ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΒΑΓΓΕΛΗ ΚΩΝΣΤΑΝΤΑΚΑΤΟΥ

Επιβλέπων
Αριστείδης Παγουρτζής
Καθηγητής Ε.Μ.Π

Αθήνα, Ιούλιος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΒΑΓΓΕΛΗ ΚΩΝΣΤΑΝΤΑΚΑΤΟΥ

Επιβλέπων: Αριστείδης Παγουρτζής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 14/7/2022.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Αριστείδης Παγουρτζής	Μιχαήλ Λουλάκης	Πέτρος Στεφανέας
Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2022

Περίληψη

Στη παρούσα εργασία μελετάμε ψηφιακές υπογραφές με επιπρόσθετες λειτουργικότητες. Εστιάζουμε στις Συνδέσιμες Υπογραφές Δακτυλίου (LRS) και στις Υπογραφές Καθορισμένου Επαληθευτή (DVS), και παρουσιάζουμε τον δικό μας καινοτόμο συνδυασμό τους, τις Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή. Για καθένα από τα είδη υπογραφών με τα οποία ασχολούμαστε, παρουσιάζουμε τις εκδοχές τους που συναντώνται στη βιβλιογραφία, τα μοντέλα τους, ενώ ιδιαίτερη έμφαση δίνουμε στις ιδιότητες ασφάλειες. Για τις DVLRS παρουσιάζουμε το δικό μας καινοτόμο μοντέλο, αυστηρούς ορισμούς για όλες τις απαραίτητες ιδιότητες ασφάλειας. Επιπλέον, παρέχουμε μια ασφαλή κατασκευή, της οποίας αποδεικνύουμε την ασφάλεια στο μοντέλο τυχαίου μαντείο $\mathcal{RO}$. Τέλος αναλύουμε το πως η δουλειά μας μπορεί να αξιοποιηθεί στην σχεδίαση ενός συστήματος εποικοδομητικών κριτικών, που προστατεύουν τον παραλήπτη των κριτικών ακόμα και αν το ιδιωτικό του κλειδί αποκαλυφθεί.

Λέξεις Κλειδιά

Ασύμμετρη Κρυπτογραφία, Ψηφιακές Υπογραφές, Συνδέσιμες Υπογραφές Δακτυλίου, Υπογραφές Καθορισμένου Επαληθευτή, Μη-Πλαστογραφησιμότητα, Ανωνυμία, Συνδεσιμότητα, Μη-Μεταφερσιμότητα, Ανώνυμες Κριτικές

Abstract

In this work we study digital signatures with additional functionalities. We focus on Linkable Ring Signatures (LRS) and Designated Verifier Signatures (DVS) and present a novel cryptographic primitive, Designated Verifier Linkable Ring Signatures (DVLRS). We study the main results on these primitives and analyse their security models. For DVLRS we present our own novel model and formally define all the relevant security properties. Furthermore, we provide a secure construction, with proofs in the random oracle model $\mathcal{RO}$. Finally we showcase how our work can be utilised to design an anonymous feedback system, that protects not only the reviewers, but also the reviewee from any malicious third party, even if their private keys are compromised.

Keywords

Public Key Cryptography, Digital Signatures, Linkable Ring Signatures, Designated Verifier Signautres, Unforgeability, Anonymity, Linkability, Non-Transferability, Anonymous Feedback

Περιεχόμενα

Κατάλογος Πειραμάτων Ασφάλειας

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Οι ψηφιακές υπογραφές είναι ένα από τα κύρια επιτεύγματα της σύγχρονης κρυπτογραφίας. Πέρα από τις κοινές ψηφιακές υπογραφές που πιστοποιούν ότι ένα μήνυμα προέρχεται όντως από αυτόν που δηλώνει ότι το έστειλε, έχουν κατασκευαστεί και πολλές ψηφιακές με επιπρόσθετες λειτουργίες. Δύο από αυτές με ιδιαίτερο ενδιαφέρον είναι οι συνδέσιμες υπογραφές δακτυλίου, που επιτρέπουν σε κάποιον να υπογράψει ένα μήνυμα, παραμένοντας όμως ανώνυμος ανάμεσα σε ένα σύνολο από άλλους πιθανούς υπογράφοντες, και οι υπογραφές καθορισμένου επαληθευτή, που είναι χρήσιμες μόνο για τον επιδιωκόμενο παραλήπτη. Εμείς αναπτύξαμε ένα νέο είδος ψηφιακών υπογραφών που συνδυάζει έξυπνα τις ιδιότητες των δύο προηγουμένων. Ορίσαμε ένα γενικό μοντέλο ασφαλείας σύμφωνα με το οποίο θα μπορεί να αναλυθεί η ασφάλεια κάθε τέτοιας υπογραφής και σχεδιάσαμε ένα πρωτόκολλο που πληρεί όλες τις ιδιότητες, με αποδείξεις της ασφάλειας στο μοντέλο τυχαίου μαντείου($\mathcal{RO}$ model). Τέλος εξηγήσαμε πως με βάση τις DVLRS μπορούμε να χτίσουμε ένα σύστημα ανώνυμων αξιολογήσεων, που προστατεύει όχι μόνο την ανωνυμία των κριτών, αλλά και τον δέκτη των αξιολογήσεων, αφού του επιτρέπουμε να δημιουργεί πλαστές αξιολογήσεις, πανομοιότυπες με τις πραγματικές. Έτσι εξασφαλίζουμε ότι μπορεί να λάβει εποικοδομητικές κριτική που θα είναι απόλυτα προσωπικές, χωρίς το φόβο ότι αυτές μπορεί να έχουν αρνητική επίδραση στην υπόληψη του.

Στα πρώτα κεφάλαια παρουσιάζουμε κάποιες προαπαιτούμενες γνώσεις. Συγκεκριμένα, στο κεφάλαιο 2 κάνουμε μια σύντομη παρουσίαση των βασικών αρχών της κρυπτογραφίας δημοσίου κλειδιού (public key cryptography) ή αλλιώς ασύμμετρης κρυπτογραφίας. Στο κεφάλαιο 3 μιλάμε για ψηφιακές υπογραφές (digital signatures). Εξηγούμε το τρόπο λειτουργίας τους και τις βασικές απαιτήσεις ασφαλείας. Ως παράδειγμα χρησιμοποιούμε το κλασικό σχήμα υπογραφών ElGamal. Η εμπέδωση αυτού το κεφαλαίου είναι απαραίτητη για την κατανόηση των επόμενων κεφαλαίων. Στους αναγνώστες που είναι εξοικειωμένοι με την κρυπτογραφία, προτείνουμε να προσπεράσουν τα δύο προηγούμενα κεφάλαια. Στο κεφάλαιο 4 αναλύουμε τις αδιαμφισβήτητες υπογραφές (undeniable signatures), τις υπογραφές καθορισμένου επιβεβαιωτή (designated confirmer signatures) και τις υπογραφές καθορισμένου επαληθευτή (DVS), καθώς και την παραλλαγή τους, τις υπογραφές ισχυρά καθορισμένου επαληθευτή (sDVS). Στο κεφάλαιο 5 μιλάμε για τις ομαδικές υπογραφές (group signatures), τις υπογραφές δακτυλίου (RS), και και μια παραλλαγή των τελευταίων, τις συνδέσιμες υπογραφές δακτυλίου (LRS). Το σημαντικότερο ίσως κομμάτι της ΔΕ βρίσκεται στο κεφάλαιο 6, όπου παρουσιάζουμε ένα καινοτόμο σχήμα υπογραφών, τις συνδέσιμες υπογραφές δακτυλίου

καθορισμένου επαληθευτή (DVLRS). Αναλύουμε πλήρως το μοντέλο ασφάλειας και κατασκευάζουμε ένα ολοκληρωμένο πρωτόκολλο, του οποίου την ασφάλεια αποδεικνύουμε στο μοντέλο $\mathcal{RO}$. Στη συνέχεια, στο κεφάλαιο 7 συζητάμε το πως οι DVLRS μπορούν να χρησιμοποιηθούν για τη σχεδίαση ενός συστήματος ανώνυμης εποικοδομητικής κριτικής. Τέλος στο κεφάλαιο 8 αναφέρουμε κάποιες μελλοντικές κατευθύνσεις που σκοπεύουμε να ακολουθήσουμε.

Για τη πληρότητα της ΔΕ, υπάρχουν επίσης τρία παραρτήματα. Στο Παράρτημα Α΄ κάνουμε μια συνοπτική παρουσίαση των μαθηματικών εργαλείων με τα οποία ο αναγνώστης θα πρέπει να είναι εξοικειωμένος. Πρόκειται για απλές γνώσεις θεωρίας αριθμών και θεωρίας ομάδων. Στο Παράρτημα Β΄ μιλάμε για κρυπτογραφικές συναρτήσεις σύνοψης και το μοντέλο τυχαίου μαντείου RO και παρουσιάζουμε μια κλασική τεχνική αποδείξεων για ψηφιακές υπογραφές βασισμένη στο Λήμμα Διακλάδωσης (Forking Lemma). Τέλος, στο Παράρτημα Γ΄ μιλάμε για αποδείξεις μηδενικής γνώσεις.

ΚΕΦΑΛΑΙΟ 2

Εισαγωγή στη Κρυπτογραφία Δημοσίου Κλειδιού

Η ιδέα για την κρυπτογραφία δημοσίου κλειδιού προτάθηκε από τους Diffie και Hellman το 1976[31]. Η επαναστατική τους πρόταση ήταν να επιτρέψουν την ασφαλή ανταλλαγή μηνυμάτων, χωρίς ο αποστολέας και ο αποδέκτης να πρέπει να έχουν προσυμφωνήσει ένα κλειδί. Εισήγαγαν την έννοια της συνάρτησης μονής κατεύθυνσης με καταπακτή (one-way trapdoor function) και εξήγησαν πως αυτές μπορούν να χρησιμοποιηθούν για να λύσουν το πρόβλημα ασφαλούς ανταλλαγής κλειδιών. Ένα χρόνο αργότερα οι Rivest, Shamir και Adleman πρότειναν το πρώτο κρυπτοσύστημα δημοσίου κλειδιού, το ονομαζόμενο RSA[61].

Στην συνέχεια του κεφαλαίου θα δούμε κάποια βασικά εργαλεία της κρυπτογραφίας δημοσίου κλειδιού, θα μιλήσουμε για την ασφάλεια τους και για μερικές από τις πιο ευρέως διαδεδομένες παραδοχές. Καθοδηγητικό μας παράδειγμα θα είναι το κρυπτοσύστημα ElGamal[32].

Για την κατανόηση αυτού του κεφαλαίου, απαιτούνται κάποιες βασικές γνώσεις θεωρίας αριθμών και θεωρίας ομάδων. Προτείνουμε στους αναγνώστες που δεν είναι εξοικειωμένοι με αυτά να ανατρέξουν στο Παράρτημα Α΄. Το παρόν κεφάλαιο έχει βασιστεί σε μεγάλο βαθμό στα [15, 37, 67, 69]. Επισημαίνουμε ότι τα παρακάτω δεν αποτελούν διεξοδική μελέτη των εργαλείων της κρυπτογραφίας δημοσίου κλειδιού. Παρουσιάζουμε με συντομία, αλλά σαφήνειά μόνο όσα θα χρειαστεί ο αναγνώστης για να κατανοήσει τα επόμενα κεφάλαια.

2.1 Συναρτήσεις Μονής Κατεύθυνσης με Καταπακτή

Σε αυτή την ενότητα θα μιλήσουμε για τις συναρτήσεις μονής κατεύθυνσης με καταπακτή, και θα δούμε πως οι Diffie και Hellman σκέφτηκαν να τις χρησιμοποιήσουν για να λύσουν το πρόβλημα της ασφαλούς ανταλλαγής κλειδιών.

Πριν δώσουμε τον ορισμός αυτών τον συναρτήσεων, θα δώσουμε δύο βοηθητικούς ορισμούς:

Ορισμός 2.1. *Αμελητέα Συνάρτηση*

Μια συνάρτηση neg θα λέμε ότι είναι αμελητέα, αν για για κάθε πολυώνυμο p υπάρχει k_0 ώστε για για κάθε $k \geq k_0$ $neg(k) < \frac{1}{p(k)}$

Για παράδειγμα η συνάρτηση $f(x) = \frac{1}{2^x}$ είναι αμελητέα.

Ορισμός 2.2. *Πιθανοτικός Πολυωνυμικού Χρόνου Αλγόριθμος(PPT)*

Αν υπάρχει πολυώνυμο p τέτοιο ώστε για κάθε είσοδο $x \in \{0,1\}$ ο αλγόριθμος $\mathcal{A}$ υπολογίζει το $\mathcal{A}(x)$ το πολύ σε χρόνο $p(|x|)$ και ο $\mathcal{A}$ έχει τη δυνατότητα να ρίχνει τυχαία νομίσματα θα λέμε ότι είναι ένα PPT αλγόριθμος.

Σε αυτό το σύγγραμα θα ταυτίσουμε το ¨ εύκολα υπολογίσιμο¨, με το ¨ υπάρχει PPT αλγόριθμος που το υπολογίζει¨. Επίσης όταν θα λέμε αποδοτικός αλγόριθμος, θα εννοούμε PPT.

Ορισμός 2.3. *Συνάρτηση Μονής Κατεύθυνσης*
Έστω μια συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$. Η f είναι μονής κατεύθυνσης αν:

1. *υπάρχει* PPT *αλγόριθμος που με είσοδο x, υπολογίζει το $f(x)$*
2. *για κάθε* PPT *αλγόριθμο $\mathcal{A}$ υπάρχει αμελητέα συνάρτηση $neg_{\mathcal{A}}$ τέτοια ώστε για k αρκετά μεγάλο:*

$$Pr[f(w) = y : x \leftarrow\$ \{0,1\}^k; y \leftarrow f(x); w \leftarrow \mathcal{A}(1^k, y)] \leq neg_{\mathcal{A}}(k)$$

Διαισθητικά μια συνάρτηση μονής κατεύθυνσης είναι μια συνάρτηση που είναι εύκολη να υπολογιστεί, και δύσκολο να αντιστραφεί. Αξίζει να σημειώσουμε ότι μας ενδιαφέρει η συνάρτηση να είναι δύσκολο να αντιστραφεί όχι μόνο για κάποιες τιμές της(πολυπλοκότητα χειρότερης περιπτώσεις) αλλά να είναι δύσκολη για (σχεδόν) όλες. Ιδιαίτερο ενδιαφέρον για εμάς έχει μια ειδική κατηγορία συναρτήσεων μονής κατεύθυνσης, αυτές με καταπακτή:

Ορισμός 2.4. *Συνάρτηση Μονής Κατεύθυνσης με Καταπακτή*
Αν f συνάρτηση μονής κατεύθυνσης, αλλά ο υπολογισμός της f^{-1} είναι εύκολος όταν είναι γνωστή κάποια επιπλέον μυστική πληροφορία, θα λέμε ότι η f είναι συνάρτηση μονής κατεύθυνσης με καταπακτή.

Υπάρχουν πολλές υποψήφιες συναρτήσεις μονής κατεύθυνσης με καταπακτή. Λέμε υποψήφιες, γιατί η ύπαρξη τέτοιων συναρτήσεων δεν έχει αποδειχθεί. Η συνθήκη $P \neq NP$ είναι αναγκαία, αλλά όχι ικανή για την ύπαρξη τέτοιων συναρτήσεων. Παρόλα αυτά υπάρχουν κάποια προβλήματα που πιστεύουμε ότι είναι δύσκολα, και χρησιμοποιούνται ευρέως στη πράξη.

Ένα από αυτά είναι η παραγοντοποίηση ακεραίων. Η συνάρτηση $f(p,q) = p \cdot q$ (p, q πρώτοι), είναι εύκολα υπολογίσιμη. Η αντιστροφή της όμως είναι απρόσιτη. Ένα πρόβλημα που σχετίζεται με την παραγοντοποίηση πρώτων, είναι το *RSA*. Η συνάρτηση που είναι εύκολα υπολογίσιμη, είναι η $RSA(n,e,m) = m^e \mod n$, όπου $n = p \cdot q$ με p, q πρώτους αριθμούς και $\text{ΜΚΔ}((e,(p-1)(q-1)) = 1$. Το να αντιστραφεί όμως, να βρεθεί δηλαδή το m, είναι δύσκολο. Αν όμως κάποιος ξέρει την παραγοντοποίηση του n, δηλαδή τα p, q τότε η αντιστροφή γίνεται πολύ εύκολα ως εξής:

1. $\varphi(n) = (p-1)(q-1)$
2. $d = e^{-1} \mod \varphi(n)$
3. $m = (m^e)^d \mod n$

Η *RSA* όπως ορίστηκε παραπάνω λοιπόν, πιστεύεται ότι είναι μια συνάρτηση μονής κατεύθυνσης με καταπακτή. Είναι προφανές από τα παραπάνω, ότι αν η

παραγοντοποίηση ακεραίων αποδειχθεί εύκολη, τότε και το *RSA* είναι εύκολο. Το αν τα δύο προβλήματα είναι ισοδύναμα όμως, είναι ακόμα ανοιχτό πρόβλημα.

Άλλες πιθανές συναρτήσεις μονής κατεύθυνσης βασίζονται σε προβλήματα όπως το Πρόβλημα του Διακριτού Λογαρίθμου ή η συνάρτηση του Rabin που βασίζεται στον τετραγωνισμό $\bmod (pq)$. Σε αυτήν τη ΔΕ, θα μας απασχολήσουν περισσότερο μια κλάση προβλημάτων που είναι βασισμένη στο πρόβλημα του διακριτού λογαρίθμου και παραλλαγές τους.

2.1.1 Πρόβλημα του Διακριτού Λογαρίθμου

Ορισμός 2.5. *Πρόβλημα του Διακριτού Λογαρίθμου(DLP)*

Έστω πεπερασμένη κυκλική ομάδα $\mathbb{G}$ *και γεννήτορας της* g*. Δοθέντος στοιχείο* $h \in \mathbb{G}$ *να βρεθεί* $x < ord(\mathbb{G})$ *τ.ω.* $h = g^x$*.*

Το πρόβλημα όπως το διατυπώσαμε παραπάνω δεν είναι πάντα δύσκολο. Για παράδειγμα αν η $\mathbb{G}$ είναι η αθροιστική ομάδα $\bmod p$ τότε το πρόβλημα μπορεί να λυθεί εύκολα. Ουσιαστικά πρέπει να βρεθεί x τέτοιο ώστε $x * g = h \mod p$. Αυτό όπως ξέρουμε μπορεί να γίνει γρήγορα με τον Επεκτεταμένο Αλγόριθμο του Ευκλείδη(Α΄).

Αν όμως $\mathbb{G}$ είναι υποομάδα τάξης q της πολλαπλασιαστικής ομάδας $\mathbb{Z}_p^*$ με p, q αρκετά μεγάλους πρώτους αριθμούς, τότε πιστεύεται ότι το πρόβλημα είναι δύσκολο.

Ορισμός 2.6. *Υπόθεση του Διακριτού Λογαρίθμου(DLOG)*

Θα λέμε ότι η Υπόθεση του Διακριτού Λογαρίθμου ισχύει για την ομάδα $\mathbb{G}$ *αν για κάθε* PPT *αλγόριθμο* $\mathcal{A}$ *υπάρχει αμελητέα συνάρτηση* neg_A *ώστε:*

$$Pr[x \leftarrow \mathcal{A}(1^\lambda, \mathbb{G}, g, h) : g^x = h] \leq neg_A(\lambda)$$

Συχνά μας είναι χρήσιμες δύο ακόμα υποθέσεις που σχετίζονται άμεσα με την υπόθεση του διακριτού λογαρίθμου. Στη συνέχεια ορίζουμε τα αντίστοιχα προβλήματα. Οι υποθέσεις ορίζονται ανάλογα με τον ορισμό 2.6.

Ορισμός 2.7. *Υπολογιστικό Πρόβλημα Diffie-Hellman(CDH)*

Έστω πεπερασμένη κυκλική ομάδα $\mathbb{G}$*, γεννήτορας της* g*, και* $a, b \in \mathbb{G}$*. Αν* $a = g^x$ *και* $b = g^y$ *να υπολογιστεί* $c \in \mathbb{G}$ *τέτοιο ώστε* $c = g^{xy}$*.*

Ορισμός 2.8. *Πρόβλημα Απόφασης Diffie-Hellman(DDH)*

Έστω πεπερασμένη κυκλική ομάδα $\mathbb{G}$*, γεννήτορας της* g*, και* $a, b, c \in \mathbb{G}$*. Αν* $a = g^x$*,*$b = g^y$ *και* $c = g^z$*, να βρεθεί αν ισχύει ότι* $z = xy$*.*

Είναι προφανές ότι DDH≤CDH≤DLOG. Δεν είναι όμως γνωστό αν κάποια από αυτά είναι και ισοδύναμα. Αυτό που μας ενδιαφέρει στη πράξη είναι ότι υπάρχουν ομάδες $\mathbb{G}$ στις οποίες πιστεύουμε ότι και τα τρία προβλήματα είναι δύσκολα. Πολλά από τα συστήματα που θα δούμε στη συνέχεια της ΔΕ βασίζονται σε αυτή τη παραδοχή. Συχνά θα λέμε ότι δουλεύουμε σε ομάδα $\mathbb{G}$ τάξης q στην οποία θεωρούμε ότι η υπόθεση που θέλουμε ισχύει, χωρίς να γινόμαστε πιο συγκεκριμένοι.

2.1.2 Ανταλλαγή κλειδιού Diffie-Hellman

Ένα από τα πρώτα προβλήματα που η κρυπτογραφία δημοσίου κλειδιού προσπάθησε να λύσει, είναι αυτό της ασφαλής ανταλλαγής κλειδιού. Ας υποθέσουμε ότι η A και ο B θέλουν να συμφωνήσουν σε ένα κοινό μυστικό κλειδί. Οι Diffie και Hellman έδωσαν έναν ασφαλή πρωτόκολλο για να γίνει αυτή η ανταλλαγή[31]. Έστω κυκλική ομάδα $\mathbb{G}$ τάξης q για την οποία υποθέτουμε ότι ισχύει η υπόθεση CDH. Το πρωτόκολλο είναι το εξής:

Πρωτόκολλο Ανταλλαγής Κλειδιών Diffie Hellman		
A		**B**
$a \leftarrow\$ \mathbb{Z}_q$		
$u \leftarrow g^a$	$\xrightarrow{u}$	
		$b \leftarrow\$ \mathbb{Z}_q$
	$\xleftarrow{v}$	$v \leftarrow g^b$
$k \leftarrow u^a (= g^{ab})$		$k \leftarrow v^b = (g^{ab})$
Το k είναι το κοινό τους κλειδί		

Ας υποθέσουμε ότι υπάρχει ένας παθητικός αντίπαλος, η E που παρακολουθεί την επικοινωνία μεταξύ των A και B. Αυτά που βλέπει είναι τα u, v. Το να υπολογίσει το k από τα u, v είναι ακριβώς το υπολογιστικό πρόβλημα Diffie-Hellman που υποθέσαμε ότι είναι δύσκολο!

Τι συμβαίνει όμως αν η E δεν παρακολουθεί μόνο παθητικά την επικοινωνία, αλλά προσπαθήσει να επιτεθεί με πιο ενεργό τρόπο; Αν μπορεί να παρεμβληθεί στην επικοινωνία των A και B μπορεί να συμφωνήσει ένα κλειδί k με την A παριστάνοντας ότι είναι ο B, και ένα κλειδί k' με τον B παριστάνοντας ότι είναι η A. Αυτή η επίθεση είναι γνωστή ως man in middle attack.

Είναι λοιπόν φανερό ότι πρέπει να βρούμε ένα τρόπο να επιβεβαιώνουμε ότι επικοινωνούμε πραγματικά με αυτόν που νομίζουμε. Οι ψηφιακές υπογραφές μας επιτρέπουν να κάνουμε ακριβώς αυτό!

Μια άλλη πιθανή αδυναμία του πρωτοκόλλου είναι ότι η υπόθεση CDH μας λέει ότι είναι δύσκολο να υπολογιστεί το g^{ab} από τα g^a,g^b, αλλά δε μας εξασφαλίζει ότι δε μπορούμε να πάρουμε καμία πληροφορία για το g^{ab}. Στη πράξη μπορούμε να χρησιμοποιήσουμε μια κρυπτογραφική συνάρτηση σύνοψης H (Παράρτημα Β′) και το κλειδί στο οποίο συμφωνούμε να είναι το $\mathsf{H}(k)$.

2.2 Κρυπτοσυστήματα Δημοσίου Κλειδιού

Το βασικότερο αντικείμενο της κρυπτογραφίας, είναι η αποστολή μυστικών μηνυμάτων. Η πιο απλή περίπτωση είναι ότι η A θέλει να στείλει στον B ένα μήνυμα $\mathtt{m}$, το οποίο όμως να μπορεί να διαβάσει μόνο ο B. Η A χρησιμοποιεί

λοιπόν ένα κλειδί κρυπτογράφησης k και έναν αλγόριθμο κρυπτογράφησης Enc, και στέλνει στον B το κρυπτοκείμενο $c \leftarrow \mathsf{Enc}k(\mathtt{m})$. Ο B με τη σειρά του αφού λάβει το μήνυμα χρησιμοποιεί το αντίστοιχο κλειδί k' και τον κατάλληλο αλγόριθμο αποκρυπτογράφησης Dec, και αποκτά το αρχικό μήνυμα $\mathtt{m} \leftarrow \mathsf{Dec}_{k'}(c)$.

Κρυπτοσύστημα ονομάζουμε μια σειρά αλγορίθμων (KGen, Enc, Dec) που επιτυγχάνουν τα παραπάνω.

Μπορούμε να χρησιμοποιήσουμε κρυπτογραφία δημοσίου κλειδιού, ώστε να κατασκευάσουμε ένα κρυπτοσύστημα που λειτουργεί χωρίς να πρέπει αποστολέας και ο παραλήπτης να έχουν προσυμφωνήσει κάποιο κλειδί. Αν $(\mathsf{sk}_b, \mathsf{pk}_b) \leftarrow \mathsf{KGen}()$ είναι το ιδιωτικό και το δημόσιο κλειδί του B, τότε η A μπορεί να χρησιμοποιήσει ως κλειδί κρυπτογράφησης το pk_b. Τότε ο B, και μόνο ο B, μπορεί να χρησιμοποιήσει το pk_b ως κλειδί αποκρυπτογράφησης και να ανακτήσει το αρχικό μήνυμα. Ακριβώς επειδή το κλειδί κρυπτογράφησης και αποκρυπτογράφησης δεν είναι το ίδιο, η κρυπτογραφία δημοσίου κλειδιού λέγεται και ασύμμετρη κρυπτογραφία.

Έχουν προταθεί και χρησιμοποιούνται πολλά κρυπτοσυστήματα με τα δικά τους πλεονεκτήματα και μειονεκτήματα, όπως για παράδειγμα το RSA[61], το κρυπτοσύστημα Paillier[58] και πολλά άλλα. Εμείς επιλέξαμε ενδεικτικά να παρουσιάσουμε το κρυπτοσύστημα Elgamal.

2.2.1 Κρυπτοσύστημα ElGamal

Ένας από τα πιο απλά κρυπτοσυστήματα που βασίζονται στο πρόβλημα του διακριτούς λογαρίθμου(DLOG) είναι το κρυπτοσύστημα ElGamal[32]. Σε αυτό το κρυπτοσύστημα υπάρχουν ως δημόσιες παράμετροι, δύο αρκετά μεγάλοι πρώτοι p, q τέτοιοι ώστε ο q να διαιρεί το $p-1$ και ένας γεννήτορας g της υποομάδας $\mathbb{G}$ τάξης q του $\mathbb{Z}_p^*$. Η επιλογή των παραμέτρων έχει γίνει με τέτοιων τρόπο, που πιστεύεται ότι το DDH είναι δύσκολο στη $\mathbb{G}$. Για τα πιθανά μηνύματα υποθέτουμε ότι ισχύει $\mathtt{m} \in \mathbb{G}$. Αφού οι παράμετροι έχουν αποφασισθεί, μπορούμε να δημιουργήσουμε ένα ζευγάρι κλειδιών, να κρυπτογραφήσουμε και αν αποκρυπτογραφήσουμε ένα μήνυμα ως εξής:

Δημιουργία Κλειδιών KGen()	
1 :	$x \leftarrow\$ \mathbb{Z}_q$
2 :	$y \leftarrow g^x \mod q$
3 :	$\mathsf{sk} \leftarrow x$, $\mathsf{pk} \leftarrow y$
Κρυπτογράφηση $\mathsf{Enc}_{\mathsf{pk}}(\mathtt{m})$	
1 :	$r \leftarrow\$ \mathbb{Z}_q$
2 :	$R \leftarrow g^r \mod q$
3 :	$M \leftarrow my^r \mod q$
4 :	$c \leftarrow (R, M)$
Αποκρυπτογράφηση $\mathsf{Dec}_{\mathsf{sk}}(c)$	
1 :	$m \leftarrow MR^{-x}$

Πράγματι $\mathsf{Dec}(\mathsf{Enc}(m)) = m$ αφού $MR^{-x} = my^r g^{-xr} = mg^{xr-xr} = m$.

Είναι όμως αυτό το κρυπτοσύστημα ασφαλές; Διαισθητικά, θα θέλαμε ένα αντίπαλος $\mathcal{A}$ ο οποίος δε γνωρίζει το μυστικό κλειδί x να μη μπορεί να ανακτήσει το μήνυμα $\mathtt{m}$. Όμως τι έχει στη διάθεση του ο $\mathcal{A}$; Για να μπορέσουμε να δώσουμε μια απάντηση σε αυτά τα ερωτήματα, πρέπει πρώτα να ορίσουμε τι σημαίνει για ένα κρυπτοσύστημα να είναι ασφαλές. Θα επιστρέψουμε στην ασφάλεια του ElGamal αφού δούμε πρώτα τους ορισμούς.

2.2.2 Ασφάλεια Κρυπτοσυστημάτων Δημοσίου Κλειδιού

Ας σκεφτούμε πρώτα ποιες ιδιότητες θα θέλαμε να έχει ένα κρυπτοσύστημα. Σίγουρα δε θα πρέπει ένας αντίπαλος $\mathcal{A}$ να μπορεί να ανακτήσει το μυστικό κλειδί sk μόνο από το δημόσιο κλειδί pk. Επιπρόσθετα θα θέλαμε ο $\mathcal{A}$ να μη μπορεί να ανακτήσει καμία πληροφορία για το μήνυμα $\mathtt{m}$ από το κρυπτοκείμενο c και τις δημόσιες πληροφορίες. Επιπρόσθετες εγγυήσεις θα ήταν επιθυμητές, όπως για παράδειγμα να μη μπορεί να ανακτηθεί το μήνυμα ακόμα και αν ο $\mathcal{A}$ έχει στη διάθεση του κρυπτογραφήσεις από μηνύματα της επιλογής του, ή ακόμα και αν έχει στη διάθεση του αποκρυπτογραφήσεις από κρυπτοκείμενα της επιλογής του.

Έχουν προταθεί διάφοροι ορισμοί που προσπαθούν να αποτυπώσουν αυτές τις απαιτήσεις ασφαλείας. Επιλέγουμε να παρουσιάσουμε αυτούς που διατυπώνονται μέσα από τα λεγόμενα παιχνίδια ασφάλειας. Ουσιαστικά, δίνουμε τους ορισμούς μέσα από ένα παιχνίδι μεταξύ ενός προκαλούντα C και ενός αντιπάλου $\mathcal{A}$. Και οι δύο οντότητες θεωρούμε ότι είναι PPT αλγόριθμοι οι οποίοι επικοινωνούν. Ο $\mathcal{A}$ διαλέγει δύο μηνύματα $\mathtt{m}_0, \mathtt{m}_1$ και τα δίνει στον C. Ο C επιλέγει ένα από τα δύο τυχαία, το κρυπτογραφεί και το στέλνει στον $\mathcal{A}$. Ο $\mathcal{A}$ προσπαθεί να μαντέψει σε πιο από τα δύο μηνύματα αντιστοιχεί το κρυπτοκείμενο. Αν η πιθανότητα να μαντέψει σωστά είναι αμελητέα κοντά στο $\frac{1}{2}$ τότε θεωρούμε ότι το κρυπτοσύστημα είναι ασφαλές. Ανάλογα με τις δυνατότητες που υποθέτουμε ότι έχει ο $\mathcal{A}$, ορίζουμε τα αντίστοιχα παιχνίδια ασφάλειας. Στα παιχνίδια μοντελοποιούμε τις δυνατότητες αυτές με κάποια μαντεία. Για παράδειγμα αν ο αντίπαλος μπορεί να κρυπτογραφεί μηνύματα της επιλογής του θα γράφουμε $\mathcal{A}^{\mathsf{Enc}}$ (ο $\mathcal{A}$ με πρόσβαση στο μαντείο κρυπτογράφησης), ενώ αν μπορεί και να αποκρυπτογραφεί $\mathcal{A}^{\mathsf{Enc,Dec}}$ κτλπ.

Επίθεση Επιλεγμένου Μηνύματος(CPA)

Σε ένα κρυπτοσύστημα δημοσίου κλειδιού οποιοσδήποτε μπορεί να κρυπτογραφεί μηνύματα της αρεσκείας του. Για αυτό και ο πιο αδύναμος αντίπαλος που έχει νόημα να υποθέσουμε, είναι αυτός που μπορεί να κάνει Επίθεση Επιλεγμένου Μηνύματος (CPA).

Ορισμός 2.9 (IND-CPA). *Ένα κρυπτοσύστημα έχει την ιδιότητα IND-CPA αν για κάθε* PPT *αλγόριθμο* $\mathcal{A}$*, υπάρχει αμελητέα συνάρτηση* neg_A *τέτοια ώστε:*

$$Pr[\mathtt{Exp}_{\mathcal{A}}^{IND-CPA} = 1] \leq \frac{1}{2} + neg_A(\lambda)$$

Παιχνίδι 2.1: Επίθεση Επιλεγμένου Μηνύματος (CPA) $\mathtt{Exp}_{\mathcal{A}}^{IND-CPA}$

Είσοδος: λ
Έξοδος: $\{0, 1\}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\mathtt{m}_0, \mathtt{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc}}(1^\lambda, \mathsf{pk})$
$b \leftarrow\$ \{0, 1\}$
$c \leftarrow \mathsf{Enc}(\mathtt{m}_b)$
$b' \leftarrow \mathcal{A}^{\mathsf{Enc}}(1^\lambda, \mathsf{pk}, c)$
επέστρεψε $b = b'$

Επίθεση Επιλεγμένου Κρυπτοκειμένου(CCA)

Ένας δυνατότερος αντίπαλος $\mathcal{A}$, μπορεί να ζητά αποκρυπτογραφήσεις κρυπτοκειμένων της αρεσκείας του. Εδώ διακρίνουμε δύο περιπτώσεις, είτε ο αντίπαλος μπορεί να αποκρυπτογραφεί μέχρι να του δοθεί η πρόκληση, είτε μπορεί να αποκρυπτογραφεί και μηνύματα αφού του δοθεί η πρόκληση, εκτός φυσικά από το κρυπτοκείμενο της πρόκλησης. Σε κάθε περίπτωση φυσικά είναι περιορισμένος σε πολυωνυμικό πλήθος κρυπτογραφήσεων.

Παιχνίδι 2.2: Επίθεση Γνωστού Κρυπτοκειμένου 1(CCA) $\mathtt{Exp}_{\mathcal{A}}^{IND-CCA1}$

Είσοδος: λ
Έξοδος: $\{0, 1\}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\mathtt{m}_0, \mathtt{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc},\mathsf{Dec}}(1^\lambda, \mathsf{pk})$
$b \leftarrow\$ \{0, 1\}$
$c \leftarrow \mathsf{Enc}(\mathtt{m}_b)$
$b' \leftarrow \mathcal{A}^{\mathsf{Enc}}(1^\lambda, \mathsf{pk}, c)$
επέστρεψε $b = b'$

Ορισμός 2.10 (IND-CCA1). *Ένα κρυπτοσύστημα έχει την ιδιότητα IND-CCA1 αν για κάθε* PPT *αλγόριθμο $\mathcal{A}$, υπάρχει αμελητέα συνάρτηση neg_A τέτοια ώστε:*

$$Pr[\mathtt{Exp}_{\mathcal{A}}^{IND-CCA1} = 1] \leq \frac{1}{2} + neg_A(\lambda)$$

Ορισμός 2.11 (IND-CCA2). *Ένα κρυπτοσύστημα έχει την ιδιότητα IND-CCA2 αν για κάθε* PPT *αλγόριθμο $\mathcal{A}$, υπάρχει αμελητέα συνάρτηση neg_A τέτοια ώστε:*

$$Pr[\mathtt{Exp}_{\mathcal{A}}^{IND-CCA2} = 1] \leq \frac{1}{2} + neg_A(\lambda)$$

Λήμμα 2.1. *IND-CCA2 $\Longrightarrow$ IND-CCA1 $\Longrightarrow$ IND-CPA*

Παιχνίδι 2.3: Επίθεση Γνωστού Κρυπτοκειμένου 2(CCA) $\mathtt{Exp}_{\mathcal{A}}^{IND-CCA2}$

Είσοδος: λ
Έξοδος: $\{0, 1\}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\mathtt{m}_0, \mathtt{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc},\mathsf{Dec}}(1^\lambda, \mathsf{pk})$
$b \leftarrow\$ \{0, 1\}$
$c \leftarrow \mathsf{Enc}(\mathtt{m}_b)$
$b' \leftarrow \mathcal{A}^{\mathsf{Enc},\mathsf{Dec}}(1^\lambda, \mathsf{pk}, c)$
Αν *c δεν είναι είσοδος στο* Dec **τότε**
| **επέστρεψε** $b = b'$
αλλιώς
| **επέστρεψε** $\perp$

Ασφάλεια Κρυπτοσυστήματος ElGamal

Επιστρέψουμε τώρα στο κρυπτοσύστημα ElGamal και θα αναλύσουμε την ασφάλεια του.

Θεώρημα 2.1. *Το κρυπτοσύστημα ElGamal διαθέτει την ιδιότητα IND-CPA, αν ισχύει η υπόθεση DDH.*

Απόδειξη. Θα υποθέσουμε προς άτοπο, ότι υπάρχει *PPT* αντίπαλος $\mathcal{A}$ που νικάει το Παιχνίδι 2.1 με μη αμελητέα πιθανότητα. Θα κατασκευάσουμε αλγόριθμο $\mathcal{M}$ που έχει ως είσοδο μια τριάδα $g^x, g^y, g^z \in \mathbb{G}$, και χρησιμοποιώντας τον $\mathcal{A}$ σαν υπορουτίνα, αποφαίνεται για το DDH με μη αμελητέα πιθανότητα. Ο $\mathcal{M}$ θέτει $\mathsf{pk} = g^x$ και παίζει με τον $\mathcal{A}$ το Παιχνίδι 2.1. Όταν ο $\mathcal{A}$ ζητά την πρόκληση c, ο $\mathcal{M}$ στέλνει το $c = (g^y, \mathtt{m}_b g^z)$. Αν ο $\mathcal{A}$ απαντήσει σωστά, ο $\mathcal{M}$ επιστρέφει 1, αλλιώς 0.

Στη περίπτωση που η είσοδος δεν ήταν τριάδα Diffie-Hellman το c δεν είναι έγκυρο κρυπτοκείμενο, άρα ο $\mathcal{A}$ αναγκαστικά απαντάει τυχαία. Αν ήταν τριάδα όμως, έχουμε έγκυρο κρυπτοκείμενο και από την υπόθεση μας ο $\mathcal{A}$ θα απαντήσει σωστά με πιθανότητα μη αμελητέα μεγαλύτερη του $\frac{1}{2}$. Άρα ελικά ο $\mathcal{M}$ ξεχωρίζει μια τριάδα Diffie-Hellman από μια τυχαία, με μη αμελητέα πιθανότητα. □

Θεώρημα 2.2. *Το κρυπτοσύστημα ElGamal δε διαθέτει την ιδιότητα IND-CCA2.*

Απόδειξη. Έστω ότι ο $\mathcal{A}$ δέχεται τη πρόκληση $c = (g^r, \mathtt{m}_b y^r)$. Κατασκευάζει το $c' = (g^{r+r'}, \mathtt{m}_b m' y^{r+r'})$, όπου r', m' της επιλογής του. Αυτή είναι μια έγκυρη κρυπτογράφηση του $\mathtt{m}_b m'$, και συνεπώς μπορεί να λάβει την αποκρυπτογράφηση του M' από το μαντείο. Αυτό επιτρέπεται αφού $c \neq c'$, άρα ο $\mathcal{A}$ μπορεί να υπολογίσει το $\mathtt{m}_b = M' m'^{-1}$ □

Σημείωση 2.1. *Ενδιαφέρον έχει ότι η ασφάλεια IND-CCA1 του ElGamal αποτελούσε για πολλά χρόνια ανοικτό πρόβλημα. Σχετικά πρόσφατα [46] αποδείχτηκε ότι είναι IND-CCA, αλλά με μη συνηθισμένη υπόθεση, γνήσια ισχυρότερη της DDH.*

ΚΕΦΑΛΑΙΟ 3

Ψηφιακές Υπογραφές

Η έννοια της ψηφιακής υπογραφής(digital signature) είναι ίσως από τις σημαντικότερες της σύγχρονης κρυπτογραφίας. Ένα σχήμα υπογραφών επιτρέπει σε ένα χρήστη να υπογράφει μηνύματα έτσι ώστε οποιοσδήποτε να μπορεί να επαληθεύσει ότι το μήνυμα δεν έχει παραποιηθεί και προέρχεται όντως από αυτόν το χρήστη. Η βασική ιδέα είναι παρόμοια με αυτή του κεφαλαίου 2. Εδώ η υπογραφή παράγεται με το ιδιωτικό κλειδί του υπογράφοντα, και οποιασδήποτε μπορεί να πεισθεί ότι μόνο κάποιος που ξέρει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί θα μπορούσε να την έχει παράγει.

Σε αυτό το κεφάλαιο θα δούμε τι αποτελεί μια ψηφιακή υπογραφή, ποιες είναι οι απαιτήσεις ασφάλειας και ποιος ο βασικός ρόλος τους. Σαν βασικό μας παράδειγμα θα χρησιμοποιήσουμε το σχήμα υπογραφών ElGamal.

