Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία

Ψηφιακές Υπογραφές
Υπογραφές Επιπρόσθετης Λειτουργικότητας

Άρης Παγουρτζής – Στάθης Ζάχος

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Ψηφιακές Υπογραφές

Απαιτήσεις

- Message authentication (γνησιότητα): το μήνυμα προέρχεται από το σωστό αποστολέα.

Ψηφιακές Υπογραφές

Απαιτήσεις

- Message authentication (γνησιότητα): το μήνυμα προέρχεται από το σωστό αποστολέα.
- Non-repudiation (μη αποκήρυξη): δεν μπορεί κάποιος να "αποκηρύξει" τη δική του υπογραφή.

Ψηφιακές Υπογραφές

Απαιτήσεις

- Message authentication (γνησιότητα): το μήνυμα προέρχεται από το σωστό αποστολέα.
- Non-repudiation (μη αποκήρυξη): δεν μπορεί κάποιος να “αποκηρύξει” τη δική του υπογραφή.
- Integrity (ακεραιότητα): συνήθως προκύπτει σαν παράπλευρο αποτέλεσμα.

Ψηφιακές Υπογραφές

Απαιτήσεις

- Message authentication (γνησιότητα): το μήνυμα προέρχεται από το σωστό αποστολέα.
- Non-repudiation (μη αποκήρυξη): δεν μπορεί κάποιος να "αποκηρύξει" τη δική του υπογραφή.
- Integrity (ακεραιότητα): συνήθως προκύπτει σαν παράπλευρο αποτέλεσμα.
- Υπολογιστική εφικτότητα: αποδοτικοί αλγόριθμοι δημιουργίας υπογραφής (για το νόμιμο αποστολέα μόνο) και επαλήθευσης (για όλους).

Απαιτήσεις

- Message authentication (γνησιότητα): το μήνυμα προέρχεται από το σωστό αποστολέα.
- Non-repudiation (μη αποκήρυξη): δεν μπορεί κάποιος να "αποκηρύξει" τη δική του υπογραφή.
- Integrity (ακεραιότητα): συνήθως προκύπτει σαν παράπλευρο αποτέλεσμα.
- Υπολογιστική εφικτότητα: αποδοτικοί αλγόριθμοι δημιουργίας υπογραφής (για το νόμιμο αποστολέα μόνο) και επαλήθευσης (για όλους).
- Existential unforgeability: δεν μπορεί να παραχθεί από ζεύγη κειμένου - υπογραφής πλαστή υπογραφή για οποιοδήποτε άλλο κείμενο.

Ψηφιακές Υπογραφές

Απαιτήσεις

- Message authentication (γνησιότητα): το μήνυμα προέρχεται από το σωστό αποστολέα.
- Non-repudiation (μη αποκήρυξη): δεν μπορεί κάποιος να “αποκηρύξει” τη δική του υπογραφή.
- Integrity (ακεραιότητα): συνήθως προκύπτει σαν παράπλευρο αποτέλεσμα.
- Υπολογιστική εφικτότητα: αποδοτικοί αλγόριθμοι δημιουργίας υπογραφής (για το νόμιμο αποστολέα μόνο) και επαλήθευσης (για όλους).
- Existential unforgeability: δεν μπορεί να παραχθεί από ζεύγη κειμένου - υπογραφής πλαστή υπογραφή για οποιοδήποτε άλλο κείμενο.
- Selective unforgeability: δεν μπορεί να παραχθεί από ζεύγη κειμένου - υπογραφής πλαστή υπογραφή για επιλεγμένο άλλο

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με συμμετρική κρυπτογραφία

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με συμμετρική κρυπτογραφία

- Η κρυπτογράφηση δίνει και εγγύηση γνησιότητας (αν το απλό κείμενο έχει γνωστή ή συμφωνημένη δομή).

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με συμμετρική κρυπτογραφία

- Η κρυπτογράφηση δίνει και εγγύηση γνησιότητας (αν το απλό κείμενο έχει γνωστή ή συμφωνημένη δομή).
- Σαν ξεχωριστή λειτουργία: χρήση ιδιωτικού κλειδιού για δημιουργία και επαλήθευση υπογραφής.

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με συμμετρική κρυπτογραφία

- Η κρυπτογράφηση δίνει και εγγύηση γνησιότητας (αν το απλό κείμενο έχει γνωστή ή συμφωνημένη δομή).
- Σαν ξεχωριστή λειτουργία: χρήση ιδιωτικού κλειδιού για δημιουργία και επαλήθευση υπογραφής.
- Συνήθως πάνω σε αποτύπωμα, δημιουργημένο με *συνάρτηση σύνοψης (hash function)*: message authentication code (MAC).

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με συμμετρική κρυπτογραφία

- Η κρυπτογράφηση δίνει και εγγύηση γνησιότητας (αν το απλό κείμενο έχει γνωστή ή συμφωνημένη δομή).
- Σαν ξεχωριστή λειτουργία: χρήση ιδιωτικού κλειδιού για δημιουργία και επαλήθευση υπογραφής.
- Συνήθως πάνω σε αποτύπωμα, δημιουργημένο με *συνάρτηση σύνοψης (hash function)*: message authentication code (MAC).
- Παρεμφερής τρόπος: αλυσιδωτή κρυπτογράφηση και λήψη τελευταίου κρυπτοκειμένου (CBC-MAC).

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με κρυπτογραφία δημοσίου κλειδιού

- *Η κρυπτογράφηση δεν εξασφαλίζει γνησιότητα.*

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με κρυπτογραφία δημοσίου κλειδιού

- *Η κρυπτογράφηση δεν εξασφαλίζει γνησιότητα.*
- Ιδιωτικό κλειδί: δημιουργία υπογραφής

Σχήματα ψηφιακών υπογραφών: συμμετρικά ή δημοσίου κλειδιού

Με κρυπτογραφία δημοσίου κλειδιού

- *Η κρυπτογράφηση δεν εξασφαλίζει γνησιότητα.*
- Ιδιωτικό κλειδί: δημιουργία υπογραφής
- Δημόσιο κλειδί: επαλήθευση υπογραφής
- Συνήθως πάνω σε αποτύπωμα, με χρήση hash function.

Γενικό σχήμα υπογραφών (δημοσίου κλειδιού)

- Αλγόριθμος παραγωγής κλειδιών (`KeyGen`): συνήθως όπως στο αντίστοιχο σχήμα κρυπτογράφησης / αποκρυπτογράφησης.

Γενικό σχήμα υπογραφών (δημοσίου κλειδιού)

- Αλγόριθμος παραγωγής κλειδιών (`KeyGen`): συνήθως όπως στο αντίστοιχο σχήμα κρυπτογράφησης / αποκρυπτογράφησης.
- Συνάρτηση (αλγόριθμος) υπογραφής $\texttt{sig} : \mathcal{M} \times \mathcal{SK} \to \mathcal{S}$, όπου $\mathcal{M}$ είναι τα μηνύματα, $\mathcal{SK}$ είναι τα ιδιωτικά κλειδιά και $\mathcal{S}$ είναι οι υπογραφές.

  Για συγκεκριμένο κλειδί $\texttt{sig}_{s_A} : M \to S$, όπου $s_A \in \mathcal{SK}$ είναι το ιδιωτικό κλειδί του χρήστη A.

Γενικό σχήμα υπογραφών (δημοσίου κλειδιού)

- Αλγόριθμος παραγωγής κλειδιών (`KeyGen`): συνήθως όπως στο αντίστοιχο σχήμα κρυπτογράφησης / αποκρυπτογράφησης.
- Συνάρτηση (αλγόριθμος) υπογραφής $\mathtt{sig} : \mathcal{M} \times \mathcal{SK} \to \mathcal{S}$, όπου $\mathcal{M}$ είναι τα μηνύματα, $\mathcal{SK}$ είναι τα ιδιωτικά κλειδιά και $\mathcal{S}$ είναι οι υπογραφές.

  Για συγκεκριμένο κλειδί $\mathtt{sig}_{s_A} : M \to S$, όπου $s_A \in \mathcal{SK}$ είναι το ιδιωτικό κλειδί του χρήστη A.
- Συνάρτηση (αλγόριθμος) επαλήθευσης $\mathtt{ver} : \mathcal{M} \times \mathcal{S} \times \mathcal{PK} \to \{\mathtt{true}, \mathtt{false}\}$, όπου $\mathcal{PK}$ τα δημόσια κλειδιά.

