

Κρυπτογραφία

Συναρτήσεις μονής κατεύθυνσης - Συναρτήσεις κατακερματισμού

Άρης Παγουρτζής - Πέτρος Ποτίκας

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Περιεχόμενα

- 1 Συναρτήσεις μονής-κατεύθυνσης
- 2 Συναρτήσεις σύνοψης (hash functions)
- 3 Δένδρα Merkle

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

- ▶ Συνάρτηση που είναι εύκολο να υπολογιστεί, αλλά “δύσκολο” να αντιστραφεί

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

- ▶ Συνάρτηση που είναι εύκολο να υπολογιστεί, αλλά “δύσκολο” να αντιστραφεί
- ▶ Απαραίτητη προϋπόθεση για κρυπτογραφία ιδιωτικού κλειδιού

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

- ▶ Συνάρτηση που είναι εύκολο να υπολογιστεί, αλλά “δύσκολο” να αντιστραφεί
- ▶ Απαραίτητη προϋπόθεση για κρυπτογραφία ιδιωτικού κλειδιού
- ▶ Γεννήτριες ψευδοτυχαιότητας βασίζονται στην υπόθεση ύπαρξης συναρτήσεων μονής-κατεύθυνσης

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

- ▶ Συνάρτηση που είναι εύκολο να υπολογιστεί, αλλά “δύσκολο” να αντιστραφεί
- ▶ Απαραίτητη προϋπόθεση για κρυπτογραφία ιδιωτικού κλειδιού
- ▶ Γεννήτριες ψευδοτυχειότητας βασίζονται στην υπόθεση ύπαρξης συναρτήσεων μονής-κατεύθυνσης
- ▶ Με αμελητέα πιθανότητα μπορώ να αντιστρέψω μια συνάρτηση f

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

- ▶ Συνάρτηση που είναι εύκολο να υπολογιστεί, αλλά “δύσκολο” να αντιστραφεί
- ▶ Απαραίτητη προϋπόθεση για κρυπτογραφία ιδιωτικού κλειδιού
- ▶ Γεννήτριες ψευδοτυχαιότητας βασίζονται στην υπόθεση ύπαρξης συναρτήσεων μονής-κατεύθυνσης
- ▶ Με αμελητέα πιθανότητα μπορώ να αντιστρέψω μια συνάρτηση f
- ▶ Με εξαντλητική αναζήτηση (εκθετικό χρόνο) μπορώ να αντιστρέψω μια συνάρτηση f

Συναρτήσεις μονής-κατεύθυνσης

Έστω συνάρτηση $f: \{0, 1\}^* \mapsto \{0, 1\}^*$.

Συναρτήσεις μονής-κατεύθυνσης

Έστω συνάρτηση $f: \{0, 1\}^* \mapsto \{0, 1\}^*$.

Ορίζουμε για κάθε αλγόριθμο \mathcal{A} και κάθε παράμετρο ασφαλείας n το

Πείραμα αντιστρεψιμότητας $Invert_{\mathcal{A},f}(n)$

1. Διάλεξε $x \leftarrow \{0, 1\}^n$. Υπολόγισε $y = f(x)$
2. Ο \mathcal{A} με είσοδο το 1^n και το y επιστρέφει το x'
3. Η έξοδος είναι 1, αν $f(x') = y$, αλλιώς 0

Συναρτήσεις μονής-κατεύθυνσης

Έστω συνάρτηση $f: \{0, 1\}^* \mapsto \{0, 1\}^*$.

Ορίζουμε για κάθε αλγόριθμο \mathcal{A} και κάθε παράμετρο ασφαλείας n το

Πείραμα αντιστρεψιμότητας $Invert_{\mathcal{A},f}(n)$

1. Διάλεξε $x \leftarrow \{0, 1\}^n$. Υπολόγισε $y = f(x)$
2. Ο \mathcal{A} με είσοδο το 1^n και το y επιστρέφει το x'
3. Η έξοδος είναι 1, αν $f(x') = y$, αλλιώς 0

Παρατήρηση: Δε χρειάζεται να βρούμε το ίδιο το x , αλλά οποιαδήποτε x' , τ.ώ. $f(x') = y = f(x)$.

Συναρτήσεις μονής-κατεύθυνσης

Ορισμός

Μία συνάρτηση $f: \{0, 1\}^* \mapsto \{0, 1\}^*$ είναι *συνάρτηση μονής-κατεύθυνσης* αν είναι:

1. (Εύκολα υπολογίσιμη) Υπάρχει πολυωνυμικού χρόνου αλγόριθμος M που την υπολογίζει, δηλ. $M_f(x) = f(x), \forall x$
2. (Δύσκολα αντιστρέψιμη) Για κάθε PPT αλγόριθμο \mathcal{A} υπάρχει αμελητέα συνάρτηση ϵ έτσι ώστε:

$$\Pr[\text{Invert}_{\mathcal{A},f}(n) = 1] \leq \epsilon(n)$$

Συναρτήσεις μονής-κατεύθυνσης

Ορισμός

Μία συνάρτηση $f: \{0, 1\}^* \mapsto \{0, 1\}^*$ είναι *συνάρτηση μονής-κατεύθυνσης* αν είναι:

1. (Εύκολα υπολογίσιμη) Υπάρχει πολυωνυμικού χρόνου αλγόριθμος M που την υπολογίζει, δηλ. $M_f(x) = f(x), \forall x$
2. (Δύσκολα αντιστρέψιμη) Για κάθε PPT αλγόριθμο \mathcal{A} υπάρχει αμελητέα συνάρτηση ϵ έτσι ώστε:

$$\Pr[\text{Invert}_{\mathcal{A},f}(n) = 1] \leq \epsilon(n)$$

Πιο αναλυτικά,

$$\Pr_{x \leftarrow \{0,1\}^n} [\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \leq \epsilon(n)$$

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

Παρατηρήσεις:

1. Μια συνάρτηση που δεν είναι μονής-κατεύθυνσης δεν είναι απαραίτητο να αντιστρέφεται εύκολα πάντα (ή “συχνά”).

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

Παρατηρήσεις:

1. Μια συνάρτηση που δεν είναι μονής-κατεύθυνσης δεν είναι απαραίτητο να αντιστρέφεται εύκολα πάντα (ή “συχνά”).
Π.χ. αν υπάρχει αντίπαλος που αντιστρέφει μια συνάρτηση με πιθανότητα n^{-10} για όλους άρτιους n (αλλά αποτυγχάνει για τους μονούς), τότε δεν είναι μονής-κατεύθυνσης.

Συναρτήσεις μονής-κατεύθυνσης (one-way functions)

Παρατηρήσεις:

1. Μια συνάρτηση που δεν είναι μονής-κατεύθυνσης δεν είναι απαραίτητο να αντιστρέφεται εύκολα πάντα (ή “συχνά”).
Π.χ. αν υπάρχει αντίπαλος που αντιστρέφει μια συνάρτηση με πιθανότητα n^{-10} για όλους άρτιους n (αλλά αποτυγχάνει για τους μονούς), τότε δεν είναι μονής-κατεύθυνσης.
2. Αν έχουμε εκθετικό χρόνο, τότε αν μας δίνεται ένα y και η παράμετρος ασφαλείας 1^n , τότε μπορούμε να δοκιμάσουμε όλα τα $x \in \{0, 1\}^n$, μέχρι να βρούμε ένα x , τέτοιο ώστε $f(x) = y$.

