Κεφάλαιο 10

Ψηφιακές Υπογραφές

Πάνος Παπαδημητράτος

Informatique et Communications (IC), LCA
Ecole Polytechnique Fédéral de Lausanne (EPFL)
Email: panos.papadimitratos@epfl.ch

10.1 Εισαγωγή

Οι χειρόγραφες υπογραφές είναι κομμάτια πληροφορίας που δεν μπορούν να παραχαραχθούν και πιστοποιούν ότι ο υπογράφων συμφωνεί ή ότι έγραψε το υπογεγραμμένο κείμενο. Με άλλα λόγια, συνδέουν τον υπογράφοντα με το κείμενο με τέτοιο τρόπο ώστε αυτό να μπορεί να επιβεβαιωθεί από οποιονδήποτε, αλλά και ώστε ο υπογράφων να μην μπορεί αργότερα να αρνηθεί ότι έβαλε την υπογραφή του. Κατ' αναλογία, οι *ψηφιακές υπογραφές* είναι κομμάτια δεδομένων, συγκεκριμένα μακρές συμβολοσειρές, τα οποία συνδέουν μία οντότητα του συστήματος, για παράδειγμα έναν υπολογιστή, ένα δικτυακό τόπο, ένα χρήστη, σε οποιαδήποτε ηλεκτρονική πληροφορία, π.χ., ένα μήνυμα ή ένα αρχείο δεδομένων που στάλθηκε στο δίκτυο ή αποθηκεύτηκε σε έναν εξυπηρετητή. Όπως και με τις χειρόγραφες υπογραφές, οι ψηφιακές υπογραφές πρέπει να μπορούν να επιβεβαιωθούν σε περίπτωση αντιδικίας (που μπορεί να προκληθεί από έναν υπογράφοντα που ψεύδεται προσπαθώντας να αρνηθεί ότι δημιούργησε (έβαλε) μια υπογραφή ή κάποιον που ισχυρίζεται μια ψευδή υπογραφή). Κάθε αντικειμενικό τρίτο μέρος πρέπει να μπορεί να επιλύσει ένα πρόβλημα του είδους (χωρίς να χρειάζεται οποιαδήποτε μυστική πληροφορία που κατέχει μονό ο υπογραφών).

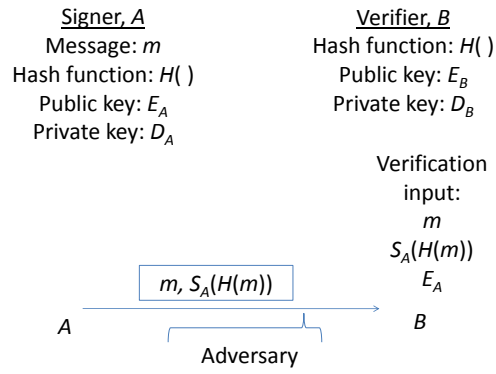
Τα σχήματα ψηφιακών υπογραφών παρέχουν αλγόριθμους για την παραγωγή και για την επιβεβαίωση υπογραφών. Η παραγωγή πρέπει να είναι τέτοια ώστε μόνο η υπογράφουσα οντότητα, A, να μπορεί να υπολογίσει την υπογραφή της πάνω σε κάποιο κείμενο ή μήνυμα m, αλλά και ταυτόχρονα να μην μπορεί αργότερα να αρνηθεί την δημιουργία της υπογραφής. Η επιβεβαίωση πρέπει να είναι έτσι ώστε οποιαδήποτε άλλη οντότητα, B, να μπορεί να επιβεβαιώσει (ή όχι) ότι την υπογραφή πάνω στο m την παρήγαγε ο A. Σε συντομία, υπάρχουν δύο βασικές ιδιότητες που πρέπει να έχουν τα σχήματα ψηφιακών υπογραφών: *γενική ικανότητα επαλήθευσης* και *μη άρνηση αναγνώρισης*. Η χρήση κρυπτογραφίας με δημόσια κλειδιά ταιριάζει απόλυτα με αυτές τις ιδιότητες: με απλά λόγια, ο υπογράφων χρησιμοποιεί το ιδιωτικό του κλειδί για την δημιουργία της υπογραφής και οποιαδήποτε οντότητα επιβεβαιώνει την υπογραφή με το δημόσιο κλειδί του υπογράφοντα.

Ένας *αντίπαλος* θα επιχειρήσει να *παραχαράξει* υπογραφές, δηλαδή να παραχαράξει υπογραφές που θα γίνουν δεκτές ως υπογραφές μιας άλλης οντότητας του συστήματος. Φυσικά, αυτό θα ήταν προφανές για τον αντίπαλο αν είχε στην διάθεση του το ιδιωτικό κλειδί του υποτιθεμένου υπογράφοντος. Αλλά τα ιδιωτικά κλειδιά και άλλη μυστική πληροφορία πρέπει πράγματι να κρατείται μυστική και να μην μοιράζεται από τις οντότητες του συστήματος. Ο αντίπαλος μπορεί να μάθει με ευκολία το δημόσιο κλειδί μιας οντότητας της οποίας θέλει να παραχαράξει την υπογραφή. Επιπλέον, μπορεί να έχει και άλλη γνώση, δια μέσου μηνυμάτων που υπέγραψε στο παρελθόν οι στοχοποιημένη οντότητα: μηνύματα γνωστά στον αντίπαλο (π.χ., δημόσια γνωστά ή υποκλεμμένα), ή μηνύματα που επιλεγεί ο αντίπαλος (π.χ., δοσμένα στην στοχοποιημένη οντότητα για να τα υπογράψει, πιθανώς με προσαρμοστικό τρόπο και με εξαρτήσεις μεταξύ μηνυμάτων και υπογραφών).

Προφανώς, κάθε σχήμα υπογραφών οφείλει να ανθίσταται σε τέτοιου είδους παραχαράξεις. Κατ' αρχή, ο αντίπαλος πρέπει να εμποδιστεί από το να υπολογίσει το ιδιωτικό κλειδί του υπογράφοντος. Αλλιώς, θα μπορούσε να "σπάσει" το κρυπτοσύστημα και να κατόπιν να υπογράφει κατά βούληση εκ μέρους του υπογράφοντος (θύματος). Επιπλέον, ο αντίπαλος πρέπει να εμποδιστεί από το να πράξει έστω και μια έγκυρη υπογραφή για ένα μήνυμα (*existential forgery*). Ή ένα σχετικά λιγότερο ισχυρό ζητούμενο μπορεί να αρκεί σε κάποιες περιπτώσεις: Ο αντίπαλος πρέπει να μην μπορεί να παραχαράξει υπογραφές για κάποιο μήνυμα ή κάποιο τύπο μηνύματος (*selective forgery*). Στις περισσότερες περιπτώσεις, το ισχυρότερο ζητούμενο, η αντίσταση στην παραχάραξη οποιασδήποτε υπογραφής, πρέπει να ικανοποιείται.

Οι υπογραφές χωρίζονται βασικά σε *υπογραφές με προσθήκη*, οι οποίες χρειάζονται το αρχικό μήνυμα σαν είσοδο στον αλγόριθμο επιβεβαίωσης, και σε *υπογραφές με ανάκτηση μηνύματος* οι οποίες αναδημιουργούν το μήνυμα από την ίδια την υπογραφή. Βασικά, τα σχήματα ψηφιακών υπογραφών με ανάκτηση μηνύματος δεν χρειάζονται το αρχικό μήνυμα για την επιβεβαίωση της υπογραφής, αλλά το μήνυμα αναδημιουργείται από την υπογραφή. Στην πράξη, χρησιμοποιούνται οι υπογραφές με προσθήκη, επειδή είναι πιο αποδοτικές και πιο ευέλικτες. Για παράδειγμα, μπορούν υπολογιστούν για μηνύματα κάθε μήκους, σε αντιθεση με τις υπογραφές με ανάκτηση που χρειάζονται μηνύματα σταθερού και συγκεκριμένου μήκους. Μια διαφορετική κατηγοριοποίηση (ανεξάρτητη από το αν είναι το σχήμα με ανάκτηση μηνύματος ή με προσθήκη) κατατάσσει τα σχήματα σε ντετερμινιστικά και τυχαία. Με απλά λόγια, ένα τυχαίο σχήμα υπογραφών παράγει μια διαφορετική υπογραφή κάθε φορά που καλείται ο αλγόριθμος παραγωγής για το ίδιο μνήμα και τον ίδιο υπογράφοντα.

Το Σχήμα 10.1 παρουσιάζει σχηματικά την χρήση υπογραφών με προσθήκη: η υπογραφή δεν υπολογίζεται πάνω στο προς υπογραφή μήνυμα, m, αλλά πάνω σε μια συμπιεσμένη έκδοση του, που υπολογίζεται ως η έξοδος μιας συνάρτησης σύνοψης H. Το $S_A\{\}$ δηλώνει την υπογραφή που δημιουργείται από την οντότητα A, και τα E_A, E_B, είναι τα δημόσια κλειδιά των A, B, και τα D_A, D_B είναι τα ιδιωτικά κλειδιά των A, B. Είναι ενδιαφέρον ότι η πιο κοινά χρησιμοποιούμενες υπογραφές,



Σχήμα 10.1. Δημιουργία και επιβεβαίωση υπογραφής με προσθήκη. Παράδειγμα με μετάδοση ενός υπογεγραμμένου από τον υπογράφοντα, A, προς το παραλήπτη, B, που επιβεβαιώνει την υπογραφή.

αυτές που βασίζονται πάνω στο κρυπτοσύστημα RSA, είναι υπογραφές με ανάκτηση μηνύματος. Παρόλα αυτά, η παραλλαγή τους με προσθήκη είναι αυτή που χρησιμοποιείται ευρέως. Οι υπογραφές ElGamal, που είναι η βάση του τυποποιημένου Digital Signature Algorithm (DSA) (Sec. 10.4), είναι επίσης υπογραφές με προσθήκη.

Σχήματα ψηφιακών υπογραφών έχουν βρει ευρεία χρήση για επαλήθευση και ταυτοποίηση/αναγνώριση, ακεραιότητα δεδομένων, μη άρνηση αναγνώρισης, και πιστοποίηση κλειδιών. Το ηλεκτρονικό εμπόριο έχει μεγάλα οφέλη από την χρήση ψηφιακών υπογραφών, οι οποίες έχουν βρει πολλές εφαρμογές στην ασφάλεια πληροφορίας γενικότερα. Μια από τις πιο σημαντικές είναι η πιστοποίηση δημόσιων κλειδιών σε με μεγάλα δίκτυα. Μια αξιόπιστη οντότητα ή αρχή συνδέει μια ταυτότητα, π.χ. ενός χρηστή, με ένα δημόσιο κλειδί, έτσι ώστε αργότερα άλλες οντότητες να μπορέσουν να επαληθεύσουν το δημόσιο κλειδί χωρίς περαιτέρω βοήθεια από την αξιόπιστη οντότητα/αρχή.

Η ιδέα και η χρησιμότητα των ψηφιακών υπογραφών ανακαλύφθηκε από τους Diffie και Hellman, που πρότειναν μια υπογραφή με ανάκτηση. Η πρώτη μέθοδος ήταν το σχήμα υπογραφών RSA, που παραμένει ακόμα και σήμερα ένα από το πιο πρακτικά σχήματα. Αργότερα, η έρευνα έδωσε πολλά εναλλακτικά σχήματα υπογραφών, με διαφορά πλεονεκτήματα σε ότι αφορά την λειτουργικότητα και την υλοποίηση τους.

