Εθνικό και Καποδιστριακό Πανεπιστήμιο
Αθηνών

Μεταπτυχιακό Πρόγραμμα Λογικής και
Αλγορίθμων

$\mu\Pi\lambda\forall$

Πλεξίδες και Κρυπτογραφία

Χρήστος Τζέτζιας
Επιβλέπων: Ράπτης Ευάγγελος

Σεπτέμβρης 2003

Στην Ελένη

Πρόλογος

Το κείμενο που ακολουθεί αποτελεί τη διπλωματική μου εργασία, όπως προβλέπει το πρόγραμμα σπουδών του Μ.Π.Λ.Α. Πρόκειται για μια προσπάθεια να παρουσιαστεί κατά το δυνατόν ολοκληρωμένα η πρόσφατη δραστηριοποίηση γύρω από το χρήση των ομάδων πλεξίδων στην κρυπτογραφία. Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Ευάγγελο Ράπτη για τη βοήθειά του και για την πρότασή του να ασχοληθώ με το ενδιαφέρον αυτό θέμα. Επίσης ευχαριστώ το Ίδρυμα Κρατικών Υποτροφιών για την υποτροφία που μου παρείχε κατά το δεύτερο έτος των μεταπτυχιακών σπουδών μου.

Σχήμα 1: Ποιός είπε ότι η κρυπτογραφία πλεξίδων είναι πρόσφατη ιδέα;

Περιεχόμενα

1 Κρυπτογραφία

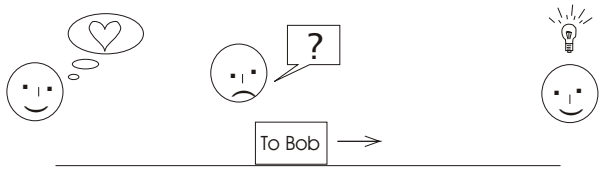
1.1 Γενικά

Έφταιξε άραγε η Εύα που έφαγε το μήλο, ή μήπως η Πανδώρα που άνοιξε το περίφημο κουτί της; Κατά πάσα πιθανότητα μια δαρβινική προσέγγιση του ζητήματος θα ήταν πιο αποδοτική, αλλά δεν είναι το ποιος και το γιατί που μας αφορά εδώ. Αυτό που μας αφορά είναι το αποτέλεσμα, και το αποτέλεσμα είναι ότι από νωρίς (ή εξαρχής) η ειρηνική και ευτυχισμένη συνύπαρξη των ανθρώπων κάθε άλλο παρά δεδομένη ήταν. Ως εκ τούτου, από νωρίς φάνηκε ότι υπήρχαν σοβαροί λόγοι να μένουν κάποιες πληροφορίες καλά κριμένες από αδιάκριτα βλέμματα, και κάπου εκεί άρχισε να εμφανίζεται δειλά η έννοια της κρυπτογραφίας.

Σχηματικά, η κατάσταση έχει ως εξής: ένας πομπός Α, που θα τον αποκαλούμε Αλίκη, επιθυμεί να στείλει ένα μήνυμα p σε ένα δέκτη Β, που εδώ θα αποκαλούμε Βασίλη. Για το σκοπό αυτόν χρησιμοποιεί κάποιο μέσο, κάποιο κανάλι. Κατά τη διάρκεια της μεταφοράς του, το p είναι εκτεθειμένο στα μάτια κάποιου εχθρού Ο, ο οποίος ενδεχομένως επιθυμεί να μάθει το περιεχόμενο του, να το αλλοιώσει κ.τ.λ. και από τον οποίο η Αλίκη και ο Βασίλης θέλουν να κρατήσουν το περιεχόμενο του p κρυφό, αναλλοίωτο κ.τ.λ. Μια πολύ καλή εισαγωγή στην κρυπτογραφία μπορεί να βρει κανείς στο [21].

1.2 Κρυπτογράφηση

Ο βασικότερος κλάδος της κρυπτογραφίας καλείται να λύσει το εξής πρόβλημα: Πως μπορεί να στείλει η Αλίκη το p μέσω του καναλιού έτσι ώστε ο εχθρός να μην μπορεί να αποκαλύψει το περιεχόμενό του, αλλά όταν αυτό φτάσει στο Βασίλη, ο τελευταίος να μπορεί σχετικά εύκολα να το κατανοήσει.



Σχήμα 2: Η κρυπτογραφία με μια ματιά.

Ας δούμε συνοπτικά πως λύνεται το πρόβλημα, εισάγοντας παράλληλα και τους κατάλληλους ορισμούς. Αρχικά, η Αλίκη και ο Βασίλης επιλέγουν ένα

αλφάβητο A_1 με το οποίο μπορούν να γράφουν και να διαβάζουν τα μηνύματα. Κατόπιν επιλέγουν ένα αλφάβητο A_2 με βάση το οποίο θα μεταφέρεται το μήνυμα στο κανάλι. Τα A_1 και A_2 μπορεί να διαφέρουν. Κατόπιν η Αλίκη σχηματίζει το προς αποστολή κείμενο, μια ακολουθία από στοιχεία του A_1, το οποίο ονομάζουμε **αρχικό κείμενο** ή απλά **κείμενο**. Το σύνολο των κειμένων που μπορεί να σχηματιστούν ονομάζεται **χώρος μηνυμάτων** και συμβολίζεται με M. Αφού αποφασίσει το κείμενό της, το μετασχηματίζει και το στέλνει στο κανάλι. Το μετασχηματισμένο κείμενο αποτελείται από γράμματα του A_2 και ονομάζεται **κρυπτοκείμενο**. Το σύνολο των κρυπτοκειμένων που μπορεί να σχηματιστούν ονομάζεται **χώρος κρυπτοκειμένων** και συμβολίζεται με C. Ο μετασχηματισμός του κειμένου σε κρυπτοκείμενο γίνεται με την επιλογή και χρήση μιας κατάλληλης συνάρτησης E_e: $M \to C$ που εξαρτάται από το e και είναι 1-1. Η E_e λέγεται *συνάρτηση κρυπτογράφησης* και η διαδικασία που ακολουθεί η Αλίκη *κρυπτογράφηση*.

Τώρα, μέσω του καναλιού το κρυπτοκείμενο $E_e(p)$ φτάνει στο Βασίλη. Αυτός με τη σειρά του επιλέγει μια κατάλληλη συνάρτηση $D_d : C \to M$ που εξαρτάται από το d και είναι επίσης 1-1, και με τη βοήθειά της ανακτά το p. Η D_d λέγεται *συνάρτηση αποκρυπτογράφησης* και η διαδικασία που ακολουθεί ο Βασίλης *αποκρυπτογράφηση*. Τα e και d που καθορίζουν τις συναρτήσεις λέγονται κλειδιά και το σύνολο των πιθανών κλειδιών λέγεται *χώρος κλειδιών* και συμβολίζεται με K. Προφανώς, οι E_e και D_d που χρησιμοποιούνται κατά την κρυπτογράφηση και την αντίστοιχη αποκρυπτογράφηση δεν είναι τυχαίες, αλλά σχετίζονται μεταξύ τους από την απλή σχέση $D_d(E_e(m)) = m, \forall m \in M$.

Για την κατασκευή ενός κρυπτοσυστήματος απαιτείται η επιλογή ενός χώρου κειμένων, ενός χώρου κρυπτοκειμένων, ενός χώρου κλειδιών, ενός συνόλου συναρτήσεων κρυπτογράφησης $\{E_e : e \in K\}$ και ενός συνόλου συναρτήσεων αποκρυπτογράφησης $\{D_d : d \in K\}$ όπου τα τελευταία δυο έχουν την ιδιότητα ότι για κάθε $e \in K$ υπάρχει μοναδικό $d \in K$, τέτοιο ώστε $D_d(E_e(m)) = m$, για κάθε κείμενο m.

Φυσικά, στην καθημερινή ζωή, τα κρυπτοσυστήματα έχουν συγκεκριμένη μορφή και οι τριάδες Αλίκη, Βασίλης, Εχθρός ποικίλουν, όπως και τα μηνύματα, τα κανάλια αλλά και ο σκοπός της κρυπτογράφησης. Για παράδειγμα, η Αλίκη μπορεί να είναι ο πρόεδρος Μπους, ο Βασίλης ο αρχηγός των επιχειρήσεων στο Ιράκ, ο Εχθρός οι μυστικές υπηρεσίες του Σαντάμ, το κανάλι κάποιος δορυφόρος και το μήνυμα οδηγίες για το βομβαρδισμό κάποιου στόχου στρατηγικής (;) σημασίας. Σε μια πιο ειρηνική εκδοχή, η διαδικασία είναι μια συναλλαγή στο διαδίκτυο και ο Εχθρός κάποιος χάκερ.

Μια από τις πιο παλιές γνωστές περιπτώσεις χρήσης της κρυπτογραφίας είναι αυτή του Ιούλιου Καίσαρα. Ο ρωμαίος αυτοκράτορας, χρησιμοποιούσε σαν E_e τον κανόνα 'αντικατέστησε κάθε γράμμα με το γράμμα που θα βρεις τρεις θέσεις μετά στο αλφάβητο' (προφανώς τα τρία τελευταία πάνε στα τρία

αρχικά). Έτσι, για παράδειγμα, το κείμενο ‘attack¨, αποτελούμενο από έξι μηνύματα, μετασχηματιζόταν στο κρυπτοκείμενο ‘dwwdfn¨.

Αρχικό κείμενο	a	b	c	d	e	f	g	h	i	j	k
Κρυπτοκείμενο	d	e	f	g	h	i	j	k	l	m	n

l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Πίνακας 1: Ο κανόνας κρυπτογράφησης του καίσαρα

Οι στρατηγοί του έπαιρναν το κρυπτοκείμενο και σαν D_d εφάρμοζαν τον κανόνα ‘κάθε γράμμα που βρίσκεις μετέτρεπέ το σε αυτό που βρίσκεται τρεις θέσεις πριν στο αλφάβητο’. Εύκολα βλέπουμε ότι με τον τρόπο αυτό ανακτούσαν το αρχικό μήνυμα.

Κρυπτοκείμενο	a	b	c	d	e	f	g	h	i	j	k
Αρχικό κείμενο	x	y	z	a	b	c	d	e	f	g	h

l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Πίνακας 2: Ο κανόνας αποκρυπτογράφησης του καίσαρα

Κάνοντας μια παρένθεση εδώ, να πούμε ότι δεν είναι τυχαίο που ένα από τα χρονολογικά πρώτα παραδείγματα κρυπτοσυστήματος αφορά στρατιωτική χρήση της κρυπτογραφίας. Στην πραγματικότητα η μεγάλη πλειονότητα των κρυπτογραφικών εφαρμογών, μέχρι και πριν από λίγες δεκαετίες, αφορούσαν τη διαφύλαξη κρατικών και στρατιωτικών μυστικών. Οι ειδήμονες του κλάδου ήταν στρατιωτικοί, διπλωμάτες και γενικότερα άνθρωποι της κυβέρνησης.

Ο κανόνας του Καίσαρα είναι εφαρμογή του κρυπτοσυστήματος που βασίζεται στον κανόνα ‘αντικατέστησε κάθε γράμμα που συναντάς με το κατά k θέσεις δεξιότερο του στο αλφάβητο’. Τα κλειδιά είναι τα διάφορα k (26 για το λατινικό αλφάβητο) και οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης είναι οι αντίστοιχες μεταθέσεις των γραμμάτων. Όπως βλέπουμε, στο κρυπτοσύστημα αυτό τα κλειδιά της Αλίκης και του Βασίλη είναι ίδια. Ανήκει στα **συμμετρικά κρυπτοσυστήματα**, μια από τις δυο βασικές κατηγορίες κρυπτοσυστημάτων. Χαρακτηριστική τους ιδιότητα είναι ότι η γνώση ενός εκ των e, d επιτρέπει τον ‘εύκολο’ υπολογισμό του άλλου. Σήμερα, τα συμμετρικά κρυπτοσυστήματα δεν θεωρούνται ασφαλή. Αντίθετα, η έρευνα στρέφεται κυρίως προς την άλλη βασική κατηγορία, τα κρυπτοσυστήματα δημοσίου κλειδιού.

1.2.1 Κρυπτοσυστήματα Δημοσίου Κλειδιού

Πριν προχωρήσουμε, θα δώσουμε δυο χρήσιμους ορισμούς:

Ορισμός 1.1 *Μια συνάρτηση f από ένα σύνολο X σε ένα σύνολο Y λέγεται* ***μονόδρομη συνάρτηση*** *(one-way function) αν το $f(x)$ είναι 'εύκολο' να υπολογιστεί για όλα τα $x \in X$ αλλά για 'σχεδόν όλα' τα στοιχεία $y \in Im(f)$ είναι 'υπολογιστικά ακατόρθωτο' να βρεθεί κάποιο x τέτοιο ώστε $f(x) = y$. Μια* ***trapdoor μονόδρομη συνάρτηση*** *είναι μια μονόδρομη συνάρτηση με την επιπλέον ιδιότητα ότι αν δοθεί κάποια επιπλέον πληροφορία (η λεγόμενη 'trapdoor πληροφορία') γίνεται εφικτό, για οποιοδήποτε $y \in Im(f)$, να βρούμε ένα $x \in X$ τέτοιο ώστε $f(x) = y$.*

Ορισμός 1.2 *Μια* ***hash συνάρτηση*** *είναι μια εύκολα υπολογίσιμη συνάρτηση, που απεικονίζει δυαδικές ακολουθίες τυχαίου μήκους σε δυαδικές ακολουθίες κάποιου προκαθορισμένου μήκους k, οι οποίες ονομάζονται hash-τιμές. Επειδή συνήθως τα αρχικά μηνύματα δεν είναι γραμμένα στο δυαδικό, αλλά μετατρέπονται σε αυτό με κάποια άλλη συνάρτηση, συχνά θεωρούμε τη hash συνάρτηση κατευθείαν από το χώρο των μηνυμάτων στο $\{0,1\}^k$.*

Οι πιο κοινές εφαρμογές των hash συναρτήσεων είναι στις ψηφιακές υπογραφές, όπου βοηθούν στην εξοικονόμηση χώρου, και στην εξασφάλιση της ακεραιότητας δεδομένων. Βασική προϋπόθεση για τη καταλληλότητά τους είναι η μηδενική πιθανότητα να βρεθούν δυο μηνύματα με την ίδια hash τιμή.

Έστω $\{E_e : e \in K\}$ το σύνολο των συναρτήσεων κρυπτογράφησης και έστω $\{D_d : d \in K\}$ το σύνολο των συναρτήσεων αποκρυπτογράφησης ενός κρυπτοσυστήματος, όπου K είναι ο χώρος κλειδιών. Θεωρούμε όλα τα ζευγάρια αντίστοιχων συναρτήσεων (E_e, D_d). Το κρυπτοσύστημα θα λέγεται **κρυπτοσύστημα δημοσίου κλειδιού**, αν έχει την ιδιότητα ότι, για κάθε τέτοιο ζευγάρι, παρά την ενδεχόμενη γνώση της E_e, είναι υπολογιστικά ακατόρθωτο, αν μας δοθεί ένα κρυπτοκείμενο c, να βρούμε ένα κείμενο m τέτοιο ώστε $E_e(m) = c$. Όπως θα έχετε ίσως ήδη παρατηρήσει, η ιδιότητα αυτή που χαρακτηρίζει τα κρυπτοσυστήματα δημοσίου κλειδιού είναι ακριβώς η αντίθετη από την αντίστοιχη για τα συμμετρικά κρυπτοσυστήματα. Επίσης, αυτό που στην ουσία συμβαίνει είναι ότι η E_e είναι μια trapdoor μονόδρομη συνάρτηση, για την οποία η trapdoor πληροφορία, που επιτρέπει την αποκρυπτογράφηση, είναι το d.

Ένας καλός τρόπος να τα περιγράψουμε διαισθητικά είναι ο εξής: φανταστείτε ότι ο Βασίλης έστειλε στην Αλίκη πολλά ανοιχτά λουκέτα, χωρίς τα κλειδιά τους, που τα κρατά ο ίδιος. Όποτε η Αλίκη θέλει να του στείλει κάτι, το βάζει σε ένα μπαούλο, το κλειδώνει με ένα από τα λουκέτα και του το στέλνει. Ο Βασίλης το παίρνει και το ξεκλειδώνει με τα κλειδιά του. (Στην αντίστοιχη

περιγραφή για τα συμμετρικά κρυπτοσυστήματα, έχουν μόνο ένα λουκέτο, αλλά αυτός που το αγόρασε πρέπει να βρει ένα ασφαλή τρόπο να στείλει αντικλείδι στον άλλο. Επιπλέον, αυτό θα γίνεται κάθε φορά που για κάποιο λόγο θέλουν να αλλάξουν λουκέτο.)

Τα κρυπτοσυστήματα δημοσίου κλειδιού δεν προϋποθέτουν την ύπαρξη ασφαλούς καναλιού. Αυτό από τη μια διευρύνει το πεδίο χρήσεων τους. Από την άλλη όμως εισάγει μια επιπλέον δυσκολία, διότι στην πράξη σημαίνει ότι τα απαραίτητα, για το εκάστοτε κρυπτοσύστημα, κλειδιά πρέπει να φτάσουν στα χέρια της Αλίκης και του Βασίλη μέσω του ανασφαλούς καναλιού, χωρίς όμως να πέσουν στα χέρια του Εχθρού. Αυτό απαιτεί μια ξεχωριστή διαδικασία, η οποία ονομάζεται **καθορισμός κλειδιού** (key establishment). Έχουν γίνει αρκετές προσεγγίσεις για την επίλυση του προβλήματος, οι οποίες χωρίζονται σε δύο βασικές κατηγορίες: α) **Διανομή κλειδιού** (key distribution), όπου ανήκουν οι μηχανισμοί στους οποίους η μια πλευρά αποφασίζει ένα κλειδί και το στέλνει στις υπόλοιπες πλευρές και β) **Συμφωνία κλειδιού** (key agreement), όπου οι δυο πλευρές μαζί καθορίζουν ένα κλειδί. Το ποιο είδος διαδικασίας θα ακολουθηθεί εξαρτάται κάθε φορά από το κρυπτοσύστημα.

Την ιδέα της κρυπτογραφίας δημοσίου κλειδιού εισήγαγαν οι Diffie και Hellman σε ένα άρθρο τους, το 1976. Η ιδέα υπήρξε επαναστατική και αποτελεί το πιο σημαντικό σημείο στην ιστορία της κρυπτογραφίας. Προκάλεσε μεγάλο ενδιαφέρον, και σύντομα απέδωσε καρπούς. Το 1978, οι Rivest, Shamir και Adleman ανακάλυψαν το πρώτο πρακτικό κρυπτοσύστημα δημοσίου κλειδιού, το οποίο, από τα αρχικά τους, πήρε το όνομα RSA. Όπως έγινε γνωστό το Δεκέμβριο του 1997, μετά το θάνατο του James Ellis, από το άρθρο του 'The Story of Non-Secret Encryption", κάποιοι κρυπτογράφοι στη μεγάλη Βρετανία είχαν γνώση αυτών των τεχνικών κρυπτογράφησης από τις αρχές της δεκαετίας του 1970.

1.2.2 Το RSA

Η ασφάλεια του RSA βασίζεται στη δυσκολία του λεγόμενου **RSA προβλήματος**: 'Δοθέντος ενός θετικού ακεραίου n που είναι γινόμενο δυο διαφορετικών περιττών πρώτων p και q, ενός θετικού ακεραίου e τέτοιου ώστε $(e,(p-1)(q-1))=1$, και ενός ακεραίου c, να βρεθεί ένας ακέραιος m τέτοιος ώστε $me = c(modn)$.' Πιστεύεται ότι το RSA πρόβλημα είναι υπολογιστικά ισοδύναμο με το πρόβλημα της παραγοντοποίησης ακεραίων.

Το RSA λειτουργεί ως εξής: Η Αλίκη επιλέγει δυο πολύ μεγάλους πρώτους p και q και υπολογίζει το γινόμενο τους $n = pq$. Κρατά τους πρώτους κρυφούς και δημοσιεύει το n. Κατόπιν επιλέγει ένα e σχετικά πρώτο με το $(p-1)(q-1)$ και τον δημοσιεύει μαζί με το n. Τώρα, όταν ο Βασίλης θελήσει να της στείλει

ένα κείμενο m, απλά υπολογίζει το $me\,(mod\,n)$ και στέλνει την τιμή που βρίσκει στην Αλίκη. Αυτή χρησιμοποιεί σαν κλειδί d έναν ακέραιο με την ιδιότητα $de = 1\,(mod\,p-1)$ και $de = 1\,(mod\,q-1)$. Υπολογίζοντας το $cd\,(mod\,n)$, ανακτά το αρχικό μήνυμα m.