Μεταθέσεις μονής-κατεύθυνσης

Μια συνάρτηση λέμε ότι *διατηρεί το μήκος* αν $|f(x)| = |x|, \forall x$.

Μεταθέσεις μονής-κατεύθυνσης

Μια συνάρτηση λέμε ότι *διατηρεί το μήκος* αν $|f(x)| = |x|, \forall x$.

Ορισμός

Μια συνάρτηση μονής-κατεύθυνσης που διατηρεί το μήκος και είναι 1-1, είναι μια *μετάθεση μονής-κατεύθυνσης*.

Η τιμή y καθορίζει μοναδικά το x από το οποίο προήλθε. Παρόλα αυτά είναι δύσκολο να βρούμε το x σε πολυωνυμικό χρόνο.

Υποψήφιες συναρτήσεις μονής-κατεύθυνσης

- ▶ Υπάρχουν συναρτήσεις μονής-κατεύθυνσης με την προϋπόθεση πως κάποια προβλήματα είναι δύσκολα, π.χ. παραγοντοποίηση ακεραίων σε πρώτους αριθμούς κ.λπ.

Υποψήφιες συναρτήσεις μονής-κατεύθυνσης

- ▶ Υπάρχουν συναρτήσεις μονής-κατεύθυνσης με την προϋπόθεση πως κάποια προβλήματα είναι δύσκολα, π.χ. παραγοντοποίηση ακεραίων σε πρώτους αριθμούς κ.λπ.

Παράδειγμα 1:

$f_{mult}(x, y) = xy$, με μεγάλη πιθανότητα, το αποτέλεσμα άρτιος, οπότε $(2, xy/2)$ είναι ο αντίστροφος.

Υποψήφιες συναρτήσεις μονής-κατεύθυνσης

- ▶ Υπάρχουν συναρτήσεις μονής-κατεύθυνσης με την προϋπόθεση πως κάποια προβλήματα είναι δύσκολα, π.χ. παραγοντοποίηση ακεραίων σε πρώτους αριθμούς κ.λπ.

Παράδειγμα 1:

$f_{mult}(x, y) = xy$, με μεγάλη πιθανότητα, το αποτέλεσμα άρτιος, οπότε $(2, xy/2)$ είναι ο αντίστροφος. Με περιορισμό, είναι μονής-κατεύθυνσης:

Υποψήφιες συναρτήσεις μονής-κατεύθυνσης

- ▶ Υπάρχουν συναρτήσεις μονής-κατεύθυνσης με την προϋπόθεση πως κάποια προβλήματα είναι δύσκολα, π.χ. παραγοντοποίηση ακεραίων σε πρώτους αριθμούς κ.λπ.

Παράδειγμα 1:

$f_{mult}(x, y) = xy$, με μεγάλη πιθανότητα, το αποτέλεσμα άρτιος, οπότε $(2, xy/2)$ είναι ο αντίστροφος. Με περιορισμό, είναι μονής-κατεύθυνσης:

1. $f_{mult}(x, y) = (xy, |x|, |y|)$, (εναλλακτικά, x, y έχουν ίδιο μήκος)

Υποψήφιες συναρτήσεις μονής-κατεύθυνσης

- ▶ Υπάρχουν συναρτήσεις μονής-κατεύθυνσης με την προϋπόθεση πως κάποια προβλήματα είναι δύσκολα, π.χ. παραγοντοποίηση ακεραίων σε πρώτους αριθμούς κ.λπ.

Παράδειγμα 1:

$f_{mult}(x, y) = xy$, με μεγάλη πιθανότητα, το αποτέλεσμα άρτιος, οπότε $(2, xy/2)$ είναι ο αντίστροφος. Με περιορισμό, είναι μονής-κατεύθυνσης:

1. $f_{mult}(x, y) = (xy, |x|, |y|)$, (εναλλακτικά, x, y έχουν ίδιο μήκος)
2. x, y πρώτοι αριθμοί ίσου μήκους

Υποψήφιες μεταθέσεις μονής-κατεύθυνσης

Παράδειγμα 2: Η συνάρτηση $f(x_1, \dots, x_n, J) = (x_1, \dots, x_n, \sum_{j \in J} x_j)$, όπου κάθε x_i είναι ένα ακέραιος και $J \subseteq \{1, 2, \dots, n\}$. Εύρεση αντιστρόφου είναι το γνωστό \mathcal{NP} -πλήρες πρόβλημα Subset Sum.

Υποψήφιες μεταθέσεις μονής-κατεύθυνσης

Παράδειγμα 3: Έστω Gen συνάρτηση που με είσοδο το 1^n επιστρέφει έναν πρώτο αριθμό p μήκους n -bits μαζί με ένα ξεχωριστό στοιχείο $g \in \{2, \dots, p - 1\}$. Έστω $Samp$ αλγόριθμος που επιστρέφει ένα στοιχείο $x \in \{1, \dots, p - 1\}$.

Υποψήφιες μεταθέσεις μονής-κατεύθυνσης

Παράδειγμα 3: Έστω *Gen* συνάρτηση που με είσοδο το 1^n επιστρέφει έναν πρώτο αριθμό p μήκους n -bits μαζί με ένα ξεχωριστό στοιχείο $g \in \{2, \dots, p-1\}$. Έστω *Samp* αλγόριθμος που επιστρέφει ένα στοιχείο $x \in \{1, \dots, p-1\}$. Ορίζουμε

$$f_{p,g}(x) = g^x \bmod p$$

Υποψήφιες μεταθέσεις μονής-κατεύθυνσης

Παράδειγμα 3: Έστω Gen συνάρτηση που με είσοδο το 1^n επιστρέφει έναν πρώτο αριθμό p μήκους n -bits μαζί με ένα ξεχωριστό στοιχείο $g \in \{2, \dots, p-1\}$. Έστω $Samp$ αλγόριθμος που επιστρέφει ένα στοιχείο $x \in \{1, \dots, p-1\}$. Ορίζουμε

$$f_{p,g}(x) = g^x \bmod p$$

- ▶ Η συνάρτηση αυτή διατηρεί το μήκος και είναι 1-1, άρα μετάθεση.
- ▶ Η δυσκολία αντιστροφής της βασίζεται στη δυσκολία του προβλήματος διακριτού λογάριθμου.

Υποψήφιες μεταθέσεις μονής-κατεύθυνσης

Παράδειγμα 3: Έστω *Gen* συνάρτηση που με είσοδο το 1^n επιστρέφει έναν πρώτο αριθμό p μήκους n -bits μαζί με ένα ξεχωριστό στοιχείο $g \in \{2, \dots, p-1\}$. Έστω *Samp* αλγόριθμος που επιστρέφει ένα στοιχείο $x \in \{1, \dots, p-1\}$. Ορίζουμε

$$f_{p,g}(x) = g^x \bmod p$$

- ▶ Η συνάρτηση αυτή διατηρεί το μήκος και είναι 1-1, άρα μετάθεση.
- ▶ Η δυσκολία αντιστροφής της βασίζεται στη δυσκολία του προβλήματος διακριτού λογάριθμου.

Τα SHA-1 ή AES δίνουν συναρτήσεις μονής-κατεύθυνσης, με την υπόθεση ότι είναι ελεύθερες συγκρούσεων ή ψευδοτυχαίες μεταθέσεις.

