ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή με Άνευ Όρων Ανωνυμία

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΙΩΑΝΝΗ Ζ. ΒΡΕΤΤΟΥ

Επιβλέπων
Αριστείδης Παγουρτζής
Καθηγητής Ε.Μ.Π

Αθήνα, Φεβρουάριος 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευητή με Άνευ Όρων Ανωνυμία

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΙΩΑΝΝΗ Ζ. ΒΡΕΤΤΟΥ

Επιβλέπων: Αριστείδης Παγουρτζής

Αθήνα, Φεβρουάριος 2023

Ευχαριστίες

Η ολοκλήρωση της διπλωματίκης εργασίας σηματοδοτεί και την ολοκλήρωση των προπτυχιακών σπουδών, ως εκ τούτο επιθυμώ να αδράξω την ευκαιρία και να ευχαριστήσω όλους όσους με βοήθησαν να φέρω εις πέρας όχι μόνο τη συγκεκριμένη εργασία άλλα και τις σπουδές μου στο συνολό τους.

Για αρχή έχω να πω ένα μεγάλο ευχαριστώ στον Άρη Παγουρτζή. Η βοηθειά του κατά την διάρκεια της εκπόνησης ήταν ανεκτίμητη, πάντα διαθέσιμος για να εκφράσω απορίες και προβληματισμούς παρά το δικό του τεράστιο φόρτο ευθηνών και υποχρεώσεων. Πέραν όμως της επίβλεψης με ωθούσε συνέχεια να προσπαθώ να βελτιώνομαι, με ενθάρυνε παρά τις ανασφαλειές μου και μου έδινε χώρο να εκφράσω ελεύθερα και ισάξια τη θέση μου. Θεωρώ πως αποτελεί ένα λαμπρό παράδειγμα εκπαδευτικού, επιστήμονα και ανθρώπου πάντα δίπλα στους φοιτητές του, ακόμα και με προσωπικό του κόστος.

Θα ήθελα επίσης να ευχαριστήσω τον Παναγιώτη Γροντά για την υπομονή που έδειξε στο να προσαρμοστώ στα δεδομένα εργασίας στο πλαίσιο ομάδας, για την συνεργασία μας στην συγγραφή της εργασίας που δημοσιεύσαμε και στην διαθεσιμοτητά του στο να μου λύνει απορίες όποτε και αν προέκυπταν.

Επίσης θα ήθελα να ευχαριστήσω τις Pouran Behrouz, Μαριάννα Σπυράκου και Δανάη Μπάλλα. Ο χρόνος που πέρασα μαζί τους τόσο στη συνεργατική δουλεία μας όσο και σε απλές και καθημερινές στιγμές ήταν υπέροχος, γεμάτος γέλια, αστεία και εξαιρετική συνεργασία.

Ένα ευχαριστώ πρέπει να δωθεί και στο Βαγγέλη Κωνσταντακάκο του οποίο η δουλεία και διπλωματίκη εργασία αποτέλεσαν τη βάση για το παρόν έργο.

Ο χρόνος που πέρασα με όλα τα μέλη του CoRe Lab και ιδιαίτερα με την ομάδα του Crypto Group είναι οι ωραιότερες στιγμές των μέχρι τώρα σπουδών μου και θα μου μείνουν αξέχαστες.

Οφείλω ένα τεράστιο ευχαριστώ στην οικογενειά μου, και ιδιαίτερα στη μητέρα μου Κατερίνα, στον αδελφό μου Βασίλη, στη γιαγιά μου Κούλα και στη θεία μου Ματίνα, που ήταν εκεί για εμένα από μικρό παιδί, που με στήριξαν καθ' όλη την διάρκεια των σπουδών μου και που πίστεψαν σε εμένα πολύ περισσότερο από πίστεψα εγώ σε εμένα.

Θέλω επίσης να ευχαριστήσω τους φίλους μου που ήταν δίπλα μου κατά την διάρκεια των σπουδών και που αναγκάστηκαν να ακούσουν ατελείωτες ώρες διαλέξων για μαθηματικά και ιδιαίτερα για κρυπτογραφία, συχνά παρά τη θελησή τους.

Τέλος θα ήθελα να ευχαριστήσω το Γιώργο Λιακόγγονα, που έστω και αθελά του, με ενέπνευσε να ακολουθήσω σπουδές στο χώρο των μαθηματικών και με στήριξε ιδιαίτερα κατά τη διάρκεια των σπουδών μου.

Περίληψη

Σκοπός της παρούσας εργασίας είναι η μελέτη των ψηφιακών υπογραφών με επιπλέον λειτουργικότητες. Εστιάζουμε σε δύο κύρια είδη, τις Συνδέσιμες Υπογραφές Δακτυλίου (LRS) και τις Υπογραφές Καθορισμένου Επαληθευτή (DVS), καθώς και στον καινοτόμο συνδυασμό τους τις Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή (DVLRS). Κύριος στόχος μας είναι η αναβαθμισή των DVLRS σε σχήμα με άνευ όρων ανωνυμία. Το επίτευγμα αυτό το ονομάζουμε Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή με άνευ όρων ανωνυμία (UDVLRS). Θα παρουσιάσουμε την πορεία που έχουν ακολουθήσει οι προηγούμενες υπογραφές μέσα στην βιβλιογραφία, θα μελετήσουμε τις κατασκευές τους, τα μοντέλα που προτείνονται, ενώ θα δώσουμε ιδιαίτερη έμφεση στις ιδιότητες ασφάλειας που προσφέρει το κάθε σχήμα υπογραφής. Για τις UDVLRS θα παρουσιάσουμε το τροποποιημένο μοντέλο που προκύπτει από τις DVLRS και τις LRS με άνευ όρων ανωνυμία, τους ορισμούς για τις ιδιότητες ασφάλειας καθώς και μία ασφαλή κατασκευή την ασφάλεια της οποίας αποδεικνύομε στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$.

Λέξεις Κλειδιά

Κρυπτογραφία Δημοσίου Κλειδιού, Ψηφιακές Υπογραφές, Συνδέσιμες Υπογραφές Δακτυλίου, Υπογραφές Καθορισμένου Επαληθευτή, Μη-Πλαστογραφισημότητα, Άνευ Όρων Ανωνυμία, Μη-Μεταφερσημότητα, Συνδεσιμότητα, Μη-Συκοφαντία.

Abstract

In this thesis we study digital signature schemes with additional functionalities. We focus on two main types, Linkable Ring Signatures (LRS) and Designated Verifier Signatures (DVS) along with their novel combination Designated Verifier Linkable Ring Signatures (DVLRS). Our main target is to upgrade the DVLRS scheme to one with unconditional anonymity. This combination of DVLRS and LRS with unconditional anonymity we call Designated Verifier Linkable Ring Signatures with unconditional anonymity (UDVLRS). We present the evolution of the previous signature schemes, we will study their constructions and the proposed models with great emphasis on the security properties of each signature scheme. For UDVLRS we will provide the augmented security model which comes from combining DVLRS and LRS with unconditional anonymity, the definitions of the security properties alongside a secure construction whose security is proven in the random oracle $\mathcal{RO}$ model.

Keywords

Public Key Cryptography, Digital Signatures, Linkable Ring Signatures, Designated Verifier Signatures, Unforgeability, Unconditional Anonymity, Non-Transferability, Linkability, Non-Slanderability.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Ένα από τα μεγαλύτερα επιτεύγματα της σύγχρονης κρυπτογραφίας αποτελούν οι ψηφιακές υπογραφές. Η ανάγκη τους προκύπτει ταυτόχρονα με τη γέννηση αυτού που αποκαλούμε σύγχρονη ή ασύμμετρη κρυπτογραφία, ενώ η δημιουργία τους συμπίπτει με τη δημιουργία των πρώτων μη-συμμετρικών κρυπτοσυστημάτων.

Η κύρια χρήση μίας ψηφιακής υπογραφής είναι η απόδειξη της ταυτότητας του συγγραφέα ενός μηνύματος. Σε αυτό δεν διαφέρουν από το αναλογικό τους ανάλογο, όμως με το πέρασμα των χρόνων έχει προκύψει μία πληθώρα ψηφιακών υπογραφών που διαθέτουν περαιτέρω λειτουργηκότητες. Δύο που θα μας απασχολήσουν σε αυτή τη διπλωματική εργασία είναι οι συνδέσιμες υπογαραφές δακτυλίου (linkable ring signatures-LRS) και οι υπογραφές καθορισμένου επαληθευτή (designated verifier signatures-DVS). Οι πρώτες επιτρέπουν στον υπογράφων να κρύβεται μέσα σε ένα σύνλο ανωνυμίας άλλων ατόμων, δισφαλίζοντας έτσι την ανωνυμία του ενώ αποδεικνύουν τη συμμετοχή σε αυτό το σύνολο, ενώ παράλληλα συνδέουν τις υπογραφές με ίδια προέλευση χωρίς όμως να προδίδουν την ταυτότητα του υπογραφοντά τους. Οι δεύτερες επιτρέπουν σε μία υπογραφή να είναι χρήσιμη μόνο για μία οντότητα, αυτή του καθορισμένου επαληθευτή.

Το 2021 οι Behrouz, Γροντάς, Κωνσταντακάκος, Παγουρτζής, και Σπυράκου εισήγαγαν τις DVLRS [13] (Designated Verifier Linkable Ring Signatures), ή αλλιώς Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή. Έδωσαν επίσης υλοποίηση τους και μοντέλο ασφάλειας το οποίο απέδειξαν στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$. Οι DVLRS αποτελούν την πρώτη επιτυχή ένωση των LRS και DVS.

Ένα ζήτημα που ταλανίζει τις LRS είναι αυτό της ανωνυμίας, συγκεκριμένα η ανωνυμία οποιουδήποτε σχήματος LRS είναι υπολογιστική και βασισμένη στην δυσκολία επίλυσης κάποιου NP προβλήματος, με συνηθέστερο το DLOG. Το 2014 οι δημιουργοί των LRS εισάγουν τις ULRS [56], Linkable Ring Signatures

with unconditional anonymity, ή αλλιώς Συνδέσιμες Υπογραφές Δακτυλίου με άνευ όρων Ανωνυμία. Οι DVLRS κληρονομούν και αυτές το πρόβλημα της υπό όρων ανωνυμίας από τις LRS και η βλέψη για αναβαθμισή τους σε σχήμα υπογραφών με άνευ όρων ανωνυμία υπήρχε ήδη από τη δημιουργία τους. Στη συγκεκριμένη εργασία επιτυχγάνουμε ακριβώς αυτό, συνδυάζουμε τις ULRS με τις DVLRS δίνοντας γέννηση στις UDVLRS (Designated Verifier Linkable Ring Signatures with unconditional anonymity-Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή με άνευ όρων ανωνυμία), παραθέτουμε υλοποιησή τους και μοντέλο ασφάλειας το οποίο και αποδεικνύομε στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$.

Η εργάσια διαθρώνεται με τον ακόλουθω τρόπο:

Στο κεφάλαιο 2 κάνουμε μία εισαγωγή σε βασικές γνώσης κρυπτογραφίας που κρίνονται αναγκαίες για την κατανόηση της ΔΕ. Δίνουμε παραδείγματα κρυπτοσυστημάτων δημοσίου κλειδιού και παραθέτουμε βασικούς ορισμούς.

Στο κεφάλαιο 3 ορίζουμε τα σχήματα ψηφιακών υπογραφών, τις απαιτήσεις ασφαλείας και μελετάμε τις ψηφιακές υπογραφές ElGamal, DSA, και Schnorr.

Στο κεφάλαιο 4 μελετάμε τις αδιαμφισβήτητες υπογραφές (Undeniable Signatures) και τις υπογραφές καθορισμένου επαληθευτή (Designated Verifier Signature - DVS).

Στο κεφάλαιο 5 μελετάμε τις υπογραφές δακτυλίου (Ring Signatures - RS), τις υπογραφές ομάδων (Group Signatures), και τις συνδέσιμες υπογραφές δακτυλίου (Linkable Ring Signatures - LRS). Επιπλέον μελετάμε το πρόβλημα ανωνυμίας στα σχήματα LRS και πως αυτό μπορεί να λυθεί σε ορισμένες περιπτώσεις.

Στο κεφάλαιο 6 παραθέτουμε το σχήμα υπογραφών DVLRS.

Στο κεφάλαιο 7 έχουμε το σημαντικότερο μέρος της ΔΕ. Προτείνουμε τις Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή με άνευ όρων ανωνυμία (UDVLRS), αναλύουμε το μοντέλο ασφαλειάς τους, και παραθέτουμε κατασκευή την ασφάλεια της οποίας αποδεικνύομε πλήρως στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$.

Στο κεφάλαιο 8 θα αναφέρουμε δύο εφαμογές των UDVLRS.

Τέλος στο κεφάλαιο 9 αναφέρουμε ορισμένες μελλοντικές κατευθύνσεις που σκοπεύουμε να ακολουθήσουμε με τις DVLRS και UDVLRS.

Σημειώση: Καθ' όλη την έκταση της ΔΕ γίνεται αναφορά στην έννοια *Άνευ Όρων*. Με αυτό τον όρο μεταφράζουμε τον όρο *Uncondtional* της ξένης βιβλιογραφίας, η σημασία του συγκεκριμένου όρου εξηγεί ότι η ασφάλεια δε βασίζεται σε κάποια υπόθεση δυσκολίας ενός προβλήματος. Ένας άλλος πιο εύστοχος τρόπος περιγραφής της συγκεκριμένης έννοιας αποτελεί η λεγώμενη *Πληροφοριοθεωρητική (Inforamation Theoretic - IT)* όπως αυτή ορίζεται από τον Shannon [74].

Κεφάλαιο 2

Βασικές Έννοιες Κρυπτογραφίας Δημοσίου Κλειδιού

Ο κύριος στόχος της κρυπτογραφίας είναι η ανταλλαγή μηνυμάτων μεταξύ δύο ή περισσότερων οντοτήτων με τέτοιο τρόπο ώστε το περιεχόμενό τους να μην μπορεί να αναγνωσθεί από τρίτες οντότητες, δηλαδή πιθανούς ωτακουστές. Ιστορικά για την κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος ήταν αναγκαία η γνώση μόνο ενός μυστικού κλειδιού, π.χ. στον κώδικα του Καίσαρα για την ανάγνωση και την κρυπτογράφηση ενός μηνύματος έπρεπε να έχει προσυμφωνηθεί κατά πόσο θα μετακινηθούν τα γράμματα του Λατινικού αλφάβητου. Σε πιο σύγχρονες περιπτώσεις, π.χ. στον κώδικα Enigma, υπήρχαν βιβλία με κώδικες και ήταν αναγκαστική η επικοινωνία με τα εκάστοτε επιτελεία ώστε να ακολουθούν όλες οι συσκευές τις ίδιες ρυθμίσεις.

Είναι κατανοητό πως όταν αυξάνεται σημαντικά το πλήθος των οντοτήτων που πρέπει να επικοινωνούν μεταξύ τους η πολυπλοκότητα της ανταλλαγής των απαραίτητων πληροφοριών για να είναι εφικτή η μεταξύ τους επικοινωνία αυξάνεται σημαντικά. Συγκεκριμένα είναι εξαιρετικά δύσκολη η ανταλλαγή, διαφύλαξη, και διαχείρηση ενός μεγάλου πλήθους κλειδιών κρυπτογράφησης.

Το παραπάνω πρόβλημα ονομάζεται το Πρόβλημα Διανομής Κλειδιών (Key Distribution Problem), και λύση σε αυτό το πρόβλημα προσφέρει η κρυπτογραφία δημοσίου κλειδιού, ή αλλιώς ασύμμετρη κρυπτογραφία. Η ιδέα της κρυπτογραφίας δημοσίου κλειδιού βασίζεται στη θεμελιώδη δουλεία των Diffie και Hellman [34], που την πρότειναν το 1976, ενώ το 1977 προτάθηκε και το πρώτο κρυπτσύστημα δημοσίου κλειδιού από τους Rivest, Shamir,και Adleman στην εργασία [68].

Το συγκεκριμένο κεφάλαιο θα αποτελέσει μια απλή εισαγωγή σε μερικές από τις βασικές έννοιες της κρυπτογραφίας δημοσίου κλειδιού. Συγκεκριμένα

θα δώσουμε μερικούς ορισμούς ασφάλειας που θα χρειαστούμε στη συνέχεια της ΔΕ, καθώς και μερικές από τις πιο συνηθισμένες παραδοχές που γίνονται στη κρυπτογραφία δημοσίου κλειδιού. Θα βασιστούμε, επί το πλήστον, στα αντίστοιχα κεφάλαια εισαγωγής στην ασύμμετρη κρυπρογραφία των ακόλουθων βιβλίων : [33, 81, 82, 48]. Σημειώνουμε πως για την καλύτερη κατανόηση του συγκεκριμένου κεφαλαίαου είναι αναγκαίες ορισμένες βασικές έννοιες θεωρίας αριθμών, θεωρίας ομάδων, και θεωρίας υπολογισμού.

2.1 Συναρτήσεις Μονής Κατεύθυνησης με Καταπακτή

Ξεκινάμε με τη συγκεκριμένη ενότητα ορίζοντας ένα ισχυρό εργαλείο της ασύμμετρης κρυπρογραφίας, τις συναρτήσεις μονής κατεύθυνησης με καταπακτή. Εν συνεχεία θα δούμε πως αξιοποιήθηκαν για την επίλυση του προβλήματος διαμείρασης κλειδιών, καθώς και για το πως χρησιμοποιούνται στο κρυπτοσύστημα RSA .

Πριν όμως αναφερθούμε σε αυτές τις εξαιρετικά χρήσιμες συναρτήσεις θα δώσουμε δύο επιπλέον ορισμούς που είναι βοηθητικές στην καλύτερη κατανόηση της εν λόγω ΔΕ.

Ορισμός 2.1. *Αμελητέα Συνάρτηση*

Μία συνάρτηση negl θα αποκαλείται αμελητέα, εάν για κάθε πολυώνυμο p υπάρχει n_0 τέτοιο ώστε για κάθε $n \geq n_0$ να ισχύει :

$$negl(n) < \frac{1}{p(n)}$$

Ένα εύκολο, και συχνό, παράδειγμα είναι η $f(x) = \frac{1}{2^x}$

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

Ένας αλγόριθμος $\mathcal{A}$ θα καλείτε Πιθανοτικός Αλγόριθμος Πολυωνιμικού Χρόνου, από τούδε και στο εξής απλά PPT*, εάν για κάθε είσοδο $x \in \{0,1\}^*$ υπάρχει πολυώνυμο p, έτσι ώστε ο $\mathcal{A}$ να υπολογίζει το $\mathcal{A}(x)$ σε χρόνο $O(p(|x|))$, και ο $\mathcal{A}$ μπορεί να ρίχνει τυχαία νομίσματα.*

Στην έκταση αυτής τη ΔΕ γίνεται η παρακάτω σύμβαση, η οποία είναι μια σύμβαση που ακολουθείτε εκτενώς στον χώρο της Κρυπτογραφίας: Όταν λέμε ότι κάτι είναι 'ευκόλος υπολογίσιμο', ή όταν αναφερόμαστε σε 'αποδοτικό αλγόριθμο', εννοούμε πως υπάρχει PPT αλγόριθμος για να εκτελέσει τον συγκεκριμένο υπολογισμό.

Ορισμός 2.3. *Συναρτήσεις Μονής Κατεύθυνησης*
Μία συνάρτηση $f : \{0,1\}^* \to \{0,1\}^*$ θα καλείτε συνάρτηση μονής κατεύθυνησης εάν ισχύει ότι:

- *Η f είναι $1-1$*
- *Υπάρχει* PPT *αλγόριθμος που για κάθε έγκυρη είσοδο x, υπολογίζει το $f(x)$*
- *Για κάθε* PPT $\mathcal{A}$ *η πιθανότητα αντιστροφής του $f(x)$ είναι αμελητέα, ή πιο αυστηρά Για κάθε* PPT $\mathcal{A}$ *υπάρχει αμελητέα συνάρτηση $negl_{\mathcal{A}}$ ώστε για μεγάλα k να ισχύει:*

$$Pr[f(z) = y; x \leftarrow \{0,1\}^k; y \to f(x); z \to \mathcal{A}(1^k, y)] \leq negl_{\mathcal{A}}(k)$$

Διαισθητικά μία συνάρτηση μονής κατεύθυνησης είναι εύκολη στον υπολογισμό, αλλά η αντιστροφή της αποτελεί απρόσιτο πρόβλημα. Η ύπαρξη συναρτήσεων μονής κατεύθυνης αποτελεί ανοιχτό πρόβλημα της Θεωρίας Πολυπλοκότητας, συγκεκριμένα συναρτήσεις μονής κατεύθυνησης υπάρχουν ανν $P \neq UP$. Για μερικές παραπάνω λεπτομέρειες συνιστάται το Κεφάλαιο 3 από το σύγγραμμα[81].

Ορισμός 2.4. *Συνάρτηση Μονής Κατεύθυνσης με Καταπακτή*
Έστω μια συνάρτηση μονής κατεύθυνησης f. Αν υπάρχει μυστική πληροφορία τέτοια ώστε ο υπολογισμός της f^{-1} να είναι εύκολος, τότε θα λέμε ότι η f είναι συνάρτηση μονής κατεύθυνησης με καταπατκή.

Δε ξέρουμε ακόμα θεωρητικά αν υπάρχουν συναρτήσεις μονής κατεύθυνησης με καταπακτή, το $P \neq NP$ αποτελεί μια ικανή συνθήκη για το πρόβλημα ύπαρξης τους. Παρ' όλα αυτά υπάρχουν ορισμένα προβλήματα τα οποία θεωρούνται δύσκολα και πάνω σε αυτά μπορούμε να κατασκευάσουμε συναρτήσεις μονής κατεύθυνης με καταπατκή.

Ένα από αυτά, το πρόβλημα παραγοντοποίησης σε πρώτους, θα αναλυθεί περαιτέρω στην παρακάτω υποενότητα.

2.1.1 Το Πρόβλημα Παραγοντοποίησης - Μία Απλή Συνάρτηση Μονής Κατεύθυνησης με Καταπακτή

Έστω $f(p,q) = p \cdot q$. Ο υπολογισμός γινομένου είναι ένα εύκολο πρόβλημα, όμως η παραγοντοποίηση ενός αριθμού σε γινόμενο πρώτων αποτελεί ένα δύσκολο πρόβλημα. Ακόμα δεν έχει βρεθεί κάποιος αποδοτικός αλγόριθμος,

το 2021 ο Schnorr είχε δημοσιεύσει μια εργασία στην οποία δήλωνε πως έλυνε το πρόβλημα παραγοντοποίησης ακεραίων [73], κάτι τέτοιο όμως (ευτυχώς) δεν ισχύει.

Από το πρόβλημα της παραγοντοποίησης πηγάζει και ένα ακόμα πρόβλημα, το λεγώμενο πρόβλημα RSA. Ας δούμε πως προκύπτει:

Ορισμός 2.5. *Πρόβλημα RSA*
Δοθέντος $n = p \cdot q$, όπου p, q πρώτοι, e τέτοιο ώστε $MK\Delta(e, (\phi(n))) = 1$, και c ζητείται m έτσι ώστε $c = m^e \mod n$

Ο υπλογισμός της συνάρτησης $RSA_{(n,e)}(m) = m^e \mod n = c$ είναι εύκολος, όμως η αντιστροφή της, γνωστή και ως εύρεση της e-οστής ρίζας του c είναι δύσκολη.

Αν κάποιος γνωρίζει την παραγοντοποίηση του n, δηλαδή τα p και q, τότε μπορεί με ευκολία να μάθει το n ακολουθώντας τηςν παρακάτω διαδικασία:

1. Υπολόγισε $\varphi(n) = (p-1)(q-1)$

2. Με χρήση επεκτεταμένου ευκλείδιου αλγόριθμου βρες d τέτοιο ώστε: $d = e^{-1} \mod \varphi(n)$

3. Υπολόγισε $c^d \mod n = (m^e)^d \mod n = m$

Βλέπουμε πως η $RSA_{(n,e)}$ με τον τρόπο που ορίστηκε αποτελεί μία συνάρτηση μονής κατεύθυνησης με καταπακτή. Ακόμα βλέπουμε πως αν το πρόβλημα της παραγοντοποίησης είναι εύκολο τότε και το πρόβλημα RSA είναι εύκολο, το αντίστροφο είναι ακόμα ανοιχτό πρόβλημα.

Σε αυτό το σημείο σημειώνουμε πως υπάρχουν και άλλα προβλήματα που σχετίζονται με το RSA και την παραγοντοποίηση, καθώς και με αναγωγές αυτών. Για όποιον ενδιαφέρεται το κεφάλαιο 6 του συγγράμματος [81] μπορεί να προσφέρει περαιτέρω πληροφορίες.

2.1.2 Το Πρόβλημα του Διακριτού Λογαρίθμου - Υποθέσεις CDH / DDH

Ένα ακόμα σημαντικό πρόβλημα που χρησιμοποιείται εκτενώς στην Κρυπτογραφία είναι το Πρόβλημα του Διακριτού Λογαρίθμου. Αυστηρά το ορίζουμε ως εξής:

Ορισμός 2.6. *Πρόβλημα Διακριτού Λογαρίθμου (*DLP*)*
Έστω $\mathbb{G}$ πεπερασμένη κυκλική ομάδα και g ένας από τους γεννήτορες της. Δοθέντος $h \in \mathbb{G}$ ζητείται $x < |\mathbb{G}|$, έτσι ώστε $g^x = h$.

Το παραπάνω πρόβλημα δεν είναι το ίδιο δύσκολο για όλα τα δυνατά στιγμυότυπα. Αν για παράδειγμα στη θέση της ομάδας $\mathbb{G}$ έχουμε την $(\mathbb{Z}_p, +)$, με p πρώτο, τότε μπορούμε να λύσουμε το πρόβλημα του διακριτού λογαρίθμου απλά με χρήση του επεκτεταμένου ευκλείδιου αλγόριθμου.

Από την άλλη αν ισχύει ότι $(\mathbb{G}, \cdot) < (\mathbb{Z}_p^*, \cdot)$, με $|\mathbb{G}| = q$ και p, q είναι μεγάλοι πρώτοι, τουλάχιστον 1024 bits, τότε το Πρόβλημα του Διακριτού Λογαρίθμου δε θεωρείται εύκολα επιλύσιμο. Μια ακόμα καλή επιλογή ομάδων για τις οποίες το DLP θεωρείται δύσκολο είναι οι προσθετικές υποομάδες σημείων ελλειπτικών καμπυλών πάνω από πεπερασμένα σώματα, $(\mathbb{G}, +) < (\mathcal{E}(\mathbb{F}_p), +)$.

Ορισμός 2.7. *Υπόθεση Διακριτού Λογαρίθμου (*DLOG*)*
Θα λέμε ότι σε μια ομάδα $\mathbb{G}$ ισχύει η Υπόθεση του Διακριτού Λογαρίθμου εάν για κάθε PPT *αλγόριθμο $\mathcal{A}$ υπάρχει αμελητέα συνάρτηση $negl_{\mathcal{A}}$ έτσι ώστε:*

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

Εκτός από το Πρόβλημα του Διακριτού υπάρχουν ακόμα δύο προβλήματα που σχετίζονται άμεσα μαζί του. Πρόκειται για το Υπολογιστικό Πρόβλημα Diffie - Hellman (CDH) και το Πρόβλημα Απόφασης Diffie - Hellman (DDH).

Ορισμός 2.8. *Υπολογιστικό Πρόβλημα Diffie - Hellman (*CDHP*)*
Έστω $\mathbb{G}$ πεπερασμένη κυκλική ομάδα, με g κάποιο γεννήτορα της και εστω ακόμα $g^{\alpha}, g^{\beta} \in \mathbb{G}$. Ζητείται να υπολογιστεί $g^{\alpha\beta} \in \mathbb{G}$.

Ορισμός 2.9. *Πρόβλημα Απόφασης Diffie - Hellman(*DDHP*)*
Έστω $\mathbb{G}$ πεπερασμένη κυκλική ομάδα, με g κάποιο γεννήτορα της και εστω ακόμα $g^{\alpha}, g^{\beta}, g^{\gamma} \in \mathbb{G}$. Ζητείται να βρεθεί αν $\gamma = \alpha \cdot \beta$.

Τα παραπάνω προβλήματα έχουν και αυτά τις δικές τους υποθέσεις που ορίζονται με ανάλογο τρόπο όπως η υπόθεση 2.7.

Στα σχήματα υπογραφών, καθώς και στα υπόλοιπα κρυπτογραφικά πρωτόκολλα που θα συναντήσουμε δε θα μπούμε σε πολλές λεπτομέρειες για αυτές τις ομάδες. Το σημαντικό για τώρα είναι ότι υπάρχουν και ότι μπορούμε, δουλεύοντας πάνω τους, να βασίσουμε στις προηγούμενες υποθέσεις την ασφάλεια των κατασκευών μας. Θα λέμε για παράδειγμα ότι δουλεύουμε σε μια ομάδα $\mathbb{G}$ τάξης q για την οποία ισχύει η DLOG.

Ένα ακόμα σημαντικό θεώρημα που θα φανεί ιδιαίτερα χρήσιμο σε αποδείξεις είναι το ακόλουθω:

Θεώρημα 2.1. DDHP $\leq$ CDHP $\leq$ DLP

Απόδειξη: Αν μπορούμε να λύσουμε το DLP*, τότε από το $x = g^{\alpha}$ και $y = g^{\beta}$ μπορούμε να υπολογίσουμε τα α, β και με ύψωση σε δύναμη να βρούμε το $g^{\alpha\beta}$. Αν μπορούμε να λύσουμε το* CDHP *τότε με τα δεδομένα*

του DDHP *μπορούμε να υπολογίσουμε το* $g^{\alpha\beta}$ *και να αποφανθούμε περί της ορθότητας της ισότητας.* □

Το αντίστροφο δεν έχει αποδειχθεί ακόμα.

2.1.3 Το Σχήμα Ανταλλαγής Κλειδιών Diffie - Hellman

Στην εισαγωγή του κεφαλαίαου αναφέραμε πως ένα από τα σημαντικότερα προβλήματα της Κρυπτογραφίας του 20ου αιώνα ήταν το πρόβλημα διανομής κλειδιών πάνω από δημόσια, και άρα μη ασφαλή, κανάλια επικοινωνίας. Όπως είπαμε στην ιστορική εργασία τους οι Diffie και Hellman [34] κατάφεραν να λύσουν αυτό το πρόβλημα δίνοντας ένα πρωτόκολλο για ακριβώς αυτή τη δουλεία. Με αυτό τον τρόπο δύο άτομα που ήθελαν να ανταλλάξουν ένα κοινό μυστικό, π.χ. ένα κλειδί DES, μπορούσαν να το κάνουν δίχως να είναι αναγκάια κάποια συνάντηση από πριν.

Παρακάτω παραθέτουμε το πρωτόκολλο ανταλλαγής κλειδιών Diffie - Hellman.

Έστω δύο άτομα η Alice και ο Bob που θέλουν να συμφωνήσουν σε ένα κοινό μυστικό, όμως υπάρχει το μόνο διαθέσιμο κανάλι επικοινωνίας είναι δημόσιο και άρα διατρέχουν το κύνδινο το μυστικό τους να υποπέσει στα χέρια ωτακουστών. Για να επικοινωνήσουν με ασφάλεια μπορούν να εκτελέσουν την εξής διαδικασία:

1. Αρχικά δημοσιεύεται ένας πρώτος αριθμός p, κατάλληλα επιλεγμένος ώστε να ισχύει η υπόθεση DLOG, μαζί με έναν γεννήτορα g της $\mathbb{Z}_p^*$.

2. Η Alice επιλέγει τυχαία $\alpha \in_R \mathbb{Z}_p^*$, υπολογίζει $y_\alpha = g^\alpha \mod p$, και το στέλνει στον Bob.

3. Ο Bob επιλέγει τυχαία $\beta \in_R \mathbb{Z}_p^*$, υπολογίζει $y_\beta = g^\beta \mod p$, και το στέλνει στην Alice.

4. Ο Bob λαμβάνει $g^\alpha \mod p$ και υπολογίζει $K = (g^\alpha)^\beta \mod p$.

5. Η Alice λαμβάνει $g^\beta \mod p$ και υπολογίζει $K = (g^\beta)^\alpha \mod p$.

6. Το κοινό μυστικό είναι $K = g^{\alpha\beta} \mod p$

Το παραπάνω πρωτόκολλο είναι ασφαλές ενάντια παθητικών αντιπάλων, απλών ωτακουστών. Μια απλή, αλλά όχι αυστηρή, απόδειξη είναι η εξής. Έστω ότι η Eve παρακολουθεί το κανάλι και επιθυμεί να μάθει ποιο είναι το μυστικό μεταξύ της Alice και του Bob. Έχει γνώση των επιλεγμένων παραμέτρων,

δηλαδή της ομάδας και του γεννήτορα στον οποίο γίνεται η κωδικοποίηση των μηνυμάτων, και επιπλέον μπορεί να δει τα y_α, y_β. Πρέπει λοιπόν από αυτά τα δεδομένα να εξάγει το $K = g^{\alpha\beta}$. Αυτό όμως είναι ακριβώς ένα στιγμυότυπο του CDHP το οποίο θεωρούμε ότι είναι δύσκολο με αυτές τις παραμέτρους. Άρα η Eve δε μπορεί να μάθει ποιο είναι το μυστικό. Για μία πιο ενδελεχή απόδειξη προτείνεται το κεφάλαιο κρυπτογραφίας δημοσίου κλειδιού του παρακάτω συγγραμμάτος [81].

Το πρόβλημα που τίθεται όμως είναι το εξής: Τι συμβαίνει στην ασφάλεια του πρωτοκόλλου εάν ο αντίπαλος δεν είναι παθητικός; Ένα απλό παράδειγμα είναι αν ο αντίπαλος αναχαιτίζει τα μηνύματα που στέλνει η Alice και ο Bob και προωθεί κακόβουλα μηνύματα της επιλογής του. Με αυτό τον τρόπο η Alice και ο Bob δεν μπορούν να ορίσουν ένα κοινό μυστικό. Τέτοιες επιθέσεις λέγονται Man in the Middle Attacks.

Ένα ακόμα θέμα είναι κάποια πιθανή διαρροή πληροφοριών απο τα δημόσια μηνύματα.

Για περισσότερες πληροφορίες σχετικά με τα προβλήματα του Ανώνυμου Πρωτοκόλλου Diffie - Hellman μπορούν να βρεθούν στο κεφάλαιο 10 του [33].

Ένας τρόπος για να αντιμετωπιστούν οι επιθέσεις τύπου Man in the Middle είναι μέσω των ψηφιακών υπογραφών. Μέσω αυτών κάποιος μπορεί να βεβαιώσει την ταυτότητα του αποστολέα ενός μηνύματος και άρα να αντιμετωπίσει το πρόβλημα αυτών των επιθέσεων.

2.2 Κρυπτοσυστήματα Δημοσίου Κλειδιού

Σε αυτή την ενότητα θα ορίσουμε αυστηρά από τι αποτελείται ένα Κρυπτοσύστημα Δημοσίου Κλειδιού, επιπλέον θα ορίσουμε την ασφάλεια ενός κρυπτοσυστήματος ενάντια σε παθητικούς και ενεργούς αντιπάλους. Το κύριο παράδειγμα θα είναι το κρυπτοσύστημα ElGamal [37].

Ορισμός 2.10. *Κρυπτοσύστημα*

Ένα κρυπτοσύστημα είναι μια τριάδα αποδοτικών αλγορίθμων (KGen, Enc, Dec) *έτσι ώστε αν* $\mathtt{m}$ *είναι κάποιο έγκυρο μήνυμα τότε:*

- $k \leftarrow \mathsf{KGen}()$
- $c = \mathsf{Enc}(k, \mathtt{m})$
- $m = \mathsf{Dec}(k, c)$
- *Επιπλέον ισχύει ότι :* $\mathsf{Dec}(\mathsf{Enc}(m)) = m$

Σημείωση: Ορισμένες φορές για λόγους πληρότητας ορίζονται τα ακόλουθα σύνολα: $\mathcal{K}$, $\mathcal{M}$, $\mathcal{C}$. Τα σύνολα αυτά ονομάζονται ΄χώροι κλειδιών, μηνυμάτων, και κρυπτοκειμένων αντίστοιχα. Συνηθίζεται να παραλήπεται ο αυστηρός ορισμός τους μιας και συχνά εννοούνται από τις παραμέτρους και τους αλγορίθμους του κρυπτοσυστήματος.

Σε ένα κρυπτοσύστημα δημοσίου κλειδιού έχουμε τις εξής ιδιαιτερότητες:

Για αρχή ο αλγόριθμος KGen() έχει ως έξοδο ένα ζευγάρι κλειδιών συχνά συμβολιζόμενο ως (sk, pk). Το sk καλείτε ιδιωτικό κλειδί και πρέπει να διατηρείται μυστικό από τον κάθε χρήστη του συστήματος. Το pk καλείται δημόσιο κλειδί και είναι αυτό που γίνεται γνωστό σε όλους τους συμμετέχοντες του συστήματος. Όταν κάποιος επιθυμεί να στείλει ένα μήνυμα τότε πολύ απλά χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης Enc() μαζί με το μήνυμα και το δημόσιο κλειδί του παραλήπτη και το στέλνει. Εν συνεχεία ο παραλήπτης με χρήση του ιδιωτικού του κλειδιού και του αλγόριθμου αποκρυπτογράφησης Dec() μπορεί να διαβάσει το μήνυμα που έχει λάβει.

Το θετικό της κρυπρογραφίας δημοσίου κλειδιού είναι το ότι δεν απαιτείται ανταλλαγή κλειδιών μεταξύ κάθε χρήστη του συσήματος, μόλις ένα νέο άτομο εισέρχεται στο δίκτυο αρκεί να δημοσιεύει το δημόσιο κλειδί του και έτσι μπορεί να λάβει μηνύματα από οποιονδήποτε άλλο χρήστη. Από την άλλη η ασύμμετρη κρυπτογραφία απαιτεί κλειδιά μεγαλύτερου μήκους για να επιτύχει επίπεδα ασφάλειας ίσα με αυτά συμμετρικής κρυπρογραφίας. Ακόμα η υλοποίηση των περισσότερων αλγορίθμων είναι πιο κοστοβόρα από άποψη υπολογιστικών πόρων σε σχέση με παραδείγματα συμμετρικής κρυπρογραφίας, ως αποτέλεσμα η χρήση της ασύμμετρης κρυπτογραφίας δεν ενδείκνυται για όλες τις εφαρμογές ασφάλειας.

Υπάρχουν πολλά παραδείγματα κρυπτοσυστημάτων δημοσίου κλειδιού. Όπως αναφέραμε στην αρχή το πρώτο ήταν το RSA [68], ενώ μόλις της επόμενη χρονιά προτάθηκε και το κρυπτοσύστημα Rabin [66]. Ένα άλλο ενδιαφέρον κρυπτοσύστημα είναι είναι και αυτό του Paillier [63] που βρίσκει συχνά εφαρμογές σε συστήματα ηλεκτρονικών ψηφοφοριών, π.χ. [40]. Όπως αναφέρθηκε και στην αρχή αυτής της ενότητας ένα ακόμα κρυπτοσύστημα είναι το ElGamal [37], το οποίο θα είναι και το παράδειγμα οδηγός για το παρακάτω κομμάτι.

2.2.1 Το Κρυπτοσύστημα ElGamal

Το κρυπτοσύστημα ElGamal είναι ένα απλό κρυποτσύστημα που βασίζεται στο πρωτόκολλο Diffie - Hellman και στο Πρόβλημα του Διακριτού Λογαρίθμου. Παρακάτω παραθέτουμε τους αλγορίθμους που το απαρτίζουν:

- **Δημιουργία Κλειδιών** - $\mathsf{KGen}()$:
  1. Επιλέγουμε δύο μεγάλους πρώτους p, q έτσι ώστε $q|(p-1)$ και έναν γεννήτορα g της υποομάδας $\mathbb{G}$ τάξης q της $\mathbb{Z}_p^*$.
  2. Επιλέγουμε τυχαίο $x \in_R \mathbb{Z}_q$
  3. Υπολογίζουμε $y = g^x \mod p$
  4. Επιστρέφουμε το ζεύγος ιδιωτικού - δημόσιου κλειδιού $(\mathsf{sk}, \mathsf{pk}) = (x, y)$
- **Κρυπτογράφηση** - $\mathsf{Enc}(\mathsf{pk}, \mathtt{m})$:
  1. Επιλέγουμε τυχαίο $r \in_R \mathbb{Z}_q$
  2. Υπολογίζουμε $G = g^r \mod p$
  3. Υπολογίζουμε $M = \mathtt{m}y^r \mod p$
  4. Επιστρέφουμε το κρυπτοκείμενο ως $c = (G, M)$
- **Αποκρυπτογράφηση** - $\mathsf{Dec}(\mathsf{sk}, c)$:
  1. Δοθέντος κρυπτοκειμένου $c = (G, M)$ και χρησιμοποιώντας το ιδιωτικό κλειδί $\mathsf{sk} = x$ υπολογίζουμε $\mathtt{m} = \frac{M}{G^x}$

Εύκολα βλέπουμε ότι $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathtt{m})) = \mathtt{m}$, διότι :

$$\frac{M}{G^x} = \frac{\mathtt{m}y^r}{g^r} = \frac{\mathtt{m}g^{rx}}{g^r} = \mathtt{m}$$

Παρατηρούμε επίσης ότι το μέγεθος του κρυπτοκειμένου είναι διπλάσιο από αυτό του αρχικού κειμένου.

Τέλος σημειώνουμε πως υπάρχει μία ακόμη έκδοση του ElGamal, το εκθετικό ElGamal, στο οποίο επιστρέφεται η κρυπτογράφηση του $g^{\mathtt{m}}$ αντί για την κρυπτογράφηση του $\mathtt{m}$.

2.2.2 Ασφάλεια Κρυπτοσυστήματος Δημοσίου Κλειδιού

Έχοντας τώρα ένα παράδειγμα κρυπτοσυστήματος τίθεται το ζήτημα της ασφάλειάς του. Προστατεύει ενάντια σε αντιπάλους; Αν ναι τι ικανότητες θεωρούμε πως έχουν αυτοί οι αντίπαλοι; Έχουν πρόσβαση σε γνωστά αρχικά κείμενα, plaintexts, ή έχουν πρόσβαση σε κρυπτογραφημένα κείμενα, ciphertexts, της αρεσκείας τους;

Για να μοντελοποιήσουμε αυτές τις δυνατότητες του αντιπάλου χρησιμοποιούμε τα λεγώμενα Πειράματα - Παιχνίδια Ασφάλειας (Security Experiments - Games)

μεταξύ του αντιπάλου $\mathcal{A}$ και ενός προκαλούντα $\mathcal{C}$. Και οι δύο οντότητες ειναι PPT αλγόριθμοι που επικοινωνούν μεταξύ τους. Ο $\mathcal{A}$ επιλέγει δύο μηνύματα $\mathtt{m}_0, \mathtt{m}_1$ και τα δίνει στον $\mathcal{C}$. Ο $\mathcal{C}$ επιλέγει ένα από τα δύο στη τύχη, το κρυπτογραφεί, και το επιστρέφει στον $\mathcal{A}$. Ο $\mathcal{A}$ καλείται να αποφανθεί το κρυπτοκείμενο το οποίο έλαβε σε ποιο από τα δύο αρχικά μηνύματα αντιστοιχεί. Αν η πιθανότητα του $\mathcal{A}$ να μαντέψει σωστά είναι αμελητέα κοντά στο $\frac{1}{2}$ τότε θα λέμε ότι το κρυπτοσύστημα είναι ασφαλές για αντιπάλους με τις δυνατότητες του $\mathcal{A}$. Γενικά για να μοντελοποιήσουμε τις δυνατότες ενός αντιπάλου στα παιχνίδια ασφάλειας δίνουμε πρόσβαση σε μαντεία που προσφέρουν ακριβώς αυτή την λειτουργικότητα στον $\mathcal{A}$. Για παράδειγμα αν ο $\mathcal{A}$ μπορεί να κρυπτογραφεί μηνύματα της αρεσκείας του τότε θα λέμε ότι έχει πρόσβαση στο μαντείο κρυπτογράφησης και θα γράφουμε $\mathcal{A}^{\mathsf{Enc}}$, ομοίως αν μπορεί να αποκρυπτογραφεί κιόλας όποιο μήνυμα επιθυμεί $\mathcal{A}^{\mathsf{Enc},\mathsf{Dec}}$.

Επίθεση Επιλεγμένου Μηνύματος - Chosen Plaintext Attack (CPA)

Όπως ορίσαμε τα κρυπτοσυστήματα δημοσίου κλειδιού είναι εμφανές πως οποιοσδήποτε μπορεί κατ' ελάχιστο να κρυπτογραφεί μηνύματα της επιλογής του προς οποιονδήποτε παραλήπτη επιθυμεί. Έτσι λοιπόν το ελάχιστο επίπεδο ασφάλειας για ένα κρυπτοσύστημα είναι η προστασία από επιθέσεις επιλεγμένου μηνύματος. Παρακάτω παραθέτουμε το παιχνίδι ασφάλειας και τον ορισμό που πηγάζει από αυτό.

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

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

Ορισμός 2.11. *(IND-CPA)*

Ένα κρυπτσύστημα έχει την ιδιότητα IND-CPA εάν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

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

Επιθέσεις Επιλεγμένου Κρυπτοκειμένου - Chosen Ciphertext Attack (CCA)

Ένας αντίπαλος ισχυρότερος από τον προηγούμενο είναι αυτός που έχει πρόσβαση σε γνωστά ζεύγη μηνύματος - κρυπτοκειμένου. Για να μοντελοποιήσουμε αυτή τη δυνατότητα στα παιχνίδια ασφαλείας προσφέρουμε στον $\mathcal{A}$ πρόσβαση στο μαντείο αποκρυπτογράφησης Dec. Εδώ πρέπει να διακρύνουμε δύο ξεχωριστές περιπτώσεις:

- Ο $\mathcal{A}$ μπορεί να αποκρυπτογραφεί όσα μηνύματα επιθυμεί μέχρι να λάβει το μήνυμα - πρόκληση. Αφού το λάβει δε μπορεί να χρησιμοποιήσει το μαντείο Dec για να απαντήσει στην πρόκληση που έχει δεκτεί. Αυτό το επίπεδο ασφάλειας καλείται $IND-CCA1$.

- Ο $\mathcal{A}$ μπορεί να αποκρυπτογραφεί όσα μηνύματα επιθυμεί και αφού λάβει το μήνυμα - πρόκληση, αρκεί το μήνυμα αυτό να μην χρησιμοποιηθεί ως είσοδος στο μαντείο Dec. Αυτό το επίπεδο ασφάλειας καλείται $IND-CCA2$

Παρακάτω δίνονται τα παιχνίδια μαζί με τους αντίστοιχους ορισμούς:

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

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

Ορισμός 2.12. *(IND-CCA1)*

Ένα κρυπτσύστημα έχει την ιδιότητα IND-CCA1 εάν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

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

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\mathtt{m}_0,\mathtt{m}_1) \leftarrow \mathcal{A}^{\mathsf{Enc},\mathsf{Dec}}(1^\lambda,\mathsf{pk})$
$b \leftarrow\!\!\$\ \{0,1\}$
$c \leftarrow \mathsf{Enc}(\mathsf{pk},\mathtt{m}_b)$
$b' \leftarrow \mathcal{A}^{\mathsf{Enc},\mathsf{Dec}}(1^\lambda,\mathsf{pk},c)$
if *c δεν είναι είσοδος στο* Dec **then**
  Επέστρεψε: $b' = b$
else
  Επέστρεψε: $\perp$
end

Ορισμός 2.13. *(IND-CCA2)*
Ένα κρυπτσύστημα έχει την ιδιότητα IND-CCA2 εάν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

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

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

Ασφάλεια του Κρυπτοσυστήματος ElGamal

Εφοδιασμένοι με τους προηγούμενους ορισμούς θα μελετήσουμε τώρα πιο ασυστηρά την ασφάλεια που προσφέρει το κρυπτοσύστημα ElGamal.

Θεώρημα 2.2. *Το ElGamal διαθέτει την ιδιότητα* $IND-CPA$ *αν ισχύει η υπόθεση* DDH*.*

Απόδειξη*:Έστω ότι το ElGamal δε διαθέτει την ιδιότητα* $IND-CPA$*, αυτό σημαίνει πως υπάρχει* PPT *αντίπαλος* $\mathcal{A}$ *που μπορεί να κερδίσει το Παιχνίδι 2.1 με μη-αμελητέα πιθανότητα. Θα κατασκευάσουμε έναν αλγόριθμο* $\mathcal{B}$ *ο οποίος χρησιμοποιώντας τον* $\mathcal{A}$ *ως υπορουτίνα θα μπορεί να λύνει με μη αμελητέα πιθανότητα το* DDHP*.*

- *Δίνουμε για είσοδο στο* $\mathcal{B}$ *ένα στιγμιότυπο* DDHP ($g^\alpha \mod p$, $g^\beta \mod p$, $g^\gamma \mod p$)*.*
- *Χτίζουμε τώρα τα δεδομένα για να δωθούν στον* $\mathcal{A}$*. Θέτουμε* $y = g^\alpha \mod p$

- *Όταν ο $\mathcal{A}$ εξάγει δύο μηνύματα διαλέγουμε στη τύχη $b \in \{0,1\}$ και θέτουμε $c = (G = g^{\beta}, M = \mathtt{m}_b g^{\gamma})$*
- *Ο $\mathcal{A}$ επιστρέφει την τιμή b'.*
- *Αν ο $\mathcal{A}$ επέλεξε σωστά, τότε επιστρέφουμε 1, αλλιώς επιστρέφουμε 0.*

Αν η τριάδα που δίνεται ως είσοδος είναι τριάδα Diffie - Hellman τότε ο $\mathcal{A}$ έχει λάβει ένα έγκυρο κρυπτοκείμενο ElGamal, και επομένως μπορεί να μαντέψει σωστά με μη - αμελητέα πιθανότητα. Διαφορετικά ο $\mathcal{A}$ θα πρέπει να μαντέψει τυχαία και άρα έχει πιθανότητα $\frac{1}{2}$ να απαντήσει σωστά. Ως αποτέλεσμα ο $\mathcal{B}$ έχει πιθανότητα τουλάχιστον μη - αμελητέα να κερδίσει το παιχνίδι, και άρα να ξεχωρίσει μια τριάδα Diffie - Hellman. Αυτό όμως είναι άτοπο και επομένως το ElGamal διαθέτει την ιδιότητα $IND - CPA$. □

Θεώρημα 2.3. *Το ElGamal δε διαθέτει την ιδιότητα $IND - CCA2$*

Απόδειξη:*Έστω ότι ο $\mathcal{A}$ έχει πρόσβαση σε οπαιδήποτε αποκρυπτογράφηση της αρεσκείας του πλην μίας, έστω $c = (G, M) = (g^r, \mathtt{m}_b y^r)$, το οποίο και επιθυμεί να αποκρυπτογραφήσει. Μπορεί να ακολουθήσει την παρακάτω διαδικασία για να το καταφέρει:*

- *Κατασκευάζει ένα νέο κρυπτοκείμενο $c' = (G', M') = (Gg^{r'}, M\alpha y^{r'}) = (g^{r+r'}, \mathtt{m}_b \alpha y^{r+r'})$, όπου το α είναι κάποιο στοιχείο της ομάδας που δουλεύουμε επιλογής του $\mathcal{A}$.*
- *$\mathsf{Dec}(\mathsf{sk}, c') = \frac{M'}{G'^x} = \alpha \mathtt{m}_b$, και αφού το α είναι επιλογής του $\mathcal{A}$ τότε έχει στα χέρια του και την αποκρυπτογράφηση του $\mathtt{m}_b$.*
- *Αν $\mathtt{m}_b = \mathtt{m}_0$ τότε επιστρέφει $b' = 0$, αλλιώς επιστρέφει $b' = 1$.*

□

Τίθεται τώρα το ζήτημα αν το ElGamal διαθέτει την ιδιότητα IND - CCA1. Αυτό μέχρι και πρόσφατα ήταν ανοιχτό ζήτημα, όμως το 2010 δώθηκε απάντηση. Η απόδειξη μπορεί να βρεθεί στην ακόλουθη εργασία : [54].

