Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Θανάσης Ανδρεου

Διδάσκοντες:
Στάθης Ζαχος
Άρης Παγουρτζης

3 Φεβρουαρίου 2012

Chaum-Van Heisjt-Pfitzman Hash Function

Έστω p, q primes, με $q = \frac{p-1}{2}$ και a, b primitive elements του $\mathbb{Z}_p^*$ με $b = a^k$, k secret.
Έστω μια συνάρτηση $h : \{\mathbb{Z}_q * \mathbb{Z}_q \to \mathbb{Z}_p^* |\ h(x_1, x_2) = a^{x_1} b^{x_2} \underline{\mathrm{mod}} p\}$
Η εύρεση σύγκρουσης για την h ισοδυναμεί με τον υπολογισμό του k.
Απόδειξη:

$\Leftarrow$
Έστω ότι γνωρίζω k: $h(x_1, x_2) = a^{x_1+kx_2} \underline{\mathrm{mod}} p$,
αρκεί να βρεθούν

$$(x_3, x_4) : a^{x_1+kx_2} \equiv a^{x_3+kx_4} \pmod{p} \Rightarrow$$

$$x_3 + kx_4 \equiv x_1 + kx_2 \pmod{p-1}.$$

$\Rightarrow$

$$(x_3, x_4) : a^{x_1+kx_2} \equiv a^{x_3+kx_4} \pmod{p} \Rightarrow$$

$$x_3 + kx_4 \equiv x_1 + kx_2 \pmod{p-1} \Rightarrow$$

$$k(x_2 - x_4) \equiv (x_1 - x_3) \pmod{p-1}$$

Οπότε έχουμε 4 περιπτώσεις(πιθανούς διαιρέτες του $p - 1 = 2q$):
$d = ((x_2 - x_4), (p - 1)) =$

- 1. Τότε υπολογίζουμε k.
- 2. Τότε έχουμε 2 πιθανά k και απλώς δοκιμάζουμε ποιό από αυτά είναι το το k που θέλουμε.
- q. Γνωρίζουμε ότι $0 \leq x_2, x_4 \leq q - 1 \Rightarrow |x_2 - x_4| \leq q - 1 \Rightarrow q \not| (x_2 - x_4)$. (άτοπο)
- $p - 1$. Αυτό μπορεί να ισχύει μόνο στην περίπτωση που $x_2 - x_4 = 0$,που αυτό θα σημαίνει ότ $x_1 = x_3$, οπότε δεν έχουμε σύγκρουση(άτοπο).

Merkle-Damgard Hash Function Extention

given $h : \{0,1\}^m \to \{0,1\}^t$,
construct $h^* : \{0,1\}^* \to \{0,1\}^t$, $m > t+1$

Για είσοδο $x \in \{0,1\}^*$ γράφουμε: $x = x_1x_2...x_k$, $|x_i| = m-t-1, 1 \leq i \leq k-1$, $x_k^{'} = x_k0^d$, x_{k+1} περιέχει πληροφορία για το d. (το $x = x_1x_2...x_k$ και όλοι οι υπόλοιποι παρόμοιοι συμβολισμοί σε αυτό το κεφάλαιο, εννοούν παράθεση και όχι πολλαπλασιασμό)
Οπότε τελικά έχουμε: $x = x_1x_2...x_{k-1}x_k^{'}x_{k+1}$. Έστω g που ορίζεται αναδρομικά ως:

$$g_1 = h(0^{t+1}x_1)$$

$$g_{i+1} = h(g_i1x_{i+1}).$$

Επιλέγουμε ώς $h^*(x) = g_{k+1}$. Η απόδειξη για το οτί η συγκέκριμένη συνάρτηση είναι collision free είναι σχετικά απλή:
Έστω $x^{'} = x_1^{'}, x_2{'}... : h^*(x) = h^*(x^{'}) \Rightarrow g_{k+1} = g_{k+1}^{'} \Rightarrow h(g_i1_xi+1 = h(g_i^{'}1x_{i+1}^{'}))$.
Αυτό σημαίνει ότι άν τα $g_i1_xi+1 = g^{'}1x_{i+1}^{'}$,οπότε έχουμε σύγκρουση στην h (άτοπο), ή συνεχίζουμε επαγωγικά στις $g_i, g_i^{'}$ για να ξανακαταλήξουμε σε άτοπο.

Σχήματα αναγνώρισης ή πιστοποίησης ταυτοποίησης Identification Schemes

Χρησιμοποιούνται σε:

- ATM's
- Server Access
- Credit Cards

Ο στόχος τους είναι η Αλίκή να πιστοποιείται από τον Βασίλη και κανείς άλλος να μη μπορεί να πιστοποιηθεί ως Αλίκη, ουτε και ο Βασίλης.

Γενικά σχήματα από κρυπτοσυστήματα

1. Συμμετρικά:
   Έστω $enc_{KAB} : x \to y$
   Η Α στέλνει αίτηση στον Β.
   Ο Β υπολογίζει $x \xrightarrow{R} x$ και το στέλνει πίσω στην Α. Επίσης υπολογίζει

και το $y = enc_{KAB}(x)$.
Η Α στέλνει στον Β το $y^{'} = enc_{KAB}(x)$.
Ο Β ελέγχει αν $y = y^{'}$.

2. Δημοσίου κλειδου της Αλίκης:
   Έστω p_A το δημόσιο κλειδί και s_A το ιδιωτικό που το έχει μόνο η Α.
   Η Α στέλνει αίτηση στον Β.
   Ο Β υπολογίζει $x \xrightarrow{R} x$ και το $y = enc_{p_A}(x)$ και στέλνει το y στην Α.
   Η Α υπολογίζει το $x^{'} = dec_{s_A}(y)$ και το στέλνει στον Β.
   Ο Β ελέγχει αν $x = x^{'}$.

Όσον αφορά το τελευταίο σχήμα μπορούμε να παρατηρήσουμε ότι άν χρησιμοποιήσουμε το κρυπτοσύστημα Rabin το $x^{'}$ που θα υπολογίσει η Αλίκη μπορεί να μην είναι το ίδιο με το x που μπορεί να έχει ο Βασίλης (αφού η κρυπτογράφηση Rabin είναι ambiguous). Σε αυτή την περίπτωση, ο τελικός έλεγχος που πρέπει να κάνει ο Βασίλης είναι αν $x^{'2} = x^2$.

Βιβλιογραφία

1. [Ζάχος]: Ε. Ζάχος, «Σημειώσεις στη Θεωρία Αριθμων και την Κρυπτογραφία», 2007