Hard-core predicates

- ▶ Κατηγορημα μιας συνάρτησης που δείχνει τη δυσκολία αντιστροφής μιας συνάρτησης
- ▶ f μονής-κατεύθυνσης, μπορεί όμως να αποκαλύψει μέρος του x , π.χ. έστω f μονής-κατεύθυνσης, τότε η $g(x_1, x_2) = (x_1, f(x_2))$, με $|x_1| = |x_2|$ είναι μονής-κατεύθυνσης

Hard-core predicates

Ορισμός

Μια συνάρτηση $hc : \{0, 1\}^* \mapsto \{0, 1\}$ είναι *hard-core predicate* μιας συνάρτησης f αν: (1) μπορεί να υπολογιστεί σε πολυωνυμικό χρόνο και (2) για κάθε PPT \mathcal{A} υπάρχει μια αμελητέα συνάρτηση ϵ ώστε

$$\Pr[\mathcal{A}(f(x)) = hc(x)] \leq \frac{1}{2} + \epsilon(n)$$

Hard-core predicates

Παράδειγμα: $hc(x) = \bigoplus_i^n x_i$.

Hard-core predicates

Παράδειγμα: $hc(x) = \bigoplus_i^n x_i$. Είναι hard-core οποιασδήποτε συνάρτησης μονής-κατεύθυνσης;

Hard-core predicates

Παράδειγμα: $hc(x) = \bigoplus_i^n x_i$. Είναι hard-core οποιασδήποτε συνάρτησης μονής-κατεύθυνσης;

Δεν είναι hard-core predicate!

Hard-core predicates

Παράδειγμα: $hc(x) = \bigoplus_i^n x_i$. Είναι hard-core οποιασδήποτε συνάρτησης μονής-κατεύθυνσης;

Δεν είναι hard-core predicate!

Αν πάρω $f(x) = (g(x), \bigoplus_i^n x_i)$, όπου $g(x)$ μια συνάρτηση μονής-κατεύθυνσης.

Hard-core predicates

Παράδειγμα: $hc(x) = \bigoplus_i^n x_i$. Είναι hard-core οποιασδήποτε συνάρτησης μονής-κατεύθυνσης;

Δεν είναι hard-core predicate!

Αν πάρω $f(x) = (g(x), \bigoplus_i^n x_i)$, όπου $g(x)$ μια συνάρτηση μονής-κατεύθυνσης.

- ▶ Γενικότερα: Για σταθερό κατηγορημα hc , υπάρχει συνάρτηση f για την οποία το hc δεν είναι hard-core κατηγορημα.

Γεννήτρια Ψευδοτυχαιότητας από Μετάθεση Μονής-κατεύθυνσης

Για κάθε συνάρτηση μονής-κατεύθυνσης υπάρχει ένα hard-core predicate.

Γεννήτρια Ψευδοτυχαιότητας από Μετάθεση Μονής-κατεύθυνσης

Για κάθε συνάρτηση μονής-κατεύθυνσης υπάρχει ένα hard-core predicate.

Ανοικτό πρόβλημα.

Γεννήτρια Ψευδοτυχαιότητας από Μετάθεση Μονής-κατεύθυνσης

Για κάθε συνάρτηση μονής-κατεύθυνσης υπάρχει ένα hard-core predicate.

Ανοικτό πρόβλημα.

Από δοσμένη συνάρτηση μονής-κατεύθυνσης f θα φτιάξουμε μια “άλλη” συνάρτηση μονής-κατεύθυνσης g με ένα hard-core predicate για αυτήν.

Θεώρημα

Έστω ότι υπάρχουν συναρτήσεις μονής-κατεύθυνσης. Τότε υπάρχει μια συνάρτηση μονής-κατεύθυνσης g και ένα hard-core predicate hc της g .

Έστω f μια συνάρτηση μονής-κατεύθυνσης. Τότε οι συναρτήσεις g και hc κατασκευάζονται ως εξής:

Γεννήτρια Ψευδοτυχαιότητας από Μετάθεση Μονής-κατεύθυνσης

Για κάθε συνάρτηση μονής-κατεύθυνσης υπάρχει ένα hard-core predicate.

Ανοικτό πρόβλημα.

Από δοσμένη συνάρτηση μονής-κατεύθυνσης f θα φτιάξουμε μια “άλλη” συνάρτηση μονής-κατεύθυνσης g με ένα hard-core predicate για αυτήν.

Θεώρημα

Εστω ότι υπάρχουν συναρτήσεις μονής-κατεύθυνσης. Τότε υπάρχει μια συνάρτηση μονής-κατεύθυνσης g και ένα hard-core predicate hc της g .

Εστω f μια συνάρτηση μονής-κατεύθυνσης. Τότε οι συναρτήσεις g και hc κατασκευάζονται ως εξής: $g(x, r) = (f(x), r)$, $|x| = |r|$

$$hc(x, r) = \bigoplus_{i=1}^n x_i r_i$$

Γεννήτρια Ψευδοτυχαιότητας από Μετάθεση Μονής-κατεύθυνσης

Για κάθε συνάρτηση μονής-κατεύθυνσης υπάρχει ένα hard-core predicate.

Ανοικτό πρόβλημα.

Από δοσμένη συνάρτηση μονής-κατεύθυνσης f θα φτιάξουμε μια “άλλη” συνάρτηση μονής-κατεύθυνσης g με ένα hard-core predicate για αυτήν.

Θεώρημα

Εστω ότι υπάρχουν συναρτήσεις μονής-κατεύθυνσης. Τότε υπάρχει μια συνάρτηση μονής-κατεύθυνσης g και ένα hard-core predicate hc της g .

Εστω f μια συνάρτηση μονής-κατεύθυνσης. Τότε οι συναρτήσεις g και hc κατασκευάζονται ως εξής: $g(x, r) = (f(x), r)$, $|x| = |r|$

$$hc(x, r) = \bigoplus_{i=1}^n x_i r_i$$

αν r ομοιόμορφα τυχαίο, τότε παίρνω XOR τυχαίων bits του x .

Γεννήτρια Ψευδοτυχειότητας από Μετάθεση Μονής-κατεύθυνσης

- ▶ Το θεώρημα λέει: αν η f είναι συνάρτηση μονής-κατεύθυνσης, τότε η $hc(x, r)$ κρύβει το XOR τυχαίων bits του x .
- ▶ Αν f μετάθεση, τότε και g μετάθεση.

Γεννήτρια Ψευδοτυχαιότητας από Μετάθεση Μονής-Κατεύθυνσης

Θεώρημα

Έστω f μια μετάθεση μονής-κατεύθυνσης και hc το *hard-core predicate* της f . Τότε η $G(s) = f(s) || hc(s)$ είναι μια γεννήτρια ψευδοτυχαιότητας.

Γεννήτρια ψευδοτυχαιότητας \Rightarrow Κρυπτογραφία ιδιωτικού κλειδιού

Συναρτήσεις σύνοψης (hash functions)

- ▶ Γνωστές και ως **συναρτήσεις κατακερματισμού**.
- ▶ Σημαντικές ιδιότητες:
 - ▶ **Συμπίεση** $h : X \rightarrow Y, |Y| < |X|$.
Συνήθως $X = \Sigma^*$, $Y = \Sigma^n$, δηλαδή η $h(x)$ έχει συγκεκριμένο μήκος για οποιαδήποτε είσοδο x .
 - ▶ **Ευκολία Υπολογισμού** Ο υπολογισμός της τιμής $h(x)$ για κάποιο x γίνεται “εύκολα”. Δηλαδή υπάρχει αλγόριθμος A πολυωνυμικού χρόνου, έτσι ώστε για κάθε x να ισχύει $h(x) = A(x)$.
 - ▶ Μια συνάρτηση σύνοψης ορίζει σχέση ισοδυναμίας:

$$x \sim x' : h(x) = h(x')$$

Δύο στοιχεία στην ίδια κλάση ισοδυναμίας λέμε ότι προκαλούν **σύγκρουση (collision)**.