Στην συνέχεια αυτού του κεφαλαίου, το πιο διαδεδομένο σχήμα υπογραφών RSA (Ενότητα 10.2) αλλά και το σχήμα ElGamal (Sec. 10.3) και οι παραλλαγές του, που περιλαμβάνουν το πρώτο σχήμα που υιοθετήθηκε από μια κυβέρνηση (Ενότητα 10.4), συζητούνται αρχικά. Για να είναι ευνόητο πως σχετίζονται η κρυπτογράφηση και η αποκρυπτογράφηση με την δημιουργία και επιβεβαίωση υπογραφών αντίστοιχα,

η (απο-)κρυπτογράφηση με τα σχήματα RSA και ElGamal συζητείται σύντομα. Το πρώτο μέρος του κεφαλαίου τελειώνει με την παραλλαγή του DSA με βάση ελλειπτικές καμπύλες (Elliptic Curve Digital Signature Algorithm (EC-DSA)(Ενότητα 10.5). Αυτά τα σχήματα ικανοποιούν τις ιδιότητες της γενικής ικανότητα επαλήθευσης και της μη άρνησης αναγνώρισης. Πέραν αυτών των "κλασικών", άλλα σχήματα που διαφέρουν παρουσιάζονται κατόπιν. Γενική ικανότητα επαλήθευσης ίσως δεν χρειάζεται για κάποιες εφαρμογές. Σε αυτή την κατεύθυνση, αναμφισβήτητες υπογραφές (Ενότητα 10.6), και τυφλές υπογραφές (Ενότητα 10.7) συζητούνται. Για αυτά τα σχήματα, η συζήτηση παρέχει μια εισαγωγή στις εφαρμογές κάθε σχήματος, μια σύντομη επισκόπηση μέρους της σχετικής βιβλιογραφίας, και περισσότερες λεπτομέρειες για ένα αντιπροσωπευτικό σχήμα για κάθε περίπτωση. Με μια σύντομη αναφορά σε άλλους τύπους υπογραφών (Ενότητα 10.8) καταλήγει το κεφαλαίο.

10.2 Υπογραφές RSA

Το κρυπτοσύστημα των Rivest, Shamir και Adelman (RSA) βασίζεται στην μη επιλυσιμότητα του προβλήματος παραγοντοποίησης ακεραίου [1]: Στην ουσία, είναι εύκολο να διαλέξει κανείς δυο πρώτους αριθμούς (δηλαδή, αριθμούς που διαιρούνται μόνο από τον εαυτό τους και την μονάδα) και να υπολογίσει το γινόμενο τους, αλλά είναι υπολογιστικά δύσκολο να υπολογιστούν οι πρώτοι παράγοντες ενός αριθμού n. Η παραγοντοποίηση απαιτεί εκθετικά μεγάλο χρόνο σε σχέση με το μέγεθος του n. Για να δημιουργήσει ένα ζεύγος δημοσίου/ιδιωτικού κλειδιού, μια οντότητα A πρέπει:

Δημιουργία Κλειδιών RSA

1. Επέλεξε δυο μεγάλους πρώτους αριθμούς p και q με (κατά προσέγγιση) ίδιο μήκος.
2. Υπολόγισε το γινόμενο τους $n = pq$.
3. Υπολόγισε $t = (p-1)(q-1)$.
4. Διάλεξε τυχαία έναν ακέραιο e που είναι σχετικά πρώτος με τον t, δηλαδή $1 < e < t$ και $\gcd(e,t) = 1$.
5. Υπολόγισε, χρησιμοποιώντας τον εκτεταμένο αλγόριθμο του Ευκλείδη, τον (μοναδικό)ακέραιο d, τέτοιον ώστε $1 < d < t$ και $ed = 1 \mod t$.

Το δημόσιο κλειδί του A είναι το $E_A = (n, e)$ και το $D_A = d$ είναι το αντίστοιχο ιδιωτικό του κλειδί. Οι e και d καλούνται οι εκθέτες κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα, ο n είναι το υπόλοιπο (modulus), και οι d και n είναι σχετικά πρώτοι. Μετά την δημιουργία των κλειδιών, τα p, q δεν είναι πλέον αναγκαίοι και πρέπει να διαγραφούν μόλις είναι διαθέσιμα τα E_A και D_A. Αν δυο οντότητες A και B χρειάζονται να ασφαλίσουν την επικοινωνία τους, η A πρέπει να βρει το E_B, το δημόσιο κλειδί της B, και αντίθετα. Η A *κρυπτογραφεί* ένα μήνυμα m για την B με

τον ακόλουθο τρόπο:

Κρυπτογράφηση RSA

1. Αναπαράστησε το m ως ακέραιο(ους) στο διάστημα $[0, n-1]$, κόβοντας το m σε ένα αριθμό από τμήματα, m_i, τέτοια ώστε $0 < m_i < n-1$. Αν $m < n-1$, προφανώς, το m είναι το μόνο τμήμα.
2. Χρησιμοποιώντας το $E_B = (n, e)$, υπολόγισε το κρυπτογράφημα $c_i = m_i^e \mod n$ για κάθε m_i.
3. Στείλε κάθε ένα από τα κρυπτογραφήματα c_i στην B.

Κατόπιν, η B *αποκρυπτογραφεί* κάθε ένα από τα c_i που λαμβάνει χρησιμοποιώντας το $D_B = d$:

Αποκρυπτογράφηση RSA

1. Υπολόγισε το $c_i^d \mod n = m_i$.

Η δημιουργία και επιβεβαίωση μιας υπογραφής RSA για το m είναι ουσιαστικά ίδια με την κρυπτογράφηση και αποκρυπτογράφηση του m. Η διαφορά είναι ότι ο υπογράφων κρυπτογραφεί το m χρησιμοποιώντας το ιδιωτικό του κλειδί, και μια άλλη οντότητα επιβεβαιώνει την υπογραφή πάνω στο m χρησιμοποιώντας το δημόσιο κλειδί του υπογράφοντος. Οι υπογραφές RSA είναι ντετερμινιστικές και επιτρέπουν την ανάκτηση του μηνύματος. Στην πράξη όμως, το σχήμα RSA χρησιμοποιείται ως υπογραφή με προσθήκη: η υπογραφή υπολογίζεται όχι πάνω στο m αλλά σε μια σύνοψη του m. Ο υπογράφων, A, εκτελεί τα παρακάτω βήματα για να υπολογίσει την υπογραφή του, S_A, πάνω σε ένα μήνυμα m, χρησιμοποιώντας μια μονόδρομη συνάρτηση σύνοψης h (με εξόδους στο διάστημα $[0, n-1]$):

Δημιουργία Υπογραφής RSA

1. Υπολόγισε το $H = h(m)$.
2. Υπολόγισε το $S_A = H^d \mod n$.

Οποιαδήποτε οντότητα, B, η οποία ξέρει το δημόσιο κλειδί του υπογράφοντος, E_A, μπορεί να επιβεβαιώσει την υπογραφή S_A πάνω στο m:

Επιβεβαίωση Υπογραφής RSA

1. Υπολόγισε το $S^e \mod n = H$.
2. Υπολόγισε το $H' = h(m)$.
3. Σύγκρινε το H' με το H. Αν είναι ίσα, αποδέξου την S_A. Αν όχι, απέρριψέ την.

10.2.1 Πρακτικές Πλευρές των Υπογραφών RSA

Με δεδομένο ένα $E_A = (n, e)$, η ανάκτηση του μηνύματος m από το κρυπτογράφημα c είναι γνωστή ως το πρόβλημα RSA: το να υπολογιστεί ο εκθέτης αποκρυπτογράφησης του RSA, d, από το E_A είναι υπολογιστικά ισοδύναμο με το να παραγοντοποιηθεί ο n, με το τελευταίο να είναι ένα υπολογιστικά δύσκολο πρόβλημα. Παρόλα αυτά, μια σειρά από θέματα σχετικά με την υλοποίηση είναι κρίσιμα για να μην τρωθεί το RSA. Πρώτον, μικρού μεγέθους εκθέτες κρυπτογράφησης, π.χ., $e = 3$, χρησιμοποιούνται σε κάποιες εφαρμογές για πιο αποδοτική κρυπτογράφηση. Αν όμως το ίδιο κρυπτογραφημένο μήνυμα σταλεί σε πολλές οντότητες (με διαφορετικά δημόσια κλειδιά και άρα διαφορετικά υπόλοιπα αφού όλες έχουν $e = 3$), τότε ένας αντίπαλος μπορεί να τα χρησιμοποιήσει για να ανακτήσει το m. Η επιλογή ενός $e = 2^{16} + 1 = 65537$ διατηρεί την αποδοτικότητα του υπολογισμού αλλά εξαλείφει την προαναφερθείσα αδυναμία. Ένα παρόμοιο πρόβλημα ανακύπτει αν το m είναι μικρού μεγέθους. Και στις δυο περιπτώσεις, η προσθήκη μιας τυχαίας επιπρόσθετης συμβολοσειράς στο m πριν την κρυπτογράφηση του εμποδίζει την ανάκτηση από τον αντίπαλο. Σε αντίθεση, η χρήση ενός ειδικού, μικρού σε μέγεθος εκθέτη αποκρυπτογράφησης, d, δεν είναι δυνατή: ο d πρέπει αναγκαστικά να έχει το ίδιο μέγεθος με τον n.

Η διαδικασία υπογραφής και επιβεβαίωσης περιγράφονται με λεπτομέρειες στην τυποποίηση *Public Key Cryptography Standard* (PKCS), και οι μέθοδοι που συζητήθηκαν παραπάνω είναι απλοποιημένες παραλλαγές αυτών της διαδικασίας PKCS #1 [2]. Για παράδειγμα, το H δεν (απο-) κρυπτογραφείται απευθείας, αλλά (απο-) κωδικοποιείται μετά και πριν την (απο-) κρυπτογράφηση για να εμποδιστεί η παραχάραξη υπογραφών. Η κωδικοποίηση συμφωνά με το PKCS διασφαλίζει ότι το μήνυμα (ή ουσιαστικά η σύνοψη του) είναι αρκετά μεγάλο (όχι ένας ομαλός αριθμός μικρότερος του ενός τρίτου του n), έτσι ώστε να μην μπορεί ο αντίπαλος να υπογράψει μηνύματα που μάντεψε σωστά. Επιθέσεις λόγω μικρών εκθετών, ή λόγω αποστολής του ίδιου μηνύματος σε πολλαπλούς αποδεκτές, αποφεύγονται χάρη στο PKCS.

Οι παράμετροι του σχήματος πρέπει να επιλέγονται με προσοχή. Για παράδειγμα, το υπόλοιπο του RSA, n, πρέπει να υπολογιστεί με μεγάλους σε μέγεθος πρώτους αριθμούς, με την ασφάλεια να αντισταθμίζεται από την αποδοτικότητα. Αυτήν την περίοδο, ένα υπόλοιπο μεγέθους τουλάχιστον 1024 bits συνίσταται για τις περισσότερες εφαρμογές. Η παραγοντοποίηση του n δεν είναι πρακτικά επιτεύξιμη για αυτά τα μεγέθη, με p, q να έχουν παρόμοια αλλά άνισα μεγέθη περίπου 512 bits το καθένα. Για προστασία σε βάθος χρόνου, ακόμα μεγαλύτερα υπόλοιπα χρειάζονται, πιθανώς διαφορετικά για κα8ε οντότητα αντί για ένα κοινό n για όλο το σύστημα. Υπόλοιπα 1024 bits (και άρα κλειδιά του ιδίου μεγέθους) προσφέρουν ασφάλεια επιπέδου 80 bits (δηλαδή ισοδύναμη με αυτή συμμετρικών κλειδιών μήκους 80 bits), κλειδιά μήκους 2048 bits αντιστοιχούν σε ασφάλεια επιπέδου 112 bits, κλπ. Η ασφάλεια της πληροφορίας εξαρτάται από την ισχύ των κλειδιών, με συγκεκριμένες συ-

στάσεις διαθέσιμες από το Αμερικανικό Ινστιτούτο Τυποποίησης και Τεχνολογίας (U.S. National Institute of Standards και Technology (NIST)) [3].

10.3 Υπογραφές ElGamal

Οι υπογραφές ElGamal βασίζονται στην μη υπολογισιμότητα του προβλήματος του διακριτού λογαρίθμου σε ένα πεπερασμένο πεδίο: είναι εύκολο να υψωθεί ένας ακέραιος, g, σε μια δύναμη x, αλλά είναι δύσκολο να υπολογιστεί το x από το g^x. για την δημιουργία κλειδιών, κάθε οντότητα, A, τρέχει τον παρακάτω βασικό αλγόριθμο για το σχήμα ElGamal:

Δημιουργία κλειδιών ElGamal

1. Επέλεξε ένα μεγάλου μεγέθους πρώτο αριθμό, p, και ένα γεννήτορα, g, για μια ομάδα $\mathbb{Z}_p^*$.
2. Επέλεξε ένα τυχαίο αριθμό x, τέτοιον ώστε $1 \leq x \leq p-2$.
3. Υπολόγισε $y = g^x \mod p$.