Αποτέλεσε για χρόνια, και αποτελεί ακόμα ίσως, το πιο ασφαλές διαδεδομένο κρυπτοσύστημα δημοσίου κλειδιού, και οι δημιουργοί του έχουν ιδρύσει εταιρία με την επωνυμία RSA Laboratories. Φαίνεται όμως ότι όσο επιτυχημένο και αν έχει αποδειχτεί μέχρι τώρα το RSA, η κρυπτογραφία δεν θα σταματήσει σε αυτό.

Ένα μειονέκτημα του RSA είναι ότι σε περιβάλλοντα με περιορισμένη μνήμη και υπολογιστική ισχύ, είναι πολύ αργό. Επίσης, από το 1978 μέχρι σήμερα, έχει γίνει αρκετή πρόοδος στην παραγοντοποίηση, με αποτέλεσμα να πρέπει να βρίσκονται όλο και μεγαλύτεροι πρώτοι, ώστε να εξασφαλίζεται η ασφάλεια του RSA (ποιος να το περίμενε ότι θα θεωρούνταν κάποτε πολύτιμοι οι μεγάλοι πρώτοι...). Έτσι όλο και μεγαλύτερο μέρος όσων ασχολούνται με την κρυπτογραφία, στρέφει την προσοχή του στην εύρεση εναλλακτικών λύσεων, που, κατά προτίμηση, να μην βασίζονται στη θεωρία αριθμών. Μια πρώτη προσπάθεια έγινε με τη χρήση NP-hard προβλημάτων, όπως το Merkle-Hellman Knapsack. Αυτού του είδους τα κρυπτοσυστήματα γρήγορα έσπασαν, και μέχρι σήμερα δεν έχει δοθεί αξιόπιστη λύση από αυτή την κατεύθυνση. Μια άλλη προσπάθεια γίνεται με την κβαντική κρυπτογραφία και την lattice κρυπτογραφία.

Στα μαθηματικά γίνονται προσπάθειες προς την κατεύθυνση των ελλειπτικών καμπυλών και της χρήσης δύσκολων προβλημάτων από τη συνδυαστική θεωρία ομάδων. Σε αυτή την κατηγορία προβλημάτων βασίζονται και τα κρυπτοσυστήματα που χρησιμοποιούν ομάδες πλεξίδων.

1.3 Ψηφιακές υπογραφές

Στην πράξη, συμβαίνει, κάποιες φορές, τα σχέδια του Εχθρού να μπορούν να εξυπηρετηθούν χωρίς αυτός να είναι αναγκασμένος να 'σπάσει' το κρυπτοσύστημα. Για παράδειγμα, μια άλλου είδους επίθεση, είναι να στείλει στο Βασίλη κάποιο μήνυμα, ισχυριζόμενος ότι είναι η Αλίκη, πετυχαίνοντας έτσι κάποια οφέλη. Ακολουθεί η λύση που προσφέρει η ψηφιακή υπογραφή στη γενική της μορφή.

Οι δυο πλευρές ορίζουν δυο σύνολα και δυο συναρτήσεις: Το M, που είναι το σύνολο των μηνυμάτων που μπορούν να υπογραφούν. Το S , τα στοιχεία του οποίου ονομάζουμε υπογραφές, και τα οποία συνήθως είναι δυαδικές ακολουθίες καθορισμένου μήκους. Το μετασχηματισμό S_A από το M στο S που καλείται μετασχηματισμός υπογραφής της Αλίκης και τον οποίο η Αλίκη κρατά κρυφό. Το μετασχηματισμό V_A από το $M \times S$ στο Αλήθεια, Ψέμα,

που ονομάζεται μετασχηματισμός πιστοποίησης για τις υπογραφές της Αλίκης, κοινοποιείται και τον χρησιμοποιούν οι άλλοι για να πιστοποιήσουν τις υπογραφές που βάζει η Αλίκη. Κάθε ζεύγος S_A και V_A δίνει ένα σχήμα ψηφιακής υπογραφής της Αλίκης.

Τώρα, από τη στιγμή που θα ορίσουν τα παραπάνω, ακολουθούν τα εξής βήματα: η Αλίκη, που θέλει να στείλει το μήνυμα m, υπολογίζει το $s = S_A(m)$, που λέγεται υπογραφή του μηνύματος m, και στέλνει στο Βασίλη το ζεύγος (m, s). Από τη μεριά του, ο Βασίλης έχει στα χέρια του τη V_A, λαμβάνει το (m, s) και θέλει να επιβεβαιώσει ότι το έστειλε η Αλίκη. Αρκεί να υπολογίσει το $V_A(m, s)$ και να δεχτεί την αυθεντικότητα της υπογραφής, αν $V_A(m, s) =$ Αλήθεια, ή να την απορρίψει αν $V_A(m, s) =$ Ψέμα.

Όπως και στα κρυπτοσυστήματα, έτσι και εδώ συνήθως οι S_A και V_A ανήκουν σε οικογένειες συναρτήσεων και κάθε μια τους προσδιορίζεται από ένα κλειδί. Επίσης θα πρέπει και σε αυτή την περίπτωση να ικανοποιούν κάποιες προφανείς προϋποθέσεις: α) το s να είναι γνήσια υπογραφή του κειμένου m αν και μόνο αν $V_A(m, s) =$ Αλήθεια, και β) να είναι υπολογιστικά ακατόρθωτο για κάποιον άλλο, πέραν της Αλίκης, να βρει για κάποιο μήνυμα m ένα s τέτοιο ώστε $V_A(m, s) =$ Αλήθεια.

1.4 Πρωτόκολλα Ταυτοποίησης

Οι ψηφιακές υπογραφές, που είδαμε στην προηγούμενη παράγραφο, αποτελούν τη λύση σε μια ειδική (ίσως την πιο σημαντική) περίπτωση του προβλήματος ταυτοποίησης ενός προσώπου. Το πρόβλημα αυτό εμφανίζεται συχνά στην καθημερινή ζωή. Για παράδειγμα, όταν θέλουμε να κάνουμε ανάληψη χρημάτων από κάποιο τραπεζικό μηχάνημα (ATM) ή όταν θέλουμε να κάνουμε login σε κάποιο μηχάνημα, από απόσταση. Τα πρωτόκολλα ταυτοποίησης καλούνται να λύσουν αυτό το πρόβλημα.

Βασικό ζητούμενο από ένα πρωτόκολλο ταυτοποίησης είναι, όταν ο Εχθρός παρακολουθεί την Αλίκη να πιστοποιεί την ταυτότητά της στο Βασίλη, να μην μπορεί στη συνέχεια να πείσει το Βασίλη ότι είναι η Αλίκη. Επίσης, καλό θα ήταν ούτε ο Βασίλης να μην μπορεί να παρουσιαστεί ως Αλίκη.

Οι συνθήκες επικοινωνίας μπορεί να διαφέρουν από περίπτωση σε περίπτωση. Για παράδειγμα, άλλοτε μπορεί να γίνεται η επικοινωνία σε πραγματικό χρόνο και άλλοτε όχι, άλλοτε μπορεί να επιτρέπεται η μυστικότητα στο κανάλι και άλλοτε όχι, ή ακόμα μπορεί η επικοινωνία να μην είναι αμφίδρομη, αλλά μονόδρομη. Ως εκ τούτου, συμβαίνει τα πρωτόκολλα ταυτοποίησης να εμφανίζουν διαφοροποιήσεις ως προς τη μορφή, ανάλογα με το σκοπό που εξυπηρετούν.

2 Πλεξίδες

2.1 Γενικά

Όταν, στη δεκαετία του 1920, μια εταιρία υφαντουργίας (!) παράγγελνε στον γερμανό αλγεβρίστα E. Artin να επινοήσει την θεωρία των πλεξίδων (σύμφωνα με το [16]), κανείς ίσως δεν περίμενε την εξέλιξη που ακολούθησαν. Δεν είναι γνωστό το κατά πόσο βοήθησαν την υφαντουργία, βρήκαν όμως εφαρμογές σε περιοχές όπως η μιγαδική ανάλυση, η τοπολογία και, κυρίως, η θεωρία κόμβων (μάλιστα η μελέτη των κόμβων ήταν που οδήγησε τον Artin στις πλεξίδες). Έξω από το χώρο των μαθηματικών, οι πλεξίδες έδωσαν ένα ευρύ φάσμα ενδιαφερόντων ιδεών και εφαρμογών, από τη κβαντική φυσική, τη χημεία, τη μελέτη του DNA, μέχρι σε ταχυδακτυλουργικά κόλπα και σε Μεξικάνικες ζώνες! Να σημειώσουμε εδώ, ότι η έννοια της πλεξίδας απασχόλησε πρώτο τον, συνήθη ύποπτο, Gauss, όταν μελετούσε την τροχιά του πρώτου αστεροειδούς που παρατηρήθηκε, του Ceres.

Αν μη τι άλλο, πιστεύεται ότι οι εφαρμογές τους δεν έχουν εξαντληθεί, και εξακολουθεί να εκδηλώνεται ενδιαφέρον για τις πλεξίδες. Χαρακτηριστικό είναι ότι (σύμφωνα με το [18]) από το 1947 ως το 2002 γύρω στις 400 εργασίες δημοσιεύθηκαν για τις ιδιότητες και τις χρήσεις τους. Μόλις τα τελευταία λίγα χρόνια εκδηλώθηκε έντονο ενδιαφέρον από τους κρυπτογράφους, με την ελπίδα ότι θα βρουν και κρυπτογραφικές εφαρμογές, ειδικότερα σε συσκευές με μικρή χωρητικότητα μνήμης, όπως τα κινητά τηλέφωνα, η οποία καθιστά τις σύγχρονες κρυπτογραφικές τεχνικές δύσχρηστες.

2.2 Περιγραφή

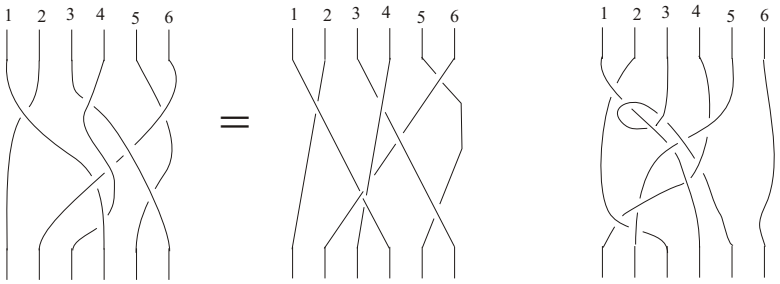
Τί είναι όμως οι πλεξίδες; Έχουν κάποια σχέση με την άλλοτε δημοφιλή γυναικεία πλεξίδα; Η απάντηση είναι ότι η παραδοσιακή αυτή κόμμωση είναι μια ειδική περίπτωση πλεξίδας. Ας προσπαθήσουμε όμως να περιγράψουμε τα γεωμετρικά αντικείμενα που θα μας απασχολήσουν στο εξής.

Φανταστείτε δυο ράβδους, οριζόντιες, παράλληλες μεταξύ τους, με το επίπεδο που ορίζουν να είναι κάθετο στο έδαφος. Σε κάθε μια τους υπάρχουν τοποθετημένοι n γάντζοι-σημεία, τα $\mathrm{A}_1, ..., A_n$ στην πάνω και τα Γ_1, ..., Γ_n στην κάτω, έτσι ώστε

$$\mid A_{i+1} - A_i \mid = c = \mid \Gamma_{i+1} - \Gamma_i \mid$$

$\forall i$ με $0 \leq i \leq n-1$, και έτσι ώστε το A_i να βρίσκεται ακριβώς πάνω από το Γ_i. Φανταστείτε τώρα n κλωστές, με το ένα άκρο τους δεμένο σε κάποιον από τους A_i και το άλλο σε κάποιον από τους Γ_i. Διαισθητικά μιλώντας, δεν θέλουμε οι κλωστές να μπλέκονται με τον εαυτό τους, ούτε να δημιουργούν 'κόμπους' ή άλλες παρόμοιες καταστάσεις. Πιο αυστηρά, μπορούμε να πούμε

('χάνονταs' κάποιες πιθανές μορφές μιας πλεξίδας) ότι απαιτούμε τα παρακάτω χαρακτηριστικά: α) κάθε ένας από τους A_i και Γ_i έχει δεμένη ακριβώς μια κλωστή και β) κάθε επίπεδο κάθετο στο επίπεδο των ράβδων, παράλληλο σε αυτές και διερχόμενο ανάμεσα τους, τέμνει κάθε κλωστή σε ακριβώς ένα σημείο. Ένας τέτοιος σχηματισμός θα λέγεται **πλεξίδα σε n κλωστές** ή αλλιώς **n-πλεξίδα**. Δυο πλεξίδες που μπορούν να προκύψουν η μια από την άλλη με απλή μετακίνηση ή αυξομείωση του μήκους των κλωστών, δηλαδή χωρίς να λυθεί ή να κοπεί καμία από αυτές, θα τις θεωρούμε ίδιες και δεν θα κάνουμε καμιά διάκριση μεταξύ τους (βλ. σχήμα 3).

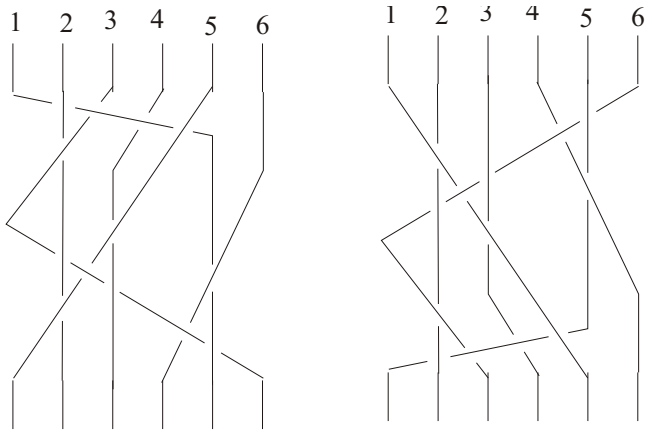


Σχήμα 3: Τα δυο πρώτα σχέδια απεικονίζουν δυο 6-πλεξίδες, ίδιες μεταξύ τους, ενώ στο τρίτο σχέδιο το αντικείμενο δεν είναι πλεξίδα.

Ορισμός 2.1 *Έστω μια n-πλεξίδα A. Θα λέμε ότι δυο κλωστές* ***διασταυρώνονται θετικά*** *στην A , αν αυτή που έρχεται από δεξιά περνά πάνω από αυτήν που έρχεται από αριστερά.*

Η πρώτη καλή ιδιότητα των πλεξίδων είναι ότι μπορούμε να ορίσουμε κατά φυσικό και διαισθητικά αποδεκτό τρόπο μια πράξη πολλαπλασιασμού ανάμεσα σε δυο πλεξίδες με ίδιο αριθμό κλωστών: απλά τοποθετούμε την πρώτη πάνω από τη δεύτερη, ξεγαντζώνουμε και ενώνουμε τα αντικείμενα ελεύθερα άκρα (βλ. σχήμα 5). Προφανώς αυτό που προκύπτει είναι επίσης μια πλεξίδα σε n κλωστές. Εύκολα βλέπουμε επίσης ότι η πράξη αυτή δεν είναι αντιμεταθετική (αν και στο σχήμα 5 φαίνεται να είναι, λόγο του ότι οι πλεξίδες είναι αντίστροφες).

Δεύτερη καλή ιδιότητα των πλεξίδων είναι ότι για κάθε n, το σύνολο των πλεξίδων σε n κλωστές αποτελεί ομάδα με πράξη τον πολλαπλασιασμό που μόλις ορίσαμε. Πράγματι υπάρχει η μοναδιαία πλεξίδα e_n, που αποτελείται από n παράλληλες κατακόρυφες κλωστές. Επιπλέον για κάθε πλεξίδα μπορούμε να σχηματίσουμε την αντίστροφή της, ανακλώντας την αρχική ως προς την κάτω ράβδο (βλ. σχήμα 4). Τέλος, η πράξη είναι κλειστή και προσεταιριστική. Η επιβεβαίωση όσων από τα παραπάνω χρειάζεται, γίνεται εύκολα γεωμετρικά. Θα συμβολίζουμε την ομάδα των πλεξίδων σε n κλωστές με B_n.



Σχήμα 4: Δυο αντίστροφες. Η δεύτερη προκύπτει από την πρώτη με ανάκλαση ως προς την κάτω ράβδο.

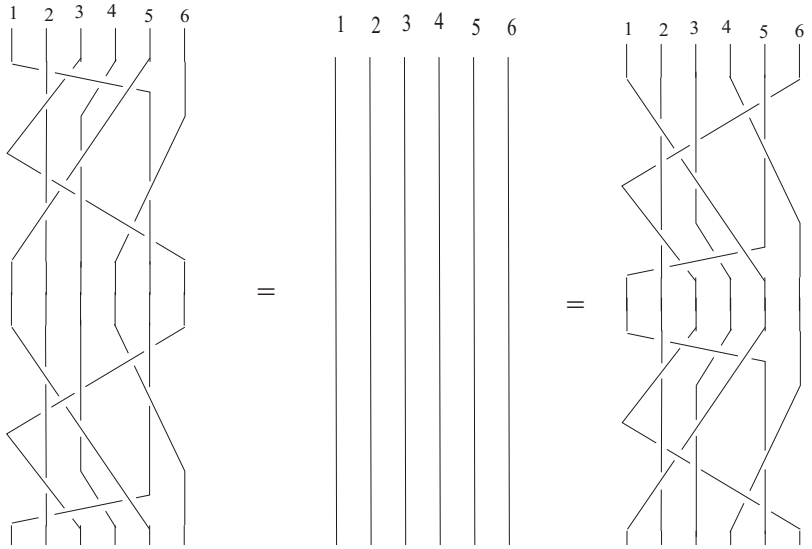
2.3 Αλγεβρική αναπαράσταση

Προχωρούμε τώρα στα μαθηματικά των ομάδων πλεξίδων, και πριν απ'ολα θα μας απασχολήσει η αλγεβρική αναπαράσταση τους. Έστω $n \in N$. Ορίζουμε $n-1$ n-πλεξίδες, τις $s_1, s_2, ..., s_{n-1}$, τις οποίες θα ονομάζουμε **στοιχειώδεις n-πλεξίδες**, ως εξής: η s_i είναι η n-πλεξίδα πανομοιότυπη με την ταυτοτική, με μοναδική διαφορά ότι η κλωστή που ξεκινά από το A_i καταλήγει στο Γ_{i+1}, ενώ αυτή που ξεκινά από το A_{i+1} καταλήγει στο Γ_i, και διασταυρώνονται θετικά.

Ο Artin έδειξε [26] ότι κάθε n-πλεξίδα μπορεί να αναπαρασταθεί ως σύνθεση στοιχειωδών n-πλεξίδων και των αντίστροφων τους. Για παράδειγμα, στο σχήμα 4 απεικονίζεται η 6-πλεξίδα $s_1 s_2^{-1} s_3^{-1} s_4 s_1 s_3 s_1 s_2^{-1} s_3 s_5 s_1 s_4^{-1} s_5$ και η αντίστροφή της. Οι γεωμετρικοί συλλογισμοί μας οδηγούν στις παρακάτω ταυτότητες:

1. Τετριμμένες σχέσεις:
$$s_i s_i^{-1} = s_i^{-1} s_i = 1$$
και
$$s_i \cdot 1 = 1 \cdot s_i = s_i, \quad (i = 1, 2, 3, .., n-1)$$

2. Ασθενής αντιμεταθετικότητα:
$$s_i s_j = s_j s_i$$
όταν
$$|i - j| \geq 2, \quad (i = 1, 2, 3, .., n-1) \quad (1)$$



Σχήμα 5: Οι δυο αντίστροφες πλεξίδες του σχήματος 4, πολλαπλασιασμένες με τους δυο δυνατούς τρόπους. Και τα δυο γινόμενα είναι ίδια με την ταυτοτική.

3. Σχέσεις πλεξίδων:

$$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, \quad (i = 1, 2, 3, .., n-2) \quad (2)$$

Την 3 μπορούμε να τη δούμε διαισθητικά ως εξής: οι τρεις κλωστές που εμπλέκονται στο σχηματισμό των πλεξίδων, κινούνται σε ΄διαφορετικά΄ επίπεδα, οπότε μπορούν να μετατοπίζονται εύκολα οι διασταυρώσεις.