Οι δύο ενότητες που ακολουθούν πραγματεύονται τις Κρυπτογραφικές Συναρτήσεις Σύνοψης (Cryptographic Hash Functions) και τις Αποδείξεις Μηδενικής Γνώσης (Zero Knowledge Proofs). Και τα δύο αυτά κομμάτια της Κρυπτογραφίας δεν ανήκουν αμιγώς στην Κρυπτογραφία Δημοσίου Κλειδιού, τουναντίον αποτελούν ξεχωριστούς τομείς έρευνας. Συμπεριλαμβάνονται σε αυτό το κεφάλαιο μόνο λίγα από τα τμηματά τους τα οποία χρησιμοποιούνται εκτεταμένα στο πεδίο των ψηφιακών υπογραφών και στα οποία θα γίνονται συχνές αναφορές στα επόμενα κεφάλαια. Επομένως οι επερχόμενες ενότητες έχουν απλό αποσαφηνιστικό χαρακτήρα και δίνουν τα άκρως απαραίτητα για όσα θα ακολουθήσουν στην υπόλοιπη ΔΕ.

2.3 Κρυπτογραφικές Συναρτήσεις Σύνοψης

Οι συναρτήσεις σύνοψης είναι εργαλείο το οποίο βρίσκει ευρεία χρήση σε πολλά πεδία της πληροφορικής. Μία συχνή χρήση τους είναι για την κατασκευή hash tables για την υλοποίηση λεξικών.

Γενικά οι συναρτήσεις σύνοψης, ή συναρτήσεις κατακερματισμού, εκτελούν την εξής διαδικασία:

Μετατρέπουν οποιαδήποτε είσοδο, ας πούμε για παράδειγμα δυαδικές ακολουθίες οποιουδήποτε μήκους $\{0,1\}^*$, σε έξοδο που έχει πάντα συγκεκριμένο μήκος, π.χ. 256 bits ($\{0,1\}^{256}$).

Στη κρυπτογραφία χρησιμοποιούνται συχνά για να μοντελοποιήσουμε τις τυχαίες συναρτήσεις. Πολύ συχνά ακολουθείτε στην θεωρητική κρυπτογραφία το λεγώμενο Μοντέλο Τυχαίου Μαντείου, Random Orcale Model ή $\mathcal{RO}$ Model. Σε αυτό το μοντέλο θεωρούμε πως υπάρχουν συναρτήσεις οι οποίες είναι πραγματικά τυχαίες, δηλαδή η εικόνα της εκάστωτε εισόδου είναι ομοιόμορφα κατανεμημένη πάνω από το σύνολο τιμών της συνάρτησης. Προφανώς κάτι τέτοιο είναι αδύνατο να υπάρχει στη πραγματικότητα.

Καταλήγουμε λοιπόν στην εξής κατάσταση: Στη θεωρία οι κατασκευές μας και οι αποδείξεις μας γίνονται με βάση πραγματικά τυχαίες συναρτήσεις, ενώ πρακτικά όταν υλοποιούμε ένα π.χ. ένα primitive όπως κάποια ψηφιακή υπογραφή χρησιμοποιούμε μία κρυπτογραφική συνάρτηση σύνοψης. Ενώ αυτό υποβαθμίζει ίσως πρακτικά σε ένα βαθμό την ασφάλεια που μπορούμε να επιτύχουμε από τη θεωρία στη πράξη, μας επιτρέπει να έχουμε ευκολότερες αποδείξεις και αποδοτικότερα πρωτόκολλα.

Οι κύριες πηγές για αυτή την ενότητα είναι [33, 81, 48].

Ας επιστρέψουμε τώρα στις ιδιότητες που θέλουμε να έχει μία συναρτήση σύνοψης που χρησιμοποιείται για κρυπτογραφικούς σκοπούς.

Για αρχή θέλουμε να είναι ταχέως υπολογίσιμη, κάτι που είναι γενική απαίτηση αλλά είναι ιδιαίτερα αναγκαίο για την κρυπτογραφία. Όπως θα δούμε παρακάτω ένα κρυπτογραφικό σχήμα όπως μια υπογραφή μπορεί να κάνει χρήση μίας συνάρτησης σύνοψης $\mathcal{H}$ πάρα πολλές φορές, έτσι αν ο υπολογισμός της είναι χρονοβόρος το σχήμα μπορεί να είναι άχρηστο πρακτικά.

Το άλλον μείζον ζήτημα είναι οι συγκρούσεις. Όπως είναι αναμενώμενο όταν περιορίζουμε την εικόνα διατηρόντας το πεδίο ορισμού σημαντικά μεγαλύτερο, θεωρητικά και άπειρο αν μιλάμε για κάθε δυνατή είσοδο, είναι βέβαιο πως θα προκύψουν συγκρούσεις. Αυτό όμως μπορεί να έχει ολέθριες συνέπειες όταν μιλάμε για κρυπτογραφικές εφαρμογές. Αναλυτικό παράδειγμα δίνεται στο Κεφάλαιο 3. Θα θέλαμε λοιπόν οι συναρτήσεις σύνοψης να είναι ελεύθερες συγκρούσεων, όμως αυτό από μόνο του δεν αρκεί.

Αναλυτικά έχουμε τις παρακάτω επιθυμητές ιδιότητες:

1. Αντίσταση Πρώτου Ορίσματος: Είναι υπολογιστικά δύσκολο για δεδομένο c να βρεθεί $\mathtt{m}$ τέτοι ώστε $c \leftarrow \mathcal{H}(\mathtt{m})$.

2. Αντίσταση Δεύτερου Ορίσματος: Είναι υπολογιστικά δύσκολο για δεδομένο $\mathtt{m}$ να βρεθεί $\mathtt{m}' \neq \mathtt{m}$ τέτοιο ώστε $\mathcal{H}(\mathtt{m}) = \mathcal{H}(\mathtt{m}')$.

3. Δυσκολία Εύρεσης Συγκρούσεων: Είναι υπολογιστικά δύσκολο να βρεθούν $\mathtt{m}, \mathtt{m}'$ διαφορετικά μεταξύ τους έτσι ώστε $\mathcal{H}(\mathtt{m}) = \mathcal{H}(\mathtt{m}')$.

Ορισμός 2.14. *Κρυπτογραφική Συνάρτηση Σύνοψης*
Μία συνάρτση σύνοψης $\mathcal{H}$ θα λέγεται κρυπτογραφική εάν έχει και τις τρεις προηγούμενες ιδιότητες.

Λήμμα 2.2. *Για τις προηγούμενες ιδιότητες ισχύει ότι:* (3) $\implies$ (2) $\implies$ (1)

Απόδειξη:

- (2) $\implies$ (1). Έστω ότι η $\mathcal{H}$ δε διαθέτει αντίσταση πρώτου ορίσματος και έστω $\mathtt{m}$ για το οποίο θέλω να παραβιάσω την ιδιότητα αντίστασης δεύτερου ορίσματος. Υπολογίζω $c \leftarrow \mathcal{H}(m)$. Αφού η $\mathcal{H}$ δε διαθέτει αντίσταση πρώτου ορίσματος μπορούμε να βρούμε $\mathtt{m}'$, τέτοιο ώστε $c = \mathtt{m}'$. Επειδή το πεδίο ορισμού είναι σημαντικά μεγαλύτερο του συνόλου τιμών η πιθανότητα $\mathtt{m} = \mathtt{m}'$ είναι αμελητέα και άρα η $\mathcal{H}$ δε διαθέτει ούτε αντίσταση δεύτερου ορίσματος.

- (3) $\implies$ (2).Έστω ότι η $\mathcal{H}$ δε διαθέτει αντίσταση δεύτερου ορίσματος, τότε για δεδομένο $\mathtt{m}$ μπορεί να βρεθεί $\mathtt{m}' \neq \mathtt{m}$, έτσι ώστε $\mathcal{H}(\mathtt{m}) = \mathcal{H}(\mathtt{m}')$. Καταφέραμε λοιπόν να βρούμε μία σύγκρουση για την $\mathcal{H}$ και άρα δεν είναι ελεύθερη συγκρούσεων.

Για μία αναλυτική μελέτη των κρυπτογραφικών συναρτήσεων σύνοψης προτείνεται το παρακάτω [70].

Ορισμένα παραδείγματα συναρτήσεων σύνοψης στη κρυπτογραφία είναι η $MD5$ [67], η bcrypt [65] που προέρχεται από τον γρύφο Blowfish [71], η οικογένεια συναρτήσεων SHA [41], η συνάρτηση $BLAKE$ [9], και πολλές άλλες.

Γενικά οι κρυπτογραφικές συναρτήσεις σύνοψης βρίσκουν πληθώρα εφαρμογών στον χώρο της κρυπτογραφίας αλλά και της κυβερνοασφάλειας γενικότερα. Έχουν εκτεταμένη χρήση σε σχήματα υπογραφών μέσω σχημάτων δέσμευσης, χρησιμοποιούνται για timestamping, και ασφαλή αποθήκευση κωδικών.

Μία ακόμα ενδιφέρουσα χρήση τους είναι η αξιοποιησή τους για τη δημιουργία "δαχτυλικών αποτυπωμάτων" για λογισμικά. Συγκεκριμένα όταν ένα νέο κακόβουλο

λογισμικό εντοπίζεται τότε εταιρίες που παράγουν antivirus υπολογίζουν το hash του λογισμικού, κάτι σαν να του παίρνουν τα αποτυπωματά του, και το ανεβάζουν σε βάσεις δεδομένων έτσι ώστε αν εισβάλει σε κάποιον υπολογιστή από το hash και μόνο μπορεί να ξεκινήσει η διαδικασία άμυνας.

2.4 Αποδείξεις Μηδενικής Γνώσης

Οι αποδείξεις μηδενικής γνώσης προτάθηκαν για πρώτη φορά το 1985 από τους Goldwasser, Micalli, και Rackoff στη θεμελιώδη εργασία τους [39]. Αποτελούν μία παραλλαγή των διαλογικών συστημάτων απόδειξης, μελετόντας περαιτέρω την ποσότητα πληροφορίας που διαρεεί μεταξύ των εμπλεκόμενων οντοτήτων.

Πιο συγκεκριμένα μία απόδειξη μηδενικής γνώσης είναι μια διαλογική απόδειξη μεταξύ δύο οντοτήτων, ενός Prover $\mathcal{P}$ ο οποίος θέλει να δείξει ότι μια πρόταση είναι αληθής και ενός Verifier $\mathcal{V}$.

Η συγκεκριμένη ενότητα βασίζεται κυρίως στις αντίστοιχες ενότητες των [33, 81]. Όπως έχει προαναφερθεί θα εστιάσουμε μόνο σε έννοιες που είναι βοηθητικές στην καλύτερη κατανόηση της ΔΕ, για περαιτέρω εμβάθυνση συνιστάται η προσφυγή του αναγνώστη στα προηγούμενα συγγράμματα.

Από ένα πρωτόκολλο Απόδειξης Μηδενικής Γνώσης απαιτούμε τις ακόλουθες ιδιότητες:

- Πληρότητα: Ένας τίμιος $\mathcal{P}$, δηλαδή που γνωρίζει τον μάρτυρα w και εκτελεί ορθά το πρωτόκολλο, πείθει έναν τίμιο $\mathcal{V}$ με συντριπτική πιθανότητα.

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

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

Σημείωση: Η έννοια της γνώσης μάρτυρα w είναι ισοδύναμη με την έννοια της απόδειξης μίας πρόταση. Στη κρυπρογραφία για παράδειγμα συνηθίζεται να δείχνει κάποιος ότι γνωρίζει έναν μάρτυρα, για παράδειγμα τον διακριτό λογάριθμο ενός στοιχείου ομάδας ως προς έναν συγκεκριμένο γεννήτορα.

Μία παραλλαγή εξαιρετικής σημασίας είναι τα λεγώμενα πρωτόκολλα Τίμιου Επαληθευτή (Honest Verifier Zero Knowledge - HVZK), και πιο συγκεκριμένα τα Σ-Πρωτόκολλα.

2.4.1 HVZK και Σ-Πρωτόκολλα

Ένα πρωτόκολλο HVZK είναι ένα πρωτόκολλο μηδενικής γνώσης για το οποίο υποθέτουμε το εξής:

Ορισμός 2.15. *Πρωτόκολλο Τίμιου Επαληθευτή*
Ένα πρωτόκολλο μηδενικής γνώσης είναι τίμιου επαληθευτή εάν ο $\mathcal{V}$ είναι τίμιος και επιπλέον τα μηνύματα που δίνει είναι ομοιόμορφα κατανεμημένα.

Ορισμός 2.16. *Σ-Πρωτόκολλο*
Σ-Πρωτόκολλο είναι ένα HVZK πρωτόκολλο που εκτελείτε σε 3 γύρους:

1. ***Commit - Δέσμευση**: Ο $\mathcal{P}$ δεσμεύεται σε μία τιμή και τη στέλνει στον $\mathcal{V}$.*

2. ***Challenge - Πρόκληση**: Ο $\mathcal{V}$ επιλέγει τίμια και ομοιόμορφα μια τιμή - πρόκληση και τη στέλνει στον $\mathcal{P}$.*

3. ***Response - Απόκριση**: Ο $\mathcal{P}$ απαντάει στην πρόκληση που έθεσε $\mathcal{V}$.*

Για τα Σ-Πρωτόκολλα ισχύει μία ειδική περίπτωση της ορθότητας, η επονομαζώμενη ειδική ορθότητα, η οποία έχει δειχθεί πως είναι ισοδύναμη με την ορθότητα στην περίπτωση τίμιου επαληθευτή.

Ορισμός 2.17. *Ειδική ορθότητα (Special Soundness)*
Ένα Σ-Πρωτόκολλο έχει την ιδιότητα της ειδικής ορθότητας εάν με δύο εκτελέσεις του πρωτοκόλλου με ίδια δέσμευση αλλά διαφορετικές προκλήσεις μπορεί να αποκαλυφθεί ο μάρτυρας w του $\mathcal{P}$.

2.4.2 Το πρωτόκολλο Schnorr

Ένα από τα κλασσικότερα Σ-Πρωτόκολλα είναι αυτό που προτάθηκε από το Schnorr το 1989 [72].

Έστω $\mathcal{P}, \mathcal{V}$ οι οποίοι γνωρίζουν έναν γεννήτορα g μιας ομάδας τάξης q. Ο $\mathcal{P}$ θέλει να δείξει στον $\mathcal{V}$ ότι για κάποιο στοιχείο h της ομάδας γνωρίζει x έτσι ώστε $h = g^x$, χωρίς όμως να αποκαλύψει το x.

Οι γύροι του πρωτοκόλλου είναι οι εξής:

- **Commit** ($\mathcal{P} \to \mathcal{V}$): Επιλέγεται τυχαίο $t \in_R \mathbb{Z}_q$, υπολογίζεται $y = g^t$ και αποστέλλεται στον $\mathcal{V}$.

- **Challenge** ($\mathcal{V} \to \mathcal{P}$): Ο $\mathcal{V}$ επιλέγει τυχαία $c \in_R \mathbb{Z}_q$ και το στέλνει στον $\mathcal{P}$.

- **Response** ($\mathcal{P} \to \mathcal{V}$): Ο $\mathcal{P}$ υπολογίζει $s = t + cx \mod q$ και στο στέλνει στον $\mathcal{V}$.

Ο $\mathcal{V}$ αποδέχεται εάν $g^s = yh^c$.

Θα αποδείξουμε τώρα τις ιδιότητες του πρωτοκόλλου.

- **Πληρότητα**:
$$g^s = g^{t+cx} = g^t g^{cx} = yg^{x^c} = yh^c$$

- **Ορθότητα**: Για την απόδειξη της ορθότητας θα εκμεταλευτούμε το γεγονός ότι το πρωτόκολλο Schnorr είναι Σ-Πρωτόκολλο και άρα η ορθότητα είναι ισοδύναμη με την ειδική ορθότητα. Επομένως, έστω δύο εκτελέσεις του πρωτοκόλλου με $t = t'$ ίδιες δεσμεύσεις και c, c' δύο διαφορετικές μεταξύ τους προκλήσεις. Υπολογίζουμε
$$y = g^s h^{-c} = g^{s'} h^{-c'} = y' \implies s - cx = s' - c'x \implies x = \frac{s - s'}{c - c'}$$
Και άρα έχουμε εξάγει το μάρτυρα x.

- **Μηδενική Γνώση**: Το πρωτόκολλο αυτό είναι μηδενικής γνώσης για τίμιους επαληθευτές (HVZK), δε διαθέτει την ιδιότητα της τέλειας μηδενικής γνώσης παρά μόνο αν ο χώρος προκλήσεων, δηλαδή το σύνολο από το οποίο επιλέγει ο $\mathcal{V}$ στο 2ο βήμα είναι πολύ μικρός (π.χ. $\{0, 1\}$).

2.4.3 Το πρωτόκολλο Chaum - Pedersen

Ένα επίσης κλασσικό Σ-Πρωτόκολλο είναι αυτό των Chaum και Pedersen [30]. Το συγκεκριμένο πρωτόκολλο μας επιτρέπει να αποδείξουμε την ισότητα δύο διακριτών λογαρίθμων ως προς δύο διαφορετικούς γεννήτορες.

Κοινή πληροφορία είναι δύο γεννήτορες g_1, g_2 μιας ομάδας τάξης q. Οι γύροι του πρωτοκόλλου περιγράφονται παρακάτω:

- **Commit** ($\mathcal{P} \to \mathcal{V}$): Ο $\mathcal{P}$ επιλέγει τυχαίο $t \in_R \mathbb{Z}_q$, υπολογίζει $y_1 = g_1^t$ και $y_2 = g_2^t$ και τα στέλνει στον $\mathcal{V}$.

- **Challenge** ($\mathcal{V} \to \mathcal{P}$): Ο $\mathcal{V}$ διαλέγει τυχαία $c \in_R \mathbb{Z}_q$ και το στέλνει στον $\mathcal{P}$.

- **Response** ($\mathcal{P} \to \mathcal{V}$): Ο $\mathcal{P}$ υπολογίζει $s = t + cx \mod q$ και στέλνει στον $\mathcal{V}$.

Ο $\mathcal{V}$ αποδέχεται εάν $g_1^s = y_1 h_1^c$ και $g_2^s = y_2 h_2^c$, όπου $h_1 = g_1^x$ και $h_2 = g_2^x$.

Οι αποδείξεις των ιδιοτήτων του πρωτοκόλλου είναι όμοιες με αυτές του Schnorr.

2.4.4 Συνθέσεις Σ-Πρωτοκόλλων

Είναι εφικτό να γίνει συνδυασμός Σ-Πρωτοκόλλων, π.χ. μπορούμε να έχουμε OR Σ-Πρωτόκολλα, AND Σ-Πρωτόκολλα κλπ. Θα εστιάσουμε παραπάνω στη διάζευξη Σ-Πρωτοκόλλων (OR Σ-Πρωτόκολλο) μιας και εμφανίζει μεγάλη χρήση σε μετέπειτα κομμάτια της ΔΕ.

Το τρόπο για να γίνεται διάζευξη πρωτοκόλλων των προτάσουν στην εργασία τους [32] οι Cramer, Damgård, και Schoenmakers. Παρακάτω θα δείξουμε το πρωτόκολλο OR Schnorr, δηλαδή τη διάζευξη 2 πρωτοκόλλων Schnorr.

Έστω δημόσιοι παράμετροι $\mathbb{G}$ τάξης q και g_1, g_2 δύο διφαορετικοί μεταξύ τους γεννητορές της. Θα δείξουμε πως ο $\mathcal{P}$ μπορεί να δείξει ότι ξέρει είτε x_1 έτσι ώστε $h_1 = g^{x_1}$, είτε x_2 έτσι ώστε $h_2 = g^{x_2}$. Ας υποθέσουμε, δίχως βλάβη της γενικότητας, ότι ο $\mathcal{P}$ γνωρίζει το x_1.

Το πρωτόκολλο εκτελείτε ως εξής:

- **Commit** ($\mathcal{P} \to \mathcal{V}$): Ο $\mathcal{P}$ επιλέγει τυχαίο $t, c_2, s_2 \in_R \mathbb{Z}_q$, υπολογίζει $y_1 = g_1^t$ και $y_2 = g^{s_2} h_2^{-c_2}$ και τα στέλνει στον $\mathcal{V}$.
- **Challenge** ($\mathcal{V} \to \mathcal{P}$): Ο $\mathcal{V}$ διαλέγει τυχαία $c \in_R \mathbb{Z}_q$ και το στέλνει στον $\mathcal{P}$.
- **Response** ($\mathcal{P} \to \mathcal{V}$): Ο $\mathcal{P}$ υπολογίζει $c_1 = c + c_2 \mod q$ και $s_1 = t + c_1 x_1$ και τα στέλνει στον $\mathcal{V}$.

Ο $\mathcal{V}$ αποδέχεται εάν $c = c_1 + c_2$, $g_1^{s_1} = y_1 h_1^{c_1}$, και $g_2^{s_2} = y_2 h_2^{c_2}$.

2.4.5 Ο Μετασχηματισμός Fiat - Shamir

Μέχρι στιγμής τα πρωτόκολλα που έχουμε δείξει είναι διαλογικά, δηλαδή χρειάζονται τη συμμετοχή δύο οντοτήτων. Κάτι τέτοιο δεν είναι ιδιαίτερα αποδοτικό εάν σκεφτούμε ότι σε πρακτικό επίπεδο θα ήταν αναγκαίο κάθε φορά που κάποιος θέλει να μπορέσει να κάνει μια απόδειξη, ότι γνωρίζει π.χ. ένα συνθηματικό σε κάποια ιστοσελίδα, θα πρέπει να υπάρχει κάποιος που θα δίνει την κατάλληλη πρόκληση και θα επαληθεύει την ορθότητα της απόδειξης.

Για την περίπτωση των Σ-Πρωτοκόλλων υπάρχει μια ιδιαίτερα βολική λύση που δώθηκε από τους Fiat και Shamir το 1986 [35], με την οποία είναι εφικτό να μετατραπούν από διαλογικά σε μη διαλογικά.

Η ιδέα είναι η εξής: Στη θέση του $\mathcal{V}$ θα χρησιμοποιείτε μία κρυπτογραφική συνάρτηση σύνοψης. Τώρα αντί ο $\mathcal{P}$ να στέλνει την τιμή στην οποία δεσμεύεται θα την χρησιμοποιεί σαν είσοδο στη συνάρτηση και θα λαμβάνει από εκεί μία τιμή. Αυτό είναι ισοδύναμο με την τυχαία επιλογή πρόκλησης που κάνει ο $\mathcal{V}$.

Ας δούμε τώρα πως γίνεται το μη διαλογικό πρωτόκολλο Schnorr με χρήση μίας κρυπτογραφικής συνάρτησης σύνοψης $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_q$

- **Commit**: Ο $\mathcal{P}$ επιλέγει τυχαίο $t \in_R \mathbb{Z}_q$, υπολογίζεται $y = g^t$.
- **Challenge**: Ο $\mathcal{P}$ υπολογίζει $c = \mathcal{H}(y)$.
- **Response** : Ο $\mathcal{P}$ υπολογίζει $s = t + cx \mod q$ και δημοσιεύει (h, c, s).

Οποιοσδήποτε θέλει να πιστεί για το αν ο $\mathcal{P}$ πράγματι γνωρίζει το διακριτό λογάριθμο που δηλώνει ότι ξέρει αρκεί να ελέγξει αν:

$$c = \mathcal{H}(g^s h^{-c})$$

.

Μια εξαιρετικά σημαντική συνέπεια αυτής της διαδικασίας είναι το γεγονός ότι η παραπάνω διαδικασία μπορεί να προσφέρει και σχήματα υπογραφών, αρκεί στο δεύτερο βήμα να εισαχθεί στη συνάρτηση σύνοψης και το μήνυμα το οποίο υπογράφεται. Με αυτό ακριβώς τον τρόπο προκύπτει το σχήμα υπογραφών Schnorr [72]. Θα μπούμε σε περισσότερες λεπτομέρειες στο επόμενο κεφάλαιο.

Κεφάλαιο 3

Εισαγωγή στις Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές αποτελούν μία από τις σημαντικότερες έννοιες της Κρυπτογραφίας Δημοσίου Κλειδιού. Όπως είδαμε και στο κεφάλαιο 2 η ανάγκη για αυτές προέκυψε μαζί με τη δημιουργία της ασύμμετρης κρυπρογραφίας, αποτελούσε μία έκφανση της ανάγκης επιβεβαίωσης ταυτότητας σε μη ασφαλή κανάλια επικοινωνίας.

Η φυσική σύνδεση που έχουν συχνά τα σχήμτα υπογραφών με τα συστήματα κρυπτογραφίας δημοσίου κλειδιού είναι άμεσα εμφανής. Αρκεί κάποιος να δει εργασίες που εισάγουν νέα κρυπτοσυστήματα, η εργασία των Rivest, Shamir, και Adleman [68] εκτός από το κρυπτοσύστημα RSA εισήγαγε και τις RSA υπογραφές. Αντίστοιχα ο Taher ElGamal εκτός από το κρυπτοσύστημα ElGamal στην εργασία [37] εισήγαγε και τις υπογραφές ElGamal.

Η βασική ιδέα πίσω από ένα σχήμα ψηφιακής υπογραφής είναι η εξής: Κάποιος που θέλει να υπογράψει ένα μήνυμα το συντάσει και έπειτα το υπογράφει με το ιδιωτικό του κλειδί. Εν συνεχεία ο παραλήπτης, καθώς και όποιος τρίτος επιθυμεί, μπορεί να επιβεβαιώσει την εγκυρότητα της υπογραφής χρησιμοποιώντας το δημόσιο κλειδί του υπογράφοντα.

Ένας βοηθητικός τρόπος για να δει κάποιος μία ψηφιακή υπογραφή είναι ως μια απόδειξη του ότι ο υπογράφων γνωρίζει το μυστικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που δηλώνει ότι του ανήκει και ότι το μήνυμα που έχει υπογραφεί είναι αυτό που έχει σταλεί από τον ίδιο.

Σε αυτό το κεφάλαιο θα δούμε από τι αποτελείτε ένα σχήμα ψηφιακής υπογραφής, θα μιλήσουμε για τις ιδιότητες που ζητάμε, και θα μιλήσουμε για τα διαφορετικά επίπεδα ασφάλειας που υπάρχουν. Εν συνεχεία θα δούμε διάφορα παραδείγματα ψηφιακών υπογραφών και θα αναφεθούμε εν τάχυ στις ιδιότητες που διαθέτουν.

Κύριες πηγές του κεφαλαίου αυτού είναι τα αντίστοιχα κεφάλαια των [81,

33, 48, 82] καθώς και η εργασία των Pointcheval και Stern [64]

3.1 Βασικοί Ορισμοί

Ορισμός 3.1. *Σχήμα Ψηφιακών Υπογραφών*
Ένα σχήμα υπογραφών είναι μία τριάδα αποδοτικών αλγορίθμων (KGen, Sign, Vrfy) *έτσι ώστε:*

- ***Αλγόριθμος Δημιουργίας Κλειδιών*** - KGen*: Με είσοδο την παράμετρο ασφαλείας λ δημιουργεί ένα ζεύγος ιδιωτικού - δημόσιου κλειδιού.*

  $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$.

- ***Αλγόριθμος Υπογραφής Μηνύματος*** - Sign*: Με είσοδο ένα ιδιωτικό κλειδί* sk *και ένα μήνυμα* m *δημιουργεί μια υπογραφή.*

  $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathtt{m})$.

- ***Αλγόριθμος Επαλήθευσης Υπογραφής*** - Vrfy*: Με είσοδο μία υπογραφή σ και ένα δημόσιο κλειδί* pk *ελέγχει την εγκυρότητα της υπογραφής, αν δηλαδή προέρχεται από τον υπογράφοντα με αυτό το δημόσιο κλειδί.*

  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\mathsf{pk}, \sigma)$.

Όπως και στον ορισμό του σχήματος υπογραφής έχουμε επίσης τα σύνολα $\mathcal{K}$, $\mathcal{M}$, $\mathcal{S}$, τους χώρους κλειδιών, μηνυμάτων, και υπογραφών αντίστοιχα. Συχνά όμως παραλήπεται ο αυστηρός ορισμός τους μιας και εννοούνται από τις παραμέτρους και τους αλγορίθμους του σχήματος υπογραφής.

Σημείωση: Η παράμετρος ασφαλείας λ εμφανίζεται συχνά σε αλγορίθμους κρυπτογραφικών πρωτοκόλλων. Συχνά είναι το επίπεδο ασφαλείας σε bits που επιθυμούμε να έχει το σύστημα.

Ασφάλεια Ψηφιακών Υπογραφών

Θα αρχίσουμε βλέποντας τις επιθυμητές ιδιότητες, τις δυνατές επιθέσεις, και έναν αυστηρό ορισμό ασφάλειας για σχήματα υπογραφών.

Όπως και στις κανονικές υπογραφές έτσι και στις ψηφιακές υπογραφές ζητάμε τις ακόλουθες ιδιότητες:

- Γνησιότητα Μηνύματος (Message Authentication): Μία υπογραφή προέρχεται από το σωστό υπογραφέα.

- Ακεραιότηα Περιχομένου (Content Integrity): Το περιεχόμενο του υπογραφέντος μηνύματος δεν μπορεί να παραποιηθεί.

- Μη-Αποκύρηξη Υπογραφής (Non-Repudiation): Όταν κάποιος υπογράφει ένα μήνυμα δεν μπορεί έπειτα να πει ότι δε το έχει υπογράψει.

- Μη-Πλαστογραφίσιμη (Unforgeable): Δε πρέπει να είναι εφικτή η πλαστογράφησει υπογραφών.

Η ιδιότητα της μη-πλαστογράφησης είναι ιδιαίτερα σημαντική, συχνά αποτελεί μία από τις κύριες, αν όχι την κύρια, ιδιότητες ασφάλειας ενός σχήματος υπογραφής. Συνηθίζεται η πλαστογράφια χωρίζεται σε τρία ξεχωριστά επίπεδα ανάλογα με την δριμυτητά της:

- Υπαρξιακή Πλαστογραφία (Existential Forgery): Ο αντίπαλος μπορεί να πλαστογραφήσει την υπογραφή για κάποιο μήνυμα, χωρίς όμως να είναι απαραίτητα της επιλογής του. Στην πράξη οι υπαρξιακές πλαστογραφίες δεν έχουν ιδιαίτερη δύναμη μιας και το περιεχόμενο του μηνύματος που υπογραφέται δεν έχει κάποια σημασία. Παρ' όλα αυτά ένα σχήμα υπογραφών που μπορεί υποστεί υπαρξιακές υπογραφές δεν είναι ασφαλές μιας και αν το περιεχόμενο των υπογεγραφέντων μηνυμάτων είναι τυχαίας μορφής, π.χ. πιστοποιητικό για κάποιο κλειδί, μια υπαρξιακή κρυπτογραφία μπορεί να αποτελέσει πρόβλημα.

- Επιλεγμένη Πλαστογραφία (Selective Forgery): Ο αντίπαλος μπροεί να πλαστογράφησει την υπογραφή για κάποιο μήνυμα της αρεσκείας του.

- Ολική Πλαστογραφία (Universal Forgery): Ο αντίπαλος μπορεί να πλαστογραφήσει την υπογραφή για οποιοδήποτε μήνυμα της αρεσκείας του. Για να συμβεί αυτό υπάρχουν δύο σενάρια. Το πρώτο είναι ότι ο αντίπαλος έχει καταφέρει να κατασκευάσει έναν αποδοτικό αλγόριθμο για να υπογράφει μηνύματα που θέλει. Το δεύτερο σενάριο είναι ο αντίπαλος να έχει ανακτήσει το ιδιωτικό κλειδί του υπογράφοντα. Σε αυτό το σενάριο το σύστημα έχει σπάσει τελείως (total break of the signature scheme).

Θα αναλύσουμε τώρα τις επιθέσεις που μπορεί να εκτελέσει ένας αντίπαλος $\mathcal{A}$ σε ένα σχήμα υπογραφών.

- Επίθεση άνευ μηνύματος (No Message Attack): Γνωστή και ως επίθεση δημοσίου κλειδιού, εκτελείτε με μόνη γνώση τις δημόσιες παραμέτρους του σχήματος και τίποτα παραπάνω.

- Απλή επίθεση γνωστού μηνύματος (Plain Known Message Attack): Γνωστή και ως επίθεση γνωστής υπογραφής, ο αντίπαλος γνωρίζει ζεύγη υπογραφής - μηνύματος, όμως δεν έχει δυνατότητα επιλογής του μηνύματος. Αυτή, υπό ρεαλιστικές συνθήκες, αποτελεί την ελάχιστη υπόθεση που μπορούμε να κάνουμε για τις δυνατότητες ενός αντιπάλου.

- Γενική επίθεση επιλεγμένου μηνύματος (Generic Chosen Message Attack): Ο αντίπαλος μπορεί να επιλέξει λίστα μηνυμάτων που θα υπογραφούν, αλλά η λίστα επιλέγεται πριν επιλεχθεί το δημόσιο κλειδί του υπογράφοντα. Λόγω αυτού του περιορισμού η επίθεση αυτή καλείται *γενική*.

- Προσανατολισμένη επίθεση επιλεγμένου μηνύματος (Oriented Chosen Message Attack): Ο αντίπαλος επιλέγει πρώτα το δημόσιο κλειδί του υπογράφοντα και *έπειτα* τη λίστα μηνυμάτων που θα υπογραφούν. Η επίθεση αυτή βασίζεται στα δημόσια δεδομένα ενός συγκεκριμένου υπογραφέα, προβλέπει έναν *ενεργό (active)* αντίπαλο, που όμως δεν ακαλουθεί κάποια στρατηγική στην επιλογή των μηνυμάτων που ζητά να υπογραφούν.

- Προσαρμοζώμενη επίθεση επιλεγμένου μηνύματος (Adaptively Chosen Message Attack): Ο αντίπαλος μπορεί να ζητάει υπογραφές για οποιοδήποτε μήνυμα της αρεσκείας του, επιπλέον μπορεί να προσαρμόζει κατάλληλα την στρατιγική που ακολουθεί και να ζητάει υπογραφές με βάση αυτές που έχει ήδη ζητήσει. Σε αυτή την περίπτωση μιλάμε για έναν *ενεργό (active)* και *προσαρμοστικό (adaptive)* αντίπαλο.

Για να απλοποιήσουμε τη μελέτη ασφάλειας των σχημάτων υπογραφής κάνουμε την ακόλουθη παραδοχή: Ένα σχήμα υπογραφών θα θεωρείται ότι διαθέτει την ιδίοτητα της μη-πλαστογραφισημότητας (unforgeability) εάν δεν γίνεται να παραχθούν υπαρξιακές πλαστογραφίες όταν ένας αντίπαλος εκτελεί προσαρμοζώμενες επιθέσεις επιλεγμένου μηνύματος.

Για τη μοντελοποίηση θα χρησιμοποιήσουμε και πάλι παιχνίδια ασφαλείας. Η ικανότητα του αντιπάλου να ζητάει υπογραφές της αρεσκείας του μοντελοποιείται από ένα μαντείο, το μαντείο υπογραφών, που συμβολίζεται ως $\mathcal{SO}$.

Παρακάτω παραθέτουμε το παιχνίδι ασφαλείας για τη μη-πλαστογραφισημότητα στην προσαρμοζώμενη επίθεση επιλεγμένου κειμένου:

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\sigma,\mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{SO}}(1^\lambda,\mathsf{pk})$
if *σ δεν είναι είσοδος στο* $\mathcal{SO}$ **then**
| **Επέστρεψε:** $\mathsf{Vrfy}(\mathtt{m},\sigma,pk)$

else
| **Επέστρεψε:** $\perp$
end

Ορισμός 3.2. *Μη-πλαστογραφισιμότητα(Unforgeability)*
Ένα σχήμα υπογραφών θα λέμε ότι διαθέτει την ιδιότητα της μη-πλαστογραφισημότητας εάν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *υπάρχει αμελητέα συνάρτηση* $negl_{\mathcal{A}}$ *έτσι ώστε:*

$$Pr[\mathsf{Exp}_{\mathcal{A}}^{Unf}] \leq negl_{\mathcal{A}}(\lambda)$$

3.2 Παραδείγματα Ψηφιακών Υπογραφών

Θα δώσουμε τώρα ορισμένα παραδείγματα ψηφιακών υπογραφών. Ένας διαχωρισμός που μπορούμε να κάνουμε έχει να κάνει με τον τρόπο που προκύπτει ένα σχήμα ψηφιακών υπογραφών. Έτσι αν ένα σχήμα προέρχεται από ένα κρυπτοσύστημα με την χρήση μίας κρυπτογραφικής συνάρτησης σύνοψης για τη δέσμευση του υπογραφέα ως προς το μήνυμα, τότε έχουμε μία υπογραφή **Type-H** (από το *Hash and Sign*). Παράδειγμα αυτού του τύπου υπογραφών είναι οι υπογραφές ElGamal με κρυπτογραφική συνάρτηση σύνοψης και οι Full Domain Hash RSA υπογραφές (FDH-RSA). Αν τώρα το σχήμα υπογραφείς προέρχεται από ένα μη-διαδραστικό Σ-Πρωτόκολλο στο οποίο ο υπογραφέας δεσμεύεται στο μήνυμα τότε μιλάμε για υπογραφές **Type-T** (από το *Three Move Protocol*). Μία από τις πιο κλασσικές υπογραφές **Type-T** είναι και οι υπογραφές Schnorr.

Ένας ακόμα διαχωρισμός που μπορεί να γίνει στα σχήματα υπογραφών είναι αν προσφέρεται η δυνατότητα ανάκτησης του υπογραφέντος μήνυματος κατά τη διάρκεια της επιβεβαίωσης της υπογραφής. Τα περισσότερα σχήματα υπογραφών δεν προσφέρουν πια αυτή την ιδιότητα. Οι κλασσικές ElGamal και RSA υπογραφές προσφέρουν ανάκτηση μηνύματος, όμως αυτή τους η εκδοχή δε προτιμάτε μιας και αφήνει ανοιχτό το ενδεχόμενο για επιθέσεις υπαρξιακής πλαστογραφίας.

Οι υπογραφές ElGamal και DSA

Σε αυτό το σημείο θα μελετήσουμε το σχήμα υπογραφλών ElGamal και τον Αλγόριθμο Ψηφιακών Υπογραφών, ή όπως είναι καλύτερα γνωστός, DSA.

Σχήμα Υπογραφών ElGamal

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

  1. Επιλέγουμε έναν πρώτο p έτσι ώστε το DLOG να είναι υπολογιστικά απρόσιτο στο $\mathbb{Z}_p^*$, και έναν γεννήτορα $g \in \mathbb{Z}_p^*$.
  2. Επιλέγουμε τυχαίο ακέραιο $x \in [0, p-2]$ και υπολογίζουμε $y = g^x \mod p$.
  3. Το δημόσιο κλειδί είναι $\mathsf{pk} = (p, g, y)$ και το ιδιωτικό κλειδί είναι $\mathsf{sk} = x$.

- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(x, \mathtt{m})$:

  1. Ο υπογραφέας επιλέγει το μήνυμα $\mathtt{m}$ που θέλει να υπογράψει και έναν τυχαίο ακέραιο $k \in \mathbb{Z}_p^*$.
  2. Υπολογίζει τις τιμές :
     $r = g^k \mod p$
     $s = (m - xr)k^{-1} \mod p - 1$
  3. Η υπογραφή θα είναι $\sigma = (r, s)$

- **Επαλήθευση Υπογραφής** - $\mathsf{Vrfy}(y, \sigma)$:
  Ελέγχουμε αν:

  1. $r \in (0, p)$ και $s \in (0, p-1)$
  2. $g^m = y^r r^s \mod p$

  Αν ισχύουν τα παραπάνω τότε ο αλγόριθμος επιστρέφει 1, αλλιώς επιστρέφει 0.

Ας μελετήσουμε τώρα την ασφάλεια και την ορθότητα της υπογραφής ElGamal.

Λήμμα 3.1. *Ορθότητα υπογραφής ElGamal*
Ο αλγόριθμος επαλήθευσης επιστρέφει 1 *για τις ορθώς συνταγμένες υπογραφές.*

Απόδειξη:

$$y^r r^s \mod p = g^{xr} g^{k(m-xr)k^{-1}} \mod p = g^{xr+m-xr} = g^m \mod p$$

□

Ας δούμε σε αυτό το σημείο την ασφάλεια της υπογραφής μέσω μερικών πιθανών επιθέσεων.

Επιθέσεις ανάκτησης του ιδιωτικού κλειδιού $\mathsf{sk} = x$**:**

Για αρχή για να μπορέσει ένας αντίπαλος να βρει το ιδιωτικό κλειδί θα πρέπει να μπορεί να σπάσει το DLP για το στοιχείο y.

Δύο ακόμα πιθανά σενάρια υπάρχουν για την ανάκτηση του ιδιωτικού με βάση τα δημόσια δεδομένα και συλλογές υπογραφών, όμως όλα τα προβλήματα αυτά καταλήγουν στο να είναι εξίσου δύσκολα με το DLP. Λεπτομερέστερη ανάλυση τους μπορεί να βρεθεί στο [37].

Είναι πάρα πολύ σημαντικό η τυχαιότητα k να μην επαναλαμβάνεται καθώς κάτι τέτοιο μπορεί να οδηγήσει σε αποκάλυψη του ιδιωτικού κλειδιού x. Εδώ αξίζει να αναφέρουμε πως το μία τέτοια παράλειψη οδήγησε στο hack για το Playstation 3 της Sony από το group *fail0Overflow*. Ο αλγόριθμος υπογραφών δεν ήταν ο ElGamal αλλά ο ECDSA [47], ο οποίος αποτελεί παραλλαγή του ElGamal υλοποιημένος με ελλειπτικές καμπύλες.

Επιθέσεις για πλαστογράφηση μηνύματος:

Ο αντίπαλος μπορεί για δεδομένα $\mathtt{m}, s$, να προσπαθήσει να υπολογίσει κατάλληλο r, έτσι ώστε $y^r r^s = g^m$. Αυτό το πρόβλημα δεν έχει αναχθεί μέχρι στιγμής σε κάποιο γνωστό δύσκολο πρόβλημα, παρ' όλα αυτά πιστεύετε πως είναι ένα δύσκολο πρόβλημα χώρις κάποιο πολυωνιμικό αλγόριθμο.

Αν τώρα ο αντίπαλος επιχειρήσει για δεδομένο $\mathtt{m}$ να βρεί r, s ώστε η υπογραφή να επαληθεύει τότε θα έρθει αντιμέτωπος με ένα στιγμυότυπο DLP.

Ένα πρόβλημα που αντιμετωπίζει το σχήμα ElGamal είναι οι υπαρξιακές πλαστογραφίες. Στις εργασίες τους τόσο ο ElGamal [37] όσο και οι Pointcheval και Stern [64] παραθέτουν επιθέσεις υπαρξιακής πλαστογραφίας, με τους τελευταίους μάλιστα να γενικεύουν την επίθεση του Taher ElGamal. Η επίθεση αυτή απαιτεί ένα γνωστό και έγκυρο μήνυμα-υπογαρφή και οφείλεται στην ευπλαστότητα (malleability) του κρυπτοσυστήματος ElGamal. Για περαιτέρω λεπτομέρειες προτείνονται τα [37, 81, 64].

Για την αποφυγεί αυτής της επίθεσης μπορεί να τροποποιηθεί ελαφρώς το σχήμα με τον ακόλουθω τρόπο. Στον αλγόριθμο δημιουργίας υπογραφής υπολογίζουμε $s = (\mathcal{H}(\mathtt{m}, r) - xr)k^{-1}$ (και τροποποιούμε κατάλληλα και το υπόλοιπο σχήμα), όπου $\mathcal{H}$ είναι μια κρυπτογραφική συνάρτηση σύνοψης. Με αυτό τον τρόπο ο υπογράφων δεσμεύεται στο μήνυμα και στη τυχαιότητα που χρησιμοποιεί και έτσι δε μπορεί να γίνει πρσδιορισμός του μηνύματος εκ των υστέρων. Αξίζει να σημειωθεί πως η τροποποίηση αυτή προτείνεται ήδη απο τον ElGa-

mal στην εργασία του και δεν προκύπτει αργότερα, όπως πχ συμβαίνει με τις υπογραφές RSA [15].

Πρότυπο Ψηφιακών Υπογραφών (DSS) - Αλγόριθμος Ψηφιακών Υπογραφών (DSA)

Το 1994 δημοσιεύεται από το NIST (National Institute of Standards and Technology) το πρότυπο ψηφιακών υπογραφών (DSS) ως FIPS (Federal Information Processing Standard) υπ' αριθμόν 186. Μέσα στο DSS περιγράφεται ο αλγόριθμος ψηφιακών υπογραφών DSA. Έκτοτε ο αλγόριθμος έχει υποστεί ορισμένες τροποποιήσεις, όχι ως προς τη διαδικασία υπογραφής αλλά ως προς τις παραμέτρους του, η έκδοση που θα παρουσιάσουμε θα είναι η αρχική. Σημειώνουμε εδώ πως σε μια πρώτη έκδοση της πέμπτης αναθεώρησης του FIPS 186, δηλαδή το FIPS 186-5, προτείνεται η πάυση χρήσης του DSA για δημιουργία νέων υπογραφών και η μετάβαση στον ECDSA (Elliptic Curve Digital Signature Algorithm). Ένα τελευταίο διευκρινιστικό σημείωμα είναι ότι το DSS αποτελεί ένα πρότυπο που ορίζει πως πρέπει να λειτουργεί ένα σχήμα ψηφιακών υπογραφών, ενώ ο DSA αποτελεί μία υλοποίηση που πληρεί τις προδιαγραφές αυτού του προτύπου.

Η βάση του DSA είναι το σχήμα ElGamal, με μερικές τροποποιήσεις ώστε να επιτυχγάνεται μικρότερο μέγεθος υπογραφής και προτυποίηση των επιπέδων ασφαλείας.

Παρακάτω παρατείθενται οι αλγόριθμοι του σχήματος:

- **Επιλογή Δημοσίων Παραμέτρων:**

  1. Επιλέγεται L, το οποίο είναι το μήκος του κλειδιού σε bit. Το L είναι πολλαπλάσιο του 64, στην αρχική έκδοση του DSS ίσχυε ότι: $L = 64r, r = 8, 9, 10, \cdots, 16$. Σε επόμενες εκδόσεις προτείενται $L = 2048$ ή $L = 3072$.
  2. Επιλέγεται N, το οποίο είναι το μήκος του modulo της υποομαδάς που χρησιμοποιείται από το σύστημα σε bit. Ισχύει ότι $N < L$. Προτεινόμενα ζευγάρια (L, N) είναι $(1024, 160), (2048, 224), (2048, 256), (3072, 256)$
  3. Επιλέγεται πρώτος p έτσι ώστε $2^{L-1} < p < 2^L$
  4. Επιλέγεται πρώτος q έτσι ώστε $2^{N-1} < q < 2^N$ και $q|(p-1)$
  5. Επιλέγεται μία κρυπτογραφική συνάρτηση σύνοψης $\mathcal{H}$ με μήκος εξόδου $|\mathcal{H}|$ bits η οποία πληρεί τα πρότυπα που προβλέπονται από τη νεότερη έκδοση DSS. Στο FIPS 186, δηλαδή την αρχική έκδοση του DSS, προτεινόταν η χρήση της SHA-1, ενώ στη τελευταία επίσημη έκδοση FIPS 186-4 προτείνεται η χρήση της SHA-2. Αν $N < |\mathcal{H}|$,

τότε χρησιμοποιούνται μόνο τα N σημαντικότερα ψηφία της εξόδου της $\mathcal{H}$.

6. Επιλέγεται h τυχαίος ακέραιος από το διάστημα $\{2, \cdots, p-2\}$.
7. Υπολογίζεται $g = h^{(p-1)/q} \mod p$. Στο σπάνιο σενάριο που $g = 1$ υπολογίζεται εξ' αρχής νέο h και νέο g. Το g είναι γεννήτορας της υπομάδας $\mathbb{G}$ τάξης q της $\mathbb{Z}_p^*$. Οι δημόσιοι παράμετροι του συστήματος είναι (p, q, g)

- **Δημιουργία Κλειδιών** - KGen():

  Με δεδομένες τις δημόσιες παραμέτρους του συστήματος κάθε χρήστης υπολογίζει με προβλεπόμενο τρόπο (με βάση κάποιο άλλο πρότυπο FIPS) τυχαίο x από το $\{1, \cdots, q-1\}$. Αυτό είναι το ιδιωτικό κλειδί του χρήστη και πρέπει να μείνει μυστικό. Δημοσιεύεται μέσω ενός έμπιστου καναλιού η τιμή $y = g^x \mod p$. Το y είναι το δημόσιο κλειδί του χρήστη.

