολογισμό των κανονικών μορφών των στοιχείων. Για το λόγο αυτό θα γίνεται αναφορά εφεξής στην άπειρη παράσταση της F η οποία σκοπώντας το σύνολο των σχέσεών της, παρέχει το ακόλουθο σύστημα μεταβάσεων (rewriting system):

$$\mathcal{R} = \left\{ \begin{array}{cc} x_k x_i \longrightarrow x_i x_{k+1} & x_k^{-1} x_i \longrightarrow x_i x_{k+1}^{-1} \\ x_i^{-1} x_k \longrightarrow x_{k+1} x_i^{-1} & x_i^{-1} x_k^{-1} \longrightarrow x_{k+1}^{-1} x_i^{-1} \\ x_j x_j^{-1} \longrightarrow \varepsilon & x_j^{-1} x_j \longrightarrow \varepsilon \end{array} \right\} \quad i < k \qquad (i, j, k \in \mathbb{N}_0)$$

η δράση του οποίου θα συμβολίζεται είτε ως $\sim_F$, είτε ρητώς ως $\xrightarrow{\mathcal{R}}$.

Θεώρημα 8.3 ([Gu06])**.** Η ομάδα Thompson F έχει εύκολα επιλύσιμο πρόβλημα της λέξης.

8.1.1 Δύο υποομάδες της ομάδος Thompson F

Έστω $s \in \mathbb{N}$. Θεωρείται το σύνολο

$$A_s := \left\{ x_{i_1} \cdots x_{i_m} x_{j_m} \cdots x_{j_1} \in F : (\forall k = 1, 2, \ldots, s)[i_k - k < s \wedge j_k - k < s] \right\}$$

$\equiv$ τα στοιχεία της F οι κανονικές μορφές των οποίων έχουν ισομήκη θετικά κι αρνητικά μέρη

καθώς και το σύνολο

$$B_s := \left\langle x_{s+1}, x_{s+2}, \ldots \mid (\forall i, k \in \mathbb{N})[k > i \implies x_{s+i} x_{s+k} x_{s+i} = x_{s+k+1}] \right\rangle$$

$\equiv$ τα στοιχεία της F που συνθέτουν οι γεννήτορές της $x_{s+1}, x_{s+2}, \ldots$.

Επιπλέον, ορίζεται η μερική συνάρτηση

$$\delta : \mathbb{Z} \times F \rightharpoonup F, \qquad \delta(n, w_{k_1}^{\alpha_1} \cdots w_{k_q}^{\alpha_q}) := w_{k_1+n}^{\alpha_1} \cdots w_{k_q+n}^{\alpha_q}$$

δεδομένου ότι $k_1 + n, \ldots, k_q + n \geqslant 0$. Εφεξής, όποτε γίνεται αναφορά στη συνάρτηση $\delta(n, w) \equiv \delta_n(w)$ θα υποτίθεται ότι είναι καλώς ορισμένη.

Ορισμός 8.4. Θεωρείται μια ομάδα $G = \langle X \mid R \rangle$ και $H \leqslant G$. Ως **γράφημα Schreier** ορίζεται η δομή (V, E), όπου $V := \{Hg \subseteq G : g \in G\}$ και $E := \left\{Hg \xrightarrow{x} Hgx : x \in X\right\}$.

Πρόταση 8.5. Έστω $s \in \mathbb{N} \setminus \{1\}$.

(α′) Οι A_s, B_s είναι υποομάδες της F.

(β′) $H\ A_s = \mathrm{gp}\left(\left\{x_0x_1^{-1}, \ldots, x_0x_s^{-1}\right\}\right)$.

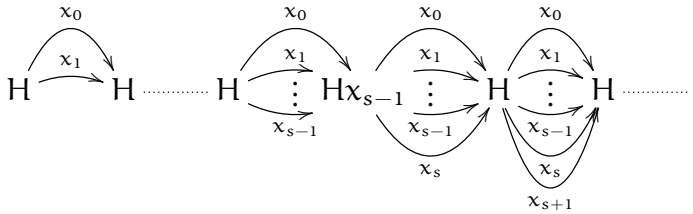
Απόδειξη. (α′) Εξ ορισμού $B_s \leqslant F$. Επιπλέον, $A_s \leqslant F$ αφού ισχύει:

Κλειστότητα του A_s ως προς τα αντίστροφα: $A_s^{-1} = \{x_1x_0^{-1}, \ldots, x_sx_0^{-1}\} \subseteq A_s$, αφού

- έχουν ίσα θετικά κι αρνητικά μέρη·
- για τον δείκτη του θετικού μέρους ισχύει ότι $0 \leqslant i_1 - 1 \leqslant s - 1 < s$·
- για τον δείκτη του αρνητικού μέρους $j_1 - 1 = 0 - 1 = -1 < s$.

Κλειστότητα του A_s ως προς την πράξη: Εάν $u, v \in A_s$, τότε και $uv \in A_s$ [βλ. §8.4].

(β′) $\mathrm{gp}\left(x_0x_1^{-1}, \ldots, x_0x_s^{-1}\right) \leqslant A_s$: Προφανώς, αφού $x_0x_1^{-1}, \ldots, x_0x_s^{-1} \in A_s$.
$\mathrm{gp}\left(x_0x_1^{-1}, \ldots, x_0x_s^{-1}\right) \geqslant A_s$: Το γράφημα Schreier της $H := \mathrm{gp}\left(x_0x_1^{-1}, \ldots, x_0x_s^{-1}\right)$ στην A_s δίδει το ζητούμενο:



□

Πρόταση 8.6. $(\forall s \in \mathbb{N})(\forall a \in A_s)(\forall b \in B_s)[ab \sim_F ba]$.

Απόδειξη. Έστω $a = x_{i_1} \cdots x_{i_m} x_{j_m} \cdots x_{j_1} \in A_s$ και $b = x_{k_1}^{\zeta_1} \cdots x_{k_\ell}^{\zeta_\ell} \in B_s$, όπου εξ ορισμού του B_s ισχύει ότι $(\forall q = 1, \ldots, \ell)[k_q > s]$. Με διπλή επαγωγή, πρώτα στο ℓ και κατόπιν στο m έπεται πως:

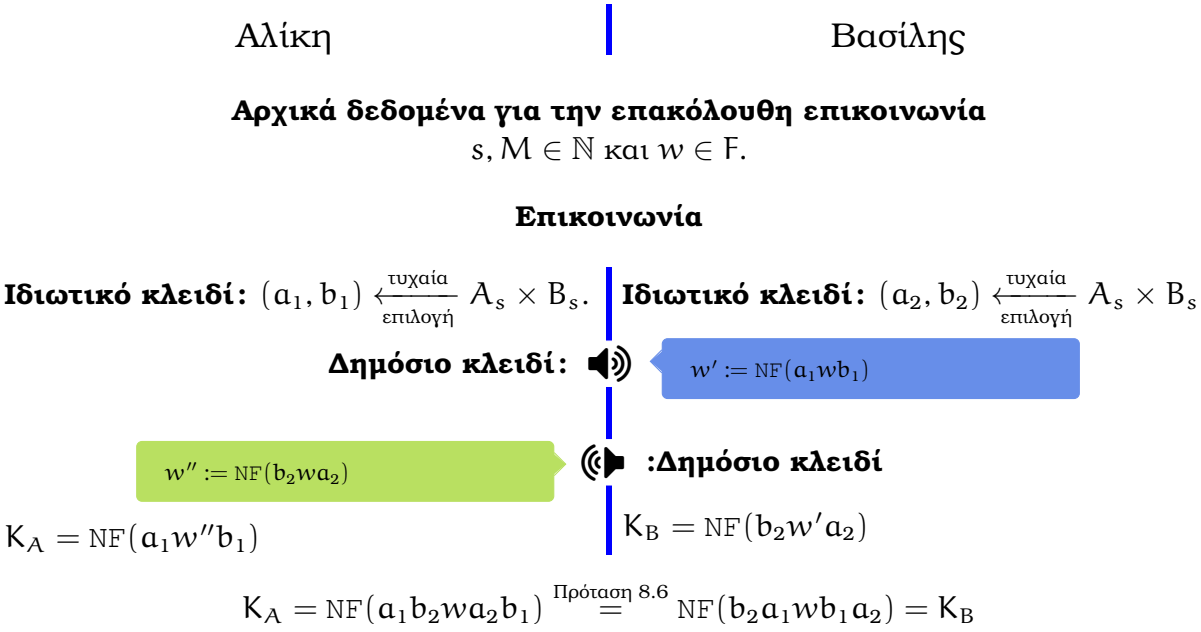
$$ab = x_{i_1} \cdots x_{i_m} \delta_m\left(x_{k_1}^{\delta_1} \cdots x_{k_\ell}^{\delta_\ell}\right) x_{j_m} \cdots x_{j_1} = ba$$

Η περίπτωση "πρότυπο" για τις επόμενες είναι η $\ell = m = 1$:

$$\left.\begin{aligned} ab = x_{i_1}x_{j_1}^{-1}x_{k_1}^{\zeta_1} &\xrightarrow[j_1-1<s \implies j_1<s+1 \implies j_1 \leqslant s<k_1]{\mathcal{R}:\, x_i^{-1}x_k \longrightarrow x_{k+1}x_i^{-1}\ (\text{για } i<k)} x_{i_1}\delta_1(x_{k+1}^{\delta_1})x_{j_1}^{-1} \\ ba = x_{k_1}^{\zeta_1}x_{i_1}x_{j_1}^{-1} &\xrightarrow[i_1-1<s \implies i_1<s+1 \implies i_1 \leqslant s<k_1]{\mathcal{R}:\, x_kx_1 \longrightarrow x_ix_{k+1}\ (\text{για } i<k)} x_{i_1}\delta_1(x_{k+1}^{\delta_1})x_{j_1}^{-1} \end{aligned}\right\} ab = ba$$

Οι υπόλοιπες περιπτώσεις στηρίζονται στην παραπάνω. □

8.2 Το "στρεβλωμένο" πρωτόκολλο των Shpilrain-Ushakov



Σχήμα 8.6: Το "στρεβλωμένο" πρωτόκολλο ανταλλαγής κλειδιού Shpilrain-Ushakov

8.2.1 Προτεινόμενες παράμετροι

- $s \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{3, 4, 5, 6, 7, 8\}$.
- $M \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{256, 258, \ldots, 318, 320\}$.
- $a_1, a_2 \in F(S_A)$, όπου

  $$S_A = \left\{x_0 x_1^{-1}, x_0 x_2^{-1}, \ldots, x_0 x_s^{-1}\right\}$$

  Μεθοδολογία: Για $j \in \{1, 2\}$

  $a_j \leftarrow \varepsilon$;
  επανάλαβε
  $x \xleftarrow[\text{επιλογή}]{\text{τυχαία}} S_A^{\pm}$; $a_j \leftarrow \mathrm{NF}(a_j x)$;
  έως ότου $(|a_j| = M)$
  επίστρεψε a_j;
- $w \in F(S_W)$, όπου

  $$S_W = \left\{x_0, x_1, \ldots, x_{s+2}\right\}$$

  Μεθοδολογία:

  $w \leftarrow \varepsilon$;
  επανάλαβε
  $u \xleftarrow[\text{επιλογή}]{\text{τυχαία}} S_W^{\pm}$; $w \leftarrow \mathrm{NF}(wu)$;
  έως ότου $(|w| = M)$
  επίστρεψε w;
- $b_1, b_2 \in F(S_B)$, όπου

  $$S_B = \left\{x_{s+1}, x_{s+2}, \ldots, x_{2s}\right\}$$

  Μεθοδολογία: Για $k \in \{1, 2\}$

  $b_k \leftarrow \varepsilon$;
  επανάλαβε
  $y \xleftarrow[\text{επιλογή}]{\text{τυχαία}} S_B^{\pm}$; $b_k \leftarrow \mathrm{NF}(y b_k)$;
  έως ότου $(|b_k| = M)$
  επίστρεψε b_k;

8.3 Κρυπτανάλυση

Οι προτεινόμενες τιμές των παραμέτρων έχουν επιλεχθεί με τέτοιο τρόπο ώστε να αποφεύγονται επιθέσεις βασισμένες στο μήκος των μεταδιδόμενων λέξεων, δηλαδή:

> Έστω η δημοσίως γνωστή λέξη $w \in F$ και η μετάδοση της Αλίκης $w' \in F$. Θεωρείται το γράφημα $\Gamma = (V, E)$, όπου
>
> - $V = \{w \in F\}$, (όλα τα στοιχεία της ομάδας Thompson F) και
> - $E = \left\{v_1 \xrightarrow{(x,y)} v_2 \in V \times V : x \in S_A^{\pm} \wedge y \in S_B^{\pm} \wedge v_2 = xv_1y\right\}$, δηλαδή κάθε ακμή φέρει και μία "ετικέτα" [εναλλακτικά $E = \left\{(w, xwy, x, y) \in F \times F \times S_A^{\pm} \times S_B^{\pm}\right\}$].
>
> Η επίθεση στοχεύει στην εύρεση ενός μονοπατιού
>
> $$w \xrightarrow{(x_1,y_1)} w_1 \xrightarrow{(x_2,y_2)} \cdots \xrightarrow{(x_{\ell-1},y_{\ell-1})} w_{\ell-1} \xrightarrow{(x_\ell,y_\ell)} w'$$
>
> και τότε -μέσω των ετικετών- είναι δυνατή η εύρεση ενός $(s, t) \in S_A^{\pm} \times S_B^{\pm}$, με $w' = swt$.

Αλγόριθμος 8.7 $\texttt{LBA}(w, w')$: Επίθεση βασισμένη στο μήκος.

Είσοδος: Η δημοσίως γνωστή λέξη $w \in F$ και η μετάδοση της Αλίκης $w' \in F$.
Έξοδος: $(s, t) \in S_A \times S_B$, έτσι ώστε $w' = swt$.

1: $E_w \leftarrow \{(w, w, \varepsilon, \varepsilon)\}$; $E_{w'} \leftarrow \{(w', w', \varepsilon, \varepsilon)\}$; $M_w \leftarrow M_{w'} \leftarrow \varnothing$; $S_w \leftarrow \{w\}$; $S_{w'} \leftarrow \{w'\}$;
2: **επανάλαβε**
3: $\quad u \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \left\{v \in S_w \setminus M_w : |v| = \min\{|z| \in \mathbb{N} : z \in S_w \setminus M_w\}\right\}$;
4: $\quad E_w \leftarrow E_w \cup \left\{(u, xuy, x, y) \in F \times F \times S_A^{\pm} \times S_B^{\pm}\right\}$; /* Όλες οι ακμές με αρχή την u */
5: $\quad S_w \leftarrow S_w \cup \left\{xuy \in F : x \in S_A^{\pm} \wedge y \in S_B^{\pm}\right\}$; /* Οι κορυφές προς εξερεύνηση */
6: $\quad M_w \leftarrow M_w \cup \{u\}$; /* Η κορυφή u εξερευνήθηκε */
/* Τα προηγούμενα βήματα για $S_{w'}$ και $M_{w'}$ αντί των S_w και M_w αντιστοίχως. */
7: $\quad u' \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \left\{v' \in S_{w'} \setminus M_{w'} : |v'| = \min\{|z'| \in \mathbb{N} : z' \in S_{w'} \setminus M_{w'}\}\right\}$;
8: $\quad E_{w'} \leftarrow E_{w'} \cup \left\{(u', xu'y, x, y) \in F \times F \times S_A^{\pm} \times S_B^{\pm}\right\}$;
9: $\quad S_{w'} \leftarrow S_{w'} \cup \left\{xu'y \in F : x \in S_A^{\pm} \wedge y \in S_B^{\pm}\right\}$;
10: $\quad M_{w'} \leftarrow M_{w'} \cup \{u'\}$;
11: **έως ότου** $(\exists u,u' \in F)(\exists x,x' \in S_A^{\pm})(\exists y,y' \in S_B^{\pm})\left[(u,xuy,x,y) \in E_w \wedge (u',x'u'y',x',y') \in E_{w'} \wedge xuy = x'u'y' =: \overline{w}\right]$
Έστω τα μονοπάτια
$$(w, w, \varepsilon, \varepsilon) \longrightarrow (w, w_1, x_1, y_1) \longrightarrow \cdots \longrightarrow (w_{n-1}, \overline{w}, x_n, y_n) \quad \text{(στοιχεία του } S_w\text{)}$$
$$(w', w', \varepsilon, \varepsilon) \longrightarrow (w', w'_1, x'_1, y'_1) \longrightarrow \cdots \longrightarrow (w'_{m-1}, \overline{w}, x'_m, y'_m) \quad \text{(στοιχεία του } S_{w'}\text{)}$$
12: **επίστρεψε** $\left((x'_1)^{-1} \cdots (x'_m)^{-1} x_n \cdots x_1,\ y_1 \cdots y_n (y'_m)^{-1} \cdots (y'_1)^{-1}\right)$;

Όπως αναφέρουν οι εμπνευστές του πρωτοκόλλου στο [SU05] όλες οι εκτελέσεις του Αλγορίθμου 8.7 δεν απέδωσαν αποτέλεσμα, παρά τη μεγάλη ποσότητα χρόνου που του δόθηκε κάθε φορά. Έτσι το ποσοστό επιτυχίας μιας τέτοιας επίθεσης είναι 0.

