Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών
&
Εφαρμογές στην Κρυπτογραφία

Επιμέλεια Σημειώσεων
Γεώργιος Ρούτης

Διδάσκοντες
Στάθης Ζάχος
Άρης Παγουρτζής

14 Ιανουαρίου 2013

1 Εισαγωγή

Οι έννοιες *proof of knowledge* και *zero knowledge* είναι διακριτές.

Στην πρώτη περίπτωση ο αιτών Α αποδεικνύει ότι γνωρίζει κάτι, χωρίς να το αποκαλύψει, και στον Β δίνονται πληροφορίες που δε θα μπορούσε να τις υπολογίσει αποδοτικά (θα μπορούσε όμως μη αποδοτικά).

Στα zero knowledge σχήματα αναγνώρισης, ο Β δεν παίρνει καμία πληροφορία που δε θα μπορούσε να την υπολογίσει και μόνος του.

Ανάλογα με το πόσο γρήγορα, αποδοτικά κ.τ.λ. θα μπορούσε ο Β να υπολογίσει τις πληροφορίες του, δημιουργούνται επίπεδα ασφάλειας στα proof of knowledge και zero knowledge σχήματα.

Αν η αποκάλυψη ή μη του μυστικού είναι τυχαία μεταβλητή και έχουμε δύο από αυτές, τότε, στα perfect zero knowledge συστήματα, δεν μπορούν οι δύο αυτές μεταβλητές να διακριθούν. Στα statistical συστήματα, η διαφορά $P[x] - P[y]$ είναι πολύ μικρή, ενώ, στα computational συστήματα, με τις πληροφορίες που λαμβάνει ο Β δεν μπορεί σε πολυωνυμικό χρόνο να μάθει τίποτα παρ απάνω απ' ό,τι θα μάθαινε χωρίς αυτές.

2 Fiat-Shamir Identification protocol

Αρχικοποίηση: έμπιστη αρχή δημοσιεύει $n = pq$, p, q μυστικό.

Η Alice επιλέγει s, τέτοιο ώστε $1 \leq s \leq n-1$, $gcd(s, n) = 1$ υπολογίζει το $u = s^2 \bmod n$ και το στέλνει στην έμπιστη αρχή για να το κατοχυρώσει ως δημόσιο κλειδί της.

Εκτέλεση:

1. Η Α επιλέγει ένα τυχαίο r, τέτοιο ώστε $1 \leq r \leq n-1$ και υπολογίζει το x, τέτοιο ώστε $x = r^2 \pmod n$ // δέσμευση
2. Ο Β επιλέγει $e \in^{\Re} 0, 1$ // πρόκληση
3. Ο Α στέλνει $r \cdot s^e \bmod n$ στον Β // ανταπόκριση
4. Ο Β ελέγχει $y^2 = x \cdot u^2 \pmod n$

Σχόλια …

Πληρότητα: Ναι, υπάρχει.

Ορθότητα: Με t επαναλήψεις

$$\Pr(\text{success}) \leq \frac{1}{2^t}$$

περίπου. Αυτό όμως δεν μας εξασφαλίζει zero knowledge.

Απόπειρες εξαπάτησης του Β: Α': επιλέγει r' στέλνει $x = r'^2$ Αν $e = 0$, τότε ok (στέλνει $y = y'$) Αν $e = 1$ θα πρέπει να βρει τέτοιο ώστε

$$y^2 = (r'^2) \cdot u = (y' \cdot s)^2 \pmod n$$

δηλαδή απαιτείται υπολογισμός παραγοντικού ρίζας, κάτι το οποίο υπολογίζεται δύσκολα. $y = y'$ $y^2 = x \cdot u = \frac{r'^2}{u} = r'^2$

2.1 Feige-Fiat-Shamir identification protocol

$$s_1, \cdots, s_k$$

$$u_1, \cdots, u_k$$

1. Ο Α στέλνει $x = \pm r^2 \bmod n$ στον Β
2. Ο Β στέλνει $\langle e_1, \ldots, e_k \rangle$
3. Ο Α στέλνει $y = r \cdot \prod s_i^{e_i} \pmod n$
4. Ο Β ελέγχει αν $y^2 = \pm x \cdot \prod u_i^{e_i}$

3 Πιθανοτική Κρυπτογράφηση

Με τον όρο πιθανοτικό εννοούμε κατά μία έννοια μη ντετερμινιστικό. Η συνάρτηση κρυπτογράφησης δεν είναι αυτό που ονομάζουμε 1 προς 1 (πχ. El Gamal).