  Για συγκεκριμένο κλειδί $\mathtt{ver}_p : \mathcal{M} \times \mathcal{S} \to \{\mathtt{true}, \mathtt{false}\}$, όπου $p_A \in \mathcal{PK}$ είναι το δημόσιο κλειδί του χρήστη A.

Γενικό σχήμα υπογραφών (δημοσίου κλειδιού)

- Αλγόριθμος παραγωγής κλειδιών (`KeyGen`): συνήθως όπως στο αντίστοιχο σχήμα κρυπτογράφησης / αποκρυπτογράφησης.
- Συνάρτηση (αλγόριθμος) υπογραφής $\mathtt{sig} : \mathcal{M} \times \mathcal{SK} \rightarrow \mathcal{S}$, όπου $\mathcal{M}$ είναι τα μηνύματα, $\mathcal{SK}$ είναι τα ιδιωτικά κλειδιά και $\mathcal{S}$ είναι οι υπογραφές.

  Για συγκεκριμένο κλειδί $\mathtt{sig}_{s_A} : M \rightarrow S$, όπου $s_A \in \mathcal{SK}$ είναι το ιδιωτικό κλειδί του χρήστη A.
- Συνάρτηση (αλγόριθμος) επαλήθευσης $\mathtt{ver} : \mathcal{M} \times \mathcal{S} \times \mathcal{PK} \rightarrow \{\mathtt{true}, \mathtt{false}\}$, όπου $\mathcal{PK}$ τα δημόσια κλειδιά.

  Για συγκεκριμένο κλειδί $\mathtt{ver}_p : \mathcal{M} \times \mathcal{S} \rightarrow \{\mathtt{true}, \mathtt{false}\}$, όπου $p_A \in \mathcal{PK}$ είναι το δημόσιο κλειδί του χρήστη A.

$A : m, s_A$

Γενικό σχήμα υπογραφών (δημοσίου κλειδιού)

- Αλγόριθμος παραγωγής κλειδιών (`KeyGen`): συνήθως όπως στο αντίστοιχο σχήμα κρυπτογράφησης / αποκρυπτογράφησης.
- Συνάρτηση (αλγόριθμος) υπογραφής $\mathtt{sig} : \mathcal{M} \times \mathcal{SK} \to \mathcal{S}$, όπου $\mathcal{M}$ είναι τα μηνύματα, $\mathcal{SK}$ είναι τα ιδιωτικά κλειδιά και $\mathcal{S}$ είναι οι υπογραφές.

  Για συγκεκριμένο κλειδί $\mathtt{sig}_{s_A} : M \to S$, όπου $s_A \in \mathcal{SK}$ είναι το ιδιωτικό κλειδί του χρήστη A.
- Συνάρτηση (αλγόριθμος) επαλήθευσης $\mathtt{ver} : \mathcal{M} \times \mathcal{S} \times \mathcal{PK} \to \{\mathtt{true}, \mathtt{false}\}$, όπου $\mathcal{PK}$ τα δημόσια κλειδιά.

  Για συγκεκριμένο κλειδί $\mathtt{ver}_p : \mathcal{M} \times \mathcal{S} \to \{\mathtt{true}, \mathtt{false}\}$, όπου $p_A \in \mathcal{PK}$ είναι το δημόσιο κλειδί του χρήστη A.

$$A : m, s_A \xrightarrow{(m,s)=(m,sig_{s_A}(m))} B :$$

Γενικό σχήμα υπογραφών (δημοσίου κλειδιού)

- Αλγόριθμος παραγωγής κλειδιών (`KeyGen`): συνήθως όπως στο αντίστοιχο σχήμα κρυπτογράφησης / αποκρυπτογράφησης.
- Συνάρτηση (αλγόριθμος) υπογραφής $\mathtt{sig} : \mathcal{M} \times \mathcal{SK} \to \mathcal{S}$, όπου $\mathcal{M}$ είναι τα μηνύματα, $\mathcal{SK}$ είναι τα ιδιωτικά κλειδιά και $\mathcal{S}$ είναι οι υπογραφές.

  Για συγκεκριμένο κλειδί $\mathtt{sig}_{s_A} : M \to S$, όπου $s_A \in \mathcal{SK}$ είναι το ιδιωτικό κλειδί του χρήστη A.
- Συνάρτηση (αλγόριθμος) επαλήθευσης $\mathtt{ver} : \mathcal{M} \times \mathcal{S} \times \mathcal{PK} \to \{\mathtt{true}, \mathtt{false}\}$, όπου $\mathcal{PK}$ τα δημόσια κλειδιά.

  Για συγκεκριμένο κλειδί $\mathtt{ver}_p : \mathcal{M} \times \mathcal{S} \to \{\mathtt{true}, \mathtt{false}\}$, όπου $p_A \in \mathcal{PK}$ είναι το δημόσιο κλειδί του χρήστη A.

$$A : m, s_A \xrightarrow{(m,s)=(m,sig_{s_A}(m))} B : ver_{p_A}(m,s) \stackrel{?}{=} \mathtt{true}$$

Κατηγοριοποίηση υπογραφών

1. Σχήματα Ψηφιακής Υπογραφής με παράρτημα (with appendix). Εδώ ανήκουν τα σχήματα στα οποία το αρχικό μήνυμα είναι απαραίτητο για την πιστοποίηση γνησιότητας της αντίστοιχης υπογραφής (όπως είναι το ElGamal και το DSS).
   Επίσης όλα τα σχήματα που χρησιμοποιούν hash function.

Κατηγοριοποίηση υπογραφών

1. Σχήματα Ψηφιακής Υπογραφής με παράρτημα (with appendix). Εδώ ανήκουν τα σχήματα στα οποία το αρχικό μήνυμα είναι απαραίτητο για την πιστοποίηση γνησιότητας της αντίστοιχης υπογραφής (όπως είναι το ElGamal και το DSS).
   Επίσης όλα τα σχήματα που χρησιμοποιούν hash function.

2. Σχήματα Ψηφιακής Υπογραφής με ικανότητα ανάκτησης του μηνύματος (message recovery), στα οποία το αρχικό μήνυμα μπορεί να παραχθεί από την ίδια την υπογραφή. (π.χ. το RSA).
   Σε ένα τέτοιο σχήμα μπορεί να σταλεί μόνο η υπογραφή s (υποθέτοντας κάποιες συμβάσεις στη μορφή του αρχικού μηνύματος), μειώνοντας έτσι το μέγεθος. Η χρήση τέτοιων σχημάτων έχει πάντως ατονήσει.

Το σχήμα υπογραφής RSA

Όπως το σχήμα κρυπτογράφησης, με αντιστροφή των κλειδιών.

Το σχήμα υπογραφής RSA

Όπως το σχήμα κρυπτογράφησης, με αντιστροφή των κλειδιών.

Κλειδιά: $s_A = (d, p, q), p_A = (e, n)$ όπου $(e, d) \in \mathbb{Z}_n$ και $ed \equiv 1 \bmod \phi(n)$

$\texttt{sig} : \forall m \in M : s = \texttt{sig}_{s_A}(m) = m^d \bmod n$

$\texttt{ver} : \texttt{ver}_{p_A}(m, s) = \text{true} \Leftrightarrow m = s^e \bmod n$

Το σχήμα υπογραφής RSA

Όπως το σχήμα κρυπτογράφησης, με αντιστροφή των κλειδιών.

Κλειδιά: $s_A = (d, p, q), p_A = (e, n)$ όπου $(e, d) \in \mathbb{Z}_n$ και $ed \equiv 1 \bmod \phi(n)$

$\mathtt{sig} : \forall m \in M : s = \mathtt{sig}_{s_A}(m) = m^d \mathrm{mod} n$

$\mathtt{ver} : \mathtt{ver}_{p_A}(m, s) = \text{true} \Leftrightarrow m = s^e \mathrm{mod} n$

Σημαντικό πρόβλημα ασφάλειας: existential forgery: καθένας μπορεί να κατασκευάσει πολλά έγκυρα ζεύγη (m', s') (πώς;).

Το σχήμα υπογραφής RSA

Όπως το σχήμα κρυπτογράφησης, με αντιστροφή των κλειδιών.