- **Δημιουργία Υπογραφής** - Sign$(x, \mathtt{m})$:

  Έστω τώρα πως ο Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα στον Β. Για να το καταφέρει αυτό θα χρησιμοποιήσει το κλειδί $K = (p, q, g, x, y)$.

  1. Ο Α αρχικά επιλέγει τυχαίο k απο το $\{1, \cdots, q-1\}$
  2. Εν συνεχεία ο Α υπολογίζει $r = g^k \mod q$, αν $r = 0$ τότε υπολογίζεται νέο k εξ' αρχής και επαναυπλογίζεται νέο r.
  3. Ο Α υπολογίζει $s = (k^{-1}(\mathcal{H}(\mathtt{m}) + xr) \mod q)$, αν $s = 0$ τότε υπολογίζεται νέο k εξ' αρχής και επαναυπλογίζονται νέα r, s.

     Η υπογραφή είναι $\sigma = (r, s)$.

- **Επαλήθευση Υπογραφής** - Vrfy(σ, y):

  Οποιοδήποτε επιθυμεί να επιβεβαιώσει την ορθότητα της υπογραφής για ένα μύνημα m ελέγχει τα εξής:

  1. Ελέγχει αν $0 < r < q$ και $0 < s < q$
  2. Υπολογίζει $w = s^{-1} \mod q$
  3. Υπολογίζει $u_1 = \mathcal{H}(\mathtt{m})w \mod q$
  4. Υπολογίζει $u_2 = rw \mod q$
  5. Υπολογίζει $v = (g^{u_1} y^{u_2} \mod p) \mod q$

  Ο αλγόριθμος επιστρέφει 1 ανν $v = r$.

Λήμμα 3.2. *Ο γεννήτορας g όπως περιγράφηκε στα προηγούμενα είναι q-οστή ρίζα της μονάδας modulo p.*

Απόδειξη:

$$g^q \equiv h^{(p-1)q/q} \equiv h^{p-1} \equiv 1 \pmod{p}$$

Λήμμα 3.3. *Ορθότητα υπογραφής DSA*

Ο αλγόριθμος επαλήθευσης επιστρέφει 1 *για τις ορθώς συνταγμένες υπογραφές.*

Απόδειξη: Ισχύει ότι $s = k^{-1}(\mathcal{H}(\mathtt{m}) + xr) \mod q$

Άρα

$$k \equiv (\mathcal{H}(\mathtt{m}) + xr)s^{-1} \equiv \mathcal{H}(\mathtt{m})w + xrw \pmod{q}$$

Επομένως, επειδή g είναι τάξης q έχουμε:

$$g^k \equiv g^{\mathcal{H}(\mathtt{m})w} g^{xrw} \equiv g^{\mathcal{H}(\mathtt{m})w} y^{rw} \equiv g^{u_1} y^{u_2} \pmod{p}$$

Από τα προηγούμενα έχουμε ότι:

$$r = (g^k \mod p) \mod q = (g^{u_1} y^{u_2} \mod p) \mod q = v$$

□

Μερικά Σχόλια για τον DSA:

Ο αλγόριθμος DSA χρησιμοποιείται ευρέως, υλοποιήσεις του υπάρχουν στο OpenSSL, GnuTLS, crpyptlib, Crypto++, Nettle, και πολλές ακόμα. Παράλληλα προσφέρει υπογραφές μικρότερες από αυτές του σχήματος ElGamal, κανοντάς τον έτσι ιδανική επιλογή για εφαρμογές όπως έξυπνες κάρτες. Η ασφαλειά του έχει όμως αρχίσει να φθήνει, ακόμα και στο σενάριο που γίνεται χρήση πρώτων p, q με μήκη 3072 και 256 bits αντίστοιχα το σχήμα θεωρείται ασφαλές μέχρι το 2030. Για αυτό το λόγο έχει γίνει ήδη μεταφορά σε μεγάλο βαθμό στον αλγόριθμο ECDSA, δηλαδή τον ίδιο αλγόριθμο υλοποιημένο με ελλειπτικές καμπύλες πάνω από πεπερασμένα σώματα. Όπως προαναφέρθηκε η τυχαιότητα, εντροπία, και μοναδικότητα της τιμής k είναι νευραλγικής σημασίας για το σχήμα. Σε περίπτωση που γίνεται χρήση της ίδιας τιμής για διαφορετικές υπογραφές τα αποτελέσματα θα είναι ολέθρια, καθώς κάτι τέτοιο μπορεί να οδηγήσει σε πλήρη έκθεση του ιδιωτικού κλειδιού και άρα σε πλήρες σπάσιμο του συστήματος. Αυτή η αδυναμία υπάρχει τόσο στις κλασσικές εκδόσεις του ElGamal και DSA όσο και στις υλοποιήσεις του με ελλειπτικές καμπύλες.

Ένα μειονέκτημα, για κάποιους, που φέρει ο DSA είναι το γεγονός ότι προέρχεται απο το NIST, ή πιο συγκεκριμένα απο συνεργασία του NIST και της NSA (National Security Agency - Υπηρεσία Κρατικής Ασφάλειας των ΗΠΑ). Αυτό δεν είναι κάτι το καινούργιο πολλά κρυπτογραφικά primitives, standards, και υλοποιήσεις αυτών προέρχονται απο τέτοιες συνεργασίες.Τέτοια παραδείγματα αποτελούν οι συναρτήσεις κατακερματισμού SHA-1 και SHA-2, το συμμετρικό σύστημα κρυπτογράφησης DES, η γεννήτρια ψευδοτυχαίων bit Dual

Elliptic Curve Deterministic Random Bit Generator και άλλα πολλά. Ενώ η ασφάλεια αυτών των κατασκευών έχει αποδεικτεί ή καταρηφθεί (στη περίπτωση της DECDRBH), υπάρχουν πολλοί που θεωρούν πως είναι πιθανό η NSA να έχει φυτέψει κάποια πίσω πόρτα (backdoor), με απόταιρω σκοπό την παραβίαση του συστήματος σε κάποια στιγμή στο μέλλον. Κάτι τέτοιο φυσικά δεν έχει αποδειχθεί, όμως αυτό δεν αποτρέπει ορισμένα άτομα και οργανισμούς από το να συνομοσιολογούν και να μην εμπιστεύονται τις συγκεκριμένες υλοποιήσεις και κατασκευές.

Σχήμα Υπογραφών Schnorr

Ένα από τα πιο σημαντικά σχήματα υπογραφών είναι αυτό του Schnorr [72]. Οι υπογραφές Schnorr αποτελούν το πιο απλό είδος υπογραφών Type-T. Η ιδέα πίσω από τις υπογραφές Schnorr είναι η μετατροπή ενός Σ-Πρωτοκόλλου για γνώση διακριτού λογαρίθμου σε σχήμα υπογραφών. Ένας άλλος χαρακτηρισμός για αυτού του είδους της υπογραφές είναι και Signatures of Knowledge. Σαν primitive έχουν εισαχθεί από τις Chase και Lysyanskaya [25] και η ιδέα από πίσω τους είναι το πως να μετατραπεί ενός πρωτοκόλλου για γνώση μάρτυρα σε μια NP γλώσσα σε σχήμα υπογραφής.

Γενικότερα οι υπογραφές τύπου Schnorr και παραλλαγές αυτών είναι πολύ ισχυρό εργαλείο και όπως θα δούμε παρακάτω αποτελούν την βάση των περισσότερων από των σχημάτων υπογραφής με επιπρόσθετες λειτουργίες που θα δούμε στα επόμενα κεφάλαια.

Παραθέτουμε παρακάτω τους αλγορίθμους που απαρτίζουν το σχήμα υπογραφής Schnorr:

- **Δημόσιοι Παράμετροι:**
  1. Οι χρήστες συμφωνούν σε πρώτους p και q έτσι ώστε $q|(p-1)$, ομάδα $\mathbb{G}$ τάξης q όπου το DLOG θεωρείται δύσκολο και g κάποιο γεννήτορα της $\mathbb{G}$.
  2. Οι χρήστες συμφωνούν σε μία συνάρτηση σύνοψης $\mathcal{H}$, $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{G}$
- **Δημιουργία Κλειδιών** -$\mathsf{KGen}(1^\lambda)$:
  1. Κάθε χρήστης επιλέγει τυχαία $x \in_R \mathbb{Z}_q^*$.
  2. Υπολογίζει $y = g^x$ και το δημοσιεύει.
- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(x, \mathtt{m})$:

  Για να υπογράψει ένας χρήστης ένα μήνυμα $\mathtt{m}$ ακολουθεί τα παρακάτω βήματα:

1. Επιλέγει τυχαίο $k \in_R \mathbb{Z}_q^*$
2. Υπολογίζει $r = g^k$
3. Υπολογίζει $e = \mathcal{H}(r, \mathtt{m})$
4. Υπολογίζει $s = k - xe$

Η υπογραφή σ είναι $\sigma = (s, e)$

- **Επαλήθευση Υπογραφής** - $\mathsf{Vrfy}(\sigma, y)$:

  Για να επιβεβαιώσει κάποιος την ορθότητα της υπογραφής ακολουθεί την εξής διαδικασία:

  1. Υπολογίζει $r_v = g^s y^e$
  2. Υπολογίζει $e_v = \mathcal{H}(r_v, \mathtt{m})$

  Ο αλγόριθμος επιστρέφει 1 ανν $e_v = e$.

Λήμμα 3.4. *Ορθότητα υπογραφής Schnorr*
Ο αλγόριθμος επαλήθευσης επιστρέφει 1 *για τις ορθώς συνταγμένες υπογραφές.*

Απόδειξη:

$$r_v = g^s y^e = g^{k-xe} g^{xe} = g^k = r$$

Επομένως

$$e_v = \mathcal{H}(r_v, \mathtt{m}) = \mathcal{H}(r, \mathtt{m}) = e$$

. □

Ανάκτηση κλειδιού απο επαναχρησιμοποίηση τυχαιότητας:
Όπως και στο ElGamal, DSA, και ECDSA έτσι και στο σχήμα Schnorr δεν πρέπει να γίνεται πολλαπλή χρήση της τυχαιότητας από υπογραφή σε υπογραφή.

Παρακάτω δίνουμε τον τρόπο με τον οποίο μπορεί να γίνει η ανάκτηση του ιδιωτικού κλειδιού $\mathsf{sk} = x$ από δύο υπογραφές Schnorr διαφορετικών μηνυμάτων που έχουν την ίδια τυχαιότητα k.

Για αρχή ο αντίπαλος έχει στη διάθεσή του δύο υπογραφές που πληρούν τις παραπάνω προϋποθέσεις, έστω $\sigma = (s, e)$ και $\sigma' = (s', e')$. Επειδή $k = k'$ θα ισχύει ότι $s - s' = k - xe - (k - xe') \implies x = \frac{s-s'}{e'-e}$.

Επειδή s, s', e, e' είναι δημόσια ο αντίπαλος μπορεί να ανακτήσει με αυτό τον τρόπο το ιδιωτικό κλειδί του αντιπάλου χωρίς να χρειαστεί να βρει περαιτέρω πληροφορίες.

Γενικότερα όλα τα προαναφερθέντα σχήματα υπογραφών είναι ευάλωτα στη διαρροή της τυχαιότητας. Η εύρεση κατάλληλου τρόπου επιλογής της είναι ζωτικής σημασίας για το σχήμα αφού ακόμα και μικρά επίπεδα μεροληψείας στην

εντροπία της πηγής ή έστω και μερική διαρροή της τιμής k μπορούν να οδηγήσουν σε ανάκτηση του ιδιωτικού κλειδιού. Μια τέτοια παράβλεψη θα πρέπει να συνδυαστεί με ένα πλήθος υπογραφών από το ίδιο άτομο, κάτι όχι ιδιαίτερα τραβηγμένο σαν σενάριο επίθεσης, ώστε να μπορέσει έτσι ο αντίπαλος να λύσει το πρόβλημα του κρυμμένου αριθμού (Hidden Number Problem - HNP) [20, 2].

3.3 Σχήματα Υπογραφών με Επιπλέον Λειτουργικότητες

Έχοντας εφοδιαστεί με βασικές έννοιες κρυπτογραφίας δημοσίου κλειδιού θα μελετήσουμε στα επόμενα κεφάλαια σχήματα ψηφιακών υπογραφών που προσφέρουν επιπλέον λειτουργίες. Στο κεφάλαιο 4 θα δούμε τις αδιαμφησβήτητες υπογραφές και τις υπογραφές καθορισμένου επαληθευτή. Στο κεφάλαιο 5 θα μελετήσουμε τις υπογραφές δακτυλίου και τις συνδέσιμες υπογραφές δακτυλίου, ενώ στο κεφάλαιο 6 θα δούμε των συνδυασμό των συνδέσιμων υπογραφών δακτυλίου και των υπογραφών καθορισμένου επαληθευτή, το DVLRS. Το τελευταίο σχήμα που θα μελετήσουμε στο κεφάλαιο 7 θα είναι το UDVLRS, το οποίο αποτελεί και το κύριο κομμάτι της ΔΕ.

Κεφάλαιο 4

Υπογραφές Καθορισμένου Επαληθευτή

Στο κεφάλαιο αυτό θα ασχοληθούμε με το πρώτο κύριο συστατικό των DVLRS και UDVLRS, τις υπογραφές Καθορισμένου Επαληθευτή (Designated Verifier Signatures - DVS).

Πολλές φορές είναι επιθυμητό να περιορίζεται τεχνητά ποιος είναι ικανός να επιβεβαιώση την εγκυρότητα μιας υπογραφής. Για την επίτευξη αυτού του σκοπού έχουν προταθεί διάφορα είδη υπογραφών που προσεγγίζουν το πρόβλημα από διαφορετικές οπτικές γωνίες και προσφέρουν ποικίλες ιδιότητες.

Μία πρώτη λύση είναι οι αδιαμφισβήτητες υπογραφές (undeniable signatures) [28, 62]. Οι αδιαμφισβήτητες υπογραφές έχουν την απαίτηση ο υπογράφοντας να συμμετάσχει στη διαδικασία επαλήθεσης της υπογραφής ενώ παράλληλα δεν έχει τη δυνατότητα να αμφισβητήσει την ιδιοκτησία μιας υπογραφής του. Ο υπογράφοντας έχει πάντα τη δυνατότητα να αποδείξει ότι μια έγκυρη υπογραφή είναι έγκυρη, και μία άκυρη υπογραφή είναι άκυρη.

Οι υπογραφές καθορισμένου επαληθευτή [45] αποτελούν μία τροποποίηση του σχήματος των αδιαμφισβήτητων υπογραφών. Η ιδέα πίσω από τις DVS είναι ότι μόνο ένα άτομο, ο καθορισμένος επαληθευτής, μπορεί να πεισθεί για την εγκυρότητα μιας υπογραφής, χωρίς όμως να είναι ικανός να πείσει οποιονδήποτε άλλο ότι μια υπογραφή προέρχεται από έναν συγκεκριμένο υπογράφοντα. Ο τρόπος με τον οποίο επιτυγχάνεται η συγκεκριμένη ιδιότητα είναι με την προσθήκη της δυνατότητας παραγωγής προσομοιώσεων υπογραφών από τον ίδιο τον επαληθευτή, οι οποίες είναι μη-διακρίσιμες από έγκυρες υπογραφές κανονικών υπογράφοντων.

Μία ακόμα επιλογή αποτελούν οι υπογραφές καθορισμένου επιβεβαιωτή (designated confirmer signatures) [26], στις οποίες η επαλήθεση της εγκυρότητας μιας υπογραφής γίνεται με τη βοήθεια μιας τρίτης ημι-έμπιστης οντότητας, του καθορισμένου επιβεβαιωτή, χωρίς να είναι αναγκαία η συμμετοχή του υπ-

ογράφοντα. Οι υπογραφές καθορισμένου επιβεβαιωτή βασίζονται στις μετατρέψιμες αδιαμφισβήτητες υπογραφές [21] και θεωρούνται μια βελτιωσή τους.

Στο συγκεκριμένο κεφάλαιο θα ασχοληθούμε με τις αδιαμφισβήτητες υπογραφές και τις υπογραφές καθορισμένου επαληθευτή, αναφέρουμε όμως και τα τρία είδη μιας και η ονοματολογία τους μπορεί να προκαλέσει σύγχηση στον αναγνώστη.

4.1 Αδιαμφισβήτητες Υπογραφές

Για να γίνει πιο κατανοητή η χρήση των αδιαμφισβήτητων υπογραφών από τον αναγνώστη θα παραθέσουμε το παράδειγμα που δίνεται στη [62]. Έστω λοιπόν ότι μια εταιρεία ανάπτυξης λογισμικού θέλει να υπογράφει το λογισμικό που πουλάει για λόγους διασφάλισης γνησιότητας αντιγράφου. Οι κλασικές ψηφιακές υπογραφές δε θα πρόσφεραν απόδειξη γνησιότητας μιας και οποιοσδήποτε θα μπορούσε να μεταπουλήσει το αντιγραφό του σε κάποιον τρίτο, ενώ όλοι θα μπορούσαν να πειστούν ότι πρόκειται για γνήσιο αντίγραφο.

Τη λύση σε αυτό το πρόβλημα την προσέφεραν οι Chaum και Antwerpen το 1989 στην εργασία τους [28] με την εισαγωγή των αδιαμφισβήτητων υπογραφών. Η ιδέα πίσω από τις αδιαμφισβήτητες υπογραφές είναι η εξής: Έστω η οντότητα A η οποία υπογράφει κάποιο μήνυμα $\mathtt{m}$ με χρήση του ιδιωτικού της κλειδιού sk και παίρνει έτσι την υπαογραφή σ. Ως εδώ έχουμε περιγράψει το γενικό πλαίσιο μιας ψηφιακής υπογραφής. Η διαφορά έγγυται στο τρόπο με τον οποίο λειτουργεί ο αλγόριθμος επαλήθεσης. Σε αντίθεση με τις συνήθεις ψηφιακές υπογραφές που είναι δημοσίως επαληθεύσιμες οποιοσδήποτε θέλει να αποδείξει την εγκυρότητα της σ θα πρέπει να εμπλακεί σε ένα διαλογικό πρωτόκολλο με τον A. Οι συγκεκριμένες υπογραφές καλούνται αδιαμφισβήτητες από το γεγονός ότι μία έγκυρη υπογραφή δε μπορεί να αποκηρυχθεί από τον υπογραφοντά της, ενώ ταυτόχρονα ο υπογράφοντας μπορεί να αποδείξει ότι μια υπογραφή δεν είναι έγκυρη. Για την απόδειξη εγκυρότητας ο κάτοχος μιας υπογραφής μπορεί να ξεκινήσει ένα διαλογικό πρωτόκολλο ώστε να αποδειχθεί η γνησιότητα της υπογραφής, ακόμα και αν ο υπογράφοντας είναι κακόβουλος και προσπαθήσει να αποποιηθεί της σύνταξης της υπογραφής. Μη συμμετοχή του υπογράφοντα στο πρωτόκολλο μπορεί να θεωρηθεί απόδειξη ότι η συγκεκριμένη υπογραφή ανήκει στον φερόμενο ως υπογράφοντα.

Μοντέλο Αδιαμφισβήτητων Υπογραφών

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

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

  Δεδομένης παραμέτρου ασφαλείας λ δημιουργεί ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού $(\mathsf{sk}, \mathsf{pk})$.

  Καλούμε $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$

- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(\mathsf{sk}, \mathtt{m})$:

  Με είσοδο το ιδιωτικό κλειδί του υπογράφοντα sk και ένα μήνυμα $\mathtt{m}$ επιστρέφει μία υπογραφή σ.

  Καλούμε $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, \mathtt{m})$.

- **Πρωτόκολλο Επιβεβαίωσης** - Conf:

  Διαλογικό πρωτόκολλο μεταξύ του υπογράφοντα S και ενό επαληθευτή V όπου με είσοδο μία υπογραφη σ και ένα μήνυμα $\mathtt{m}$ ο υπογράφοντας αποδεικνύει ότι η υπογραφή είναι έγκυρη.

- **Πρωτόκολλο Αποκήρυξης** - Dvow:

  Διαλογικό πρωτόκολλο μεταξύ του υπογράφοντα S και ενό επαληθευτή V όπου με είσοδο μία υπογραφη σ και ένα μήνυμα $\mathtt{m}$ ο υπογράφοντας αποδεικνύει ότι η υπογραφή είναι μη-έγκυρη.

Σημείωση: Δεν είναι πάντα αναγκαστικό τα πρωτόκολλα επιβεβαιώσης και αποκήρυξης να είναι διαφορετικά μεταξύ τους, σε ορισμένα σχήματα υπάρχει μόνο ένα πρωτόκολλο το οποίο είναι ικανό να αποφανθεί για την εγκυρότητα ή μη της υπογραφής και να το αποδείξει.

Σχήμα Αδιαμφισβήτητων Υπογραφών Chaum

Το παράδειγμα αδιαμφισβήτητων υπογραφών που θα μελετήσουμε είναι αυτό του Chaum τροποποιημένο ώστε να χρησιμοποιεί κρυπτογραφικές συναρτήσεις σύνοψης [62]. Για το πρωτόκολλο αποκήρυξης χρησιμοποιείται το σχήμα δέσμευσης των [22].

Για αρχή θα δουλεύουμε σε μία ομάδα $\mathbb{G}$, τάξης πρώτου q με γεννήτορα g στην οποία υποθέτουμε πως ισχύει η υπόθεση DDH. Επιπλέον θεωρούμε μία κρυπταγραφική συνάρτηση σύνοψης $\mathcal{H} : \{0,1\}^* \to \mathbb{G}$.

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

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

- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(x, \mathtt{m})$:
  1. $\sigma \leftarrow \mathcal{H}(m)^x$
- **Πρωτόκολλο Επιβεβαίωσης** - $\mathsf{Conf}_{S \leftrightarrow V}(\sigma, \mathtt{m})$:
  1. V $\rightarrow$ S :
     - $a, b \leftarrow \$\mathbb{Z}_q$
     - $c \leftarrow g^a \mathcal{H}(\mathtt{m})^b$
     - S στέλνει c στον V
  2. S $\rightarrow$ V :
     - $r \leftarrow \$\mathbb{Z}_q$
     - $z_1 \leftarrow cg^r$
     - $z_2 \leftarrow z_1^x$
     - V στέλνει z_1, z_2 στον S
  3. V $\rightarrow$ S :
     - Ο V λαμβάνει z_1, z_2
     - Στέλνει a, b στον S
  4. S $\rightarrow$ V :
     - Ο S λαμβάνει a, b και υπολογίζει $g^a \mathcal{H}(\mathtt{m})^b$
     - Αν $c = g^a \mathcal{H}(\mathtt{m})^b$ τότε στέλνει r στον V
  5. V $\rightarrow$ S :
     - Ο V λαμβάνει r και υπολογίζει $g^{a+r}\mathcal{H}(\mathtt{m})^b$ και $y^{a+r}\mathcal{H}(\mathtt{m})^b$
     - Αν $z_1 = g^{a+r}\mathcal{H}(\mathtt{m})^b$ **ΚΑΙ** $z_2 = y^{a+r}\mathcal{H}(\mathtt{m})^b$, τότε **Επέστρεψε** 1
- **Πρωτόκολλο Αποκύρηξης** - $\mathsf{Dvow}_{S \leftrightarrow V}(\sigma, \mathtt{m})$:
  1. V $\rightarrow$ S :
     - $s \leftarrow \$\{1, \ldots, \lambda\}$
     - $a \leftarrow \$\mathbb{Z}_q$
     - $c \leftarrow g^a \mathcal{H}(\mathtt{m})^s$
     - $c' y^a \sigma^s$
     - S στέλνει c, c' στον V
  2. S $\rightarrow$ V :
     - Βρίσκει s' τ.ω. $cc'^{-1} = (\mathcal{H}(\mathtt{m})^x \sigma^{-1})^{s'}$

   - Δεσμεύεται στη τιμή s'

3. $\mathsf{V} \rightarrow \mathsf{S}$:
   - Ο V λαμβάνει τη δέσμευση του S
   - Στέλνει a στον S

4. $\mathsf{S} \rightarrow \mathsf{V}$:
   - Ο S λαμβάνει a και υπολογίζει $g^a \mathcal{H}(\mathtt{m})^{s'}$
   - Αν $c = g^a \mathcal{H}(\mathtt{m})^{s'}$ αποδεσμεύεται για το s'

5. $\mathsf{V} \rightarrow \mathsf{S}$:
   - Ο V λαμβάνει s
   - Αν $s = s'$ τότε **Επέστρεψε** 1

Ιδιότητες Ασφάλειας Αδιαμφισβήτων Υπογραφών

Όπως και όλες οι υπογραφές έτσι και Αδιαμφισβήτητες Υπογραφές πρέπει να είναι μη-πλαστογραφήσιμες. Η κύρια ιδιότητα ασφάλειας που διαθέτουν είναι η αορατότητα (invisibility στη βιβλιογραφία [21, 27]), η οποία δηλώνει ότι δε πρέπει να είναι εφικτό μία έγκυρη υπογραφή να μπορεί διακριθεί από μία μη-έγκυρη με μη-αμελητέο πλεονέκτημα, χωρίς τη συνδρομή του υπογράφοντα στη διαδικασία. Οι [36] προτείνουν μία ακόμα ιδιότητα αυτή της ανωνυμίας, η οποία δηλώνει ότι δοσμένης μίας έγκυρης υπογραφής και τα δημόσια κλειδία δύο πιθανών υπογραφόντων, η πραγματική προέλευση της υπογραφής δε μπορεί να διακριθεί. Στην ίδια εργασία αποδεικνύεται ότι η έννοια της αορατότητας και της ανωνυμίας είναι ισοδύναμες.

Ασφάλεια Σχήματος Υπογραφών Chaum

Για το σχήμα υπογραφών Chaum με κρυπτογραφική συνάρτηση σύνοψης που παραθέσαμε έχουν αποδεικτεί από τους [62] τα ακόλουθα θεωρήματα:

Θεώρημα 4.1. *Μη-Πλαστογραφησιμότητα*
Η υπογραφή Chaum είναι μη-πλαστογραφήσιμη στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν και μόνο αν ισχύει η υπόθεση DDH *στη* $\mathbb{G}$.

Θεώρημα 4.2. *Αορατότητα*
Η υπογραφή Chaum είναι αόρατη στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν ισχύει η υπόθεση CDH *στη* $\mathbb{G}$.

4.2 Υπογραφές Καθορισμένου Επαληθευτή

Στη προηγούμενη ενότητα παραθέσαμε τις αδιαμφισβήτητες υπογραφές. Ενώ ο στόχος τους ήταν να μπορούν να περιορίσουν το ποιος μπορεί να πειστεί για την εγκυρότητα τους στη πραγματικά επιτυγχάνουν μόνο το πότε θα πειστεί κάποιος για την εγκυρότητα τους. Το 1996 οι Jakobsson, Sako και Impagliazzo σκέφτηκαν έναν τρόπο κατασκευής υπογραφών οι οποίες θα έχουν την ιδιότητα να πείθουν πραγματικά μόνο τον επιθυμητό παραλήπτη του μηνύματος [45].

Ας θέσουμε λοιπόν το εξής ερώτημα: Με ποιο τρόπο μπορώ να είμαι σίγουρος πως το μήνυμα που στέλνω θα μπορεί να είναι χρήσιμο μόνο για τον παραλήπτη που επιθυμώ, ενώ ταυτόχρονα να είναι άχρηστο για οποιονδήποτε άλλο;

Ένας τρόπος θα ήταν με συμμετρική κρυπτογραφία, τα δύο άτομα που επιθυμούν να επικοινωνούν θα έρχονταν σε επαφή, θα αντάλλαζαν μεταξύ τους ένα κλειδί συμμετρικού κρυπτοσυστήματος (π.χ. AES, DES κ.ο.κ) και θα αντάλλαζαν μηνύματα έτσι. Ενώ αυτό αποτελεί μία λύση στο πρόβλημα γεννιούνται ταυτόχρονα και άλλα προβλήματα που υπάρχουν τώρα στη Συμμετρική Κρυπτογραφία, όπως π.χ. η διαχείρηση των κλειδιών, το ζήτημα της ασφάλειας της ανταλλαγής και άλλα πολλά.

Οι Jakobsson, Sako και Impagliazzo σκέφτηκαν έναν ιδιαίτερα ιδιοφυή τρόπο να λύσουν αυτό το πρόβλημα μέσω της Κρυπτογραφίας Δημοσίου Κλειδιού, τις υπογραφές καθορισμένου επαληθευτή (designated verifier signatures - DVS). Έστω λοιπόν ότι ο S θέλει να στείλει ένα μήνυμα $\mathtt{m}$ ώστε το μόνο άτομο που θα μπορεί να πειστεί για από τη συγκεκριμένη υπογραφή είναι η V. Ένας απλός τρόπος να το καταφέρει είναι να κατασκευάσει μία υπογραφή η οποία θα αποδεικνύει την εξής πρόταση: Είμαι ο S και υπογράφω το $\mathtt{m}$ *Ή* είμαι η V. Με αυτό το τρόπο πετυχαίνουμε τον σκοπό μας αφού σε οποιονδήποτε τρίτο εκτός του S και της V η υπογραφή φαίνεται να έχει προέλθει είτε από τον S είτε από τη V ενώ παράλληλα η V ξέρει ότι υπογραφή προέρχεται από τον S μιας και ξέρει ότι δεν την έχει φτίαξει η ίδια.

Για να μπορέσει να επιτευχθεί το σενάριο που περιγράψαμε στη προηγούμενη παράγραφο θα χρειαστούμε την εισαγωγή ενός ακόμα αλγορίθμου. Έτσι λοιπόν εκτός από τον αλγορίθμο υπογραφής Sign που θα διαθέτει το σχήμα μας και θα μπορεί να επικαλεστεί ο υπογράφοντας όταν θέλει να υπγράψει ένα μήνυμα θα εισάγουμε έναν αλγόριθμος προσομοίωσεις Sim. Τον Sim θα τον επικαλείται ο καθορισμένος επαληθευτής ώστε να κατασκευάζει προσομοίωσεις υπογραφών οι οποίες είναι μη-διακρίσιμες από τις υπογραφές που μπορεί να παράξει οποιοσδήποτε υπογράφοντας. Με αυτό τον τρόπο κανένας, πέραν του καθορισμένου επαληθευτή και του εκάστωτε υπογράφοντα, δε θα μπορεί να είναι σίγουρος για την προέλευση μίας υπογραφής που βλέπει, κάνοντας τις έτσι χρήσιμες μόνο για τον υπογράφοντα και τον παραλήπτη που επιθυμεί.

Σημείωση: Ο καθορισμένος επαληθευτής θα είναι ο παραλήπτης στο σενάριο που περιγράψαμε προηγουμένως.

Μια ενδιαφέρουσα εφαρμογή των DVS είναι η χρήση σε συστήματα ηλεκτρονικών εκλογών. Ας υποθέσουμε πως ένας ψηφοφόρος επιθυμεί μία απόδειξη ότι η ψήφος έχει καταμετρηθεί ορθά (counted as cast). Αυτό ενώ αποτελεί μία λογική απαίτηση σε οποιαδήποτε ψηφοφορία, και ιδιαίτερα στις ηλεκτρονικές, μπορεί να χρησιμοποιηθεί για κακόβουλους σκοπούς. Έτσι λοιπόν ο ψηφοφόρος αυτός μπορεί να χρησιμοποιήσει αυτή την απόδειξη για να πουλήσει τη ψήφο του. Αν όμως στις εκλογές χρησιμοποιούνται υπογραφές DVS τότε ο κακόβουλος ψηφοφόρος δε θα μπορεί να αποδείξει ότι η ψήφος προέρχεται πράγματι από εκείνον και όχι από τον καθορισμένο επαληθευτή, προστατεύοντας έτσι το εκλογικό αποτέλεσμα.

Το προαναφερθές παράδειγμα προσφέρει τη διαίσθηση πίσω από τις υπογραφές καθορισμένου επαληθευτή, οι υπογραφές που παράγονται είναι χρήσιμες μόνο για τον καθορσιμένο επαληθευτή και κανέναν άλλο, μιας μία προσομοίωση και μία κανονική υπογραφή είναι μη-διακρίσιμες μεταξύ τους.

4.2.1 Το Μοντέλο DVS

Τυπικά ένα σχήμα υπογραφών καθορισμένου επαληθευτή (DVS) αποτελείται από μία τετράδα αλγορίθμων $(\mathsf{KGen}, \mathsf{Sign}, \mathsf{Sim}, \mathsf{Vrfy})$:

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

  Κάθε χρήστης επικαλείται τον αλγόριθμο KGen ώστε να λάβει το ζεύγος κλειδιών του $(\mathsf{sk}, \mathsf{pk})$. Τα κλειδιά δημιουργούνται κατά βούληση από τον εκάστοτε χρήστη.

  Καλούμε $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}()$.

- **Δημιουργία Υπογραφής -** $\mathsf{Sign}(\mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_S)$:

  Για να υπογράψει ένας υπογράφοντας S ένα μήνυμα $\mathtt{m}$ επικαλείται τον αλγόριθμο Sign το μήνυμα $\mathtt{m}$, το δημόσιο κλειδί του designated verifier pk_D και το ιδιωτικό κλειδί του sk_S.

  Καλούμε $\sigma \leftarrow \mathsf{Sign}(\mathtt{m}, \mathsf{pk}_D, \mathsf{sk})$.

- **Δημιουργία Προσομοίωσης -** $\mathsf{Sim}(\mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D)$:

  Ο καθορισμένος επαληθευτής επικαλείται τον αλγόριθμο Sim όταν θέλει να προσομοιώσει μία υπογραφή. Για είσοδο δίνει το μήνυμα $\mathtt{m}$, το ζεύγος κλειδιών του $(\mathsf{sk}_D, \mathsf{pk}_D)$.

  Καλούμε $\sigma \leftarrow Sim(\mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D)$.

- **Επαλήθευση** - $\mathsf{Vrfy}(\sigma, \mathtt{m}, \mathsf{pk}_D)$:

  Ο αλγόριθμος επαλήθευσης επιστρέφει 1 αν η υπογραφή σ είναι έγκυρη, αλλίως επιστρέφει 0.

  Καλούμε $\{0,1\} \leftarrow \mathsf{Vrfy}(\sigma, \mathtt{m}, pk_D)$.

Όπως είναι αναμενώμενο έγκυρη είναι τόσο μία υπογραφή που είναι έξοδος του αλγορίθμου Sign όσο και μία προσομοίωση που είναι έξοδος του αλγορίθμου Sim. Επομένως ο αλγόιθμος Vrfy θα απαντάει με 1 και στις δύο περιπτώσεις. Είναι σημαντικό να κατανοήσουμε ότι μία προσομοίωση δεν αποτελεί πλαστογραφία μιας και είναι μια διαδικασία που προβλέπεται εκ κατασκευής του σχήματος. Για να αντικατροπτίσουμε αυτή την ιδιαιτερότητα των DVS θα τροποποιήσουμε κατάλληλα τα ήδη υπάρχοντα μοντέλα ασφάλειας ψηφιακών υπογραφών σε επόμενη ενότητα.

4.2.2 Το Σχήμα JSI

Σε αυτή την ενότητα θα παρουσίασουμε το σχήμα που προτάθηκε από τους Jakobsson, Sako και Impagliazzo στην εργασία τους [45]. Η κατασκεύη βασίζεται στη κατασκευή των αδιαμφισβήτητων υπογραφών του Chaum, μαζί με το σχήμα δέσμευσης με καταπακτή [22] για τις προσομοιώσεις υπογραφών και το μετασχηματισμό Fiat Shamir για μη-διαλογικές αποδείξεις.

Το σχήμα δουλεύει σε μία ομάδα $\mathbb{G}$ τάξης πρώτου q και γεννήτορα g στην οποία θεωρούμε πως ισχύει η υπόθεση DDH. Επιπλέον θεωρούμε και μία κρυπτογραφική συνάρτηση σύνοψης $\mathcal{H}_q : \{0,1\}^* \rightarrow \mathbb{Z}_q$.

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

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

- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(\mathtt{m}, y_D, x_S,)$:

  1. $s \leftarrow \mathtt{m}^{x_S}$
  2. $w, r, t \leftarrow \$\mathbb{Z}_q$
  3. $c \leftarrow g^w y_D^r$
  4. $G \leftarrow g^t$
  5. $M \leftarrow m^t$
  6. $h \leftarrow \mathcal{H}_q(c, G, M)$

7. $d \leftarrow t + x_S(h + w)$
8. $\sigma \leftarrow (s, w, r, G, M, d)$
9. **Επέστρεψε** σ

- **Δημιουργία Προσομοίωσης** - $\mathsf{Sim}(\mathtt{m}, x_D, y_S)$:

1. $s \leftarrow \$\mathbb{G}$
2. $d, \alpha, \beta, \leftarrow \$\mathbb{Z}_q$
3. $c \leftarrow g^{\alpha}$
4. $G \leftarrow g^{d} y_S^{-\beta}$
5. $M \leftarrow \mathtt{m}^{d} s^{-\beta}$
6. $h \leftarrow \mathcal{H}_q(c, G, M)$
7. $w \leftarrow \beta - h$
8. $r \leftarrow (\alpha - w) x_D^{-1}$
9. $\sigma \leftarrow (s, w, r, G, M, d)$
10. **Επέστρεψε** σ

- **Επαλήθευση** - $\mathsf{Vrfy}(\sigma, y_S, y_D, \mathtt{m})$:

1. $c \leftarrow g^{w} y_D^{r}$
2. $h \leftarrow \mathcal{H}_q(c, G, M)$
3. Αν $G y_S^{h+w} = g^{d}$ **ΚΑΙ** $M s^{h+w} = m^{d}$ **Επέστρεψε** 1

Θα αποδείξουμε τώρα την ορθότητα του σχήματος που μόλις παρατέθηκε, δηλαδή ότι οι τίμια κατασκευασμένες υπογραφές και προσομοιώσεις επαληθεύονται ορθά.

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

Απόδειξη.

$$G y_S^{h+w} = g^{t} g^{x_S(h+w)} = g^{t + x_S(h+w)} = g^{d}$$
$$M s^{h+w} = \mathtt{m}^{t} \mathtt{m}^{x_S(h+w)} = \mathtt{m}^{t + x_S(h+w)} = m^{d}$$

□

Λήμμα 4.2. *Μία τίμια προσομοίωση σ επαληθεύεται ορθά.*

Απόδειξη.

$$G y_S^{h+w} = g^{d} y_S^{-\beta} g_S^{x_S(h+w)} = g^{t - x_S\beta + x_S(h+\beta-h)} = g^{d}$$
$$M s^{h+w} = \mathtt{m}^{d} s^{-\beta} s^{h+w} = \mathtt{m}^{d} s^{-\beta+h+\beta-h} = m^{d}$$

□

4.2.3 Ιδιότητες Ασφάλειας DVS

Συνεχίζουμε την παρουσίαση των DVS παραθέτοντας το μοντέλο ασφαλείας που ακολουθείτε.

Για αρχή, όπως σε όλες τις ψηφιακές υπογραφές, οι DVS πρέπει να είναι μη-πλάστογραφίσιμες. Όπως εξηγήσαμε και πριν αυτό χρειάζεται μια ελαφριά τροποποίηση από τον συνηθισμένο ορισμό μιας και τώρα εκτός του υπογράφοντα υπάρχει ακόμα μία οντότητα που μπορεί να δημιουργεί υπογραφές οι οποίες φαίνεται να προέρχονται από κάποιο διαφορετικό άτομο. Επομένως για τη μη-πλαστογραφησιμότητα απαιτούμε κανένας πέραν του υπογράφοντα και του καθορισμένου επαληθευτή να μη μπορεί να παράξει γνήσιες υπογραφές.

Η δεύτερη ιδότητα που προσφέρουν οι DVS είναι η μη-μεταφερσιμότητα. Η μη-μεταφερσιμότητα επιτυγχάνεται με τη μη-διακρισιμότητα μεταξύ των υπογραφών και των προσομοιώσεων. Η συγκεκριμένη ιδιότητα μπορεί να χωριστεί σε δύο ξεχωριστά επίπεδα. Αν οι υπογραφές και οι προσομοιώσει είναι ισόνομες, τότε θα λέμε πως το σχήμα είνα *τέλεια μη-μεταφέρσιμο*. Αν τώρα η δυσκολία διάκρισης μίας υπογραφής και μίας προσομοίωσης βασίζεται σε κάποιο δύσκολο πρόβλημα τότε μιλάμε για *υπολογιστική μη-μεταφερσιμότητα*. Σε αντίθεση με άλλες ιδιότητες, όπως π.χ. η ανωνυμία που θα δούμε στο κεφάλαιο 5, η υπολογιστική και η τέλεια μη-μεταφερσιμότητα είναι εξίσου σημαντικές και προσφέρουν διαφορετική χρηστικότητα σε ένα σχήμα.

Τέλος υπάρχει η ιδιότητα μία υπογραφή να είναι μη-εξουσιοδοτήσιμη [55]. Εδώ η απαίτηση είναι να μη μπορεί ούτε ο καθορισμένος επαληθευτής, ούτε ο υπογράφοντας να παραχωρήσουν σε κάποιν τρίτο το δικαίωμα να υπογράφουν ή να προσομοιώνουν με το αντίστοιχο δημόσιο κλειδί, χωρίς όμως να αποκαλύπτουν το ιδιωτικό τους κλειδί. Ο λόγος που προκύπτει η συγκεκριμένη ιδιότητα είναι γιατί δεν καλύπτεται από τους συνήθεις ορισμούς της μη-πλαστογραφισημότητας μιας και απαιτεί την συνεργασία τουλάχιστον δύο οντοτήτων, είναι δηλάδη ένα παράδειγμα επίθεσης συννενόησης (collusion attack). Για τις εφαρμογές και το εύρος αξιοποίησης των DVS στη συγκεκριμένη ΔΕ θα αρκεστούμε στη θέση των [55], η οποία είναι η εξής: Αν κάποιος δείξει ότι η υπογραφή αποτελεί απόδειξη γνώση του κλειδιού του υπογράφοντα ή του καθορισμένου επαληθευτή, και ισχύει ότι η υπογραφή είναι μη-πλαστογραφίσιμη τότε έπεται άμεσα ότι η υπογραφή είναι μη-εξουσιοδοτήσιμη.

Θα δείξουμε τώρα τους τυπικούς ορισμούς για τις παραπάνω ιδιότητες μέσω παιχνιδιών ασφαλείας. Τη δυνατότητα του αντιπάλου $\mathcal{A}$ να ζητά υπογραφές και προσομοιώσεις της αρεσκείας τη μοντελοποιούμε με χρήση των μαντείων υπογρφής και προσομοίωσης $\mathcal{SO}, \mathcal{MO}$ αντίστοιχα. Τέλος θεωρούμε πως η κρυπτογραφική συνάρτηση σύνοψης καθώς και οποιαδήποτε άλλη μορφή τυχαιότητας που χρειάζεται ο $\mathcal{A}$ μοντελοποιείται μέσω του τυχαίου μαντείου $\mathcal{RO}$.

Μη-Πλαστογραφησιμότητα

Για το πείραμα μη-πλαστογραφισημότητας ζητείται από τον $\mathcal{A}$ να παράξει μία έγκυρη υπογραφή, χωρίς να γνωρίζει κάποιο από τα διαθέσιμα μυστικά κλειδιά. Επιτρέπεται να ζητά με οποιαδήποτε προσαρμοστική στρατηγική υπογραφές και προσομοίωσεις της αρεσκείας του, όμως δεν θα είναι αποδεκτή καμία από αυτές ως απάντηση στο παιχνίδι.

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$(\mathsf{sk}_S, \mathsf{pk}_S, \mathsf{sk}_D, \mathsf{pk}_D) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)$
$(\sigma, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{SO},\mathcal{MO}}(1^\lambda, \mathsf{pk}_D, \mathsf{pk}_S)$
if *σ δεν είναι έξοδος του* $\mathcal{SO}$ ***ΚΑΙ*** *δεν είναι έξοδος του* $\mathcal{MO}$ **then**
| **Επέστρεψε** $\mathsf{Vrfy}(\sigma, \mathsf{pk}_S, \mathsf{pk}_D, \mathtt{m})$

else
| **Επέστρεψε:** $\perp$
end

Ορισμός 4.1. *Μη-Πλαστογραφησιμότητα*

Ένα DVS σχήμα Π θα λέγεται ότι διαθέτει την ιδιότητα της μη-πλαστογραφισημότητας αν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *ισχύει:*

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

Μη-Μεταφερσιμότητα

Θα εστιάσουμε στον ορισμό της τέλειας μη-μεταφερσιμότητας. Επειδή υποθέτουμε έναν υπολογιστικά μη-φραγμένο αντίπαλο δε θα δώσουμε πρόσβαση στα $\mathcal{SO}$ και $\mathcal{MO}$, μιας και είναι ικανός να υπολογίσει τα ιδιωτικά κλειδιά μέσω των αντίστοιχων δημοσίων κλειδιών και να παράξει τις υπογραφές και προσομοιώσεις που επιθυμεί. Το πείραμα λειτουργεί με τον ακόλουθω τρόπο: ο $\mathcal{A}$ επιλέγει ένα μήνυμα $\mathtt{m}$ και το σύστημα παράγει μία υπογραφή σ_0 και μια προσομοίωση σ_1 και στέλνει στη τύχη μία από τις δύο στον $\mathcal{A}$. Ο $\mathcal{A}$ με τη σειρά του πρέπει να αποφανθεί για το αν έλαβε την υπογραφή ή την προσομοίωση.

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

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

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

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

Ασφάλεια Υπογραφών JSI

Για το σχήμα των Jakobsson, Sako και Impagliazzo [45] αποδεικνόνται από τους [55] τα ακόλουθα θεωρήματα:

Θεώρημα 4.3. *Μη-Πλαστογραφήσιμη*
Η υπογραφή JSI είναι μη-πλαστογραφίσιμη (και μη-εξουσιοδοτήσιμη) στο μοντέλου του τυχαίου μαντείου $\mathcal{RO}$ αν ισχύει η υποθεση DDH *στην ομάδα $\mathbb{G}$.*

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

4.2.4 Άλλες Υπογραφές Καθορισμένου Επαληθευτή

Θα παρουσίασουμε ταχέως ορισμένες ακόμα εκδοχές υπογραφών καθορισμένου επαληθευτή.

Υπογραφές Ισχυρά Καθορισμένου Επαληθευτή

Ξεκινάμε με τις υπογραφές ισχυρά καθορισμένου επαληθευτή (strong designated verifer signatures - sDVS). Οι sDVS προτάθηκαν στην ίδια εργασία με τις απλές DVS [45] και έχουν την επιπλεόν ιδιότητα ότι δεν είναι δημόσια επαληθεύσιμες. Ο αλγόριθμος επαλήθευσης έχει ως είσοδο και το ιδιωτικό κλειδί του υπαληθευτή. Αυτή η τροποποίηση υπάρχει για το σενάριο στο οποίο κάποιος

τρίτος είναι απόλυτα σίγουρος ότι ο καθορισμένος επαληθευτής δε χρησιμοποιεί καθόλου τον αλγόριθμο προσομοίωσης, και έτσι θα ήταν εφικτό να πεισθεί για την εγκυρότητα και την προέλευση των υπογραφών μέσω της δημόσιας επαληθευσής τους. Για να κατασκευαστεί ένα sDVS σχήμα αρκεί κάποιος να κρυπτογραφήσει μία υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του καθορισμένου επαληθευτή και ένα ασφαλές κρυπτοσύστημα (δημοσίου κλειδιού στην προκειμένη περίπτωση). Με αυτό τον τρόπο η επαλήθευση μιας υπογραφής απαιτεί πρώτα την αποκρυπτογραφησή της, κάτι που μπορεί να κάνει μόνο ο καθορισμένος επαληθευτής. Οι απαιτήσεις ασφάλειας δε διαφέρουν καθόλου σε σχέση με τις DVS που αναφέραμε στη προηγούμενη ενότητα.

Καθολικές Υπογραφές Καθορισμένου Επαληθευτή

Οι καθολικές υπογαραφές καθορισμένου επαληθευτή [50] λειτουργούν ως κοινές ψηφιακές υπογραφές, οι οποίες μπορούν να μετατραπούν από οποιοδήποτε κατοχό τους, όχι κατ' ανάγκη τον ίδιο τον υπογραφοντά τους, σε υπογραφές καθορισμένου επαληθευτή καθορίζοντας ένα επαληθευτή.

Υπογραφές Πολλών Καθορισμένων Επαληθευτών

Μία άλλη ενδιαφέρουσα εκδοχή των DVS είναι οι υπογραφές πολλών καθορισμένων επαληθευτών [49], οι οποίες επιτρέπουν τον καθορισμό ενός συνόλου επαληθευτών. Για την παραγωγή της προσομοίωσης χρειάζεται η συνεργασία των επαληθευτών κάνοντας χρήση ασφαλούς υπολογισμού πολλών μερών (secure multi-party computation - SMPC)

Για ευκολότερη ανάγνωση προτείνεται η [52], που παραθέτει ένα ενοποιημένο μοντέλο για όλες τις προηγούμενες εκδοχές που παρατέθηκαν.

Κεφάλαιο 5

Υπογραφές Δακτυλίου

Σε αυτό το κεφάλαιο θα δούμε το δεύτερο κύριο συστατικό των UDVLRS, τις υπογραφές δακτυλίου. Οι υπογραφές δακτυλίου επιτρέπουν σε έναν υπογράφοντα να κρύψει την ταυτότητα του μέσα σε ένα σύνολο ανωνυμίας ή όπως θα το αποκαλούμε πιο συχνά έναν δακτύλιο. Ως αποτέλεσμα ένας παραλήπτης μίας υπογραφής δακτυλίου μπορεί να είναι σίγουρος πως ο υπογράφοντας είναι ένα από τα μέλη του δακτυλίου, χωρίς όμως να μπορεί να ξέρει με σιγουριά ποιος ακριβώς είναι.

Πριν όμως μιλήσουμε για τις υπογραφές δακτυλίου είναι αναγκαίο να μιλήσουμε για ένα άλλο σχετικό είδος υπογραφών, τις ομαδικές υπογραφές. Οι Ομαδικές Υπογραφές (Group Signatures) προτάθηκαν από τους Chaum και van Heyst το 1991 [29]. Σε ένα σχήμα ομαδικής υπογραφής δικαίωμα υπογραφής έχουν μόνο τα μέλη της ομάδας, ενώ ο πιθανός παραλήπτης μπορεί να είναι σίγουρος ότι ο υπογράφων αποτελεί μέλος της ομάδας. Η ομάδα έχει αυστηρή δομή, και επιπλέον έχει και έναν αρχηγό ο οποίος έχει την δυνατότητα να αποκαλύψη την ταυτότητα του συγγραφέα μιας υπογραφής εάν αυτό κριθεί αναγκαίο.

