ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΑΠΟΔΕΚΤΗΣ ΔΙΓΡΑΜΜΙΚΗΣ ΑΠΕΙΚΟΝΙΣΗΣ WEIL ΣΕ ΠΡΩΤΟΚΟΛΛΑ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΑΝΔΡΕΑΣ ΤΣΙΛΙΦΩΝΗΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΝΟΕΜΒΡΙΟΣ 2004

ΠΕΡΙΛΗΨΗ

Η εργασία αυτή αναφέρεται σε εφαρμογές της αποδεκτής διγραμμικής απεικόνισης (Α.Δ.Α.) Weil, σε πρωτόκολλα ψηφιακών υπογραφών. Αρχικά παρουσιάζουμε το πρόβλημα των Diffie-Hellman καθώς επίσης και το πρόβλημα του Διακριτού Λογαρίθμου. Στη συνέχεια ορίζουμε τα σχήματα υπογραφής βασισμένα σε διακριτικά ταυτότητας (ID-σχήματα) καθώς επίσης και τις έννοιες των επιθέσεων και πλαστογραφιών σε αυτά. Έχοντας πρώτα ορίσει τι σημαίνει ένα σχήμα να είναι ασφαλές, παραθέτουμε κάποια σχήματα υπογραφών καθώς επίσης και τις αποδείξεις ασφάλειας σ' αυτά, σε ένα χώρο τον οποίο ονομάζουμε Μοντέλο Χρησμών Τυχαιότητας. Τέλος παραθέτουμε ένα νέο ID-σχήμα υπογραφής από την Α.Δ.Α. Weil, η οποία παρέχει τη σημαντική ιδιότητα ανάκτησης του μηνύματος από την υπογραφή σε αυτό.

Η μεταπτυχιακή αυτή εργασία κατατέθηκε τον Νοέμβριο του 2004 στο Πανεπιστήμιο Κρήτης. Την επιτροπή αξιολόγησης της, αποτέλεσαν, εκτός του επιβλέποντα καθηγητή κ. Γαρεφαλάκη Θεόδουλου, οι κ. Αντωνιάδης Ιωάννης και Τζανάκης Νικόλαος.

Ευχαριστίες

Η εργασία που παρατίθεται στη συνέχεια, είναι καρπός μιας συνεργασίας με ανθρωπους που "αξίζουν πολλά". Ευχαριστώ ***απεριόριστα*** τους Γαρεφαλάκη Θεόδουλο, Γιαννόπουλο Αποστόλη και Μίχο Ιωάννη, για τις ώρες που μου αφιέρωσαν, προσπαθώντας να μου μεταδώσουν λίγη από τη γνώση τους. Ευχαριστώ τους Κώδικες (K. Banach, V. G"Latos, G. Torsione), την M. Bougeló και όλους όσους πέρασαν από τη Γ114 για την βοήθεια σε πραγματικά εξωπραγματικές καταστάσεις. Ευχαριστώ επίσης τους φίλους μου Σταυρουλάκη Χάρη και Τριαντάφυλλο Βασίλη για τις προ διετίας παροτρύνσεις τους, τους Αντωνιάδη Δημήτρη και Θρασυβούλου Άγγελο για τις αναζητήσεις μας, τους Bob, Βλάχο Νίκο και Ζάρα Γιάννη για τις εξωπανεπιστημιακές διαφυγές μας, την πριγκίπισσα Πένυ που δεν έλειψε ποτέ από το πλάι μου και τη βασίλισσα Ζουζού για υπεραριθμήσιμους -το πλήθος, λόγους. Τέλος, θα ήθελα να ευχαριστήσω τους Βλαχούλη Γεράσιμο, Μικέ D.K.K. και Τσιλιφώνη Παντελή για όλα όσα μου έχουν προσφέρει και δεν ξέρω πώς να τους τα ανταποδόσω.

Στον Γιωργο Ζαρακα

Περιεχόμενα

1 ΕΙΣΑΓΩΓΗ **7**
1.1 Γενική επισκόπιση 9

2 ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΙΓΡΑΜΜΙΚΩΝ ΑΠΕΙΚΟΝΙΣΕΩΝ **11**
2.1 Κρυπτογραφικές διγραμμικές απεικονίσεις 12

3 ΔΟΜΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΧΗΜΑΤΩΝ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ **15**
3.1 Βασικοί ορισμοί και έννοιες 15
3.2 Επιχειρήματα ασφάλειας 16
3.3 Το Μοντέλο Χρησμών Τυχαιότητας 17
3.4 Επιθέσεις 18
3.5 Πλαστογραφίες 18

4 ΣΥΝΤΟΜΕΣ ΥΠΟΓΡΑΦΕΣ ΑΠΟ ΤΗΝ Α.Δ.Α. WEIL **21**
4.1 Γενικά 21
4.2 GDH-ομάδες και διγραμμικές απεικονίσεις 22
4.2.1 GDH ομάδες από διγραμμικές απεικονίσεις 23
4.3 Σχήματα υπογραφής βασισμένα σε GDH-ομάδες 24
4.3.1 Ασφάλεια 25
4.3.2 Η αναγκαιότητα της $\psi : G_2 \to G_1$ 29

5 ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΩΝ ΒΑΣΙΣΜΕΝΑ ΣΕ ΔΙΑΚΡΙΤΙΚΑ ΤΑΥΤΟΤΗΤΑΣ, ΑΠΟ Α.Δ.Α. **31**
5.1 Κατασκευή ID-σχήματος ψηφιακής υπογραφής 31
5.2 Βασική ιδέα ορισμού ασφάλειας ενός ID-σχήματος ψηφιακής υπογραφής 33

6 ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΗΣ ΕΚΘΕΤΙΚΩΝ ΟΜΑΔΩΝ ΚΑΙ ID-ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΗΣ ΒΑΣΙΣΜΕΝΑ ΣΕ Α.Δ.Α. 35

6.1 Κλασικά σχήματα υπογραφής από εκθετικές ομάδες 35

6.2 ID-σχήματα υπογραφής από Α.Δ.Α. 37

6.2.1 Παραγωγή ID-σχημάτων υπογραφής (μέρος Ι) : μέθοδος μετατροπής σχημάτων υπογραφής εκθετικών ομάδων 37

6.2.2 Παραγωγή ID-σχημάτων υπογραφής (μέρος ΙΙ) 38

6.3 Αποδείξεις ασφάλειας 40

6.3.1 Ασφάλεια κλασικών σχημάτων υπογραφής εκθετικών ομάδων 40

6.3.2 Ασφάλεια ID-σχημάτων υπογραφής από εκθετικές ομάδες 42

6.3.3 Ασφάλεια ID-σχημάτων υπογραφής 43

7 ΕΝΑ ID-ΠΡΩΤΟΚΟΛΛΟ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΑΠΟ Α.Δ.Α. , ΑΝΑΚΤΩΜΕΝΟΥ ΜΗΝΥΜΑΤΟΣ 45

8 ΠΑΡΑΡΤΗΜΑ Α′: ID-ΣΧΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΜΟΙΡΑΣΜΑΤΟΣ ΚΛΕΙΔΙΟΥ 49

8.1 Σχήματα κρυπτογράφησης 49

8.1.1 Βασικοί ορισμοί και έννοιες 49

8.1.2 ID-σχήμα κρυπτογράφησης σημαντικής ασφάλειας 52

8.2 Σχήματα συμφωνίας κλειδιού 55

9 ΠΑΡΑΡΤΗΜΑ Β′: ΣΤΟΙΧΕΙΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ ΚΑΙ ΚΑΤΑΣΚΕΥΗ ΤΗΣ Α.Δ.Α. WEIL 59

9.1 Η ομάδα των σημείων μιας ελλειπτικής καμπύλης 59

9.2 Η Α.Δ.Α. Weil 64

Κεφάλαιο 1

ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια, η έννοια κρυπτογραφία παράλληλα με τις υποστάσεις της ως παιγνίου και εργαλείου στρατιωτικών εφαρμογών, απέκτησε και μια τρίτη, αυτή του μαθηματικού πεδίου έρευνας. Η άποψη αυτή δικαιολογείται αν λάβουμε υπόψην την κεντρική ιδέα που τη διέπει, την εξασφάλιση δηλαδή της δυσκολίας αποκρυπτογράφησης μηνυμάτων όταν αυτά έχουν κρυπτογραφηθεί με εύκολο τρόπο. Προβλήματα της Θεωρίας Αριθμών, όπως το πρόβλημα του Διακριτού Λογαρίθμου (Discrete Logarithm Problem, συμβ. DLP) και το πρόβλημα ανάλυσης ακεραίων σε πρώτους παράγοντες, αποτέλεσαν το πρώτο έναυσμα στο να αποτυπωθεί η ιδέα αυτή σε μαθηματικούς χώρους, ακριβώς λόγω της μορφής τους, που παραπέμπει στην εν λόγω ιδέα.
Το 1976 οι Diffie και Hellman εισήγαγαν την έννοια της κρυπτογραφίας δημόσιου κλειδιού, με την παρουσίαση του πρώτου πρωτοκόλλου ανταλλαγής κλειδιών: η ιστορία του προβλήματος του Διακριτού Λογάριθμου είχε μόλις ξεκινήσει να γράφεται. Το πρωτόκολλο αυτό βασίζεται στην υπόθεση κατά την οποία ένα συγκεκριμένο πρόβλημα, το πρόβλημα των Diffie-Hellman (συμβ. DH), είναι υπολογιστικά μη επιλύσιμο σε κάποια ομάδα G. Θεωρώντας την G πολλαπλασιαστική ομάδα, είμαστε σε θέση να δώσουμε τους ακόλουθους ορισμούς.

Ορισμός 1 ***Το πρόβλημα Diffie-Hellman***
Για μια δοσμένη πεπερασμένη πολ/κή αβελιανή ομάδα G, ένα στοιχείο $g \in G$ και g^a, g^b με $a, b \in \{1, ..., \# < g >\}$, να υπολογισθεί η τιμή g^{ab}.

Προφανώς το DH πρόβλημα μπορεί να λυθεί αν εξαγχθεί το a από το g^a, το οποίο αποτελεί ακριβώς το DLP πρόβλημα για την ομάδα G.

Ορισμός 2 ***Το πρόβλημα του Διακριτού Λογαρίθμου***
Για μια δοσμένη πεπερασμένη πολ/κή αβελιανή ομάδα G, ένα στοιχείο $g \in G$

και
$y \in < g >$, να υπολογισθεί ο μικρότερος θετικός ακέραιος ρ τ.ω. $y = g^{\rho}$. Ο ακέραιος ρ ονομάζεται διακριτός λογάριθμος του y για τη βάση g και συμβολίζεται ως $\log_g y$.

Μέχρι σήμερα η μοναδική γνωστή μέθοδος επίλυσης του DH προβλήματος, προϋποθέτει αυτή του DLP προβλήματος και η όποια πρόοδος έχει σημειωθεί στη μελέτη του, βασίζεται στη μέθοδο επίλυσης του DLP [2],[3].

Ανάμεσα στην πλειάδα των ομάδων στις οποίες μελετήθηκε το DLP ξεχωρίζουν η ομάδα των μη μηδενικών ακεραίων modulo έναν πρώτο αριθμό p και η ομάδα των σημείων μιας ελλειπτικής καμπύλης πάνω από πεπερασμένα σώματα.

Για πολλούς, η πιο επιτυχής μέθοδος υπολογισμού του διακριτού λογαρίθμου σε πεπερασμένα σώματα είναι η Μέθοδος Υπολογισμού Δεικτών (Index Calculus Method). Από τη δεκαετία του '70 και έπειτα, αρκετοί αλγόριθμοι και παραλλαγές της μεθόδου αυτής εμφανίσθηκαν: οι μοναδικοί αποδείξιμα υποεκθετικοί αλγόριθμοι που είναι γνωστοί, έχουν χρονική πολυπλοκότητα της μορφής

$$\exp\left(c + o(1)\right)(\log q \ \log\log q)^{1/2}$$

όπου q είναι το πλήθος των στοιχείων του σώματος και $c \geq 1$ είναι μια σταθερά, που ποικίλει ανάλογα με τα δεδομένα του προβλήματος.

Όσον αφορά την ομάδα των σημείων μιας ελλειπτικής καμπύλης, αξιοσημείωτο είναι το γεγονός ότι κανένας γενικός υποεκθετικός αλγόριθμος δεν υπάρχει ο οποίος να δίνει λύσεις στο DLP για κάθε ελλειπτική καμπύλη E πάνω από οποιοδήποτε σώμα $\mathbb{F}_q$. Αν δε, αναλογισθούμε ότι το πλήθος των σημείων μιας τέτοιας καμπύλης ισούται με $\#E(\mathbb{F}_q) = q+1-a_q$ όπου $|a_q| \leq 2\sqrt{q}$, μπορούμε να ισχυρισθούμε πως προσεγγίζει το πλήθοςτων σημείων ενός πεπερασμένου σώματος, αλλά δεν είναι εν γένει ίσο. Το DLP σε ελλειπτικές καμπύλες (συμβ. ECDLP) είναι πιο εύχρηστο από το ανάλογό του σε πεπερασμένα σώματα. Αυτό εξηγείται απ' το ότι η δυσκολία του έγκειται όχι μόνο στο πεπερασμένο σώμα πάνω απ' το οποίο ορίζεται, αλλά επιπροσθέτως στην εξίσωση ορισμού της ελλειπτικής καμπύλης. Έτσι ειδικές περιπτώσεις του ECDLP είναι επιδεκτικές λύσεων, όπως π.χ. αυτή κατά την οποία ο αριθμός $q + 1 - a_q$ διαιρείται μόνο από μικρούς πρώτους αριθμούς (μέθοδος Pohlig-Hellman) ή στις περιπτώσεις των Ανώμαλων καμπύλων - που έχουν δηλαδή $a_q = 1$ - όπου το ECDLP λύνεται σε πολυωνυμικό χρόνο!

1.1 Γενική επισκόπιση

Η συγκεκριμένη μεταπτυχιακή εργασία ξεκινά (Κεφ. 2) κάνοντας αναφορά στον τομέα της Κρυπτογραφίας που στηρίζεται σε αποδεκτές διγραμμικές απεικονίσεις (συμβ. Α.Δ.Α.), παραθέτοντας στοιχεία και ιδιότητες αυτών. Στη συνέχεια (Κεφ. 3) περνά στον ορισμό των σχημάτων υπογραφής και σε πολύ βασικές έννοιες αναφορικά με επιχειρήματα ασφάλειας, επιθέσεις και πλαστογραφίες στα σχήματα αυτά. Παράλληλα με τα προηγούμενα, ορίζεται και το Μοντέλο Χρησμών Τυχαιότητας, η έννοια του οποίου είναι πολύ βασική για τις αποδείξεις της ασφάλειας που παρέχει ένα κρυπτογραφικό πρωτόκολλο. Η εργασία συνεχίζεται με ένα παράδειγμα ψηφιακής υπογραφής το οποίο προκύπτει μέσω της Α.Δ.Α. Weil (Κεφ. 4) και ακολουθεί η μετάβαση στα ID-σχήματα υπογραφών από αποδεκτές διγραμμικές απεικονίσεις (Κεφ. 5), όπου μεταξύ άλλων παρατίθενται αποδείξεις της ασφάλειας για κάποια εξ' αυτών (Κεφ. 6). Ίσως το πιο αξιοπρόσεκτο σημείο της εργασίας αποτελεί η εφαρμογή όλων των παραπάνω στην κατασκευή ενός νέου πρωτοκόλλου ψηφιακής υπογραφής από την Α.Δ.Α. Weil, ανακτώμενου μηνύματος (Κεφ. 7). Τέλος, παραθέτουμε τη δομή κάποιων ακόμη κρυπτογραφικών σχημάτων -αυτών της κρυπτογράφησης και της συμφωνίας κλειδιού- στα οποία έχουμε προσαρμόσει την έννοια της ID-ιδιότητας των πρωτοκόλλων (Παράρτημα Α′) και κατόπιν κάποια στοιχεία σχετικά με τη δομή των ελλειπτικών καμπυλών καθώς επίσης και μια αρκετά τεχνική αναφορά στην κατασκευή της Α.Δ.Α. Weil (Παράρτημα Β′).

Κεφάλαιο 2

ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΙΓΡΑΜΜΙΚΩΝ ΑΠΕΙΚΟΝΙΣΕΩΝ

Η ιδέα για ένα κρυπτοσύστημα βασισμένο σε διακριτικά ταυτότητας αποδίδεται στον A.Shamir. Σε ένα τέτοιο σχήμα απαντάται η ιδιότητα σύμφωνα με την οποία το δημόσιο κλειδί του χρήστη προκύπτει ως μια εύκολα υπολογισμένη τιμή από μια συνάρτηση πάνω σε διακριτικά του (Identity), ενώ το προσωπικό του κλειδί μπορεί να υπολογισθεί αντ' αυτού, από μια Έμπιστη Αρχή (Trusted Aythority). Ένα κρυπτοσύστημα δημοσίου κλειδιού βασισμένο σε διακριτικά ταυτότητας (συμβ. ID-κρυπτοσύστημα) , αποτελεί εναλλακτικό κρυπτοσύστημα του κλασικού κρυπτοσυστήματος δημοσίου κλειδιού, ειδικά σε περιπτώσεις όπως αυτές, όπου η διαχείριση κλειδιών (key managment) αποτελεί πρόβλημα και αυτές των χαμηλών απαιτήσεων ασφάλειας.

Η αποδεκτή διγραμμική απεικόνιση Weil με την εισαγωγή της στο χώρο της Κρυπτογραφίας, αντιμετωπίσθηκε με επιφυλακτικότητα, επειδή ανάγει το πρόβλημα του διακριτού λογαρίθμου πάνω σε υπεριδιάζουσα ελλειπτική καμπύλη, σε εκείνο πάνω σε κάποιο πεπερασμένο σώμα. Αυτό ενώ κατ' αρχάς οδήγησε στην απομάκρυνση των καμπυλών αυτών από τον εν λόγω χώρο, όταν παρουσιάσθηκε ένα απλό Diffie-Hellman πρωτόκολλο μεταξύ τριών συμμετεχόντων από τον A.Joux που βασιζόταν στην Α.Δ.Α. Weil σε υπεριδιάζουσες ελλειπτικές καμπύλες, η στάση αυτή αναθεωρήθηκε. Ακολούθησε μελέτη πάνω σε μεγαλυτέρου γένους καμπύλες παράλληλα με εφαρμογές της Α.Δ.Α. Weil σ' αυτές , με φυσικό επακόλουθο την αναπτέρωση του κρυπτογραφικού ενδιαφέροντος σχετικά με τις καμπύλες αυτές.

Τα τελευταία χρόνια οι διγραμμικές απεικονίσεις έχουν βρεί πληθώρα εφαρμογών στην κρυπτογραφία, όσον αφορά την κατασκευή νέων ID-κρυπτογραφικών αρχών. Βασικές εφαρμογές αποτελούν το πρωτόκολλο ενός γύρου Diffie-

Hellman τριμελούς συμφωνίας κλειδιού, το ID-σχήμα κρυπτογράφησης των Boneh-Franklin (το οποίο είναι το πρώτο λειτουργικό, αποτελεσματικό και αποδείξιμα ασφαλές ID-σχήμα κρυπτογράφησης) και το σχήμα υπογραφής των Boneh-Lynn-Shacham του οποίου οι υπογραφές έχουν μικρότερο μήκος σε σχέση με αυτό που έχουν οι υπογραφές κάθε άλλου κλασικού κρυπτοσυστήματος δημοσίου κλειδιού. Κάποιες άλλες εφαρμογές που δεν υπάγονται σε αυτές των θεμελιωδών αρχών της κρυπτογραφίας (δηλαδή του σχήματος κρυπτογράφησης, του σχήματος υπογραφής και του σχήματος συμφωνίας κλειδιού) αποτελούν τα σχήματα εξακρίβωσης (identification scheme) [10], οριακής αποκρυπτογράφησης (threshold scheme) [11], μοιράσματος κλειδιού (key sharing) [12] κ.α.

2.1 Κρυπτογραφικές διγραμμικές απεικονίσεις

Θεωρούμε τις πεπερασμένες αβελιανές ομάδες G_1, G_2, της ίδιας τάξης πρώτου $p \in \mathbb{P}$. Έστω P ένας τυχαίος γεννήτορας της G_1. Υποθέτουμε πως το πρόβλημα του διακριτού λογαρίθμου (DLP) είναι δύσκολο στις G_1, G_2. Μια απεικόνιση e: $G_1 \times G_1 \rightarrow G_2$ η οποία ικανοποιεί τις επόμενες ιδιότητες, ονομάζεται αποδεκτή διγραμμική απεικόνιση:

•*Διγραμμικότητα*: $e(aP, bQ) = e(P, Q)^{ab}$ $\forall P, Q \in G_1$ και $\forall a, b \in \mathbb{Z}$.

•*Μη εκφυλισμός* : Η απεικόνιση δεν στέλνει όλα τα ζεύγη από το $G_1 \times G_1$ σε ταυτοτικό στοιχείο της G_2 . Αν P είναι ένας γεννήτορας της G_1, τότε το στοιχείο $e(P, P)$ αποτελεί γεννήτορα της G_2 .

•*Ικανότητα υπολογισμού*: Υπάρχει αποτελεσματικός αλγόριθμος, ο οποίος μπορεί να υπολογίζει την τιμή $e(P, Q)$ $\forall P, Q \in G_1$.

Η ομάδα G_1, είναι συνήθως μια υποομάδα της προσθετικής ομάδας των σημείων μιας ελλειπτικής καμπύλης $\mathrm{E}/\mathbb{F}_p$, ενώ η ομάδα G_2 είναι συνήθως μια υποομάδα της πολλαπλασιαστικής ομάδας $\mathbb{F}^*_{p^2}$.

Η ύπαρξη της e: $G_1 \times G_1 \rightarrow G_2$ όπως την ορίσαμε παραπάνω, μας παρέχει άμεσα δύο εφαρμογές στις ομάδες αυτές.

1) Η αναγωγή MOV :
Οι Menezes-Okamoto-Vanstone απέδειξαν ότι το DLP στην G_1 δεν είναι δυσκολότερο από το DLP στην G_2. Για να το δούμε αυτό θεωρούμε τα $P, Q \in G_1$, όπου αμφότερα έχουν τάξη $p \in \mathbb{P}$. Επιθυμούμε να βρούμε ένα $a \in \mathbb{Z}^*_p$ τ.ω. $Q = aP$. Έστω $g = e(P, P)$ και $h = e(Q, P)$. Τότε από τη διγραμμικότητα της e ξέρουμε ότι $h = g^a$. Από το μη εκφυλισμό της e έχουμε πως τόσο η g, όσο και η h έχουν τάξη p στην G_2. Έτσι, αναγάγαμε το DLP

από τη G_1 στη G_2 άρα για να είναι το DLP δύσκολο στη G_1 πρέπει να έχουμε εξασφαλίσει τέτοιες παραμέτρους ασφαλείας που να μας εγγυώνται πως το DLP είναι όντως δύσκολο στη G_2.

2) Το πρόβλημα απόφασης Diffie-Hellman είναι εύκολο
Το πρόβλημα απόφασης Diffie-Hellman (Decisional Diffie-Hellman, συμβ. DDH) στη G_1 συνίσταται στη διάκριση μεταξύ των στιγμιότυπων (P, aP, bP, abP) και (P, aP, bP, cP) όπου τα a, b, c είναι τυχαία στο $\mathbb{Z}_p^*$ και το P είναι τυχαίο στοιχείο στο G_1^*. Οι Joux-Nguyen παρατήρησαν ότι το DDH στη G_1 είναι εύκολο. Για να το δούμε αυτό, παρατηρούμε πως για δοσμένα $P, aP, bP, cP \in G_1^*$ έχουμε

$$c = ab \pmod{p} \iff e(P, cP) = e(aP, bP).$$

Το πρόβλημα υπολογισμού Diffie-Hellman (Computational Diffie-Hellman, συμβ. CDH) στη G_1 μπορεί να εξακολουθεί να είναι δύσκολο (το CDH στη G_1 είναι ο υπολογισμός του abP για δοσμένο τυχαίο στιγμιότυπο (P, aP, bP)). Οι Joux-Nguyen έδωσαν παραδείγματα απεικονίσεων $e : G_1 \times G_1 \to G_2$ όπου το CDH στη G_1 εξακολουθούσε να είναι δύσκολο ακόμα και όταν το DDH στη G_1 είναι εύκολο. Εν κατακλείδι, δεν μπορούμε να αποδείξουμε ότι το CDH στη G_1 είναι δύσκολο, αλλά δεν έχουμε κανένα λόγο να πιστεύουμε ότι δεν είναι.