Κλειδιά: $s_A = (d, p, q), p_A = (e, n)$ όπου $(e, d) \in \mathbb{Z}_n$ και $ed \equiv 1 \bmod \phi(n)$

$\mathtt{sig} : \forall m \in M : s = \mathtt{sig}_{s_A}(m) = m^d \mathrm{mod} n$

$\mathtt{ver} : \mathtt{ver}_{p_A}(m, s) = \mathrm{true} \Leftrightarrow m = s^e \mathrm{mod} n$

Σημαντικό πρόβλημα ασφάλειας: existential forgery: καθένας μπορεί να κατασκευάσει πολλά έγκυρα ζεύγη (m', s') (πώς;).

Λύσεις: χρήση hash function, χρήση redundancy.

Συνάρτηση πλεονάζουσας πληροφορίας (redundancy function)

Απαιτούμε συγκεκριμένη μορφή του αρχικού μηνύματος, εισάγοντας πλεονάζουσα πληροφορία. Π.χ.:

$$f(m) = m||01101$$

Συνάρτηση πλεονάζουσας πληροφορίας (redundancy function)

Απαιτούμε συγκεκριμένη μορφή του αρχικού μηνύματος, εισάγοντας πλεονάζουσα πληροφορία. Π.χ.:

$$f(m) = m||01101$$

Προσοχή: χρήση συνάρτησης f που *να μην έχει πολλαπλασιαστική ιδιότητα* (αν η συνάρτηση υπογραφής την έχει):

Για το σχήμα RSA: $f(m_1 m_2) \neq f(m_1) f(m_2)$

Συνάρτηση πλεονάζουσας πληροφορίας (redundancy function)

Απαιτούμε συγκεκριμένη μορφή του αρχικού μηνύματος, εισάγοντας πλεονάζουσα πληροφορία. Π.χ.:

$$f(m) = m||01101$$

Προσοχή: χρήση συνάρτησης f που *να μην έχει πολλαπλασιαστική ιδιότητα* (αν η συνάρτηση υπογραφής την έχει):

Για το σχήμα RSA: $f(m_1 m_2) \neq f(m_1) f(m_2)$

Αλλιώς το γινόμενο των υπογραφών είναι η υπογραφή του γινομένου!

Κρυπτογράφηση και Υπογραφή: Sign-then-Encrypt or Encrypt-then-Sign?

Encrypt-then-Sign

- Ο B λαμβάνει: $(enc_{p_B}(m), sig_{s_A}(enc_{p_B}(m)))$, επαληθεύει και αποκρυπτογραφεί.
- Πρόβλημα: MitM attack - αλλαγή αποστολέα.
  Έστω ότι ο O βρίσκεται ανάμεσα στους A, B.
  Ο O παίρνει το παραπάνω ζευγάρι, βάζει τη δική του υπογραφή και στέλνει, σαν δικό του, αυτό που θα έστελνε η A, π.χ.

  "Στείλε μου ηλεκτρονική επιταγή 100K ευρώ. Κωδικός επαλήθευσης: JVxu153wb%".

  Στέλνει, δηλαδή, $(enc_{p_B}(m), sig_{s_O}(enc_{p_B}(m)))$.

Καλή πρακτική: προσθέτουμε αποστολέα, παραλήπτη και χρόνο αποστολής στα μηνύματα.

Κρυπτογράφηση και Υπογραφή: Sign-then-Encrypt or Encrypt-then-Sign?

Sign-then-Encrypt

- Ο B λαμβάνει: $enc_{p_B}(m, sig_{s_A}(m))$, αποκρυπτογραφεί και έχει: $(m, sig_{s_A}(m))$.
- Πρόβλημα (μικρότερο): αλλαγή παραλήπτη
  Ο B έχει την υπογραφή της A στο m και μπορεί να κρυπτογραφήσει το ζεύγος $(m, sig_{s_A}(m))$ με p_C και να το στείλει στον C (σα να το στέλνει η), π.χ.

  "Συνόδεψε αύριο στο αεροδρόμιο τον Διευθυντή".

Καλή πρακτική: προσθέτουμε αποστολέα, παραλήπτη και χρόνο αποστολής στα μηνύματα.

Σχήμα υπογραφής ElGamal

- Κλειδιά:
  Δημόσιο: πρώτος p, γεννήτορας g της $\mathbb{Z}_p^*$, g^a, $a \stackrel{R}{\leftarrow} [2, ..., p-2]$
  Ιδιωτικό: a.
- Υπογραφή: επιλογή τυχαίου $k \in U(\mathbb{Z}_{p-1})$.
  $\gamma = g^k \bmod p$
  $\delta = (m - a\gamma)k^{-1} \bmod (p-1)$
  $sig(m) = (\gamma, \delta)$
- Επαλήθευση:
  $ver(m, \gamma, \delta) = \texttt{true} \Leftrightarrow (g^a)^\gamma \cdot \gamma^\delta \equiv g^m \pmod p$

Σημείωση: Μη ντετερμινιστικό σχήμα, υπάρχουν πολλές έγκυρες υπογραφές για το m.

Σενάρια πλαστογράφησης υπογραφής ElGamal

Στόχος: $g^{a\gamma} \cdot \gamma^{\delta} \equiv g^{m} \pmod{p}$ (*)

1. Επιλέγω *m* και προσπαθώ να βρώ γ, δ ώστε να ισχύει (*).
   - Επιλέγω γ, ψάχνω δ τέτοιο ώστε να ισχύει (*): θα πρέπει $\gamma^{\delta} \equiv g^{m} \cdot g^{-a\gamma} \pmod{p}$ (επίλυση DLP).
   - Επιλέγω δ, ψάχνω γ τέτοιο ώστε να ισχύει $(*)$. Το πρόβλημα επίλυσης της $(*)$ ως προς γ είναι ανοιχτό (ούτε γνωρίζουμε κάποια σχέση του με τα άλλα προβλήματα διακριτού λογαρίθμου).

Σενάρια πλαστογράφησης υπογραφής ElGamal

Στόχος: $g^{a\gamma} \cdot \gamma^{\delta} \equiv g^{m} \pmod p$ (*)

1. Επιλέγω m και προσπαθώ να βρώ γ, δ ώστε να ισχύει (*).
   - Επιλέγω γ, ψάχνω δ τέτοιο ώστε να ισχύει (*): θα πρέπει $\gamma^{\delta} \equiv g^{m} \cdot g^{-a\gamma} \pmod p$ (επίλυση DLP).
   - Επιλέγω δ, ψάχνω γ τέτοιο ώστε να ισχύει $(*)$. Το πρόβλημα επίλυσης της $(*)$ ως προς γ είναι ανοιχτό (ούτε γνωρίζουμε κάποια σχέση του με τα άλλα προβλήματα διακριτού λογαρίθμου).
2. Επιλέγω γ και δ, ψάχνω m: DLP ξανά.

Σενάρια πλαστογράφησης υπογραφής ElGamal

Στόχος: $g^{a\gamma} \cdot \gamma^{\delta} \equiv g^m \pmod{p}$ (*)

1. Επιλέγω m και προσπαθώ να βρώ γ, δ ώστε να ισχύει (*).
   - Επιλέγω γ, ψάχνω δ τέτοιο ώστε να ισχύει (*): θα πρέπει $\gamma^{\delta} \equiv g^m \cdot g^{-a\gamma} \pmod{p}$ (επίλυση DLP).
   - Επιλέγω δ, ψάχνω γ τέτοιο ώστε να ισχύει $(*)$. Το πρόβλημα επίλυσης της $(*)$ ως προς γ είναι ανοιχτό (ούτε γνωρίζουμε κάποια σχέση του με τα άλλα προβλήματα διακριτού λογαρίθμου).
2. Επιλέγω γ και δ, ψάχνω m: DLP ξανά.
3. Κατασκευή γ, δ, m ταυτόχρονα.