Μία χαλάρωση της παραπάνω ιδέας αποτελούν οι Υπογραφές Δακτυλίου (Ring Signatures) οι οποίες εισήχθησαν από τους Rivset, Shamir και Tauman το 2001 [69]. Στις υπογραφές δακτυλίου, όπως έχουμε ήδη πει, ο υπογράφων κρύβει την ταυτότητα του μέσα στο δακτύλιο, και για οποιονδήποτε άλλο η υπογραφή που παράγεται αποτελεί απόδειξη του ότι προέρχεται από κάποιον στο δακτύλιο, χωρίς όμως να είναι γνωστό από ποιον. Σε αντίθεση όμως με τις ομαδικές υπογραφές δεν υπάρχει αυστηρή δομή στο δακτύλιο. Όταν κάποιος επιλέγει να υπογράψει τα υπόλοιπα μέλη του δακτυλίου δε γνώριζουν ότι συμμετάσχουν στη διαδικασία, ενώ δεν υπάρχει κάποια ηγετική οντότητα η οποία φέρει την δυνατότητα άρσης της ανωνυμίας του υπογράφοντα.

Η πιο σημαντική για εμάς παραλλαγή των υπογραφών δακτυλίου είναι οι Συνδέσιμες Υπογραφές Δακτυλίου (Linkable Ring Signatures) [57] που προ-

τάθηκαν από τους Liu, Wei και Wong το 2004. Σε αυτή την παραλλαγή οι υπογραφές που παράγονται από έναν υπογράφοντα συνδέονται μεταξύ τους με τη χρήση ενός ψευδώνυμου (pid) ή αλλίως ετικέτας σύνδεσης ή απλά ετικέτας (linking tag, tag) t. Έτσι ένας εξωτερικός παρατηρητής μπορεί να ξέρει ότι δύο υπογραφές προέρχονται από τον ίδιο υπογράφοντα, όμως η ταυτότητα του υπογράφοντα παραμένει κρυμμένη. Οι συνδέσιμες υπογραφές δακτυλίου εμφανίζουν μεγάλη χρησιμότητα σε συστήματα ηλεκτρονικών ψηφοφοριών. Θα δώσουμε επίσης μεγάλη σημασία και σε μία τροποποιημένη έκδοση των LRS, αυτές με άνευ όρων ανωνυμία [56].

5.1 Ομαδικές Υπογραφές

Σε αυτή την ενότητα θα κάνουμε μία επιφανειακή αναφορά στις ομαδικές υπογραφές. Το κίνητρο πίσω από τις ομαδικές υπογραφές μας δίνεται στην πρωταρχική επί του θέματος εργασία των Chaum και van Heyst [29]. Ας σκεφτούμαι πως βρισκόμαστε σε μια εταιρεία με πολλά διαφορετικά τμήματα. Κάθε τμήμα διαθέται το δικό του εκτυπωτή και μόνο τα μέλη του εκάστοτε τμήματος έχουν το δικαίωμα να κάνουν χρήση αυτού. Για λόγους ιδιωτικότητας η εταιρεία δεν προβάλει σε όλους ποιος κάνει χρήση του εκτυπωτή, όμως σε περίπτωση κατάχρησης ο υπεύθηνος του τμήματος θα πρέπει να μπορεί να άρει την ανωνυμία του χρήστη που παραφέρεται.

Για να επιτευχθεί αυτός ο σκοπός είναι αναγκαίο ένα είδος υπογραφών το οποίο θα ικανοποιεί τις ακόλουθες ιδιότητες:

1. Δικαίωμα σύνταξης υπογραφών φέρουν μόνο τα μέλη της ομάδας.

2. Η υπογραφή πρέπει να προστατεύει την ταυτότητα του υπογράφοντα, ένας παραλήπτης θα μπορεί να είναι βέβαιως πως η υπογραφή που έλαβε προέρχεται από ένα μέλος της ομάδας όχι όμως ποιο ακριβώς.

3. Σε περίπτωση που κρίνεται αναγκαίο ο αρχηγός της ομάδας θα μπορεί να άρει την ανωνυμία της υπογραφής, δημοσιεύοντας έτσι την ταυτότητα του υπογράφοντα.

5.1.1 Μοντέλο Ομαδικών Υπογραφών

Ένας σχήμα ομαδικών υπογραφών είναι μία τετράδα αλγορίθμων (KGen, Vrfy, Sign, Open) έτσι ώστε:

- **Δημιουργία Κλειδιών** -$\mathsf{KGen}(1^\lambda, n)$:

  Δεδομένης παραμέτρου ασφάλειας λ και μέγεθος ομάδας n ο αλγόριθμος επιστρέφει το κλειδί της ομάδας gpk και τα ιδιωτικά κλειδιά του αρχηγού gsk_M και των μελών $\{\mathsf{gsk}_i\}_{i=1}^n$ αντίστοιχα.

  $(\mathsf{gpk}, \mathsf{gsk}_M, \{\mathsf{gsk}_i\}_{i=1}^n) \leftarrow \mathsf{KGen}(1^\lambda, n)$.

- **Δημιουργία Υπογραφής** -$\mathsf{Sign}(\mathsf{gpk}, \mathsf{gsk}_\pi, \mathtt{m})$:

  Με είσοδο το κλειδί της ομάδας, το ιδιωτικό κλειδί του υπογράφοντα gsk_π με $\pi \in [n]$ και το μήνυμα της αρεσκείας ο αλγόριθμος δημιουργίας υπογραφής επιστρέφει μία έγκυρη υπογραφή.

  $\sigma \leftarrow \mathsf{Sign}(\mathsf{gpk}, \mathsf{gsk}_\pi, \mathtt{m})$.

- **Επιβεβαίωση** -$\mathsf{Vrfy}(\sigma, \mathsf{gpk}, \mathtt{m})$:

  Με είσοδο μία υπογραφή σ, το δημόσιο κλειδί της ομάδας gpk και το μήνυμα $\mathtt{m}$ ο αλγόριθμος επιστρέφει αν η υπογραφή είναι έγκυρη ή όχι.

  $\{0, 1\} \leftarrow \mathsf{Vrfy}(\sigma, \mathsf{gpk}, \mathtt{m})$.

- **Άνοιγμα** -$\mathsf{Open}(\sigma, \mathsf{gsk}_M, \mathtt{m})$:

  Με είσδο μία υπογραφή σ, το μήνυμα που αντιστοιχεί στην υπογραφή $\mathtt{m}$ και το ιδιωτικό κλειδί gsk_M του αρχηγού της ομάδας επιστρέφει την ταυτότητα π του υπογράφοντα.

  $\pi \leftarrow \mathsf{Open}(\sigma, \mathsf{gsk}_M, \mathtt{m})$.

Εδώ αξίζει να σημειώσουμε πως η συγκεκριμένη μορφή ομάδας που περιγράφουμε είναι στατική, δεν έχουμε προσθήκη ή αποχώρηση μελών. Μέσα στη βιβλιογραφία παρουσιάζονται μοντέλα και κατασκευές που το λαμβάνουν αυτό υπ' όψη. Για παράδειγμα [31, 4] επιτρέπουν προσθήκη μελών, [5] επιτρέπεται η αφαίρεση, ενώ υπάρχουν και μοντέλα για πλήρως δυναμικές ομάδες με προσθήκη και αφαίρεση μελών [75]. Για να επιτευχθούν αυτές οι νέες λειτουργηκότητες τα μοντέλα επαυξάνονται με κατάλληλους αλγορίθμους.

Μία κατασκευή ενός σχήματος ομαδικής υπογραφής για στατικές ομάδες μας δίνεται από τους Bellare, Miccianzio και Warinschi στην εργασία [14]. Οι λεπτομέριες της κατασκευής δε μας απασχολούν ιδιαιτέρως μιας και το ενδιαφέρον μας εστιάζεται στις υπογραφές δακτυλίου. Ως εκ τούτο αφήνουμε στον αναγνώστη τις προηγούμενες παραπομές για ενδεχόμενη προσωπική ενασχόληση.

5.2 Υπογραφές Δακτυλίου

Το 2001 οι Rivset, Shamir και Tauman πρότειναν τις υπογραφές δακτυλίου (Ring Signatures - RS) [69]. Οι RS βασίζονται στις ομαδικές υπογραφές, όμως

το μοντέλο τους φέρει μερικές σημαντικές διαφορές. Όπως και στις ομαδικές υπογραφές έτσι και στις RS ο υπογράφοντας κρύβει την ταυτοτητά του μέσα σε μία ομάδα ατόμων. Συγκεκρίμενα όταν κάποιος επιθυμεί να κατασκευάσει μια RS αρκεί να επιλέξει τα δημόσια κλειδιά τα οποία θα αποτελέσουν το δακτύλιο και να εκτελέσει τον αλγόριθμο δημιουργίας υπογραφής. Το σημαντικό χαρακτηριστικό των RS είναι η ανωνυμία που προσφέρουν. Κανένας από τους ιδιοκτήτες των δημοσιών κλειδιών του δακτυλίου δεν συμμετάσχει ενεργά στην δημιουργία της υπογραφής, ούτε είναι αναγκαίο να έχει γνώση πως το κλειδί του συμμετέχει σε έναν δακτύλιο. Επιπλέον δεν υπάρχει κάποια ηγετική φιγούρα η οποία έχει την ικανότητα να άρει την ανωνυμία μίας υπογραφής. Τέλος σημειώνουμε εδώ πως η εκ φύσεως κάθε οντότητα που συμμετέχει στο δακτύλιο έχει το δικό της ζεύγος δημοσίου-ιδιωτικού κλειδιού, ενώ αν δούμε ένα σχήμα ομαδικών υπογραφών κάθε χρήστης έχει ένα ιδιωτικό κλειδί η ομάδα ολόκληρη έχει ένα κοινό δημόσιο κλειδί.

Οι Rivest, Shamir και Tauman πρότειναν τις RS ως ένα τρόπο για να γίνεται ασφαλής και ανώνυμη διαρροή μυστικών, κάτι που γίνεται άμεσα αντιλυπτό και από τον τίτλο της εργασίας τους (*How to leak a secret*[69]). Η κατασκευή που παραθέτουν βασίζεται στο πρόβλημα RSA και σε έναν ασφαλές συμμετρικό κρυπτοσύστημα, όπως για παράδειγμα το AES. Παρ' όλα αυτά το σχήμα που θα επιλέξουμε να αναλύσουμε είναι αυτό των Abe, Ohkubo και Suzuki [1], μιας και αποτελεί τη βάση για τα σχήματα υπογραφών που οδηγούν στις UDVLRS.

5.2.1 Το μοντέλο RS

Ξεκινάμε την ανάλυση των RS παραθέτοντας το μοντέλο των υπογραφών δακτυλίου.

Ένα σχήμα υπογραφών δακτυλίου αποτελείται από μία τριάδα αλγορίθων $(\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$:

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

  Κατασκευάζει ένα έγκυρο ζεύγος δημόσιου-ιδιωτικού κλειδιού. Όλα τα κλειδιά του συστήματος αποτελούν έξοδο αυτού του αλγορίθμου, κάθε χρήστης πρέπει να έχει το δικό του ζεύγος κλειδιών για να μπορεί να υπογράφει και να συμμετάσχει σε δακτύλιους.
  Καλούμε $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$.

- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$:

  Με είσοδο το ιδιωτικό κλειδί sk_π του υπογράφοντα, ένα σύνολο δημοσιών κλειδιών L όπου $\mathsf{pk}_\pi \in L$ και π είναι ο δείκτης του κλειδιού του υπογράφοντα στο δακτύλιο, και ένα μήνυμα $\mathtt{m}$ επιστρέφει μία έγκυρη υπογραφή

σ.
Καλούμε $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_\pi, L, \mathtt{m})$.

- **Επιβεβαίωση Υπογραφής** -$\mathsf{Vrfy}(\sigma, L, \mathtt{m})$:

  Με είσοδο μία υπογραφή σ, τον δακτύλιο κλειδιών L, και το μήνυμα $\mathtt{m}$ επιστρέφει 1 αν η υπογραφή είναι έγκυρη και προέρχεται από υπογράφοντα με κλειδί που ανήκει στο σύνολο L.
  Καλούμε $\{0,1\} \leftarrow \mathsf{Vrfy}(\sigma, L, \mathtt{m})$.

Σημείωση: Σε ορισμένες εργασίες στη βιβλιογραφία θεωρούμε την ύπαρξη ενός σύμπαντος από όλα τα πιθανά δημόσια κλειδιά $\mathcal{U}$, και ότι για κάθε δακτύλιο L ισχύει ότι $L \subseteq \mathcal{U}$.

5.2.2 Υπογραφές 1 από n κλειδιά

Όπως είχαμε αναφέρει στο κεφάλαιο 3 ένας συχνός τρόπος κατασκευής σχημάτων υπογραφής είναι η χρήση ενός Σ-Πρωτοκόλλου. Η ιδέα μιας υπογραφής δακτυλίου είναι ότι ο υπογράφοντας δείχνει ότι ανήκει σε ένα σύνολο ατόμων, χωρίς όμως να μπορεί να αποκαλυφθεί η ταυτοτητά του. Έτσι λοιπόν μπορούμε χρησιμοποιώντας μια απόδειξη μηδενικής γνώσης ενός στοιχείου από ένα σύνολο ως βάση να κατασκεύασουμε μία υπογραφή δακτυλίου. Αυτή ακριβώς είναι η ιδέα πίσω από τις υπογραφές για 1 από n κλειδιά των Abe, Ohkubo και Suzuki [1], βάση των οποίων είναι η ιδέα των αποδείξεων μηδενικής μερικής γνώσης [32]. Στην εργασία τους οι Abe, Ohkubo και Suzuki δίνουν κατασκευή για δύο τύπους κλειδιών, τύπου RSA και τύπου DLOG. Εμείς θα εστιάσουμε στην εκδοχή για κλειδιά τύπου DLOG.

Πριν δώσουμε την κατασκευή θα παραθέσουμε τις υποθέσεις που γίνονται για να κατασκευαστεί το σχήμα. Για αρχή θεωρούμε πως όλα τα κλειδιά είναι στοιχεία της ίδιας ομάδα $\mathbb{G}$, η οποία είναι τάξης πρώτου q με γεννήτορα g και στην οποία ισχύει η υπόθεση του διακριτού λογαρίθμου (DLOG). Επιπλέον θεωρούμε μία κρυπτογραφική συνάρτηση σύνοψης $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{Z}_q$.

Οι αλγόριθμοι του σχήματος είναι οι ακόλουθοι:

- **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. $u \leftarrow \$\mathbb{Z}_q$

2. $c_{\pi+1} \leftarrow \mathcal{H}(L, \mathtt{m}, g^u)$
3. Για $i \in \{\pi+1, \ldots, n_L, 1, \ldots, \pi-1\}$:

   $s_i \leftarrow \$\mathbb{Z}_q$
   $c_{i+1} \leftarrow \mathcal{H}(L, \mathtt{m}, g^{s_i} y_i^{c_i})$
4. $s_\pi \leftarrow u - c_\pi x_\pi$
5. **Επέστρεψε:** $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L})$

- :

  Για $i \in [n_L]$:

  1. $z_i' \leftarrow g^{s_i} y_i^{c_i}$
  2. $c_{i+1} \leftarrow \mathcal{H}(L, \mathtt{m}, z_i')$
  3. **Επέστρεψε:** $c_1 = c_{n_L+1}$

Παρατηρούμε ότι αν το μέγεθος του δακτυλίου L ισούται με ένα, δηλαδή $n_L = 1$, η υπογραφή που προκύπτει είναι η το σχήμα υπογραφής Schnorr [72].

5.2.3 Ιδιότητες Ασφάλειας Υπογραφών RS

Όπως και σε όλα τα σχήματα υπογραφής κύρια απαίτηση είναι η *μη-πλαστογραφησιμότητα*. Στις υπογαρφές δακτυλίου αυτό που εννοούμε είναι να μη μπορεί κανένας να κατασκευάσει μία έγκυρη υπογραφή δίχως γνώση του ιδιωτικού κλειδιού ενός εκ των κλειδιών που απαρτίζουν τον δακτυλίο.

Η κύρια ιδιότητα που προσφέρουν οι υπογραφές δακτυλίου είναι η ανωνυμία. Δεν θα πρέπει να είναι εφικτό για έναν αντίπαλο να προσδιορίσει την ταυτότητα του υπογράφοντα μιας υπογραφής. Βέβαια λόγω του ότι η προκύπτουσα υπογραφή προέρχεται από ένα συγκεκριμένο σύνολο πιθανών υπογραφόντων ο αντίπαλος πάντα μπορεί να επιλέξει τυχαία ένα μέλος του δακτυλίου, και άρα να έχει πιθανότητα να βρει τον πραγματικό υπογράφοντα ίση με $\frac{1}{n_L}$. Για το λόγο αυτό από την αρχή κιόλας χρησιμοποιείται συχνά ο όρος *ασάφεια υπογράφοντος(signer ambiguity)* [69], που περιγράφει πιο εύστοχα το γεγονός ότι η ανωνυμία έχει να κάνει με τα υπόλοιπα μέλη του δακτυλίου. Η ανωνυμία διακρίνεται σε επίπεδα ανάλογα με τις δυνατότητες του αντιπάλου. Έτσι αν υποθέσουμε πως έχουμε έναν PPT αντίπαλο τότε η ανωνυμία είναι υπολογιστική και η πιθανότητα επιτυχίας του αντιπάλου στο να βρει την ταυτοτητά του υπογράφοντα μιας δεδομένης υπογραφής είναι αμελητέα κοντά στην τυχαία μαντεψιά. Αν υποθέσουμε πως ο αντίπαλος είναι μη-φραγμένος και έχει πιθανότητα ακριβώς ίση με $\frac{1}{n_L}$ τότε μιλάμε για τέλεια ανωνυμία.

Μη-Πλαστογραφησιμότητα

Σε αυτό το σημείο θα ορίσουμε αυστηρά τη μη-πλαστογραφησιμότητα με τη χρήση ενός πειράματος ασφαλείας. Σε αυτό το πείραμα ο σκοπός του αντιπάλου $\mathcal{A}$ είναι να μπορέσει να παράξει μία έγκυρη υπογραφή για κάποιο δακτύλιο L για τον οποίο δε ξέρει κανένα από τα ιδιωτικά κλειδιά. Για να μοντελοποιήσουμε τη δυνατότητα του $\mathcal{A}$ να έχει πρόσβαση σε προηγούμενες υπογραφές του δίνουμε το δικαίωμα χρήσης του μαντείου υπογραφών $\mathcal{SO}$. Σημειώνουμε εδώ πως ο αντίπαλος δεν χρειάζεται να περισοστεί στη χρήση του, έτσι μπορεί να ρωτάει για υπογραφές από οποιοδήποτε δακτύλιο L' (διαφορετικό αν επιθυμεί και από τον αρχικό L), για οποιοδήποτε δημόσιο κλειδί και για οποιοδήποτε μήνυμα της επιλογής του. Επιπλέον ο αντίπαλος μπορεί να προσθέτει νέα κλειδιά στο σύστημα και άρα έχει πρόσβαση στο μαντείο εγγραφής $\mathcal{JO}$, ενώ μπορεί ακόμα να μαθαίνει το ιδιωτικό κλειδί οποιουδήποτε δημόσιου κλειδιού με χρήση του μαντείου διαφθοράς $\mathcal{CO}$. Με αυτό τον τρόπο μοντελοποιούμε έναν ισχυρό προσαρμοστικό αντίπαλο (strong adaptive adversary) που έχει την δυνατότητα να γνωρίζει πολλά από τα ιδιωτικά κλειδιά. Ο λόγος για αυτές τις δυνατότητες είναι ο εξής, ένα άτομο που επιλέγει κλειδιά για να κατασκευάσει ένα δακτυλίο με σκοπό να υπογράφει δε μπορεί να είναι σίγουρος εάν τα κλείδια που χρησιμοποιεί είναι ασφαλή ή αν έχει υπάρξει κάποια διαρροή των ιδιωιτκών κλειδιών. Προφανώς αν η υπογραφή που επιστρέψει ο αντίπαλος είναι έξοδος του $\mathcal{SO}$ τότε δεν θα θεωρηθεί επιτυχής. Ανεπιτυχής θα θεωρηθεί εάν επίσης ο δακτύλιος για τον οποίο παράχθηκε η υπογραφή περιείχε έστω και ένα διεφθαρμένο κλειδί. Στα σχήματα υπογραφών που ακολουθούν σε αυτή τη ΔΕ με D_t θα συμβολίζεται το σύνολο των δεικτών των διεφθαρμένων κλειδιών του δακτυλίου L. Η ισχυρή αυτή έννοια μη-πλαστογραφισημότητας δώθηκε αυστηρά από τους Bender, Katz και Morselli [17], και χρησιμοποείται τόσο στις LRS όσο και στις DVLRS.

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^n$
$(\sigma, L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(1^\lambda, \mathcal{U})$
Επέστρεψε: $\mathsf{Vrfy}(\sigma, L, \mathtt{m})$ **ΚΑΙ** σ δεν είναι είσοδος των $\mathcal{SO}$ **ΚΑΙ**
$\forall i \in D_t : pk_i \notin D_t$

Ορισμός 5.1. *Μη-Πλαστογραφησιμότητα*

Ένα RS σχήμα Π υπογραφών είναι μη-πλαστογραφήσιμο εάν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

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

Ανωνυμία

Περνάμε τώρα στη μοντελοποίηση του αντιπάλου $\mathcal{A}$ για τον ορισμό της ανωνυμίας, τόσο της υπολογιστικής όσο και της τέλειας και άνευ όρων.

Στον αντίπαλο της υπολογιστικής ανωνυμίας δίνεται πρόσβαση στα ίδια μαντεία με αυτά που είδαμε και στη μη-πλαστογραφησιμότητα. Έτσι λοιπόν ο $\mathcal{A}$ μπορεί να ρωτάει τα μαντεία $\mathcal{JO}$, διαφθοράς $\mathcal{CO}$ και υπογραφής $\mathcal{SO}$, με οποιαδήποτε προσαρμοστική στρατηγική και για οποιαδήποτε είσοδο της επιλογής του. Χωρίζουμε τώρα το πείραμα ασφάλειας σε δύο φάσεις. Στη πρώτη φάση ο $\mathcal{A}$ καλεί τα μαντεία με όποιο τρόπο θέλει, επιλέγει επιπλέον ένα δακτύλιο και ένα μήνυμα της αρεσκείας του πάνω στα οποία θα κατασκευαστεί μία υπογραφή-πρόκληση. Τώρα στη δεύτερη φάση ο αντίπαλος καλείται, διατηρώντας πρόσβαση στα προηγούμενα μαντεία, να μαντέψει ποιος είναι ο υπογράφοντας της υπογραφής-πρόκλησης. Βλέπουμε πως η ελάχιστη πιθανότητα επιτυχίας για έναν αντίπαλο $\mathcal{A}$ στο συγκεκριμένο πείραμα είναι ίση με την τυχαία επιλογή ενός μέλους του δακτυλίου. Επιπλέον είναι επιθυμητό ο αντίπαλος να μη μπορεί να μάθει τη ταυτότητα του υπογράφοντα, ακόμα και αν γνωρίζει όλα τα ιδιωτικά κλειδιά του δακτυλίου. Αυτό είναι εφικτό μιας και μια υπογραφή δακτυλίου δε περιέχει κανένα κομμάτι που να διαρρέει την ταυτότητα του υπογράφοντα.

Παιχνίδι 5.2: Πείραμα Υπολογιστικής Ανωνυμίας $\mathsf{Exp}^{AnonRS}_{\mathcal{A},\Pi,n}(\lambda)$

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(\mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow \$[n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{sk}_\pi)$
$\xi \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(L, \mathtt{m}, \sigma, \textbf{εικασία})$
Επέστρεψε: $\xi = \pi$

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

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

Για τον αντίπαλο της τέλειας άνευ όρων ανωνυμίας πρέπει να κάνουμε ορισμένες αλλαγές. Κατ' αρχάς η πρώτη και σημαντική αλλαγή είναι το γεγονός ότι ο αντίπαλος είναι υπολογιστικά μη-φραγμένος, οπότε είναι ικανός να υπολογίσει το ιδιωτικό κλειδί που αντιστοιχεί σε οποιδήποτε δημόσιο κλειδί βλέπει. Για αυτό το λόγο δεν δίνεται και πρόσβαση στο μαντείο διαφθοράς $\mathcal{CO}$. Αφήνεται πρόσβαση στο μαντείο υπογραφής $\mathcal{SO}$, για να μοντελοποιήσουμε το γεγονός ότι ο $\mathcal{A}$ έχει πρόσβση σε υπογραφές με γνωστό υποαγράφοντα.

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(\mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow \$[n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{sk}_\pi)$
$\xi \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(L, \mathtt{m}, \sigma, \textbf{εικασία})$
Επέστρεψε: $\xi = \pi$

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

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

Ασφάλεια Σχήματος 1 από n με κλειδιά τύπου DLOG

Για το σχήμα υπογραφών των Abe, Ohkubo και Suzuki με κλειδιά τύπου DLOG αποδεικνύονται τα δύο παρακάτω θεωρήματα για την ασφάλεια του:

Θεώρημα 5.1. *(Μη-Πλαστογραφησιμότητα)*
Το σχήμα 1 από n με κλειδιά τύπου DLOG *είναι μη-πλαστογραφήσιμο στο μοντέλο $\mathcal{RO}$ αν ισχύει η υπόθεση του* DLOG *στην $\mathbb{G}$.*

Θεώρημα 5.2. *(Ανωνυμία)*
Το σχήμα 1 από n με κλειδιά τύπου DLOG *είναι τέλεια ανώνυμο.*

5.3 Συνδέσιμες Υπογραφές Δακτυλίου

Μία εφαρμογή για την οποία φαίνεται να ταιριάζουν οι υπογραφές δακτυλίου είναι οι ηλεκτρονικές ψηφοφορίες. Αν το σκεφτούμαι ο δακτύλιος θα αποτελούνταν από τους ψηφοφόρους και κάθε ψήφος θα ήταν μία υπογραφή από το δακτύλιο. Με αυτό τον τρόπο διασφαλίζεται το ότι η ψήφος προέρχεται από μόνο έγκυρους ψηφοφόρους, ενώ η ανωνυμία και εγκυρότητα της ψήφους μπορεί να διασφαλιστεί από τις ιδιότητες ασφάλειας των RS. Δημιουργείτε όμως ένα μεγάλο πρόβλημα. Επειδή οι υπογραφές μοιάζουν να προέρχονται από οποιδήποτε μέλος του δακτυλίου είναι αδύνατο να μπορούμε να εντωπύσουμε άτομα τα οποία ψηφίζουν πολλές φορές. Θα χρειαζόταν λοιπόν με κάποιο τρόπο να ξέραμε ποιες υπογραφές προέρχονται από το ίδιο άτομο, χωρίς όμως να μπορούμε να μάθουμε ποιο είναι αυτό το άτομο.

Τη λύση σε αυτό το πρόβλημα την έφεραν οι Liu, Wei και Wong, με τις συνδέσιμες υπογραφές δακτυλίου τις οποίες εισήγαγαν το 2004 [57]. Η ιδέα τους ήταν η ακόλουθη: Κάθε χρήστης εκτός του δημόσιου κλειδιού του θα έχει και ένα ψευδώνυμο(pseudoidentity) ή αλλιώς ετικέτα σύνδεσης ή πιο απλά ετικέτα (linking tag, tag), το οποίο θα χρησιμοποιείται αναγκαστικά κατά την διάρκεια κατασκευής της υπογραφής ώστε το αποτέλεσμα να είναι έγκυρο. Έτσι λοιπόν είναι εύκολο για οποιονδήποτε να μπορεί να ξεχωρίσει αν δύο υπογραφές προέρχονται από τον ίδιο υπογράφοντα ή όχι, χωρίς όμως να μπορεί να καταλάβει κάποιος ποιος ακριβώς είναι αυτός που υπογράφει. Στις κατασκευές που θα δούμε το ψευδώνυμο δεν είναι τίποτα άλλο παρά μία δύσκολα αντιστρέψιμη συνάρτηση του ιδιωτικού κλειδιού του υπογράφοντα, έτσι διασφαλίζεται ταυτόχρονα η ταυτοποίηση και η ανωνυμία.

Οι υπογραφές δακτυλίου επαυξημένες με αυτή την ιδιότητα της συνδεσιμότητας λύνουν το πρόβλημα των πολλαπλών ψήφων, αφού τώρα είναι εφικτό να εντοπιστούν τα άτομα που ψήφισαν πολλές φορές και έτσι οι διοργανωτές της ψηφοφορίας μπορούν να ενεργήσουν κατάλληλα με βάση το πρωτόκολλο που ακολουθείτε.

Οι LRS βρήκαν σχετικά πρόσφατα χρήση στο κρυπτονόμισμα Monero [61], το οποίο έχει γίνει εν μέρη διαβόητο για την ανωνυμία που προσφέρει. Συγκεκριμένα λόγω της ανωνυμίας τόσο σε επίπεδο αποστολέα και παραλήπτη όσο και σε επίπεδο ποσού και είδους συναλλαγής πολλά άτομα που θέλουν να "ξεπλύνουν" κρυπτονομίσματα που έχουν αποκτηθεί μέσω παράνομων ενεργειών χρησιμοποιούν το Monero για να τα εισάγουν στη νόμιμη κυκλοφορία. Αυτό βέβαια δεν αφαιρεί τίποτα από τις LRS, τουναντίον αποτελεί μάλλον πειστήριο της ασφάλειας που προσφέρουν ως υπογραφές.

5.3.1 Το μοντέλο LRS

Θα δούμε τώρα τους αλγορίθμους από τους οποίους αποτελείται ένα σχήμα συνδέσιμων υπογραφών δακτυλίου (LRS).

Επειδή η βάση των LRS είναι οι RS θα έχουμε και πάλι τους αλγόριθμους δημιουργίας κλειδιών, δημιουργίας υπογραφής και επαλήθευσης (όπως άλλωστε και κάθε σχήμα υπογραφών). Λόγω της προσθήκης της νέας ιδιότητας της συνδεσιμότητας έχουμε και την προσθήκη ενός νέου αλγόριθμου τον αλγόριθμο Σύνδεση, που ελέγχει αν δύο υπογραφές είναι συνδεδδμλενες μεταξύ τους. Επιπλέον μπορεί για λόγους ευκολίας να προστεθεί ένας ακόμα αλγόριθμος, ονόματι Εξαγωγή, ο οποίος εξάγει το ψευδώνυμο μίας υπογραφής. Ο αλγόριθμος εξαγωγής δεν δίνεται συνήθως στα περισσότερα σχήματα που συναντιούνται στην βιβλιογραφία, η προσθήκη του όμως από τους [13] κάνει λίγο πιο οργανωμένη, καθαρή και πλήρη την εξήγηση ορισμένων ιδιοτήτων.

Αυστηρά ένα σχήμα συνδέσιμων υπογραφών δακτυλίου (LRS) είναι μια πεντάδα αλγορίθμων (KGen, Sign, Vrfy, Extract, Link):

- **Δημιουργία Κλειδιών -** KGen():

  Κάθε χρήστης επικαλείται τον αλγόριθμο KGen ώστε να λάβει το ζεύγος κλειδιών του (sk, pk). Τα κλειδιά δημιουργούνται κατά βούληση από τον εκάστοτε χρήστη.

  Καλούμε (sk, pk) $\leftarrow$ KGen().

- **Δημιουργία Υπογραφής -** Sign$(L, \mathtt{m}, \mathsf{sk}_\pi)$:

  Για να υπογράψει ένα μέλος του δακτυλίου L ένα μήνυμα $\mathtt{m}$ επικαλείται τον αλγόριθμο Sign και χρησιμοποιεί για είσοδο τον δακτυλίο L, το μήνυμα $\mathtt{m}$ και το ιδιωτικό του κλειδί sk_π, όπου π είναι ο δείκτης του συγκεκριμένου υπογράφοντα στο δακτυλίο L.

  Καλούμε $\sigma \leftarrow$ Sign$(L, \mathtt{m}, \mathsf{sk}_\pi)$.

- **Εξαγωγή -** Extract(σ):

  Ο αλγόριθμος Extract με είσοδο μία υπογραφή σ εξάγει το pid της υπογραφής.

  Καλούμε pid $\leftarrow$ Extract(σ).

- **Επαλήθευση -** Vrfy$(\sigma, L, \mathtt{m})$:

  Ο αλγόριθμος επαλήθευσης επιστρέφει 1 αν η υπογραφή σ είναι έγκυρη, αλλίως επιστρέφει 0.

  Καλούμε $\{0,1\} \leftarrow$ Vrfy$(\sigma, L, \mathtt{m})$.

- **Σύνδεση -** Link(σ, L, σ', L):

  Με την κλήση του αλγορίθμου σύνδεσης ελέγχεται εάν δύο υπογραφές σ, σ' από τον ίδιο δακτυλίο L είναι συνδεδεμένες ή όχι.Ο αλγόριθμος επιστρέφει 1 εάν είναι συνδεδεμένες, αλλιώς επιστρέφει 0.

  Καλούμε $\{0,1\} \leftarrow$ Link(σ, L, σ', L).

Σημείωση: Θεωρούμε πως η σύνδεση στο μοντέλο γίνεται μεταξύ υπογραφών που ανήκουν στον ίδιο δακτύλιο. Αυτό δεν είναι απαραίτητα αναγκαστικό, για παράδειγμα [56] η σύνδεση γίνεται με βάση κάποιο κοινό event ev, ενώ θα μπορούσε να γίνεται με τέτοιο τρόπο ώστε όλες οι υπογραφές ενός υπογραφέα να συνδέονται μεταξύ τους σε όλους τους δακτυλίους που λαμβάνει μέρος. Όλα έχουν να κάνουν με το πλαίσιο στο οποίο αξιοποιείται το σχήμα υπογραφής. Στην πρωταρχική τους δουλειά όπως θα δούμε οι Liu, Wei και Wong [57] η σύνδεση υπογραφής περιορίζεται στον εκάστοτε δακτύλιο υπογραφής.

5.3.2 LSAG

Όπως έχουμε ήδη αναφέρει το πρώτο σχήμα συνδέσιμων υπογραφών δακτυλίου είναι αυτό των Liu, Wei και Wong [57] και φέρει το όνομα LSAG. Το όνομα σημαίνει Linkable Spontaneous Anonymous Group Signatures, δηλαδή Συνδέσιμε Αυθόρμητες Ομαδικές Υπογραφές, και περιγράφει ακριβώς το την φύση τους. Πιο συγκεκριμένα οι υπογραφές αυτές σε αντίθεση με τις ομαδικές δεν χρείαζονται την αυστηρή δομή και οργάνωση που διέπει τις τελευταίες, ενώ διασφαλίζουν ανωνυμία και συνδεσιμότητα.

Η βάση του σχήματος είναι αυτή των 1 από n κλειδιά DLOG των Abe, Ohkubo και Suzuki [1] που περιγράψαμε στην προηγούμενη ενότητα. Η κύρια προσθήκη είναι αυτή των ψευδώνυμων pid για να επιτευχθεί η συνδεσιμότητα. Πιο συγκεκριμένα στο σχήμα προστίθεται μία ακόμα κρυπτογραφική συνάρτηση σύνοψης η $\mathcal{H}_{\mathbb{G}} : \{0,1\}^* \to \mathbb{G}$, σκοπός της οποίας είναι η παραγωγή γεννητόρων της $\mathbb{G}$. Όταν κάποιος υπογράφει ένα μήνυμα $\mathtt{m}$ πρέπει πρώτα να κατασκευάσει το ψευδώνυμο του $\hat{y}$. Για να το κάνει αυτό υπολογίζει $h = \mathcal{H}_{\mathbb{G}}(L)$, όπου L είναι ο δακτύλιος που υπογράφει και έπειτα θέτει $\hat{y} = h^{\mathsf{sk}_\pi}$ όπου sk_π το ιδιωτικό κλειδί του υπογράφοντα. Παρατηρούμε λοιπόν ότι το ψευδώνυμο είναι κάτι σαν ένα δεύτερο δημόσιο κλειδί που μπορεί να χρησιμοποιεί ο υπογράφοντας, χωρίς όμως να μπορεί να διαρεύσει η ταυτοτητά του λόγω των παραμέτρων του συστήματος, χαίρει δηλαδή της ίδιας ασφάλειας με το pk_π του υπογράφοντα σε ότι έχει να κάνει με τη διαρροή πληροφοριών για το ιδιωτικό κλειδί του. Αξίζει να σημειώσουμε πως για να διασφαλιστεί η υποχρεωτική συνδεσιμότητα του σχήματος ο υπογράφων είναι υποχρεωμένος να δεσμευτεί κατά την κατασκευή της υπογραφής, όπως και με το κλειδί του, μέσω των δεσμεύσεων της συνάρτησης σύνοψης. Όπως και στην 1 από n υπογραφή θέλουμε μία κρυπτογραφική συνάρτηση σύνοψης $\mathcal{H}_q : \{0,1\}^* \to \mathbb{Z}_q$, εργαζόμαστε σε μια ομάδα $\mathbb{G}$ τάξης πρώτου q στην οποία υποθέτουμε πως ισχύει η υπόθεση του DDH και όχι απλά η υπόθεση 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. $h \leftarrow \mathcal{H}_{\mathbb{G}}(L)$
  2. $\hat{y} = h^{\mathsf{sk}_\pi}$
  3. $u \leftarrow \$\mathbb{Z}_q$

4. $c_{\pi+1} \leftarrow \mathcal{H}(L, \mathtt{m}, g^u, h^u)$
5. Για $i \in \{\pi+1, \ldots, n_L, 1, \ldots, \pi-1\}$:

   $s_i \leftarrow \$\mathbb{Z}_q$
   $c_{i+1} \leftarrow \mathcal{H}(L, \mathtt{m}, g^{s_i} y_i^{c_i}, h^{s_i} \hat{y}^{c_i})$
6. $s_\pi \leftarrow u - c_\pi x_\pi$
7. $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \hat{y})$
8. **Επέστρεψε:** σ

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

  Για $i \in [n_L]$:

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

- **Εξαγωγή** - $\mathsf{Extract}(\sigma)$

  1. **Επέστρεψε:** $\hat{y}$.

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

  1. **Επέστρεψε:** $\mathsf{Extract}(\sigma) = \mathsf{Extract}(\sigma')$

5.3.3 Ιδιότητες Ασφάλειας LRS

Σε αυτό το σημείο θα αναλύσουμε το μοντέλο ασφάλειας των LRS εξετάζοντας τις ιδιότητες που διαθέτουν ως σχήμα.

Μη-Πλαστογραφησιμότητα

Η μη-πλαστογραφησιμότητα ως ιδιότητα ορίζεται ακριβώς με τον ίδιο τρόπο όπως με τις RS. Η εισαγωγή του ψευδώνυμου και του αλγορίθμου Σύνδεσης δεν επηρεάζουν την ιδιότητα: Ο αντίπαλος δε πρέπει να είναι σε θέση να παράξει έγκυρη υπογραφή χωρίς να έχει γνώση ενός ιδιωτικού κλειδιού του δακτυλίου.

Ανωνυμία

Η ανωνυμία στις LRS πρέπει να τροποποιηθεί ελαφρώς. Όπως είπαμε στις RS κάθε υπογράφοντας μπορεί να κρυφθεί εντός του δακτυλίου και δεν θα πρέπει να είναι εφικτό για κάποιον να καταλάβει από ποιον προέρχεται η υπογραφή. Ενώ στις LRS δεν έχουμε άμεση διαρροή της ταυτότητας του υπογράφοντα έχουμε σύνδεση των υπογραφών, που αποτελεί μια πληροφορία που δε διέθετε ο αντίπαλος στις RS.

Συνδεσιμότητα

Όπως αναφέραμε και στην εισαγωγή αυτής της ενότητας η καινοτομία των LRS είναι η σύνδεση των υπογραφών που προέρχονται από τον ίδιο υπογράφοντα. Η συνδεσιμότητα ως ιδιότητα απαιτεί ένας υπογράφοντας να μη μπορεί να παράξει δύο υπογραφές που δεν είναι συνδέσιμες μεταξύ τους, δηλαδή υπάρχει η απαίτηση της υποχρεωτικής σύνδεσης υπογραφών που αντιστοιχούν στο ίδιο ιδιωτικό κλειδί. Για τις LRS ισχύει και μια ακόμα πιο αυστηρή απαίτηση. Αν ένας χρήστης έχει γνώση k ιδιωτκών κλειδιών τότε θα πρέπει να είναι αδύνατο να παράξει $k+1$ υπογραφές που να είναι ασύνδετες ανά δύο. Μία ακόμα ιδιότητα που πηγάζει από τη συνδεσιμότητα είναι η μη-δυσφημισιμότητα. Η μη-δυσφημισιμότητα απαιτεί να είναι αδύνατο για έναν αντίπαλο να παράξει υπογραφή που να μπορεί να συνδεθεί με υπογραφές κάποιου μέλους του δακτυλίου. Ο στόχος αυτής της ιδιότητας είναι η προστασία των μελών του δακτυλίου από την ενοχοποίηση από κακόβουλες οντότητες (framing). Αρχίκα [58] η μη-δυσφημισιμότητα θεωρούταν ως υποκατηγορία της συνδεσιμότητας και ότι προκύπτει φυσικά από τις ήδη υπάρχουσες ιδιότητες του σχήματος, συγκεκριμένα όπως θα δούμε είναι απόρροια της μη-πλαστογραφησιμότητας και της συνδεσιμότητας. Έχει εμφανιστεί σε μετέπειτα δημοσιεύεις ως μη-δυσφημισιμότητα [76, 6].

Η ανάγκη για τον διαχωρισμό της συνδεσιμότητας και της μη-δυσφημισιμότητας προέκυψε όταν οι συγγραφείς προσπάθησαν να κατασκευάσουν ένα σχήμα LRS το οποίο διέθετε ανωνυμία άνευ όρων. Αυτό ήταν εφικτό και η εργασία αυτή [56] θα αποτελέσει αντικείμενο μελέτης στη συγκεκριμένη ΔΕ, είναι μάλιστα η βάση πάνω στην οποία μαζί με τις DVLRS δίνουν τις UDVLRS. Για να επιτευχθεί όμως η άνευ όρων ανωνυμία ήταν αναγκαία η αποδυνάμωση της συνδεσιμότητας. Συγκεκρίμενα η συνδεσιμότητα ορίζεται ως εξής: ένας υπογράφοντας που γνωρίζει ένα ιδιωτικό κλειδί δε πρέπει να είναι ικανός να παράξει 2 μη-συνδεδεμένες μεταξύ τους υπογραφές. Σε επόμενη ενότητα θα παρουσιάσουμε και μία πολύ εύκολη επίθεση που μπορεί να διεξαχθεί σε αυτό το σενάριο και θα δούμε τις πρακτικές συνέπειες που προκύπτουν.

Μη-Πλαστογραφησιμότητα

Όπως αναφέραμε και στις προηγούμενες παραγράφους ο ορισμός της μη-πλαστογραφησιμότητας δεν αλλάζει από τις RS. Έτσι λοιπόν έχουμε το ακόλουθο πείραμα και ορισμό:

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}(1^\lambda)\}_{i=1}^{n}$
$(\sigma, L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(1^\lambda, \mathcal{U})$
Επέστρεψε: $\mathsf{Vrfy}(\sigma, L, \mathtt{m})$ **ΚΑΙ** σ δεν είναι είσοδος των $\mathcal{SO}$ **ΚΑΙ**
$\forall i \in D_t : pk_i \notin D_t$

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

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

Ανωνυμία

Όπως αναφέραμε η συνδεσιμότητα και η ανωνυμία δεν είναι ανεξάρτητες μεταξύ τους. Η προσθήκη της νέας ιδιότητας μπορεί να προκαλέσει πρόβλημα στο πως χειριζόμαστε το μοντέλο. Για αρχή αφού ο αντίπαλος μπορεί να ζητήσει υπογραφές από το $\mathcal{SO}$ για οποιδήποτε δημόσιο κλειδί της αρεσκείας του μπορεί να συνδέσει αμέσως ποιο ψευδώνυμο αντιστοιχεί σε ποιο δημόσιο κλειδί. Ως αποτέλεσμα η ανωνυμία του συστήματος καταρρέει τετριμμένα. Η ολική αφαίρεση του μαντείου $\mathcal{SO}$ δεν αποτελεί λύση μιας και τότε μοντελοποιούμε έναν αντίπαλο ο οποίος δεν γνωρίζει σε ποιο δημόσιο κλειδί αντιστοιχεί κανένα ψευδώνυμο κάτι το οποίο είναι υπερβολικό σαν απαίτηση. Για να διατηρηθεί το μαντείο $\mathcal{SO}$ στο πείραμα τροποποιείται ελαφρώς, τώρα αντί να επιστρέφει υπογραφή για κλειδί της αρεσκείας του αντιπάλου επιλέγει στη τύχη ένα κλεδί από το δακτυλίο και κατασκευάζει την υπογραφή για αυτό το τυχαίο κλειδί. Σημειώνουμε εδώ πως γνώση υπογραφών για δακτύλιους διαφορετικούς από αυτόν που κατασκευάζεται η πρόκληση δεν δίνουν κανένα απολύτως πλεονέκτημα σε υπολογιστικά περιορισμένους αντιπάλους, αφού είναι αδύνατο για κάποιον να αντιστρέψει την συνάρτηση του ψευδώνυμου και να υπολογίσει το ιδιωτικό κλειδί.

Και στις LRS, όπως και στις RS, μπορούν να δωθούν δύο εκδοχές ανωνυμίας, η υπολογιστική και η τέλεια (άνευ όρων), ανάλογα αν υποθέτουμε PPT ή μη-φραγμένο αντίπαλο αντίστοιχα. Για την υπολογιστική ανωνυμία πρέπει να σημειώσουμε πως η πιθναότητα επιτυχίας στο πείραμα εξαρτάται από το πλήθος των ιδιωτικών κλειδιών, t, που γνωρίζει ο $\mathcal{A}$. Έχοντας γνώση ο $\mathcal{A}$ ενός ιδιωτικού κλειδιού μπορεί να υπολίσει το ψευδώνυμο και το δημόσιο κλειδί

που αντιστοιχούν σε αυτό και έτσι να ξέρει απευθείας αν μία υπογραφή που του δίνεται αντιστοιχεί σε κάποιο κλειδί που γνωρίζει μέσω του ψευδώνυμου. Για τη τέλεια ανωνυμία τα πράγματα είναι απλούστερα αφού θεωρούμε πως ο αντίπαλος γνωρίζει ή μάλλον καλύτερα μπορεί να υπολογίσει όλα τα κλειδιά.

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(\mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow \$[n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{sk}_\pi)$
$(\xi, D'_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(L, \mathtt{m}, \sigma, D_t, \textbf{εικασία})$
if $\pi \notin D'_t$ **then**
  Επέστρεψε: $\xi = \pi$

else
  Επέστρεψε: $\perp$
end

Ορισμός 5.5. *Υπολογιστική Ανωνυμία*
Ένα LRS σχήμα Π είναι υπολογιστικά t-ανώνυμο αν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

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

Για την τέλεια ανωνυμία το πείραμα παραμένει το ίδιο με αυτό των RS, δηλαδή ένας μη-φραγμένος αντίπαλος δεν επωφελείται με κάποιο ουσιαστικό τρόπο από την ύπαρξη των ψευδώνυμων.

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(\mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow \$[n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{sk}_\pi)$
$\xi \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{SO}}(L, \mathtt{m}, \sigma, \textbf{εικασία})$
Επέστρεψε: $\xi = \pi$

Ορισμός 5.6. *Τέλεια Ανωνυμία*

Ένα LRS σχήμα Π είναι τέλεια ανώνυμο αν για κάθε μη-φραγμένο αντίπαλο $\mathcal{A}$ ισχύει ότι:

$$Pr[\mathsf{Exp}^{UAnonLRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] = \frac{1}{n_L}$$

Συνδεσιμότητα

Η συνδεσιμότητα απαιτεί αν δύο υπογραφές έχουν συνταχθεί από τον ίδιο υπογράφοντα τότε να είναι συνδεδεμένες, και να είναι αδύνατο για οποιονδήποτε αντίπαλο να παράξει ανά δύο μη-συνδεδεμένες υπογραφές από ότι έχει κλειδιά στη διαθεσή του. Στον αντίπαλο αφήνεται πρόσβαση σε όλα τα μαντεία $\mathcal{RO}, \mathcal{SO}, \mathcal{CO}, \mathcal{JO}$ και έχει το ελεύθερο να τα ρωτάει με οποιαδήποτε προσαρμοστική στρατηγική επιθυμεί. Σκοπός του πειράματος είναι για τον $\mathcal{A}$ να παράξει k έγκυρες υπογραφές για τον ίδιο δακτύλιο L της αρεσκείας του που να είναι ασύνδετες μεταξύ τους, έχοντας όμως διαφθείρει γνησίως λιγότερα από k κλειδιά του L. Προφανώς καμία υπογραφή που προκύπτει ως έξοδος του $\mathcal{SO}$ δε γίνεται δεκτή.

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

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

Ορισμός 5.7. *Συνδεσιμότητα*

Ένα LRS σχήμα Π είναι συνδέσιμο εάν για κάθε PPT *αντίπαλο $\mathcal{A}$ ισχύει ότι:*

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

Όπως αναφέρθηκε και πιο πάνω για τον ισχυρό ορισμό της συνδεσιμότητας η μη-δυσφημισιμότητα προκύπτει ως απόρροια της συνδεσιμότητας και της μη-πλαστογραφησιμότητας. Πιο αναλυτικά: ως μη-δυσφημισιμότητα εννοούμε την ιδιότητα εκείνη που δεν επιτρέπει σε κανένα αντίπαλο να παράξει υπογραφή που να συνδέεται με υπογραφές μέλους του δακτυλίου του οποίο το κλειδί είναι άγνωστο. Θα αποδείξουμε τώρα ότι η μη-δυσφημισιμότητα απορρέει από τις ήδη υπάρχουσες ιδιότητες των LRS. Για αρχή έστω ένας αντίπαλος $\mathcal{A}$ που μπορεί να δυσφημίσει ένα μέλος του δακτυλίου. Αν δεν γνωρίζει το μυστικό

κλειδί του στόχου τότε μιλάμε για μία πλαστογραφία το οποίο αντίκειται στις ιδιότητες του σχήματος. Έστω από την άλλη ότι έχει γνώση $k > 0$ ιδιωτικών κλειδιών. Τότε υπάρχουν δύο σενάριο: Αν το κλειδί του στόχου το γνωρίζει αυτό σημαίνει πως δεν έχουμε πλαστογραφία ή παραβίαση της συνδεσιμότητας. Από την άλλη αν το κλειδί δεν ανήκει στα γνωστά του και είναι ικανός να παράξει τη συγκεκριμένη υπογραφή τότε έχουμε παραβίαση της ιδιότητας της συνδεσιμότητας αφού θα έχει την ικανότητα να παράξει $k + 1$ υπογραφές οι οποίες είναι ασύνδετες μεταξύ τους. Επομένως αν το σχήμα διαθέτει την ισχυρή συνδεσιμότητα και τη μη-πλαστογραφησιμότητα τότε διαθέτει και την ιδιόττηα της μη-δυσφημισιμότητας.

