Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Δημητρέλλος Παναγιώτης

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

17 Δεκεμβρίου 2012

1 Πρότυπο Ψηφιακής Υπογραφής(Digital Signature Standard)

Το *Πρότυπο Ψηφιακής Υπογραφής(DSS)* αποτελεί μία παραλλαγή του σχήματος υπογραφής του *ElGamal* , που προσπαθεί να μειώσει το μέγεθος της ψηφιακής υπογραφής που παράγεται. Πριν αναλύσουμε το *DSS* ας θυμηθούμε πως λειτουργεί,περιληπτικώς,το σχήμα του *ElGamal*:
Έστω p πρώτος,τότε επιλέγουμε τυχαίο ακέραιο $k \in \mathbb{Z}_{p-1}^*$.Υπολογίζουμε τα γ, δ, όπου

$$\gamma = g^k \underline{\text{mod}} p$$
$$\delta = (m - \alpha\gamma)k^{-1} \underline{\text{mod}} (p-1)$$

και θυμίζουμε ότι $\beta = g^\alpha \underline{\text{mod}} p$,με g το γεννήτορα της ομάδας.
και για την επαλήθευση έχουμε:

$$ver(m, \gamma, \delta) = True \Leftrightarrow \beta^\gamma \cdot \gamma^\delta \equiv g^m (\underline{\text{mod}} p)$$

Παρατηρούμε πως οι εκθέτες ανήκουν στην ομάδα $\mathbb{Z}_{p-1}^*$, και το γεγονός αυτό μας υποχρεώνει να επεξεργαζόμαστε μεγάλες υπογραφές. Η λειτουργία που επιτελεί το *DSS* είναι να μειώνει το μέγεθος της ομάδας στην οποία δουλεύουμε.Έτσι λοιπόν έστω g γεννήτορας υποομάδας της $\mathbb{Z}_{p-1}^*$, τάξης q, όπου q πρώτος αριθμός,και ισχύει $q|p-1$. Συνεπώς,αν g_0 ο γεννήτορας της $\mathbb{Z}_{p-1}^*$,τότε ισχύει:

$$g = (g_0)^{\frac{p-1}{q}} \underline{\text{mod}} p \Rightarrow g^q \equiv 1 (\underline{\text{mod}} p)$$

δηλαδή κάθε αποτέλεσμα που εμφανίζεται ανήκει στο $< q >$, συνεπώς $\beta, \gamma \in < q >$, και προφανώς όλοι οι εκθέτες είναι το πολύ μεχρι q, άρα τους επεξεργαζόμαστε $(\text{mod} q)$.
Υπολογίζουμε:

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

αλλά για να έχουμε ουσιαστικό υπολογιστικό κέρδος πρέπει να υπολογίσουμε και το γ σε $(\underline{\text{mod}} q)$.Αυτό γίνεται με τη παρακάτω διαδικασία: Ισχύει ότι $\delta = (m + \alpha\gamma)k^{-1} \text{ mod } q \Rightarrow k\delta \equiv (m + \alpha\gamma)(\text{mod} q) \Rightarrow g^{k\delta} \equiv g^m \cdot g^{\alpha\gamma} (\text{mod} p) \Rightarrow \gamma^\delta \equiv g^m \cdot \beta^\gamma (\text{mod} p) \Rightarrow \gamma \equiv g^{m\delta^{-1}} \cdot \beta^{\gamma\delta^{-1}} (\text{mod} p)$ όπου το δ^{-1} είναι υπολογισμένο $(\text{mod} q)$,και αν θεωρήσουμε:

$$\gamma' = g^k \underline{\text{mod}} p \quad \text{(I)}$$
$$\gamma = (g^k \underline{\text{mod}} p) \underline{\text{mod}} q \quad \text{(II)}$$