   Επιλέγω $i, j, 0 \leq i, j \leq p-2,\ \gcd(j, p-1) = 1$ και θέτω:

   $\gamma = g^i \cdot (g^a)^j \bmod p$

   $\delta = -\gamma \cdot j^{-1} \bmod p-1$

   $m = -\gamma \cdot i \cdot j^{-1} \bmod p-1$

   Εφικτό σενάριο, δίνει υπογραφή για τυχαίο m:

Σενάρια πλαστογράφησης υπογραφής ElGamal

Στόχος: $g^{a\gamma} \cdot \gamma^{\delta} \equiv g^{m} \pmod{p}$ (*)

1. Επιλέγω m και προσπαθώ να βρώ γ, δ ώστε να ισχύει (*).
   - Επιλέγω γ, ψάχνω δ τέτοιο ώστε να ισχύει (*): θα πρέπει $\gamma^{\delta} \equiv g^{m} \cdot g^{-a\gamma} \pmod{p}$ (επίλυση DLP).
   - Επιλέγω δ, ψάχνω γ τέτοιο ώστε να ισχύει $(*)$. Το πρόβλημα επίλυσης της $(*)$ ως προς γ είναι ανοιχτό (ούτε γνωρίζουμε κάποια σχέση του με τα άλλα προβλήματα διακριτού λογαρίθμου).
2. Επιλέγω γ και δ, ψάχνω m: DLP ξανά.
3. Κατασκευή γ, δ, m ταυτόχρονα.

   Επιλέγω $i, j, 0 \leq i, j \leq p-2, \ \gcd(j, p-1) = 1$ και θέτω:

   $\gamma = g^{i} \cdot (g^{a})^{j} \bmod p$

   $\delta = -\gamma \cdot j^{-1} \bmod p-1$

   $m = -\gamma \cdot i \cdot j^{-1} \bmod p-1$

   Εφικτό σενάριο, δίνει υπογραφή για τυχαίο m: αντιμετώπιση με redundancy function ή και με hash function.

Δύο απλές επιθέσεις στις υπογραφές ElGamal

Προφυλάξεις για το τυχαίο k: όχι γνωστοποίηση, όχι επανάληψη

- Το τυχαία επιλεγμένο k πρέπει να μένει κρυφό – η γνώση του δίνει στον “ωτακουστή” τη δυνατότητα να υπολογίσει το ιδιωτικό κλειδί a.

Δύο απλές επιθέσεις στις υπογραφές ElGamal

Προφυλάξεις για το τυχαίο k: όχι γνωστοποίηση, όχι επανάληψη

- Το τυχαία επιλεγμένο k πρέπει να μένει κρυφό – η γνώση του δίνει στον "ωτακουστή" τη δυνατότητα να υπολογίσει το ιδιωτικό κλειδί a.

- Η επανάληψη της χρήσης του ίδιου k επιτρέπει στον ωτακουστή να το ανακτήσει και επομένως να υπολογίσει και το a.

Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard – DSS)

- NIST, 1991.

Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard – DSS)

- NIST, 1991.
- Παραλλαγή του ElGamal, μικρότερο μέγεθος υπογραφής.

Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard – DSS)

- NIST, 1991.
- Παραλλαγή του ElGamal, μικρότερο μέγεθος υπογραφής.
- Ιδέα: λειτουργία σε μια υποομάδα της $\mathbb{Z}_p^*$, τάξης 2^{160}.

Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard – DSS)

- NIST, 1991.
- Παραλλαγή του ElGamal, μικρότερο μέγεθος υπογραφής.
- Ιδέα: λειτουργία σε μια υποομάδα της $\mathbb{Z}_p^*$, τάξης 2^{160}.
- Τα γ, δ είναι εκθέτες δυνάμεων του γεννήτορα της υποομάδας.

Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard – DSS)

- NIST, 1991.
- Παραλλαγή του ElGamal, μικρότερο μέγεθος υπογραφής.
- Ιδέα: λειτουργία σε μια υποομάδα της $\mathbb{Z}_p^*$, τάξης 2^{160}.
- Τα γ, δ είναι εκθέτες δυνάμεων του γεννήτορα της υποομάδας.
- Προσοχή: το γ χρησιμοποιείται και σαν βάση και σαν εκθέτης στην επαλήθευση!

Παραγωγή κλειδιών DSS

1. Επιλογή πρώτων q μεγέθους 160-bit και p μεγέθους n-bit, $n = 64r, r = 8, 9, 10, \ldots, 16$, με $q \mid (p-1)$.
2. Εύρεση g τάξης q: $g = g_0^{\frac{p-1}{q}}$, g_0 γεννήτορας της $\mathbb{Z}_p^*$.
3. Επιλογή ιδιωτικού κλειδιού $a \in \mathbb{Z}_q$.
4. Υπολογισμός $g^a \bmod p$.

Παραγωγή κλειδιών DSS

1. Επιλογή πρώτων q μεγέθους 160-bit και p μεγέθους n-bit, $n = 64r, r = 8, 9, 10, \ldots, 16$, με $q \mid (p-1)$.
2. Εύρεση g τάξης q: $g = g_0^{\frac{p-1}{q}}$, g_0 γεννήτορας της $\mathbb{Z}_p^*$.
3. Επιλογή ιδιωτικού κλειδιού $a \in \mathbb{Z}_q$.
4. Υπολογισμός $g^a \bmod p$.

Δημόσιο κλειδί: $(p, q, g, \beta), \beta = g^a \bmod p$.
Ιδιωτικό κλειδί: a.

Δημιουργία υπογραφής DSS

1. H επιλέγει έναν τυχαίο ακέραιο k, $1 \leq k \leq (q-1)$.
2. H υπολογίζει τα

$$
\begin{aligned}
\gamma &= (g^k \mod p) \mod q \\
\delta &= (m + a\gamma)k^{-1} \mod q.
\end{aligned}
$$

3. Υπογραφή: $sig(m,k) = (\gamma, \delta)$.

Επαλήθευση υπογραφής DSS

1. Ο B υπολογίζει:

$$\begin{aligned} e_1 &= m\delta^{-1} \mod q \\ e_2 &= \gamma\delta^{-1} \mod q\,. \end{aligned}$$

2. $ver(m, \gamma, \delta) = \text{true} \Leftrightarrow (g^{e_1}\beta^{e_2} \bmod p) \bmod q = \gamma$

Παρατηρήσεις στο DSS

1. Αν ορίζαμε:

$$\gamma = g^k \bmod q \quad \text{και}$$
$$\delta = (m + \alpha\gamma)k^{-1} \bmod q$$

δεν θα είχαμε ορθότητα (*γιατί;*).

Παρατηρήσεις στο DSS

1. Αν ορίζαμε:

$$\gamma = g^k \bmod q \quad \text{και}$$
$$\delta = (m + \alpha\gamma)k^{-1} \bmod q$$

   δεν θα είχαμε ορθότητα (*γιατί;*).
2. Αν συμβεί $\delta \equiv 0 \pmod{q}$ η διαδικασία επαναλαμβάνεται.
3. Η ασφάλεια του DSS στηρίζεται στην εικασία ότι η επίλυση του DLP είναι υπολογιστικά δύσκολη σε ομάδα τάξης 2^{160}. Αυτό πλέον αμφισβητείται.
4. Υπογραφή γρηγορότερη από επαλήθευση.

Υπογραφές μιας χρήσης

Lamport Signature Scheme

- Χρήση *one-way* συνάρτησης $f : Y \to Z$.
- Απλό μήνυμα: $m = (x_1, x_2, ..., x_k)$, με $x_i \in \{0, 1\}$.