8.4 Κανονικές μορφές στην ομάδα Thompson F

Στο πρωτόκολλο των Shpilrain-Ushakov γίνεται χρήση των κανονικών μορφών των μεταδιδομένων στοιχείων. Στην παρούσα Ενότητα παρέχεται η μεθοδολογία υπολογισμού της κανονικής μορφής των στοιχείων στην ομάδα Thompson, από την οποία προκύπτει το

Θεώρημα 8.8. Η κανονική μορφή μιας $w \in F$ υπολογίζεται σε χρόνο $\mathcal{O}\big(|w| \log_2 |w|\big)$.

8.4.1 Ημικανονική μορφή συγκόλλησης ημικανονικών μορφών

Ορισμός 8.9. Μία $w \in F$ είναι σε **ημικανονική μορφή** εάν είναι της μορφής (8.1) και ικανοποιεί τη συνθήκη (KM1).

- Δεδομένων των $w_1, w_2 \in F$ σε ημικανονική μορφή, όπου $w_1 = p_1 n_1$ και $w_2 = p_2 n_2$, ποια είναι η ημικανονική μορφή της $w_1 w_2 = p_1 n_1 p_2 n_2 \in F$;

Αρκεί

1. να βρεθεί η ημικανονική μορφή $p_3 n_3$ (μέσω του $\texttt{Merge}_{-,+}(n_1, p_1, 0, 0)$) του $n_1 p_2$ και τότε θα είναι $w_1 w_2 = p_1 p_3 n_3 n_2$·
2. κατόπιν να βρεθούν οι ημικανονικές μορφές των $p_1 p_3$ (μέσω του $\texttt{Merge}_{+,+}(p_1, p_3, 0, 0)$) και $n_3 n_2$ (μέσω του $\texttt{Merge}_{-,+}(n_3, n_2, 0, 0)$).

Συνεπώς, ο αλγόριθμος θα έχει την εξής μορφή:

Αλγόριθμος 8.10 $\texttt{Merge}(w_1, w_2)$: Ημικανονική μορφή παράθεσης ημικανονικών μορφών

Είσοδος: Δύο λέξεις $w_1, w_2 \in F$ σε ημικανονική μορφή.
Δεδομένα: Έστω $p_1 n_1$ και $p_2 n_2$ οι ημικανονικές μορφές των w_1 και w_2 αντίστοιχα.
Έξοδος: Η ημικανονική μορφή της $w_1 w_2 \in F$.

1: $p_3 n_3 \leftarrow \texttt{Merge}_{-,+}(n_1, p_2, 0, 0)$;
2: $u \leftarrow \texttt{Merge}_{+,+}(p_1, p_3, 0, 0)$;
3: $v \leftarrow \texttt{Merge}_{-,-}(n_3, n_2, 0, 0)$;
4: **επίστρεψε** uv;

Ορθότητα και χρονική πολυπλοκότητα του Αλγορίθμου 8.10. Έπονται απ' τ' αποτελέσματα για τον Αλγόριθμο 8.12 ($\texttt{Merge}_{-,+}(n, p, \kappa, \lambda)$) και τους παρόμοιους του.⊣

Το παρακάτω πρόδηλο αποτέλεσμα θα αποτελέσει οδηγό για τον Αλγόριθμο 8.12:

Λήμμα 8.11. *Μία λέξη της ομάδας* F *είναι σε ημικανονική μορφή εάν και μόνον εάν είναι* $\mathcal{R}$*-ανηγμένη (:δεν μπορούν να λάβουν χώρα άλλες εφαρμογές των κανόνων του* $\mathcal{R}$*).*

Παρουσιάζονται τώρα τα βασικά συστατικά του Αλγορίθμου 8.10 ($\texttt{Merge}(w_1, w_2)$):

Αλγόριθμος 8.12 $\texttt{Merge}_{-,+}(n,\ p,\ \kappa, \lambda)$: Υπολογισμός ημικανονικής μορφής του np

---

Είσοδος: Το αρνητικό μέρος $n = x_{j_t}^{-1} \cdots x_{j_1}^{-1}$ και το θετικό μέρος $p = x_{i_1} \cdots x_{i_s}$ δύο ημικανονικών μορφών και $\kappa, \lambda \in \mathbb{Z}$.

Έξοδος: $\delta_\kappa(n)\delta_\lambda(p)$ που είναι η ημικανονική μορφή της $np \in$ F.

1: **εάν** $\big((s = 0) \vee (t = 0)\big)$ **τότε**
2: **επίστρεψε** np;
3: **αλλιώς εάν** $(j_1 + \kappa = i_1 + \lambda)$ **τότε**
4: **επίστρεψε** $\texttt{Merge}_{-,+}(x_{j_t}^{-1} \cdots x_{j_2}^{-1},\ x_{i_2} \cdots x_{i_s},\ \kappa,\ \lambda)$;
5: **αλλιώς εάν** $(j_1 + \kappa < i_1 + \lambda)$ **τότε**
6: $w \leftarrow \texttt{Merge}_{-,+}(x_{j_t}^{-1} \cdots x_{j_2}^{-1},\ x_{i_1} \cdots x_{i_s},\ \kappa,\ \lambda + 1)$;
7: **επίστρεψε** $w x_{j_1+\kappa}^{-1}$;
8: **αλλιώς**
9: $w \leftarrow \texttt{Merge}_{-,+}(x_{j_t}^{-1} \cdots x_{j_1}^{-1},\ x_{i_2} \cdots x_{i_s},\ \kappa + 1,\ \lambda)$;
10: **επίστρεψε** $x_{i_1+\lambda}^{-1} w$;
11: **τέλος εάν**

Χρονική πολυπλοκότητα του Αλγορίθμου 8.12. Σε κάθε αναδρομική κλήση παραλείπονται 1 ή 2 γράμματα από τη λέξη np (κι άρα ο αλγόριθμος τερματίζει), συνεπώς η επεξεργασία των λέξεων είναι γραμμική, άρα η χρονική πολυπλοκότητα του αλγορίθμου έγκειται σε $C\big(|n| + |p|\big)$, με $C \not\sim |n|, |p|$. ⊣

Ορθότητα του Αλγορίθμου 8.12. Με επαγωγή στο $|n| + |p| \in \mathbb{N}_0$:

Επαγωγική Βάση. Εάν $|n| + |p| = 0$, τότε $np = \varepsilon$ η οποία είναι (τετριμμένα) σε ημικανονική μορφή.

Επαγωγική Υπόθεση. Η $\texttt{Merge}_{-,+}(n, p, \kappa, \lambda)$ είναι ημικανονική μορφή της $np \in$ F, για κάθε $|n| + |p| \leqslant N \in \mathbb{N}$.

Επαγωγικό Βήμα. Έστω $|n| + |p| = N + 1$. Διακρίνονται οι εξής περιπτώσεις:

(α′) Εάν $|n| = 0$ (αντίστοιχα $|p| = 0$), τότε $np = p$ (αντίστοιχα $np = n$) κι άρα είναι σε ημικανονική μορφή.

(β′) Εάν $j_1 + \kappa = i_1 + \lambda$, τότε

$$x_{j_t+\kappa}^{-1} \cdots x_{j_1+\kappa}^{-1} x_{i_1+\lambda} \cdots x_{i_s+\lambda} \xrightarrow{\mathcal{R}} x_{j_t+\kappa}^{-1} \cdots x_{j_2+\kappa}^{-1} x_{i_2+\lambda} \cdots x_{i_s+\lambda}$$

μήκους $N - 1$ και από την Επαγωγική Υπόθεση το αποτέλεσμα έπεται.

(γ') Εάν $j_1 + \kappa < i_1 + \lambda$, τότε από τη συνθήκη (KM1) ο $j_1 + \kappa$ είναι ο μικρότερος δείκτης της $\delta_\kappa(n)\delta_\lambda(p)$. Άρα (κανόνας $x_i^{-1}x_k \xrightarrow{\mathcal{R}} x_{k+1}x_i^{-1}$ $(i < k)$ του $\mathcal{R}$)

$$\begin{aligned}\delta_\kappa(n)\delta_\lambda(p) = x_{j_t+\kappa}^{-1}\cdots x_{j_2+\kappa}^{-1}x_{j_1+\kappa}^{-1}x_{i_1+\lambda}\cdots x_{i_s+\lambda} &\xrightarrow{\mathcal{R}} \\ &\xrightarrow{\mathcal{R}} x_{j_t+\kappa}^{-1}\cdots x_{j_2+\kappa}^{-1}x_{i_1+\lambda+1}\cdots x_{i_s+\lambda+1}x_{j_1+\kappa}^{-1}\end{aligned} \tag{8.2}$$

Επειδή $\left|\delta_\kappa(x_{j_t}\cdots x_{j_2})\delta_{\lambda+1}(p)\right| < N + 1$, από την Επαγωγική Υπόθεση η $w := \texttt{Merge}(x_{j_t}\cdots x_{j_2}, p, \kappa, \lambda+1)$ είναι η ημικανονική μορφή της $\delta_\kappa(x_{j_t}\cdots x_{j_2})\delta_{\lambda+1}(p)$. Συνεπώς, η $wx_{j_1+\kappa}^{-1}$ είναι σε ημικανονική μορφή και είναι η ημικανονική μορφή της $\delta_\kappa(n)\delta_\lambda(p)$ (λόγω της μετάβασης (8.2)).

(δ') Εάν $j_1+\kappa > i_1+\lambda$, τότε η ανάλυση είναι παρόμοια με εκείνη της περίπτωσης $j_1 + \kappa < i_1 + \lambda$. ⊣

▶ Με παρόμοιους συλλογισμούς όπως του Αλγορίθμου 8.10 ($\texttt{Merge}_{-,+}(n, p, \kappa, \lambda)$) προκύπτουν και οι αλγόριθμοι $\texttt{Merge}_{-,-}(n_1, n_2, \kappa, \lambda)$ και $\texttt{Merge}_{+,+}(p_1, p_2, \kappa, \lambda)$.

8.4.2 Υπολογισμός ημικανονικών μορφών

Παρατήρηση 8.13. *Η ημικανουική μορφή ενός $w \in F$ δεν είναι μοναδική.*

Αλγόριθμος 8.14 $\texttt{SNF}(w)$: Υπολογισμός (μιας) ημικανονικής μορφής της w

Είσοδος: $w \in F$.
Έξοδος: Η ημικανονική μορφή της $w \in F$.
1: **εάν** $(|w| \leqslant 1)$ **επίστρεψε** w;
2: $w \rightsquigarrow w_1w_2$, όπου $|w_2| = |w_1| \pm 1$.
3: **επίστρεψε** $\texttt{Merge}\big(\texttt{SNF}(w_1), \texttt{SNF}(w_2)\big)$;

Χρονική πολυπλοκότητα του Αλγορίθμου 8.14. Ισχύει ότι $|w_1|, |w_2| \simeq |w|/2$, διότι είναι $|w_2| = |w_1| \pm 1$, κι άρα

$$T\big(|w|\big) = T\big(|w|/2\big) + Cn$$

όπου Cn είναι η χρονική πολυπλοκότητα της σύνθεσης [βλ. Αλγόριθμο 8.10]. Συνεπώς, ο αλγόριθμος έχει χρονική πολυπλοκότητα $\mathcal{O}(C|w|\log_2|w|)$

8.4.3 Υπολογισμός κανονικών μορφών

Ως τελευταίο βήμα του υπολογισμού της κανονικής μορφής της $u \in F$ –δεδομένου ότι βρίσκεται ήδη σε ημικανονική μορφή– είναι η ικανοποίηση της συνθήκης (KM2), δηλαδή

> η διαγραφή των "ανεπιθύμητων" ζευγών (x_i, x_i^{-1}) για τα οποία δεν περιέχεται στην u καμμία εμφάνιση, είτε του x_{i+1}, είτε του x_{i+1}^{-1}.

Λήμμα 8.15 (Ορθότητα Αλγορίθμου 8.16)**.** *Έστω* $w = x_{i_1} \cdots x_{i_s} x_{j_t}^{-1} \cdots x_{j_1}^{-1}$ *σε ημικανονική μορφή και* $(x_{i_a}, x_{j_b}^{-1})$ *ένα ζεύγος γεννητόρων που αντιφάσκει στη συνθήκη (KM2), με τα* a, b *μεγιστικά. Για τη* $w' := x_{i_1} \cdots x_{i_{a-1}} \delta_{-1}\big(x_{i_{a+1}} \cdots x_{i_s} x_{j_t}^{-1} \cdots x_{j_{b+1}}^{-1}\big) x_{j_{b+1}}^{-1} \cdots x_{j_1}^{-1}$ *ισχύουν:*

1. $w \sim_F w'$.
2. *Εάν* $(x_{i_c}, x_{j_d}^{-1})$ *ένα άλλο ζεύγος γεννητόρων που αντιφάσκει στη συνθήκη (KM2), τότε* $c < a$ *και* $d < b$.

Απόδειξη. Η συνθήκη (KM2) και ο Ορισμός 8.9 επάγουν πως $i_{a+1}, \ldots, i_s, j_{b+1}, \ldots, j_t > i_a + 1$ (οι δείκτες της $x_{i_{a+1}} \cdots x_{i_s} x_{j_t}^{-1} \cdots x_{j_{b+1}}^{-1}$ είναι μεγαλύτεροι του $i_a + 1$). Συνεπώς, οι δείκτες της $\delta_{-1}\big(x_{i_{a+1}} \cdots x_{i_s} x_{j_t}^{-1} \cdots x_{j_{b+1}}^{-1}\big)$ είναι μεγαλύτεροι του i_a. Εφαρμόζοντας ανάστροφα τους κανόνες του $\mathcal{R}$, προκύπτει ότι $w \sim_F w'$.

Όντας τα a, b μεγιστικά, διακρίνονται οι ακόλουθες περιπτώσεις:

- $c < a$ και $d < b$.
- $c > a$ και $d > b$ άτοπο.

  [Έστω $c > a$ και $d > b$. Το ζεύγος γεννητόρων $(x_{i_a}, x_{j_b}^{-1})$ αντιφάσκει στη συνθήκη (KM2) στην $w \in F$, κατ' επέκτασην το ζεύγος γεννητόρων $(x_{i_a+\varepsilon}, x_{j_b+\varepsilon}^{-1})$ αντιφάσκει στη συνθήκη (KM2) στη λέξη $\delta_\varepsilon(w)$ που αντίκειται στην μεγιστικότητα των a, b.] □

Χρονική πολυπλοκότητα του Αλγορίθμου 8.16. Εξαιρουμένου του βήματος της μετατροπής της $u \in F$ σε ημικανονική μορφή (γραμμή 2), ο αλγόριθμος προσπελάζει γράμμα προς γράμμα τη λέξη $u \in F$ (γραμμή 8, 12, 15 και 19, 20). Επίσης, ο αλγόριθμος συνθέτει τις $u_1, u_2 \in F$ γράμμα προς γράμμα (γραμμή 27 και 33). Συνεπώς, η χρονική πολυπλοκότητα του Αλγορίθμου 8.16 είναι $D \cdot |u|$, όπου $D \not\sim |u|$ (και οφείλεται στις λειτουργίες των στοιβών).

Σκιαγράφηση του Αλγορίθμου 8.16. *Ο αλγόριθμος διακρίνεται στα εξής δύο μέρη:*

Α΄: Εντοπισμός όλων των "ανεπιθυμήτων" ζευγών ξεκινώντας από τη μέση της u *[λόγῳ του Λήμματος 8.15].*

Β΄: Εφαρμογή της συνάρτησης $\delta : \mathbb{Z} \times F \longrightarrow F$*, στη* $u \in F$*, όπου αυτό κρίνεται απαραίτητο.*

Ένα σημαντικό γνώρισμα του αλγορίθμου είναι ότι η εφαρμογή της $\delta_{-1} : F \longrightarrow F$ *δεν γίνεται αμέσως [όπως στην απόδειξη του Λήμματος 8.15], αλλά η πληροφορία αυτή φυλάσσεται σε δύο στοίβες, μία για το θετικό μέρος και μία για το αρνητικό μέρος της κανονικής μορφής. Επίσης, το μήκος της στοίβας* S_1 *(αντίστοιχα* S_2*) ισούται με το* $|w_1| \leqslant |u|$ *(αντίστοιχα* $|w_2| \leqslant |u|$*) για κάποιες βοηθητικές λέξεις* $w_1, w_2 \in F$*. Συνεπώς, το πρώτο γράμμα της* $w_1 \in F$ *(αντίστοιχα το τελευταίο γράμμα της* $w_2 \in F$*) ορίζεται εάν και μόνον εάν* $S_1 \neq \varnothing$ *(αντίστοιχα* $S_2 \neq \varnothing$*).*

Αλγόριθμος 8.16 $\mathtt{NF}(u)$: Η κανονική μορφή της $u \in F$.

Είσοδος: $u \in F$.