Το δημόσιο κλειδί του A είναι το $E_A = (p, g, y)$ και το ιδιωτικό του κλειδί είναι το $D_A = x$.

Για την κρυπτογράφηση ενός μνήματος, m, για την B, η A αποκτά το E_B και εκτελεί τον παρακάτω αλγόριθμο:

Κρυπτογράφηση ElGamal

1. Αναπαράστησε το m με ένα σύνολο από τμήματα m_i το καθένα στο διάστημα $[0, p-1]$.
2. Διάλεξε ένα τυχαίο ακέραιο, k, τέτοιον ώστε $1 \leq k \leq p-2$.
3. Υπολόγισε τα $a = g^k \mod p$ και $b = my^k \mod p$.

Το κρυπτογράφημα για την B είναι το (a, b). Η B αποκρυπτογραφεί το (a, b), το οποίο είναι δυο φορές το μέγεθος του αρχικού μηνύματος, χρησιμοποιώντας το D_B και εκτελώντας:

Αποκρυπτογράφηση ElGamal

1. Υπολόγισε το $a^{p-1-x} \mod p$.
2. Υπολόγισε το $m = a^{-x}b \mod p$.

Το "σπάσιμο" της κρυπτογράφησης ElGamal είναι ισοδύναμο με το να λυθεί το πρόβλημα του διακριτού λογάριθμου. Παρόλα αυτά, ο τυχαίος αριθμός k πρέπει να επιλεχθεί διαφορετικός και ανεξάρτητα για διαφορετικές κρυπτογραφήσεις. Αλλιώς, η πιθανή γνώση του μηνύματος θα μπορούσε να οδηγήσει στην ανάκτηση άλλων μηνυμάτων που κρυπτογραφηθήκαν με το ίδιο k.

Η υπογραφή ElGamal είναι ένα τυχαίο σχήμα, και δημιουργεί υπογραφές με προσθήκη, χρησιμοποιώντας μια μονόδρομη συνάρτηση σύνοψης $h : \{0,1\}^* \longrightarrow \mathbb{Z}_p$. για να υπογράψει ένα μήνυμα m οποιουδήποτε μήκους, ο A εκτελεί το παρακάτω αλγόριθμο με το ιδιωτικό του κλειδί, D_A:

Δημιουργία Υπογραφής ElGamal

1. Επέλεξε ένα τυχαίο ακέραιο k, τέτοιον ώστε $1 \leq k \leq p-2$ και $\gcd(k, p-1) = 1$. Ο k πρέπει να κρατηθεί μυστικός.
2. Υπολόγισε $r = g^k \mod p$.
3. Υπολόγισε $k^{-1} \mod (p-1)$.
4. Υπολόγισε $s = k^{-1}(h(m) - xr) \mod (p-1)$.

Το ζεύγος (r, s) είναι η υπογραφή του A στο m. Οποιαδήποτε άλλη οντότητα που έχει το E_A μπορεί να επιβεβαιώσει την υπογραφή με τα παρακάτω βήματα:

Επιβεβαίωση Υπογραφής ElGamal

1. Επιβεβαίωσε ότι $1 \leq r \leq p-1$, αλλιώς, απέρριψε την υπογραφή.
2. Υπολόγισε $u_1 = y^r r^s \mod p$.
3. Υπολόγισε $h(m)$.
4. Υπολόγισε $u_2 = g^h(m) \mod p$.
5. Έλεγξε αν $u_1 = u_2$. Αν ναι, αποδέξου την υπογραφή.

Η επιβεβαίωση μιας υπογραφής ElGamal είναι πιο αργή από αυτή μιας υπογραφής RSA με μικρό εκθέτη. Είναι δυνατόν να γίνουν η ύψωση σε δύναμη με υπόλοιπο και ο Ευκλείδειος Αλγόριθμος (Βήματα 2 και 3 της Δημιουργίας Υπογραφής) εκ των προτέρων. Παρόλα αυτά η επιβεβαίωση θα παραμείνει σημαντικά πιο αργή από αυτή του RSA (μια πιο αποδοτική υλοποίηση μπορεί να μειώσει το κόστος κατά έναν παράγοντα 2.5 [4]). Συνιστάται η χρήση υπολοίπου, p, μήκους 1024 bits ή μεγαλύτερου.

10.4 DSA

Ο *Digital Signature Algorithm* (DSA) είναι μια παραλλαγή του σχήματος ElGamal και είναι υπογραφή με προσθήκη. Είναι το πρώτο σχήμα υπογραφών που αναγνωρίστηκε από μια κυβέρνηση: Ο DSA προτάθηκε από το NIST το 1991 και έγινε η Αμερικανική τυποποίηση *Federal Information Processing Standard* (FIPS 186), επίσης γνωστή και ως *Digital Signature Standard* (DSS) [5]. Το DSS απαιτεί την χρήση του Secure Hash Algorithm (SHA-1). Κάθε οντότητα, A, χρειάζεται:

Δημιουργία Κλειδιού DSA

1. Επέλεξε έναν πρώτο q τέτοιον ώστε $2^{N-1} < q < 2^N$.
2. Επέλεξε έναν πρώτο p μήκους L bits, τέτοιον ώστε $q|p-1$.

3. Επέλεξε ένα στοιχείο $h \in \mathbb{Z}_p^*$ και υπολόγισε $g = h^{(p-1)/q} \mod p$. Επανέλαβε μέχρι $g \neq 1$ (δηλαδή, να είναι ο γεννήτορας του μοναδικής κυκλικής ομάδας τάξης q).
4. Επέλεξε ένα τυχαίο ακέραιο x στο διάστημα $[1, q-1]$.
5. Υπολόγισε το $y = g^x \mod p$.

Οι παράμετροι N και L μπορούν να πάρουν ένα από τέσσερα ζεύγη τιμών που προσδιορίζει η τυποποίηση, π.χ., $N = 160$ και $L = 1024$. Το δημόσιο κλειδί είναι $E_A = (p, q, g, y)$ και το ιδιωτικό είναι $D_A = x$. Οι *παράμετροι πεδίου του DSA*, p, q, g, δεν χρειάζεται να είναι μέρος του δημόσιου κλειδιού. Ο DSA απαιτεί να δημιουργούνται τα ζεύγη δημόσιων/ιδιωτικών κλειδιών με βάση τις παραμέτρους πεδίου, οι οποίες είναι δημόσια γνωστές. Φυσικά, όλες οι οντότητες πρέπει να είναι διασφαλισμένες ότι αυτές οι παράμετροι είναι έγκυρες. Με δημόσιες παραμέτρους πεδίου, μπορούμε να πούμε ότι $E_A = y$. Για να υπογράψει ένα μήνυμα m, μια οντότητα A που χρησιμοποιεί την SHA-1 συνάρτηση, την οποία συμβολίζουμε εδώ ως H, πρέπει:

Δημιουργία Υπογραφής DSA

1. Επέλεξε ένα τυχαίο ακέραιο, k, στο διάστημα $[1, q-1]$.
2. Υπολόγισε το $r = (g^k \mod p) \mod q$.
3. Υπολόγισε το $k^{-1} \mod q$.
4. Υπολόγισε το $s = k^{-1}(H(m) + xr) \mod q$.
5. Αν $s = 0$, τότε πήγαινε στο Βήμα 1 (επειδή $s = 0$ συνεπάγεται ότι το $s^{-1} \mod q$, το οποίο χρειάζεται για την επιβεβαίωση της υπογραφής, δεν υπάρχει).

Η υπογραφή στο m είναι το ζεύγος ακεραίων (r, s). Σημειωτέο, αν το k επιλεγεί εκ των προτέρων, δηλαδή πριν το m προς υπογραφή, τα k^{-1} και r (που είναι μέρη της υπογραφής) μπορούν να προ-υπολογιστούν. αλλά είναι απολύτως απαραίτητο να προστατευτούν με τον ίδιο τρόπο που προφυλάσεται το ιδιωτικό κλειδί. Για κάποιες εφαρμογές, ένας τέτοιος πρώιμος υπολογισμός μπορεί να μειώσει την καθυστέρηση δημιουργίας της υπογραφής.

Κάθε οντότητα, B, που ξέρει το E_A μπορεί να επιβεβαιώσει την υπογραφή (r, s) πάνω στο m ως εξής:

Επιβεβαίωση Υπογραφής DSA

1. Επιβεβαίωσε ότι τα r και s είναι ακέραιοι στο διάστημα $[1, q-1]$. Αν όχι, απέρριψε την υπογραφή.
2. Υπολόγισε το $w = s^{-1} \mod q$ και $H(m)$.
3. Υπολόγισε το $u_1 = H(m)w \mod q$ και $u_2 = rw \mod q$.
4. Υπολόγισε το $v = (g^{u_1} y^{u_2} \mod p) \mod q$.
5. Αποδέξου την υπογραφή αν και μόνο αν $v = r$.

Το ιδιωτικό κλειδί για τον DSA έχει το ίδιο μέγεθος με το q, ενώ και τα r και s μέρη της υπογραφής έχουν και αυτά, το καθένα, το ίδιο μέγεθος. Το δημόσιο κλειδί

έχει το ίδιο μέγεθος με το p. Για παράδειγμα, για 80-bit ασφάλεια, ένα δημόσιο κλειδί είναι 1024 bits, ένα ιδιωτικό κλειδί είναι 160 bits, και μια υπογραφή είναι 320 bits.

10.5 EC-DSA

Υπογραφές ElGamal που βασίζονται σε ελλειπτικές καμπύλες πάνω σε πεπερασμένα πεδία προτάθηκαν για πρώτη φορά από τον Koblitz [6] και το Miller [7]. Μια παραλλαγή του DSA με ελλειπτικές καμπύλες, ο *Elliptic Curve DSA* (EC-DSA) [8], έχει τυποποιηθεί από την IEEE [9] (αλλά από τους οργανισμούς ANSI και ISO). Μια οντότητα, A, πρέπει να:

Δημιουργία Κλειδιών EC-DSA

1. Επέλεξε μια ελλειπτική καμπύλη, E, ορισμένη πάνω στο $\mathbb{Z}_p$, τέτοια ώστε ο αριθμός των σημείων στην $E(\mathbb{Z}_p)$ να διαιρείται έναν μεγάλο πρώτο αριθμό n.
2. Επέλεξε ένα σημείο $P \in E(\mathbb{Z}_p)$ τάξης n.
3. Επέλεξε ένα τυχαίο ακέραιο $d \in [1, n-1]$.
4. Υπολόγισε το $Q = dP$.

Το δημόσιο κλειδί είναι το $E_A = (E, P, n, Q)$ και το ιδιωτικό κλειδί είναι το $D_A = d$. Με E, P, n δημόσια γνωστές παραμέτρους, το δημόσιο κλειδί είναι το $E_A = Q$. Είναι χρήσιμο να παρατηρήσουμε την αναλογία με τις παραμέτρους p, q, g του. Η επιλογή της καμπύλης γιατί τον EC-DSA γίνεται με βάση τις συστάσεις από την NIST: η καμπύλη μπορεί να είναι πάνω σε πεδίο πρώτων ή δυαδικών αριθμών, ή μπορεί να ανήκει σε μια τρίτη κατηγορία, τις καμπύλες Koblitz. Οι συμβολισμοί είναι κατ' αντιστοιχία P-xxx, B-xxx και K-xxx, όπου xxx είναι το μήκος, σε αριθμό bit, του πεδίου. Σημειώστε επίσης ότι το d (Βήμα 3 της Δημιουργίας Κλειδιών EC-DSA) και το k χρειάζονται για την δημιουργία υπογραφής (Βήμα 1) και δεν είναι απλώς τυχαίοι αλλά ονομάζονται, για την ακρίβεια, στατιστικά μοναδικοί και απρόβλεπτοι. Για την υπογραφή ενός μηνύματος m, μια A κάνει τα παρακάτω (με το H να είναι η SHA-1):

Δημιουργία Υπογραφής EC-DSA

1. Επέλεξε ένα τυχαίο ακέραιο, k, στο διάστημα $[1, n-1]$.
2. Υπολόγισε το $kP = (x_1, y_1)$ και το $r = x_1 \mod n$. Αν $r = 0$ πήγαινε στο Βήμα 1 (Αν $r = 0$, η εξίσωση υπογραφής (Βήμα 4) δεν περιλαμβάνει το ιδιωτικό κλειδί).
3. Υπολόγισε το $k^{-1} \mod n$.
4. Υπολόγισε το $s = k^{-1}(H(m) + dr) \mod n$.
5. Αν $s = 0$, πήγαινε στο Βήμα 1 (Επειδή $s = 0$ σημαίνει ότι το $s^{-1} \mod n$, που χρειάζεται για την επιβεβαίωση της υπογραφής, δεν υπάρχει).