$\Rightarrow \gamma' = g^{m\delta^{-1}} \cdot \beta^{\gamma\delta^{-1}} (\mathrm{mod} p)$, αλλά αφού $\gamma' < p$ τότε
$\gamma' = g^{m\delta^{-1}} \cdot \beta^{\gamma\delta^{-1}} \underline{\mathrm{mod}} p$, άρα από τη σχέση (II) έχουμε:

$$\gamma = (g^{m\delta^{-1}} \cdot \beta^{\gamma\delta^{-1}} \underline{\mathrm{mod}} p) \underline{\mathrm{mod}} q$$

Παρατηρούμε ότι το γ είναι τώρα εκπεφρασμένο ως προς $(\mathrm{mod} q)$,άρα πετυχαίνουμε το υπολογιστικό κέρδος που αναζητούσαμε.Είναι όμως απαραίτητο να ελέγξουμε και την ορθότητα της παραπάνω υπογραφής.
Προς απλοποίηση των υπολογισμών,ας συμβολίσουμε:

$$e_1 = m\delta^{-1} \underline{\mathrm{mod}} q$$
$$e_2 = \gamma\delta^{-1} \underline{\mathrm{mod}} q$$

Τότε:
$ver(m, \gamma, \delta) = True \Leftrightarrow \gamma = (g^{e_1} \cdot \beta^{e_2} \underline{\mathrm{mod}} p) \underline{\mathrm{mod}} q \Leftrightarrow \gamma = (g^{e_1} \cdot \beta^{e_2} \underline{\mathrm{mod}} p)(\underline{\mathrm{mod}} q)$
Άρα η υπογραφή ειναι ορθή, και με αυτό το τρόπο τη μειώσαμε σε μήκος, και παρατηρούμε ότι η υπογραφή γίνεται γρηγορότερα από την επαλήθευση.Άς σημειώσουμε ότι μετά την εφαρμογή του *DSS*, η επίλυση του *DLP* παραμένει δύσκολη στην υποομάδα τάξης 2^{160}.

2 Γενικό Σχήμα Υπογραφής(Lamport Scheme)

Το σχήμα υπογραφής του *Lamport* αποτελεί ένα *one-time scheme* το οποίο υλοποιείται ως εξής:

Έστω μια *one-way* συνάρτηση f :

$$f : Y \to Z$$

Έστω ενα μύνημα $m = (x_1, x_2, ..., x_k)$,με $x_i \in \{0, 1\}$.
Επιλέγουμε

$$(y_{10}, y_{20}, ..., y_{k0})$$
$$(y_{11}, y_{21}, ..., y_{k1})$$

τα οποία αποτελούν και το *ιδιωτικό κλειδί* του χρήστη. Άς σημειωθεί ότι τα y_{ij} επιλέγονται από το πεδίο ορισμού της f τυχαία,$(y_{ij} \leftarrow Y)$.Έπειτα υπολογίζουμε τα

$$(z_{10}, z_{20}, ..., z_{k0})$$
$$(z_{11}, z_{21}, ..., z_{k1})$$

όπου $z_{ij} = f(y_{ij})$,τα οποία αποτελούν το *δημόσιο κλειδί*.
Παράδειγμα λειτουργίας:Έστω $m = (1, 0, ..., 1)$,τότε

$$\textit{secret key: } y_{11}, y_{20}, ..., y_{k1}$$
$$\textit{public key: } z_{11}, z_{20}, ..., z_{k1}$$

Και ως προς την υπογραφή έχουμε:
$s = sig(m) = (y_{1x_1}, y_{2x_2}, ..., y_{kx_k})$,και η *Alice* στέλνει στον *Bob* τα (m, s).
Τότε ο *Bob* για να επαληθεύσει την υπογραφή ελέγχει τη συνθήκη:

$$ver(m, s) = True \Leftrightarrow \forall i : f(s_i) = z_{ix_i}$$

Παρατηρούμε πως για κάθε υπογραφή παίρνουμε ένα υποσύνολο k στοιχείων από ένα σύνολο $2k$ στοιχείων,συνεπώς χρησιμοποιούμε 2^k από ένα σύνολο $\binom{2k}{k}$ δυνατών υπογραφών.
Από το τύπο του *Stirling* έχουμε:
$\binom{2k}{k} \approx \frac{(2^k)^2}{\sqrt{\pi k}} \Rightarrow \binom{2k}{k} \gg 2^k$
άρα το σύστημα είναι "σπάταλο".