Κεφάλαιο 3

ΔΟΜΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΧΗΜΑΤΩΝ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

3.1 Βασικοί ορισμοί και έννοιες

Οι ψηφιακές υπογραφές, η ηλεκτρονική έκδοση των χειρόγραφων υπογραφών για ψηφιακά έγγραφα, αποτελούν ίσως τη σημαντικότερη εφαρμογή - υπηρεσία ασφαλείας, που μας παρέχει η Κρυπτογραφία. Στους αλγόριθμους υπογραφής, στην κλασική Κρυπτογραφία δημοσίου κλειδιού, το δημόσιο κλειδί του υπογράφοντος είναι κατά κύριο λόγο μια τυχαία ακολουθία bits επιλεγμένη από ένα δοσμένο σύνολο. Αυτό όμως οδηγεί στο πρόβλημα του πώς θα σχετισθεί το δημόσιο κλειδί με τα φυσικά χαρακτηριστικά και διακριτικά του χρήστη στον οποίο αυτό αποδίδεται. Στα κλασικά κρυπτοσυστήματα το "δέσιμο"αυτό μεταξύ της ταυτότητας του χρήστη και του δημόσιου κλειδιού του, επιτυγχάνεται μέσω ενός ψηφιακού πιστοποιητικού. Όπως παρατήρησε ο Shamir [7] θα ήταν πιο αποτελεσματικό αν δεν υπήρχε ανάγκη για ένα τέτοιο "δέσιμο"και αντ' αυτού μπορούσαμε να λάβουμε το δημόσιο κλειδί από κάποια διακριτικά του χρήστη ή πιο εύστοχα από έναν δημοσίως γνωστό ντετερμινιστικό αλγόριθμο, αν για είσοδο σ' αυτόν δίναμε τα διακριτικά του υπογράφοντος.

Επανεξετάζοντας τη δομή ενός σχήματος ψηφιακών υπογραφών παρατηρούμε ότι η υπογραφή ενός χρήστη για ένα μήνυμα m είναι μια λέξη η οποία εξαρτάται από το m και από συγκεκριμένα δημόσια (δημόσιο κλειδί) και προσωπικά (προσωπικό κλειδί) δεδομένα του. Την εγκυρότητα της υπογραφής μπορεί να την ελέγξει ο καθένας, χρησιμοποιώντας μόνο τα δημοσίως γνωστά δεδομένα του χρήστη. Προφανώς μας ενδιαφέρει το εκάστοτε σχήμα που χρησιμοποιούμε, να μην είναι επιρρεπές σε πλαστογραφήσεις, δηλαδή στην πα-

ραγωγή γνήσιων υπογραφών χωρίς τη γνώση των προσωπικών δεδομένων του υπογράφοντος.

Ορισμός 3 *Ένα σχήμα ψηφιακών υπογραφών αποτελείται από :*
∘ *Έναν αλγόριθμο παραγωγής κλειδιών $\mathcal{G}$.*
Στον αλγόριθμο αυτό δίνουμε ως δεδομένα 1^k [1] , όπου k είναι η παράμετρος ασφαλείας του συστήματος και στην έξοδό του μας δίνει ένα ζεύγος (K_p, K_s) δημοσίου/προσωπικού κλειδιού του χρήστη, με n το μήκος του δημοσίου κλειδιού. Σημειώνουμε ότι ο $\mathcal{G}$ είναι ένας πιθανοθεωρητικός αλγόριθμος.
∘ *Έναν αλγόριθμο υπογραφής Σ.*
Για ένα δοσμένο μήνυμα m και ένα ζεύγος (K_p, K_s) δημοσίου/προσωπικού κλειδιού, ο Σ παράγει μια υπογραφή σ. Ο αλγόριθμος υπογραφής ενδέχεται να είναι πιθανοθεωρητικός και σε κάποια σχήματα ενδεχομένως να χρειάζεται περισσότερα δεδομένα.
∘ *Έναν αλγόριθμο πιστοποίησης V.*
Για μια δοσμένη υπογραφή σ, ένα μήνυμα m και ένα δημόσιο κλειδί K_p, ο V ελέγχει αν η σ είναι ισχύουσα υπογραφή για το m, όσον αφορά το K_p. Σε γενικές γραμμές ο V δε χρειάζεται να είναι πιθανοθεωρητικός.

3.2 Επιχειρήματα ασφάλειας

Την εισαγωγή της κρυπτογραφίας δημοσίου κλειδιού από τους Diffie-Hellman ακολούθησε μια πλειάδα νέων σχημάτων (κρυπτογράφησης, υπογραφής κ.α.) πολλά από τα οποία μετέπειτα "έσπασαν". Αποτέλεσμα αυτού ήταν η προσπάθεια δημιουργίας αποδείξιμης ασφάλειας των κρυπτογραφικών σχημάτων. Δυστυχώς όμως σε πολλές περιπτώσεις, η επίτευξη της αποδείξιμης ασφάλειας ενός σχήματος, είχε ως αντίτιμο τη σημαντική απώλεια παραμέτρων που σχετίζονται με την αποδοτικότητα των σχημάτων αυτών. Ένας εναλλακτικός τρόπος επίτευξης κάποιου είδους αποδείξιμης ασφάλειας είναι η ταύτιση συγκεκριμένων κρυπτογραφικών αντικειμένων, όπως π.χ. μιας συνάρτησης "κόφτη", με κάποια ιδανικά αντικείμενα. Η προαναφερθείσα προσέγγιση, καθώς επίσης και η χρησιμοποίηση επιχειρημάτων και εννοιών της Θεωρίας Πολυπλοκότητας οδήγησαν στον ορισμό του μοντέλου το οποίο ονομάζουμε Μοντέλο Χρησμών Τυχαιότητας (Random Oracle Model, συμβ. Μ.Χ.Τ.). Η λέξη "επιχειρήματα"που θα χρησιμοποιούμε στο εξής, θα αναφέρεται σε αποτελέσματα ασφάλειας που αποδεικνύονται στο μοντέλο αυτό. Όπως θεωρούσαμε πάντοτε μέχρι τώρα, τα παραπάνω επιχειρήματα σχετίζονται κι αυτά με θεμελιωδώς

[1] Ο συμβολισμός 1^k υπάγεται στη Θεωρία Υπολογισιμότητας και αντιπροσωπεύει μια λέξη μήκους k που αποτελείται μόνο από 1, την οποία δίνουμε ως είσοδο στη μηχανή Turing που αντιπροσωπεύει τον αλγόριθμο $\mathcal{G}$

δύσκολα αριθμητικά προβλήματα όπως το πρόβλημα της ανάλυσης ακεραίων σε πρώτους παράγοντες ή το πρόβλημα του διακριτού λογαρίθμου.

3.3 Το Μοντέλο Χρησμών Τυχαιότητας

Πολλά κρυπτογραφικά σχήματα, χρησιμοποιούν μια συνάρτηση "κόφτη" f, η χρήση της οποίας γεννήθηκε από την επιθυμία να υπογραφούν μεγάλα σε μήκος μηνύματα, από μία μόνο, μικρού μήκους υπογραφή. Προκειμένου να αποφύγουμε τετριμμένες πλαστογραφήσεις, ένα ελάχιστο ζητούμενο από μια τέτοια συνάρτηση είναι να πληροί την προϋπόθεση, ο υπογράφων να είναι αδύνατο να βρεί δύο διαφορετικά μηνύματα που η τιμή τους μέσω αυτής να είναι η ίδια. Καλούμε την εν λόγω ιδιότητα της συνάρτησης αυτής ως *ελευθερία αντιπαράθεσης* (collision freeness).

Με την πάροδο του χρόνου διαπιστώθηκε πως οι συναρτήσεις "κόφτες" αποτελούν βασικό συστατικό αναφορικά με την ασφάλεια ενός σχήματος υπογραφών. Προκειμένου δε να εξασφαλισθούν επιχειρήματα ασφάλειας ταυτόχρονα με το να διατηρηθεί η αποτελεσματικότητα των κατασκευών που τις χρησιμοποιούν, προτάθηκε η υιοθέτηση της υπόθεσης σύμφωνα με την οποία η f να είναι στην ουσία μια τυχαία συνάρτηση. Ακολουθώντας την πρόταση αυτή ορίζεται το μοντέλο μέσα στο οποίο υπάρχουν οι συναρτήσεις αυτές και αυτό ακριβώς ονομάζουμε Μοντέλο Χρησμών Τυχαιότητας (Μ.Χ.Τ.). Στο μοντέλο αυτό μπορούμε να φανταστούμε πως οι τιμές που αποδίδονται στις συναρτήσεις του, μπορούν να παρομοιασθούν με ένα χρησμό, ο οποίος αποδίδει μια παντελώς τυχαία τιμή κάθε φορά που υπάρχει κάποιο ερώτημα προς αυτό: φυσικά, αν το ίδιο ερώτημα τεθεί εις διπλούν, οι απαντήσεις που θα δώσει θα ταυτίζονται. Στο σημείο αυτό μπορούμε να κάνουμε τη σύμβαση πως οι αποδείξεις στο μοντέλο αυτό, συνεπάγονται ασφάλεια για ένα σχήμα υπογραφής, υπό τον όρο ότι οι συναρτήσεις του να μην αποκλίνουν του ιδανικού ορισμού τους.

Ανακεφαλαιώνουμε: ορίσαμε, μη αυστηρά, ένας χρησμός τυχαιότητας να είναι μια συνάρτηση $H : X \to Y$ η οποία επιλέγεται τυχαία από το σύνολο όλων των συναρτήσεων $\{h : X \to Y\}$ (υποθέτουμε πως το σύνολο Y είναι πεπερασμένο). Ένας αλγόριθμος δύναται να θέτει ερωτήματα στους χρησμούς τυχαιότητας, σε κάθε σημείο $x \in X$ και να παίρνει απάντηση σ' αυτό, την τιμή $H(x)$. Σημειώνουμε πως αν είναι ασφαλές ένα σχήμα στο Μοντέλο Χρησμών Τυχαιότητας, δε σημαίνει πως είναι ασφαλές και στον πραγματικό κόσμο.

3.4 Επιθέσεις

Εστιάζουμε το ενδιαφέρον μας σε δυο συγκεκριμένα είδη επιθέσεων σε υπογραφές: στις επιθέσεις άνευ μηνύματος και τις επιθέσεις γνώσης μηνυμάτων. Στις επιθέσεις άνευ μηνύματος ο Επιτιθέμενος δε γνωρίζει τίποτε παραπάνω από το δημόσιο κλειδί του υπογράφοντος, ενώ αντιθέτως στις επιθέσεις γνώσης μηνυμάτων έχει πρόσβαση σε μια λίστα ζευγών μηνύματος - υπογραφής. Η κατηγορία των επιθέσεων γνώσης μηνυμάτων χωρίζεται στις εξής υποκατηγορίες:

Επιθέσεις γνώσης καθαρών μηνυμάτων: Ο Επιτιθέμενος στις επιθέσεις αυτές έχει πρόσβαση σε μια λίστα από υπογεγραμμένα μηνύματα, τα οποία όμως δεν έχουν επιλεγεί από τον ίδιο.

Αυθαίρετες επιθέσεις επιλεγομένων μηνυμάτων: Ο Επιτιθέμενος στις επιθέσεις αυτές μπορεί να επιλέξει μια λίστα μηνυμάτων προς υπογραφήν. Η επιλογή αυτή γίνεται πριν λάβει γνώση του δημοσίου κλειδιού του υπογράφοντος. Ονομάζονται "αυθαίρετες", αφού η επιλογή των μηνυμάτων θεωρείται ανεξάρτητη του υπογράφοντος.

Προσανατολισμένες επιθέσεις επιλεγομένων μηνυμάτων: Ξανά ο Επιτιθέμενος στις επιθέσεις αυτές, μπορεί να επιλέξει μια λίστα μηνυμάτων προς υπογραφήν, αλλά η επιλογή αυτή γίνεται κατόπιν γνώσης του δημοσίου κλειδιού του υπογραφόντος. Ονομάζονται "προσανατολισμένες"επιθέσεις κατά του συγκεκριμένου υπογράφοντος.

Προσαρμοζόμενες επιθέσεις επιλεγομένων μηνυμάτων: Ο Επιτιθέμενος, στις επιθέσεις αυτές, έχοντας γνώση του δημοσίου κλειδιού του υπογράφοντος, έχει τη δυνατότητα να ζητά στον τελευταίο να του υπογράψει όποιο μήνυμα του ζητήσει. Μπορεί επίσης να προσαρμόζει τα ερωτήματά του ανάλογα με την απάντηση ζεύγους μηνύματος-υπογραφής που παίρνει κάθε φορά.

Βασική Παρατήρηση: Η αποτίμηση της ασφάλειας ενός σχήματος υπογραφής, γίνεται με βάση το αν είναι ή όχι ασφαλές έναντι των προσαρμοζόμενων επιθέσεων επιλεγομένων μηνυμάτων.

3.5 Πλαστογραφίες

Τα αναμενόμενα αποτελέσματα μιας επίθεσης σε ένα σχήμα υπογραφής, μπορούν να ταξινομηθούν σε κάποια από τις παρακάτω κατηγορίες πλαστογραφίας:

- Πλαστογραφία σπασμένου συστήματος (total break).

Πρόκειται για πλαστογραφία που προκύπτει από επιθέσεις που επιφέρουν τη φανέρωση του προσωπικού κλειδιού του υπογράφοντος .

- Καθολική πλαστογραφία (universal forgery).

Κατ' αυτές έχουμε την κατασκευή ενός αλγόριθμου ο οποίος έχει την ικανότητα να υπογράφει οποιοδήποτε μήνυμα ο Επιτιθέμενος θελήσει.

- Υπαρκτή πλαστογραφία (existential forgery).

Το αποτέλεσμα μιας επίθεσης κατά το οποίο στο τέλος της ο Επιτιθέμενος παρουσιάζει ένα ζεύγος μηνύματος -υπογραφής σ' αυτό. Τις περισσότερες φορές επιθέσεις που η δράση τους κινείται προς την εξόρυξη τέτοιων ζευγών, δεν είναι επικίνδυνη, αφού το μήνυμα που ο πλαστογράφος τελικά υπογράφει μπορεί να μην έχει κανένα νόημα.

Ορισμός 4 *Ένα σχήμα υπογραφής ονομάζεται ασφαλές αν μια υπαρκτή πλαστογραφία επ' αυτού είναι υπολογιστικά ανέφικτη, ακόμα κι αν υφίσταται προσαρμοσμένες επιθέσεις επιλεγομένων μηνυμάτων.*

Κεφάλαιο 4

ΣΥΝΤΟΜΕΣ ΥΠΟΓΡΑΦΕΣ ΑΠΟ ΤΗΝ Α.Δ.Α. WEIL

4.1 Γενικά

Πριν προχωρήσουμε στη μελέτη και κατ' επέκταση στις αποδείξεις ασφάλειας ID-πρωτοκόλλων ψηφιακών υπογραφών από Α.Δ.Α. , θα ασχοληθούμε με ένα συγκεκριμένο πρωτόκολλο κλασικής υπογραφής και την ασφάλεια που παρέχει αυτό. Είναι γνωστό ότι οπουδήποτε ζητείται μια υπογραφή, αναζητείται η μικρότερη δυνατή παράσταση αυτής π.χ. στην απόδοση μιας bar-coded υπογραφής σε ένα γραμματόσημο. Οι Σύντομες (Short) ψηφιακές υπογραφές είναι υπογραφές που βρίσκουν εφαρμογές σε περιβάλλον με ισχυρούς περιορισμούς αναφορικά με το εύρος (το μήκος δηλαδή) των υπογραφών.

Τα δύο πιο διαδεδομένα ως προς τη χρήση τους σχήματα υπογραφών, το RSA και το DSA, παράγουν σχετικά μεγάλες σε μήκος υπογραφές σε σχέση με την ασφάλεια που παρέχουν. Για παράδειγμα, όταν κάποιος χρησιμοποιεί το σχήμα μιας 1024-bit modulus, RSA υπογραφής, τότε αυτή θα έχει μήκος 1024-bit. Ομοίως, όταν χρησιμοποιήσει το σχήμα της 1024-bit modulus, standard DSA υπογραφής, τότε η υπογραφή του θα έχει μήκος 320-bit. Στο σχήμα των Σύντομων υπογραφών το μήκος των υπογραφών είναι προσεγγιστικά 170-bit και παρέχει τα ίδια επίπεδα ασφάλειας με αυτά ενός σχήματος με υπογραφές DSA μήκους 320-bit. Το συγκεκριμένο σχήμα είναι ασφαλές έναντι των προσαρμοζόμενων επιθέσεων επιλεγομένων μηνυμάτων εξαγωγής μηνύματος - υπογραφής, όταν υποθέσουμε πως το πρόβλημα Υπολογισμού των Diffie - Hellman (CDH), είναι δύσκολο σε συγκεκριμένες ελλειπτικές καμπύλες πάνω από ένα πεπερασμένο σώμα. Η πιστοποίηση της εγκυρότητας των υπογραφών του σχήματος γίνεται απλά με τη χρησιμοποίηση μιας Α.Δ.Α. στα σημεία της καμπύλης και επειδή ακριβώς χρησιμοποιούνται ιδιότητες των ση-

μείων της καμπύλης, προκύπτει ότι δεν υπάρχει ισοδύναμο προς αυτό, σχήμα στο $\mathbb{F}_p^*$.

Το σχήμα των Σύντομων υπογραφών που θα παρουσιάσουμε χρησιμοποιεί ομάδες στις οποίες το πρόβλημα Απόφασης των Diffie - Hellman (DDH) είναι εύκολο, ενώ το πρόβλημα Υπολογισμού των Diffie - Hellman (CDH) είναι δύσκολο. Καλούμε αυτές τις ομάδες *χασματικές Diffie - Hellman ομάδες* (Gap-DH, συμβ. GDH). Στη συνέχεια θα δείξουμε πώς κατασκευάζεται ένα σχήμα υπογραφών από τέτοιες ομάδες και θα αποδείξουμε την ασφάλειά του.

4.2 GDH-ομάδες και διγραμμικές απεικονίσεις

Πριν παρουσιάσουμε ένα σχήμα υπογραφής από GDH ομάδες, παραθέτουμε κάποιες έννοιες σχετικές με διγραμμικές απεικονίσεις και με GDH-ομάδες. Χρησιμοποιούμε τον ακόλουθο συμβολισμό :

1. G_1 και G_2 είναι πολλαπλασιαστικές ομάδες τάξεως $p \in \mathbb{P}$,
2. g_1, g_2 είναι γεννήτορες των G_1 και G_2 αντίστοιχα,
3. ψ είναι ένας υπολογίσιμος ισομορφισμός από τη G_2 στη G_1 με $\psi(g_2) = g_1$
4. e είναι μια Α.Δ.Α. $e : G_1 \times G_2 \to G_T$, όπου G_T προσθετική ομάδα γνωστής τάξεως $p \in \mathbb{P}$.

Οι αποδείξεις ασφάλειας προϋποθέτουν έναν υπολογίσιμο ισομορφισμό ψ: $G_2 \to G_1$. Όταν $G_1 = G_2$ και $g_1 = g_2$ μπορούμε να πάρουμε ως ψ την ταυτοτική απεικόνιση, σε κάθε άλλη περίπτωση όμως πρέπει να την καθορίσουμε αυστηρά. Για να γίνει αυτό πιο σαφές θα δώσουμε ένα παράδειγμα στο οποίο από μια διγραμμική απεικόνιση θα παράγεται ένα μη ασφαλές σχήμα, ακριβώς επειδή η ψ δεν είναι εύκολα υπολογίσιμη. Στο σημείο αυτό θα πρέπει να τονίσουμε πως η χρησιμότητα του ισομορφισμού ψ έγκειται στην εξασφάλιση της ασφάλειας του σχήματος ενώ δεν εμφανίζεται σε κανένα στάδιο των αλγορίθμων που απαρτίζουν το σχήμα αυτό.
Στη συνέχεια παραθέτουμε κάποιους ορισμούς γενίκευσης των προβλημάτων CDH και DDH.

Γενικευμένο πρόβλημα Υπολογισμού Diffie-Hellman στις (G_1, G_2) (συμβ. co-CDH): Έστω $g_2, g_2^a \in G_2$ και $h \in G_1$. Να υπολογισθεί το $h^a \in G_1$.

Γενικευμένο πρόβλημα Απόφασης Diffie-Hellman στις (G_1, G_2) (συμβ. co-DDH): Έστω $g_2, g_2^a \in G_2$ και $h, h^b \in G_1$. Να απαντηθεί `NAI` αν $a = b$ και `OXI` σε κάθε άλλη περίπτωση. Αν δε, η απάντηση είναι `NAI`, λέμε πως η τετράδα (g_2, g_2^a, h, h^a) είναι μια co-Diffie-Hellman τετράδα.

Προφανώς όταν $G_1 = G_2$ τα παραπάνω προβλήματα ανάγονται στα CDH, DDH με τον αρχικό ορισμό τους.

Στη συνέχεια ορίζουμε ένα ζεύγος ομάδων για το γενικευμένο πρόβλημα Diffie-Hellman να είναι το ζεύγος αυτό των ομάδων (G_1, G_2), για το οποίο το co-DDH είναι εύκολο ενώ το co-CDH είναι δύσκολο. Ως πλεονέκτημα του αλγορίθμου A που λύνει το γενικευμένο πρόβλημα Υπολογισμού Diffie-Hellman στις (G_1, G_2) ορίζουμε την πιθανότητα:

$$Adv(co-CDH)_A := Pr[A(g_2, g_2^a, h) = h^a : a \in_R \mathbb{Z}_p, h \in_R G_1].$$

Παρατηρούμε ότι η πιθανότητα είναι πάνω από την ομοιόμορφα τυχαία επιλογή του a από το $\mathbb{Z}_p$ και του h από τη G_1. Λέμε ότι ένας αλγόριθμος A σπάει με παραμέτρους (t, ϵ) ((t, ϵ)-αλγόριθμος) το γενικευμένο πρόβλημα Υπολογισμού Diffie-Hellman στις (G_1, G_2) αν ο αλγόριθμος A υλοποιείται το πολύ σε χρόνο t και η πιθανότητα $Adv(co-CDH)_A$ αυτού, είναι τουλάχιστον ϵ.

Ορισμός 5 *Δύο ομάδες (G_1, G_2) αποτελούν ένα (t,ϵ) co-GDH ζεύγος ομάδων αν πληρούν τις παρακάτω ιδιότητες:*

1. Οι πράξεις στις ομάδες G_1, G_2 καθώς επίσης και ο υπολογισμός των τιμών της ψ, γίνονται σε μια μονάδα χρόνου.

2. Το γενικευμένο πρόβλημα Απόφασης Diffie-Hellman στις (G_1, G_2), λύνεται σε μια μονάδα χρόνου.

3. Κανένας αλγόριθμος (t, ϵ) δε σπάει το γενικευμένο πρόβλημα Υπολογισμού Diffie-Hellman στις (G_1, G_2).