Υπογραφές μιας χρήσης

Lamport Signature Scheme

- Χρήση *one-way* συνάρτησης $f : Y \to Z$.
- Απλό μήνυμα: $m = (x_1, x_2, ..., x_k)$, με $x_i \in \{0, 1\}$.
- Ιδιωτικό κλειδί: επιλογή $y_{i,j} \xleftarrow{R} Y, 1 \leq i \leq k, j \in \{0, 1\}$:

$$(y_{1,0}, y_{2,0}, ..., y_{k,0})$$
$$(y_{1,1}, y_{2,1}, ..., y_{k,1})$$

Υπογραφές μιας χρήσης

Lamport Signature Scheme

- Χρήση *one-way* συνάρτησης $f : Y \to Z$.
- Απλό μήνυμα: $m = (x_1, x_2, ..., x_k)$, με $x_i \in \{0, 1\}$.
- Ιδιωτικό κλειδί: επιλογή $y_{i,j} \xleftarrow{R} Y, 1 \leq i \leq k, j \in \{0, 1\}$:

$$(y_{1,0}, y_{2,0}, \ldots, y_{k,0})$$
$$(y_{1,1}, y_{2,1}, \ldots, y_{k,1})$$

- Δημόσιο κλειδί: υπολογισμός $z_{i,j} = f(y_{i,j})$:

$$(z_{1,0}, z_{2,0}, \ldots, z_{k,0})$$
$$(z_{1,1}, z_{2,1}, \ldots, z_{k,1})$$

Υπογραφές μιας χρήσης

Lamport Signature Scheme

- Χρήση *one-way* συνάρτησης $f : Y \to Z$.
- Απλό μήνυμα: $m = (x_1, x_2, \ldots, x_k)$, με $x_i \in \{0, 1\}$.
- Ιδιωτικό κλειδί: επιλογή $y_{i,j} \xleftarrow{R} Y, 1 \leq i \leq k, j \in \{0, 1\}$:

$$(y_{1,0}, y_{2,0}, \ldots, y_{k,0})$$
$$(y_{1,1}, y_{2,1}, \ldots, y_{k,1})$$

- Δημόσιο κλειδί: υπολογισμός $z_{i,j} = f(y_{i,j})$:

$$(z_{1,0}, z_{2,0}, \ldots, z_{k,0})$$
$$(z_{1,1}, z_{2,1}, \ldots, z_{k,1})$$

- Υπογραφή: $s = sig(m) = (y_{1,x_1}, y_{2,x_2}, \ldots, y_{k,x_k})$

Υπογραφές μιας χρήσης

Lamport Signature Scheme

- Χρήση *one-way* συνάρτησης $f : Y \to Z$.
- Απλό μήνυμα: $m = (x_1, x_2, ..., x_k)$, με $x_i \in \{0, 1\}$.
- Ιδιωτικό κλειδί: επιλογή $y_{i,j} \overset{R}{\leftarrow} Y, 1 \leq i \leq k, j \in \{0, 1\}$:

$$(y_{1,0}, y_{2,0}, ..., y_{k,0})$$
$$(y_{1,1}, y_{2,1}, ..., y_{k,1})$$

- Δημόσιο κλειδί: υπολογισμός $z_{i,j} = f(y_{i,j})$:

$$(z_{1,0}, z_{2,0}, ..., z_{k,0})$$
$$(z_{1,1}, z_{2,1}, ..., z_{k,1})$$

- Υπογραφή: $s = sig(m) = (y_{1,x_1}, y_{2,x_2}, ..., y_{k,x_k})$
- Επαλήθευση: $ver(m, s) = True \Leftrightarrow \forall i, 1 \leq i \leq k : f(s_i) = z_{i,x_i}$

Υπογραφές μιας χρήσης: σχήματα Lamport και Bos-Chaum

Παρατηρήσεις:

- Κλειδιά μιας χρήσης. Επαναχρησιμοποίηση κλειδιού επιτρέπει υπογραφή νέων μηνυμάτων.

- Αυξημένη ασφάλεια: το σύστημα μπορεί να 'επιζήσει' και στην εποχή των κβαντικών υπολογιστών (με κατάλληλη επιλογή της μονόδρομης συνάρτησης).

- Το σχήμα Lamport είναι "σπάταλο": $\binom{2k}{k} \approx \frac{(2^k)^2}{\sqrt{\pi k}} \Rightarrow \binom{2k}{k} \gg 2^k$.

- Βελτίωση Bos-Chaum: αρκούν περίπου τα μισά κλειδιά.

Τυφλές υπογραφές (blind signatures)

- Σενάριο ανώνυμης ψηφοφορίας: η Alice στέλνει στην Έμπιστη Αρχή μια ψήφο κατάλληλα "μασκαρεμένη". Η αρχή την υπογράφει και την στέλνει στην Alice. Η Alice την μετατρέπει σε κανονική ψήφο, υπογεγραμμένη από την Έμπιστη Αρχή.
- Συναρτήσεις τύφλωσης και αποτύφλωσης:
  $f : M \to M \quad g : S \to S$

Τυφλές υπογραφές (blind signatures)

- Σενάριο ανώνυμης ψηφοφορίας: η Alice στέλνει στην Έμπιστη Αρχή μια ψήφο κατάλληλα "μασκαρεμένη". Η αρχή την υπογράφει και την στέλνει στην Alice. Η Alice την μετατρέπει σε κανονική ψήφο, υπογεγραμμένη από την Έμπιστη Αρχή.
- Συναρτήσεις τύφλωσης και αποτύφλωσης:
  $f : M \to M \quad g : S \to S$
- $A \xrightarrow{m^* = f(m)} TTP$

Τυφλές υπογραφές (blind signatures)

- Σενάριο ανώνυμης ψηφοφορίας: η Alice στέλνει στην Έμπιστη Αρχή μια ψήφο κατάλληλα "μασκαρεμένη". Η αρχή την υπογράφει και την στέλνει στην Alice. Η Alice την μετατρέπει σε κανονική ψήφο, υπογεγραμμένη από την Έμπιστη Αρχή.
- Συναρτήσεις τύφλωσης και αποτύφλωσης:
  $f : M \to M \quad g : S \to S$
- $A \xrightarrow{m^*=f(m)} TTP$
- $A \xleftarrow{sig(m^*)} TTP$

Τυφλές υπογραφές (blind signatures)

- Σενάριο ανώνυμης ψηφοφορίας: η Alice στέλνει στην Έμπιστη Αρχή μια ψήφο κατάλληλα "μασκαρεμένη". Η αρχή την υπογράφει και την στέλνει στην Alice. Η Alice την μετατρέπει σε κανονική ψήφο, υπογεγραμμένη από την Έμπιστη Αρχή.
- Συναρτήσεις τύφλωσης και αποτύφλωσης:
  $f : M \to M \quad g : S \to S$
- $A \xrightarrow{m^*=f(m)} TTP$
- $A \xleftarrow{sig(m^*)} TTP$
- $A : \; g(sig(m^*)) = sig(m)$.

Έστω ότι ο Bob έχει τα ζεύγη (p_B, n) *(δημόσιο κλειδί)* και (s_B, p, q) *(ιδιωτικό κλειδί)*. Η Alice ζητά την υπογραφή του Bob.

(i) Η Alice επιλέγει τυχαίο $k \leftarrow \mathbb{Z}_n^*$, και υπολογίζει το $m^* = m \cdot k^{p_B}$,

και το στέλνει στον Bob (blinding).

Τυφλές υπογραφές: Σχήμα Chaum

Έστω ότι ο Bob έχει τα ζεύγη (p_B, n) *(δημόσιο κλειδί)* και (s_B, p, q) *(ιδιωτικό κλειδί)*. Η Alice ζητά την υπογραφή του Bob.

(i) Η Alice επιλέγει τυχαίο $k \leftarrow \mathbb{Z}_n^*$, και υπολογίζει το
$m^* = m \cdot k^{p_B}$,

και το στέλνει στον Bob (blinding).

(ii) Ο Bob υπογράφει το m^* ως εξής:
$s^* = sig(m^*) = (m^*)^{s_B} \bmod n \equiv (m \cdot k^{p_B})^{s_B} \equiv (m^{s_B} \cdot k) \equiv sig_{s_B}(m) \cdot k \pmod{n}$

και στέλνει το s^* στην Alice.

Τυφλές υπογραφές: Σχήμα Chaum

Έστω ότι ο Bob έχει τα ζεύγη (p_B, n) *(δημόσιο κλειδί)* και (s_B, p, q) *(ιδιωτικό κλειδί)*. Η Alice ζητά την υπογραφή του Bob.

(i) Η Alice επιλέγει τυχαίο $k \leftarrow \mathbb{Z}_n^*$, και υπολογίζει το

$m^* = m \cdot k^{p_B}$,

και το στέλνει στον Bob (blinding).

(ii) Ο Bob υπογράφει το m^* ως εξής:

$s^* = sig(m^*) = (m^*)^{s_B} \bmod n \equiv (m \cdot k^{p_B})^{s_B} \equiv (m^{s_B} \cdot k) \equiv sig_{s_B}(m) \cdot k \pmod n$

και στέλνει το s^* στην Alice.

(iii) Η Alice δέχεται το s^* από τον Bob και υπολογίζει:

$s = s^* \cdot k^{-1} \bmod n \equiv sig(m) \cdot k \cdot k^{-1} \equiv sig_{s_B}(m) \pmod n = sig_{s_B}(m)$.