Ασφάλεια Σχήματος LSAG

Οι Liu, Wei και Wong απέδειξαν στην εργασία τους [57] την ασφάλεια του σχήματος LSAG στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$. Έτσι λοιπόν προκύπτουν τα ακόλουθα θεωρήματα:

Θεώρημα 5.3. *Μη-Πλαστογραφησιμότητα*
Το σχήμα LSAG είναι μη-πλαστογραφήσιμο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν ισχύει η υπόθεση DLOG *στην ομάδα $\mathbb{G}$.*

Θεώρημα 5.4. *Ανωνυμία*
Το σχήμα LSAG είναι ανώνυμο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν ισχύει η υπόθεση DDH *στην ομάδα $\mathbb{G}$.*

Θεώρημα 5.5. *Συνδεσιμότητα*
Το σχήμα LSAG είναι συνδέσιμο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν ισχύει η υπόθεση DLOG *στην ομάδα $\mathbb{G}$.*

5.4 Συνδέσιμες Υπογραφές Δακτυλίου με Άνευ Όρων Ανωνυμία

5.4.1 Το πρόβλημα ανωνυμίας στις LRS

Η προσθήκη της ιδιότητας της συνδεσημότητας στις υπογραφές δακτυλίου ενώ τις κάνει πολύ χρήσιμες θυσιάζει σε ένα βαθμό την ανωνυμία του σχήματος. Το ψευδώνυμο που χρησιμοποιείται περιέχει πληροφορίες για το ιδιωτικό κλειδί του υπογράφοντα, ενώ ταυτοχρόνως συνδέει την ταυτότητα του υπογράφοντα με συγκεκριμένες υπογραφές. Γίνεται λοιπόν εμφανές πως το ψευδώνυμο, ή αλλιώς η ετικέτα σύνδεσης, αποτελεί την αχίλλειο πτέρνα του σχήματος, και όπως θα δούμε λίαν συντόμως όχι μόνο για την ανωνυμία του σχήματος αλλά και για την ασφάλεια όλου του σχήματος.

Όπως εξηγήσαμε και στην προηγούμενη ενότητα το ψευδώνυμο είναι μία δυσκόλος αντιστρέψιμη συνάρτηση του ιδιωτικού κλειδιού του υπογράφοντα. Υπάρχουν διάφορες μορφές που μπορεί να πάρει:

- Στις LRS [57] και στις DVLRS [13] για να κατασκευαστεί το ψευδώνυμο χρησιμοποείται η τιμή σύνοψης των δημοσίων κλειδιών του δακτυλίο L, $h = \mathcal{H}_{\mathbb{G}}(L)$, και εν συνεχεία η τιμή αυτή χρησιμοποείται ως βάση για ύψωση σε δύναμη h^{sk}, είναι δηλαδή η ίδια διαδικασία με τον υπολογισμό του δημοσίου κλειδιού του υπογράφοντα.

- Στις LRS με άνευ όρων ανωνυμία (ULRS) [56] όπως θα δούμε χρησιμοποιείται ένα κοινό συμβάν-event ev για είσοδος στη συνάρτηση σύνοψης, $h = \mathcal{H}_{\mathbb{G}}(\mathsf{ev})$, και εν συνεχεία το linking tag t υπολογίζεται με τον ίδιο τρόπο $t = h^x$.

- Μία άλλη προσέγγιση είναι αυτή των Tsang και Wei [76] είναι η χρήση ενός γεννήτορα g της $\mathbb{G}$ και η ετικέτα σύνδεσης είναι γενικά g^x.

Το κοινό που εμφανίζουν όλες αυτές οι προσεγγίσεις είναι το γεγονός ότι η ασφάλεια το ότι πληροφορία δε διαρρέει είναι η δυσκολία του DLP στη $\mathbb{G}$. Τι γίνεται όμως αν ο αντίπαλος που αντιμετοπίζουμε μπορεί να λύσει το DLP ή για κάποιο λόγο το DLP δεν είναι όσο δύσκολο υποθέταμε για την ομάδα στην οποία δουλεύουμε; [1]

Στην περίπτωση του LSAG [57], του DVLRS [13] και των άλλων αντίστοιχων κατασκευών [76, 6] τότε μιλάμε για ολικό σπάσιμο (total break) του συστήματος αφού είναι εφικτό να διαρεύσει πλήρως το ιδιωτικό κλειδί κάποιου υπογράφοντα από τον δακτυλίο. Ως αποτέλεσμα ο αντίπαλος είναι ικανός να παράξει ελεύθερα πλαστογραφίες, να συνδέει τις υπογραφές και να κινείται γενικώς ως το συγκεκριμένο μέλος.

Για τους παραπάνω λόγους το ζήτημα ενός σχήματος LRS με άνευ όρων ανωνυμία παρέμενε ως ανοιχτό πρόβλημα, μάλιστα οι Liu, Wei και Wong το είχαν θέσει πρώτοι ως ανοιχτό πρόβλημα στην εργασία [57]. Ανατρέχοντας στη βιβλιογραφία (π.χ. [57, 58, 51, 6, 80, 76, 1, 69]) παρατειρήται ότι ο ορισμός για το πιο αυστηρό επίπεδο ανωνυμίας είναι σχεδόν πάντα ο ίδιος και ταυτίζεται με τον ορισμό που έχει ήδη δοθεί για τις υπογραφές δακτυλίου και τις συνδέσιμες υπογραφές δακτυλίου. Με άλλα λόγια θεωρείται ότι

Η πιθανότητα για οποιονδήποτε μη-περιορισμένο αντίπαλο να μάθει τον πραγματικό υπογράφοντα μιας υπογραφής δακτυλίου δεν είναι καλύτερη από

[1] Κάτι τέτοιο ίσως να είναι ένα ρεαλιστικό πρόβλημα στις ελλειπτικές καμπύλες αφού χρησιμοποιείται ένας περιορισμένος αριθμός τους σε κρυπτογραφικές εφαρμογές. Όπως έχει πει και ο Bonneh έχουμε βάλει όλα τα αυγά μας σε ένα καλάθι και ίσως να εκπληχθούμε δυσάρεστα κάποια στιγμή.

την τυχαία επιλογή ενός μέλους του δακτυλίου από τον οποίο προέρχεται η υπογραφή.

Οι Jeong, Kwon και Lee στην εργασία τους [46] δηλώνουν πως κανένα σχήμα συνδέσιμων υπογραφών δακτυλίου με υποχρεωτική σύνδεση δε μπορεί να διαθέτει ανωνυμία εναντίον ενός απεριόριστου αντιπάλου και αποδεικνύουν αυτή τους τη θέση στο πρώτο θεώρημα της εργασίας. Το ζήτημα που δημιουργείται όμως είναι το εξής: Δεν είναι ξεκάθαρο τι ορίζουν ως ανωνυμία μιας και ο ορισμός που δίνουν είναι διαφορετικός από αυτόν που έχουμε περιγράψει και αφήνεται ανοικτός σε ερμηνεία από τον αναγνώστη.

Ορμώμενοι από αυτή την ασάφεια που έχει προκύψει οι Liu, Au, Susilo και Zhou προσπάθησαν να ξεκαθαρίσουν ελαφρώς το τοπίο, έτσι στην εργασία τους [56] δίνουν δύο διαφορετικούς ορισμούς για την λεγώμενη ισχυρή ή αλλιώς τέλεια ή αλλιώς άνευ όρων ανωνυμία, και με βάση αυτούς τους ορισμούς προχωρούν στη δημιουργία ενός νέου είδους υπογραφών τις συνδέσιμες υπογραφές δακτυλίου με άνευ όρων ανωνυμία (Linkable Ring Signatures with Unconditional Anonymity - ULRS).

Στην [56] βλέπουμε δύο πιθανούς ορισμούς της ισχυρής ανωνυμίας τους οποίος και παραθέτουμε:

Ορισμός 5.8. *Δεδομένων των δημοσίων κλειδιών (ή ταυτοτήτων για την περίπτωση σχημάτων ID) όλων των μελών μίας υπογραφής δακτυλίου, καμία οντότητα δε μπορεί να μάθει τον πραγματικό υπογράφοντα ακόμα και αν όλα τα ιδιωτικά κλειδιά* ***που ανήκουν*** *στα μέλη του δακτυλίου είναι γνωστά.*

Ορισμός 5.9. *Δεδομένων των δημοσίων κλειδιών (ή ταυτοτήτων για την περίπτωση σχημάτων ID) όλων των μελών μίας υπογραφής δακτυλίου, καμία οντότητα δε μπορεί να μάθει τον πραγματικό υπογράφοντα ακόμα και αν όλα τα ιδιωτικά κλειδιά* ***που αντιστοιχούν*** *στα μέλη του δακτυλίου είναι γνωστά.*

Οι δύο αυτοί ορισμοί ταυτίζονται όταν έχουμε ένα-προς-ένα αντιστοιχία ιδιωτικού και δημοσίου κλειδιού, δηλαδή όπως συμβαίνει με τα σχήματα που έχουμε ήδη αναφέρει. Υπάρχουν όμως περιπτώσεις, κυρίως σε ID-based σχήματα, για τις οποίες δεν ισχύει αυτή η αντιστοιχία. Παράδειγμα αποτελούν τα σχήματα των τύπου Boney-Boyen [19, 18], τύπου Waters [77] και τύπου Gentry [38].

Όπως έχουμε ήδη δει αν διαρεύσει πλήρως το ιδιωτικό κλειδί των μελών του δακτυλίου τότε είναι αδύνατο ένα LRS σχήμα με υποχρεωτική συνδεσημότητα να διατηρήσει την ανωνυμία. Κάτι τέτοιο είναι εφικτό να συμβεί στις LRS διότι το ψευδώνυμο περιέχει το ιδιωτκό κλειδί του υπογράφοντα και είναι εφικτό για έναν μη-φραγμένο αντίπαλο να το εξάγει και άρα να σπάσει τελείως το σύστημα. Αν όμως σε ένα δημόσιο κλειδί αντισχτοιχούν πολλαπλά ιδιωτικά κλειδιά τότε

τι θα γινόταν; Με αυτή ακριβώς την σκέψη κινήθηκαν και οι Liu, Au, Susilo και Zhou και κατάφεραν να κατασκευάσουν τις ULRS.

5.4.2 Το μοντέλο ULRS

Όπως προαναφέρθηκε η ιδέα πίσω από τις ULRS είναι να αλλάξουν τα κλειδιά. Πιο συγκεκριμένα θα πρέπει το ιδιωτικό κλειδί του υπογράφοντα να μη προσδιορίζεται πλήρως από το ψευδώνυμο, ή αλλιώς την ετικέτας όπως αναφέρεται στην εργασία.

Για να επιτευχθεί το ζητούμενο σκέφτονται το εξής: Το ιδιωτικό κλειδί του υπογράφοντα δεν είναι απλά ένας τυχαίος ακέραιος $x \in \mathbb{Z}_q$ αλλά ένα ζεύγος ακεραίων $(x, y) \in \mathbb{Z}_q^2$. Τώρα το δημόσιο κλειδί του υπογράφοντα θα υπολογίζεται ως $g^x h^y$, ενώ η ετικέτα σύνδεσης θα είναι $t = e^x$, όπου g, h, e είναι γεννήτορες της ομάδας $\mathbb{G}$ στην οποία εργαζόμαστε.

Σε αυτό το σχήμα συμβαίνει το εξής: Αν η αρχικοποίηση είναι σωστή, δηλαδή η τάξη της ομάδα $\mathbb{G}$ είναι κάποιος πρώτος q και οι γεννήτορες έχουν επιλεγεί με τρόπο τέτοιο ώστε να μην είναι γνωστός ο σχετικός διακριτός τους λογάριθμος τότε η συνάρτηση υπολογισμού των δημοσιών κλειδιών $\phi(x, y) = g^x h^y$ δεν είναι ένα-προς-ένα όπως στη συνηθισμένη περίπτωση των LRS, όπου το δημόσιο κλειδί είναι g^x, αλλά q-προς-ένα. Αυτό έχει δύο αποτελέσματα: πρώτον είναι τώρα εφικτό για 2 μέλη του δακτυλίου να έχουν ακριβώς το ίδιο δημόσιο κλειδί, έχοντας όμως τελειώς διαφορετικά ιδιωτικά κλειδιά. Δεύτερον ακόμα και αν κάποιος βρει το ένα μέρος του ιδιωτικού κλειδιού μέσω της ετικέτας της υπογραφής δεν μπορεί να μάθει ποιος είναι ο υπογράφοντας μιας και κάθε υπογράφοντας θα μπορούσε να έχει δημόσιο κλειδί που να αντιστοιχεί σε ιδιωτικό κλειδί του οποίου το ένα μέρος είναι αυτό που βρέθηκε στην ετικέτα.

Θα περιγράψουμε τώρα τους αλγορίθμους από τους οποίους αποτελείται ένα σχήμα ULRS:

- **Δημιουργία Παραμέτρων Συστήματος** - $\mathsf{Setup}(\lambda)$:

  Με είσοδο την παράμετρο ασφαλείας λ δημιουργούνται οι παράμετροι του συστήματος params. Πιο συγκεκριμένα ορίζονται οι χώροι κλειδιών, μηνυμάτων, συμβάντων και υπογραφών.

  Καλούμε $\mathsf{params} \leftarrow \mathsf{Setup}(\lambda)$.

- **Δημιουργία Κλειδιών** - $\mathsf{KGen}(\mathsf{params})$:

  Κάθε χρήστης επικαλείται τον αλγόριθμο KGen ώστε να λάβει το ζεύγος κλειδιών του $(\mathsf{sk}, \mathsf{pk})$. Τα κλειδιά δημιουργούνται κατά βούληση από τον εκάστοτε χρήστη.

  Καλούμε $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(\mathsf{params})$.

- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(\mathtt{ev}, n, L, \mathtt{m}, \mathsf{sk}_\pi)$:

  Για να υπογράψει ένα μέλος του δακτυλίου L ένα μήνυμα $\mathtt{m}$ επικαλείται τον αλγόριθμο Sign και χρησιμοποιεί για είσοδο τον δακτυλίο L μεγέθους n, το μήνυμα $\mathtt{m}$, το κοινό συμβάν $\mathtt{ev}$ και το ιδιωτικό του κλειδί sk_π, όπου π είναι ο δείκτης του συγκεκριμένου υπογράφοντα στο δακτυλίο L.

  Καλούμε $\sigma \leftarrow \mathsf{Sign}(\mathtt{ev}, n, L, \mathtt{m}, \mathsf{sk}_\pi)$.

- **Εξαγωγή** - $\mathsf{Extract}(\sigma)$:

  Ο αλγόριθμος Extract με είσοδο μία υπογραφή σ εξάγει το pid της υπογραφής.

  Καλούμε $\mathsf{pid} \leftarrow \mathsf{Extract}(\sigma)$.

- **Επαλήθευση** - $\mathsf{Vrfy}(\mathtt{ev}, n, \sigma, L, \mathtt{m})$:

  Ο αλγόριθμος επαλήθευσης επιστρέφει 1 αν η υπογραφή σ είναι έγκυρη, αλλίως επιστρέφει 0.

  Καλούμε $\{0,1\} \leftarrow \mathsf{Vrfy}(\mathtt{ev}, n, \sigma, L, \mathtt{m})$.

- **Σύνδεση** - $\mathsf{Link}(\mathtt{ev}, n_1, n_2, L_1, L_2, \sigma_1, \sigma_2)$:

  Με την κλήση του αλγορίθμου σύνδεσης ελέγχεται εάν δύο υπογραφές σ_1, σ_2 με ίδιο συμβάν $\mathtt{ev}$, απο δακτυλίους L_1 και L_2 αντίστοιχα είναι συνδεδεμένες ή όχι. Ο αλγόριθμος επιστρέφει 1 εάν είναι συνδεδεμένες, αλλιώς επιστρέφει 0.

  Καλούμε $\{0,1\} \leftarrow \mathsf{Link}(\mathtt{ev}, n_1, n_2, L_1, L_2, \sigma_1, \sigma_2)$.

5.4.3 Κατασκευή ενός ULRS σχήματος

Θα δούμε τώρα την κατασκευή ενός ULRS σχήματος όπως αυτή δίνεται στην [56].

- **Δημιουργία Παραμέτρων Συστήματος** - $\mathsf{Setup}(\lambda)$:

  Όπως και στο LSAG έτσι και εδώ θα εργαστούμε σε μία ομάδα $\mathbb{G}$ τάξης πρώτου q στην οποία θεωρούμε ότι είναι δύσκολο το DLP. Επιπλέον χρειαζόμαστε δύο συναρτήσεις σύνοψης $\mathcal{H}_q : \{0,1\}^* \rightarrow \mathbb{Z}_q$ και $\mathcal{H}_\mathbb{G} : \{0,1\}^* \rightarrow \mathbb{G}$. Ακόμα κατασκευάζονται δύο γεννήτορες της $\mathbb{G}$ g, h με τον ακόλουθο τρόπο: $g = \mathcal{H}_\mathbb{G}(\text{"}GENERATOR - g\text{"})$ και $h = \mathcal{H}_\mathbb{G}(\text{"}GENERATOR - h\text{"})$. Σημειώνουμε πως οποιοδήποτε επιθυμεί μπορεί να επανυπολογίσει αυτές τις τιμές και να τις ελέγξει ως προς την ορθότητά τους. Ορίζουμε ως δημόσιες παραμέτρους $\mathsf{params} = (\mathbb{G}, g, h, q, \mathcal{H}_q, \mathcal{H}_\mathbb{G})$.

- **Δημιουργία Κλειδιών -** KGen(params):

  Κάθε χρήστης:

  1. Επιλέγει τυχαία $x, y \leftarrow \$\mathbb{Z}_q$
  2. Υπολογίζει $Z = g^x h^y$
  3. Θέτει $\mathsf{sk} = (x, y)$ και $\mathsf{pk} = Z$

- **Δημιουργία Υπογραφής -** Sign($\mathtt{ev}, n, L, \mathtt{m}, \mathsf{sk}_\pi$):

  Ο υπογράφοντας :

  1. Υπολογίζει $e = \mathcal{H}_{\mathbb{G}}(\mathtt{ev})$ και $t = e^{x_\pi}$
  2. Επιλέγει τυχαία $r_{x_\pi}, r_{y_\pi}, c_1, \ldots, c_{\pi-1}, c_{\pi+1}, \ldots c_n \in_R \mathbb{Z}_q$ και υπολογίζει

  $$K = g^{r_{x_\pi}} h^{r_{y_\pi}} \prod_{i=1, i\neq\pi}^{n} Z_i^{c_i}, K' = e^{r_{x_\pi}} t^{\sum_{i=1,i\neq\pi}^{n} c_i}$$

  3. Βρίσκει c_π έτσι ώστε

  $$c_1 + \cdots + c_n \mod q = \mathcal{H}_q = (L, \mathtt{ev}, t, \mathtt{m}, K, K')$$

  4. Υπολογίζει $\tilde{x} = r_{x_\pi} - c_\pi x_\pi \mod q$, $\tilde{y} = r_{y_\pi} - c_\pi y_\pi \mod q$ Η υπογραφή είναι $\sigma = (t, \tilde{x}, \tilde{y}, \{c_i\}_{i=1}^n)$
  5. **Επέστρεψε** σ

- **Εξαγωγή -** Extract(σ):

  1. **Επέστρεψε** t

- **Επαλήθευση -** Vrfy($\mathtt{ev}, n, \sigma, L, \mathtt{m}$):

  1. Υπολόγισε $e = \mathcal{H}_{\mathbb{G}}(\mathtt{ev})$
  2. Υπολόγισε $c_0 = \mathcal{H}_q(L, \mathtt{ev}, t, \mathtt{m}, g^{\tilde{x}} h^{\tilde{y}} \prod_{i=1}^{n} Z_i^{c_i}, e^{\tilde{x}} t^{\sum_{i=1}^{n} c_i})$
  3. **Επέστρεψε** 1 αν $\sum_{i=1}^{n} c_i \mod q = c_0$, αλλίως **Επέστρεψε** 0.

- **Σύνδεση -** Link($\mathtt{ev}, n_1, n_2, L_1, L_2, \sigma_1, \sigma_2$):

  1. **Επέστρεψε** 1 αν Extract(σ_1) = Extract(σ_2), αλλίως **Επέστρεψε** 0.

5.4.4 Ιδιότητες Ασφάλειας ULRS

Θα μελετήσουμε τώρα τις ιδιότητες ασφάλειας ενός ULRS σχήματος. Για την μοντελοποίηση του αντιπάλου άφηνουμε πάλι πρόσβαση στα μαντεία $\mathcal{RO}, \mathcal{CO}, \mathcal{SO}, \mathcal{JO}$.

Σημείωνουμε εδώ πως σε όλα τα πειράματα ο αντίπαλος όταν επιλέγει τις παραμέτρους επιλέγει και το συμβάν $\mathtt{ev}$ που θα χρησιμοποιηθεί για τις ετικέτες σύνδεσης των υπογραφών.

Μη-Πλαστογραφησιμότητα

Η μη-πλαστογραφησιμότητα ενός ULRS σχήματος παραμένει ίδια με αυτή των απλών LRS. Έτσι η απαίτηση είναι να μη μπορεί ένας αντίπαλος να παράξει μία έγκυρη υπογραφή χωρίς να έχει γνώση ενός ιδιωτικού κλειδιού του δακτυλίου.

Για το παιχνίδι της μη-πλαστογραφησιμότητας έχουμε ακριβώς την ίδια μοντελοποίηση με αυτή των LRS

Παιχνίδι 5.8: Πείραμα Μη-Πλαστογραφησιμότητας $\mathsf{Exp}^{UnfULRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$
$(\mathtt{ev}, \sigma, L = \{\mathsf{pk}_i\}_{i=1}^{n}, \mathtt{m}, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(1^\lambda)$
Επέστρεψε: $\mathsf{Vrfy}(\mathtt{ev}, n, \sigma, L, \mathtt{m})$ **ΚΑΙ** σ δεν είναι είσοδος των $\mathcal{SO}$ **ΚΑΙ** $\forall i \in D_t : pk_i \notin D_t$

Ορισμός 5.10. *Μη-Πλαστογραφησιμότητα*

Ένα ULRS σχήμα Π *είναι μη-πλαστογραφήσιμο αν για κάθε* PPT *αντίπαλο* $\mathcal{A}$ *ισχύει:*

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

Ανωνυμία

Η ανωνυμία είναι επίσης ίδια στις ULRS με τις LRS. Όπως θα δούμε όμως είναι αναγκαίο κάθε ULRS σχήμα να είναι τέλεια ανώνυμο, ακόμα και για αντιπάλους που είναι μη-περιορισμένοι υπολογιστικά και χρονικά.

Έτσι λοιπόν το πείραμα και ο ορισμός για την ανωνυμία είναι ίδια με αυτά της τέλειας ανωνυμίας για τις ULRS. Σημειώνουμε εδώ πως δε δίνεται πρόσβαση στον αντίπαλο $\mathcal{A}$ σε κάνενα μαντείο πλην του Μαντείου Εγγραφής $\mathcal{JO}$, μιας και υποθέτουμε πως ο $\mathcal{A}$ είναι μη-περιορισμένος.

Παιχνίδι 5.9: Πείραμα Τέλειας Ανωνυμίας $\mathsf{Exp}^{UAnonULRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$
$(\mathtt{ev}, L = \{\mathsf{pk}_i\}_{i=1}^{n}, \mathtt{m}) \leftarrow \mathcal{A}^{\mathcal{JO}}(\textbf{επιλογή})$
$\pi \leftarrow \$[n]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(\mathtt{ev}, n, L, \mathtt{m}, \mathsf{sk}_\pi)$
$\xi \leftarrow \mathcal{A}(\mathtt{ev}, n, L, \mathtt{m}, \sigma, \textbf{εικασία})$
Επέστρεψε: $\xi = \pi$

Ορισμός 5.11. *Τέλεια Ανωνυμία*

Ένα ULRS σχήμα Π είναι τέλεια ανώνυμο αν για κάθε μη-φραγμένο αντίπαλο $\mathcal{A}$ ισχύει ότι:

$$Pr[\mathsf{Exp}^{UAnonULRS}_{\mathcal{A},\Pi,n}(\lambda) = 1] = \frac{1}{n}$$

Συνδεσιμότητα

Η βελτίωση της ανωνυμίας σε τέλεια οδηγεί σε ένα πρόβλημα για τη συνδεσημότητα. Σε αντίθεση με τις LRS οι ULRS έχουν την πιο ασθενή ιδιότητα της συνδεσιμότητας η οποία λέει ότι: Αν ένας αντίπαλος γνωρίζει 1 ιδιωτικό κλειδί τότε δε μπορεί να παράξει 2 μη συνδεδεμένες μεταξύ τους υπογραφές. Ο λόγος για αυτή την εξασθένηση για γίνει εμφανής σε παράδειγμα που θα δωθεί σε επόμενη ενότητα.

Λόγω αυτής της αλλαγής το παιχνίδι της συνδεσιμότητας τροποποιείται και τώρα χρειάζεται να παραχθούν επιτυχώς μόνο 2 συνδέσιμες μεταξύ τους υπογραφές οι οποίες να μην αποτελούν έξοδο του Μαντείου Υπογραφής $\mathcal{SO}$, ενώ ακόμα ο αντίπαλος περιορίζεται σε μόνο μία κλήση στο Μαντείο Διαφθοράς $\mathcal{CO}$.

Παιχνίδι 5.10: Πείραμα Συνδεσιμότητας $\mathsf{Exp}^{LinkULRS}_{\mathcal{A},\Pi,n}$

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$(\sigma_1, \sigma_2, \mathtt{ev}, L_1 = \{\mathsf{pk}_i\}_{i=1}^{n_1}, L_2 = \{\mathsf{pk}_i\}_{i=1}^{n_2}, \mathtt{m}_1, \mathtt{m}_2) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}()$
Επέστρεψε: $|\mathcal{CO} = 1|$ **ΚΑΙ** σ_1, σ_2 δεν είναι έξοδος του $\mathcal{SO}$ **ΚΑΙ**
$\mathsf{Vrfy}(\mathtt{ev}, n_1, L_1, \sigma_1, \mathtt{m}_1) = 1$ **ΚΑΙ** $\mathsf{Vrfy}(\mathtt{ev}, n_2, L_2, \sigma_2, \mathtt{m}_2) = 1$ **ΚΑΙ**
$\mathsf{Link}(\mathtt{ev}, n_1, n_2, L_1, L_2, \sigma_1, \sigma_2) = 0$

Ορισμός 5.12. *Συνδεσιμότητα*

Ένα ULRS σχήμα Π είναι συνδέσιμο εάν για κάθε PPT *αντίπαλο $\mathcal{A}$ ισχύει ότι:*

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

Μη-Δυσφημισιμότητα

Όπως εξηγήσαμε και στις LRS όταν ένα σχήμα διαθέτει μόνο την απλή ιδιότητα της συνδεσιμότητας τότε είναι αναγκαίο να αποδειχθεί η ιδιότητα της μη-δυσφημισιμότητας. Η μη-δυσφημισιμότητα ως ιδιότητα δηλώνει ότι κανένας αντίπαλός δε πρέπει να μπορεί να παράξει υπογραφή που να συνδέεται επιτυχώς με άλλη υπογραφή, για την οποία ο αντίπαλος δεν έχει γνώση του ιδιωτικού κλειδιού που την έχει παράξει.

Στο πείραμα της μη-δυσφημισιμότητας ζητείται από τον αντίπαλο να παράξει υπογραφή σ_2 έτσι ώστε $\mathsf{Link}(\mathsf{ev}, n_1, n_2, L_1, L_2, \sigma_1, \sigma_2) = 1$, όπου σ_1 είναι μία υπογραφή-πρόκληση. Ο αντίπαλος $\mathcal{A}$ επιλέγει το δημόσιο κλειδί στο οποίο θα αντιστοιχεί η υπογραφή-πρόκληση που θα παραχθεί, καθώς και τον δακτύλιο και το μήνυμα της υπογραφής. Με βάση τα προηγούμενα παράγεται μία υπογραφεί σ_1 και δίνεται στον $\mathcal{A}$. Σημειώνουμε πως το δημόσιο κλειδί της υπογραφής δε μπορεί να είναι είσοδος στο Μαντείο Διαφθοράς $\mathcal{CO}$, ούτε μπορεί να χρησιμοποιηθεί σε ερώτηση στο Μαντείο Υπογραφών $\mathcal{SO}$. Εκτός από αυτούς τους περιορισμούς ο $\mathcal{A}$ μπορεί να ρωτάει ελεύθερα τα μαντεία με οποιαδήποτε στρατηγική επιθυμεί. Ο $\mathcal{A}$ πρέπει τώρα να παράξει μία νέα υπογραφή $\sigma_2 \neq \sigma_1$ για κάποιο δακτύλιο L_2 και μήνυμα $\mathtt{m}_2$ της αρεσκείας του.

Παιχνίδι 5.11: Πείραμα Μη-Δυσφημισιμότητας $\mathsf{Exp}^{SlandULRS}_{\mathcal{A},\Pi}$

$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$
$(\mathsf{ev}, L_1 = \{\mathsf{pk}_i\}_{i=1}^{n_1}, \mathtt{m}_1, \mathsf{pk}_\pi) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO},}$
$\sigma_1 \leftarrow \Pi.\mathsf{Sign}(\mathsf{ev}, n_1, L_1, \mathtt{m}_1, \mathsf{sk}_\pi)$
$(\sigma_2, n_2, L_2 = \{\mathsf{pk}_i\}_{i=1}^{n_2}, \mathtt{m}_2) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO}}$
Επέστρεψε: $\sigma_2 \neq \sigma_1$ **ΚΑΙ** $\mathsf{Vrfy}(\mathsf{ev}, n_2, \sigma_2, L_2, \mathtt{m}_2) = 1$ **ΚΑΙ**
$\sigma_2 \notin \mathcal{SO}$ **ΚΑΙ** $\pi \notin \mathcal{CO}$ **ΚΑΙ** $\mathsf{Link}(\mathsf{ev}, n_1, n_2, L_1, L_2, \sigma_1, \sigma_2) = 1$

Ορισμός 5.13. *Μη-Δυσφημισιμότητα*
Ένα ULRS σχήμα Π είναι μη-δυσφημίσιμο εάν για κάθε PPT *αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

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

5.4.5 Ασφάλεια Κατασκευής ULRS

Σε αυτό το σημείο θα μελετήσουμε την ασφάλεια που προσφέρει η κατασκευή των [56].

Θεώρημα 5.6. *Μη-Πλαστογραφησιμότητα*
Το σχήμα ULRS είναι μη-πλαστογραφήσιμο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ *αν ισχύει η υπόθεση* DLOG *στην ομάδα* $\mathbb{G}$.

Θεώρημα 5.7. *Ανωνυμία*
Το σχήμα ULRS είναι τέλεια ανώνυμο (άνευ όρων) για κάθε μη-φραγμένο αντίπαλο $\mathcal{A}$.

Θεώρημα 5.8. *Συνδεσιμότητα*
Το σχήμα ULRS είναι συνδέσιμο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν ισχύει η υπόθεση DLOG *στην ομάδα $\mathbb{G}$.*

Θεώρημα 5.9. *Μη-Δυσφημισιμότητα*
Το σχήμα LSAG είναι μη-δυσφημίσιμο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν ισχύει η υπόθεση DLOG *στην ομάδα $\mathbb{G}$.*

5.4.6 Επίθεση στη Συνδεσιμότητα

Όπως περιγράψαμε το ULRS δε διαθέτει την ισχυρή συνδεσιμότητα του LRS αλλά μία πιο ασθενή εκδοχή της. Αυτό οφείλεται στην ίδια την προσθήκη της ισχυρότερης ανωνυμίας. Για να γίνει καλύτερα κατανοητό παραθέτουμε το ακόλουθο σενάριο:

Έστω δύο μέλη του δακτυλίου L στον οποίο δουλεύουμε με ιδιωτικά κλειδιά (x_1, y_1) και (x_2, y_2) αντίστοιχα, ενώ $Z_1 = g^{x_1}h^{y_1}$ και $Z_2 = g^{x_2}h^{y_2}$ είναι αντίστοιχα δημόσια κλειδιά τους. Αν αυτά τα δύο άτομα συνεργαστούν και μοιραστούν τα κλειδιά τους τότε θα είναι εφικτό να παράξουν υπογραφές που θα συνδέονται με οποιδήποτε πιθανό μέλος του δακτυλίου.

Για να το κάνουν αυτό ξεκινούν υπολογίζοντας $e = \mathcal{H}_{\mathbb{G}}(\mathtt{ev})$. Εν συνεχεία επιλέγουν $\lambda \in \mathbb{Z}_q$ και υπολογίζουν $t = e^{\frac{x_1+\lambda x_2}{\lambda+1}} = e^{\mu}$. Το t είναι η ετικέτα σύνδεσης που θα χρησιμοποιήσουν για την υπογραφή που θα παράξουν.

Προχωρόντας τώρα στη δημιουργία της υπογραφής επιλέγουν στη τύχη $r_x, r_y, c_3, c_4, \ldots, c_n \in_R \mathbb{Z}_q$ και υπολογίζουν :

$$K = g^{r_x}h^{r_y}\prod_{i=3}^{n} Z_i^{c_i}$$

και

$$K' = e^{r_x}t^{\sum_{i=3}^{n} c_i}$$

Έπειτα υπολογίζουν c_1 και c_2 έτσι ώστε:

$$c_1 + c_2 + \cdots + c_n = \mathcal{H}_q(L, \mathtt{ev}, t, \mathtt{m}, K, K')$$

και

$$\lambda c_1 = c_2$$

Στη συνέχεια υπολογίζουν

$$\tilde{x} = r_x - \mu(c_1 + c_2)$$

$$\tilde{y} = r_y - c_1 y_1 - c_2 y_2$$

Η υπογραφή θα είναι $\sigma = (t, \tilde{x}, \tilde{y}, c_1, \ldots, c_n)$.

Εδώ σημειώνουμε πως η συγκεκριμένη υπογραφή είναι έγκυρη μιας και:

$$c_1 + c_2 + c_3 + \cdots + c_n = \mathcal{H}_q(L, \mathtt{ev}, t, \mathtt{m}, g^{r_x} h^{r_y} \prod_{i=3}^{n} Z_i^{c_i}, e^{r_x} t^{\sum_{i=3}^{n} c_i})$$

$$= \mathcal{H}_q(L, \mathtt{ev}, t, \mathtt{m}, g^{\tilde{x}} h^{\tilde{y}} \prod_{i=1}^{n} Z_i^{c_i}, e^{\tilde{x}} t^{\sum_{i=1}^{n} c_i})$$

αφού:

$$g^{\tilde{x}} h^{\tilde{y}} \prod_{i=1}^{n} Z_i^{c_i} = g^{r_x} g^{-\mu(c_1+c_2)} h^{r_y} h^{-y_1 c_1} h^{-y_2 c_2} g^{x_1 c_1} g^{x_2 c_2} h^{y_1 c_1} h^{y_2 c_2} \prod_{i=3}^{n} Z_i^{c_i} =$$

$$= g^{r_x} g^{-\frac{x_1+\lambda x_2}{\lambda+1}(\lambda+1)c_1} h^{r_y} g^{x_1 c_1} g^{\lambda x_2 c_1} \prod_{i=3}^{n} Z_i^{c_i} =$$

$$= g^{r_x} g^{-x_1 c_1} g^{-\lambda x_2 c_1} h^{r_y} g^{x_1 c_1} g^{\lambda x_2 c_1} \prod_{i=3}^{n} Z_i^{c_i} =$$

$$= g^{r_x} h^{r_y} \prod_{i=3}^{n} Z_i^{c_i}$$

και

$$e^{\tilde{x}} t^{\sum_{i=1}^{n} c_i} = e^{r_x} e^{-\mu(c_1+c_2)} t^{c_1+c_2} t^{\sum_{i=3}^{n} c_i} =$$

$$= e^{\tilde{x}} t^{\sum_{i=1}^{n} c_i} = e^{r_x} e^{-\mu(c_1+c_2)} e^{\mu(c_1+c_2)} t^{\sum_{i=3}^{n} c_i} =$$

$$= e^{r_x} t^{\sum_{i=3}^{n} c_i}$$

Η παραπάνω επίθεση αποτελεί ένα παράδειγμα *επίθεσης συννενόησης (collusion attack)* και έχει ως αποτέλεσμα δύο άτομα να μπορούν να παράξουν q το πλήθος ασύνδετες μεταξύ τους υπογραφές. Έδω πρέπει να σημειώσουμε πως η επίθεση αυτή είναι εφικτή μόνο όταν κάποιος έχει γνώση 2 ζεύγων ιδιωτικών κλειδιών μιας και με ένα μόνο ζεύγος ο αντίπαλος θα πρέπει να μαντέψει στη τύχη ένα έγκυρο ιδιωτικό κλειδί το οποίο να ανήκει στο δακτυλίου L, κάτι στατικά απίθανο για τα μεγέθη ομάδων στα οποία δουλεύουμε.

Το γεγονός ότι η συγκεκριμένη επίθεση είναι εκτελέσιμη είναι και ο λόγος που οι ULRS δε πρέπει να χρησιμοποιούνται για χρήση σε ηλεκτρονικές ψηφοφορίες αφού δύο μόλις ψηφοφόροι θα ήταν ικανοί να καταστρέψουν όλο το εκλογικό αποτέλεσμα.

Κεφάλαιο 6

Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή

Το 2021 οι Behrouz, Γροντάς, Κωνσταντακάκος, Παγουρτζής, και Σπυράκου προέταξαν τις Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή (Designated Verifier Linkable Ring Signatures-DVLRS) [13]. Οι DVLRS αποτελούν την πρώτη επιτυχή ζεύξη των LRS και των απλών DVS. Η ιδέα πίσω από τις DVLRS υπογραφές είναι η διάζευξη δύο Σ-Πρωτοκόλλων, το πρώτο είναι γνώση για 1 από n DLOG [1] ενώ το δεύτερο είναι για γνώση ενός DLOG κλειδιού που μας το προσφέρει ένα απλό πρωτόκολλο Schnorr. Δηλαδή μία DVLRS υπογραφή δείχνει ότι ο υπογράφων έχει γνώση είτε ενός ιδιωτικού κλειδιού από τον δακτυλίο είτε ότι γνωρίζει το ιδιωτικό κλειδί του καθορισμένου επαληθευτή (Designated Verifier - DV). Οι DVLRS έχουν την ιδιότητα ότι είναι πραγματικά χρήσιμες για ένα μόνο άτομο, τον DV. Ενώ μπορεί να προέρχονται από ένα σύνολο ατόμων η δυνατότητα του DV να παράγει προσομοιώσεις καθιστά τις υπογραφές χρήσιμες μόνο για εκείνον, επιτυγχάνεται έτσι μία γενίκευση της ιδέας που είχαν προτείνει οι Rivest, Shamir, και Tauman στην εργασία τους [69].

Θα προσπαθήσουμε να δώσουμε μια αρκετά αναλυτική περιγραφή των DVLRS μιας και η κατανοησή τους είναι ύψιστης σημασίας για την κατανοησή των Συνδέσιμων Υπογραφών Δακτυλίου Καθορισμένου Επαληθευτή με άνευ όρων ανωνυμία που αποτελούν το σημαντικότερο σκέλος της ΔΕ και παρουσιάζονται στο επόμενο κεφάλαιο.

Σε αυτή την ενότητα θα δούμε από τι αποτελείται ένα σχήμα DVLRS, θα αναφέρουμε τις ιδιοτητές του και θα προσπαθήσουμε να προσφέρουμε την διαίσθηση πίσω από τη χρήση τους.

6.1 Το μοντέλο DVLRS

Πριν απαριθμίσουμε τους αλγορίθμους που απαρτίζουν ένα σχήμα DVLRS θα προσπαθήσουμε να δώσουμε λίγο τη διαίσθηση πίσω από το μοντέλο. Όπως αναφέραμε και στην εισαγωγή του κεφαλαίου οι DVLRS αποτελούν μία ζεύξη των DVS και LRS, αυτό γίνεται άμεσα αντιλυπτό από τους αλγορίθμους του σχήματος. Για αρχή αφού έχουμε σχήμα υπογραφής υπάρχουν οι κλασσικοί αλγόριθμοι (KGen, Sign, Vrfy), μαζί φυσικά με έναν αλγόριθμο για τον ορισμό παραμέτρων Setup. Από τις LRS κληρονομεί τον αλγόριθμο Link, με τον οποίο ελέγχεται αν δύο υπογραφές έχουν παραχθεί από τον ίδιο υπογράφοντα. Από τις DVS κληρονομεί τον αλγόριθμο Sim, ο οποίος αξιοποιείται από τον DV με σκοπό να παράξει προσομοιώσεις της αρεσκείας του. Τέλος εισάγεται και ένας νέος αλγόριθμος Extract, ο οποίος χρησιμοποιείται από τον DV για να εξάγει το pid από κάποια υπογραφή που βλέπει.

Όταν ένα μέλος του δακτυλίου θέλει να υπογράψει ένα μήνυμα αρκεί να επικαλεστεί τον αλγόριθμο Sign, οποίος έχει παρόμοια είσοδο με τον κλασσικό αλγόριθμο Sign του LRS με την προσθήκη του δημοσίου κλειδιού του DV.

Όταν ο DV θέλει να δημιουργήσει μία προσομοίωση πρέπει αρχικά να επιλέξει ένα pid. Αν επιθυμεί η υπογραφή που θα παραχθεί να είναι συνδέσιμη με τις υπογραφές που έχουν παράξει άλλα μέλη του δακτυλίου τότε πρέπει να εξάγει το pid από το μέλος του δακτυλίου που επιθυμεί και εν συνεχεία να χρησιμοποιήσει τον αλγόριθμο Sim. Είναι επίσης εφικτό το pid που θα χρησιμοποιήσει να μην ανήκει σε κάποιο μέλος του δακτυλίου, σε αυτή την περίπτωση η προσομοίωση που προκύπτει δε θα μπορεί να συνδεθεί με καμία ήδη υπάρχουσα υπογραφή.

Ορισμός 6.1. *Σχήμα DVLRS*

Ένα σχήμα Συνδέσιμων Υπογραφών Δακτυλίου Καθορισμένου Επαληθευτή Π *είναι μια συλλογή* PPT *αλγορίθμων* (Setup, KGen, Sign, Extract, Sim, Vrfy, Link) *με την ακόλουθη σύνταξη:*

- ***Αλγόριθμος Εγκατάστασης*** - Setup(1^λ)*:*

  Ο αλγόριθμος Setup *με είσοδο την παράμετρο ασφαλείας* λ *κατασκευάζει τις παραμέτρους του σχήματος DVLRS. Σε αυτές συμπεριλαμβάνονται οι κρυπτογραφικές ομάδες, ο χώρος μηνυμάτων* $\mathcal{MSG}$*, και ο χώρος όλων των δυνατών* pid $\mathcal{PID}$*.*

  Καλούμε params $\leftarrow$ Setup(1^λ)*.*

- ***Δημιουργία Κλειδιών*** - KGen()*:*

  Κάθε χρήστης επικαλείται τον αλγόριθμο KGen *ώστε να λάβει το ζεύγος κλειδιών του* (sk, pk)*. Τα κλειδιά δημιουργούνται κατά βούληση από τον εκάστοτε χρήστη.*

Καλούμε $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}()$.

- ***Δημιουργία Υπογραφής*** - $\mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$*:*

  Για να υπογράψει ένα μέλος του δακτυλίου L *ένα μήνυμα* $\mathtt{m}$ *επικαλείται τον αλγόριθμο* Sign *και χρησιμοποιεί για είσοδο τον δακτυλίο* L*, το μήνυμα* $\mathtt{m}$*, το δημόσιο κλειδί του designated verifier* pk_D*, και το ιδιωτικό του κλειδί* sk_π*, όπου* π *είναι ο δείκτης του συγκεκριμένου υπογράφοντα στο δακτυλίο* L*.*

  Καλούμε $\sigma \leftarrow \mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$.

- ***Εξαγωγή*** - $\mathsf{Extract}(\sigma)$*:*

  Ο αλγόριθμος Extract *με είσοδο μία υπογραφή* σ *εξάγει το* pid *της υπογραφής.*

  Καλούμε $\mathsf{pid} \leftarrow \mathsf{Extract}(\sigma)$.

- ***Δημιουργία Προσομοίωσης*** - $\mathsf{Sim}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$*:*

  Ο designated verifier επικαλείται τον αλγόριθμο Sim *όταν θέλει να προσομοιώσει μία υπογραφή. Για είσοδο δίνει το δακτυλίο* L*, το μήνυμα* $\mathtt{m}$*, το ζεύγος κλειδιών του* $(\mathsf{sk}_D, \mathsf{pk}_D)$*, και το* pid *του υπογράφοντα στον οποίο θα συνδεθεί η προσομοίωση που θα παραχθεί.*

  Καλούμε $\sigma \leftarrow Sim(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$.

- ***Επαλήθευση*** - $\mathsf{Vrfy}(\sigma, L, \mathtt{m}, \mathsf{pk}_D)$*:*

  Ο αλγόριθμος επαλήθευσης επιστρέφει 1 *αν η υπογραφή* σ *είναι έγκυρη, αλλίως επιστρέφει* 0*.*

  Καλούμε $\{0, 1\} \leftarrow \mathsf{Vrfy}(\sigma, L, \mathtt{m}, pk_D)$.

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

  Με την κλήση του αλγορίθμου σύνδεσης ελέγχεται εάν δύο υπογραφές σ, σ' *από τον ίδιο δακτυλίο* L *είναι συνδεδεμένες ή όχι.Ο αλγόριθμος επιστρέφει* 1 *εάν είναι συνδεδεμένες, αλλιώς επιστρέφει* 0*.*

  Καλούμε $\{0, 1\} \leftarrow \mathsf{Link}(\sigma, L, \sigma', L)$.

Ένα λεπτό σημείο που πρέπει να αποσαφηνιστεί είναι το ζήτημα της συνδεσημότητας υπογραφών. Οι DVLRS επειδή προέρχονται απο τις LRS [57] έχουν υποχρεωτική σύνδεση, δηλαδή όταν κάποιος υπογράφει πρέπει αναγκαστικά να συνδέσει την υπογραφή του με τις υπόλοιπες που έχει δημιουργήσει. Επιπλέον στο DVLRS η σύνδεση υπογραφών περιορίζεται στον ίδιο δακτυλίο. Δηλαδή ένας υπογράφων θα μπορούσε να έχει τα ίδια ακριβώς κλειδιά, όμως αν

αλλάζει δακτύλιο οι υπογραφές που παράγονται να είναι πλήρως ασυσχέτιστες (εκ πρώτης όψεως) [1] μεταξύ τους. Υπάρχουν και άλλες επιλογές, π.χ. στο [56] η σύνδεση γίνεται με βάση ένα κοινό συμβάν ev, ενώ στο [6] η σύνδεση υπογραφών είναι τελείως ελεύθερη και βασίζεται απλά στο κλειδί του υπογράφοντα.

Έχοντας υπ' όψη τα προηγούμενα βλέπουμε πως δύο υπογραφές είναι συνδεδεμένες όταν έχουν το ίδιο pid και βρίσκονται στον ίδιο δακτυλίο. Το ότι έχουν το ίδιο pid σημαίνει πως είτε είναι και οι δύο έξοδος του αλγορίθμου Sign από τον ίδιο υπογράφοντα, είτε είναι και οι δύο προσομοιώσεις από τον DV με χρήση του Sim για το ίδιο pid, είτε ότι η μία είναι γνήσια υπογραφή και η άλλη γνήσια προσομοίωση για το ίδιο pid.

Πιο αυστηρά ορίζουμε παρακάτω την έννοια της *ορθότητας σύνδεσης (linking correctness)*.

Ορισμός 6.2. *Ορθότητα Σύνδεσης - Linking Correctness*

Ο αλγόριθμος $\mathsf{Link}(\sigma, L, \sigma', L)$ *θα επιστρέφει* 1 *εάν και μόνο εάν ισχύει ένα από τα παρακάτω:*

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

6.2 Ορισμοί Ασφάλειας - Δυνατότητες Αντιπάλου

Θεωρούμε έναν ισχυρό προσαρμοστικό αντίπαλο $\mathcal{A}$, που έχει τη δυνατότητα να προσθέτει νέους χρήστες στο σύστημα, να αποκτά τον έλεγχο χρηστών της επιλογής του, να μπορεί να συλλέξει όλες τις υπογραφές που έχουν συνταχθεί, και να ζητά υπογραφές και προσομοιώσεις για οποιονδήποτε χρήστη σε οποιονδήποτε δακτύλιο. Για τη μοντελοποίηση αυτών των δυνατοτήτων θα γίνει χρήση μαντείων [2], όπως γίνεται και στα [56, 55, 59].

[1] Όπως έχουμε δει και στο προηγούμενο κεφάλαιο έτσι και εδώ το pid του κάθε υπογράφοντα εξαρτάται από το μυστικό του κλειδί sk. Πιο συγκεκριμένα στην κατασκευή που θα δώσουμε σε επόμενη ενότητα βλέπουμε πως για δεδομένο δακτύλιο L το pid $\hat{y} = \mathcal{H}_{\mathbb{G}}(L)^x$. Επομένως ένας αντίπαλος που μπορεί να λύσει το DLP μπορεί να κάνει σύνδεση μεταξύ 2 υπογραφών από διαφορετικούς δακτυλίους.

[2] Για λόγους ευκολίας το όνομα του μαντείου συμβολίζει τόσο το μαντείο ως αλγόριθμο όσο και το σύνολο στοιχείων το οποίο έχει ως έξοδο.

- Μαντείο Εγγραφής (Joining Oracle - $\mathcal{JO}$): Με κλήση στο μαντείο εγγραφής προστίθεται ένα καινούργιο δημόσιο κλειδί pk στο σύνολο των δημόσιων κλειδιών $\mathcal{U}$.