3.1 Πιθανοτική Κρυπτογράφηση Goldwasser – Micali

$$n = p \cdot q$$

$x \in QR(n)$: δυσκολο αν δεν γνωρίζουμε p, q.

$$QR(n) = \left\{x \mid \exists m \in \mathbb{Z}_m : m^2 = x \pmod n\right\}$$

$$= \{x \mid (x/p) = 1 \wedge (x/p) = -1\}$$

$$x \in R(n) \Rightarrow \frac{x}{n} = 1$$

$$\widetilde{Q}R(n) = \left\{x \mid \frac{x}{n} = 1 \wedge x \mid \frac{x}{n} = -1\right\}$$

(Το σύμβολο $\widetilde{Q}R(n)$ ονομάζεται ψευδοτετράγωνο modulo n)

$$\widetilde{Q}R(n) = \left\{x \mid \frac{x}{n}\right\} = 1$$

Αρχικοποίηση: Επιλέγουμε $t \in \widetilde{Q}R(n)$ Κρυπτογράφηση του x, με τη χρήση τυχαίου r:

$$y = e_k(x, r) = t^x \cdot r^2 \bmod n$$

Σημείωση: το x είναι 1 bit

$$x \in \{0, 1\}, r \in^R \mathbb{Z}_n$$

$$d_k = 0, y \in QR(n)$$

$$d_k = 1, y \in \widetilde{Q}R(n)$$

Σημείωση: Το σύστημα φαίνεται να είναι πολύ ασφαλές υπολογιστικά.

3.2 BBS Generator

Παίρνει seed $S_o \in QR(x)$. Για $i = 1, \cdots, l$.

$$S_i = S_{i-1}^2 \bmod n$$

$Z_i = S_i \bmod 2$ (ουσιαστικά παίρνει το τελευταίο bit) Αυτό το σύστημα λέγεται (k, l) γεννήτρια ψευδοτυχαίων αριθμών με $k = \lceil logn \rceil$. Δηλαδή έχουμε την συνάρτηση f (που είναι γεννήτρια) που για είσοδο S_o δίνει το διάνυσμα $(z_o, \cdots, z_l)$.

Επιλέγουμε p, q πρώτους ώστε $p \equiv q \equiv 3 \bmod 4$ γιατί έτσι υπολογίζουμε εύκολα ρίζες $C^{\frac{p+1}{4}^2} \equiv C^{\frac{p-1}{2}+1} \equiv C \pmod p$

Έστω το μήνυμα $x = (x_1, \cdots, x_l)$. Τότε $enc(x) = (y_1, \cdots, y_l, y_{l+1})$ όπου $y_i = x_i + z_i \bmod 2 = x_i \oplus$ όπου $s_{l+1} \equiv s_l^2 \equiv s_{2^{l+1}}^1 \bmod n$

Για την αποκρυπτογράφηση υπολογίζουμε $s_{o,p} \equiv s_{\frac{p+1}{4} \bmod p-1}^{l+1} \bmod p$. Με CRT τότε ανακτάμε το s_o και με BBS λαμβάνουμε το $(z_1, \ldots, z_l)$, οπότε υπολογίζουμε το $x = (x_1, \ldots, x_l)$.

4 Factoring: Dixon's Sieve

Ιδέα: Πιθανώς να μπορούμε να εκφράσουμε τον αριθμό που ψάχνουμε να παραγοντοποιήσουμε, σαν ένα γινόμενο μερικών πρώτων αριθμών.

Έστω n, αν βρούμε t, s τέτοιο ώστε $t^2 \equiv s^2$, $t \neq \pm s \pmod n$ τότε $gcd(t-s, n) = p(q)$

π.χ. $n = 187 (= 17 \cdot 11)$

$$B = \langle -1, 2, 3, 5, 7 \rangle$$

$$\left(\text{χρήση mod } n \in -\frac{n}{2}, \cdots, \frac{n}{2} \right)$$

$$13^2 \equiv 169 \equiv -18 \leftrightarrow \langle 1, 1, 2, 0, 0 \rangle$$

$$18^2 \equiv 324 \equiv -50 \leftrightarrow \langle 1, 1, 0, 2, 0 \rangle$$

(Τα 2 τελευταία διανύσματα ονομάζονται B vectors)

$$47^2 \equiv (13 \cdot 18)^2 \leftrightarrow \langle 2, 2, 2, 2, 0 \rangle \text{ " = " } \langle 1, 1, 0, 2, 0 \rangle^2 \leftrightarrow O(e^c \sqrt{logn \cdot log(logn)}))$$

Καταλήξαμε δηλαδή σε κάτι το οποίο δεν είναι αποδοτικό αλλά είναι καλύτερο από τις απλές προσεγγίσεις που μπορεί να κάνει κάποιος.