Συναρτήσεις σύννοψης (hash functions): επιθυμητές ιδιότητες

Έστω hash function $h : X \rightarrow Y$. Η h έχει:

1. Αντίσταση πρώτου ορίσματος (preimage resistance), αν για $y \in Y$ είναι υπολογιστικά δύσκολο να βρεθεί $x \in X$ τ.ώ. $h(x) = y$.
2. Αντίσταση δεύτερου ορίσματος (2nd preimage resistance), αν για $x \in X$ είναι υπολογιστικά δύσκολο να βρεθεί $x' \in X$ τ.ώ. $x \neq x'$ και $h(x) = h(x')$.
3. Δυσκολία εύρεσης συγκρούσεων (collision resistance / freeness), αν είναι υπολογιστικά δύσκολο να βρεθούν $x, x' \in X$ έτσι ώστε $h(x) = h(x')$.

Άλλα ονόματα: για το (2) weak collision freeness, για το (1) non-invertibility.

Σειρά ισχύος: (3) \Rightarrow (2) \Rightarrow (1) (υπό προϋποθέσεις).

One-way hash functions (OWHFs): (1) & (2).

Collision-resistant hash functions (CRHFs): (1) & (2) & (3).

Συναρτήσεις σύνοψης (hash functions): παραδείγματα

1. $f(x) = (x^2 - c) \bmod p$: δεν είναι μονής κατεύθυνσης αφού η εύρεση τετραγωνικών ριζών στο \mathbb{Z}_p είναι δυνατή σε πολυωνυμικό χρόνο.
2. $g(x) = x^2 \bmod n$, $n = pq$, p, q κρυφοί: αντίσταση πρώτου ορίσματος, αλλά όχι αντίσταση δεύτερου ορίσματος (γιατί;), επομένως δεν είναι CRHF.
3. $h : \mathbb{Z}_q^2 \rightarrow \mathbb{Z}_p^*$, $h(x_1, x_2) = \alpha^{x_1} \beta^{x_2} \bmod p$, p, q πρώτοι, $p = 2q + 1$, α, β γεννήτορες του \mathbb{Z}_p^* .
Είναι γνωστή ως συνάρτηση σύνοψης **Chaum-van Heijst-Pfitzman** και είναι CRHF αν ισχύει η Υπόθεση Διακριτού Λογαρίθμου στη \mathbb{Z}_p^* .

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

Θεώρημα

Έστω συνάρτηση σύνοψης $h : X \rightarrow Y$ και η $h(x) \in Y$ ακολουθεί ομοιόμορφη κατανομή πιθανότητας όταν η $x \in X$ ακολουθεί ομοιόμορφη κατανομή. Η πιθανότητα να βρεθεί σύγκρουση μετά από τυχαία επιλογή x_1, x_2, \dots, x_k είναι περίπου $\frac{1}{2}$ όταν $k \cong 1.17\sqrt{n}$, όπου $n = |Y|$.

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

Θεώρημα

Έστω συνάρτηση σύνοψης $h : X \rightarrow Y$ και η $h(x) \in Y$ ακολουθεί ομοιόμορφη κατανομή πιθανότητας όταν η $x \in X$ ακολουθεί ομοιόμορφη κατανομή. Η πιθανότητα να βρεθεί σύγκρουση μετά από τυχαία επιλογή x_1, x_2, \dots, x_k είναι περίπου $\frac{1}{2}$ όταν $k \cong 1.17\sqrt{n}$, όπου $n = |Y|$.

Απόδειξη

$NoColl_i$: δεν έχουμε σύγκρουση στα $\{y_1, y_2, \dots, y_i\}$

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

Θεώρημα

Έστω συνάρτηση σύνοψης $h : X \rightarrow Y$ και η $h(x) \in Y$ ακολουθεί ομοιόμορφη κατανομή πιθανότητας όταν η $x \in X$ ακολουθεί ομοιόμορφη κατανομή. Η πιθανότητα να βρεθεί σύγκρουση μετά από τυχαία επιλογή x_1, x_2, \dots, x_k είναι περίπου $\frac{1}{2}$ όταν $k \cong 1.17\sqrt{n}$, όπου $n = |Y|$.

Απόδειξη

$NoColl_i$: δεν έχουμε σύγκρουση στα $\{y_1, y_2, \dots, y_i\}$
Έχουμε $NoColl_k$ αν $NoColl_i$ για όλα τα $i \leq k$, δηλαδή

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

Θεώρημα

Έστω συνάρτηση σύνοψης $h : X \rightarrow Y$ και η $h(x) \in Y$ ακολουθεί ομοιόμορφη κατανομή πιθανότητας όταν η $x \in X$ ακολουθεί ομοιόμορφη κατανομή. Η πιθανότητα να βρεθεί σύγκρουση μετά από τυχαία επιλογή x_1, x_2, \dots, x_k είναι περίπου $\frac{1}{2}$ όταν $k \cong 1.17\sqrt{n}$, όπου $n = |Y|$.

Απόδειξη

$NoColl_i$: δεν έχουμε σύγκρουση στα $\{y_1, y_2, \dots, y_i\}$

Έχουμε $NoColl_k$ αν $NoColl_i$ για όλα τα $i \leq k$, δηλαδή

$$Pr[NoColl_k] = Pr[NoColl_1]Pr[NoColl_2|NoColl_1] \cdots Pr[NoColl_k|NoColl_{k-1}]$$

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

Θεώρημα

Έστω συνάρτηση σύνοψης $h : X \rightarrow Y$ και η $h(x) \in Y$ ακολουθεί ομοιόμορφη κατανομή πιθανότητας όταν η $x \in X$ ακολουθεί ομοιόμορφη κατανομή. Η πιθανότητα να βρεθεί σύγκρουση μετά από τυχαία επιλογή x_1, x_2, \dots, x_k είναι περίπου $\frac{1}{2}$ όταν $k \cong 1.17\sqrt{n}$, όπου $n = |Y|$.