Το παρόν κεφάλαιο έχει βασιστεί στα αντίστοιχα κεφάλαια των [15, 37, 67, 69]. Για την κατανόηση κάποιων από των εννοιών αυτού του κεφαλαίου, συμβουλεύουμε τους αναγνώστες να ανατρέξουν στα Παραρτήματα Α΄,Β΄,Γ΄.

3.1 Ορισμοί

Ένα σχήμα ψηφιακών υπογραφών αποτελείται από μια τριάδα αποδοτικών αλγορίθμων (KGen, Sign, Vrfy):

- *Δημιουργία κλειδιών*: Δημιουργεί ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού.
  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$

- *Υπογραφή*: Με είσοδο ένα ιδιωτικό κλειδί και ένα μήνυμα, επιστρέφει μια υπογραφή.
  $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathtt{m})$

- *Επαλήθευση*: Με είσοδο ένα δημόσιο κλειδί και μια υπογραφή και το μήνυμα, επιστρέφει αν είναι έγκυρη ή όχι.
  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\mathsf{pk}, \sigma, \mathtt{m})$

Κάποιες φορές επισημαίνουμε επίσης και τους χώρους των πιθανών κλειδιών, των πιθανών μηνυμάτων και των πιθανών υπογραφών, αλλά συχνά θα εννοούνται.

Ασφάλεια Ψηφιακών Υπογραφών

Από μια ψηφιακή υπογραφή, απαιτούμε να έχει τις παρακάτω ιδιότητες:

- *Γνησιότητα*(message authentication): Το μήνυμα προέρχεται από το σωστό αποστολέα
- *Ακεραιότητα*: Το περιεχόμενο του μηνύματος δεν έχεις παραποιηθεί.
- *Μη-Αποκήρυξη*(non-repudiation): Αν κάποιος υπογράψει ένα μήνυμα, δε μπορεί μετά να ισχυριστεί ότι δεν το έκανε.
- *Μη-Πλαστογραφήσιμη*(unforgeable): Δε μπορεί κάποιος να πλαστογραφήσει την υπογραφή.

Η τελευταία ιδιότητα συχνά χωρίζεται σε υποκατηγορίες με βάση το τι μπορεί να καταφέρει ένας αντίπαλος που πλαστογραφεί:

- *Υπαρξιακή Πλαστογραφία*(Existential Forgery): Ο αντίπαλος μπορεί να πλαστογραφήσει την υπογραφή για κάποιο μήνυμα, όχι αναγκαστηκά της επιλογής του.
- *Επιλεγμένη Πλαστογραφία*(Selective Forgery): Ο αντίπαλος μπορεί να πλαστογραφήσει την υπογραφή για κάποιο μήνυμα της επιλογής του.
- *Ολική Πλαστογραφία*(Universal Forgery): Ο αντίπαλος μπορεί να πλαστογραφεί την υπογραφή για οποιοδήποτε μήνυμα της επιλογής του. Αν αυτό συμβαίνει επειδή μπορεί να υπολογίσει τον ιδιωτικό κλειδί, μιλάμε για ολοκληρωτικό σπάσιμο(total break) του σχήματος.

Ένα άλλος διαχωρισμός που κάνουμε, είναι ανάλογα με το ποιες δυνατότητες υποθέτουμε ότι έχει ο αντίπαλος $\mathcal{A}$ στη διάθεση του:

- *Επίθεση Δημοσίου Κλειδιού*: Ο αντίπαλος έχει στη διάθεση του μόνο τις δημόσιες παραμέτρους και το δημόσιο κλειδί του υπογράφοντα.
- *Επίθεση Γνωστής Υπογραφής*(Known Signature Attack): Ο αντίπαλος έχει στη διάθεση του ζεύγη υπογραφών-μηνυμάτων υπογεγραμμένα από τον πραγματικό υπογράφοντα. Ρεαλιστικά αυτό είναι το ελάχιστο που μπορεί να κάνει ένας αντίπαλος.
- *Επίθεση Γνωστού Μηνύματος*(Known Message Attack): Ο αντίπαλος μπορεί να ζητήσει από τον πραγματικό υπογράφοντα να υπογράψει μηνύματα της επιλογής του. Η επιλογή του μπορεί να βασίζεται και στις προηγούμενες υπογραφές που έχει δει.

Σε αυτή τη ΔΕ μας ενδιαφέρει κυρίως το μεγαλύτερο επίπεδο ασφάλειας, δηλαδή θα λέμε ότι μια ψηφιακή είναι μη-πλαστογραφήσιμη, όταν είναι αδύνατη η υπαρξιακή πλαστογραφία ενάντια σε μια επίθεση γνωστού μηνύματος. Όπως και στο κεφάλαιο 2, μπορούμε να δώσουμε έναν ορισμό με βάση ένα παιχνίδι. Τη δυνατότητα του αντιπάλου να ζητάει υπογραφές για μηνύματα της επιλογής του την μοντελοποιήσουμε με το μαντείο $\mathcal{SO}$.

Παιχνίδι 3.1: Επίθεση Επιλεγμένου Μηνύματος $\mathtt{Exp}_{\mathcal{A}}^{Unf}$

Είσοδος: λ
Έξοδος: $\{0, 1\}$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\sigma, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{SO}}(1^\lambda, \mathsf{pk})$
Αν *σ δεν είναι έξοδος του* $\mathcal{SO}$ **τότε**
  επέστρεψε $\mathsf{Vrfy}(\mathsf{pk}, \sigma, \mathtt{m})$
αλλιώς
  επέστρεψε $\perp$

Ορισμός 3.1 (Μη-Πλαστογραφήσιμη). *Μια ψηφιακή υπογραφή θα λέμε ότι είναι μη-πλαστογραφήσιμη αν για κάθε* PPT *αλγόριθμο* $\mathcal{A}$, *υπάρχει αμελητέα συνάρτηση* neg_A *τέτοια ώστε:*

$$Pr[\mathtt{Exp}_{\mathcal{A}}^{Unf} = 1] \leq neg_A(\lambda)$$

Υποδομή Δημοσίου Κλειδιού(PKI)

Οι ψηφιακές υπογραφές μας εξασφαλίζουν ότι ένα υπογεγραμμένο μήνυμα προέρχεται από τον κάτοχο του αντίστοιχου δημοσίου κλειδιού. Όμως πως ξέρουμε ότι ο κάτοχος του κλειδιού είναι αυτός που ισχυρίζεται ότι είναι; Μπορεί ένα κλειδί να πιστεύουμε για παράδειγμα ότι ανήκει στην Αλίκη, επειδή το βρήκαμε στην ιστοσελίδα της, αλλά πως ξέρουμε ότι ένας ενεργός αντίπαλος δε το έχει αντικαταστήσει με το δικό του; Αυτό είναι ένα μεγάλο πρόβλημα, και ενώ έχουν προταθεί πολλές λύσεις που χρησιμοποιούνται πρακτικά, δεν έχει βρεθεί κάποια τέλεια λύσει, αλλά το πρόβλημα έχει μετατεθεί.

Η πιο συνήθεις λύση είναι η υπόθεση ότι υπάρχει μια υποδομή δημοσίου κλειδιού(PKI). Ουσιαστικά υπάρχουν κάποιες αρχές που εκδίδουν πιστοποιητικά γνησιότητας για δημόσια κλειδιά. Οπότε το πρόβλημα της πιστοποίησης μετατίθεται από το χρήστη σε αυτές τις αρχές, οι οποίες πρέπει να υποθέσουμε ότι είναι έμπιστες.

Μια εναλλακτική λύση σε αυτό το πρόβλημα είναι η κρυπτογράφηση με βάση τη ταυτότητα(identity base cryptography)[66]. Η βασική ιδέα είναι ότι τα δημόσια κλειδιά προέρχονται από κάποιο στοιχείο της ταυτότητας το κάθε χρήστη, όπως για παράδειγμα τη διεύθυνση ηλεκτρονικού ταχυδρομείου, το τηλέφωνο ή τη διεύθυνση IP του κάθε χρήστη. Πάλι όμως πρέπει να υποθέσουμε ότι υπάρχει μια έμπιστη αρχή που θα διανέμει τα ιδιωτικά κλειδιά στους χρήστες. Τα προβλήματα είναι ανάλογα με την λύση της PKI[59].

Σε αυτή τη ΔΕ δε θα μας απασχολήσει αυτό το πρόβλημά. Κάθε φορά που θα έχουμε ένα σύστημα δημοσίων κλειδιών, θα ταυτίζουμε το δημόσιο κλειδί με μια οντότητα, και δε θα μας απασχολεί το πρόβλημα της αυθεντικότητας. Στη πράξη αυτό ισοδυναμεί με την υπόθεση ότι υπάρχει μια υποδομή δημοσίου κλειδιού που εμπιστευόμαστε.

3.2 Το σχήμα υπογραφών ElGamal

Σαν ένα παράδειγμα ψηφιακής υπογραφής, θα εξετάσουμε το κλασικό σχήμα ElGamal[32].

Δουλεύουμε στην ομάδα $\mathbb{Z}_q^*$ τάξης πρώτου p όπου θεωρούμε ότι ισχύει η υπόθεση DLOG με γεννήτορα το g.

Δημιουργία Κλειδιών KGen()
1 : $x \leftarrow\$ \{1, p-2\}$
2 : $y \leftarrow g^x \mod p$
3 : $\mathsf{sk} \leftarrow x$, $\mathsf{pk} \leftarrow y$
Υπογραφή Sign($x, \mathtt{m}$)
1 : $k \leftarrow\$ U(\mathbb{Z}_{p-1})$
2 : $r \leftarrow g^k \mod p$
3 : $s \leftarrow (\mathtt{m} - xr)k^{-1} \mod p-1$
4 : $\sigma \leftarrow (r, s)$
Επαλήθευση Vrfy(y, σ)
1 : $0 < r < p$ ΚΑΙ $0 < s < p-1$
2 : $g^{\mathtt{m}} = y^r r^s \mod p$
3 : Αν ισχύουν τα 1,2 επέστρεψε 1, αλλιώς 0.

Λήμμα 3.1 (Ορθότητα). *Ο αλγόριθμος επαλήθευσης επιστρέφει 1 για υπογραφές που είναι αποτέλεσμα του αλγόριθμου υπογραφής.*

Απόδειξη. Έχουμε ότι $y^r r^s = g^{xr} g^{ks} = g^{xr+\mathtt{m}-xr} = g^{\mathtt{m}}$ □

Ας εξετάσουμε τώρα την ασφάλεια του σχήματος. Για να υπολογίσει το ιδιωτικό κλειδί y θα πρέπει να μπορεί να λύσει το DLOG.

Μια άλλη πιθανή επίθεση θα είναι, για δεδομένα $\mathtt{m}, s$ να προσπαθήσει να υπολογίσει r τέτοιο ώστε $y^r r^s = g^{\mathtt{m}}$. Αυτό, παρότι δεν είναι γνωστό αν ανάγεται σε κάποιο από τις γνωστές μας παραδοχές, πιστεύουμε ότι είναι ένα δύσκολο πρόβλημα.

Παρότι όμως ο $\mathcal{A}$ φαίνεται να μη μπορεί να πλαστογραφήσει την υπογραφή για ένα μήνυμα της επιλογής του, μπορεί να πετύχει υπαρξιακή πλαστογραφία ως εξής:

1. $e \leftarrow\$ \{1, \ldots, p-1\}$
2. $r \leftarrow g^e y \mod p$
3. $s \leftarrow -r \mod p$
4. $\mathtt{m} \leftarrow es \mod p-1$

Πράγματι, $y^r r^s = g^{xr+es} y^{-r} = g^{es} = g^{\mathtt{m}}$

Αυτό το πρόβλημα μπορεί να λυθεί με τη χρήση μια κρυπτογραφικής συνάρτησης σύνοψης H(Παράρτημα Β΄). Αντί για το $\mathtt{m}$, χρησιμοποιούμε το $\mathsf{H}(\mathtt{m}, r)$. Αυτό αποτρέπει τον αντίπαλο από το να παράξει το $\mathtt{m}$ αφού έχει παράξει την υπογραφή. Είναι σημαντικό το k να μένει κρυφό, και η επιλογή του να είναι τυχαία(να μην χρησιμοποιείται το ίδιο k πάνω από μια φορά), αλλιώς είναι εύκολο να δούμε ότι υπάρχουν επιθέσεις που μπορούν να υπολογίσουν το ιδιωτικό κλειδί.

Τα παραπάνω δεν αποτελούν φυσικά απόδειξη για την ασφάλεια του σχήματος. Περισσότερες λεπτομέρειες για μεθόδους απόδειξης για σχήματα ψηφιακών υπογραφών μπορούν να βρεθούν στο Παράρτημα Β΄.

3.2.1 Άλλες Υπογραφές

Άλλες υπογραφές που είναι συγγενείς με το σχήμα ElGamal, καθώς όπως και αυτές βασίζονται σε παραδοχές τύπου DLOG, είναι οι υπογραφές Schnorr[65](βλ. και Παράρτημα Γ΄) και ο Αλγόριθμος Ψηφιακών Υπογραφών DSA[54].

Τέλος σημειώνουμε ότι στη πράξη πολλές φορές χρησιμοποιούμε παραλλαγές που αξιοποιούν ελλειπτικές καμπύλες, όπως είναι ο ECDSA[14]. Η κρυπτογραφία ελλειπτικών καμπυλών, για παρόμοια επίπεδα ασφάλειας, χρειάζεται πολύ μικρότερα κλειδιά. Επειδή πιστεύουμε ότι ο μέσος αναγνώστης είναι πιο εξοικειωμένος με τη θεωρία ομάδων, από ότι με τις ελλειπτικές καμπύλες, σε αυτή τη ΔΕ δε θα αναφερόμαστε σε αυτές. Αυτό είναι καθαρά για την ευκολία της παρουσίασης. Συχνά τα σχήματα στα οποία αναφερόμαστε έχουν παραλλαγές με ελλειπτικές καμπύλες, αλλά η παρουσίαση τους ξεφεύγει από το σκοπό αυτής της ΔΕ.

Στα επόμενα κεφάλαια θα δούμε κάποιες υπογραφές με επιπρόσθετη λειτουργικότητα που έχουν ιδιαίτερο ενδιαφέρον για εμάς. Πρόκειται για υπογραφές που έχουν διαφορετικές ιδιότητες και η χρήση τους διαφέρει από τις απλές ψηφιακές υπογραφές. Στο κεφάλαιο 4 θα δούμε τις Υπογραφές Καθορισμένου Επαληθευτή (DVS), στο κεφάλαιο 4 τις Υπογραφές Δακτυλίου (Ring Signatures), και στο κεφάλαιο 6 θα δούμε το καινοτόμο συνδυασμό των δύο προηγούμενων, τις Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή (DVLRS) που αποτελούν ίσως τη σημαντικότερη συνεισφορά αυτής της ΔΕ.

ΚΕΦΑΛΑΙΟ 4

Υπογραφές Καθορισμένου Επαληθευτή

Κάποιες φορές είναι επιθυμούμε να περιορίσουμε το ποιος μπορεί να πειστεί για την εγκυρότητα μιας υπογραφής. Έχουν προταθεί διάφορα είδη υπογραφών που επιτυγχάνουν διάφορες παραλλαγές αυτή της ιδιότητας, όλες με χρήσιμες εφαρμογές.

Οι αδιαμφισβήτητες υπογραφές (undeniable signatures)[22], απαιτούν τη συμμετοχή του υπογράφοντα στον αλγόριθμο επαλήθευσης, χωρίς όμως να μπορεί να ισχυριστεί ότι μια δικιά του υπογραφή δεν είναι δικιά του. Ο υπογράφοντας μπορεί πάντα να αποδείξει ότι μια έγκυρη υπογραφή είναι έγκυρη, και μια άκυρη υπογραφή είναι άκυρη.

Οι υπογραφές καθορισμένου επιβεβαιωτή (designated confirmer signatures)[20], μπορούν να επαληθευτούν με τη συμμετοχή μιας τρίτης οντότητας, που αποκαλείτε καθορισμένος επιβεβαιωτής, ο οποίος μπορεί να αποδείξει την εγκυρότητα μιας υπογραφής χωρίς τη συμμετοχή του υπογράφοντα.

Τέλος, οι υπογραφές καθορισμένου επαληθευτή (designated verifier signatures) [42], είναι υπογραφές που μπορούν να πείσουν μόνο έναν επαληθευτή, ο οποίος δε μπορεί όμως να αποδείξει σε κανέναν άλλο ότι η υπογραφή προέρχεται από τον υπογράφοντα. Αυτό επιτυγχάνεται επειδή ο ίδιο ο επαληθευτής έχει τη δυνατότητα να παράξει μόνος του προσομοιώσεις υπογραφών, τις οποίες κανένας άλλος δε μπορεί να διακρίνει από μια έγκυρη υπογραφή.

Σε αυτή τη ΔΕ ενδιαφερόμαστε κυρίως για το τρίτο είδος (DVS), αναφερόμαστε όμως σε σύντομα και στα άλλα είδη, για να γίνουν ξεκάθαρες οι ομοιότητες και οι διαφορές των συγγενικών αυτών συστημάτων. Καθότι τα ονόματα είναι παρόμοια και όχι αναγκαστικά αντιπροσωπευτικά των ιδιοτήτων του κάθε είδος, είναι πολύ εύκολο για έναν αναγνώστη που δεν είναι εξοικειωμένος να συγχέει το ένα με το άλλο.

4.1 Αδιαμφισβήτητες Υπογραφές

Ας υποθέσουμε ότι μια εταιρεία ανάπτυξης λογισμικού, θέλει να υπογράψει το λογισμικό που πουλάει, ώστε οι αγοραστές του να γνωρίζουν ότι είναι γνήσιο. Θέλει όμως, μόνο οι πελάτες που έχουν πληρώσει να μπορούν να λάβουν αυτή τη πιστοποίηση. Με μια απλή ψηφιακή υπογραφή, οποιοσδήποτε θα μπορούσε να μεταπουλήσει το λογισμικό, και όλοι θα ήταν πεπεισμένοι για τη γνησιότητα του, αφού έχει την υπογραφή της εταιρείας.

Το 1989, οι Chaum και van Antwerpen, εισήγαγαν την έννοια της Αδιαμφισβήτητης Υπογραφής(Undeniable Signature)[22]. Η ιδέα ήταν η εξής. Όπως και

σε μια απλή ψηφιακή υπογραφή, ο υπογράφων A χρησιμοποιεί το ιδιωτικό κλειδί sk για να υπογράψει ένα μήνυμα $\mathtt{m}$ και παράγει μια υπογραφή σ. Σε αντίθεση όμως με τις απλές ψηφιακές υπογραφές, κανείς δε μπορεί να πιστοποιήσει τη γνησιότητα μιας υπογραφής, χωρίς τη συμμετοχή του A σε ένα διαλογικό πρωτόκολλο. Η ονομασία αδιαμφισβήτητη, προέρχεται από την ιδιότητα μια γνήσιας υπογραφής, να μην μπορεί να αποκηρυχθεί από αυτό που την υπέγραψε, ενώ μπορεί να αποδεικνύει όταν μια υπογραφή δεν είναι έγκυρη. Ο κάτοχος της υπογραφής μπορεί να ξεκινήσει ένα διαλογικό πρωτόκολλο στο οποίο θα αποδειχθεί ότι η υπογραφή είναι γνήσια, ακόμα και αν ο υπογράφοντας είναι κακόβουλος και προσπαθήσει να αρνηθεί ότι η υπογραφή είναι δικιά του. Ο υπογράφοντας μπορεί φυσικά να αρνηθεί να συμμετάσχει στο πρωτόκολλο, αλλά η ιδέα είναι ότι ο νόμιμος λήπτης της υπογραφής θα μπορέσει να καταφύγει για παράδειγμα στο δικαστήριο, το οποίο θα αναγκάσει τον υπογράφοντα να προσπαθήσει να αποκηρύξει την υπογραφή. Άρνηση του να συμμετάσχει στο πρωτόκολλο σε αυτή τη περίπτωση μπορεί να θεωρηθεί ως απόδειξη ότι η υπογραφή είναι όντως δικιά του.

Με αυτές τις υπογραφές, η εταιρεία λογισμικού μπορεί να υπογράφει το λογισμικό της, και να δέχεται να αποδείξει την εγκυρότητα του μόνο σε πελάτες που το έχουν αγοράσει. Έτσι ένας πειρατής που προσπαθεί να μεταπουλήσει το λογισμικό, δε μπορεί να αποδείξει στους πελάτες τους ότι το λογισμικό είναι γνήσιο. Ένας κανονικός πελάτης όμως, μπορεί σε περίπτωση που το λογισμικό είναι ελαττωματικό, να αποδείξει ότι είναι κάτοχος γνήσιου λογισμικού.

Μοντέλο

Ένα σχήμα αδιαμφισβήτητων υπογραφών αποτελείται από τους ακόλουθους αλγόριθμους και πρωτόκολλα (KGen, Sign, Conf, Dvow):

- *Δημιουργία κλειδιών*: Δημιουργεί ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού.
  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$

- *Υπογραφή*: Με είσοδο ένα ιδιωτικό κλειδί και ένα μήνυμα, επιστρέφει μια υπογραφή.
  $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathtt{m})$

- *Επιβεβαίωση*: Διαλογικό πρωτόκολλο μεταξύ του υπογράφοντα S και ενός επαληθευτή $\mathcal{V}$ όπου, με είσοδο μια υπογραφή και ένα μήνυμα, ο υπογράφοντας αποδεικνύει ότι η υπογραφή είναι έγκυρη.

- *Αποκήρυξη*: Διαλογικό πρωτόκολλο μεταξύ του υπογράφοντα S και ενός επαληθευτή $\mathcal{V}$ όπου, με είσοδο μια υπογραφή και ένα μήνυμα, ο υπογράφοντας αποδεικνύει ότι η υπογραφή είναι μη-έγκυρη.

Τα πρωτόκολλα επιβεβαίωσης και αποκήρυξης, σε κάποια σχήματα είναι ένα μόνο πρωτόκολλο, το οποίο αποφαίνεται αν μια υπογραφή είναι έγκυρη ή όχι, και το αποδεικνύει.

Σχήμα Αδιαμφισβήτητων Υπογραφών Chaum

Ως παράδειγμα ενός σχήματος αδιαμφισβήτητων υπογραφών, θα δούμε αυτό του Chaum[23], ή για την ακρίβεια στη παραλλαγή του [56], που χρησιμοποιεί κρυπτογραφικές συναρτήσεις σύνοψης(Γ'). Το πρωτόκολλο αποκήρυξης χρησιμοποιεί το σχήμα δέσμευσης των [17].

Έστω ομάδα $\mathbb{G}$ τάξης πρώτου q και γεννήτορας της g, όπου υποθέτουμε ότι ισχύει η υπόθεση DDH, καθώς και μια κρυπτογραφική συνάρτηση σύνοψης H, με $\mathsf{H} : \{0,1\}^* \to \mathbb{G}$.

Δημιουργία Κλειδιών $\mathsf{KGen}(1^\lambda)$

1 : $x \leftarrow\$ \mathbb{Z}_q$
2 : $y \leftarrow g^x$
3 : $\mathsf{sk} \leftarrow x$, $\mathsf{pk} \leftarrow y$

Επιβεβαίωση $\mathsf{Conf}_{\mathsf{S}\leftrightarrow\mathcal{V}}(\sigma, \mathtt{m})$

	$\mathcal{V}$		S
1 :	$a, b \leftarrow\$ \mathbb{Z}_q$		
2 :	$c \leftarrow g^a \mathsf{H}(\mathtt{m})^b$	$\xrightarrow{c}$	
3 :			$r \leftarrow\$ \mathbb{Z}_q$
4 :			$z_1 \leftarrow cg^r$
5 :		$\xleftarrow{z_1, z_2}$	$z_2 \leftarrow z_1^x$
6 :		$\xrightarrow{a, b}$	
7 :		$\xleftarrow{r}$	Αν $c = g^a \mathsf{H}(\mathtt{m})^b$
8 :	Αν $z_1 = g^{a+r}\mathsf{H}(\mathtt{m})^b$ ΚΑΙ $z_2 = y^{a+r}\mathsf{H}(\mathtt{m})^b$ επέστρεψε 1		

Υπογραφή $\mathsf{Sign}(x, \mathtt{m})$

1 : $\sigma \leftarrow \mathsf{H}(\mathtt{m})^x$

Αποκήρυξη $\mathsf{Dvow}_{\mathsf{S}\leftrightarrow\mathcal{V}}(\sigma, \mathtt{m})$

	$\mathcal{V}$		S
1 :	$s \leftarrow\$ \{1, \ldots, \lambda\}$		
2 :	$a \leftarrow\$ \mathbb{Z}_q$		
3 :	$c \leftarrow g^a \mathsf{H}(\mathtt{m})^s$		
4 :	$c' \leftarrow y^a \sigma^s$		
5 :		βρίσκει s' τ.ω. $cc'^{-1} = (\mathsf{H}(\mathtt{m})^x \sigma^{-1})^{s'}$	
6 :		$\xleftarrow{commit(s')}$	
7 :		$\xrightarrow{a}$	
8 :		$\xleftarrow{decommit(s')}$	Αν $c = g^a \mathsf{H}(\mathtt{m})^{s'}$
9 :	Αν $s = s'$	επέστρεψε 1	

Σημείωση 4.1. *Τα πρωτόκολλα επιβεβαίωσης και αποκήρυξης ουσιαστικά αποδεικνύουν σε μηδενική γνώση ότι η τριάδα* $(y, \mathsf{H}(\mathtt{m}), \sigma)$, *είναι, ή αντίστοιχα δεν είναι, τριάδα Diffie-Hellman.*

Σημείωση 4.2. *Το πρωτόκολλο αποκήρυξης δεν είναι πολύ αποδοτικό. Ο* S *προσπαθεί ουσιαστικά να βρει τη τιμή* s *που έχει διαλέξει τυχαία η* $\mathcal{V}$*. Δεσμεύεται στη μαντεψιά του, και αφού βεβαιωθεί ότι η* $\mathcal{V}$ *έχει υπολογίσει τίμια τη τιμή* c*, αποκαλύπτει ότι βρήκε το* s*. Η ιδέα είναι ότι ο* S *δε μπορεί παρά να μαντέψει τυχαία το* s *αν η υπογραφή* σ *είναι έγκυρη, άρα δε μπορεί να αποκηρύξει έγκυρες υπογραφές παρά με πιθανότητα* λ^{-1}*. Αυτό γιατί για έγκυρες υπογραφές* $c^x c'^{-1} = 1$*.*

Ιδιότητες Ασφάλειας

Υπάρχουν πολλές ιδιότητες που θα θέλαμε να ικανοποιεί μια αδιαμφισβήτητη υπογραφή, πέρα από την μη-πλαστογραφησιμότητα(unforgeability που έχουμε στις ψηφιακές υπογραφές. Στην αρχική δουλειά των Chaum και Antwerpen, δεν παρουσιάστηκε μοντέλο ασφάλειας. Ένα χρόνο αργότερα[19], εμφανίστηκε ένα σχήμα στο οποίο πρωτόκολλα επιβεβαίωσης και αποκήρυξης είναι μηδενικής γνώσης(Γ′). Η ιδέα είναι να μη μπορεί ένας κακόβουλος επιβεβαιωτής να πείσει κάποιον τρίτο για την γνησιότητα μια υπογραφής από τα πρακτικά της επικοινωνίας του με τον υπογράφοντα. Η βασικότερη ιδιότητα ασφάλειας είναι ίσως η αορατότητα(invisibility)[16, 19], σύμφωνα με την οποία, κανείς δε πρέπει να μπορεί να ξεχωρίσει με μη αμελητέο πλεονέκτημα αν μια υπογραφή είναι έγκυρη ή όχι, χωρίς τη βοήθεια του υπογράφοντα. Η ιδιότητα της ανωνυμίας(anonymity)[36], λέει ότι δοσμένης μιας έγκυρης υπογραφής και τα δημόσια κλειδιά δύο πιθανών υπογραφόντων, δε μπορεί να ξεχωρίσει την πραγματική προέλευση της. Στην ίδια δουλειά, η ανωνυμία αποδείχθηκε ισοδύναμη με την αορατότητα.

Τέλος αναφέρουμε μια παραλλαγή, που επιτρέπει στον υπογράφοντα να μετατρέπει τις αδιαμφισβήτητες υπογραφές του σε κοινές ψηφιακές υπογραφές, όταν το επιθυμεί. Η παραλλαγή αυτή ονομάζεται Μετατρέψιμες Αδιαμφισβήτητες Υπογραφές(Convertible Undeniable Signatures)[16]. Οι ιδιότητες ασφάλειας τους είναι παρόμοιες.

Παραλείπουμε τους τυπικούς ορισμούς, καθώς η αδιαμφισβήτητες υπογραφές δεν είναι το κύριο αντικείμενο αυτής της εργασίας, αφού κάποιες αδυναμίες [30, 41] τις καθιστούν ακατάλληλες για πολλές εφαρμογές. Ένα βασικό πρόβλημα είναι ότι ακόμα και αν τα πρωτόκολλα επιβεβαίωσης/αποκήρυξης είναι μηδενικής γνώσης, ένα κακόβουλος επαληθευτής μπορεί να ξεκινήσει το διαλογικό πρωτόκολλο με τον υπογράφοντα, ενώ ταυτόχρονα συνομιλεί με έναν ή περισσότερους συνεπαληθευτές. Χρησιμοποιώντας τεχνικές ασφαλούς υπολογισμού πολλών μερών(Secure Multi-Party Computation), μπορούν να πεισθούν όλοι ταυτόχρονα χωρίς να απαιτείτε να έχουν εμπιστοσύνη στον επαληθευτή. Κατά μία έννοια η αδιαμφισβήτητη υπογραφή δε περιορίζει πραγματικά το ποιος μπορεί να πεισθεί από μια υπογραφή, αλλά το πότε.

Ασφάλεια σχήματος υπογραφών Chaum

Όσων αφορά την ασφάλεια των αδιαμφισβήτητων υπογραφών Chaum με κρυπτογραφική συνάρτηση σύνοψης, έχουν αποδειχθεί τα παρακάτω θεωρήματα[56]:

Θεώρημα 4.1. *(Μη-Πλαστογραφήσιμη) Η υπογραφή Chaum είναι μη-πλαστογραφήσιμη στο μοντέλο $\mathcal{RO}$ αν και μόνο αν ισχύει η υπόθεση DDH.*

Θεώρημα 4.2. *(Αόρατη) Η υπογραφή Chaum είναι αόρατη αν ισχύει η υπόθεση CDH.*

4.2 Υπογραφές Καθορισμένου Επιβεβαιωτή

Οι Υπογραφές Καθορισμένου Επιβεβαιωτή (DCS)[20] είναι ένα είδος υπογραφής που μοιάζει αρκετά με τις αδιαμφισβήτητες υπογραφές. Εισάγεται μια τρίτη οντότητα, ο επιβεβαιωτής C, ο οποίος μπορεί, στη θέση του υπογράφοντα, να αποδεικνύει την εγκυρότητα ή μη, της υπογραφής. Αυτό μπορεί να είναι χρήσιμο σε περίπτωση που ο υπογράφοντας δεν είναι διαθέσιμος, ή αρνείται να συνεργαστεί.

Όταν λοιπόν κάποιος υπογράφει με μια υπογραφή καθορισμένου επιβεβαιωτή, εκτός από το ιδιωτικό του κλειδί, χρησιμοποιεί και το δημόσιο κλειδί του επιβεβαιωτή. Κάποιος που θέλει να επαληθεύσει την υπογραφή, μπορεί να ξεκινήσει το διαλογικό πρωτόκολλο επιβεβαίωσης με τον επιβεβαιωτή, αντί με τον υπογράφοντα. Επιπλέον, όπως στις Μετατρέψιμες Αδιαμφισβήτητες Υπογραφές, ο επιβεβαιωτής μπορεί να μετατρέψει όποια υπογραφή επιλέξει σε μια κοινή ψηφιακή υπογραφή.

Σε κάποια από τα πρώτα σχήματα [57], ο υπογράφοντας μπορούσε, εκ προθέσεως, να επιβεβαιώνει και να αποκηρύσσει τις υπογραφές του, και απλά ο επιβεβαιωτής μπορούσε να κάνει το ίδιο. Αργότερα [18], οι Camenisch και Michels επεσήμαναν ένα μειονέκτημα αυτής της προσέγγισης: ένας ενεργός αντίπαλος μπορεί να αναγκάσει τον υπογράφοντα να του αποδείξει αν του ανήκει μια υπογραφή. Αυτό βγάζει νόημα αν σκεφτούμε ότι σε μια τυπική εφαρμογή, ο υπογράφοντας μπορεί να είναι ένας απλός χρήστης, ενώ ο επιβεβαιωτής μια έμπιστη αρχή που δύσκολα θα υπέκυπτε σε εκβιασμό.

Μοντέλο

Ένα σχήμα υπογραφών καθορισμένου επιβεβαιωτή αποτελείτε από τους ακόλουθους αλγόριθμους και πρωτόκολλα (KGen, Sign, Conf, Dvow, Conv, Vrfy):

- *Δημιουργία Κλειδιών*: Δημιουργεί ένα ζεύγος δημοσίου ιδιωτικού κλειδιού. Και ο υπογράφοντας και ο επιβεβαιωτής απαιτείται να έχουν από ένα ζεύγος κλειδιών.
  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$

- *Υπογραφή*: Με είσοδο το ιδιωτικό κλειδί του υπογράφοντα sk_S, ένα μήνυμα και το δημόσιο κλειδί του επιβεβαιωτή pk_C επιστρέφει μια υπογραφή.
  $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_S, \mathsf{pk}_C, \mathtt{m})$

- *Επιβεβαίωση*: Διαλογικό πρωτόκολλο μεταξύ του επιβεβαιωτή C και ενός επαληθευτή $\mathcal{V}$ όπου, με είσοδο μια υπογραφή, ένα δημόσιο κλειδί υπογράφοντα pk_S και ένα μήνυμα, ο επιβεβαιωτής αποδεικνύει ότι η υπογραφή είναι έγκυρη, δηλαδή προέρχεται από τον S.

- *Αποκήρυξη*: Διαλογικό πρωτόκολλο μεταξύ του επιβεβαιωτή C και ενός επαληθευτή $\mathcal{V}$ όπου, με είσοδο μια υπογραφή, ένα δημόσιο κλειδί υπογράφοντα pk_S και ένα μήνυμα, ο επιβεβαιωτής αποδεικνύει ότι η υπογραφή δεν είναι έγκυρη, δηλαδή δεν προέρχεται από τον S.

- *Μετατροπή*: Με είσοδο μια υπογραφή σ, ένα μήνυμα, το δημόσιο κλειδί του υπογράφοντα pk_S και το ζεύγος κλειδιών του επιβεβαιωτή $\mathsf{sk}_C, \mathsf{pk}_C$, και επιστρέφει μια δημοσίως επαληθεύσιμη υπογραφή s.
  $s \leftarrow \mathsf{Conv}(\sigma, \mathsf{pk}_S, \mathsf{sk}_c, \mathsf{pk}_c)$

- *Επαλήθευση*: Με είσοδο μια μετατρεμμένη υπογραφή s, το μήνυμα και το δημόσιο κλειδί του υπογράφοντα pk_S, επιστρέφει αν η υπογραφή είναι έγκυρη ή όχι.
  $\{0, 1\} \leftarrow \mathsf{Vrfy}(s, \mathsf{pk}_S, \mathtt{m})$

Όπως και στις αδιαμφισβήτητες υπογραφές, τα πρωτοκολλά επιβεβαίωσης και αποκήρυξης μπορούν να αντικατασταθούν από ένα μόνο πρωτόκολλο που κάνει τη δουλειά και των δύο.

Παρότι εδώ στο μοντέλο αναφέρουμε τον αλγόριθμο δημιουργία κλειδιών ως ένα αλγόριθμο, σημειώνουμε ότι μπορεί κάλλιστα ο αλγόριθμος για τα κλειδιά του υπογράφοντα και το επιβεβαιωτή να είναι διαφορετικός[18].

Σχήμα Camenisch-Michels

Δε θα παρουσιάσουμε αναλυτικά κάποιο σχήμα υπογραφών επιβεβαιωμένου επιβεβαιωτή, καθώς από όσο γνωρίζουμε, κανένα από τα σχήματα που έχουν αποδειχθεί ασφαλή δε μπορεί να παρουσιασθεί χωρίς προαπαιτούμενες γνώσεις που ξεφεύγουν από αυτές που έχουμε παρουσιάσει σε αυτή τη ΔΕ. Για τον αναγνώστη που ενδιαφέρεται προτείνουμε το σχήμα των Camenisch και Michels[18], το οποίο χρησιμοποιεί το κρυπτοσύστημα Cramer-Shoup[28] και παράλληλες αποδείξεις μηδενικής γνώσης[29].

Ιδιότητες Ασφάλειας

Σε αυτήν την υποενότητα θα εξηγήσουμε την διαίσθηση πίσω από τις απαιτήσεις ασφαλείας για τις υπογραφές καθορισμένου επιβεβαιωτή. Θα παραλείψουμε τους τυπικούς ορισμούς, καθώς οι υπογραφές αυτές δεν είναι άμεσα αντικείμενο της ΔΕ.

Πρώτον είναι εύλογο να απαιτήσουμε οι υπογραφές να είναι μη-πλαστογραφήσιμες ενάντια σε έναν προσαρμοστικό αντίπαλο. Πρέπει δηλαδή, κανείς να μη μπορεί να παράγει μια υπογραφή που να φαίνεται ως έγκυρη, χωρίς να έχει γνώση του ιδιωτικού κλειδιού του υπογράφοντα. Ούτε ο επιβεβαιωτής, σε περίπτωση που είναι κακόβουλος, θα πρέπει να μπορεί να πείσει κάποιον μέσω του πρωτοκόλλου επιβεβαίωσης ότι μια υπογραφή είναι γνήσια, χωρίς να είναι, αλλά ούτε και να μπορεί να πείσει κάποιον ότι μια υπογραφή s είναι γνήσια μετατροπή μια υπογραφής του S, ενώ αυτό δεν είναι αλήθεια.

Δεύτερον, πρέπει να υπάρχει και εδώ η ιδιότητα της αορατότητας, δηλαδή κανείς εκτός από τον επιβεβαιωτή να μη μπορεί να ξεχωρίσει αν μια υπογραφή είναι έγκυρη ή όχι. Μπορούμε να απαιτήσουμε ότι, ακόμα και αν ο αντίπαλος με κάποιο τρόπο ανακαλύψει το κλειδί του υπογράφοντα, να μη μπορεί να ξεχωρίσει χωρίς τη βοήθεια του επιβεβαιωτή αν μια υπογραφή είναι γνήσια ή όχι. Φυσικά ο υπογράφοντας πάντα μπορεί να αποδείξει ότι μια υπογραφή είναι δικιά του, αφού μπορεί να δώσει όλα τα τυχαία bit που χρησιμοποίησε κατά την κατασκευή της, αλλά αν δε επιθυμεί να το κάνει, μπορεί εύλογα να ισχυριστεί ότι η υπογραφή δεν είναι δικιά του, χωρίς να μπορεί κάποιος να τον αναγκάσει να το αποδείξει. Μόνο με τη συμμετοχή του επιβεβαιωτή, είτε με το διαλογικό πρωτόκολλο επιβεβαίωσης, είτε με τον αλγόριθμο μετατροπής μπορεί κάποιος να πειστεί ότι η υπογραφή είναι έγκυρη.

Τέλος απαιτείται τα πρωτόκολλα επιβεβαίωσης και αποκήρυξης να είναι μηδενικής γνώσης, δηλαδή να μην δίνουν καμία επιπλέον πληροφορία πέρα από το αν η υπογραφή είναι έγκυρη ή όχι. Πολλές φορές στη βιβλιογραφία αυτή η ιδιότητα καλείτε και μη-μεταφερσιμότητα(non-transferability), αφού κατά κάποιο τρόπο προσπαθεί να εξασφαλίσει ότι τα πρακτικά των πρωτοκόλλων δε μπορούν να μεταβιβαστούν και να πείσουν κανέναν πέρα από τους συμμετέχοντες τους. Μια επιπλέον ιδιότητα που απαιτείτε από κάποιους είναι αυτή της ανωνυμίας, δηλαδή ένας αντίπαλος δε πρέπει να μπορεί να ξεχωρίσει, δοσμένης μιας έγκυρης υπογραφής, ποιο είναι το δημόσιο κλειδί του υπογράφοντα. Για πιο λεπτομερή ανάλυση των ιδιοτήτων ασφαλείας προτρέπουμε τον αναγνώστη να συμβουλευτεί τη βιβλιογραφία [2, 18, 74].

Δυστυχώς οι υπογραφές καθορισμένου επιβεβαιωτή, κληρονομούν το βασικό πρόβλημα των αδιαμφισβήτητων υπογραφών(4.1), δηλαδή ο επιβεβαιωτής δε μπορεί ποτέ να είναι σίγουρος όταν αποδεικνύει την εγκυρότητα μια υπογραφής, σε πόσους πραγματικά το αποδεικνύει. Ένα επιπλέον μειονέκτημα αυτόν τον υπογραφών, είναι ότι πρέπει να υποθέσουμε ότι ο επιβεβαιωτής είναι τουλάχιστον μερικώς εμπιστεύσιμος. Στη πράξη θα πρέπει να ακολουθεί κάποια πολιτική για το σε ποιους επαληθευτές θα αποδεικνύει την γνησιότητα υπογραφών, και πότε θα πρέπει να μετατρέψει μια υπογραφή σε δημόσια επαληθεύσιμη. Για αυτό το λόγο περιορίζονται πολύ οι εφαρμογές στο οποίο οι υπογραφές αυτές είναι χρήσιμες.

4.3 Υπογραφές Καθορισμένου Επαληθευτή(DVS)

Το 1996, οι Jakobsson, Sako και Impagliazzo, σκέφτηκαν έναν ιδιοφυές τρόπο να κατασκευάσουν υπογραφές που μπορούν να πείσουν πραγματικά μόνο τον παραλήπτη που επιθυμεί ο υπογράφοντας[42]. Οι αδιαμφισβήτητες υπογραφές που είδαμε σε προηγούμενη ενότητα, ενώ έχουν παρόμοιο στόχο, όπως είδαμε έχουν μια σημαντική αδυναμία: δεν περιορίζουν πραγματικά το ποιον θα πείσει η υπογραφή, αλλά το πότε(4.1).