Η υπογραφή στο m είναι το ζεύγος (r, s). Κάθε οντότητα B που ξέρει το E_A κάνει τα παρακάτω για να επιβεβαιώσει την (r, s) για το m:

EC-DSA Επιβεβαίωση Υπογραφής

1. Επιβεβαίωσε ότι τα r και s είναι ακέραιοι στο $[1, n-1]$. Αν όχι, απέρριψε την υπογραφή.
2. Υπολόγισε το $w = s^{-1} \mod n$ και το $H(m)$.
3. Υπολόγισε το $u_1 = H(m)w \mod n$ και το $u_2 = rw \mod n$.
4. Υπολόγισε το $u_1P + u_2Q = (x_0, y_0)$ και το $v = x_0 \mod n$.
5. Αποδέξου την υπογραφή αν και μόνο αν $v = r$.

Για επίπεδο ασφάλειας παρόμοιο με αυτό του DSA (με $N = 160$-bit q και $L = 1024$-bit p), το n για τον EC-DSA πρέπει να είναι 160 bits με μέγεθος. Τότε, οι υπογραφές του DSA και του EC-DSA έχουν το ίδιο μέγεθος, δηλαδή 320 bits. Συγκρίνοντας με το DSA, παρατηρούμε ότι το EC-DSA έχει ουσιαστικά την ίδια εξίσωση για την δημιουργία υπογραφής, και ότι και οι τα δυο σχήματα χρησιμοποιούν την SHA-1.Αλλά το EC-DSA έχει ένα ενδιαφέρον πλεονέκτημα σε σχέση με το DSA: μία μέθοδος *συμπίεσης σημείου* επιτρέπει την συμπαγή αναπαράσταση ενός σημείου πάνω στην ελλειπτική καμπύλη (π.χ., ένα δημόσιο κλειδί) με ένα στοιχείο πεδίου και ένα επιπρόσθετο bit (αντί για δύο στοιχεία πεδίου). Το πλεονέκτημα του EC-DSA σε ότι αφορά το μέγεθος του κλειδιού μεγαλώνει με το επίπεδο ασφάλειας: π.χ., για 128-bit ασφάλεια, ένα EC-DSA δημόσιο κλειδί μπορεί να αναπαρασταθεί με 33 bytes, το DSA δημόσιο κλειδί με 64 bytes, και το RSA κλειδί με 384 bytes. Αυτό μπορεί να είναι σημαντικό για εφαρμογές όπου πιστοποιητικά πρέπει να μεταδίδονται συχνά, π.χ., από πρωτόκολλα ασφάλειας δικτύων. Η καθυστέρηση επεξεργασίας για κάθε σχήμα υπογραφών εξαρτάται από την υλοποίηση και την πλατφόρμα πάνω στην οποία χρησιμοποιείται. Μια εκτεταμένη λίστα από ελέγχους επιδόσεων είναι διαθέσιμη στο [10].

10.6 Αναμφισβήτητες Υπογραφές

Τα σχήματα *αναμφισβήτητων υπογραφών* από τις κλασσικές ψηφιακές υπογραφές στο ότι η επιβεβαίωση της υπογραφής χρειάζεται την συνεργασία του υπογράφοντος, ή, πιο συγκεκριμένα, την αλληλεπίδραση με τον υπογράφοντα μέσω ενός πρωτοκόλλου. Αυτό σημαίνει ότι οι αναμφισβήτητες υπογραφές δεν είναι γενικώς επιβεβαιώσιμες. Σε αντίθεση, ο υπογράφων ελέγχει πότε μια επιβεβαίωση μπορεί να γίνει και από ποιόν.

Αντίθετα με τις κοινές ψηφιακές υπογραφές, η επιβεβαίωση γίνεται μέσω του πρωτόκολλου *επιβεβαίωσης*. Παρότι μόνο η συγκατάθεση του υπογράφοντος επιτρέπει την επιβεβαίωση, είναι δυνατόν ένας ανειλικρινής υπογράφων να αρνηθεί να συμμετάσχει στο πρωτόκολλο επιβεβαίωσης. Αυτό μπορεί να αντιμετωπιστεί με ένα επιπλέον αμφίδρομο πρωτόκολλο, το πρωτόκολλο *διάψευσης* ή *άρνησης*, που εκτελείται

όταν η επιβεβαίωση αποτυγχάνει. Ουσιαστικά, ελέγχει αν η αποτυχία της επιβεβαίωσης ήταν λόγω μιας άκυρης υπογραφής ή λόγω μιας άκυρης απόκρισης του (ανειλικρινούς) υπογράφοντος. Άρνηση να εκτελέσει το πρωτόκολλο διάψευσης θεωρείται άρνηση να επιβεβαιώσει μια έγκυρη υπογραφή. Άρα, οι αναμφισβήτητες υπογραφές προστατεύουν και τον υπογράφοντα και τον επιβεβαιώνονται: ο υπογράφων ελέγχει την επιβεβαίωση ενώ ο επιβεβαιώνουν ξέρει ότι ο υπογράφων δεν μπορεί να πείσει τον οποιονδήποτε ότι μια σωστή (λάθος) υπογραφή είναι άκυρη (έγκυρη); άρα επιτυγχάνεται μη άρνηση αναγνώρισης.

Οι αναμφισβήτητες υπογραφές προταθήκαν από τον Chaum και τον van Antwerpen το 1989 [11], με προεκτάσεις κατόπιν στο [12] και στο [13]. Στο δεύτερο, οι αναμφισβήτητες υπογραφές έγιναν ασφαλείς κάτω από οποιεσδήποτε συνθήκες, δηλαδή δεν γίνεται να παραπλανήσει ο υπογράφων ακόμα κι αν μια κρυπτογραφική (υπολογιστική) παραδοχή αποδειχτεί όχι τόσο ισχυρή όσο πιστευόταν. Το βασικό σχήμα αναμφισβήτητων υπογραφών υλοποιείται με την χρήση κρυπτογραφίας δημόσιου κλειδιού και βασίζεται στο πρόβλημα διακριτής λογαρίθμησης. Το μέρος της υπογραφής του σχήματος είναι παρόμοιο με αυτό άλλων σχημάτων με βάση την διακριτή λογαρίθμηση.

Εφαρμογές Ο έλεγχος που έχει ο υπογράφων πάνω στην επιβεβαίωση της υπογραφής του είναι χρήσιμη σε διάφορες εφαρμογές όπως η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange (EDI)) ή η ηλεκτρονική δημοσίευση [12,4].

Για την EDI, δηλαδή την δομημένη ανταλλαγή δεδομένων μεταξύ οργανισμών, οι αναμφισβήτητες υπογραφές επιτρέπουν την επιβεβαίωση (υπογραφών) σε περίπτωση διαμάχης αλλά εμποδίζουν οποιονδήποτε από το να επωφεληθεί από την ύπαρξη της υπογραφής, π.χ., με το να την δείξει σε κάποιο τρίτο μέρος. Ακόμα και για προσωπικές συναλλαγές, η επιβεβαίωση μιας υπογραφής ίσως χρειάζεται μόνο σπάνια (π.χ., με περίπτωση διαμάχης) και χωρίς κανείς να έχει ένα αντίγραφό της. Αυτό αυξάνει την προστασία της ιδιωτικότητας ενώ παραμένει η δυνατότητα να αποδοθούν ευθύνες όταν αυτό είναι αναγκαίο.

Σε ένα τραπεζικό περιβάλλον, ας θεωρήσουμε μια οντότητα A (ο πελάτης) που επιθυμεί πρόσβαση σε έναν ασφαλισμένο χώρο υπό τον έλεγχο την οντότητας B (η τράπεζα). Ο ασφαλισμένος χώρος μπορεί να είναι για παράδειγμα ένα δωμάτιο με θησαυροφυλάκιο. Η B απαιτεί από τον A να υπογράψει ένα έγγραφο με την ώρα πρόσβασης προτού την επιτρέψει. Αν ο A χρησιμοποιήσει μια αναμφισβήτητη υπογραφή, τότε η B δεν μπορεί να αποδείξει (κάποια στιγμή αργότερα) σε κανέναν ότι ο A χρησιμοποίησε την εγκατάσταση, εκτός κι αν έχει την άμεση συμμετοχή του A στην διαδικασία επιβεβαίωσης της υπογραφής.

Σε ένα περιβάλλον ηλεκτρονικών εκδόσεων (π.χ., λογισμικού, κειμένων, νέων), ας θεωρήσουμε κάποια μεγάλη εταιρεία, A, που δημιουργεί ένα πακέτο λογισμικού. Η A υπογράφει το πακέτο και το πουλάει στον B, ο οποίος αποφασίζει να κάνει αντίγραφα και να τα μεταπωλήσει σε τρίτους. Ένας τελικός αγοραστής, ο C, είναι αδύνατον να επιβεβαιώσει την αυθεντικότητα του πακέτου χωρίς την συμμετοχή του A. Φυσικά, σε αυτό το σενάριο, ο B δεν μπορεί να εμποδιστεί από το να ξανά-υπογράψει

το πακέτο με την δική του υπογραφή. Αλλά τότε θα χάσει το εμπορικό πλεονέκτημα χάρη στην συσχέτιση με το όνομα του A (χωρίς να παραλείψουμε ότι έτσι ο B θα έκανε ευκολότερο και τον εντοπισμό της παράνομης δραστηριότητάς του). Κάθε πελάτης μπορεί να Each ζητήσει την επιβεβαίωση της γνησιότητας του δημοσιευμένου υλικού. Ο εκδότης/δημιουργός μπορεί να ελέγξει ποιος έχει αυτό το δικαίωμα και να εξουσιοδοτήσει μόνο ένα υποσύνολο χρηστών, πχ, αυτών που πλήρωσαν.

Λεπτομέρειες Σχήματος: Σε συντομία, η επιβεβαίωση μέσω ενός πρωτοκόλλου πρόκλησης-απάντησης (challenge-response): το μέρος που επιθυμεί την επιβεβαίωση της υπογραφής στέλνει μια πρόκληση στον υπογράφοντα και μόλις δει την απάντησή του μπορεί να προχωρήσει στην επιβεβαίωση. Η διαδικασία διάψευσης είναι παρόμοια: μια πρόκληση στέλνεται και η απάντηση από τον υπογράφοντα δείχνει ότι η υπογραφή δεν είναι δικιά του (αν ο υπογραφών δεν πάρει μέρος, το υπογραμμένο κείμενο θεωρείται αυθεντικό). Η πιθανότητα να μπορέσει ένας ανειλικρινής υπογράφων να παραπλανήσει είτε σε ότι αφορά την επιβεβαίωση είτε την διάψευση είναι $1/q$, όπου q είναι ο πρώτος αριθμός στο ιδιωτικό κλειδί του υπογράφοντα. Αν για παράδειγμα ένας αριθμός μήκους 1024 bits χρησιμοποιηθεί, τότε πράγματι η πιθανότητα να αρνηθεί ο υπογράφων την αναγνώριση ενός κειμένου του είναι αμελητέα. Το σχήμα αναμφισβήτητης υπογραφής από το [11], δηλαδή, τα πρωτοκόλλα δημιουργίας κλειδιών, υπογραφής, επιβεβαίωσης και διάψευσης συζητούνται παρακάτω:

Κάθε οντότητα, A, επιλέγει ένα ιδιωτικό και δημόσιο κλειδί με την παρακάτω μέθοδο:

Δημιουργία Κλειδιού για Αναμφισβήτητη Υπογραφή

1. Επέλεξε ένα τυχαίο πρώτο αριθμό q και υπολόγισε τον πρώτο $p = 2q + 1$.
2. Επέλεξε ένα τυχαίο $\beta \in \mathbb{Z}_p^*$ και υπολόγισε $\alpha = \beta^{(p-1)/q} \mod p$. Αν $\alpha = 1$, επανέλαβε το Βήμα 2.
3. Επέλεξε ένα τυχαίο ακέραιο $x \in \{1, 2, \ldots, q-1\}$ και υπολόγισε το $y = \alpha^x \mod p$.