Απόδειξη

$NoColl_i$: δεν έχουμε σύγκρουση στα $\{y_1, y_2, \dots, y_i\}$

Έχουμε $NoColl_k$ αν $NoColl_i$ για όλα τα $i \leq k$, δηλαδή

$$Pr[NoColl_k] = Pr[NoColl_1]Pr[NoColl_2|NoColl_1] \cdots Pr[NoColl_k|NoColl_{k-1}]$$

- ▶ $Pr[NoColl_1] = 1$
- ▶ Αν συμβαίνει το $NoColl_i$, τότε η πιθανότητα να συγκρουστεί το y_{i+1} με τα προηγούμενα είναι $\frac{i}{n}$

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$\Pr[\text{NoColl}_k] = \frac{n(n-1)\dots(n-k+1)}{n^k} = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$$

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$Pr[NoColl_k] = \frac{n(n-1)\dots(n-k+1)}{n^k} = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$$

Ισχύει $\forall x \in \mathbb{R}, 1 + x \leq e^x$, οπότε:

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$Pr[NoColl_k] = \frac{n(n-1)\dots(n-k+1)}{n^k} = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$$

Ισχύει $\forall x \in \mathbb{R}, 1 + x \leq e^x$, οπότε:

$$\prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right) \leq \prod_{i=1}^{k-1} e^{-\frac{i}{n}} = e^{-\frac{\sum_{i=1}^{k-1} i}{n}} = e^{-\frac{k(k-1)}{2n}} \Rightarrow$$

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$Pr[NoColl_k] = \frac{n(n-1)\dots(n-k+1)}{n^k} = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$$

Ισχύει $\forall x \in \mathbb{R}, 1 + x \leq e^x$, οπότε:

$$\prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right) \leq \prod_{i=1}^{k-1} e^{-\frac{i}{n}} = e^{-\frac{\sum_{i=1}^{k-1} i}{n}} = e^{-\frac{k(k-1)}{2n}} \Rightarrow$$

$$Pr[Coll_k] \geq 1 - e^{-\frac{k(k-1)}{2n}}$$



Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$\Pr[\text{Coll}_k] \geq 1 - e^{-\frac{k(k-1)}{2n}}$$

Για να είναι επομένως η πιθανότητα σύγκρουσης τουλάχιστον p αρκεί:

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$\Pr[\text{Coll}_k] \geq 1 - e^{-\frac{k(k-1)}{2n}}$$

Για να είναι επομένως η πιθανότητα σύγκρουσης τουλάχιστον p αρκεί:

$$1 - e^{-\frac{k(k-1)}{2n}} \geq p \Rightarrow \ln(1 - p) \geq -\frac{k(k-1)}{2n} \Rightarrow k^2 - k - 2n \ln \frac{1}{1-p} \geq 0$$

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$\Pr[\text{Coll}_k] \geq 1 - e^{-\frac{k(k-1)}{2n}}$$

Για να είναι επομένως η πιθανότητα σύγκρουσης τουλάχιστον p αρκεί:

$$1 - e^{-\frac{k(k-1)}{2n}} \geq p \Rightarrow \ln(1 - p) \geq -\frac{k(k-1)}{2n} \Rightarrow k^2 - k - 2n \ln \frac{1}{1-p} \geq 0$$

Λύνοντας ως προς k : $k \geq 1 + \sqrt{2n \ln \frac{1}{1-p}}$

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$\Pr[\text{Coll}_k] \geq 1 - e^{-\frac{k(k-1)}{2n}}$$

Για να είναι επομένως η πιθανότητα σύγκρουσης τουλάχιστον p αρκεί:

$$1 - e^{-\frac{k(k-1)}{2n}} \geq p \Rightarrow \ln(1 - p) \geq -\frac{k(k-1)}{2n} \Rightarrow k^2 - k - 2n \ln \frac{1}{1-p} \geq 0$$

Λύνοντας ως προς k : $k \geq 1 + \sqrt{2n \ln \frac{1}{1-p}}$

Για $p = \frac{1}{2}$ προκύπτει $k \geq 1.17\sqrt{n} + 1$. Για $n = 365$, $k \geq 23$. □

Επίθεση τετραγωνικής ρίζας (Παράδοξο Γενεθλίων)

απόδειξη – συν.

$$\Pr[\text{Coll}_k] \geq 1 - e^{-\frac{k(k-1)}{2n}}$$

Για να είναι επομένως η πιθανότητα σύγκρουσης τουλάχιστον p αρκεί:

$$1 - e^{-\frac{k(k-1)}{2n}} \geq p \Rightarrow \ln(1 - p) \geq -\frac{k(k-1)}{2n} \Rightarrow k^2 - k - 2n \ln \frac{1}{1-p} \geq 0$$

Λύνοντας ως προς k : $k \geq 1 + \sqrt{2n \ln \frac{1}{1-p}}$

Για $p = \frac{1}{2}$ προκύπτει $k \geq 1.17\sqrt{n} + 1$. Για $n = 365$, $k \geq 23$. □

Σημαντική εφαρμογή (μεταξύ άλλων): **μέθοδος παραγοντοποίησης ρ**

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Συμπέρασμα, αν $h : \{0, 1\}^* \mapsto \{0, 1\}^l$, τότε αν πάρω $k = \mathcal{O}(2^{l/2})$ τυχαία στοιχεία από το $\{0, 1\}^*$, η πιθανότητα να έχω σύγκρουση είναι $1/2$

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Συμπέρασμα, αν $h : \{0, 1\}^* \mapsto \{0, 1\}^l$, τότε αν πάρω $k = \mathcal{O}(2^{l/2})$ τυχαία στοιχεία από το $\{0, 1\}^*$, η πιθανότητα να έχω σύγκρουση είναι $1/2$
- ▶ Ως προς ασυμπτωτική πολυπλοκότητα, $2^l, 2^{l/2}$ το ίδιο, όχι όμως στην πράξη

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Συμπέρασμα, αν $h : \{0, 1\}^* \mapsto \{0, 1\}^l$, τότε αν πάρω $k = \mathcal{O}(2^{l/2})$ τυχαία στοιχεία από το $\{0, 1\}^*$, η πιθανότητα να έχω σύγκρουση είναι $1/2$
- ▶ Ως προς ασυμπτωτική πολυπλοκότητα, $2^l, 2^{l/2}$ το ίδιο, όχι όμως στην πράξη
- ▶ Η προσέγγιση αυτή έχει δύο αδυναμίες:
 1. μεγάλος χώρος

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Συμπέρασμα, αν $h : \{0, 1\}^* \mapsto \{0, 1\}^l$, τότε αν πάρω $k = \mathcal{O}(2^{l/2})$ τυχαία στοιχεία από το $\{0, 1\}^*$, η πιθανότητα να έχω σύγκρουση είναι $1/2$
- ▶ Ως προς ασυμπτωτική πολυπλοκότητα, $2^l, 2^{l/2}$ το ίδιο, όχι όμως στην πράξη
- ▶ Η προσέγγιση αυτή έχει δύο αδυναμίες:
 1. μεγάλος χώρος
 2. τυχαία επιλογή τιμών εισόδου

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Επιλογή των μηνυμάτων:

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Επιλογή των μηνυμάτων: Οι τιμές που δίνουμε για να πετύχουμε σύγκρουση, μπορούν να έχουν σχέση μεταξύ τους π.χ. η Alice απολύεται και θέλει να βρει δύο μηνύματα x και x' έτσι ώστε $H(x) = H(x')$, όπου το πρώτο λέει τους λόγους της απόλυσής της, ενώ το δεύτερο κολακευτικά λόγια

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Επιλογή των μηνυμάτων: Οι τιμές που δίνουμε για να πετύχουμε σύγκρουση, μπορούν να έχουν σχέση μεταξύ τους π.χ. η Alice απολύεται και θέλει να βρει δύο μηνύματα x και x' έτσι ώστε $H(x) = H(x')$, όπου το πρώτο λέει τους λόγους της απόλυσής της, ενώ το δεύτερο κολακευτικά λόγια
- ▶ Φτιάχνουμε $k = \Theta(2^{l/2})$ μηνύματα από τον πρώτο τύπο και άλλα τόσα από το δεύτερο τύπο και ψάχνουμε σύγκρουση μεταξύ αυτών των δύο τύπων μηνυμάτων.