Η ιδέα τους ήταν η εξής: Έστω ότι ο S θέλει να υπογράψει το μήνυμα m έτσι ώστε να μπορεί να πειστεί από αυτή την υπογραφή μόνο η $\mathcal{V}$. Αυτό που μπορεί να

κάνει είναι να κατασκευάσει μια (μη-διαλογική) απόδειξη μηδενικής γνώσης(Γ'), της πρότασης ¨Είμαι ο S και υπογράφω το m Ή Είμαι η $\mathcal{V}$¨. Η $\mathcal{V}$ βλέποντας αυτή την απόδειξη, ξέρει ότι είναι μια γνήσια υπογραφή του S, καθώς η ίδια γνωρίζει ότι δε μπορεί να ισχύει το κομμάτι της πρότασης ¨είμαι η $\mathcal{V}$¨. Οποιασδήποτε άλλος όμως δει αυτή την υπογραφή, δεν έχει τρόπο να ξεχωρίσει αν προέρχεται από τον S ή τη $\mathcal{V}$. Ο μόνος λόγος που η $\mathcal{V}$ μπορεί να πειστεί από την υπογραφή, είναι επειδή η ίδια ξέρει ότι ποτέ δε κατασκεύασε αυτήν την συγκεκριμένη υπογραφή, άρα αναγκαστικά είναι του S.

Ένας άλλος τρόπος να σκεφτούμε την ιδέα είναι ο εξής. Πέρα από τον αλγόριθμο υπογραφής Sign που έχει στη διάθεση του ο υπογράφοντας, έχουμε και έναν αλγόριθμο προσομοίωσης Sim, τον οποίο μπορεί να χρησιμοποιεί ο καθορισμένος επαληθευτής για να παράγει υπογραφές που είναι πανομοιότυπες με τις πραγματικές.

Μια εφαρμογή αυτών των υπογραφών αφορά τις ηλεκτρονικές ψηφοφορίες. Έστω ότι ένας ψηφοφόρος θέλει μια απόδειξη ότι η ψήφος του καταμετρήθηκε σωστά. Ένα πρόβλημα που μπορεί να παρουσιαστεί είναι ότι μπορεί να χρησιμοποιήσει αυτήν την απόδειξη για να πουλήσει την ψήφο του. Αν όμως η απόδειξη είναι μια υπογραφή καθορισμένου επαληθευτή, ο ψηφοφόρος θα πειστεί για ότι η ψήφος του καταμετρήθηκε σωστά, αλλά δε θα μπορεί να πείσει κανέναν άλλο.

4.3.1 Μοντέλο DVS

Τυπικά ένα σχήμα υπογραφών καθορισμένου επαληθευτή(DVS), είναι μια τετράδα αλγορίθμων (KGen, Sign, Sim, Vrfy):

- *Δημιουργία κλειδιών:* Δημιουργεί ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού. Και ο υπογράφοντας και ο επαληθευτής απαιτείται να έχουν από ένα ζεύγος κλειδιών.
  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$

- *Υπογραφή:* Με είσοδο το ιδιωτικό κλειδί του υπογράφοντα sk_S, ένα μήνυμα m και το δημόσιο κλειδί του επιβεβαιωτή pk_D επιστρέφει μια υπογραφή.
  $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_S, \mathsf{pk}_D, \mathtt{m})$

- *Προσομοίωση:* Με είσοδο το ιδιωτικό κλειδί του επαληθευτήsk_D, το δημόσιο κλειδί του υπογράφονταsk_S και το ένα μήνυμα m επιστρέφει μια υπογραφή.
  $\sigma \leftarrow \mathtt{Sim}(\mathsf{sk}_D, \mathsf{pk}_S, \mathtt{m})$

- *Επαλήθεση:* Με είσοδο μια υπογραφή σ, το μήνυμα m και τα δημόσια κλειδιά του υπογράφοντα και του επαληθευτή, επιστρέφει αν η υπογραφή είναι έγκυρη ή όχι.
  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\sigma, \mathsf{pk}_S, \mathsf{pk}_D, \mathtt{m}))$

Σημειώνουμε ότι φυσικά δεν είναι υποχρεωτικό ο αλγόριθμος δημιουργίας κλειδιών να είναι κοινός για τον υπογράφοντα και τον επαληθευτή.

Ο αλγόριθμος επαλήθευσης απαιτούμε να απαντάει ναι, τόσο για τις εξόδους του αλγορίθμου υπογραφής όσο και για τις εξόδους του αλγορίθμου προσομοίωσης. Μια προσομοίωση δεν αποτελεί πλαστογραφία, αφού είναι κάτι που επιτρέπουμε εκ του σχεδιασμού. Θα δούμε στην επόμενη υποενότητα πως αυτό απαιτείται για να είναι η υπογραφή μη-μεταφέρσιμη. Πράγματι, κάποιοι συγγραφείς(πχ. [68, 52]), δεν θεωρούν τον αλγόριθμο προσομοίωσης μέρος του μοντέλου, αλλά απαιτούν την ύπαρξη του ως ιδιότητα ασφάλειας.

4.3.2 Σχήμα JSI

Θα παρουσιάσουμε το σχήμα που πρότειναν οι Jakobsson, Sako και Impagliazzo[42]. Η ιδέα του σχήματος είναι να τροποποιηθεί το σχήμα αδιαμφισβήτητων υπογραφών του Chaum(4.1), χρησιμοποιώντας σχήμα δέσμευσης με καταπακτή(trapdoor commitment scheme)[17] για να έχει τη δυνατότητα ο επαληθευτής να προσομοιώνει και κάνοντας το πρωτόκολλο μη-διαλογικό με την μέθοδο Fiat-Shamir[34] (βλ. και Γ′).

Έστω ομάδα $\mathbb{G}$ τάξης πρώτου q όπου υποθέτουμε ότι ισχύει η υπόθεση DDH και γεννήτορας της g. Υποθέτουμε και μια κρυπτογραφική συνάρτηση σύνοψης $\mathsf{H}_q : \{0,1\}^* \to \mathbb{Z}_q$

Δημιουργία Κλειδιών $\mathsf{KGen}(1^\lambda)$	*Επαλήθευση* $\mathsf{Vrfy}(\sigma, y_S, y_D, \mathtt{m})$
$x \leftarrow\$ \mathbb{Z}_q$	$c \leftarrow g^w y_D^r$
$y \leftarrow g^x$	$h \leftarrow \mathsf{H}_q(c, G, M)$
$\mathsf{sk} \leftarrow x$, $\mathsf{pk} \leftarrow y$	Αν $G y_S^{h+w} = g^d$ ΚΑΙ $M s^{h+w} = m^d$ επέστρεψε 1
Υπογραφή $\mathsf{Sign}(x_S, y_D.\mathtt{m})$	*Προσομοίωση* $\mathtt{Sim}(x_D, y_S, \mathtt{m})$
$s \leftarrow \mathtt{m}^{x_S}$	$s \leftarrow\$ \mathbb{G}$
$w, r, t \leftarrow\$ \mathbb{Z}_q$	$d, a, \beta \leftarrow\$ \mathbb{Z}_q$
$c \leftarrow g^w y_D^r$	$c \leftarrow g^a$
$G \leftarrow g^t$	$G \leftarrow g^d y_S^{-\beta}$
$M \leftarrow m^t$	$M \leftarrow \mathtt{m}^d s^{-\beta}$
$h \leftarrow \mathsf{H}_q(c, G, M)$	$h \leftarrow \mathsf{H}_q(c, G, M)$
$d \leftarrow t + x_S(h + w)$	$w \leftarrow \beta - h$
$\sigma \leftarrow (s, w, r, G, M, d)$	$r \leftarrow (a - w)x_D^{-1}$
	$\sigma \leftarrow (s, w, r, G, M, d))$

Είναι εύκολο να δούμε ότι ο αλγόριθμος επαλήθευσης είναι ορθός, δηλαδή ότι μια τίμια κατασκευασμένη υπογραφή και μια τίμια κατασκευασμένη προσομοίωση, επαληθεύονται.

Λήμμα 4.1. *Μια τίμια κατασκευασμένη υπογραφή σ επαληθεύεται ορθά.*

Απόδειξη.

$$G y_S^{h+w} = g^t g^{x_S(h+w)} = g^{t+x_S(h+w)} = g^d$$

$$Ms^{h+w} = \mathfrak{m}^t \mathfrak{m}^{x_S(h+w)=\mathfrak{m}^{t+x_S(h+w)}} = \mathfrak{m}^d$$

□

Λήμμα 4.2. *Μια τίμια κατασκευασμένη προσομοίωση σ επαληθεύεται ορθά.*

Απόδειξη.

$$Gy_S^{h+w} = g^d y_S^{-\beta} g^{x_S(h+w)} = g^{d-x_S\beta+x_S(h+\beta-h)} = g^d$$
$$Ms^{h+w} = \mathfrak{m}^d s^{-\beta} s^{h+w} = \mathfrak{m}^d s^{-\beta+h+\beta-h} = m^d$$

□

Αφού ορίσουμε τις ιδιότητες ασφάλειας για ένα σχήμα DVS, θα αναλύσουμε περαιτέρω την ασφάλεια του σχήματος JSI(4.3.3).

4.3.3 Ιδιότητες Ασφάλειας

Όπως σε όλες τις υπογραφές, απαιτούμε μια DVS να είναι μη-πλαστογραφήσιμη. Η διαφορά εδώ είναι ότι επιτρέπουμε στον καθορισμένο επαληθευτή να παράγει έγκυρες υπογραφές, οπότε ο ορισμός τροποποιείται ώστε να απαιτεί κανείς να μη μπορεί να παράγει έγκυρες υπογραφές εκτός από τον υπογράφοντα και τον καθορισμένο επαληθευτή.

Η δεύτερη ιδιότητα που απαιτούμε είναι η υπογραφή να είναι μη-μεταφέρσιμη. Αυτό επιτυγχάνεται κάνοντας υπογραφές και προσομοιώσεις μη-διακρίσιμες. Εδώ διακρίνουμε δύο περιπτώσεις, αν οι πιθανοί έξοδοι των υπογραφών και των προσομοιώσεων ακολουθούν ακριβώς την ίδια κατανομή, τότε λέμε ότι η υπογραφή είναι *τέλεια* μη-διακρίσιμη. Αν το πρόβλημα του να διακρίνεις μια υπογραφή από μια προσομοίωση είναι απλά δύσκολο, τότε λέμε ότι η υπογραφή είναι *υπολογιστικά* μη-διακρίσιμη.

Μια επιπλέον ιδιότητα είναι η υπογραφή να είναι μη-εξουσιοδοτήσιμη[47]. Πρακτικά αυτό σημαίνει ότι απαιτούμε να μη μπορεί είτε ο υπογράφοντας, είτε ο καθορισμένος επαληθευτής, να παραχωρήσει σε κάποιον τρίτο το δικαίωμα να υπογράφει ή να προσομοιώνει με το αντίστοιχο δημόσιο κλειδί, χωρίς να αποκαλύψει το ιδιωτικό του κλειδί. Αυτή η περίπτωση δε καλύπτεται από τους συνηθισμένους ορισμούς για τη μη-πλαστογραφησιμότητα, αφού απαιτεί την συνεργασία μιας οντότητας που έχει όντως δικαίωμα να παράγει αυτές τις υπογραφές. Σε αυτή τη ΔΕ δε θα εστιάσουμε σε αυτή την ιδιότητα. Θα αρκεστούμε στο να πούμε ότι, όπως αναφέρεται και στο [47], αρκεί κανείς να δείξει ότι η υπογραφή αποτελεί απόδειξη γνώσεις του κλειδιού του υπογράφοντα Ή του κλειδιού του καθορισμένου επαληθευτή. Οπότε αν η απόδειξη ότι η υπογραφή είναι μη-πλαστογραφήσιμη ανάγεται σε απόδειξη γνώσης των κλειδιών, έπεται και ότι η υπογραφή είναι μη-εξουσιοδοτήσιμη.

Παρακάτω δίνουμε τυπικούς ορισμούς για τις ιδιότητες μέσω παιχνιδιών στα οποία ένας αντίπαλος $\mathcal{A}$ προσπαθεί να παραβιάσει τις ιδιότητες. Τη δυνατότητα του αντιπάλου να ζητά υπογραφές και προσομοιώσεις της επιλογής του, τις μοντελοποιούμε με τα μαντεία $\mathcal{SO}$ και $\mathcal{MO}$ αντίστοιχα. Την συνάρτηση σύνοψης H_q, την μοντελοποιούμε με το τυχαίο μαντείο $\mathcal{RO}$.

Μη-Πλαστογραφησιμότητα

Στο πείραμα μη-πλαστογραφησιμότητας, ο αντίπαλος $\mathcal{A}$ προσπαθεί να παράγει μια έγκυρη υπογραφή, χωρίς να γνωρίσει κάποιο από τα μυστικά κλειδιά. Μπορεί προσαρμοστικά να ζητάει υπογραφές και προσομοιώσεις για μηνύματα της επιλογής του. Φυσικά το να επιστρέψει την έξοδο των μαντείων ως τη προσπάθεια του για πλαστογραφία δεν έχει κανένα νόημα.

Παιχνίδι 4.1: Πείραμα Μη-Πλαστογραφησιμότητας $\mathtt{Exp}^{UnfDVS}_{\mathcal{A},\Pi}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$(\mathsf{sk}_S, \mathsf{pk}_S, \mathsf{sk}_D, \mathsf{pk}_D) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)$
$(\sigma, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{SO},\mathcal{MO}}(1^\lambda, \mathsf{pk}_D, \mathsf{pk}_S)$
Αν *σ δεν είναι έξοδος του* $\mathcal{SO}$**ΚΑΙ** *δεν είναι έξοδος του* $\mathcal{MO}$ **τότε**
  επέστρεψε $\mathsf{Vrfy}(\sigma, \mathsf{pk}_S, \mathsf{pk}_D, \mathtt{m})$
αλλιώς
  επέστρεψε $\perp$

Ορισμός 4.1. *Ένα DVS σχήμα Π είναι μη-πλαστογραφήσιμο αν για κάθε* PPT *αντίπαλο* $\mathcal{A}$*:*

$$Pr[\mathtt{Exp}^{UnfDVS}_{\mathcal{A},\Pi}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$$

Μη-Μεταφερσιμότητα

Επιλέγουμε να δώσουμε τον ορισμό της τέλειας μη-μεταφερσιμότητας. Σημειώνουμε ότι εδώ ο αντίπαλος $\mathcal{A}$ μπορεί να είναι υπολογιστικά μη φραγμένος. Για αυτό το λόγο δεν έχει νόημα να του δώσουμε πρόσβαση στα μαντεία $\mathcal{SO}, \mathcal{MO}$ αφού μπορεί απλά να αντιστρέψει κλειδιά και υπολογίσει τις εξόδους των μαντείων. Το πείραμα λειτουργεί ως εξής: ο αντίπαλος $\mathcal{A}$ διαλέγει ένα μήνυμα $\mathtt{m}$ και το σύστημα παράγει μια υπογραφή σ_0 και μια προσομοίωση σ_1 για το $\mathtt{m}$. Διαλέγει τυχαία να στείλει στον αντίπαλο ένα από τα δύο και ο αντίπαλος προσπαθεί να διακρίνει αν έλαβε την υπογραφή ή τη προσομοίωση.

Ορισμός 4.2. *Ένα DVS σχήμα Π είναι τέλεια μη-μεταφέρσιμο αν για κάθε μη φραγμένο αντίπαλο* $\mathcal{A}$*:*

$$Pr[\mathtt{Exp}^{TransDVS}_{\mathcal{A},\Pi}(\lambda) = 1] - \frac{1}{2} = 0$$

Αξίζει να κάνουμε μια σύγκριση της *τέλειας* και της *υπολογιστικής* μη-μεταφερσιμότητας. Ένα χαρακτηριστικό των DVS με *τέλεια* μη-μεταφερσιμότητα είναι ότι ο υπογράφοντας δε μπορεί να αποδείξει ότι μια υπογραφή είναι όντως δική του, ή να αποκηρύξει μια προσομοίωση του επαληθευτή. Αυτό σε μια εφαρμογή όπως ήταν αυτή της εταιρείας λογισμικού που θέλει να υπογράφει το λογισμικό της με τρόπο που να είναι επαληθεύσιμο μόνο από πελάτες δεν είναι ιδανικό. Αυτό γιατί σε περίπτωση που ο πελάτης θέλει να αποδώσει ευθύνες στην εταιρία για

Παιχνίδι 4.2: Πείραμα Μη-Μεταφερσιμότητας $\mathtt{Exp}^{TransDVS}_{\mathcal{A},\Pi}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$(\mathsf{sk}_S, \mathsf{pk}_S, \mathsf{sk}_D, \mathsf{pk}_D) \leftarrow \Pi\mathsf{KGen}(1^\lambda)$
$\mathtt{m} \leftarrow \mathcal{A}^{\mathcal{RO}}(1^\lambda, \mathsf{pk}_D, \mathsf{pk}_S)$
$\sigma_0 \leftarrow \Pi.\mathsf{Sign}(\mathsf{sk}_S, \mathsf{pk}_D, \mathtt{m})$
$\sigma_1 \leftarrow \Pi.\mathtt{Sim}(\mathsf{sk}_D, \mathsf{pk}_S, \mathtt{m})$
$b \leftarrow\$ \{0,1\}$
$b' \leftarrow \mathcal{A}^{\mathcal{RO}}(1^\lambda, \mathsf{pk}_D, \mathsf{pk}_S, \sigma_b)$
επέστρεψε $b = b'$

κάποιο καταστροφικό πρόβλημα του λογισμικού, δεν έχει στα χέρια του καμία απόδειξη ότι το λογισμικό είναι γνήσιο. Οι μόνοι που το ξέρουν είναι η εταιρεία και ο πελάτης. Αν απαιτήσουμε όμως μόνο υπολογιστική μη-μεταφερσιμότητα, αυτό μπορεί να επιτρέψει στο υπογράφοντα να αποκηρύσσει προσομοιώσεις αν το επιθυμεί. Αυτή η δυνατότητα δεν είναι φυσικά πάντα επιθυμητή, ούτε είναι απαραίτητο ότι την έχει κάθε σχήμα με υπολογιστική μη-μεταφερσιμότητα χωρίς να έχει σχεδιαστεί ώστε να υπάρχει πρωτόκολλο αποκήρυξης[47]. Η τέλεια μη-μεταφερσιμότητα έχει το πλεονέκτημα ότι διατηρείτε ακόμα και ενάντια σε έναν αντίπαλο που είναι υπολογιστικά πανίσχυρος. Αυτό έχει νόημα είτε στη περίπτωση που θέλουμε οι υπογραφές να παραμείνουν μη-μεταφέρσιμες για πάντα, είτε στη περίπτωση που ο υπογράφοντας ή ο επαληθευτής έχουν κίνητρο να αποκαλύψουν το μυστικό κλειδί τους για να ¨σπάσουν¨ τη μη-μεταφερσιμότητα. Σε αυτή τη ΔΕ εστιάζουμε στην τέλεια μη-μεταφερσιμότητα απλά γιατί είναι πιο κατάλληλη για τις εφαρμογές μας.

Ασφάλεια Υπογραφών JSI

Σχετικά με το σχήμα JSI[42], που παρουσιάσαμε στην προηγούμενη υποενότητα, αποδεικνύονται τα παρακάτω θεωρήματα[47].

Θεώρημα 4.3 (Μη-Πλαστογραφήσιμη). *Η υπογραφή JSI είναι μη-πλαστογραφήσιμη (και μη-εξουσιοδοτήσιμη) στο μοντέλο $\mathcal{RO}$ αν ισχύει η υπόθεση DDH.*

Θεώρημα 4.4 (Τέλεια Μη-Μεταφέρσιμη). *Η υπογραφή JSI είναι τέλεια μη-μεταφέρσιμη.*

Εκ πρώτης όψεως, το σχήμα JSI δε μοιάζει να είναι τέλεια μη-μεταφέρσιμο. Στον αλγόριθμο υπογραφής $s \leftarrow \mathtt{m}^{x_S}$, ενώ στον αλγόριθμο προσομοίωσης $s \leftarrow\$ \mathbb{G}$. Άρα θα μπορούσε κανείς να σκεφτεί ότι ο S μπορεί να αποκηρύξει μια προσομοιώσει αποδεικνύοντας ότι $s \neq \mathtt{m}^{x_S}$. Αυτή φαίνεται να ήταν και η αρχική πρόθεση των δημιουργών. Αποδείχθηκε όμως[47], ότι ο υπογράφοντας μπορεί να δημιουργεί έγκυρες υπογραφές με $s \neq \mathtt{m}^{x_S}$. Αυτό φυσικά δεν αποτελεί πλαστογραφία, αφού εξακολουθεί να χρειάζεται το ιδιωτικό κλειδί του υπογράφοντα ως είσοδος στον τροποποιημένο αλγόριθμο υπογραφής.

4.3.4 Υπογραφές Ισχυρά Καθορισμένου Επαληθευτή

Μια παραλλαγή των DVS είναι οι υπογραφές ισχυρά καθορισμένου επαληθευτή(strong designated verifier signatures). Αυτές προτάθηκαν στην ίδια δουλειά με τις DVS[42]. Η επιπλέον ιδιότητα τους είναι ότι οι sDVS δεν είναι δημόσια επαληθεύσιμες. Ο αλγόριθμος επαλήθευσης απαιτεί ως είσοδο του το ιδιωτικό κλειδί του επαληθευτή. Το κίνητρο για την εισαγωγή αυτής της ιδιότητας ήταν ότι σε περίπτωση που κάποιος εμπιστεύεται απόλυτα ότι ο επαληθευτής δεν χρησιμοποιεί τον αλγόριθμο προσομοίωσης, θα πειθόταν από υπογραφές του υπογράφοντα αν ήταν δημόσια επαληθεύσιμες. Ένας απλό τρόπος να δημιουργήσει κάποιος ένα σχήμα sDVS από ένα σχήμα DVS είναι να κρυπτογραφήσει την υπογραφή με το δημόσιο κλειδί του επαληθευτή με οποιοδήποτε ασφαλές κρυπτοσύστημα. Έτσι για να γίνει επαλήθευση απαιτείτε πρώτα αποκρυπτογράφηση της υπογραφής, κάτι που μπορεί να κάνει μόνο ο καθορισμένος επαληθευτής. Όσον αφορά τις απαιτήσεις ασφαλείας, δεν υπάρχει καμία διαφορά ως προς τα δύο είδη υπογραφών.

Άλλες παραλλαγές

Αναφέρουμε και δύο ακόμα παραλλαγές των DVS που συναντώνται στη βιβλιογραφία:

Οι *καθολικές* υπογραφές καθορισμένου επαληθευτή (UDVS)[68] μπορούν να δράσουν ως κοινές ψηφιακές υπογραφές, αλλά οποιοσδήποτε κάτοχος μια υπογραφής, όχι απαραίτητα ο υπογράφοντας, μπορεί να μετατρέψει σε DVS την υπογραφή καθορίζοντας ένα επαληθευτή. Ουσιαστικά δηλαδή διαχωρίζεται η υπογραφή από και ο καθορισμός σε δύο διακριτά βήματα, που μπορούν να γίνουν σε διαφορετικές στιγμές και από διαφορετικές οντότητες.

Οι υπογραφές *πολλών* καθορισμένων επαληθευτών[43], επιτρέπουν τον καθορισμό της υπογραφής από κοινού σε ένα σύνολο επαληθευτών. Οι επαληθευτές για να παράγουν μια προσομοίωση πρέπει να συνεργαστούν χρησιμοποιώντας τεχνικές ασφαλούς υπολογισμού πολλών μερών.

Οι [52] παρουσίασαν ένα ενοποιημένο μοντέλο για όλες τις παραλλαγές των DVS που έχουμε αναφέρει.

ΚΕΦΑΛΑΙΟ 5

Υπογραφές Δακτυλίου

Οι συνηθισμένες υπογραφές, εγγυούνται τη ταυτότητα του αποστολέα ενός μηνύματος. Σε ορισμένες περιπτώσεις όμως, δε μας ενδιαφέρει ποιος συγκεκριμένα είναι ο παραλήπτης, αλλά ότι ανήκει σε μια συγκεκριμένη ομάδα. Για παράδειγμα μπορεί να μας ενδιαφέρει ότι ένα μήνυμα προέρχεται από υπάλληλο μιας εταιρείας, χωρίς να μας ενδιαφέρει ποιος συγκεκριμένος υπάλληλος είναι. Ο αποστολέας μπορεί να θέλει στη πραγματικότητα να διατηρήσει την ανωνυμία του.

Οι Chaum και van Heyst πρότειναν τις ομαδικές υπογραφές (group signatures)[24]. Μόνο μέλη μιας ομάδας μπορούν να υπογράψουν και ο παραλήπτης είναι σίγουρος ότι η υπογραφή προέρχεται από μέλος της ομάδας αλλά δε μπορεί να διακρίνει ποιο μέλος της ομάδας. Υπάρχει όμως ένας αρχηγός της ομάδας, που αν χρειαστεί μπορεί να αποκαλύψει το μέλος που υπέγραψε.

Οι Rivest, Shamir και Tauman εισήγαγαν τις υπογραφές δακτυλίου (Ring Signatures)[62]. Όπως στις ομαδικές υπογραφές, μια υπογραφή δακτυλίου αποδεικνύει ότι ένα μήνυμα προέρχεται από το το μέλος μια ομάδας ή δακτυλίου όπως έχει καθιερωθεί. Αντίθετα όμως με τις ομαδικές υπογραφές, αυτό μπορεί να γίνει χωρίς τη συμμετοχή των άλλων μελών του δακτυλίου, χωρίς τη γνώση τους και χωρίς κανέναν αρχηγό που να μπορεί να άρει την ανωνυμία του υπογράφοντα.

Μια παραλλαγή των RS, οι συνδέσιμες υπογραφές δακτυλίου (linkable ring signatures) που προτάθηκαν από τους Liu, Wei και Wong[50], προσθέτει μια ενδιαφέρουσα ιδιότητα. Ο υπογράφοντας διατηρεί την ανωνυμία του ως μέλος του δακτυλίου, αλλά όλες του οι υπογραφές είναι συνδέσιμες μεταξύ τους, δηλαδή δοθέντος δύο υπογραφών οποιασδήποτε μπορεί να καταλάβει αν προέρχονται από έναν υπογράφοντα ή από δύο διαφορετικούς.

Στη ΔΕ θα επικεντρωθούμε κυρίως στις LRS, επειδή έχουν ενδιαφέρουσες εφαρμογές στις ψηφιακές ψηφοφορίες και αποτελούν έμπνευση για το καινούριο είδος υπογραφών που παρουσιάζουμε στο κεφάλαιο 6. Παρουσιάζουμε όμως και τους προκατόχους τους, τις ομαδικές υπογραφές και τις υπογραφές δακτυλίου για μια πιο σφαιρική κατανόηση του θέματος.

5.1 Ομαδικές Υπογραφές

Ως παράδειγμα χρήσης των ομαδικών υπογραφών, οι συγγραφείς που της εφηύραν παρουσίασαν το εξής[24]: Μια εταιρεία με πολλά τμήματα, έχει έναν εκτυπωτή για κάθε τμήμα, και μόνο τα μέλη του κάθε τμήματος επιτρέπεται να χρησιμοποιήσουν τον αντίστοιχο εκτυπωτή. Η εταιρεία σέβεται την ιδιωτικότητα των υπάλληλων, οπότε το όνομα του χρήστη δεν φαίνεται κάθε φορά. Αν όμως γίνει

υπερβολική χρήση του εκτυπωτή ο υπεύθυνος θα πρέπει να μπορεί να ανακαλύψει την ταυτότητα αυτού που έκανε τη κατάχρηση.

Οι ομαδικές υπογραφές είναι φτιαγμένες για αυτό το σενάριο, αφού έχουν τις εξής ιδιότητες:

1. Μόνο τα μέλη της ομάδας μπορούν να υπογράψουν.

2. Ο λήπτης της υπογραφής μπορεί να επαληθεύσει ότι η υπογραφή προέρχεται από κάποιο μέλος της ομάδας, αλλά όχι από ποιο.

3. Σε περίπτωση αντιδικίας, ο αρχηγός της ομάδας μπορεί να ¨ανοίξει¨ την υπογραφή και να αποκαλύψει τη ταυτότητα του υπογράφοντα.

Μοντέλο

Ένα σχήμα ομαδικών υπογραφών αποτελείτε από τους ακόλουθους αλγορίθμους (KGen, Sign, Vrfy, Open):

- *Δημιουργία Κλειδιών Ομάδας*: Για μέγεθος ομάδας n δημιουργεί ένα δημόσιο κλειδί ομάδας $g\mathsf{pk}$, και τα αντίστοιχα ιδιωτικά κλειδιά του αρχηγού $g\mathsf{sk}_M$ και των μελών $\{g\mathsf{sk}_i\}_{i=1}^n$
  $(g\mathsf{pk}, g\mathsf{sk}_M, \{g\mathsf{sk}_i\}_{i=1}^n) \leftarrow \mathsf{KGen}(1^\lambda, n)$

- *Υπογραφή*: Με είσοδο το ιδιωτικό κλειδί του υπογράφοντα sk_π,όπου $\pi \in [n]$, και ένα μήνυμα $\mathtt{m}$ επιστρέφει μια υπογραφή.
  $\sigma \leftarrow \mathsf{Sign}(g\mathsf{pk}, g\mathsf{sk}_\pi, \mathtt{m})$

- *Επαλήθευση*: Με είσοδο μια υπογραφή σ, το μήνυμα $\mathtt{m}$ και το δημόσιο κλειδί της ομάδας $g\mathsf{pk}$, επιστρέφει αν η υπογραφή είναι έγκυρη ή όχι.
  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\sigma, g\mathsf{pk}, \mathtt{m})$

- *΄Ανοιγμα*: Με είσοδο μια υπογραφή σ, το μήνυμα $\mathtt{m}$ και το ιδιωτικό κλειδί του αρχηγού $g\mathsf{sk}_M$ επιστρέφει τη ταυτότητα π.
  $\pi \leftarrow \mathsf{Open}(\sigma, g\mathsf{sk}_M, \mathtt{m})$

Στο μοντέλο που ακολουθούμε μια ομάδα είναι μια στατική δομή, δηλαδή δεν επιτρέπουμε μετά της δημιουργία των κλειδιών να προστεθούν ή να διαγραφούν μέλη. Σε πολλές δουλειές ακολουθείτε ένα μοντέλο δυναμικών ομάδων με τη δυνατότητα να προστίθενται μέλη(πχ.[3, 26]) ή και να διαγράφονται μέλη(πχ.[4]). Σε αυτή τη περίπτωση προκύπτουν πολλά προβλήματα, όπως για παράδειγμα το πως θα πρέπει να επαληθεύονται υπογραφές που προέρχονται από ένα διαγραμμένο πλέον μέλος. Αυτά τα ερωτήματα όμως ξεφεύγουν από τη απλή παρουσίαση στην οποία στοχεύουμε σε αυτή την ενότητα. Για μια πλήρη ανάλυση του θέματος προτείνουμε τους [11].

Σχήμα ομαδικών υπογραφών Bellare,Micciancio,Warinschi

Θα δούμε το σχήμα ομαδικών υπογραφών BMW[8] που μπορεί να κατασκευαστεί συνθέτοντας ένα κρυπτοσύστημα με ασφάλεια IND-CCA2 $(\mathsf{KGen}_e, \mathsf{Enc}, \mathsf{Dec})$, ένα σχήμα ψηφιακών υπογραφών μη-πλαστογραφίσιμο ενάντια σε επίθεση επιλεγμένου μηνύματος $(\mathsf{KGen}_s, \mathsf{Sign}_s, \mathsf{Vrfy}_s)$ και ένα μη-διαλογικό σύστημα αποδείξεων μηδενικής γνώσης (P, V) για μια σχέση ρ[1]. Σε αντίθεση με τα σχήματα που έχουμε παρουσιάσει ως τώρα, δεν ήμαστε στο μοντέλο $\mathcal{RO}$, αλλά στο μοντέλο συμβολοσειράς κοινής αναφοράς(common reference string)[13]. Οπότε υποθέτουμε ότι R είναι το CRS.

Το σύστημα (P, V) θα αποδεικνύει ότι $((\mathsf{pk}_e, \mathsf{pk}_s, \mathtt{m}, C), (i, \mathsf{pk}', c, s, r)) \in \rho$:

$$\mathsf{Vrfy}_s(\mathsf{pk}_s, c, < i, \mathsf{pk}' >) = 1 \wedge \mathsf{Vrfy}_s(\mathsf{pk}', \mathtt{m}, s) = 1 \wedge \mathsf{Enc}(\mathsf{pk}_e, < i, pk', c, s >; r) = C$$

Με r συμβολίσαμε τα τυχαία νομίσματα του αλγόριθμου κρυπτογράφησης και $< i, pk' >$ συμβολίσαμε την αναπαράσταση στο χώρο τον μηνυμάτων των i, pk' κ.ο.κ.

Δημιουργία Κλειδιών Ομάδας $\mathsf{KGen}(1^\lambda, n, R)$

1 : $(\mathsf{pk}_e, \mathsf{sk}_e) \leftarrow \mathsf{KGen}_e(1^\lambda)$
2 : $(\mathsf{pk}_s, \mathsf{sk}_s) \leftarrow \mathsf{KGen}_s(1^\lambda)$
3 : $g\mathsf{pk} \leftarrow (R, \mathsf{pk}_e, \mathsf{pk}_s)$
4 : $g\mathsf{sk}_M \leftarrow (\mathsf{pk}_e, \mathsf{sk}_e, \mathsf{pk}_s)$
5 : $i \in [n](\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KGen}_s(1^\lambda)$
6 : $c_i \leftarrow \mathsf{Sign}_s(\mathsf{sk}_s, < i, \mathsf{pk}_i >)$
7 : $g\mathsf{sk}_i \leftarrow (\{i, \mathsf{pk}_i, \mathsf{sk}_i, c_i\}_{i=0}^n)$
8 : Επέστρεψε $(g\mathsf{pk}, \mathsf{sk}_M, \{\mathsf{sk}_i)\}_{i=1}^n$

Επαλήθευση $\mathsf{Vrfy}(\sigma, g\mathsf{pk}, \mathtt{m})$

1 : Επέστρεψε $V((\mathsf{pk}_e, \mathsf{pk}_s, \mathtt{m}, C), p)$

Υπογραφή $\mathsf{Sign}(g\mathsf{pk}, g\mathsf{sk}_\pi, \mathtt{m})$

1 : $s \leftarrow \mathsf{Sign}_s(\mathsf{sk}_\pi, \mathtt{m})$
2 : $C \leftarrow \mathsf{Enc}(\mathsf{pk}_e, < \pi, \mathsf{pk}_\pi, c_\pi, s >; r)$
3 : $p \leftarrow P((\mathsf{pk}_s, c, \mathtt{m}, C), (\pi, \mathsf{pk}', c, s, r))$
4 : $\sigma \leftarrow (C, p)$
5 : Επέστρεψε σ

΄Ανοιγμα $\mathsf{Open}(\sigma, g\mathsf{sk}_M, \mathtt{m})$

1 : Αν $\mathsf{Vrfy}(\sigma, g\mathsf{pk}, \mathtt{m}) = 0$ επέστρεψε $\perp$
2 : $< i, \mathsf{pk}_i, c_i, s > \leftarrow \mathsf{Dec}(\mathsf{sk}_e, C)$
3 : Επέστρεψεi

Η ιδέα για τη λειτουργία του σχήματος είναι η εξής: Όλοι έχουν στην κατοχή τους ένα ιδιωτικό κλειδί για το σχήμα κοινών ψηφιακών υπογραφών. Τα κλειδιά κάθε μέλους της ομάδας υπογράφονται από από μια ανεξάρτητη αρχή που έχει στη κατοχή της το κλειδί sk_s, που είναι ουσιαστικά ένα κλειδί για έκδοση πιστοποιητικών. Η αρχή αυτή πιστοποιεί κατά τη δημιουργία των κλειδιών ότι το κάθε κλειδί ανήκει όντως σε αυτόν που υποστηρίζει ότι του ανήκει. Το ιδιωτικό κλειδί

[1]Για την ακρίβεια, για κάποιους τεχνικούς λόγους στις αποδείξεις ασφάλειας του σχήματος, απαιτείται ένα ορθό ως προς προσομοίωση μη διαλογικό σύστημα αποδείξεων μηδενικής γνώσης για γλώσσες NP[33, 64].

αυτό *δεν* πρέπει να δοθεί στον αρχηγό της ομάδας, αφού αυτό θα του επέτρεπε στον αρχηγό να πιστοποιεί κλειδιά που δημιούργησε ο ίδιος. Στον αρχηγό δίνεται όμως το κλειδί αποκρυπτογράφησης sk_e. Για να υπογράψει ένα μέλος της ομάδας ανώνυμα, υπογράφει με το ιδιωτικό του κλειδί ψηφιακής υπογραφής, αλλά δεν αποκαλύπτει την υπογραφή αυτή. Κρυπτογραφεί την υπογραφή με το κλειδί κρυπτογράφησης pk_e, την οποία μπορεί να αποκρυπτογραφήσει ο αρχηγός σε περίπτωση που θέλει να την ανοίξει και να αποκαλύψει τη ταυτότητα του υπογράφοντα. Για να είναι η υπογραφεί δημόσια επαληθεύσιμη, αποδεικνύει σε μηδενική γνώση, ότι κατέχει ένα κλειδί υπογραφής pk_π το οποίο έχει πιστοποιηθεί, ότι γνωρίζει μια επαληθεύσιμη υπογραφή για το μήνυμα $\mathtt{m}$ με αυτό το κλειδί υπογραφής, και ότι έχει κάνει την κρυπτογράφηση ορθά.

Ιδιότητες Ασφάλειας

Θα κάνουμε μια άτυπη παρουσίαση των ιδιοτήτων ασφαλείας που έχουν εμφανιστεί κατά καιρούς στη βιβλιογραφία.

Φυσικά όπως σε κάθε σχήμα υπογραφών απαιτούμε η ομαδική υπογραφή να είναι *μη-πλαστογραφήσιμη*. Δηλαδή κανείς δε μπορεί να παράγει μια υπογραφή, για κάποιο μήνυμα $\mathtt{m}$, για την οποία ο αλγόριθμος επαλήθευσης να επιστρέφει 1, χωρίς να γνωρίζει το ιδιωτικό κλειδί κάποιου μέλους της ομάδας.

Η *ανωνυμία*, μας λέει ότι ένας αντίπαλος που δεν γνωρίζει το ιδιωτικό κλειδί του αρχηγού ή τα ιδιωτικά κλειδιά των μελών της ομάδας, δε μπορεί για καμία γνήσια ομαδική υπογραφή να αποφανθεί για την ταυτότητα του υπογράφοντα με πιθανότητα μη-αμελητέα καλύτερη από το να μαντέψει τυχαία.

Μια απαίτηση που σχετίζεται με την ανωνυμία είναι η *μη-συνδεσιμότητα*[4]. Για να είναι μια υπογραφή μη-συνδέσιμη πρέπει να ένας αντίπαλος με τις ίδιες δυνατότητες με τον αντίπαλο της ανωνυμίας, δε μπορεί να αποφανθεί αν δύο γνήσιες ομαδικές υπογραφές προέρχονται από το ίδιο ή από διαφορετικό υπογράφοντα.

Η ιδιότητα η υπογραφή να είναι *δίκαια*(exculpable)[4], απαιτεί κανείς να μη μπορεί να υπογράφει(συμπεριλαμβανομένου του αρχηγού), με τρόπο που αν ανοιχτεί η υπογραφή να φαίνεται ότι έχει υπογράψει κάποιο μέλος της ομάδας, πέρα από αυτό που όντως υπέγραψε.

Μια ιδιότητα που δεν είναι ξεκάθαρο αν είναι ιδιότητα ασφαλείας ή απλά ιδιότητα ορθότητας, είναι η *ανιχνευσιμότητα*[24], σύμφωνα με την οποία πρέπει αν μια υπογραφή έχει παραχθεί από το μέλος της ομάδας με ταυτότητα π, θα πρέπει ο αλγόριθμος ανοίγματος να επιστρέφει π.

Η *ανθεκτικότητα στις συμμαχίες*(coalition-resistance)[3] δίνει ένα περιορισμό στο τι μπορούν να κάνουν τα μέλη της ομάδας αν συνεργαστούν μεταξύ τους, ή ισοδύναμα αν ένας αντίπαλο καταφέρει να υποκλέψει τα κλειδιά πολλών, ή και όλων των μελών της ομάδας. Ακόμα και σε αυτή τη περίπτωση ο αντίπαλος δε θα πρέπει να μπορεί να παράγει μια γνήσια υπογραφή, που αν ανοιχτεί να μην αντιστοιχεί στη ταυτότητα ενός από τα μέλη της ομάδας που το κλειδί τους χρησιμοποιήθηκε στη κατασκευή της ομαδικής υπογραφής.

Η *προστασία από ενοχοποίηση*(framing)[26] είναι παρεμφερής με την ιδιότητα

της υπογραφής να είναι ανθεκτική στις συμμαχίες και δίκαιη. Απαγορεύει σε οποιαδήποτε συμμαχία μελών της ομάδας, ακόμη και του αρχηγού, να παράξουν μία υπογραφή που φαίνεται να ανήκει σε κάποιο άλλο μέλος της ομάδας, εκτός της συμμαχίας.

Έχουν προταθεί και δύο ισχυρές ιδιότητες, η *πλήρης ανωνυμία* και η *πλήρης ανιχνευσιμότητα*[8]. Είναι ιδιότητές φτιαγμένες ώστε να συνεπάγονται όλες τις προηγούμενες ενάντια σε έναν ισχυρό αντίπαλο.

Ασφάλεια Σχήματος BMW

Το σχήμα BMW ικανοποιεί αποδεδειγμένα, στο μοντέλο CRS τις παρακάτω ιδιότητες ασφάλειας.