Οι σχέσεις αυτές αποδεικνύονται γεωμετρικά και μπορούμε να τις χρησιμοποιήσουμε για την αλγεβρική απόδειξη άλλων σχέσεων. Ακολουθούν μερικά παραδείγματα:

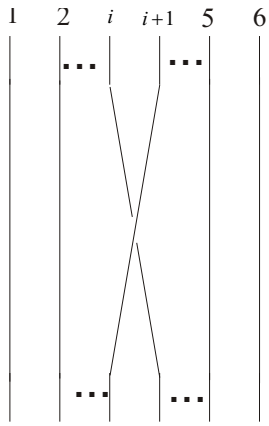
Παράδειγμα 2.1

1. $s_i s_j^{-1} = s_j^{-1} s_i$, *όταν* $|i-j| \geq 2$

   Απόδειξη: $s_i s_j^{-1} = s_j^{-1} s_i \Leftrightarrow s_i s_j^{-1} s_j = s_j^{-1} s_i s_j \Leftrightarrow s_i = s_j^{-1} s_j s_i$ *που ισχύει.*

2. $s_i^{-1} s_j = s_j s_i^{-1}$, $|i-j| \geq 2$

   Απόδειξη: $s_i^{-1} s_j \overset{1.}{=} (s_j^{-1} s_i)^{-1} = (s_i sj^{-1})^{-1} = s_j s_i^{-1}$



Σχήμα 6: Η s_i στην $B6$.

3. $s_i^{-1}s_j^{-1} = s_j^{-1}s_i^{-1},\ |i-j| \geq 2$
   Απόδειξη: $s_i^{-1}s_j^{-1} = (s_j s_i)^{-1} = (s_i s_j)^{-1} = s_j^{-1}s_i^{-1}$

4. $s_i^{-1}s_{i+1}^{-1}s_i^{-1} = s_{i+1}^{-1}s_i^{-1}s_{i+1}^{-1}$
   Απόδειξη: $s_i^{-1}s_{i+1}^{-1}s_i^{-1} = (s_i s_{i+1} s_i)^{-1} = (s_{i+1} s_i s_{i+1})^{-1} = s_{i+1}^{-1}s_i^{-1}s_{i+1}^{-1}$

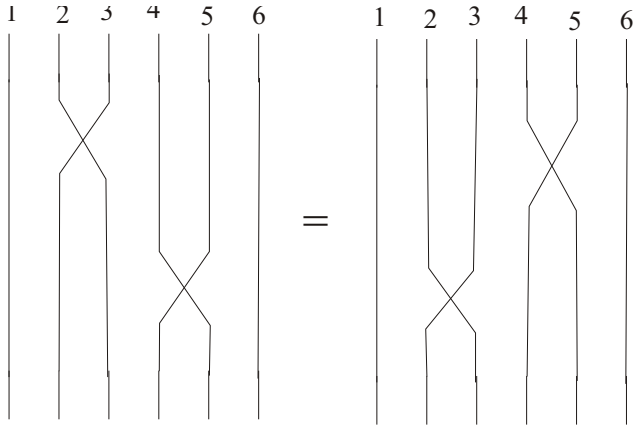
5. $s_1 s_2 s_1 s_2^{-1}s_1^{-1} = s_3 s_1 s_3^{-1}s_1^{-1}s_2$
   Απόδειξη: $s_1 s_2 s_1 s_2^{-1}s_1^{-1} = s_2 s_1 s_2 s_2^{-1}s_1^{-1} = s_2 s_1 s_1^{-1} = s_2 = s_3 s_3^{-1}s_1 s_1^{-1}s_2 = s_3 s_1 s_3^{-1}s_1^{-1}s_2$

6. $s_i s_{i+1} \neq s_{i+1}s_i$, *για* $n \geq 3$.
   Απόδειξη: $s_i s_{i+1} = s_{i+1}s_i \Leftrightarrow s_{i+1}s_i s_{i+1} = s_{i+1}s_{i+1}s_i \Leftrightarrow s_i s_{i+1} s_i = s_{i+1}s_{i+1}s_i \Leftrightarrow s_i s_{i+1} = s_{i+1}s_{i+1} \Leftrightarrow s_i = s_{i+1}$, *άτοπο.*

Το 1936, ο Artin απέδειξε επίσης, ότι κάθε ισότητα στη θεωρία πλεξίδων προκύπτει με συνδυασμό ταυτοτήτων από τις κατηγορίες 1 - 3. Μια άλλη απόδειξη μπορεί να βρει κανείς στο [28]. Τα παραπάνω μας επιτρέπουν να πούμε ότι τα $s_i,\ i = 1, 2, ..., n-1$ αποτελούν ένα σύνολο γεννητόρων της B_n, και να γράψουμε:

$$B_n = \langle s_1, s_2, ..., s_{n-1} | s_i s_j = s_j s_i \ \text{ αν } \ |i-j| \geq 2,\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \rangle$$

Η περιγραφή αυτή της B_n μας οδηγεί εύκολα σε δυο συμπεράσματα. Πρώτο, η B_n έχει άπειρα στοιχεία, καθώς, για παράδειγμα, μπορούμε να πολλαπλασιάζουμε συνεχώς με το s_1 και να παίρνουμε πάντα κάτι διαφορετικό ($s_1^i \neq s_1^j$



Σχήμα 7: Η $s_2 s_4$ και η $s_4 s_2$ στην $B6$.

όταν $i \neq j$). Πίσω από την απειρία των ομάδων πλεξίδων, κρύβεται το γεγονός ότι είναι **ελεύθερες στρέψης** (torsion free), δηλαδή η $B_n (n \in N)$ δεν έχει κανένα **στοιχείο στρέψης**, που με τη σειρά του σημαίνει ότι δεν υπέρχει κάποιο άλλο στοιχείο g, πέρα από το e (την ταυτοτική πλεξίδα), τέτοιο ώστε να ισχύει $g^m = e$ για κάποιο $m \in N$. Δεύτερο, γενικά δεν υπάρχει μοναδικός τρόπος να αναπαραστήσουμε μια πλεξίδα σαν μια λέξη από s_i. Για παράδειγμα, η πρώτη πλεξίδα του σχήματος 3 είναι η $s_1 s_2^{-1} s_3^{-1} s_4 s_1 s_3 s_1 s_2^{-1} s_5 s_1 s_4^{-1} s_5$, οποία, εφαρμόζοντας κάποιες από τις παραπάνω σχέσεις, μπορεί να γραφτεί και ως $s_1 s_2^{-1} s_3^{-1} s_4 s_5 s_3 s_4^{-1} s_5 s_1^2 s_2^{-1} s_1$ Το πρώτο είναι καλό για την κρυπτογραφία, ενώ το δεύτερο, που είναι κάπως ενοχλητικό, μελετήθηκε και προέκυψαν κάποια συμπεράσματα στα οποία αναφερόμαστε στη συνέχεια.

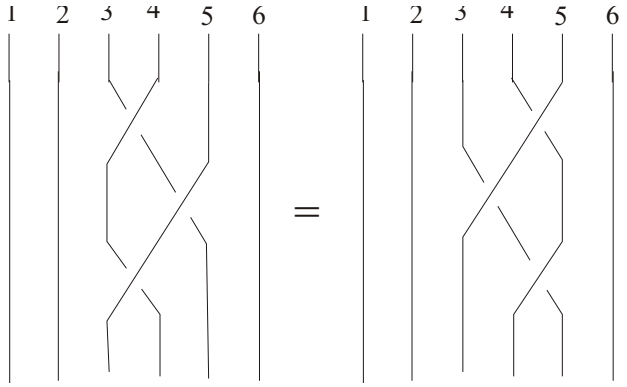
Υπάρχει ένας τρόπος να χαρακτηρίσουμε τις ομάδες πλεξίδων ως ειδική περίπτωση μιας ευρύτερης κατηγορίας ομάδων, των ομάδων Artin:

Ορισμός 2.2 *Έστω G ομάδα. Για τα $a, b \in G$ ορίζουμε $< a, b >^q = aba...$, γινόμενο με q παράγοντες.*

Για παράδειγμα $< a, b >^3 = aba$, $< b, a >^4 = baba$, κ.τ.λ.

Ορισμός 2.3 *Μια ομάδα Artin είναι μια ομάδα G η οποία επιδέχεται ένα σύνολο γεννητόρων $\{a_i\}_{i \in I}$, με I ένα ολικά διατεταγμένο σύνολο δεικτών, και σχέσεις της μορφής $< a_i a_j >^{m_{ij}} = < a_j a_i >^{m_{ji}}$, για κάθε i, j στο I και m_{ij} μη αρνητικούς ακεραίους.*

Σύμφωνα με τα παραπάνω, η ομάδα πλεξίδων B_n είναι μια ομάδα Artin με $I = \{1, ..., n\}$ και $m_{ij} = 2$ για $|i - j| > 1$, $m_{ij} = 3$, αλλιώς.



Σχήμα 8: Η $s_3s_4s_3$ και η $s_4s_3s_4$ στην B_6.

Η αναπαράσταση BKL

Μια εναλλακτική αναπαράσταση δόθηκε από τους Birman, Ko, και Lee το 1998 σε μια εργασία τους [4], όπου προτείνουν ένα άλλο σύνολο γεννητόρων. Σύμφωνα με την πρότασή τους, το σύνολο των γεννητόρων της B_n αποτελείται από όλες τις πλεξίδες a_{ts}, με $1 \leq s < t \leq n$ (επομένως προτείνουν $\frac{(n-1)(n-2)}{2}$ γεννήτορες), όπου η πλεξίδα a_{ts} ορίζεται ως εξής: είναι πανομοιότυπη με την ταυτοτική, με μόνη διαφορά ότι η κλωστή που ξεκινά από το A_s καταλήγει στο Γ_t, ενώ αυτή που ξεκινά από το A_t καταλήγει στο Γ_s, περνώντας πάνω από την προηγούμενη. Και οι δυο περνούν πάνω από τυχούσες ενδιάμεσες κλωστές (θα υπάρχουν αν $t > s+1$, βλ. σχήμα 10).

Οι σχέσεις που συμπληρώνουν την περιγραφή είναι οι εξής:

$$a_{ts}a_{rq} = a_{rq}a_{ts} \text{ αν } (t-r)(t-q)(s-r)(s-q) > 0 \qquad (1)$$

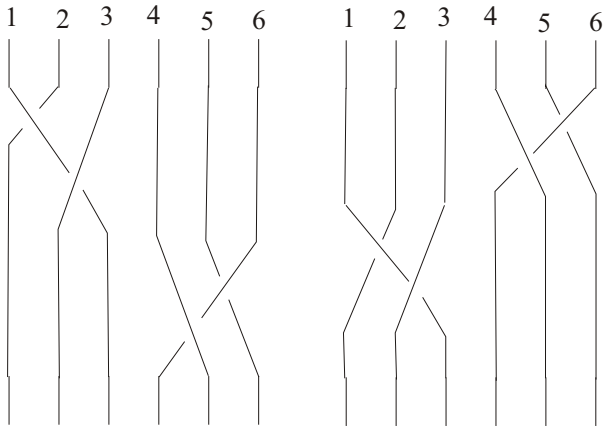
$$a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr} \text{ για όλα τα } t,s,r \text{ με } n \geq t > s > r \geq 1 \qquad (2)$$

Η γεωμετρική ερμηνεία της πρώτης είναι ότι οι a_{ts} και a_{rq} αντιμετατίθονται αν ισχύει ότι $t > s > r > q$ ή $t > r > q > s$ ή $r > q > t > s$ ή $r > t > s > q$. Η δεύτερη μας λέει ότι μπορούμε να 'παίξουμε' με τους γεννήτορες που σχηματίζονται από τρεις κλωστές.

Παρατηρούμε ότι:

1. Το νέο σύνολο γεννητόρων αποτελεί υπερσύνολο των s_i, με τα s_i να αποτελούν την ειδική περίπτωση όπου $t = s+1$, δηλαδή $s_i = a_{(i+1)i}$.

2. Οι νέοι γεννήτορες δίνονται, σε σχέση με τους παλιούς, από τις σχέσεις $a_{ts} = (s_{t-1}s_{t-2}...s_{s+1})s_s(s_{t-1}s_{t-2}...s_{s+1})^{-1}$.



Σχήμα 9: Η $s_1^{-1}s_2s_5s_4^{-1}$ και η $s_5s4^{-1}s_1^{-1}s_2$.

Ισοδυναμία των δυο αναπαραστάσεων

Θα δείξουμε τώρα ότι η αναπαράσταση του Artin και η BKL-αναπαράσταση είναι ισοδύναμες. Πιο συγκεκριμένα, έστω

$$B_n = \langle s_1, s_2, ..., s_{n-1} \,|\, s_is_j = s_js_i \text{ αν } |i-j| \geq 2,\ s_is_{i+1}s_i = s_{i+1}s_is_{i+1} \rangle$$

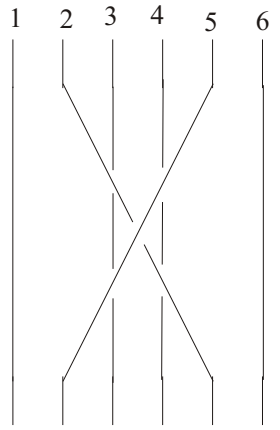
και

$$L_n = \langle a_{ts}, 1 \leq s < t \leq n \,|\, a_{ts}a_{rq} = a_{rq}a_{ts} \text{ αν } (t-r)(t-q)(s-r)(s-q) > 0,$$

$$a_{ts}a_{sr} = a_{tr}a_{ts} = a_{sr}a_{tr} \text{ για όλα τα } t, s, r \text{ με } n \geq t > s > r \geq 1 \rangle$$

οι δυο ομάδες που αντιστοιχούν στις εν λόγω αναπαραστάσεις . Θα δείξουμε ότι είναι ισόμορφες. Για να το πετύχουμε, θα χρησιμοποιήσουμε ένα εργαλείο από τη συνδυαστική θεωρία ομάδων (του κλάδου της άγεβρας, ένα από τα αντικείμενα του οποίου είναι και η αναπαράσταση μιας ομάδας, βλ. [27]). Για το συμβολισμό, σημειώνουμε ότι S είναι το σύνολο των γεννητόρων της G και D είναι το σύνολο των οριζουσών σχέσεων, εκφρασμένων στη μορφή $A = 1$, όπου A είναι μια λέξη από γράμματα του S.

Θεώρημα 2.1 *Έστω $G = \langle S \,|\, D \rangle$ και H δυο ομάδες, και έστω $\psi : S \to H$ μια συνάρτηση. Τότε η ψ επεκτείνεται σε ένα ομομορφισμό $\psi : G \to H$ αν και μόνο αν $\widetilde{\psi}(r) =_H 1$, για όλα τα $r \in D$, όπου $\widetilde{\psi}$ είναι η τυπική επέκταση της ψ σε όλες τις λέξεις από το S.*



Σχήμα 10: Η a_{52} στην B_6.

Για τις ανάγκες του θεωρήματος, οι αναπαραστάσεις μας γίνονται

$$B_n = \langle s_1, s_2, ..., s_{n-1} \,|\, s_i s_j s_i^{-1} s_j^{-1} = 1 \text{ αν } |i-j| \geq 2,\ s_i s_{i+1} s_i s_{i+1}^{-1} s_i^{-1} s_{i+1}^{-1} = 1 \rangle$$

και

$$H_n = \langle a_{ts}, 1 \leq s < t \leq n \,|\, a_{ts} a_{rq} a_{ts}^{-1} a_{rq}^{-1} = 1 \text{ αν } (t-r)(t-q)(s-r)(s-q) > 0,$$

$$a_{ts} a_{sr} a_{ts}^{-1} a_{tr}^{-1} = 1 = a_{sr} a_{tr} a_{ts}^{-1} a_{tr}^{-1} \text{ για όλα τα } t, s, r \text{ με } n \geq t > s > r \geq 1 \rangle$$

Τώρα, ορίζουμε τις $\phi : \{s_1, s_2, ..., s_{n-1}\} \to H_n$ και $\psi : \{a_{ts}, 1 \leq s < t \leq n\} \to B_n$ με $\phi(s_i) = a_{(i+1)i}$ και $\psi(a_{ts}) = (s_{t-1} s_{t-2} ... s_{s+1}) s_s (s_{t-1} s_{t-2} ... s_{s+1})^{-1}$.

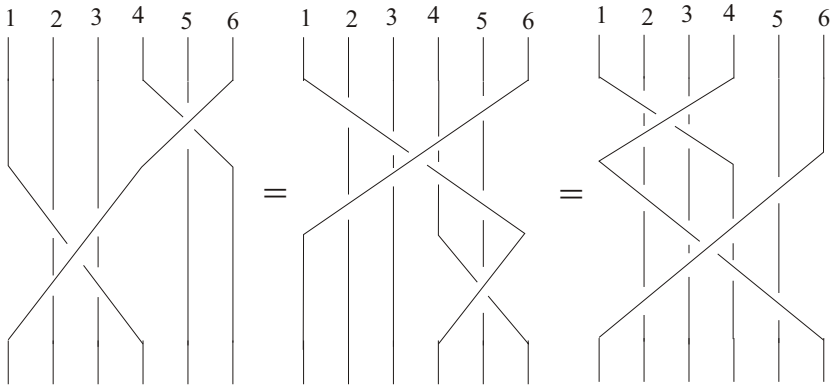
Για την ϕ υπολογίζουμε ότι για κάθε i:

- $\widetilde{\phi}(s_i s_{i+1} s_i \ s_{i+1}^{-1} \ s_i^{-1} \ s_{i+1}^{-1}) = a_{(i+1)i} \ a_{(i+2)(i+1)} \ a_{(i+1)i} \ a_{(i+2)(i+1)}^{-1} \ a_{(i+1)i}^{-1}$ $a_{(i+2)(i+1)}^{-1} = a_{(i+1)i} \, a_{(i+2)i} \, a_{(i+2)(i+1)} \, a_{(i+2)(i+1)}^{-1} \, a_{(i+1)i}^{-1} \, a_{(i+2)(i+1)}^{-1} = a_{(i+1)i} a_{(i+2)i}$ $a_{(i+1)i}^{-1} \, a_{(i+2)(i+1)}^{-1} = a_{(i+2)(i+1)} a_{(i+1)i} a_{(i+1)i}^{-1} \, a_{(i+2)(i+1)}^{-1} = 1.$

και (όταν $|i-j| \geq 2$):

- $\widetilde{\phi}(s_i s_j s_i^{-1} s_j^{-1}) = a_{(i+1)i} s_{(j+1)j} s_{(i+1)i}^{-1} s_{(j+1)j}^{-1} = s_{(j+1)j} a_{(i+1)i} \ s_{(i+1)i}^{-1} s_{(j+1)j}^{-1}$ $= 1.$

Επίσης, για την ψ υπολογίζουμε:



Σχήμα 11: $a_{64}a_{41} = a_{61}a_{64} = a_{41}a_{61}$.

- Για $t > s > r$ είναι $|t-(s-1)| > 1$, $|s-(r-1)| > 1$ οπότε $\widetilde{\psi}(a_{ts}a_{sr}a_{ts}^{-1}a_{tr}^{-1}) =$

  $(s_{t-1}s_{t-2}...s_{s+1})\ s_s\ (s_{t-1}\ s_{t-2}...s_{s+1})^{-1}\ (s_{s-1}s_{s-2}...s_{r+1})\ s_r$
  $(s_{s-1}\ s_{s-2}...s_{r+1})^{-1}\ (s_{t-1}\ s_{t-2}...s_{s+1})\ s_s^{-1}\ (s_{t-1}s_{t-2}...s_{s+1})^{-1}$
  $(s_{t-1}s_{t-2}...s_{r+1})\ s_r^{-1}\ (s_{t-1}s_{t-2}...s_{r+1})^{-1} =$
  $(s_{t-1}s_{t-2}...s_{s+1})\ s_s\ (s_{t-1}s_{t-2}...s_{s+1})^{-1}\ (s_{t-1}s_{t-2}...s_{s+1})\ (s_{s-1}s_{s-2}...s_{r+1})$
  $s_r\ (s_{s-1}\ s_{s-2}...s_{r+1})^{-1}\ s_s^{-1}(s_{t-1}\ s_{t-2}...s_{s+1})^{-1}\ (s_{t-1}s_{t-2}...s_{r+1})\ s_r^{-1}\ (s_{t-1}$
  $s_{t-2}...s_{r+1})^{-1} =$
  $(s_{t-1}s_{t-2}...s_{s+1})\ s_s\ (s_{s-1}s_{s-2}...s_{r+1})\ s_r\ (s_{s-1}s_{s-2}...s_{r+1})^{-1}\ s_s^{-1}(s_{t-1}\ s_{t-2}...s_{s+1})^{-1}$
  $(s_{t-1}s_{t-2}...s_{r+1})\ s_r^{-1}\ (s_{t-1}\ s_{t-2}...s_{r+1})^{-1} =$
  $s_{t-1}s_{t-2}...s_{s+1}\ \ s_s\ \ s_{s-1}s_{s-2}...s_{r+1}\ \ s_r\ \ s_{r+1}^{-1}...s_{s-2}^{-1}\ \ s_{s-1}^{-1}\ \ s_s^{-1}s_{s+1}^{-1}...s_{t-2}^{-1}s_{t-1}^{-1}$
  $s_{t-1}s_{t-2}...s_{r+1}\ \ s_r^{-1}\ \ s_{r+1}^{-1}...s_{t-2}^{-1}\ \ s_{t-1}^{-1} = 1$

  Ανάλογα πέρνουμε $\widetilde{\psi}(a_{sr}a_{tr}a_{ts}^{-1}a_{tr}^{-1}) = 1$

ενώ όταν $(t-r)(t-q)(s-r)(s-q) > 0$, ισοδύναμα $t > s > r > q$ (1) ή $t > r > q > s$ (2) ή $r > q > t > s$ (3) ή $r > t > s > q$ (4), τότε

- Στις περιπτώσεις (1) και (3): $\widetilde{\psi}(a_{ts}a_{rq}a_{ts}^{-1}a_{rq}^{-1}) =$

  $s_{t-1}\ s_{t-2}...s_{s+1}\ s_s\ s_{s+1}^{-1}...s_{t-2}^{-1}\ s_{t-1}^{-1}\ s_{r-1}s_{r-2}...s_{q+1}\ s_q s_{q+1}^{-1}...s_{r-2}^{-1}s_{r-1}^{-1}\ s_{t-1}s_{t-2}...s_{s+1}s_s^{-1}$
  $s_{s+1}^{-1}...s_{t-2}^{-1}\ s_{t-1}^{-1}\ s_{r-1}s_{r-2}...s_{q+1}\ s_q^{-1}s_{q+1}^{-1}...s_{r-2}^{-1}\ s_{r-1}^{-1} = s_{t-1}s_{t-2}...s_{s+1}\ s_s s_{s+1}^{-1}...s_{t-2}^{-1}s_{t-1}^{-1}$
  $s_{t-1}s_{t-2}...s_{s+1}s_s^{-1}\ s_{s+1}^{-1}...s_{t-2}^{-1}\ s_{t-1}^{-1}\ s_{r-1}s_{r-2}...s_{q+1}\ s_q\ s_{q+1}^{-1}...s_{r-2}^{-1}\ s_{r-1}^{-1}\ s_{r-1}$
  $s_{r-2}...s_{q+1}\ s_q^{-1}\ s_{q+1}^{-1}...s_{r-2}^{-1}\ s_{r-1}^{-1} = 1$

- Στις περιπτώσεις (2) και (4):Υπολογίζουμε ότι $\widetilde{\psi}(a_{ts}a_{rq}a_{ts}^{-1}a_{rq}^{-1}) = 1$.