Δεδομένα: Λειτουργίες διαχείρησης λιστών όπως εισαγωγή στην αρχή της λίστας Q ενός στοιχείου a ($\mathtt{Push}(a, Q)$), επιστροφή της τιμής του αρχικού στοιχείου της λίστας Q ($\mathtt{Top}(Q)$) και εξαγωγή του αρχικού στοιχείου της λίστας Q ($\mathtt{Pop}(Q)$). (*Σύμβαση.* $Q = \varnothing \iff \mathtt{Top}(Q) = \infty$.)

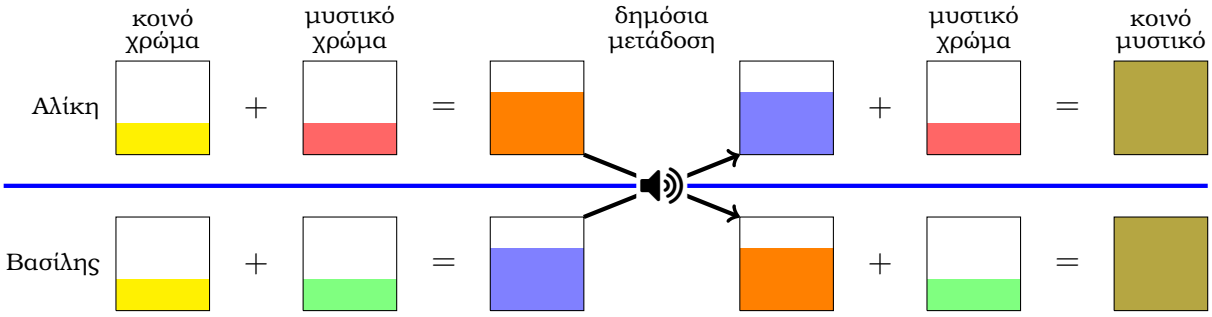
Έξοδος: Η κανονική μορφή της $u \in F$.

$\delta \leftarrow \delta_1 \leftarrow \delta_2 \leftarrow 0$; $w_1 \leftarrow w_2 \leftarrow \varepsilon$; $S_1 \leftarrow S_2 \leftarrow \varnothing$; $\mathtt{Push}(\infty, S_1)$; $\mathtt{Push}(\infty, S_2)$;
$x_{i_1} \cdots x_{i_s} x_{j_t}^{-1} \cdots x_{j_1}^{-1} \leftarrow \mathtt{SNF}(u)$;
$u_1 \leftarrow x_{i_1} \cdots x_{i_s}$; $u_2 \leftarrow x_{j_t}^{-1} \cdots x_{j_1}^{-1}$;
Ως x_a (αντ. x_b) θα συμβολίζεται το πρώτο (αντ. τελευταίο) γράμμα της w_1 (αντ. w_2).
όσο $((s > 0) \vee (t > 0))$
  εάν $\big((s > 0) \wedge \big((t = 0) \vee (i_s > j_t)\big)\big)$ **τότε**
    $w_1 \leftarrow x_{i_s} w_1$; /* Πολ/μός εξ αριστερών της w_1 με το δεξιότερο στοιχείο της u_2 */
    $s \leftarrow s - 1$; /* "Διαγραφή" του δεξιότερου στοιχείου της u_1 */
    $\mathtt{Push}(0, S_1)$;
  αλλιώς εάν $\big((t > 0) \wedge \big((s = 0) \vee (j_t > i_s)\big)\big)$ **τότε**
    $w_2 \leftarrow w_2 x_{j_t}$; /* Πολ/μός εκ δεξιών της w_2 με το αριστερότερο στοιχείο της u_2 */
    $t \leftarrow t - 1$; /* "Διαγραφή" του "αριστερότερου" στοιχείου της u_2 */
    $\mathtt{Push}(0, S_2)$;
  αλλιώς εάν $\big((i_s = j_t) \wedge \big(\alpha - \mathtt{Top}(S_1), \beta - \mathtt{Top}(S_2) \notin \{i_s, i_s + 1\}\big)\big)$ **τότε**
    $s \leftarrow s - 1$; $t \leftarrow t - 1$;
    $\mathtt{Top}(S_1) \leftarrow \mathtt{Top}(S_1) + 1$;
    $\mathtt{Top}(S_2) \leftarrow \mathtt{Top}(S_2) + 1$;
  αλλιώς
    $w_1 \leftarrow x_{i_s} w_1$; $s \leftarrow s - 1$; $\mathtt{Push}(0, S_1)$;
    $w_2 \leftarrow w_2 x_{j_t}^{-1}$; $t \leftarrow t - 1$; $\mathtt{Push}(0, S_2)$;
  τέλος εάν
τέλος όσο
όσο $(w_1 \not\equiv_F \varepsilon)$
  Έστω ότι $w_1 = x_{i_1} w_1'$ /* ήτοι το x_{i_1} είναι το αριστερότερο στοιχείο της w_1 */
  $\delta_1 \leftarrow \delta_1 + \mathtt{Pop}(S_1)$;
  $u_1 \leftarrow u_1 x_{i_1 - \delta_1}$;
  $w_1 \leftarrow w_1'$ /* "Διαγραφή" του αριστερότερου στοιχείου της w_1 */
τέλος όσο
όσο $(w_2 \not\equiv_F \varepsilon)$
  Έστω ότι $w_2 = w_2' x_{j_1}^{-1}$ /* ήτοι το $x_{j_1}^{-1}$ είναι το δεξιότερο στοιχείο της w_2 */
  $\delta_2 \leftarrow \delta_2 + \mathtt{Pop}(S_2)$;
  $u_2 \leftarrow x_{j_1 - \delta_2}^{-1} u_2$;
  $w_2 \leftarrow w_2'$ /* "Διαγραφή" του αριστερότερου στοιχείου της w_2 */
τέλος όσο
επίστρεψε $u_1 u_2$;

Κεφάλαιο 9

Το πρωτόκολλο του Stickel

Βασιζόμενος στο σκεπτικό του κλασσικού πρωτοκόλλου των Whitfield Diffie και Martin Hellman από το [DH76], ο E. Stickel παρέχει το μη-μεταθετικό ανάλογό του στην εργασία του [St05]. Το σχήμα χρησιμοποιεί ως ομάδα εφαρμογής, την ομάδα των πινάκων, γεγονός που το κάνει ευάλωτο σε επιθέσεις Γραμμικής Άλγεβρας [§9.2]. Ακολούθως στο Κεφάλαιο παρουσιάζονται δύο ακόμη εκδοχές του σχήματος: η πολυωνυμική εκδοχή και η τροπική εκδοχή, οι οποίες και εξετάζονται ενδελεχώς.



Σχήμα 9.0: Το σχήμα ανταλλαγής κλειδιού Diffie-Helmann

9.1 Το πρωτόκολλο του Stickel

Υπενθυμίζονται οι εξής βασικές έννοιες:

Ορισμός 9.1. Έστω μια ομάδα $(G, *)$. Ορίζεται

1. η **τάξη** του $g \in G$ ως $o(g) := \min\{n \in \mathbb{N} \cup \{+\infty\} : g^n = 1_G\}$, με $g^t = \begin{cases} g * g^{t-1}, & \text{εάν } t>0 \\ 1_G, & \text{εάν } t=0 \\ g^{-1} * g^{t+1}, & \text{εάν } t<0 \end{cases}$.
2. το **κέντρο** της ομάδας G ως $\mathcal{Z}(G) = \{c \in G : (\forall h \in G)[ch = hc]\}$.

Αλίκη	Βασίλης

Δημοσίως γνωστά:
Μη-αβελιανή ομάδα G και $w, a, b \in G$, με $o(a) = N$, $o(b) = M$ και $ab \neq ba$.

Προετοιμασία για την επακόλουθη επικοινωνία

$c_1 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathcal{Z}(G)$	$c_2 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \mathcal{Z}(G)$
$n \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{1, 2, \ldots, N-1\}$	$r \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{1, 2, \ldots, N-1\}$
$m \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{1, 2, \ldots, M-1\}$	$s \xleftarrow[\text{επιλογή}]{\text{τυχαία}} \{1, 2, \ldots, M-1\}$

Επικοινωνία

Ιδιωτικό κλειδί: n, m.	**Ιδιωτικό κλειδί:** r, s.
Δημόσιο κλειδί: $u := c_1 a^n w b^m \in G$	
$v := c_2 a^r w b^s \in G$ **:Δημόσιο κλειδί**	
$K_A = c_1 a^m v b^n$	$K_B = c_2 a^r u b^s$

$$K_A = c_1 a^n v b^m = c_1 a^n (c_2 a^r w b^s) b^m = c_1 c_2 a^{n+r} w b^{m+s} = c_2 a^r (c_1 a^n w b^m) b^s = c_2 a^r u b^s = K_B$$

Σχήμα 9.1: Το σχήμα ανταλλαγής κλειδιού Stickel

Παρατήρηση 9.2. *Μια πιο απλή έκδοση του πρωτοκόλλου επιτάσσει* $c_1 = c_2 = w = 1_G$.

9.1.1 Προτεινόμενες παράμετροι

- $G = \mathrm{GL}\left(k, \mathbb{F}_{2^\ell}\right)$ [οι αντιστρέψιμοι $k \times k$ πίνακες με στοιχεία από το σώμα $\mathbb{F}_{2^\ell}$].
- $k = 31$.
- $\ell \in \mathbb{N} \cap [2, k]$ (παρ' όλο που στο [St05] δεν προσδιορίζεται).
- $a, b \in \mathrm{GL}(k, \mathbb{F}_2) \leqslant \mathrm{GL}\left(k, \mathbb{F}_{2^\ell}\right)$ (ήτοι τα στοιχεία των πινάκων a, b είναι ή 0, ή 1).

9.2 Επίθεση Γραμμικής Άλγεβρας

Παρόλο που οι προθέσεις ήταν η ασφάλεια του σχήματος να βασισθεί στο

Πρόβλημα του διακριτού λογαρίθμου (στις ομάδες). Δεδομένων μιας ομάδας G και $b, g \in G$, να βρεθεί $k \in \mathbb{Z}$, τέτοιο ώστε $b^k = g$.

δηλαδή στην δυσκολία ανάκτησης των εκθετών $(n, m) \in \{1, \ldots, N-1\} \times \{1, \ldots, M-1\}$ (αντίστοιχα για το ζεύγος (r, s)), προέκυψε πως η ασφάλεια έγκειται στη δυσκολία του (απλούστερου) προβλήματος της αναλύσεως.

Η ιδέα της επίθεσης οφείλεται στον Vladimir Shpilrain, περιλαμβάνεται στο [Sh08]. Στηρίζεται στο γεγονός ότι η G είναι ομάδα και κατ' επέκτασην κάθε στοιχείο της είναι *αντιστρέψιμο*, κι έχει ως εξής:

Εν γνώσει του επιτιθέμενου είναι τα δημόσιοποιημένα στοιχεία:

- $w, a, b \in G$,
- $u \in G$ (το δημόσιο κλειδί της Αλίκης, όπου $u = c_1 a^n w b^m$) και
- $v \in G$ (το δημόσιο κλειδί του Βασίλη, όπου $v = c_2 a^r w b^s$).

Για την παρείσφρηση στο πρωτόκολλο του Stickel:

> Αρκεί να βρεθούν $x, y \in G$, τέτοια ώστε
>
> $$xa = ax \qquad yb = by \qquad u = xwy \tag{9.1}$$
>
> Χαρακτηριστικά του συστήματος (9.1):
>
> - $2k^2$ *γραμμικές* εξισώσεις, λόγῳ των $\{ xa = ax,\ \ yb = by \}$.
> - $2k^2$ αγνώστους (τα στοιχεία των $k \times k$ αντιστρεψίμων πινάκων $x, y \in G$).
> - k^2 *μη-γραμμικές*(!) εξισώσεις, λόγῳ της ισότητας $u = xwy$.

Επιλύοντας το σύστημα (9.1) θα ήταν δυνατόν να εξαχθεί το (κοινό) κλειδί ως ακολούθως:

$$xvy = x(c_2 a^r w b^s)y \overset{c_2 \in Z(G)}{=} c_2 x(a^r w b^s)y \underset{yb=by}{\overset{xa=ax}{=}} c_2 a^r (xwy) b^s \overset{u=xwy}{=} c_2 a^r u b^s = K_B = K_A$$

Συνεπώς, το πρόβλημα προς επίλυση τυποποιείται στο ακόλουθο:

Πρόβλημα της αναλύσεως (περιορισμένο στις υποομάδες). Δεδομένης μια αναδρομικά παριστάμενης (ημι)ομάδας G, δύο αναδρομικά παριστάμενων υπο(ημι)ομάδων $A, B \leqslant G$ και των $u, w \in G$, να βρεθεί $(x, y) \in A \times B$, τέτοιο ώστε $xwy = u$, δεδομένου ότι τουλάχιστον ένα τέτοιο ζεύγος υπάρχει.

Για ευκολία, θα ήταν επιθυμητό οι εξισώσεις στο σύστημα (9.1) να ήναι γραμμικές. Ισχύουν:

$$u = xwy \iff x^{-1}u = wy \qquad\qquad xa = ax \iff ax^{-1} = x^{-1}a$$

(το βήμα είναι εφικτό, αφού κάθε στοιχείο της G είναι αντιστρέψιμο). Θέτοντας $x_1 := x^{-1}$, το σύστημα για το σπάσιμο του πρωτοκόλλου του Stickel τυποποιείται ως εξής:

> Αρκεί να βρεθούν $x, y \in G$, τέτοια ώστε
>
> $$x_1 a = a x_1 \qquad\qquad yb = by \qquad\qquad x_1 u = wy \tag{9.2}$$
>
> όπου $x_1 = x^{-1}$. Χαρακτηριστικά του συστήματος (9.2):
>
> - $3k^2$ *γραμμικές* εξισώσεις.
> - $2k^2$ αγνώστους (τα στοιχεία των $k \times k$ αντιστρεψίμων πινάκων $x, y \in G$).

Επειδή $x_1 u = wy \iff x_1 = wyu^{-1}$ (πάλι χρησιμοποιήθηκε το γεγονός ότι το $u \in G$ είναι αντιστρέψιμο!), μπορεί να απαλλοιφθεί ο πίνακας $x_1 \in G$ και να προκύψει ότι

> Αρκεί να βρεθεί $y \in G$, τέτοιο ώστε
>
> $$wyu^{-1}a = awyu^{-1} \qquad\qquad yb = by \tag{9.3}$$
>
> Χαρακτηριστικά του συστήματος (9.3):
>
> - $2k^2$ *γραμμικές* εξισώσεις.
> - k^2 αγνώστους (τα στοιχεία του $k \times k$ αντιστρεψίμου πίνακα $y \in G$).

Για $k = 31$ (όπως προτείνεται στην αρχική εργασία [St$_{05}$]) το σύστημα (9.3) περιλαμβάνει 1922 $(= 2k^2)$ εξισώσεις, με 961 $(= k^2)$ αγνώστους.

9.2.1 Προτάσεις για βελτιστοποίηση

Τα $w, a, b \in G$ **να είναι *μη*-αντιστρέψιμα:** Συνεπώς, η G θα πρέπει να είναι *ημι*ομάδα με (αρκετά) μη-αντιστρέψιμα στοιχεία.

Δυναμική έκδοση: Εάν είναι να χρησιμοποιηθούν πίνακες, τότε προτείνεται $G = \mathbb{M}_k(R)$ το σύνολο *όλων* των $k \times k$ πινάκων υπεράνω ενός πεπερασμένου *δακτυλίου* R.

Πολυωνυμική έκδοση: Ένα επιπλέον πλεονέκτημα του μη περιορισμού σε αντιστρέψιμους πίνακες, είναι η δυνατότητα χρήσης ως στοιχείων του πρωτοκόλλου αυθαίρετες εκφράσεις της μορφής $\sum_{i=1}^{p} c_i a^i$, $p \in \mathbb{N}$, για $c_1, \ldots, c_p \in R$. [Βλ. Σχήμα 9.4]

- Μία επίθεση που ανακτά το μυστικό κλειδί $(n, m) \in \{1, \dots, M-1\} \times \{1, \dots, N-1\}$ οφείλεται στον Sramka και περιλαμβάνεται στο [Sr08].