Θεώρημα 5.1. *Αν το κρυπτοσύστημα είναι IND-CCA2, και το (P, V) είναι ένα ορθό ως προς προσομοίωση, υπολογιστικό σύστημα αποδείξεων μηδενικής γνώσης, τότε το σχήμα ομαδικών υπογραφών BMW είναι πλήρως ανιχνεύσιμο.*

Θεώρημα 5.2. *Αν το σύστημα ψηφιακών υπογραφών είναι μη-πλαστογραφήσιμο ενάντια σε επίθεση επιλεγμένου μηνύματος, και το σύστημα (P, V) είναι ένα ορθό μη-διαλογικό σύστημα αποδείξεων μηδενικής γνώσης , τότε το σχήμα ομαδικών υπογραφών BMW είναι πλήρως ανώνυμο.*

Μια αδυναμία του σχήματος όμως είναι η αρχή έκδοσης πιστοποιητικών, που θεωρείται ότι είναι απόλυτα εμπιστεύσιμη. Χωρίς αυτή την υπόθεση, δηλαδή αν για παράδειγμα η αρχή μοιραστεί το κλειδί πιστοποίησης με τον αρχηγό της ομάδας, τότε ξεκάθαρα δεν ισχύουν οι παραπάνω ιδιότητες, αφού ο αρχηγός θα μπορούσε να δημιουργεί υπογραφές που δεν αντιστοιχούν στη ταυτότητα κανενός από τα πραγματικά μέλη της ομάδας.

5.2 Υπογραφές Δακτυλίου

Οι υπογραφές δακτυλίου(RS) χτίστηκαν πάνω στην ιδέα των ομαδικών υπογραφών, αλλά με μερικές σημαντικές διαφορές. Στις RS δεν υπάρχει αρχηγός που να μπορεί να ανοίξει τις υπογραφές και να αποκαλύψει τη ταυτότητα του υπογράφοντα, και δεν απαιτείται συνεργασία με άλλα μέλη τις ομάδας για καμία από τις διαδικασίες. Ο υπογράφοντας, αρκεί να χρησιμοποιήσει τα δημόσια κλειδιά όποιων θέλει, χωρίς να τους ενημερώσει, για να υπογράψει ως μέλος της αυτοσχέδιας ομάδας, ή δακτυλίου όπως έχει καθιερωθεί να ονομάζεται. Οι RS προτάθηκαν από τους Rivest, Shamir και Tauman[62], ως ένας τρόπος να διαρρεύσεις ανώνυμα μυστικά, και έδωσαν μια κατασκευή βασισμένη στο πρόβλημα RSA σε συνδυασμό με κάποιο ασφαλές συμμετρικό κρυπτοσύστημα(πχ. AES).

Όπως και στις ομαδικές υπογραφές, οι RS προσφέρουν ανωνυμία μέσα σε ένα σύνολο οντοτήτων. Οι διαφορές τους συνοψίζονται ως εξής:

- Δημιουργία κλειδιών: Στις ομαδικές υπογραφές συνήθως υπάρχει ένα κοινό δημόσιο κλειδί ομάδας, και τα κλειδιά των μελών της ομάδας δημιουργούνται όχι ανεξάρτητα, και για να ενταχθεί κάποιο μέλος στην ομάδα πρέπει κατά κανόνα να αλληλεπιδράσει με τον αρχηγό. Αντίθετα στις υπογραφές δακτυλίου ο κάθε χρήστης δημιουργεί το ζεύγος κλειδιών του ανεξάρτητα, και ο δακτύλιος αποφασίζεται από τον υπογράφοντα κατά της διαδικασία της υπογραφής, απλά με την επιλογή των δημοσίων κλειδιών των χρηστών που επιθυμεί να συμπεριλάβει.

- Ανάκληση Ανωνυμίας: Στις ομαδικές υπογραφές ο αρχηγός μπορεί κατά τη κρίση του να ανοίξει μια υπογραφή, δηλαδή να αποκαλύψει τη ταυτότητα του υπογράφοντα. Στις υπογραφές δακτυλίου, δεν υπάρχει καν αρχηγός, όλα τα μέλη του δακτυλίου είναι ισάξια, και κανείς δε μπορεί να αποκαλύψει τη ταυτότητα του υπογράφοντα, εκτός ίσως αν ο ίδιος ο υπογράφοντας αποφασίσει να αποκαλυφθεί.

5.2.1 Μοντέλο RS

Τυπικά ένα σχήμα υπογραφών δακτυλίου(RS), είναι μια τετράδα αλγορίθμων $(\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$:

- *Δημιουργία Κλειδιών*: Δημιουργεί ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού. Όλοι οι χρήστες του συστήματος πρέπει να έχουν ένα ζεύγος κλειδιών αποτέλεσμα αυτού του αλγορίθμου.
  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$

- *Υπογραφή*: Με είσοδο ένα ιδιωτικό κλειδί sk_π, ένα σύνολο δημοσίων κλειδιών L με $\mathsf{pk}_\pi \in L$, και το μήνυμα $\mathtt{m}$, επιστρέφει μια υπογραφή σ.
  $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$

- *Επαλήθευση*: Με είσοδο μια υπογραφή σ, το μήνυμα $\mathtt{m}$, και ένα σύνολο δημοσίων κλειδιών L, επιστρέφει 1 αν η υπογραφή είναι έγκυρη και αντιστοιχεί σε κάποιο κλειδί του L.
  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\sigma, L, \mathtt{m})$

Το σύνολο L των δημοσίων κλειδιών το αποκαλούμε δακτύλιο, ή αν σκεφτούμε ως ένα υποσύνολο του σύμπαντος όλων των δημοσίων κλειδιών του συστήματος $L \subset \mathcal{U}$, υποδακτύλιο.

5.2.2 Υπογραφές 1 από n με κλειδιά DLP

Ένα από τα πρώτα σχήματα υπογραφών δακτυλίων είναι αυτό των Abe, Ohkubo και Suzuki[1]. Η υπογραφή τους βασίζεται στην ιδέα των [27] για αποδείξεις μηδενικής μερικής γνώσης. Θα παρουσιάσουμε εδώ την εκδοχή με κλειδιά τύπου DLP. Στην αρχική τους δουλειά, το κάθε μέλος του δακτυλίου μπορούσε να διαλέγει είτε κλειδί τύπου DLOG είτε κλειδί τύπου RSA με διαφορετικές παραμέτρους.

Εμείς θα υποθέσουμε όταν όλα τα κλειδιά προέρχονται από την ίδια ομάδα $\mathbb{G}$ τάξης q με γεννήτορα g, όπου ισχύει η υπόθεση του διακριτού λογαρίθμου(DLOG), καθώς και μια κρυπτογραφική συνάρτηση σύνοψης(B′) $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_q$.

Δημιουργία Κλειδιών $\mathsf{KGen}(1^\lambda)$	*Επαλήθευση* $\mathsf{Vrfy}(\sigma, L, \mathtt{m})$
1 : $x \leftarrow\$ \mathbb{Z}_q$	1 : $i \in [n_L] : z'_i \leftarrow g^{s_i} y_i^{c_i}$
2 : $y \leftarrow g^x$	2 : $c_{i+1} \leftarrow \mathsf{H}(L, \mathtt{m}, z'_i)$
3 : $\mathsf{sk} \leftarrow x$, $\mathsf{pk} \leftarrow y$	3 : Επέστρεψε $c_1 = c_{n_L+1}$

Υπογραφή $\mathsf{Sign}(x_\pi, L, \mathtt{m})$

1 : $u \leftarrow\$ \mathbb{Z}_q$
2 : $c_{\pi+1} \leftarrow \mathsf{H}(L, \mathtt{m}, g^u)$
3 : $i \in \{\pi+1, \ldots, n_L, 1, \ldots, \pi-1\} : s_i \leftarrow\$ \mathbb{Z}_q$
4 : $c_{i+1} \leftarrow \mathsf{H}(L, \mathtt{m}, g^{s_i} y_i^{c_i})$
5 : $s_\pi \leftarrow u - x_\pi c_\pi$
6 : $\sigma \leftarrow (c_1, s_1, \ldots, s_{n_L})$
7 : Επέστρεψε σ

Το παραπάνω σχήμα είναι ουσιαστικά βασισμένο στις υπογραφές Schnorr[65]. Πράγματι για $n_L = 1$ έχουμε το σχήμα του Schnorr. Για παραπάνω από ένα χρήστη, κάθε πρόκληση προέρχεται από το προηγούμενο βήμα, και ο δακτύλιος μπορεί να ¨κλείσει¨ στο βήμα που χρησιμοποιείται το δημόσιο κλειδί του υπογράφοντα.

5.2.3 Ιδιότητες Ασφάλειας RS

Όπως σε όλα τα σχήματα υπογραφών, η κύρια απαίτηση είναι η υπογραφή να είναι *μη-πλαστογραφήσιμη*. Στο πλαίσιο των υπογραφών δακτυλίου, αυτό σημαίνει κανείς να μη μπορεί να δημιουργήσει μια έγκυρη υπογραφή, χωρίς να ξέρει τουλάχιστον ένα από τα κλειδιά που ανήκουν στον δακτύλιο που αντιστοιχεί στην υπογραφή.

Η ιδιότητα που χαρακτηρίζει τις RS είναι η *ανωνυμία*. Απαιτούμε κανένας αντίπαλος να μη μπορεί να μαντέψει τη ταυτότητα του υπογράφοντα. Φυσικά, πάντα μπορεί να μαντέψει τυχαία με πιθανότητα $\frac{1}{n_L}$. Για αυτό το λόγο χρησιμοποιείται και ο όρος ασάφεια υπογράφοντος(signer ambiguity)(πχ. [62]), ο οποίος καταδεικνύει ίσως πιο εύστοχα ότι η ανωνυμία είναι σε σχέση μόνο με τα υπόλοιπα μέλη του δακτυλίου. Η ανωνυμία μπορεί να είναι υπολογιστική, αν υποθέσουμε *PPT* αντίπαλο και πιθανότητα αμελητέα κοντά στη τυχαία μαντεψιά, ή τέλεια αν υποθέσουμε μη-φραγμένο αντίπαλο και πιθανότητα ακριβώς ίση με $\frac{1}{n_L}$.

Μη-Πλαστογραφησιμότητα

Θα ορίσουμε και τυπικά τη μη-πλαστογραφησιμότητας χρησιμοποιώντας ένα πείραμα στο οποίο ο αντίπαλος $\mathcal{A}$, προσπαθεί να παράγει μια έγκυρη υπογραφή, για κάποιο υποδακτύλιο L για τον οποίο δε ξέρει κανένα από τα ιδιωτικά

κλειδιά. Στη διάθεση του έχει φυσικά ένα μαντείο υπογραφών $\mathcal{SO}$, που του επιτρέπει να ζητά υπογραφές για μήνυμα, υποδακτύλιο και δημόσιο κλειδί της επιλογής του. Τονίζουμε ότι μπορεί να ζητάει υπογραφές και για διαφορετικούς υποδακτύλιο $L' \neq L$ από αυτόν για τον οποίο θα επιχειρήσει να παράξει πλαστογραφία. Επιπλέον του δίνουμε τη δυνατότητα να αυξήσει τα κλειδιά στο σύστημα με το μαντείο εγγραφής $\mathcal{JO}$ και ακόμα και να μαθαίνει το αντίστοιχο ιδιωτικό κλειδί για δημόσια κλειδιά της επιλογής του με το μαντείο διαφθοράς $\mathcal{CO}$. Αυτό μοντελοποιεί έναν ισχυρό προσαρμοστικό αντίπαλο, που μπορεί να ξέρει πολλά ιδιωτικά κλειδιά. Στη πράξη όταν ένας χρήστης υπογράφει, δε μπορεί να ξέρει αν υπάρχει κάποιος που ξέρει πολλά κλειδιά μέσα στο δακτύλιο που διάλεξε. Φυσικά δε θα θεωρείται επιτυχείς πλαστογραφία μία έξοδος του $\mathcal{SO}$ ή μια υπογραφή που αφορά δακτύλιο με έστω και ένα διεφθαρμένο κλειδί. Συμβολίζουμε το σύνολο των δεικτών των διεφθαρμένων κλειδιών με D_t. Αυτή η δυνατότερη έννοια μη-πλαστογραφησιμότητας ορίστηκε για πρώτη φορά από τους [12], αν και είχαν γίνει και έμμεσες αναφορές σε σχετικές επιθέσεις νωρίτερα[50, 53].

Παιχνίδι 5.1: Πείραμα Μη-Πλαστογραφησιμότητας $\mathtt{Exp}^{UnfRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(\sigma, L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}(1^\lambda, \mathcal{U})$
επέστρεψε $\mathsf{Vrfy}(\sigma, L, \mathtt{m})$ **ΚΑΙ** σ δεν είναι έξοδος του $\mathcal{SO}$ **ΚΑΙ** $\forall i \in D_t : \mathsf{pk}_i \notin L$

Ορισμός 5.1. *Ένα RS σχήμα Π είναι μη-πλαστογραφήσιμο αν για κάθε* PPT *αντίπαλο* $\mathcal{A}$*:*

$$Pr[\mathtt{Exp}^{UnfRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$$

Ανωνυμία

Ο αντίπαλος $\mathcal{A}$ της υπολογιστικής ανωνυμίας έχει και πάλι πρόσβαση στα μαντεία εγγραφής $\mathcal{JO}$, διαφθοράς $\mathcal{CO}$ και υπογραφής $\mathcal{SO}$, τα οποία χρησιμοποιεί προσαρμοστικά και για υποδακτύλιους της επιλογής του. Στη πρώτη φάση ο αντίπαλος μπορεί να καλέσει τα μαντεία με όποιο τρόπο θέλει, και διαλέγει ένα υποδακτύλιο και ένα μήνυμα για να του δοθεί η πρόκληση. Το σύστημα παράγει την υπογραφή και ο $\mathcal{A}$ προσπαθεί να μαντέψει τη ταυτότητα του υπογράφοντα. Η αποδεκτή πιθανότητα επιτυχίας εξαρτάται φυσικά από το μέγεθος του υποδακτυλίου, αφού πάντα ο αντίπαλος μπορεί να μαντέψει τυχαία. Όπως στον ορισμός των [12], Θέλουμε ακόμα και αν ο $\mathcal{A}$ μάθει όλα τα ιδιωτικά κλειδιά, να μη μπορεί να μάθει τη ταυτότητα το υπογράφοντα. Αυτό δε συμβαίνει, γιατί ακόμα και αν ο αντίπαλος γνωρίζει τα μυστικά κλειδιά, δε μπορεί να αναγνωρίσει μια υπογραφή που δημιουργήθηκε με ένα τέτοιο κλειδί, αν δε την έχει δημιουργήσει ο ίδιος.

Παιχνίδι 5.2: Πείραμα Υπολογιστικής Ανωνυμίας $\mathtt{Exp}^{AnonRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}(1^\lambda, \mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow\$ [n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$
$(\xi, D_t') \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}(1^\lambda, L, \mathtt{m}, D_t, \sigma, \textbf{εικασία})$
επέστρεψε $\xi = \pi$

Ορισμός 5.2. *Ένα RS σχήμα Π είναι υπολογιστικά ανώνυμο αν για κάθε* PPT *αντίπαλο* $\mathcal{A}$*:*

$$Pr[\mathtt{Exp}^{AnonRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] - \frac{1}{n_L} \leq \mathsf{negl}(\lambda)$$

Για την τέλεια ανωνυμία, οι απαιτήσεις είναι πιο αυστηρές. Ο αντίπαλος είναι υπολογιστικά μη-φραγμένος, οπότε μπορεί να υπολογίσει οποιοδήποτε ιδιωτικό κλειδί θέλει. Οπότε το σχήμα πρέπει να είναι ανώνυμο ακόμα και ενάντια σε κάποιον που γνωρίζει όλα τα κλειδιά. Η πιθανότητα επιτυχίας δεν αρκεί να είναι αμελητέα κοντά στην τυχαία μαντεψιά, αλλά πρέπει να είναι ακριβώς ίδια. Δίνουμε στον αντίπαλο πρόσβαση στον μαντείο $\mathcal{SO}$, αφού ακόμα και ένας μη φραγμένος αντίπαλος, δε μπορεί αναγκαστικά να υπολογίσει μόνος του την έξοδο του μαντείου, όπως συμβαίνει για παράδειγμα στο σχήμα των [48].

Παιχνίδι 5.3: Πείραμα Τέλειας Ανωνυμίας $\mathtt{Exp}^{UAnonRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(1^\lambda, \mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow\$ [n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$
$\xi \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(1^\lambda, L, \mathtt{m}, \sigma, \textbf{εικασία})$
επέστρεψε $\xi = \pi$

Ορισμός 5.3. *Ένα RS σχήμα Π είναι τέλεια ανώνυμο αν για κάθε (μη-φραγμένο) αντίπαλο* $\mathcal{A}$*:*

$$Pr[\mathtt{Exp}^{UAnonRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] - \frac{1}{n_L} = 0$$

Ασφάλεια Σχήματος 1 από n με κλειδιά DLP

Για σχήμα που παρουσιάσαμε στην υποενότητα 5.2.2, οι συγγραφείς του απέδειξαν τα παρακάτω θεωρήματα για την ασφάλεια του[1]:

Θεώρημα 5.3 (Μη-πλαστογραφησιμότητα). *Το σχήμα 1 από n με κλειδιά τύπου DLP είναι μη-πλαστογραφήσιμο στο μοντέλο $\mathcal{RO}$ αν ισχύει η υπόθεση* DLOG *στη* $\mathbb{G}$.

Θεώρημα 5.4 (Ανωνυμία). *Το σχήμα 1 από n με κλειδιά τύπου DLP είναι τέλεια ανώνυμο.*

5.3 Συνδέσιμες Υπογραφές Δακτυλίου

Η ανωνυμία που προσφέρουν οι υπογραφές δακτυλίου φαίνεται να έχει πολλές προοπτικές για εφαρμογές όπως οι ηλεκτρονικές ψηφοφορίες. Ο δακτύλιος μπορεί να αποτελείται από τους ψηφοφόρου,έτσι μπορεί να ελεγχθεί ότι μόνο όσοι έχουν δικαίωμα ψήφου συμμετέχουν, ενώ η ανωνυμία των διασφαλίζεται από τις ιδιότητες της υπογραφής. Το πρόβλημα είναι όμως, ότι δε μπορούν εντοπιστεί αν κάποιος ψηφίζει παραπάνω από μια φορά.

Λύση σε αυτό το πρόβλημα έδωσαν οι Liu, Wei και Wong, εισάγοντας τις συνδέσιμες υπογραφές δακτυλίου[50]. Η ιδέα ήταν να εισάγουν για κάθε χρήστη ένα ψευδώνυμο(pseudoidentity), το οποίο αναγκαστικά πρέπει να χρησιμοποιηθεί ώστε να προκύψει μια έγκυρη υπογραφή. Έτσι ο καθένας μπορεί να δει αν δυο υπογραφές προέρχονται από τον ίδιο χρήστη, ή από δύο διαφορετικούς, χωρίς όμως να μπορεί να μάθει την ταυτότητα του υπογράφοντως. Στη πράξη το ψευδώνυμο είναι κάποια δύσκολα αντιστρέψιμη συνάρτηση του ιδιωτικού κλειδιού του χρήστη.

Με αυτή λοιπόν την επιπλέον ιδιότητα, την συνδεσιμότητα, λύνεται το πρόβλημα των διπλών ψήφων. Αν κάποιος ψηφοφόρος επιχειρήσει να ψηφίσει δύο φορές, η απάτη του θα αποκαλυφθεί αμέσως.

Μια πιο πρόσφατη μεγάλη επιτυχία των LRS είναι η χρήση τους στο κρυπτονόμισμα Monero[55]. Με έξυπνη χρήση μιας παραλλαγής των LRS, μπορούν να γίνουν εμπιστευτικές συναλλαγές, όπου δεν αποκαλύπτεται η ταυτότητα, ούτε του αποστολέα, ούτε του παραλήπτη, αλλά ούτε και το πόσο της συναλλαγής.

5.3.1 Μοντέλο LRS

Το μοντέλο των LRS είναι φυσικά παρόμοιο με αυτό των RS, υπάρχουν όμως μερικές βασικές διαφορές:

- Υπάρχει ένας παραπάνω αλγόριθμος, ο αλγόριθμος *σύνδεσης*, ο οποίος αποκρίνεται ναι ή όχι για το αν δύο υπογραφές προέρχονται από τον ίδιο μέλος του δακτυλίου.

- Συνήθως είναι θεμιτό η σύνδεση να μην αφορά όλες τις υπογραφές ενός χρήστη, αλλά μόνο τις υπογραφές που σχετίζονται με μια συγκεκριμένη εκδήλωση, όπως για παράδειγμα μία ψηφοφορία, ή να αφορά μόνο τις υπογραφές από τον ίδιο υποδακτύλιο L ή οποιοδήποτε άλλο κριτήριο. Η επιλογή αυτή καθορίζεται κάθε φορά από τις ανάγκες της εφαρμογής. Σε αυτή τη ΔΕ θα περιορίσουμε τη συνδεσιμότητα μόνο σε υπογραφές ως προς τον ίδιο

υποδακτύλιου. Η τροποποίηση για άλλους τρόπους περιορισμού της συνδεσιμότητας είναι αρκετά άμεση, αλλά επισημαίνουμε ότι όλοι οι ορισμοί που δίνουμε παρακάτω πρέπει να τροποποιηθούν κατάλληλα σε αυτή τη περίπτωση.

- Για ευκολία στην παρουσίαση, θεωρούμε ως μέλος του μοντέλου και έναν αλγόριθμο *εξαγωγής* του ψευδώνυμου pid από μια υπογραφή. Στη βιβλιογραφία συναντάται μόνο ο αλγόριθμος σύνδεσης και η δυνατότητα εξαγωγής εννοείται.

Τυπικά ένα σχήμα συνδέσιμων υπογραφών δακτυλίου(LRS) αποτελείται από μια τετράδα αλγορίθμων (KGen, Sign, Vrfy, Link):

- *Δημιουργία Κλειδιών*: Δημιουργεί ένα ζεύγος κλειδιών.
  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$

- *Υπογραφή*: Με είσοδο το ιδιωτικό κλειδί του υπογράφοντα sk_π, ένα σύνολο δημοσίων κλειδιών L με $\mathsf{pk} \in L$ και το μήνυμα $\mathtt{m}$ επιστρέφει μια υπογραφή σ.
  $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$

- *Εξαγωγή*: Με είσοδο μια υπογραφή σ, επιστρέφει το ψευδώνυμο που αντιστοιχεί στον υπογράφοντα.
  $\mathsf{pid} \leftarrow \mathtt{Extract}(\sigma)$

- *Επαλήθευση*: Με είσοδο μια υπογραφή σ, το μήνυμα $\mathtt{m}$, και ένα σύνολο δημοσίων κλειδιών L, επιστρέφει αν η υπογραφή είναι έγκυρη.
  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\sigma, L, \mathtt{m})$

- *Σύνδεση*: Με είσοδο δύο έγκυρες υπογραφές σ,σ' και έναν υποδακτύλιο L, επιστρέφει 1 αν η υπογραφές προέρχονται από τον ίδιο χρήστη, και 0 αλλιώς.
  $\sigma \leftarrow \mathsf{Link}(\sigma, \sigma', L)$

Για ευκολία στην παρουσίαση, εισάγαμε ως μέλος του μοντέλου και έναν αλγόριθμο *εξαγωγής* του ψευδώνυμου pid από μια υπογραφή. Στη βιβλιογραφία συναντάται μόνο ο αλγόριθμος σύνδεσης και η δυνατότητα εξαγωγής εννοείται. Ουσιαστικά ισχύει ότι $\mathsf{Link}(\sigma, \sigma', L) \iff \mathtt{Extract}(\sigma) = \mathtt{Extract}(sig')$ και οι υπογραφές είναι έγκυρες και αφορούν τον ίδιο υποδακτύλιο L. Αν ο αλγόριθμος δεχτεί ως είσοδο μη έγκυρες υπογραφές, η έξοδος του δεν έχει καμία σημασία.

5.3.2 LSAG

Το πρώτο σχήμα συνδέσιμων υπογραφών δακτυλίου είναι όπως είπαμε αυτό των [50]. Οι συγγραφείς του το ονόμασαν Συνδέσιμες Αυθόρμητες Ανώνυμες Ομαδικές Υπογραφές(Linkable Spontaneous Anonymous Group Signatures) ή LSAG για συντομία. Η ονομασία πρόερχεται από το γεγονός, ότι σε αντίθεση με τις ομαδικές υπογραφές, η δημιουργία της υπογραφής δεν απαιτεί προεργασία, αρχηγό

ή συμμετοχή των άλλων μελών της ομάδας, αλλά μπορεί να γίνει αυθόρμητα, ενώ είναι φυσικά συνδέσιμες και ανώνυμες.

Το σχήμα τους βασίζεται στο σχήμα υπογραφών 1 από n. Η μετατροπή που έκαναν για να εισάγουν την ιδιότητα της συνδεσιμότητας, ήταν να εφεύρουν τα ψευδώνυμα. Για την δημιουργία του ψευδώνυμου οι χρήστες χρησιμοποιούν μια δεύτερη κρυπτογραφική συνάρτηση σύνοψης $\mathsf{H}_{\mathbb{G}} : \{0,1\}^* \to \mathbb{G}$, για να παράγουν έναν εναλλακτικό γεννήτορα της ομάδας h. Το ψευδώνυμο τους είναι $\hat{y} \leftarrow h^{\mathsf{sk}_\pi}$. Για να εξασφαλίσουν ότι οι χρήστες δε μπορούν να παράγουν υπογραφές χωρίς το ψευδώνυμο τους, εισήγαγαν έναν αντίστοιχο όρο με αυτόν που εξασφαλίζει την μη-πλαστογραφησιμότητα στη συνάρτηση σύνοψης, χρησιμοποιώντας όμως τον εναλλακτικό γεννήτορα h. Υπενθυμίζουμε ότι δουλεύουμε σε ομάδα $\mathbb{G}$ τάξης πρώτου q και μια συνάρτηση $\mathsf{H}_q : \{0,1\}^* \to \mathbb{Z}_q$. Υποθέτουμε ότι ισχύει η ισχυρότερη υπόθεση DDH, και όχι απλά η DLOG.

Δημιουργία Κλειδιών $\mathsf{KGen}(1^\lambda)$

1 : $x \leftarrow\$ \mathbb{Z}_q$
2 : $y \leftarrow g^x$
3 : $\mathsf{sk} \leftarrow x$, $\mathsf{pk} \leftarrow y$

Υπογραφή $\mathsf{Sign}(x_\pi, L, \mathtt{m})$

1 : $h \leftarrow \mathsf{H}_{\mathbb{G}}(L)$
2 : $\hat{y} \leftarrow h_\pi^x$
3 : $u \leftarrow\$ \mathbb{Z}_q$
4 : $c_{\pi+1} \leftarrow \mathsf{H}(L, \mathtt{m}, g^u, h^u)$
5 : $i \in \{\pi+1, \ldots, n_L, 1, \ldots, \pi-1\} : s_i \leftarrow\$ \mathbb{Z}_q$
6 : $c_{i+1} \leftarrow \mathsf{H}(L, \mathtt{m}, g^{s_i} y_i^{c_i}, h^{s_i} \hat{y}^{c_i})$
7 : $s_\pi \leftarrow u - x_\pi c_\pi$
8 : $\sigma \leftarrow (c_1, s_1, \ldots, s_{n_L}, \hat{y})$
9 : Επέστρεψε σ

Επαλήθευση $\mathsf{Vrfy}(\sigma, L, \mathtt{m})$

1 : $i \in [n_L] : z_i' \leftarrow g^{s_i} y_i^{c_i}$
2 : $z_i'' \leftarrow h^{s_i} \hat{y}^{c_i}$
3 : $c_{i+1} \leftarrow \mathsf{H}(L, \mathtt{m}, z_i', z_i'')$
4 : Επέστρεψε $c_1 = c_{n_L+1}$

Εξαγωγή $\mathtt{Extract}(\sigma)$

1 : Επέστρεψε $\hat{y}$

Σύνδεση $\mathsf{Link}(\sigma, \sigma', L)$

1 : Επέστρεψε $\mathtt{Extract}(\sigma) = \mathtt{Extract}(\sigma')$

5.3.3 Ιδιότητες Ασφάλειας LRS

Ο ορισμός της μη-πλαστογραφησιμότητας, είναι ακριβώς ο ίδιος με αυτόν των απλών RS(5.2.3). Ο αντίπαλος έχει τη δυνατότητα να βλέπει τα ψευδώνυμα και να χρησιμοποιεί τον δημόσιο αλγόριθμο Σύνδεσης, όμως η ουσία παραμένει η ίδια: δε θα πρέπει να μπορεί να παράγει έγκυρη υπογραφή χωρίς να γνωρίζει κάποιο από τα ιδιωτικά κλειδιά.

Για την ανωνυμία τα πράγματα είναι λίγο πιο περίπλοκα, αφού ο ορισμός της ανωνυμίας για τις RS, απαγορεύει ρητά τη συνδεσιμότητα. Οπότε πρέπει προσεκτικά να τροποποιήσουμε τον ορισμό, ώστε να επιτρέπει την συνδεσιμότητα, χωρίς όμως να επιτρέπει στον αντίπαλο να βρίσκει την ταυτότητα του υπογράφοντα.

Η κύρια προσθήκη είναι φυσικά η ιδιότητα της *συνδεσιμότητας*[50]. Η ιδιότητα αυτή περιλαμβάνει την απαίτηση ένα υπογράφοντας να μη μπορεί να παράγει

δύο υπογραφές που να μην είναι συνδεδεμένες μεταξύ τους, δηλαδή η συνδεσιμότητα είναι υποχρεωτική και όχι προαιρετική. Επιπλέον θα πρέπει ένα χρήστης που έχει στη κατοχή του k κλειδιά, να μη μπορεί να παράγει $k+1$ υπογραφές που να είναι μεταξύ τους ανά δύο ασύνδετες. Το άλλο σκέλος της ιδιότητας είναι κανένας αντίπαλος να μη μπορεί να παράγει μια υπογραφή που να είναι συνδεδεμένη μια μια υπογραφή που προέρχεται από άλλο μέλος του δακτυλίου. Είναι ουσιαστικά μια ιδιότητα που προστατεύει τους χρήστες από να την ενοχοποίηση(framing). Στη βιβλιογραφία έχει εμφανιστεί ξεχωριστά η ιδιότητα αυτή ως μη-δυσφημισιμότητα (non-slanderability). Η ιδιότητα αυτή αναφέρθηκε ως υποκατηγορία της συνδεσιμότητας πρώτα[51], και αργότερα πήρε το όνομα της ως μη-δυσφημισιμότητα[5, 71].

Ένας από τους λόγους για το διαχωρισμό των ιδιοτήτων που ξεκίνησε από τους [51], φαίνεται να είναι η αποδυνάμωση της ιδιότητας της συνδεσιμότητας. Στην προσπάθεια τους οι συγγραφείς να κατασκευάσουν ένα σχήμα υπολογιστικά αποτελεσματικότερο από αυτό των [50], ρητά περιόρισαν τον ορισμό της συνδεσιμότητας στο να επιτρέπει έναν αντίπαλο με k κλειδιά να παράγει περισσότερες από k υπογραφές όχι ανά δύο συνδεδεμένες. Ο ορισμός τους απαιτεί μόνο στην ειδική περίπτωση που ο αντίπαλος κατέχει μονάχα ένα ιδιωτικό κλειδί, να μη μπορεί να παράγει δύο μη συνδεδεμένες υπογραφές. Κατά τη γνώμη μας, αυτή είναι μια έκπτωση που δε θα πρέπει να δεχτούμε εύκολα. Για παράδειγμα σε μια εφαρμογή όπως αυτή των ηλεκτρονικών ψηφοφοριών, αυτό συνεπάγεται ότι αν και ένα χρήστης μόνος του δε μπορεί να ψηφίσει δύο φορές, αρκεί να συνεργαστεί με έναν μόνο δεύτερο χρήστη και να παράγουν τρεις έγκυρες ψήφους. Εύκολα μάλιστα μπορεί κανείς να δει ότι στο σχήμα των [51] μπορούν να παράγουν όσους υπογραφές θέλουν από τα δύο κλειδιά τους, περιορισμένοι μόνο από το μέγεθος της ομάδας $\mathbb{G}$. Παρόλα αυτά ο ορισμός αυτός έχει υιοθετηθεί σε αρκετές δουλειές(πχ.[5, 48, 70]).

Μη-Πλαστογραφησιμότητα

Ο ορισμός είναι ουσιαστικά ο ίδιος με αυτόν στην ενότητα 5.2.3. Για πληρότητα τον παραθέτουμε και σε αυτή την ενότητα.

Παιχνίδι 5.4: Πείραμα Μη-Πλαστογραφησιμότητας $\mathtt{Exp}^{UnfLRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(\sigma, L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}(1^\lambda, \mathcal{U})$
επέστρεψε $\mathsf{Vrfy}(\sigma, L, \mathtt{m})$ **ΚΑΙ** σ δεν είναι έξοδος του $\mathcal{SO}$ **ΚΑΙ** $\forall i \in D_t : \mathsf{pk}_i \notin L$

Ορισμός 5.4. *Ένα LRS σχήμα Π είναι μη-πλαστογραφήσιμο αν για κάθε* PPT *αντίπαλο $\mathcal{A}$:*

$$Pr[\mathtt{Exp}^{UnfLRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$$

Ανωνυμία

Η ιδιότητα της συνδεσιμότητας αλληλεπιδρά με την ιδιότητας την ανωνυμίας, για αυτό πρέπει να τροποποιήσουμε κατάλληλα τους ορισμούς στην ενότητα 5.2.3. Αφού ο αντίπαλος $\mathcal{A}$ έχει πρόσβαση στο μαντείο υπογραφής $\mathcal{SO}$, για το οποίο μπορεί να επιλέγει σε πιο δημόσιο κλειδί θα αντιστοιχεί η υπογραφή που θα έχει ως έξοδο, μπορεί τετριμμένα να βρει το ψευδώνυμο που αντιστοιχεί σε κάποιον χρήστη, και έτσι άμεσα να παραβιάσει την ανωνυμία. Δε θέλουμε να αφαιρέσουμε όμως τελείως την πρόσβαση του αντιπάλου στο μαντείο αυτό, αφού ρεαλιστικά θέλουμε ακόμα και αν ένας αντίπαλος με κάποιο τρόπο έχει στη κατοχή του στοιχεία για το ψευδώνυμο ενός συγκεκριμένου χρήστη, δε θα πρέπει αυτό να τον βοηθάει στο να βρει τη ταυτότητα για την υπογραφή ενός διαφορετικού χρήστη. Οπότε για τον ορισμό της ανωνυμίας μόνο, τροποποιούμε το μαντείο $\mathcal{SO}$ ώστε να μη δέχεται ως είσοδο ένα συγκεκριμένο δημόσιο κλειδί από τον αντίπαλο, αλλά να διαλέγει τυχαία από τα κλειδιά του L. Επειδή έχουμε περιορίσει την συνδεσιμότητα σε υπογραφές στον ίδιο υποδακτύλιο, ακόμα και αν ο αντίπαλος έχει στην κατοχή του την έξοδο του $\mathcal{SO}$ για κάποιο δακτύλιο L', αυτό δε θα πρέπει να του δίνει κανένα πλεονέκτημα για έναν δακτύλιο $L \neq L'$.

Έχουμε και εδώ δύο εκδοχές για την ανωνυμία, την υπολογιστική και την τέλεια, υποθέτοντας έναν PPT αντίπαλο ή έναν μη φραγμένο αντίστοιχα. Στην περίπτωση της υπολογιστικής ανωνυμίας, η πιθανότητα επιτυχίας του $\mathcal{A}$ εξαρτάται από τον αριθμό t των ιδιωτικών κλειδιών του δακτυλίου που γνωρίζει. Η γνώση των ιδιωτικών κλειδιών, μπορεί λόγω του ψευδώνυμου να αποκαλύψει στον αντίπαλο η υπογραφή πρόκληση σίγουρα δε προέρχεται από ένα από τα κλειδιά που γνωρίζει. Έτσι η πιθανότητα της τυχαίας μαντεψιάς εξαρτάται από το t. Στην περίπτωση της τέλειας ανωνυμίας, δεν έχει νόημα κάτι τέτοιο, αφού ο αντίπαλος μπορεί να υπολογίσει όλα τα κλειδιά.

Παιχνίδι 5.5: Πείραμα Υπολογιστικής Ανωνυμίας $\mathtt{Exp}^{AnonLRS}_{\mathcal{A},\Pi,n,t}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}(1^\lambda, \mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow\$ [n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$
$(\xi, D_t') \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}(1^\lambda, L, \mathtt{m}, D_t, \sigma, \textbf{εικασία})$
Αν $\pi \notin D_t'$ **τότε**
  επέστρεψε $\xi = \pi$
αλλιώς
  επέστρεψε $\perp$

Ορισμός 5.5. *Ένα LRS σχήμα Π είναι υπολογιστικά t-ανώνυμο αν για κάθε* PPT

αντίπαλο $\mathcal{A}$:

$$Pr[\mathtt{Exp}^{AnonLRS}_{\mathcal{A},\Pi,n,t}(\lambda) = 1] - \frac{1}{n_L - t} \leq \mathsf{negl}(\lambda)$$

Για την τέλεια ανωνυμία, παρατηρήστε ότι το παιχνίδι είναι ακριβώς το ίδιο με αυτό των RS(5.3). Η παρουσία των ψευδωνύμων δεν δίνουν κανένα ουσιαστικό πλεονέκτημα σε έναν μη φραγμένο αντίπαλο.

Παιχνίδι 5.6: Πείραμα Τέλειας Ανωνυμίας $\mathtt{Exp}^{UAnonLRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
΄Εξοδος: $\{0, 1\}$

$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(1^\lambda, \mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow\$ [n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$
$\xi \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(1^\lambda, L, \mathtt{m}, \sigma, \textbf{εικασία})$
επέστρεψε $\xi = \pi$

Ορισμός 5.6. *΄Ενα LRS σχήμα Π είναι τέλεια ανώνυμο αν για κάθε (μη-φραγμένο) αντίπαλο $\mathcal{A}$:*

$$Pr[\mathtt{Exp}^{UAnonRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] - \frac{1}{n_L} = 0$$

Συνδεσιμότητα

Η συνδεσιμότητα απαιτεί, αν δύο υπογραφές προέρχονται από τον ίδιο υπογράφοντα τότε να είναι συνδεδεμένες, και κανένας αντίπαλος να μη μπορεί να παράγει παραπάνω ανά δύο μη συνδεδεμένες υπογραφές από ότι έχει κλειδιά στη κατοχή του. Ο αντίπαλος έχει στη διάθεση του όλα τα μαντεία($\mathcal{RO}, \mathcal{JO}, \mathcal{CO}, \mathcal{SO}$) και μπορεί να χρησιμοποιήσει οποιαδήποτε (προσαρμοστική) στρατηγική επιθυμεί. Στόχος του στο παιχνίδι συνδεσιμότητας είναι να παράγει k έγκυρες υπογραφές για υποδακτύλιο L της επιλογής του που να μη συνδέονται μεταξύ τους, έχοντας διαφθείρει γνήσια λιγότερα από k κλειδιά του L. Δεν γίνονται δεκτές υπογραφές που είναι έξοδος του $\mathcal{SO}$, αφού ο αντίπαλος πρέπει να παράγει ο ίδιο τις υπογραφές.

Παιχνίδι 5.7: Πείραμα Συνδεσιμότητας $\mathtt{Exp}^{LinkLRS}_{\mathcal{A},\Pi,n}$

$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(\{\sigma_i\}_{i=1}^k, L = \left\{\mathsf{pk}_i\right\}_{i=1}^{n_L}, \{\mathtt{m}_i\}_{i=1}^k, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}(1^\lambda, \mathcal{U})$
επέστρεψε $\mathsf{Vrfy}(\sigma_i, L, \mathtt{m}_i)\ \forall i \in [k]$ **ΚΑΙ**
$\mathsf{Link}(\sigma_i, \sigma_j, L) = 0\ \forall i, j \in [k],\ i \neq j$ **ΚΑΙ**
$|\{pk_i : i \in D_t\} \cap L| < k$ **ΚΑΙ**
$\sigma_i \notin \mathcal{SO}\ \forall i \in [k]$

Ορισμός 5.7. *Ένα LRS σχήμα Π είναι συνδέσιμο αν για κάθε* PPT *αντίπαλο* $\mathcal{A}$*:*

$$Pr[\mathtt{Exp}^{LinkLRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$$

Η ιδιότητα της μη-δυσφημισιμότητας[5, 71], που απαιτεί ο $\mathcal{A}$ να μη μπορεί να παράγει υπογραφή που να είναι συνδεδεμένη με μια υπογραφή ενός χρήστη του οποίου δε ξέρει το ιδιωτικό κλειδί, έπεται από τον ορισμό της συνδεσιμότητας που δώσαμε, σε συνδυασμό με την μη-πλαστογραφησιμότητα. Για να το αποδείξουμε αυτό, ας υποθέσουμε ότι υπάρχει ένας $\mathcal{A}$ που μπορεί να δυσφημίσει έναν χρήστη δημιουργώντας μια έγκυρη υπογραφή με το ψευδώνυμο του y. Αν δεν γνωρίζει κανένα ιδιωτικό κλειδί, τότε αυτό αποτελεί πλαστογραφία και παραβιάζει την ιδιότητα της μη-πλαστογραφησιμότητας. Αν γνωρίζει $k > 0$ ιδιωτικά κλειδιά έχουμε δύο περιπτώσεις, είτε ο $\mathcal{A}$ γνωρίζει το κλειδί που αντιστοιχεί στο y είτε όχι. Αν το γνωρίζει τότε αυτό δεν αποτελεί επιτυχημένη επίθεση, αφού τότε προφανώς και είναι σε θέση να δημιουργεί υπογραφές συνδεδεμένες με αυτές του χρήστη. Αν δε γνωρίζει το κλειδί, τότε από την ορθότητα του αλγορίθμου σύνδεσης, μπορεί να παράγει k υπογραφές από τα κλειδιά που γνωρίζει, και μία ακόμα, αυτή που έχει ψευδώνυμο y. Δηλαδή έχει παράγει $k+1$ υπογραφές και έχει παραβιάσει την ιδιότητας της συνδεσιμότητας.

Για τον αναγνώστη που ενδιαφέρεται να δει τον αδύναμο ορισμό της συνδεσιμότητας και τον ορισμό της μη-δυσφημισιμότητας προτείνουμε αυτούς των [48].