Επομένως, σύμφωνα με το θεώρημα, οι ϕ και ψ είναι ομομορφισμοί. Τώρα, παρατηρούμε ότι:

$$\psi(\phi(s_i)) = \phi(a_{(i+1)i}) = s_i$$

και:

$$\psi(\phi(a_{ts})) = \psi(s_{t-1}...s_{s+1}s_s s_{s+1}^{-1}...s_{t-1}^{-1}) =$$

$$a_{t(t-1)}...a_{(s+2)(s+1)}a_{(s+1)s}a_{(s+2)(s+1)}^{-1}...a_{t(t-1)}^{-1} =$$

$$a_{t(t-1)}...a_{(s+3)(s+2)}a_{(s+2)s}a_{(s+2)(s+1)}a_{(s+2)(s+1)}^{-1}a_{(s+3)(s+2)}^{-1}...a_{t(t-1)}^{-1} =$$

$$a_{(s+3)(s+2)}a_{(s+2)s}a_{(s+3)(s+2)}^{-1}...a_{t(t-1)}^{-1} =$$

$$...$$

$$= a_{t(t-1)}a_{(t-1)s}a_{t(t-1)}^{-1} = a_{ts}a_{t(t-1)}a_{t(t-1)}^{-1} = a_{ts}$$

Αυτό σημαίνει ότι οι ϕ και ψ είναι αντίστροφες, και επομένως είναι και οι δυο ισομορφισμοί. Συμπεραίνουμε ότι οι ομάδες S_n και H_n είναι ισόμορφες, που είναι και το ζητούμενο.

2.4 Πλεξίδες και Πίνακες

Παρά την δυνατότητά μας για πολύ καλή διαισθητική και γεωμετρική περιγραφή των πλεξίδων, οι γνώσεις μας και η έρευνα που έχει γίνει για αυτές είναι ελάχιστες συγκριτικά με άλλες ομάδες, όπως τις ομάδες πινάκων. Το ερώτημα του κατά πόσο υπάρχει αναπαράσταση των πλεξίδων με πίνακες τέθηκε νωρίς, τόσο λόγο του ενδιαφέροντος που από μόνο του παρουσιάζει, όσο και για τις ενδιαφέρουσες επιπτώσεις που θα είχε μια ενδεχόμενη καταφατική απάντηση. Επιπλέον, αν υπάρχουν τέτοιες αναπαραστάσεις, μας ενδιαφέρει ο τύπος τους και το αν είναι 1-1 (faithful). Στην περίπτωση που υπάρχει μια 1-1 απεικόνιση της B_n σε μια ομάδα πινάκων, τότε λέμε ότι η B_n είναι **γραμμική**.

Η πρώτη προσέγγιση στο πρόβλημα έγινε το 1935 από τον W. Burau, ο οποίος σε μια εργασία του παρουσίασε την Burau αναπαράσταση β και την reduced Burau αναπαράσταση β'. Και οι δυο έχουν ως πεδίο ορισμού την B_n και ως πεδίο τιμών το σύνολο των $n \times n$ (για τη β) και $(n-1) \times (n-1)$ (για τη β') πινάκων με στοιχεία ρητές συναρτήσεις. Περιγράφονται ως εξής:

$$\beta(s_i) = \begin{pmatrix} I_{i-1} & & & \\ & 1-t & t & \\ & 1 & 0 & \\ & & & I_{n-i-1} \end{pmatrix}$$

και

$$\beta'(s_1) = \begin{pmatrix} -t & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & I_{n-3} \end{pmatrix},$$

$$\beta'(s_i) = \begin{pmatrix} I_{i-2} & & & & \\ & 1 & -t & t & \\ & 0 & -t & 0 & \\ & 0 & -1 & 1 & \\ & & & & I_{n-i-2} \end{pmatrix}, (i \neq 1, n-1),$$

$$\beta'(s_{n-1}) = \begin{pmatrix} I_{n-3} & 0 & 0 \\ & 1 & -t \\ 0 & 0 & -t \end{pmatrix}.$$

Από νωρίς ήταν γνωστό ότι η αναπαράσταση της B_3 είναι 1-1. Για τα υπόλοιπα n όμως, το ερώτημα έμεινε ανοικτό για πολλά χρόνια. Μόλις το 1991, ο J.Moody απέδειξε ότι δεν είναι 1-1 για $n \geq 9$. Αργότερα την ίδια χρονιά, οι D.D.Long και M.Paton, βελτιώνοντας τις ιδέες του Moody, έδειξαν ότι δεν είναι 1-1 για $n \geq 6$. Τέλος, το 1999, ο S.Bigelow χρησιμοποίησε παρόμοιες ιδέες για να δείξει ότι δεν είναι 1-1 ούτε για $n = 5$. Έτσι, σε ότι αφορά το συγκεκριμένο μετασχηματισμό, παραμένει ανοιχτό το ερώτημα για $n = 4$.

Φαίνεται ότι η κατάρριψη των ελπίδων ότι η Burau αναπαράσταση θα έδινε τη γραμμικότητα των ομάδων πλεξίδων, αναθέρμανε το ερευνητικό ενδιαφέρον. Έτσι, το 1999, ο D.Krammer παρουσίασε μια νέα αναπαράσταση, την οποία πρώτος είχε μελετήσει ο Lawrence, με τη βοήθεια της οποίας απέδειξε τη γραμμικότητα της B_4. Πολύ σύντομα, ο Bigelow και ο Krammer, ανεξάρτητα, απέδειξαν ότι ο μετασχηματισμός είναι 1-1 για όλα τα n. Έτσι σήμερα ξέρουμε ότι οι B_n είναι γραμμικές.

Παρά το γεγονός ότι η γραμμικότητα δίνεται από την αναπαράσταση Krammer, στην πράξη χρησιμοποιείται η αναπαράσταση Bureau, επειδή έχει πιο ευκολόχρηστο τύπο.

2.5 Πλεξίδες και μεταθέσεις

Αν διαβάζοντας μέχρι εδώ, σας πέρασε με οποιοδήποτε τρόπο από το μυαλό η έννοια της μετάθεσης, τότε η διαίσθησή σας βρίσκεται σε καλό δρόμο. Πράγματι, αν αριθμήσουμε τους γάντζους από αριστερά προς τα δεξιά και δούμε την πλεξίδα ως ένα μηχανισμό που στέλνει τα $A_1, A_2, A_3..., A_n$ της πάνω ράβδου, στα $\Gamma_{\alpha_1}, \Gamma_{\alpha_2}, \Gamma_{\alpha_3}$,...,$\Gamma_{\alpha_n}$ της κάτω ράβδου, τότε η συγκεκριμένη πλεξίδα πραγματοποιεί τη μετάθεση $\alpha_1\alpha_2\alpha_3...\alpha_n$. Έτσι δεν λαμβάνουμε, βέβαια, υπόψη μας τον τρόπο που πλέκονται οι κλωστές, και γενικά δυο διαφορετικές πλεξίδες μπορούν να δίνουν την ίδια μετάθεση (για παράδειγμα, αν σε μια τυχαία πλεξίδα

αντικαταστήστε ένα παράγοντα s_i με τον s_i^{-1}, η μετάθεση). Από αλγεβρική άποψη, η περιγραφή της S_n προκύπτει από αυτή της B_n αν επιπλέον προσθέσουμε τις σχέσεις

$$s_i^2 = e, \;\; i = 1, 2, .., n-1$$

(απλές φαινομενικά σχέσεις, με μεγάλη δύναμη όμως, αφού κάνουν την ομάδα πεπερασμένη).

Πάντως, από τα παραπάνω προκύπτει ένας επίμορφισμός ϑ από μια ομάδα πλεξίδων B_n στην αντίστοιχη ομάδα μεταθέσεων των n στοιχείων, την S_n. Ο πυρήνας του ϑ θα αποτελείται από όλες εκείνες τις πλεξίδες με την εξής ιδιότητα: *Για κάθε i, η κλωστή που ξεκινά από το A_i, καταλήγει στο Γ_i.* Προφανώς ο πυρήνας αυτός περιέχει άπειρες πλέξίδες. Επίσης μπορούμε να ορίσουμε μια άλλη απεικόνιση από την ομάδα μεταθέσεων S_n στο δυναμοσύνολο της B_n, η οποία αντιστοιχίζει κάθε μετάθεση π στο σύνολο των πλεξίδων που απεικον΄ιζονται μέσω της ϑ στην π. Διαμερίζεται με αυτόν τον τρόπο το B_n σε n! κλάσεις ισοδυναμίας (όσα και τα στοιχεία της S_n). Τώρα, από κάθε τέτοια κλάση, επιλέγουμε ένα αντιπρόσωπο, την πλεξίδα που περιέχει μόνο θετικές διασταυρώσεις. Υπάρχουν n! τέτοιες για κάθε n (μια για κάθε μετάθεση), τις οποίες ονομάζουμε **μεταθετικές πλεξίδες** και το σύνολό τους συμβολίζεται με $\widetilde{S}_n$. (Χαρακτηριστικό τους είναι ότι η συντομότερη λέξη από στοιχειώδεις πλεξίδες που τις περιγράφει δεν περιέχει κανένα s_i^{-1}, και ότι κάθε ζεύγος κλωστών διασταυρώνεται το πολύ μια φορά, και αυτή θετικά.)

Μια ειδική κατηγορία μεταθετικών πλεξίδων είναι αυτές που αντιστοιχούν στις μεταθέσεις της μορφής $n(n-1)...(2)1$. Ονομάζονται **θεμελιώδεις** και υπάρχει μια για κάθε n, η οποία ονομάζεται Δ_n, ή απλά Δ όταν το n είναι προφανές. Η Δ_n έχει την ιδιότητα ότι η Δ_n^2 αντιμετατίθεται με οποιαδήποτε πλεξίδα. Πιο συγκεκριμένα, ισχύει ότι $s_i\Delta_n = \Delta_n s_{n-i}$, οπότε $s_i\Delta_n^2 = \Delta_n s_{n-i}\Delta_n = \Delta_n^2 s_i$.

Θα χρειαστούμε ένα ακόμη ορισμό:

Ορισμός 2.4 *Έστω B_n^+ η ημιομάδα που προκύπτει από την εφαρμογή των σχέσεων 1-3 της παραγράφου 2.3 στις s_i (και όχι στις αντίστροφές τους, βλ. αντίστοιχο ορισμό 2.6). Τα στοιχεία της B_n^+ τα λέμε **θετικές λέξεις**. Έστω $R \in B_n$, με $R = A\Gamma$. Θα λέμε ότι η ανάλυση αυτή της R είναι **αριστερά βεβαρημένη** αν ισχύει*

$$A \in \widetilde{S}_n \wedge \Gamma \in B_n^+ \wedge \forall i[\exists P \in B_n^+(\Gamma = s_i P) \rightarrow \exists Q \in B_n^+(A = Q s_i)].$$

Αν A_1, A_2 δυο μεταθετικές πλεξίδες, θα λέμε ότι το γινόμενο A_1A_2 είναι αριστερά βεβαρημένο αν ισχύει ότι

$$\exists \Gamma_1, \Gamma_2 \in \widetilde{S}_n(A_1A_2 = \Gamma_1\Gamma_2) \rightarrow \exists Z \in \widetilde{S}_n(A_1 = \Gamma_1 Z).$$

Είμαστε τώρα έτοιμοι να διατυπώσουμε κάποια θεωρήματα για την αναπαράσταση των πλεξίδων.

Θεώρημα 2.2 *Για κάθε $W \in B_n$, υπάρχει μια μοναδική αναπαράσταση, η* ***αριστερή κανονική μορφή****, ως $W = \Delta^k A_1 A_2 ... A_p, k \in \mathbb{Z}$, $A_i \in \widetilde{S}_n \setminus \{e, \Delta\}$, όπου το $A_i A_{i+1}$ είναι αριστερά βεβαρημένο. Το p θα το λέμε* ***κανονικό μήκος*** *της W, και θα το συμβολίζουμε με $len(W)$. Επίσης θα συμβολίζουμε: $inf(W) = k$ και $sup(W) = p + k$.*

Απόδειξη: Το θεώρημα αποδείχτηκε από τους Elrifai και Morton στο [13]. Για την απόδειξή τους ακολουθούν τον παρακάτω συλλογισμό, βασιζόμενοι και σε παλιότερα αποτελέσματα:

1. Οι σχέσεις στην αναπαράσταση του Artin σχετίζουν δυο θετικές λέξεις ίδιου μήκους. Όπως έδειξε ο Garside, ο φυσικός αυτομορφισμός από την B_n^+ στην B_n είναι $1-1$, και επομένως, δυο λέξεις P και Q είναι ισοδύναμες στην B_n, αν και μόνο αν είναι ισοδύναμες στην B_n^+.

2. Για μια θετική λέξη P, το αρχικό σύνολο $S(P)$ και το τελικό σύνολο $F(P)$ ορίζονται ως

$$S(P) = \{i | P = s_i P' \text{ για κάποιο } P' \in B_n^+\}$$

$$F(P) = \{i | P = Q' s_i \text{ για κάποιο } Q' \in B_n^+\}$$

   Για ένα κανονικό παράγοντα A που αντιστοιχεί σε μια μετάθεση $\pi \in S_n$, είναι $S(A) = \{i | \pi(i) > \pi(i+1)\}$ και ανάλογα $F(A) = \{i | \pi^{-1}(i) > \pi^{-1}(i+1)\}$

3. Η θεμελιώδης πλεξίδα Δ έχει τις ακόλουθες δυο ιδιότητες:

   (α′) Για κάθε $1 \leq i \leq n-1$, είναι $\Delta = s_i A_i = \Gamma_i s_i$, για κάποιες μεταθετικές πλεξίδες A_i και Γ_i.

   (β′) Για κάθε $1 \leq i \leq n-1$, είναι $s_i \Delta = \Delta s_{n-1}$.

   Για μια τυχαία λέξη W από s_i, μπορούμε να αντικαταστήσουμε κάθε εμφάνιση ενός s_i με τον τύπο $\Delta^{-1}\Gamma_i$, από την πρώτη ιδιότητα, και να μαζέψουμε όλα τα Δ^{-1} στα αριστερά, χρησιμοποιώντας την τη δεύτερη ιδιότητα, έτσι ώστε στο τέλος να πάρουμε την έκφραση $W = \Delta^v P$, $P \in B_n^+, v \in Z$.

4. Για κάθε θετική λέξη P, υπάρχει μια μοναδική ανάλυση, που ονομάζεται αριστερά βεβαρημένη ανάλυση:

$$P = A_1 P_1, \text{ όπου } A_1 \in \widetilde{S}_n,\ P_1 \in B_n^+,\ F(A_1) \supset S(P_1)$$

Επαναλαμβάνοντας την αριστερά βεβαρημένη ανάλυση: $P = A_1P_1$, $P_1 = A_2P_2, ...$, και κατόπιν συλλέγοντας τα Δ στα αριστερά, παίρνουμε την αριστερή κανονική μορφή

$$P = \Delta^t A_1 A_2 ... A_p, \quad t \in Z,\ A_i \in \widetilde{S}_n \setminus \{e, \Delta\},$$

όπου κάθε A_iA_{i+1} είναι αριστερά βεβαρημένο. Αυτή η κανονική μορφή είναι μοναδική.

5. Συνδυάζοντας τα 3 και 4, παίρνουμε την αριστερή κανονική μορφή του θεωρήματος.

Μια βασική του χρησιμότητα είναι ότι μας επιτρέπει να κωδικοποιήσουμε την $W \in B_n$ με την $(p+1)$-άδα $(k, x_1, x_2, ..., x_p)$, όπου $x_1, x_2, ..., x_p$ είναι οι μεταθέσεις που αντιστοιχούν στις μεταθετικές πλεξίδες $A_1, A_2, ..., A_p$ αντίστοιχα. Ανοίγει έτσι ο δρόμος για την υπολογιστική επεξεργασία των καμπυλών. Επίσης, αν έχουμε δυο πλεξίδες v και w, τις πολλαπλασιάσουμε και κατόπιν γράψουμε το γινόμενο wv στην κανονική του μορφή, τότε είναι δύσκολο από αυτή την κανονική μορφή να βρούμε τους παράγοντες v και w. Τέτοιου είδους ιδιότητες μπορούν να φανούν χρήσιμες στην κρυπτογραφία.

Θεώρημα 2.3 *Έστω P μια λέξη από s_i με μήκος l. Τότε η αριστερή κανονική μορφή της P μπορεί να υπολογιστεί σε χρόνο $O(l^2 n \log n)$.*

Θεώρημα 2.4 *Έστω $P = \Delta_u A_1 ... A_p$ και $T = \Delta_v \Gamma_1 ... \Gamma_q$ οι αριστερές κανονικές μορφές δυο n-πλεξίδων. Τότε μπορούμε να υπολογίσουμε την αριστερή κανονική μορφή της PT σε χρόνο $O(pqn \log n)$.*

Θεώρημα 2.5 *Αν $P = \Delta_u A_1 ... A_p$ είναι η αριστερή κανονική μορφή της $P \in B_n$, τότε μπορούμε να υπολογίσουμε την αριστερή κανονική μορφή της P^{-1} σε χρόνο $O(pn)$.*

Θεώρημα 2.6 *Το πλήθος των n-πλεξίδων με κανονικό μήκος p είναι τουλάχιστον*

$$\left(\left\lfloor \frac{n-1}{2} \right\rfloor ! \right)^p .$$

2.6 Προβλήματα στις ομάδες πλεξίδων

Κλείνοντας το κεφάλαιο αυτό, θα αναφερθούμε σε κάποια ενδιαφέροντα προβλήματα που παρουσιάζονται στις ομάδες πλεξίδων. Πρώτα θα δώσουμε τους απαραίτητους ορισμούς, κατόπιν θα αναφέρουμε συνοπτικά κάποια ενδιαφέροντα προβλήματα που δεν θα μας απασχολήσουν και τέλος θα μιλήσουμε για τα δυο προβλήματα που χρησιμοποιούνται στην κρυπτογραφία.