Το Βήμα 2 της δημιουργίας κλειδιού είναι η επιλογή του γεννήτορα α για την υποομάδα τάξης q στο $\mathbb{Z}_p^*$. Το δημόσιο κλειδί είναι το $E_A = (p, \alpha, y)$ και το ιδιωτικό κλειδί το $D_V = x$. Για την δημιουργία μιας υπογραφής στο m (στην ίδια υποομάδα τάξης q), η A πρέπει να εκτελέσει:

Δημιουργία Αναμφισβήτητης Υπογραφής

1. Υπολόγισε το $S = m^\alpha \mod p$.

Κάθε οντότητα, B, μπορεί να επιβεβαιώσει μια υπογραφή, S, με την συνεργασία του A. Για να γίνει αυτό, η B πρέπει να έχει το E_A και να εκτελέσει το παρακάτω πρωτόκολλο με τον A πάνω στην υπογραφή S:

Επιβεβαίωση Αναμφισβήτητης Υπογραφής

1. B:
   - Επέλεξε τυχαίους ακεραίους $x_1, x_2 \in \{1, 2, \ldots, q-1\}$.
   - Υπολόγισε το $z = S^{x_1} y^{x_2} \mod p$.
   - $B \longrightarrow A$: z.
2. A:
   - Υπολόγισε το $w = z^{x^{-1}} \mod p$ (Σημείωση: $xx^{-1} \equiv 1 \mod q$).
   - $A \longrightarrow B$: w.
3. B:
   - Υπολόγισε το $w' = m^{x_1} \alpha^{x_2} \mod p$.
   - Αποδέξου την υπογραφή αν και μόνο αν $w' = w$.

Η άμυνα ενάντια σε έναν υπογράφοντα που αρνείται να συμμετάσχει στο πρωτόκολλο επιβεβαίωσης, ή το εκτελεί λανθασμένα, ή υποστηρίζει λανθασμένα ότι η υπογραφή είναι παραχαραγμένη, είναι η εκτέλεση (από τους ίδιους A και B) το παρακάτω πρωτόκολλου πάνω στην υπογραφή S:

Διάψευση Αναμφισβήτητης Υπογραφής

1. B:
   - Επέλεξε τυχαίους ακεραίους $x_1, x_2 \in \{1, 2, \ldots, q-1\}$.
   - Υπολόγισε το $z = S^{x_1} y^{x_2} \mod p$.
   - $B \longrightarrow A$: z.
2. A:
   - Υπολόγισε το $w = z^{x^{-1}} \mod p$.
   - $A \longrightarrow B$: w.
3. B:
   - Υπολόγισε το $w' = m^{x_1} \alpha^{x_2} \mod p$.
   - Αν $w' = w$, αποδέξου την υπογραφή και τερμάτισε το πρωτόκολλο. Αλλιώς,
   - Επέλεξε τυχαίους ακεραίους $x'_1, x'_2 \in \{1, 2, \ldots, q-1\}$.
   - Υπολόγισε το $z' = S^{x'_1} y^{x'_2} \mod p$.
   - $B \longrightarrow A$: z'.
4. A:
   - Υπολόγισε το $w' = (z')^{x^{-1}} \mod p$.
   - $A \longrightarrow B$: w'.
5. B:
   - Υπολόγισε το $w'' = m^{x'_1} \alpha^{x'_2} \mod p$.
   - Αν $w'' = w'$, αποδέξου την υπογραφή και τερμάτισε το πρωτόκολλο. Αλλιώς,
   - Υπολόγισε το $c = (w\alpha^{-x_2})^{x'_1} \mod p$ και το $c' = (w'\alpha^{-x'_2})^{x_1} \mod p$.
   - Αν $c = c'$, η S είναι παραχαραγμένη. Αλλιώς,
   - Η S είναι έγκυρη και ο A επιχείρησε να διαψεύσει την S.

10.6.1 Μετατρέψιμες Αναμφισβήτητες Υπογραφές

Μια ερώτηση σχετικά με την βασική ιδέα για αναμφισβήτητες υπογραφές προκύπτει: Τι συμβαίνει αν ο αρχικός υπογράφων δεν είναι πλέον διαθέσιμος; Για απαιτηθεί αυτό το ζήτημα, οι *Μετατρέψιμες Αναμφισβήτητες Υπογραφές* προτάθηκαν. Ο αρχικός υπογράφων έχει την ικανότητα να μετατρέπει την αρχική αναμφισβήτητη υπογραφή, παρέχοντας κάποια πληροφορία που επιτρέπει την επιβεβαίωση χωρίς αλληλεπίδραση. Στην πραγματικότητα, υπάρχει ένα ξεχωριστό κλειδί επιβεβαίωσης. Ο υπογράφων μπορεί άρα να μεταβιβάσει την αρμοδιότητα της επιβεβαίωσης υπογραφών σε μια ή περισσότερες οντότητες, ή τελικά ακόμα και να κάνει δημόσιο το κλειδί μετατροπής και άρα να μετατρέψει όλες τις αναμφισβήτητες υπογραφές σε βασικές αναμφισβήτητες. Η μετατροπή μπορεί να γίνει είτε επιλεκτικά για κάποιες υπογραφές είτε γενικά για όλες υπογραφές μιας οντότητας. Οι μετατρέψιμες αναμφισβήτητες υπογραφές προταθήκαν στο [14], που έδειξε πως αναμφισβήτητες υπογραφές μπορούν να μετατραπούν σε γενικά επιβεβαιώσιμες όταν ο υπογράφων παρέχει επίπλων πληροφορία. Στο [15] οι συγγραφείς έδειξαν μια επίθεση ενάντια στο σχήμα αυτό, το οποίο μπορούσε να σπάσει μετά την μετατροπή κάποιων αναμφισβήτητων υπογραφών. Τρόποι διόρθωσης δόθηκαν στα [16] και [17].

Εφαρμογές: Οι μετατρέψιμες υπογραφές είναι ιδανικές όταν η ικανότητα επαλήθευσης πρέπει να προστατευτεί για μια χρονική περίοδο και κατόπιν να απελευθερωθεί. Μια τυπική εφαρμογή για μετατρέψιμες υπογραφές μπορεί να είναι τα εμπιστευτικά αρχεία ενός κράτους. Ακόμα κι αν ένα τέτοιο κείμενο κοινολογηθεί κατά λάθος, η αυθεντικότητά του δεν μπορεί να επιβεβαιωθεί. Αλλά μετά από μερικές δεκαετίες, όταν το σχετικό αρχείο δημοσιοποιηθεί, οι αναμφισβήτητες υπογραφές μπορούν να μετατραπούν έτσι ώστε ο οποιοσδήποτε να μπορέσει να επιβεβαιώσει την εγκυρότητα τους.

Σε άλλες εφαρμογές, μετατρέψιμες υπογραφές επιτρέπουν την επιβεβαίωση στο μέλλον ακόμα και αν ο αρχικός υπογράφων δεν είναι πλέον διαθέσιμος. Η επιπλέον πληροφορία δίνεται σε ένα κοινό σημείο εμπιστοσύνης όταν δημιουργούνται οι υπογραφές. Όταν προκύψει ανάγκη επιβεβαίωσης μιας αρχικής υπογραφής, πχ λόγω μιας νομικής διαμάχης, η πληροφορία στο κοινό σημείο εμπιστοσύνης αποκαλύπτεται, πράγμα που επιτρέπει την μετατροπή της ή των υπογραφών και την επιβεβαίωση χωρίς να παρίσταται ο αρχικός υπογράφων.

Ακόμα κι αν υπογραφές δεν μετατραπούν ποτέ με τον παραπάνω τρόπο, σχήματα μετατρέψιμων υπογραφών μπορεί να είναι χρήσιμα αλλιώς: σε πολλές εφαρμογές, υπογραφές δημιουργούνται μια φορά αλλά επιβεβαιώνονται πολλές φορές. Αν υπάρχει ένα ξεχωριστό κλειδί επιβεβαίωσης, μπορεί να μοιραστεί σε πολλαπλές τοποθεσίες και έτσι να διευκολύνει πολλαπλές επιβεβαιώσεις χωρίς να "φθείρει" την ασφάλεια του κλειδιού για την δημιουργία των υπογραφών.

Λεπτομέρειες Σχήματος: Οι μετατρέψιμες αναμφισβήτητες υπογραφές του [17] συζητούνται παρακάτω. Πέρα από την δημιουργία κλειδιών και υπογραφών, το σχήμα συνίσταται από: (i) την αμφίδρομη επιβεβαίωση της υπογραφής, (ii) την δημιουρ-

γία μιας "απόδειξης'' για την επιλεκτική μετατροπή μιας υπογραφής, και την αντίστοιχη επιβεβαίωση, και (iii) την δημιουργία μιας γενικής "απόδειξης'' για την μετατροπή όλων των υπογραφών. Οι παράμετροι του συστήματος είναι: μια κυκλική ομάδα G πρώτης τάξης q ο γεννήτοράς της g, και μονόδρομες συναρτήσεις σύνοψης $H_l = \{0,1\}^* \times G \to \{0,1\}^l$ και $H_G = \{0,1\}^* \to G$. Κάθε οντότητα, A, δημιουργεί τα κλειδιά της ως εξής:

Δημιουργία Κλειδιών

1. Επέλεξε x_1, x_2 in the group $\mathbb{Z}_q$.
2. Υπολόγισε τα $y_1 = g^{x_1}$ και $y_2 = g^{x_2}$.

Τα x_1 και x_2 είναι το ιδιωτικό κλειδί του A και τα y_1 και y_2 είναι το αντίστοιχο δημόσιο κλειδί. Για να υπογράψει ένα μήνυμα, m, ο A πρέπει:

Δημιουργία Υπογραφής

1. Επέλεξε ένα τυχαίο $k \in \mathbb{Z}_q$.
2. Υπολόγισε το $r = g^k$ και το $\tilde{r} = (H_G(r))^{x_2}$.
3. Υπολόγισε το $c = H_l(m, \tilde{r})$.
4. Υπολόγισε το $s = k - cx_1$.

Η υπογραφή στο m είναι το $(\tilde{r}, s)$ και μπορεί να επιβεβαιωθεί (ή να απορριφθεί) δείχνοντας την ισότητα (ή ανισότητα) των διακριτών λογαρίθμων του $\tilde{r}$ και του y_2. Βασικά, μια οντότητα B που έχει τον ρόλο της επιβεβαίωσης της υπογραφής πρέπει να διευκολυνθεί, από την οντότητα που αποδεικνύει την εγκυρότητα (ή μη) της υπογραφής (δηλαδή του υπογράφοντος A, που ξέρει τον διακριτό λογάριθμο, x, του $y = \alpha^x$), ως προς το να αποφασίσει αν $\log_\beta z = \log_\alpha y$, για β και z στοιχεία της ομάδας. Το αμφίδρομο πρωτόκολλο ισότητας των λογαρίθμων είναι μέρος του πρωτόκολλου επιβεβαίωσης. Για ευκολότερη παρουσίαση, το πρωτόκολλο ισότητας λογαρίθμων παρουσιάζεται ξεχωριστά παρακάτω.

Αμφίδρομη Επιβεβαίωση

1. Ο A, που αποδεικνύει, και ο B, που επιβεβαιώνει, εκτελούν το αμφίδρομο πρωτόκολλο απόδειξης της ισότητας των λογαρίθμων, έτσι ώστε ο να αποφασίσει κατά πόσον $\log_\beta \tilde{r}$ και $\log_g y_2$, είναι ίσα, με $\beta = H_G(g^s y_1^c)$.
2. Αν οι δυο λογάριθμοι είναι ίσοι, η υπογραφή επιβεβαιώνεται, αλλιώς απορρίπτεται.

Αμφίδρομη Απόδειξη Ισότητας Διακριτών Λογαρίθμων

1. Επαληθευτής, V:
   - Επέλεξε ένα τυχαίο v, $u \in \mathbb{Z}_q$.
   - Υπολόγισε το $a = \alpha^u y^v$ (Σημείωση: δέσμευση).