Όταν το (G_1, G_1) είναι ένα (t, ϵ) co-GDH ζεύγος ομάδων, τότε λέμε ότι η G_1 είναι μια *χασματική Diffie-Hellman ομάδα* (Gap-DH, συμβ. GDH). Άξιο αναφοράς επίσης είναι το ότι στον παραπάνω ορισμό γίνεται μια κανονικοποίηση του χρόνου έτσι ώστε όλοι οι παραπάνω αλγόριθμοι να υλοποιούνται σε μια μονάδα χρόνου και κάτω από τη συγκεκριμένη κανονικοποίηση λέμε πως δεν υπάρχει αλγόριθμος που να σπάει το γενικευμένο πρόβλημα Υπολογισμού Diffie-Hellman στις (G_1, G_2) με παραμέτρους (t, ϵ).

4.2.1 GDH ομάδες από διγραμμικές απεικονίσεις

Τα μοναδικά παραδείγματα GDH ομάδων που έχουμε στη διάθεσή μας προέρχονται από Α.Δ.Α. (αυτό βέβαια δεν αποκλείει το ενδεχόμενο να υπάρχουν κι από άλλες δομές, που να τις κατασκευάζουν). Έστω ότι G_1, G_2 είναι οι ομάδες που ορίσαμε προηγουμένως και G_T μια προσθετική ομάδα τ.ω. $|G_1| = |G_2| = |G_T|$. Χρησιμοποιούμε την Α.Δ.Α. Weil $e : G_1 \times G_2 \to G_T$ για την οποία ισχύει :

1. Διγραμμικότητα: Για κάθε $u \in G_1, v \in G_2$ και $a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$.

2. Μη εκφυλισμός: $e(g_1, g_2) \neq 1$.

Ορισμός 6 *Δύο ομάδες G_1, G_2 τάξεως p αποτελούν ένα (t,ϵ)-διγραμμικό ζεύγος ομάδων αν ικανοποιούν τις εξής συνθήκες:*

1. Οι πράξεις στις ομάδες G_1, G_2 καθώς επίσης και ο υπολογισμός των τιμών της ψ, γίνονται σε μια μονάδα χρόνου.

2. Υπάρχει ομάδα G_T τάξεως p και μια Α.Δ.Α. $e : G_1 \times G_2 \to G_T$ υπάρχουν, με την e να είναι υπολογίσιμη σε μια μονάδα χρόνου.

3. Κανένας (t, ϵ) αλγόριθμος δε σπάει το γενικευμένο πρόβλημα Υπολογισμού Diffie-Hellman στις (G_1, G_2).

Με βάση τα παραπάνω οι Joux - Nguyen [8] κατάφεραν να αποδείξουν πως μια αποτελεσματική, υπολογίσιμη αποδεκτή διγραμμική απεικόνιση e, παρέχει έναν αλγόριθμο για τη λύση του γενικευμένου προβλήματος Απόφασης Diffie-Hellman με τον ακόλουθο τρόπο: Για μια τετράδα (g_2, g_2^a, h, h^b), όπου $h \in G_1$, έχουμε:

$$a = b \pmod{p} \iff e(h, g_2^a) = e(h^b, g_2).$$

Οι τετράδες (g_2, g_2^a, h, h^b) στις οποίες ισχύουν οι ισότητες εκατέρωθεν της παραπάνω ισοδυναμίας ονομάζονται *co-DH τετράδες*.Βλέπουμε ότι ένα (t, ϵ)-διγραμμικό ζεύγος ομάδων είναι ένα (t, ϵ) co-GDH ζεύγος ομάδων.

4.3 Σχήματα υπογραφής βασισμένα σε GDH-ομάδες

Παρουσιάζουμε ένα σχήμα υπογραφής το οποίο είναι ισχύον για κάθε co-GDH ζεύγος ομάδων (G_1, G_2).

Έστω (G_1, G_2) ένα (t, ϵ) co-GDH ζεύγος ομάδων με $|G_1| = |G_2| = p$. Μια υπογραφή σ είναι ένα στοιχείο της G_1. Το σχήμα περιλαμβάνει τους αλγορίθμους Προεργασιών, Υπογραφής και Πιστοποίησης καθώς επίσης και μια κρυπτογραφική συνάρτηση "κόφτη" $H : \{0,1\}^* \to G_1$.

Αλγόριθμος Προεργασιών Επιλέγουμε τυχαίο $x \in \mathbb{Z}_p$ και υπολογίζουμε $u := g_2^x$. Το δημόσιο κλειδί θα είναι το $u \in G_2$, ενώ το μυστικό κλειδί το x.

Αλγόριθμος Υπογραφής Για ένα δοσμένο $x \in \mathbb{Z}_p$ και μήνυμα $M \in \{0,1\}^*$, υπολογίζουμε τα $h := H(M) \in G_1, \sigma := h^x$. Η υπογραφή στο M θα είναι η σ.

Αλγόριθμος Πιστοποίησης Για ένα δοσμένο δημόσιο κλειδί $u \in G_2$, μήνυμα $M \in \{0,1\}^*$ και υπογραφή σ υπολογίζουμε την τιμή $h = H(M) \in G_1$ και εξετάζουμε αν η τετράδα (g_2, u, h, σ) είναι όντως μια co-DH τετράδα. Αν είναι, τότε ο αλγόριθμος απαντά θετικά για κάθε "νόμιμη" υπογραφή (αφού

$u = g_2^x$ και $\sigma = h^x$) και αποφαίνεται: ΙΣΧΥΟΥΣΑ, ενώ σε κάθε άλλη περίπτωση αποφαίνεται: ΜΗ-ΙΣΧΥΟΥΣΑ.

Μια υπογραφή είναι ένα στοιχείο της G_1. Για την κατασκευή Σύντομων υπογραφών επιθυμούμε co-GDH ζεύγη ομάδων στα οποία τα στοιχεία της G_1 να έχουν "μικρή"σε μήκος αναπαράσταση.

4.3.1 Ασφάλεια

Αποδεικνύουμε την ασφάλεια που παρέχει το σχήμα υπογραφής μας, έναντι των προσαρμοζόμενων επιθέσεων επιλεγομένων μηνυμάτων εξαγωγής μηνύματος - υπογραφής. Η ιδιότητα της μη πλαστογράφησης του σχήματος μας, ορίζεται μέσω του ακόλουθου παιχνιδιού μεταξύ ενός Επιτιθέμενου στο σχήμα και ενός Προκαλούντα ο οποίος θα απαντά στα ερωτήματα του πρώτου.

Προεργασία Ο Προκαλών έχοντας υλοποιήσει τον αλγόριθμο Προεργασιών, παίρνει ένα δημόσιο κλειδί PK και ένα προσωπικό κλειδί SK. Στον Επιτιθέμενο δίνει μόνο το PK.

Ερωτήματα Κάνοντάς το με προσαρμογή στις εκάστοτε απαντήσεις, ο Επιτιθέμενος ζητά υπογραφές (κάποιου χρήστη διακριτικών PK) για το πολύ q_s το πλήθος μηνύματα της επιλογής του $M_1, M_2, ..., M_{q_s} \in \{0,1\}^*$. Ο Προκαλών απαντά σε κάθε ένα από αυτά και του δίνει τις αντίστοιχες υπογραφές σ_i για κάθε $i = 1, ..., q_s$.

Απόφανση Ο Επιτιθέμενος μετά το τέλος των ερωτημάτων, παρουσιάζει ένα ζεύγος μηνύματος -υπογραφής (M, σ) και κερδίζει το παιγνίδι (i) αν το M δεν είναι ένα εκ των $M_1, M_2, ..., M_{q_s}$ και (ii) αν ο αλγόριθμος Πιστοποίησης αποφανθεί για την συγκεκριμένη υπογραφή πως είναι ΙΣΧΥΟΥΣΑ.

Ορισμός 7 *Έστω $\mathcal{A}$ ένας Επιτιθέμενος σ' ένα σχήμα υπογραφής ο οποίος ζητά και παίρνει απαντήσεις σε ένα πλήθος q_s ερωτημάτων υπογραφής και q_H ερωτημάτων των τιμών συναρτήσεων που υπάγονται στο M.X.T. . Θα λέμε ότι ο $\mathcal{A}$ σπάει με παραμέτρους (t, q_s, q_H, ϵ) το σχήμα αυτό, αν σε χρόνο το πολύ t και με πιθανότητα τουλάχιστον ϵ, θα είναι σε θέση να υπογράψει τυχαίο μήνυμα, δίχως τη γνώση του προσωπικού κλειδιού κάποιου υπογράφοντα, με βάση τις ερωτήσεις στα παραπάνω ερωτήματα.*
Ένα σχήμα υπογραφής ορίζεται ως (t, q_s, q_H, ϵ)-μη πλαστογραφήσιμο έναντι των προσαρμοζόμενων επιθέσεων επιλεγομένων μηνυμάτων εξαγωγής μηνύματος - υπογραφής, αν καμμία (t, q_s, q_H, ϵ) επίθεση δεν το σπάει.

Το ακόλουθο Θεώρημα μας δείχνει ότι το σχήμα υπογραφής μας, είναι ασφαλές.

ΘΕΩΡΗΜΑ 8 *Έστω (G_1, G_2) ένα (t', ϵ') co-GDH ζεύγος ομάδων τάξεως $p \in \mathbb{P}$. Τότε το σχήμα υπογραφής στις (G_1, G_2) είναι (t, q_s, q_H, ϵ) ασφαλές έναντι των προσαρμοζόμενων επιθέσεων επιλεγομένων μηνυμάτων εξαγωγής μηνύματος - υπογραφής, για κάθε t, ϵ τα οποία θα ικανοποιούν τις*

$$\epsilon \geq e(q_s + 1)\epsilon' \quad , \quad t \leq t' - c_{G_1}(q_H + 2q_s),$$

όπου c_{G_1} είναι μια σταθερά η οποία εξαρτάται από τη G_1 και e η βάση του Νεπέριου λογάριθμου.

Η ασφάλεια του σχήματος έγκειται στη δυσκολία του co-CDH στις (G_1, G_2). Όταν $G_1 = G_2$ η ασφάλεια του έγκειται στην υπόθεση δυσκολίας του CDH στη G_1.

Απόδειξη Έστω A ένας αλγόριθμος επίθεσης ο οποίος (t, q_s, q_H, ϵ) σπάει το σχήμα υπογραφής. Δείχνουμε πως κατασκευάζουμε έναν αλγόριθμο B που να υλοποιείται σε χρόνο το πολύ t' και ο οποίος θα λύνει το co-CDH στις (G_1, G_2) με πιθανότητα τουλάχιστον ϵ'. Αυτό θα έρθει σε αντίθεση με το γεγονός ότι το (G_1, G_2) είναι ένα (t', ϵ') co-GDH ζεύγος ομάδων.

Έστω g_2 ένας γεννήτορας της G_2. Δίνουμε στον B τα $g_2, u \in G_2$ και $h \in G_1$, όπου $u := g_2^a$. Στόχο μας αποτελεί ο υπολογισμός του $h^a \in G_1$. Ο αλγόριθμος B αντιπροσωπεύει τον Προκαλούντα και συνεργάζεται με τον A με τον τρόπο που παραθέτουμε στη συνέχεια.

ΠΡΟΕΡΓΑΣΙΑ. Ο αλγόριθμος B στο ξεκίνημά του δίνει στον A το γεννήτορα g_2 και το δημόσιο κλειδί $u \cdot g_2^r \in G_2$ όπου το r είναι ένα τυχαίο στοιχείο του $\mathbb{Z}_p$.

ΕΡΩΤΗΜΑΤΑ ΤΙΜΩΝ ΤΗΣ ΣΥΝΑΡΤΗΣΗΣ H. Όποια στιγμή θελήσει ο αλγόριθμος A μπορεί να ζητήσει κάποια τιμή της H στο σημείο του πεδίου ορισμού της που αυτός επιθυμεί. Προκειμένου να απαντήσει στα ερωτήματα αυτά ο B διατηρεί μια λίστα από τετράδες $< M_j, w_j, b_j, c_j >$ την οποία στο εξής θα καλούμε H-λίστα. Αρχικά δεχόμαστε πως η λίστα αυτή θα είναι κενή και κάθε φορά που ο A θα θέτει ένα ερώτημα H σε ένα σημείο $M_i \in \{0,1\}^*$, ο B ανταποκρίνεται στο ερώτημά του ως εξής:

1. Αν το ερώτημα M_i ήδη υπάρχει στη H-λίστα στην τετράδα $< M_j, w_j, b_j, c_j >$, τότε ο B απαντά $H(M_i) = w_i \in G_1$.
2. Σε διαφορετική της άνωθεν περίπτωση, ο B δημιουργεί ένα "νόμισμα" $c \in \{0,1\}$ τ.ω. $Pr[c_i = 0] = 1/(q_s + 1)$.
3. Ο αλγόριθμος B επιλέγει έναν τυχαίο ακέραιο $b_i \in \mathbb{Z}_p$.

Αν $c_i = 0$, ο B υπολογίζει το $w_i := h \cdot \psi(g_2)^{b_i} \in G_1$ ενώ αν $c = 1$ ο B υπολογίζει το $w_i := \psi(g_2)^{b_i} \in G_1$.

4. Ο αλγόριθμος B προσθέτει στη H-λίστα την τετράδα $< M_j, w_j, b_j, c_j >$ και απαντά στον A έχοντας θέσει $H(M_i) = w_i$.
Σημειώνουμε πως οι παραπάνω ορισμοί κατασκευάσθηκαν έτσι ώστε τα w_i να κατανέμονται ομοιόμορφα σε όλο το G_1 και να είναι ανεξάρτητες οι τιμές τους από τις τιμές των προηγούμενων ερωτημάτων.

ΕΡΩΤΗΜΑΤΑ ΥΠΟΓΡΑΦΩΝ. Έστω M_i ότι είναι ένα ερώτημα υπογραφής το οποίο έχει τεθεί από τον A. Ο αλγόριθμος B ανταποκρίνεται στο ερώτημά του ως εξής:

1. Στην αρχή υλοποιεί τον σχετικό με τα H-ερωτήματα αλγόριθμο ώστε να πάρει την τιμή $w_i \in G_1$ με $H(M_i) = w_i$. Έστω $< M_j, w_j, b_j, c_j >$ η σχετική μ' αυτό τετράδα στη H-λίστα. Αν $c_i = 0$ τότε ο B αποφαίνεται `ΑΠΟΤΥΧΙΑ` και τερματίζει (η συγκεκριμένη ενέργεια του B οφείλεται στην αποτυχία αυτής της περίπτωσης να περάσει τον αλγόριθμο Πιστοποίησης της υπογραφής).

2. Γνωρίζουμε ότι $c_i = 1$ οπότε $w_i := \psi(g_2)^{b_i} \in G_1$. Ορίζουμε $\sigma_i := \psi(u)^{b_i} \cdot \psi(g_2)^{rb_i} \in G_1$. Παρατηρούμε ότι $\sigma_i := w_i^{a+r}$ οπότε η σ_i είναι μια ισχύουσα υπογραφή στο M_i για το δημόσιο κλειδί $u \cdot g_2^r = g_2^{a+r}$. Κατόπιν ο A δίνει την υπογραφή σ_i στον A.

ΑΠΟΦΑΝΣΗ. Στο τελικό αυτό στάδιο της συνεργασίας των A και B, ο A παρουσιάζει ένα ζεύγος μηνύματος -υπογραφής (M_f, σ_f) όπου κανένα ερώτημα υπογραφής δεν απευθύνετο στο συγκεκριμένο M_f. Αν δεν υπάρχει τετράδα στη H-λίστα που να περιέχει το M_f τότε ο B ρωτά (στην ουσία τον εαυτό του) την τιμή $H(M_f)$ για να βεβαιωθεί για την ύπαρξη μιας τέτοιας τετράδας. Υποθέτουμε πως η σ_f είναι μια ισχύουσα υπογραφή για το M_f αναφορικά με το δοσμένο δημόσιο κλειδί ενώ σε διαφορετική περίπτωση ο B αποφαίνεται `ΑΠΟΤΥΧΙΑ` και τερματίζει. Στη συνέχεια ο B εντοπίζει την τετράδα $< M_j, w, b, c >$ στη H-λίστα. Αν $c = 1$ τότε αναφέρει `ΑΠΟΤΥΧΙΑ` και τερματίζει, ενώ αν $c = 0$ (έχω τότε w_i που έχει σαν παράγοντα το h όπου μας χρειάζεται για τη λύση του co-CDH (g_2, g_2^a, h)) τότε υπολογίζει το $H(M_f) = w = h \cdot \psi(g_2)^b$. Κατ' επέκταση έχουμε $\sigma = h^{a+r} \cdot \psi(g_2)^{b(a+r)}$ και ο B υπολογίζει το ζητούμενο h^a ως $h^a = \sigma/(h^r \cdot \psi(u)^b \cdot \psi(g_2)^{rb})$.

Κάπου εδώ ολοκληρώνεται η περιγραφή της λειτουργίας του αλγορίθμου B. Απομένει να δείξουμε ότι ο B λύνει το ζητούμενο co-CDH στις (G_1, G_2) με πιθανότητα τουλάχιστον ϵ'. Για την απόδειξη αυτή μπορούμε να αναλύσουμε τις κάτωθι τρεις καταστάσεις οι οποίες απαιτούνται προκειμένου ο B να πετύχει το στόχο του:
ε_1: Η υλοποίηση του B δε σταματά ποτέ, ως αποτέλεσμα οποιουδήποτε ερωτήματος υπογραφής του A.

ε_2: Ο A παρουσιάζει ένα ζεύγος ισχύουσας υπογραφής (M_f, σ_f).
ε_3: Η κατάσταση ε_2 και $c = 0$ βρίσκονται στην τετράδα που περιέχει το M_f στη H-λίστα.

Ο αλγόριθμος B κρίνεται "πετυχημένος"αν και οι τρεις αυτές καταστάσεις υφίστανται. Η πιθανότητα $Pr[\varepsilon_1 \wedge \varepsilon_3]$ μπορεί να αναλυθεί ως:

$$Pr[\varepsilon_1 \wedge \varepsilon_3] = Pr[\varepsilon_1] \cdot Pr[\varepsilon_2|\varepsilon_1] \cdot Pr[\varepsilon_3|\varepsilon_1 \wedge \varepsilon_2]$$

Ισχυρισμός Α: Η πιθανότητα του αλγορίθμου B να μη σταματήσει, ως αποτέλεσμα οποιασδήποτε ερώτησης υπογραφής του A, είναι τουλάχιστον $1/e$, άρα $Pr[\varepsilon_1] \geq 1/e$.
Απόδειξη. Χωρίς βλάβη της γενικότητας, υποθέτουμε πως ο A δε θέτει ερωτήματα υπογραφών του ιδίου μηνύματος πάνω από μια φορά. Αποδεικνύουμε επαγωγικά ότι μετά από i το πλήθος τέτοια ερωτήματα, η πιθανότητα ο B να μην έχει σταματήσει είναι τουλάχιστον $(1 - 1/(q_s + 1))^i$. Ο ισχυρισμός είναι τετριμμένος για $i = 0$. Έστω M_i το i-στό ερώτημα υπογραφής του A και $< M_i, w_i, b_i, c_i >$ η σχετική μ' αυτό τετράδα στη H-λίστα. Τότε προτού απαντηθεί το ερώτημα - αφού η τιμή c_i είναι ανεξάρτητη των κινήσεων του A - η μοναδική τιμή που να μπορεί να δοθεί στον A και να εξαρτάται από τη c_i είναι η $H(M_i)$. Όμως η κατανομή των τιμών στην H είναι η ίδια είτε $c_i = 0$ είτε $c_i = 1$, οπότε η πιθανότητα σ' αυτό το ερώτημα ο B να σταματήσει είναι το πολύ $1/(q_s + 1)$. Από την επαγωγική υπόθεση και την ανεξαρτησία των c_i η πιθανότητα μετά απ' αυτό το ερώτημα ο B να μη σταματήσει είναι τουλάχιστον $(1 - 1/(q_s + 1))^i$ όπου και αποδεικνύει τον Ισχυρισμό. Από τη στιγμή που ο A θέτει q_s το πολύ ερωτήματα υπογραφών, η πιθανότητα ο B να μη σταματήσει, ως αποτέλεσμα όλων των ερωτήσεων υπογραφής είναι τουλάχιστον $(1 - 1/(q_s + 1))^{q_s} \geq 1/e$.

Ισχυρισμός Β: Αν ο αλγόριθμος B δε σταματήσει ως αποτέλεσμα των ερωτημάτων του A, τότε η συμπεριφορά του αλγόριθμου A ταυτίζεται με αυτή μιας πραγματικής επίθεσης, συνεπώς $Pr[\varepsilon_2|\varepsilon_1] \geq \epsilon$.
Απόδειξη. Το δημόσιο κλειδί που δίδεται στον A προκύπτει από την ίδια κατανομή που προκύπτει ένα δημόσιο κλειδί το οποίο παρέχεται από τον αλγόριθμο Απόδοσης Κλειδιών. Οι απαντήσεις στα H-ερωτήματα είναι όπως ακριβώς και στις πραγματικές επιθέσεις από τη στιγμή που κάθε ανταπόκριση σ' αυτά είναι ομοιόμορφα και ανεξάρτητα κατανεμημένη στη G_1. Αφού όλες οι απαντήσεις στα ερωτήματα υπογραφών είναι ισχύουσες, ο A θα παρουσιάσει ένα ισχύον ζεύγος μηνύματος - υπογραφής με πιθανότητα τουλάχιστον ϵ άρα $Pr[\varepsilon_2|\varepsilon_1] \geq \epsilon$.

Ισχυρισμός Γ: Η πιθανότητα ο αλγόριθμος B να μη σταματήσει μετά

που ο A θα έχει παρουσιάσει ένα ισχύον ζεύγος μηνύματος -υπογραφής είναι τουλάχιστον $1/(q_s+1)$, οπότε $Pr[\varepsilon_3|\varepsilon_1 \wedge \varepsilon_2] \geq 1/(q_s+1)$.
Απόδειξη. Έχοντας ως δεδομένο ότι τα $\varepsilon_1, \varepsilon_2$ πραγματοποιούνται, ο B θα σταματήσει μόνο όταν ο A θα δώσει μια πλαστογραφία (M_f, σ_f) η οποία στην τετράδα $< M_f, w, b, c >$ της H-λίστας έχει $c = 1$. Τη στιγμή που ο A εξάγει τα αποτελέσματά του, γνωρίζει τις τιμές των c_i για κάθε ένα M_i στο οποίο τίθεται ερώτημα υπογραφής. Όλα τα εναπομείναντα c_i είναι ανεξάρτητα της δράσης του A. Έτσι αν ο A δε ζητήσει υπογραφή για το M_i τότε η μοναδική τιμή που του δίνεται και εξαρτάται από τα c_i, είναι η τιμή $H(M_i)$ η οποία είναι η ίδια είτε $c_i = 0$ είτε $c_i = 1$. Επειδή ο A δε γίνεται να έχει ζητήσει υπογραφή για το M_f, ξέρουμε πως το c είναι ανεξάρτητο των προηγούμενων κινήσεων του A οπότε $Pr[c = 0|\varepsilon_1 \wedge \varepsilon_2] \geq 1/(q_s+1)$ όπως ακριβώς απαιτείται.

Χρησιμοποιώντας τα φράγματα που βρήκαμε στους παραπάνω Ισχυρισμούς παίρνουμε το ότι ο B παρέχει τη σωστή απάντηση στο πρόβλημά μας με πιθανότητα τουλάχιστον $\epsilon/e \cdot (q_s+1) \geq \epsilon'$. Ο χρόνος που χρειάζεται να εκτελεσθεί ο B είναι ίσος με αυτόν που χρειάζεται να εκτελεσθεί ο A συν το χρόνο που απαιτείται να απαντηθούν $(q_s + q_H)$ το πλήθος ερωτήματα τιμών της H και q_s το πλήθος ερωτήματα υπογραφών. Κάθε ερώτημα περιέχει μια εκθετοποίηση στη G_1 η οποία δεχόμαστε ότι εκτελείται σε χρόνο c_{G_1} άρα ο συνολικός χρόνος υλοποίησης του αλγορίθμου μας θα ισούται με $t + c_{G_1}(q_H + q_s) \leq t'$ όπως και απαιτείται. ο.ε.δ.