Ορισμός 2.5 *Έστω G μια ομάδα και $x, y \in G$. Τα x, y θα λέγονται* **συζυγή**, *αν υπάρχει $z \in G$ τέτοιο ώστε $y = zxz^{-1}$. Θα γράφουμε $x \sim y$ για να πούμε ότι τα x και y είναι συζυγή.*

Ορισμός 2.6 *Έστω G μια ομάδα με γεννήτορες $g_1, ..., g_n$. Μια* **λέξη** *w στη G είναι ένα γινόμενο της μορφής $g_{i_1}^{j_1} g_{i_2}^{j_2} ... g_{i_m}^{j_m}$, όπου $i_1, ..., i_m \in \{1, ..., n\}$ και $j_1, ..., j_m \in \{-1, +1\}$. Με άλλα λόγια, είναι ένα γινόμενο από γεννήτορες και αντίστροφα γεννητόρων.*

Έστω $n, m \in \mathbb{N}$ με $m < n$. Αν σε κάθε στοιχείο της B_m προσθέσουμε $n - m$ κλωστές στο τέλος, έχουμε μια φυσική απεικόνιση από την B_m στη B_n που μας επιτρέπει να πούμε ότι η B_m είναι υποομάδα της B_n (συμβολίζουμε με $B_m < B_n$) και να κάνουμε πράξεις ανάμεσα στα στοιχεία των δυο ομάδων. Συγκεκριμένα, θεωρούμε τη B_m ως την υποομάδα της B_n που παράγεται από τα $s_1, s_2, ..., s_{m-1}$.

Ορισμός 2.7 *Για μια n-πλεξίδα $x = D^u A_1 ... A_p$ στην αριστερή κανονική μορφή, το* ***cycling*** *του x ορίζεται ως $c(x) = D^u A_2 ... A_p r_u(A_1)$, όπου ο αυτομορφισμός $r : B_n \to B_n$ ορίζεται από τη σχέση $r(s_i) = s_{n-i}$ για $i = 1, ..., n-1$.*

Στο **Πρόβλημα της p-στής Ρίζας**, μας δίνεται ένα $y \in B_n$ για το οποίο ισχύει $y = x^p$ για κάποια $x \in B_n$ και $p \in \mathbb{Z}$ και αναζητούμε ένα τέτοιο x.

Στο **Κυκλικό Πρόβλημα** (Cycling Problem) μας δίνονται ένα $y \in B_n$ και ένα $r \in \mathbb{Z}$ τέτοια ώστε $y = c^r(x)$ για κάποιο $x \in B_n$ και πρέπει να βρούμε ένα τέτοιο x.

Στο **Πρόβλημα Markov** (Markov Problem) μας δίνεται μια $y \in B_n$ η οποία είναι συζυγής με μια πλεξίδα της μορφής $ws_{n-1}^{\pm 1}$ για κάποιο $w \in B_{n-1}$. Σκοπός μας είναι να βρούμε ένα $z \in B_n$ και ένα $x \in B_{n-1}$, τέτοια ώστε $zyz^{-1} = xs_{n-1}^{\pm 1}$.Το πρόβλημα αυτό σχετίζεται με τη μελέτη των κόμβων.

2.6.1 Το Πρόβλημα της Συζυγίας

Όταν μιλάμε για το Πρόβλημα Συζυγίας, αναφερόμαστε στο Πρόβλημα Απόφασης Συζυγίας, υπάρχουν όμως και αρκετές παραλλαγές του:

Το **Πρόβλημα της Απόφασης Συζυγίας** (Conjugacy Decision Problem): Μας δίνονται δυο στοιχεία x, y κάποιας B_n και πρέπει να αποφασίσουμε αν τα x και y είναι συζυγή.

Αν η απάντηση είναι θετική, τότε προκύπτει εύλογα ένα νέο ερώτημα, το **Πρόβλημα της Αναζήτησης Συζυγοποιητή** (Conjugator Search Problem): Αν τα $x, y \in B_n$ είναι συζυγή, ποιο είναι το z για το οποίο $y = zxz^{-1}$;

Αυτό είναι και ένα από τα δυο προβλήματα που πρέπει να λυθούν για την εφαρμογή της θεωρίας πλεξίδων στην low dimensional τοπολογία.

Το $(n,m)-$**Γενικευμένο Πρόβλημα Αναζήτησης Συζυγοποιητή** (Generalized Conjugator Search Problem), για $m < n$: Μας δίνονται δυο στοιχεία a, z της B_n για τα οποία υπάρχει $x \in B_m$ τέτοιο ώστε $z = xax^{-1}$ και στόχος μας είναι να βρούμε ένα x με αυτή την ιδιότητα.

Αναφορικά με τη συζυγία, υπάρχει ακόμα ένα πρόβλημα, το **Πρόβλημα της Αποσύνθεσης Συζυγίας** (Conjugacy Decomposition Problem): Μας δίνονται δυο στοιχεία x, y κάποιας B_n τέτοια ώστε $y = bxb^{-1}$ για κάποιο $b \in B_m$, $m < n$ και ψάχνουμε να βρούμε δυο a_1 και a_2 στη B_m τέτοια ώστε $y = a_1 x a_2$. Γενικά είναι πιο εύκολο από το Γενικευμένο Αναζήτησης, αλλά στο B9 εικάζονται ότι για κάποιες επιλογές του x είναι ισοδύναμα.

Η μελέτη των πλεξίδων στην κρυπτογραφία καθιέρωσε και δυο άλλες παραλλαγές, το $k-$**Ταυτόχρονο Πρόβλημα Αναζήτησης Συζυγίας**, το οποίο θα δούμε αργότερα, καθώς και το **Diffie-Helmann-Like Πρόβλημα Συζυγίας**: Μας δίνεται μια πλεξίδα $b \in B_n$ και οι πλεξίδες $b_1 = sbs^{-1}$ και $b_2 = rbr^{-1}$, όπου οι s και r βρίσκονται σε δυο υποομάδες της B_n που αντιμετατίθονται μεταξύ τους, και πρέπει να βρούμε την sb_2s^{-1} $(= rb_1r^{-1})$.

Το Πρόβλημα Συζυγίας αποτελεί σημαντικό κομμάτι της εφαρμογής των πλεξίδων στην κρυπτογραφία, και ως εκ τούτου η επίλυσή του παρουσιάζει ιδιαίτερο ενδιαφέρον (γενικά, όσο πιο δύσκολο αποδειχτεί το πρόβλημα της αναζήτησης συζυγοποιητή, τόσο ασφαλέστερα θα είναι τα κρυπτοσυστήματα). Έχουν προταθεί αρκετές λύσεις του:

Το 1969, ο Garside απέδειξε ότι το Πρόβλημα Απόφασης Συζυγιας είναι επιλύσημο. Για την τυχαία πλεξίδα P όρισε το summit σύνολο: αποτελείται από όλα τα συζυγή της P που έχουν maximal inf (βλ. θεώρημα 2.2). Για να δούμε αν δυο πλεξίδες είναι συζυγείς, αρκεί να συγκρίνουμε τα summit σύνολά τους, άρα το πρόβλημα μεταφέρεται στην εύρεση ενός κατάλληλου αλγορίθμου για τον προσδιορισμό του summit συνόλου.

Το 1994, οι E.Elrifai και H.Morton βελτίωσαν την ιδέα του Garside, ορίζοντας, για την τυχαία πλεξίδα P, το super summit σύνολο: αποτελείται από τα συζυγή της P που έχουν ταυτόχρονα minimal sup και maximal inf. Είναι υποσύνολο του summit και ευκολότερο να υπολογιστεί.

Οι Birman, Ko και Lee μελέτησαν τις παραπάνω λύσεις μέσα από τη δική τους αναπαράσταση και τη βελτίωσαν ακόμα περισσότερο.

Οι λύσεις αυτές είναι εκθετικές ως προς το μήκος των λέξεων που χειρίζονται.

Το 2002 δόθηκε από τους Franco και Meneses ένας πολύ βελτιωμένος αλγόριθμος, τόσο θεωρητικά όσο και πρακτικά. Τα πειραματικά αποτελέσματα που παρουσιάζουν στην εργασία τους δείχνουν μια αρκετά εντυπωσιακή βελτί-

ωση. Ο αλγόριθμός τους, όπως θα δούμε, έδωσε βάση για κάποιες επιθέσεις.

Μια άλλη προσέγγιση είναι να λύσουμε το πρόβλημα έμμεσα χρησιμοποιώντας απεικονίσεις σε πίνακες: μετατρέπουμε σε πίνακες τις δυο πλεξίδες που μας δίνουν, και λύνουμε το πρόβλημα για τους πίνακες που προέκυψαν. Η μέθοδος αυτή δεν φαίνεται να έχει βοηθήσει ακόμα στην επίλυση του Προβλήματος Εύρεσης Συζυγοποιητή, έχει δώσει όμως ένα αρκετά καλό αλγόριθμο για την επίλυση του Προβλήματος Απόφασης Συζυγίας. Όπως θα δούμε παρακάτω αυτό είναι αρκετά σημαντικό.

2.6.2 Το Πρόβλημα της Λέξης

Το **Πρόβλημα Λέξης** (Word Problem) είναι ένα πρόβλημα που μας απασχολεί γενικότερα στις ομάδες και διατυπώνεται ως εξής: Έστω G ομάδα και w μια λέξη στη G. Ισχύει $w = I_G$; Μια άλλη διατύπωση που μπορεί να συναντήσει κανείς είναι: Έστω G μια ομάδα και w_1, w_2 δυο λέξεις της G. Ισχύει $w_1 = w_2$;

Οι δυο αυτές διατυπώσεις είναι ισοδύναμες: Αν μπορούμε να λύσουμε το δεύτερο πρόβλημα, απλά θέτουμε $w_1 = w$ και $w_2 = I_G$ και παίρνουμε τη λύση του πρώτου, ενώ αν μπορούμε να λύσουμε το πρώτο, θέτουμε $w = w_1 w_2^{-1}$ και παίρνουμε τη λύση του δεύτερου.

Το Πρόβλημα της Λέξης στις ομάδες πλεξίδων είναι επιλύσημο: Η επιλυσημότητα προκύπτει από το γεγονός ότι υπάρχει ομομορφισμός από τη B_n στην ομάδα αυτομορφισμών της ελεύθερης ομάδας σε n γεννήτορες και από το ότι το πρόβλημα της λέξης στις ελεύθερες ομάδες είναι επιλύσημο.

Αυτό βέβαια δεν αρκεί για να ικανοποιήσει τα ανήσυχα πνεύματα των μαθηματικών που σε αυτές τις περιπτώσεις αμέσως θέτουν το ερώτημα: Ωραία λοιπόν, λύνεται το πρόβλημα, αλλά πόσο εύκολα και με ποιο αλγόριθμο; Το ερώτημα στην περίπτωσή μας το έθεσε ο Artin, μελετώντας τις πλεξίδες.

Μια πρώτη απάντηση δόθηκε από τον ίδιο τον Artin το 1925. Μελετώντας τον πυρήνα του επιμορφισμού ϑ, που αναφέραμε παραπάνω, από τη B_n στην S_n, κατέληξε σε μια λύση του προβλήματος, που απ'οτι φαίνεται είναι εκθετική στο μήκος της λέξης.

Πέρασαν αρκετά χρόνια μέχρι να βελτιωθεί η πολυπλοκότητα της λύσης. Αυτό έγινε το 1992 από τον Thurston, ο οποίος, βελτιώνοντας μια ιδέα που παρουσίασε ο Garside το 1969, κατέβασε την πολυπλοκότητα σε $|W|^2 nlogn$, για λέξη μήκους $|W|$. Ο Garside είχε καταφέρει να δείξει ότι κάθε πλεξίδα μπορεί να γραφεί ως $\Delta^k P$, όπου Δ η θεμελιώδης πλεξίδα που ορίσαμε, k ο μέγιστος ακέραιος για τέτοια αναπαράσταση και P μια θετική λέξη. Το πρόβλημα ήταν ότι η λέξη αυτή δεν ήταν μοναδική, γεγονός που δεν επέτρεπε στην πολυπλοκότητα να πέσει από το εκθετικό. Η βελτίωση του Thurston ήταν να δείξει ότι η P παραγοντοποιείται με μοναδικό τρόπο, όπως περιγράφουμε στο θεώρημα 2.1. Τώρα, η μορφή που προέκυψε είναι μοναδική. Δόθηκε

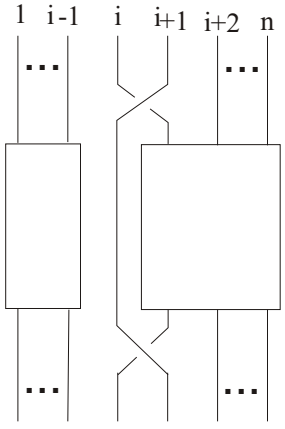
λοιπόν μια κανονική μορφή, η οποία για την τυχαία πλεξίδα μπορεί να βρεθεί σε χρόνο $|W|^2 nlogn$. Έτσι, αν μας δώσουν δυο λέξεις - πλεξίδες μπορούμε να τις φέρουμε σε κανονική μορφή στον παραπάνω χρόνο, και κατόπιν απλά να ελέγξουμε αν οι δυο παραστάσεις που προέκυψαν είναι ίδιες. Αυτό αποτελεί λύση του προβλήματος λέξης σε $O(|W|^2 nlogn)$.

Το 1998, οι Birman, Ko και Lee πρότειναν την αναπαράσταση που αναφέραμε, και με τη βοήθειά της έδωσαν μια παρόμοια κανονική μορφή, η οποία για την τυχαία πλεξίδα βρίσκεται σε χρόνο $O(|W|^2 n)$ και συνεπώς δίνει στον ίδιο χρόνο λύση για το Πρόβλημα Λέξης. Φαίνεται ότι στην πράξη χρησιμοποιείται ο αλγόριθμος των Garside-Thurston, γι' αυτό και όταν ενδιαφέρει η υλοποίηση του αλγορίθμου για μετατροπή των πλεξίδων σε κανονική μορφή, αναφέρεται ο χρόνος $|W|^2 nlogn$.

Από μια άλλη οπτική γωνία, ο Dehornoy, πρότεινε σε μια εργασία του ([5]) ένα διαφορετικό αλγόριθμο για την επίλυση του Προβλήματος Λέξης. Ισχυρίζεται ότι στην πράξη ο αλγόριθμός του είναι πιο γρήγορος από αυτόν του Thurston. Ακολουθεί μια σύντομη εισαγωγή στη μέθοδο του Dehornoy.

Αρχικά δίνουμε δυο απαραίτητους ορισμούς:

Ορισμός 2.8 *Μια λέξη στις ομάδες πλεξίδων ονομάζεται s_i-χερούλι (handle) όταν είναι της μορφής $s_i^e v s_i^{-e}$, όπου το e είναι +1 ή -1 και η v είναι μια λέξη που δεν περιέχει γράμματα της μορφής $s_k^{\pm 1}$, με $k < i-1$ ή $k > i$, και, επιπλέον, είτε το s_{i+1} είτε το s_{i+1}^{-1} δεν εμφανίζονται στην v.*



Σχήμα 12: Ένα s_i-χερούλι (τα κουτιά περιέχουν πλεξίδες, αδιάφορες ως προς τη μορφή). Η προέλευση της ονομασίας του γίνεται τώρα προφανής.

Ορισμός 2.9 *Έστω ότι η u είναι ένα s_i-χερούλι, $u = s_i^e v s_i^{-e}$. Ορίζουμε $red(u)$ να είναι η λέξη που προκύπτει από τη u αντικαθιστώντας κάθε γράμμα $s_{i+1}^{\pm 1}$ με $s_{i+1}^{-e} s_i^{\pm 1} s_{i+1}^{e}$, και αφήνοντας τα υπόλοιπα γράμματα απαράλλαχτα. Αν w και w' είναι δυο λέξεις στις πλεξίδες, λέμε ότι η w' έχει προέλθει από την w με* ***handle-αναγωγή*** *(reduction), αν μπορούμε να μετατρέψουμε την w στην w' αντικαθιστώντας διαδοχικά κάποια χερούλια u με τις αντίστοιχες λέξεις $red(u)$.*

Με βάση αυτούς τους ορισμούς αποδεικνύεται η ακόλουθη πρόταση:

Πρόταση 2.1 *Έστω w μια λέξη στις πλεξίδες, μήκους l. Τότε η w είναι ίση με την κενή λέξη e (δηλαδή την ταυτοτική πλεξίδα) αν και μόνο αν η w ανάγεται στην e, αν και μόνο αν κάθε ακολουθία αναγωγών που ξεκινούν με την w καταλήγουν στην e. Επιπλέον, κάθε ακολουθία αναγωγών που ξεκινά από την w τερματίζει το αργότερο σε εκθετικό χρόνο.*

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

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

3 Πλεξίδες και Κρυπτογραφία

Πολλά από όσα προαναφέραμε για τις πλεξίδες και τις ομάδες τους ήταν γνωστά για αρκετά χρόνια. Πιθανό είναι ότι κάποιοι διαισθάνονταν το ρόλο που μπορούν να παίξουν στην κρυπτογραφία, τίποτα χειροπιαστό δεν υπήρχε όμως ως το 1999. Τότε έγινε το πρώτο σημαντικό βήμα από τους Anshel, Anshel και Goldfeld, οι οποίοι παρουσίασαν στο [1] ένα πρωτόκολλο για αλγεβρικό καθορισμό κλειδιού. Το πρωτόκολλο αυτό (που πλέον αναφέρεται ως commutator key agreement protocol) εφαρμόζεται σε αλγεβρικές δομές γενικότερα, εμείς θα το δούμε εδώ στην εξειδικευμένη περίπτωση που οι δομές είναι ομάδες.

3.1 Η πρώτη ιδέα (commutator key agreement protocol)

Έστω G μια ομάδα. Όπως συνηθίζουν, οι ήρωες μας θέλουν να επικοινωνήσουν μυστικά, αλλά το κανάλι τους είναι ανασφαλές. Με βάση τη G, ακολουθούν την παρακάτω διαδικασία:

1. Η Αλίκη επιλέγει μια πεπερασμένα παραγόμενη υποομάδα της G, την $S_A =< x_1, x_2, ..., x_m >$ (δηλαδή την υποομάδα της G που παράγεται από τα $x_1, x_2, ..., x_m$), ενώ παράλληλα ο Βασίλης επιλέγει μια υποομάδα $S_B =< y_1, y_2, ..., y_n >$. (Το βήμα αυτό δεν είναι απαραίτητο να επαναλαμβάνεται κάθε φορά.)

2. Στη συνέχεια, ο καθένας τους επιλέγει ένα στοιχείο της υποομάδας του και το κρατά μυστικό. Έστω $a \in S_A$ το στοιχείο της Αλίκης και $b \in S_B$ το στοιχείο του Βασίλη.

3. Γενικά, οι δυο αυτές ομάδες μπορούν να δημοσιευτούν, η ασφάλεια του συστήματος δεν εξαρτάται από τη μυστικότητά τους. Ειδικότερα, ο Βασίλης στέλνει, μέσω του ανασφαλούς καναλιού, στην Αλίκη τα $y_1, y_2, ..., y_n$ και η Αλίκη τα $x_1, x_2, ..., x_m$ στο Βασίλη.

4. Μόλις η Αλίκη λάβει τα y_i, υπολογίζει και στέλνει στο Βασίλη καθένα από τα στοιχεία $k_1 = ay_1a^{-1}, k_2 = ay_2a^{-1}, ..., k_n = ay_na^{-1}$. Παράλληλα, ο Βασίλης υπολογίζει και στέλνει στη Αλίκη καθένα από τα $l_1 = bx_1b^{-1}, l_2 = bx_2b^{-1}, ..., l_m = bx_mb^{-1}$. Παρατηρούμε εδώ, ότι αν ο Εχθρός παρακολουθεί το κανάλι με σκοπό να υποκλέψει τα a και b, για να το πετύχει θα πρέπει να είναι σε θέση, έχοντας τα $k_1, k_2, ...k_n$ και $l_1, l_2, ..., l_m$ να λύσει τα συστήματα $k_1 = ay_1a^{-1}, k_2 = ay_2a^{-1}, ..., k_n = ay_na^{-1}$ και $l^1 = ax_1a^{-1}, l_2 = ax_2a^{-1}, ..., l_m = ax_ma^{-1}$ ως προς a και b αντίστοιχα.

5. Έχοντας λάβει τα $ay_1a^{-1}, ay_2a^{-1}, ..., ay_na^{-1}$ και $ax_1a^{-1}, ax_2a^{-1}, ..., ax_ma^{-1}$, μπορούν να επιλέξουν ανεξάρτητα ο καθένας οποιοδήποτε στοιχείο g_A και g_B της υποομάδας του και να σχηματίσουν το συζυγές του, bg_Ab^{-1} και ag_Ba^{-1} αντίστοιχα. Για παράδειγμα, αν η Αλίκη θέλει να υπολογίσει το συζυγές του $x = x_{i_1}x_{i_2}...x_{i_s}$, δεν έχει παρά να υπολογίσει το γινόμενο $l_{i_1}l_{i_2}...l_{i_s}$. Ειδικότερα, μπορούν να σχηματίσουν τα $a^* = bab^{-1}$ και $b^* = aba^{-1}$.

6. Τέλος, η Αλίκη υπολογίζει το $a(a^*)^{-1} = aba^{-1}b^{-1} = [a, b]$ και ο Βασίλης το $(b^*)b^{-1} = aba^{-1}b^{-1} = [a, b]$.