   - $V \longrightarrow P$: a.
2. Αποδεικνύων, P:
   - Επέλεξε ένα τυχαίο k, $\tilde{k}$, $w \in \mathbb{Z}_q$.
   - Υπολόγισε το $r_\alpha = \alpha^k$, $r_\beta = \beta^k$, $\tilde{r}_\alpha = \alpha^{\tilde{k}}$, $\tilde{r}_\beta = \beta^{\tilde{k}}$.
   - $P \longrightarrow V$: r_α, r_β, $\tilde{r}_\alpha$, $\tilde{r}_\beta$.
3. V: $V \longrightarrow P$: u, v (Σημείωση: απόδειξη της δέσμευσης).
4. P: Αν $a \neq \alpha^u y^v$, τερμάτισε το πρωτόκολλο. Αλλιώς
   - Υπολόγισε το $s = k - (v + w)x$.
   - Υπολόγισε το $\tilde{s} = \tilde{k} - (v + w)k$.
   - $P \longrightarrow V$: s, $\tilde{s}$.
5. V:
   - Έλεγξε αν $\alpha^s y^{v+w} = r_\alpha$ και αν $\alpha^{\tilde{s}} y^{v+w} = \tilde{r}_\alpha$ και αν $\beta^{\tilde{s}} y^{v+w} = \tilde{r}_\beta$. Αν ναι,
     - Αν $\beta^s y^{v+w} = r_\beta$, τότε $\log_\beta z = \log_\alpha y$.
     - Αν $\beta^s y^{v+w} \neq r_\beta$, τότε $\log_\beta z \neq \log_\alpha y$.

Επιλεκτική Μετατροπή

1. Εκτέλεσε μια παραλλαγή της Αμφίδρομης Απόδειξης Ισότητας Διακριτών Λογαρίθμων, αλλά χωρίς την δέσμευση (Βήμα 1) και χωρίς την απόδειξη της δέσμευσης (Βήμα 3), και με $w = 0$ και $v = H_8(\alpha, y, \beta, z, r_\alpha, r_\beta, \tilde{r}_\alpha, \tilde{r}_\beta)$ (Το $H_8()$ είναι μια συνάρτηση σύνοψης με οκτώ εισόδους).

Γενική Μετατροπή

1. Ο A παρέχει το x_2.
2. Ο B καταλήγει στο αν η υπογραφή έγκυρη με βάση την ισότητα $H_G(g^s y_1^c)^{x_2} = \tilde{r}$.

10.6.2 Έλεγχος Επιβεβαίωσης

Οι βασικές αναμφισβήτητες υπογραφές δίνουν στον υπογράφοντα έλεγχο πάνω στην επιβεβαίωση της υπογραφής, αλλά μόνο σε ότι αφορά το πότε γίνεται η επιβεβαίωση. Δεν υπάρχει έλεγχος ως προς το ποια οντότητα κάνει την επιβεβαίωση. Αυτό σημαίνει ότι μια εκτέλεση του πρωτόκολλου επιβεβαίωσης μπορεί αργότερα να χρησιμοποιηθεί από οποιαδήποτε οντότητα (που συμμετείχε στο πρωτόκολλο για να πείσει για την εγκυρότητα της υπογραφής. Πράγματι, ο υπογράφων μπορεί να πέσει θύμα ενός αντιπάλου, που μπορεί να τον εκβιάσει με την ικανότητα να κοινολογήσει την υπογραφή αφού το πρωτόκολλο επιβεβαίωσης έχει εκτελεστεί [18]. Μια λύση είναι να επεκταθεί το βασικό σχήμα με την ικανότητα *αποδείξεων με καθορισμένο επαληθευτή*: μόνο ο επαληθευτής του οποίου το δημόσιο κλειδί χρησιμοποιήθηκε στην απόδειξη μπορεί να πειστεί, κανείς άλλος. Με αυτό τον τρόπο, μπορούν να εμποδιστούν πολλαπλοί επαληθευτές που προσπαθούν να πιέσουν έναν υπογράφοντα για επιβεβαίωση μιας υπογραφής πολλαπλές φορές ταυτόχρονα.

Εφαρμογές: Ο έλεγχος επιβεβαίωσης εκτείνει τις αναμφισβήτητες υπογραφές scheme, προσφέροντας επιπλέον προστασία της ιδιωτικότητας χωρίς να θυσιάζει την

δυνατότητα επαλήθευσης. Η δημοσίευση ηλεκτρονικού υλικού μπορεί να έχει ωφέλειες. Με έλεγχο επιβεβαίωσης, ένας πελάτης που πληρώνει μπορεί να επιβεβαιώσει την γνησιότητα του λογισμικού, των νέων, ή των κειμένων, που του παρέχει ο εκδότης/δημιουργός τους. Ταυτόχρονα, ο εκδότης μπορεί να ελέγχει ποιος μπορεί να κάνει αυτή την επαλήθευση. Μετά την επιβεβαίωση, ο επαληθευτής δεν μπορεί να διανείμει το αρχικό πακέτο, επειδή κανείς άλλος δεν θα μπορέσει να πειστεί για την αυθεντικότητα του. Μια άλλη εφαρμογή είναι η ηλεκτρονική ψηφοφορία. Μια ψηφοφόρος μπορεί να πειστεί ότι η ψήφος της μετρήθηκε αλλά κανείς δεν μπορεί να την εκβιάσει ότι θα αποκαλύψει το περιεχόμενο της (επειδή κάθε δυνατή απάντηση δεν θα ήταν πειστική παρά μονό για την ίδια την ψηφοφόρο).

Λεπτομερείς Σχήματος: Βασικά, το σχήμα του [19] που συζητείται παρακάτω, επιλύει την σύγκρουση μεταξύ επαλήθευσης της αυθεντικότητας και προστασίας της ιδιωτικότητας: αντί να αποδεικνύει Θ, ο A αποδεικνύει "είτε το $\Theta = true$ ή εγώ είμαι ο B." Ο B σίγουρα μπορεί να πειστεί, αλλά θα αποτύγχανε αν προσπαθούσε να χρησιμοποιήσει το αποτέλεσμα της απόδειξης για να πείσει κάποιον άλλον. Ένας C δεν θα είχε κανένα λόγω να πιστέψει "είτε το $\Theta = true$ ή εγώ είμαι ο B" απλά και μονό επειδή ο B μπορεί εύκολα να αποδείξει ότι είναι ο εαυτός του. Έστω ο A και ο B ο υπογράφων και ο επαληθευτής αντίστοιχα και το βασικό σχήμα αναμφισβήτητων υπογραφών [12].

Οργάνωση

1. Το p είναι ένας μεγάλος πρώτος αριθμός.
2. Το G_q είναι μια ομάδα τάξης q και ο g ο γεννήτορας της.
3. Ο A επιλέγει το x_A ως το ιδιωτικό κλειδί του και υπολογίζει $y_A = g^{x_A} \mod p$ ως το δημόσιο κλειδί του.
4. Ο B επιλέγει το x_B ως το ιδιωτικό κλειδί του και υπολογίζει το $y_B = g^{x_B} \mod p$ ως το δημόσιο κλειδί του.

Δημιουργία Υπογραφής

1. Ο A υπογράφει ένα μήνυμα m υπολογίζοντας το $s = m^{x_A} \mod p$

Πρωτόκολλο επιβεβαίωσης

1. B:
   - Επέλεξε τυχαίους a, b στην ομάδα $\mathcal{Z}_q$.
   - Υπολόγισε το $v = m^a g^b \mod p$.
   - $B \longrightarrow A$: v.
2. A:
   - Υπολόγισε το $w = v^{x_A} \mod p$.
   - Επέλεξε ένα τυχαίο r στο $\mathcal{Z}_q$ και υπολόγισε το $c = g^w y_B^r \mod p$ (Σημείωση: Δέσμευση).
   - $A \longrightarrow B$: c.

3. B:
   - Συνέθεσε το $z = (m, s, a, b)$.
   - $B \longrightarrow A$: z.
4. A:
   - Επιβεβαίωσε ότι το v έχει την ορθή δομή.
   - $A \longrightarrow B$: w, r (Σημείωση: απόδειξη της δέσμευσης).
5. B:
   - Επιβεβαίωσε ότι το c έχει την ορθή δομή.
   - Επιβεβαίωσε ότι $w = s^a y_A^b \mod p$. Αν όχι, απέρριψε την υπογραφή.

Το σχήμα γίνεται *καθορισμένου επαληθευτή* με την χρήση σχήματος δέσμευσης με σημείο εισόδου παγίδας με το δημόσιο κλειδί του καθορισμένου επαληθευτή.

10.6.3 Αναμφισβήτητες Υπογραφές με βάση το Σχήμα RSA

Οι αναμφισβήτητες υπογραφές βασίζονται κυρίως στην δυσκολία του προβλήματος της διακριτής λογαρίθμησης. Για συμβατότητα με τις δημοφιλείς υπογραφές RSA, αναμφισβήτητες υπογραφές με την ίδια μορφή με RSA υπογραφές προτάθηκαν [20]. Η ουσιαστική διαφορά από τις παραδοσιακές υπογραφές RSA είναι ότι τόσο η υπογραφή όσο και η is that both υπογραφή και επιβεβαίωση RSA exponents need to be kept secret.

Ένας περιορισμός είναι ότι χρειάζονται ειδικά υπόλοιπα (moduli), που είναι γινόμενα ασφαλών πρώτων. Αυτό άλλαξε από το [21], επιτρέποντας γενικών moduli και το [22] παρείχε μετατρέψιμες αναμφισβήτητες υπογραφές. Πέρα από το πλεονέκτημα της συμβατότητας με τις υπογραφές RSA, ενδιαφέρουσες προεκτάσεις είναι δυνατές: (i) Μετατροπή σε υπογραφές γενικώς ή επιλεκτικώς επιβεβαιώσιμες, (ii) Εξουσιοδότηση ενός κοινού σημείου εμπιστοσύνης για επιβεβαίωση και άρνηση υπογραφών, (iii) Καθορισμός επαληθευτή για συγκεκριμένες υπογραφές.

Λεπτομέρειες Σχήματος: Οι αναμφισβήτητες υπογραφές που βασίζονται στο RSA από το [20], η οργάνωση, η δημιουργία, επιβεβαίωση και διάψευση υπογραφών συζητούνται παρακάτω. Κάθε οντότητα, A, για να υπογράψει ένα μήνυμα κάνει τα παρακάτω:

Οργάνωση

1. Επέλεξε n τέτοιον ώστε $n = pq$, $p < q$, $p = 2p' + 1$, και $q = 2q' + 1$, όπου όλοι οι p, q, p', q' είναι πρώτοι.
2. Επέλεξε στοιχεία e, d τέτοιαν ώστε $ed \equiv 1 \mod \phi(n)$.
3. Επέλεξε $w \in Z_n^*$, $w \neq 1$ και υπολόγισε το $S_w = w^d \mod n$.

The ιδιωτικό κλειδί είναι το $D_A = (e, d)$ και το δημόσιο είναι το $E_A = (n, w, S_w)$. Για δημιουργία υπογραφής σε ένα μήνυμα m:

Δημιουργία Υπογραφής

1. Υπολόγισε το $\bar{m} = h(m)$, την μονόδρομη σύνοψη του m.
2. Υπολόγισε την υπογραφή $S_m = \bar{m}^d \mod n$.

Το πρωτόκολλο επιβεβαίωσης υπογραφής εκτελείται από την οντότητα που αποδεικνύει (υπογράφων), P, τον επαληθευτή, V, με εισόδους τα E_A, $\tilde{S}$, και m. Αν $\tilde{S}$ είναι μια έγκυρη υπογραφή, τότε η οντότητα που αποδεικνύει θα πείσει τον επαληθευτή. Αλλιώς, κανενας επαληθευτής δεν μπορει να πεισει τον οποιονδηποτε.