Ασφάλεια Σχήματος LSAG

Για το σχήμα LSAG οι συγγραφείς του απέδειξαν την ασφάλεια του[50], στο μοντέλο τυχαίου μαντείου $\mathcal{RO}$. Χρησιμοποίησαν μια δικιά τους παραλλαγή του Λήμματος Διακλάδωσης, το λήμμα Επαναφοράς στην Επιτυχία.

Θεώρημα 5.5 (Μη-πλαστογραφησιμότητα). *Το σχήμα LSAG είναι μη-πλαστογραφήσιμο στο μοντέλο* $\mathcal{RO}$ *αν ισχύει η υπόθεση* DLOG *στη* $\mathbb{G}$.

Θεώρημα 5.6 (Ανωνυμία). *Το σχήμα LSAG είναι υπολογιστικά ανώνυμο στο μοντέλο* $\mathcal{RO}$ *αν ισχύει η υπόθεση DDH στη* $\mathbb{G}$.

Σημείωση 5.1. *Ένα τίμημα που πληρώνει το σχήμα LSAG για την συνδεσιμότητα, είναι ότι πλέον η ανωνυμία δεν είναι τέλεια, αλλά υπολογιστική. Αυτό είναι αναμενόμενο αφού τα ψευδώνυμα δίνουν σε έναν υπολογιστικά μη φραγμένο αντίπαλο έναν εύκολο τρόπο να μάθουν την ταυτότητα του υπογράφοντα συγκρίνοντας το ψευδώνυμο και τα δημόσια κλειδιά του δακτυλίου. Αρκεί να βρει ποιο κλειδί έχει τον ίδιο διακριτό λογάριθμο με το ψευδώνυμο, δηλαδή να λύσει ένα στιγμιότυπο του προβλήματος DDH. Αυτή η αδυναμία θα λυθεί αργότερα στο πρώτο σχήμα LRS με τέλεια ανωνυμία[48].*

Θεώρημα 5.7 (Συνδεσιμότητα). *Το σχήμα LSAG είναι συνδέσιμο στο μοντέλο* $\mathcal{RO}$ *αν ισχύει η υπόθεση* DLOG *στη* $\mathbb{G}$.

ΚΕΦΑΛΑΙΟ 6

Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή

Σε αυτό το κεφάλαιο θα δούμε πως μπορούμε να συνδυάσουμε τις Υπογραφές Καθορισμένου Επαληθευτή (DVS) του κεφαλαίου 4 και τις Συνδέσιμες Υπογραφές ΔακτυλίουLRS του κεφαλαίου 5 για να κατασκευάσουμε ένα καινούριο είδος ψηφιακών υπογραφών με ενδιαφέρουσες εφαρμογές, τις Συνδέσιμες Υπογραφές Δακτυλίου Καθοσιμένου Επαληθευτή (DVLRS). Η δουλειά αυτή, που αποτελεί ίσως τη κύρια συνεισφορά της ΔΕ, είναι μια συνεργατική δουλειά των Behrouz, Grontas, Konstantakatos, Pagourtzis και Spyrakou. Παρουσιάστηκε στο 24th International Conference on Information Security and Cryptology (ICISC 2021). Επειδή η δημοσίευση του δεν έχει ολοκληρωθεί ως σήμερα, παραπέμπουμε προς το παρόν στην διαδικτυακή του έκδοση στο [7].

Θα ξεκινήσουμε με μια σύντομη αναφορά σε υπογραφές δακτυλίου με καθορισμένο επαληθευτή που δεν έχουν την ιδιότητα της συνδεσιμότητας. Θα δούμε ότι αυτές έχουν μια φυσική κατασκευή από τα επιμέρους σχήματα. Στη συνέχεια θα αναφερθούμε σε σχετικές παλαιότερες δουλειές στη βιβλιογραφία.

Στο κυρίως μέρος του κεφαλαίου θα παρουσιάσουμε το καινοτόμο μοντέλο για τις DVLRS, τις ιδιότητες ασφαλείας και τους ορισμούς τους, και μια κατασκευή που υλοποιεί τα παραπάνω, με αποδείξεις ασφάλειας στο μοντέλο τυχαίου μαντείου $\mathcal{RO}$.

Η εξερεύνηση των εφαρμογών του σχήματος μας είναι μεγάλης σημασίας και για αυτό την έχουμε μεταθέσει στο δικό της κεφάλαιο 7.

6.1 Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή

Οι DVS και οι RS έχουν μια ενδιαφέρουσα φυσική σχέση. Αν έχουμε ένα σχήμα υπογραφών δακτυλίου, και περιορίσουμε τον δακτύλιο στο να έχει μόνο δύο μέλη, τότε έχουμε στα χέρια μας ένα σχήμα DVS. Οι μόνοι που μπορούν να υπογράψουν σε αυτό το σχήμα είναι τα δύο μέλη του δακτυλίου. Λόγω της ανωνυμίας, κανείς δε μπορεί να ξεχωρίσει ποιος από τους δύο υπογράφει. Αν καθορίσουμε έναν από τους δύο ως τον επαληθευτή και τον άλλο ως τον υπογράφοντα τότε ο επαληθευτή μπορεί να είναι σίγουρος πότε ένα μήνυμα προέρχεται από τον υπογράφοντας, αφού ξέρει ότι, όλες οι υπογραφές που δεν προέρχονται από τον ίδιο, πρέπει αναγκαστικά να προέρχονται από τον υπογράφοντα. Δεν μπορεί όμως να πείσει κανέναν τρίτο για αυτό. Εδώ έχουμε ουσιαστικά τον ίδιο αλγόριθμο υπογραφής, να δρα και ως αλγόριθμος προσομοίωσης.

Η παραπάνω ιδέα μας επιτρέπει να γενικεύσουμε και να ορίσουμε με φυσικό τρόπο το τι σημαίνει μια υπογραφή δακτυλίου καθορισμένου επαληθευτή. Στο δακτύλιο θα έχουμε έναν αριθμό από μέλη-υπογράφοντες και ένα μέλος-επαληθευτή. Ο επαληθευτής βλέποντας μια υπογραφή θα γνωρίζει ότι προέρχεται από κάποιον από τους υπογράφοντες, εφόσον δεν είναι δικιά του. Από την άλλη οι υπογράφοντες βλέποντας μια υπογραφή δε μπορούν, λόγω της ανωνυμίας, να ξεχωρίσουν αν προέρχεται από κάποιο άλλο υπογράφοντα, ή από τον επαληθευτή.

Αυτή η σχέση είχε ήδη επισημανθεί από τους αρχικούς δημιουργούς των υπογραφών δακτυλίου[62]. Σημειώνουμε όμως ότι υπάρχουν και δουλειές εξειδικευμένες σε αυτού του είδους τις υπογραφές, προσφέροντας διάφορες παραλλαγές και επιπλέον λειτουργίες, όπως π.χ. [44, 45, 72].

6.2 Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή

Η φυσική σχέση των DVS με τις RS, δεν υφίσταται αν προσπαθήσουμε να εισάγουμε την ιδιότητα της συνδεσιμότητας. Αυτό συμβαίνει γιατί όλες οι προσομοιώσεις του καθορισμένου επαληθευτή, θα έχουν σε αυτή τη περίπτωση το ίδιο ψευδώνυμο. Για να πείσει κάποιον τρίτο ότι μια υπογραφή είναι γνήσια, και όχι δικιά του προσομοίωση, αρκεί να αποκαλύψει ποιο είναι το ψευδώνυμο του. Όλες οι υπογραφές που έχουν διαφορετικό ψευδώνυμο από το δικό του, προέρχονται αναγκαστικά από κάποιο μέλος του δακτυλίου. Οπότε η κατασκευή μιας DVLRS δεν είναι τόσο απλή.

Πριν προχωρήσουμε στη παρουσίαση του μοντέλου και της κατασκευή μας θα αναφερθούμε σύντομα σε προηγούμενες προσπάθειες. Μια ενδιαφέρουσα δουλειά[49], εισάγει την έννοια των υπογραφών δακτυλίου με καθορισμένη συνδεσιμότητα. Πρόκειται για συνδέσιμες υπογραφές δακτυλίου, στις οποίες όμως ο αλγόριθμος σύνδεσης, δε μπορεί να χρησιμοποιηθεί από τον οποιαδήποτε. Ενώ οι υπογραφές είναι δημόσια επαληθεύσιμες, μόνο ένας καθορισμένος επαληθευτή μπορεί να αναγνωρίσει τα ψευδώνυμα και να ξέρει αν δύο υπογραφές προέρχονται από τον ίδιο χρήστη. Αυτό είναι τελείως διαφορετικό από τη δουλειά μας, όμως λόγο του παρεμφερούς ονόματος μπορεί κανείς να συγχύσει τις δύο έννοιες. Μια πιο σχετική δουλειά, παρουσιάζει Συνδέσιμες Υπογραφές Δακτυλίου Ισχυρά Καθορισμένου Επαληθευτή[25]. Σε αντίθεση με τη δικιά μας δουλειά, η υπογραφή τους έχει ισχυρά καθορισμένου επαληθευτή, δηλαδή δεν είναι δημόσια επαληθεύσιμη όπως η δικιά μας. Επιπλέον, πετυχαίνουν μόνο υπολογιστική μη-μεταφερσιμότητα, σε αντίθεση με το δικό μας σχήμα που επιτυγχάνει τέλεια μη-μεταφερσιμότητα. Τέλος, δεν δίνουν μοντέλο, ή αποδείξεις ασφάλειας.

6.2.1 Μοντέλο DVLRS

Ορισμός 6.1. *Ένα σχήμα υπογραφών DVLRS είναι μία επτάδα* PPT *αλγορίθμων (*Setup, KGen, Sign, `Sim`, Vrfy, `Extract`, Link*):*

- *Αρχικοποίηση: αρχικοποιεί τις παραμέτρους του σχήματος, όπως είναι ομάδες, γεννήτορες και ο χώρος των πιθανών μηνυμάτων.*
  $\mathtt{params} \leftarrow \mathsf{Setup}(\lambda)$

- *Δημιουργία Κλειδιών: για κάθε χρήστη, συμπεριλαμβανομένου του καθορισμένου επαληθευτή, δημιουργεί ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού.*
  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(\mathtt{params})$

- *Υπογραφή: με είσοδο το ιδιωτικό κλειδί του υπογράφοντα* sk_π*, το δημόσιο κλειδί του επαληθευτή* pk_D*, έναν υποδακτύλιο* L *και το μήνυμα* $\mathtt{m}$ *επιστρέφει την υπογραφή.*
  $\sigma \leftarrow \mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pk}_\pi)$

- *Προσομοίωση: με είσοδο το ιδιωτικό και το δημόσιο κλειδί του επαληθευτή* $\mathsf{sk}_D, \mathsf{pk}_D$*, έναν υποδακτύλιο* L*, ένα ψευδώνυμο* pid *και το μήνυμα* $\mathtt{m}$ *επιστρέφει μια μη διακρίσιμη υπογραφή με ψευδώνυμο* pid*.*
  $\sigma \leftarrow \mathtt{Sim}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$

- *Εξαγωγή: με είσοδο μια υπογραφή* σ *επιστρέφει το ψευδώνυμο* pid*.*
  $\mathsf{pid} \leftarrow \mathtt{Extract}(\sigma)$

- *Επαλήθευση: επιστρέφει 1 αν η υπογραφή είναι έγκυρη και 0 αν δεν είναι.*
  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\sigma, L, \mathtt{m}, \mathsf{pk}_D)$

- *Σύνδεση: με είσοδο δύο υπογραφές από τον ίδιο δακτύλιο* L*, επιστρέφει 1 αν προέρχονται από τον ίδιο υπογράφοντα, ή είναι προσομοιωμένες έτσι ώστε να φαίνεται ότι προέρχονται από τον ίδιο υπογράφοντα.*
  $\{0, 1\} \leftarrow \mathsf{Link}(\sigma, L, \sigma')$

Σε όλους τους παραπάνω αλγορίθμους, και γενικά σε όλο το κεφάλαιο, η παράμετρος ασφάλειας 1^λ, θεωρείτε πάντα μέρος της εισόδου. Συνήθως την παραλείπουμε για συντομία. Το ίδιο ισχύει για τις δημόσιες παραμέτρους του συστήματος $\mathtt{params}$.

Η συνάρτηση εξαγωγής επιστρέφει το ψευδώνυμο που περιέχεται σε κάθε υπογραφή σ. Για υπογραφές που είναι αποτέλεσμα του αλγορίθμου υπογραφής, το pid θα προέρχεται με κάποιο τρόπο από ιδιωτικό κλειδί του υπογράφοντα. Για τις προσομοιώσεις, η εξαγωγή θα πρέπει να επιστρέφει το pid που χρησιμοποιήθηκε ως είσοδος στην προσομοίωση για να παραχθεί η σ.

Για την συνάρτηση επαλήθευσης, έγκυρη πρέπει να είναι κάθε υπογραφή έχει προκύψει από τον αλγόριθμο υπογραφής, αλλά και κάθε υπογραφή που έχει προκύψει από τον αλγόριθμο προσομοίωσης. Ορίζουμε τυπικά τη παρακάτω ιδιότητα ορθότητας.

Ορισμός 6.2 (Ορθότητα Επαλήθευσης). *Αν* $\sigma \leftarrow \mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk})$ *με* $\mathsf{sk} \in L$ *ή* $\sigma \leftarrow \mathtt{Sim}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$ *με* $(\mathsf{sk}_D, \mathsf{pk}_D) \leftarrow \mathsf{KGen}()$*, τότε θα πρέπει* $\mathsf{Vrfy}(\sigma, L, \mathtt{m}, \mathsf{pk}_D) = 1$*. Αλλιώς* $\mathsf{Vrfy}(\sigma, L, \mathtt{m}, \mathsf{pk}_D) = 0$ *με συντριπτική πιθανότητα.*

Αντίστοιχα πρέπει να ορίσουμε και την ορθότητα για τον αλγόριθμο σύνδεσης. Όπως και στο προηγούμενο κεφάλαιο (5.3), περιορίζουμε την συνδεσιμότητα σε

υπογραφές που αφορούν τον ίδιο υποδακτύλιο L. Η βασική διαφορά εδώ είναι ότι πρέπει να εξασφαλίσουμε ότι οι προσομοιώσεις είναι μη διακρίσιμες από τις κανονικές υπογραφές. Για να το καταφέρουμε αυτό θα πρέπει ο αλγόριθμος σύνδεσης να μη προδίδει πότε μια υπογραφή είναι προσομοίωση. Θα πρέπει δηλαδή, ο αλγόριθμος σύνδεσης να επιστρέφει ναι, και σε κάποιες περιπτώσεις όπου η είσοδος του είναι μια υπογραφή σ και μια προσομοίωση σ'. Αυτό το καταφέρνουμε δίνοντας ως είσοδο στον αλγόριθμο προσομοίωσης το ψευδώνυμο pid. Έτσι αν ο επαληθευτής έχει δει ένα ψευδώνυμο, μπορεί, χωρίς φυσικά να γνωρίζει σε ποιον ανήκει αυτό το ψευδώνυμο, να κατασκευάσει μια προσομοιώσεις που να συνδέονται με όλες τις υπογραφές που έχουν αυτό το ψευδώνυμο. Αντίθετα ο αλγόριθμος δεν έχει αυτή την επιλογή, αφού για τον υπογράφοντα η συνδεσιμότητα είναι μη προαιρετική, και συνεπώς το ψευδώνυμο του θα πρέπει διαισθητικά να προέρχεται με κάποιον τρόπο από το ιδιωτικό κλειδί του. Ο επαληθευτής φυσικά θα πρέπει πρώτα να έχει δει τουλάχιστον μια υπογραφή με ένα συγκεκριμένο ψευδώνυμο για να μπορέσει να κατασκευάσει τις προσομοιώσεις του. Αυτό αρχικά μπορεί να φανεί ως μεγάλο μειονέκτημα, αλλά πρακτικά αυτό μπορεί να λυθεί απαιτώντας από όλους τους χρήστες να υπογράφουν ένα ακίνδυνο μήνυμα εγγραφής στην αρχή, ώστε να έχει ο επαληθευτής μια λίστα με όλα τα ψευδώνυμα στην διάθεση του. Τέλος, σημειώνουμε ότι δεν έχει νόημα να μιλάμε για τη συνδεσιμότητα μη έγκυρων υπογραφών. Σε αυτή τη περίπτωση η έξοδος του αλγόριθμου σύνδεσης στερείται σημασίας.

Ορισμός 6.3 (Ορθότητα Σύνδεσης). $\mathsf{Link}(\sigma, L, \sigma') = 1$ *αν και μόνο αν ισχύει ένα από τα παρακάτω:*

1. $\sigma \leftarrow \mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$ *KAI* $\sigma' \leftarrow (L, \mathtt{m}', \mathsf{pk}'_D, \mathsf{sk}_\pi)$
2. $\sigma \leftarrow \mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$ *KAI* $\sigma' \leftarrow \mathtt{Sim}(L, \mathtt{m}', \mathsf{pk}'_D, \mathsf{sk}'_D, \mathtt{Extract}(\sigma))$
3. $\sigma \leftarrow \mathtt{Sim}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$ *KAI* $\sigma' \leftarrow (L, \mathtt{m}', \mathsf{pk}'_D, \mathsf{sk}'_D, \mathsf{pid})$

6.2.2 Ιδιότητες Ασφάλειας

Οι ιδιότητες ασφάλειας που θα απαιτήσουμε, είναι συνδυασμός αυτών των LRS και των DVS. Στη συνέχεια θα ορίσουμε και θα εξηγήσουμε τις τέσσερις απαιτούμενες ιδιότητες: μη-πλαστογραφησιμότητα, ανωνυμία, συνδεσιμότητα και μη-μεταφερσιμότητα. Οι ορισμοί των ιδιοτήτων βασίζονται σε αυτές των σχημάτων από τα οποία της κληρονομούν, με μερικές όμως σημαντικές διαφορές, που προκύπτουν από την αλληλεπίδραση των ιδιοτήτων μεταξύ τους. Πριν όμως προχωρήσουμε στις ιδιότητες, θα αναλύσουμε τις δυνατότητες που υποθέτουμε ότι έχει ο αντίπαλος $\mathcal{A}$.

Δυνατότητες του Αντίπαλου

Για να ορίσουμε τις ιδιότητες ασφαλείας υποθέτουμε έναν αντίπαλο $\mathcal{A}$ που προσπαθεί να τις παραβιάσει. Υποθέτουμε ότι είναι ένα δυνατός προσαρμοστικός

αντίπαλος, με τη δυνατότητα να προσθέτει χρήστες στο σύστημα, να υποκλέβει τα ιδιωτικά κλειδιά χρηστών της επιλογής του, τα ζητάει υπογραφές και προσομοιώσεις από χρήστες και με παραμέτρους της επιλογής του και με πρόσβαση σε όλα τα υπογεγραμμένα μηνύματα που έχουν ανταλλαχθεί από την αρχικοποίηση του συστήματος. Για όλες τις ιδιότητες εκτός από την μη-μεταφερσιμότητα, υποθέτουμε ότι ο αντίπαλος $\mathcal{A}$ είναι PPT.

Για να μοντελοποιήσουμε αυτές τις δυνατότητες, δίνουμε στον $\mathcal{A}$ πρόσβαση στα εξής μαντεία:

- *Μαντείο Εγγραφής*: Εισάγει ένα καινούριο δημόσιο κλειδί pk στη λίστα με όλα τα δημόσια κλειδιά του συστήματος $\mathcal{U}$.
  $\mathsf{pk} \leftarrow \mathcal{GO}()$

- *Μαντείο Διαφθοράς*: Με είσοδο ένα δημόσιο κλειδί $\mathsf{pk} \in \mathcal{U}$, επιστρέφει το ιδιωτικό κλειδί sk που του αντιστοιχεί.
  $\mathsf{sk} \leftarrow \mathcal{CO}(\mathsf{pk})$

- *Μαντείο Υπογραφής*: Με είσοδο έναν δακτύλιο L, ένα μήνυμα $\mathtt{m}$, το δημόσιο κλειδί του επαληθευτή pk_D και το δημόσιο κλειδί του υπογράφοντα pk_π, επιστρέφει την υπογραφή που προκύπτει από τον αλγόριθμο υπογραφής με αυτές τις παραμέτρους, αλλά με το αντίστοιχο ιδιωτικό κλειδί sk_π που αντιστοιχεί στο pk_π.
  $\sigma \leftarrow \mathcal{SO}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pk}_\pi)$

- *Μαντείο Προσομοίωσης*: Με είσοδο έναν δακτύλιο L, ένα μήνυμα $\mathtt{m}$, το δημόσιο κλειδί του επαληθευτή pk_D και ένα ψευδώνυμο pid επιστρέφει την προσομοίωση που προκύπτει από τον αλγόριθμο προσομοίωσης για αυτές τις εισόδους αλλά με το αντίστοιχο ιδιωτικό κλειδί του επαληθευτή sk_D.
  $\sigma \leftarrow \mathtt{Sim}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pid})$

Επιπλέον των παραπάνω μαντείων, έχει πρόσβαση και σε οποιαδήποτε συνάρτηση σύνοψης χρησιμοποιείται στο σχήμα. Στο μοντέλο τις συναρτήσεις σύνοψης τις μοντελοποιούμε με ένα τυχαίο μαντείο $\mathcal{RO}$.

Οφείλουμε να διευκρινίσουμε, ότι ο αντίπαλος έχει πρόσβαση σε όλα τα υπογεγραμμένα μηνύματα, σαν αυτά να είναι δημοσιευμένα σε κάποια δημόσια βάση δεδομένων. Δεν μπορεί να παρακολουθεί το δίκτυο και να βρίσκει την προέλευση των υπογραφών ή άλλα παρόμοια στοιχεία. Τέτοιου είδους επιθέσεις θα μπορούσαν τετριμμένα να παραβιάσουν ιδιότητες όπως η ανωνυμία, και είναι εκτός του αντικειμένου του σχεδιασμού μια ψηφιακής υπογραφής. Επιπλέον, πρέπει να υποθέσουμε ότι ο εκάστοτε καθορισμένος επαληθευτής, ακολουθεί κάποια στρατηγική παραπλάνησης του αντιπάλου. Αν οι προσομοιώσεις που δημιουργεί ακολουθούν κάποιο προβλέψιμο μοτίβο, αυτό μπορεί να δώσει ένα πλεονέκτημα σε έναν αντίπαλο που προσπαθεί να διακρίνει προσομοιώσεις από γνήσιες υπογραφές. Ακόμα και σε αυτή τη περίπτωση όμως δε θα μπορούσε ποτέ να τις ξεχωρίσει με απόλυτη βεβαιότητα.

Μη-Πλαστογραφησιμότητα

Όπως σε κάθε σχήμα ψηφιακών υπογραφών, η πρωταρχική μας απαίτηση είναι να μην μπορούν να υπάρξουν πλαστογραφίες. Επιτρέπεται δηλαδή να παράγουν έγκυρες υπογραφές μόνο όποιος γνωρίζει είτε το ιδιωτικό κλειδί που αντιστοιχεί σε ένα από τα δημόσια κλειδιά του υποδακτυλίου L, είτε το ιδιωτικό κλειδί του καθορισμένου επαληθευτή. Για τον ορισμό χρησιμοποιούμε το παιχνίδι 6.1.

Παιχνίδι 6.1: Πείραμα Μη-Πλαστογραφησιμότητας $\mathtt{Exp}^{UnfDVLRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$\mathtt{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(\sigma, L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, pk_D, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
επέστρεψε $\mathsf{Vrfy}(\sigma, L, \mathtt{m}, \mathsf{pk}_D)$ **ΚΑΙ** σ δεν είναι έξοδος των $\mathcal{SO}, \mathcal{MO}$ **ΚΑΙ** $\forall i \in D_t : \mathsf{pk}_i \notin L$ **ΚΑΙ** $D \notin D_t$

Το πείραμα λειτουργεί ως εξής: το σύστημα αρχικοποιείται με τις παραμέτρους $\mathtt{params}$ ανάλογα με την παράμετρο ασφάλειας λ και η λίστα των κλειδιών αρχικοποιείται με n κλειδιά. Έπειτα ο $\mathcal{A}$ μπορεί να ρωτήσει όλα τα μαντεία ό,τι ερωτήσεις θέλει με βάση οποιαδήποτε προσαρμοστική στρατηγική της αρεσκείας του. Με D_t συμβολίζουμε τον δείκτη των κλειδιών που ο $\mathcal{A}$ αποφάσισε να υποκλέψει με το $\mathcal{CO}$. Στο τέλος επιστρέφει μια υπογραφή σ, για υποδακτύλιο L, μήνυμα $\mathtt{m}$ και επαληθευτή pk_D, όλα της επιλογής του. Νικάει το παιχνίδι αν η υπογραφή είναι έγκυρη, και δεν είναι έξοδος των μαντείων $\mathcal{SO}$ ή $\mathcal{MO}$, και δεν έχει διαφθείρει κανένα από τα κλειδιά του L ή του επαληθευτή. Οι τελευταίες απαιτήσεις είναι λογικές, αφού με τις εξόδους των μαντείων η νίκη του θα ήταν τετριμμένα εύκολη, και το ίδιο θα ίσχυε αν ήξερε κάποιο από τα ιδιωτικά κλειδιά που θα μπορούσαν τίμια να παράξουν την υπογραφή.

Ορισμός 6.4 (Μη-Πλαστογραφησιμότητα). *Ένα DVLRS σχήμα Π είναι μη-πλαστογραφήσιμο αν για κάθε* PPT *αντίπαλο $\mathcal{A}$:*

$$Pr[\mathtt{Exp}^{UnfDVLRS}_{\mathcal{A},\Pi,n}(\lambda)] \leq \mathsf{negl}(\lambda)$$

Ο ορισμός μας αντιστοιχεί στην ισχυρή ιδιότητα ασφάλειας της μη-πλαστογραφησιμότητα με υποκλοπή κλειδιών των [12], προσαρμοσμένη όμως για την ύπαρξη του καθορισμένου επαληθευτή.

Ανωνυμία

Η ανωνυμία είναι η απαίτηση να μη μπορεί κανείς να βρει την ταυτότητα του δημιουργού μιας υπογραφής. Φυσικά πάντα ένας αντίπαλος θα μπορεί να μαντέψει εντελώς τυχαία ανάμεσα σε όλα τα μέλη του δακτυλίου, οπότε η πιθανότητα επιτυχίας δε θα είναι ποτέ αμελητέα, αλλά αμελητέα κοντά στην τυχαία

μαντεψιά. Πρακτικά, τα μέλη του δακτυλίου, θέλουν να μην μπορεί να μάθει την ταυτότητα τους ούτε ο καθορισμένος επαληθευτής, και συνεπώς για αυτόν τον ορισμό επιτρέπουμε στον αντίπαλο ελεύθερα να υποκλέψει το κλειδί του επαληθευτή. Ορίζουμε την ανωνυμία τυπικά με βάση το παιχνίδι 6.2.

Παιχνίδι 6.2: Πείραμα Υπολογιστικής Ανωνυμίας $\mathtt{Exp}^{AnonDVLRS}_{\mathcal{A},\Pi,n,t}$

Είσοδος: λ
Έξοδος: $\{0,1\}$

$\mathtt{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, \mathsf{pk}_D, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{GO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow\$ [n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$
$(\xi, D_t') \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{GO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(L, \mathtt{m}, \mathsf{pk}_D, \sigma, D_t, \textbf{εικασία})$
Αν $\pi \notin D_t'$ **τότε**
  επέστρεψε $\xi = \pi$
αλλιώς
  επέστρεψε $\perp$

Σε αυτό το πείραμα το μαντείο υπογραφής $\mathcal{SO}$, διαφέρει από τον ορισμό που δώσαμε προηγούμενος. Για την ανωνυμία, λόγω της συνδεσιμότητας, αν ο αντίπαλος μπορούσε να επιλέγει ένα δημόσιο κλειδί για να του επιστραφεί μια υπογραφή με το αντίστοιχο ιδιωτικό κλειδί, αυτό θα ισοδυναμούσε με το να μάθει το ψευδώνυμο που αντιστοιχεί σε αυτό το κλειδί. Κάτι τέτοιο θα του έδινε προφανώς τη δυνατότητα να σπάσει την ανωνυμία. Θα μπορούσαμε να γεμίσουμε τον ορισμό με συνθήκες που να μην επιτρέπουν αυτή τη τετριμμένη επίθεση, αλλά είναι πολύ πιο απλό να τροποποιήσουμε το μαντείο, μόνο για αυτόν το ορισμό, ώστε να επιλέγει ένα από τα κλειδιά του L της εισόδου του τυχαία, αντί για να διαλέγει ο αντίπαλος.

Στο πείραμα, αρχικοποιούνται οι παράμετροι, και ο $\mathcal{A}$ δρα σε δύο φάσεις. Στη φάση της **επιλογής**, αφού καλέσει όλα τα μαντεία με όποια στρατηγική επιθυμεί, επιλέγει έναν υποδακτύλιο $L \subseteq \mathcal{U}$, ένα μήνυμα $\mathtt{m}$, έναν καθορισμένο επαληθευτή pk_D, έχοντας υποκλέψει κάποια κλειδιά με δείκτες στο D_t. Το σύστημα διαλέγει τυχαία έναν χρήστη από τον L και παράγει την αντίστοιχη υπογραφή. Έτσι ξεκινάει η φάση της **εικασίας**, όπου ο αντίπαλος έχει πάλι πρόσβαση στα μαντεία, και αφού τα συμβουλευτεί με τη στρατηγική της αρεσκείας του, επιστρέφει τελικά τη μαντεψιά του για την ταυτότητα του υπογράφοντα. Με D_t' συμβολίσαμε το σύνολο των δεικτών που έχει υποκλέψει ο αντίπαλος μετά τη δεύτερη φάση. Προφανώς $D_t' \supseteq D_t$. Ο $\mathcal{A}$ νικάει αν μαντέψει σωστά.

Η επιλογή μας να περιορίσουμε την συνδεσιμότητα, σε υπογραφές που αφορούν τον ίδιο υποδακτύλιο L, διευκολύνει λίγο τον ορισμό, αφού καθιστά μη χρήσιμες επιθέσεις όπως αυτή όπου ο αντίπαλο ζητάει από το $\mathcal{SO}$ υπογραφές για τετριμμένους υποδακτυλίους με ένα μόνο κλειδί. Αν δεν περιορίζαμε την συνδεσιμότητα,

αυτό θα έδινε άμεσα στον αντίπαλο το ψευδώνυμο του μοναδικού χρήστη του υποδακτυλίου. Βέβαια σε ένα τέτοιο σύστημα, κανένας πραγματικός χρήστης δε θα δεχόταν ποτέ να υπογράψει οτιδήποτε για έναν υποδακτύλιο χωρίς κανέναν άλλο χρήστη. Όμως, αν έστω και μια φορά υπέγραφε σε κάποιον υποδακτύλιο όπου όλα τα άλλα μέλη ήταν υπό τον έλεγχο του αντιπάλου, τότε θα αποκάλυπτε το ψευδώνυμο του για κάθε άλλη υπογραφή που είχε παράξει ποτέ, και θα έχανε την ανωνυμία του.

Ορισμός 6.5 (Ανωνυμία). *Ένα DVLRS σχήμα είναι t-ανώνυμο αν για κάθε* PPT *αντίπαλο $\mathcal{A}$:*

$$Pr[\mathtt{Exp}^{AnonDVLRS}_{\mathcal{A},\Pi,n,t}(\lambda)] \leq \frac{1}{n_L - t} + \mathsf{negl}(\lambda)$$

Ο ορισμός μας εδώ αντιστοιχεί στην υπολογιστική ανωνυμία, αφού ο αντίπαλος είναι υπολογιστικά φραγμένος (PPT).

Συνδεσιμότητα

Η συνδεσιμότητα απαιτεί αν δύο υπογραφές ως προς τον ίδιο δακτύλιο L προέρχονται από τον ίδιο υπογράφοντα ο αλγόριθμος σύνδεσης να επιστρέφει 1. Συνεπώς κανείς δε πρέπει, γνωρίζοντας μόνο το δικό του ιδιωτικό κλειδί να παράγει δύο υπογραφές που να μην συνδέονται. Επιπλέον θέλουμε ακόμα και αν κάποιος έχει στη κατοχή του παραπάνω από ένα κλειδί, έστω k, δε θα πρέπει να μπορεί να παράγει πάνω από k μεταξύ τους μη συνδεδεμένες υπογραφές. Ο ορισμός αυτό συνεπάγεται και την ιδιότητα της μη-δυσφημισιμότητας. Δείτε και την αντίστοιχη παράγραφο στην ενότητα 5.3.3. Η συνδεσιμότητα, σε σχέση με ένα απλό σχήμα LRS, είναι πιο περίπλοκη με την εισαγωγή του καθορισμένου επαληθευτή, αφού οφείλουμε να του επιτρέψουμε να παράγει υπογραφές συνδεδεμένες με οποιουδήποτε χρήστη. Ορίζουμε την ιδιότητα με βάση το παιχνίδι 6.3.

Παιχνίδι 6.3: Πείραμα Συνδεσιμότητας $\mathtt{Exp}^{LinkDVLRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathtt{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(\{\sigma_i\}_{i=1}^{k}, L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \{\mathtt{m}_i\}_{i=1}^{k}, \{\mathsf{pk}_{D_i}\}_{i=1}^{k}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
επέστρεψε $\mathsf{Vrfy}(\sigma_i, L, \mathtt{m}_i)\ \forall i \in [k]$ **ΚΑΙ**
$\mathsf{Link}(\sigma_i, L, \sigma_j) = 0\ \forall i, j \in [k],\ i \neq j$ **ΚΑΙ**
$|\{pk_i : i \in D_t\} \cap L| < k$ **ΚΑΙ**
σ_i δεν είναι έξοδος των $\mathcal{SO}, \mathcal{MO}\ \forall i \in [k]$ **ΚΑΙ**
$D_i \notin D_t\ \forall i \in [k]$

Στο πείραμα, αφού αρχικοποιηθούν οι παράμετροι και κάποια αρχικά κλειδιά, ο αντίπαλο $\mathcal{A}$ έχοντας στη διάθεση του όλα τα μαντεία, προσπαθεί να κατασκευάσει περισσότερες από τα κλειδιά που γνωρίζει, ανά δύο μη συνδεδεμένες έγκυρες

υπογραφές. Αυτό μπορεί να το επιχειρήσει στον δακτύλιο της επιλογής του, για μηνύματα και καθορισμένους επαληθευτές επίσης της επιλογής του. Φυσικά δεν μπορεί να επιστρέψει τις ίδιες τις εξόδους των μαντείων $\mathcal{SO}, \mathcal{MO}$, ούτε και να θέσει ως κλειδί του επαληθευτή pk_D κάποιο από τα κλειδιά που έχει υποκλέψει, αφού με αυτό το τρόπο θα νικούσε τετριμμένα. Αυτό συμβαίνει, διότι από το σχεδιασμό των DVLRS, επιτρέπουμε στον καθορισμένο επαληθευτή να προσομοιώνει υπογραφές με όποιο ψευδώνυμο θέλει.

Ορισμός 6.6 (Συνδεσιμότητα). *Ένα DVLLRS σχήμα Π είναι συνδέσιμο αν για κάθε* PPT *αντίπαλο $\mathcal{A}$:*

$$Pr[\mathtt{Exp}^{LinkDVLRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$$

Μη-Μεταφερσιμότητα

Η μη-μεταφερσιμότητα είναι η ιδιότητα που διαισθητικά εξασφαλίζει ότι μια υπογραφή είναι χρήσιμη μόνο για τον προοριζόμενο παραλήπτη, δηλαδή τον καθορισμένο επαληθευτή. Αυτό το πετυχαίνουμε απαιτώντας ένας αντίπαλος να μη μπορεί να ξεχωρίσει μια υπογραφή από μια προσομοίωση που έχει παράγει ο ίδιος ο επαληθευτής. Ορίζουμε τη μη-μεταφερσιμότητα μέσα από το παιχνίδι 6.4.

Παιχνίδι 6.4: Πείραμα Τέλειας Μη-Μεταφερσιμότητας $\mathtt{Exp}^{TransDVLRS}_{\mathcal{A},\Pi}$

Είσοδος: λ
Έξοδος: $\{0, 1\}$

$\mathtt{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$\mathcal{U} \leftarrow \{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pk}_\pi) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO}}(\mathcal{U}, \textbf{επιλογή})$
$\sigma_0 \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pk}_\pi)$
$\mathsf{pid}_0 \leftarrow \Pi.\mathtt{Extract}(\sigma_0)$
$\sigma_1 \leftarrow \Pi.\mathtt{Sim}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid}_0)$
$b \leftarrow\$ \{0, 1\}$
$b' \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO}}(L, \mathtt{m}, \mathsf{pk}_D, \sigma_b, \textbf{εικασία})$
επέστρεψε $b = b'$

Σε αυτό το πείραμα ο αντίπαλος $\mathcal{A}$ μπορεί να είναι υπολογιστικά μη φραγμένος. Για αυτόν τον λόγο δε χρειάζεται να του δώσουμε πρόσβαση στα μαντεία $\mathcal{CO}, \mathcal{SO}$ και $\mathcal{MO}$, αφού μπορεί με την υπολογιστική του δύναμη να αντιστρέψει όλα τα δημόσια κλειδιά, και να παράγει μόνος του όσες υπογραφές και προσομοιώσεις επιθυμεί. Στη πρώτη φάση επιλέγει έναν υποδακτύλιο L, ένα μήνυμα $\mathtt{m}$, ένα δημόσιο κλειδί επαληθευτή pk_D και έναν χρήστη του δακτυλίου pk_π. Το σύστημα στη συνέχεια παράγει μια υπογραφή και μια προσομοίωση που να μοιάζουν να προέρχονται από αυτόν τον χρήστη. Για να μπορεί να γίνει η προσομοίωση πρέπει πρώτα να παραχθεί η υπογραφή, ώστε να μπορέσει να εξαχθεί το ψευδώνυμο της pid_0 και να χρησιμοποιηθεί στην προσομοίωση. Το σύστημα διαλέγει τυχαία να

δώσει στον $\mathcal{A}$ είτε την υπογραφή σ_1 είτε την προσομοίωση σ_2. Έπειτα ο $\mathcal{A}$ προσπαθεί στη φάση της **εικασίας** να διακρίνει τι από τα δύο έλαβε. Αν μαντέψει σωστά νικάει το παιχνίδι.

Ορισμός 6.7 (Τέλεια Μη-Μεταφερσιμότητα). *Ένα DVLRS σχήμα Π είναι τέλεια μη-μεταφέρσιμο αν για κάθε μη φραγμένο αντίπαλο $\mathcal{A}$:*

$$Pr[\mathtt{Exp}^{TransDVLRS}_{\mathcal{A},\Pi}(\lambda) = 1] = \frac{1}{2}$$

Επειδή ο αντίπαλος στη χειρότερη περίπτωση μπορεί να μαντέψει τελείως τυχαία, και να επιτύχει με πιθανότητα $\frac{1}{2}$, αυτή είναι η πιθανότητα επιτυχίας που του επιτρέπουμε. Επειδή δεν είναι υπολογιστικά φραγμένος, δεν αρκεί η πιθανότητα επιτυχίας να είναι αμελητέα κοντά, αλλά πρέπει να είναι ακριβώς ίση με $\frac{1}{2}$.

Θα μπορούσαμε να είχαμε ορίσει την μη-μεταφερσιμότητα και με έναν πιο γενικό τρόπο. Αντί για τον αντίπαλο να ορίζει έναν συγκεκριμένο χρήστη ως προς τον οποίο το σύστημα θα παράγει την πρόκληση, θα μπορούσε να γίνετε ομοιόμορφα τυχαία επιλογή ενός χρήστη $\pi \leftarrow\$ [n_L]$ και ενός pid ώστε να παράγει την υπογραφή $\sigma_0 \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$ και την προσομοίωση $\sigma_2 \leftarrow \Pi.\mathtt{Sim}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$. Κάτι τέτοιο δεν είναι όμως αναγκαίο για να καλύψουμε το τι σημαίνει διαισθητικά για μια υπογραφή να είναι μη-μεταφέρσιμη.

6.2.3 Κατασκευή

Η κατασκευή μας, δανείζεται ιδέες από το σχήμα LRS των [50] και το σχήμα DVS των [41], ώστε να έχουμε μια υπογραφή με όλες τις ιδιότητες που ορίσαμε παραπάνω. Ουσιαστικά ο αλγόριθμος υπογραφής παίρνει ως είσοδο το δημόσιο κλειδί του καθορισμένου επαληθευτή, δίνοντας του έτσι μια καταπακτή ώστε να δημιουργεί πανομοιότυπες προσομοιώσεις. Εναλλακτικά μπορούμε να σκεφτούμε τη κατασκευή ως μια μη διαλογική απόδειξη μηδενικής γνώσης (Γ΄), της πρότασης ¨Γνωρίζω το ιδιωτικό κλειδί ενός μέλους του δακτυλίου Ή γνωρίζω το ιδιωτικό κλειδί του καθορισμένου επαληθευτή¨. Αν το πρώτο κομμάτι της διάζευξης είναι αληθές, τότε έχουμε μια κανονική υπογραφή, ενώ αν το δεύτερο κομμάτι είναι αληθές, τότε έχουμε μια προσομοιωμένη υπογραφή.

Αρχικοποίηση

Δουλεύουμε σε μια ομάδα $\mathbb{G}$ τάξης πρώτου q,με γεννήτορα g, όπου υποθέτουμε ότι ισχύει η υπόθεση DDH. Κάθε χρήστης, είτε δρα ως υπογράφοντας είτε ως καθορισμένος επαληθευτής, έχει στη διάθεση του ένα ζεύγος κλειδιών, ώστε $\mathsf{sk}_i = x_i \in \mathbb{Z}_q$ και $\mathsf{pk}_i = y_i = g^{x_i} \in \mathbb{G}$. Τα ψευδώνυμα είναι επίσης στοιχεία της ομάδας, δηλαδή $\mathsf{pid}_i \in \mathbb{G}$. Ως μήνυμα μπορούμε να έχουμε οποιαδήποτε συμβολοσειρά $\mathtt{m} \in \{0,1\}^*$. Τέλος θα χρειαστούμε δύο τυχαία μαντεία $\mathsf{H}_q, \mathsf{H}_{\mathbb{G}}$ που απεικονίζουν συμβολοσειρές στη $\mathbb{G}$ και στο $\mathbb{Z}_q$ αντίστοιχα. Όποτε τα μαντεία θα δέχονται ως είσοδο στοιχεία της $\mathbb{G}$ και του $\mathbb{Z}_q$ θεωρούμε ότι δέχονται την αναπαράσταση τους σε συμβολοσειρά.