  $\mathsf{pk} \leftarrow \mathcal{JO}()$.

- Μαντείο Διαφθοράς (Corruption Oracle - $\mathcal{CO}$): Έχοντας ως είσοδο ένα δημόσιο κλειδί $\mathsf{pk} \in \mathcal{U}$, το μαντείο διαφθοράς επιστρέφει το ιδιωτικό κλειδί sk που του αντιστοιχεί.

  $\mathsf{sk} \leftarrow \mathcal{SO}(\mathsf{pk})$.

- Μαντείο Υπογραφής (Signing Oracle - $\mathcal{SO}$): Με είσοδο έναν δακτύλιο L, ένα μήνυμα $\mathtt{m}$, ένα δημόσιο κλειδί DV pk_D και το δημόσιο κλειδί pk_π του επιθυμητού υπογράφοντα (που είναι μέλος του L), το μαντείο υπογραφής υπογραφής επιστρέφει μία έγκυρη υπογραφή. Με τον όρο έγκυρη εννοούμε πως το μαντείο χρησιμοποιεί τον αλγόριθμο Sign, έχοντας την αντιστοιχία μεταξύ $\mathsf{sk}_\pi - \mathsf{pk}_\pi$.

  $\sigma \leftarrow \mathcal{SO}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pk}_\pi)$.

- Μαντείο Προσομοίωσης (Simulation Oracle - $\mathcal{MO}$): Με είσοδο ένα δακτυλίο L, ένα μήνυμα $\mathtt{m}$, ένα δημόσιο κλειδί DV pk_D και pid επιστρέφει την προσομοίωση που προκύπτει από τον αλγόριθμο Sim με αυτές της εισόδους, το αντίστοικο μυστικό κλειδί sk_D είναι αυτό που αντιστοιχεί στο επιλεγμένο pk_D.

  $\sigma \leftarrow \mathcal{MO}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pid})$.

Ο $\mathcal{A}$ έχει επίσης πρόσβαση στις συναρτήσεις σύνοψης που χρησιμοποιεί το σύστημα. Επειδή οι αποδείξεις γίνονται στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$, θεωρούμε πως οι συναρτήσεις αυτές μοντελοποιούνται από το $\mathcal{RO}$. Επιπλέον οποιαδήποτε κλήση σε συνάρτηση τυχαίας επιλογής μοντελοποιείται επίσης με κλήση στο $\mathcal{RO}$.

Είναι σημαντικό να σημειώσουμε το εξής, τόσο στη μοντελοποίηση του αντιπάλου στο DVLRS όσο και στο UDVLRS θεωρούμε πως ο αντίπαλος έχει πρόσβαση μόνο στα δεδομένα του συστήματος. Δηλαδή ο αντίπαλος δε βλέπει καθόλου τις διευθήνσεις IP που στέλνουν τις υπογραφές, δεν αναλύει την κίνηση στο δίκτυο, δε μελετάει μεταδεδομένα των υπογραφών. Τέτοιες επιθέσεις μπορούν να σπάσουν την ανωνυμία του συστήματος με τετριμμένο τρόπο. Επιπλέον ο εκάστοτε καθορισμένος επαληθευτής ακολουθεί κάποια στρατηγική απόκρυψης και παραπλάνησης όταν προσομοιώνει και δημοσιεύει προσομοίωσεις, καθώς αν οι προσομοίωσεις που γίνονται δημόσιες έχουν συγκεκριμένη μορφή και μοτίβο θα είναι ευκολότερη η διακρισή τους από υπογραφές χρηστών.

Ας μελετήσουμε τώρα τις ιδιότητες ασφάλειας ενός σχήματος DVLRS.

Σημείωση: Για την καλύτερη κατανόηση του μοντέλου που προτείνεται από τους συγγραφείς του DVLRS συνστάται η μελέτη της εργασίας τους [13], στη ΔΕ θα κάνουμε μόνο αναφορά στους ορισμούς.

Μη-Πλαστογραφησιμότητα:

Πρώτη και βασική απαίτηση για την ασφάλεια στις υπογραφές οποιουδήποτε είδους είναι η μη-πλαστογραφησιμότητα, θα πρέπει να είναι εφικτό να μία γνήσια υπογραφή να προέρχεται μόνο από τον γνώστη ενός ιδιωτικού κλειδιού στο δακτύλιο ή το γνώστη του κλειδιού του επαληθευτή.

Πιο αυστηρά ο ορισμός της μη-πλαστογραφισημότητας βασίζεται στο ακόλουθο παιχνίδι 6.1

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(\sigma, L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, \mathsf{pk}_D, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{MO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(\mathcal{U})$
Επέστρεψε: $\mathsf{Vrfy}(\sigma, L, \mathtt{m}, \mathsf{pk}_D)$ **ΚΑΙ** σ δεν είναι είσοδος των $\mathcal{SO}, \mathcal{MO}$ **ΚΑΙ** $\forall i \in D_t : pk_i \notin D_t$ **ΚΑΙ** $D \notin D_t$

Ορισμός 6.3. *Μη-Πλαστογραφησιμότητα*
Ένα DVLRS σχήμα Π θα λέγεται ότι διαθέτει την ιδιότητα της μη-πλαστογραφισημότητας αν για κάθε PPT *αντίπαλο $\mathcal{A}$ ισχύει:*

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

Σημειώνουμε εδώ πως ο συγκεκριμένος ορισμός μη-πλαστογραφισημότητας βασίζεται στην ισχυρή ιδιότητα μη-πλαστογραφισημότητας με υποκλοπή κλειδιών [17] κατάλληλα προσαρμοσμένη για να την ύπαρξη του καθορισμένου επαληθευτή.

Ανωνυμία:

Η ανωνυμία αποτελεί την απαίτηση να μη μπορεί να βρει κανείς την ταυτότητα του δημιουργού μιας υπογραφής. Επειδή μιλάμε για μία υπογραφή δακτυλίου οι πιθανές επιλογές συντάκτη μειώνονται στα μέλη του δακτυλίου. Έτσι το καλύτερο που μπορούμε να κάνουμε είναι να περιορίσουμε τον αντίπαλο με τέτοιο τρόπο ώστε η στρατιγική του να του δίνει πιθανότητα επιτυχίας κοντά στη τυχαία επίλογη των μελών του δακτυλίου.

Εδώ πρέπει να σημειώσουμε πως το σχήμα DVLRS προστατεύει τους υπογράοντες ως προς την ανωνυμία όχι μόνο από άλλες οντότητες, όπως π.χ. άλλα μέλη του δακτυλίου ή τρίτα άτομα, αλλά και από τον ίδιο τον καθορισμένο επαληθευτή.

Παρακάτω παραθέτουμε το παιχνίδι 6.2 που περιγράφει το πείραμα για την ιδιότητα της ανωνυμίας.

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

Είσοδος: λ
Έξοδος: $\{0,1\}$
$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(\lambda)$
$\mathcal{U} \leftarrow \{(\mathsf{sk}_i, \mathsf{pk}_i) \leftarrow \Pi.\mathsf{KGen}()\}_{i=1}^{n}$
$(L = \{\mathsf{pk}_i\}_{i=1}^{n_L}, \mathtt{m}, \mathsf{pk}_D, D_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{MO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(\mathcal{U}, \textbf{επιλογή})$
$\pi \leftarrow \$[n_L]$
$\sigma \leftarrow \Pi.\mathsf{Sign}(L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$
$(\xi, D'_t) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{MO},\mathcal{CO},\mathcal{JO},\mathcal{SO}}(L, \mathtt{m}, \mathsf{pk}_D, \sigma, D_t, \textbf{εικασία})$
if $\pi \notin D'_t$ **then**
| **Επέστρεψε:** $\xi = \pi$

else
| **Επέστρεψε:** $\perp$
end

Ορισμός 6.4. *Ανωνυμία*

Ένα DVLRS σχήμα Π έχει την ιδιότητα της t-ανωνυμίας αν για κάθε PPT *αντίπαλο ισχύει ότι:*

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

Σημειώνουμε εδώ πως η ανωνυμία είναι υπολογιστική, μιας και ο αντίπαλος περιορίζεται σε PPT.

Συνδεσιμότητα

Η ιδιότητα της συνδεσιμότητας απαιτεί ο αλγόριθμος επιβεβαίωσης Vrfy να επιστρέφει 1 για δύο υπογραφές που προέρχονται από τον ίδιο δακτύλιο και τον ίδιο υπογράφοντα. Έτσι λοιπόν υπάρχει η απαίτηση κανένας να μη μπορεί, γνωρίζοντας μόνο ένα ιδιωτικό κλειδί, να παράξει δύο υπογραφές που να είναι ασύνδετες μεταξύ τους. Το DVLRS προσφέρει μια ακόμα πιο ισχυρή συνδεσιμότητα συγκεκριμένα αν κάποιος γνωρίζει k το πλήθος ιδιωτικά κλειδιά

τότε μπορεί να παράξει το πολύ k ασύνδετες μεταξύ τους υπογραφές. Αυτή η ισχυροποίηση του ορισμού οδηγεί και στην κάλυψη της ιδιότητας της μη-δυσφημισιμότητας. Σημειώνουμε εδώ πως το μοντέλο της συνδεσιμότητας είναι πιο σύνθετο απο αυτό των κλασσικών LRS, αφού έχει εισαχθεί και ο επαληθευτής.

Πιο τυπικά ορίζεται το παρακάτω πείραμα 6.3:

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

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

Ορισμός 6.5. *Συνδεσιμότητα*

Ένα DVLRS σχήμα Π *είναι συνδέσιμο αν για κάθε* PPT *αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

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

Μη-Μεταφερσιμότητα

Η ιδιότητα της μη-μεταφερσιμότητας διασφαλίζει ότι μία υπογαραφή δεν μπορεί να διακριθεί από μία προσομοίωση της ίδιας υπογαραφής. Η μη-μεταφερσιμότητα είναι αυτή η οποία δίνει τη χρησιμότητα στις υπογραφές καθορισμένου επαληθευτή, κανένας τρίτος δε μπορεί να καταλάβει αν μία υπογραφή που βλέπει είναι από κάποιο μέλος του δακτυλίου ή από τον καθορισμένο επαληθευτή ως αποτέλεσμα οι υπογραφές που παράγονται είναι χρήσιμες μόνο για τον καθορισμένο επαληθευτή.

Για να ορίσουμε αυστηρά τη μη-μεταφερσιμότητα χρησιμοποιούμε το παρακάτω πείραμα 6.4:

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

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

Ορισμός 6.6. *Μη-Μεταφερσιμότητα*
Ένα DVLRS σχήμα Π είναι τέλεια μη-μεταφέρσιμο αν για κάθε μη-φραγμένο αντίπαλο $\mathcal{A}$:

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

6.3 Κατασκευή Σχήματος DVLRS

Παρακάτω παραθέτουμε μία κατασκευή ενός σχήματος DVLRS όπως αυτή δίνεται στο [13].

6.3.1 Κατασκευή

Αρχικοποίηση

Ξεκινόντας εργαζόμαστε σε μία ομάδα $\mathbb{G}$ τάξης πρώτου q, με γεννήτορα g στην οποία θεωρούμε πως ισχύει η υπόθεση DDH.

Κάθε χρήστης του σχήματος, ανεξαρτήτως αν ενεργεί ως υπογράφοντας ή ως καθορισμένος επαληθευτής, δημιουργεί ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού $(\mathsf{sk}, \mathsf{pk})$. Για το ιδιωτικό κλειδί sk ισχύει: $\mathsf{sk} = x, x \in_R \mathbb{Z}_q$, ενώ για το δημόσιο κλειδί pk ισχύει $\mathsf{pk} = y = g^x \in \mathbb{G}$. Επιπλέον στοιχεία της ομάδας $\mathbb{G}$ είναι και τα ψευδώνυμα $\mathsf{pid} = \hat{y}$ του κάθε χρήστη.

Τα μηνύματα $\mathtt{m}$ δύναται να είναι οποιαδήποτε δυαδική ακολουθία, $\mathtt{m} \in \{0,1\}^*$.

Για τους αλγόριθμους του σχήματος χρειάζονται επιπλέον δύο συναρτήσεις σύνοψης $\mathcal{H}_\mathbb{G}, \mathcal{H}_q$, με πεδίο ορισμού οποιαδήποτε δυαδική ακολουθία και εικόνα τη $\mathbb{G}$ και το $\mathbb{Z}_q$ αντίστοιχα.

Υπογραφή

Για να δημιουργήσει την υπογραφή ένας υπογράφοντας με ζεύγος κλειδιών (x_π, y_π) για μήνυμα $\mathtt{m}$ επιλέγει δακτύλιο δημοσιών κλειδιών y_i $L = \{y_i\}_{i=1}^{n_L}$ και το δημόσιο κλειδί του επαληθευτή που επιθυμεί y_D, με περιορισμό $y \notin L$. Με π συμβολίζουμε το δείκτη του κλειδιού του υπογράφοντα στο δακτύλιο L.

Ο αλγόριθμος δημιουργίας υπογραφής $\mathsf{Sign}(L, \mathtt{m}, y_D, x_\pi)$ είναι :

1. $h \leftarrow \mathcal{H}_{\mathbb{G}}(L)$
2. $\hat{y} \leftarrow h^{x_\pi}$
3. $u, w_\pi, r_\pi \leftarrow \$\mathbb{Z}_q$
4. $c_{\pi+1} \leftarrow \mathcal{H}_q(L, \hat{y}, y_D, g^u, h^u, g^{w_\pi} y_D^{r_\pi}, \mathtt{m})$
5. Για $i \in \{\pi+1, \ldots, n_L, 1, \ldots, \pi-1\}$:

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

Για να προσομοιώσει μία υπογραφή ο επαληθευτής χρησιμοποιεί το ζεύγος κλειδιών του (x_D, y_D), ένα μήνυμα της αρεσκείας του $\mathtt{m}$, το δακτύλιο $L = \{y_i\}_{i=1}^{n_L}$ με περιορισμό $y_D \notin L$ και το ψευδώνυμο $\hat{y}$ στο οποίο επιθυμεί να ανταποκρίνεται η προσομοίωση.

Ο αλγόριθμος δημιουργίας προσομοίωσης $\mathsf{Sim}(L, \mathtt{m}, y_D, x_D, \hat{y})$ είναι :

1. $h \leftarrow \mathcal{H}_{\mathbb{G}}(L)$
2. $\alpha, \beta, s_1 \leftarrow \$\mathbb{Z}_q$
3. $c_2 \leftarrow \mathcal{H}_q(L, \hat{y}, y_D, g^{s_1} y_1^{\beta}, h^{s_1} \hat{y}^{\beta}, g^{\alpha}, \mathtt{m})$
4. Για $i \in \{2, \ldots, n_L\}$:

   $s_i, w_i, r_i \leftarrow \$\mathbb{Z}_q$
   $c_{i+1} \leftarrow \mathcal{H}_q(L, \hat{y}, y_D, g^{s_i} y_i^{c_i+w_i}, h^{s_i} \hat{y}^{c_i+w_i}, g^{w_i} y_D^{r_i}, \mathtt{m})$
5. $w_1 \leftarrow \beta - s_1$ και $r_1 \leftarrow (\alpha - w_1) x_D^{-1}$
6. **Επέστρεψε:** $\sigma \leftarrow (c_1, \{s_i\}_{i=1}^{n_L}, \{w_i\}_{i=1}^{n_L}, \{r_i\}_{i=1}^{n_L}, \hat{y})$

Επαλήθευση

Όταν κάποιος θέλει να επληθεύσει μία υπογραφή σ εισάγει στον αλγόριθμο υπογραφής την υπογραφή σ, το δακτύλιο L, το μήνυμα $\mathtt{m}$ και το δημόσιο κλειδί του καθορισμένου επαληθευτή y_D.

Ο αλγόριθμος επαλήθευσης $\mathsf{Vrfy}(\sigma, L, \mathtt{m}, y_D)$ είναι:

1. $h \leftarrow \mathcal{H}_{\mathbb{G}}(L)$
2. Για $i \in [n_L]$

$$
\begin{aligned}
z_i' &= g^{s_i} y_i^{c_i + w_i} \\
z_i'' &= h^{s_i} \hat{y}^{c_i + w_i} \\
z_i''' &= g^{w_i} y_D^{r_i} \\
c_{i+1} &= \mathcal{H}_q(L, \hat{y}, z_i', z_i'', z_i''', \mathtt{m})
\end{aligned}
$$

3. **Επέστρεψε:** $c_1 = \mathcal{H}_q(L, \hat{y}, z_n', z_n'', z_n''', \mathtt{m})$

Εξαγωγή

Ο αλγόριθμος εξαγωγής $\mathsf{Extract}$ επιστρέφει το ψευδώνυμο $\hat{y}$ της υπογραφής. Παρατηρούμε πως οι υπογραφές του σχήματος αποτελούν πλειάδες στοιχείων με το τελευταίο να είναι το $\hat{y}$. Επομένως ο αλγόριθμος αρκεί απλά το επιστρέφει το τελευταίο στοιχείο της υπογραφής.

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

Σύνδεση

Ο αλγόριθμος σύνδεσης Link με είσοδο δύο έγκυρες υπογραφές σ_1, σ_2 και δακτύλιο L επιστρέφει 1 αν και μόνο αν :

$$\mathsf{Extract}(\sigma_1) = \mathsf{Extract}(\sigma_2)$$

6.3.2 Ορθότητα και Πληρότητα Κατασκευής

Σε αυτό το σημείο θα δείξουμε πως στην εν λόγω κατασκευή οι έγκυρες υπογραφές και προσομοιώσεις επιβεβαιώνουν επιτυχώς και ότι ισχύει η ορθότητα σύνδεσης.

Λήμμα 6.1. *Μία τίμια κατασκευασμένη υπογραφή DVLRS είναι έγκυρη.*

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

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

□

Λήμμα 6.2. *Μία τίμια κατασκευασμένη προσομοίωση DVLRS 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 $z'''_1 = g^\alpha$. Πράγματι:

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

□

Λήμμα 6.3. *Η παραπάνω DVLRS κατασκευή διαθέτει ορθότητα σύνδεσης.*

Απόδειξη: Θα δείξουμε ότι ο αλγόριθμος επιβεβαίωσης επιστρέφει 1 και στις 3 περιπτώσεις που αναφέρουμε στον ορισμό 6.2.

Έστω λοιπόν 2 έγκυρες υπογραφές/προσομοίωσεις σ, σ'.

Περίπτωση:1 Αν και οι δύο υπογραφές είναι υπογεγραμμένες από τον ίδιο υπογράφοντα τότε εύκολα βλέπουμε ότι $\mathsf{Extract}(\sigma) = \hat{y} = \mathsf{Extract}(\sigma')$.

Περίπτωση:2 Αν η σ είναι έγκυρη υπογραφή από τον υπογράφοντα με ψευδώνυμο $\hat{y}$ και η σ' είναι προσομοίωση με το ίδιο ψευδώνυμο τότε βλέπουμε πως $\mathsf{Extract}(\sigma) = \hat{y} = \mathsf{Extract}(\sigma')$.

Περίπτωση:3 Αν και η σ και η σ' είναι προσομοιώσεις για το ίδιο ψευδώνυμο $\hat{y}$ τότε προφανώς $\mathsf{Extract}(\sigma) = \mathsf{Extract}(\sigma') = \hat{y}$. □

6.3.3 Ανάλυση Ασφάλειας Κατασκευής

Παρακάτω παραθέτουμε τα θεωρήματα που δείχνουν την ασφάλεια της συγκεκριμένης κατασκευής στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$. Για τις αποδείξεις των παρακάτω θεωρημάτων παραπέμπουμε στην εργασία [13].

Μη-Πλαστογραφησιμότητα

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

Ανωνυμία

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

Συνδεσιμότητα

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

Μη-Μεταφερσιμότητα

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

Κεφάλαιο 7

Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή με Άνευ Όρων Ανωνυμία

Το 7ο κεφάλαιο περιέχει την κύρια συνεισφορά της συγκεκριμένης διπλώματικής εργασίας. Θα δούμε πως μπορούμε να συνδυάσουμε τις Συνδέσιμες Υπογραφές Δακτυλίου Καθορισμένου Επαληθευτή (DVLRS) [13] που είδαμε στο κεφάλαιο 6 με τις Συνδέσιμες Υπογραφές Δακτυλίου με Τέλεια, ή αλλιώς άνευ όρων, Ανωνυμία (ULRS) [56] που μελετήσμαε στο κεφάλαιο 5. Το προϊόν αυτό του συνδυασμού το καλούμε Συνδέσιμες Υπογραφές Δακτυλίου με Άνευ Όρων Ανωνυμία (Designated Verifier Linkable Ring Signatures with Uncondtional Anonymity - UDVLRS) και αποτελεί λύση σε ένα από τα ανοιχτά προβλήματα που είχαν τεθεί στο [13]. Η συγκεκριμένη δουλεία είναι αποτέλεσμα συνεργασίας των Behrouz, Βρεττός, Γροντάς, Μπάλλα, Παγουρτζή και Σπυράκου (Balla, Behrouz, Grontas, Pagourtzis, Spyrakou, Vrettos), παρουσιάστηκε στο 9ο International Conference on Algebraic Informatics (CAI 2022) και δημοσιεύτηκε από τις εκδόσεις Springer στο Lecture Notes in Computer Science [11]. Για τυχόν ενδιαφερόμενους μπορεί επίσης να βρεθεί στο archive του International Association for Cryptologic Research (IACR) [10].

Θα παρουσίασουμε το μοντέλο των UDVLRS, τις ιδιότητες και ορισμούς ασφαλείας καθώς και μία κατασκευή για την οποία δείχνουμε πως είναι ασφαλής στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$.

7.1 Προκαταρκτικά

7.1.1 Συμβολισμός

Θα ξεκινήσουμε με ορισμένες συμφωνίες που θα ισχύουν για το συμβολισμό που θα ακολουθήσει αυτό το κεφάλαιο. Για αρχή θεωρούμε πως όλα τα πειράματα ασφάλειας διαδραματίζονται μεταξύ ενός προκαλούντα $\mathcal{C}$ και ενός αντιπάλου $\mathcal{A}$. Τα πειράματα έχουν πάντα ως είσοδο την παράμετρο ασφαλείας λ και επιστρέφουν την αληθοτιμή της συνθήκης με την οποία ο $\mathcal{A}$ κερδίζει το παιχνίδι, για απλότητα απλά επιστρέφουμε την συνθήκη. Ορισμένες φορές τιμές που είναι άνευ σημασίας στο πλαίσιο στο οποίο γίνεται αναφορά θα συμβολίζονται με '$\cdot$'. Επιπλέον θεωρούμε πως ο $\mathcal{A}$ έχει μία κατάσταση την οποία παραλείπουμε αλλά διατηρείται σε όλες τις διαδοχικές ενέργειες που εκτελεί. Οι κρυπτογραφικές παράμετροι τις κατασκευής συμβολίζονται ως params. Είναι απαραίτητες είσοδοι για όλους τους αλγορίθμους του σχήματος, αλλά δε τις συμπεριλαμβάνουμε για απλότητα. Όπως έχει ήδη γίνει και σε όλη την έκταση της παρούσας ΔΕ με sk συμβολίζουμε τα ιδιωτικά κλειδιά και με pk τα δημόσια κλειδιά. Η ψευδοταυτότητα που εμφανίζεται στις υπογραφές συμβολίζεται με pid, ενώ χώρος όλων των πιθανών ψευδοταυτήτων συμβολίζεται με $\mathcal{PID}$. Για τη σύνδεση όπως και στους [56] χρησιμοποιείται ένα κοινό string ev το οποίο προέρχεται από το σύνολο όλων των πιθανών ev string $\mathcal{EID}$. Όπως έχουμε ήδη δει ο δείκτης του καθορισμένου επαληθευτή είναι D, ενώ του υπογράφοντα είναι π. Οι περισσότεροι αλγόριθμοι που παρουσιάζονται έχουν ως κοινή είσοδο τις τιμές $\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D$, που συμβολίζουν αντίστοιχα ένα συμβάν, ένα δακτύλιο, ένα μήνυμα, και το δημόσιο κλειδί του καθορισμένου επαληθευτή. Θα αναφερόμαστε σε αυτές τις τέσσερις τιμές ως παράμετροι της υπογραφής.

7.1.2 Υποθέσεις Ασφάλειας

Ορισμένες ιδιότητες ασφάλειας της κατασκευής που θα παραθέσουμε βασίζονται σε μια παραλλαγή του Πρόβληματος του Διακριτού Λογαρίθμου (DLOG) που είναι πιο βολικό στη χρήση. Πρώτη φορά ορίστηκε στην [56] και χρησιμοποιείτω ως ένα υπολογιστικά ισοδύναμο πρόβλημα με το DLOG. Ένα παρόμοι πρόβλημα είχε προταθεί από τους [3] ως το Πρόβλημα Σχέσης Διακριτών Λογαρίθμων. Στην εργασίας μας χρησιμοποιούμε την εκδοχή των [56] την οποία επανεισάγουμε ως το Τροποποιημένο Πρόβλημα Σχέσης Διακριτού Λογαρίθμου (Modified Discrete Logarithm Relation - MDLR):

Ορισμός 7.1. *Modified Discrete Logarithm Relation - MDLR*

Έστω $\mathbb{G}$ μία κυκλική ομάδα τάξης πρώτου q, g κάποιος γεννητοράς της και $Y_1, Y_2, \ldots, Y_n \leftarrow\!\!\$\ \mathbb{G}, Y_1 \neq 1_{\mathbb{G}}$. Μία λύση στο MDLR είναι μία n-αδα

$(\phi_1, \phi_2, \ldots, \phi_n) \in \mathbb{Z}_q^n$ *έτσι ώστε* $Y_1 \cdot Y_2^{\phi_2} \cdots Y_n^{\phi_n} = g^{\phi_1}$ *και* $\sum_{i=1}^n \phi_i \neq 0 \pmod q$.

Παρατηρούμε πως για $n = 1$, το MDLR είναι το απλό DLOG.

Θεώρημα 7.1. *Το* DLOG *είναι υπολογιστικά ισοδύναμο με το MDLR*

Απόδειξη. Υποθέτοντας ένα μαντείο DLOG *και ένα στιγμυότυπο MDLR* $Y_1, Y_2, \ldots Y_n$ *υπολόγισε* $x_1, x_2, \ldots x_n$ *έτσι ώστε* $Y_i = g^{x_i}, i \in [n]$. *Επέλεξε* $\{\phi_i \in \mathbb{Z}_q\}_{i=2}^n$ *και θέσε* $\phi_1 \leftarrow x_1 + \sum_{i=2}^n \phi_i x_i \mod q$. *Στο σενάριο (με αμελητέα πιθανότητα) που* $\sum_{i=1}^n \phi_i = 0 \pmod q$ *επανέλαβε τη διαδικασία. Είναι προφανές ότι,* $g^{\phi_1} = g^{x_1 + \sum_{i=2}^n \phi_i x_i} = Y_1 \cdot Y_2^{\phi_2} \cdots Y_n^{\phi_n}$.

Υποθέτοντας ένα μαντείο MDLR και ένα στιγμυότυπο DLOG $Y = g^x$, *επέλεξε* $x_2, \ldots, x_n$ *και υπολόγισε* $\{Y_i \leftarrow g^{x_i}\}_{i=2}^n$. *Κάνοντας κλήσεις στο MDLR μαντείο με* $Y, Y_2, \ldots Y_n$ *λαμβάνεις* $\phi_1, \phi_2, \ldots, \phi_n \in \mathbb{Z}_q$ *τέτοια ώστε* $Y \cdot Y_2^{\phi_2} \cdots Y_n^{\phi_n} = g^{\phi_1}$ *και* $\sum_{i=1}^n \phi_i \neq 0 \pmod q$. *Επομένως* $Y = g^{\phi_1 - \sum_{i=2}^n \phi_i x_i}$ *ο διακριτός λογάριθμος του* Y *είναι* $x = \phi_1 - \sum_{i=2}^n \phi_i x_i \pmod q$. □

7.2 Ορισμός και Μοντέλο Ασφάλειας UDVLRS

7.2.1 Ορισμός UDVLRS

Όπως είναι ίσως αναμενώμενο ο ορισμός των UDVLRS είναι ένας συνδυασμός των [13, 56]

Ορισμός 7.2. *Ένα σχήμα Συνδέσιμων Υπογραφών Δακτυλίου Καθορισμένου Επαληθευτή με Άνευ Όρων Ανωνυμία (UDVLRS)* Π *είναι μια συλλογή* PPT 7 *αλγορίθμων* $\Pi = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Sign}, \mathsf{Extract}, \mathsf{Sim}, \mathsf{Vrfy}, \mathsf{Link})$ *με την ακόλουθη σύνταξη:*

- ***Αλγόριθμος Εγκατάστασης*** - $\mathsf{Setup}(1^\lambda)$*:*

  Ο αλγόριθμος Setup *με είσοδο την παράμετρο ασφαλείας* λ *κατασκευάζει τις παραμέτρους του σχήματος UDVLRS. Σε αυτές συμπεριλαμβάνονται οι κρυπτογραφικές ομάδες, ο χώρος μηνυμάτων* $\mathcal{MSG}$*, ο χώρος των υπογραφών* $\mathcal{SG}$*, ο χώρος όλων των δυνατών* pid $\mathcal{PID}$ *και ο χώρος όλων των δυνατών* ev $\mathcal{EID}$*.*

  Καλούμε $\mathsf{params} \leftarrow \mathsf{Setup}(1^\lambda)$.

- ***Δημιουργία Κλειδιών*** - $\mathsf{KGen}()$*:*

  Κάθε χρήστης επικαλείται τον αλγόριθμο KGen *ώστε να λάβει το ζεύγος κλειδιών του* $(\mathsf{sk}, \mathsf{pk})$*. Τα κλειδιά δημιουργούνται κατά βούληση από τον εκάστοτε χρήστη.*

  Καλούμε $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}()$*.*

- ***Δημιουργία Υπογραφής*** - $\mathsf{Sign}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$*:*

  Για να υπογράψει ένα μέλος του δακτυλίου L *ένα μήνυμα* $\mathtt{m}$ *επικαλείται τον αλγόριθμο* Sign *και χρησιμοποιεί για είσοδο το κοινό string* $\mathtt{ev}$*, τον δακτύλιο* L*, το μήνυμα* $\mathtt{m}$*, το δημόσιο κλειδί του designated verifier* pk_D*, και το ιδιωτικό του κλειδί* sk_π*, όπου* π *είναι ο δείκτης του συγκεκριμένου υπογράφοντα στο δακτύλιο* L*.*

  Καλούμε $\sigma \leftarrow \mathsf{Sign}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$*.*

- ***Εξαγωγή*** - $\mathsf{Extract}(\sigma)$*:*

  Ο αλγόριθμος Extract *με είσοδο μία υπογραφή* σ *εξάγει το* pid *της υπογραφής. Είναι δημόσια εκτελέσιμος.*

  Καλούμε $\mathsf{pid} \leftarrow \mathsf{Extract}(\sigma)$*.*

- ***Δημιουργία Προσομοίωσης*** - $\mathsf{Sim}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$*:*

  Ο designated verifier επικαλείται τον αλγόριθμο Sim *όταν θέλει να προσομοιώσει μία υπογραφή. Για είσοδο δίνει το κοινό string* $\mathtt{ev}$*, το δακτύλιο* L*, το μήνυμα* $\mathtt{m}$*, το ζεύγος κλειδιών του* $(\mathsf{sk}_D, \mathsf{pk}_D)$*, και το* pid *του υπογράφοντα στον οποίο θα συνδεθεί η προσομοίωση που θα παραχθεί.*

  Καλούμε $\sigma \leftarrow Sim(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$*.*

- ***Επαλήθευση*** - $\mathsf{Vrfy}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma)$*:*

  Ο δημόσιος αλγόριθμος επαλήθευσης επιστρέφει 1 *αν η υπογραφή* σ *είναι έγκυρη, αλλίως επιστρέφει* 0*.*

  Καλούμε $\{0,1\} \leftarrow \mathsf{Vrfy}(\mathtt{ev}, L, \mathtt{m}, pk_D, \sigma)$*.*

- ***Σύνδεση*** - $\mathsf{Link}(\sigma_1, \mathtt{ev}_1, \sigma_2, \mathtt{ev}_2)$*:*

  Με την κλήση του δημόσιου αλγορίθμου σύνδεσης ελέγχεται εάν δύο υπογραφές σ_1, σ_2 *είναι συνδεδεμένες ή όχι. Ο αλγόριθμος επιστρέφει* 1 *εάν είναι συνδεδεμένες, αλλιώς επιστρέφει* 0*.*

  Καλούμε $\{0,1\} \leftarrow \mathsf{Link}(\sigma_1, \mathtt{ev}_1, \sigma_2, \mathtt{ev}_2)$*.*

Όπως και στις DVLRS έτσι και εδώ πρέπει να σημειώσουμε ότι για να μπορέσει να κατασκευάσει μία προσομοίωση ο καθορισμένος επαληθευτής πρέπει πρώτα να δει το ψευδώνυμο pid για το οποίο θέλει να προσομοιώσει υπογραφή. Αυτό δεν είναι απαραίτητα περιοριστικό αφού με το που εισέρχεται κάποιος στο σύστημα που χρησιμοποιεί τις UDVLRS μπορεί να στέλνει ένα μήνυμα, και έτσι ο καθορισμένος επαληθευτής θα μπορεί να δει το ψευδώνυμο.

7.2.2 Ορθότητα UDVLRS

Η πληρότητα (completness) του σχήματος που παραθέσαμε παρπάνω προκύπτει από δύο ιδότητες: την *ορθότητα επαλήθευσης (verification correctness)* και την *ορθότητα σύνδεσης (linking correctness)*.

Ορθότητα Επαλήθευσης. Μία υπογραφή ή προσομοίωση, για δεδομένο $\mathtt{ev}$, δακτύλιο, μήνυμα και καθορισμένο επαληθευτή είναι έγκυρη αν και μόνο αν ήταν τίμια κατασευασμένη (δηλαδή $\mathsf{Vrfy}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma) = 1 \Leftrightarrow \sigma = \mathsf{Sign}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi), \mathsf{pk}_\pi \in L$ ή $\sigma = \mathsf{Sim}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid}), (\mathsf{sk}_D, \mathsf{pk}_D) = \mathsf{KGen}(), \mathsf{pid} \in \mathcal{PID}$).

Ορθότητα Σύνδεσης. Δύο έγκυρες υπογραφές σ_1, σ_2 είναι συνδεδεμένες, $(\mathsf{Link}(\sigma_1, \mathtt{ev}_1, \sigma_2, \mathtt{ev}_2) = 1)$, αν και μόνο αν $\mathtt{ev}_1 = \mathtt{ev}_2$ και ισχύει μία από τις ακόλουθες συνθήκες:

1. $\sigma_1 = \mathsf{Sign}(\mathtt{ev}_1, L_1, \mathtt{m}_1, \mathsf{pk}_{D_1}, \mathsf{sk}_\pi), \mathsf{pk}_\pi \in L_1$ and $\sigma_2 = \mathsf{Sign}(\mathtt{ev}_2, L_2, \mathtt{m}_2, \mathsf{pk}_{D_2}, \mathsf{sk}_\pi), \mathsf{pk}_\pi \in L_2$. Και οι δύο υπογραφές είναι τίμια κατασκευασμένες από τον ίδιο υπογράφοντα π.

2. $\sigma_1 = \mathsf{Sign}(\mathtt{ev}_1, L_1, \mathtt{m}_1, \mathsf{pk}_{D_1}, \mathsf{sk}_\pi), \sigma_2 = \mathsf{Sim}(\mathtt{ev}_2, L_2, \mathtt{m}_2, \mathsf{pk}_{D_2}, \mathsf{sk}_{D_2}, \mathsf{Extract}(\sigma_1)), \mathsf{pk}_\pi \in L_1$, $(\mathsf{sk}_{D_2}, \mathsf{pk}_{D_2}) \leftarrow \mathsf{KGen}()$. σ_1 είναι τίμια κατασευασμένη από τον υπογράφοντα π και σ_2 είναι τίμια προσομοιωμένη από τον καθορισμένο επαληθευτή D_2 χρησιμοποιώντας το ψευδώνυμο που έχει εξαχθεί από τη σ_1.

3. $\sigma_1 = \mathsf{Sim}(\mathtt{ev}_1, L_1, \mathtt{m}_1, \mathsf{pk}_{D_1}, \mathsf{sk}_{D_1}, \mathsf{pid}), (\mathsf{sk}_{D_1}, \mathsf{pk}_{D_1}) = \mathsf{KGen}(), \mathsf{pid} \in \mathcal{PID}$ and $\sigma_2 = \mathsf{Sim}(\mathtt{ev}_2, L_2, \mathtt{m}_2, \mathsf{pk}_{D_2}, \mathsf{sk}_{D_2}, \mathsf{pid}), (\mathsf{sk}_{D_2}, \mathsf{pk}_{D_2}) = \mathsf{KGen}()$. σ_1, σ_2 είναι και οι δύο προσομοιώσεις από τους καθορισμένους επαληθευτές D_1, D_2 χρησιμοποιώντας το ίδιο pid.

7.2.3 Δυνατότητες Αντιπάλου

Οι δυνατότητες που έχει ο αντίπαλος $\mathcal{A}$ είναι πανομοιότυπες με αυτές του αντιπάλου στο μοντέλο των DVLRS, με μία μικρή διαφορά στο μαντείο διαφθοράς $\mathcal{CO}$. Πιο αναλυτικά έχουμε:

Θεωρούμε έναν ισχυρό προσαρμοστικό αντίπαλο $\mathcal{A}$, που έχει τη δυνατότητα να προσθέτει νέους χρήστες στο σύστημα, να αποκτά τον έλεγχο χρηστών της επιλογής του, να μπορεί να συλλέξει όλες τις υπογραφές που έχουν συνταχθεί, και να ζητά υπογραφές και προσομοιώσεις για οποιονδήποτε χρήστη σε οποιονδήποτε δακτύλιο. Για τη μοντελοποίηση αυτών των δυνατοτήτων θα γίνει χρήση μαντείων [1], όπως γίνεται και στα [56, 55, 59].

- Μαντείο Εγγραφής (Joining Oracle - $\mathcal{JO}$): Με κλήση στο μαντείο εγγραφής προστίθεται ένα καινούργιο δημόσιο κλειδί pk στο σύνολο των δημόσιων κλειδιών $\mathcal{U}$.

  $\mathsf{pk} \leftarrow \mathcal{JO}()$.

- Μαντείο Διαφθοράς (Corruption Oracle - $\mathcal{CO}$): Έχοντας ως είσοδο ένα δημόσιο κλειδί $\mathsf{pk} \in \mathcal{U}$, το μαντείο διαφθοράς επιστρέφει το ιδιωτικό κλειδί sk που του αντιστοιχεί.[2]

  $\mathsf{sk} \leftarrow \mathcal{SO}(\mathsf{pk})$.

- Μαντείο Υπογραφής (Signing Oracle - $\mathcal{SO}$): Με είσοδο έναν δακτύλιο L, ένα μήνυμα $\mathtt{m}$, ένα δημόσιο κλειδί DV pk_D και το δημόσιο κλειδί pk_π του επιθυμητού υπογράφοντα (που είναι μέλος του L), το μαντείο υπογραφής υπογραφής επιστρέφει μία έγκυρη υπογραφή. Με τον όρο έγκυρη εννοούμε πως το μαντείο χρησιμοποιεί τον αλγόριθμο Sign, έχοντας την αντιστοιχία μεταξύ $\mathsf{sk}_\pi - \mathsf{pk}_\pi$.

  $\sigma \leftarrow \mathcal{SO}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pk}_\pi)$.

- Μαντείο Προσομοίωσης (Simulation Oracle - $\mathcal{MO}$): Με είσοδο ένα δακτύλιο L, ένα μήνυμα $\mathtt{m}$, ένα δημόσιο κλειδί DV pk_D και pid επιστρέφει την προσομοίωση που προκύπτει από τον αλγόριθμο Sim με αυτές της εισόδους, το αντίστοικο μυστικό κλειδί sk_D είναι αυτό που αντιστοιχεί στο επιλεγμένο pk_D.

  $\sigma \leftarrow \mathcal{MO}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{pid})$.

Ο $\mathcal{A}$ έχει επίσης πρόσβαση στις συναρτήσεις σύνοψης που χρησιμοποιεί το σύστημα. Επειδή οι αποδείξεις γίνονται στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$, θεωρούμε πως οι συναρτήσεις αυτές μοντελοποιούνται από το $\mathcal{RO}$. Επιπλέον

[1] Για λόγους ευκολίας το όνομα του μαντείου συμβολίζει τόσο το μαντείο ως αλγόριθμο όσο και το σύνολο στοιχείων το οποίο έχει ως έξοδο.

[2] Όπως θα εξηγήσουμε και στις ιδιότητες που έχει το σχήμα UDVLRS το μαντείο $\mathcal{CO}$ μοντελοποιεί γνώση ιδιωτικού κλειδιού, κάτι που όπως θα εξηγήσουμε είναι κάτι που ο $\mathcal{A}$ δε μπορεί να κάνει μόνος του λόγω της φύσης του σχήματος. Δηλαδή το μαντείο είναι γνησίως ισχυρότερο απο οποιονδήποτε αντίπαλο $\mathcal{A}$, ακόμα και από τους υπολογιστικά μη-φραγμένους.

οποιαδήποτε κλήση σε συνάρτηση τυχαίας επιλογής μοντελοποιείται επίσης με κλήση στο $\mathcal{RO}$.

Στις επόμενες υποενότητες θα αναλύσουμε τις ιδότητες ασφαλείας που πρέπει να διαθέτει ένα UDVLRS σχήμα και θα τις ορίσουμε αυστηρά μέσω των ανάλογων πειραμάτων ασφαλείας.

7.2.4 Μη-Πλαστογραφισημότητα

Ο ορισμός της μη-πλαστογραφισημότητας είναι παρόμοιως με αυτόν που συναντάμε στο κεφάλαιο 6. Για να θεωρήσουμε ένα UDVLRS σχήμα Π μη-πλαστογραφίσημο θα πρέπει να είναι εφικτό μόνο για μέλη του δακτυλίου ή τον καθορισμένο επαληθευτή να μπορούν να παράξουν υπογραφές και προσομοιώσεις που επιβεβαιώνουν επιτυχώς. Για να ορίσουμε τη μη-πλαστογραφισημότητα θα χρησιμοποιήσουμε το ακόλουθω πείραμα 7.1. Στο πείραμα ο αντίπαλος $\mathcal{A}$ επιτρέπεται να ρωτήσει τα μαντεία με οποιαδήποτε προσαρμοστική στρατηγική. Έπειτα επιλέγει τις παραμέτρους της υπογραφής και του ζητείται να παράξια μία πλαστογραφία σ^*. Ο αντίπαλος κερδίζει αν η πλαστογραφία που έχει παράξει επιβεβαιώνει κανονικά, κανένα από τα κλειδιά του δακτυλίου L ή το pk_D δεν έχουν χρησιμοποιηθεί ως είσοδοι στο μαντείο $\mathcal{CO}$ και η πλαστογραφία δεν αποτελεί έξοδο των $\mathcal{SO}$ ή $\mathcal{MO}$.

Παιχνίδι 7.1: Πείραμα Μη-Πλαστογραφισημότητας $\mathsf{Exp}^{\mathrm{unf}}_{\mathcal{A},\Pi}$

$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$
$\mathcal{U} \leftarrow \left\{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\right\}_{i=1}^{\mu(\lambda)}$
$(\sigma^*, \mathtt{ev}, L = \{\mathsf{pk}_i\}_{i=1}^n, \mathtt{m}, \mathsf{pk}_D) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
Επέστρεψε
$\mathsf{Vrfy}(\mathtt{ev}, \sigma, L, \mathtt{m}, \mathsf{pk}_D) = 1$ **ΚΑΙ** $\forall i \in \mathcal{CO},\ \mathsf{pk}_i \notin L$ **ΚΑΙ** $D \notin \mathcal{CO}$ **ΚΑΙ**
$\sigma^* \notin \mathcal{SO}$ **ΚΑΙ** $\sigma^* \notin \mathcal{MO}$

Ορισμός 7.3. *Μη-Πλαστογραφισημότητα*

Ένα UDVLRS σχήμα Π *θα είναι μη-πλαστογραφίσημο αν για κάθε* PPT $\mathcal{A}$ *ισχύει ότι:*

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

7.2.5 Ανωνυμία

Η ανωνυμία των UDVLRS είναι άνευ όρων ή αλλιώς τέλεια (unconditional), δηλαδή δε βασίζεται σε κάποια υπόθεση υπολογιστικής δυσκολίας ενός προβλήματος. Όπως είδαμε και στο κεφάλαιο 5 για να έχει ένα σχήμα υπογραφών δακτυλίου τέλεια ανωνυμία θα πρέπει να είναι αδύνατο για έναν αντίπαλο $\mathcal{A}$

να βρει ποιο είναι το δημόσιο κλειδί του υπογράφοντα μίας συγκεκριμένης υπογραφής για ένα δακτύλιο L με πιθανότητα καλύτερη της τυχαίας επιλογής.

Τυπικά ορίζουμε την άνευ όρων ανωνυμία για ένα σχήμα UDVLRS μέσω του πειράματος 7.2 μεταξύ ενός αντιπάλου $\mathcal{A}$ και ενός προκαλούντα $\mathcal{C}$. Ο αντίπαλο μπορεί να ρώτησει τα μαντεία $\mathcal{JO}, \mathcal{CO}, \mathcal{SO}, \mathcal{MO}$ με βάση οποιαδήποτε προσαρμοστική στρατηγική, επιλέγει το pk_D, και σχηματίζει το δακτύλιο L με οποιοδήποτε σύνολο n κλειδιών. Το μαντείο προσομοιώσεων $\mathcal{MO}$ δε προσφέρει κάποιο πλεονέκτημα στον $\mathcal{A}$ που δε του δίνει το $\mathcal{SO}$, μιας και οι προσομοιώσεις δεν κατασκευάζονται με κάποιο κλειδί από τον δακτύλιο. Υποθέτουμε πως μέσω κλήσεων στο $\mathcal{CO}$ ο $\mathcal{A}$ έχει στη κατοχή του m_1 ιδιωτικά κλειδιά. Μέσω της ψευδοταυτότητας των υπογραφών και της απεριόριστης υπολογιστικής του ισχύος ο $\mathcal{A}$ μπορεί να βρει άλλα m_2 ιδιωτικά κλειδιά μέσω υπογραφών που λαμβάνει από το $\mathcal{SO}$, όπου ο υπογράφοντας είναι γνωστός. Ο $\mathcal{A}$ έχει το δικαίωμα να συμπεριλάβει αυτά τα δημόσια κλειδιά που έχει "σπάσει" στο δακτύλιο L, όμως πρέπει να ισχύει $n > m_1 + m_2 + 1$. Ο $\mathcal{A}$ δίνει στον $\mathcal{C}$ ένα event $\mathtt{ev}$, ένα μήνυμα $\mathtt{m}$, το σύνολο των δημοσίων κλειδιών που απαρτίζουν το δακτύλιο L και το δημόσιο κλειδί του καθορισμένου επαληθευτή pk_D. Ο $\mathcal{C}$ επιλέγει στη τύχη π, $\pi \leftarrow\!\!\$\ [n]$, και κατασκευάζει μία υπογραφή-πρόκληση $\sigma_c = (\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$ την οποία και δίνει στον $\mathcal{A}$, ο οποίος τώρα πρέπει να μαντέψει το π. Ο $\mathcal{A}$ κερδίζει το παιχνίδι αν μαντέψει σωστά τον υπογράφοντα και το ιδιωτικό του κλειδί δεν έχει αποκτηθεί μέσω του $\mathcal{CO}$ ή του $\mathcal{SO}$.

Παιχνίδι 7.2: Πείραμα Ανωνυμίας $\mathsf{Exp}^{\mathrm{anon}}_{\mathcal{A},\Pi}$

$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$
$\mathcal{U} \leftarrow \left\{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\right\}_{i=1}^{\mu(\lambda)}$
$(\mathtt{ev}, L = \{\mathsf{pk}_i\}_{i=1}^{n}, \mathtt{m}, \mathsf{pk}_D) \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
$\pi \leftarrow\!\!\$\ [n]$
$\sigma_c \leftarrow \Pi.\mathsf{Sign}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$
$\xi \leftarrow \mathcal{A}^{\mathcal{CO},\mathcal{SO},\mathcal{MO}}(L, \mathtt{m}, \sigma_c)$
Επέστρεψε $\xi \neq \perp$ **ΚΑΙ** $\xi = \pi$ **ΚΑΙ** $\pi \notin \mathcal{CO}$ **ΚΑΙ** π δεν αποκτήθηκε από $\sigma \in \mathcal{SO}$

Ορισμός 7.4. *Ανωνυμία*

Ένα UDVLRS σχήμα Π *είναι τέλεια ανώνυμο αν για κάθε μη-φραγμένο αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

$$Adv_A^{anon}(\lambda) = |Pr[\mathsf{Exp}^{anon}_{\mathcal{A},\Pi}(\lambda) = 1] - \frac{1}{n - m_1 - m_2}| = 0$$

7.2.6 Μη-Μεταφερσιμότητα

Όπως έχουμε ήδη δει στα κεφάλαια 4 & 6 η ιδιότητα της μη-μεταφερσιμότητας διασφαλίζει τη μη-διαχώριση από τρίτα άτομα (εξαιρώντας τον υπογράφοντα και τον καθορισμένο επαληθευτή) των γνήσιων υπογραφών και των γνήσιων προσομοιώσεων.

Ο αυστηρός ορισμός δίνεται μέσω του παιχνιδιού 7.3 . Θεωρούμε πως ο αντίπαλος $\mathcal{A}$ είναι υπολογιστικά μη-φραγμένος και έχει πρόσβαση στα μαντεία $\mathcal{CO}, \mathcal{SO}, \mathcal{MO}$ για τους ίδιους λόγους που έχει πρόσβαση και στο παιχνίδι 7.2. Η προσβασή του είναι απεριόριστη και μπορεί να γίνει με βάση οποιαδήποτε προσαρμοστική στρατηγική. Ο αντίπαλος $\mathcal{A}$ επιλέγει τις παραμέτρους της υπογραφής και της στέλνει στον προκαλούντα $\mathcal{C}$. Ο $\mathcal{C}$ παράγει μία υπογραφή σ και μία προσομοίωση σ' με την ίδια ψευδοταυτότητα pid και δίνει στη τύχη μία από τις δύο στον $\mathcal{A}$, ο οποίος με τη σειρά του πρέπει να βρει εάν έλαβε την υπογραφή ή τη προσομοίωση.