Μετά και από αυτό, έχουν πλέον καταλήξει σε ένα κοινό στοιχείο της G, το $[a, b]$, το οποίο μπορούν να χρησιμοποιήσουν ως μυστικό κλειδί. Εδώ πρέπει να πούμε ότι η γραφή του $[a, b]$ που ο Βασίλης κρατά στα χέρια του ενδέχεται να είναι διαφορετική από αυτή της Αλίκης. Επομένως αν θέλουν να μοιράζονται ακριβώς την ίδια λέξη, θα πρέπει να έχουν ένα τρόπο, ώστε αν τους δίνουν δυο διαφορετικές εκφράσεις του ίδιου στοιχείου, αυτοί να μπορούν να τις μετασχηματίσουν σε μια κοινή, κάποια προσυμφωνημένη κανονική μορφή.

Μια απλή επαλήθευση θα μας επιβεβαιώσει ότι όντως, για κάθε ομάδα G, ο αλγόριθμος αυτός δίνει το ίδιο κλειδί στην Αλίκη και το Βασίλη. Στην πράξη, όμως, αυτό δεν αρκεί. Θα πρέπει ο αλγόριθμος να είναι τόσο ασφαλής, όσο και εύκολα υλοποιήσιμος. Αυτό γενικά σημαίνει ότι θα πρέπει οι πράξεις που εκτελούν η Αλίκη με το Βασίλη να γίνονται εύκολα, ενώ οι πράξεις που θα πρέπει να εκτελέσει ο Εχθρός να γίνονται σχετικά αργά. Ας τον εξετάσουμε για να δούμε ποια χαρακτηριστικά πρέπει να διαθέτει η ομάδα ώστε να είναι 'καλός '.

Καταρχήν, πρέπει η G να έχει πεπερασμένα παραγόμενες υποομάδες. Στη συνέχεια, έχοντας τα $a, x \in G$, θα πρέπει να μπορούμε να υπολογίσουμε γρήγορα το axa^{-1}. Γρήγορα επίσης θα πρέπει να γίνεται και η πράξη ab δοθέντων των a, b. Τέλος, θα πρέπει να υπάρχει γρήγορος τρόπος να γραφεί μια λέξη της G σε κάποια κανονική μορφή.

Σε ότι αφορά την ασφάλεια τώρα, όπως ήδη παρατηρήσαμε, το μόνο που μπορεί να κάνει ο Εχθρός για να σπάσει άμεσα την ασφάλεια του αλγόριθμου, είναι να λύσει τα συστήματα $k_1 = ay_1a^{-1}, k_2 = ay_2a^{-1}, ..., k_n = ay_na^{-1}$ και $l^1 = ax_1a^{-1}, l_2 = ax_2a^{-1}, ..., l_m = ax_ma^{-1}$ ως προς a και b αντίστοιχα. Θα πρέπει επομένως, στη G, τα συστήματα αυτά να λύνονται σχετικά αργά για σχετικά μεγάλο αριθμό από a και b.

Το πρόβλημα αυτό της ταυτόχρονης επίλυσης k εξισώσεων συζυγίας με κοινό a, ονομάζεται **k-Ταυτόχρονο Πρόβλημα Αναζήτησης Συζυγοποιητή**.

3.2 Γιατί οι Πλεξίδες;

Ας δούμε τώρα πως και γιατί το πρωτόκολλο που μόλις περιγράψαμε βάζει τις ομάδες πλεξίδων στο επίκεντρο του ενδιαφέροντος.

1. Υπάρχει μια κανονική μορφή, αυτή που ορίσαμε στο κεφάλαιο των πλεξίδων, η οποία προσφέρει δυο πλεονεκτήματα: α) επιτρέπει, όπως είδαμε την περιγραφή μιας πλεξίδας από μια διατεταγμένη n-άδα, για κάποιο φυσικό n, και επομένως τον εύκολο χειρισμό της πλεξίδας με υπολογιστή και β) δοσμένης μιας λέξης, η κανονική της μορφή υπολογίζεται γρήγορα.

2. Υπάρχουν γρήγοροι τρόποι να κάνουμε τις πράξεις ανάμεσα στα στοιχεία μιας ομάδας πλεξίδων.

3. Το Πρόβλημα της Αναζήτησης Συζυγοποιητή είναι δύσκολο στις ομάδες πλεξίδων, γεγονός στο οποίο μπορούμε να βασιστούμε για την ασφάλεια ενός κρυπτοσυστήματος. Επίσης υπάρχουν και άλλα δύσκολα προβλήματα που επιτρέπουν το σχεδιασμό και άλλων trapdoor συναρτήσεων.

4. Καθώς το n αυξάνει στο B_n, οι υπολογισμοί στις πλεξίδες γίνονται πιο δύσκολοι σε $O(nlogn)$, ενώ οι υπολογισμοί για το ′σπάσιμο′ των μονόδρομων συναρτήσεων φαίνεται να δυσκολεύουν σε $O(n!)$. Επομένως το n μπορεί να χρησιμοποιηθεί ως παράμετρος ασφαλείας.

Έτσι, εντατικοποιήθηκε η έρευνα γύρω από το θέμα και δεν άργησαν να φανούν τα επόμενα αποτελέσματα.

3.3 Το δεύτερο κρυπτοσύστημα

Μερικούς μήνες μετά τη δημοσίευση των Anshel, Anshel και Goldfeld, μια ομάδα κορεατών ερευνητών, αποτελούμενη από τους Ko, Lee, Cheon, Han, Kang, Park, παρουσίασε ([6]) στο Crypto 2000 το πρώτο κρυπτοσύστημα δημοσίου κλειδιού με χρήση ομάδων πλεξίδων.

Ορισμός 3.1 *Έστω μια B_n με $n = l + r$. Ονομάζουμε LB_l την υποομάδα της B_n, η οποία αποτελείται από αυτές τις πλεξίδες της B_n που σχηματίζονται μόνο από τις l πιο αριστερές κλωστές (δηλαδή οι r πιο δεξιές κλωστές σχηματίζουν την ταυτοτική I_r). Ανάλογα ονομάζουμε RB_r την υποομάδα της B_n, η οποία αποτελείται από αυτές τις πλεξίδες της B_n που σχηματίζονται μόνο από τις r πιο δεξιές κλωστές (δηλαδή οι l πιο δεξιές κλωστές σχηματίζουν την I_l).*

Πρόταση 3.1 *Για κάθε $a \in LB_l$ και κάθε $b \in RB_r$, ισχύει $ab = ba$.*

Απόδειξη: Είναι $a \in LB_l$ και $b \in RB_r$, άρα θα γράφονται ως λέξεις από τα $s_1, ..., s_{l-1}$ και $s_{l+1}, ..., s_{l+r}$ αντίστοιχα. Επομένως θα είναι $a = s_{i_1} s_{i_2} ... s_{i_p}$, με $i_1, i_2, ..., i_p \in \{1, ...l-1\}$ και $b = s_{j_1} s_{j_2} ... s_{j_q}$, με $j_1, j_2, ..., j_q \in \{l+1, ...l+r\}$. Όμως, ισχύει ότι $s_i s_j = s_j s_i$ για $|i-j| \neq 1$, οπότε $s_i s_j = s_j s_i$ για κάθε $i \in \{1, ...l-1\}$ και $j \in \{l+1, ...l+r\}$. Αυτό σημαίνει ότι πραγματοποιώντας pq διαδοχικές αντιμεταθέσεις, μπορούμε να μετατρέψουμε το $ab = s_{i_1} s_{i_2} ... s_{i_p} s_{j_1} s_{j_2} ... s_{j_q}$ σε $s_{j_1} s_{j_2} ... s_{j_q} s_{i_1} s_{i_2} ... s_{i_p} = ba$.

Η ιδέα τους βασίζεται στην δυσκολία του **Diffie-Helmann-Like Προβλήματος Συζυγίας**: Μας δίνεται μια τριάδα (x, y_1, y_2) από στοιχεία της B_n, $(n = l + r)$ τέτοια ώστε $y_1 = axa^{-1}$ και $y_2 = bxb^{-1}$ για κάποια κρυμμένα $a \in LB_l$ και $b \in RB_r$, και πρέπει να βρούμε το by_1b^{-1} $(= ay_2a^{-1} = abxa^{-1}b^{-1})$. Όπως αναφέρουν στο άρθρο, δεν είναι γνωστό εάν το Diffie-Helmann-Like Πρόβλημα Συζυγίας είναι ισοδύναμο με το Γενικευμένο Πρόβλημα Αναζήτησης Συζυγοποιητή. Μπορούμε να πούμε ότι δεν είναι δυσκολότερό του πάντως, αφού αν λύσουμε το δεύτερο μπορούμε να βρούμε κατευθείαν τα a και b του πρώτου και συνεπώς και το ζητούμενό του.

Κατά την υλοποίηση του αλγορίθμου θα μας ζητηθεί να επιλέξουμε το x, και για την ασφάλεια του θα απαιτείται να είναι δύσκολο το πρόβλημα για το x που επιλέξαμε. Χρειάζεται λίγη προσοχή εδώ, καθώς υπάρχουν 'κάκα' x για τα οποία το πρόβλημα μας είναι εύκολο. Μια 'κακή' πλεξίδα x έχει το εξής χαρακτηριστικό: είναι της μορφής $x_1 x_2 z$, όπου $x_1 \in LB_l, x_2 \in RB_r$ και η z είναι μια $(l+r)$-πλεξίδα που αντιμετατίθεται με την LB_l και με την RB_r. Στην περίπτωση αυτή, ενδεχόμενη διάσπαση της x στις συνιστώσες τις, $x_1 x_2 z$, θα ισοδυναμούσε με εύρεση του by_1b^{-1} χωρίς γνώση των a και b. Πράγματι:

$$by_1b^{-1} = baxa^{-1}b^{-1} = bax_1x_2za^{-1}b^{-1} = ax_1a^{-1}bx_2b^{-1}z = y_1y_2z.$$

Οι Fenn, Rolfsen και Zhu έδειξαν στο [29] ότι οι $l+r$-πλεξίδες που αντιμετατίθονται με την RB_r (ή την LB_l) είναι της μορφής $q_1 z$ (ή $q_2 z$ αντίστοιχα) modulo (up to) πλήρων περιστροφών Δ_l^2 και Δ_r^2 των αριστερών l κλωστών και των δεξιών r κλωστών. Η πιθανότητα, πάντως, να επιλέξουμε τυχαία μια τέτοια πλεξίδα, κανονικού μήκους q, είναι μικρή, περίπου $(l!r!/(l+r)!)^q$. Στο εξής, λέγοντας 'κατάλληλο' x, θα εννοούμε ότι δεν είναι αυτής της μορφής.

Σύμφωνα με το πρωτόκολλο που προτείνουν, η συμφωνία κλειδιού γίνεται με τον παρακάτω τρόπο:

1. Η Αλίκη με το Βασίλη επιλέγουν δυο ακέραιους r και l και μια κατάλληλη πλεξίδα $x \in B_{l+r}$, την οποία και δημοσιεύουν.

2. Κατόπιν η Αλίκη επιλέγει τυχαία μια πλεξίδα $a \in LB_l$, υπολογίζει το $y_1 = axa^{-1}$ και το στέλνει στο Βασίλη. Από τη μεριά του, ο Βασίλης επιλέγει τυχαία μια πλεξίδα $b \in RB_r$, υπολογίζει το $y_2 = bxb^{-1}$ και το στέλνει στην Αλίκη. Αυτό είναι και το μόνο επικίνδυνο στάδιο, όπου ανταλλάσσονται στοιχεία ικανά να δώσουν κάποια πληροφορία στον Εχθρό.

3. Έχοντας τα y_2 και y_1, η Αλίκη και ο Βασίλης υπολογίζουν τα $K = ay_2a^{-1}$ και $K = by_1b^{-1}$, αντίστοιχα.

Το ότι αυτές οι δυο λέξεις είναι ίσες προκύπτει λόγω της δυνατότητας αντιμετάθεσης των a και b:

$$ay_2a^{-1} = a(bxb^{-1})a^{-1} = (ab)x(a^{-1}b^{-1}) =$$

$$(ab)x(ba)^{-1} = (ba)x(ab)^{-1} = (ba)x(a^{-1}b^{-1}) = b(axa^{-1})b^{-1} = by_1b^{-1}.$$

Επομένως έχουν και οι δυο τώρα στην κατοχή τους το κοινό κλειδί K, χωρίς να έχουν καν θέσει σε κίνδυνο τη μυστικότητα των a και b.

Συμβολισμός: Η πράξη $x_1 \oplus x_2$ ανάμεσα σε δυο στοιχεία x_1, x_2 του $\{0,1\}^k$, γνωστή ως xor, δίνει το αποτέλεσμα x ως εξής: η συντεταγμένη i του x είναι 1 αν και μόνο αν τα ψηφία των x_1 και x_2 στη θέση i είναι διαφορετικά. Προφανώς, $x \oplus x = 0$ και $0 \oplus x = x$ για κάθε x. Επίσης η $\oplus$ είναι αντιμεταθετική και προσεταιριστική.

Επίσης, μπορούν να ανταλλάξουν με ασφάλεια τα μηνύματά τους με το εξής σύστημα:

1. Επιλέγουν μια hash συνάρτηση $H : B_{l+r} \longrightarrow \{0,1\}^k$, από την ομάδα πλεξίδων τους στο χώρο μηνυμάτων.

2. Η Αλίκη επιλέγει μια 'κατάλληλη' $(l+r)$-πλεξίδα $x \in B_{l+r}$ και μια $a \in LB_l$. Στη συνέχεια υπολογίζει το $y = axa^{-1}$ και δημοσιεύει το κλειδί (x, y). Το μυστικό κλειδί της είναι το a.

3. Έστω τώρα ότι ο Βασίλης έχει λάβει το (x, y) και θέλει να στείλει ένα μήνυμα $m \in \{0,1\}^k$ στη φίλη του. Επιλέγει τυχαία μια $b \in RB_r$, υπολογίζει τα $c = bxb^{-1}$ και $d = H(byb^{-1}) \oplus m$ και στέλνει στην Αλίκη το κρυπτοκείμενο (c, d).

4. Τέλος, η Αλίκη λαμβάνει, μέσω του ανασφαλούς πάντα καναλιού, το κρυπτοκείμενο (c, d), έχοντας δημοσιεύσει το κλειδί (x, y) που αντιστοιχεί στο μυστικό της κλειδί a. Αυτό που αρκεί να κάνει για να ανακτήσει το αρχικό κείμενο m είναι να υπολογίσει το $H(aca^{-1}) \oplus d = m$.

Ας κάνουμε κάποιες πράξεις για να βεβαιωθούμε ότι η Αλίκη θα αποκρυπτογραφήσει το σωστό μήνυμα:

$$H(aca^{-1}) \oplus d = H(abxb^{-1}a^{-1}) \oplus (H(byb^{-1}) \oplus m) =$$

$$(H(abxb^{-1}a^{-1}) \oplus H(baxa^{-1}b^{-1})) \oplus m =$$

$$(H(abxb^{-1}a^{-1}) \oplus H(abxb^{-1}a^{-1})) \oplus m = m.$$

3.3.1 Θεωρητική Ανάλυση

Πόσο καλό όμως είναι το κρυπτοσύστημα· Θα προσπαθήσουμε μια θεωρητική ανάλυσή του, κάνοντας κάποιες παρατηρήσεις, από όπου θα διαφανούν κάποια στοιχεία.

1. Ξεκινώντας, ας παρατηρήσουμε ότι οι μόνες είσοδοι στον αλγόριθμο του κρυπτοσυστήματος είναι οι τρεις πλεξίδες x, a, b που επιλέγουν η Αλίκη με τον Βασίλη. Επομένως, αυτές θα καθορίσουν και τις παραμέτρους που θα μας απασχολήσουν. Όπως φαίνεται και από τα θεωρήματα της παραγράφου 2.5, όταν μας δίνουν μια πλεξίδα $x \in B_n$ σε κανονική αριστερή μορφή, αυτό που μας ενδιαφέρει είναι το κανονικό μήκος $len(x)$ της x, καθώς και το n. Αυτές θα είναι και οι παράμετροι που θα μας απασχολήσουν στην ανάλυση. Για ευκολία, θα υποθέσουμε ότι $l = r = \frac{n}{2}$ και ότι $len(x) = len(a) = len(b) = p$.

2. Τώρα, έστω ότι έχουμε μια μετάθεση n στοιχείων και θέλουμε να την αναπαραστήσουμε με μια δυαδική ακολουθία (ακολουθία από bits). Πόσο θα είναι το μήκος της; Επειδή υπάρχουν $n!$ μεταθέσεις των n στοιχείων, μπορούμε να αντιστοιχίσουμε κάθε μετάθεση με ένα αριθμό από το 0 ως το $n! - 1$ (για παράδειγμα, διατάσσοντάς τις λεξικογραφικά). Άρα για κάθε n-μετάθεση θα χρειαστεί ένας αριθμός το πολύ $n!$, που είναι της τάξης του $exp(nlogn)$, επομένως θα είναι αρκετή μια δυαδική ακολουθία μήκους το πολύ $nlogn$. Συμπεραίνουμε τώρα ότι αν θελήσουμε να αναπαραστήσουμε σε δυαδική μορφή μια n-πλεξίδα με κανονικό μήκος p, θα χρειαστούμε μια ακολουθία μήκους το πολύ $pnlogn$.

3. Αν έχουμε δυο πλεξίδες $y_1, y_2 \in B_n$, τότε $len(y_1y_2) \leq len(y_1) + len(y_2)$, ενώ αν $y_1 \in LB_l$ και $y_2 \in RB_r$, τότε $len(y_1y_2) = max\{len(y_1), len(y_2)\}$ (το δεύτερο ισχύει διότι οι μεταθέσεις που εμφανίζονται στη μια πλεξίδα δρουν ανεξάρτητα από τις μεταθέσεις που εμφανίζονται στην άλλη. Επομένως μπορούμε να συμπτήσουμε δυο μεταθέσεις (μια από κάθε πλεξίδα) σε μια, γράφοντάς τις ως μετάθεση-γινόμενο. Π.χ. στη B_6, αν μια μετάθεση της αριστερής πλεξίδας είναι (123) και μια μετάθεση της δεξιάς

είναι (465), τότε μια μετάθεση του γινομένου μπορεί να είναι (123)(465)) .

4. Από την παρατήρηση 2, το μέγεθος του μυστικού κλειδιού a είναι $pl(logl)$ ή αλλιώς $p(\frac{n}{2})log(\frac{n}{2})$, το οποίο είναι της τάξης του $\frac{1}{2}pnlogn$.

5. Το μήκος του δημοσίου κλειδιού $y = axa^{-1}$ θα είναι, από την παρατήρηση 3, $len(y) = len(axa^{-1}) \leq len(ax) + len(a^{-1}) \leq len(a) + len(x) + len(a^{-1}) \leq 3p$. Ανάλογα, για το μήκος του byb^{-1}, πάλι από την παρατήρηση 3 θα έχουμε $len(byb^{-1}) = len(baxa^{-1}b^{-1}) = len((ba)x(a^{-1}b^{-1})) \leq len(ba) + len(x) + len(a^{-1}b^{-1}) \leq 3p$. Επομένως, το μέγεθος της αναπαράστασης του καθενός του καθενός τους θα είναι $3pnlogn$.

6. Όπως προκύπτει από το Θεώρημα 2.5, το πλήθος των n-πλεξίδων με κανονικό μήκος p είναι τουλάχιστον $(\lfloor\frac{n-1}{2}\rfloor!)^{2p}$ ή αλλιώς το εκθετικό του $log(\lfloor\frac{n-1}{2}\rfloor!)^{2p}$ ή αλλιώς $2plog(\lfloor\frac{n-1}{2}\rfloor!)$. Το τελευταίο είναι της τάξης του $2plog(\frac{n}{2}!)$ που είναι της τάξης του $2p\frac{n}{2}log\frac{n}{2}$ το οποίο με τη σειρά του είναι της τάξης του $pnlogn$. Έτσι, μπορούμε να πούμε ότι το μήκος της δυαδικής αναπαράστασης του $H(abxa^{-1}b^{-1})$ θα είναι της τάξης του $pnlogn$ (αυτό προκύπτει με το ίδιο σκεπτικό της παρατήρησης 2). Τώρα, το μήκος του κρυπτοκειμένου θα είναι ίσο με το μήκος του c συν το μήκος του d δηλαδή το μήκος του bxb^{-1} συν το μήκος του $H(byb^{-1}) \oplus m$. Από τα παραπάνω και από την παρατήρηση 5, το μέγεθος του κρυπτοκειμένου θα είναι το πολύ $4pnlogn$. Αυτό μεταφράζεται στο ότι με τη χρήση αυτού του κρυπτοσυστήματος, το κρυπτοκείμενο θα μεγεθύνεται σε σχέση με το αρχικό κατά ένα παράγοντα το πολύ 4.