Υπογραφή

Ένας υπογράφοντας με ζεύγος κλειδιών (x_π, y_π), επιλέγει ένα μήνυμα $\mathtt{m}$, έναν υποδακτύλιο $L = \{y_i\}_{i=1}^{n_L} \subseteq \mathcal{U}$ με δημόσια κλειδιά με $y_\pi \in L$, και το δημόσιο κλειδί του επαληθευτεί $y_D \notin L$ που επιθυμεί να καθορίσει. Το π είναι ο δείκτης του κλειδιού του υπογράφοντα στον L.

Αλγόριθμος Υπογραφής: $\mathsf{Sign}(L, \mathtt{m}, y_D, x_\pi)$	
1 :	$h \leftarrow \mathsf{H}_{\mathbb{G}}(L)$
2 :	$\hat{y} \leftarrow h^{x_\pi}$
3 :	$u, w_\pi, r_\pi \leftarrow\$ \mathbb{Z}_q$
4 :	$c_{\pi+1} \leftarrow \mathsf{H}_q(L, \hat{y}, y_D, g^u, h^u, g^{w_\pi} y_D^{r_\pi}, \mathtt{m})$
5 :	Για $i \in \{\pi+1, \ldots, n_L, 1, \ldots, \pi-1\}$
	$s_i, w_i, r_i \leftarrow\$ \mathbb{Z}_q$
	$c_{i+1} \leftarrow \mathsf{H}_q(L, \hat{y}, y_D, g^{s_i} y_i^{c_i+w_i}, h^{s_i} \hat{y}^{c_i+w_i}, g^{w_i} y_D^{r_i}, \mathtt{m})$
6 :	$s_\pi \leftarrow u - (c_\pi + w_\pi) x_\pi$
7 :	Επέστρεψε $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \hat{y})$

Προσομοίωση

Ένας καθορισμένος επαληθευτής με ζεύγος κλειδιών (x_D, y_D), επιλέγει ένα μήνυμα $\mathtt{m}$, έναν υποδακτύλιο $L = \{y_i\}_{i=1}^{n_L} \subseteq \mathcal{U}$ με δημόσια κλειδιά με $y_D \notin L$ και το ψευδώνυμο $\hat{y} \in \mathbb{G}$ που επιθυμεί.

Αλγόριθμος Προσομοίωσης: $\mathtt{Sim}(L, \mathtt{m}, y_D, x_D, \hat{y})$	
1 :	$h \leftarrow \mathsf{H}_{\mathbb{G}}(L)$
2 :	$a, \beta, s_1 \leftarrow \mathbb{Z}_q$
3 :	$c_2 \leftarrow \mathsf{H}_q(L, \hat{y}, y_D, g^{s_1} y_1^{\beta}, h^{s_1} \hat{y}^{\beta}, g^a, \mathtt{m})$
4 :	Για $i \in \{2, \ldots, n_L\}$
	$s_i, w_i, r_i \leftarrow\$ \mathbb{Z}_q$
	$c_{i+1} \leftarrow \mathsf{H}_q(L, \hat{y}, y_D, g^{s_i} y_i^{c_i+w_i}, h^{s_i} \hat{y}^{c_i+w_i}, g^{w_i} y_D^{r_i}, \mathtt{m})$
5 :	$w_1 \leftarrow \beta - c_1$ και $r_1 \leftarrow (a - w_1) \cdot x_D^{-1}$
6 :	Επέστρεψε $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \hat{y})$

Εξαγωγή

Ο αλγόριθμος εξαγωγής είναι εξαιρετικά απλός στη κατασκευή μας. Η υπογραφές είναι πλειάδες στοιχείων όπου το τελευταίο στοιχείο είναι το ψευδώνυμο. Οπότε:

$$\hat{y} \leftarrow \mathtt{Extract}(\sigma)$$

Επαλήθευση

Ο αλγόριθμος επαλήθευσης δέχεται ως είσοδο μια υπογραφή σ, το μήνυμα $\mathtt{m}$, τον υποδακτύλιο $L \subseteq \mathcal{U}$ και το δημόσιο κλειδί του καθορισμένου επαληθευτή y_D ως προς τα οποία έχει κατασκευαστεί η υπογραφή.

Αλγόριθμος Επαλήθευσης: $\mathsf{Vrfy}(\sigma, L, \mathtt{m}, y_D)$	
1 :	$h \leftarrow \mathsf{H}_{\mathbb{G}}(L)$
2 :	Για $i \in [n_L]$
	$z'_i \leftarrow g^{s_i} y_i^{c_i + w_i}$
	$z''_i \leftarrow h^{s_i} \hat{y}^{c_i + w_i}$
	$z'''_i \leftarrow g^{w_i} y_D^{r_i}$
	$c_{i+1} \leftarrow \mathsf{H}_q(L, \hat{y}, y_D, z'_i, z''_i, z'''_i, \mathtt{m})$
3 :	Επέστρεψε $c_1 = \mathsf{H}_q(L, \hat{y}, y_D, z'_n, z''_n, z'''_n, \mathtt{m})$

Σύνδεση

Ο αλγόριθμος σύνδεσης προκύπτει άμεσα από τον αλγόριθμο εξαγωγής. Για είσοδο δύο έγκυρες υπογραφές σ, σ' για τον ίδιο υποδακτύλιο L, ο $\mathsf{Link}(\sigma, L, \sigma')$ επιστρέφει 1 αν και μόνο αν:

$$\mathtt{Extract}(\sigma) = \mathtt{Extract}(\sigma')$$

6.2.4 Ορθότητα και Πληρότητα

Θα δείξουμε ότι η κατασκευή μας ικανοποιεί όλες τις απαραίτητες ιδιότητες πληρότητας και ορθότητα. Συγκεκριμένα θα δείξουμε ότι κάθε υπογραφή που δημιουργείτε με βάση τον αλγόριθμο υπογραφής είναι έγκυρη, ότι κάθε προσομοίωση που δημιουργείτε με βάση τον αλγόριθμο προσομοίωσης είναι έγκυρη, και ότι ικανοποιείται η ορθότητα σύνδεσης.

Λήμμα 6.1. *Μια τίμια κατασκευασμένη DVLRS υπογραφή σ, είναι έγκυρη.*

Απόδειξη. Αρκεί να δείξουμε ότι $z'_\pi = g^u$ και $z''_\pi = h^u$. Πράγματι:

$$\begin{aligned} z_\pi &= g^{s_\pi} y_i^{c_\pi + w_\pi} = g^{u - x_\pi(c_\pi + w_\pi)} y_\pi^{c_\pi + w_\pi} = g^u \\ z''_\pi &= h^{s_\pi} \hat{y}^{c_\pi + w_\pi} = h^{u - x_\pi(c_\pi + w_\pi)} \hat{y}^{c_\pi + w_\pi} = h^u \end{aligned}$$

□

Λήμμα 6.2. *Μια τίμια προσομοιωμένη DVLRS υπογραφή σ, είναι έγκυρη.*

Απόδειξη. Αρκεί να δείξουμε ότι $z'_1 = g^{s_1} y_1{}^{\beta}$ και $z''_1 = h^{s_1} \hat{y}^{\beta}$ και $z'''_1 = g^a$. Πράγματι:

$$\begin{aligned} z'_1 &= g^{s_1} y_1^{c_1 + w_1} = g^{s_1} y_1^{c_1 + \beta - c_1} = g^{s_1} y_1^{\beta} \\ z''_1 &= h^{s_1} \hat{y}^{c_1 + w_1} = h^{s_1} \hat{y}^{c_1 + \beta - c_1} = h^{s_1} \hat{y}^{\beta} \\ z'''_1 &= g^{w_1} y_D^{r_1} = g^{w_1} g^{x_D (a - w_1) x_D^{-1}} = g^a \end{aligned}$$

□

Λήμμα 6.3. *Η DVLRS κατασκευή μας έχει ορθότητα σύνδεσης.*

Απόδειξη. Θα πρέπει να δείξουμε ότι ο αλγόριθμος σύνδεσης επιστρέφει 1 και στις τρεις περιπτώσεις που οφείλει.

Περίπτωση 1: Αν σ, σ' προέρχονται από τον αλγόριθμο υπογραφής, από τον ίδιο υπογράφοντα, για τον ίδιο δακτύλιο L έχουμε ότι $\texttt{Extract}(\sigma) = \hat{y} = h^{x^\pi} = \texttt{Extract}(\sigma')$

Περίπτωση 2: Αν σ υπογραφή, και σ προσομοίωση με $\hat{y} = \texttt{Extract}(\sigma)$ έχουμε ότι $\texttt{Extract}(\sigma) = \hat{y} = \texttt{Extract}(\sigma)$.

Περίπτωση 3: Αν σ, σ' προσομοιώσεις με το ίδιο ψευδώνυμο $\hat{y}$ τότε προφανώς $\texttt{Extract}(\sigma) = \hat{y} = \texttt{Extract}(\sigma)$. □

6.2.5 Ανάλυση Ασφάλειας

Στη συνέχεια θα αποδείξουμε για τη κατασκευή μας ότι ικανοποιεί όλες τις ιδιότητες ασφάλειας, δηλαδή είναι μη-πλαστογραφήσιμη, ανώνυμη, συνδέσιμη, και τέλεια μη-μεταφέρσιμη. Οι αποδείξεις είναι στο μοντέλο τυχαίου μαντείου $\mathcal{RO}$ (B′).

Μη-Πλαστογραφησιμότητα

Θεώρημα 6.1. *Το DVLRS σχήμα μας είναι μη-πλαστογραφήσιμο στο μοντέλο $\mathcal{RO}$ αν ισχύει η υπόθεση* DLOG *στη* $\mathbb{G}$.

Η απόδειξη μας χρησιμοποιεί τεχνικές από τους [40, 48, 50, 60].

Απόδειξη. Για την απόδειξη, θα υποθέσουμε ότι υπάρχει ένας PPT αντίπαλο $\mathcal{A}$ που μπορεί με μη αμελητέα πιθανότητα να πλαστογραφήσει μια υπογραφή. Θα δείξουμε ότι σε αυτή τη περίπτωση μπορούμε να κατασκευάσουμε έναν αλγόριθμο $\mathcal{M}$ που χρησιμοποιεί τον $\mathcal{A}$ ως υπορουτίνα για να λύσει το DLP. Ο $\mathcal{M}$ θα έχει ως είσοδο έναν γεννήτορα $g \in \mathbb{G}$ και n_0 το πλήθος στοιχεία της ομάδας για τα οποία θέλει να βρει τον διακριτό λογάριθμο. Θα δείξουμε ότι μπορεί να λύσει τουλάχιστον έναν από τους διακριτούς λογάριθμους, δηλαδή αν $\{y_i\}_{i=1}^{n_0}$ θα βρει x_j τ.ω. $g_j^x = y_j$ για $j \in [n_0]$.

Εφόσον ο $\mathcal{A}$ είναι PPT, υποθέτουμε ότι κάνει το πολύ q_{H} ερωτήσεις στα μαντεία H_q και $\mathsf{H}_{\mathbb{G}}$ αθροιστικά, και το πολύ q_O ερωτήσεις στα μαντεία $\mathcal{JO}, \mathcal{CO}, \mathcal{SO}\,\mathcal{MO}$ αθροιστικά. Ο $\mathcal{M}$ θέτει ως παραμέτρους του σχήματος τα $\mathbb{G}, g$ και ως αρχικά κλειδιά $\mathcal{U} \leftarrow \{y_i\}_{i=1}^{n_0}$. Για να μπορεί να χρησιμοποιήσει τον $\mathcal{A}$ ως υπορουτίνα θα πρέπει να μπορεί να απαντάει στα ερωτήματα του $\mathcal{A}$ στα μαντεία. Μπορεί να προσομοιώσει όλα τα μαντεία ως εξής:

- H_q: επιστρέφει $r \leftarrow\$ \mathbb{Z}_q$.
- $\mathsf{H}_{\mathbb{G}}$: υπολογίζει $r \leftarrow\$ \mathbb{Z}_q$ και επιστρέφει το g^r.
- $\mathcal{JO}$: υπολογίζει $r \leftarrow\$ \mathbb{Z}_q$ και εισάγει το g^r στο $\mathcal{U}$.

– $\mathcal{CO}$: για κλειδιά $y_j \notin \{y_i\}_{i=1}^{n_0}$ επιστρέφει r_j τ.ω. $g^{r_j} = y_j$. Αλλιώς σταματάει την εκτέλεση για $y_j \in \{y_i\}_{i=1}^{n_0}$.

– $\mathcal{SO}$: Ο $\mathcal{A}$ δίνει στον $\mathcal{M}$, $L \subseteq \mathcal{U}$, ένα μήνυμα $\mathtt{m}$, κλειδί υπογράφοντα $y_\pi \in L$ και κλειδί επαληθευτή $y_D \in \mathcal{U} \setminus L$. Έστω ότι $\mathsf{H}_{\mathbb{G}}(L) = h = g^r$. Για κλειδιά $y_\pi \notin \{y_i\}_{i=1}^{n_0}$ ο $\mathcal{M}$ γνωρίζει το r_π τ.ω $g^{r_\pi} = y_\pi$ οπότε επιστρέφει τη $\sigma \leftarrow \mathsf{Sign}(L, \mathtt{m}, y_D, r_\pi)$. Αλλιώς επιλέγει τυχαία $\{c_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \{s_i\}_{i=1}^{n_L} \leftarrow\$ \mathbb{Z}_q$ και υπολογίζει $\hat{y} \leftarrow g^r$. Για κάθε $i \in [n_L]$ θέτει:

$$c_{i+1} \leftarrow \mathsf{H}_q(L, \hat{y}, y_D, g^{s_i} y_i^{c_i+w_i}, h^{s_i} \hat{y}^{c_i+w_i}, g^{w_i} y_D^{r_i}, \mathtt{m})$$

και επιστρέφει $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \hat{y})$.

– $\mathcal{MO}$: Ο $\mathcal{A}$ δείνει στον $\mathcal{M}$, $L \subseteq \mathcal{U}$, ένα μήνυμα $\mathtt{m}$, κλειδί επαληθευτή $y_D \in \mathcal{U} \setminus L$ και ψευδώνυμο $\hat{y} \in \mathbb{G}$. Έστω ότι $\mathsf{H}_{\mathbb{G}}(L) = h = g^r$. Για κλειδιά $y_D \notin \{y_i\}_{i=1}^{n_0}$ ο $\mathcal{M}$ γνωρίζει το r_D τ.ω $g^{r_D} = y_D$ οπότε επιστρέφει τη $\sigma \leftarrow \mathtt{Sim}(L, \mathtt{m}, y_D, r_D, \hat{y})$. Αλλιώς επιλέγει τυχαία $\{c_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \{s_i\}_{i=1}^{n_L} \leftarrow\$ \mathbb{Z}_q$ και υπολογίζει $\hat{y} \leftarrow g^r$. Για κάθε $i \in [n_L]$ θέτει:

$$c_{i+1} \leftarrow \mathsf{H}_q(L, \hat{y}, y_D, g^{s_i} y_i^{c_i+w_i}, h^{s_i} \hat{y}^{c_i+w_i}, g^{w_i} y_D^{r_i}, \mathtt{m})$$

και επιστρέφει $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \hat{y})$.

Φυσικά σε περίπτωση που ξαναεμφανιστεί κάποιο ερώτημα για δεύτερη φορά, ο $\mathcal{M}$ απαντάει με τον ίδιο τρόπο, κρατώντας τη συνέπεια ανάμεσα στις απαντήσεις των μαντείων. Παρατηρούμε ότι από την πλευρά του $\mathcal{A}$, δε μπορεί να ξεχωρίσει αν αλληλεπιδρά με τον $\mathcal{M}$ ή με τα πραγματικά μαντεία.

Θα υποθέσουμε χωρίς βλάβη της γενικότητας ότι μια επιτυχής πλαστογραφία θα έχει $L \subseteq \{y_i\}_{i=1}^{n_0}$ και $y_D \in \{y_i\}_{i=1}^{n_0}$. Μπορούμε επίσης να υποθέτουμε ότι για να επιστρέψει ο $\mathcal{A}$ μια επιτυχημένη πλαστογραφία, θα πρέπει να έχει καλέσει τα μαντεία H_q και $\mathsf{H}_{\mathbb{G}}$ για όλες τις εισόδους που εμφανίζονται στον αλγόριθμο επαλήθευσης. Πράγματι αν δεν το είχε κάνει, τότε η υπογραφή δε θα ήταν έγκυρη μέχρι κάποιος να καλέσει το μαντείο και να κλειδώσει η τιμή του. Η πιθανότητα να συμβεί αυτό και να προκύψει έγκυρη υπογραφή είναι προφανώς $\mathsf{negl}(\lambda)$. Κάθε ένα από τα n_L ερωτήματα που εμφανίζεται στον αλγόριθμο επαλήθευσης, θα εμφανίζεται για πρώτη φορά στη ταινία του $\mathcal{A}$ σε κάποιο σημείο. Συμβολίζουμε τα ερωτήματα στο H_q με τη σειρά πρώτης εμφάνισης τους ως $\{X_i\}_{i=i_1}^{i_{n_L}}$. Θα αποκαλούμε την σ μια επιτυχημένη (l, π)-πλαστογραφία αν $i_1 = l$ και

$$X_{i_{n_L}} = \mathsf{H}_q(L, \hat{y}, y_D, g^{s_{\pi-1}} y_{\pi-1}^{c_{\pi-1}+w_{\pi-1}}, h^{s_{\pi-1}} \hat{y}^{c_{\pi-1}+w_{\pi-1}}, g^{w_{\pi-1}} y_D^{r_{\pi-1}}, \mathtt{m})$$

□

Διαισθητικά μια (l, π)-πλαστογραφία, είναι μια πλαστογραφία που το πρώτο ερώτημα εμφανίζεται στη θέση l της ταινίας και το τελευταίο ερώτημα που έκλεισε τον δακτύλιο, ήταν σαν να προήλθε από τον υπογράφοντα στη θέση π. Η πιθανότητα ο $\mathcal{A}$ να επιστρέψει μια (l, π)-πλαστογραφία είναι μη αμελητέα για κάποιο

ζεύγος (l, π), αφού $1 \leq l \leq q_{\mathsf{H}} + n_L q_O$ και $1 \leq \pi \leq n_L$. Για κάθε τιμή των l και π ο $\mathcal{M}$ θα τρέχει τον $\mathcal{A}$ και θα ελέγχει αν έλαβε μια (l, π)-πλαστογραφία. Αν όχι, σταματάει, Αν ναι, κάνει επαναφορά του $\mathcal{A}$ στο l ερώτημα. Από το Λήμμα της Επαναφοράς στην Επιτυχία[50] (βλ. και Παράρτημα Β΄), θα έχουμε με μη αμελητέα πιθανότητα δύο (l, π)-πλαστογραφίες σ, σ' με:

$$g^u = g^{s_\pi} y_\pi^{c_\pi + w_\pi} = g^{s_\pi + x_\pi(c_\pi + w_\pi)} \tag{6.1}$$

$$h^v = h^{s_\pi} \hat{y}^{c_\pi + w_\pi} = h^{s_\pi + x(c_\pi + w_\pi)} \tag{6.2}$$

$$g^\nu = g^{w_\pi} y_D^{r_\pi} = g^{w_\pi + x_D \cdot r_\pi} \tag{6.3}$$

$$g^u = g^{s'_\pi} y_\pi^{c'_\pi + w'_\pi} = g^{s'_\pi + x_\pi(c'_\pi + w'_\pi)} \tag{6.4}$$

$$h^v = h^{s'_\pi} \hat{y}^{c'_\pi + w'_\pi} = h^{s'_\pi + x(c'_\pi + w'_\pi)} \tag{6.5}$$

$$g^\nu = g^{w'_\pi} y_D^{r'_\pi} = g^{w'_\pi + x_D \cdot r'_\pi} \tag{6.6}$$

Επειδή $c_\pi \neq c'_\pi$, θα ισχύει είτε ότι $s_\pi \neq s'_\pi$ είτε ότι $w_\pi \neq w'_\pi \wedge r_\pi \neq r'_\pi$. Στην περίπτωση $s_\pi \neq s'_\pi$ από τις 6.1 και 6.4 έχουμε:

$$x_\pi = \frac{s'_\pi - s_\pi}{c_\pi - c'_\pi + w_\pi - w'_\pi} \mod q$$

Στην περίπτωση $w_\pi \neq w'_\pi \wedge r_\pi \neq r'_\pi$ από τις 6.3και 6.6 έχουμε:

$$x_D = \frac{w'_\pi - w_\pi}{r_\pi - r'_\pi} \mod q$$

Και στις δύο περιπτώσεις ο $\mathcal{M}$ έχει λύσει έναν από τους διακριτούς λογαρίθμους που έχουμε υποθέσει ότι είναι δύσκολοι.

Ανωνυμία

Θεώρημα 6.2. *Το DVLRS σχήμα μας είναι ανώνυμο στο μοντέλο $\mathcal{RO}$ αν ισχύει η υπόθεση DDH στη $\mathbb{G}$.*

Η απόδειξη μας τροποποιεί αυτές των [49, 50] για το σχήμα μας.

Απόδειξη. Υποθέτουμε προς άτοπο ότι υπάρχει ένας PPT αντίπαλος $\mathcal{A}$ που νικάει το Παιχνίδι 6.2 με πιθανότητα ϵ, μη αμελητέα μεγαλύτερη του $\frac{1}{n_L - t}$. Θα κατασκευάσουμε έναν $\mathcal{M}$ που θα χρησιμοποιεί τον $\mathcal{A}$ ως υπορουτίνα και θα λύνει το πρόβλημα DDH. Ο $\mathcal{M}$ θα έχει ως είσοδο ομάδα $\mathbb{G}$, γεννήτορα g και μια τριάδα στοιχείων $A_\beta, B_\beta, C_\beta \in \mathbb{G}$. Για κάποια, άγνωστα στον $\mathcal{M}$, $a, \beta \in \mathbb{Z}_q$ θα ισχύει ότι $A_\beta = g^a, B_\beta = g^b$. Ο $\mathcal{M}$ θα πρέπει να διακρίνει αν $C_\beta = g^{ab}$, ή όχι. Επιστρέφει $\beta = 1$ στην πρώτη περίπτωση και $\beta = 0$ αλλιώς.

Ο $\mathcal{M}$ μπορεί να προσομοιώσει τις απαντήσεις στα μαντεία με τον ίδιο τρόπο όπως στην απόδειξη μη-πλαστογραφησιμότητας (6.2.5), με τις παρακάτω διαφορές: Στην αρχικοποίηση θέτει $\mathcal{U} \leftarrow y_\pi$, όπου $y_\pi = A_\beta$. Σε κάποια κλίση του μαντείου $\mathsf{H}_{\mathbb{G}}$ θα θέσει $h \leftarrow B_\beta$. Όσον αφορά το μαντείο υπογραφής $\mathcal{SO}$, θυμηθείτε ότι για την ανωνυμία λειτουργεί διαφορετικά από ότι στους υπόλοιπους ορισμούς. Οπότε για να προσομοιώσει ένα ερώτημα $\mathcal{SO}(L' = \{y_i\}_{i=1}^{n'_L}, \mathfrak{m}', y_D, y)$:

- Επιλέγει $\pi' \leftarrow\$ [n_{L'}]$
- Αν $\mathsf{H}_{\mathbb{G}}(L) = h \neq B_\beta$ τότε $\hat{y} \leftarrow y_{\pi'}^k$, όπου $h = g^k$
- Αν $\mathsf{H}_{\mathbb{G}}(L) = h = B_\beta$ και $\pi' \neq \pi$ τότε $\hat{y} \leftarrow B_\beta^{x_{\pi'}}$
- Αν $\mathsf{H}_{\mathbb{G}}(L) = h = B_\beta$ και $\pi' = \pi$ τότε $\hat{y} \leftarrow C_\beta$
- Επιλέγει τυχαία $\{c_\pi, s_i, w_i, r_i\}_{i=1}^{n_{L'}} \leftarrow\$ \mathbb{Z}_q$
- Για κάθε $i \in [n_{L'}]$ θέτει:

$$c_{i+1} \leftarrow \mathsf{H}_q(L', \hat{y}, y_D, g^{s_i} y_i^{c_i+w_i}, h^{s_i} \hat{y}^{c_i+w_i}, g^{w_i} y_D^{r_i}, \mathtt{m}')$$

- Επιστρέφει $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \hat{y})$

Ο $\mathcal{M}$ στη φάση της **επιλογής** του 6.2, λαμβάνει τα (L, y_D, D_t) και ελέγχει αν $y_\pi \in L$ και αν $\mathsf{H}_{\mathbb{G}}(L) = B_\beta$, θέτοντας το B_β αν δεν έχει οριστεί ακόμα. Αλλιώς ο αλγόριθμος σταματάει. Στη συνέχεια παράγει την πρόκληση με το τρόπο που προσομοιώνει και το $\mathcal{SO}$, με τη μόνη διαφορά ότι αντί να επιλέξει τυχαία ένα $\pi' \in [n_L]$, θέτει $\pi' \leftarrow \pi$. Με αυτό το τρόπο $y_\pi = A_\beta$ και $\hat{y} = B_\beta$.

Στο επόμενο στάδιο ο $\mathcal{A}$ κάνει πάλι ερωτήσεις στα μαντεία, τις οποίες ο $\mathcal{M}$ απαντάει, εκτός αν γίνει το ερώτημα $\mathcal{CO}(\pi)$ όπου ο ο αλγόριθμος σταματάει. Τέλος ο $\mathcal{A}$ επιστρέφει την **εικασία** του $\xi \in [n_L]$. Αν $\xi = \pi$ επιστρέφει 1, αλλιώς επιστρέφει είτε 1 είτε 0 στη τύχη. Αν $\beta = 1$ η πιθανότητα να απαντήσει ο $\mathcal{A}$ ξ δε μπορεί να είναι μικρότερη από $\frac{1}{n_L - t} + \epsilon$. Αρα:

$$\Pr\Big[\mathcal{M}(A_\beta, B_\beta, C_\beta) = 1 | \beta = 1\Big] \geq (\frac{1}{n_L - t} + \epsilon) + \frac{1}{2}(1 - \frac{1}{n_L - t} - \epsilon) \geq \frac{1}{2} + \frac{1}{2(n_L - t)} + \frac{\epsilon}{2}$$

Αν ισχύει ότι $\beta = 0$ δε θα υπάρχει σχέση ανάμεσα στο ψευδώνυμο και το κλειδί του υπογράφοντα, οπότε η πιθανότητα να πετύχει ο $\mathcal{A}$ δε μπορεί να είναι καλύτερη από τη τυχαία μαντεψιά. Άρα:

$$\Pr\Big[\mathcal{M}(A_\beta, B_\beta, C_\beta) = 0 | \beta = 0\Big] = (\frac{1}{n_L - t}) \cdot 0 + (1 - \frac{1}{n_L - t}) \cdot \frac{1}{2} = \frac{1}{2} - \frac{1}{2(n_L - t)}$$

Συνδυάζοντάς τις παραπάνω σχέσεις έχουμε:

$$\Pr\Big[\mathcal{M}(A_\beta, B_\beta, C_\beta) = \beta\Big] \geq \frac{1}{2} + \frac{\epsilon}{4}$$

Δηλαδή ο $\mathcal{M}$ έχει πιθανότητα επιτυχίας να διακρίνει το DDH μη αμελητέα μεγαλύτερη του $\frac{1}{2}$. □

Συνδεσιμότητα

Θεώρημα 6.3. *Το DVLRS σχήμα μας είναι συνδέσιμο στο μοντέλο $\mathcal{RO}$ αν ισχύει η υπόθεση* DLOG *στη* $\mathbb{G}$.

Χρησιμοποιούμε τεχνικές από τους [40, 50, 60], τροποποιημένες για τον ισχυρότερο ορισμό της συνδεσιμότητας μας.

Απόδειξη. Υποθέτουμε PPT αντίπαλο $\mathcal{A}$ που με μη αμελητέα πιθανότητα νικάει το Παιχνίδι 6.3 κάνοντας το πολύ q_{H} ερωτήσεις στα $\mathsf{H}_{\mathbb{G}}, \mathsf{H}_q$ και το πολύ q_O ερωτήσεις στα $\mathcal{JO}, \mathcal{CO}, \mathcal{SO}, \mathcal{MO}$. Θα κατασκευάσουμε αλγόριθμο $\mathcal{M}$, που με είσοδο μια ομάδα $\mathbb{G}$, γεννήτορα g και n_0 το πλήθος στοιχεία της $\mathbb{G}$, για τα οποία θα βρίσκει τον διακριτό λογάριθμο από τουλάχιστον ένα, χρησιμοποιώντας τον $\mathcal{A}$ σαν υπορουτίνα. Δηλαδή αν $\{y_i\}_{i=1}^{n_0}$ η είσοδος, θα βρίσκει τουλάχιστον ένα x_j τ.ω. $g^{x_j} = y_j$ για $j \in [n_0]$. Ο $\mathcal{M}$ θέτει ως παραμέτρους τα $\mathbb{G}, g$ και αρχικοποιεί το $\mathcal{U} \leftarrow \{y_i\}_{i=1}^{n_0}$. Στις κλήσεις του $\mathcal{A}$ στα μαντεία απαντάει με τον ίδιο τρόπο όπως στην απόδειξη μη-πλαστογραφησιμότητας.

Μετά από μια επιτυχημένη εκτέλεση του $\mathcal{A}$, θα έχει επιστρέψει k έγκυρες υπογραφές $\{\sigma_i\}_{i=1}^{k}$ για τις οποίες θα ισχύει $0 \leftarrow \mathsf{Link}(\sigma_i, \sigma_j)$ για κάθε $i \neq j$. Οι υπογραφές αυτές θα είναι ως προς κάποιον υποδακτύλιο $L \subseteq \mathcal{U}$ της επιλογής του $\mathcal{A}$ για τον οποίο έχει υποκλέψει λιγότερα από k κλειδιά και κανένα από τα κλειδιά των καθορισμένων επαληθευτών $\left\{y_{D_i}\right\}_{i=1}^{k}$. Υποθέτουμε χωρίς βλάβη της γενικότητας, ότι $\left\{y_{D_i}\right\}_{i=1}^{k} \subseteq \{y_i\}_{i=1}^{n_0}$ και $y_i \in L$ για τουλάχιστον ένα $i \in [n_0]$. Όπως και στην απόδειξη μη-πλαστογραφησιμότητας, θεωρούμε ότι όλα τα ερωτήματα που χρησιμοποιούνται στον αλγόριθμο Vrfy έχουν γίνει, και ορίζουμε με τον ίδιο τρόπο μια (l, π)-πλαστογραφία. Συνεπώς για κάθε από τις k υπογραφές του αντιπάλου, θα είναι μια (l_i, π_i)-πλαστογραφία για κάποια $0 \leq l_i \leq q_{\mathsf{H}} + n_L q_O$ και $1 \leq \pi_i \leq n_L$. Μπορούμε να διακρίνουμε δύο περιπτώσεις:

Περίπτωση 1: Ο $\mathcal{A}$ παρήγαγε k υπογραφές με λιγότερα από k διαφορετικά π_i. Αυτό σημαίνει ότι θα υπάρχει τουλάχιστον ένα ζεύγος υπογραφών όπου μία θα είναι (l_a, π)-πλαστογραφία και η άλλη (l_b, π)-πλαστογραφία με το ίδιο π. Μπορούμε να υποθέσουμε χωρίς βλάβη ότι $l_a < l_b$. Ο $\mathcal{M}$ θα κάνει επαναφορά της ταινίας του $\mathcal{A}$ στο l_a ερώτημα, και από το Λήμμα Επιστροφής στην Επιτυχία[48](βλ. Παράρτημα Β΄), θα λάβει με μη αμελητέα πιθανότητα μια υπογραφή σ_a η οπόια θα είναι (l_a, π)-πλαστογραφία. Καταλήγουμε πάλι στις εξισώσεις 6.1,6.2,6.3,6.4,6.5,6.6.

- Αν $s_\pi \neq s'_\pi$: από τις εξισώσεις 6.1, 6.2, 6.4, 6.5 έχουμε:

$$x_\pi = x = \frac{s'_\pi - s_\pi}{c_\pi - c'_\pi + w_\pi - w'_\pi} \mod q$$

- Αν $w_\pi \neq w'_\pi \wedge r_\pi \neq r'_\pi$: από τις εξισώσεις 6.3, 6.6 έχουμε:

$$x_D = \frac{w'_\pi - w_\pi}{r_\pi - r'_\pi} \mod q$$

Αν ο $\mathcal{M}$ βρει το x_D πέτυχε αυτό που ήθελε.

Αν $x = x_\pi$ αυτό σημαίνει ότι $\hat{y_a} = h_\pi^x$. Ο $\mathcal{M}$ κάνει άλλη μια επαναφορά, αυτή τη φορά στο l_b ερώτημα, και με τον ίδιο τρόπο βρίσκει είτε το x_D, ή ισχύει ότι $\hat{y_b} = h_\pi^x$. Αυτό όμως θα σήμαινε ότι $\mathsf{Link}(\sigma_a, L, \sigma_b) = 1$ που είναι άτοπο από την αρχική μας υπόθεση.

Περίπτωση 2: Ο $\mathcal{A}$ παρήγαγε k υπογραφές με k διαφορετικά π_i. Αυτή τη φορά ο $\mathcal{M}$ θα κάνει k επαναφορές, κάθε φορά στο l_i ερώτημα για κάθε $i \in [k]$. Σε κάθε επαναφορά θα βρίσκει είτε το κλειδί του επαληθευτή, είτε ένα από τα κλειδιά του L. Αν βρει έστω και ένα από τα x_{D_i}, ο $\mathcal{M}$ κερδίζει. Αλλιώς θα βρει όλα τα x_i, και επειδή υποθέσαμε ότι τουλάχιστον ένα $x_i \in L$ με $i \in [n_0]$, ο $\mathcal{M}$ πάλι κερδίζει.

□

Μη-Μεταφερσιμότητα

Θεώρημα 6.4. *Το DVLRS σχήμα μας είναι τέλεια μη-μεταφέρσιμο στο μοντέλο $\mathcal{RO}$.*

Απόδειξη. Θα δείξουμε ότι οι κατανομές των εξόδων των αλγορίθμων Sign και Sim, για το ίδιο μήνυμα m, δακτύλιο L, καθορισμένο επαληθευτή y_D και ψευδώνυμο $\hat{y}$ είναι ακριβώς οι ίδιες. Θα κοιτάξουμε κάθε στοιχείο μιας υπογραφής $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \hat{y})$.

Το c_1 είναι έξοδος του τυχαίου μαντείου H_q, με τουλάχιστον ένα κομμάτι της εισόδου του τυχαίο. Συνεπώς το c_1, τόσο για υπογραφές όσο και για προσομοιώσεις, είναι κατανεμημένο ομοιόμορφα τυχαία στο $\mathbb{Z}_q$.

Για μια προσομοίωση όλα τα s_i επιλέγονται τυχαία από το $\mathbb{Z}_q$.Για μια υπογραφή όμως, το $s_\pi \leftarrow u - (c_\pi + w_\pi)x_\pi$. Το u είναι μια τυχαία τιμή στο $\mathbb{Z}_q$, άρα και το s_π είναι κατανεμημένο ομοιόμορφα στο $\mathbb{Z}_q$. Άρα όλα τα s_i είναι κατανεμημένα ομοιόμορφα τυχαία στο $\mathbb{Z}_q$. Με εντελώς ανάλογα επιχειρήματα μπορούμε να δούμε ότι και τα w_i, r_i έχουν την ίδια κατανομή.

Τέλος το ψευδώνυμο $\hat{y}$ θα είναι ακριβώς το ίδιο στοιχείο στην υπογραφή και την προσομοίωση. Συνεπώς δε μπορεί να δώσει κανένα στοιχείο στον $\mathcal{A}$.

Δείξαμε δηλαδή, ότι η υπογραφή σ_0 και η προσομοίωση σ_1 που λαμβάνει ο $\mathcal{A}$ στο Παιχνίδι 6.4 ακολουθούν ακριβώς την ίδια τυχαία κατανομή, συνεπώς είναι αδύνατο ο $\mathcal{A}$ να τις ξεχωρίσει με πιθανότητα καλύτερη από την τυχαία μαντεψιά.

□

ΚΕΦΑΛΑΙΟ 7

Εφαρμογές - Ανώνυμες Εποικοδομητικές Κριτικές

Σε αυτό το κεφάλαιο θα αναλύσουμε την κύρια εφαρμογή που μας οδήγησε στο να εφεύρουμε τις DVLRS[7]. Αυτή είναι ένα ανώνυμο σύστημα εποικοδομητικών κριτικών, που προστατεύουν τον κρινόμενο, αφού οι κριτικές είναι προσωπικά για αυτόν και κανείς άλλος δε μπορεί να πάρει την πληροφορία τους. Για να το πετύχουμε αυτό, απαιτούμε ένα σύστημα υπογραφών που συνδυάζει όλες τις ιδιότητες των DVLRS, δηλαδή την μη-πλαστογραφησιμότητα, την ανωνυμία, τη συνδεσιμότητα και τη μη-μεταφερσιμότητα. Στη συνέχεια θα δούμε ποιες είναι οι απαιτήσεις μας από ένα σύστημα ανώνυμων εποικοδομητικών κριτικών, και πως οι παραπάνω ιδιότητες μας επιτρέπουν να σχεδιάσουμε ένα τέτοιο σύστημα.

Μια κύρια εφαρμογή του συστήματος αφορά το χώρο της εκπαίδευσης. Οι καθηγητές ενός πανεπιστημίου μπορούν να επωφεληθούν πολύ από τις κριτικές των φοιτητών τους, όμως ο κίνδυνος του να αποκαλυφθούν οι πιθανώς κακές κριτικές που έλαβαν, μπορεί να τους κάνει αρνητικούς στο να δεχθούν να συμμετέχουν σε ένα τέτοιο σύστημα. Επιπλέον, θα ήθελαν να μπορούν να ξέρουν αν οι κριτικές προέρχονται από πολλούς διαφορετικούς φοιτητές, ή από μόνο λίγους. Θα δούμε πως οι DVLRS μπορούν να λύσουν αυτά τα προβλήματα.

Φυσικά υπάρχουν και άλλες σημαντικές εφαρμογές των DVLRS. Σε δύο από αυτές θα αναφερθούμε σύντομα στο τέλος του κεφαλαίου, στη διαρροή ενοχοποιητικών μυστικών προς τις αρχές, και στη διενέργεια δημοσκοπήσεων για πολύ ευαίσθητα στοιχεία όπως είναι το ιατρικό ή το οικονομικό ιστορικό.

7.1 Συστήματα Ανώνυμων Εποικοδομητικών Κριτικών

Ας εξετάσουμε πρώτα ποιες είναι οι απαιτήσεις μας. Η πρώτη βασική απαίτηση, είναι να υπάρχει ένα έλεγχος στο ποιος μπορεί να γράψει κριτικές. Για παράδειγμα δεν έχουν νόημα κριτικές προς έναν καθηγητή, από άτομα που δεν είναι φοιτητές του. Αν αυτό που λαμβάνει τις κριτικές είναι ένας διοργανωτής εκδηλώσεων, θα ήθελε να λάβει κριτικές μόνο από όσους πιστοποιημένα έλαβαν μέρος στην εκδήλωση του. Επιπλέον θα ήταν προτιμότερο να μπορεί να το κάνει αυτό για κάθε εκδήλωση που διοργανώνει.

Η δεύτερη απαίτηση, η ανωνυμία, αφορά το συμφέρων των αποστολέων των κριτικών. Η αναγκαιότητα αυτής είναι προφανής. Για να μπορεί μια κριτική να είναι ειλικρινής, δε θα πρέπει ο συντάκτης της να φοβάται ότι μπορεί να υπάρχουν αρνητικές επιπτώσεις για αυτόν, από το δέκτη της κριτικής, ο οποίος μπορεί συχνά να είναι σε θέση ισχύος, όπως είναι ένας καθηγητής και οι φοιτητές του.

Για ένα σύστημα ανώνυμων κριτικών μια πολύ χρήσιμη δυνατότητα είναι το να μπορεί ο λήπτης της κριτικής να ξεχωρίζει πότε μια κριτική προέρχεται από τον ίδιο, ή από διαφορετικούς αποστολείς. Αυτό, όχι μόνο επιτρέπει στους αποστολείς να στέλνουν συμπληρωματικές κριτικές, ή να αντιδρούν με καινούριες κριτικές, σε περίπτωση που κάποιο πρόβλημα που έχουν αναφέρει στο παρελθόν σε κριτική τους, έχει επιλυθεί, αλλά επιτρέπει και στον λήπτη να ξεχωρίζει την περίπτωση όπου υπάρχουν πολλοί δυσαρεστημένοι κριτές, από την περίπτωση όπου ένας πολύ δυσαρεστημένος κριτής στέλνει επαναλαμβανόμενα κακές κριτικές.

Η τελευταία απαίτηση, είναι αυτή που καθιστά το σύστημα μας ουσιαστικά διαφορετικό από ένα συνηθισμένο σύστημα ανώνυμων κριτικών. Απαιτούμε οι κριτικές να είναι προσωπικές για αυτόν τον οποίον αφορούν, και να μην δίνουν καμία πληροφορία σε οποιονδήποτε άλλο. Αυτό προστατεύει τον λήπτη των κριτικών, αφού στη περίπτωση αρνητικών κριτικών, μπορεί να αφοσιωθεί στην αυτοβελτίωση, χωρίς να ανησυχεί ότι οι κριτικές θα έχουν επίπτωση στην δημόσια εικόνα του. Επιπροσθέτως, θα ήθελε να έχει κάποια εγγύηση, ότι ακόμα και αν μελλοντικά κάποιος προϊστάμενος του, των πιέσει να μοιραστεί τις κριτικές που έλαβε, δε θα μπορεί να λάβει κάποια χρήσιμη πληροφορία. Ο τρόπος να το πετύχουμε αυτό, είναι δίνοντας τη δυνατότητα στον λήπτη των κριτικών, να γράφει μόνος του όσες κριτικές θέλει, που να είναι πανομοιότυπες με τις πραγματικές. Αυτή η μέθοδος έχει το επιπλέον πλεονέκτημα για τους κριτές, ότι η ανωνυμία τους όσον αφορά τρίτους παρατηρητές βελτιώνεται, αφού πλέον οι κριτικές τους είναι κρυμμένες όχι μόνο ανάμεσα στις κριτικές άλλων χρηστών, αλλά και ανάμεσα στις ψεύτικες κριτικές του παραλήπτη.