Παιχνίδι 7.3: Πείραμα Μη-Μεταφερσιμότητας $\mathsf{Exp}^{\mathrm{trans}}_{\mathcal{A},\Pi}$

$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$
$\mathcal{U} \leftarrow \left\{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\right\}_{i=1}^{\mu(\lambda)}$
$(\mathsf{ev}, L = \{\mathsf{pk}_i\}_{i=1}^{n}, \mathtt{m}, \mathsf{pk}_D, \mathsf{pk}_\pi) \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
$\sigma_0 \leftarrow \Pi.\mathsf{Sign}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$
$\mathsf{pid} \leftarrow \Pi.\mathsf{Extract}(\sigma_0)$
$\sigma_1 \leftarrow \Pi.\mathsf{Sim}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$
$b \leftarrow\!\!\$\ \{0,1\}$
$b' \leftarrow \mathcal{A}^{\mathcal{CO},\mathcal{SO},\mathcal{MO}}(L, \mathtt{m}, \sigma_b)$
Επέστρεψε: $b = b'$

Ορισμός 7.5. *Μη-Μεταφερσιμότητα*

Ένα UDVLRS σχήμα Π *είναι τέλεια μη-μεταφέρσιμο αν για κάθε μη-φραγμένο αντίπαλο* $\mathcal{A}$ *ισχύει ότι:*

$$Adv_A^{trans}(\lambda) = |Pr[\mathsf{Exp}^{trans}_{\mathcal{A},\Pi}(\lambda) = 1] - \frac{1}{2}| = 0$$

7.2.7 Συνδεσιμότητα

Η ιδιότητα της συνδεσιμότητας δηλώνει πως υπογραφές που προέρχονται από τον ίδιο υπογράφοντα πρέπει να είναι συνδεδεμένες, ενώ διατηρούνται όλες οι υπόλοιπες ιδιότητες. Οι προσομοιώσεις που κατασκευάζονται από τον καθορισμένο επαληθευτή για δεδομένο pid θα συνδέονται με τις υπογραφές που έχουν το ίδιο pid. Ορίζουμε την ιδιότητα αυτή μέσω του παιχνιδιού . Σκοπός του αντιπάλου $\mathcal{A}$ στο παιχνίδι είναι να κατασκευάσει 2 μη-συνδεδεμένες υπογραφές

με *ένα* ιδιωτικό κλειδί. Ο $\mathcal{A}$ ρωτάει όλα τα μαντεία σύμφωνα με οποιαδήποτε προσαρμοστική στρατηγική για να κατασκευάσει τις υπογραφές σ_1 και σ_2. Τα δημόσια κλειδιά μπορούν να προέρχονται από δύο διαφορετικούς δακτυλίους και να έχει και διαφορετικούς καθορισμένους επαληθευτές. Ο $\mathcal{A}$ κερδίζει εάν και οι δύο υπογραφές είναι έγκυρες και μη-συνδεδεμένες.

Παιχνίδι 7.4: Πείραμα Συνδεσιμότητας $\mathsf{Exp}^{\text{link}}_{\mathcal{A},\Pi}$

$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$
$\mathcal{U} \leftarrow \left\{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\right\}_{i=1}^{\mu(\lambda)}$
$(\sigma_1, \sigma_2, \mathtt{ev}, L_1 = \{\mathsf{pk}_i\}_{i=1}^{n_1}, L_2 = \{\mathsf{pk}_i\}_{i=1}^{n_2}, \mathtt{m}_1, \mathtt{m}_2, \mathsf{pk}_{D_1}, \mathsf{pk}_{D_2}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
Επέστρεψε
$|\mathcal{CO}| = 1$ **ΚΑΙ** $\sigma_1, \sigma_2 \notin \mathcal{SO}$ **ΚΑΙ** $\mathsf{Vrfy}(\mathtt{ev}, \sigma_1, L_1, \mathtt{m}_1, \mathsf{pk}_{D_1}) =$
1 **ΚΑΙ** $\mathsf{Vrfy}(\mathtt{ev}, \sigma_2, L_2, \mathtt{m}_2, \mathsf{pk}_{D_2}) = 1$ **ΚΑΙ** $\mathsf{Link}(\sigma_1, \mathtt{ev}, \sigma_2, \mathtt{ev}) = 0$

Ορισμός 7.6. *Συνδεσιμότητα*

Ένα UDVLRS σχήμα Π *θα είναι συνδέσιμο αν για κάθε* PPT $\mathcal{A}$ *ισχύει ότι:*

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

Σημειώνουμε εδώ πως ο ορισμός της συνδεσιμότητας που δίνουμε είναι αυτός της ασθενούς συνδεσιμότητας που έχουν και οι ULRS. Εν αντιθέση οι DVLRS και οι LRS διαθέτουν την ισχυρότερη συνδεσιμότητα. Ως εκ τούτου οι UDVLRS υποφέρουν και αυτές από επιθέσεις συνεννόησης και χρειάζονται εκ νέου απόδειξη της ιδιότητας της μη-δυσφημισιμότητας. Για παραπάνω λεπτομέρειες παραπέμπουμε στην ενότητα των ULRS στο κεφάλαιο 5.

7.2.8 Μη-Δυσφημισιμότητα

Η τελευταία ιδιότητα που πρέπει να ικανοποιεί ένα UDVLRS σχήμα είναι αυτή της μη-δυσφημισιμότητας. Όπως εξηγήσαμε και στο κεφάλαιο 5 για τις ULRS, η μη-δυσφημισιμότητα προστατεύει τα μέλη του δακτυλίου από κακόβολη σύνδεση μίας υπογραφής από τρίτους σε δικές τους. Έτσι λοιπόν αν μία υπογραφή συνδέεται με μία άλλη τότε πρέπει να προέρχεται είτε από τον ίδιο τον υπογράφοντα είτε από τον καθορισμένο επαληθευτή. Ο ορισμός δίνεται μέσω του παιχνιδιού 7.5. Ο αντίπαλος $\mathcal{A}$ μπορεί να ρωτήσει όλα τα μαντεία σύμφωνα με οποιαδήποτε προσαρμοστική στρατηγική, και να επιλέξει τις παραμέτρους υπογραφής και το δημόσιο κλειδί του υπογράφοντα-στόχου pk_π, τα οποία θα δώσει στον προκαλούντα $\mathcal{C}$. Ο $\mathcal{C}$ με τη σειρά του χρησιμοποιώντας τον αλγόριθμο Sign με το κλειδί sk_π κατασκευάζει την υπογραφή σ_1. Σημειώνουμε εδώ πως το pk_π που επιλέγει ο $\mathcal{A}$ δε πρέπει να είναι είσοδος στο $\mathcal{CO}$, ή να

έχει χρησιμοποιηθεί για κλήση στο $\mathcal{SO}$. Ο $\mathcal{A}$ ρωτάει τα μαντεία με τους ίδιους περιορσιμούς με πριν για το pk_π και παράγει νέες παραμέτρους υπογραφής (εξαιρουμένου του $\mathtt{ev}$) και νέα υπογραφή σ_2, διαφορετική της σ_1. Ο $\mathcal{A}$ κερδίζει αν σ_2 επιβεβαιώνεται και σ_1 και σ_2 είναι συνδεδεμένες.

Παιχνίδι 7.5: Πείραμα Μη-Δυσφημισιμότητας $\mathsf{Exp}^{\mathrm{sland}}_{\mathcal{A},\Pi}$

$\mathsf{params} \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$
$\mathcal{U} \leftarrow \left\{(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \Pi.\mathsf{KGen}()\right\}_{i=1}^{\mu(\lambda)}$
$(\mathtt{ev}, L_1 = \{\mathsf{pk}_i\}_{i=1}^{n_1}, \mathtt{m}_1, \mathsf{pk}_{D_1}, \mathsf{pk}_\pi) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
$\sigma_1 \leftarrow \Pi.\mathsf{Sign}(\mathtt{ev}, L_1, \mathtt{m}_1, \mathsf{pk}_{D_1}, \mathsf{sk}_\pi)$
$(\sigma_2, L_2 = \{\mathsf{pk}_i\}_{i=1}^{n_2}, \mathtt{m}_2, \mathsf{pk}_{D_2}) \leftarrow \mathcal{A}^{\mathcal{RO},\mathcal{JO},\mathcal{CO},\mathcal{SO},\mathcal{MO}}(\mathcal{U})$
Επέστρεψε
$\sigma_2 \neq \sigma_1$ **ΚΑΙ** $\mathsf{Vrfy}(\mathtt{ev}, \sigma_2, L_2, \mathtt{m}_2, \mathsf{pk}_{D_2}) = 1$ **ΚΑΙ** $\sigma_2 \notin \mathcal{SO}$ **ΚΑΙ** $\sigma_2 \notin \mathcal{MO}$ **ΚΑΙ** $\pi \notin \mathcal{CO}$ **ΚΑΙ** $D_2 \notin \mathcal{CO}$ **ΚΑΙ** $\mathsf{Link}(\sigma_1, \mathtt{ev}, \sigma_2, \mathtt{ev}) = 1$

Ορισμός 7.7. *Συνδεσιμότητα*
Ένα UDVLRS σχήμα Π *θα είναι μη-δυσφημίσιμο αν για κάθε* PPT $\mathcal{A}$ *ισχύει ότι:*

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

7.3 Κατασκευή UDVLRS

Θα παραθέσουμε τώρα μία κατασκευή για ένα σχήμα UDVLRS.

- **Αρχικοποίηση** - $\mathsf{Setup}(\lambda)$:

  Με είσοδο τη παράμετρο ασφαλείας επιστρέφει την ομάδα $\mathbb{G}$ τάξης πρώτου q, όπου το DLOG θεωρείται δύσκολο, δύο τυχαίους γεννήτορες $g, h \in \mathbb{G}$ και δύο κρυπτογραφικές συναρτήσεις σύνοψης $\mathcal{H}_\mathbb{G} : \{0,1\}^* \to \mathbb{G}$, $\mathcal{H}_q : \{0,1\}^* \to \mathbb{Z}_q$. Επιπλέον επιστρέφει $\mathcal{MSG} = \{0,1\}^*$, $SG = \mathbb{G} \times \mathbb{Z}_q^{2n+4}$, $\mathcal{PID} = \mathbb{G}$ και $\mathcal{EID} = \{0,1\}^*$. Σημείωνουμε εδώ πως ο σχετικός διακριτός λογάριθμος των g &q είναι άγνωστος και ότι το χώρος των υπογραφών $\mathcal{SG}$ εξαρτάται από το μέγεθος του δακτυλίου.

- **Δημιουργία Κλειδιών** - $\mathsf{KGen}()$:

  Κάθε χρήστης i:

  1. Επιλέγει τυχαία $x_i, y_i \leftarrow\!\!\$\ \mathbb{Z}_q$
  2. Υπολογίζει $Z_i \leftarrow g^{x_i} h^{y_i}$
  3. Θέτει $\mathsf{sk}_i = (x_i, y_i)$ και $\mathsf{pk}_i = Z_i$

Ο καθορισμένος επαληθευτής θέτει $\mathsf{sk}_D = (x_D, y_D)$ και $\mathsf{pk}_D = Z_D$.

Καλούμε $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}()$.

- **Δημιουργία Υπογραφής** - $\mathsf{Sign}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$:

  Ο υπογράφοντας π:

  1. Επιλέγει στη τύχη $r_x, r_y, r, s, \{c_i\}_{\substack{i\in[n]\\ i\neq\pi}}, \{w_i\}_{i\in[n]} \leftarrow_\$ \mathbb{Z}_q$
  2. Υπολογίζει:
     (a) $e \leftarrow$
     $mathchal H_{\mathbb{G}}(\mathtt{ev}), \qquad t \leftarrow e^{x_\pi}$,
     (b) $K \leftarrow g^{r_x} h^{r_y} \cdot \prod_{\substack{i\in[n]\\ i\neq\pi}} Z_i^{c_i+w_i}$,
     (c) $K' \leftarrow e^{r_x} \cdot t^{\sum_{\substack{i\in[n]\\ i\neq\pi}} c_i+w_i}$,
     (d) $K'' \leftarrow h^s \mathsf{pk}_D^r \cdot \prod_{i=1}^n g^{w_i}$
  3. Έπειτα υπολογίζει c_π έτσι ώστε $\sum_{i=1}^n c_i \mod q = \mathcal{H}_q(\mathtt{m}, L, \mathtt{ev}, t, K, K', K'')$
  4. Τέλος υπολογίζει $\tilde{x} \leftarrow (r_x - (c_\pi + w_\pi)x_\pi) \mod q, \qquad \tilde{y} \leftarrow (r_y - (c_\pi + w_\pi)y_\pi) \mod q$

  Ο αλγόριθμος επιστρέφει $\sigma \leftarrow (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$

- **Εξαγωγή** - $\mathsf{Extract}(\sigma)$:

  Αναλύσουμε την υπογραφή ως την πλειάδα $\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$.
  Ο αλγόριθμος επιστρέφει το t.

- **Δημιουργία Προσομοίωσης** - $\mathsf{Sim}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$:

  Ο καθορισμένος επαληθευτής:

  1. Επιλέγει στη τύχη $\chi, \psi, \alpha, \beta, \gamma, \{c_i\}_{i=2}^n, \{w_i\}_{i=2}^n \leftarrow_\$ \mathbb{Z}_q$
  2. Θέτει $t = \mathsf{pid}$
  3. Υπολογίζει:
     (a) $K_D \leftarrow g^\chi \cdot h^\psi \cdot Z_1^\alpha \cdot \prod_{i=2}^n Z_i^{c_i+w_i}$,
     (b) $K'_D \leftarrow e^\chi t^{\alpha+\sum_{i=2}^n c_i+w_i}$,
     (c) $K''_D \leftarrow g^\beta h^\gamma \cdot \prod_{i=2}^n g^{w_i}$
  4. Υπολογίζει c_1 έτσι ώστε $\sum_{i=1}^n c_i \mod q = \mathcal{H}_q(\mathtt{m}, L, \mathtt{ev}, t, K_D, K'_D, K''_D)$
  5. Θέτει:
     (a) $\tilde{x} \leftarrow \chi$,

(b) $\tilde{y} \leftarrow \psi$,
(c) $w_1 \leftarrow \alpha - c_1 \mod q$,
(d) $r \leftarrow (\beta - w_1)x_D^{-1} \mod q$,
(e) $s \leftarrow \gamma - ry_D \mod q$

6. Ο αλγόριθμος επιστρέφει την προσομοιωμένη υπογραφή $\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$. Σημειώνουμε πως ο αλγόριθμος Simμπορεί να χρησιμοποιήσει οποιοδήποτε από τα c_k, w_k για οποιοδήποτε $k \in [n]$ αντί για c_1, w_1.

- **Επαλήθευση** - $\mathsf{Vrfy}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma)$:

1. Ανέλυσε την υπογραφή σ ως την πλειάδα $(t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$ και υπολόγισε τη τιμή:

$$c_0 \leftarrow \mathcal{H}_q(\mathtt{m}, L, \mathtt{ev}, t, g^{\tilde{x}}h^{\tilde{y}} \cdot \prod_{i=1}^{n} Z_i^{c_i+w_i}, e^{\tilde{x}} \cdot t^{\sum_{i=1}^n c_i+w_i}, h^s \mathsf{pk}_D^r \cdot \prod_{i=1}^{n} g^{w_i})$$

2. Επέστρεψε 1 αν $c_0 = \sum_{i=1}^n c_i \pmod q$ αλλιώς επέστρεψε 0.

- **Σύνδεση** - $\mathsf{Link}(\sigma_1, \mathtt{ev}_1, \sigma_2, \mathtt{ev}_2)$:

Επέστρεψε 1 αν $\mathtt{ev}_1 = \mathtt{ev}_2$ **ΚΑΙ** $\mathsf{Extract}(\sigma_1) = \mathsf{Extract}(\sigma_2)$ και οι δύο υπογραφές επιβεβαιώνουν αλλιώς επέστρεψε 0.

7.4 Ορθότητα και Ασφάλεια Κατασκευής UDVLRS

Σε αυτή την ενότητα θα αναλύσουμε την ορθότητα και την ασφάλεια του σχήματος UDVLRS που παραθέσαμε στην προηγούμενη ενότητα δίνοντας όλες τις σχετικές αποδείξεις. Οι αποδείξεις γίνονται στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ και ορισμένες κάνουν χρήση το λήμματος διακλάδωσης (Forking Lemma) [64].

Ξεκινάμε δείχνοντας πως οι τίμια κατασκευασμένες υπογραφές και προσομοιώσεις επιβεβαιώνονται επιτυχώς:

Λήμμα 7.1. *Μία τίμια κατασευασμένη UDVLRS υπογραφή σ επιβεβαιώνει επιτυχώς.*

Απόδειξη. Η πληρότητα του σχήματος υπογραφών προκύπτει από την Εξίσωση 1 αφού:

$$g^{\tilde{x}}h^{\tilde{y}}\prod_{i=1}^{n}Z_i^{c_i+w_i} = g^{r_x-(c_\pi+w_\pi)x_\pi}h^{r_y-(c_\pi+w_\pi)y_\pi}\prod_{i=1}^{n}Z_i^{c_i+w_i} =$$

$$g^{r_x}h^{r_y}(g^{x_\pi}h^{y_\pi})^{-(c_\pi+w_\pi)}\prod_{i=1}^{n}Z_i^{c_i+w_i} = g^{r_x}h^{r_y}Z_\pi^{-(c_\pi+w)}Z_\pi^{(c_\pi+w)}\prod_{\substack{i\in[n]\\ i\neq\pi}}Z_i^{c_i+w_i} = K$$

Όμοια:

$$e^{\tilde{x}}t^{\sum_{i=1}^{n}c_i+w_i} = e^{r_x-(c_\pi+w_\pi)x_\pi}t^{c_\pi+w_\pi}t^{\sum_{\substack{i\in[n]\\ i\neq\pi}}c_i+w_i} =$$

$$e^{r_x}t^{-(c_\pi+w_\pi)}t^{c_\pi+w_\pi}t^{\sum_{\substack{i\in[n]\\ i\neq\pi}}c_i+w_i} = e^{r_x}t^{\sum_{\substack{i\in[n]\\ i\neq\pi}}c_i+w_i} = K'$$

Ακόμα έχουμε από την κατασευή πως για μία τίμια υπογραφή ισχύει πράγματι ότι:

$$h^s\mathsf{pk}_D^r\prod_{i=1}^{n}g^{w_i} = K''$$

Επομένως $\mathsf{Vrfy}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma) = 1$ □

Λήμμα 7.2. *Μία τίμια κατασευασμένη UDVLRS προσομοίωση σ επιβεβαιώνει επιτυχώς.*

Απόδειξη. Μία προσομοιωμένη υπογραφή επιβεβαιώνει αφού από την Εξίσωση 1

$$g^{\tilde{x}}h^{\tilde{y}}\prod_{i=1}^{n}Z_i^{c_i+w_i} = g^{\chi}h^{\psi}Z_1^{c_1+w_1}\prod_{i=2}^{n}Z_i^{c_i+w_i} = g^{\chi}h^{\psi}Z_1^{\alpha}\prod_{i=2}^{n}Z_i^{c_i+w_i} = K_D$$

Όμοια:

$$e^{\tilde{x}}t^{\sum_{i=1}^{n}c_i+w_i} = e^{\chi}t^{c_1+w_1}t^{\sum_{i=2}^{n}c_i+w_i} = e^{\chi}t^{\alpha+\sum_{i=2}^{n}c_i+w_i} = K'_D$$

Για το τελευταία κομμάτι της υπογραφής:

$$h^s\mathsf{pk}_D^r\prod_{i=1}^{n}g^{w_i} = h^s\mathsf{pk}_D^r g^{w_1}\prod_{i=2}^{n}g^{w_i} =$$

$$g^{\beta-rx_D}h^{\gamma-ry_D}\mathsf{pk}_D^r\prod_{i=2}^{n}g^{w_i} = g^{\beta}h^{\gamma}(g^{x_D}h^{y_D})^{-r}\mathsf{pk}_D^r\prod_{i=2}^{n}g^{w_i} = K''_D$$

Επομένως $\mathsf{Vrfy}(\mathtt{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma) = 1$ □

Λήμμα 7.3. *Το σχήμα* UDVLRS *που παρουσιάστηκε στην προηγούμενη ενότητα έχει την ιδιότητα της ορθότητας επαλήθευσης.*

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια των Λημμάτων 7.1 και 7.2. □

Λήμμα 7.4. *Το σχήμα* UDVLRS *που παρουσιάστηκε στην προηγούμενη ενότητα έχει την ιδιότητα της ορθότητας σύνδεσης.*

Απόδειξη. Έστω δύο υπογραφές σ_1, σ_2 κατασευασμένες με το ίδιο event ev.

- Αν είναι και οι δύο κατασκευασμένες από τον ίδιο υπογράφοντα π με $\mathsf{sk}_\pi = (x_\pi, y_\pi)$ τότε $\mathsf{Extract}(\sigma_1) = \mathsf{Extract}(\sigma_2) = (\mathcal{H}_{\mathbb{G}}(\mathsf{ev}))^{x_\pi}$. Επομένως $\mathsf{Link}(\sigma_1, \mathsf{ev}, \sigma_2, \mathsf{ev}) = 1$.
- Αν σ_1 είναι τίμια κατασευασμένη από τον υπογράφοντα π και σ_2 είναι προσομοιωμένη με ετικέτα σύνδεσης $t = \mathsf{Extract}(\sigma_1)$ τότε $\mathsf{Link}(\sigma_1, \mathsf{ev}, \sigma_2, \mathsf{ev}) = 1$.
- Αν σ_1, σ_2 είναι προσομοιώσεις με την ίδια ετικέτα σύνδεσης τότε $\mathsf{Link}(\sigma_1, \mathsf{ev}, \sigma_2, \mathsf{ev}) = 1$.

□

Με τα θεωρήματα που ακολουθούν θα αποδείξουμε τις ιδότητες ασφάλειας της κατασκευής που έχουμε παραθέσει.

Θεώρημα 7.2. *Μη-Πλαστογραφισημότητα*
Το σχήμα UDVLRS που παραθέσαμε είναι μη-πλαστογραφίσημο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$ αν το DLP *είναι δύσκολο στην ομάδα $\mathbb{G}$.*

Απόδειξη. Υποθέτουμε έναν PPT αντίπαλο $\mathcal{A}$ ο οποίος είναι ικανός να παράξει μία πλαστογραφία, δηλαδή μία έγκυρη υπογραφή $\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$ για κάποιο event ev, δακτύλιο με n μέλη $L = \{Z_i\}_{i=1}^n$ με μη-αμελητέα πιθανότητα. Θα κατασκευάσουμε έναν PPT αντίπαλο $\mathcal{B}$ ο οποίος χρησιμοποιώντας τον $\mathcal{A}$ θα σπάσει είτε το στιγμυότυπο DLP $\{X_D \in \mathbb{G} : X_D = g^{x_D},\ x_D \in \mathbb{Z}_q\}$ ή θα λύσει το πρόβλημα MDLR για μη-κενό υποσύνολο του $\{X_i \in \mathbb{G} : X_i = g^{x_i}, x_i \in \mathbb{Z}_q\}_{i=1}^n$ με μη-αμελητέα πιθανότητα.

Η είσοδος για τον $\mathcal{B}$ αποτελείται από $\mathbb{G}, g, q, \{X_i\}_{i=1}^n \cup \{X_D\}$. Ο $\mathcal{B}$ προσομοιώνει το περιβάλλον για τον $\mathcal{A}$:

- $\mathcal{B}$ επιστρέφει $\mathbb{G}, g, q$ όταν $\mathcal{A}$ εκτελεί τον αλγόριθμο Setup.
- Με την εκτέλεση του KGen, ο $\mathcal{B}$ επιλέγει $x' \leftarrow\!\!\$\ \mathbb{Z}_q$, θέτει $h = g^{x'}$ και δίνει g, h στον $\mathcal{A}$.

- Προσομοίωση του μαντείου $\mathcal{RO}$. Ο $\mathcal{B}$ προσομοιώνει το $\mathcal{H}_{\mathbb{G}}$ τυχαίο μαντείο επιστρέφοντας g^a για κάποιο $a \leftarrow\!\!\$\ \mathbb{Z}_q$ και το τυχαίο μαντείο $\mathcal{H}_q$ επιστρέφοντας b για κάποιο $b \leftarrow\!\!\$\ \mathbb{Z}_q$.

- Προσομοίωση του μαντείου $\mathcal{JO}$. Επειδή ο $\mathcal{A}$ είναι PPT, ο μέγιστος αριθμός κλήσεων στο $\mathcal{JO}$ θα είναι $n' = \mathsf{poly}(\lambda)$ όπου $n' \geq n+1$. Ο $\mathcal{B}$ επιλέγει ομοιόμορφα στη τύχη ένα υποσύνολο δεικτών $\mathcal{I}_{n+1} \subset [n']$. Δίχως βλάβη της γενικότητας $\mathcal{I}_{n+1} = [n+1]$. Η i-οστή κλήση στο $\mathcal{JO}$ απαντάται με τον ακόλουθω τρόπο [3]:

  - Αν $i \in \mathcal{I}_{n+1}$, $\mathcal{B}$ σταματά αφού δε γνωρίζει το διακριτό λογάριθμο το X_i.
  - Αν If $i \notin \mathcal{I}_{n+1}$, $\mathcal{B}$ επιστρέφει $x_i, y_i \in \mathbb{Z}_q$ όπως αυτά επιστράφηκαν όταν απαντήθηκε η αντίστοιχη κλήση στο $\mathcal{JO}$.

- Προσομοίωση του μαντείου $\mathcal{SO}$. Η είσοδος για αυτό το μαντείο είναι ένα μήνυμα $\mathtt{m}$, event $\mathtt{ev}$, κάποιο δακτύλιο $L = \{Z_i\}_{i=1}^n$, το δημόσιο κλειδί του καθορισμένου επαληθευτή pk_D, και έναν δείκτη π που υποδεικνύει το ότι ο υπογράφοντας πρέπει να χρησιμοποιήσει το ιδιωτικό κλειδί που ανταποκρίνεται στο Z_π. Αν $\pi \notin \mathcal{I}_n$ τότε ο $\mathcal{B}$ γνωρίζει το πλήρες ιδιωτικό κλειδί (x_i, y_i) και ως εκ τούτου υπογράφει χρησιμοποιώντας τον αλγόριθμο Sign. Αν $\pi \in \mathcal{I}_n$, τότε ο $\mathcal{B}$ πρέπει να προσομοίωσει την υπογραφή γνωρίζοντας μόνο y_π:

  - $\mathcal{B}$ θέτει $t \leftarrow X_\pi^a$ όπου $e = g^a$ ήταν η απάντηση στο $\mathcal{H}_{\mathbb{G}}(\mathtt{ev})$. Αυτό σημαίνει πως $t = e^{x_\pi}$
  - $\mathcal{B}$ επιλέγει $\tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n \leftarrow\!\!\$\ \mathbb{Z}_q$ και προγραμματίζει το τυχαίο μαντείο να απαντά $\mathcal{H}_q(\mathtt{m}, L, \mathtt{ev}, t, g^{\tilde{x}}h^{\tilde{y}} \cdot \prod_{i=1}^n Z_i^{c_i+w_i}, e^{\tilde{x}} \cdot t^{\sum_{i=1}^n c_i+w_i}, h^s \mathsf{pk}_D^r \cdot \prod_{i=1}^n g^{w_i})$ με τη τιμή $\sum_{i=1}^n c_i$.
  - Εκ κατασκευής, η προσομοιωμένη υπογραφή $\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$ είναι ορθή και μη-διακρίσιμη από την έξοδο του αλγορίθμου Sign.

- Προσομοίωση του μαντείου $\mathcal{MO}$. Υποθέτουμε πως i_D ήταν η κλήση στο $\mathcal{JO}$ που ρώταγε για το pk_D. Αν $i_D \notin \mathcal{I}_{n+1}$ τότε ο $\mathcal{B}$ γνωρίζει το πλήρες ιδιωτικό κλειδί (x_D, y_D) του καθορισμένου επαληθευτή και έτσι μπορεί να προσομοίωσει υπογραφές με τη χρήση του αλγόριθμου Sim. Αν $i_D \in \mathcal{I}_{n+1}$, τότε ο $\mathcal{B}$ πρέπει να προγραμματίσει το τυχαίο μαντείο ώστε να παράγει μη-διακρίσιμες προσομοιωμένες υπογραφές. Αυτό επιτυγχάνεται πιο εύκολα από το μαντείο $\mathcal{SO}$, επειδή στον αλγόριθμο Sim η ετικέτα είναι τυχαίο στοιχείο της ομάδας $\mathbb{G}$:

[3] Υποθέτουμε δίχως βλάβη της γενικότητας πως $X_D = X_{n+1}$

- Ο $\mathcal{B}$ επιλέγει $t \leftarrow\!\!\$\ \mathbb{G}$.
- Ο $\mathcal{B}$ επιλέγει $\tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n \leftarrow\!\!\$\ \mathbb{Z}_q$ και προγραμματίζει το τυχαίο μαντείο να απαντά με τη τιμή $\sum_{i=1}^n c_i$ στη κλήση $\mathcal{H}_q(\mathtt{m}, L, \mathsf{ev}, t, g^{\tilde{x}}h^{\tilde{y}} \cdot \prod_{i=1}^n Z_i^{c_i+w_i}, e^{\tilde{x}} \cdot t^{\sum_{i=1}^n c_i+w_i}, h^s \mathsf{pk}_D^r \cdot \prod_{i=1}^n g^{w_i})$.
- Εκ κατασκευής, η προσομοιωμένη υπογραφή $\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$ είναι ορθή και μη-διακρίσιμη από την έξοδο του αλγορίθμου Sim.

Ο αντίπαλος της μη-πλαστογραφισημότητας $\mathcal{A}$ καταφέρνει, μετά από αλληλεπίδραση με τα μαντεία $\mathcal{RO}, \mathcal{JO}, \mathcal{CO}, \mathcal{SO}, \mathcal{MO}$ που ελέγχονται από τον $\mathcal{B}$, να κατασκευάσει μία πλαστογραφία υπογραφής $\sigma_1^* = (t_1, \tilde{x}_1, \tilde{y}_1, r_1, s_1, \{c_{i1}\}_{i=1}^n, \{w_{i1}\}_{i=1}^n)$ για κάποιο event ev και δακτύλιο L. Για να μπορέσει να παράξει την υπογραφή ο $\mathcal{A}$ πρέπει να έχει κάνει κλήση στην $\mathcal{H}_q$ για ev, L, κάποιο μήνυμα $\mathtt{m}$, κάποιο $t \in \mathbb{G}$, δηλαδή $\mathcal{H}_q(\mathtt{m}, L, \mathsf{ev}, t, K_1, K_1', K_1'')$. Αφού σ_1^* είναι μία έγκυρη πλαστογραφία:

$$K_1 = g^{\tilde{x}_1} h^{\tilde{y}_1} \cdot \prod_{i=1}^n Z_i^{c_{i1}+w_{i1}}$$

Υποθέτουμε πως η τιμή K_1 ερωτήθει κατά τη διάρκει της l-οστής κλήσης και ο $\mathcal{B}$ απάντησε με c_{01}. Και πάλι αφού σ_1^* είναι έγκυρη ισχύει ότι:

$$c_{01} = \sum_{i=1}^n c_{i1} \pmod q$$

Θα αποδείξουμε ότι ο $\mathcal{B}$ μπορεί είτε να ανακτήσει τον διακριτό λογάριθμο του $X_D = g^{x_D}$ ή να λυσει το πρόβλημα MDLR για κάποιο υποσύνολο του $\{X_i \in \mathbb{G} : X_i = g^{x_i}, x_i \in \mathbb{Z}_q\}_{i=1}^n$ χρησιμοποιώντας την τεχνική επαναφοράς [64]. Ο $\mathcal{B}$ επαναφέρει τον $\mathcal{A}$ και απαντά όλες τις κλήσεις εώς την l με συνέπεια, αλλά απαντά τη l-οστή κλήση με $c_{02} \neq c_{01}$. Σύμφωνα με το λήμμα διακλάδωσης [64], $\mathcal{A}$ θα παράξει μία άλλη πλαστογραφία $\sigma_2^* = (t_2, \tilde{x}_2, \tilde{y}_2, r_2, s_2, \{c_{i2}\}_{i=1}^n, \{w_{i2}\}_{i=1}^n)$ με μη-αμελητέα πιθανότητα σε πολυωνιμικό χρόνο. Όμως $K_1 = K_2$, $K_1' = K_2'$, $K_1'' = K_2''$ και για τις δύο l-οστές κλήσεις. Αυτό σημαίνει ότι:

$$g^{\tilde{x}_1} h^{\tilde{y}_1} \cdot \prod_{i=1}^n Z_i^{c_{i1}+w_{i1}} = g^{\tilde{x}_2} h^{\tilde{y}_2} \cdot \prod_{i=1}^n Z_i^{c_{i2}+w_{i2}} \text{ και} \tag{7.1}$$

$$h^{s_1} \cdot \mathsf{pk}_D^{r_1} \cdot g^{\sum_{i=1}^n w_{i1}} = h^{s_2} \cdot \mathsf{pk}_D^{r_2} \cdot g^{\sum_{i=1}^n w_{i2}} \tag{7.2}$$

Από την εξίσωση 7.2, έχουμε ότι:

$$g^{r_1 \cdot x_D + \sum_{i=1}^n w_{i1}} \cdot h^{s_1 + r_1 \cdot y_D} = g^{r_2 \cdot x_D + \sum_{i=1}^n w_{i2}} \cdot h^{s_2 + r_2 \cdot y_D} \Rightarrow$$

$$r_1 \cdot x_D + \sum_{i=1}^n w_{i1} = r_2 \cdot x_D + \sum_{i=1}^n w_{i2}$$

Αν $r_1 \neq r_2$:

$$x_D = \frac{\sum_{i=1}^{n} w_{i1} - \sum_{i=1}^{n} w_{i2}}{r_2 - r_1}$$

Επομένως, ο $\mathcal{B}$ έχει επιτυχώς υπολογίσει τον διακριτό λογάριθμο του X_D.

Στη δεύτερη περίπτωση, αν $r_1 = r_2$ τότε $\sum_{i=1}^{n} w_{i1} = \sum_{i=1}^{n} w_{i2}$ και επειδή $K_1 = K_2$, από την εξίσωση 7.1 λαμβάνουμε το σύστημα εξισώσεν:

$$g^{\tilde{x}_1} \cdot h^{\tilde{y}_1} \cdot \prod_{i=1}^{n} Z_i^{c_{i1}+w_{i1}} = g^{\tilde{x}_2} \cdot h^{\tilde{y}_2} \cdot \prod_{i=1}^{n} Z_i^{c_{i2}+w_{i2}} \Rightarrow$$

$$g^{\tilde{x}_1+\sum_{i=1}^{n} x_i(c_{i1}+w_{i1})} \cdot h^{\tilde{y}_1+\sum_{i=1}^{n} y_i(c_{i1}+w_{i1})} = g^{\tilde{x}_2+\sum_{i=1}^{n} x_i(c_{i2}+w_{i2})} \cdot h^{\tilde{y}_2+\sum_{i=1}^{n} y_i(c_{i2}+w_{i2})} \Rightarrow$$

$$g^{\tilde{x}_1} \cdot \prod_{i=1}^{n} X_i^{c_{i1}+w_{i1}} = g^{\tilde{x}_2} \cdot \prod_{i=1}^{n} X_i^{c_{i2}+w_{i2}} \Rightarrow$$

$$\prod_{i=1}^{n} X_i^{c_{i1}+w_{i1}-(c_{i2}+w_{i2})} = g^{\tilde{x}_2-\tilde{x}_1} \tag{7.3}$$

Σημειώνουμε πως υπάρχει $i \in [n]$ τέτοιο ώστε $c_{i1} + w_{i1} \neq c_{i2} + w_{i2}$, αφού αν $c_{i1} + w_{i1} = c_{i2} + w_{i2}, \forall i \in [n]$ τότε, $\sum_{i=1}^{n} c_{i1} + w_{i1} = \sum_{i=1}^{n} c_{i2} + w_{i2} \xrightarrow{\sum_{i\in[n]} w_{i1} = \sum_{i\in[n]} w_{i2}} \sum_{i=1}^{n} c_{i1} = \sum_{i=1}^{n} c_{i2} \Rightarrow c_{01} = c_{02}$, που οδηγεί σε αντίφαση.

Υποθέτουμε πως υπάρχουν ακριβώς k δείκτες, $i_1, i_2, \ldots, i_k$ $1 \leq k \leq n$, έτσι ώστε $c_{i_j 1} + w_{i_j 1} \neq c_{i_j 2} + w_{i_j 2}$, $j \in [k]$. Τότε από την εξίσωση 7.3 έχουμε ότι:

$$X_{i_1} \cdot X_{i_2}^{\phi_2} \cdots X_{i_k}^{\phi_k} = g^{\phi_1}$$

όπου $\phi_1 = \frac{\tilde{x}_2 - \tilde{x}_1}{c_{i_1 1} + w_{i_1 1} - c_{i_1 2} - w_{i_1 2}}$ και $\phi_j = \frac{c_{i_j 1} + w_{i_j 1} - c_{i_j 2} - w_{i_j 2}}{c_{i_j 1} + w_{i_j 1} - c_{i_j 2} - w_{i_j 2}}$, $j \in [k]$. Ως αποτέλεσμα, έχουμε βρει μία λύση $\phi_1, \ldots \phi_k$ για το πρόβλημα MDLR για το $\{X_i \in \mathbb{G} : X_i = g^{x_i}, x_i \in \mathbb{Z}_q\}_{i=1}^{k}$.

Το λήμμα διακλάδωσης εγγυάται ότι ο χρόνος που θα τρέχει ο $\mathcal{B}$ είναι πολυωνιμικός και ότι η πιθανότητα επιτυχίας είναι μη-αμελητέα, οδηγόντας έτσι σε μία αντίφαση. □

Θεώρημα 7.3. *Ανωνυμία*

Το σχήμα UDVLRS που παραθέσαμε είναι άνευ όρων ανώνυμο.

Απόδειξη. Θα αποδείξουμε πως το σχήμα μας είναι τέλεια ανώνυμο χρησιμοποιώντας τις τεχνικές που χρησιμοποιούνται στο [56], κατάλληλα προσαυξημένες για να συμπεριληφθεί η εισαγωγή του καθορισμένου επαληθευτή. Πιο

συγκεκριμένα, θα δείξουμε ότι μία υπογραφή που παράγεται χρησιμοποιώντας μη-διευθαρμένα δημόσια κλειδιά είναι ισοπίθανο να έχουν κατασκευαστεί από οποιονδήποτε υπογράφοντα που δεν έχει διευθαρθεί. Όπως έχουμε εξηγήσει και στο κεφάλαιο 5 στην ενότητα για τις ULRS η χρήση της συνάρτησης $f(x,y) = g^x h^y$ είναι *q-προς-1* με σύνολο τιμών ομοιόμορφα κατανεμημένο πάνω από την ομάδα $\mathbb{G}$ προσφέρει την ισχυρή ανωνυμία του σχήματος. Πιο συγκεκριμένα ακόμα και αν ο $\mathcal{A}$ μπορεί να λύσει το DLP του είναι αδύνατο να εξάγει όλο το ιδιωτικό κλειδί ενός υπογράφοντα παρά μόνο το x κομμάτι από την ετικέτα σύνδεσης, αφού κάθε δημόσιο κλειδί μπορεί να προκύψει χρησιμοποιώντας αυτή τη τιμή x.

Για κάθε κλήση που κάνει ο $\mathcal{A}$ στο μαντείο $\mathcal{JO}$, μία τιμή $Z = g^x h^y$ επιστρέφεται για κάποιο τυχαίο ζευγάρι (x, y). Ο προκαλούντας $\mathcal{C}$ κατασκευάζει μία υπογραφή πρόκληση $\sigma_c = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}, \{w_i\})$ χρησιμοποιώντας το κλειδί ενός τυχαίου μέλους του δεδομένου δακτυλίου. Η απόδειξη θα δείξει ότι το πλεονέκτημα οποιουδήποτε αντιπάλου $\mathcal{A}$ είναι μηδενικό υπό καμία υπολογιστική υπόθεση. Υποθέτουμε δίχως βλάβη της γενικότητας ότι τα ιδιωτικά κλειδιά που ο $\mathcal{A}$ δεν έχει αποκτήσει μέσω των $\mathcal{CO}$ ή $\mathcal{SO}$ είναι τα πρώτα στοιχεία στο σύνολο $[n - m_1 - m_2]$.

Ξεκινάμε δείχνοντας ότι για κάθε υπογράφοντα στο $\pi \in [n - m_1 - m_2]$ και για κάθε δυνατό δημόσιο κλειδί $Z = g^{x_\pi} h^{y_\pi}$ υπάρχει ένα ζεύγος (x_π, y_π) τέτοιο ώστε $t = e^{x_\pi}$. Επιπλέον θα δείξουμε ότι για κάθε τέτοιο ζευγάρι υπάρχει τυχαιότητα (r_{x_π}, r_{y_π}) τέτοια ώστε σ_c να έχει κατασκευαστεί με αυτή τη τυχαιότητα, και τελικώς αποδεικνύουμε ότι οι 4 ακόλουθες τιμές $(x_\pi, y_\pi, r_{x_\pi}, r_{y_\pi})$ είναι ομοιόμορφα κατανεμημένες και άρα η υπογραφή πρόκληση μπορεί να έχει προέλθει από οποιονδήποτε υπογράφοντα από τον δακτύλιο.

Ο $\mathcal{A}$ μπορεί να λάβει τη τιμή x μέσω του $t = e^x$ και μία τιμή l από $g = h^l$. Επομένως, $Z_i = h_i^z, i \in [n - m_1 - m_2]$ και για κάθε $\pi \in [n - m_1 - m_2]$:

$$\begin{aligned} x_\pi &= x \pmod q \\ y_\pi &= z_\pi - x_\pi l \pmod q \end{aligned}$$

Παρατηρούμε ότι $Z_\pi = h^{z_\pi} = h^{y_\pi + x_\pi l} = g^{x_\pi} h^{y_\pi}$, δηλαδή τό ζευγάρι (x_π, y_π) αποτλεί ένα ζευγάρι ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί Z_π, και ότι $t = e^x = e^{x_\pi}$.

Για κάθε ιδιωτικό κλειδί (x_π, y_π), λαμβάνουμε υπ' όψη τις ακόλουθες τιμές:

$$\begin{aligned} r_{x_\pi} &= \tilde{x} - (c_\pi + w_\pi) x_\pi \pmod q \\ r_{y_\pi} &= \tilde{y} - (c_\pi + w_\pi) y_\pi \pmod q \end{aligned}$$

Εύκολα βλέπουμε ότι η σ_c μπορεί να κατασκευαστεί από το ιδιωτικό κλειδί (x_π, y_π) χρησιμοποιώντας τυχαιότητα (r_{x_π}, r_{y_π}), από οποιονδήποτε υπογράφοντα $\pi \in [n - m_1 - m_2]$.

Θα δείξουμε τώρα ότι από τα οποία αποτελείται κάθε πλειάδα $(x_\pi, y_\pi, r_{x_\pi}, r_{y_\pi})$ ακολουθούν την ίδια κατανομή στο $\mathbb{Z}_q$. Επειδή $x_\pi = x \pmod q$ και $x \leftarrow\!\!\$\ \mathbb{Z}_q$ έχουμε ότι x_π είναι ομοιόμορφα κατανεμημένο στο $\mathbb{Z}_q$. Από τον ορισμό του y_π προκύπτει ότι και αυτό ακολουθεί την ομοιόμορφη κατανομή στο $\mathbb{Z}_q$. Για το r_{x_π}, και με το ίδιο επιχείρημα και για το r_{y_π}, έχουμε ότι ακολουθεί την ομοιόμορφη κατανομή στο $\mathbb{Z}_q$ αφού είναι υπολογισμένο χρησιμοποιώντας τη τιμή w_π που είναι τυχαία επιλεγμένη από το $\mathbb{Z}_q$ όταν δημιουργείται η υπογραφή σ_c. Καταλήγουμε λοιπόν στο συμπέρασμα ότι κάθε πλειάδα $(x_\pi, y_\pi, r_{x_\pi}, r_{y_\pi})$ αποτελείται από στοιχεία ομοιόμορφα κατανεμημένα στο $\mathbb{Z}_q$ για κάθες υπογράφοντα $\pi \in [n - m_1 - m_2]$. □

Θεώρημα 7.4. *Μη-Μεταφερσιμότητα*

Το UDVLRS σχήμα που παραθέσαμε είναι τέλεια μη-μεταφέρσιμο στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$.

Απόδειξη. Έστω ότι σ και σ' είναι μία τίμια υπογραφή και προσομοιώση αντίστοιχα, για το ίδιο μήνυμα $\mathtt{m}$, δακτύλιο L, κλειδί καθορισμένου επαληθευτή $\mathsf{pk}_D = g^{x_D} h^{y_D}$, ίδια ετικέτα σύνδεσης t, και ίδιο υπογράφοντα π. Θα δείξουμε ότι κάθε κομμάτι της υπογραφής και της προσομοίωσης ακολουθούν την ίδια κατανομή.

- *Ετικέτα σύνδεσης t.* Αφού σ' είναι μία προσομοίωση της σ θα είναι η ίδια τιμή και άρα θα ακολουθούν την ίδια κατανομή.

- *$\tilde{x}$ and $\tilde{y}$.* Στη περίπτωση της σ έχουμε ότι $\tilde{x}$ και $\tilde{y}$ υπολογίζονται χρησιμοποιώντας την τυχαιότητα r_x και r_y αντίστοιχα, και ως εκ τούτου θα είναι ομοιόμορφα κατανεμημένα στο $\mathbb{Z}_q$. Στην περίπτωση της σ', $\tilde{x}$ και $\tilde{y}$ επιλέγονται στη τύχη από το $\mathbb{Z}_q$, και α'ρα είναι ομοιόμορφα κατανεμημένα στο $\mathbb{Z}_q$.

- $\{c_i\}_{i=1}^n$. Για σ έχουμε ότι $\{c_i\}_{\substack{i\in[n]\\ i\neq\pi}} \leftarrow\!\!\$\ \mathbb{Z}_q$ και c_π υπολογίζεται ως:

$$c_\pi \leftarrow \mathcal{H}_q(\mathtt{m}, L, \mathtt{ev}, t, K, K', K'') - \sum_{\substack{i\in[n]\\ i\neq\pi}} c_i \mod q$$

  Για τη σ' έχουμε $\{c_i\}_{i=2}^n \leftarrow\!\!\$\ \mathbb{Z}_q$, και για c_1 έχουμε ότι:

$$c_1 = \mathcal{H}_q(\mathtt{m}, L, \mathtt{ev}, t, K_D, K'_D, K''_D) - \sum_{\substack{i\in[n]\\ i\neq 1}} c_i \pmod q$$

  Και με το ίδιο επιχείρημα όπως και πριν, έχουμε ότι c_1 είναι ομοιόμορφα κατανεμημένο στο $\mathbb{Z}_q$. Επομένως για κάθε δείκτη $i \in [n]$ έχουμε ότι $\{c_i\}_{i=1}^n$ ακολουθούν την ίδια κατανομή και στις δύο περιπτώσεις.

- $\{w_i\}_{i=1}^n$. Για τη σ επιλέγουμε κάθε w_i στη τύχη από το $\mathbb{Z}_q$. Για τη σ' επιλέγουμε στη τύχη κάθε w_i από το $\mathbb{Z}_q$ εκτός από το w_1, για το οποίο ισχύει:

$$w_1 = \alpha - c_1 \pmod{q}$$

  Επειδή το α είναι τυχαίο στοιχείο του $\mathbb{Z}_q$ προκύπτει ότι το w_1 είναι ομοιόμορφα κατανεμημένο στο $\mathbb{Z}_q$. Έτσι λοιπόν βλέπουμε, πως και στις δύο περιπτώσεις, όπως και στην περίπτωση του $\{c_i\}_{i=1}^n$, για κάθε δείκτη i, w_i είναι ισόνομα.

- *r and s.* Για τη σ έχουμε ότι r και s επιπλέγονται στη τύχη από το $\mathbb{Z}_q$. Για τη σ' έχουμε ότι:

$$r = (\beta - w_1)x_D^{-1} \pmod{q}, \qquad s = \gamma - ry_D \pmod{q}$$

  Αφού και τα δύο περιέχουν τυχαία στοιχεία από το $\mathbb{Z}_q$, β και γ αντίστοιχα, και επομένως r, s είναι τυχαία στοιχεία του $\mathbb{Z}_q$. Έχουμε λοιπόν ότι και στις δύο υπογραφές αυτές οι δύο τιμές είναι ισόνομες.

Με βάση τις προηγούμενες παρατηρήσεις συμπεραίνουμε ότι η υπογραφή από έναν υπογράφοντα του δακτυλίου και μία προσομοίωση του καθορισμένου επαληθευτή για τον ίδιο δακτύλιο, μήνυμα, δημόσι κλειδί καθορισμένου επαληθευτή και ετικέτα σύνδεσης για τον ίδιο υπογράφοντα π ακολουθούν και οι δύο την ίδια κατανομή και επομένως είναι μη-διακρίσιμες, ακόμα και για υπολογιστικά μη-φραγμένους αντιπάλους. Ως εκ τούτου η τυχαία επιλογή είναι η καλύτερη, και μοναδική, επιλογή. □

Θα αποδείξουμε τώρα το Λήμμα 7.5 το οποίο το χρησιμοποιούμε για να αποδείξουμε το Θεώρημα 7.5.

Λήμμα 7.5. *Αν ο αντίπαλος $\mathcal{A}$ γνωρίζει μόνο ένα ιδιωτικό κλειδί $\mathsf{sk}_\pi = (x_\pi, y_\pi)$ όπου $\pi \in [n]$ και κατασκευάζει μία έγκυρη υπογραφή $\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$ για ένα event $\mathtt{ev}$, τότε $t = e^{x_\pi}$, όπου $e = \mathcal{H}_{\mathbb{G}}(\mathtt{ev})$, δεδομένου ότι το DLP είναι δύσκολο στη $\mathbb{G}$ στο μοντέλο του τυχαίου μαντείου $\mathcal{RO}$.*

Απόδειξη. Έστω ότι ο $\mathcal{A}$ παράγει μία έγκυρη υπογραφή $\sigma_1 = (t, \tilde{x}_1, \tilde{y}_1, r_1, s_1, \{c_{i1}\}_{i=1}^n, \{w_{i1}\}_{i=1}^n)$, όπου $t = \mathcal{H}_{\mathbb{G}}(\mathtt{ev})^{\hat{x}}$ για κάποιο $\hat{x} \in \mathbb{Z}_q$. Επαναφέρουμε τον $\mathcal{A}$ και δίνουμε μία διαφορετική τιμή για τη κλήση στο τυχαίο μαντείο $\mathcal{H}_q$, και ο $\mathcal{A}$ παράγει μία δεύτερη έγκυρη υπογραφή $\sigma_2 = (t, \tilde{x}_2, \tilde{y}_2, r_2, s_2, \{c_{i2}\}_{i=1}^n, \{w_{i2}\}_{i=1}^n)$.