4.3.2 Η αναγκαιότητα της $\psi : G_2 \rightarrow G_1$

Ανατρέχοντας στην απόδειξη της ασφάλειας του σχήματος υπογραφής που μόλις παραθέσαμε, συναντάμε την ύπαρξη ενός αποτελεσματικά υπολογίσιμου ισομορφισμού $\psi : G_2 \rightarrow G_1$. Για να καταλάβουμε πόσο απαραίτητος είναι αυτός ο ισομορφισμός, παραθέτουμε ένα παράδειγμα μιας αποδεκτής διγραμμικής απεικόνισης $e : G_1 \times G_2 \rightarrow G_T$ για την οποία το co-CDH θεωρείται δύσκολο στο ζεύγος (G_1, G_2), μολαταύτα το παραχθέν εξ αυτού σχήμα υπογραφής είναι μη ασφαλές.

Έστω $q \in \mathbb{P}$ και G_2 μια υποομάδα της $\mathbb{Z}_q^*$ τάξεως $p \in \mathbb{P}$ με γεννήτορα g. Έστω επίσης $G_1 := \{0, 1, ..., p-1\}$ η ομάδα με πράξη την πρόσθεση modulo p. Ορίζουμε την απεικόνιση $e : G_1 \times G_2 \rightarrow G_2$ ως $e(x, y) = y^x$. Η απεικόνιση αυτή φαίνεται καθαρά πως είναι διγραμμική αφού $e(ax, y^b) = e(x, y)^{ab}$. Το co-CDH πρόβλημα στο ζεύγος (G_1, G_2) έχει ως εξής: Αν δίδονται τα $g, g^a \in G_2$ και το $x \in G_1$ να υπολογισθεί το $ax \in G_1$. Το πρόβλημα αυτό θεωρούμε πως είναι δύσκολο αφού η ύπαρξη ενός αλγόριθμου επίλυσης του co-CDH στις (G_1, G_2) θα οδηγούσε σε κάποιον αλγόριθμο επίλυσης του προβλήματος

διακριτού λογαρίθμου στη G_2. Βλέπουμε πως το (G_1, G_2) ικανοποιεί όλες τις προϋποθέσεις του Θεωρήματος εκτός του ότι δεν υπάρχει κανένας γνωστός ισομορφισμός $\psi : G_2 \to G_1$. Το παραγόμενο από αυτή την απεικόνιση σχήμα, θα είναι μη ασφαλές: για ένα δοσμένο ζεύγος μηνύματος - υπογραφής, είναι εύκολο να ανακτήσει κάποιος το μυστικό κλειδί του υπογράφοντος (μπορούμε μέσω του ευκλείδιου αλγοριθμου να υπολογίζουμε σε μια προσθετική ομάδα την τιμή γ αν $A = \gamma B$, με τα A, B να είναι γνωστά στοιχεία της ομάδας αυτής).

Χωρίς την ύπαρξη του ψ θα έπρεπε να είναι απαραίτητη (αναφορικά με την απόδειξη της ασφάλειας του σχήματος) η υπόθεση ότι κανένας αλγόριθμος πολυωνυμικού χρόνου δεν μπορεί να υπολογίσει το h^a αν του δίδονται τα $g_2, g_2^a \in G_2$ και τα $g_1, g_1^a \in G_1$. Εφόσον όμως η ψ υπάρχει με ένα φυσικό τρόπο σε όλα τα ζεύγη ομάδων (G_1, G_2) τα οποία έχουμε θεωρήσει, δεν υπάρχει λόγος επιστράτευσης αυτής της ισχυρότερης υπόθεσης πολυπλοκότητας.

Κεφάλαιο 5

ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΩΝ ΒΑΣΙΣΜΕΝΑ ΣΕ ΔΙΑΚΡΙΤΙΚΑ ΤΑΥΤΟΤΗΤΑΣ, ΑΠΟ Α.Δ.Α.

Η κατασκευή των σχημάτων ψηφιακής υπογραφής βασισμένων σε διακριτικά ταυτότητας (ID-σχήματα ψηφιακής υπογραφής) απορρέει από την κατανόηση της σπουδαιότητας των ID-πρωτοκόλλων, αναφορικά με την "οικονομία"που παρέχουν στους διαύλους / κανάλια ανταλλαγής πληροφοριών, αφού δεν απαιτείται η διαβίβαση του δημοσίου κλειδιού του χρήστη. Η χρησιμοποίηση της Α.Δ.Α. Weil σε τέτοια σχήματα οφείλεται στην ταχύτητα υπολογισμού της, μέσα στους αλγόριθμους που εμπεριέχονται στα σχήματα αυτά. Υπάρχει βέβαια και η άποψη σύμφωνα με την οποία η χρησιμοποίηση της Α.Δ.Α. Weil, θα οδηγούσε, αν όχι στη λύση, τουλάχιστον στην απλοποίηση ενός προβλήματος από μια ομάδα σε μια άλλη (όπως π.χ. η αναγωγή του DLP από συγκεκριμένες ελλειπτικές καμπύλες σε ένα πεπερασμένο σώμα), όμως ακόμα και σ' αυτές τις περιπτώσεις μπορούμε να εξασφαλίσουμε δυσκολία λύσης του (στο παράδειγμά μας αυτό, γίνεται αν το πεπερασμένο σώμα είναι αρκετά μεγάλο).

5.1 Κατασκευή ID-σχήματος ψηφιακής υπογραφής

Παραθέτουμε τους ακόλουθους ορισμούς όσον αφορά ένα ID- σχήμα (ψηφιακής) υπογραφής και τα μέρη από τα οποία αυτό αποτελείται.

ID-σχήμα υπογραφής Ένα ID- σχήμα υπογραφής $\mathcal{E}$ αποτελείται από

τους εξής τέσσερεις αλγορίθμους: Προεργασιών, Απόδοσης Κλειδιών, Υπογραφής και Πιστοποίησης. Σε κάθε τέτοιο σύστημα θεωρούμε ότι μετέχουν τρία μέλη: ο υπογράφων, ο διαπιστευτής (που μπορεί να είναι οποιοσδήποτε θέλει να πιστοποιήσει τη γνησιότητα μιας υπογραφής, για οποιονδήποτε λόγο) και μια Έμπιστη Αρχή - συμβ. Ε.Α.-(ή κατά άλλη ορολογία *Γεννήτορας Προσωπικών Κλειδιών*) η οποία δημιουργεί κλειδιά.
Έστω $(G,+),(V,\cdot)$ ομάδες τάξεως $l \in \mathbb{P}$ και $e : G \times G \to V$ η Α.Δ.Α. Weil η οποία υπενθυμίζουμε πως ικανοποιεί τις ιδιότητες:

• Διγραμμικότητα: $e(x_1 + x_2, y) = e(x_1, y) \cdot e(x_2, y)$ και $e(x, y_1 + y_2) = e(x, y_1) \cdot e(x, y_2)$ $\forall x_1, x_2, y_1, y_2 \in G$.

• Μη εκφυλισμός: Υπάρχει $x \in G$ και $y \in G$ τ.ω. $e(x, y) \neq 1$.

• Η τιμή $e(x, y)$ είναι εύκολα υπολογίσιμη ενώ, παράλληλα, για τα τυχαία $b \in G, c \in V$ είναι μη εφικτός ο υπολογισμός ενός $x \in G$ τ. ω. $e(x, b) = c$.

Έστω επίσης

$$H : \{0,1\}^* \to G\backslash\{0\}$$

ότι είναι μια κρυπτογραφική συνάρτηση "κόφτης". Τις τιμές της H μπορούμε να τις σκεφτόμαστε ως τυχαίες, έχοντας όμως κατά νου ότι είναι απίθανο η εικόνα δύο διαφορετικών μηνυμάτων μέσω αυτής να είναι η ίδια, ενώ φυσικά αν για το ίδιο μήνυμα ζητηθεί πάνω από μια φορά η εικόνα του (μέσω της H) θα πάρουμε την ίδια τιμή.

Αλγόριθμος Προεργασιών Κατά την εκτέλεση του αλγορίθμου αυτού, η Έμπιστη Αρχή διαλέγει τυχαία ένα στοιχείο $P \in G\backslash\{0\}$ με τη G να είναι μια προσθετική ομάδα γνωστής τάξεως $l \in \mathbb{P}$ και έναν μυστικό ακέραιο $t \in \mathbb{F}_l^\times$. Στη συνέχεια υπολογίζει $Q_{EA} = tP$ και δημοσιοποιεί το (P, Q_{EA}). Η τιμή t θα παραμείνει γνωστή μόνο στην Ε.Α. .

Αλγόριθμος Απόδοσης Κλειδιών Ο αλγόριθμος αυτός υλοποιείται από την Ε.Α. οποτεδήποτε ένας υπογράφων επιθυμεί να του δοθεί το σχετικό με τα διακριτικά του ID, προσωπικό κλειδί. Συνεπώς, ενώ το δημόσιό του κλειδί προκύπτει ως $Q_{ID} = H(ID)$, το προσωπικό του κλειδί θα υπολογίζεται από την Ε.Α. ως $S_{ID} = tQ_{ID}$ και κατόπιν θα του δίδεται.

Αλγόριθμος Υπογραφής Κατά τον αλγόριθμο αυτό ο υπογράφων εκμεταλλευόμενος τα δεδομένα που διαθέτει, υπογράφει το μήνυμα που επιθυμεί, σύμφωνα με μια διαδικασία ορισμένη από το σχήμα υπογραφής το οποίο χρησιμοποιεί. Οι πράξεις οι οποίες εκτελούνται, θα καθορίσουν το πόσο ευέλικτο και γρήγορο θα είναι το σχήμα αυτό.

Αλγόριθμος Πιστοποίησης Ο αλγόριθμος αυτός θα παίρνει ως είσοδο τα δημοσίως γνωστά δεδομένα, καθώς επίσης και την προς εξακρίβωση εγκυρότητας υπογραφή και - εκμεταλλευόμενος κυρίως τις ιδιότητες που του παρέχει η Α.Δ.Α. Weil - θα αποφαίνεται κατά πόσον είναι έγκυρη ή όχι η υπογραφή αυτή.

5.2 Βασική ιδέα ορισμού ασφάλειας ενός ID-σχήματος ψηφιακής υπογραφής

Το κατά πόσον είναι ασφαλές ένα σχήμα υπογραφής, ορίζεται έμμεσα μέσω ενός ιδεατού παιγνιδιού. Το παιγνίδι αυτό θεωρούμε ότι παίζεται ανάμεσα στον Επιτιθέμενο σ' ένα τέτοιο σχήμα και σ' εκείνον που τον προκαλεί (Προκαλών) παρέχοντάς του απαντήσεις στα ερωτήματά του. Σκοπός του Επιτιθέμενου είναι η υπαρκτή πλαστογραφία, η παραγωγή δηλαδή ενός ζεύγους μηνύματος - υπογραφής, όταν το εγχείρημά του αυτό γίνεται με προσαρμοζόμενες επιθέσεις επιλεγομένων μηνυμάτων. Τα βασικά στάδια του παιγνιδιού είναι τα εξής:

1ο στάδιο - Προεργασία Στο στάδιο αυτό ο Προκαλών ταυτίζεται με το ρόλο της Ε.Α. και υλοποιεί τον αλγόριθμο Προεργασιών.

2ο στάδιο - Επίθεση Ο Επιτιθέμενος μπορεί να κάνει στον Προκαλούντα έναν πολυωνυμικά φραγμένο αριθμό ερωτημάτων, με σταδιακή προσαρμογή στις εκάστοτε απαντήσεις που αυτός του δίνει. Οι τύποι των ερωτημάτων αυτών περιγράφονται ευθύς αμέσως:

-Ερωτήματα αποτίμησης των τιμών μιας συνάρτησης "κόφτη": Ο Επιτιθέμενος έχει τη δυνατότητα να ρωτήσει την τιμή οποιασδήποτε τέτοιας συνάρτησης που εμπεριέχεται στο πρωτόκολλο του σχήματος υπογραφής κατά του οποίου επιτίθεται, σε οποιοδήποτε σημείο του πεδίου ορισμού της.

-Ερωτήματα απόδοσης προσωπικών κλειδιών: Για κάθε υπογράφοντα με διακριτικά ID τα οποία θα διαλέξει ο Επιτιθέμενος, ο Προκαλών υπολογίζει το προσωπικό του κλειδί υλοποιώντας τον σχετικό αλγόριθμο και κατόπιν απαντά στο εν λόγω ερώτημα.

-Ερωτήματα υπογραφών: Για κάθε διακριτικό ID κάποιου χρήστη και κάθε μήνυμα m το οποίο επιλέγει ο Επιτιθέμενος, ο Προκαλών υποχρεούται να του δώσει την υπογραφή σ που θα έδινε ο υπογράφων αυτών των διακριτικών για το συγκεκριμένο μήνυμα.

3ο στάδιο - Πλαστογραφία Στο στάδιο αυτό ο Επιτιθέμενος παρουσιάζει μια τριάδα δεδομένων (σ, ID, m) όπου τα (ID, m) και ID δεν εμφανίζονται σε κανένα από τα παραπάνω ερωτήματα υπογραφών και απόδοσης προσωπικών κλειδιών, αντίστοιχα, κατά το προηγούμενο στάδιο. Ο Επιτιθέμενος θα θεωρούμε ότι κερδίζει το παιγνίδι αν ο αλγόριθμος Πιστοποίησης του σχήματος, αποφανθεί υπέρ της εγκυρότητας της συγκεκριμένης υπογραφής. Τέλος ορίζουμε ως πλεονέκτημα του Επιτιθέμενου, την πιθανότητα να νικήσει στο παραπάνω παιγνίδι.

Κεφάλαιο 6

ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΗΣ ΕΚΘΕΤΙΚΩΝ ΟΜΑΔΩΝ ΚΑΙ ID-ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΗΣ ΒΑΣΙΣΜΕΝΑ ΣΕ Α.Δ.Α.

Στο κεφάλαιο αυτό δίνουμε μια περιγραφή των σχημάτων υπογραφής που κατασκευάζονται από εκθετικές ομάδες και δείχνουμε το πώς αυτά, παράλληλα με χρησιμοποίηση κατάλληλων Α.Δ.Α., δίνουν αφορμή για δημιουργία ID-σχημάτων υπογραφής. Στη συνέχεια αποδεικνύουμε την ασφάλεια των σχημάτων αυτών και κατόπιν περιγράφουμε ένα συγκεκριμένο ID-σχήμα υπογραφής το οποίο είναι αρκούντως αποτελεσματικό όσον αφορά τη διάρκεια των υπολογισμών που εκτελούνται και το εύρος του χώρου των κρυπτογραφημένων μηνυμάτων. Τέλος αναπτύσσουμε ένα σχήμα, το οποίο δεν προκύπτει από ένα σχήμα υπογραφής από εκθετική ομάδα.

6.1 Κλασικά σχήματα υπογραφής από εκθετικές ομάδες

Αν $(G,+),(V,\cdot)$ ομάδες τάξεως πρώτου $l \in \mathbb{P}$ και

$$\exp : G \to V$$

ένας ισομορφισμός, τότε η ομάδα G θα ονομάζεται εκθετική, όταν ο υπολογισμός των εικόνων της exp θα είναι εύκολος, κάτι που δεν θα ισχύει όμως για τις προεικόνες της π.χ. η ομάδα G είναι εκθετική, με $G = \mathbb{F}_l^+$, V η υποομάδα

της $\mathbb{F}_q^\times$ η οποία γεννάται από το στοιχείο $\zeta_l = \zeta^{(q-1)/l}$ με το ζ γεννήτορα της $\mathbb{F}_q^\times$, $l|q-1$ και $\exp : x \mapsto \zeta_l^x$.
Με βάση τους παραπάνω ορισμούς μπορούμε να βλέπουμε τη συνάρτηση exp ως μια διαδικασία εκθετοποίησης και το πρόβλημα του διακριτού λογαρίθμου αντικαθίσταται από το πρόβλημα υπολογισμού των προεικόνων της exp δηλαδή από την αντιστροφή της exp.

Έστω ότι $a \in G \setminus \{0\}$ και $k \in \mathbb{F}_l^\times$. Ορίζουμε την ακόλουθη συνάρτηση "κόφτη":

$$h : \{0,1\}^* \times V \to \mathbb{F}_l^\times \times \mathbb{F}_l^\times.$$

Οι επιλογές για την h ποικίλουν και θα τις σχολιάσουμε μετέπειτα.
Ένα κλασικό σχήμα υπογραφής από εκθετική ομάδα, βασισμένο σε μια εκθετοποίηση και σε κάποιο δημόσιο κλειδί, αποτελείται από τους εξής τρεις αλγορίθμους: Προεργασιών, Υπογραφής και Πιστοποίησης.

Αλγόριθμος Προεργασιών Κατά τον αλγόριθμο αυτό, ο υπογράφων δημιουργεί ένα ζεύγος προσωπικού-δημόσιου κλειδιού $(a, y) \in G\setminus\{0\}\times V\setminus\{1\}$ με το να διαλέγει ένα τυχαίο $a \in G \setminus \{0\}$. Στη συνέχεια υπολογίζει την τιμή $y = \exp(a)$ και το κοινοποιεί.

▷ ΣΧΗΜΑ 1.

Αλγόριθμος Υπογραφής Για την υπογραφή ενός μηνύματος m ο υπογράφων επιλέγει τυχαία ένα $k \in G \setminus \{0\}$ και στη συνέχεια υπολογίζει:
1. $r = \exp(k)$.
2. $(v, w) = h(m, r)$.
3. $u = av + kw$.

Η υπογραφή στο σχήμα αυτό θα είναι το ζεύγος $(u, r) \in G \times V \setminus \{1\}$.
Αλγόριθμος Πιστοποίησης Κατά τον αλγόριθμο αυτό, αναφορικά με ένα μήνυμα m και μια υπογραφή (u, r) ένας διαπιστευτής προβαίνει στα εξής :
1. Υπολογίζει την τιμή $(v, w) = h(m, r)$.
2. Δέχεται την υπογραφή ως ισχύουσα και έγκυρη αν και μόνον αν $\exp(u) = y^v \cdot r^w$.

Το ότι η ισότητα πιστοποίησης ισχύει για μια έγκυρη υπογραφή, έπεται από την ακόλουθη αλγεβρική διαδικασία :

$$\exp(u) = \exp(av + kw) = \exp(a)^v \cdot \exp(k)^w = y^v \cdot r^w.$$

Υπάρχει όπως προαναφέραμε μια ποικιλία στις επιλογές της h. Αν $h_1 : \{0,1\}^* \to \mathbb{F}_l^\times, h_2 : V \to \mathbb{F}_l^\times$ και $h_3 : \{0,1\}^* \times V \to \mathbb{F}_l^\times$, είναι συναρτήσεις "κόφτες", μπορούμε τότε για παράδειγμα να θεωρήσουμε ως $h(m, r)$ την $h(m, r) := (h_1(m), h_2(r))$ ή την $h(m, r) := (h_3(m, r), 1)$.
Η επιλογή $h(m, r) := (h_1(m), r)$ δε θα ήταν αποδεκτή σε μια τέτοια περίπτωση.

▷ ΣΧΗΜΑ 2.

Αλγόριθμος Υπογραφής Για την υπογραφή ενός μηνύματος m ο υπογράφων επιλέγει τυχαία ένα $k \in G \setminus \{0\}$ και στη συνέχεια υπολογίζει:
1. $r = \exp(k)$.
2. $v = h_3(m, r)$.
3. $u = av + k$.

Η υπογραφή στο σχήμα αυτό θα είναι το ζεύγος $(u, v) \in G \times \mathbb{F}_l^{\times}$.

Αλγόριθμος Πιστοποίησης Κατά τον αλγόριθμο αυτό, αναφορικά με ένα μήνυμα m και μια υπογραφή (u, v) ένας διαπιστευτής προβαίνει στα εξής :
1. Υπολογίζει την τιμή $r = \exp(u) \cdot y^{-v}$.
2. Δέχεται την υπογραφή ως ισχύουσα και έγκυρη αν και μόνον αν $v = h_3(m, r)$.

Από μια δοσμένη $\exp : G \to V$ μπορούμε να παράγουμε και άλλες εκθετοποιήσεις με τον εξής τρόπο: Έστω $g \in G \setminus \{0\}$. Ορίζουμε την απεικόνιση $\exp_g : \mathbb{F}_l \to V$ ως $\exp_g(x) := \exp(xg)$. Είναι εύκολο να δούμε πως αν μπορούσαμε να υπολογίσουμε τις προεικόνες της $\exp_g$, τότε θα μπορούσαμε να υπολογίσουμε και εκείνες της exp.

6.2 ID-σχήματα υπογραφής από Α.Δ.Α.

Στην παράγραφο αυτή περιγράφουμε τον τρόπο με τον οποίο μη εκφυλισμένες Α.Δ.Α. μπορούν να χρησιμοποιηθούν στην κατασκευή ID- σχημάτων υπογραφής. Υπάρχουν δύο τέτοιες μέθοδοι κατασκευής. Συγκεκριμένα, στην πρώτη από αυτές ένα σχήμα υπογραφής οποιασδήποτε εκθετικής ομάδας, μετατρέπεται μέσω μιας διαδικασίας σε ID-σχήμα υπογραφής.

6.2.1 Παραγωγή ID-σχημάτων υπογραφής (μέρος Ι) : μέθοδος μετατροπής σχημάτων υπογραφής εκθετικών ομάδων

Από μια δοσμένη Α.Δ.Α $e : G \times G \to V$ όπως η Α.Δ.Α. Weil, μπορούμε να πάρουμε έναν ισομορφισμό $\exp : G \longrightarrow V$ όπου $\exp(x) := e(x, P)$. Η ιδέα είναι να χρησιμοποιήσουμε αυτή την εκθετοποίηση στα Σχήματα 1 και 2. Προχωρώντας στους αλγόριθμους Υπογραφής και Πιστοποίησης με βάση την εκθετοποίηση exp και παίρνοντας $a = S_{ID}$, ο διαπιστευτής πρέπει να ελέγξει αν $e(u, P) = y^v \cdot r^w$ όπου $y = \exp(a)$ είναι ένα κοινοποιήσιμο δεδομένο του υπογράφοντος διακριτικών ID. Έτσι έχουμε:

$y = e(a, P) = e(tQ_{ID}, P) = e(Q_{ID}, tP) = e(Q_{ID}, Q_{EA})$.

Παρατηρούμε πως ο διαπιστευτής χρειάζεται μόνο τα διακριτικά του υπογράφοντος (δίχως κάποιο επιπλέον κοινοποιήσιμο δεδομένο παρά αυτού) και το

δημόσιο κλειδί της Ε.Α. , ώστε να αποφανθεί υπέρ της εγκυρότητας ή μη της υπογραφής. Με βάση τα παραπάνω μπορούμε να διατυπώσουμε το ακόλουθο Θεώρημα.

ΘΕΩΡΗΜΑ 9 *Τα σχήματα υπογραφών εκθετικών ομάδων, μπορούν να μετατραπούν σε ID-σχήματα υπογραφής με την προϋπόθεση να χρησιμοποιηθούν κατάλληλες Α.Δ.Α. .*

Προκειμένου να γίνουν περισσότερο κατανοητά τα όσα αναφέραμε, παρουσιάζουμε την προσαρμογή του Σχήματος 2 στη συγκεκριμένη μετατροπή.

▷ ΣΧΗΜΑ 3.

Αλγόριθμος Υπογραφής Για την υπογραφή ενός μηνύματος m ο υπογράφων επιλέγει τυχαία ένα $P_1 \in G \setminus \{0\}$, έναν τυχαίο ακέραιο $k \in \mathbb{F}_l^*$ και στη συνέχεια υπολογίζει:
1. $r = e(P_1, P)^k$.
2. $v = h_3(m, r)$.
3. $u = vS_{ID} + kP_1$.
Η υπογραφή στο σχήμα αυτό θα είναι το ζεύγος $(u, v) \in (G, \mathbb{F}_l^\times)$.