9.3 Πολυωνυμική εκδοχή

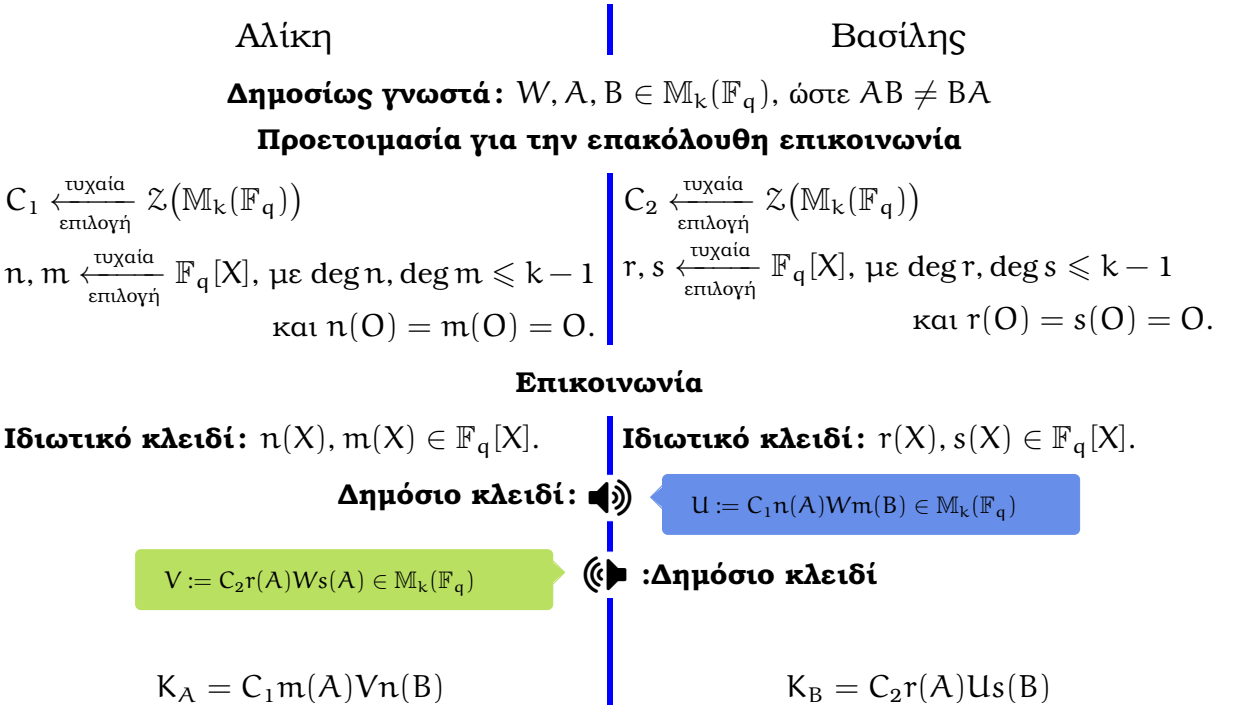
- Στα παρακάτω θεωρούνται $n \in \mathbb{N}$ και R ένας (τυχαίος) δακτύλιος.

Ορισμός 9.3. Το **χαρακτηριστικό πολυώνυμο** $\chi_A : R \longrightarrow \mathbb{R}$ του $A \in \mathbb{M}_n(R)$ ορίζεται ως $\chi_A(\lambda) := \det(\lambda I_n - A)$, όπου $\lambda \in R$ και $I_n \in \mathbb{M}_n(R)$ είναι ο ταυτοτικός $n \times n$ πίνακας.

Θεώρημα 9.4 (Cayley-Hamilton)**.** Έστω $A \in \mathbb{M}_n(R)$, τότε $\chi_A(A) = O$, όπου χ_A είναι το χαρακτηριστικό πολυώνυμο του A και $O = (o_{ij})_{1 \leqslant i,j \leqslant n}$, με $(\forall i, j = 1, \dots, n)[o_{ij} = 0]$.

Από το Θεώρημα 9.4 (Cayley-Hamilton) ικανοποιεί το χαρακτηριστικό του πολυώνυμο, επομένως $A^k = \sum_{i=0}^{n-1} c_i A^i$, για $k \geqslant n$ και κάποια $c_1, \dots, c_{n-1} \in R$. Συνεπώς, αρκεί να θεωρούνται πολυώνυμα βαθμού του πολύ $n-1$.

Μία γενίκευση του πρωτοκόλλου του Stickel [St05] είναι η ακόλουθη:



Σχήμα 9.4: Το σχήμα ανταλλαγής κλειδιού Stickel (πολυωνυμική εκδοχή)

Παρατήρηση 9.5. *Μία απλούστευση του παραπάνω πρωτοκόλλου υπαγορεύει τυχαίο δακτύλιο* R *και* $C_1 = C_2 = W = 1_R$ *(βλ. [MMR07, Sh08]).*

9.3.1 Κρυπτανάλυση

Παρατήρηση 9.6. *Το αρχικό πρωτόκολλο (Σχήμα 9.1) αποτελεί ειδική περίπτωση της πολυωνυμικής εκδοχής (Σχήμα 9.4), όπου* $n(x) = x^n$, $m(x) = x^m$, $r(x) = x^r$ *και* $s(x) = x^s$.

Ορισμός 9.7. Το **ελάχιστο πολυώνυμο** $\mu_A : \mathbb{F} \longrightarrow \mathbb{R}$ ενός $A \in \mathbb{M}_n(\mathbb{F})$ καλείται το μονικό* πολυώνυμο $P \in \mathbb{F}[x]$ ελαχίστου βαθμού, τέτοιο ώστε $P(A) = 0$.

Λήμμα 9.8. *Έστω* $A \in \mathbb{M}_n(\mathbb{F}_q)$ *και* $p(x) \in \mathbb{F}_q(x)$. *Εάν μκδ* $\big(p(x), \mu_A(x)\big) = 1$, *τότε ο* $p(A) \in \mathbb{M}_n(\mathbb{F}_q)$ *είναι αντιστρέψιμος.*

Απόδειξη. Όντας μκδ $\big(p(x), \mu_A(x)\big) = 1$, από τον αλγόριθμο του Ευκλείδου για πολυώνυμα, έπεται πως $(\exists r(x), s(x) \in \mathbb{F}_q[x])[p(x)r(x) + \mu_A(x)s(x) = 1]$. Επειδή $\mu_A(A) = 0$, έπεται ότι $p(A)r(A) = I_n$. Συνεπώς, ο $p(A) \in \mathbb{M}_n(\mathbb{F}_q)$ είναι αντιστρέψιμος. □

Για την παρείσφρηση στην πολυωνυμική εκδοχή του πρωτοκόλλου του Stickel:

> Αρκεί να βρεθεί το
> $$q(x) := \text{μκδ}\big(n(x), \mu_A(x)\big) \in \mathbb{F}_q[x]$$

καθώς τότε $(\exists p(x) \in \mathbb{F}_q[x])\big[n(x) = p(x)q(x)\big]$, με μκδ $\big(p(x), \mu_A(x)\big) = 1$. Από το Λήμμα 9.8, έπεται πως ο $p(A) \in \mathbb{M}_n(\mathbb{F}_q)$ είναι αντιστρέψιμος. Συνεπώς, για την Εύα

> Αρκεί να βρεθούν $X, Y \in \mathbb{M}_n(\mathbb{F}_q)$, τέτοιοι ώστε
> $$XA = AX \qquad YB = BY \qquad q(A)WY = XU \tag{9.4}$$
> $$\text{ο } X \in \mathbb{M}_n(\mathbb{F}_q) \text{ είναι αντιστρέψιμος} \tag{9.5}$$

Κατ' αρχάς, του σύστημα (9.4) έχει την προφανή λύση $X = \big(C_1 p(A)\big)^{-1}$ και $Y = m(B)$. Συνεπώς, έχει νόημα η αναζήτηση λύσεων. Η επίλυση μπορεί να επιτευχθεί με χρήση της μεθόδου απαλλοιφής του Gauss, η οποία θα τερματίσει αφήνοντας κάποιες μεταβλητές ελεύθερες. Κατόπιν, με εξαντλητική αναζήτηση στα στοιχεία του $\mathbb{F}_q$, μπορεί να εξαχθεί η λύση.

*Ο μεγιστοβάθμιος όρος του έχει συντελεστή ίσο με 1.

Εύρεση του $q(x)$ **στη δυναμική έκδοση:** τότε $q(x) = x^i$, για κάποιο $i \in \mathbb{N} \cap [1, \dots, n]$. Άρα[†], υπάρχουν μόνον $n - 1 \in \mathbb{N}$ υποψήφια πολυώνυμα. Η μεθοδολογία είναι:

1: $i \leftarrow 0$;
2: **επανάλαβε**
3: $\quad i \leftarrow i + 1$; $q \leftarrow x^i$;
4: $\quad (X, Y) \leftarrow$ Επίλυση με τη μέθοδο απαλλοιφής του Gauss του συστήματος (9.4);
5: **έως ότου** $(X \in \mathrm{GL}(n, \mathbb{F}_q))$

Εύρεση του $q(x)$ **στην πολυωνυμική έκδοση:** Εκ του γεγονότος ότι $n(O) = O$, έπεται πως $(\exists \pi(x) \in \mathbb{F}_q[x])\big[n(x) = x \cdot \pi(x)\big]$. Για το $\pi(x) \in \mathbb{F}_q[x]$, όντας ο $A \in \mathbb{M}_n(\mathbb{F}_q)$ δημοσίως γνωστός αρκεί να παραγοντοποιήσει η Εύα το $\chi_A \in \mathbb{F}_q[x]$ και να δοκιμάσει τους πιθανούς συνδυασμούς των αναγώγων συντελεστών του.

Παρατήρηση 9.9. *Εκτός του* $q(x)$ *οποιοδήποτε εκ των μκδ* $\big(m(x), \mu_B(x)\big)$*, μκδ* $\big(r(x), \mu_A(x)\big)$ *ή μκδ* $\big(s(x), \mu_B(x)\big)$ *ανακαλύψει η Εύα, τότε δύναται να δημιουργήσει σύστημα παρόμοιο με το* (9.4)*, το οποίο παρεισφρύει στο πρωτόκολλο του Σχήματος 9.4.*

9.3.1.Α΄ Συζήτηση

Επιλογή του $q(x) \in \mathbb{F}_q[x]$ **ώστε μκδ** $\big(n(x), \mu_A(x)\big) \neq 1$**:** Στην πολυωνυμική έκδοση αντί να επιλέγονται οι συντελεστές των $n(x), r(x) \in \mathbb{F}_q[x]$ τυχαία, να επιλέγονται ώστε τα πολυώνυμα να έχουν μη-τετριμμένο κοινό παράγοντα με το $\mu_A(x)$.

Χρήση του $\mathbb{Z}_\ell$**, αντί του** $\mathbb{F}_q$**, όπου** $\ell = pq$**, με** p, q **πρώτους αριθμούς:** Δεδομένων των $p, q \in \mathbb{N}$, δύναται να εξαχθεί πληροφορία από το κοινό κλειδί K μέσῳ των $K \mod p$ και $K \mod q$ τα οποία παρέχονται από το Κινέζικο Θεώρημα Υπολοίπων.

Χρήση του $\mathbb{Z}_{2^\ell}$**, αντί του** $\mathbb{F}_q$**:** Καθίσταται δυνατή η εξαγωγή πληροφορίας επιλύοντας τις εξισώσεις $K \equiv K \mod 2, K \equiv K \mod 2^2, \dots, K \equiv K \mod 2^n$.

Μέχρι να βρεθεί ένας κατάλληλος δακτύλιος οι ως άνω εκδόσεις θεωρούνται μη-ασφαλείς.

9.4 Τροπική εκδοχή

9.4.1 Τροπική άλγεβρα

Ένας **τροπικός ημιδακτύλιος** $(S, \oplus, \otimes)$ ορίζεται ως ένα σύνολο $S \subseteq \mathbb{R}$, με $0 \in S$, το οποίο είναι κλειστό ως προς τις πράξεις:

$$x \oplus y := \min\{x, y\} \qquad\qquad x \otimes y := x + y$$

[†]Εάν ήταν $q(x) = x^n$, τότε ο $A \in \mathbb{M}_n(\mathbb{F}_q)$ θα ήταν μηδενοδύναμος, άρα $(\forall k \in \mathbb{N})[k \geqslant n \implies A^k = O]$ και το κοινό κλειδί τα ήταν $K = O$.

Γίνεται φανερό πως ισχύουν τα εξής:

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z \qquad x \otimes (y \otimes z) = (x \otimes y) \otimes z \qquad \text{(προσεταιριστικότητα)}$$
$$x \oplus y = y \oplus x \qquad x \otimes y = y \otimes x \qquad \text{(αντιμεταθετικότητα)}$$

Επίσης, ισχύει η επιμεριστική ιδιότητα $(x \oplus y) \otimes z = (x \otimes z) \oplus (x \otimes z)$ και οι ιδιότητες $x \oplus x = x$, $x \otimes 0 = x$ και $x \oplus 0 \in \{0, x\}$. Η πράξη $\otimes$ προηγείται της $\oplus$. Επιπλέον, ορίζεται ένα ειδικό "ϵ-στοιχείο" ως $\epsilon = \infty$, ώστε

$$(\forall x \in S)[\epsilon \otimes x = x] \qquad (\forall x \in S)[\epsilon x = \epsilon]$$

Παρατήρηση 9.10. *Η παραπάνω κατασκευή μπορεί να θεωρηθεί και για* $x \oplus y := \max\{x, y\}$, *όπου τότε* $\epsilon := -\infty$.

Ένα (**τροπικό**) **μονώνυμο** μοιάζει με γραμμική συνάρτηση, ήτοι της μορφής $\alpha \otimes X \oplus \beta$, όπου $\alpha, \beta \in \mathbb{Z}$ και το X αποτελείται από μεταβλητές με πράξη ανάμεσά τους την $\otimes$.

Παράδειγμα 9.11. Ένα τροπικό μονώνυμο είναι το $x \otimes x \otimes y \otimes z \otimes z$, βαθμού 5. ⊣

Ένα **τροπικό πολυώνυμο** συντίθεται από μονώνυμα και είναι η ελάχιστη τιμή των γραμμικών συναρτήσεων που αντιπροσωπεύουν τα μονώνυμα.

Παράδειγμα 9.12. Ένα τροπικό πολυώνυμο είναι το

$$p(x, y, z) = 5 \otimes x \otimes y \otimes z \oplus x^{\otimes 2} \oplus 2 \otimes z \oplus 17$$

(τροπικού) βαθμού 3. ⊣

Συμβολισμός. Για $x \in S$ και $z \in \mathbb{N}$ θα συμβολίζεται $x^{\otimes z} = \begin{cases} x, \text{ εάν } z=1 \\ x \otimes x^{\otimes z-1}, \text{ αλλιώς} \end{cases}$

Για $S = \mathbb{M}_k(\mathbb{Z})$ οι πράξεις $\oplus, \otimes$ επεκτείνονται ως εξής: Έστω $A = (a_{ij}), B = (b_{ij}) \in S$,

$$(A \oplus B)_{ij} := \min\{a_{ij}, b_{ij}\} \qquad (A \otimes B)_{ij} := \min\left\{a_{is} + b_{sj} \in \mathbb{Z} : s = 1, \dots, k\right\} \qquad (\text{για } i, j = 1, \dots, k)$$

Το ταυτοτικό στοιχείο είναι το $I = (e_{ij}) \in S$, με $e_{ij} = \begin{cases} 0, \text{ εάν } i=j \\ \infty, \text{ αλλιώς} \end{cases}$

Η **τροπική άλγεβρα των** $k \times k$ **πινάκων** είναι ο τροπικός ημιδακτύλιος $(\mathbb{M}_k(\mathbb{Z}), \oplus, \otimes)$ εφοδιασμένος με τον εξής *βαθμωτό πολλαπλασιασμό*:

$$s \odot A := \begin{pmatrix} s & & \infty \\ & \ddots & \\ \infty & & s \end{pmatrix} \otimes A \qquad (\text{για } s \in \mathbb{Z} \text{ και } A \in \mathbb{M}_k(\mathbb{Z}))$$

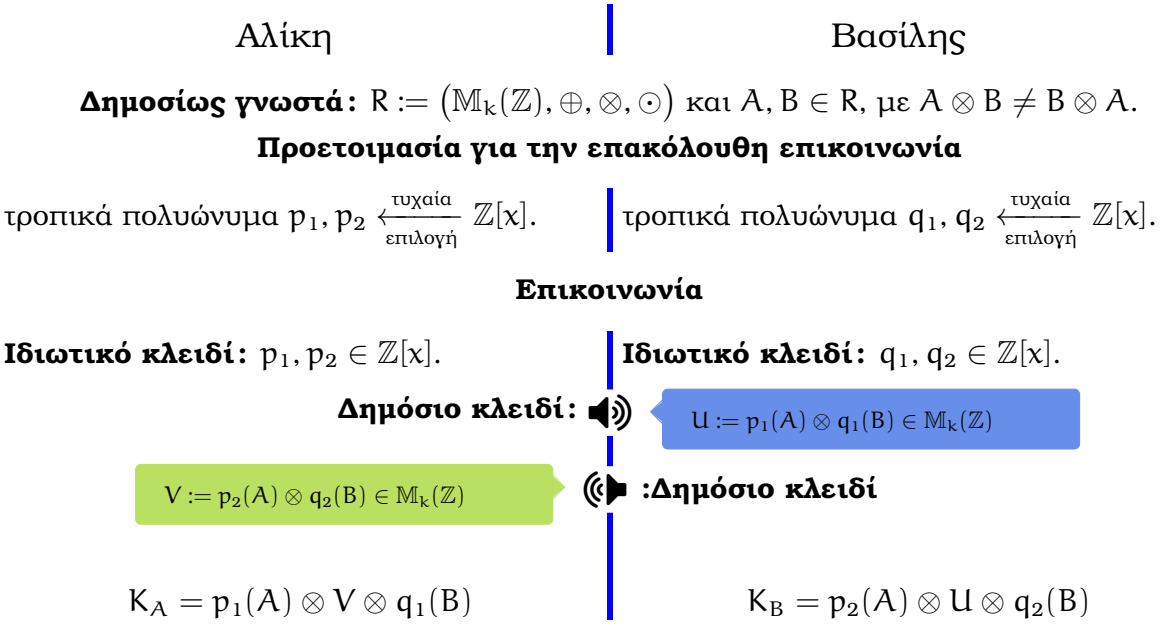
Παράδειγμα 9.13. Στην τροπική άλγεβρα των $k \times k$ πινάκων:

1. $\begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 3 \\ 2 & 8 \end{pmatrix} = \begin{pmatrix} \min\{1,0\} & \min\{2,3\} \\ \min\{2,5\} & \min\{-1,8\} \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 2 & -1 \end{pmatrix}.$
2. $\begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 3 \\ 2 & 8 \end{pmatrix} = \begin{pmatrix} \min\{1+0,2+2\} & \min\{1+3,2+8\} \\ \min\{5+0,-1+2\} & \min\{5+3,-1+8\} \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 1 & 7 \end{pmatrix}.$
3. $2 \odot \begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} \equiv \begin{pmatrix} 2 & \infty \\ \infty & 2 \end{pmatrix} \otimes \begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 7 & 1 \end{pmatrix}.$ ⊣

Παρατήρηση 9.14 ([Bu10, σ.5])**.** *Εν αντιθέσει με τη συνήθη άλγεβρα* $(\mathbb{M}_k(\mathbb{Z}), +, \times, \cdot)$*, η τροπική άλγεβρα* $(\mathbb{M}_k(\mathbb{Z}), \oplus, \otimes, \odot)$ *έχει αρκετά μη-αντιστρέψιμα στοιχεία. Κάθε αντιστρέψιμο στοιχείο του* $(\mathbb{M}_k(\mathbb{Z}), \oplus, \otimes)$ *είναι η μετάθεση γραμμών ή/και στηλών ενός διαγωνίου πίνακα* $D = (d_{ij})$*, με* $d_{ij} = \begin{cases} s, & \text{εάν } i=j \\ \infty, & \text{αλλιώς} \end{cases}$ *για κάποιο* $s \in \mathbb{Z}$*.*

9.4.2 Το τροπικό πρωτόκολλο του Stickel

Η τροπική εκδοχή του παραπάνω πρωτοκόλλου του Σχήματος 9.4 είναι (από το [GS13]) η:



$$K_A = p_1(A) \otimes \big(q_1(A) \otimes q_2(B)\big) \otimes q_1(B) = p_2(A) \otimes \big(p_1(A) \otimes p_2(B)\big) \otimes q_2(B) = K_B$$

αφού $p_1(A) \otimes q_1(A) = q_1(A) \otimes p_1(A)$ και $p_2(B) \otimes q_2(B) = q_2(B) \otimes p_2(B)$.

Σχήμα 9.14: Το τροπικό σχήμα ανταλλαγής κλειδιού Stickel

Η επίθεση Γραμμικής Άλγεβρας (βλ. §9.2) δεν αποδίδει στην παρούσα εκδοχής, διότι:

- Οι $A, B \in R$ έχουν επιλεχθεί ώστε εν γένει να είναι μη-αντιστρέψιμοι, έτσι η εξίσωση $X \otimes Y = U$, για γνωστό U και αγνώστους X, Y, δεν υλοποιείται σε γραμμικό σύστημα.
- Το σύστημα $\{ A \otimes X = X \otimes A,\ Y \otimes B = B \otimes Y \}$ μεταφράζεται αφενός σε σύστημα γραμμικών εξισώσεων, αφετέρου (από το [BNR10]) η επίλυσή του ανήκει στην κλάση $\mathsf{NP} \cap \mathsf{coNP}$ και η πεποίθηση είναι πως δεν ανήκει στην κλάση P.

9.4.2.Α΄ Προτεινόμενες παράμετροι

- $k = 10$ (το μέγεθος των πινάκων).
- Για $A = (a_{ij}), B = (b_{ij}) \in R$ να είναι $(\forall i, j = 1, \ldots, k)\big[a_{ij}, b_{ij} \in \mathbb{Z} \cap [-10^{10}, 10^{10}]\big]$.
- Για τα τροπικά πολυώνυμα $p_1(x), p_2(x), q_1(x), q_2(x) \in \mathbb{Z}[x]$:
  - οι βαθμοί επιλέγονται ομοιόμορφα στη τύχη από το διάστημα $\mathbb{N} \cap [1, 10]$·
  - οι συντελεστές επιλέγονται ομοιόμορφα στη τύχη στο διάστημα $\mathbb{Z} \cap [-1000, 1000]$.

9.4.2.Β΄ Κρυπτογράφηση με χρήση δίρρητων αυτομορφισμών μιας τροπικής άλγεβρας πολυωνύμων

Στον τροπικό ημιδακτύλιο $(S, \oplus, \otimes)$ ορίζεται επιπλέον η πράξη $x \oslash y := z$, με $y \otimes z = x$. Ακόμη, ορίζεται η σχέση ισοδυναμίας

$$(x \oslash y) \sim (z \oslash t) \iff_{\text{ορ}} x \otimes t = y \otimes z$$

και συμβολίζεται $\mathrm{Rat}(S) := S_{/\sim}$.

Τέλος, ένα πιο εξεζητημένο από εκείνο του Σχήματος 9.14 πρωτόκολλο περιέχεται στο [GS13, §3] και σκιαγραφείται ως ακόλουθα:

Δημοσίως γνωστό: $P := \mathrm{Rat}[x_1, \ldots, x_n]$ ο ημιδακτύλιος πηλίκο μιας τροπικής άλγεβρας πολυωνύμων με συντελεστές από το $\mathbb{Z}$.

Αλίκη: Δημόσιο κλειδί: $a \in \mathrm{Aut}(P)$.

Ιδιωτικό κλειδί $a^{-1} \in \mathrm{Aut}(P)$.

Βασίλης: Μήνυμα προς κρυπτογράφηση: $s := (s_1, \ldots, s_n) \in \mathbb{Z}^n$.

Δημοσιοποιεί: $E_a(s) := a(s_1, \ldots, s_n)$.

Αλίκη: Αποκρυπτογραφεί ως εξής $a^{-1}\big(E_a(s)\big) = s = (s_1, \ldots, s_n)$.

Κεφάλαιο 10

Ανάλυσης επόμενα...

Δύο επιπλέον πρωτόκολλα που βασίζονται στο πρόβλημα της αναλύσεως είναι: (ένα ακόμη) των Vladimir Shpilrain και Alexander Ushakov από την εργασία τους [SU06] και της Yeşem Kurt από την [Ku06]. Τα δύο πρωτόκολλα (ιδιαιτέρως των Shpilrain-Ushakov και η δεύτερη εκδοχή της Kurt) φέρονται να έχουν αρκετά κοινά σημεία στο σκεπτικό τους μιας και αμφότερα κάνουν χρήση της έννοιας της κεντροποιούσας υποομάδας. Έτσι παρέχουν εκ προοιμίου την προϋπόθεση που περιλαμβάνουν αρκετά από τα προηγούμενα πρωτόκολλα: $(\exists A, B \leqslant G)(\forall a \in A)(\forall b \in B)[ab = ba]$.

Για άλλη μια φορά οι ομάδες πλεξίδων συνίστανται ως βάση για τα πρωτόκολλα. Ωστόσο, η επιλογή τους δημιουργεί μία εγγενή αδυναμία στο πρωτόκολλο της Kurt (βλ. §10.2.1.Β΄) η οποία αντιμετωπίζεται με σύγχηση των στοιχείων των υποομάδων του πρωτοκόλλου.

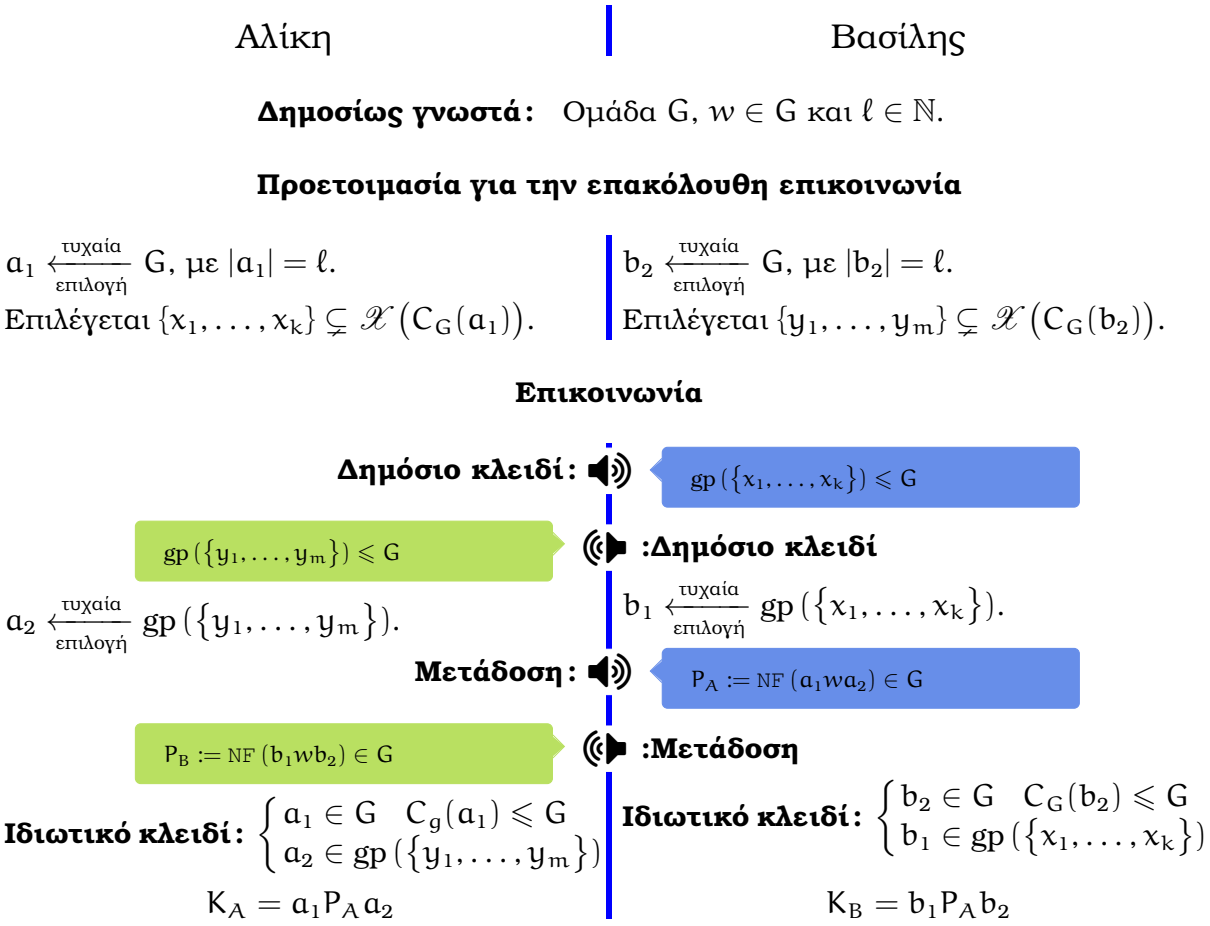
10.1 Το πρωτόκολλο των Shpilrain-Ushakov με απόκρυψη των υποομάδων

Στην παρούσα Ενότητα πρόκειται να αναπτυχθεί μία παραλλαγή του Σχηματος AN: το πρωτόκολλο των Shpilrain-Ushakov από την εργασία τους [SU06]. Επιπλέον, περιέχονται οι υποθέσεις που αφορούν την ομάδα που πρόκειται να εφαρμοσθεί το πρωτόκολλο καθώς και οι λόγοι που καθιστούν το πρωτόκολλο ασφαλές από επιθέσεις στο ιδιωτικό κλειδί, αλλά και σημαντικά ασφαλές.

Ορισμός 10.1. Έστω μια ομάδα G. Η **κεντροποιούσα υποομάδα του** $x \in G$ ορίζεται ως $C_G(x) := \{y \in G : xy = yx\}$, ήτοι όλα τα στοιχεία που μετατίθενται με το $x \in G$.

Συμβολισμός. $C_G(g_1, \ldots, g_n) := \bigcap_{i=1}^{n} C_G(g_i)$, για $g_1, \ldots, g_n \in G$ σε μια ομάδα G.

Διαφοροποίηση από το Σχήμα AN: Οι ομάδες $A, B \leqslant G$ δεν είναι πλήρως γνωστές, παρά μόνον ένα μέρος τους.



$$K_A = a_1 P_B a_2 = a_1(b_1 w b_2)a_2 = b_1(a_1 w a_2)b_2 = b_1 P_A b_2 = K_B$$

διότι $a_1 b_1 = b_1 a_1$ και $a_2 b_2 = b_2 a_2$.

Σχήμα 10.1: Το σχήμα ανταλλαγής κλειδιού Shpilrain-Ushakov

10.1.0.Α΄ Προτεινόμενες παράμετροι

- $G = B_n$ και ειδικά $n = 64$.
- $\ell = 1024$.
- Η Αλίκη υπολογίζει το ζεύγος $\left(a_1, C_G(a_1)\right)$ και ο Βασίλης το ζεύγος $\left(b_2, C_G(b_2)\right)$ με χρήση του αλγορίθμου από το [FG03] ο οποίος υπολογίζει τις κεντροποιούσες υποομάδες στις ομάδες πλεξίδων. Ωστόσο, δεν χρειάζεται ο υπολογισμός ολόκληρης της κεντροποιούσας ομάδας, μιας και μόνον μερικά στοιχεία της δημοσιοποιούνται.

Για την ομάδα G απαιτείται:

(P1) Η G να είναι μη-μεταθετική ομάδα εκθετικού ρυθμού αύξησης.

[Για $n \geqslant 3$ η B_n είναι μη-μεταθετική ομάδα εκθετικού ρυθμού αύξησης.]

(P2) Να υπάρχει αποτελεσματικός τροπος υπολογισμού των κανονικών μορφών των στοιχείων της G.

[Υπάρχουν αρκετές κανονικές μορφές πλεξίδων, όπως των Garside, Birman-Ko-Lee, οι οποίες υπολογίζονται σε τετραγωνικό χρόνο σε σχέση με το μήκος της λέξης.]

(P3) Να είναι υπολογιστικά εύκολος ο υπολογισμός του γινομένου και του αντιστρόφου των στοιχείων.

[Το γινόμενο και η αντιστροφή πλεξίδων απαιτούν τετραγωνικό -σε σχέση με το μήκος της λέξης- χρόνο υπολογισμού στην B_n.]

(P4) Να είναι υπολογιστικά εύκολη η δημιουργία ζευγών $\big(a, \{a_1, \ldots, a_k\}\big)$, τέτοιων ώστε $(\forall i = 1, \ldots, k)[aa_i = a_i a]$.

[Ο υπολογισμός του $C_G(g)$, $g \in G$, είναι ανάλογος του $|\mathrm{SSS}(g)|$, που τυπικά είναι μεγάλο —βλ. [GW04].]

(P5) Για $A := \{g_1, \ldots, g_k\} \subseteq G$, θα πρέπει να είναι δύσκολα υπολογίσιμη η $C_G(A) \leqslant G$.

[Ο υπολογισμός του $C_G(A)$ είναι ανάλογος του $|\mathrm{SS}(A)|$, που τυπικά είναι μεγάλο.]

(P6) Ακόμη κι αν υπολογισθεί η $H := C_G(g_1, \ldots, g_k)$, θα πρέπει να είναι δύσκολο να βρεθούν $x \in H$ και $y \in H_1$ (για κάποια δεδομένη $H_1 \leqslant G$) τέτοια ώστε $xwy = w'$, ήτοι να επιλυθεί το πρόβλημα του μέλους για διπλό σύμπλοκο.

[Δεν υπάρχει γνωστός αλγόριθμος για το πρόβλημα του μέλους για διπλό σύμπλοκο ομάδων πλεξίδων.]

10.1.1 Κρυπτανάλυση

10.1.1.Α΄ Επίθεση στο ιδιωτικό κλειδί

Συμβολισμός. Έστω $A := \{x_1, \ldots, x_k\} \subsetneq \mathscr{X}\big(C_G(a_1)\big)$ και $B := \{y_1, \ldots, y_m\} \subsetneq \mathscr{X}\big(C_G(b_2)\big)$.

Για την παρείσφρηση ενός αντιπάλου στο πρωτόκολλο των Shpilrain-Ushakov αρκεί να βρεθεί το ιδιωτικό κλειδί ενός εκ των οντοτήτων που επικοινωνούν.

