Κρυπτογραφία και Πολυπλοκότητα 11/1/13

Κρυπτογραφικές Συναρτήσεις Κατακερματισμού

Ονοματεπώνυμο: Κάβουρας Λουκάς-Παπαδιάς Σεραφείμ

CHAUM-VAN-HEIJST PFITZMAN Hash Function

Κατασκευή: Διαλέγουμε πρώτους p,q τ.ώ. : $q = \frac{p-1}{2}$, g γεννήτορα της Z_p^* και β=$g^k mod p$ όπου k μυστικός εκθέτης. Η h ορίζεται $h : Z_{q^2} \longrightarrow Z_p^*$ με τύπο $h(m) = g^{x_1}\beta^{x_2} mod p$ για $m = x_1 q + x_2$

Πρόταση 1:
Έυρεση σύγκρουσης για την h$\Longleftrightarrow$ με υπολογισμό του μυστικού k

Απόδειξη:

"$\Leftarrow$"Εστω ότι γνωρίζουμε τον k.Το να γνωρίζουμε το m ισοδυναμεί με το να γνωρίζουμε το ζεύγος (x_1, x_2).Θέλουμε να βρουμε $m' \leftrightarrow (x_3, x_4)$ τ.ώ. : $h(m) = h(m') \Longleftrightarrow g^{x_1+kx_2} = g^{x_3+kx_4} mod p \Longleftrightarrow x_1 + kx_2 = x_3 + kx_4 mod(p-1) \Longleftrightarrow x_3 = x_1 + k(x_2 - x_4) mod(p-1)$ Επομένως $\forall x_4$ βρίσκουμε x_3 (p-2 διαφορετικά υπάρχουν).

" $\Rightarrow$" Έστω m , m' δηλαδή x_1, x_2, x_3, x_4 τ.ώ: $h(m) = h(m') \Longleftrightarrow g^{x_1+kx_2} = g^{x_3+kx_4} mod p \Longleftrightarrow x_1 + kx_2 = x_3 + kx_4 mod(p-1) \Longleftrightarrow k(x_2 - x_4) = x_3 - x_1 mod(p-1)$ οπότε εύρεση k ανάγεται στην επίλυση μιας γραμμικής ισοτιμίας.Ο gcd του $(x_2 - x_4, p-1)$ μπορεί να είναι 1 , 2 , q , p-1. Για gcd= 1 , 2 τον βρίσκουμε εύκολα ενώ με q , p-1 καταλήγουμε σε άτοπο αφού $0 \leq x_2, x_4 \leq q-1 \Rightarrow 1-q \leq x_2 - x_4 \leq q-1$

Μέθοδος Merkle-Damgard για επέκταση πεδίου ορισμού μιας hash function

Έστω μια collision free hash function $f : S^{n+r} \longrightarrow S^n$ (συνήθως $S = \{0, 1\}$) Θα κατασκευάσουμε μία νέα συνάρτηση h:: $S^* \longrightarrow S^n$

Έστω x δεδομένα των οποίων θέλουμε να υπολογίσουμε την εικόνα μεσω της h με μήκος |x|=b. Χωρίζουμε την είσοδο x σε t μέρη $x_1, x_2, ..., x_t$ τ.ώ. : $|x_i| = r$ παραθέτοντας στο τελευταίο μέρος όσα "0" bits χρειάζονται(padding). Προσθέτουμε στο τέλος ένα ακόμη κομμάτι x_{t+1} μήκους b και υπολογίζουμε την αναδρομική συνάρτηση:

$H_0 = IV, H_i = f(H_{i-1}||x_i)$ με i=1,...,t+1 και |IV|=n ,όπου || συμβολίζει παράθεση και IV(initial vector) είναι κάποια αρχική καθορισμένη τιμή που είναι πάντα η ίδια για όλους τους υπολογισμούς της h. Η εικόνα του x μέσω της h είναι η $h(x) = H_{t+1}$

Πρόταση 2 :
Αν η f είναι μια συνάρτηση χωρίς συγκρούσεις τότε και η h όπως προκύπτει από τη μέθοδο Merkle-Damgard είναι χωρίς συγκρούσεις.
Ιδέα απόδειξης:
Έστω m , m' τ.ώ.: $h(m) = h(m') \Rightarrow H_{k+1} = H'_{k'+1}$
$\Rightarrow \begin{cases} \text{σύγκρουση για την f,άτοπο} & \text{αν } H_k||x_{k+1} \neq H'_k||x_{k'+1} \\ H_k = H'_k \text{ και } x_{k+1} = x_{k'+1} & \text{αν } H_k||x_{k+1} = H'_k||x_{k+1} \end{cases}$
με επαναληπτική εφαρμογή βρίσκουμε σύγκρουση για την f.