Αλγόριθμος Πιστοποίησης Κατά τον αλγόριθμο αυτό, αναφορικά με ένα μήνυμα m και μια υπογραφή (u, v), ένας διαπιστευτής προβαίνει στα εξής :
1. Υπολογίζει την τιμή $r = e(u, P) \cdot e(Q_{ID}, -Q_{EA})^v$.
2. Δέχεται την υπογραφή ως ισχύουσα και έγκυρη αν και μόνον αν $v = h_3(m, r)$.

Το ότι η ισότητα πιστοποίησης ισχύει για μια έγκυρη υπογραφή, έπεται από την ακόλουθη αλγεβρική διαδικασία :

$$e(u, P) = e(vS_{ID} + kP_1, P) = e(tQ_{ID}, P)^v \cdot e(kP_1, P) = e(Q_{ID}, Q_{EA})^v \cdot r.$$

6.2.2 Παραγωγή ID-σχημάτων υπογραφής (μέρος ΙΙ)

Στα προηγούμενα σχήματα υπογραφής χρησιμοποιήσαμε την ιδιότητα της διγραμμικότητας ώστε να εκφράσουμε τα επιπλέον κοινοποιήσιμα δεδομένα του υπογράφοντος συναρτήσει των διακριτικών του (στην ουσία του δημοσίου κλειδιού αυτού) καθώς επίσης συναρτήσει και του δημοσίου κλειδιού της Ε.Α. . Εκτός αυτού του σημείου η διγραμμικότητα δεν χρησιμοποιήθηκε περαιτέρω. Στο σχήμα που ακολουθεί χρησιμοποιείται κατά κάποιο τρόπο "καθολικά"η συγκεκριμένη ιδιότητα.

Έστω $h' : \{0,1\} \times G \to \mathbb{F}_l^\times$ μια συνάρτηση "κόφτης".

▷ ΣΧΗΜΑ 4.

Αλγόριθμος Υπογραφής Για την υπογραφή ενός μηνύματος m ο υπογράφων επιλέγει τυχαία ένα $k \in \mathbb{F}_l^*$ και στη συνέχεια υπολογίζει:
1. $r = kP$.
2. $v = h'(m, r)$.
3. $u = (v/k)S_{ID}$.

Η υπογραφή στο σχήμα αυτό θα είναι το ζεύγος $(u, r) \in G \setminus \{0\} \times G \setminus \{0\}$.

Αλγόριθμος Πιστοποίησης Κατά τον αλγόριθμο αυτό, αναφορικά με ένα μήνυμα m και μια υπογραφή (u, r), ένας διαπιστευτής προβαίνει στα εξής :
1. Υπολογίζει την τιμή $v = h'(m, r)$.
2. Δέχεται την υπογραφή ως ισχύουσα και έγκυρη αν και μόνον αν $e(u, r) = e(Q_{ID}, Q_{EA})^v$.

Το ότι η ισότητα πιστοποίησης ισχύει για μια έγκυρη υπογραφή, έπεται από την ακόλουθη αλγεβρική διαδικασία :

$e(u, r) = e((v/k)S_{ID}, kP) = e(S_{ID}, P)^v = e(Q_{ID}, Q_{EA})^v$.

6.3 Αποδείξεις ασφάλειας

6.3.1 Ασφάλεια κλασικών σχημάτων υπογραφής εκθετικών ομάδων

Για τη μελέτη της ασφάλειας ενός σχήματος υπογραφής εκθετικής ομάδας, απαιτείται η προσαρμογή του γενικού ορισμού ασφάλειας, πάνω στο συγκεκριμένο σχήμα: μας ενδιαφέρουν δηλαδή η πιθανότητα επιτυχίας που θα έχει μια πλαστογραφία, όταν το εγχείρημα αυτό γίνεται με προσαρμοζόμενες επιθέσεις επιλεγομένων μηνυμάτων. Ο Επιτιθέμενος A σ' ένα τέτοιο σχήμα θεωρούμε ότι είναι μια πιθανοθεωρητική μηχανή Turing η οποία τρέχει σε πολυωνυμικό χρόνο και παίρνει στην είσοδό της το δημόσιο κλειδί y του υπογράφοντος. Κατά τα γνωστά, σκοπός της επίθεσης είναι η παραγωγή ενός ζεύγους μηνύματος -υπογραφής κάποιου καθορισμένου υπογράφοντος. Προκειμένου να διευκολύνουμε μια τέτοια επίθεση επιτρέπουμε στον Επιτιθέμενο ερωτήματα υπογραφών πάνω σε οποιοδήποτε μήνυμα m και για οποιοδήποτε δημόσιο κλειδί y. Στην απόδειξη του Θεωρήματος που ακολουθεί γίνεται χρήση ενός πολύ βασικού λήμματος για τις αποδείξεις ασφάλειας των σχημάτων υπογραφής (*Λήμμα διακλάδωσης*).

Λήμμα 1 *(Λήμμα διακλάδωσης (Forking Lemma) Έστω A μια πιθανοθεωρητική μηχανή Turing που τρέχει σε πολυωνυμικό χρόνο, της οποίας είσοδο αποτελούν μόνο δημοσίως κοινοποιημένα δεδομένα. Συμβολίζουμε με Q και R το πλήθος των ερωτημάτων που θέτει ο A στο Μοντέλο Χρησμών Τυχαιότητας και στον υπογράφοντα, αντίστοιχα. Υποθέτουμε ότι σε χρόνο το πολύ T, ο A δίνει με πιθανότητα $\varepsilon \geq 10(R+1)(R+Q)/2^l$, μια ισχύουσα υπογραφή $(m, \sigma_1, h, \sigma_2)$ όπου σ_1 το ανεξάρτητο της h μέρος της υπογραφής και σ_2 το εξαρτημένο. Αν υπάρχει τρόπος να προκύψουν τριάδες (σ_1, h, σ_2) δίχως τη γνώση του προσωπικού κλειδιού του υπογράφοντος, τότε υπάρχει μια άλλη μηχανή, η οποία θα προκύπτει από την A αντικαθιστώντας τα ερωτήματα στον υπογράφοντα από τις εν λόγω τριάδες, η οποία παράγει δύο ισχύουσες υπογραφές $(m, \sigma_1, h, \sigma_2)$ και $(m, \sigma_1, h', \sigma_2')$ τ.ω. $h \neq h'$ σε αναμενόμενο χρόνο το πολύ $T' \leq 120686QT/\varepsilon$.*

ΘΕΩΡΗΜΑ 10 *Υποθέτουμε πως υπάρχει ένας Επιτιθέμενος A σε ένα κλασικό σχήμα υπογραφής εκθετικής ομάδας, ο οποίος καταφέρνει να δημιουργήσει ένα ζεύγος μηνύματος -υπογραφής (υπαρκτή πλαστογράφηση), αφού πρώτα έχει θέσει και έχει πάρει απαντήσεις σε q_s-το πλήθος ερωτήματα υπογραφών και q_h-το πλήθος ερωτήματα τιμών μιας συνάρτησης "κόφτη"h σε σημεία που αυτός επιθυμεί, υπό τη συνθήκη ότι τα ερωτήματα αυτά υπάγονται στο Μοντέλο Χρησμών Τυχαιότητας. Γνωρίζουμε επίσης πως τα ερωτήματα γίνονται με*

βάση τις όποιες απαντήσεις διαθέτει μέχρι εκείνη τη στιγμή ο A και η πλαστογραφία που μας παρέχει γίνεται σε πολυωνυμικό χρόνο το πολύ T και με μη αμελητέα πιθανότητα $\epsilon > 10 \cdot (q_s + 1) \cdot (q_s + q_h)/l$.
Τότε υπάρχει ένας άλλος πιθανοθεωρητικός αλγόριθμος ο οποίος λύνει το πρόβλημα $\exp(a) = y$ ως προς a, σε πολυωνυμικό χρόνο $T' < 120686 \cdot q_h \cdot T/\epsilon$.

Απόδειξη Έστω A ο Επιτιθέμενος στο σχήμα μας. Θα χρησιμοποιήσουμε τον A για να κατασκευάσουμε έναν άλλο αλγόριθμο B_A ο οποίος θα έχει την ικανότητα να αντιστρέφει το exp.

Θεωρούμε ότι ως είσοδο στον B_A θα δίνουμε το δημόσιο κλειδί y. Ο B_A επιλέγει τυχαία ένα μήνυμα m και χρησιμοποιώντας τον A ως υπορουτίνα του, τότε θα πάρει από αυτόν σύμφωνα με το Λήμμα διακλάδωσης, δύο διαφορετικές πλαστογραφίες για το ίδιο μήνυμα, με κοινή την πρώτη συντεταγμένη :

$$(r, (v, w) = h(m, r), u) \qquad \kappa\alpha\iota \quad (r, (v', w') = h'(m, r), u').$$

Ο χρόνος υπολογισμού που χρειάζεται ο B_A ώστε να μας δώσει αυτά τα δυο ζεύγη πλαστογραφημένων μηνυμάτων, σύμφωνα με το Λήμμα διακλάδωσης θα 'ναι $T' < 120686 \cdot q_h \cdot T/\epsilon$.

Από τη στιγμή που η τιμή r είναι κοινή στις άνωθεν δύο πλαστογραφίες (Σχήμα 1), θα ισχύει η ισότητα $\exp(u - (w/w')u') = y^{v-(w/w')v'}$.

Επιπλέον αφού οι τιμές των h, h' προκύπτουν από το Μοντέλο Χρησμών Τυχαιότητας, περιμένουμε πως τα ζεύγη $(v, w), (v', w')$ θα είναι $\mathbb{F}_l$-γραμμικώς ανεξάρτητα μεταξύ τους (το οποίο μας εξασφαλίζει αποφυγή της ιδιάζουσας περίπτωσης να έχω εκθέτη του y ταυτοτικά ίσο με μηδέν) άρα $v-(w/w')v' \neq 0$. Συνεπώς ο αλγόριθμος B_A θα μπορεί να υπολογίσει την τιμή
$y = \exp((v - (w/w')v')^{-1} \cdot (u - (w/w')u'))$ οπότε και θα καταλήγουμε στη λύση του $\exp(a) = y$ ως προς a σε χρόνο T′.

Απομένει να εξηγήσουμε πως ο αλγόριθμος B_A θα απαντά στα ερωτήματα υπογραφών που θα του θέτει ο A. Όταν δίδεται ένα μήνυμα m στον B_A προς υπογραφήν, τότε αυτός μέσω μιας διαδικασίας παράγει τυχαία $u, u' \in G \setminus \{0\}$ καθώς επίσης και τυχαία γραμμικώς ανεξάρτητα διανύσματα
$(v, w), (v', w') \in \mathbb{F}_l^{\times} \times \mathbb{F}_l^{\times}$ και στη συνέχεια υπολογίζει τις ποσότητες $\lambda = (w - 1)/w'$ και $r = exp(u - \lambda u')/y^{v-\lambda v'}$. Σημειώνουμε πως το r είναι ένα τυχαίο στοιχείο του V. Αν έχει επιλεγεί $r = 1$ τότε ένα νέο διάνυσμα (v', w') επιλέγεται ώστε η τιμή του r να ανήκει στο $V \setminus \{1\}$. Ορίζουμε η τιμή της συνάρτησης "κόφτη"h στο διάνυσμα (m, r) να προκύπτει ως $h(m, r) = (v, w)$ και η σχετική μ' αυτή την τιμή υπογραφή θα είναι η (u, r). ο.ε.δ

Έστω πως $\exp_g$ είναι η εκθετοποίηση που προκύπτει από τις exp και $g \in G \setminus \{0\}$. Το πρόβλημα αντιστροφής της $\exp_g$ είναι τουλάχιστον όσο δύσκολο είναι το πρόβλημα αντιστροφής της exp. Από το τελευταίο Θεώρημα

είμαστε σε θέση να συμπεράνουμε πως τα σχήματα υπογραφών από μια εκθετοποίηση $\exp_g$ είναι τουλάχιστον τόσο ασφαλή όσο τα αντίστοιχα σχήματα από την απεικόνιση exp.

6.3.2 Ασφάλεια ID-σχημάτων υπογραφής από εκθετικές ομάδες

Η ασφάλεια των ID-σχημάτων υπογραφής τα οποία προέρχονται από σχήματα υπογραφής εκθετικών ομάδων, είναι επόμενο πως θα εξαρτάται από την ασφάλεια που παρέχουν τα τελευταία. Μελετώντας το Σχήμα 4, θα παρατηρήσουμε πως παίρνουμε ασθενέστερα αποτελέσματα ασφάλειας, τα οποία προκύπτουν με παρόμοιο τρόπο.

Θεωρούμε ως Επιτιθέμενο στο σχήμα αυτό, μια πολυωνυμικού χρόνου πιθανοθεωρητική μηχανή Turing A η οποία δέχεται στην είσοδό της τα δεδομένα (P, Q_{EA}, Q_{ID}) όπου P είναι ένα δημοσιοποιημένο από την Ε.Α. σημείο και Q_{ID}, Q_{EA} τα δημόσια κλειδιά του υπογράφοντος και της Ε.Α. αντίστοιχα. Σκοπός της επίθεσης είναι η πλαστογραφία και κατ' επέκταση η παρουσίαση ενός ζεύγους μηνύματος -υπογραφής που να αντιστοιχεί στα συγκεκριμένα διακριτικά του υπογράφοντος. Στην προσπάθεια αυτή του Επιτιθέμενου επιτρέπουμε να γίνονται τα παρακάτω ερωτήματα:

Ερωτήματα απόδοσης προσωπικών κλειδιών: Για κάθε δοσμένα (από τον Επιτιθέμενο) διακριτικά $ID' \neq ID$ κάποιου υπογράφοντος, το Μοντέλο Χρησμών Τυχαιότητας του παρέχει το αντίστοιχο, προσωπικό κλειδί $S_{ID'}$.

Ερωτήματα υπογραφών: Για κάθε δοσμένο μήνυμα m και διακριτικά υπογράφοντος ID, ο Επιτιθέμενος δύναται να μάθει την υπογραφή του συγκεκριμένου υπογράφοντος για το συγκεκριμένο μήνυμα.

Φυσικά η πλαστογραφία που θα παρουσιάσει στο τέλος των ερωτημάτων αυτών ο Επιτιθέμενος, δηλαδή το μήνυμα με την αντίστοιχη υπογραφή του, δεν συμπίπτει με κανένα από αυτά που, κατά τη διάρκεια του παιγνιδιού, έλαβε από τον Προκαλούντα.

ΘΕΩΡΗΜΑ 11 *Υποθέτουμε πως υπάρχει ένας Επιτιθέμενος A κατά του Σχήματος 3 (ή οποιουδήποτε άλλου ID-σχήματος το οποίο προέρχεται από σχήμα υπογραφής εκθετικής ομάδας), ο οποίος παρέχει ένα ζεύγος μηνύματος-υπογραφής, αφού πρώτα έχει θέσει και έχει πάρει απαντήσεις σε q_s-το πλήθος ερωτήματα υπογραφών και q_h-το πλήθος ερωτήματα τιμών μιας συνάρτησης "κόφτη"h σε σημεία που αυτός επιθυμεί στο Μοντέλο Χρησμών Τυχαιότητας. Γνωρίζουμε επίσης πως τα ερωτήματα γίνονται με βάση τις όποιες απαντή-*

σεις διαθέτει μέχρι εκείνη τη στιγμή ο A και η πλαστογραφία που μας παρέχει γίνεται σε πολυωνυμικό χρόνο το πολύ T και με μη αμελητέα πιθανότητα $\epsilon > 10 \cdot (q_s + 1) \cdot (q_s + q_h)/l$.
Τότε υπάρχει ένας άλλος πιθανοθεωρητικός αλγόριθμος ο οποίος λύνει το πρόβλημα $e(a, P) = e(Q_{ID}, Q_{EA})$ ως προς a, σε πολυωνυμικό χρόνο
$T' < 120686 \cdot q_h \cdot T/\epsilon$.

Απόδειξη Η επίλυση της $e(a, P) = e(Q_{ID}, Q_{EA})$ ως προς a, γίνεται ακολουθώντας τα ίδια βήματα της επίλυσης της $\exp(a) = y$ ως προς a, κατά την απόδειξη της ασφάλειας ενός κλασικού σχήματος υπογραφής από εκθετική ομάδα. Προφανώς όπου a θα θέσουμε πλέον S_{ID} και το δημόσιο κλειδί θα ισούται με $y = e(S_{ID}, P)$. Απομένει να εξηγήσουμε πως ο αλγόριθμος B_A θα απαντά στα ερωτήματα υπογραφών που θα του θέτει ο A.

Ερωτήματα απόδοσης κλειδιών: Όταν ο Επιτιθέμενος ρωτήσει το προσωπικό κλειδί του υπογράφοντος με διακριτικά ID', τότε υπολογίζονται διαδοχικά οι τιμές $Q_{ID'} = \lambda \cdot P, \quad S_{ID'} = \lambda \cdot Q_{EA}$ για ένα τυχαίο $\lambda \in \mathbb{F}_l^\times$. Στη συνέχεια ορίζεται $H(ID') := Q_{ID'}$ και σαν απάντηση στο ερώτημά του ο Επιτιθέμενος παίρνει την τιμή $S_{ID'}$. Οι όποιες τιμές υπολογίζονται κατά τη διάρκεια των ερωτημάτων αυτών, αποθηκεύονται ώστε για τα ίδια πιθανώς ερωτήματα να δίνονται πάντα οι ίδιες απαντήσεις.

Ερωτήματα υπογραφών: Ένα ερώτημα υπογραφής παριστάνεται ακριβώς όπως αυτά στις αποδείξεις ασφάλειας ενός κλασικού σχήματος υπογραφής εκθετικής ομάδας, όταν έχουμε μήνυμα m και δημόσιο κλειδί $y = e(Q_{ID}, Q_{EA})$ με $Q_{ID} = H(ID)$. Γενικά μπορούμε να δεχθούμε οποιαδήποτε ερωτήματα για κάθε Q και $y = e(Q, Q_{EA})$.

6.3.3 Ασφάλεια ID-σχημάτων υπογραφής

Όσον αφορά το Σχήμα 4 παραθέτουμε μια απόδειξη της ασφάλειας αυτού η οποία δεν μπορεί να χαρακτηρισθεί "αυστηρή". Προκειμένου να απαντηθεί ένα ερώτημα υπογραφής τότε -στο Μοντέλο Χρησμών Τυχαιότητας που γίνεται αυτή η απόδειξη- για κάποια τυχαία $\lambda, \mu \in \mathbb{F}_l^\times$ τίθενται $r := \lambda \cdot Q_{EA}, u := \mu \cdot Q_{ID}$ και ορίζεται η τιμή της h' στα m, r ως $h'(m, r) := \mu \cdot \lambda$. Ξανά οι τιμές της h' καταχωρίζονται κατάλληλα. Αν η τιμή Q_{ID} δεν είναι μέχρι εκείνη τη στιγμή γνωστή, τότε υπολογίζεται μέσω κάποιου ερωτήματος για το σχετικό κλειδί.

Έστω B_A αλγόριθμος ο οποίος θα έχει την ικανότητα χρησιμοποιώντας τον A ως υπορουτίνα του , κάποια στιγμή να δώσει δύο διαφορετικές πλαστογραφήσεις για το ίδιο μήνυμα m:

$$(r, v = h'(m, r), u) \qquad \text{και} \quad (r, v' = h''(m, r), u').$$

Από τη στιγμή που η τιμή r είναι κοινή στις άνωθεν δύο πλαστογραφίες, θα ισχύει η ισότητα $e(u-u', r) = e(Q_{ID}, Q_{EA})^{v-v'}$.

Στο σημείο αυτό θα πρέπει να αναφέρουμε το ότι η τιμή r πρέπει να έχει υπολογισθεί από τον αλγόριθμο B_A ή από τον A προτού το ερώτημα $h'(m, r)$ τεθεί (υπενθυμίζουμε πως στα ερωτήματα αυτά δίνονται απαντήσεις με τυχαιότητα). Ο B_A αναμένεται να είναι σε θέση να λύσει το πρόβλημα $e(a, r) = c$ με $c \in V$ τυχαίο ως προς a (κατόπιν πεπερασμένου πλήθους υπολογισμών, συμπεριλαμβανομένου και του καθορισμού ενός $r \in G$).

Θα περίμενε κανείς πως η λύση του $e(a, r) = c$ είναι κατά κάποιο τρόπο ανάλογης δυσκολίας με τη λύση του $e(a, P) = c$ για κάποιο προκαθορισμένο P αφού η ομάδα G είναι κυκλική.

Για κάθε $r \in G \setminus \{0\}$ η δυσκολία αντιστροφής της Α.Δ.Α Weil $e(\cdot, r)$ μπορεί να σχετισθεί με προβλήματα στις G, V όπως τα ακόλουθα: Ας υποθέσουμε πως έχουμε έναν υπολογίσιμο ισομορφισμό $\iota : V \to G$ ο οποίος αντιστρέφει την Α.Δ.Α Weil e, το οποίο είναι ο υπολογισμός του $x = e(\iota(x), P)$. Έστω f πως είναι ένας γεννήτορας της V. Τότε $g := e(\iota(f), \iota(f))$ είναι επίσης ένας γεννήτορας της V και επιπλέον έχουμε πως $e(\iota(f)^{\lambda}, \iota(f)^{\mu}) = g^{\lambda \cdot \mu}$. Σ' αυτή την περίπτωση για δοσμένα f^{λ}, f^{μ} υπολογίζουμε το $g^{\lambda \cdot \mu}$ και κατ' επέκταση έχουμε λύσει ένα στιγμιότυπο, ένα παράδειγμα δηλαδή, ενός προβλήματος που είναι γνωστό ως *Ασθενές (Weak) pr'oblhma Diffie-Hellman* στο V.

Κεφάλαιο 7

ΕΝΑ ID-ΠΡΩΤΟΚΟΛΛΟ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΑΠΟ Α.Δ.Α. , ΑΝΑΚΤΩΜΕΝΟΥ ΜΗΝΥΜΑΤΟΣ

Στο κεφάλαιο αυτό παρουσιάζουμε ένα ID-πρωτόκολλο υπογραφών το οποίο διαθέτει την ιδιότητα ανάκτησης του μηνύματος, που κάποιος χρήστης έχει υπογράψει, από την υπογραφή του σε αυτό. Η σημασία που μπορούμε να αποδώσουμε σε ένα τέτοιο σχήμα είναι μεγάλη για δύο λόγους: ο πρώτος εξ αυτών αξιώνει μια είδους "οικονομία"αλλά και ταχύτητα στην ανταλλαγή και μεταφορά πληροφοριών μεταξύ των μελών ενός τέτοιου σχήματος. Η μεταφορά του μηνύματος, της υπογραφής στο μήνυμα και του δημοσίου κλειδιού του χρήστη, μέσα στους διαύλους επικοινωνίας ενός κλασικού σχήματος υπογραφών, ανάγεται, στο πρωτόκολλο που θα παρουσιάσουμε, σε μεταφορά μονάχα της υπογραφής, αφού το μήνυμα εμπεριέχεται αλλά και ανακτάται από αυτή, ενώ ανάγκη για μεταφορά του δημοσίου κλειδιού του χρήστη δεν υπάρχει από τη στιγμή που το σχήμα είναι ID και ο καθένας μπορεί να το εκλάβει μέσω ενός κοινοποιημένου αλγορίθμου από τα διακριτικά του χρήστη. Ως δεύτερο λόγο θεωρούμε την, επιθυμητή, μειωμένη πιθανότητα επίθεσης πλαστογράφησης στο σχήμα, αφού οι πληροφορίες που μεταδίδονται στους διαύλους επικοινωνίας είναι περιορισμένες. Στην πράξη τα σχήματα ψηφιακών υπογραφών ανακτώμενου μηνύματος χρησιμοποιούνται πάνω σε μηνύματα σχετικά μικρού μήκους.