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Επιλογή των μηνυμάτων: Οι τιμές που δίνουμε για να πετύχουμε σύγκρουση, μπορούν να έχουν σχέση μεταξύ τους π.χ. η Alice απολύεται και θέλει να βρει δύο μηνύματα x και x' έτσι ώστε $H(x) = H(x')$, όπου το πρώτο λέει τους λόγους της απόλυσής της, ενώ το δεύτερο κολακευτικά λόγια
- ▶ Φτιάχνουμε $k = \Theta(2^{l/2})$ μηνύματα από τον πρώτο τύπο και άλλα τόσα από το δεύτερο τύπο και ψάχνουμε σύγκρουση μεταξύ αυτών των δύο τύπων μηνυμάτων.
“Είναι δύσκολο/ανέφικτο να βρεις μια τόσο καλή/εργατική/φιλότιμη υπάλληλο σαν την Alice. Η δουλειά της είναι καταπληκτική/ανεπανάληπτη/ασύγκριτη.”

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Επιλογή των μηνυμάτων: Οι τιμές που δίνουμε για να πετύχουμε σύγκρουση, μπορούν να έχουν σχέση μεταξύ τους π.χ. η Alice απολύεται και θέλει να βρει δύο μηνύματα x και x' έτσι ώστε $H(x) = H(x')$, όπου το πρώτο λέει τους λόγους της απόλυσής της, ενώ το δεύτερο κολακευτικά λόγια
- ▶ Φτιάχνουμε $k = \Theta(2^{l/2})$ μηνύματα από τον πρώτο τύπο και άλλα τόσα από το δεύτερο τύπο και ψάχνουμε σύγκρουση μεταξύ αυτών των δύο τύπων μηνυμάτων.
“Είναι δύσκολο/ανέφικτο να βρεις μια τόσο καλή/εργατική/φιλότιμη υπάλληλο σαν την Alice. Η δουλειά της είναι καταπληκτική/ανεπανάληπτη/ασύγκριτη.”
- ▶ Ετοιμάζουμε k γράμματα της μίας κατηγορίας και k της άλλης και έχουμε μια καλή πιθανότητα να πετύχουμε σύγκρουση

Βελτιωμένες επιθέσεις γενεθλίων

- ▶ Επιλογή των μηνυμάτων: Οι τιμές που δίνουμε για να πετύχουμε σύγκρουση, μπορούν να έχουν σχέση μεταξύ τους π.χ. η Alice απολύεται και θέλει να βρει δύο μηνύματα x και x' έτσι ώστε $H(x) = H(x')$, όπου το πρώτο λέει τους λόγους της απόλυσής της, ενώ το δεύτερο κολακευτικά λόγια
- ▶ Φτιάχνουμε $k = \Theta(2^{l/2})$ μηνύματα από τον πρώτο τύπο και άλλα τόσα από το δεύτερο τύπο και ψάχνουμε σύγκρουση μεταξύ αυτών των δύο τύπων μηνυμάτων.
“Είναι δύσκολο/ανέφικτο να βρεις μια τόσο καλή/εργατική/φιλότιμη υπάλληλο σαν την Alice. Η δουλειά της είναι καταπληκτική/ανεπανάληπτη/ασύγκριτη.”
- ▶ Ετοιμάζουμε k γράμματα της μίας κατηγορίας και k της άλλης και έχουμε μια καλή πιθανότητα να πετύχουμε σύγκρουση
- ▶ Σημείωση: Θέλει πολύ χώρο

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

1. Πάρε τυχαία αρχική τιμή x_0 και για $i > 0$ υπολόγισε $x_i = H(x_{i-1})$ και $x_{2i} = H(H(x_{2(i-1)}))$

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

1. Πάρε τυχαία αρχική τιμή x_0 και για $i > 0$ υπολόγισε $x_i = H(x_{i-1})$ και $x_{2i} = H(H(x_{2(i-1)}))$
2. Σε κάθε επανάληψη $x_i \stackrel{?}{=} x_{2i}$. Εάν ίσα, τότε ψάξε από το x_0 έως το x_i για σύγκρουση.

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

1. Πάρε τυχαία αρχική τιμή x_0 και για $i > 0$ υπολόγισε $x_i = H(x_{i-1})$ και $x_{2i} = H(H(x_{2(i-1)}))$
2. Σε κάθε επανάληψη $x_i \stackrel{?}{=} x_{2i}$. Εάν ίσα, τότε ψάξε από το x_0 έως το x_i για σύγκρουση.
 - ▶ Χώρος σταθερός: δύο στοιχεία x_i, x_{2i}

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

1. Πάρε τυχαία αρχική τιμή x_0 και για $i > 0$ υπολόγισε $x_i = H(x_{i-1})$ και $x_{2i} = H(H(x_{2(i-1)}))$
2. Σε κάθε επανάληψη $x_i \stackrel{?}{=} x_{2i}$. Εάν ίσα, τότε ψάξε από το x_0 έως το x_i για σύγκρουση.
 - ▶ Χώρος σταθερός: δύο στοιχεία x_i, x_{2i}
 - ▶ Επιτυχία $1/2$ σε $\Theta(2^{l/2})$ βήματα

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

Όρισε $g: \{0, 1\}^l \mapsto \{0, 1\}^*$, όπου το τελευταίο bit δείχνει ποιά πρόταση θα επιλεγεί και τα υπόλοιπα ποιά λέξη.

Παράδειγμα

0: Bob is a good/hardworking and honest/trustworthy worker/employee.

1: Bob is a difficult/problematic and taxing/irritating worker/employee.

$g(0000)$ = Bob is a good and honest worker.

$g(0001)$ = Bob is a difficult and taxing worker.

$g(1010)$ = Bob is a hardworking and honest employee.

$g(1011)$ = Bob is a problematic and taxing employee.

- ▶ Ορίζουμε $f(x) = H(g(x))$.

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

Όρισε $g: \{0, 1\}^l \mapsto \{0, 1\}^*$, όπου το τελευταίο bit δείχνει ποιά πρόταση θα επιλεγεί και τα υπόλοιπα ποιά λέξη.

Παράδειγμα

0: Bob is a good/hardworking and honest/trustworthy worker/employee.

1: Bob is a difficult/problematic and taxing/irritating worker/employee.

$g(0000)$ = Bob is a good and honest worker.

$g(0001)$ = Bob is a difficult and taxing worker.

$g(1010)$ = Bob is a hardworking and honest employee.

$g(1011)$ = Bob is a problematic and taxing employee.

- ▶ Ορίζουμε $f(x) = H(g(x))$.
- ▶ Οποιαδήποτε σύγκρουση x, x' στην f δίνει δύο μηνύματα $g(x), g(x')$ που συγκρούονται.

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

Όρισε $g: \{0, 1\}^l \mapsto \{0, 1\}^*$, όπου το τελευταίο bit δείχνει ποιά πρόταση θα επιλεγεί και τα υπόλοιπα ποιά λέξη.

Παράδειγμα

0: Bob is a good/hardworking and honest/trustworthy worker/employee.

1: Bob is a difficult/problematic and taxing/irritating worker/employee.

$g(0000)$ = Bob is a good and honest worker.

$g(0001)$ = Bob is a difficult and taxing worker.

$g(1010)$ = Bob is a hardworking and honest employee.

$g(1011)$ = Bob is a problematic and taxing employee.