Η Alice αποκτά το s, δηλαδή έγκυρη υπογραφή του Bob πάνω στο m (unblinding), χωρίς ο Bob να μάθει το m.

Άλλα είδη υπογραφών

- Αδιαμφισβήτητες υπογραφές (undeniable signatures)

  - Απαιτούν την συνεργασία του υπογράφοντα.

  - Δεν μπορεί όμως να τις αποποιηθεί.

  - Εκτός αν είναι πλαστές, οπότε το αποδεικνύει!

Άλλα είδη υπογραφών

- Αδιαμφισβήτητες υπογραφές (undeniable signatures)

  - Απαιτούν την συνεργασία του υπογράφοντα.

  - Δεν μπορεί όμως να τις αποποιηθεί.

  - Εκτός αν είναι πλαστές, οπότε το αποδεικνύει!

- Fail-stop signatures

  - Αν πλαστογραφηθούν, ο υπογράφων μπορεί να αποδείξει την πλαστογράφηση (μέσω Έμπιστης Αρχής) και να διακόψει τη χρήση τους.

Αδιαμφισβήτητες υπογραφές

Σχήμα Chaum - van Antwerpen

- KeyGen: πρώτοι $p, q, p = 2q + 1$, γεννήτορας g της υποομάδας $QR(p)$ (τάξης q), $a \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$, $\beta = g^a \bmod p$.
  Public key: p, g, β. Secret key: a.
- Signing:
  $$A \xrightarrow{\langle m,s \rangle, \quad s=sig(m)=m^a \bmod p} B$$

Σχήμα Chaum - van Antwerpen

- KeyGen: πρώτοι $p, q, p = 2q + 1$, γεννήτορας g της υποομάδας $QR(p)$ (τάξης q), $a \xleftarrow{R} \mathbb{Z}_q^*$, $\beta = g^a \bmod p$.
  Public key: p, g, β. Secret key: a.
- Signing:
  $$A \xrightarrow{\langle m,s\rangle,\quad s=sig(m)=m^a \bmod p} B$$
- Verification:
  $$A \xleftarrow{c=s^{e_1}\beta^{e_2} \bmod p,\quad e_1,e_2 \xleftarrow{R} \mathbb{Z}_q^*} B \quad \text{(challenge)}$$

Αδιαμφισβήτητες υπογραφές

Σχήμα Chaum - van Antwerpen

- KeyGen: πρώτοι $p, q, p = 2q + 1$, γεννήτορας g της υποομάδας $QR(p)$ (τάξης q), $a \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$, $\beta = g^a \bmod p$.
  Public key: p, g, β. Secret key: a.
- Signing:
  $$A \xrightarrow{\langle m,s \rangle, \quad s=sig(m)=m^a \bmod p} B$$
- Verification:
  $$A \xleftarrow{c=s^{e_1}\beta^{e_2} \bmod p, \quad e_1,e_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q^*} B \quad \text{(challenge)}$$
  $$A \xrightarrow{d=c^{a^{-1} \pmod q} \bmod p} B \quad \text{(response)}$$

Σχήμα Chaum - van Antwerpen

- KeyGen: πρώτοι $p, q, p = 2q + 1$, γεννήτορας g της υποομάδας $QR(p)$ (τάξης q), $a \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$, $\beta = g^a \bmod p$.
  Public key: p, g, β. Secret key: a.
- Signing:
  $$A \xrightarrow{\langle m,s \rangle, \quad s=sig(m)=m^a \bmod p} B$$
- Verification:
  $$A \xleftarrow{c=s^{e_1}\beta^{e_2} \bmod p, \quad e_1,e_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q^*} B \quad \text{(challenge)}$$
  $$A \xrightarrow{d=c^{a^{-1} \pmod q} \bmod p} B \quad \text{(response)}$$
  $B : ver(m, s, d) = \texttt{true} \Leftrightarrow d \equiv m^{e_1} g^{e_2} \pmod p$

Ασφάλεια σχήματος Chaum - van Antwerpen (i)

Ας υποθέσουμε ότι ένας αντίπαλος που παρεμβάλλεται στο κανάλι προσπαθεί να κάνει τον B να δεχθεί μια πλαστή υπογραφή ως γνήσια υπογραφή της A. Για παράδειγμα, στέλνει $\langle m, s \rangle$ τ.ώ. $s \not\equiv m^a \pmod{p}$ και προσπαθεί να βρει κατάλληλο d ώστε να γίνει σωστή επαλήθευση από τον B, δηλαδή να ισχύει $d \equiv m^{e_1} g^{e_2} \pmod{p}$, για τα e_1, e_2 που επιλέγει ο B.

Ασφάλεια σχήματος Chaum - van Antwerpen (i)

Ας υποθέσουμε ότι ένας αντίπαλος που παρεμβάλλεται στο κανάλι προσπαθεί να κάνει τον B να δεχθεί μια πλαστή υπογραφή ως γνήσια υπογραφή της A. Για παράδειγμα, στέλνει $\langle m, s \rangle$ τ.ώ. $s \not\equiv m^a \pmod p$ και προσπαθεί να βρει κατάλληλο d ώστε να γίνει σωστή επαλήθευση από τον B, δηλαδή να ισχύει $d \equiv m^{e_1} g^{e_2} \pmod p$, για τα e_1, e_2 που επιλέγει ο B.

Παρατήρηση: ο επιτιθέμενος μπορεί να είναι και η ίδια η Alice, που προσπαθεί να επαληθεύσει μια πλαστή της υπογραφή, την οποία στη συνέχεια να αποποιηθεί.

Ασφάλεια σχήματος Chaum - van Antwerpen (i)

Ας υποθέσουμε ότι ένας αντίπαλος που παρεμβάλλεται στο κανάλι προσπαθεί να κάνει τον B να δεχθεί μια πλαστή υπογραφή ως γνήσια υπογραφή της A. Για παράδειγμα, στέλνει $\langle m, s\rangle$ τ.ώ. $s \not\equiv m^a \pmod p$ και προσπαθεί να βρει κατάλληλο d ώστε να γίνει σωστή επαλήθευση από τον B, δηλαδή να ισχύει $d \equiv m^{e_1} g^{e_2} \pmod p$, για τα e_1, e_2 που επιλέγει ο B.

Παρατήρηση: ο επιτιθέμενος μπορεί να είναι και η ίδια η Alice, που προσπαθεί να επαληθεύσει μια πλαστή της υπογραφή, την οποία στη συνέχεια να αποποιηθεί.

Θεώρημα

Στο σχήμα Chaum - van Antwerpen, μία πλαστή υπογραφή $s \not\equiv m^a \pmod p$ απορρίπτεται με πιθανότητα $1 - \frac{1}{q}$, ανεξαρτήτως της υπολογιστικής ισχύος του αντιπάλου.

Ασφάλεια σχήματος Chaum - van Antwerpen (ii)

Απόδειξη.

Υπάρχουν q διαφορετικα ζευγάρια (e_1^*, e_2^*) που δίνουν το ίδιο c. Ο επιτιθέμενος δεν είναι σε θέση να γνωρίζει ποιο χρησιμοποιήθηκε.

Ασφάλεια σχήματος Chaum - van Antwerpen (ii)

Απόδειξη.

Υπάρχουν q διαφορετικα ζευγάρια (e_1^*, e_2^*) που δίνουν το ίδιο c. Ο επιτιθέμενος δεν είναι σε θέση να γνωρίζει ποιο χρησιμοποιήθηκε. Επιπλέον, καθένα από αυτά τα q ζεύγη επαληθεύεται με διαφορετικό d, διότι όταν $s \not\equiv m^a \pmod{p}$ το σύστημα ισοτιμιών:

$$
\begin{aligned}
c &\equiv s^{e_1^*} \beta^{e_2^*} \pmod{p} \\
d &\equiv m^{e_1^*} g^{e_2^*} \pmod{p}
\end{aligned}
$$

έχει μοναδικη λύση ως προς (e_1^*, e_2^*). Αυτό αποδεικνύεται αν πάρουμε το αντίστοιχο σύστημα με τις ισοτιμίες των εκθετών $\pmod{q}$: η ορίζουσα είναι μη μηδενική.

Ασφάλεια σχήματος Chaum - van Antwerpen (ii)

Απόδειξη.