7.1.1 Χρήση των DVLRS

Μπορούμε να σχεδιάσουμε ένα σύστημα ανώνυμων εποικοδομητικών κριτικών ως εξής. Αποφασίζονται οι παράμετροι για ένα σχήμα DVLRS, δηλαδή η ομάδα $\mathbb{G}$ και ο γεννήτορας g, και κάθε χρήστης του συστήματος δημιουργεί ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού. Δημόσια μπορούν να είναι αναρτημένα όλα τα κλειδιά αυτών που πληρούν τις προϋποθέσεις για να αποστείλουν μια κριτική. Ο υποδακτύλιος L, ως προς τον οποίο υπογράφονται οι κριτικές, θα αποτελείται από όλα αυτά τα κλειδιά. Ως κλειδί καθορισμένου επαληθευτή, θέτουμε το κλειδί του παραλήπτη των κριτικών. Το μήνυμα $\mathtt{m}$ σε αυτή τη περίπτωση, θα είναι η κριτική. Οι κριτικές μπορούν να αποστέλωνται στον δημόσιο επαληθευτή, ή ακόμα και να αναρτώνται δημόσια. Οι ιδιότητες των DVLRS είναι σχεδόν άμεσο το πως ευθυγραμμίζονται με τις απαιτήσεις μας για τα συστήματα ανώνυμων εποικοδομητικών κριτικών. Η μη-πλαστογραφησιμότητα εξασφαλίζει ότι μόνο όσοι ανήκουν στον υποδακτύλιο L, δηλαδή όσοι θεωρούμε ότι πληρούν τις όποιες προϋποθέσεις, μπορούν να ασκήσουν κριτική. Αν κάποιος στείλει κριτική ως προς διαφορετικό υποδακτύλιο, ο επαληθευτής μπορεί να την αγνοήσει. Η ανωνυμία των κριτών, καλύπτεται από την ανωνυμία που προσφέρουν οι υπογραφές. Κανένας, συμπεριλαμβανομένου το καθορισμένου επαληθευτή, δε μπορεί να καταλάβει τον πραγματικό αποστολέα μιας κριτικής, ανάμεσα σε όλους τους πιθανούς αποστο-

λείς από τον L. Η συνδεσιμότητα είναι η ιδιότητα που επιτρέπει στον επαληθευτή να αναγνωρίζει αν δύο κριτικές προέρχονται από τον ίδιο χρήστη, ή από διαφορετικούς. Το μόνο που χρειάζεται να κάνει, είναι να ελέγξει τα ψευδώνυμα στις υπογραφές.

Τέλος, επειδή οι DVLRS είναι μη-μεταφέρσιμες, οι κριτικές είναι χρήσιμες μόνο για τον επιδιωκόμενο παραλήπτη. Ο λήπτης των υπογραφών, έχει τη δυνατότητα να δημιουργεί ψεύτικες κριτικές κατά το δοκούν, και με όποιο ψευδώνυμο θέλει. Στην πραγματικότητα, όχι μόνο έχει τη δυνατότητα, αλλά για την ορθή λειτουργία του συστήματος, θα πρέπει να δημιουργεί πολλές ψεύτικες κριτικές, τόσο θετικές αλλά και αρνητικές, ώστε σε οποιονδήποτε άλλο πέρα από τον ίδιο, οι κριτικές να φαίνονται τελείως τυχαίες. Είναι βέβαια επιθυμητό ο επαληθευτής να ακολουθεί κάποια στρατηγική συσκότισης των δεδομένων, ώστε να μην είναι προφανές από το περιεχόμενο ποιες κριτικές είναι γνήσιες και ποιες προσομοιώσεις. Η δυνατότητα του να χρησιμοποιεί αυθαίρετα ψευδώνυμα, του δίνει επιπλέον τη δυνατότητα να κρύψει ακόμα και τον αριθμό των πραγματικών συμμετεχόντων, αφού μπορεί να δημιουργήσει κριτικές με περισσότερα ψευδώνυμα από αυτά που αντιστοιχούν στον χρήστες του L. Το γεγονός ότι η μη-μεταφερσιμότητα είναι τέλεια, και όχι απλά υπολογιστική, έχει το επιπλέον πλεονέκτημα, ότι ακόμα και ένας μελλοντικός αντίπαλος, που ίσως να μπορεί να σπάσει τις παραδοχές του συστήματος και να μάθει όλα τα ιδιωτικά κλειδιά, δε θα μπορεί να ξεχωρίσει τις γνήσιες υπογραφές από τις προσομοιώσεις, και συνεπώς δε θα μπορεί να λάβει κάποια χρήσιμη πληροφορία.

Η περίπτωση της εκπαιδευτικής δομής

Ας δούμε συγκεκριμένα πως εφαρμόζονται τα παραπάνω στη περίπτωση μια εκπαιδευτικής δομής, όπως είναι ένα πανεπιστήμιο. Θα μπορούσαν όλα τα μέλη του ιδρύματος, τόσο οι φοιτητές, όσο και το διδακτικό προσωπικό να έχουν όλοι από ένα ζεύγος κλειδιών. Η εφαρμογή αυτού είναι σίγουρα πραγματοποιήσιμη στο χώρο ενός πανεπιστημίου, ήδη όλοι έχουν στη διάθεση τους ηλεκτρονικούς λογαριασμούς και ιδρυματικές διευθύνσεις ηλεκτρονικού ταχυδρομείου. Οι εγγεγραμμένοι φοιτητές ενός μαθήματος θα αποτελούν κάθε φορά τον υποδακτύλιο L ως προς τον οποίο θα υπογράφονται οι κριτικές. Ως επαληθευτή, θα καθορίζουν τον καθηγητή που διδάσκει το μάθημα. Ο καθηγητής θα μπορεί να λαμβάνει τις κριτικές ανώνυμα, ενώ παράλληλα θα δημοσιεύει και τις δικές του προσομοιωμένες κριτικές. Επιπλέον, αν για παράδειγμα αλλάξει η διοίκηση του ιδρύματος, ή αποφασιστούν περικοπές, και ο καθηγητής δεχθεί πίεση από τους ανωτέρους του ακόμα και να τους αποκαλύψει του ιδιωτικό του κλειδί, δε θα έχει κανένα πρόβλημα, λόγω των προσομοιώσεων που θα αποκρύπτουν τις πραγματικές κριτικές.

Λόγω των ψευδώνυμων, ο καθηγητής έχει τη δυνατότητα να διαχωρίσει αν κάποιο παράπονο αφορά μεγάλη μερίδα των φοιτητών του, ή αν κάποιος δυσανάλογα δυσαρεστημένος φοιτητής, στέλνει συνεχώς αρνητικές κριτικές. Επιπροσθέτως, μπορεί να βλέπει πως η γνώμη των φοιτητών αλλάζει με τη πάροδο του

χρόνου, αφού μπορεί ένας φοιτητής που αρχικά να έχει κάνει αρνητική κριτική, να στείλει νέα κριτική που να δηλώνει ότι το πρόβλημα του επιλύθηκε, ή το αντίθετο. Ο καθηγητής μπορεί ακόμα και να απευθύνει δημόσια, προς ένα συγκεκριμένο ψευδώνυμο, διευκρινιστικές ερωτήσεις, κάνοντας το σύστημα πιο διαδραστικό.

Το σύστημα είναι αρκετά ευέλικτο, αφού δε χρειάζεται να δημιουργούνται εκ νέου καινούρια κλειδιά για κάθε καθηγητή ή κάθε μάθημα. Επιπλέον, αν και οι διοικητικοί υπάλληλοί διαθέτουν ζεύγη κλειδιών, μπορεί για παράδειγμα οι φοιτητές να αποστέλλουν ανώνυμες εποικοδομητικές κριτικές και προς τα μέλη της γραμματείας.

΄Αλλες Εφαρμογές

Αναφέρουμε σύντομα δύο ακόμα πιθανές εφαρμογές. Η μια από αυτές είναι η διαρροή μυστικών, που ήταν και μια από τις πρώτες εφαρμογές των απλών υπογραφών δακτυλίου[62]. Οι DVLRS σε αυτή τη περίπτωση βελτιώνουν την ανωνυμία ενός εσωτερικού πληροφοριοδότη, που θέλει για παράδειγμα να αποκαλύψει στις αρχές πληροφορίες για μια εγκληματική οργάνωση. Σε αυτή τη περίπτωση μπορεί να χρησιμοποιήσει τις DVLRS, επιβεβαιώνοντας ότι είναι κάποιος με πληροφορίες εκ των έσω, αλλά παραμένοντας ανώνυμος. Οι αρχές παρότι δε μπορούν να χρησιμοποιήσουν την υπογραφή του ως αποδεικτικό στοιχείο, αφού θα μπορούσαν να την έχουν παράξει μόνοι τους, μπορούν όμως να πάρουν κάποια σημαντική πληροφορία που να βοηθήσει στην έρευνα τους. Ο πληροφοριοδότης είναι ασφαλής αφού, η εγκληματική οργάνωση, δε μπορεί καν να είναι σίγουρη ότι υπήρξε κάποια διαρροή, πόσο μάλλον από ποιον ακριβώς προήλθε.

Η δεύτερη εφαρμογή είναι οι ανώνυμες δημοσκοπήσεις για ευαίσθητα δεδομένα. Χρησιμοποιώντας τις DVLRS, χρήστες μπορούν να δίνουν πληροφορίες, όπως για παράδειγμα του ιατρικού ιστορικού τους, για να βοηθήσουν την ιατρική έρευνα. Αυτές οι πληροφορίες, παρότι δε μπορούν να χρησιμοποιηθούν σε κάποια δημοσίευση, μπορούν όμως να βοηθήσουν πρακτικά την ιατρική έρευνα, προστατεύοντας όμως την ανωνυμία των ασθενών απόλυτα, αφού δε οι προσομοιώσεις που μπορεί να δημιουργήσει ο καθορισμένος επαληθευτής, θα κρύβουν πλήρως το πραγματικό ιστορικό.

ΚΕΦΑΛΑΙΟ 8

Επίλογος και Μελλοντικές Κατευθύνσεις

Η εισαγωγή μας του νέου είδους ψηφιακών υπογραφών, των DVLRS, ανοίγει τους ορίζοντες για πολλές μελλοντικές δουλειές. Αρχικά, είναι ζητούμενο να υλοποιήσουμε προγραμματιστικά, αλλά και πρακτικά, το σύστημα επικοικοδομιτκών κριτικών που αναλύσαμε στο κεφάλαιο 8. Δεύτερον, θα θέλαμε να φτιάξουμε καινούριες κατασκευές, που θα έχουν βελτιωμένη ασφάλεια, λειτουργικότητα και αποδοτικότητα σε σχέση με το πρώτη κατασκευή DVLRS που παρουσιάσαμε. Συγκεκριμένα, το σχήμα μας έχει υπογραφές με μέγεθος που εξαρτάται γραμμικά με το μέγεθος του υποδακτυλίου L, πράγμα που τις καθιστά μη πρακτικές για μεγάλους υποδακτυλίους. Σκοπεύουμε να προσαρμόσουμε τις τεχνικές των [5, 71], για να κατασκευάσουμε υπογραφές σταθερού μεγέθους. Μια άλλη κατεύθυνση, είναι η κατασκευή υπογραφών που πετυχαίνουν τέλεια ανωνυμία [48], σε σχέση με τη κατασκευή μας που έχει μόνο υπολογιστική ανωνυμία.

Μια άλλη ενδιαφέρουσα προοπτική, είναι να τροποποιήσουμε τον ορισμό της μη-μεταφερσιμότητας ώστε να επιτρέπει στους υπογράφοντες, αλλά μόνο αυτούς, να αποκηρύσσουν αν το θέλουν τις προσομοιώσεις, αποδεικνύοντας ότι είναι πράγματι, προσομοιώσεις. Αυτό θα ανοίξει το δρόμο για νέες εφαρμογές των DVLRS.

ΠΑΡΑΡΤΗΜΑ Α΄

Μαθηματικό Υπόβαθρο

Σε αυτό το παράρτημα θα παρουσιάσουμε μερικές βασικές γνώσεις θεωρίας ομάδων και θεωρίας αριθμών. Θα αρκεστούμε μόνο στις ελάχιστες γνώσεις που κρίνονται απαραίτητες για την κατανόηση των κεφαλαίων του κυρίου μέρους της ΔΕ. Βασιστήκαμε σε μεγάλο βαθμό στα αντίστοιχα κεφάλαια/παραρτήματα των [37, 67, 69]. Για μια πιο εκτενή ματιά στο ίδιο υλικό, από μαθηματική σκοπιά, προτείνουμε το [35].

Α΄.1 Θεωρία Αριθμών

Θεωρία αριθμών είναι ο κλάδος των μαθηματικών που ασχολείται με τους ακέραιους αριθμούς και τις ιδιότητες τους.

Α΄.1.1 Διαιρετότητα

Θεώρημα 1.1 (Ευκλείδεια Διαίρεση). *Για κάθε ζεύγος ακεραίων (a, b) με $b \neq 0$, υπάρχουν μοναδικοί ακέραιοι (q, r) ώστε:*

$$a = bq + r$$

με $0 \leq r < |b|$

Αν $r = 0$ τότε λέμε ότι ο b διαιρεί τον a.

Ορισμός 1.1 (Πράξη Modulo). *Για κάθε ζεύγος ακεραίων (a, b) με $b \neq 0$, ορίζουμε τη πράξη modulo ως*

$$a \mod b = r$$

όπου ο αριθμός r προκύπτει από τον ορισμός της Ευκλείδειας Διαίρεσης. Ισοδύναμα

$$a \mod b = a - \lfloor \frac{a}{b} \rfloor b$$

Παράδειγμα 1.1.

$$10 \mod 3 = 1$$

$$5 \mod 3 = 2$$

$$2n \mod 2 = 0$$

Ορισμός 1.2 (Πρώτος Αριθμός). *Ένας φυσικός αριθμός $n > 1$, ονομάζεται πρώτος αν*

$$n \mod m \neq 0$$

για κάθε $m \in \mathbb{N} \setminus \{1, n\}$. Αν ένας φυσικός αριθμός $n \neq 1$ δεν είναι πρώτος, τότε λέμε ότι είναι σύνθετος.

Παράδειγμα 1.2. *Οι πρώτοι δέκα πρώτοι αριθμοί:* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$

Θεώρημα 1.2 (Ευκλείδης). *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Απόδειξη. Έστω ότι υπάρχουν πεπερασμένοι το πλήθος πρώτοι αριθμοί. Τότε θα υπάρχει ένας πρώτος, έστω n που θα είναι ο μέγιστος. Ο αριθμός q που προκύπτει πολλαπλασιάζοντας όλους τους πρώτους μέχρι το n και προσθέτοντάς 1, δηλαδή $q = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot n + 1$. Ο αριθμός q είναι μεγαλύτερος του n άρα δε μπορεί να είναι πρώτος. Άρα υπάρχει ένας πρώτος που διαιρεί το q. Κανένας όμως από τους πρώτους μέχρι το n δε μπορεί να διαιρεί το q. □

Θεώρημα 1.3 (Θεμελιώδες Θεώρημα της Αριθμητικής). *Κάθε φυσικός αριθμός μεγαλύτερος της μονάδας, αναλύεται σε γινόμενο πρώτων παραγόντων κατά μοναδικό τρόπο.*

Απόδειξη. *Ύπαρξη*: Το ζητούμενο ισχύει για τον αριθμό 2, αφού είναι πρώτος. Ας υποθέσουμε ότι το ζητούμενο ισχύει για όλους τους αριθμούς μικρότερους του n. Αν ο n είναι πρώτος, τότε ισχύει και για τον n. Αν ο n είναι σύνθετος, τότε $n = k \cdot m$ για φυσικούς $1 < k \leq m < n$. Από την επαγωγική υπόθεση $k = p_1 \cdot p_2 \cdot \ldots \cdot p_i$ και $m = q_1 \cdot q_2 \cdot \ldots \cdot q_j$. Άρα $n = k = p_1 \cdot p_2 \cdot \ldots \cdot p_i \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_j$.

Μοναδικότητα: Ας υποθέσουμε ότι ο n είναι ο μικρότερος αριθμός που έχει δύο διαφορετικές αναλύσεις σε πρώτους παράγοντες:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_i = q_1 \cdot q_2 \cdot \ldots \cdot q_j$$

Παρατηρούμε ότι όλοι οι παράγοντες πρέπει να είναι διαφορετικοί μεταξύ τους, αλλιώς ο n δε θα ήταν ο μικρότερος αριθμός με αυτή την ιδιότητα. Θέτουμε $P = p_2 \cdot \ldots \cdot p_i$ και $Q = q_2 \cdot \ldots \cdot q_j$. Συνεπώς:

$$n = p_1 \cdot P = q_1 \cdot Q \implies$$

$$(p_1 - q_1)Q = p_1(P - Q)$$

Άρα είτε ο p_1 διαρεί το $p_1 - q_1$, πράγμα αδύνατο αφού οι p_1, q_1 είναι πρώτοι, είτε ο p_1 διαιρεί το Q. Όμως $Q < n$ και η ανάλυση του σε πρώτες παράγοντες είναι μοναδική, άρα το p_1 δε μπορεί να διαιρεί ούτε το Q. Καταλήξαμε σε άτοπο και συνεπώς αποδείξαμε την μοναδικότητα. □

Α΄.1.2 Μέγιστος Κοινός Διαιρέτης

Ορισμός 1.3. *Ο Μέγιστος Κοινός Διαιρέτης δύο ακεραίων αριθμών (a, b) είναι ο μέγιστος ακέραιος που διαιρεί και τον a και τον b. Συμβολίζουμε ΜΚΔ(a, b).*

Ορισμός 1.4 (Σχετικά Πρώτοι Αριθμοί). *Δύο αριθμοί με μέγιστο κοινό διαιρέτη τη μονάδα λέμε ότι είναι σχετικά πρώτοι, ή πρώτοι μεταξύ τους.*

Για την εύρεση του Μέγιστου κοινού διαιρέτη μπορούμε να χρησιμοποιήσουμε τον παρακάτω αλγόριθμο του Ευκλείδη. Για την ακρίβεια παρουσιάζουμε τον επεκτεταμένο αλγόριθμο του Ευκλείδη, που εκτός από το ΜΚΔ(a, b), επιστρέφει και ακεραίους x, y τ.ω. ΜΚΔ$(a, b) = ax + by$.

- Επεκτεταμένος Αλγόριθμος Ευκλείδη: $(\text{ΜΚΔ}, x, y) \leftarrow \text{ΕΑΕ}(a, b)$
  1. Αν $b = 0$ επέστρεψε $(a, 1, 0)$
  2. $(temp, x_1, y_1) \leftarrow \text{ΕΑΕ}(b, a \mod b)$
  3. $\text{ΜΚΔ} \leftarrow temp$
  4. $x \leftarrow y_1$
  5. $y \leftarrow x_1 - (a/b) \cdot y_1$ (με / συμβολίζουμε ακέραια διαίρεση)
  6. Επέστρεψε $(\text{ΜΚΔ}, x, y)$

Σημείωση 1.1. *Ο Επεκτεταμένος Αλγόριθμος του Ευκλείδη έχει χρονική πολυπλοκότητα* $O(\log n)$.

Παράδειγμα 1.3. *Ας δούμε ένα αριθμητικό παράδειγμα το Επεκτεταμένου αλγορίθμου του ευκλείδη για τους ακεραίους* $(99, 78)$.

1. $21 = \mod 78,\ 1 = 99/78$
2. $15 = 78 \mod 21,\ 3 = 78/21$
3. $6 = 21 \mod 15,\ 1 = 21/15$
4. $3 = 15 \mod 6,\ 2 = 15/6$
5. $0 = 6 \mod 3,\ 2 = 6/3$

Σε αυτό το σημείο ήδη έχουμε βρει ότι $\text{ΜΚΔ}(99, 78) = 3$. *Για να βρούμε τα* x, y*:*

1. $x \leftarrow 1,\ y \leftarrow 0$
2. $x \leftarrow 0,\ y \leftarrow 1 - 2 \cdot 0 = 1$
3. $x \leftarrow 1,\ y \leftarrow 0 - 2 \cdot 1 = -2$
4. $x \leftarrow -2,\ y \leftarrow 1 - 1 \cdot (-2) = 3$
5. $x \leftarrow 3,\ y \leftarrow -2 - 3 \cdot 3 = -11$
6. $x \leftarrow -11,\ y \leftarrow 3 - 1 \cdot (-11) = 14$

Πράγματι, $3 = -11 \cdot 99 + 14 \cdot 78$

Θεώρημα 1.4 (Μικρό Θεώρημα του Fermat). *Αν* $a \in \mathbb{Z}$ *και* p *πρώτος, ώστε* $a \mod p \neq 0$, *τότε* $a^{p-1} = 1 \mod p$.

Ορισμός 1.5 (Συνάρτηση Euler). *Η συνάρτηση που με είσοδο έναν φυσικό αριθμό* n *επιστρέφει το πλήθος των φυσικών αριθμών μικρότερων του* n *που είναι σχετικά πρώτοι με το* n *ονομάζεται συνάρτηση του Euler. Συμβολίζουμε με* $\varphi(n)$.

Πρόταση 1.1. *Εύκολα αποδεικνύονται οι παρακάτω ιδιότητες:*

- $\varphi(p) = p - 1$ *για* p *πρώτο*
- $\varphi(p^a) = p^a(1 - \frac{1}{p})$, *για* p *πρώτο*
- $\varphi(mn) = \varphi(m)\varphi(n)$ *για* m, n *σχετικά πρώτους*

Α΄.2 Θεωρία Ομάδων

Ορισμός 1.6 ((Αβελιανή) Ομάδα). *Μια ομάδα* $\mathbb{G}$ *είναι ένα σύνολο στοιχείων εφοδιασμένο με μια πράξη* $\bullet : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ *που έχει τις εξής ιδιότητες:*

1. *Κλειστότητα:* $\forall a, b \in \mathbb{G},\ a \bullet b \in \mathbb{G}$
2. *Προσεταιριστική Ιδιότητα:* $\forall a, b, c \in \mathbb{G},\ (a \bullet b) \bullet c = a \bullet (b \bullet c)$
3. *Ουδέτερο Στοιχείο:* $\exists e \in \mathbb{G}$ *τ.ω.* $\forall a \in \mathbb{G}\ a \bullet e = e \bullet a = a$
4. *Αντίστροφο Στοιχείο:* $\forall a \in \mathbb{G}, \exists b \in \mathbb{G}$ *τ.ω.* $a \bullet b = b \bullet a = e$

Αν επιπλέον ισχύει και η αντιμεταθετική ιδιότητα($\forall a, b \in \mathbb{G},\ a \bullet b = b \bullet a$)*, τότε η ομάδα ονομάζεται Αβελιανή.*

Δύο απλά παραδείγματα ομάδων είναι το σύνολο των ακεραίων με πράξη τη πρόσθεση $(\mathbb{Z}, +)$ και το σύνολο των πραγματικών αριθμών με πράξη τον πολλαπλασιασμό $(\mathbb{R}, \cdot)$. Αντίθετα οι φυσικοί αριθμοί με πράξη τη πρόσθεση δεν αποτελούν ομάδα, αφού δεν υπάρχει το αντίστροφο στοιχείο, και οι ακέραιοι αριθμοί με πράξη τον πολλαπλασιασμό δεν είναι ομάδα, πάλι επειδή δεν υπάρχει το αντίστροφο στοιχείο.

Οι παραπάνω ομάδες είναι άπειρες. Στην κρυπτογραφία μας ενδιαφέρουν ομάδες που είναι πεπερασμένες. Οι ακέραιοι αριθμοί modulo έναν αριθμό n με πράξη την πρόσθεση αποτελούν την ομάδα που συμβολίζουμε $\mathbb{Z}_n$.

Παράδειγμα 1.4.

$$\mathbb{Z}_2 = \{0, 1\}$$

$$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

Μια άλλη σημαντική ομάδα είναι η $\mathbb{Z}_n^* = \{k : 1 \leq k \leq n \wedge \text{ΜΚΔ}(k, n) = 1\}$ με πράξη τον πολλαπλασιασμό.

Παράδειγμα 1.5.

$$\mathbb{Z}_2^* = \{1\}$$

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

$$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}, p \text{ πρώτος}$$

Τον αριθμό των στοιχείων μια πεπερασμένης ομάδας τον ονομάζουμε *τάξη της ομάδας* και τον συμβολίζουμε $|\mathbb{G}|$. Για τα προηγούμενα παραδείγματα, έχουμε $|\mathbb{Z}_2| = 2$, $|\mathbb{Z}_{10}| = 10$, $|\mathbb{Z}_2^*| = 1$, $|\mathbb{Z}_{10}^*| = 4$. Για την αθροιστική ομάδα $\mathbb{Z}_n$ έχουμε προφανώς $|\mathbb{Z}_n| = n$, ενώ για την πολλαπλασιαστική ομάδα $\mathbb{Z}_n^*$ έχουμε $|\mathbb{Z}_n^*| = \varphi(n)$.

Ορισμός 1.7 (Υποομάδα). *Αν ένα υποσύνολο* $S \subseteq \mathbb{G}$ *αποτελεί ομάδα με την ίδια πράξη όπως η* $\mathbb{G}$ *τότε λέγεται υποομάδα της* $\mathbb{G}$.

Παράδειγμα 1.6. *΄Εστω η προσθετική ομάδα $\mathbb{Z}_8$. ΄Εχεις τις ακόλουθες υποομάδες:*

- $\mathbb{G} = \{0, 1, 2, 3, 4, 5, 6, 7\}$, *η ίδια η ομάδα*
- $S = \{0, 2, 4, 6\}$
- $T = \{0, 4\}$
- $I = \{0\}$, *η τετριμμένη υποομάδα*

Σε κάποιες ομάδες παρατηρούμε ότι υπάρχει στοιχείο που αν του εφαρμόσουμε επαναλαμβανόμενα τη πράξη της ομάδες, θα καταλήξουμε με όλα τα στοιχεία της ομάδα. Είναι φανερό για παράδειγμα ότι αυτό θα συμβεί για οποιαδήποτε προσθετική ομάδα $\mathbb{Z}_n$, αν ξεκινήσουμε από τη μονάδα και προσθέτουμε συνέχεια τη μονάδα. Αυτές οι ομάδες ονομάζονται κυκλικές και είναι αυτές που έχουν το μεγαλύτερο ενδιαφέρον στη σύγχρονη κρυπτογραφία.

Συμβολισμός 1.1. *Συνήθως θα χρησιμοποιούμε πολλαπλασιαστικό συμβολισμό για την πράξη της ομάδας. Οπότε συμβολίζουμε $g^m = g \cdot \ldots \cdot g$($m$ φορές).*

Ορισμός 1.8 (Κυκλική Ομάδα). *Μια ομάδα $\mathbb{G}$ είναι κυκλική αν υπάρχει στοιχείο $g \in \mathbb{G}$ τέτοιο ώστε $\forall x \in \mathbb{G} \exists y \in \mathbb{Z} : x = g^y$. Το στοιχείο g ονομάζεται γεννήτορας της ομάδας.*

Για τα παρακάτω θεωρήματα και προτάσεις μπορείτε να βρείτε αποδείξεις στο βιβλίο του Fraleigh [35].

Θεώρημα 1.5. *Κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική.*

Θεώρημα 1.6 (Θεώρημα του Lagrange). *΄Εστω S υποομάδα πεπερασμένης ομάδας $\mathbb{G}$. Τότε η τάξη $|S|$ διαιρεί τη τάξη $|\mathbb{G}|$.*

Πρόταση 1.2. *Η ομάδα $\mathbb{Z}_p^*$ με $p > 3$ πρώτο, είναι κυκλική.*

Α΄.2.1 Χρήση στη Κρυπτογραφία

Στη σύγχρονη κρυπτογραφία, όπως εξηγούμε στο κεφάλαιο 1, μας ενδιαφέρουν συναρτήσεις που είναι εύκολα υπολογίσιμες, αλλά οι αντιστροφή της είναι δύσκολη. Όλες οι άλλες πράξεις που εμφανίζονται πρέπει να είναι γρήγορα υπολογίσιμες για να είναι πρακτικό ένα σχήμα.

Στα περισσότερα σχήματα που παρουσιάζουμε στη ΔΕ, υποθέτουμε ότι δουλεύουμε σε μια υποομάδα της $\mathbb{Z}_p^*$, τάξης q, όπου p, q πρώτοι. Η επιλογή που κάνουμε συνήθως είναι πρώτος p, τέτοιος ώστε $p = 2q + 1$. Ένας τέτοιος πρώτος p ονομάζεται *ασφαλής πρώτος*. Εναλλακτικά συχνά χρησιμοποιούνται πρώτοι $p = j \cdot q + 1$, για p, q πρώτους και $j \in \mathbb{Z}$. Η υποομάδα τάξης q σε αυτή τη περίπτωση ονομάζεται *ομάδα Schnorr*.

Το πρώτο ερώτημα που προκύπτει είναι, πως βρίσκουμε μια τέτοια υποομάδα. Για να το απαντήσουμε αυτό πρέπει πρώτα να αναφέρουμε ότι, υπάρχουν αποδοτικοί PPT αλγόριθμοι, που δοσμένου ενός ακεραίου n, αποφαίνονται για τον αν είναι πρώτος ή όχι. Αν και μέχρι τώρα δεν έχουμε καν αποδείξει ότι υπάρχουν

άπειροι ασφαλής πρώτοι, στη πράξη δειγματοληπτικά είναι εφικτό να βρίσκουμε τέτοιους αριθμούς δειγματοληπτικά[73].

Το δεύτερο ερώτημα είναι, πόσο εύκολο είναι να βρούμε ένα γεννήτορα για μια τέτοια ομάδα. Γενικά, για την ομάδα $\mathbb{Z}_p^*$ η εύρεση γεννήτορα δεν είναι εύκολη. Όμως για την υποομάδα τάξης $q = \frac{p-1}{2}$, η εύρεση γεννήτορα είναι τετριμμένη. Πράγματι, αφού q πρώτος, $\varphi(q) = q-1$. Άρα όλα τα στοιχεία της υποομάδας εκτός από τη μονάδα είναι γεννήτορες.

Τέλος, πρέπει να αναρωτηθούμε, αν η επαναλαμβανόμενη εφαρμογή της πράξης της ομάδας, είναι κάτι που μπορεί να υπολογιστεί αποδοτικά. Αν αυτό δεν ισχύει, τότε δεν έχουμε καταφέρει τίποτα, αφού σε όλα τα σχήματα, επανειλημμένα κάνουμε πράξης του τύπου g^x, όπου x μπορεί να είναι οποιοσδήποτε αριθμός στο $\mathbb{Z}_q$, όπου q είναι ένας μεγάλος πρώτος. Η απάντηση ευτυχώς είναι θετική, αφού έχουμε στη διάθεση μας τον αλγόριθμο επαναλαμβανόμενου τετραγωνισμού[69].

ΠΑΡΑΡΤΗΜΑ Β΄

Συναρτήσεις Σύνοψης και το Μοντέλο Τυχαίου Μαντείου

Οι συναρτήσεις σύνοψης είναι ένα εργαλείο με πολύ διαδεδομένη χρήση στη πληροφορική, με πληθώρα εφαρμογών. Στην γενική περίπτωση, πρόκειται για συναρτήσεις που απεικονίζουν ένα μεγάλο σύνολο σε ένα μικρότερο σύνολο. Στη κρυπτογραφία μας ενδιαφέρουν μια ειδική υποκατηγορία συναρτήσεων σύνοψης, που τις αποκαλούμε κρυπτογραφικές συναρτήσεις σύνοψης, που έχουν κάποιες επιπλέον ιδιότητες που θα δούμε στη συνέχεια, που τις καθιστούν κατάλληλες για κρυπτογραφικές εφαρμογές. Διαισθητικά αυτό που απαιτούμε από τις συναρτήσεις σύνοψης, είναι να προσομοιώνουν όσο πιο καλά μπορούν μια τελείως τυχαία συνάρτηση.

Στη θεωρητική κρυπτογραφία, πολλές φορές υποθέτουμε ότι οι χρήστες έχουν στη διάθεση τους ένα τυχαίο μαντείο$\mathcal{RO}$, δηλαδή μια συνάρτηση που για κάθε είσοδο από το πεδίο ορισμού, επιστρέφει τυχαία και ομοιόμορφα, μια τιμή από το πεδίο τιμών. Αυτό είναι βέβαια μια εξιδανίκευση, αφού δεν μπορούμε φυσικά στην πραγματικότητα να κατασκευάσουμε μια τέτοια συνάρτηση.

Έτσι υπάρχει το εξής χάσμα ανάμεσα στη θεωρητική κρυπτογραφία και τη κρυπτογραφική εφαρμογή. Στη μεν θεωρεία σχεδιάζουμε και αποδεικνύουμε τις ιδιότητες θεωρώντας τυχαία μαντεία, ενώ στην υλοποίηση των σχημάτων, αντικαθιστούμε τα τυχαία μαντεία με κρυπτογραφικές συναρτήσεις σύνοψης. Από αυτή τη παραδοχή, προκύπτουν πρωτόκολλα πολύ πιο αποδοτικά, και με πιο εύκολες αποδείξεις. Οι αποδείξεις αυτές στη κρυπτογραφική πρακτική θεωρούνται, αρκετά καλές για πρακτική ασφάλεια[10]. Αυτό είναι το λεγόμενο Μοντέλο Τυχαίου Μαντείου($\mathcal{RO}$).

Όσον αφορά τις ψηφιακές υπογραφές, έχουμε στη διάθεση μας ένα πολύ ισχυρό λήμμα που μας επιτρέπει να αποδεικνύουμε τις ιδιότητες ασφαλείας τους στο μοντέλο $\mathcal{RO}$, το λήμμα διακλάδωσης[60].

Το κομμάτι του παρόντος παραρτήματος που αφορά τις συναρτήσεις σύνοψης βασίζεται στα αντίστοιχα κεφάλαια των [15, 37, 67, 69].

Β΄.1 Κρυπτογραφικές Συναρτήσεις Σύνοψης

Γενικά μια συνάρτηση σύνοψης είναι οποιαδήποτε συνάρτηση απεικονίζει ένα μεγάλο σύνολο, συχνά άπειρο, σε ένα μικρότερο πεπερασμένο σύνολο. Αν σκεφτούμε ότι οποιαδήποτε είσοδος έχει κάποια δυαδική αναπαράσταση, συχνά θεωρούμε ως σύνολο τιμών το $\{0,1\}^*$, δηλαδή ως είσοδο η συνάρτηση μπορεί να έχει

οποιαδήποτε συμβολοσειρά. Σαν πεδίο τιμών θέτουμε συνήθως την ομάδα $\mathbb{G}$ στην οποία δουλεύουμε. Μια άλλη απαραίτητη προϋπόθεση είναι η συνάρτηση H να είναι γρήγορα υπολογίσιμη. Μέσα σε ένα σχήμα μπορεί η συνάρτηση να καλείται πολλές φορές, οπότε αν δεν ήταν γρήγορα υπολογίσιμη η χρήση της θα καθιστούσε το σχήμα μη πρακτικό.

Για κρυπτογραφικές εφαρμογές όμως χρειαζόμαστε κάποιες παραπάνω ιδιότητες. Στις ψηφιακές υπογραφές χρησιμοποιούμε τις συναρτήσεις σύνοψης για να δεσμευτούμε σε κάποιες παραμέτρους. Για να είναι η συνάρτηση δεσμευτική θα πρέπει για παράδειγμα να είναι δύσκολα αντιστρέψιμη. Αλλιώς ένας αντίπαλος αντί να βρει το $c \leftarrow \mathsf{H}(\mathtt{m})$, θα μπορούσε να επιλέξει το c που τον βολεύει, και να βρει εκ των υστέρων το $\mathtt{m}$ που το ικανοποιεί. Αυτό θα μπορούσε εύκολα να οδηγήσει σε μια υπαρξιακή πλαστογραφία. Αυτή η ιδιότητα δεν είναι όμως αρκετή. Οι ιδιότητες που επιθυμούμε είναι οι παρακάτω:

1. *Αντίσταση Πρώτου Ορίσματος*: Είναι υπολογιστικά δύσκολο, για δεδομένο c, να βρεθεί $\mathtt{m}$ τ.ω. $c \leftarrow \mathsf{H}(\mathtt{m})$.

2. *Αντίσταση Δεύτερου Ορίσματος*: Είναι υπολογιστικά δύσκολο, για δεδομένο $\mathtt{m}$, να βρεθεί $\mathtt{m}' \neq \mathtt{m}$ τ.ω. $\mathsf{H}(\mathtt{m}) = \mathsf{H}(\mathtt{m}')$

3. *Δυσκολία Εύρεσης Συγκρούσεων*: Είναι υπολογιστικά δύσκολο να βρεθούν διαφορετικά μεταξύ τους $\mathtt{m}, \mathtt{m}'$ τ.ω $\mathsf{H}(\mathtt{m}) = \mathsf{H}(\mathtt{m}')$

Ορισμός 2.1 (Κρυπτογραφική Συνάρτηση Σύνοψης). *Μια συνάρτηση σύνοψης* H *θα λέμε ότι είναι κρυπτογραφική αν ικανοποιεί τις ιδιότητες* $1-3$ *παραπάνω.*

Με μια πιο προσεκτική ματιά μπορούμε όμως να δούμε ότι οι τρεις ιδιότητες δεν είναι ανεξάρτητες μεταξύ τους. Πράγματι η αντίσταση πρώτου ορίσματος είναι πιο αδύναμη απαίτηση από τις άλλες δύο, και η αντίσταση δεύτερου ορίσματος είναι πιο αδύναμη από τη δυσκολία εύρεσης συγκρούσεων.

Λήμμα 2.1. *Η υπόθεση ότι μια συνάρτηση έχει αντίσταση πρώτου ορίσματος για κάθε στοιχείο του πεδίου τιμών της είναι πιο αδύναμη από την υπόθεση ότι έχει αντίσταση δεύτερου ορίσματος, όταν το πεδίο ορισμού είναι άπειρο.*

Απόδειξη. Έστω ότι δεν έχουμε αντίσταση πρώτου ορίσματος και έστω $\mathtt{m}$ για το οποίο προσπαθούμε να παραβιάσουμε την ιδιότητα της αντίστασης δεύτερου ορίσματος. Τότε μπορούμε να υπολογίσουμε το $c \leftarrow \mathsf{H}(\mathtt{m})$. Αφού δεν έχουμε αντίσταση πρώτου ορίσματος, μπορούμε να βρούμε $\mathtt{m}'$, τ.ω. $c \leftarrow \mathsf{H}(\mathtt{m}')$. Η πιθανότητα $\mathtt{m} = \mathtt{m}'$ είναι αμελητέα, άρα βρήκαμε δεύτερο όρισμα. □

Λήμμα 2.2. *Η υπόθεση ότι μια συνάρτηση έχει αντίσταση δεύτερου ορίσματος είναι πιο αδύναμη από την υπόθεση ότι έχει δυσκολία εύρεσης συγκρούσεων.*

Απόδειξη. Έστω ότι δεν έχουμε αντίσταση δεύτερου ορίσματος. Θα δείξουμε ότι δεν έχουμε ούτε δυσκολία εύρεση συγκρούσεων. Πράγματι έστω $\mathtt{m}$, για το οποίου μπορούμε να βρούμε $\mathtt{m}'$ τ.ω $\mathsf{H}(\mathtt{m}) = \mathsf{H}(\mathtt{m}')$. Αυτό αποτελεί σύγκρουση. □

Η θεώρηση μας στα παραπάνω δεν ήταν ιδιαίτερα τυπική. Για μια πιο διεξοδική μελέτη των ορισμών, και τα προβλήματα στα οποία μπορούν να οδηγήσουν οι μη τυπικοί ορισμοί στη περίπτωση των κρυπτογραφικών συναρτήσεων σύνοψης παραπέμπουμε στους [63].

Κρυπτογραφικές Συναρτήσεις Σύνοψης στη Πράξη

Στη πράξη έχουν σχεδιαστεί διάφορες συναρτήσεις σύνοψης, που πιστεύεται ευρέως ότι ικανοποιούν την ιδιότητα δυσκολίας εύρεσης συγκρούσεων. Το Αμερικάνικο Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας(NIST) έχει δημοσιεύσει για παράδειγμα την οικογένεια συναρτήσεων SHA[39]. Αν και στις πρώτες εκδόσεις τους MD5 και SHA-1 έχουν βρεθεί συγκρούσεις και δε θεωρούνται πλέον ασφαλείς, οι συναρτήσεις SHA-2 και SHA-3 χρησιμοποιούνται σε πολλές εφαρμογές. Μια άλλη δημοφιλής συνάρτηση είναι η BLAKE[6].

Β΄.2 Μοντέλο Τυχαίου Μαντείου

Παρότι στη πράξη χρησιμοποιούμε κρυπτογραφικές συναρτήσεις σύνοψης, πολλές φορές για την θεωρητική παρουσίαση ενός σχήματος μοντελοποιούμε την κρυπτογραφική συνάρτηση σύνοψης με ένα τυχαίο μαντείο $\mathcal{RO}$, δηλαδή μια ομοιόμορφα τυχαία συνάρτηση. Το $\mathcal{RO}$ μπορούμε να το σκεφτούμε σαν ένα ¨μαύρο κουτί¨ που για κάθε είσοδο:

- Αν έχει ξαναδεχτεί την ίδια είσοδο, επιστρέφει την ίδια έξοδο που είχε επιστρέψει τη προηγούμενη φορά
- Αν δέχεται την είσοδο για πρώτη φορά, επιλέγει ένα στοιχείο από το πεδίο τιμών τυχαία ομοιόμορφα και το επιστρέφει.