3 Bos-Chaum Scheme

Έστω ένα σύνολο με $2n$ στοιχεία και διαλέγουμε τα n από αυτά.Βρίσκουμε το ελάχιστο k για το οποίο ισχύει:
$2^k \geq \binom{2k}{k}$ Έτσι από το τύπο του *Stirling* έχουμε $n \approx \frac{k}{2}$,για μεγάλο k,και έτσι προκύπτει η μισή υπογραφή.

4 Τυφλές Υπογραφές

Σκοπός του σχήματος αυτού είναι η υπογραφή άγνωστων από το χρήστη κειμένων που προέρχονται από έμπιστη πηγή,με στόχο την απόκρυψη κάποιων πληροφοριών από τον αποστολέα για λόγους ιδιωτικότητας.
Η διαδικασία έχει ως εξής:
Έστω συναρτήσεις

$$f : M \to M$$
$$g : S \to S$$

Τότε αν m το μύνημα,η Alice στέλνει στον Bob το $m^* = f(m)$, *τύφλωση(blinding)*,και ο Bob καλείται να υπογράψει το m^*, το οποίο δεν αντιλαμβάνεται.Η συνάρτηση g έχει επιλεχθεί ώστε να εχει την ιδιότητα:

$g(sig(m^*)) = sig(m) \Rightarrow sig(m) = g(sig(f(m)))$
άρα η Alice μπορεί να χρησιμοποιήσει την υπογραφή του Bob, επειδή αυτή που θα λάβει με εφαρμογή της g πάνω της είναι έγκυρη. Μια εφαρμογή του παραπάνω είναι η εξής:

1. Chaum's Signature Scheme

   Το σχήμα του *Chaum* βασίζεται στο σύστημα *RSA* και η υλοποίησή του γίνεται με το παρακάτω τρόπο:
   Έστω ότι ο Bob έχει τα ζεύγη (p_B, n) *(δημόσιο κλειδί)* και (s_B, p, q) *(ιδιωτικό κλειδί)*. Στο σημείο αυτό 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:
   $s = sig(m^*) = (m^*)^{s_B} \underline{\text{mod}} n = (m \cdot k^{p_B})^{s_B} \underline{\text{mod}} n = (m^{s_B} \cdot k) \underline{\text{mod}} n \equiv sig(m) \cdot k (\text{mod} n)$
   και ο Bob στέλνει το s στην Alice.

   iii) Η Alice δέχεται το s από τον Bob και υπολογίζει:
   $s' = s \cdot k^{-1} \underline{\text{mod}} n = sig(m) \cdot k \cdot k^{-1} \underline{\text{mod}} n = sig_B(m)$
   Άρα η Alice έχει την υπογραφή του Bob πάνω στο m που του έστειλε αρχικά,η οποία είναι απολύτως έγκυρη *(unblinding)*.

5 Αδιαμφισβήτητα Σχήματα Υπογραφής(Undeniable Signature Schemes)

- Η επαλήθευση απαιτεί τη συμμετοχή του υπογράφοντα (προστασία από επαναχρησιμοποίηση,διάδοση υπογραφής κλπ...)

- Χρειάζεται προστασία και η άλλη πλευρά,δηλαδή να μη μπορεί ο υπογράφων να αρνηθεί την επαλήθευση ,ούτε να εκτελέσει λανθασμένα το πρωτόκολλο επαλήθευσης.