Πρωτόκολλο Επιβεβαίωσης

1. V:
   - Επέλεξε ακεραίους $i, j \leq n$.
   - Υπολόγισε $Q = \tilde{S}^{2i} S_w^j \mod n$.
   - $V \longrightarrow P$: Q.
2. P:
   - Υπολόγισε $A = Q^e \mod n$.
   - $P \longrightarrow V$: A.
3. V:
   - Έλεγξε αν $A = \bar{m}^{2i} w^j \mod n$.
   - Αν η ισότητα ισχύει, αποδέξου το $\tilde{S}$ ως έγκυρη υπογραφή στο m. Αλλιώς μείνε "αναποφάσιστος"

Με το $\tilde{S}$ να είναι μια υποτιθεμένη άκυρη υπογραφή σε κάποιο m, ο αποδεικνύων πρέπει να πείσει τον επαληθευτή ότι η υπογραφή δεν είναι έγκυρη αν έτσι είναι πράγματι. Αλλιώς, κανένας αποδεικνύων δεν θα μπορεί να πείσει οποιονδήποτε επαληθευτή για την εγκυρότητα του $\tilde{S}$.

Πρωτόκολλο Διάψευσης

1. V:
   - Επέλεξε ακεραίους $b \leq k$, $i = 4b$, $j \leq n$.
   - Υπολόγισε το $Q_1 = \tilde{m}^i w^j \mod n$.
   - Υπολόγισε το $Q_2 = \tilde{S}^i S_w^j \mod n$.
   - $V \longrightarrow P$: (Q_1, Q_2).
2. P:
   - Υπολόγισε το $Q_1/Q_2^e = (\bar{m}/\tilde{S}^e)^i$.
   - Υπολόγισε το $i = 4b$ ελέγχοντας όλες τις δυνατές τιμές του ακεραίου $b \leq k$, και θέσε $A = i$. Αν δεν βρεθεί τέτοια τιμή, εγκατέλειψε.
   -
   - $P \longrightarrow V$: A.
3. V:
   - Έλεγξε αν $A = i$. Αν ναι, απέρριψε το $\tilde{S}$ ως υπογραφή στο m. Αλλιώς, μείνε "αναποφάσιστος".

10.7 Τυφλές Υπογραφές

Οι *τυφλές υπογραφές* έχουν την ιδιότητα ότι ο υπογράφων δεν ξέρει το μήνυμα που υπογράφει. Βασικά, τα σχήματα τυφλών υπογραφών είναι πρωτόκολλα με δύο μέρη, ενός αποστολέα A και ενός υπογράφοντα B. Ο A επιλέγει/δημιουργεί ένα μήνυμα m και στέλνει κάποια πληροφορία που αντιστοιχεί σε αυτό το μήνυμα στον B emphχωρίς να αποκαλύπτει το m. Ο B υπογράφει αυτή την πληροφορία και την επιστρέφει στον A, ο οποίος μπορεί τότε να υπολογίσει την υπογραφή του B πάνω στο αρχικό μήνυμα m. Το σημαντικό είναι ότι ο B δεν ξέρει ούτε το m ούτε την υπογραφή που σχετίζεται με αυτό. Μόλις ο A αποκτήσει αυτή την υπογραφή, μπορεί να την δείξει it και anyone can validate it. But the sender, A, cannot be associated with the signed μήνυμα.

Εφαρμογές: Οι τυφλές υπογραφές βελτιώνουν την προστασία της ιδιωτικότητας με το να κρύβουν τις λεπτομέρειες συναλλαγών ενώ επιτρέπουν τον έλεγχο και την ασφάλεια των συναλλαγών [23].

Τα *ηλεκτρονικά μετρητά* είναι μια σημαντική εφαρμογή για τυφλές υπογραφές. Ο αποστολέας, A, είναι ένας πελάτης μιας τράπεζας και δεν θέλει να επιτρέψει στην τράπεζα, δηλ., στον υπογράφοντα, B, να μπορεί να συσχετίσει το m, δηλ., την χρηματική αξία που αργότερα ο A θα θελήσει να ξοδέψει. Όταν αργότερα η υπογεγραμμένη αξία δειχθεί, για πληρωμή από την τράπεζα, B, είναι αδύνατο για την τράπεζα να καθορίσει ποιος είναι ο A. Με απλά λόγια, κάθε "νόμισμα" με προκαθορισμένη αξία που δημιούργησε ο πελάτης στέλνεται στην τράπεζα κωδικοποιημένο. Η τράπεζα χρεώνει το λογαριασμό του πελάτη, υπογράφει το κωδικοποιημένο νόμισμα, και το επιστρέφει στον πελάτη. Τότε, ο πελάτης εξάγει την υπογραφή από την κωδικοποίηση και αποκτά μια έγκυρη υπογραφή στο σκέτο νόμισμα. Αργότερα, για να κάνει μια πληρωμή χρησιμοποιεί αυτό το ηλεκτρονικό νόμισμα, και ο έμπορος επιβεβαιώνει την εγκυρότητα του με το να το προωθήσει στην τράπεζα. Αν το νόμισμα είναι έγκυρο, η τράπεζα το σημαδεύει ως χρησιμοποιημένο, πιστώνει τον λογαριασμό του εμπόρου, και επιβεβαιώνει την επιτυχία της συναλλαγής.

Ηλεκτρονική ψηφοφορία είναι άλλη μια εφαρμογή για τυφλές υπογραφές. Είναι χρήσιμο να θεωρήσουμε την αναλογία με την ψήφο εξ αποστάσεως με (χάρτινα) έντυπα: Ο ψηφοφόρος χρησιμοποιεί φάκελους με χαρτί καρμπόν, έτσι ώστε η υπογραφή στο εξωτερικό του φάκελου να αφήνει ένα αντίγραφο της υπογραφής σε ένα φύλλο χαρτί μέσα στο φάκελο. Αρχικά, ο ψηφοφόρος βάζει το ψηφοδέλτιο του μέσα στον φάκελο από χαρτί καρμπόν, μετά βάζει αυτό τον φάκελο μέσα σε ένα δεύτερο κανονικό φάκελο, και ταχυδρομεί τον "διπλό'' φάκελο στην επιτροπή εκλογών. Έχοντας την διεύθυνση επιστροφής στον εξωτερικό φάκελο, η επιτροπή ελέγχει τους εκλογικούς καταλόγους έτσι ώστε να εξασφαλίσει ότι πρόκειται για εγγεγραμμένο ψηφοφόρο. Κατόπιν, ανοίγει τον εξωτερικό φάκελο, και υπογράφει την εξωτερική επιφάνεια του εσωτερικού φακέλου που έχει το καρμπόν, βάζοντας έτσι την υπογραφή της επιτροπής στο ψηφοδέλτιο. Κατόπιν, βάζουν (η επιτροπή) τον φάκελο που είναι υπενδεδυμένος με καρμπόν μέσα σε έναν κανονικό φάκελο και τον αποστέλ-

λουν πίσω στον ψηφοφόρο. Το αποτέλεσμα αυτής της διαδικασίας είναι ότι μόνο εγγεγραμμένοι ψηφοφόροι λαμβάνουν τα υπογεγραμμένα ψηφοδέλτια. Κατά την δεύτερη φάση, όταν η ψηφοφορία καθαυτή λαμβάνει χώρα, ο ψηφοφόρος ταχυδρομεί τον υπογεγραμμένο φάκελο χωρίς την διεύθυνση του (του αποστολέα). Η επιτροπή μαζεύει και καταμετρά τους ψήφους αφού τους βγάλει από τους φακέλους τους (τους υπενδεδυμένους με καρμπόν). Όμως, η υπογραφή της παραμένει πάνω στους ψήφους, άρα οποιοσδήποτε μπορεί δημόσια να επιβεβαιώσει τα εκλογικά αποτελέσματα.

Οι τυφλές υπογραφές προτάθηκαν από τον Chaum στο [23] το οποίο περιγράφει τα κίνητρα και βασικές ιδέες του σχήματος, με τα [24,25] να παρουσιάζουν υλοποιήσεις και τα [26,27] να εξηγούν πως μπορεί να γίνουν ηλεκτρονικές πληρωμές χωρίς ίχνη. Στο [28] δείχθηκε ότι υπάρχει ένα σχήμα τυφλής υπογραφής που ικανοποιεί τις ισχυρές απαιτήσεις ασφάλειας που διατυπώθηκαν στο [25]. Στο [29] προτάθηκε η ιδέα της δίκαιης τυφλής υπογραφής, που επιτρέπει σε ένα κοινό σημείο εμπιστοσύνης να άρει την ιδιότητα να μην αφήνοντας ίχνη σε περίπτωση που προκύψουν νομικά θέματα.

Λεπτομέρειες Σχήματος: Θεωρώντας ξανά την οργάνωση του RSA, έστω $n = pq$ και S_B την υπογραφή RSA από μια οντότητα B με κλειδιά $E_B = (n, e)$ και $D_B = d$. Ένας αποστολέας, A, αποκτά το δημόσιο κλειδί E_B και για ένα μήνυμα $0 \leq m \leq n-1$ κάνει τα παρακάτω:

Πράξη Απόκρυψης

1. Επέλεξε ένα k τέτοιον ώστε $0 \leq k \leq n-1$ και $\gcd(n, k) = 1$.
2. Υπολόγισε το $m^* = mk^e \mod n$.
3. $A \longrightarrow B$: m^*.

Η τιμή m^* αποκρύπτεται ("τυφλώνεται") από τον τυχαίο k που επιλέγει ο αποστολέας, έτσι ώστε ο υπογράφοντας να μην εξάγει καμία χρήσιμη πληροφορία. Ο υπογράφων, B, κάνει κατόπιν τα παρακάτω:

Πράξη Υπογραφής

1. Υπολόγισε το $s^* = (m^*)^d \mod n$.
2. $B \longrightarrow A$: s^*.

Το s^* είναι ουσιαστικά η υπογραφή από τον B στο m^*. Για να αποκτήσει την υπογραφή στο m, ο αποστολέας, A, κάνει τα παρακάτω:

Πράξη Αποκάλυψης

1. Υπολόγισε το $s = k^{-1}s^* \mod n$.

Η υπογραφή στο m είναι το s.

Σε ότι αφορά στη χρήση και δημιουργία ηλεκτρονικών μετρητών και συναλλαγών μετρητών που δεν αφήνουν ίχνη, αυτό πρέπει να είναι δύσκολο εκτός αν γίνονταν σε συνεργασία με μια τράπεζα, B. Παρακάτω είναι τα βασικά του σχεδίου του [27], με έναν πελάτη να συμβολίζεται ως A:

Οργάνωση

1. Ο $n = pq$ με p και q γνωστά μόνο στην τράπεζα.
2. Η f είναι μια συνάρτηση σύνοψης.
3. Κάθε νόμισμα έχει μια σταθερή αξία ενός \$.

Έκδοση Μετρητών

1. A:
   - Επέλεξε τυχαίους x και r.
   - $A \longrightarrow B$: $a = r^3 f(x) \mod n$.
2. B:
   - Υπολόγισε το $b = \sqrt[3]{a} = r\sqrt[3]{f(x)}$.
   - Κάνε ανάληψη ενός \$ από τον λογαριασμό του A.
   - $B \longrightarrow A$: b.
3. A:
   - Απέσπασε το $c = \sqrt[3]{f(x)}$.

Πληρωμή

1. Ο A στέλνει τα x, C σε έναν άλλο πελάτη (της τράπεζας), πχ., ένα κατάστημα για να πληρώσει ένα \$
2. Το κατάστημα επικοινωνεί αμέσως με την τράπεζα, για να ελέγξει την ισχύ του ηλεκτρονικού νομίσματος (δηλ., ότι το νόμισμα δεν κατατέθηκε ήδη)
3. Εάν το νόμισμα ισχύει, η τράπεζα επιβεβαιώνει τα σημάδια συναλλαγής και το νόμισμα ως χρησιμοποιημένο

10.8 Other Signature Schemes

Υπογραφές Fail-Stop (FS): Αυτά τα σχήματα επιτρέπουν σε οποιαδήποτε οντότητα A να αποδείξει ότι μια υπογραφή που κάποιος ισχυρίζεται ότι παράχθηκε από τον A είναι μια παραχάραξη. Αυτό μπορεί να γίνει με το να δείξει ότι η υπόθεση στην οποία βασίζεται ο μηχανισμός υπογραφών παραβιάστηκε. Η παρουσίαση αποδείξεων για την παραχάραξη δεν στηρίζεται σε οποιαδήποτε κρυπτογραφική υπόθεση, και μπορεί να αποτύχει με κάποια μικρή πιθανότητα (ανεξάρτητα από τη υπολογιστική ισχύ του παραχαράκτη). Το πλεονέκτημα των υπογραφών αυτών είναι ότι ακόμα κι αν ένας πολύ ισχυρός αντίπαλος παραχαράξει μια υπογραφή, αυτό μπορεί να ανιχνευθεί και το FS σχήμα να πάψει να χρησιμοποιείται: “Αποτυγχάνω-έπειτα-Σταματώ’’.