Και στις δύο εκτελέσεις, η κλήση του $\mathcal{A}$ στο $\mathcal{H}_q$ είναι:

$$\mathcal{H}_q(\mathtt{m}, L, \mathtt{ev}, \mathcal{H}_{\mathbb{G}}(\mathtt{ev})^{\hat{x}}, g^\eta h^{\eta'}, \mathcal{H}_{\mathbb{G}}(\mathtt{ev})^\kappa, g^\theta h^{\theta'})$$

και στις δύο εκτελέσεις η λίστα δημοσίων κλειδιών L, το event $\mathtt{ev}$, το μήνυμα $\mathtt{m}$, οι τιμές $\eta, \eta', \kappa, \theta, \theta', \hat{x} \in \mathbb{Z}_q$ είναι σταθερές. Υποθέτουμε πως στη πρώτη κλήση του $\mathcal{A}$ στο $\mathcal{H}_q$ επιστρέφουμε τη τιμή c_{01}, και στη δεύτερη επιστρέφουμε τη τιμή $c_{02} \neq c_{01}$.

Από τις δύο έγκυρες υπογραφές σ_1 και σ_2 και με τα ίδια επιχειρήματα με το θεώρημα 7.4 (εξισώσεις 7.1 και 7.2) λαμβάνουμε τις ακόλουθες εξισώσεις:

$$c_{01} = c_{11} + \cdots + c_{n1},$$
$$c_{02} = c_{12} + \cdots + c_{n2},$$

$$\eta = \tilde{x}_1 + \sum_{i=1}^{n} x_i(c_{i1} + w_{i1}) = \tilde{x}_2 + \sum_{i=1}^{n} x_i(c_{i2} + w_{i2}) \tag{7.4}$$

$$\kappa = \tilde{x}_1 + \hat{x} \sum_{i=1}^{n} (c_{i1} + w_{i1}) = \tilde{x}_2 + \hat{x} \sum_{i=1}^{n} (c_{i2} + w_{i2}) \tag{7.5}$$

$$\theta = r_1 x_D + \sum_{i=1}^{n} w_{i1} = r_2 x_D + \sum_{i=1}^{n} w_{i2} \tag{7.6}$$

Από την εξίσωση 7.6 συμπεραίνουμε ότι είτε ο $\mathcal{A}$ γνωρίζει το x_D, που είναι αντίφαση, ή $\sum_{i=1}^{n} w_{i1} = \sum_{i=1}^{n} w_{i2}$. Επομένως, παρόμοια με την απόδειξη του θεωρήματος 7.4 μπορούμε να συμπεράνουμε ότι υπάρχει τουλάχιστον ένα $j \in [n]$ έτσι ώστε $(c_{j1} + w_{j1}) - (c_{j2} + w_{j2}) \neq 0$.

Θα εξετάσουμε τώρα τις πιθανές τιμές του $\hat{x}$ ώστε ο $\mathcal{A}$ να μπορεί να παράξει δύο τέτοιες υπογραφές γνωρίζοντας μόνο ένα ιδιωτικό κλειδί. Μελετάμε δύο σενάρια:

1. Έστω ότι $(c_{i1} + w_{i1}) = (c_{i2} + w_{i2})$ για κάθε $i \in [n]$ εκτός από $i = j$ για κάποιο $j \in [n]$, δηλαδή, $(c_{j1} + w_{j1}) \neq (c_{j2} + w_{j2})$.

   Τότε από την εξίσωση 7.4 έχουμε ότι

   $$\tilde{x}_1 + x_j(c_{j1} + w_{j1}) = \tilde{x}_2 + x_j(c_{j2} + w_{j2})$$

   και από την εξίσωση 7.5 έχουμε ότι

   $$\tilde{x}_1 + \hat{x}(c_{j1} + w_{j1}) = \tilde{x}_2 + \hat{x}(c_{j2} + w_{j2})$$

   Επομένως $\hat{x} = x_j = \frac{\tilde{x}_2 - \tilde{x}_1}{c_{j1} + w_{j1} - c_{j2} - w_{j2}}$. Η τιμή $\hat{x}$ είναι γνωστή στον $\mathcal{A}$, και αφού ο $\mathcal{A}$ θεωρείται ότι γνωρίζει μόνο ένα ιδιωτικό κλειδί έπεται ότι $j = \pi$.

2. Έστω ότι $(c_{i1} + w_{i1}) = (c_{i2} + w_{i2})$ για όλα τα $i \in [n]$ εκτός από $i = j$ για $j \in \{j_1, j_2\}$. Δηλαδή, $(c_{j_1 1} + w_{j_1 1}) \neq (c_{j_1 2} + w_{j_1 2})$ και $(c_{j_2 1} + w_{j_2 1}) \neq (c_{j_2 2} + w_{j_2 2})$. Ακόμα $\tilde{x}_1 \neq \tilde{x}_2$. Από την εξίσωση 7.4 έχουμε ότι

$$\tilde{x}_1 + x_{j_1}(c_{j_1 1} + w_{j_1 1}) + x_{j_2}(c_{j_2 1} + w_{j_2 1}) = \tilde{x}_2 + x_{j_1}(c_{j_1 2} + w_{j_1 2}) + x_{j_2}(c_{j_2 2} + w_{j_2 2}) \tag{7.7}$$

   - Αν $\pi \in \{j_1, j_2\}$ τότε από την εξίσωση 7.7, ο $\mathcal{A}$ γνωρίζει και x_{j_1} και x_{j_2}, που είναι αντίφαση μιας και ο $\mathcal{A}$ γννωρίζει μόνο ένα ιδιωτικό κλειδί.
   - Αλλιώς, αν $\pi \notin \{j_1, j_2\}$ τότε έπεται ότι:

     $$x_{j_1} + x_{j_2}\phi_2 = \phi_1,$$

     όπου $\phi_2 = \frac{c_{j_2 1} + w_{j_2 1} - c_{j_2 2} - w_{j_2 2}}{c_{j_1 1} + w_{j_1 1} - c_{j_1 2} - w_{j_1 2}}$ και $\phi_1 = \frac{\tilde{x}_2 - \tilde{x}_1}{c_{j_1 1} + w_{j_1 1} - c_{j_1 2} - w_{j_1 2}}$.
     Αυτό συνάγει ότι ο $\mathcal{A}$ μπορεί να λύσει το πρόβλημα MDLR . Από το Θεώρημα 7.1, έχουμε ότι αυτό το πρόβλημα είναι ισοδύναμο με το DLP, και αφού υποθέσαμε ότι το DLP είναι δύσκολο στη $\mathbb{G}$, αυτή η περίπτωση δε πρέπει να υπάρχει.

   Το ίδιο επιχείρημα μπορεί να γενικευτεί για να τρία ή περισσότερα $c_{i1} + w_{i1}$ άνισα με τα αντίστοιχα $c_{i2} + w_{i2}$.

Θεώρημα 7.5. *Συνδεσιμότητα*
Το UDVLRS σχήμα που παραθέσαμε είναι συνδέσιμο στο μοντέλου του τυχαίο μαντείο $\mathcal{RO}$ αν ισχύει η υπόθεση DLOG *στη* $\mathbb{G}$.

Απόδειξη. Έστω ότι ο $\mathcal{A}$ γνωρίζοντας μόνο ένα ιδιωτικό κλειδί μπορεί να παράξει δύο έγκυρες ασύνδετες υπογραφές, δηλαδή δύο υπογραφές σ_1, σ_2 έτσι ώστε για τις ετικέτες σύνδεσής t_1 και t_2 να ισχύει $t_1 \neq t_2$. Τότε από το Λήμμα 7.5 θα ισχύει ότι $t_i = e^{x_i}, i = 1, 2$ όπου $e = \mathcal{H}_{\mathbb{G}}(\mathsf{ev})$. Τότε όμως ο $\mathcal{A}$ θα πρέπει είτε να γνωρίζει δύο διαφορετικά ιδιωτικά κλειδιά είτε να μπορεί να λύσει το DLP, όμως και τα δύο αποτελούν αντιφάσεις. □

Θεώρημα 7.6. *Μη-Δυσφημισιμότητα*
Το UDVLRS σχήμα που παραθέσαμε είναι μη-δυσφημίσιμο στο μοντέλου του τυχαίο μαντείο $\mathcal{RO}$ αν ισχύει η υπόθεση DLOG *στη* $\mathbb{G}$.

Απόδειξη. Έστω αντίπαλος $\mathcal{A}$ ο οποίος μπορεί δοθέντος έγκυρης υπογραφής $\sigma_1 = (t_1, \cdot)$ να παράξει μία έγκυρη υπογραφή $\sigma_2 = (t_2, \cdots)$ έτσι ώστε $t_1 = t_2$, δίχως να γνωρίζει το ιδιωτικό κλειδί που χρησιμοποιήθηκε για να

παραχθεί η σ_1. Θα κατασκευάσουμε έναν PPT αντίπαλο $\mathcal{B}$ ο οποίος δοθέντος δύο στιγμυοτύπων DLP μπορεί να λύσει ένα εκ των δύο χρησιμοποιώντας τον $\mathcal{A}$.

Η είσοδος για τον $\mathcal{B}$ είναι $\mathbb{G}, g, q, X_\pi, X_D$. Ο αντίπαλος $\mathcal{B}$ προσομοιώνει το περιβάλλον για τον $\mathcal{A}$ όπως και στην απόδειξη του Θεωρήματος 7.4. Σε κάποιο σημείο της εκτέλεσης, ο $\mathcal{A}$ επιλέγει το δημόσιο κλειδί $\mathsf{pk}_{\pi'}$ του χρήστη π' και το δίνει στον $\mathcal{B}$.

- Αν $\pi' = \pi$ τότε ο $\mathcal{B}$ προγραμματίζει τα μαντεία όπως στην απόδειξη του Θεωρήματος 7.4 και φτίαχνει την υπογραφή $\sigma_1 = (t_1, \cdot)$ όπου $t_1 = \mathcal{H}_{\mathbb{G}}(\mathsf{ev})^{x_\pi}$ και x_π είναι ο διακριτός λογάριθμος του X_π. Όπως και στην απόδειξη 7.4, ο $\mathcal{B}$ καταφέρνει να κατασκευάσει μία υπογραφή δίχως να ξέρει x_π θέτοντας $t_1 = X_\pi^a$, όπου $e = g^a$ ήταν η απάντηση στη κλήση $\mathcal{H}_{\mathbb{G}}(\mathsf{ev})$. Ο αντίπαλος $\mathcal{B}$ επιστρέφει τη σ_1 στον $\mathcal{A}$.

- Αν $\pi' \neq \pi$ τότε ο $\mathcal{B}$ σταματά.

Ο αντίπαλος $\mathcal{A}$ καταφέρνει, μετά από αλληλεπίδραση με τα μαντεία $\mathcal{RO}, \mathcal{JO}, \mathcal{CO}, \mathcal{SO}, \mathcal{MO}$ που ελέγχονται από τον $\mathcal{B}$, να κατασκευάσει μία υπογραφή

$$\sigma_2 = (t_2, \tilde{x}_2, \tilde{y}_2, r_2, s_2, \{c_{i2}\}_{i=1}^n, \{w_{i2}\}_{i=1}^n)$$

. Ο $\mathcal{B}$ επαναφέρει τον $\mathcal{A}$ και για την ίδια είσοδο στη κλήση στο τυχαίο μαντείο $\mathcal{H}_q$ επιστρέφει μία διαφορετική τιμή στον $\mathcal{A}$, και ο $\mathcal{A}$ παράγει μία ακόμα υπαογραφή $\sigma_2^* = (t_2^*, \tilde{x}_2^*, \tilde{y}_2^*, r_2^*, s_2^*, \{c_{i2}^*\}_{i=1}^n, \{w_{i2}^*\}_{i=1}^n)$. Όμοια με την απόδειξη του Θεωρήματος 7.4 και επειδή $\mathcal{H}_{\mathbb{G}}(\mathsf{ev})^{x_\pi} = t_1 = t_2 = t_2^*$ και $K_2' = K_2^{*\prime}$, λαμβάνουμε τις ακόλουθες εξισώσεις:

$$\tilde{x}_2 + x_\pi \sum_{i=1}^{n}(c_{i2} + w_{i2}) = \tilde{x}_2^* + x_\pi \sum_{i=1}^{n}(c_{i2}^* + w_{i2}^*) \tag{7.8}$$

Χωρίζουμε σε δύο ξεχωριστές περιπτώσεις:

1. Αν $\sum_{i=1}^n(c_{i2} + w_{i2}) = \sum_{i=1}^n(c_{i2}^* + w_{i2}^*)$ και επειδή $\sum_{i=1}^n c_{i2} \neq \sum_{i=1}^n c_{i2}^*$, έχουμε ότι $\sum_{i=1}^n w_{i2} \neq \sum_{i=1}^n w_{i2}^*$. Χρησιμοποιόντας παρόμοια σχέση με την Eq. 7.2 της απόδειξης του 7.4, ο $\mathcal{B}$ μπορεί να βρει το x_D, το διακριτό λογάριθμο του X_D.

2. Αν $\sum_{i=1}^n(c_{i2} + w_{i2}) \neq \sum_{i=1}^n(c_{i2}^* + w_{i2}^*)$ τότε ο $\mathcal{B}$ μπορεί να λύσει την εξίσωση 7.8 και να λάβει x_π.

Αυτό σημαίνει ότι ο $\mathcal{B}$ μπορεί να βρει το διακριτό λογάριθμο είτε του X_π είτε του X_D, το οποίο είναι αντίφαση αφού υποθέσαμε πως το DLP είναι δύσκολο στη $\mathbb{G}$. □

7.5 Σύγκριση UDVLRS και DVLRS

Θα κλείσουμε αυτό το κεφάλαιο με μία γρήγορη σύγκριση των UDVLRS και DVLRS.

Για αρχή οι UDVLRS είναι ελαφρώς μικρότερες από τις DVLRS. Συγκεκριμένα οι UDVLRS αποτελούνται από $2n + 4$ κομμάτια σε αντίθεση με τα $3n + 1$ των DVLRS, εξαιρουμένου των ετικετών σύνδεσης. Το μέγεθος τους όμως παραμένει ακόμα γραμμικό ως προς το δακτυλίο και πρέπει σίγουρα να μικρύνει σε μελλοντικές εργασίες.

Το προφανές πλεονέκτημα των UDVLRS έναντι των DVLRS είναι η τέλεια ανωνυμία που διαθέτουν. Δεν έρχεται όμως αυτή η ανωνυμία δίχως τίμημα μιας και οι UDVLRS έχουν ασθενέστερη συνδεσιμότητα από τις DVLRS κάτι που τις κάνει ευάλωτες σε επιθέσεις συνεννόησης κακόβουλων υπογραφόντων.

Η τελευταία διαφορά των UDVLRS και των DVLRS είναι η γενίκευση της σύνδεσης που προσφέρουν οι UDVLRS έναντι των DVRLS, αφού τώρα πια δεν είναι αναγκαστικό η σύνδεση των υπογραφών να περιορίζεται στον ίδιο δακτύλιο υπογραφής, αλλά γενικεύεται για να λειτουργεί με π.χ. κοινές δραστηριότητες.

Θα κλείσουμε τη ΔΕ με τα κεφάλαια 8 και 9 στα οποία θα μελετήσουμε δύο εφαρμογές των UDVLRS και DVLRS, καθώς και μελλοντικές ερευνητικές κατευθύνσεις που μπορούν να ακολουθηθούν.

Κεφάλαιο 8

Εφαμογές των Συνδέσιμων Υπογραφών Δακτυλίου Καθορισμένου Επαληθευτή με Άνευ Όρων Ανωνυμία

Οι DVLRS και οι UDVLRS είναι νέα primitives και οι εφαρμογές τους δεν είναι ακόμα πλήρως εμφανείς. Παρ' όλα αυτά υπάρχουν δύο πολύ ενδιαφέρουσες που θα παραθέσουμε παρακάτω. Η μία είναι ένα ανώνυμο σύστημα αξιολόγησης που προστατεύει τον αξιολογούμενο και η άλλη είναι ένα σύστημα ανταλλαγής ιατρικών δεδομένων.

8.1 Σύστημα Ανώνυμων Αξιολογήσεων

Η πρώτη εφαρμογή που θα μελετήσουμε δίνεται από τους [13] και προσαρμόζεται άμεσα για τις UDVLRS.

Η ιδέα είναι η εξής: Έστω ότι σε ένα εκπαιδευτικό ίδρυμα οι εκπαιδευτικοί πρέπει να αξιολογούνται από τους μαθητές τους. Ενώ η φύση της αξιολόγησης είναι για τη βελτίωση του μαθήματος και του εκπαιδευτικού ένας προϊστάμενος θα μπορούσε να τις χρησιμοποιήσει για να τιμωρήσει ή και να απωλύσει έναν εκπαιδευτικό. Οι DVLRS και οι UDVLRS μπορούν να προσφέρουν έναν τρόπο ώστε ο εκπαιδευτικός να λαμβάνει ανατροφοδότηση για το μαθημά του χωρίς να έχει το φόβο άδικης αντιμετώπισης από ανωτέρους του.

Το σύστημα αξιολόγησης θα δούλευε με τον παρακάτω τρόπο. Κάθε μαθητής θα μπορεί να κατασκευάζει μία αξιολόγηση για τον εκπαιδευτικό. Η αξιολόγηση θα είναι στην πραγματικότητα μία υπογραφή DVLRS ή UDVLRS. Λόγω της ανωνυμίας που προσφέρουν οι LRS θα μπορεί οποιοσδήποτε να ξέρει

ότι οι αξιολογήσεις προέρχονται από μαθητές, χωρίς όμως να προσδιορίσουν την ακριβή πηγή. Καθ' όλη τη διάρκεια του εξαμήνου ο κάθε μαθητής μπορεί να κατασκευάζει νέες αξιολογήσεις τις οποίες ο εκπαιδευτικός θα μπορεί να ξέρει ότι είναι από το ίδιο άτομο λόγω της συνδεσιμότητας. Με αυτό τον τρόπο έχουμε καλύτερη ανατροφοδότηση του εκπαιδευτικού κατά την εκπαιδευτική διαδικασία.

Ο εκπαιδευτικός θα ενεργεί ως καθορισμένος επαληθευτής. Αν κρίνει αναγκαίο θα μπορεί να κατασκευάζει δικές του αξιολογήσεις και να τις συνδέει με οποιονδήποτε μαθητή, χωρίς όμως να ξέρει ποιος ακριβώς είναι ο μαθητής που συνδέει τις προσομοιώσεις του. Η δυνατότητα αυτή του εκπαιδευτικού του προσφέρει ασφάλεια αφού κανένας πλην του ίδιου και του μαθητή που έχουν συνδεθεί οι υπογραφές δε μπορεί να ξέρει από ποιον προέρχεται πραγματικά η αξιολόγηση, ενώ κανένας από τους δύο δε μπορεί να αποδείξει, ακόμα και αν εξαναγκαστεί, ότι μία αξιολόγηση είναι πραγματική ή προσομοίωση.

8.2 Σύστημα Ανταλλαγής και Ανάλυσης Ιατρικών Δεδομένων

Μια νέα εφαρμογή για τις UDVLRS είναι η ιδέα για ένα σύστημα ανταλλαγής και ανάλυσης ιατρικών δεδομένων.

Ως καθορισμένο επαληθευτή θα έχουμε μία κεντρική αρχή η οποία θέλει να διεξάγει κάποια στατιστική έρευνα, ενώ ο δακτύλιος θα είναι ένα σύνολο από δομές υγείας οι οποίες θα στέλνουν τα δεδομένα των ασθενών στη κεντρική αρχή.

Λόγω της ιδιαιτερότητας των δεδομένων που ανταλλάσονται είναι σημαντικό να ληφθούν επιπλέον βήματα ώστε να διασφαλιστεί η ανωνυμία των δεδομένων. Για αρχή θα πρέπει να γίνει ένας συνδυασμός των UDVLRS με κομμάτια differential privacy [44, 78, 53]. Επιπλέον η μετατροπή των UDVLRS σε sUDVLRS ίσως να είναι χρήσιμη, μαζί με την αποδυνάμωση της μη-μεταφερσιμότητας σε υπολογιστική και την εισαγωγή ενός πρωτοκόλλου αποκύρηξης. Αυτά τα βήματα αποβλέπουν στην αύξηση της ασφάλειας των υπογραφών καθώς και στη διασφάλιση ότι σε περίπτωση κακοδιαχείρισης ή διαστρέβλωσης δεδομένων ο υπαίτιος θα μπορεί να εντωπυστεί και να αποπεμφθεί στις αρμόδιες αρχές.

Κεφάλαιο 9

Επίλογος και Μελλοντικές Κατευθύνσεις

Ενώ οι UDVLRS βελτιώνουν τις DVLRS στο ζήτημα τις ανωνυμίας υπάρχουν ακόμα βελτιώσεις που μπορούν να γίνουν και στις δύο. Το κυριότερο τροχοπέδι για μία πρακτική υλοποίηση τους είναι το μέγεθος. Όντας υπογραφές δακτυλίου το μέγεθος μίας υπογραφής είναι γραμμικό, δηλαδή ανάλογο, ως προς το μέγεθος του δακτυλίου που χρησιμοποιείται. Κάτι τέτοιο φυσικά τις καθιστά μη πρακτικές για χρήση σε τεχνολογίες όπως τα blockchain. Για να προκύψουν μικρότερες υπογραφές υπάρχουν δύο λυσεις οι οποίες μπορούν να χρησιμοποιηθούν. Η πρώτη είναι αυτή των κρυπτογραφικών accumulators [24, 7, 8, 12, 16], η οποία έχει ήδη γίνει σε απλές LRS [76, 6]. Το θετικό με αυτή την προσέγγιση είναι το ότι οι υπογραφές που προκύπτουν είναι σταθερού μεγέθους, αλλά έχουν ως υπόθεση την ύπαρξη έμπιστης τρίτης αρχής και χρείουν έμπιστης εγκατάστασης, κάτι που δεν είναι αποδεκτό για χρήση σε ορισμένα blockchains. Η άλλη επιλογή είναι η χρήση των Bulletproofs [23] σε μια κατασκευή ανάλογη με αυτή που δίνεται στο [79]. Το εν μέρη αρνητικό αυτής της προσέγγισης είναι το γεγονός ότι η προκύπτυσα υπογραφή θα είναι λογαριθμικού μεγέθους ως προς το πλήθος των συμμετεχόντων στο δακτυλίο υπογραφής, όμως σε αντίθεση με τα κρυπτογραφικά accumulators δεν είναι αναγκαία η έμπιστη εγκατάσταση.

Μία ακόμα πιθανή αλλαγή που θα μπορούσε να γίνει και στις UDVLRS και στις DVLRS είναι η χαλάρωση της ιδιότητας της μη-μεταφερσιμότητας από άνευ όρων σε υπολογιστική. Κάτι τέτοιο θα μπορούσε να επιτρέψει σε έναν υπογράφοντα να αποκαλύψει, αν το επιθυμεί, σε κάποια χρονική στιγμή ποιες απο τις συνδεδεμένες με το tag του υπογραφές είναι δικές του και ποιες αποτελούν προσομοίωση. Αυτή η προοπτική θα ανοίξει νέους ορίζοντες αξιοποίησης των υπογραφών σε τεχνολογίες όπως blockchain, IoT, e-voting, συστήματα αξιολόγησης κλπ.

Τέλος είναι σημαντικό να προσπαθήσουμε να κατασκευάσουμε εκδοχές των DVLRS και UDVLRS που θα μπορούν να αντέξουν και στη μετα-κβαντική εποχή (post-quantum cryptography). Ο μόνος επιτυχών του διαγωνισμού του NIST για ασφαλή post-quantum υποψήφιους είναι οι κατασκευές που βασίζονται στα Lattices. Έχουν ήδη υπάρξει ορισμένα σχήματα LRS που βασίζονται σε lattice based cryptography [42, 43, 60] και πιθανώς να μπορούν να αποτελέσουν τη βάση για lattice based DVLRS και UDVLRS.

Βιβλιογραφία

[1] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. «1-out-of-n Signatures from a Variety of Keys». In: *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*. Ed. by Yuliang Zheng. Vol. 2501. Lecture Notes in Computer Science. Springer, 2002, pp. 415–432. DOI: 10.1007/3-540-36178-2_26. URL: https://doi.org/10.1007/3-540-36178-2_26.

[2] Adi Akavia. «Solving Hidden Number Problem with One Bit Oracle and Advice». In: *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Ed. by Shai Halevi. Vol. 5677. Lecture Notes in Computer Science. Springer, 2009, pp. 337–354. DOI: 10.1007/978-3-642-03356-8_20. URL: https://doi.org/10.1007/978-3-642-03356-8_20.

[3] Handan Kilinç Alper and Jeffrey Burdges. «Two-Round Trip Schnorr Multi-signatures via Delinearized Witnesses». In: *CRYPTO 2021*. Vol. 12825. LNCS. Springer, 2021, pp. 157–188.

[4] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. «A Practical and Provably Secure Coalition-Resistant Group Signature Scheme». In: *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*. Ed. by Mihir Bellare. Vol. 1880. Lecture Notes in Computer Science. Springer, 2000, pp. 255–270. DOI: 10.1007/3-540-44598-6_16. URL: https://doi.org/10.1007/3-540-44598-6_16.

[5] Giuseppe Ateniese and Gene Tsudik. «Some Open Issues and New Directions in Group Signatures». In: *Financial Cryptography, Third International Conference, FC'99, Anguilla, British West Indies, February 1999, Proceedings*. Ed. by Matthew K. Franklin. Vol. 1648. Lec-

ture Notes in Computer Science. Springer, 1999, pp. 196–211. DOI: 10.1007/3-540-48390-X_15. URL: https://doi.org/10.1007/3-540-48390-X_15.

[6] Man Ho Au, Sherman S. M. Chow, Willy Susilo, and Patrick P. Tsang. «Short Linkable Ring Signatures Revisited». In: *Public Key Infrastructure, Third European PKI Workshop: Theory and Practice, EuroPKI 2006, Turin, Italy, June 19-20, 2006, Proceedings*. Ed. by Andrea S. Atzeni and Antonio Lioy. Vol. 4043. Lecture Notes in Computer Science. Springer, 2006, pp. 101–115. DOI: 10.1007/11774716_9. URL: https://doi.org/10.1007/11774716_9.

[7] Man Ho Au, Willy Susilo, and Yi Mu. «Constant-Size Dynamic k-TAA». In: *Security and Cryptography for Networks, 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006, Proceedings*. Ed. by Roberto De Prisco and Moti Yung. Vol. 4116. Lecture Notes in Computer Science. Springer, 2006, pp. 111–125. DOI: 10.1007/11832072_8. URL: https://doi.org/10.1007/11832072_8.

[8] Man Ho Au, Patrick P. Tsang, Willy Susilo, and Yi Mu. «Dynamic Universal Accumulators for DDH Groups and Their Application to Attribute-Based Anonymous Credential Systems». In: *Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings*. Ed. by Marc Fischlin. Vol. 5473. Lecture Notes in Computer Science. Springer, 2009, pp. 295–308. DOI: 10.1007/978-3-642-00862-7_20. URL: https://doi.org/10.1007/978-3-642-00862-7_20.

[9] Jean-Philippe Aumasson, Willi Meier, Raphael C.-W. Phan, and Luca Henzen. *The Hash Function BLAKE*. Information Security and Cryptography. Springer, 2014. ISBN: 978-3-662-44756-7. DOI: 10.1007/978-3-662-44757-4. URL: https://doi.org/10.1007/978-3-662-44757-4.

[10] Danai Balla, Pourandokht Behrouz, Panagiotis Grontas, Aris Pagourtzis, Marianna Spyrakou, and Giannis Vrettos. «Designated-Verifier Linkable Ring Signatures with unconditional anonymity». In: *IACR Cryptol. ePrint Arch.* (2022), p. 1138. URL: https://eprint.iacr.org/2022/1138.

[11] Danai Balla, Pourandokht Behrouz, Panagiotis Grontas, Aris Pagourtzis, Marianna Spyrakou, and Giannis Vrettos. «Designated-Verifier Linkable Ring Signatures with Unconditional Anonymity». In: *Algebraic Informatics - 9th International Conference, CAI 2022, Virtual Event, October 27-29, 2022, Proceedings*. Ed. by Dimitrios Poulakis and George

Rahonis. Vol. 13706. Lecture Notes in Computer Science. Springer, 2022, pp. 55–68. DOI: 10.1007/978-3-031-19685-0_5. URL: https://doi.org/10.1007/978-3-031-19685-0_5.

[12] Niko Baric and Birgit Pfitzmann. «Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees». In: *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*. Ed. by Walter Fumy. Vol. 1233. Lecture Notes in Computer Science. Springer, 1997, pp. 480–494. DOI: 10.1007/3-540-69053-0_33. URL: https://doi.org/10.1007/3-540-69053-0_33.

[13] Pourandokht Behrouz, Panagiotis Grontas, Vangelis Konstantakatos, Aris Pagourtzis, and Marianna Spyrakou. «Designated-Verifier Linkable Ring Signatures». In: *Information Security and Cryptology - ICISC 2021 - 24th International Conference, Seoul, South Korea, December 1-3, 2021, Revised Selected Papers*. Ed. by Jong Hwan Park and Seung-Hyun Seo. Vol. 13218. Lecture Notes in Computer Science. Springer, 2021, pp. 51–70. DOI: 10.1007/978-3-031-08896-4_3. URL: https://doi.org/10.1007/978-3-031-08896-4_3.

[14] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. «Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions». In: *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*. Ed. by Eli Biham. Vol. 2656. Lecture Notes in Computer Science. Springer, 2003, pp. 614–629. DOI: 10.1007/3-540-39200-9_38. URL: https://doi.org/10.1007/3-540-39200-9_38.

[15] Mihir Bellare and Phillip Rogaway. «Random Oracles are Practical: A Paradigm for Designing Efficient Protocols». In: *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*. Ed. by Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby. ACM, 1993, pp. 62–73. DOI: 10.1145/168588.168596. URL: https://doi.org/10.1145/168588.168596.

[16] Josh Cohen Benaloh and Michael de Mare. «One-Way Accumulators: A Decentralized Alternative to Digital Sinatures (Extended Abstract)». In: *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*. Ed. by Tor Helleseth. Vol. 765. Lec-

ture Notes in Computer Science. Springer, 1993, pp. 274–285. DOI: 10.1007/3-540-48285-7_24. URL: https://doi.org/10.1007/3-540-48285-7_24.

[17] Adam Bender, Jonathan Katz, and Ruggero Morselli. «Ring Signatures: Stronger Definitions, and Constructions without Random Oracles». In: *J. Cryptol.* 22.1 (2009), pp. 114–138.

[18] Dan Boneh and Xavier Boyen. «Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles». In: *IACR Cryptol. ePrint Arch.* (2004), p. 172. URL: http://eprint.iacr.org/2004/172.

[19] Dan Boneh and Xavier Boyen. «Secure Identity Based Encryption Without Random Oracles». In: *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*. Ed. by Matthew K. Franklin. Vol. 3152. Lecture Notes in Computer Science. Springer, 2004, pp. 443–459. DOI: 10.1007/978-3-540-28628-8_27. URL: https://doi.org/10.1007/978-3-540-28628-8_27.

[20] Dan Boneh and Ramarathnam Venkatesan. «Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes». In: *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*. Ed. by Neal Koblitz. Vol. 1109. Lecture Notes in Computer Science. Springer, 1996, pp. 129–142. DOI: 10.1007/3-540-68697-5_11. URL: https://doi.org/10.1007/3-540-68697-5_11.

[21] Joan Boyar, David Chaum, Ivan Damgård, and Torben Pedersen. «Convertible Undeniable Signatures». In: vol. 19. Aug. 1990, pp. 189–205. ISBN: 978-3-540-54508-8. DOI: 10.1007/3-540-38424-3_14.

[22] Gilles Brassard, David Chaum, and Claude Crépeau. «Minimum Disclosure Proofs of Knowledge». In: *J. Comput. Syst. Sci.* 37.2 (1988), pp. 156–189. DOI: 10.1016/0022-0000(88)90005-0. URL: https://doi.org/10.1016/0022-0000(88)90005-0.

[23] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Gregory Maxwell. «Bulletproofs: Short Proofs for Confidential Transactions and More». In: *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA*. IEEE Computer Society, 2018, pp. 315–334. DOI: 10.1109/SP.2018.00020. URL: https://doi.org/10.1109/SP.2018.00020.

[24] Jan Camenisch and Anna Lysyanskaya. «Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials». In: *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*. Ed. by Moti Yung. Vol. 2442. Lecture Notes in Computer Science. Springer, 2002, pp. 61–76. DOI: 10.1007/3-540-45708-9_5. URL: https://doi.org/10.1007/3-540-45708-9_5.

[25] Melissa Chase and Anna Lysyanskaya. «On Signatures of Knowledge». In: *IACR Cryptol. ePrint Arch.* (2006), p. 184. URL: http://eprint.iacr.org/2006/184.

[26] David Chaum. «Designated Confirmer Signatures». In: *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*. Ed. by Alfredo De Santis. Vol. 950. Lecture Notes in Computer Science. Springer, 1994, pp. 86–91. DOI: 10.1007/BFb0053427. URL: https://doi.org/10.1007/BFb0053427.

[27] David Chaum. «Zero-Knowledge Undeniable Signatures». In: *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, Proceedings*. Ed. by Ivan Damgård. Vol. 473. Lecture Notes in Computer Science. Springer, 1990, pp. 458–464. DOI: 10.1007/3-540-46877-3_41. URL: https://doi.org/10.1007/3-540-46877-3_41.

[28] David Chaum and Hans Van Antwerpen. «Undeniable Signatures». In: *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*. Ed. by Gilles Brassard. Vol. 435. Lecture Notes in Computer Science. Springer, 1989, pp. 212–216. DOI: 10.1007/0-387-34805-0_20. URL: https://doi.org/10.1007/0-387-34805-0_20.

[29] David Chaum and Eugène van Heyst. «Group Signatures». In: *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*. Ed. by Donald W. Davies. Vol. 547. Lecture Notes in Computer Science. Springer, 1991, pp. 257–265. DOI: 10.1007/3-540-46416-6_22. URL: https://doi.org/10.1007/3-540-46416-6_22.

[30] David Chaum and Torben P. Pedersen. «Wallet Databases with Observers». In: *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*. Ed. by Ernest F. Brickell. Vol. 740. Lecture Notes in Computer Science. Springer, 1992, pp. 89–105. DOI:

10.1007/3-540-48071-4_7. URL: https://doi.org/10.1007/3-540-48071-4_7.

[31] Lidong Chen and Torben P. Pedersen. «New Group Signature Schemes (Extended Abstract)». In: *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*. Ed. by Alfredo De Santis. Vol. 950. Lecture Notes in Computer Science. Springer, 1994, pp. 171–181. DOI: 10.1007/BFb0053433. URL: https://doi.org/10.1007/BFb0053433.

[32] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. «Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols». In: *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*. Ed. by Yvo Desmedt. Vol. 839. Lecture Notes in Computer Science. Springer, 1994, pp. 174–187. DOI: 10.1007/3-540-48658-5_19. URL: https://doi.org/10.1007/3-540-48658-5_19.

[33] Victor Shoup Dan Boneh. *A Graduate Course in Applied Cryptography*. Ebook Version 0.5 Jan 2020. URL: https://toc.cryptobook.us/.

[34] Whitfield Diffie and Martin E. Hellman. «New directions in cryptography». In: *IEEE Trans. Inf. Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638. URL: https://doi.org/10.1109/TIT.1976.1055638.

[35] Amos Fiat and Adi Shamir. «How to Prove Yourself: Practical Solutions to Identification and Signature Problems». In: *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*. Ed. by Andrew M. Odlyzko. Vol. 263. Lecture Notes in Computer Science. Springer, 1986, pp. 186–194. DOI: 10.1007/3-540-47721-7_12. URL: https://doi.org/10.1007/3-540-47721-7_12.

[36] Steven D. Galbraith and Wenbo Mao. «Invisibility and Anonymity of Undeniable and Confirmer Signatures». In: *Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings*. Ed. by Marc Joye. Vol. 2612. Lecture Notes in Computer Science. Springer, 2003, pp. 80–97. DOI: 10.1007/3-540-36563-X_6. URL: https://doi.org/10.1007/3-540-36563-X_6.

[37] Taher El Gamal. «A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms». In: *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22,*

1984, Proceedings. Ed. by G. R. Blakley and David Chaum. Vol. 196. Lecture Notes in Computer Science. Springer, 1984, pp. 10–18. DOI: 10.1007/3-540-39568-7_2. URL: https://doi.org/10.1007/3-540-39568-7_2.

[38] Craig Gentry. «Practical Identity-Based Encryption Without Random Oracles». In: *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*. Ed. by Serge Vaudenay. Vol. 4004. Lecture Notes in Computer Science. Springer, 2006, pp. 445–464. DOI: 10.1007/11761679_27. URL: https://doi.org/10.1007/11761679_27.

[39] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. «The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract)». In: *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*. Ed. by Robert Sedgewick. ACM, 1985, pp. 291–304. DOI: 10.1145/22145.22178. URL: https://doi.org/10.1145/22145.22178.

[40] Thomas Haines. «Cronus: Everlasting Privacy with Audit and Cast». In: *Secure IT Systems - 24th Nordic Conference, NordSec 2019, Aalborg, Denmark, November 18-20, 2019, Proceedings*. Ed. by Aslan Askarov, René Rydhof Hansen, and Willard Rafnsson. Vol. 11875. Lecture Notes in Computer Science. Springer, 2019, pp. 53–68. DOI: 10.1007/978-3-030-35055-0_4. URL: https://doi.org/10.1007/978-3-030-35055-0_4.

[41] Helena Handschuh. «SHA Family (Secure Hash Algorithm)». In: (Jan. 2005). DOI: 10.1007/0-387-23483-7_388.

[42] Mingxing Hu and Zhen Liu. «Lattice-Based Linkable Ring Signature in the Standard Model». In: *IACR Cryptol. ePrint Arch.* (2022), p. 101. URL: https://eprint.iacr.org/2022/101.

[43] Mingxing Hu, Weijiong Zhang, and Zhen Liu. «An Improved Lattice-Based Ring Signature with Unclaimable Anonymity in the Standard Model». In: *CoRR* abs/2206.12093 (2022). DOI: 10.48550/arXiv.2206.12093. arXiv: 2206.12093. URL: https://doi.org/10.48550/arXiv.2206.12093.

[44] Yugu Hu, Lina Ge, Guifen Zhang, and Donghong Qin. «Research on Differential Privacy for Medical Health Big Data Processing». In: *20th International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2019, Gold Coast, Australia, December 5-7, 2019*. IEEE, 2019, pp. 140–145. DOI: 10.1109/PDCAT46702.

2019.00036. URL: https://doi.org/10.1109/PDCAT46702.2019.00036.

[45] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. «Designated Verifier Proofs and Their Applications». In: *EUROCRYPT 96*. Vol. 1070. LNCS. Springer, 1996, pp. 143–154.

[46] Ik Rae Jeong, Jeong Ok Kwon, and Dong Hoon Lee. «Ring Signature with Weak Linkability and Its Applications». In: *IEEE Trans. Knowl. Data Eng.* 20.8 (2008), pp. 1145–1148. DOI: 10.1109/TKDE.2008.19. URL: https://doi.org/10.1109/TKDE.2008.19.

[47] Don Johnson, Alfred Menezes, and Scott A. Vanstone. «The Elliptic Curve Digital Signature Algorithm (ECDSA)». In: *Int. J. Inf. Sec.* 1.1 (2001), pp. 36–63. DOI: 10.1007/s102070100002. URL: https://doi.org/10.1007/s102070100002.

[48] Yehuda Lindell Jonathan Katz. *Introduction to Modern Cryptography Second Edition*. CRC Press, Taylor and Francis Group, 2015.

[49] Fabien Laguillaumie and Damien Vergnaud. «Multi-designated Verifiers Signatures». In: *Information and Communications Security, 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004, Proceedings*. Ed. by Javier López, Sihan Qing, and Eiji Okamoto. Vol. 3269. Lecture Notes in Computer Science. Springer, 2004, pp. 495–507. DOI: 10.1007/978-3-540-30191-2_38. URL: https://doi.org/10.1007/978-3-540-30191-2_38.

[50] Jin Li and Yanming Wang. «Universal Designated Verifier Ring Signature (Proof) Without Random Oracles». In: *Emerging Directions in Embedded and Ubiquitous Computing*. Springer, 2006, pp. 332–341.

[51] Xiangxue Li, Dong Zheng, and Kefei Chen. «Efficient Linkable Ring Signatures and Threshold Signatures from Linear Feedback Shift Register». In: *Algorithms and Architectures for Parallel Processing, 7th International Conference, ICA3PP 2007, Hangzhou, China, June 11-14, 2007, Proceedings*. Ed. by Hai Jin, Omer F. Rana, Yi Pan, and Viktor K. Prasanna. Vol. 4494. Lecture Notes in Computer Science. Springer, 2007, pp. 95–106. DOI: 10.1007/978-3-540-72905-1_9. URL: https://doi.org/10.1007/978-3-540-72905-1_9.

[52] Yong Li, Willy Susilo, Yi Mu, and Dingyi Pei. «Designated Verifier Signature: Definition, Framework and New Constructions». In: *Ubiquitous Intelligence and Computing*. Vol. 4611. LNCS. Springer, 2007, pp. 1191–1200. DOI: 10.1007/978-3-540-73549-6_116.

[53] Chi Lin, Zihao Song, Houbing Song, Yanhong Zhou, Yi Wang, and Guowei Wu. «Differential Privacy Preserving in Big Data Analytics for Connected Health». In: *J. Medical Syst.* 40.4 (2016), 97:1–97:9. DOI: 10.1007/s10916-016-0446-0. URL: https://doi.org/10.1007/s10916-016-0446-0.

[54] Helger Lipmaa. «On the CCA1-Security of Elgamal and Damgård's Elgamal». In: *Information Security and Cryptology - 6th International Conference, Inscrypt 2010, Shanghai, China, October 20-24, 2010, Revised Selected Papers*. Ed. by Xuejia Lai, Moti Yung, and Dongdai Lin. Vol. 6584. Lecture Notes in Computer Science. Springer, 2010, pp. 18–35. DOI: 10.1007/978-3-642-21518-6_2. URL: https://doi.org/10.1007/978-3-642-21518-6_2.

[55] Helger Lipmaa, Guilin Wang, and Feng Bao. «Designated Verifier Signature Schemes: Attacks, New Security Notions and a New Construction». In: *ICALP*. Vol. 3580. LNCS. Springer, 2005, pp. 459–471.

[56] Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou. «Linkable Ring Signature with Unconditional Anonymity». In: *IEEE Trans. Knowl. Data Eng.* 26.1 (2014), pp. 157–165.

[57] Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. «Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract)». In: *ACISP*. Vol. 3108. LNCS. Springer, 2004, pp. 325–335.

[58] Joseph K. Liu and Duncan S. Wong. «Linkable Ring Signatures: Security Models and New Schemes». In: *ICCSA 2005*. Vol. 3481. LNCS. Springer, 2005, pp. 614–623.

[59] Joseph K. Liu and Duncan S. Wong. «Solutions to Key Exposure Problem in Ring Signature». In: *Int. J. Netw. Secur.* 6.2 (2008), pp. 170–180.

[60] Xingye Lu, Man Ho Au, and Zhenfei Zhang. «Raptor: A Practical Lattice-Based (Linkable) Ring Signature». In: *Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7, 2019, Proceedings*. Ed. by Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung. Vol. 11464. Lecture Notes in Computer Science. Springer, 2019, pp. 110–130. DOI: 10.1007/978-3-030-21568-2_6. URL: https://doi.org/10.1007/978-3-030-21568-2_6.

[61] Shen Noether. «Ring SIgnature Confidential Transactions for Monero». In: *IACR Cryptol. ePrint Arch.* (2015), p. 1098. URL: http://eprint.iacr.org/2015/1098.

[62] Wakaha Ogata, Kaoru Kurosawa, and Swee-Huay Heng. «The Security of the FDH Variant of Chaum's Undeniable Signature Scheme». In: *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings*. Ed. by Serge Vaudenay. Vol. 3386. Lecture Notes in Computer Science. Springer, 2005, pp. 328–345. DOI: 10.1007/978-3-540-30580-4_23. URL: https://doi.org/10.1007/978-3-540-30580-4_23.

[63] Pascal Paillier. «Public-Key Cryptosystems Based on Composite Degree Residuosity Classes». In: vol. 5. May 1999, pp. 223–238. ISBN: 978-3-540-65889-4. DOI: 10.1007/3-540-48910-X_16.

[64] David Pointcheval and Jacques Stern. «Security Arguments for Digital Signatures and Blind Signatures». In: *J. Cryptol.* 13.3 (2000), pp. 361–396.

[65] Niels Provos and David Mazières. «A Future-Adaptable Password Scheme». In: *Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference, June 6-11, 1999, Monterey, California, USA*. USENIX, 1999, pp. 81–91. URL: http://www.usenix.org/events/usenix99/provos.html.

[66] M. O. Rabin. *DIGITALIZED SIGNATURES AND PUBLIC-KEY FUNCTIONS AS INTRACTABLE AS FACTORIZATION*. Tech. rep. USA, 1979.

[67] Ronald L. Rivest. «The MD5 Message-Digest Algorithm». In: *RFC* 1321 (1992), pp. 1–21. DOI: 10.17487/RFC1321. URL: https://doi.org/10.17487/RFC1321.

[68] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems». In: *Commun. ACM* 21.2 (1978), pp. 120–126. DOI: 10.1145/359340.359342. URL: http://doi.acm.org/10.1145/359340.359342.

[69] Ronald L. Rivest, Adi Shamir, and Yael Tauman. «How to Leak a Secret». In: *ASIACRYPT 01*. Vol. 2248. LNCS. Springer, 2001, pp. 552–565.

[70] Phillip Rogaway and Thomas Shrimpton. «Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance». In: *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*. Ed. by Bimal K. Roy and Willi Meier. Vol. 3017. Lecture Notes in Computer Science. Springer,

2004, pp. 371–388. DOI: 10.1007/978-3-540-25937-4_24. URL: https://doi.org/10.1007/978-3-540-25937-4_24.

[71] Bruce Schneier. «Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)». In: *Fast Software Encryption, Cambridge Security Workshop, Cambridge, UK, December 9-11, 1993, Proceedings*. Ed. by Ross J. Anderson. Vol. 809. Lecture Notes in Computer Science. Springer, 1993, pp. 191–204. DOI: 10.1007/3-540-58108-1_24. URL: https://doi.org/10.1007/3-540-58108-1_24.

[72] Claus-Peter Schnorr. «Efficient Identification and Signatures for Smart Cards». In: *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*. Ed. by Gilles Brassard. Vol. 435. Lecture Notes in Computer Science. Springer, 1989, pp. 239–252. DOI: 10.1007/0-387-34805-0_22. URL: https://doi.org/10.1007/0-387-34805-0_22.

[73] Claus-Peter Schnorr. «Fast Factoring Integers by SVP Algorithms, corrected». In: *IACR Cryptol. ePrint Arch.* (2021), p. 933. URL: https://eprint.iacr.org/2021/933.

[74] Claude E. Shannon. «Communication theory of secrecy systems». In: *Bell Syst. Tech. J.* 28.4 (1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x. URL: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

[75] Yiru Sun, Yanyan Liu, and Bo Wu. «An efficient full dynamic group signature scheme over ring». In: *Cybersecur.* 2.1 (2019), p. 21. DOI: 10.1186/s42400-019-0037-8. URL: https://doi.org/10.1186/s42400-019-0037-8.

[76] Patrick P. Tsang and Victor K. Wei. «Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation». In: *Information Security Practice and Experience*. Vol. 3439. LNCS. Springer, 2005, pp. 48–60.

[77] Brent Waters. «Efficient Identity-Based Encryption Without Random Oracles». In: *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*. Ed. by Ronald Cramer. Vol. 3494. Lecture Notes in Computer Science. Springer, 2005, pp. 114–127. DOI: 10.1007/11426639_7. URL: https://doi.org/10.1007/11426639_7.

[78] Christina M. Wölk. «Methods To Ensure Privacy Regarding Medical Data - Including an examination of the differential privacy algorithm RAPPOR and its implementation in "Cryptool 2"». In: *CoRR* abs/2210.09963 (2022). DOI: 10.48550/arXiv.2210.09963. arXiv: 2210.09963. URL: https://doi.org/10.48550/arXiv.2210.09963.

[79] Tsz Hon Yuen, Muhammed F. Esgin, Joseph K. Liu, Man Ho Au, and Zhimin Ding. «DualRing: Generic Construction of Ring Signatures with Efficient Instantiations». In: *IACR Cryptol. ePrint Arch.* (2021), p. 1213. URL: https://eprint.iacr.org/2021/1213.

[80] Dong Zheng, Xiangxue Li, Kefei Chen, and Jianhua Li. «Linkable Ring Signatures from Linear Feedback Shift Register». In: *Emerging Directions in Embedded and Ubiquitous Computing, EUC 2007 Workshops: TRUST, WSOC, NCUS, UUWSN, USN, ESO, and SECUBIQ, Taipei, Taiwan, December 17-20, 2007, Proceedings*. Ed. by Mieso K. Denko, Chi-Sheng Shih, Kuan-Ching Li, Shiao-Li Tsao, Qing-An Zeng, Soo-Hyun Park, Young-Bae Ko, Shih-Hao Hung, and Jong Hyuk Park. Vol. 4809. Lecture Notes in Computer Science. Springer, 2007, pp. 716–727. DOI: 10.1007/978-3-540-77090-9_66. URL: https://doi.org/10.1007/978-3-540-77090-9_66.

[81] Παναγιώτης Γροντάς Ευστάθιος Ζάχος Αριστείδης Παγουρτζής. *Υπολογιστική Κρυπτογραφία*. ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ, 2015.

[82] Βασίλης Χρυσικόπουλος Στέφανος Γκρίτζαλης Σωκράτης Κάτσικας. *Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές*. Εκδόσεις Παπασωτηρίου, 2011.