- Τελικά χρειάζεται *"πρωτόκολλο αποκήρυξης"(disavowal protocol)*

- αν η υπογραφή είναι γνήσια δε μπορεί να αποτύχει το πρωτόκολλο.

- αν η υπογραφή είναι πλαστή τότε το πρωτόκολλο αποτυγχάνει,και ο υπογράφων μπορεί να αποποιηθεί την υπογραφή.

1. Chaum-van Antwerpen Scheme
   Η διαδικασία δημιουργίας του κλειδιού *(key generation)* γίνεται ως εξής:
   επιλέγουμε δύο πρώτους αριθμούς p, q τέτοιους ώστε $p = 2q + 1$,και με τη χρήση του *DSS* προκύπτει $g = (g_0)^2$,όπου g είναι η τάξη του $q = \frac{p-1}{2}$.
   Το *secret key* είναι κάποιο $a \in \mathbb{Z}_q$
   Το *public key* είναι η τετράδα (p, q, g, β),όπου $\beta = g^a \underline{\text{mod}} p$
   Υπογραφή
   $s = sig(m) = m^a \underline{\text{mod}} p$ και η Alice στέλνει στον Bob τα (m, s).
   Επαλήθευση
   Ο Bob ζητάει *verification* από την Alice.

   i) Ο Bob επιλέγει τυχαία ένα ζεύγος (e_1, e_2) από το σύνολο $\mathbb{Z}_q^* \times \mathbb{Z}_q^*$.
   Έπειτα στέλνει Alice το $c = s^{e_1} \cdot \beta^{e_2} \underline{\text{mod}} p$.

   ii) Η Alice δέχεται το c και υπολογίζει το

   $$d = \left(c^{a^{-1} \underline{\text{ mod } q}}\right) \underline{\text{mod}} p$$

   και το στέλνει στον Bob.

   iii) Ο Bob επαληθεύει: $ver(m, s, d) = True \Leftrightarrow d \equiv m^{e_1} \cdot g^{e_2} (\underline{\text{mod}} p)$

   Το παραπάνω σύστημα δουλεύει σωστά,καθώς:
   $c \equiv m^{ae_1} \cdot g^{ae_2} (\underline{\text{mod}} p) \Rightarrow c^{a^{-1} \underline{\text{ mod } q}} = d \equiv m^{e_1} \cdot g^{e_2} (\underline{\text{mod}} p)$
   Θεώρημα:Αν για το ζεύγος (m, s) ισχύει
   $m \neq s (\text{mod} p) \Rightarrow Pr[ver(m, s, d) = True] = \frac{1}{q}$
   *Απόδειξη:*Παρατηρούμε πως υπάρχουν q διαφορετικά ζεύγη (e_1, e_2) τα οποία δίνουν το ίδιο c (προκύπτει κρατώντας το ένα σταθερό και αλλάζοντας το άλλο στο $\mathbb{Z}_q$).Έτσι ο Oscar δε μπορεί να γνωρίζει πιο από αυτά χρησιμοποιήθηκε, και έχει πιθανότητες να το μαντέψει σωστά $\frac{1}{q}$.
   Πρωτόκολλο αποκήρυξης
   i) έως **iii)** :εκτελούμε την επαλήθευση.
   iv) έως **vi)** :αν η πρώτη επαλήθευση αποτύχει εκτελούμε την επαλήθευση ξανά με άλλο ζεύγος.
   vii) Αν $(d_1 \cdot g^{-e_2})^{f_1} \equiv (d_2 \cdot g^{-f_2})^{e_1} (\text{mod} p)$
   είναι αληθές τότε ο Bob δέχεται ότι η υπογραφή είναι πλαστή,με πιθανότητα να ξεγελαστεί ίση με $\frac{1}{q}$.

Βιβλιογραφία

Zac12 : Σημειώσεις Ζάχου, ΕΜΠ, 2012.

Sti06 : D. Stinson: Cryptography: Theory and Practice, 3rd edition, CRC Press, 2005.