7. Με δεδομένο ότι η hash συνάρτηση H υπολογίζεται γρήγορα, όλο το βάρος των υπολογισμών στο κρυπτοσύστημα πέφτει στον υπολογισμό των συζυγών πλεξίδων από τις αρχικές. Όπως προκύπτει από το Θεώρημα 2.2 και από τις προηγούμενες παρατηρήσεις, ο πιο αργός από αυτούς τους υπολογισμούς θα γίνεται σε $O(p^2nlogn)$, τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση. Επομένως, μπορούμε να πούμε ότι η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης του συστήματος είναι $O(p^2nlogn)$.

8. Η δυσκολία της άμεσης επίθεσης (brute force attack) για να υπολογίσουμε το a από το axa^{-1} (δηλαδή να λύσουμε το πρόβλημα της συζυγίας), είναι ανάλογο προς το $(l!)^p = (\frac{n}{2}!)^p$, που είναι της τάξης του $exp(\frac{1}{2}pnlogn)$.

Ακολουθεί ένας συνοπτικός πίνακας με τα χαρακτηριστικά:

Μπλοκ αρχικού κειμένου	$pnlogn \quad bits$
Μπλοκ κρυπτοκειμένου	$4pnnlogn \quad bits$
Ταχύτητα κρυπτογράφησης	$O(p^2nlogn)$ πράξεις
Ταχύτητα αποκρυπτογράφησης	$O(p^2nlogn)$ πράξεις
Επέκταση μηνύματος	4-1
Μήκος ιδιοτικού κλειδιού	$\frac{1}{2}pnlogn \quad bits$
Μήκος δημοσίου κλειδού	$3pnlogn \quad bits$
Δυσκολία της άμεσης επίθεσης	$\left(\frac{n}{2}!\right)^p \sim \exp\left(\frac{1}{2}pn\log n\right)$

3.4 Ένα Πρωτόκολλο Ομαδικής Συμφωνίας Κλειδιού

Εμπνευσμένοι από το πρωτόκολλο συμφωνίας κλειδιού που πρότειναν ο Ko και οι συνεργάτες του για το κρυπτοσύστημά τους, οι Lee, Lee και Lee παρουσίασαν φέτος (2003), με το [22] μια γενίκευσή του, ένα πρωτόκολλο ομαδικής συμφωνίας κλειδιού. Πρόκειται για ένα πρωτόκολλο που δίνει τη δυνατότητα να συμφωνήσουν ένα κοινό κλειδί παραπάνω από δυο άτομα, μια ομάδα ατόμων.

Πριν το περιγράψουμε θα δώσουμε κάποιους ορισμούς και συμβολισμούς.

Ορισμός 3.2 *1. Θα λέμε ότι ένα πρωτόκολλο συμφωνίας κλειδιού παρέχει* ***αποκλειστική αυθεντικοποίηση κλειδιού*** *(implicit key authentication) (του B προς τον A), αν παρέχει στον A τη βεβαιότητα ότι κανείς άλλος πλην του B δεν μπορεί να μάθει την τιμή ενός συγκεκριμένου κλειδιού. Ένα τέτοιο πρωτόκολλο λέγεται* ***authenticated key agreement protocol****.*

2. Θα λέμε ότι παρέχει ***επιβεβαίωση κλειδιού****, αν παρέχει στον A τη βεβαιότητα ότι κάθε συμβαλλόμενος στη διαδικασία έχει τελικά στην κατοχή του ένα συγκεκριμένο κλειδί.*

3. Θα λέμε ότι παρέχει ***ακεραιότητα κλειδιού****, αν παρέχει στον A τη βεβαιότητα ότι για τη δημιουργία του κλειδιού που έχει στα χέρια του έχουν συμβάλει οι επιθυμητοί συνδιαλεγόμενοι και μόνο.*

4. Θα λέμε ότι έχει ***perfect forward secrecy*** *αν η ενδεχόμενη αποκάλυψη (compromise) των κλειδιών διαρκείας δεν επιφέρει αποκάλυψη των προσωρινών κλειδιών (session keys).*

5. *Τέλος, θα λέγεται* ***ευάλωτο σε επίθεση γνωστού κλειδιού****, αν η αποκάλυψη προηγούμενων προσωρινών κλειδιών, επιτρέπει στον Εχθρό να αποκαλύψει μελλοντικά προσωρινά κλειδιά ή να προσποιηθεί ότι είναι κάποιος από τους συμβαλλόμενους στο πρωτόκολλο.*

Κατά την περιγραφή θα χρησιμοποιήσουμε τον παρακάτω συμβολισμό:

1. n: ο αριθμός των μελών της ομάδας
2. M_i: το i-στο μέλος της ομάδας
3. B_{l_i}: Η υποομάδα της B_l που προέρχεται από το πλέξιμο l_i συνεχόμενων κλωστών, από την $(l_1+...+l_{i-1}+1)$-οστή μέχρι την $(l_1+...+l_{i-1}+l_i)$-οστή (επεκτείνουμε τον ορισμό των RB_r και LB_l). Θα είναι $l_1 + ... + l_n = l$. Επιπλέον, οι B_{l_i} αντιμετατίθονται.
4. x_i: το μυστικό κλειδί διαρκείας του M_i στην B_{l_i}.
5. r_i: το τυχαίο μυστικό κλειδί του M_i στην B_{l_i}.
6. S_n: το ομαδικό κλειδί που μοιράζονται και τα n μέλη.

Ας δούμε τώρα πως δουλεύει το authenticated πρωτόκολλο ομαδικής συμφωνίας κλειδιού $(A-GKA)$ των τριών Lee.

1. Οι συναλλασσόμενοι επιλέγουν μια κατάλληλη πλεξίδα $a \in B_l$, ο καθένας ξεχωριστά επιλέγει τη μυστική του x_i και κατόπιν υπολογίζει το $x_i a x_{i-1}$. Οι δημόσιες τιμές του συστήματος είναι οι $l_1, ..., l_n, x_1 a x_1^{-1} ... x_n a x_n^{-1}$.
2. Το δεύτερο βήμα αποτελείται από n γύρους: Στον i-στο γύρο (για i από 1 ως $n-1$), ο M_i επιλέγει μια τυχαία $r_i \in B_{l_i}$ και στέλνει στον $i+1$ τις λέξεις $\{r_i ... \tilde{r}_j ... r_1 a r_1^{-1} ... \tilde{r}_j^{-1} ... r_i^{-1} | j = 1, ..., i\}$ (το $\sim$ πάνω από το τυχόν r_k σημαίνει ότι το r_k δεν εμφανίζεται στη συγκεκριμένη παράσταση), και την $r_i r_{i-1} ... r_1 a r_1^{-1} ... r_{i-1}^{-1} r_i^{-1}$.

   Στο n-στό γύρο, ο M_n επιλέγει ένα τυχαίο $r_n \in B_{l_n}$, υπολογίζει τα $k_{in} = x_n x_i a x_i^{-1} x_{n-1}$ για κάθε $i \in \{1, ..., n-1\}$ και στέλνει σε κάθε M_i το

   $\sigma_i = k_{in} r_n ... \tilde{r}_i ... r_1 a r_1^{-1} ... \tilde{r}_i^{-1} ... r_n^1 k_{in}^{-1}$.
3. Όταν ο M_i λαμβάνει το s_i, υπολογίζει το k_{in} και το $S_n(M_i)$=$r_i k_{in}^{-1} s_i k_{in} r_i^{-1}$.
   Τώρα, το κοινό κλειδί των M_i είναι το $S_n(M_i) = r_i k_{in}^{-1} s_i k_{in} r_i^{-1} = r_i r_n ... \tilde{r}_i ... r_1 a r_1^{-1} ... \tilde{r}_i^{-1} ... r_n^1 r_i^{-1}$ $= r_n ... r_i ... r_1 a r_1^{-1} ... r_i^{-1} ... r_n^1$. Το ίδιο υπολογίζει και ο M_n.

Όπως αποδεικνύουν στην εργασία τους, ισχύει το εξής

Θεώρημα 3.1 *Το $A-GKA$ είναι authenticated πρωτόκολλο συμφωνίας κλειδιού, παρέχει perfect forward security και είναι ανθεκτικό στις επιθέσεις γνωστού κλειδιού.*

3.5 Ψηφιακές Υπογραφές

Το 2002 δημοσιεύτηκε μια εργασία από τους Ko, Choi, Cho και Lee, στην οποία προτείνουν ένα νέο σχήμα ψηφιακής υπογραφής, το conjugacy signature scheme, όπως το ονομάζουν.

Για τη θεμελίωσή του εισάγουν δυο νέες παραλλαγές του προβλήματος συζυγίας:

Matching Conjugate Search Problem, MCSP: Σε μια ομάδα G, μας δίνεται ένα ζευγάρι συζυγών $x \in G$ και $x' \in G$ για τα οποία το πρόβλημα αναζήτησης συζυγίας είναι δύσκολο, και ένα $y \in G$. Ψάχνουμε να βρούμε ένα $y' \in G$, τέτοιο ώστε $y \sim y'$ και $xy \sim x'y'$

Matching Triple Search Problem, MTSP: Σε μια ομάδα G, μας δίνεται ένα ζευγάρι συζυγών $x \in G$ και $x' \in G$ για τα οποία το πρόβλημα αναζήτησης συζυγίας είναι δύσκολο και ένα $y \in G$. Ψάχνουμε μια τριάδα $(\alpha, \beta, \gamma) \in G \times G \times G$ τέτοια ώστε $\alpha \sim x, \beta \sim \gamma \sim y, \alpha\beta \sim xy$ και $\alpha\gamma \sim x'y$. Κατόπιν, αποδεικνύουν το παρακάτω θεώρημα:

Θεώρημα 3.2 *Σε μια μη αντιμεταθετική ομάδα G, το MCSP είναι εύκολο (feasible) αν και μόνο αν το MTSP είναι εύκολο.*

Η βασική τους ιδέα, για τη θεμελίωση του σχήματος, είναι να χρησιμοποιήσουν το γεγονός ότι υπάρχει ένα μεγάλο υπολογιστικό κενό ανάμεσα στα δυο βασικά προβλήματα συζυγίας: Για την Εύρεση Συζυγίας δεν υπάρχει γρήγορος αλγόριθμος, ενώ για την Απόφαση Συζυγίας υπάρχει.

Για τον αλγόριθμο υπογραφής επιλέγουμε μια hash συνάρτηση $h : \{0,1\}^* \rightarrow G$. Όπως συνήθως, η Αλίκη θέλει να στείλει ένα υπογεγραμμένο μήνυμα στο Βασίλη. Για τη δημιουργία των κλειδιών και την υπογραφή του m κάνει τα εξής:

1. Επιλέγει ένα ζευγάρι συζυγών στοιχείων (x, x') για το οποίο το πρόβλημα αναζήτησης συζυγίας είναι δύσκολο.

2. Δημοσιεύει το (x, x') και κρατά σαν μυστικό κλειδί το a για το οποίο $x' = a^{-1}xa$.

3. Επιλέγει τυχαία ένα $b \in G$ και κατόπιν θέτει $\alpha = b^{-1}xb$ και $y = h(m||\alpha)$. Σαν υπογραφή s στέλνει την τριάδα $s = (\alpha, \beta, \gamma)$, όπου $\beta = b^{-1}yb$ και $\gamma = b^{-1}aya^{-1}b$.

Τώρα, ο Βασίλης αποδέχεται την υπογραφή s αν και μόνο αν $\alpha \sim x, \beta \sim \gamma \sim y, \alpha\beta \sim xy$ και $\alpha\gamma \sim x'y$.

Παρατηρείστε ότι μέχρι τώρα δεν έχει γίνει αναφορά σε ομάδες πλεξίδων. Ο αλγόριθμος αυτός είναι η βασική ιδέα, η οποία μπορεί να εφαρμοστεί σε κάθε ομάδα όπου δεν υπάρχει γρήγορος αλγόριθμος για την Εύρεση Συζυγίας, ενώ για την Απόφαση Συζυγίας υπάρχει. Για την εφαρμογή του αλγορίθμου στις ομάδες πλεξίδων, κάνουν κάποιες παρατηρήσεις για την ασφάλειά του, και τον μετατρέπουν κατάλληλα ώστε να τη βελτιώσουν.

Ο αλγόριθμος που προτείνουν για να ελέγξει ο Βασίλης τις απαιτούμενες συζυγίες είναι πιθανοτικός και ονομάζεται τεστ των πολυωνύμων Alexander. Βασίζεται στη σύγκριση των πλεξίδων, μέσω των εικόνων τους, όπως αυτές προκύπτουν από τη απεικόνιση Burau, και συγκεκριμένα στη σύγκριση των πολυωνύμων Alexander των δυο πλεξίδων. (Τα πολυώνυμα Alexander ορίζονται ως εξής: έστω $\Phi(b)$ η εικόνα της b μέσω της απεικόνισης Burau, τότε το πολυώνυμο Alexander της b είναι το $P_b(t) = det(\Phi(b) - I)$.) Ελέγχει πιθανοτικά την ισότητα των πολυωνύμων, συγκρίνοντας τις τιμές τους σε διάφορα σημεία, και αποδέχεται τη συζυγία αν και μόνο αν τα βρει ίσα. Η πιθανότητα αποτυχίας του αλγορίθμου μπορεί να γίνει όσο μικρή θέλουμε με την κατάλληλη επιλογή παραμέτρων. Η ταχύτητά του είναι $O(lrn^3)$, όπου l το κανονικό μήκος της μεγαλύτερης πλεξίδας και r το πλήθος των δοκιμών που εκτελεί (αύξηση του r μειώνει εκθετικά την πιθανότητα λάθους του αλγορίθμου).

3.6 Πρωτόκολλα Ταυτοποίησης

Τα πρώτα πρωτόκολλα ταυτοποίησης παρουσιάστηκαν το 2002, από τους Sibert, Dehornoy, και Girault. Στην εργασία τους παρουσιάζουν τρία πρωτόκολλα:

Το πρωτόκολλο I είναι εμπνευσμένο από το κρυπτοσύστημα της παραγράφου 3.3, βασίζεται στη δυσκολία του Diffie-Helmann-Like Προβλήματος Συζυγίας και χρησιμοποιεί τις υποομάδες LB_l και RB_r που ορίσαμε. Είναι σχεδιασμένο για άρτιο n και για $l = r = 1/2$.

Το πρωτόκολλο I αποτελείται από τα ακόλουθα βήματα:

1. Η Αλίκη και ο Βασίλης επιλέγουν μια πλεξίδα b στην B_n για την οποία το Diffie-Helmann-Like Πρόβλημα Συζυγίας είναι δύσκολο.

2. Η Αλίκη επιλέγει μια μυστική πλεξίδα s στην $LB_{n/2}$, που αποτελεί το μυστικό κλειδί της, και δημοσιεύει το $b' = sbs^{-1}$. Το δημόσιο κλειδί είναι το (b, b').

3. Ο Βασίλης επιλέγει μια πλεξίδα $r \in RB_{n/2}$, και στέλνει στην Αλίκη ως ερώτηση-πρόκληση την $x = rbr^{-1}$.

4. Η Αλίκη στέλνει στο Βασίλη ως απάντηση την $y = H(sxs^{-1})$, και ο Βασίλης δέχεται την ταυτοποίηση αν και μόνο αν $y = H(rbr^{-1})$.

Αποδεικνύουν ότι:

Πρόταση 3.2 *Το πρωτόκολλο I είναι μια perfectly honest-verifier zero knowledge interactive proof of knowledge του s.*

Το πρωτόκολλο II βασίζεται στο Πρόβλημα Αναζήτησης Συζυγίας και περιγράφεται ως εξής:

1. Η Αλίκη και ο Βασίλης επιλέγουν μια πλεξίδα b στην B_n για την οποία το Diffie-Helmann-Like Πρόβλημα Συζυγίας είναι δύσκολο.

2. Η Αλίκη επιλέγει μια μυστική πλεξίδα s στην B_n, που αποτελεί το μυστικό κλειδί της, και δημοσιεύει το $b' = sbs^{-1}$. Το δημόσιο κλειδί είναι το (b, b').

3. Η Αλίκη επιλέγει μια τυχαία πλεξίδα r και στέλνει στο Βασίλη τη $x = rbr^{-1}$.

4. Ο Βασίλης στέλνει ένα τυχαίο bit ε στην Αλίκη.

5. α. Για ε=0, η Αλίκη στέλνει στο Βασίλη την $y = r$ και αυτός ελέγχει εάν $x = yby^{-1}$.

   β. Για ε=1, η Αλίκη στέλνει στο Βασίλη την $y = rs^{-1}$ και αυτός ελέγχει εάν $x = yb'y^{-1}$.

6. Εκτελούμε τα βήματα 2-4 k φορές, όπου k ένα πολυώνυμο του μήκους των λέξεων (braid specifiers) των πλεξίδων.

Για το II αποδεικνύουν την

Πρόταση 3.3 *Όποτε η κατανομή πιθανότητας της r στο βήμα 3 είναι right-invariant, το πρωτόκολλο II είναι μια zero knowledge interactive proof of knowledge του s.*

Το πρωτόκολλο αυτό μπορεί να εφαρμοστεί για οποιαδήποτε ομάδα στην οποία το πρόβλημα αναζήτησης συζυγίας είναι δύσκολο.

Το III είναι παρόμοιο με το II, αλλά επιπλέον περιέχει και το πρόβλημα της ρίζας.

3.7 Επιθέσεις στην κρυπτογραφία πλεξίδων

Θα αναφέρουμε τις βασικότερες προσπάθειες επίθεσης που έχουν γίνει και θα περιγράψουμε δυο από αυτές.

3.7.1 Επίθεση Μήκους στο Πρόβλημα Συζυγίας

Η ιδέα για αυτού του είδους την επίθεση, παρουσιάστηκε από τους J.Hughes και A. Tannenbaum, σε ένα άρθρο τους ([9]), το 2000. Στοχεύει στο πρόβλημα της συζυγίας, και συγκεκριμένα στη μορφή με την οποία εμφανίζεται στο Commutator key-agreement protocol, δηλαδή το k-Ταυτόχρονο Πρόβλημα Συζυγίας. Ως εκ τούτου, αυτό είναι και το κρυπτοσύστημα που κυρίως πλήχθηκε.

Η επίθεση βασίζεται στο γεγονός ότι στις πλεξίδες υπάρχει μια κανονική μορφή, με βάση την οποία μπορεί να οριστεί μια συνάρτηση μήκους (εξ ου και το όνομα της). Η ιδέα είναι απλή: Ξέρουμε τα δημόσια x_i και $l_i = bx_ib^{-1}$, και θα θέλαμε να βρούμε το b. Θα χρησιμοποιήσουμε το γεγονός ότι όταν έχουμε μια συνάρτηση μήκους, l, κατά κανόνα θα ισχύει ότι $l(x_i) < l(bx_ib^{-1})$, και στην ουσία θα προσπαθήσουμε να αποκαλύψουμε ένα-ένα τους παράγοντες του b. Έστω ότι είναι $b = g_1...g_k$, όπου $g_i \in \{y_1, ...y_n, y_1^{-1}, ..., y_n^{-1}\}$. Ορίζουμε μια γραμμική διάταξη σε όλες τις πιθανές n-άδες από μήκη, και επιλέγουμε το $g \in \{y_1, ...y_n, y_1^{-1}, ..., y_n^{-1}\}$ για το οποίο το $\langle l(gb^{-1}x_1bg^{-1}), ..., l(gb^{-1}x_nbg^{-1})\rangle$ ελαχιστοποιείται, με βάση τη διάταξη που ορίσαμε. Με κάποια μη μηδενική πιθανότητα, το g θα είναι ίσο με το g_1, ή το b μπορεί να γραφτεί ως γινόμενο από k ή λιγότερους γεννήτορες, με πρώτο το g. Έτσι, το $g^{-1}b$ ισούται με ένα γινόμενο μικρότερου μήκους, και διαδοχικές τέτοιες απαλοιφές θα μας δώσουν, τελικά, όλα τα g_i.

Βασικό κλειδί για την επίθεση, είναι η κατάλληλη επιλογή της συνάρτησης μήκους, l, για την οποία η εργασία δεν περιείχε κάποια μελέτη. Μια πιο ολοκληρωμένη εργασία παρουσιάστηκε το 2002 από τους Garber, Kaplan, Teicher, Tsaban και Vishne. Εκεί, οι συγγραφείς προτείνουν τρεις υποψήφιες συναρτήσεις μήκους, οι δυο εκ των οποίων νέες, και κάνουν μια εκτενή πειραματική μελέτη της αποτελεσματικότητας της κάθε μιας τους. Επίσης, προτείνουν τρόπους για τη βελτίωση του αλγόριθμου της επίθεσης.