Ανάκτηση του ιδιωτικού κλειδιού της Αλίκης:
Να βρεθεί ένα $(a_1', a_2') \in G \times \mathrm{gp}(B)$, με $(\forall x \in \mathrm{gp}(A))[a_1' x = x a_1']$ και $P_A = \mathtt{NF}(a_1' w a_2')$.

Εν τοιαύτη περιπτώσει θα είναι $a_1' w a_2' = a_1 w a_2$ κι άρα το ζεύγος (a_1', a_2') αντικαθιστά το πραγματικό ιδιωτικό κλειδί της Αλίκης (a_1, a_2). Για την επιτυχία της επιθέσεως θα πρέπει

(A1) Να υπολογισθεί η κεντροποιούσα υποομάδα $C_G(A)$.

(A2) Να επιλυθεί το πρόβλημα του μέλους για το διπλό σύμπλοκο $C_G(A) \cdot w \cdot \mathrm{gp}(B)$.

Παρόμοια, είναι και η

Ανάκτηση του ιδιωτικού κλειδιού του Βασίλη:
Να βρεθεί ένα $(b_1', b_2') \in \mathrm{gp}(A) \times G$, με $(\forall y \in \mathrm{gp}(B))[b_2' y = y b_2']$ και $P_B = \mathtt{NF}(b_1' w b_2')$.

10.1.1.Β΄ Σημαντική ασφάλεια

Η βασική *υπόθεση υπολογιστικής ασφαλείας* του πρωτοκόλλου είναι:

> Δεδομένων των (δημοσίων γνωστών) $w, P_A, P_B \in G$, είναι δύσκολο να υπολογισθεί το κοινό κλειδί $K \in G$.

Η εκδοχή απόφασης της υπόθεσης έγκειται στην:

> Δεδομένων των w, P_A, P_B είναι δύσκολο να ξεχωρίσει το K από κάποιο τυχόν $awb \in G$, για $a \in \mathrm{gp}(\{y_1, \ldots, y_m\})$ και $b \in \mathrm{gp}(\{x_1, \ldots, x_k\})$.

η οποία φαντάζει να μην ισχύει για τις περισσότερες επιλογές των w, P_A, P_B, λόγῳ του ότι

$$\left.\begin{array}{rl} P_A = a_1 w a_2 \implies & a_1 = P_A a_2^{-1} w^{-1} \\ & K = a_1 b_1 w a_2 b_2 \end{array}\right\} \implies K = P_A a_2^{-1} (w^{-1} P_B) a_2$$

ήτοι το κοινό κλειδί είναι γινόμενο των δημοσίων γνωστών $P_A, w^{-1} P_B$ κι ενός στοιχείου της $\mathrm{gp}(\{y_1, \ldots, y_m\})$.

Έστω $G = B_n$ όπως ορίζουν οι προτεινόμενες παράμετροι (§10.1.0.Α΄). Μία πλεξίδα $b \in B_n$ καλείται *μη-γνήσια* εάν αντιστοιχεί σε μία μετάθεση $\sigma \in S_n$. Έστω ο επιμορφισμός $\pi : B_n \longrightarrow S_n$.

⟦Εάν η $w^{-1} P_B$ είναι μη-γνήσια πλεξίδα⟧: τότε $(\exists \rho_B \in S_n)[\rho_B \neq \mathrm{id}]$. Η $\pi(a_2)^{-1} \rho_B \pi(a_2) \in S_n$ έχει την ίδια κυκλική δομή με την $\rho_B \in S_n$ κι αυτό αποφέρει κάποια πληροφορία για την $\pi(K) = \pi(P_A)\pi(a_2)^{-1} \rho_B \pi(a_2)$· για παράδειγμα η γνώση της $\pi(P_A) \in S_n$ και της κυκλικής δομής της $\pi(a_2)^{-1} \rho_B \pi(a_2) \in S_n$ δίδουν πληροφορία για την πιθανή τάξη της $\pi(K)$.

⟦Εάν οι $P_A, w^{-1} P_B$ είναι μη-γνήσιες πλεξίδες⟧: τότε με χρήση ομομορφισμών μπορεί να εξαχθεί πληροφορία για το K —βλ. [GM02].

⟦Εάν η $w^{-1} P_B$ είναι γνήσια πλεξίδα και η P_A είναι μη-γνήσια πλεξίδα⟧: τότε ο ομομορφισμός $\pi : B_n \longrightarrow S_n$ αποκαλύπτει πληροφορία για το κοινό κλειδί K.

10.2 Το πρωτόκολλο της Kurt

Έπονται δύο σχήματα ανταλλαγής κλειδιού που οφείλονται στην Yeşem Kurt από την εργασία [Ku06], η ασφάλεια των οποίων στηρίζεται στο πρόβλημα της τριπλής αναλύσεως.

10.2.1 Πρωτόκολλο I

Συμβολισμός. Έστω το μονοειδές G και $A, B \subseteq G$. Ο συμβολισμός $[A, B]$ είναι συντομογραφία του $(\forall a \in A)(\forall b \in B)[ab = ba]$.

Αλίκη	Βασίλης

Δημοσίως γνωστά: Μονοειδές G.

Αρχικά δεδομένα για την επακόλουθη επικοινωνία

$\mathcal{A} := \{A_1, A_2, A_3, X_1, X_2\} \subseteq \mathcal{P}(G)$	$\mathcal{B} := \{B_1, B_2, B_3, Y_1, Y_2\} \subseteq \mathcal{P}(G)$

τέτοια ώστε να ικανοποιούν τις:
Συνθήκες αντιστρεψιμότητας: Τα στοιχεία των $X_1, X_2, Y_1, Y_2 \subseteq G$ είναι αντιστρέψιμα.
Συνθήκες μεταθετικότητας: $[A_2, Y_1] = 1$, $[A_3, Y_2] = 1$, $[B_1, X_1] = 1$, $[B_2, X_2] = 1$.

Προετοιμασία για την επακόλουθη επικοινωνία

$a_1 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} A_1$, $a_2 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} A_2$, $a_3 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} A_3$,	$b_1 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} B_1$, $b_2 \xleftarrow[\text{επιλογή}]{\text{επιλογή}} B_2$, $b_3 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} B_3$,
$x_1 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} X_1$, $x_2 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} X_2$.	$y_1 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} Y_1$, $y_2 \xleftarrow[\text{επιλογή}]{\text{τυχαία}} Y_2$.

Επικοινωνία

Ιδιωτικό κλειδί: $(a_1, a_2, a_3) \in A_1 \times A_2 \times A_3$

Δημόσιο κλειδί: $(u, v, w) := (a_1x_1, x_1^{-1}a_2x_2, x_2^{-1}a_3)$

Ιδιωτικό κλειδί: $(b_1, b_2, b_3) \in B_1 \times B_2 \times B_3$

Δημόσιο κλειδί: $(p, q, r) := (b_1y_1, y_1^{-1}b_2y_2, y_2^{-1}b_3)$

$K_A = a_1pa_2qa_3r$	$K_B = ub_1vb_2wb_3$

$$K_A = a_1pa_2qa_3r = a_1(b_1y_1)a_2(y_1^{-1}b_2y_2)a_3(y_2^{-1}b_3) = a_1b_1a_2b_2a_3b_3 =$$
$$= (a_1x_1)b_1(x_1^{-1}a_2x_2)b_2(x_2^{-1}a_3)b_3 = ub_1vb_2wb_3 = K_B$$

Σχήμα 10.1: Το σχήμα ανταλλαγής κλειδιού Kurt (I)

10.2.1.Α΄ Κρυπτανάλυση

Κατά την επιλογή των $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}(G)$ θα πρέπει να ληφθεί πρόνοια στην αποφυγή των κάτωθι περιπτώσεων:

⟦**Περίπτωση** $[X_1, Y_1] = [X_2, Y_2] = [X_2, Y_1] = 1$⟧**:** τότε το κοινό κλειδί δύναται να εξαχθεί από την δημόσια πληροφορία (u, v, w) και (p, q, r) ως εξής:

$$\begin{aligned} upvqwr &= (a_1x_1)(b_1y_1)(x_1^{-1}a_2x_2)(y_1^{-1}b_2y_2)(x_2a_3)(y_2b_3) && \text{(εξ ορισμού)} \\ &= a_1b_1a_2b_2a_3b_3 && \text{(Υποθέσεις: } [X_1, Y_1] = [X_2, Y_2] = [X_2, Y_1] = 1\text{)} \end{aligned}$$

⟦**Περίπτωση** $[A_2, B_1] = [A_3, B_2] = [A_3, B_1] = 1$⟧**:** τότε το κοινό κλειδί δύναται να εξαχθεί από την δημόσια πληροφορία (u, v, w) και (p, q, r) ως εξής:

$$\begin{aligned} uvwpqr &= (a_1x_1)(x_1^{-1}a_2x_2)(x_2a_3)(b_1y_1)(y_1^{-1}b_2y_2)(y_2b_3) && \text{(εξ ορισμού)} \\ &= a_1a_2a_3b_1b_2b_3 && \text{(εξ ορισμού)} \\ &= a_1b_1a_2b_2a_3b_3 && \text{(Υποθέσεις: } [A_2, B_1] = [A_3, B_2] = [A_3, B_1] = 1\text{)} \end{aligned}$$

⟦**Περίπτωση** $[A_2, B_1] = [X_2, B_1] = 1$⟧**:** Είναι $K_A = a_1b_1a_2b_2a_3b_3 \overset{[A_2,B_1]=1}{=} a_1a_2b_1b_2a_3b_3$. Όμως και $uv = a_1a_2x_2$. Συνεπώς, αναλύοντας το $uv \in G$ σε δύο στοιχεία, ήτοι $uv = ax_2$, για $a \in G$ και $x_2 \in X_2$, έπεται ότι

$$\begin{aligned} apqa_3r &= a(b_1b_2y_2)a_3r && (pq = b_1b_2y_2) \\ &= a(b_1b_2y_2)a_3y_2^{-1}b_3 && (r = y_2^{-1}b_2) \\ &= a(b_1b_2)a_3b_3 && \text{(Συνθήκη μεταθετικότητας: } [A_3, Y_2] = 1\text{)} \\ &= (uvx_2^{-1})(b_1b_2)(x_2w)b_3 && (w = x_2^{-1}a_3) \\ &= uvx_2^{-1}b_1x_2b_2wb_3 && \text{(Συνθήκη μεταθετικότητας: } [B_2, X_2] = 1\text{)} \\ &= uvb_1b_2wb_3 && \text{(Υπόθεση: } [X_2, B_1] = 1\text{)} \\ &= ub_1vb_2wb_3 && (v = x_1^{-1}a_2x_2 \text{ και } [X_2, B_1] = [A_2, B_1] = [B_1, X_1] = 1) \\ &= K_B \equiv K_A \end{aligned}$$

⟦**Περίπτωση** $[A_3, B_2] = [A_3, Y_1] = 1$⟧**:** Όμοια με την περίπτωση $[A_2, B_1] = [X_2, B_1] = 1$.

⟦**Εύρεση ψευδο-κλειδιού**⟧**:** δηλαδή αρκεί να βρεθούν $a_1, x_1, a_2, x_2, a_3 \in G$, τέτοια ώστε

$$a_1x_1 = u \tag{10.1}$$

$$x_1^{-1}a_2x_2 = v \tag{10.2}$$

$$x_2^{-1}a_3 = w \tag{10.3}$$

$$\begin{cases} \text{τα } a_1, x_1, a_2, x_2, a_3 \in G \text{ ικανοποιούν τις} \\ \text{συνθήκες αντιστρεψιμότητας και μεταθετικότητας} \end{cases} \tag{10.4}$$

[Η (10.3) περιέχει γραμμικές εξισώσεις, ενώ η (10.2) τετραγωνικές εξισώσεις (δύσκολο να επιλυθούν), αφού (10.2) $\iff a_2x_2 = x_1v$.]

Έστω ότι:

0. $x_1 \in X_1$, $a_2 \in A_2$, $x_2 \in X_2$ και $a_3 \in A_3$, τότε η απαίτηση (10.4) ικανοποιείται.
1. Έστω πως η (10.3) έχει μοναδική λύση, τότε αρκεί η ανάλυση του w σε *δύο* στοιχεία, ήτοι $w = x_2^{-1} a_3$.
2. Δεδομένης της μοναδικής λύσης της (10.3) αρκεί να αναλυθεί το ν σε *δύο* στοιχεία, ήτοι (10.2) $\iff \nu x_2^{-1} = x_1^{-1} a_2$, αφού το $x_2 \in G$ είναι γνωστό.
3. Όντας το $a_1 \in G$ ελεύθερο περιορισμών, θα είναι $a_1 = u x_1^{-1}$.

Συνεπώς, *αρκεί η εξίσωση* (10.3) *να έχει πολλές λύσεις*.

10.2.1.Β΄ Προτεινόμενες παράμετροι

► Έστω $n = 3d + 1$, για $d \in \mathbb{N} \setminus \{1\}$.

Θεωρούνται

$$\mathcal{A} = \Big\{ A_1 = B_n, \quad A_2 = X_1 = \mathrm{gp}\left(\{\sigma_1, \ldots, \sigma_{d-1}\}\right), \qquad A_3 = X_2 = \mathrm{gp}\left(\{\sigma_1, \ldots, \sigma_{2d-1}\}\right) \Big\} \tag{10.5}$$

$$\mathcal{B} = \Big\{ B_3 = B_n, \quad B_1 = Y_1 = \mathrm{gp}\left(\{\sigma_{d+1}, \ldots, \sigma_{n-1}\}\right), \quad B_2 = Y_2 = \mathrm{gp}\left(\{\sigma_{2d+1}, \ldots, \sigma_{n-1}\}\right) \Big\} \tag{10.6}$$

που ικανοποιούν τις συνθήκες αντιστρεψιμότητας και μεταθετικότητας, όπου $\sigma_i \in B_n$ είναι ο i-οστός Artin γεννήτορας της ομάδας πλεξίδων B_n [βλ. §1.3].

Θεωρώντας την αναπαράσταση του Burau [βλ. §1.3.3], επειδή είναι $n - 1 = 3d$, για $d \in \mathbb{N} \setminus \{1\}$, κάθε γεννήτορας $\sigma_i \in B_n$, $i = 1, 2, \ldots, n-1$, αντιστοιχεί σε έναν πίνακα της $\mathrm{GL}(3d, \mathbb{Z}[t^{\pm 1}])$, ο οποίος χωρίζεται σε 9 υποπίνακες της $\mathbb{M}_d(\mathbb{Z}[t^{\pm 1}])$. Έτσι -για παράδειγμα- τα στοιχεία $a_1 \in A_1$ και $x_1 \in X_1$, μεταφέρονται σε πίνακες της μορφής

$$x_1 = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix} \qquad\qquad a_1 = \begin{pmatrix} X_{11} & 0_d & 0_d \\ 0_d & I_d & I_d \\ 0_d & 0_d & I_d \end{pmatrix}$$

όπου $0_d, I_d \in \mathbb{M}_d(\mathbb{Z}[t^{\pm 1}])$ ο ταυτοτικός και ο μηδενικός αντίστοιχα $d \times d$ πίνακας. Συνεπώς η πρώτη συνιστώσα του δημοσίου κλειδιού της Αλίκης είναι της μορφής:

$$u := a_1 x_1 = \begin{pmatrix} A_{11}X_{11} & A_{12} & A_{13} \\ A_{21}X_{11} & A_{22} & A_{23} \\ A_{31}X_{11} & X_{32} & A_{33} \end{pmatrix} \tag{10.7}$$

δηλαδή η δεύτερη και η τρίτη στήλη του u συμπίπτουν με τις αντίστοιχες του a_1 αποκαλύπτοντας έτσι αρκετή πληροφορία.

Για την αποφυγή των παραπάνω, θεωρούνται οι κάτωθι τροποποιήσεις των συλλογών (10.5) και (10.6): Έστω $s_1, s_2, s_3, s_4 \in B_n$, τότε

$$\mathcal{A}' = \Big\{ A_1' = B_n, \qquad A_2' = \{s_2 x s_2^{-1} : a \in A_2\}, \qquad A_3' = \{s_4 a s_4^{-1} : a \in A_3\}$$
$$X_1' = \{s_1 x s_1^{-1} : x \in X_1\}, \qquad X_2' = \{s_3 x s_3^{-1} : x \in X_2\}\Big\}$$
$$\mathcal{B}' = \Big\{ B_3' = B_n, \qquad B_1' = \{s_1 b s_1^{-1} : b \in B_1\}, \qquad B_2' = \{s_3 b s_3^{-1} : b \in B_2\}$$
$$Y_1' = \{s_2 y s_2^{-1} : y \in Y_1\}, \qquad Y_2' = \{s_4 y s_4^{-1} : x \in Y_2\}\Big\}$$

με τις καινούργιες συλλογές $\mathcal{A}', \mathcal{B}' \subseteq \mathcal{P}(B_n)$ να ικανοποιούν τις συνθήκες μεταθετικότητας μιας και $(\forall a, b, s \in B_n)\big[ab = ba \implies (sas^{-1})(sbs^{-1}) = (sbs^{-1})(sas^{-1})\big]$.