Υπάρχουν q διαφορετικα ζευγάρια (e_1^*, e_2^*) που δίνουν το ίδιο c. Ο επιτιθέμενος δεν είναι σε θέση να γνωρίζει ποιο χρησιμοποιήθηκε. Επιπλέον, καθένα από αυτά τα q ζεύγη επαληθεύεται με διαφορετικό d, διότι όταν $s \not\equiv m^a \pmod p$ το σύστημα ισοτιμιών:

$$c \equiv s^{e_1^*} \beta^{e_2^*} \pmod p$$
$$d \equiv m^{e_1^*} g^{e_2^*} \pmod p$$

έχει μοναδικη λύση ως προς (e_1^*, e_2^*). Αυτό αποδεικνύεται αν πάρουμε το αντίστοιχο σύστημα με τις ισοτιμίες των εκθετών $\pmod q$: η ορίζουσα είναι μη μηδενική.

Έτσι, η πιθανότητα του επιτιθέμενου να βρει το σωστό d είναι $\frac{1}{q}$. □

Ασφάλεια σχήματος Chaum - van Antwerpen (iii)

Όπως είπαμε, χρειάζεται η δυνατότητα να μην μπορεί να αποποιηθεί η A μια γνήσια υπογραφή, αλλά να μπορεί να αποδείξει την πλαστότητα μιας πλαστής. Αυτά επιτυγχάνονται με το παρακάτω:

Πρωτόκολλο αποκήρυξης (disavowal protocol)

Αποτελείται από 2 διαδοχικές εκτελέσεις του πρωτοκόλλου επαλήθευσης, έστω e_1', e_2', c', d' οι παράμετροι της δεύτερης εκτέλεσης:
Έστω ότι το πρωτόκολλο αποτυγχάνει και τις δύο φορές: είτε η υπογραφή είναι πλαστή, είτε η A δίνει λανθασμένες απαντησεις d, d'.
Στο τέλος γίνεται ο έλεγχος:

$$(dg^{-e_2})^{e_1'} \equiv (d'g^{-e_2'})^{e_1} \mod p$$

Αν ισχύει ισοτιμία σημαίνει (με πολύ μεγάλη πιθανότητα) ότι η υπογραφή είναι πλαστή, αν όχι η υπογραφή είναι γνήσια.

Ασφάλεια σχήματος Chaum - van Antwerpen (iv)

Έλεγχος αποκήρυξης:

$$(dg^{-e_2})^{e'1} \equiv (d'g^{-e'_2})^{e1} \mod p \quad (1)$$

Αν ισχύει ισοτιμία ⇒ υπογραφή πλαστή, αν όχι ⇒ υπογραφή γνήσια.

Θα δείξουμε ότι:

Θεώρημα

Στο σχήμα Chaum - van Antwerpen αν η υπογραφή είναι όντως πλαστή τότε η A θα μπορέσει με βεβαιότητα να το αποδείξει, ενώ αν είναι γνήσια, η πιθανότητα της A να εμφανίσει την υπογραφή ως πλαστή είναι $\frac{1}{q}$ *ανεξάρτητα από την υπολογιστική της ισχύ*.

Ασφάλεια σχήματος Chaum - van Antwerpen: απόδειξη (i)

Σενάριο 1: η υπογραφή είναι πλαστή: $s \not\equiv m^a \pmod p$

Η A παρέχει σωστά κατασκευασμένα d, d' όμως το πρωτόκολλο επαλήθευσης αποτυγχάνει και τις δύο φορές καθώς $s \not\equiv m^a \pmod p$.
Ισχύει όμως ότι (λόγω σωστής κατασκευής των d, d'):

$$dg^{-e_2} \equiv s^{e_1 a^{-1}} \pmod p \Rightarrow (dg^{-e_2})^{e_1'} \equiv s^{e_1 a^{-1} e_1'}$$
$$dg^{-e_2'} \equiv s^{e_1' a^{-1}} \pmod p \Rightarrow (dg^{-e_2'})^{e_1} \equiv s^{e_1' a^{-1} e_1}$$

Επομένως το πρωτόκολλο αποκήρυξης θα δείξει ότι η υπογραφή είναι πλαστή.

Ασφάλεια σχήματος Chaum - van Antwerpen: απόδειξη (ii)

Σενάριο 2: η υπογραφή είναι γνήσια: $s \equiv m^a \pmod{p}$

Η A παρέχει ψευδή d, d' προκειμένου να αποτύχει το πρωτόκολλο επαλήθευσης και τις δύο φορές. Από τα c, c' που έχει λάβει η A μπορεί (αν διαθέτει μεγάλη υπολογιστική δύναμη) να υπολογίσει q διαφορετικά ζεύγη e_1^*, e_2^* που δίνουν το συγκεκριμένο c και q διαφορετικά ζεύγη $e_1'^*, e_2'^*$ που δίνουν το συγκεκριμένο c'.

(i) Η πιθανότητά της να μαντέψει τη σωστή τετράδα και έτσι να υπολογίσει ψευδή d, d' που να κάνουν την (1) να ισχύει είναι $1/q^2$.

(ii) Η πιθανότητα της A να δημιουργήσει d, d' με οποιονδήποτε άλλο τρόπο που να επαληθεύουν την (1) φράσσεται από το $1/q$:

Ασφάλεια σχήματος Chaum - van Antwerpen: απόδειξη (iii)

Σενάριο 2 (συν.): η υπογραφή είναι γνήσια: $s \equiv m^a \pmod p$

Αν η (1) επαληθεύεται τότε $d' \equiv d_0^{e_1'} g^{e_2'} \pmod p$ για $d_0 = d^{e_1^{-1}} g^{-e_2 e_1^{-1}}$.
Αυτό σημαίνει ότι η s είναι έγκυρη υπογραφή για d_0.

Ισχύει όμως: $d \not\equiv m^{e_1} g^{e_2} \pmod p \quad (2)$
Έστω $d_0 \equiv m \pmod p$. Τότε (από (2)) $d \not\equiv (d^{e_1^{-1}} g{-}e_2 e_1^{-1})^{e_1} g^{e_2} \equiv d$.
Αντίφαση.
Επομένως ισχύει $s \not\equiv d_0^a \pmod p$, παρ'όλα αυτά η A καταφέρνει να φτιάξει d' ώστε η s να φαίνεται σαν έγκυρη υπογραφή για το d_0.
Σύμφωνα με προηγούμενη ανάλυση, η πιθανότητα να συμβαίνει αυτό είναι $1/q$ *ανεξαρτήτως υπολογιστικής ισχύος* της A.

Υπογραφές Fail-Stop: σχήμα van Heyst - Pedersen

- KeyGen:
  Έμπιστη αρχή (TTP): επιλογή πρώτων $p, q, p = 2q + 1$, γεννήτορα g της υποομάδας $QR(p)$ (τάξης q), $a \overset{R}{\leftarrow} \mathbb{Z}_q^*$, $\beta = g^a \bmod p$.
  $TTP \xrightarrow{(p,q,g,\beta)} A$. Γνωστό μόνο στην TTP: a.
  $A : a_1, a_2, b_1, b_2 \overset{R}{\leftarrow} \mathbb{Z}_q$,
  $$\gamma_1 = g^{a_1}\beta^{a_2} \bmod p$$
  $$\gamma_2 = g^{b_1}\beta^{b_2} \bmod p.$$
  Public key: $p_A = (\gamma_1, \gamma_2, p, q, g, \beta)$.
  Secret key: $s_A = (a_1, a_2, b_1, b_2)$.

Υπογραφές Fail-Stop: σχήμα van Heyst - Pedersen

- KeyGen:
  Έμπιστη αρχή (TTP): επιλογή πρώτων $p, q, p = 2q + 1$,
  γεννήτορα g της υποομάδας $QR(p)$ (τάξης q), $a \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$,
  $\beta = g^a \bmod p$.