Βασικά, εάν ένας υπογράφων ακολουθήσει πράγματι το FS σχήμα, τότε μια έγκυρη υπογραφή γίνεται αποδεκτή. Ένας υπολογιστικά ισχυρός παραχαράκτης δεν μπορεί να "περάσει'' την επαλήθευση υπογραφών του FS σχήματος. Αλλά εάν ο παραχαράκτης κατόρθωσε να δημιουργήσει ένα μήνυμα που ανακριβώς περνά την επαλήθευση, τότε με υψηλή πιθανότητα ο αληθινός υπογράφων μπορεί να παραγάγει μια απόδειξη της παραποίησης. Τέλος, οποιαδήποτε υπογραφή που παράγεται από έναν νόμιμο υπογράφοντα δεν μπορεί αργότερα να θεωρηθεί παραποιημένη. Οι FS υπογραφές καθορίστηκαν τυπικά στο [30,31], και αποδοτικότερες τεχνικές προτάθηκαν αργότερα στο [32] και πρόσφατες εργασίες όπως το [33] για παράδειγμα παρέχουν μικρότερους μήκους FS υπογραφές.

Υπογραφές Μιας Χρήσης: Σχήματα υπογραφών μιας χρήσης μπορούν να χρησιμοποιηθούν για να υπογράψουν, το περισσότερο ένα μήνυμα. Διαφορετικά, οι υπογραφές μπορούν να παραχαραχθούν. Οι υπογραφές μιας χρήσης του Rabin [34] ήταν μια από τις πρώτες προτάσεις ψηφιακών υπογραφών οποιουδήποτε είδους. Επιτρέπουν την υπογραφή ενός και μόνο μηνύματος, η επαλήθευση των υπογραφών μπορεί να γίνει μόνο μια φορά, και απαιτεί την αλληλεπίδραση μεταξύ του υπογράφοντος και του ελεγκτή. Σε γενικές γραμμές, ένα νέο δημόσιο κλειδί απαιτείται για κάθε μήνυμα που υπογράφεται. Η δημόσια πληροφορία που είναι απαραίτητη για να εκλεχθούν οι υπογραφές μιας καλείται συχνά παράμετροι επικύρωσης. Η βασική ιδέα της δέσμευσης σε κλειδιά μέσω των μονόδρομων συναρτήσεων [35] ήταν αρχικά θεωρητικής αξίας, αλλά βελτιώθηκε αργότερα από τα σχήματα όπως το [36].

Συνολικά, οι υπογραφές μιας χρήσης έχουν το πλεονέκτημα της αποδοτικής παραγωγής και της επαλήθευσης υπογραφών. Στα αρνητικά, είναι το μέγεθος εκείνων των υπογραφών (γενικά, κάποια Kbytes). Πιο πρόσφατες εργασίες προσέφεραν βελτιώσεις, παραδείγματος χάριν, το [37] εστίασε στη γρήγορη επαλήθευση υπογραφών, ή το [38] στη γρήγορη παραγωγή υπογραφών. Βασικά, η επαναχρησιμοποίηση του ίδιου κλειδιού (τέτοια σχέδια αποκαλούνται "υπογραφές κάμποσων χρήσεων'') υπονοεί μια μικρή πιθανότητα επιτυχημένης επίθεσης, κάτι που μπορεί να είναι στο κατάλληλο (αποδεκτά χαμηλό) επίπεδο για μια δεδομένη εφαρμογή. Εάν πολλαπλά μηνύματα πρόκειται να υπογραφούν, οι υπογραφές μιας χρήσης μπορούν να συνδυαστούν με τεχνικές για την επικύρωση των παραμέτρων επικύρωσης - παραδείγματος χάριν, ένα τέτοιο πρόσφατο σχήμα [39] στηρίζεται σε μια παραλλαγή των δέντρων Merkle [40].

10.9 Αναφορές

1. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM*, vol. 27, pp. 120–126, February 2000.
2. "PKCS1:RSA Encryption Standard," Tech. Rep. Version 1.5, RSA Laboratories, November 1993.
3. NIST, "Special Publication 800-57: Recommendation for Key Management. Part 1: General Guideline," Tech. Rep. IST-2002-507932-D.VAM.9, January 2007.
4. A. Menezes, P. V. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. October 1996.
5. "Digital Signature Standard (DSS)," Tech. Rep. FIPS 186, Federal Information Processing Standards Publication, May 1994.
6. N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–209, 1987.
7. V. Miller, "Use of Elliptic Curve Cryptosystems," *Advances in Cryptology - CRYPTO 85 (LNCS 218)*, pp. 417–426, 1986.
8. D. B. Johnson and A. J. Menezes, "Elliptic curve DSA (ECSDA): An Enhanced DSA," in *7th USENIX Security Symposium*, 1998.
9. I. 1363a 2004, "IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional techniques," tech. rep., 2004.
10. D. Page, D. Bernstein, and T. Lange, "Report on eBATS Performance Benchmarks," Tech. Rep. IST-2002-507932-D.VAM.9, European Network of Excellence in Cryptology, March 2007.
11. D. Chaum and H. Antwerpen, "Undeniable Signatures," in *Advances in Cryptology - CRYPTO '89*, pp. 212–216, August 1990.
12. D. Chaum, "Zero-knowledge Undeniable Signatures (extended abstract)," in *EUROCRYPT '90*, pp. 458–464, 1990.
13. D. Chaum, E. Heijst, and B. Pfitzmann, "Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer," in *CRYPTO '91*, pp. 470–484, 1992.
14. J. Boyar, D. Chaum, I. Damgård, and T. Pedersen, "Convertible Undeniable Signatures," in *Advances in Cryptology - CRYPTO '90*, pp. 189–205, 1991.
15. M. Michels, H. Petersen, and P. Horster, "Breaking and Repairing a Convertible Undeniable Signature Scheme," in *3rd ACM conference on Computer and Communications Security (CCS)*, pp. 148–152, 1996.
16. I. Damgård and T. Pedersen, "New Convertible Undeniable Signature Schemes," in *Advances in Cryptology - EUROCRYPT '96*, pp. 372–386, May 1996.
17. M. Michels and M. Stadler, "Efficient Convertible Undeniable Signature Schemes," in *Selected Areas in Cryptography (SAC)*, pp. 231–244, 1997.
18. M. Jakobsson, "Blackmailing Using Undeniable Signatures," in *Advances in Cryptology - EUROCRYPT '94*, pp. 425–427, May 1994.
19. M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated Verifier Proofs and Their Applications," in *Advances in Cryptology - EUROCRYPT '96*, pp. 143–154, May 1996.
20. R. Gennaro, H. Krawczyk, and T. Rabin, "RSA-Based Undeniable Signatures," *Journal of Cryptology*, vol. 13, no. 4, pp. 397–416, 2000.
21. S. Galbraith, W. Mao, and K. Paterson, "RSA-Based Undeniable Signatures for General Moduli," in *CT-RSA: The Cryptographer's Track, RSA Conference on Topics in Cryptology*, pp. 200–217, 2002.
22. K. Kurosawa and T. Takagi, "New Approach for Selectively Convertible Undeniable Signature Schemes," in *Advances in Cryptology - ASIACRYPT 2006*, pp. 428–443, December 2006.
23. D. Chaum, "Blind Signatures for Untraceable Payments," in *Advances in Cryptology - CRYPTO '82*, pp. 199–203, 1982.
24. D. Chaum, "Blind Signature System," in *Advances in Cryptology - CRYPTO '83*, 1984.
25. D. Chaum, "Blinding for Unanticipated Signatures," in *Advances in Cryptology - EUROCRYPT '87*, pp. 227–233, 1988.

26. D. Chaum, “Security Without Identification: Transaction Systems to Make Big Brother Obsolete,” *Communications of the ACM*, vol. 28, pp. 1030–1044, October 1985.
27. D. Chaum, A. Fiat, and M. Naor, “Untraceable Electronic Cash,” in *Advances in Cryptology - CRYPTO ’88*, pp. 319–327, 1990.
28. A. Juels, M. Luby, and R. Ostrovsky, “Security of Blind Digital Signatures,” in *Advances in Cryptology - CRYPTO ’97*, pp. 150–164, August 1997.
29. M. Stadler, J. Piveteau, and J. Camenisch, “Fair Blind signatures,” in *Advances in Cryptology - EUROCRYPT ’95*, pp. 209–219, 1995.
30. B. Pfitzmann and M. Waidner, “Formal Aspects of Fail-Stop Signatures,” Tech. Rep. 22/90, Fakultät für Informatik, 1990.
31. B. Pfitzmann and M. Waidner, “Fail-Stop Signatures and Their Application,” in *Securicom’91*, pp. 145–160, March 1991.
32. E. van Heijst and T. Pedersen, “How to Make Efficient Fail-Stop Signatures,” in *Advances in Cryptology - Eurocrypt’92*, pp. 366–377, 1992.
33. W. Susilo, “Short Fail-Stop Signature Scheme Based on Factorization and Discrete Logarithm Assumptions,” vol. 410, pp. 736–744, March 2009.
34. M. O. Rabin, “Digitalized Signatures,” in *Foundations of Secure Computation, R. A. DeMillo, D. P. Dobkin, A. K. Jones, and R. J. Lipton, editors*, pp. 155–168, 1978.
35. L. Lamport, “Constructing Digital Signatures from One-Way Function,” Tech. Rep. SRI-CSL-98, SRI International, October 1979.
36. R. C. Merkle, “A Digital Signature based on a Conventional Encryption Function,” in *CRYPTO 1987, Lecture Notes in Computer Science 293, Springer*, 1988.
37. A. Perrig, “The BiBa One-Time Signature and Broadcast Authentication Protocol,” in *ACM Conference on Computer and Communications Security*, pp. 28–37, 2001.
38. L. Reyzin and N. Reyzin, “Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying,” in *7th Australian Conference In Information Security and Privacy (ACISP)*, pp. 144–153, 2002.
39. L. Lamport, “One-Time Signatures Revisited: Have They Become Practical?,” tech. rep., http://eprint.iacr.org/2005/442.pdf, December 2005.
40. M. Jakobsson, F. Leighton, S. Micali, and M. Szydlo, “Merkle Tree Representation and Traversal,” in *Topics in Cryptology - CT-RSA 2003, The Cryptographers’ Track at the RSA Conference*, pp. 314–326, 2003.

10.10 Αντιστοίχηση Ελληνικών - Αγγλικών Όρων

Ψηφιακή υπογραφή	Digital signature
Δημιουργία υπογραφής	Signature generation
Επιβεβαίωση υπογραφής	Signature verification
Επαληθευτής	Verifier
Γενική ικανότητα επιβεβαίωσης	Universal verifiability
Μη άρνηση αναγνώρισης	Non repudiation
Ακεραιότητα δεδομένων	Data integrity
Πιστοποιητικό	Certificate
Κρυπτογραφία με δημόσια κλειδιά	Public key cryptography
Αντίπαλος	Adversary
Παραχαράσσω	Forge
Υπογραφές με προσθήκη	Signatures with an appendix
Κοινό σημείο εμπιστοσύνης	Trusted third party
Υπογραφές με ανάκτηση μηνύματος	Signatures with message recovery
Μονόδρομη συνάρτηση σύνοψης	Hash function
Επαλήθευση (ή Αναγνώριση)	Authentication
Ακεραιότητα δεδομένων	Data integrity
Πιστοποίηση κλειδιού	Key certification
Έλεγχος επιδόσεων	Benchmark
Αναμφισβήτητη υπογραφή	Undeniable signature
Τυφλή υπογραφή (ή με απόκρυψη)	Blind signature
Μη επιλυσιμότητα	Intractability
Αναμφισβήτητη υπογραφή	Undeniable signature
Πρωτόκολλο διάψευσης	Disavowal protocol
Πρωτόκολλο επιβεβαίωσης	Confirmation protocol
Υπογραφές Μιας Χρήσης	One-time signatures