Παρατήρηση 10.2. *Επιλέγουτας τα $s_1, s_2, s_3, s_4 \in B_n$ να περιέχουν μεγάλο πλήθος γευνητόρων της B_n, τότε αποφεύγεται η αποκάλυψη πληροφορίας, όπως στην* (10.7).

Παρατήρηση 10.3. *Όπως αναφέρθηκε, θα πρέπει να ληφθεί πρόνοια ώστε η εξίσωση*

$$(s_3 x_2^{-1} s_3^{-1})(s_4 a_3 s_4^{-1}) = w'$$

ή ισοδύναμα η εξίσωση

$$x_2^{-1} s_3^{-1} s_4 a_3 = s_3^{-1} w' s_4$$

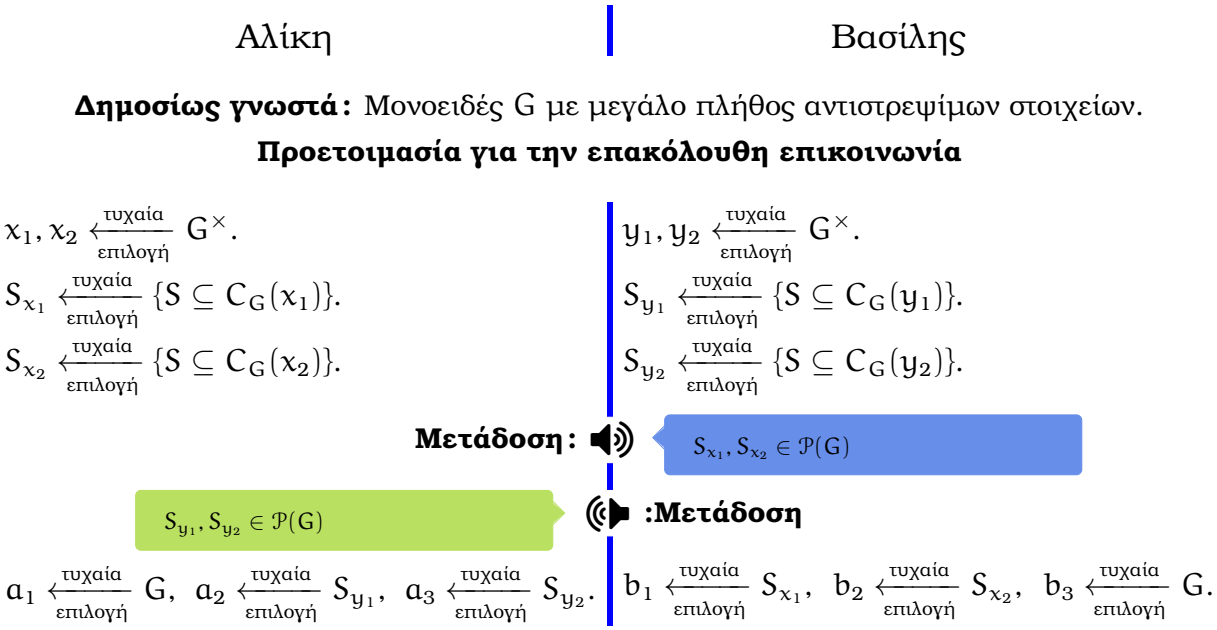
(που είναι η αντίστοιχη της (10.3) *για τις συλλογές $\mathcal{A}', \mathcal{B}' \subseteq \mathcal{P}(B_n)$) να έχει μεγάλο πλήθος λύσεων.*

Παρατήρηση 10.4 (επιθέσεις βασισμένες στο μήκος)**.** *Στο [Gar10] οι D. Garber και λοιποί, προσφέρουν μία πιθανοτική μέθοδο επίλυσης συστήματος εξισώσεων σε μια (τυχαία) πεπερασμένα παραγόμενη υποομάδα της B_n. Ο αλγόριθμος επιτυγχάνει εάν οι άγνωστοι ανήκουν σε υποομάδες που παράγονται από μεγάλο πλήθος Artin γευνητόρων· ωστόσο, σύμφωνα με τις παραμέτρους που προτάθηκαν, οι άγνωστοι ανήκουν σε υποομάδες που παράγονται από έναν Artin γευνήτορα. Έτσι οι επιθέσεις βασισμένες στο μήκος αποτυγχάνουν.*

10.2.2 Πρωτόκολλο II

Στην ουσία πρόκειται για μια τροποποίηση του Σχήματος 10.1.

Συμβολισμός. Έστω ένα μονοειδές G. Το σύνολο των αντιστρεψίμων στοιχείων του G συμβολίζεται ως $G^\times := \big\{x \in G : (\exists y \in G)[xy = e = yx]\big\}$



Σχήμα 10.4: Το σχήμα ανταλλαγής κλειδιού Kurt (II)

10.2.2.Α΄ Κρυπτανάλυση

Όπως αναφέρεται και στην §10.2.1.Α΄ η εύρεση ενός ψευδοκλειδού έγκειται στην επίλυση της εξισώσεως

$$x_1^{-1} a_2 x_2 = \nu$$

όπου εδώ $x_1, x_2 \in G^\times$ και $a_2 \in S_{y_1} \subseteq C_G(y_1)$, τα οποία ικανοποιούν τις συνθήκες μεταθετικότητας. Με άλλα λόγια θα πρέπει το $\nu \in G$ να αναλυθεί σε

- $a_2 \in S(y_1)$·
- $x_1 \in G^\times$ ώστε να μετατίθεται με κάθε στοιχείο του S_{x_1} και
- $x_2 \in G^\times$ ώστε να μετατίθεται με κάθε στοιχείο του S_{x_2}.

Υπενθυμίζεται πως

- ► Τα $S_{x_1}, S_{x_2}, S_{y_1} \subseteq \mathcal{P}(G)$ είναι δημοσίως γνωστά.

Κατά συνέπεια, αρχικά, ο επιτθέμενος θα πρέπει να επιλύσει

Το πρόβλημα εύρεσης της κεντροποιούσας υποομάδας. Δεδομένης μιας ομάδος G και $g_1, \ldots, g_k \in G$, να βρεθεί η κεντροποιούσα υποομάδα τους $C_G(g_1, \ldots, g_k) \leqslant G$.

Έστω ότι $S_{x_1} = \mathrm{gp}(g_1, \ldots, g_k)$. Για τον υπολογισμό του $x_1 \in G^\times$ δεν είναι γνωστή καμμία πληροφορία, παρά μόνον ότι μετατίθεται με κάθε στοιχείο του $S_{x_1} \subseteq \mathcal{P}(G)$. Επομένως, $x_1 \in C_G(g_1) \cap \cdots \cap C_G(g_k) = C_G(g_1, \ldots, g_k)$. Παρόμοια, $x_2 \in C_G(g'_1, \ldots, g'_\ell)$, για $S_{x_2} = \mathrm{gp}(g'_1, \ldots, g'_\ell)$.

Άπαξ και ο επιτιθέμενος επιλύσει το παραπάνω πρόβλημα, κατόπιν, έρχεται αντιμέτωπος με

Το πρόβλημα της τριπλής αναλύσεως. Θεωρείται η ομάδα G, $\nu \in G$ και $H, A, H' \leqslant G$, όπου $H = C_G(g_1, \ldots, g_k)$, $H' = C_G(g'_1, \ldots, g'_\ell)$ και $A = \mathrm{gp}(y_1, \ldots, y_m)$. Να βρεθεί μία τριάδα $(x_1, a_2, x_2) \in H \times A \times H'$, τέτοια ώστε $\nu = x_1^{-1} a_2 x_2$, δεδομένου ότι υπάρχει τουλάχιστον μία τέτοια τριάδα.

Το σύνηθες πρόβλημα της αναλύσεως επιτάσσει την ανάλυση ενός γνωστού στοιχείου σε τρεις παράγοντες, ο μεσαίος εκ των οποίων είναι γνωστός. Στο πρόβλημα της τριπλής αναλύσεως και οι τρεις παράγοντες είναι άγνωστοι.

Παρατήρηση 10.5. *Οι υποθέσεις* ***(P1)*****–*****(P6)*** *για την ομάδα* G *που περιέχονται στην* § *10.1.0.Α΄ αφορούν και τα πρωτόκολλα της Kurt. Επιπλέον, υπεισέρχεται η υπόθεση:*

(P7) *Ακόμη κι αν βρεθούν οι* $H_1 = C_G(g_1, \ldots, g_k)$ *και* $H_2 = C_G(g'_1, \ldots, g'_\ell)$*, θα πρέπει να είναι δύσκολο να βρεθούν* $x_1 \in H_1$*,* $x_2 \in H_2$ *και* $a \in H$*, τέτοια ώστε* $\nu = x_1 a x_2$*, για κάποια δεδομένη* $H \leqslant G$ *με γνωστούς τους γεννήτορές της και δεδομένο* $\nu \in G$*.*

Παράρτημα

Παράρτημα Α΄

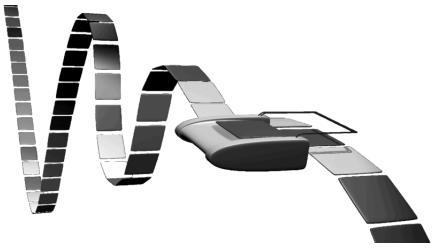
Αλγόριθμοι και Πολυπλοκότητα

► *Στα παρακάτω θεωρείται ένα σύνολο* Σ *το οποίο θα διαδραματίζει το ρόλο του αλφαβήτου.*

Ορισμός Α΄.1. Κάθε $L \subseteq \Sigma^*$ καλείται **γλώσσα**.

Τα *μηχανικά μέρη* της **αιτιοκρατικής** (deterministic) **μηχανής Turing** είναι

- μία ταινία απείρου μήκους με αρχή,
- μία κεφαλή ανάγνωσης



Πηγή: `en.wikipedia.org`

και συνίσταται ως η επτάδα

$$\langle \Sigma,\ \Gamma,\ Q,\ \delta,\ q_0,\ q_{\text{deny}},\ q_{\text{accept}} \rangle$$

όπου

- Σ είναι το αλφάβητο της γλώσσας,
- Γ είναι το αλφάβητο της ταινίας,
- Q είναι ένα σύνολο καταστάσεων,
  - Η $q_0 \in Q$ είναι η αρχική κατάσταση της μηχανης,
  - Οι $q_{\text{deny}}, q_{\text{accept}} \in Q$ είναι δύο *ειδικές* διακεκριμένες καταστάσεις όπου η μηχανή περατώνει τη λειτουργία της και απορρίπτει/αποδέχεται την είσοδό της·
- $\delta : \Gamma \times Q \longrightarrow \Gamma \times Q \times \{L, R\}$, με τα σύμβολα L, R να εννοούν τη μετάβαση της κεφαλής ανάγνωσης της μηχανής μία θέση αριστερά/δεξιά από τη τρέχουσα θέση.

Η αιτιοκρατική μηχανή Turing υλοποιείται από ένα πρόγραμμα με οδηγίες της μορφής:

$$\mathfrak{l}: \textbf{ εάν } \sigma \textbf{ τότε } (\sigma'; o; \mathfrak{l}')$$

όπου ξεκινώντας από την οδηγία με ετικέτα $\mathfrak{l} = 1$,

1. Εάν το σύμβολο που διαβάστηκε είναι το $\sigma \in \Sigma$, τότε η μηχανή
   (α′) αντικαθιστά το $\sigma \in \Sigma$ με το $\sigma' \in \Sigma$,
   (β′) μετακινεί την κεφαλή της κατά $o \in \mathbb{Z}$ θέσεις
   [εάν $o \in \mathbb{N}$, τότε η κίνηση είναι προς τα δεξιά, αλλιώς προς τ′ αριστερά]
   (γ′) εκτελεί την οδηγία με ετικέτα $\mathfrak{l}'$.
2. Αλλιώς, εκτελεί την οδηγία με ετικέτα $\mathfrak{l} + 1$.

Η **αναιτιοκρατική** (nondeterministic) **μηχανή Turing** καθόλα ίδια με την αιτιοκρατική μηχανή Turing, με τη μόνη διαφοροποίηση ότι

- $\delta \subseteq (\Gamma \times Q) \times \big(\Gamma \times Q \times \{L, R\}\big)$

και υλοποιείται από ένα πρόγραμμα με οδηγίες της μορφής:

$$\mathfrak{l}: \textbf{ εάν } \sigma \textbf{ τότε επίλεξε μία από τις οδηγίες } \big\{(\sigma'_1; o_1; \mathfrak{l}'_1), \ldots, (\sigma'_n; o_n; \mathfrak{l}'_n)\big\}$$

Ορισμός Α′.2. Η (αν)αιτιοκρατική μηχανή Turing $\langle \Sigma, \Gamma, Q, \delta, q_0, q_{\text{deny}}, q_{\text{accept}} \rangle$ **αποδέχεται** την γλώσσα $L \equiv L(\Gamma)$ εάν τερματίζει και η κατάστασή της είναι η q_{accept}.

Ορισμός Α′.3 (Ασυμπτωτικός συμβολισμός)**.** Έστω $f, g : \mathbb{N} \longrightarrow \mathbb{N}$. Ορίζονται

$$f = \mathcal{O}(g) \iff_{\text{ορ}} (\exists k \in \mathbb{R}^*_+)(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})\big[n > n_0 \implies \big|f(n)\big| \leqslant k \cdot g(n)\big]$$
$$f = \Theta(g) \iff_{\text{ορ}} (\exists k_1, k_2 \in \mathbb{R}^*_+)(\exists n_0 \in \mathbb{N})(\forall n \in \mathbb{N})\big[n > n_0 \implies k_1 \cdot g(n) \leqslant \big|f(n)\big| \leqslant k_2 \cdot g(n)\big]$$
$$f = \Omega(g) \iff_{\text{ορ}} (\exists k \in \mathbb{R}^*_+)(\forall n_0 \in \mathbb{N})(\exists n \in \mathbb{N})\big[n > n_0 \wedge \big|f(n)\big| \geqslant k \cdot g(n)\big]$$

Λήμμα Α′.4. *Έστω* $f, g : \mathbb{N} \longrightarrow \mathbb{N}$. *Ισχύει ότι:*

(i) $f = \Omega(g) \iff g = \mathcal{O}(f)$.

(ii) $f = \Theta(g) \iff (f = \mathcal{O}(g)) \wedge (g = \mathcal{O}(f))$.

Ορισμός Α΄.5. Η (αν)αιτιοκρατική μηχανή Turing M **αποφασίζει** την $L \subseteq \Sigma^*$, εάν δοθέντος ενός $x \in \Sigma^*$, τότε

(α΄) Εάν $x \in L$, τότε η $M(x)$ τερματίζει στην κατάσταση q_{accept}.

(β΄) Εάν $x \notin L$, τότε η $M(x)$ τερματίζει στην κατάσταση q_{deny}.

Ορισμός Α΄.6. Έστω μία αύξουσα συνάρτηση $f : \mathbb{N} \longrightarrow \mathbb{N}$. Ορίζονται οι **κλάσεις πολυπλοκότητας** ως ακόλουθα:

$$\mathsf{DTIME}(f) := \big\{ L \subseteq \Sigma^* : \text{ υπάρχει αιτιοκρατική μηχανή Turing η οποία αποφασίζει την } L \text{ σε χρόνο } \mathcal{O}(f(n)) \big\}$$

καθώς και

$$\mathsf{DSPACE}(f) := \big\{ L \subseteq \{0,1\}^* : \text{ υπάρχει αιτιοκρατική μηχανή Turing η οποία αποφασίζει την } L \text{ χρησιμοποιώντας } \mathcal{O}(f(n)) \text{ θέσεις της ταινίας της} \big\}$$

Παραπάνω $n \in \mathbb{N}_0$ είναι το μήκος[¶] του $x \in \Sigma^*$ από τον Ορισμό Α΄.5. Ανάλογα ορίζονται τα αναιτιοκρατικά ανάλογα $\mathsf{NTIME}(f)$ και $\mathsf{NSPACE}(f)$ των $\mathsf{DTIME}(f)$ και $\mathsf{DSPACE}(f)$ αντίστοιχα.

Ιδιαιτέρως,

$$\mathsf{P} := \bigcup_{c \in \mathbb{N}} \mathsf{DTIME}(|x|^c) \qquad\qquad \mathsf{NP} := \bigcup_{c \in \mathbb{N}} \mathsf{NTIME}(|x|^c)$$

όπου ως $n \in \mathbb{N}_0$ συμβολίζεται το μήκος[¶] του $x \in \Sigma$ από τον Ορισμό Α΄.5.

Σημαντικά αποτελέσματα της Θεωρίας Πολυπλοκότητας υπαγορεύουν πως

$$\mathsf{L} \subseteq \mathsf{NL} \subseteq \mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSPACE} = \mathsf{PSPACE} \subseteq \mathsf{EXP} \subseteq \mathsf{NEXP}$$

όπου παραπάνω είναι: $\mathsf{L} := \bigcup_{c \in \mathbb{N}} \mathsf{DSPACE}(\big(\log n\big)^c)$, $\mathsf{PSPACE} := \bigcup_{c \in \mathbb{N}} \mathsf{DSPACE}(n^c)$, $\mathsf{EXP} := \bigcup_{c \in \mathbb{N}} \mathsf{DSPACE}(2^{n^c})$ και οι NL, NSPACE και NEXP τα αναιτιοκρατικά ανάλογά τους.