Το πρωτόκολλο που παρουσιάζουμε αποτελείται από τους αλγόριθμους Προεργασιών, Απόδοσης Κλειδιών, Υπογραφής και Ανάκτησης Μηνύματος. Τα μέλη που μετέχουν σ' αυτό θα είναι ένας υπογράφων, ένας διαπιστευτής και μια Έμπιστη Αρχή η οποία διαθέτει την ιδιότητα παραγωγής και απόδοσης

κλειδιών. Στο συγκεκριμένο πρωτόκολλο παίρνει μέρος μια κρυπτογραφική συνάρτηση "κόφτης"

$$H : \{0,1\}^* \to G$$

την οποία μπορούμε να βλέπουμε ως μια τυχαία επιλεγμένη συνάρτηση από το σύνολο των συναρτήσεων με πεδίο ορισμού το $\{0,1\}^*$. Εδώ η G είναι μια υποομάδα κάποιας ελλειπτικής καμπύλης Ε. Η διαδικασία που επιτελείται σε κάθε αλγόριθμο περιγράφεται ευθύς αμέσως:

Αλγόριθμος Προεργασιών
Κατά τον αλγόριθμο αυτό η Ε.Α. διαλέγει ένα τυχαίο σημείο P της G ($P \neq \mathcal{O}$), καθώς επίσης και έναν τυχαίο ακέραιο $t \in \mathbb{F}_q^*$ με $q \in \mathbb{P}$. Το t θα θεωρείται το μυστικό κλειδί της Ε.Α. . Στη συνέχεια υπολογίζει το δημόσιο κλειδί της Q_{EA} αποδίδοντάς του την τιμή $Q_{EA} = tP$ και κατόπιν το δημοσιοποιεί ταυτόχρονα με το σημείο P.

Αλγόριθμος Απόδοσης Κλειδιών
Όταν ένας χρήστης του πρωτοκόλλου επιθυμεί να υπολογίσει το δημόσιο κλειδί που αντιστοιχεί στα διακριτικά του ID, τότε απλά υπολογίζει την τιμή της H πάνω σ' αυτά και τελικά παίρνει το $Q_{ID} = H(ID)$. Το προσωπικό του κλειδί υπολογίζεται αντ' αυτού από την Ε.Α. ως $S_{ID} = tQ_{ID}$ και στη συνέχεια του παραδίδεται .

Προτού περιγράψουμε τη λειτουργία των αλγορίθμων Υπογραφής και Πιστοποίησης θα πρέπει να κάνουμε μια αναφορά σε μια ειδική κατηγορία συναρτήσεων, τις *συναρτήσεις πλεονασμού (redudancy functions)* που εμπεριέχονται σ' αυτούς. Έστω $\mathcal{M}$ ο χώρος των καθαρών μηνυμάτων και $\mathcal{M}'$ ο χώρος των υπογραφόμενων μηνυμάτων (είναι βασική αρχή των ψηφιακών υπογραφών να μην υπογράφεται ένα μήνυμα $m \in \mathcal{M}$, αλλά κάποιο υποκατάστατό του $m' \in \mathcal{M}'$). Οι συναρτήσεις πλεονασμού είναι δημοσίως γνωστές αμφιμονοσήμαντες συναρτήσεις $R : \mathcal{M} \to \mathcal{M}'$ όπου τα στοιχεία του $\mathcal{M}'$ διαθέτουν πολύ ιδιαίτερες ιδιότητες, έτσι ώστε τα στοιχεία του $R(\mathcal{M})$ να είναι, από πρακτική άποψη, αναγνωρίσιμα πολύ εύκολα και η πιθανότητα ένα τυχαία επιλεγμένο στοιχείο του $\mathcal{M}'$ να ανήκει στο $R(\mathcal{M})$, είναι πρακτικώς αμελητέα. Αφ' ετέρου, όμως, ο πρακτικός υπολογισμός των τιμών της $R^{-1} : R(\mathcal{M}) \to \mathcal{M}$ είναι εύκολος.

Αλγόριθμος Υπογραφής
Το πρωτόκολλο προϋποθέτει μια συνάρτηση πλεονασμού $R_1 : \mathcal{M} \to \mathcal{M}'$. Έχοντας επιλέξει το q να είναι πολύ μεγάλο, θεωρούμε τη συνάρτηση
$R_2 : R_1(\mathcal{M}) \to \mathbb{F}_q$ η οποία θα δίνει την q-αδική αναπαράσταση της τιμής $R_1(m)$ για το τυχαίο $m \in \mathcal{M}$. Ορίζουμε $R := R_2 \circ R_1$ με $R : \mathcal{M} \to \mathbb{F}_q$. Στη συνέχεια εκτελούνται τα παρακάτω βήματα:
ΒΗΜΑ 1ο Ο υπογράφων υπολογίζει το $\tilde{m} := R(m)$.

ΒΗΜΑ 2ο Ο υπογράφων επιλέγει έναν τυχαίο ακέραιο $k \in [1, ..., q-1]$ και τυχαίο $Q \in G$.

Στο πρωτόκολλο χρησιμοποιούμε την Α.Δ.Α. Weil
$e : G \times G \to \mathbb{F}_q^*$ η οποία ικανοποιεί τις παρακάτω ιδιότητες:
• Διγραμμικότητα: $\forall\ P, Q, R \in G$ έχουμε $e(P+Q, R) = e(P, R) \cdot e(Q, R)$ και $e(P, Q+R) = e(P, Q) \cdot e(P, R)$.
• Μη εκφυλισμός: $\exists\ P, Q \in G$ τ.ω. $e(P, Q) \neq 1$.
• Ικανότητα υπολογισμού: υπάρχει αποτελεσματικός αλγόριθμος που να υπολογίζει την τιμή $e(P, Q) \quad \forall\, P, Q \in G$.
Επιστρέφοντας στην περιγραφή του δεύτερου βήματος, έχουμε τον υπογράφοντα να υπολογίζει την τιμή $r := \tilde{m} \cdot e(Q, P)^k$.
ΒΗΜΑ 3ο Ο υπογράφων υπολογίζει την τιμή $s := S_{ID} + kQ$ και ορίζουμε την υπογραφή για το μήνυμα m, του χρήστη με διακριτικά ID να είναι το ζεύγος (r, s).

Αλγόριθμος Ανάκτησης Μηνύματος
Στο συγκεκριμένο αλγόριθμο ο διαπιστευτής της εγκυρότητας της υπογραφής, ελέγχει κατ' αρχάς αν $0 < r < q$ και αν $s \in G$. Αν δεν ισχύει κάτι εξ αυτών, απορρίπτει την υπογραφή. Στη συνέχεια υπολογίζει την τιμή

$$\tilde{m} = e(Q_{ID}, Q_{EA}) \cdot (e(s, P))^{-1} \cdot r \pmod{q}.$$

Αν η υπογραφή είναι έγκυρη, τότε θα ισχύει:

$$e(s, P) r^{-1} = e(Q_{ID}, Q_{EA}) \tilde{m}^{-1}$$

διότι

$$\begin{aligned} e(s, P) &= e(S_{ID} + kQ, P) = e(S_{ID}, P) \cdot e(kQ, P) = e(S_{ID}, P) \cdot e(Q, P)^k \\ &= e(tQ_{ID}, P) \cdot e(Q, P)^k = e(Q_{ID}, P)^t \cdot r \cdot \tilde{m}^{-1} \\ &= e(Q_{ID}, Q_{EA}) \cdot r \cdot \tilde{m}^{-1}. \end{aligned}$$

Αποκτώντας το $\tilde{m}$, ο διαπιστευτής το μετατρέπει σε ακολουθία bit και ελέγχει αν ανήκει στο $R_1(\mathcal{M})$ Σε περίπτωση που όντως ανήκει, βρίσκει από ποιό μήνυμα m προέρχεται αυτό, υπολογίζοντας την τιμή $m = R_1^{-1}(m)$, ενώ σε κάθε άλλη περίπτωση απορρίπτει την υπογραφή.

Κεφάλαιο 8

ΠΑΡΑΡΤΗΜΑ Α′: ID-ΣΧΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΚΑΙ ΜΟΙΡΑΣΜΑΤΟΣ ΚΛΕΙΔΙΟΥ

8.1 Σχήματα κρυπτογράφησης

8.1.1 Βασικοί ορισμοί και έννοιες

Στην ID-κρυπτογράφηση δημοσίου κλειδιού, η απόδοση του δημοσίου κλειδιού του χρήστη επιτυγχάνεται, αν θεωρήσουμε ότι μπορεί να παραχθεί από κάποιο χαρακτηριστικό ή διακριτικό του γνώρισμα π.χ. από την ηλεκτρονική του διεύθυνση. Θέλοντας να δούμε την ID-κρυπτογράφηση από μια πιο φορμαλιστική σκοπιά παραθέτουμε τις ακόλουθες έννοιες:

ID-κρυπτογράφηση Ένα ID-σχήμα κρυπτογράφησης $\mathcal{E}$ αποτελείται από τους εξής τέσσερεις αλγορίθμους : Προεργασιών, Απόδοσης Κλειδιών, Κρυπτογράφησης και Αποκρυπτογράφησης.

Αλγόριθμος Προεργασιών (Setup) Ο αλγόριθμος αυτός δέχεται ως δεδομένα μια παράμετρο k (που ονομάζεται παράμετρος ασφαλείας του σχήματος και εξαρτάται από αυτό) και ως αποτέλεσμα δίνει τις *παραμέτρους προεργασιών* (συμβ. params) και ένα *μυστικό κλειδί* (συμβ. secret key). Οι παράμετροι προεργασιών είναι κάποιες παράμετροι που μεταξύ άλλων περιέχουν περιγραφή για τον πεπερασμένο χώρο μηνυμάτων $\mathcal{M}$ και περιγραφή για τον πεπερασμένο χώρο κρυπτογραφημένων μηνυμάτων $\mathcal{C}$. Ενώ όμως οι πα-

ράμετροι προεργασιών γίνονται δημοσίως γνωστές, το μυστικό κλειδί θα είναι γνωστό μόνο σε μια Έμπιστη Αρχή η οποία θα διαθέτει την ιδιότητα παραγωγής προσωπικών κλειδιών.

Αλγόριθμος Απόδοσης Κλειδιών (Extract) Ο αλγόριθμος αυτός παίρνει ως δεδομένα τις παραμέτρους προεργασιών, το μυστικό κλειδί και μια τυχαία λέξη $ID \in \{0,1\}^*$ και ως εξαγόμενο δίνει το προσωπικό κλειδί (του χρήστη με το διακριτικό ID) d. Έτσι το ID, που είναι μια τυχαία λέξη, θα χρησιμοποιείται ως το δημόσιο κλειδί του χρήστη και το d θα είναι το αντίστοιχο για αυτό το δημόσιο κλειδί, προσωπικό του κλειδί.

Αλγόριθμος Κρυπτογράφησης (Encrypt) Ο αλγόριθμος αυτός παίρνει ως δεδομένα τα ID, ένα $M \in \mathcal{M}$ και ως εξαγόμενο δίνει ένα κρυπτογραφημένο μήνυμα $C \in \mathcal{C}$.

Αλγόριθμος Αποκρυπτογράφησης (Decrypt) Ο αλγόριθμος αυτός παίρνει ως δεδομένα το κρυπτογραφημένο μήνυμα $C \in \mathcal{C}$ και τα δημοσίως κοινοποιημένα δεδομένα και ως εξαγόμενο δίνει το καθαρό μήνυμα $M \in \mathcal{M}$ από το οποίο προέκυψε το C.

Ασφάλεια επιλεγομένων κρυπτογραφημένων μηνυμάτων Η *ασφάλεια επιλεγομένων κρυπτογραφημένων μηνυμάτων* (Chosen Ciphertext Security συμβ. IND-CCA) αποτελεί μια ευρείας αποδοχής έννοια για την ασφάλεια ενός σχήματος κρυπτογράφησης δημοσίου κλειδιού . Όταν κάποιος επιτίθεται (δηλαδή προσπαθεί να αποκρυπτογραφήσει κάποιο μήνυμα, αντί κάποιου χρήστη με δημόσιο κλειδί ID, χωρίς να διαθέτει το προσωπικό κλειδί του χρήστη) το συγκεκριμένο μοντέλο ασφάλειας του παρέχει τη δυνατότητα διάθεσης των προσωπικών κλειδιών σε οποιαδήποτε ακολουθία δημοσίων κλειδιών $ID_1, ID_2, ..., ID_n$ επιθυμεί αυτός - όλα διάφορα του ID - όμως το σύστημα οφείλει να παραμείνει ασφαλές ακόμα και τότε.

Προκειμένου να ορίσουμε ένα ID-σχήμα κρυπτογράφησης $\mathcal{E}$ ως *σημαντικά ασφαλές σχετικά με επιθέσεις επιλεγομένων κρυπτογραφημένων μηνυμάτων* (συμβ. IND-ID-CCA), θα θεωρούμε ότι γίνεται ένα παιγνίδι μεταξύ του Επιτιθέμενου και ενός προσώπου που απαντά στις κλήσεις των ερωτημάτων του για προσωπικά κλειδιά, τον οποίο θα καλούμε Προκαλούντα. Ζητάμε να μην όταν υπάρχει αλγόριθμος $\mathcal{A}$ ο οποίος θα εκτελείται σε μικρότερο του πολυωνυμικού χρόνου και ο οποίος θα έχει διαφορετική της αμελητέας [1] πιθανότητα κατά του Προκαλούντα, στο παρακάτω παιγνίδι:

- *Προεργασία*: Ο Προκαλών, διαθέτοντας την παράμετρο ασφαλείας k,

[1] Μια συνάρτηση $g : \mathbb{R} \to \mathbb{R}$ την ονομάζουμε *αμελητέα*, αν οι τιμές της $g(k)$ είναι μικρότερες από $1/f(k)$, για κάθε μη μηδενικό πολυώνυμο f.

εκτελεί τον αλγόριθμο Προεργασιών. Παίρνοντας τα αποτελέσματα αυτού, δίνει στον Επιτιθέμενο τις παραμέτρους προεργασιών και κρατά το μυστικό κλειδί κρυφό.

• *Πρώτη φάση*: Ο Επιτιθέμενος θέτει $q_1, q_2, ..., q_m$ ερωτήματα, όπου κάθε q_i μπορεί να ανήκει σε μια από τις παρακάτω κατηγορίες:
∘ Ερώτημα προσωπικού κλειδιού $< ID_i >$, με τον Προκαλούντα να απαντά στον Επιτιθέμενο, σύμφωνα με τον αλγόριθμο Απόδοσης Κλειδιών, το προσωπικό κλειδί d_i που αντιστοιχεί στο $< ID_i >$,
∘ Ερώτημα αποκρυπτογράφησης $< ID_i, C_i >$, με τον Προκαλούντα να απαντά στον Επιτιθέμενο, σύμφωνα με τους αλγορίθμους Απόδοσης Κλειδιών και Κρυπτογράφησης, το αποκρυπτογραφημένο μήνυμα που αντιστοιχεί στο κρυπτογραφημένο C_i.
Φυσικά ο Επιτιθέμενος, μπορεί να θέτει τα ερωτήματά του, προσαρμοζόμενος κάθε φορά στις απαντήσεις που λαμβάνει.

• *Πρόκληση*: Από τη στιγμή που ο Επιτιθέμενος αποφασίσει ότι η πρώτη φάση έχει τελειώσει, τότε εξάγει δύο ίσου μήκους καθαρά μηνύματα
$M_0, M_1 \in \mathcal{M}$ και ένα δημόσιο κλειδί ID στο οποίο επιθυμεί να προκληθεί. Ο μόνος περιορισμός για το ID είναι να μην εμφανίζεται στα ερωτήματα προσωπικών κλειδιών κατά την προηγούμενη φάση. Κατόπιν, ο Προκαλών διαλέγει ένα τυχαίο bit $b \in \{0, 1\}$, υπολογίζει το κρυπτογραφημένο μήνυμα $C = Encrypt(params, ID, M_b)$ και το στέλνει στον Επιτιθέμενο.

• *Δεύτερη φάση*: Ο Επιτιθέμενος θέτει επιπλέον ερωτήματα $q_{m+1}, q_{m+2}, ..., q_n$ όπου κάθε q_i μπορεί να είναι ερώτημα μιας από τις εξής κατηγορίες:
∘ Ερώτημα προσωπικού κλειδιού $< ID_i >$, όπου $ID_i \neq ID$. Ο Προκαλών τότε συμπεριφέρεται όπως ακριβώς στην πρώτη φάση.
∘ Ερώτημα αποκρυπτογράφησης $< ID_i, C_i > \neq < ID, C >$. Ο Προκαλών τότε συμπεριφέρεται όπως στην πρώτη φάση.
Ακριβώς όπως και στην πρώτη φάση, τα ερωτήματα μπορούν να γίνονται, ανάλογα με τις εκάστοτε απαντήσεις.

• *Απόφανση*: Ο Επιτιθέμενος αποφαίνεται το $b' \in \{0, 1\}$ και κερδίζει το παιγνίδι αν $b' = b$.
Καλούμε μια τέτοιου είδους επίθεση, στην οποία εμφανίζεται αλγόριθμος $\mathcal{A}$ (*επίθεση* $\mathcal{A}$) όπως η παραπάνω, ως IND-ID-CCA επίθεση. Ορίζουμε επίσης ως πλεονέκτημα της επίθεσης $\mathcal{A}$ κατά του σχήματος $\mathcal{E}$, να είναι η ακόλουθη συνάρτηση της παραμέτρου ασφαλείας k (η οποία δίδεται ως δεδομένο στον Προκαλούντα) :

$$Adv_{\mathcal{E},\mathcal{A}}(k) = |Pr[b = b'] - 1/2|.$$

Η πιθανότητα που εμπεριέχεται στον παραπάνω ορισμό αφορά την τυχαία επιλογή του b καθώς επίσης και τις τυχαίες επιλογές του $\mathcal{A}$. Χρησιμοποιώντας πλέον το παιγνίδι IND-ID-CCA, μπορούμε να ορίσουμε την ασφάλεια για ID-σχήματα κρυπτογράφησης.

Ορισμός 12 *Ορίζουμε ένα ID-σχήμα κρυπτογράφησης $\mathcal{E}$ ως σημαντικά ασφαλές σχετικά με επιθέσεις επιλεγομένων κρυπτογραφημένων μηνυμάτων, όταν για κάθε πολυωνυμικού χρόνου IND-ID-CCA επίθεση $\mathcal{A}$, η συνάρτηση $Adv_{\mathcal{E},\mathcal{A}}(k)$ είναι αμελητέα. Εν συντομία λέμε σ' αυτή την περίπτωση ότι το $\mathcal{E}$ να είναι IND-ID-CCA ασφαλές.*

Σε αυτό το σημείο μπορούμε να σημειώσουμε ότι ο ορισμός της ασφάλειας επιλεγομένων μηνυμάτων των κλασικών κρυπτοσυστημάτων (IND-CCA) είναι ο ίδιος με τον παραπάνω ορισμό, με τη μόνη διαφορά πως ο Επιτιθέμενος στο σχήμα προκαλείται αναφορικά με ένα τυχαίο δημόσιο κλειδί και όχι με κάποιο της επιλογής του.

8.1.2 ID-σχήμα κρυπτογράφησης σημαντικής ασφάλειας

Οι αποδείξεις ασφάλειας των Boneh-Franklin χρησιμοποιούν έναν ασθενέσθερο ορισμό ασφάλειας, γνωστό ως *σημαντική ασφάλεια* (ή αλλιώς σημαντική ασφάλεια σχετικά με επιθέσεις επιλεγομένων καθαρών μηνυμάτων). Η σημαντική ασφάλεια είναι μεν παρόμοια με την ασφάλεια σχετικά με επιθέσεις επιλεγομένων κρυπτογραφημένων μηνυμάτων, αλλά προϋποθέτει έναν επιπλέον περιορισμό για τον Επιτιθέμενο: του απαγορεύει να θέτει ερωτήματα αποκρυπτογράφησης κατά τη διάρκεια της επίθεσης για το προκληθέν δημόσιο κλειδί.

Όσον αφορά τα κλασικά κρυπτοσυστήματα δημοσίου κλειδιού, η σημαντική ασφάλεια αυτών ορίζεται από το ακόλουθο παιγνίδι:
(Βήμα 1) Δίνεται από τον Προκαλούντα στον Επιτιθέμενο ένα τυχαίο δημόσιο κλειδί.
(Βήμα 2) Ο Επιτιθέμενος δίνει δύο ίδιου μήκους μηνύματα M_0 και M_1 στον Προκαλούντα και κατόπιν λαμβάνει από αυτόν το κρυπτογραφημένο M_b, όπου το b είναι τυχαία επιλεγμένο από το $\{0,1\}$.
(Βήμα 3) Ο Επιτιθέμενος στο σχήμα, δίνει ως απάντησή του την b' σχετικά με το πιο μήνυμα κρυπτογραφήθηκε και νικά το παιγνίδι αν $b = b'$.
Το σχήμα δημοσίου κλειδιού που μελετάμε, θα είναι σημαντικά ασφαλές αν καμμία πολυωνυμικού χρόνου επίθεση δεν μπορέσει να νικήσει το παιγνίδι, με πιθανότητα διάφορη της αμελητέας.

Για να ορίσουμε τώρα σημαντική ασφάλεια σε ένα ID-σχήμα κρυπτογράφησης (συμβ. IND-ID-CPA) ενισχύουμε τον ορισμό που δώσαμε για τα κλασικά σχήματα κρυπτογράφησης, επιτρέποντας στον Επιτιθέμενο να κάνει και ερωτήματα προσωπικών κλειδιών που αντιστοιχούν σε ερωτηθέντα δημόσια κλειδιά. Αρχικά ο Επιτιθέμενος επιλέγει ένα δημόσιο κλειδί στο οποίο θα προκληθεί. Θα ορίσουμε τη σημαντική ασφάλεια σε ID-σχήματα κρυπτογράφησης χρησιμοποιώντας ένα IND-ID-CPA παιγνίδι, το οποίο διαφέρει από το IND-ID-CCA παιγνίδι μόνο κατά το ότι στο πρώτο δεν επιτρέπονται ερωτήματα αποκρυπτογράφησης εκ μέρους του Επιτιθέμενου.

Για να ορίσουμε ένα ID-σχήμα κρυπτογράφησης $\mathcal{E}$ ως σημαντικά ασφαλές (συμβ. IND-ID-CPA), μελετάμε ένα παιγνίδι μεταξύ του Προκαλούντα και του Επιτιθέμενου στο σχήμα. Για το παιγνίδι αυτό, που παραθέτουμε ευθύς αμέσως, δεν υπάρχει αλγόριθμος $\mathcal{A}$ που να τρέχει σε μικρότερο του πολυωνυμικού χρόνου, ο οποίος να έχει διαφορετική της αμελητέας πιθανότητα κατά του Προκαλούντα :

• *Προεργασία*: Ο Προκαλών διαθέτοντας την παράμετρο ασφαλείας k εκτελεί τον αλγόριθμο Προεργασιών. Παίρνοντας τα αποτελέσματα αυτού, δίνει στον Επιτιθέμενο τις παραμέτρους προεργασιών και κρατά το μυστικό κλειδί κρυφό.

• *Πρώτη φάση*: Ο Επιτιθέμενος θέτει $ID_1, ID_2, ..., ID_m$ ερωτήματα στον Προκαλούντα και λαμβάνει τα αντίστοιχα προσωπικά κλειδιά. Ο Προκαλών, δίνει στον Επιτιθέμενο, σύμφωνα με τον αλγόριθμο Απόδοσης Κλειδιών, το προσωπικό κλειδί d_i που αντιστοιχεί στο κάθε $< ID_i >$.
Τα ερωτήματα δύναται να γίνονται από τον Επιτιθέμενο με κάποιου είδους προσαρμογή στις απαντήσεις που λαμβάνει, ανάλογα με τις απαιτήσεις του.