- ▶ Ορίζουμε $f(x) = H(g(x))$.
- ▶ Οποιαδήποτε σύγκρουση x, x' στην f δίνει δύο μηνύματα $g(x), g(x')$ που συγκρούονται.
- ▶ Η πιθανότητα να είναι μηνύματα διαφορετικού τύπου είναι $1/2$.

Βελτιωμένες επιθέσεις γενεθλίων σταθερού χώρου

Όρισε $g: \{0, 1\}^l \mapsto \{0, 1\}^*$, όπου το τελευταίο bit δείχνει ποιά πρόταση θα επιλεγεί και τα υπόλοιπα ποιά λέξη.

Παράδειγμα

0: Bob is a good/hardworking and honest/trustworthy worker/employee.

1: Bob is a difficult/problematic and taxing/irritating worker/employee.

$g(0000)$ = Bob is a good and honest worker.

$g(0001)$ = Bob is a difficult and taxing worker.

$g(1010)$ = Bob is a hardworking and honest employee.

$g(1011)$ = Bob is a problematic and taxing employee.

- ▶ Ορίζουμε $f(x) = H(g(x))$.
- ▶ Οποιαδήποτε σύγκρουση x, x' στην f δίνει δύο μηνύματα $g(x), g(x')$ που συγκρούονται.
- ▶ Η πιθανότητα να είναι μηνύματα διαφορετικού τύπου είναι $1/2$.
- ▶ Αν είναι ίδιου τύπου, επαναλαμβάνουμε.

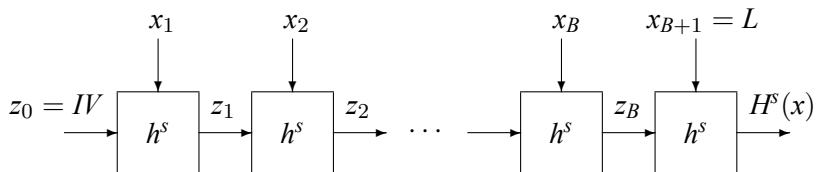
Επέκταση συναρτήσεων σύνοψης

Merkle-Damgård Hash Function Extention

Έστω (Gen, h) μια συνάρτηση σύνοψης που απεικονίζει είσοδο μήκους $2n$ σε έξοδο μήκους n . Κατασκευάζουμε μια συνάρτηση σύνοψης (Gen, H) μεταβλητού μήκους ως εξής:

- ▶ Gen : όπως προηγουμένως
- ▶ H : με είσοδο ένα string $x \in \{0, 1\}^*$ μήκους $L \leq 2^n$:
 1. Θέσε $B = \lceil \frac{L}{n} \rceil$ (πλήθος block του x). Πρόσθεσε μηδενικά στο x ώστε το μήκος να είναι πολλαπλάσιο του n ($x = x_1, \dots, x_B$). Θέσε $x_{B+1} = L$ (το L κωδικοποιημένο δυαδικά)
 2. Θέσε $z_0 = 0^n$ (Initialization vector)
 3. Για $i = 1, \dots, B + 1$, υπολόγισε το $z_i = h(z_{i-1} || x_i)$
 4. Έξοδος: z_{B+1}

Κατασκευή Merkle-Damgård



Σχήμα : Merkle-Damgård

Επέκταση συναρτήσεων σύνοψης

Θεώρημα

Αν η συνάρτηση σύνοψης h είναι *collision resistant*, τότε και η H που κατασκευάζεται με τη μέθοδο *Merkle-Damgård* είναι επίσης *collision resistant*.

Απόδειξη.

1. $L \neq L'$, οπότε στο τελευταίο βήμα είναι $z_{B+1} = h^s(z_B || L)$ και $z'_{B'+1} = h^s(z'_B || L')$, άρα σύγκρουση στην h^s , αφού τα strings $z_B || L$ και $z'_B || L'$ είναι διαφορετικά.
2. $L = L'$, οπότε $B = B'$, άρα $x_{B+1} = x'_{B+1}$ οπότε θα υπάρχει κάποιο προηγούμενο i , έτσι ώστε $x_i \neq x'_i$ για το οποίο υπάρχει σύγκρουση.



Δένδρα Merkle

- ▶ Ένας χρήστης θέλει να ανεβάσει αρχείο x σε έναν server.

Δένδρα Merkle

- ▶ Ένας χρήστης θέλει να ανεβάσει αρχείο x σε έναν server.
- ▶ Όταν το κατεβάσει, θέλει να ελέγξει αν είναι το ίδιο.

Δένδρα Merkle

- ▶ Ένας χρήστης θέλει να ανεβάσει αρχείο x σε έναν server.
- ▶ Όταν το κατεβάσει, θέλει να ελέγξει αν είναι το ίδιο.
- ▶ Λύση: αποθηκεύει τοπικά το $h = H(x)$, και όταν καταβάζει το ζητούμενο αρχείο x' ελέγχει $H(x') \stackrel{?}{=} h$.

Δένδρα Merkle

- ▶ Ένας χρήστης θέλει να ανεβάσει αρχείο x σε έναν server.
- ▶ Όταν το κατεβάσει, θέλει να ελέγξει αν είναι το ίδιο.
- ▶ Λύση: αποθηκεύει τοπικά το $h = H(x)$, και όταν καταβάζει το ζητούμενο αρχείο x' ελέγχει $H(x') \stackrel{?}{=} h$.
- ▶ Αν έχει πολλά αρχεία;

Δένδρα Merkle

- ▶ Ένας χρήστης θέλει να ανεβάσει αρχείο x σε έναν server.
- ▶ Όταν το κατεβάσει, θέλει να ελέγξει αν είναι το ίδιο.
- ▶ Λύση: αποθηκεύει τοπικά το $h = H(x)$, και όταν καταβάξει το ζητούμενο αρχείο x' ελέγχει $H(x') \stackrel{?}{=} h$.
- ▶ Αν έχει πολλά αρχεία; Διάφορες λύσεις

Δένδρα Merkle

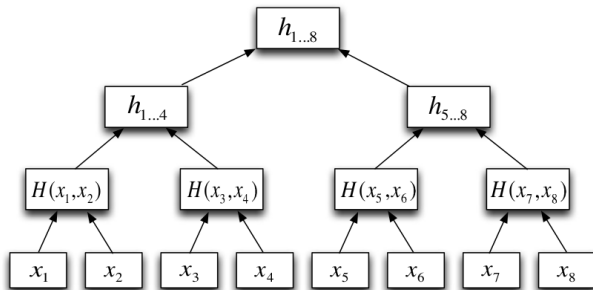
- ▶ Δένδρο Merkle με είσοδο x_1, x_2, \dots, x_n :

Δένδρα Merkle

- ▶ Δένδρο Merkle με είσοδο x_1, x_2, \dots, x_n : ένα δυαδικό δένδρο με φύλλα τα x_1, \dots, x_n και εσωτερικούς κόμβους τις κατακερματισμένες τιμές των παιδιών του.

Δένδρα Merkle

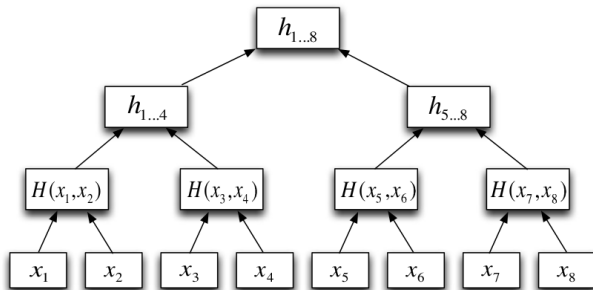
- ▶ Δένδρο Merkle με είσοδο x_1, x_2, \dots, x_n : ένα δυαδικό δένδρο με φύλλα τα x_1, \dots, x_n και εσωτερικούς κόμβους τις κατακερματισμένες τιμές των παιδιών του.