Μια τέτοια συνάρτηση προφανώς ικανοποιεί τετριμμένα τις ιδιότητες που απαιτούμε από τις κρυπτογραφικές συναρτήσεις σύνοψης. Δεν είναι όμως μια συνάρτηση που μπορούμε να υλοποιήσουμε στη πράξη. Η μοντελοποίηση όμως των συναρτήσεων σύνοψης με ένα τυχαίο μαντείο $\mathcal{RO}$ διευκολύνει πάρα πολύ την ανάλυση της ασφάλειας του σχήματος, αφού έχουμε στη διάθεση μας ισχυρά εργαλεία όπως το λήμμα διακλάδωσης που θα δούμε στην επόμενη υποενότητα. Παρότι οι αποδείξεις που κατασκευάζουμε κατά αυτόν τον τρόπο δεν αντιστοιχούν ακριβώς στην πραγματικότητα, υπάρχουν πολλά επιχειρήματα, ότι είναι αρκετά καλές από πρακτικής άποψης[10]. Αυτό ονομάζεται το Μοντέλο Τυχαίου Μαντείου.

Αντίθετα, τα σχήματα που αποδεικνύουν την ασφάλεια τους υποθέτοντας μόνο μια συνάρτηση σύνοψης με δυσκολία εύρεση συγκρούσεων, λέμε ότι δουλεύουν στο Κανονικό Μοντέλο(Standard Model)

Β΄.2.1 Λήμμα Διακλάδωσης

Μια πολύ ισχυρή τεχνική αποδείξεων για σχήματα ψηφιακών υπογραφών στο μοντέλο τυχαίου μαντείου εισήχθηκε από τους Pointcheval και Stern[60]. Η ιδέα

είναι εξής. Υποθέτουμε ότι ένας αντίπαλος $\mathcal{A}$ μπορεί να παραβιάσει την ιδιότητα ασφάλειας που προσπαθούμε να αποδείξουμε ότι το σχήμα μας ικανοποιεί. Δείχνουμε ότι ένας άλλος αλγόριθμος $\mathcal{M}$ μπορεί να χρησιμοποιήσει τον $\mathcal{A}$ ως υπορουτίνα και να λύσει κάποιο πρόβλημα που έχουμε υπόθεση ότι είναι δυσεπίλυτο, όπως π.χ. το DLP. Για να το κάνει αυτό, επαναφέρει την ταινία του $\mathcal{A}$ σε ένα προγενέστερο σημείο. Λαμβάνει έτσι δύο εξόδους του αντιπάλου, από τις οποίες λύνει το δύσκολο πρόβλημα, καταλήγοντας σε αντίφαση. Για να λειτουργήσει αυτή η τεχνική πρέπει να εξασφαλίσουμε ότι μετά την επαναφορά της ταινίας ο $\mathcal{A}$ θα μας επιστρέφει με μη αμελητέα πιθανότητα την έξοδο που θέλουμε. Αυτό μας το εξασφαλίζει το λήμμα διακλάδωσης(forking lemma).

Λήμμα 2.3 (Λήμμα Διακλάδωσης). *Έστω $\mathcal{A}$ ένας* PPT *αλγόριθμος. Αν ο $\mathcal{A}$ επιστρέφει με μη αμελητέα πιθανότητα $(\mathtt{m}, \sigma_1, h, \sigma_2)$, όπου $\mathtt{m}$ το μήνυμα και $h \leftarrow \mathsf{H}(\sigma_1, \mathtt{m})$ και σ_2 εξαρτάται από το σ_1, τότε μια επαναφορά του $\mathcal{A}$ με την ίδια τυχαία ταινία αλλά διαφορετικό τυχαίο μαντείο επιστρέφει $(\mathtt{m}, \sigma_1, h', \sigma_2)$.*

Αργότερα παρουσιάστηκαν μια έκδοση του λήμματος που λαμβάνει υπόψη της υπογραφές δακτυλίου[40] και μια γενικευμένη έκδοση[9] που δεν αναφέρεται συγκεκριμένα σε τυχαία μαντεία και υπογραφές, αλλά πιο γενικά στις εξόδους ενός αλγορίθμου που τρέχει δύο φορές με παρόμοια είσοδο.

Λήμμα Επαναφοράς στην Επιτυχία

Στις αποδείξεις στο κεφάλαιο 6 εφαρμόζουμε μια παραλλαγή του λήμματος διακλάδωσης, το λήμμα επαναφοράς στην επιτυχίαrewind on success lemma[50]. Το όνομα προέρχεται από το γεγονός ότι η προσομοίωση γίνεται επιλεκτικά. Η επαναφορά γίνεται μόνο στην περίπτωση που ο $\mathcal{A}$ τερμάτισε με επιτυχία.

Έστω $\mathcal{M}$ ο αλγόριθμος που χρησιμοποιεί τον αλγόριθμο $\mathcal{A}$ και T η ταινία με τα πρακτικά της εκτέλεσης του αλγορίθμου. Αν ο $\mathcal{M}$ επαναφέρει σε κάποιο σημείο του αλγορίθμου H, θα έχει τα καινούρια πρακτικά T', Που θα είναι πανομοιότυπα με αυτά του T μέχρι το σημείο H και διαφορετικά μετά, αφού θα αλλάξει η τυχαιότητα. Τα πρακτικά T μπορεί είτε να αποτελούν για τον $\mathcal{A}$ επιτυχία, είτε όχι(π.χ. επιτυχημένη πλαστογραφία). Τότε αποδεικνύουν το ακόλουθο λήμμα:

Λήμμα 2.4 (Λήμμα Επαναφοράς στην Επιτυχία). *Αν $Pr[T\ \epsilon\pi\iota\tau\upsilon\chi\acute{\iota}\alpha] = e$, τότε $Pr[T'\ \epsilon\pi\iota\tau\upsilon\chi\acute{\iota}\alpha] = e$*

ΠΑΡΑΡΤΗΜΑ Γ΄

Αποδείξεις Μηδενικής Γνώσης

Οι αποδείξεις μηδενικής γνώσης είναι ένα χρήσιμο εργαλείο στην κρυπτογραφία, που μας επιτρέπει να αποδεικνύουμε προτάσεις σε κάποιον, χωρίς να δίνουμε καμία επιπλέον πληροφορία πέρα από την ορθότητα της πρότασης που αποδείξαμε. Για παράδειγμα μπορεί να θέλουμε να αποδείξουμε ότι ξέρουμε x τ.ω. $y = g^x$, χωρίς όμως να αποκαλύψουμε το x ή οποιαδήποτε πληροφορία θα έδινε σε έναν αντίπαλο προβάδισμα στο να βρει το x. Αν σκεφτούμε το y ως ένα δημόσιο και το x ως ένα ιδιωτικό κλειδί ενός συστήματος κρυπτογραφίας δημοσίου κλειδιού, με αυτό το τρόπο μπορούμε να πιστοποιήσουμε ότι το δημόσιο κλειδί μας ανήκει, χωρίς όμως να αποκαλύψουμε το μυστικό μας κλειδί. Η έννοια εισήχθηκε για πρώτη φορά από του Goldwasser, Micali και Rackoff[38]. Το παρόν παράρτημα έχει ως κύριες πηγές τα αντίστοιχα κεφάλαιο των [67, 69].

Τέτοιες αποδείξεις μπορεί να είναι διαλογικές, αν αποτελούν ένα πρωτόκολλο μεταξύ ενός αποδείκτη $\mathcal{P}$ και ενός επαληθευτή $\mathcal{V}$, ή μη διαλογικές αν ο $\mathcal{P}$ αποδεικνύει χωρίς την ενεργή συμμετοχή κάποιου άλλου.

Από ένα πρωτόκολλο μηδενική γνώσης απαιτούμε να ικανοποιεί τις ακόλουθες τρεις ιδιότητες:

1. *Πληρότητα*: Ένας τίμιος $\mathcal{P}$(που ξέρει το μυστικό και ακολουθεί πιστά το πρωτόκολλο) πείθει ένα τίμιο $\mathcal{V}$ με συντριπτική πιθανότητα.

2. *Ορθότητα*: Ο $\mathcal{P}$ δε μπορεί να πείσει τον $\mathcal{V}$ για μια πρόταση που δεν είναι αληθής, παρά μόνο με αμελητέα πιθανότητα.

3. *Μηδενική Γνώση*: Ο $\mathcal{V}$ δε μαθαίνει τίποτα παραπάνω από την εκτέλεση του πρωτοκόλλου πέρα από την αλήθεια της πρότασης που αποδεικνύει ο $\mathcal{P}$.

Στη συνέχεια θα ασχοληθούμε με μια ειδική κατηγορία αποδείξεων μηδενική γνώσης, τα Σ-Πρωτόκολλα και έπειτα θα δούμε μια μέθοδο που μετατρέπει ένα διαλογικό σύστημα αποδείξεων σε ένα μη διαλογικό.

Γ΄.1 Σ-Πρωτόκολλα

Στη γενική περίπτωση μιας απόδειξης μηδενικής γνώσης, ο $\mathcal{V}$ μπορεί να είναι κακόβουλος, δηλαδή να μην ακολουθεί πιστά το πρωτόκολλο, ίσως με σκοπό να παγιδεύσει τον $\mathcal{P}$ να αποκαλύψει κάποια επιπλέον πληροφορία. Αν όμως υποθέσουμε ότι ο $\mathcal{V}$ είναι τίμιος τότε έχουμε μια ενδιαφέρουσα κατηγορία αποδείξεων που λέγονται Honest Verifier Zero Knowledge (HVZK).

Ορισμός 3.1 (Σ-Πρωτόκολλο). *Ονομάζουμε Σ-Πρωτόκολλο ένα HVZK σχήμα με τους ακόλουθους 3 γύρους:*

1. *Δέσμευση: Ο $\mathcal{P}$ επιλέγει μια τιμή-δέσμευση και την στέλνει στον $\mathcal{V}$.*
2. *Πρόκληση: Ο $\mathcal{V}$ επιλέγει τίμια (ομοιόμορφα τυχαία) μια τιμή-πρόκληση και την στέλνει στον $\mathcal{P}$.*
3. *Απάντηση: Ο $\mathcal{P}$ απαντάει στη πρόκληση του $\mathcal{V}$.*

Για τα Σ-Πρωτόκολλα μπορούμε να χρησιμοποιούμε μια διαφορετική έννοια ορθότητας, την ειδική ορθότητα που συχνά είναι πιο εύκολο να αποδειχθεί στη πράξη.

Ορισμός 3.2 (Ειδική Ορθότητα). *Ένα Σ-Πρωτόκολλο έχει την ιδιότητα της ειδικής ορθότητας, αν δύο εκτελέσεις του πρωτοκόλλου με την ίδια δέσμευση αλλά διαφορετικές προκλήσεις αποκαλύπτουν το μυστικό του $\mathcal{P}$.*

Στην περίπτωση τον Σ-Πρωτοκόλλων μπορεί να αποδειχθεί ότι η ειδική ορθότητα συνεπάγεται την ορθότητα[67].

Γ΄.1.1 Πρωτόκολλο του Schnorr

Θα παρουσιάσουμε ένα κλασικό πρωτόκολλο που οφείλεται στον Schnorr[65]. Σε αυτό το πρωτόκολλο έχουμε έναν $\mathcal{P}$ ο οποίος θέλει να αποδείξει στον $\mathcal{V}$ ό,τι γνωρίζει τον διακριτό λογάριθμο x, ενός $y \in \mathbb{G}$, ως προς τον γεννήτορα g. Η ομάδα $\mathbb{G}$ τάξης πρώτου q και ο γεννήτορας g θεωρούμε ότι είναι δημόσιες παράμετροι.

Πρωτόκολλο του Schnorr		
$\mathcal{P}$		$\mathcal{V}$
$k \leftarrow\$ \mathbb{Z}_q$		
$r \leftarrow g^k$	$\xrightarrow{r}$	
	$\xleftarrow{c}$	$c \leftarrow\$ \mathbb{Z}_q$
$s \leftarrow k + cx$	$\xrightarrow{s}$	$g^s = ry^c$

Για την πληρότητα του πρωτοκόλλου έχουμε:

$$g^s = g^{k+cx} = g^k g^{cx} = ry^c$$

Αν ο $\mathcal{P}$ δεν γνώριζε τον διακριτό λογάριθμο, τότε θα μπορούσε να προσπαθήσει να παραπλανήσει τον $\mathcal{V}$ μαντεύοντας την πρόκληση c από το πρώτο βήμα και διαλέγοντας $r \leftarrow g^k y^{-c}$. Η πιθανότητα όμως να μαντέψει το c που θα επιλέξει ο $\mathcal{V}$ στο επόμενο βήμα είναι μόνο $\frac{1}{q}$, δηλαδή αμελητέα. Αυτό φυσικά δεν αποτελεί απόδειξη ορθότητας. Μπορούμε όμως εύκολα να αποδείξουμε την ορθότητα, δείχνοντας την ειδική ορθότητα.

Πράγματι έστω δύο εκτελέσεις του πρωτοκόλλου με $r = r'$, $c \neq c'$, $s \neq s'$. Θα δείξουμε ότι μπορούμε να βρούμε τον διακριτό λογάριθμο x. Θα πρέπει να ισχύει ότι:

$$r = g^s y^{-c} = g^{s'} y^{-c'} = r \implies$$
$$s + x(-c) = s' + x(-c')$$

Άρα μπορούμε να υπολογίσουμε το x ως:

$$x \leftarrow \frac{s' - s}{c - c'}$$

Τέλος μένει να δείξουμε ότι το πρωτόκολλο είναι μηδενικής γνώσης. Αρκεί να δούμε ότι ο $\mathcal{V}$ θα μπορούσε να έχει προσομοιώσει όλη την εκτέλεση του πρωτοκόλλου μόνος του ως εξής:

1. $c, s \leftarrow\$ \mathbb{Z}_q$
2. $r \leftarrow g^s y^{-c}$

Πράγματι θα έχει ότι $g^s = ry^c$. Αφού μπορεί να προσομοιώσει όλο το πρωτόκολλο χωρίς καμία γνώση πέρα από τις δημόσιες παραμέτρους, τότε σίγουρα δε θα μπορούσε να λάβει κάποια γνώση από την εκτέλεση αυτού του πρωτοκόλλου.

Γ΄.1.2 Πρωτόκολλο Chaum-Pedersen

Ένα άλλο κλασικό Σ-Πρωτόκολλο είναι αυτό που οφείλεται στους Chaum και Pedersen[21]. Σε αυτό το πρωτόκολλο δημόσιες παράμετροι είναι μια ομάδα $\mathbb{G}$ τάξης πρώτου q και δύο διαφορετικοί της γεννήτορες g, h. Ο $\mathcal{P}$ θέλει να αποδείξει σε μηδενική γνώση ότι γνωρίζει x τ.ω. $y_1 = g^x$ και $y_2 = h^x$. Είναι ουσιαστικά μια απόδειξη ισότητας δύο διακριτών λογαρίθμων ως προς δύο διαφορετικούς γεννήτορες. το πρωτόκολλο έχει ως εξής:

Πρωτόκολλο Chaum-Pedersen		
$\mathcal{P}$		$\mathcal{V}$
$k \leftarrow\$ \mathbb{Z}_q$		
$r_1 \leftarrow g^k$		
$r_2 \leftarrow h^k$	$\xrightarrow{r_1, r_2}$	
	$\xleftarrow{c}$	$c \leftarrow\$ \mathbb{Z}_q$
$s \leftarrow k + cx$	$\xrightarrow{s}$	$g^s = ry^c$
		$h^s = r_2 y_2^c$

Μπορούμε να αποδείξουμε με ανάλογο τρόπο με το πρωτόκολλο του Schnorr την πληρότητα, την ορθότητα και την μηδενική γνώση.

Γ΄.1.3 Απόδειξη Διαζευτικών Προτάσεων

Σε κάποιες περιπτώσεις μπορεί να θέλουμε να αποδείξουμε σε μηδενική γνώση ότι ισχύει τουλάχιστον μία από δύο προτάσεις Θ_1, Θ_2. Αν έχουμε στη διάθεση μας Σ-πρωτόκολλα για την απόδειξη τον προτάσεων Θ_1 και Θ_2 ξεχωριστά, τότε οι Cramer, Damgård και Schoenmakers[27] εισήγαγαν έναν τρόπο να αποδείξουμε και την πρόταση $\Theta_1 \vee \Theta_2$, χωρίς φυσικά να διαρρέει το ποια από της δύο (ή και οι δύο) προτάσεις ισχύουν πραγματικά.

Θα παρουσιάσουμε τη μέθοδο τους μέσα από ένα παράδειγμα. Έστω πάλι δημόσιες παράμετροι $\mathbb{G}$ τάξης q και γεννήτορας g. Ο $\mathcal{P}$ θέλει να αποδείξει ότι ξέρει είτε x_1 ώστε $g^{x_1} = y_1$, είτε $g^{x_2} = y_2$. Θα δούμε δηλαδή τη διάζευξη δύο πρωτοκόλλων Schnorr. Θα υποθέσουμε χωρίς βλάβη της γενικότητας ότι ο $\mathcal{P}$ γνωρίζει το x_1.

Διάζευξη Πρωτοκόλλων Schnorr		
$\mathcal{P}$		$\mathcal{V}$
$k, c_2, s_2 \leftarrow\$ \mathbb{Z}_q$		
$r_1 \leftarrow g^k$		
$r_2 \leftarrow g^{s_2} y_2^{-c_2}$	$\xrightarrow{r_1, r_2}$	
	$\xleftarrow{c}$	$c \leftarrow\$ \mathbb{Z}_q$
$c_1 \leftarrow c + c_2$		
$s_1 \leftarrow k + c_1 x_1$	$\xrightarrow{c_1, s_1}$	$c = c_1 + c_2$
		$g^{s_1} = r_1 y_1^{c_1}$
		$g^{s_2} = r_2 y_2^{c_2}$

Η μέθοδος αυτή μπορεί να γενικευτεί για την απόδειξη ενός αυθαίρετου αριθμού προτάσεων $\Theta_1 \vee \Theta_1 \vee \cdots \vee \Theta_n$ με τον προφανή τρόπο.

Σημειώνουμε επίσης ότι και άλλου είδους συνθέσεων Σ-Πρωτοκόλλων είναι δυνατές. Για παράδειγμα για την απόδειξη συζευκτικής πρότασης μπορούμε να τρέξουμε τα δύο πρωτόκολλα παράλληλα, αλλά με κοινή πρόκληση.

Γ΄.1.4 Μέθοδος Fiat-Shamir

Μέχρι τώρα παρουσιάσαμε πρωτόκολλα που απαιτούν την ενεργή συμμετοχή δύο οντοτήτων. Μιλούσαμε δηλαδή για πρωτόκολλα διαλογικά. Οι Fiat και Shamir παρουσίασαν μια μέθοδο που μετατρέπει ένα Σ-Πρωτόκολλο από διαλογικό σε μη διαλογικό[34]. Η ιδέα είναι ότι η πρόκληση μπορεί να προέρχεται από μια κρυπτογραφική συνάρτηση σύνοψης. Αν η είσοδος της συνάρτηση σύνοψης περιλαμβάνει την δέσμευση του $\mathcal{P}$, αυτό θεωρούμε ότι ισοδυναμεί πρακτικά με την τυχαία επιλογή της πρόκλησης από κάποιον $\mathcal{V}$. Έτσι για το πρωτόκολλο του Schnorr, αν $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_q$ έχουμε:

1. $k \leftarrow\$ \mathbb{Z}_q$, $r \leftarrow g^k$
2. $c \leftarrow \mathsf{H}(r)$
3. $s \leftarrow k + cx$

Οποιασδήποτε λαμβάνοντας τα (k, c, s) μπορεί να ελέγξει ότι $c = \mathsf{H}(g^s y^{-c})$.

Με μια μικρή τροποποίηση μπορούμε να μετατρέψουμε την απόδειξη μηδενική γνώσης σε ψηφιακή υπογραφή. Αν στο δεύτερο βήμα, χρησιμοποιήσουμε ως είσοδο στην συνάρτηση σύνοψης και το μήνυμα $\mathtt{m}$, δηλαδή $c \leftarrow \mathsf{H}(r\mathtt{m})$, τότε έχουμε ένα σχήμα που αποδεικνύει την γνώση ενός ιδιωτικού κλειδιού x που αντιστοιχεί σε ένα δημόσιο κλειδί y, έχοντας ταυτόχρονα δεσμευτεί σε συγκεκριμένο μήνυμα ώστε να αποφευχθεί μια υπαρξιακή πλαστογραφία. Αυτό δεν είναι άλλο παρά το κλασικό σχήμα υπογραφών Schnorr[65].

Οι αποδείξεις μηδενικής γνώσης σχετίζονται φυσικά και με τις Υπογραφές Καθορισμένου Επαληθευτή (DVS) του κεφαλαίου 4, και με τις Υπογραφές Δακτυλίου (RS) του κεφαλαίου 5. Μπορούμε να σκεφτούμε μια DVS ως μια απόδειξη μηδενική γνώσης είτε του ιδιωτικού κλειδιού του υπογράφοντα, είτε του ιδιωτικού κλειδιού του καθορισμένου επαληθευτή. Για τις RS μπορούμε να σκεφτόμαστε ως την απόδειξη μηδενικής γνώσης ενός από τα n ιδιωτικών κλειδιών ενός συνόλου δημοσίων κλειδιών.

Βιβλιογραφία

[1] Masayuki Abe, Miyako Ohkubo και Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. Στο *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*Yuliang Zheng, επιμελητής, τόμος 2501 στο *Lecture Notes in Computer Science*, σελίδες 415–432. Springer, 2002.

[2] Laila El Aimani. On generic constructions of designated confirmer signatures. Στο *Progress in Cryptology - INDOCRYPT 2009, 10th International Conference on Cryptology in India, New Delhi, India, December 13-16, 2009. Proceedings*Bimal K. Roy και Nicolas Sendrier, επιμελητές, τόμος 5922 στο *Lecture Notes in Computer Science*, σελίδες 343–362. Springer, 2009.

[3] Giuseppe Ateniese, Jan Camenisch, Marc Joye και Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. Στο *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*Mihir Bellare, επιμελητής, τόμος 1880 στο *Lecture Notes in Computer Science*, σελίδες 255–270. Springer, 2000.

[4] Giuseppe Ateniese και Gene Tsudik. Some open issues and new directions in group signatures. Στο *Financial Cryptography, Third International Conference, FC'99, Anguilla, British West Indies, February 1999, Proceedings*Matthew K. Franklin, επιμελητής, τόμος 1648 στο *Lecture Notes in Computer Science*, σελίδες 196–211. Springer, 1999.

[5] Man Ho Au, Sherman S. M. Chow, Willy Susilo και Patrick P. Tsang. Short linkable ring signatures revisited. Στο *Public Key Infrastructure, Third European PKI Workshop: Theory and Practice, EuroPKI 2006, Turin, Italy, June 19-20, 2006, Proceedings*Andrea S. Atzeni και Antonio Lioy, επιμελητές, τόμος 4043 στο *Lecture Notes in Computer Science*, σελίδες 101–115. Springer, 2006.

[6] Jean Philippe Aumasson, Willi Meier, Raphael Phan και Luca Henzen. *The Hash Function BLAKE*. Springer Publishing Company, Incorporated, 2014.

[7] Pourandokht Behrouz, Panagiotis Grontas, Vangelis Konstantakatos, Aris Pagourtzis και Marianna Spyrakou. Designated-verifier linkable ring signatures. Cryptology ePrint Archive, Report 2022/470, 2022.

[8] Mihir Bellare, Daniele Micciancio και Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. Στο *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*Eli Biham, επιμελητής, τόμος 2656 στο *Lecture Notes in Computer Science*, σελίδες 614–629. Springer, 2003.

[9] Mihir Bellare και Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. Στο *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, October 30 - November 3, 2006*Ari Juels, Rebecca N. Wright και Sabrina De Capitanidi Vimercati, επιμελητές, σελίδες 390–399. ACM, 2006.

[10] Mihir Bellare και Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. Στο *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu και Victoria Ashby, επιμελητές, σελίδες 62–73. ACM, 1993.

[11] Mihir Bellare, Haixia Shi και Chong Zhang. Foundations of group signatures: The case of dynamic groups. Στο *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*Alfred Menezes, επιμελητής, τόμος 3376 στο *Lecture Notes in Computer Science*, σελίδες 136–153. Springer, 2005.

[12] Adam Bender, Jonathan Katz και Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. *IACR Cryptol. ePrint Arch.*, σελίδα 304, 2005.

[13] Manuel Blum, Alfredo De Santis, Silvio Micali και Giuseppe Persiano. Noninteractive zero-knowledge. *SIAM J. Comput.*, 20(6):1084–1118, 1991.

[14] Carlo Blundo, Paolo D'Arco και Alfredo De Santis. A t-private k-database information retrieval scheme. *Int. J. Inf. Sec.*, 1(1):64–68, 2001.

[15] Dan Boneh και Victor Shoup. *A Graduate Course in Applied Cryptography*. ebook, 2015.

[16] Joan Boyar, David Chaum, Ivan Damgård και Torben P. Pedersen. Convertible undeniable signatures. Στο *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*Alfred Menezes και Scott A. Vanstone,

επιμελητές, τόμος 537 στο *Lecture Notes in Computer Science*, σελίδες 189–205. Springer, 1990.

[17] Gilles Brassard, David Chaum και Claude Crépeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, 1988.

[18] Jan Camenisch και Markus Michels. Confirmer signature schemes secure against adaptive adversaries. Στο *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*Bart Preneel, επιμελητής, τόμος 1807 στο *Lecture Notes in Computer Science*, σελίδες 243–258. Springer, 2000.

[19] David Chaum. Zero-knowledge undeniable signatures. Στο *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, Proceedings*Ivan Damgård, επιμελητής, τόμος 473 στο *Lecture Notes in Computer Science*, σελίδες 458–464. Springer, 1990.

[20] David Chaum. Designated confirmer signatures. Στο *Advances in Cryptology — EUROCRYPT'94*Alfredo De Santis, επιμελητής, σελίδες 86–91, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[21] David Chaum και Torben P. Pedersen. Wallet databases with observers. Στο *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*Ernest F. Brickell, επιμελητής, τόμος 740 στο *Lecture Notes in Computer Science*, σελίδες 89–105. Springer, 1992.

[22] David Chaum και Hansvan Antwerpen. Undeniable signatures. Στο *Advances in Cryptology — CRYPTO' 89 Proceedings*Gilles Brassard, επιμελητής, σελίδες 212–216, New York, NY, 1990. Springer New York.

[23] David Chaum, Eugènevan Heijst και Birgit Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer. Στο *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*Joan Feigenbaum, επιμελητής, τόμος 576 στο *Lecture Notes in Computer Science*, σελίδες 470–484. Springer, 1991.

[24] David Chaum και Eugènevan Heyst. Group signatures. Στο *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*Donald W. Davies, επιμελητής, τόμος 547 στο *Lecture Notes in Computer Science*, σελίδες 257–265. Springer, 1991.

[25] Guomin Chen, Chunhui Wu, Wei Han, Xiaofeng Chen, Hyunrok Lee και Kwangjo Kim. A new receipt-free voting scheme based on linkable ring

signature for designated verifiers. Στο *2008 International Conference on Embedded Software and Systems Symposia*, σελίδες 18–23, 2008.

[26] Lidong Chen και Torben P. Pedersen. New group signature schemes (extended abstract). Στο *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*Alfredo De Santis, επιμελητής, τόμος 950 στο *Lecture Notes in Computer Science*, σελίδες 171–181. Springer, 1994.

[27] Ronald Cramer, Ivan Damgård και Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. Στο *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*Yvo Desmedt, επιμελητής, τόμος 839 στο *Lecture Notes in Computer Science*, σελίδες 174–187. Springer, 1994.

[28] Ronald Cramer και Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. Στο *Advances in Cryptology — CRYPTO '98*Hugo Krawczyk, επιμελητής, σελίδες 13–25, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[29] Giovanni Di Crescenzo και Rafail Ostrovsky. On concurrent zero-knowledge with pre-processing. Στο *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*Michael J. Wiener, επιμελητής, τόμος 1666 στο *Lecture Notes in Computer Science*, σελίδες 485–502. Springer, 1999.

[30] Yvo Desmedt και Moti Yung. Weakness of undeniable signature schemes (extended abstract). Στο *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*Donald W. Davies, επιμελητής, τόμος 547 στο *Lecture Notes in Computer Science*, σελίδες 205–220. Springer, 1991.

[31] Whitfield Diffie και Martin E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976.

[32] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[33] Uriel Feige, Dror Lapidot και Adi Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. *SIAM J. Comput.*, 29(1):1–28, 1999.

[34] Amos Fiat και Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. Στο *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*Andrew M. Odlyzko,

επιμελητής, τόμος 263 στο *Lecture Notes in Computer Science*, σελίδες 186–194. Springer, 1986.

[35] J.B. Fraleigh. *A First Course in Abstract Algebra*. Pearson Education, 2003.

[36] Steven D. Galbraith και Wenbo Mao. Invisibility and anonymity of undeniable and confirmer signatures. Στο *Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings*Marc Joye, επιμελητής, τόμος 2612 στο *Lecture Notes in Computer Science*, σελίδες 80–97. Springer, 2003.

[37] S. Goldwasser και M. Bellare. Lecture notes on cryptography, 2001.

[38] Shafi Goldwasser, Silvio Micali και Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[39] Helena Handschuh. *SHA Family (Secure Hash Algorithm)*, σελίδες 565–567. Springer US, Boston, MA, 2005.

[40] Javier Herranz και Germán Sáez. Forking lemmas in the ring signatures' scenario. *IACR Cryptol. ePrint Arch.*, σελίδα 67, 2003.

[41] Markus Jakobsson. Blackmailing using undeniable signatures. Στο *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*Alfredo De Santis, επιμελητής, τόμος 950 στο *Lecture Notes in Computer Science*, σελίδες 425–427. Springer, 1994.

[42] Markus Jakobsson, Kazue Sako και Russell Impagliazzo. Designated verifier proofs and their applications. Στο *Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'96, σελίδα 143–154, Berlin, Heidelberg, 1996. Springer-Verlag.

[43] Fabien Laguillaumie και Damien Vergnaud. Multi-designated verifiers signatures. Στο *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*Javier López, Sihan Qing και Eiji Okamoto, επιμελητές, τόμος 3269 στο *Lecture Notes in Computer Science*, σελίδες 495–507. Springer, 2004.

[44] Ji Seon Lee και Jik Hyun Chang. Strong designated verifier ring signature scheme. Στο *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering*Tarek Sobh, επιμελητής, σελίδες 543–547, Dordrecht, 2007. Springer Netherlands.

[45] Jin Li και Yanming Wang. Universal designated verifier ring signature (proof) without random oracles. Στο *Emerging Directions in Embedded and Ubiquitous Computing, EUC 2006 Workshops: NCUS, SecUbiq, USN, TRUST, ESO, and*

*MSA, Seoul, Korea, August 1-4, 2006, Proceedings*Xiaobo Zhou, Oleg Sokolsky, Lu Yan, Eun-Sun Jung, Zili Shao, Yi Mu, Dong Chun Lee, Daeyoung Kim, Young-Sik Jeong και Cheng-Zhong Xu, επιμελητές, τόμος 4097 στο *Lecture Notes in Computer Science*, σελίδες 332–341. Springer, 2006.

[46] Helger Lipmaa. On the cca1-security of elgamal and damgård's elgamal. Στο *Information Security and Cryptology - 6th International Conference, Inscrypt 2010, Shanghai, China, October 20-24, 2010, Revised Selected Papers*Xuejia Lai, Moti Yung και Dongdai Lin, επιμελητές, τόμος 6584 στο *Lecture Notes in Computer Science*, σελίδες 18–35. Springer, 2010.

[47] Helger Lipmaa, Guilin Wang και Feng Bao. Designated verifier signature schemes: Attacks, new security notions and a new construction. Στο *Automata, Languages and Programming, 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005, Proceedings*Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi και Moti Yung, επιμελητές, τόμος 3580 στο *Lecture Notes in Computer Science*, σελίδες 459–471. Springer, 2005.

[48] Joseph K. Liu, Man Ho Au, Willy Susilo και Jianying Zhou. Linkable ring signature with unconditional anonymity. *IEEE Trans. Knowl. Data Eng.*, 26(1):157–165, 2014.

[49] Joseph K. Liu, Willy Susilo και Duncan S. Wong. Ring signature with designated linkability. Στο *Advances in Information and Computer Security, First International Workshop on Security, IWSEC 2006, Kyoto, Japan, October 23-24, 2006, Proceedings*Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama και Shin-ichi Kawamura, επιμελητές, τόμος 4266 στο *Lecture Notes in Computer Science*, σελίδες 104–119. Springer, 2006.

[50] Joseph K. Liu, Victor K. Wei και Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups. *IACR Cryptol. ePrint Arch.*, 2004:27, 2004.

[51] Joseph K. Liu και Duncan S. Wong. Linkable ring signatures: Security models and new schemes. Στο *Computational Science and Its Applications - ICCSA 2005, International Conference, Singapore, May 9-12, 2005, Proceedings, Part II*Osvaldo Gervasi, Marina L. Gavrilova, Vipin Kumar, Antonio Laganà, Heow Pueh Lee, Youngsong Mun, David Taniar και Chih Jeng Kenneth Tan, επιμελητές, τόμος 3481 στο *Lecture Notes in Computer Science*, σελίδες 614–623. Springer, 2005.

[52] Yong Li, Willy Susilo, Yi Mu και Dingyi Pei. Designated verifier signature: Definition, framework and new constructions. Στο *Ubiquitous Intelligence and Computing*Jadwiga Indulska, Jianhua Ma, Laurence T. Yang, Theo Ungerer και Jiannong Cao, επιμελητές, σελίδες 1191–1200, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[53] Moni Naor. Deniable ring authentication. Στο *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*Moti Yung, επιμελητής, τόμος 2442 στο *Lecture Notes in Computer Science*, σελίδες 481–498. Springer, 2002.

[54] CORPORATE NIST. The digital signature standard. *Commun. ACM*, 35(7):36–40, 1992.

[55] Shen Noether. Ring signature confidential transactions for monero. *IACR Cryptol. ePrint Arch.*, σελίδα 1098, 2015.

[56] Wakaha Ogata, Kaoru Kurosawa και Swee Huay Heng. The security of the fdh variant of chaum's undeniable signature scheme. Στο *Public Key Cryptography - PKC 2005*Serge Vaudenay, επιμελητής, σελίδες 328–345, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[57] Tatsuaki Okamoto. Designated confirmer signatures and public-key encryption are equivalent. Στο *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*Yvo Desmedt, επιμελητής, τόμος 839 στο *Lecture Notes in Computer Science*, σελίδες 61–74. Springer, 1994.

[58] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. Στο *Advances in Cryptology — EUROCRYPT '99*Jacques Stern, επιμελητής, σελίδες 223–238, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[59] K.G. Paterson και Geraint Price. A comparison between traditional public key infrastructures and identity-based cryptography. *Information Security Technical Report*, 8:57–72, 2003.

[60] David Pointcheval και Jacques Stern. Security proofs for signature schemes. Στο *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*Ueli M. Maurer, επιμελητής, τόμος 1070 στο *Lecture Notes in Computer Science*, σελίδες 387–398. Springer, 1996.

[61] R. L. Rivest, A. Shamir και L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[62] Ronald L. Rivest, Adi Shamir και Yael Tauman. How to leak a secret. Στο *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*Colin Boyd, επιμελητής, τόμος 2248 στο *Lecture Notes in Computer Science*, σελίδες 552–565. Springer, 2001.

[63] Phillip Rogaway και Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. Στο *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*Bimal K. Roy και Willi Meier, επιμελητές, τόμος 3017 στο *Lecture Notes in Computer Science*, σελίδες 371–388. Springer, 2004.

[64] Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. Στο *40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA*, σελίδες 543–553. IEEE Computer Society, 1999.

[65] C. P. Schnorr. Efficient identification and signatures for smart cards. Στο *Advances in Cryptology — CRYPTO' 89 Proceedings*Gilles Brassard, επιμελητής, σελίδες 239–252, New York, NY, 1990. Springer New York.

[66] Adi Shamir. Identity-based cryptosystems and signature schemes. Στο *Advances in Cryptology*George Robert Blakley και David Chaum, επιμελητές, σελίδες 47–53, Berlin, Heidelberg, 1985. Springer Berlin Heidelberg.

[67] N.P. Smart. *Cryptography: An Introduction*. Mcgraw-hill education. McGraw-Hill, 2003.

[68] Ron Steinfeld, Laurence Bull, Huaxiong Wang και Josef Pieprzyk. Universal designated-verifier signatures. Στο *Advances in Cryptology - ASIACRYPT 2003*Chi Sung Laih, επιμελητής, σελίδες 523–542, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[69] Παγουρτζής, Α, Ζάχος, Ε και Γροντάς, Π. Υπολογιστική Κρυπτογραφία. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2015.

[70] Wilson Abel Alberto Torres, Ron Steinfeld, Amin Sakzad και Veronika Kuchta. Post-quantum linkable ring signature enabling distributed authorised ring confidential transactions in blockchain. *IACR Cryptol. ePrint Arch.*, σελίδα 1121, 2020.

[71] Patrick P. Tsang και Victor K. Wei. Short linkable ring signatures for e-voting, e-cash and attestation. *IACR Cryptol. ePrint Arch.*, σελίδα 281, 2004.

[72] Raylin Tso. A new way to generate a ring: Universal ring signature. *Comput. Math. Appl.*, 65(9):1350–1359, 2013.

[73] Joachimvon zur Gathen και Igor E. Shparlinski. Generating safe primes. *J. Math. Cryptol.*, 7(4):333–365, 2013.

[74] Douglas Wikström. Designated confirmer signatures revisited. *IACR Cryptol. ePrint Arch.*, σελίδα 123, 2006.

Συντομογραφίες - Ακρωνύμια

ΔΕ	Διπλωματική Εργασία
ΕΑΕ	Επεκτεταμένος Ευκλείδειος Αλγόριθμος
ΜΚΔ	Μέγιστος Κοινός Διαιρέτης
CCA	Chosen Ciphertext Attack
CDH	Computational Diffie-Hellman
CPA	Chosen Plaintext Attack
DDH	Decisional Diffie-Hellman
DLOG	Discrete Logarithm Assumption
DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm
DVLRS	Designated Verifier Linkable Ring Signatures
DVS	Designated Verifier Signatures
ECDSA	Elliptic Curve Digitan Signature Algorithm
LRS	Linkable Ring Signatures
LSAG	Linkable Spontaneous Anonymous Group
PKI	Public Key Infastructure
$\mathcal{RO}$	Random Oracle
RS	Ring Signatures
UDVS	Universal Designated Verifier Signatures
sDVS	strong Designated Verifier Signatures

Απόδοση ξενόγλωσσων όρων

Απόδοση	Ξενόγλωσσος όρος
αδιαμφισβήτητες υπογραφές	undeniable signatures
αδιαμφισβήτητες υπογραφές	undeniable signatures
ακεραιότητα	integrity
αλγόριθμος ψηφιακών υπογραφών	digital signature algorithm
αμελητέα συνάρτηση	negligible function
αντίσταση δεύτερου ορίσματος	second preimage resistance
αντίσταση πρώτου ορίσματος	first preimage resistance
ανωνυμία	anonymity
αποδείκτης	prover
αποκήρυξη	disavowal
αρχικοποίηση	setup
ασάφεια υπογράφοντος	signer ambiguity
ασφαλής πρώτος	safe prime
ασφαλής υπολογισμός πολλών μερών	secure multi party computation
γνησιότητα	message authentication
δέσμευση	commitment
δίκαιος	exculpable
διακρίσιμος	distinguishable
διαλογικός	interactive
δυσκολία εύρεσης συγκρούσεων	collision resistance
έγκυρη	valid
εγκυρότητα	validity
ειδική ορθότητα	special soundness
εξαγωγή	extract
εξουσιοδοτήσιμος	delegatable
επίθεση γνωστής υπογραφής	known signature attack
επίθεση γνωστού κρυπτοκειμένου	known ciphertext attack
επίθεση γνωστού μηνύματος	known message attack
επίθεση δημοσίου κλειδιού	key-only attack
επίθεση επιλεγμένου μηνύματος	chosen plaintext attack
επαναφορά στην επιτυχία	rewind on success
επαναφορά	rewind
καθολικός	universal

καθορισμένος επαληθευτής	designated verifier
κανονικό μοντέλο	standard model
κρυπτογραφία δημοσίου κλειδιού	public key cryptography
κρυπτοκείμενο	ciphertext
κρυπτοσύστημα	cryptosystem
λήμμα διακλάδωσης	forking lemma
λήμμα επαναφοράς στην επιτυχία	rewind on success lemma
μαντείο διαφθοράς	corruption oracle
μαντείο εγγραφής	joining oracle
μετατρέψιμες αδιαμφισβήτητες υπογραφές	convertible undeniable signatures
μη-αποκήρυξη	non-repudiation
μη-δυσφημίσιμος	non-slanderable
μη-μεταφέρσιμος	non-transferable
μη-πλαστογραφήσιμη	unforgeable
μη-φραγμένος	unbounded
μηδενική γνώσης	zero-knowledge
μοντέλο τυχαίου μαντείου	random oracle model
ολοκληρωτικό σπάσιμο	total break
ομαδικές υπογραφές	group signatures
ορθό ως προς προσομοίωση	simulation sound
πλεονέκτημα	advantage
πρακτικά	transcript
προσαρμοστικός	adaptive
προσομοίωση	simulation
πρόβλημα του διακριτού λογαρίθμου	discrete logarithm problem
πρόκληση	challenge
συμβολοσειρά κοινής αναφοράς	common reference string
συμβολοσειρά	string
συνάρτηση μονής κατεύθυνσης με καταπακτή	one-way trapdoor function
συνάρτηση σύνοψης	hash function
συνδέσιμος	linkable
συντριπτικός	overwhelming
σχετικά πρώτοι αριθμοί	coprime numbers
τίμιος	honest
υπογράφοντας	signer
υπογραφές ισχυρά καθορισμένου επαληθευτή	strong designated verifier signatures
υπογραφές καθορισμένου επαληθευτή	designated verifier signatures
υπογραφές καθορισμένου επιβεβαιωτή	designated confirmer signatures
υπογραφή δακτυλίου	ring signature
υποδομή δημοσίου κλειδιού	public key infastructure
υπολογιστικά	computationally
ψευδώνυμο	pseudoidentity
ψηφιακή υπογραφή	digital signature