• *Πρόκληση*: Από τη στιγμή που ο Επιτιθέμενος αποφασίσει ότι η πρώτη φάση έχει τελειώσει, τότε εξάγει δύο ίσου μήκους καθαρά μηνύματα
$M_0, M_1 \in \mathcal{M}$ και ένα δημόσιο κλειδί ID στο οποίο επιθυμεί να προκληθεί. Ο μόνος περιορισμός για το ID είναι να μην εμφανίζεται στα ερωτήματα προσωπικών κλειδιών κατά την προηγούμενη φάση. Κατόπιν, ο Προκαλών διαλέγει ένα τυχαίο bit $b \in \{0, 1\}$, υπολογίζει το κρυπτογραφημένο μήνυμα $C = Encrypt(params, ID, M_b)$ και το στέλνει στον Επιτιθέμενο, προς αποκρυπτογράφηση.

• *Δεύτερη φάση*: Ο Επιτιθέμενος θέτει επιπλέον ερωτήματα
$ID_{m+1}, ID_{m+2}, ..., ID_n$ όπου κάθε ID_i είναι ερώτημα προσωπικού κλειδιού με $ID_i \neq ID$. Ο Προκαλών τότε συμπεριφέρεται όπως ακριβώς στην πρώτη φά-

ση.
Εντελώς ανάλογα με την πρώτη φάση, τα ερωτήματα που γίνονται, προσαρμόζονται στις εκάστοτε απαντήσεις.

• *Απόφανση*: Ο Επιτιθέμενος αποφαίνεται το $b' \in \{0,1\}$ και κερδίζει το παιγνίδι αν $b' = b$.

Καλούμε μια τέτοιου είδους επίθεση $\mathcal{A}$ ως IND-ID-CPA επίθεση. Ορίζουμε όπως προηγουμένως, ως πλεονέκτημα της επίθεσης $\mathcal{A}$ κατά του σχήματος $\mathcal{E}$ να είναι η ακόλουθη συνάρτηση της παραμέτρου ασφαλείας k (η οποία δίδεται ως δεδομένο στον Προκαλούντα) :

$$Adv_{\mathcal{E},\mathcal{A}}(k) = |Pr[b = b'] - 1/2|.$$

Η πιθανότητα αυτή αφορά τα τυχαία bits που χρησιμοποιήθηκαν τόσο από τον Επιτιθέμενο, όσο και από τον Προκαλούντα. Είμαστε σε θέση πλέον, να ορίσουμε τη σημαντική ασφάλεια σε οποιοδήποτε ID-σχήμα κρυπτογράφησης.

Ορισμός 13 *Ορίζουμε ένα ID-σχήμα κρυπτογράφησης $\mathcal{E}$ ως σημαντικά ασφαλές, όταν για κάθε πολυωνυμικού χρόνου IND-ID-CPA επίθεση $\mathcal{A}$, η συνάρτηση $Adv_{\mathcal{E},\mathcal{A}}(k)$ είναι αμελητέα. Εν συντομία λέμε σ' αυτή την περίπτωση ότι το $\mathcal{E}$ να είναι IND-ID-CPA ασφαλές.*

Από τα παραπάνω γίνεται σαφές ότι, αν ένα σχήμα υπογραφής είναι IND-ID-CCA ασφαλές, τότε προφανώς θα είναι και IND-ID-CPA ασφαλές. Πράγματι, η μόνη διαφορά τους έγκειται στα ερωτήματα αποκρυπτογράφησης, τα οποία δεν υπάρχουν στο παιγνίδι, που καθορίζει τον δεύτερο από αυτούς ορισμό ασφάλειας.

8.2 Σχήματα συμφωνίας κλειδιού

Η επόμενη θεμελιώδης αρχή της Κρυπτογραφίας, την οποία θα μελετήσουμε, είναι το σχήμα συμφωνίας κλειδιού . Το πρώτο σύγχρονο πρωτόκολλο είναι αυτό των Diffie-Hellman [5], του οποίου οι εφαρμογές ήταν περιορισμένες. Παράλληλα άρχισαν να θεωρούνται αναγκαίες ορισμένες πολύ βασικές απαιτήσεις ασφάλειας για τα πρωτόκολλα αυτά (αφού π.χ. πρωτόκολλα, όπως το βασικό πρωτόκολλο των Diffie-Hellman, μειονεκτούσαν στις επιθέσεις παρεμβολής τρίτου, από την στιγμή που δεν απαιτείτο διαπίστευση των συμμετεχόντων σ' αυτό).

Μια απλή λύση έδωσε ο συνδυασμός ενός σχήματος συμφωνίας κλειδιού με ένα σχήμα ψηφιακής υπογραφής, ώστε να προκύψει ένα *πιστοποιήσιμο σχήμα συμφωνίας κλειδιού* (Authenticated Key Agreement Protocol, συμβ. A.K.) [6]. Μια τέτοια λύση, όμως, δημιουργεί τεχνικά προβλήματα, όπως η σημαντική αύξηση του μήκους των μηνυμάτων.

Οι Law, Menezes, Qu, Solinas και Vanstone [6] εισήγαγαν ένα A.K.-πρωτόκολλο, γνωστό και ως M.Q.V. πρωτόκολλο, το οποίο παρέχει πιστοποίηση των συμμετεχόντων, δίχως αύξηση ούτε του εύρους, ούτε του πλήθους των μεταβιβάσεων των μηνυμάτων αυτών. Επιπροσθέτως το πρωτόκολλο M.Q.V. μπορεί εύκολα να μετατραπεί σε πρωτόκολλο, στο οποίο οι μεταβιβάσεις γίνονται από τρείς εστίες και το οποίο παρέχει την επιπλέον ιδιότητα της επισφράγισης κλειδιού (δηλαδή της de facto εγκυρότητας των κλειδιών των συμμετεχόντων) και ονομάζεται *πιστοποιήσιμο σχήμα συμφωνίας κλειδιού με επισφράγιση κλειδιού* (Authenticated Key Agreement Protocol with Key Confirmation, συμβ. *A.K.C.*).

Η λειτουργία του πρωτοκόλλου M.Q.V. στηρίζεται στην υπόθεση κατά την οποία κάθε συμμετέχων, διαθέτει ένα ζεύγος κλειδιών Diffie-Hellman, δημόσιο και προσωπικό (χαρακτηριζόμενα και ως *στατικά κλειδιά*) και κάθε συμμετέχων γνωρίζει τα δημόσια κλειδιά των υπολοίπων. Όταν ξεκινά μια συνεδρία συμφωνίας κλειδιού, ορίζεται αρχικά το *κλειδί της συνεδρίας* μέσω μιας ανταλλαγής *προσωρινών* δημόσιων κλειδιών Diffie-Hellman. Τα προσωρινά και τα στατικά κλειδιά συνδυάζονται με έναν αρκετά έξυπνο τρόπο ώστε να παραχθεί το συμφωνηθέν κλειδί της συνεδρίας. Παρατηρούμε πως το πρόβλημα της πιστοποίησης του κλειδιού της συνεδρίας αντικαθίσταται από αυτό της πιστοποίησης των στατικών δημόσιων κλειδιών, το οποίο όμως μπορεί να λυθεί χρησιμοποιώντας μια θεμελιώδη προσέγγιση της κλασικής κρυπτογραφίας δημοσίου κλειδιού.

Στη συνέχεια παραθέτουμε ένα παράδειγμα ενός ID-πιστοποιήσιμου πρωτοκόλλου συμφωνίας κλειδιού, σε μια συνεδρία δύο συμμετεχόντων. Στον τρόπο με τον οποίο το κλειδί της συνεδρίας παράγεται φαίνεται καθαρά η χρήση μιας Α.Δ.Α. καθώς επίσης και των - ID - στατικών δημόσιων κλειδιών. Το πρω-

τόκολλο έχει επίσης την, ασυνήθιστη, ιδιότητα, η Έμπιστη Αρχή που μετέχει σ' αυτό (γεννήτορας προσωπικών κλειδιών, συμβ. Γ.Π.Κ.) να επανακτά το συμφωνηθέν κλειδί της συνεδρίας από τα μηνύματα και το μυστικό της κλειδί.

▷*Παράδειγμα Πιστοποιήσιμου Σχήματος Συμφωνίας Κλειδιού*
Υποθέτουμε ότι έχουμε μια υποομάδα $\mathbb{G}$ μιας ελλειπτικής καμύλης και μια αποδεκτή διγραμμική απεικόνιση $\hat{e}$ (στη συγκεκριμένη περίπτωση δουλεύουμε με την τροποποιημένη A.Δ.A. Weil), η οποία απεικονίζει τα στοιχεία της $\mathbb{G}$ σε ένα πεπερασμένο σώμα $\mathbb{F}_{q^k}$. Υποθέτουμε ότι q^k ($q \in \mathbb{P}$, $k \in \mathbb{N}$) είναι ένας αρκετά μεγάλος αριθμός ώστε το DLP να είναι δύσκολο στο εν λόγω πεπερασμένο σώμα. Επίσης υποθέτουμε πως η ελλειπτική καμπύλη περιέχει μια υποομάδα τάξης l στην οποία το DLP να είναι επίσης δύσκολο.
Έστω

$$V : \mathbb{F}_{q^k}^* \to \{0, 1\}$$

ότι είναι μια συνάρτηση παραγωγής κλειδιών. Έστω επίσης

$$H : \{0, 1\}^* \to \mathbb{G}$$

ότι είναι μια κρυπτογραφική συνάρτηση "κόφτης"(hush function).

Προεργασίες συστήματος (System setup)
Αρχικά ο Γ.Π.Κ. διαλέγει ένα μυστικό κλειδί $s \in \{1, ..., l-1\}$, κατόπιν παράγει ένα $P \in \mathbb{G}$ υπολογίζοντας το $P_{\Gamma\Pi K} = [s]P$, και στη συνέχεια δημοσιοποιεί το ζεύγος $(P, P_{\Gamma\Pi K})$. Όταν ένας χρήστης διακριτικών ID επιθυμεί να του αποδοθεί ένας ζεύγος προσωπικού/δημόσιου κλειδιού, τότε το δημόσιο κλειδί Q_{ID} προκύπτει από τον υπολογισμό

$$Q_{ID} = H(ID)$$

ενώ το προσωπικό του κλειδί S_{ID} παρέχεται δια του Γ.Π.Κ. , αφού έχει πρώτα υπολογίσει την τιμή

$$S_{ID} = [s]Q_{ID}.$$

Πιστοποιήσιμη ανταλλαγή κλειδιών
Υποθέτουμε ότι δύο χρήστες, A και B, επιθυμούν να συμφωνήσουν σε κάποιο κλειδί. Τα προσωπικά κλειδιά των δύο χρηστών τα συμβολίζουμε ως S_A, S_B όπου

$$S_A = [s]Q_A, S_B = [s]Q_B$$

τα έχουν παραλάβει από τον Γ.Π.Κ. . Ας θεωρήσουμε πως κάθε χρήστης διαθέτει από ένα προσωρινό κλειδί και έστω a, b τα κλειδιά αυτά για τους A και B, αντίστοιχα. Στη συνέχεια ξεκινά μια διαδικασία κατά την οποία ο A

στέλνει στον Β το $T_A = [a]P$ και ο Β στον Α το $T_B = [b]P$. Εν συνεχεία υπολογίζει ο Α το

$$k_A = \hat{e}([a]Q_B, P_{\Gamma\Pi K}) \cdot \hat{e}(S_A, T_B)$$

και ο Β το

$$k_B = \hat{e}([b]Q_A, P_{\Gamma\Pi K}) \cdot \hat{e}(S_B, T_A).$$

Το συμφωνηθέν κλειδί της συνεδρίας θα είναι το $K = V(k_A) = V(k_B)$. Το γεγονός ότι οι Α και Β μοιράζονται το ίδιο κλειδί φαίνεται εύκολα :

$$\begin{aligned} k_A &= \hat{e}([a]Q_B, P_{\Gamma\Pi K}) \cdot \hat{e}(S_A, T_B) = \hat{e}(Q_B, P_{\Gamma\Pi K})^a \cdot \hat{e}(S_A, T_B) \\ &= \hat{e}(Q_B, P)^{as} \cdot \hat{e}(Q_A, P)^{bs} = \hat{e}(S_B, T_A) \cdot \hat{e}(Q_A, P_{\Gamma\Pi K})^b \\ &= \hat{e}(S_B, T_A) \cdot \hat{e}([b]Q_A, P_{\Gamma\Pi K}) = \hat{e}([b]Q_A, P_{\Gamma\Pi K}) \cdot \hat{e}(S_B, T_A) \\ &= k_B \end{aligned}$$

Επισημαίνουμε πως από τη σχέση $k_A = \hat{e}([a]Q_B + [b]Q_A, [s]P)$ είναι εμφανές το ότι το συμφωνηθέν κλειδί της συνεδρίας εξαρτάται από τα δημόσια κλειδιά των Α και Β, από το μυστικό κλειδί s της Έμπιστης Αρχής, αλλά και από τα προσωρινά κλειδιά a και b των χρηστών.

Ασφάλεια

Οι παρατηρήσεις μας ως προς την ασφάλεια του παραπάνω πρωτοκόλλου εστιάζονται σε δύο βασικά σημεία:

1ο. : Το κλειδί κάθε συνεδρίας είναι διαφορετικό και από τη γνώση προηγούμενων τέτοιων κλειδιών, δεν συνάγεται κανενός είδους συμπέρασμα αναφορικά με τις επόμενες συνεδρίες.

2ο. : Κανένας μετέχων δεν μπορεί να ελέγξει την τιμή του κλειδιού μιας συνεδρίας περιορίζοντας τις τιμές του σε κάποιο προκαθορισμένο μικρό σύνολο.

Κεφάλαιο 9

ΠΑΡΑΡΤΗΜΑ Β′: ΣΤΟΙΧΕΙΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ ΚΑΙ ΚΑΤΑΣΚΕΥΗ ΤΗΣ Α.Δ.Α. WEIL

9.1 Η ομάδα των σημείων μιας ελλειπτικής καμπύλης

Οι ελλειπτικές καμπύλες έχουν βρεί πολλές εφαρμογές σε προβλήματα όπως το πρόβλημα της ανάλυσης ακεραίων σε πρώτους παράγοντες, στο πρόβλημα της πιστοποίησης πρώτων αριθμών καθώς επίσης και στο σχεδιασμό πρωτοκόλλων κρυπτογραφικών σχημάτων δημοσίου κλειδιού.

▷ **Ορισμός εξίσωσης ελλειπτικής καμπύλης**
Μια ελλειπτική καμπύλη Ε πάνω από ένα σώμα F ορίζεται μέσω μιας εξίσωσης Weierstrass:

$$E/F : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{9.1}$$

όπου $a_1, a_2, a_3, a_4, a_6 \in F$ και $\Delta \neq 0$ όπου Δ είναι η διακρίνουσα της Ε και ορίζεται ως:

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \tag{9.2}$$

με $d_2 = a_1^2 + 4a_2, d_4 = 2a_4 + a_1a_3, d_6 = a_3^2 + 4a_6, d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

Αν L είναι μια οποιαδήποτε επέκταση του σώματος F, τότε το σύνολο των L-ρητών σημείων στην E είναι το:
$\mathrm{E}(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \mathcal{O}$
όπου το $\mathcal{O}$ είναι το *σημείο στο άπειρο*.

Δυο ελλειπτικές καμπύλες E_1, E_2 ορισμένες πάνω απ' το F οι οποίες δίδονται από εξισώσεις Weierstrass, λέγονται ισόμορφες πάνω από το F, αν υπάρχουν $u, r, s, t \in F$ τ.ω. η αλλαγή μεταβλητών

$$(x, y) \to (u^2x + r, u^3y + u^2sx + t) \tag{9.3}$$

να μετατρέπει την E_1 στη E_2. Ο μετασχηματισμός αυτός ονομάζεται *αποδεκτή αλλαγή μεταβλητών* (admissible change of variables).

▷ **Απλοποίηση της εξίσωσης Weierstrass**
Η εξίσωση Weierstrass που ορίζεται πάνω απ' το σώμα F, δύναται να απλοποιηθεί με την εφαρμογή αποδεκτών αλλαγών των μεταβλητών της.
1. Αν η χαρακτηριστική του σώματος F δεν είναι ίση με 2 ή 3, τότε η κάτωθι αποδεκτή αλλαγή μεταβλητών

$$(x, y) \to ((x - 3a_1^2 - 12a_2)/36, (y - 3a_1x)/216 - (a_1^3 + 4a_1a_2 - 12a_3)/24),$$

μετατρέπει την E, στην καμπύλη $y^2 = x^3 + ax + b$ με $a, b \in F$ η οποία θα έχει διακρίνουσα $\Delta = -16(4a^3 + 27b^2)$.
2. Αν η χαρακτηριστική του σώματος F είναι ίση με 2 τότε διακρίνουμε δύο περιπτώσεις. Αν $a \neq 0$ τότε η κάτωθι αποδεκτή αλλαγή μεταβλητών

$$(x, y) \to (a_1^2x + a_3/a_1, a_1^3y + (a_1^2a_4 + a_3^2/a_1^3),$$

μετατρέπει την E, στην καμπύλη $y^2 + xy = x^3 + ax^2 + b$ με $a, b \in F$ η οποία θα έχει διακρίνουσα $\Delta = b$. Αν τώρα $a_1 = 0$ τότε η κάτωθι αποδεκτή αλλαγή μεταβλητών

$$(x, y) \to (x + a_2, y),$$

μετατρέπει την E, στην καμπύλη $y^2 + cy = x^3 + ax + b$ με $a, b, c \in F$ η οποία θα έχει διακρίνουσα $\Delta = c^4$.
3.Αν η χαρακτηριστική του σώματος F είναι ίση με 3 τότε διακρίνουμε δύο περιπτώσεις. Αν $a_1^2 \neq -a_2$ τότε η κάτωθι αποδεκτή αλλαγή μεταβλητών

$$(x, y) \to (x + d_4/d_2, y + a_1x + a_1d_4/d_2 + a_3),$$

όπου $d_2 = a_1^2 + a_2$ και $d_4 = a_4 - a_1a_3$, μετατρέπει την E, στην καμπύλη $y^2 = x^3 + ax^2 + b$ με $a, b \in F$ η οποία θα έχει διακρίνουσα $\Delta = -a^3b$. Αν $a_1^2 = -a_2$ τότε η κάτωθι αποδεκτή αλλαγή μεταβλητών

$$(x, y) \to (x, y + a_1x + a_3),$$

μετατρέπει την Ε, στην καμπύλη $y^2 = x^3 + ax + b$ με $a, b \in F$ η οποία θα έχει διακρίνουσα $\Delta = -a^3$.

▷ **Η πράξη στην ομάδα των ελλειπτικών καμπύλων**

Έστω Ε μια ελλειπτική καμπύλη η οποία ορίζεται πάνω από ένα σώμα F. Υπάρχει ένας *κανόνας χορδής-εφαπτομένης* αναφορικά με την πρόσθεση δύο σημείων που ανήκουν στο $E(F)$ (το άθροισμα των οποίων θα ανήκει επίσης στο $E(F)$). Με την πρόσθεση αυτή, το σύνολο των σημείων $E(F)$ μαζί με το σημείο στο άπειρο $\mathcal{O}$ το οποίο θα συμπεριφέρεται σαν το ταυτοτικό στοιχείο, αποτελεί αβελιανή ομάδα: τέτοιες ακριβώς ομάδες χρησιμοποιούνται στην κατασκευή κρυπτογραφικών σχημάτων ελλειπτικών καμπύλων.

Η πρόσθεση των σημείων μιας ελλειπτικής καμπύλης μπορεί να εξηγηθεί γεωμετρικά: ας υποθέσουμε παραδείγματος χάρην, πως έχουμε μια καμπύλη $y^2 = x^3 - x$ πάνω απ' το $\mathbb{R}$ και τα διαφορετικά μεταξύ τους σημεία αυτής, $P = (x_1, y_1)$ και $Q = (x_2, y_2)$. Το παραγόμενο άθροισμα R, των P και Q, θα είναι ένα σημείο της καμπύλης που θα προκύπτει, ως συμμετρικό σημείο προς τον άξονα xx', ενός σημείου που θα ανήκει στην καμπύλη και θα είναι συνευθειακό με τα P και Q. Το *διπλάσιο* R, ενός σημείου P, που συμβολίζεται ως $2P$ προκύπτει ως συμμετρικό σημείο προς τον άξονα xx', ενός σημείου που θα ανήκει τόσο στην καμπύλη, όσο και στην εφαπτομένη ευθεία της καμπύλης που φέρεται δια του P.

Διάφοροι αλγεβρικοί τύποι για την πράξη της ομάδας μπορούν εύκολα να προκύψουν από την παραπάνω γεωμετρική της περιγραφή. Παραθέτουμε τους τύπους αυτούς, για ελλειπτικές καμπύλες Ε που πληρούν την απλοποιημένη εξίσωση Weierstrass $y^2 = x^3 + ax^2 + b$ για αφινικές συντεταγμένες όταν η χαρακτηριστική του F είναι διάφορη των 2 και 3 αλλά και για ελλειπτικές καμπύλες τύπου $y^2 + xy = x^3 + ax^2 + b$ όταν αυτή είναι ορισμένη πάνω από πεπερασμένο σώμα χαρακτηριστικής 2.

ΚΑΝΟΝΕΣ ΠΡΟΣΘΕΣΗΣ ΓΙΑ ΤΗΝ $E/F : y^2 = x^3 + ax^2 + b$, με $\text{χαρ}(F) \neq 2, 3$.

1. Ταυτοτικό στοιχείο $\mathcal{O} : P + \mathcal{O} = \mathcal{O} + P = P \ \forall P \in E(F)$.
2. Αντίθετο σημείου: Αν $P = (x, y) \in E(F)$ τότε $(x, y) + (x, -y) = \mathcal{O}$. Το σημείο $(x, -y)$ το ονομάζουμε αντίθετο του P, ανήκει στο $E(F)$ και συμβολίζεται ως $-P$.Σημειώνουμε επίσης πως $-\mathcal{O} = \mathcal{O}$.
3. Πρόσθεση σημείων: Έστω $P = (x_1, y_1) \in E(F)$ και $Q = (x_2, y_2) \in E(F)$ με $P \neq \pm Q$. Τότε $P + Q = (x_3, y_3)$ όπου

$$x_3 = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2 \quad \kappa\alpha\iota \quad y_3 = (\frac{y_2 - y_1}{x_2 - x_1}\Big)(x_1 - x_3) - y_1.$$

4. Διπλασιασμός σημείου: Έστω $P = (x_1, y_1) \in E(F)$ με $P \neq -P$. Τότε

$2P = (x_3, y_3)$ όπου

$$x_3 = \Big(\frac{3x_1^2 + a}{2y_1}\Big)^2 - 2x_1 \quad \kappa\alpha\iota \quad y_3 = \Big(\frac{3x_1^2 + a}{2y_1}\Big)(x_1 - x_3) - y_1.$$

ΚΑΝΟΝΕΣ ΠΡΟΣΘΕΣΗΣ ΓΙΑ ΤΗΝ $E/F : y^2 + xy = x^3 + ax^2 + b$, με $\chi\alpha\rho(F) = 2$.