  $TTP \xrightarrow{(p,q,g,\beta)} A$. Γνωστό μόνο στην TTP: a.
  $A : a_1, a_2, b_1, b_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q$,

  $$\gamma_1 = g^{a_1} \beta^{a_2} \bmod p$$

  $$\gamma_2 = g^{b_1} \beta^{b_2} \bmod p.$$

  Public key: $p_A = (\gamma_1, \gamma_2, p, q, g, \beta)$.
  Secret key: $s_A = (a_1, a_2, b_1, b_2)$.
- Signing:
  $A : m \in \mathbb{Z}_q^* \xrightarrow{\langle m, s_1, s_2 \rangle, \quad s_1 = a_1 + mb_1 \bmod q, \ s_2 = a_2 + mb_2 \bmod q} B$

Υπογραφές Fail-Stop: σχήμα van Heyst - Pedersen

- KeyGen:
  Έμπιστη αρχή (TTP): επιλογή πρώτων $p, q, p = 2q + 1$,
  γεννήτορα g της υποομάδας $QR(p)$ (τάξης q), $a \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$,
  $\beta = g^a \bmod p$.
  $TTP \xrightarrow{(p,q,g,\beta)} A$. Γνωστό μόνο στην TTP: a.
  $A : a_1, a_2, b_1, b_2 \stackrel{R}{\leftarrow} \mathbb{Z}_q$,
  $$\gamma_1 = g^{a_1}\beta^{a_2} \bmod p$$
  $$\gamma_2 = g^{b_1}\beta^{b_2} \bmod p.$$
  Public key: $p_A = (\gamma_1, \gamma_2, p, q, g, \beta)$.
  Secret key: $s_A = (a_1, a_2, b_1, b_2)$.
- Signing:
  $$A : m \in \mathbb{Z}_q^* \xrightarrow{\langle m, s_1, s_2 \rangle, \quad s_1 = a_1 + mb_1 \bmod q, \;\; s_2 = a_2 + mb_2 \bmod q} B$$
- Verification:
  $ver(m, s_1, s_2) = \texttt{true} \Leftrightarrow \gamma_1 \gamma_2^m = g^{s_1}\beta^{s_2} \pmod{p}$

Σχήμα van Heyst - Pedersen: παρατηρήσεις

- Σχήμα μιας χρήσης (one-time): αν δύο μηνύματα υπογραφούν με το ίδιο ιδιωτικό κλειδί, μπορεί να βρεθεί το κλειδί.

Σχήμα van Heyst - Pedersen: παρατηρήσεις

- Σχήμα μιας χρήσης (one-time): αν δύο μηνύματα υπογραφούν με το ίδιο ιδιωτικό κλειδί, μπορεί να βρεθεί το κλειδί.
- Υπάρχουν q^2 ιδιωτικά κλειδιά (a_1, a_2, b_1, b_2) που δίνουν το ίδιο (γ_1, γ_2).

Σχήμα van Heyst - Pedersen: παρατηρήσεις

- Σχήμα μιας χρήσης (one-time): αν δύο μηνύματα υπογραφούν με το ίδιο ιδιωτικό κλειδί, μπορεί να βρεθεί το κλειδί.
- Υπάρχουν q^2 ιδιωτικά κλειδιά (a_1, a_2, b_1, b_2) που δίνουν το ίδιο (γ_1, γ_2).
- Από αυτά, ακριβώς q δίνουν την ίδια υπογραφή s_1, s_2 για ένα μήνυμα m. Επομένως, τα q^2 πιθανά ιδιωτικά κλειδιά παράγουν ακριβώς q διαφορετικές υπογραφές για το m.

Σχήμα van Heyst - Pedersen: παρατηρήσεις

- Σχήμα μιας χρήσης (one-time): αν δύο μηνύματα υπογραφούν με το ίδιο ιδιωτικό κλειδί, μπορεί να βρεθεί το κλειδί.
- Υπάρχουν q^2 ιδιωτικά κλειδιά (a_1, a_2, b_1, b_2) που δίνουν το ίδιο (γ_1, γ_2).
- Από αυτά, ακριβώς q δίνουν την ίδια υπογραφή s_1, s_2 για ένα μήνυμα m. Επομένως, τα q^2 πιθανά ιδιωτικά κλειδιά παράγουν ακριβώς q διαφορετικές υπογραφές για το m.
- Για δύο διαφορετικά μηνύματα m, m', τα q κλειδιά που δίνουν την "σωστή" υπογραφή για το m δίνουν q διαφορετικές υπογραφές για το m'.

Σχήμα van Heyst - Pedersen: ασφάλεια

- Δυσκολία πλαστογράφησης:

  - Ένας πλαστογράφος που γνωρίζει μόνο το δημόσιο κλειδί έχει πιθανότητα $\frac{q}{q^2} = \frac{1}{q}$ να κατασκευάσει "σωστή" υπογραφή για ένα μήνυμα m' της επιλογής του, ανεξαρτήτως υπολογιστικής ισχύος.

  - Ένας πλαστογράφος που αποκτά μια έγκυρη τριάδα (m, s_1, s_2) έχει πιθανότητα $\frac{1}{q}$ να κατασκευάσει σωστή υπογραφή για ένα μήνυμα m' της επιλογής του, ανεξαρτήτως υπολογιστικής ισχύος (ακόμη και αν μπορεί να υπολογίσει τα q κλειδιά που δίνουν την "σωστή" υπογραφή για το m).

Σχήμα van Heyst - Pedersen: ασφάλεια

- Απόδειξη πλαστογράφησης:

  Το σχήμα παρέχει επιπρόσθετη ασφάλεια (χωρίς υπολογιστικές προϋποθέσεις) έναντι πλαστογράφησης. Συγκεκριμένα, ο νόμιμος υπογράφων μπορεί να αποδείξει ότι μια υπογραφή είναι πλαστογραφημένη, χρησιμοποιώντας την για να αποκαλύψει τον – γνωστό μόνο στην έμπιστη αρχή – εκθέτη a.

  Επειδή η εύρεση του εκθέτη είναι υπολογιστικά απρόσιτη, η παραπάνω μέθοδος συνιστά απόδειξη πλαστογράφησης.

Σχήμα van Heyst - Pedersen: απόδειξη πλαστογράφησης

Θεώρημα

Στο σχήμα van Heyst - Pedersen μία κατασκευασμενη από τον αντίπαλο υπογραφή που περνάει το πρωτόκολλο επαλήθευσης μπορεί (με πολύ μεγάλη πιθανότητα) να χρησιμοποιηθεί για την αποκάλυψη του εκθέτη a, ανεξαρτήτως της υπολογιστικής ισχύος του αντιπάλου.

Σχήμα van Heyst - Pedersen: απόδειξη πλαστογράφησης

Θεώρημα

Στο σχήμα van Heyst - Pedersen μία κατασκευασμενη από τον αντίπαλο υπογραφή που περνάει το πρωτόκολλο επαλήθευσης μπορεί (με πολύ μεγάλη πιθανότητα) να χρησιμοποιηθεί για την αποκάλυψη του εκθέτη a, ανεξαρτήτως της υπολογιστικής ισχύος του αντιπάλου.

Απόδειξη.

Για κάθε υπογραφή που επαληθεύεται υπάρχουν και άλλες $q - 1$ υπογραφές που επαληθεύονται για το ίδιο μήνυμα. Η πιθανότητα να έχει βρει ο αντίπαλος μία από τις υπόλοιπες ειναι $1 - \frac{1}{q}$.

Αν ισχύει κάτι τέτοιο, τότε ο υπολογισμος

$$a = (s_1 - s_1') \cdot (s_2 - s_2')^{-1} \bmod q$$

αποκαλύπτει τον εκθέτη a. $\square$

Ανακεφαλαιώνοντας

- Ψηφιακές υπογραφές: κυρίως με χρήση ασύμμετρης κρυπτογραφίας (RSA, ElGamal, DSS).

Ανακεφαλαιώνοντας

- Ψηφιακές υπογραφές: κυρίως με χρήση ασύμμετρης κρυπτογραφίας (RSA, ElGamal, DSS).
- Τριάδα αλγορίθμων: παραγωγή κλειδιών, υπογραφή, επαλήθευση.

Ανακεφαλαιώνοντας

- Ψηφιακές υπογραφές: κυρίως με χρήση ασύμμετρης κρυπτογραφίας (RSA, ElGamal, DSS).
- Τριάδα αλγορίθμων: παραγωγή κλειδιών, υπογραφή, επαλήθευση.
- Υπογραφές επιπρόσθετης λειτουργικότητας: τυφλές (blind), αδιαμφισβήτητες (undeniable – παρέχουν απόδειξη πλαστογράφησης), με διακοπή αν πλαστογραφηθούν (fail-stop).