Σχήμα : Δένδρο Merkle

Δένδρα Merkle

- ▶ Δένδρο Merkle με είσοδο x_1, x_2, \dots, x_n : ένα δυαδικό δένδρο με φύλλα τα x_1, \dots, x_n και εσωτερικούς κόμβους τις κατακερματισμένες τιμές των παιδιών του.

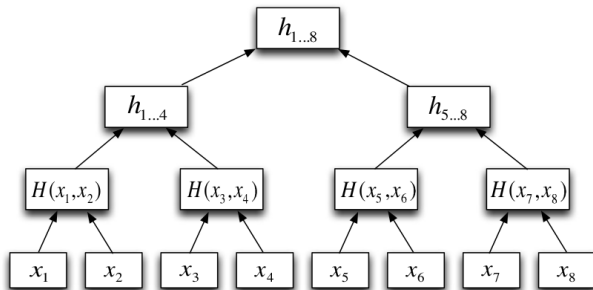


Σχήμα : Δένδρο Merkle

- ▶ Με δοσμένη συνάρτηση κατακερματισμού H , \mathcal{MT}_t είναι η συνάρτηση που με είσοδο τα x_1, \dots, x_t , υπολογίζει το δένδρο Merkle και τη ρίζα του δένδρου.

Δένδρα Merkle

- ▶ Δένδρο Merkle με είσοδο x_1, x_2, \dots, x_n : ένα δυαδικό δένδρο με φύλλα τα x_1, \dots, x_n και εσωτερικούς κόμβους τις κατακερματισμένες τιμές των παιδιών του.



Σχήμα : Δένδρο Merkle

- ▶ Με δοσμένη συνάρτηση κατακερματισμού H , \mathcal{MT}_t είναι η συνάρτηση που με είσοδο τα x_1, \dots, x_t , υπολογίζει το δένδρο Merkle και τη ρίζα του δένδρου.

Δένδρα Merkle

- ▶ Ο χρήστης υπολογίζει το $h = \mathcal{MT}_t(x_1, \dots, x_t)$, ανεβάζει τα x_1, \dots, x_t στον server και φυλάει το h (και το t)

Δένδρα Merkle

- ▶ Ο χρήστης υπολογίζει το $h = \mathcal{MT}_t(x_1, \dots, x_t)$, ανεβάζει τα x_1, \dots, x_t στον server και φυλάει το h (και το t)
- ▶ Όταν ο χρήστης θέλει το i -οστό αρχείο, ο server του στέλνει το x_i μαζί με μια “απόδειξη” π_i ότι είναι το σωστό αρχείο

Δένδρα Merkle

- ▶ Ο χρήστης υπολογίζει το $h = \mathcal{MT}_t(x_1, \dots, x_t)$, ανεβάζει τα x_1, \dots, x_t στον server και φυλάει το h (και το t)
- ▶ Όταν ο χρήστης θέλει το i -οστό αρχείο, ο server του στέλνει το x_i μαζί με μια “απόδειξη” π_i ότι είναι το σωστό αρχείο
- ▶ Η απόδειξη αποτελείται από τις τιμές που είναι γειτονικές στο μονοπάτι από το x_i προς τη ρίζα.

Δένδρα Merkle

- ▶ Ο χρήστης υπολογίζει το $h = \mathcal{MT}_t(x_1, \dots, x_t)$, ανεβάζει τα x_1, \dots, x_t στον server και φυλάει το h (και το t)
- ▶ Όταν ο χρήστης θέλει το i -οστό αρχείο, ο server του στέλνει το x_i μαζί με μια “απόδειξη” π_i ότι είναι το σωστό αρχείο
- ▶ Η απόδειξη αποτελείται από τις τιμές που είναι γειτονικές στο μονοπάτι από το x_i προς τη ρίζα.

Παράδειγμα Έστω ότι ζητάει το x_3 . Τότε ο server του στέλνει το x_3 μαζί και τα $x_4, h_{1..2}, h_{5..8}$

Δένδρα Merkle

- ▶ Αν η H είναι ελεύθερη συγκρούσεων, τότε είναι αδύνατο ο server να στείλει ψεύτικο αρχείο (και απόδειξη) που να επαληθεύεται.

Δένδρα Merkle

- ▶ Αν η H είναι ελεύθερη συγκρούσεων, τότε είναι αδύνατο ο server να στείλει ψεύτικο αρχείο (και απόδειξη) που να επαληθεύεται.
- ▶ Ο χρήστης χρειάζεται σταθερό χώρο και $\mathcal{O}(\log t)$ επικοινωνία με τον server.

Χρήσεις συναρτήσεων σύνοψης

- ▶ Ψηφιακές υπογραφές. Σε συνδυασμό με αλγόριθμο υπογραφής, για επιτάχυνση της διαδικασίας. Παραδείγματα: MD5, που χρησιμοποιείται με RSA στο PGP, SHA-1 (τόρα SHA-2), που χρησιμοποιείται στο DSS (Digital Signature Standard), κ.ά.
- ▶ Έλεγχος γνησιότητας μηνύματος – αυθεντικοποίηση (με συμμετρικό κλειδί): keyed hash functions, π.χ. HMAC.
- ▶ Ακεραιότητα δεδομένων (με ή χωρίς κλειδί).

Χρήσεις συναρτήσεων σύνοψης

- ▶ Ψηφιακές υπογραφές. Σε συνδυασμό με αλγόριθμο υπογραφής, για επιτάχυνση της διαδικασίας. Παραδείγματα: MD5, που χρησιμοποιείται με RSA στο PGP, SHA-1 (τόρα SHA-2), που χρησιμοποιείται στο DSS (Digital Signature Standard), κ.ά.
- ▶ Έλεγχος γνησιότητας μηνύματος – αυθεντικοποίηση (με συμμετρικό κλειδί): keyed hash functions, π.χ. HMAC.
- ▶ Ακεραιότητα δεδομένων (με ή χωρίς κλειδί).
- ▶ **Bitcoin**: blockchain, proof of work, **Merkle trees**.

Χρήσεις συναρτήσεων σύνοψης

- ▶ Ψηφιακές υπογραφές. Σε συνδυασμό με αλγόριθμο υπογραφής, για επιτάχυνση της διαδικασίας. Παραδείγματα: MD5, που χρησιμοποιείται με RSA στο PGP, SHA-1 (τόρα SHA-2), που χρησιμοποιείται στο DSS (Digital Signature Standard), κ.ά.
- ▶ Έλεγχος γνησιότητας μηνύματος – αυθεντικοποίηση (με συμμετρικό κλειδί): keyed hash functions, π.χ. HMAC.
- ▶ Ακεραιότητα δεδομένων (με ή χωρίς κλειδί).
- ▶ **Bitcoin**: blockchain, proof of work, **Merkle trees**.
- ▶ Γεννήτριες ψευδοτυχαίων αριθμών (με random seed + counter).
- ▶ Stream ciphers, αλλά και block ciphers (SHACAL).