1. Ταυτοτικό Στοιχείο $\mathcal{O} : P + \mathcal{O} = \mathcal{O} + P = P \ \forall P \in E(F)$.
2. Αντίθετο σημείου: Αν $P = (x, y) \in E(F)$ τότε $(x, y) + (x, x + y) = \mathcal{O}$. Το σημείο $(x, x + y)$ το ονομάζουμε αντίθετο του P, ανήκει στο $E(F)$ και συμβολίζεται ως $-P$. Ομοίως όπως και πρίν $-\mathcal{O} = \mathcal{O}$.
3. Πρόσθεση σημείων: Έστω $P = (x_1, y_1) \in E(F)$ και $Q = (x_2, y_2) \in E(F)$ με $P \neq \pm Q$. Τότε $P + Q = (x_3, y_3)$ όπου

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}, \quad x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, \quad \kappa\alpha\iota \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

4. Διπλασιασμός σημείου: Έστω $P = (x_1, y_1) \in E(F)$ με $P \neq -P$. Τότε $2P = (x_3, y_3)$ όπου

$$x_3 = \Big(x_1 + \frac{y_1}{x_1}\Big)^2 + \Big(x_1 + \frac{y_1}{x_1}\Big) + a \qquad \kappa\alpha\iota \quad y_3 = x_1^2 + \Big(x_1 + \frac{y_1}{x_1}\Big)x_3 + x_3.$$

▷ **Τάξη ομάδας των ελλειπτικών καμπύλων**

Έστω E μια ελλειπτική καμπύλη ορισμένη πάνω από ένα πεπερασμένο σώμα $F = \mathbb{F}_q, q \in \mathbb{P}$. Το πλήθος των σημείων του συνόλου $E(\mathbb{F}_q)$, έστω $\#E(\mathbb{F}_q)$ αυτό, καλείται τάξη της E πάνω απ' το $\mathbb{F}_q$. Από τη στιγμή που η εξίσωση Weierstrass έχει δύο το πολύ λύσεις για κάθε $x \in \mathbb{F}_q$ γνωρίζουμε πως $\#E(\mathbb{F}_q) \in [1, 2q + 1]$. Το Θεώρημα του Hasse δίνει ένα καλύτερο φράγμα για το $\#E(\mathbb{F}_q)$:

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

Το πλήθος των σημείων του συνόλου $E(\mathbb{F}_q)$ στην πράξη υπολογίζεται σε πολυωνυμικό χρόνο από τον αλγόριθμο του Schoof είτε από κάποιον άλλο εκ των πολλών αλγορίθμων που στηρίχθηκαν μετέπειτα σ' αυτόν.

Εάν η χαρακτηριστική του $\mathbb{F}_q$ είναι p και E μια ελλειπτική καμπύλη ορισμένη πάνω απ' το $\mathbb{F}_q$, τότε θα ονομάζουμε την E *υπεριδιάζουσα* (supersingular), αν $p \mid t$ με $t = q + 1 - \#E(\mathbb{F}_q)$.

Αν E είναι μια ελλειπτική καμπύλη ορισμένη πάνω απ' το $\mathbb{F}_q$, τότε η E θα ορίζεται πάνω και από οποιαδήποτε επέκταση $\mathbb{F}_{q^n}$ της $\mathbb{F}_q$. Η ομάδα $E(\mathbb{F}_q)$ των $\mathbb{F}_q$-ρητών σημείων αποτελεί υποομάδα της $E(\mathbb{F}_{q^n})$ των $\mathbb{F}_{q^n}$-ρητών σημείων

οπότε ο αριθμός $\#E(\mathbb{F}_q)$ διαιρεί τον $\#E(\mathbb{F}_{q^n})$. Αν ο $\#E(\mathbb{F}_q)$ είναι γνωστός , τότε ο $\#E(\mathbb{F}_{q^n})$ μπορεί, σύμφωνα με τον Weil να προσδιορισθεί ως εξής:

Αν $\#E(\mathbb{F}_q) = q+1-t$, τότε $\#E(\mathbb{F}_{q^n}) = q^n - 1 - V_n$ για κάθε $n \geq 7$ όπου $\{V_n\}$ είναι η ακολουθία που ορίζεται αναδρομικά από τα $V_0 = 2, V_1 = t$ και για $n \geq 2$ από το $V_n = V_1 V_{n-1} - qV_{n-2}$.

▷ **Δομή ομάδας των ελλειπτικών καμπύλων**

Ορίσαμε ως E να είναι μια ελλειπτική καμπύλη ορισμένη πάνω από ένα πεπερασμένο σώμα $F = \mathbb{F}_q$. Στην περίπτωση αυτή η $E(\mathbb{F}_q)$ είναι μια ομάδα, ισόμορφη με τη $\mathbb{Z}_{n_1} \bigoplus \mathbb{Z}_{n_2}$ όπου τα n_1, n_2 είναι με μοναδικό τρόπο ορισμένοι θετικοί ακέραιοι τέτοιοι ώστε ο n_2 να διαιρεί τόσο το n_1, όσο και το $q-1$.

Σ' αυτό το σημείο σημειώνουμε ότι $\#E(\mathbb{F}_q) = n_1 n_2$. Αν $n_2 = 1$ τότε η $E(\mathbb{F}_q)$ είναι κυκλική ομάδα, ενώ αν $n_2 \geq 1$ και συγκεκριμένα για μικρές τιμές (δηλ. 2, 8 ή 4) τότε λέμε ότι είναι σχεδόν κυκλική. Από τη στιγμή που ο n_2 διαιρεί τόσο το n_1, όσο και το $q-1$ μπορεί κάποιος να επικαλεσθεί πως η $E(\mathbb{F}_q)$ είναι κυκλική ή σχεδόν κυκλική ομάδα, για τις περισσότερες ελλειπτικές καμπύλες E πάνω από το $\mathbb{F}_q$.

▷ **Παράδειγμα**

Θεωρούμε την ελλειπτική καμπύλη

$$E : y^2 = x^3 + 2x + 4,$$

ορισμένη πάνω απ' το $\mathbb{F}_{13}$. Τα στοιχεία της $E(\mathbb{F}_{13})$ είναι τα εξής:
(0, 2), (0, 11), (2, 4), (2, 9), (5, 3), (5, 10), (7, 6), (7, 7), (8, 5), (8, 8),
(9, 6), (9. 7), (10, 6), (10, 7), (12, 1), (12, 12), $\mathcal{O}$
άρα $\#E(\mathbb{F}_{13}) = 17$. Ως παραδείγματα για την πράξη στην ομάδα έχουμε τα $(8,5)+(2,4) = (7,6)$ και $2(8,5) = (0,2)$. Τέλος αφού η τάξη της είναι πρώτος αριθμός, συμπεραίνουμε πως η $E(\mathbb{F}_{13})$ είναι κυκλική ομάδα.

9.2 Η Α.Δ.Α. Weil

Θεωρούμε το πεπερασμένο σώμα $\mathbb{F}_q, q \in \mathbb{P}$ για το οποίο κάνουμε τη σύμβαση να έχει χαρακτηριστική μεγαλύτερη του 3. Έστω $E : y^2 - (x^3 + Ax + B) = 0$ μια ελλειπτική καμπύλη πάνω απ' το $\mathbb{F}_q$ και $\mathrm{E}(\mathbb{F}_q) = \{(X, Y) \in \mathbb{F}_q \times \mathbb{F}_q : Y^2 - (X^3 + AX + B) = 0\} \cup \mathcal{O}$ όπου $\mathcal{O}$ είναι το *σημείο στο άπειρο*. Έστω επίσης ένας πρώτος αριθμός n τ.ω. (i) $n \mid E(\mathbb{F}_q), (ii)$ ο n δεν διαιρεί το $q-1$ και (iii) $(n, q) = 1$. Τότε για κάποιο ακέραιο k, η επέκταση $E(\mathbb{F}_{q^k})$ του $E(\mathbb{F}_q)$ θα περιέχει n^2-το πλήθος στοιχεία τάξεως n, αν και μόνον αν $n \mid q^k - 1$. Στο εξής θα συμβολίζουμε ως $E[n]$ το σύνολο αυτών των n^2-το πλήθος, τάξεως n στοιχείων: $\forall\ P \in E[n] : nP = \mathcal{O}$.

▷ **Διγραμμικές και μη εκφυλισμένες Α.Δ.Α.**

Η Α.Δ.Α. Weil e_n αποτελεί μια απεικόνιση από το $E[n] \times E[n]$ στο μ_n, όπου το μ_n είναι η πολλαπλασιαστική ομάδα των n-οστών ριζών της μονάδας στο $\mathbb{F}_{q^k}$, δηλαδή $\forall\ a \in \mu_n : a^n = 1$. Είναι φανερό πως η ομάδα μ_n (η οποία διαθέτει n-το πλήθος στοιχεία) είναι η μοναδική υποομάδα της $\mathbb{F}_{q^k}$ (αφού η τελευταία είναι κυκλική).

ΙΔΙΟΤΗΤΕΣ Για τα $P, Q, R \in E[n]$ έχουμε:

- $e_n(P, P) = 1$. (Στο σημείο αυτό μπορούμε να αναφέρουμε πως η Α.Δ.Α. Weil επιδέχεται μια συγκεκριμένη τροποποίηση, από την οποία παίρνουμε την τροποποιημένη Α.Δ.Α. Weil $\hat{e}(\cdot, \cdot)$, για την οποία ισχύει $\hat{e}(P, P) \neq 1$).
- Διγραμμικότητα: $e_n(P+Q, R) = e_n(P, R)e_n(Q, R)$ και $e_n(R, P+Q) = e_n(R, P)e_n(R, Q)$.
- Μη εκφυλισμός: $e_n(P, Q) \neq 1$ για κάποια $P, Q \in E[n]$.

▷ **Διαιρέτες**

Προκειμένου να γίνει εμφανές από πού προκύπτουν οι ιδιότητες των Α.Δ.Α. και ακόμη περισσότερο το πώς κατασκευάζονται αυτές, οφείλουμε να μελετήσουμε την έννοια ενός *διαιρέτη* (divisor). Ένας διαιρέτης D, ορίζουμε να είναι ένα τυπικό άθροισμα της μορφής:

$$D = \sum_{P \in E} a_P[P],$$

όπου $a_P \in \mathbb{Z}$ και $a_P = 0$ εκτός από πεπερασμένο πλήθος σημείων. Ορίζουμε επίσης ως *βαθμό ενός διαιρέτη deg(D)*, να είναι το άθροισμα των συντελεστών του "τυπικού" τυχαίου σημείου [P] στο άθροισμα που παριστάνει ένας διαιρέτης:

$$deg(D) = \sum_{P \in E} a_P.$$

Πιο συγκεκριμένα, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι διαιρέτες οι οποίοι

έχουν βαθμό ίσο με μηδέν (για τους υπόλοιπους υπάρχει συγκεκριμένη διαδικασία που να τους μετατρέπει έτσι ώστε να έχουν κι αυτοί μηδενικό βαθμό).

▷ **Μηδενικά σημεία και πόλοι μιας συνάρτησης (zeros & poles)**
Αν P σημείο στην ελλειπτική καμπύλη E, τότε το P ονομάζεται *μηδενικό σημείο της* f αν $f(P) = 0$, ενώ αν $f(P) = \infty$ ονομάζεται *πόλος* αυτής.

Στη συνέχεια ορίζουμε την πολλαπλότητα ενός μηδενικού σημείου και ενός πόλου, με τη βοήθεια του παρακάτω Θεωρήματος.

ΘΕΩΡΗΜΑ 14 *Για κάθε σημείο $P \in E$, υπάρχει μια ρητή συνάρτηση u_P, η οποία έχει σημείο μηδενισμού το P, με την παρακάτω ιδιότητα:*

αν r είναι οποιαδήποτε μη μηδενική ρητή συνάρτηση, τότε $r = u_P^d s$, για κάποιον ακέραιο d και κάποια ρητή συνάρτηση s που είναι πεπερασμένη και μη μηδενική στο P (ο αριθμός d είναι ανεξάρτητος της επιλογής της συνάρτησης u_P). Η δε συνάρτηση u_P, ονομάζεται ομοιομορφοποιητής (uniformizer) του σημείου P.

Ορισμός 15 *Αν r είναι μια ρητή συνάρτηση και $r = u_P^d s$, με την u_P να είναι ομοιομορφοποιητής του σημείου P, καλούμε ως τάξη της r στο σημείο P, τον αριθμό d και γράφουμε $ord_P(r) = d$. Αν η r έχει σημείο μηδενισμού ή πόλο, το σημείο P, ορίζουμε ως πολλαπλότητα του P την τιμή $|ord_P(r)|$*

ΥΠΟΔΕΙΞΗ
Αν $ord_P > 0$ τότε το P είναι μηδενικό σημείο.
Αν $ord_P < 0$ τότε το P είναι πόλος.
Αν $ord_P = 0$ τότε το P δεν είναι ούτε πόλος, ούτε μηδενικό σημείο.

▷ **Συμπεράσματα για την τάξη σημαντικών μηδενικών σημείων και πόλων**
Τα μηδενικά σημεία των γραμμικών συναρτήσεων θεωρούνται αρκετά σημαντικά. Έστω $l : y = ux+v, (u \neq 0)$ μια γραμμική συνάρτηση, την οποία στο εξής θα καλούμε *γραμμή*. Ένα σημείο μηδενισμού $P(x_0, y_0)$ της l, αποτελεί μια πεπερασμένη λύση του $l \bigcap E : (ux+v)^2 = y^2 = x^3+Ax+B$, δηλαδή το x_0 είναι λύση του $(ux+v)^2 - (x^3+Ax+B) = 0$. Η συνάρτηση 0 που εμφανίζεται στην ισότητα, λόγω του τελευταίου Θεωρήματος, παρίσταται ως $(x - x_0)^d \cdot g$ όπου $g(x_0) \neq 0$ και $d = \begin{cases} 2, & \text{αν το P είναι σημείο από το οποίο φέρεται εφαπτομένη} \\ 1, & \text{αλλιώς} \end{cases}$,
οπότε

$$ord_P(l) = \begin{cases} 1, & \text{αν η } l \text{ τέμνει την E στο P} \\ 2, & \text{αν η } l \text{ εφάπτεται της E στο P.} \end{cases}$$

Ακριβώς το ίδιο αποτέλεσμα παίρνουμε και στην ειδική περίπτωση που θα θεωρείται ως l μια τυχαία κάθετη ευθεία $x = c$.

Οι πόλοι των γραμμικών συναρτήσεων είναι εξίσου σημαντικοί. Μελετώντας τα $\mathrm{ord}_{\mathcal{O}}(x)$ και $\mathrm{ord}_{\mathcal{O}}(y)$, τότε αν πάρουμε ως $(\frac{x}{y})^2 = \frac{x^2}{x^3(1+\cdots)}$ έχουμε $x = (\frac{x}{y})^{-2}\frac{1}{(1+\cdots)}$. Όμως στο $\mathcal{O}$ ξέρουμε ότι $\frac{x}{y} = 0$ και $\frac{1}{(1+\cdots)} = 1$ άρα $\mathrm{ord}_{\mathcal{O}}(x) = -2$. Επίσης, έχοντας $y = (\frac{x}{y})^{-1} \cdot x = (\frac{x}{y})^{-3} \cdot \frac{1}{(1+\cdots)}$ παίρνουμε $\mathrm{ord}_{\mathcal{O}}(y) = -3$.
Συμπέρασμα: για μια γραμμική συνάρτηση $l : ux + vy + w = 0$, ισχύει

$$ord_{\mathcal{O}}(l) = \begin{cases} -3, & \text{αν } v \neq 0 \\ -2, & \text{αλλιώς.} \end{cases}$$

▷ **Διαιρέτες συναρτήσεων**
Αν $f \neq 0$ μια συνάρτηση σε ελλειπτική καμπύλη E, τότε ορίζουμε ως *διαιρέτη της συνάρτησης* f να είναι το τυπικό άθροισμα:

$$div(f) = \sum_{P \in E} ord_P(f)[P].$$

Για μια γραμμική συνάρτηση $l : ux + vy + w = 0$ $(u, v \neq 0)$, γνωρίζουμε ότι τέμνει την E σε τρία ακριβώς σημεία P_1, P_2, P_3 (όπου τα δύο μπορεί και να ταυτίζονται, αν π.χ. η l εφάπτεται της E σε κάποιο σημείο). Κάθε ένα από αυτά τα σημεία, είναι ένα διακριτό σημείο μηδενισμού της l (ή αν πρόκειται για σημείο δια του οποίου η l εφάπτεται της E, έχουμε διπλό σημείο μηδενισμού). Ακόμη, έχοντας δεί πως η l έχει πόλο στο $\mathcal{O}$ και με δεδομένο ότι $v \neq 0$, ο πόλος αυτός θα είναι τριπλός συνεπώς:

$$div(l) = [P_1] + [P_2] + [P_3] - 3[\mathcal{O}].$$

Έστω l' μια κάθετη γραμμή $(v = 0)$ η οποία τέμνει την E στα σημεία $P_3, -P_3$. Τα σημεία αυτά αποτελούν διακριτά σημεία μηδενισμού (εκτός αν $y = 0$, που έχουμε περίπτωση εφαπτομένης και κατ' επέκταση διπλό σημείο μηδενισμού). Αφού η l' έχει διπλό πόλο στο $\mathcal{O}$ θα ισχύει:

$$div(l') = [P_3] + [-P_3] - 2[\mathcal{O}].$$

Παίρνοντας $P_3 = -(P_1 + P_2)$ τότε για τη διαφορά $div(l) - div(l')$ έχουμε

$$div(l/l') = div(l) - div(l') = [P_1] + [P_2] - [P_1 + P_2] - [\mathcal{O}] \qquad (9.4)$$

ΛΗΜΜΑ
i) Ένα μηδενικό στοιχείο της l, είναι και μηδενικό στοιχείο της l/l'.
ii) Ένα μηδενικό στοιχείο της l', είναι και πόλος της l/l'.

iii) Ένας πόλος της l', είναι και μηδενικό στοιχείο της l/l'.
iv) Ένας πόλος της l, είναι και πόλος της l/l'.

▷ **Κατασκευή Α.Δ.Α. από επαναλαμβανόμενες προσθέσεις διαιρετών**

Έστω $P \in E[n]$ και $P = P_1 = P_2$. Η σχέση (9.4) σ' αυτή την περίπτωση θα γίνει $div(f_1) = 2[P] - [2P] - [\mathcal{O}]$, για κάποια συνάρτηση f_1. Αν συνεχίσουμε να προσθέτουμε P, τότε με βάση την (9.4) θα πάρουμε διαδοχικά:
$div(f_2) = 3[P] - [3P] - 2[\mathcal{O}]$,
$div(f_3) = 4[P] - [4P] - 3[\mathcal{O}]$,
$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$
$div(f_{n-1}) = n[P] - [nP] - (n-1)[\mathcal{O}]$.

Εφόσον $nP = \mathcal{O}$, η τελική εξίσωση $div(f_{n-1})$ θα είναι

$$div(f_P) = n[P] - n[\mathcal{O}] \tag{9.5}$$

(έχουμε μετονομάσει την f_{n-1} σε f_P) για κάποια συνάρτηση f_P στην Ε. Με βάση τα παραπάνω, καταφέραμε χρησιμοποιώντας ένα στοιχείο $P \in E[n]$ να κατασκευάσουμε μια συνάρτηση f_P η οποία να ικανοποιεί την (9.5).

▷ **Κατασκευή των Α.Δ.Α. Tate και Weil με τη χρήση της f_P**

Για τα τυχαία σημεία Q, S της ελλειπτικής καμπύλης, ορίζουμε μία "ανώνυμη"Α.Δ.Α. να είναι η απεικόνιση

$$\alpha_n(P,Q)_S = \frac{f_P(Q+S)}{f_P(S)}, \tag{9.6}$$

της οποίας οι τιμές, δεν εξαρτώνται μόνο από τα P, Q αλλά και από το τυχαίο S. Παίρνοντας τα $\alpha_n(P,Q)_S$ και $\alpha_n(P,Q)_{S'}$ για $S \neq S'$, τότε αποδεικνύεται πως $\frac{\alpha_n(P,Q)_S}{\alpha_n(P,Q)_{S'}} = \xi^n$ για κάποιο $\xi \in \mathbb{F}_{q^k}$. Όμως από το Θεώρημα του Fermat έχουμε $\left(\frac{\alpha_n(P,Q)_S}{\alpha_n(P,Q)_{S'}}\right)^{(q^k-1)/n} = \xi^{q^k-1} = 1$, δηλαδή
$(\alpha_n(P,Q)_S)^{(q^k-1)/n} = (\alpha_n(P,Q)_{S'})^{(q^k-1)/n}$, οπότε η απεικόνιση είναι ανεξάρτητη οποιωνδήποτε τυχαίων σημείων S, S' και μπορούμε πλέον να ορίσουμε την Α.Δ.Α. Tate στα σημεία P, Q με την τιμή τους σε αυτά να δίνεται από την

$$t_n(P,Q) = (\alpha_n(P,Q)_S)^{(q^k-1)/n}.$$

Τέλος η Α.Δ.Α. Weil πάνω σε δύο σημεία $P, Q \in E[n]$, ορίζεται μέσω της Α.Δ.Α. Tate ως

$$e_n(P,Q) = \frac{t_n(P,Q)}{t_n(Q,P)}.$$

Η διγραμμικότητα αυτού αποδεικνύεται (όχι τετριμμένα) με βάση τη σχέση (9.6):
$\alpha_n(P,Q_1)_S \cdot \alpha_n(P,Q_2)_{Q_1+S} = \frac{f_P(Q_1+S)}{f_P(S)} \cdot \frac{f_P(Q_2+(Q_1+S))}{f_P(Q_1+S)} = \frac{f_P((Q_1+Q_2)+S)}{f_P(S)} = \alpha_n(P,Q_1+Q_2)_S$. Από τη στιγμή που ξέρουμε ότι η Α.Δ.Α. Weil είναι ανεξάρτητη των $S, S+Q_1$ έπεται ότι

$$e_n(P,Q_1) \cdot e_n(P,Q_2) = e_n(P,Q_1+Q_2). \qquad o.\varepsilon.\delta.$$

Βιβλιογραφία

[1] W. Diffie - M. Hellman, New Directions In Cryptography, *IEEE Trans. Inform. Theory*, **IT-22** (1976), 472-492.

[2] U. M. Maurer,Towards The Equivalence Of Breaking The Diffie-Hellman Protocol & Computing Discrete Logarithms, *Lecture Notes In Computer Science*, Springer-Verlag, **839** (1994), 271-281.

[3] U. M. Mayrer - S. Wolf,The Relationship Between Breaking The Diffie-Hellman Protocol & Computing Discrete Logarithms, *SIAM Journal On Computing*, **28** (1999), 1689-1721.

[4] D. Boneh - M. Franklin, Identity Based Encryption From The Weil Pairing, *Advances In Cryptology-CRYPTO 2001*, Springer-Verlag, **LNCS 2139** (2001), 213-229.

[5] W. Diffie - M. Hellman, New Directions In Cryptography, *IEEE Trans. Inform. Theory*, **IT-22** (1976), 644-654.

[6] L. Law - A. J. Menezes - M. Qu - J. Solinas - S. Vanstone, An Efficient Protocol For Authenticated Key Agreement.

[7] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, *Advances In Cryptology-CRYPTO '84*, Springer-Verlag, **LNCS 196** (1984), 47-53.

[8] A.Joux, A One Round Protocol for Tripartite Diffie-Hellman, *Proceedings Of ANTS IV*, **LNCS 1838** (2000), 385-394.

[9] D. Pointcheval - J. Stern, Security Arguments For Digital Signatures And Blind Signatures,*Journal Of Cryptology*, **13** (2000), 361-396.

[10] M. Kim, K. Kim, A New Identification Scheme Based On The Bilinear Diffie-Hellman Problem, *ACISP* (2002).

[11] B. Libert - J. J. Quisquater, Efficient Revocation And Threshold Pairing-Based Cryptosystems, *PODC* (2003), 163-171.

[12] R. Sakai - K. Ohgishi - K. Kasahara, Crypyosystems Based On Pairing, **SCIS 2000** (2000).

[13] Wenbo Mao, Divisors, Billinear Pairings and Pairings Enabled Cryptographic applications.

[14] Lawrence C. Washington, Elliptic Curves: Number theory and Cryptography, *CRC Press Company.*

[15] A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, *CRC Press Series On Discrete Mathematics and It' s Applications*, CRC Press.

[16] J. H. Silverman, The Arithmetic of Elliptic Curves, *Of Graduate Texts In Mathematics*, Springer-Verlag, **106** (1986).