Εάν $\mathcal{C}$ είναι μία κλάση πολυπλοκότητας, τότε ορίζεται η **συμπληρωματική** της κλάση $\mathrm{co}\mathcal{C} := \{\Sigma^* \setminus L \subseteq \Sigma^* : L \in \mathcal{C}\}$.

Στην Θεωρία της Πολυπλοκότητας τα προβλήματα μιας κλάσης πολυπλοκότητας "συνδέονται" μεταξύ τους με μία σχέση μερικής διάταξης, η οποία καλείται **αναγωγή** και υποδηλώνει την έννοια ότι *ένα πρόβλημα είναι τουλάχιστον τόσο δύσκολο να επιλυθεί ότι ένα άλλο.*

Σημείωση. *Η υπολογιστική πολυπλοκότητα της αναγωγής πρέπει να ανήκει το πολύ στην κλάση πολυπλοκότητας που ανήκουν και τα προβλήματα.*

[¶] το πλήθος των συμβόλων του Σ που απαιτούνται ώστε να γραφεί το x.

Θεωρείται μία κλάση πολυπλοκότητας $\mathcal{C}$. Ένα πρόβλημα P καλείται **δύσκολο** (hard) εάν κάθε πρόβλημα της $\mathcal{C}$ ανάγεται (με την υπολογιστική πολυπλοκότητα της αναγωγής να ανήκει το πολύ στην κλάση $\mathcal{C}$) στο P. Το πρόβλημα P καλείται $\mathcal{C}$**-πλήρες** εάν $P \in \mathcal{C}$ και είναι δύσκολο.

Ορισμός Α΄.7. Μία γλώσσα $L \subseteq \Sigma^*$ καλείται **αναδρομική** εάν υπάρχει μηχανή Turing που την αποφασίζει [βλ. Ορισμό Α΄.5].

Ορισμός Α΄.8. Μία γλώσσα $L \subseteq \Sigma^*$ καλείται **αριθμήσιμα αναδρομική** (recursively enumerable), υπάρχει μία μηχανή Turing M, η οποία σε κάθε είσοδο $x \in \Sigma^*$,

- εάν $x \in L$, τότε η M τερματίζει στην κατάσταση q_{accept} κι
- εάν $x \notin L$, τότε η M τρέχει για πάντα

Θεώρημα Α΄.9. Εάν μία γλώσσα $L \subseteq \Sigma^*$ είναι αναδρομική, τότε είναι και αριθμήσιμα αναδρομική.

Ορισμός Α΄.10. Μία συνάρτηση $f : \Sigma^* \longrightarrow \Sigma^*$ καλείται **αναδρομική** εάν υπάρχει μηχανή Turing, τέτοια ώστε $(\forall x \in \Sigma^*)\big[M(x) = f(x)\big]$.

Περαιτέρω Μελέτη

Για μια πιο εμπεριστατομένη ματιά στον κόσμο της Πολυπλοκότητας, ο ενδιαφερόμενος μπορεί να ανατρέξει (ενδεικτικά) στα κάτωθι συγγράμματα:

[1] Χ. Παπαδημητρίου, *Computational Complexity*, Addison-Wesley, 1^{η} έκδοση (1994).

[2] Χ. Παπαδημητρίου, Η. R. Lewis, *Στοιχεία Θεωρίας Υπολογισμού*, εκδόσεις Κριτική, 2^{η} έκδοση (2005).

[3] S. Arora, B. Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press (2009).

[4] O. Goldreich, *Computational Complexity: A Coneptual Perspective*, Cambridge University Press (2008).

[5] M. Sipser, *Introduction to the Theory of Computation*, Thompson Course Technology, 2^{η} έκδοση (2006).

ή (ενδεικτικά) στις παρακάτω επισκοπήσεις:

[1] S. Cook, *An overview of computational complexity*, Commun. ACM, ACM, **26**(6) (1983), 400—408.

[2] L. Trevisan, *Lecture Notes in Computational Complexity*, UC Berkeley (2002).

Βιβλιογραφία

[AAG99] I. Anshel, M. Anshel, D. Goldfeld, *An algebraic method for public-key encryption*, Math. Res. Lett. **6** (1999), 287–291.

[Ad84] S. I. Adjan, *Fragments of the word Delts in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984), 505—510.

[AAFG01] I. Anshel, M. Anshel, B. Fisher, D. Goldfeld, *New Key Agreement Protocols in Braid Grouop Cryptography*, in David Naccache, editor, "Topics in Cryptology — CT-RSA 2001", Lecture Notes in Computer Science **2020** (2001), 13—27, Springer.

[Ar45] E. Artin, *Theorie der Zopfe*, Hamburg **4** (1925), 47—72.

[Ar47] E. Artin, *Theory of Braids*, Ann. Math. **48** (1947), 101—126.

[BKL98] J. Birman, K. Ko, S. Lee, *A new approach to the word problem in braid groups*, Adv. Math. **139** (1998), 322—353.

[Bir06] J.-C. Birget, *Circuits, coNP-completeness, and the groups of Richard Thompson*, J. Algebra Comput., **16** (1) (2006), 35–90.

[BMS06] J.-C. Birget, Σ. Μαγκλιβέρας, M. Sramka, *On public-key cryptosystems based on combinatorial group theory*, Tatra Mountains Methematical Publications, **33** (2006), 137–148.

[BNR10] M. Bezem, R. Nieuwenhuis, E. Rodriguez-Carbonell, *Hard problems in maxal-gebra, control theory, hypergraphs amd other areas*, Information Processing Letters **110(4)** (2010), 133—138.

[Bo58] W. Boone, *The word problem*, Proceedings of the National Academy of Sciences **44**(10), `www.pnas.org/sgi/reprint/44/10/1061.pdf`, (1958), 1061—1065.

[Bu10] P. Butkovic, *Max-linear systems: theory and algorithms*, Springer-Verlag London (2010).

[CMI] Clay Mathematical Institute.
http://www.claymath.org/prizeproblems/pvsnp.htm.

[CKLHC01] J. C. Cha, K. H. Ko, S. J. Lee, J. W. Han, J. H. Cheon, *An Efficient Implementation of Braid Groups*, ASIACRYPT'01, LNCS **2248** (2001, 144—156.

[Co94] D. Collins, *Relations among the squares of the generators of the braid group*, Invent. Math. **117** (1994), 525—529.

[De11] M. Dehn, *Uber unendliche diskontinuierliche Gruppen*, Math. Annaeln **71**(1) (1911), 116—144.

[De12] M. Dehn, *Transformation der Kurven auf zweiseitigen Flächen*, Math. Annaeln **72**(3) (1912), 413—421.

[Deh97] P. Dehornoy, *A Fast Method for Computing Braids*, Adv. Math. **125** (1997), 200—235.

[Del72] P. Deligne, *Les immeubles des groupes detresses généralisés*, Invent. Math. **17** (1972), 273—302.

[DH76] W. Diffie, M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22** (1976), 644—654.

[DS04] C. Druţu, M. Sapir, *Non-linear residually finite groups* (2004).

[ECHLPT92] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Patterson, W. Thurston, *Word Processing in Groups*, Jones and Bartlett, Boston, Mass. (1992).

[EG85] T. El-Gamal, *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms* (1985).

[EM94] E. A. El-Rifai, H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45**(2) (1994), 479—497.

[Fe03] E. Fedder, *Algorithmic Problems in the Braid Group*, διδακτορική διατριβή, https://arxiv.org/ftp/math/papers/0305/0305205.pdf, (2003).

[FG03] N. Franco, J. Gonzalez-Meneses, *Computation of Centralizers n Braid groups and Garside groups*, Rev. Mat. Iberoamericana **19** (2) (2002), 367—384.

[Fou11] J. Fountain, *An Introduction to Thompson's Group* V (2011), διαθέσιμο στον http://www-users.york.ac.uk/~varg1/thompson-11.pdf .

[FRZ96] R. Fenn, D. Rolfsen, J. Zhu *Centralisers in the braid group and singular braid monoid*, Enseign. Math. (2) **42** (1996), 75—96.

[Ga69] F. A. Garside, *The Braid Group and Other Groups*, Quart. J. Math. Oxford **20**, No.78 (1969), 235—254.

[Gar05] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, *Probabilistic Solutions of Equations in the Braid Group*, arXiv:math.GR/020967v1 (2002).

[Gar10] D. Garber, *Braids: Introductory Lectures on Braids, Configurations and Their Applications*, Κεφάλαιο 1, https://arXiv.org/pdf/0711.3941.pdf (2010).

[GM84] Goldwasser, S. Micali, *Probabilistic encryption*, JCSS **28**, No.2 (1984), 270—299.

[GM02] R. Gennaro, D. Micciancio, *Cryptanalysis of a pseudorandom generator based on braid groups*, in EUROCRYPT 2002, Lecture Notes in Comput. Sci. **2332** (2002), 367—384.

[Grig85] R. Grigorchyk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Math. USSR-Izv. **25** (1985), 259-300.

[GS] D. Grigoriev, V. Shpilrain, *Unconditionally secure multiparty computation of secret sharing*, preprint.

[GS13] D. Grigoriev, V. Shpilrain, *Tropical Cryptography* (2013). Διαθέσιμο στον: http://arxiv.org/abs/1301.1195.

[Gu06] V. S. Guba, *The Dehn function of Richard Thompson's group* F *is quadratic*, Inventiones Mathematicae **163**, No.2 (2006), 313—342.

[GW04] J. Gonzalez-Meneses, B. Weist, *On the structure of centraliser of a braid*, Ann. Sci. Écol. Norm. Sup. **37** (5) (2004), 729—757.

[GZ85] M. Garzon, Y. Zalcstein, *The Complexity of Grigorchyk Groups with Application to Cryptography*, Theoretical Computer Science **88** (1991) 83-98, Elsevier.

[HGS99] C. Hall, I. Goldberg, B. Schneider, *Reaction Attacks Against Several Public-Key Cryptosystems*, In Vijay Varadharajan and Yi Mu, editors, Information and Communication Security, Second International Conference, ICICS'99, vol. 1726 of Lecture Notes in Computer Science (1999) 2—12, Springer.

[HKS13] M. Habeeb, D. Kahrobaei, V. Shpilrain, *A secret sharing scheme based on group presentations and the word problem* IACR Cryptology ePrint Archive 2013: **226** (2013).

[HS] D. Hofheinz, R. Steinwandt, *Cryptanalysis of a Public Key Cryptosystem Based on Grigorchyk Groups*, αδημοσίευτο.

[HS02] D. Hofheinz, R. Steinwandt, *A Practical Attack on Some Braid Group Based Cryptographic Primitives*, in Public Key Cryptography, 6th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2003 Proceedings, Y. G. Desmedt, ed., Lecture Notes in Computer Science **2567** (2002), 187—198.

[Hu02] J. Hughes, *A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem*, 7th Australasian Conference of Information Security and Privacy - ACISP 2002, Lecture Notes in Computer Science **2384**, Springer-Verlag (2002), 176—189.

[KLCHKP00] K. Ko, S. Lee, J. Cheon, J. Han, C. Park, *New Public Key Cryptosystem using Braid Groups*, Proc. of Crypto 2000, Lecture Notes in Computer Science, **1880**, Springer-Verlag (2000), 166—183.

[Ku06] Yeşem Kurt, *A New Key Exchange Primitive Based on the Triple Decomposition Problem*, IACR Cryptology (2006), διαθέσιμο στον http://eprint.iacr.org/2006/378.

[LePa03] E. Lee, H. Park, *Cryptanalysis of the Public Key Encryption Based on Braid Groups*, Proc. of EUROCRYPT'03, Lecture Notes on Computer Science **2656**, Springer-Verlag (2003), 166—183.

[LL02] S. J. Lee, E. Lee, *Potential Weaknesses of the Commutator Key Agreement Protocol Based on Braid Groups*, in Lars Knudsen, editor, Advances in Cryptology – EUROCRYPT 2002, Lecture Notes in Computer Science **2332** (2002), 14—28.

[LP05] F. Levy-dit-Vehel, L. Perret *On the Wagner-Magyarik Cryptosystem* in Coding and Cryptography (Ø. Ytrehus, ed.) (2005) 316–329, Springer-Berlin.

[Ma40] A. I. Malcev, *On isomorphic matrix representations of infinite groups of matrices*, Mat. Sb. **8** (1940), 405—422· και μεταφρασμένο στα αγγλικά Amer. Math. Soc. Transl. (2) **45** (1965), 1—18.

[McK43] J. C. C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, The Journal of Symbolic Logic, **8** (1943), 61-76.

[Mih58] K. A. Mihailova, *The occurrence problem for direct products of groups*, Dokl. Akad. Nauk SSSR **119** (1958), 1103–1105 (στα ρώσικα).

[MMR07] G. Maze, C. Monico, J. Rosenthal, *Public key cryptography based on semigroup actions*, Advances in Mathematics of Communications **4** (2007), 489—507.

[MSU08] A. Myasnikov, V. Shpilrain, A. Ushakov, *Group-Based Cryptography*, Advanced Courses in Mathematics, CRM Barcelona, (2008), Birkhuser Verlag, Basel.

[MO85] K. Madlener, F. Otto, *Pseudo-natural aglorithms for the word problem for finitely presented monoids and groups*, J. of Symbolic Computation, **1** (1985), 383-418.

[No55] P. S. Nobikov, *On the akgorithmic unsolvability of the word problem*, Proceedings of the Steklov Institute of Mathematics, **44** (1955), 1-143 (στα ρώσικα).

[Pa10] Δ. Παναγόπουλος, *A secret sharing scheme using groups*, preprint (2010), http://arxiv.org/PScache/arxiv/pdf/1009/1009.0026v1.pdf.

[Pai99] P. Paillier, *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*, Advances in Cryptography, Proceedings of EUROCRYPT'85, Springer-Verlag (1999), 50—61.

[Petr03] George Petrides *Cryptanalysis of the Public Key Cryptosystem Based on the Word Problem on the Grigorchyk Grouops* 9th IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science 2898 (2003), 234-244, Springer, Berlin.

[PR1991] M. S. Paterson, A. A. Razborov, *The Set of Minimal Braids is coNP-complete*, J. Algorithms **12** (1991), 393—408.

[RfC2828] Request for Comments 2828, Internet Security Glossary (2000).

[RSA78] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtainiing Digital Signatures and Public Key Cryptosystems*, Communications of the ACM **21**, No.2 (1978), 120—126.

[Sh79] A. Shamir, *How to share a secret*, Communications of the ACM **22** (11) (1979, 612—613.

[Sh04] V. Shpilrain, *Assessing security of some group based cryptosystems*, Group theory, statistics, and cryptography, Contemporary Mathematics 360 (2004), 167—177.

[Sh08] V. Shpilrain, *Cryptanalysis of Stickel's Key Exchange Scheme*, Computer Science in Russia 2008, Lecture Notes on Computer Science 5010 (2008) 283—288, Springer.

[Sr08] M. Sramka, *On the Security of Stickel's Key Exchange Scheme* (2008).

[St05] E. Stickel, *A New Method for Exchanging Secret Keys*. In: Proc. of the Third International Conference on Information Technology and Applications (ICITA05) **2** (2005) 426—430.

[SU05] V. Shpilrain, A. Ushakov *Thompson's group and public key cryptography* Lecture Notes Comp. Sc. **3531** (2005) 151-164.

[SU06] V. Shpilrain, A. Ushakov *A New Key Exchange Protocol Based on the Decomposition Problem* Contemp. Math. **418** (2006) 161–167.

[SU06] V. Shpilrain, A. Ushakov, *The conjugacy search problem in public key cryptography: unnessecary and insufficient*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), 285–289.

[SZ09] V. Sphilrain, G. Zapata, *Using decision problems in public key cryptography*, Groups Complexity in Cryptography **1** (2009), 33—49. Διαθέσιμο στον: http://www.sci.ccny.cuny.edu/~shpil/res.html.

[Th88] W. Thurston, *Finite state algorithms for the braid group*, Circulated notes (1988), 23 σελίδες.

[VS02] M.I. Gonzalez Vasco, Reiner Steinwandt, *Reaction attacks on public key cryptosystems based on the word problem, preprint* (2002).

[We73] B. A. F. Wehrfritz, *Generalized free products of linear groups*, Proc. London Math. Soc. (3) **27** (1973), 402—424.

[WM85] N. Wagner, M. Magyarik, *A Public Key Cryptosystem Based on the Word Problem*, Proc. CRYPTO'84, Lecture Notes in Computer Science Vol. 196 (1985) 19–36, Springer.

[Za14] Ε. Ζάχος, *Διαφάνειες στο μεταπτυχιακό μάθημα Αλγόριθμοι και Πολυπλοκότητα ΙΙ*, επιμέλεια: Α. Αντωνόπουλος, Εθνικό Μετσόβειο Πολυτεχνείο (2014).