Σε μια ανανεωμένη έκδοση του Commutator key-agreement protocol ([2]), οι Anshel, Anshel, Fisher και Goldfeld πρότειναν το 2001, την προσθήκη ενός Εξαγωγέα Κλειδιών (Key Extractor). Πρόκειται για μια συνάρτηση, η οποία σε κάθε πλεξίδα της B_n (και ειδικότερα αυτή στην οποία καταλήγουν η Αλίκη με το Βασίλη) αντιστοιχίζει ένα ζευγάρι, αποτελούμενο από μια μετάθεση και ένα πίνακα με στοιχεία από ένα πεπερασμένο σώμα. Όμως, την επόμενη χρονιά, οι Lee και Lee δημοσίευσαν μια επίθεση ([11]), η οποία εντοπίζει κάποιες αδυναμίες στον Εξαγωγέα Κλειδιών.

3.7.2 Επιθέσεις με το Summit σύνολο.

Με βάση τον αλγόριθμο των Franco και Meneses για την επίλυση του προβλήματος συζυγίας, οι Lee και Lee πρότειναν και μια επίθεση στο βασικό πρόβλημα

του ίδιου κρυπτοσυστήματος. Τον αλγόριθμό τους βελτίωσε λίγο αργότερα ο Meneses. Μετά από αυτή την επίθεση, η ασφάλεια του Commutator key-agreement protocol, μειώνεται πιο πολύ.

3.7.3 Επιθέσεις προβολής

Η φιλοσοφία αυτού του τύπου των επιθέσεων είναι να αποσπάσουν πληροφορίες, προβάλλοντας τις ομάδες πλεξίδων στις ομάδες πηλίκα τους. Από μόνη της μια τέτοια επίθεση δεν είναι ιδιαίτερα αποτελεσματική ενάντια σε υπολογιστικά προβλήματα, μπορεί να είναι αποτελεσματική, όμως, όταν πρόκειται για πρόβλημα απόφασης. Με μια επίθεση προβολής ([30]), οι Gennaro και Micciancio έπληξαν μια ψευδοτυχαία γεννήτρια που είχαν προτείνει οι Lee, Lee και Hahn ([7]). Τέτοιου τύπου είναι και η επίθεση που δημοσίευσαν πρόσφατα οι Hofheinz και Steinwandt ([25]).

3.7.4 Επιθέσεις Αναπαράστασης

Η πιο δημοφιλής ίσως κατηγορία επιθέσεων, περιλαμβάνει επιθέσεις που βασ΄ιζονται στην αναπαράσταση των πλεξίδων από πίνακες, και κατόπιν στην επίθεση με τη βοήθεια των γνωστών ιδιοτήτων των πινάκων. Θα επιχειρήσουμε να περιγράψουμε μια από αυτές, τη γραμμική αλγεβρική επίθεση του Hughes στο Commutator key-agreement protocol.

Η γραμμική αλγεβρική επίθεση του Hughes

Η επίθεση αυτή παρουσιάστηκε από τον Hughes στο [10], και απευθήνεται στο commutator key agreement protocol. Σημαντικό χαρακτηριστικό της είναι ότι το κρίσιμο επιχείρημά της δεν είναι θεωρητικό. Αντίθετα, βασίζεται σε εμπειρικές παρατηρήσεις. Η βασική ιδέα είναι ότι μπορεί κάποιος να υπολογίσει, τις περισσότερες φορές, τα a και b (και κατ' επέκταση το $[a, b]$), με το να απεικονίσει σε ομάδες πινάκων, μέσω του μετασχηματισμού Bureau, τις υποομάαδες και τις συζυγείς τους, να υπολογίσει τους συζυγοποιητές με γραμμική άλγεβρα, και κατόπιν να γυρίσει στην αρχική μορφή. Ας δούμε όμως αναλυτικότερα το σκεπτικό του Hughes. Έστω ότι βρισκόμαστε στη B_n και έστω $s = s_{i_1}...s_{i_m}$ μια λέξη της. Υπολογίζουμε τον πίνακα $\beta(s)$, δηλαδή την εικόνα της s μέσω του μετασχηματισμού Bereau. Αυτό που παρατηρεί είναι ότι μπορούμε να 'διαβάσουμε' εύκολα τα s_{i_j} από τον $\beta(s)$: Έστω i η μικρότερή από όλες τις στήλες στις οποίες εμφανίζεται η μικρότερη, σε ολόκληρο τον πίνακα, θετική δύναμη του t. Τότε είτε $s_{i_n} = s_i$, είτε η γραφή αυτή της s μπορεί να μετατραπεί, μέσω των $s_i s_j = s_j s_i$ αν $|i - j| > 2$ και $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$, σε μια ισοδύναμη γραφή, που θα έχει σαν τελευταίο όρο το s_i. Με αφετηρία αυτή

την παρατήρηση, πρότεινε τα παρακάτω βήματα για την απόδοση μιας πλεξίδας, δοσμένης στη Bereau μορφή της, σε λέξη από γεννήτορες:

1. Βρες την πρώτη στήλη i με τη μεγαλύτερη θετική δύναμη
2. Αν $i = n$, τότε αποτυχία.
3. Πολλαπλασίασε από αριστερά με s_i^{-1}.
4. Επανέλαβε τα βήματα 1-3 μέχρι να μην υπάρχουν πια θετικοί εκθέτες.
5. Αν ο πίνακας είναι ο μοναδιαίος, τότε επιτυχία.
6. Αν η λίστα των πιθανών στοιχείων είναι πολύ μεγάλη, τότε αποτυχία.
7. Αντέστρεψε τον πίνακα και τη λίστα των απομακρυσμένων γεννητόρων και επανέλαβε τα βήματα 1-6.

Για να δει πόσο αποδοτικός είναι ο αλγόριθμος, τον έτρεξε σε 50 λέξεις, από τις οποίες οι 48, δηλαδή ποσοστό 96%, ανακτήθηκε σωστά. Θεωρεί καλό αυτό το ποσοστό, και χρησιμοποιεί τη μέθοδο για να διαμορφώσει την επίθεσή του, η οποία λειτουργεί ως εξής:

Έστω ότι θέλει να βρει το στοιχείο a της Αλίκης. Έχουν δημοσιευτεί τα $y_1, y_2, ..., y_n$ από το Βασίλη, και τα $k_1 = ay_1a^{-1}, k_2 = ay_2a^{-1}, ..., k_n = ay_na^{-1}$ από την Αλίκη. Βρίσκει την Bereau μορφή καθεμιάς από αυτές τις $2n$ λέξεις, και με γραμμική άλγεβρα λύνει το σύστημα $k_ia = ay_i$, $i = 1, ...n$. Για την επίλυση αποδεικνύει πρώτα τα εξής δυο λήμματα:

Λήμμα 3.1 *Κάθε πίνακας στην εικόνα μιας ομάδας πλεξίδων, μέσω του μετασχηματισμού Bereau, έχει στήλες που όλες αθροίζονται στο 1.*

Λήμμα 3.2 *Κάθε πίνακας $[a_{ij}]$ στην εικόνα μιας ομάδας πλεξίδων, μέσω του μετασχηματισμού Bereau, ικανοποιεί τη συνθήκη* $\sum_{i=1}^{n} a_{ij}t^i = t^j$ *(για* j = 1, ..., n*).*

Επιπλέον κάνει και κάποιες παρατηρήσεις για τη βελτίωση της ταχύτητας επίλυσης του συστήματος, που είναι και η βασική αδυναμία της επίθεσης.

Τελικό συμπέρασμα του Hughes είναι ότι μια κλάση κλειδιών είναι ευπρόσβλητη στην επίθεση, οπότε οι συνιστώμενες από τους δημιουργούς παράμετροι (στο [1]) θα πρέπει να επαναπροσδιοριστούν.

4 Το κρυπτοσύστημα πλεξίδων και οι ... άλλοι

Μήπως όλα όσα είπαμε μέχρι τώρα δεν αξίζουν; Μήπως η όλη ιστορία πρόκειται απλά για σαπουνόφουσκες; Μήπως ακόμα και αν τελικά το κρυπτοσύστημα πλεξίδων καταφέρει να αποδειχτεί ασφαλές, μείνει τελικά στο ράφι;

Σε αυτό το κεφάλαιο θα παρουσιάσουμε τους βασικούς ανταγωνιστές του, και τις συγκρίσεις που έχουν γίνει.

4.1 Οι ... άλλοι

Πρόκειται, βέβαια, για τα υπόλοιπα αξιόλογα κρυπτοσυστήματα δημοσίου κλειδιού, τρία στον αριθμό. Πρώτο και καλύτερο, ο 'βασιλιάς ' του χώρου, το RSA. Έχουμε ήδη αναφερθεί σε αυτό, θα προσθέσουμε μόνο ότι το σύνηθες μέγεθος κλειδιών που χρησιμοποιούνται στο RSA είναι 1024 bits. Θα αποτελέσει κατά κάποιο τρόπο το μέτρο σύγκρισης σε όσα αναφερθούν. Το δεύτερο είναι πιο καινούριο, δεν είναι τόσο ευρέως διαδεδομένο όσο το RSA, έχει γίνει όμως αρκετή μελέτη πάνω του. Πρόκειται για το ECC, το κρυπτοσύστημα ελλειπτικών καμπυλών. Το τρίτο είναι ένα καινούριο κρυπτοσύστημα, όπως και το κρυπτοσύστημα πλεξίδων, και το όνομα του είναι NTRU.

4.1.1 Το ECC

Το ECC βασίζεται στη δυσκολία του προβλήματος διακριτού λογαρίθμου στις ελλειπτικές καμπύλες. Τα μέχρι τώρα δεδομένα δείχνουν ότι πλεονεκτεί απέναντι στο RSA, κυρίως λόγω ταχύτητας και μικρότερων απαιτήσεων μνήμης.

Για την εφαρμογή, η Αλίκη και ο Βασίλης επιλέγουν μια ελλειπτική καμπύλη E πάνω από κάποιο σώμα, και ένα σημείο Q της καμπύλης. Δεν τους ενδιαφέρει η μυστικότητα των παραπάνω.

Για τη δημιουργία του κλειδιού, Η Αλίκη επιλέγει μυστικά ένα τυχαίο ακέραιο k_A και υπολογίζει το σημείο $P_A = k_A Q$, το οποίο στέλνει στο Βασίλη. Παρομοίως, ο Βασίλης επιλέγει μυστικά ένα τυχαίο k_B, υπολογίζει το $P_B = k_B Q$, και το στέλνει στην Αλίκη. Το κοινό κλειδί είναι το $P = k_A k_B Q$. Έστω τώρα ότι η Αλίκη θέλει να του στείλει ένα μήνυμα M, που είναι ένα σημείο της ελλειπτικής καμπύλης. Επιλέγει ένα τυχαίο $l \in Z_n$ και υπολογίζει τις τιμές $S_1 = lP_B$ και $S_2 = M + lP$. Το κρυπτογραφημένο κείμενο θα είναι το ζεύγος των σημείων της ελλειπτικής καμπύλης (S_1, S_2). Όταν ο Βασίλης λάβει το μήνυμα (S_1, S_2), ανακτά το M υπολογίζοντας το $S_2 - k_A S_1 = M$.

Χονδρικά υπολογίζεται ότι η ασφάλεια του ECC με κλειδιά των 112 bit είναι όση και του RSA με κλειδιά 512 bit, του ECC με κλειδιά των 168 bit είναι όση και του RSA με κλειδιά 1024 bit και του ECC με κλειδιά των 196 bit είναι όση και του RSA με κλειδιά μεγέθους 2048 bit.

4.1.2 Το NTRU

Το NTRU παρουσιάστηκε αρχικά από τον Jeffrey Hoffstein στο CRYPTO ′96, δημοσιεύτηκε το 1998 στο [24] και από τις 24 Ιουλίου του 2000 αποτελεί πατέντα της NTRU Cryptosystems, Inc. Χρησιμοποιεί άλγεβρα πολυωνύμων για την κρυπτογράφηση και στοιχειώδη θεωρία πιθανοτήτων για την αποκρυπτογράφηση. Η ασφάλειά του βασίζεται στην ανεξαρτησία της αναγωγής modulo p, καθώς και στο πειραματικά παρατηρημένο γεγονός, ότι στα περισσότερα lattices είναι δύσκολο να βρει κανείς πολύ μικρά διανύσματα. Η κρυπτογράφηση ή η αποκρυπτογράφηση ενός μπλοκ κειμένου μήκους N, απαιτεί χρόνο $O(N)$, ενώ για το ίδιο κείμενο, τα κλειδιά θα έχουν μήκος $O(N)$.

4.2 Τα συγκριτικά τεστ

Γενικά είναι αρκετά δύσκολο να συγκρίνει κανείς αυτά τα κρυπτοσυστήματα, καθώς παρουσιάζονται κάποια προβλήματα. Το RSA έχει μελετηθεί πολύ και ξέρουμε καλά τα επίπεδα ασφαλείας του. Επίσης, οι αλγόριθμοι υλοποίησής του έχουν βελτιστοποιηθεί πολύ. Για το ECC έχουν μελετηθεί καλά τα επίπεδα ασφαλείας, δεν έχει γίνει όμως καλή βελτιστοποίηση των αλγορίθμων του. Τα άλλα δυο είναι καινούρια και μπορούμε να δώσουμε μόνο προσεγγιστικές τιμές. Το αποτέλεσμα είναι να μην είναι απόλυτα 'δίκαιες ' οι παράμετροι στα τεστ. Άλλο πρόβλημα είναι το ότι το μέγεθος του μπλοκ στο κρυπτοσύστημα πλεξίδων εξαρτάται από τη hush συνάρτηση. Παρόλα αυτά, μπορούμε να πάρουμε μια γενική εικόνα.

Σύγκριση 1

Τα αποτελέσματα που θα παραθέσουμε εδώ, παρουσιάζονται στο [20] από τους Karu και Loikkanen, το 2001. Αυτό σημαίνει ότι κάποια πράγματα μπορεί να έχουν αλλάξει στα ενδιάμεσα δυο χρόνια. Η υλοποίηση των αλγορίθμων έγινε με C^{++} και οι απαιτήσεις σε μνήμη κρατήθηκαν χαμηλές. Οι συγγραφείς θεωρούν ότι το NTRU 263 και το κρυπτοσύστημα πλεξίδων (BCG) με $n = 48$ και κανονικά μήκη $len(a) = len(b) = len(x) = 2$, δίνουν ασφάλεια ανάλογη αυτής του RSA 1024. Τα τεστ για το ECC και το NTRU έγιναν σε ένα Celeron 500MHz που έτρεχε Linux, για το κρυπτοσύστημα πλεξίδων σε ένα Celeron 533MHz, ενώ για RSA 1024 σε ένα PentiumII 400MHz με Windows NT. Τα αποτελέσματα φαίνονται στον παρακάτω πίνακα:

	$RSA1024$	$ECC168$	$NTRU263$	BGC
Επέκταση μηνύματος	$1-1$	$2-1$	$4,5-1$	$4-1$
Μπλοκ αρχικού κειμένου $(bits)$	1024	160	416	1088
Δημοσίο κλειδί $(bits)$	1024	169	1841	1000
Δημιουργία κλειδιού (ms)	1432	65	$19,8$	$8,5$
Κρυπτογράφηση (ms)	$4,28$	140	$1,9$	$29,8$
Αποκρυπτογράφηση (ms)	$48,5$	67	$3,5$	$14,9$

Σύγκριση 2

Τα αποτελέσματα εδώ χρονολογούνται επίσης από το 2001. Δεν υπάρχουν πολλές λεπτομέρειες, απλώς θα αναφέρουμε την προέλευση των αποτελεσμάτων: για το RSA και το ECC από την ιστοσελίδα Weidai benchmark se Celeron 850MHz, για το NTRU από την ιστοσελίδα του NTRU και για το κρυπτοσύστημα πλεξίδων από τον Dr. Cha σε PentiumIII 866MHz. Τα αποτελέσματα φαίνονται στον παρακάτω πίνακα (τα αποτελέσματα του πρώτου σε millisecond/πράξη, για το κρυπτοσύστημα πλεξίδων n=100,p=15,):

	RSA1024	ECC168	NTRU263	BGC
Κρυπτογράφηση (ms/op)	0,32	14,27	0,27	13,4
Κρυπτογράφηση (Kbyte/sec)	396	1,472	996,79	146,53
Αποκρυπτογράφηση (ms/op)	10,23	25,72	0,64	10,4
Αποκρυπτογράφηση (Kbyte/sec)	12,52	0,817	425,80	188,13

Επίλογος

Είδαμε, αλλού συνοπτικά και αλλού αναλυτικά κάποια από τα σημαντικότερα βήματα που έχουν γίνει γύρω από τη χρήση των ομάδων πλεξίδων στην κρυπτογραφία. Ο χώρος είναι ζεστός: όσο γράφονταν αυτή η εργασία, αρκετά νέες εργασίες παρουσιάστηκαν. Επίσης τα πράγματα είναι κάπως ρευστά: παρουσιάζονται απόψεις και υπέρ αλλά και κατά της χρήσης των πλεξίδων. Κάποια από αυτά που δημοσιεύονται σήμερα είναι πιθανό να αποδειχθούν λάθος αύριο. Είναι μάλλον νωρίς για συμπεράσματα, θα ευχηθούμε όμως να βγουν αληθινές οι προβλέψεις των αισιόδοξων. Ο χρόνος θα δείξει.

Αναφορές

[1] *An algebraic method for public-key cryptography*, I. Anshel, M. Anshel & D. Goldfeld, Math. Research Letters 6 (1999) 287-291.

[2] *New key agreement schemes in braid group cryptography*, I. Anshel, M. Anshel, B. Fisher & D. Goldfeld, RSA 2001.

[3] *Theory of braids*, E. Artin, Ann of Math. 48 (1947) 101-126

[4] *A new approach to the word problem in the braid groups*, J. Birman, K.H. Ko & S.J. Lee Advances in Math 139-2 (1998) 322-353.

[5] *A fast method for comparing braids*, P. Dehornoy, Advances in Math. 125 (1997) 200-235.

[6] *New public-key cryptosystem using braid groups*, K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang & C. Park, Crypto 2000 166-184.

[7] *Pseudorandomness from braid groups*, E.K. Lee, S.J. Lee & S.G. Hahn, Crypto 2001.

[8] *Algorithms for positive braids*, E.A. Elrifai & H.P. Morton, Quart. J, Math. 20 (1994) 479-497.

[9] *Length-based attacks for certain group based encryption rewriting systems*, J. Hughes, A. Tannenbaum, 2000 (Published in SECI 02).

[10] *A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem*, Jim Hughes, ACISP 2002.

[11] *Potential Weaknesses of the Commutator Key Agreement Protocol Based on Braid Groups*, Sang Jin Lee, Eonkyung Lee, EUROCRYPT 2002.

[12] *Reaction Attacks on Public Key Cryptosystems Based on the Word Problem*, Maria Isabel Gonzalez Vasco & Rainer Steinwandt, eprint 2002/139.

[13] *Length-based conjugacy search in the Braid group*, D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, math.GR/0209267.

[14] *Entity Authentication Schemes Using Braid Word Reduction*, H. Sibert, P. Dehornoy and M. Girault, eprint 2002/187.

[15] *Assessing security of some group based cryptosystems*, Vladimir Shpilrain, eprint 2003/123.

[16] *Πλεξίδες και κόμβοι*, Alexey Sosinsky, Quantum, Μάρτιος -Απρίλιος 1995

[17] *Algorithmic problems in the braid group*, Elie Feder, 2003 (dissertation)

[18] *Cryptosystem using braids*, S. Lemieux, P. Yap, 2002.

[19] *Overview of the cryptosystems using braid groups*, S. Lee, E. Lee, 2001

[20] *Practical comparison of Fast Public-key Cryptosystems* (Priit Karu, Jonne Loikkanen, 2001)

[21] *Handbook of Applied Cryptography*, A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, Inc. 1997

[22] *An Authenticated Group Key Agreement Protocol on Braid groups*,H-K. Lee, H-S. Lee, Y-R. Lee

[23] *New Signature Scheme Using Conjugasy Problem*, K.Ko, D. Choi, M. Cho J. Lee, e-print, 2002

[24] *NTRU: A ring based public key cryptosystem*, J. Hoffstein, J. Pipher, J. Silverman, Lecture Notes in Computer Science 1423, 267-288, 1998.

[25] *A Practical Attack on Some Braid Group Based Cryptographic Primitives*, D. Hofheinz, R. Steinwandt, PKC 2003.

[26] *Theorie der Zopfe*, E. Artin, Hamburger Abhandlungen, vol.4

[27] *Combinatorial Group Theory*, C. Miller, 2002

[28] *The algebraical braid group*, F. Bohnenblust, An. of Math. vol. 48, 1947

[29] *Centralizers in the braid group and singular braid monoid*, R. Fenn, D. Rolfsen, J. Zhu, Enseign. Math. (2) 42 ((1996), no. 1-2, 75-96.

[30] *Cryptanalysis of a pseudorandom generator based on braid groups*, R. Gennaro, D. Micciancio.