6/4/2017

Μετά την πρόταση των ασύρματων πρωτοκόλλων από τους Diffie-Hellman το 1976, το 1978 προτάθηκε ένα πρωτόκολλο από τους Merkle-Hellman το οποίο βασίστηκε στο ότι δεν μπορούμε να λύσουμε γρήγορα NP-πλήρη προβλήματα. Ο λόγος για τον οποίο το πρωτόκολλο αυτό δεν χρησιμοποιήθηκε αλλά έσπασε το 1979 από τον Shamir είναι ότι υπάρχουν στιγμιότυπα για τα οποία τα NP-πλήρη προβλήματα λύνονται εύκολα, πράγμα που είναι καταστροφικό για την κρυπτογραφία.

Πρόβλημα Knapsack

Ένας τύπος NP-πλήρη προβλημάτων είναι το πρόβλημα knapsack, σύμφωνα με το οποίο έχουμε ένα σακίδιο το οποίο θέλουμε να γεμίσουμε με αντικείμενα έτσι ώστε να μεγιστοποιήσουμε το κέρδος που θα έχουμε.

Χαρακτηριστικά

- Σύνολο αντικειμένων: κάθε αντικείμενο έχει αξία V_i και βάρος W_i
- Κατώφλι βάρους W
- Πρόβλημα: βρες το υποσύνολο $S : \sum_{i \in S} W_i \leq W \ και \ max(\sum_{i \in S} V_i)$

Subset Sum

Μια παραλλαγή του προβλήματος knapsack είναι το πρόβλημα Subset Sum, το οποίο δεν λαμβάνει υπόψιν την αξία των αντικειμένων:

Χαρακτηριστικά

- Σύνολο αντικειμένων: κάθε αντικείμενο έχει βάρος W_i
- Κατώφλι βάρους W
- Πρόβλημα: βρες το υποσύνολο $S : \sum_{i \in S} W_i \leq W$

Παράδειγμα 1

Έστω το σύνολο Σ={14, 28, 56, 82, 90, 132, 197, 284, 341, 455} και W=516.

Υπάρχει ένα υποσύνολο αντικειμένων τα οποία αν τα επιλέξουμε από μια φορά να μας δίνουν άθροισμα 516;

Σε αυτή την περίπτωση δεν υπάρχει λύση, αλλά υπάρχει λύση για το 515: S={28, 56, 90, 341}

Παράδειγμα 2 – superincreasing ακολουθίες

Έστω το σύνολο Σ={1, 2, 4, 9, 18, 35, 70} και W=101.

Παρατηρούμε ότι σε αυτή την περίπτωση, η κάθε λύση θα πρέπει να περιέχει το 70. Γενικά, η παρατήρηση για όλο το σύνολο είναι ότι ο κάθε αριθμός είναι μεγαλύτερος από το άθροισμα όλων των προηγούμενων αριθμών, ή αλλιώς $\sum_{i=1}^{k-1} a_i < a_k$ Όταν έχουμε μια τέτοια ακολουθία ως είσοδο του προβλήματος, μπορούμε να το λύσουμε σε

γραμμικό χρόνο, προσθέτοντας τους αριθμούς από το μεγαλύτερο προς το μικρότερο μέχρι να φτάσουμε στο κατώφλι που θέλουμε.

Μετατροπή superincreasing ακολουθιών σε γενικές

Βλέπουμε ότι αν έχουμε μια τέτοια ακολουθία ως μήνυμα, είναι πολύ εύκολο να αποκρυπτογραφηθεί. Για να αντιμετωπίσουμε το πρόβλημα αυτό θα πρέπει να τη μετατρέψουμε σε γενική ακολουθία και ύστερα να την κρυπτογραφήσουμε.

Δημιουργία Κλειδιού

- Επιλέγω superincreasing ακολουθία $\{\alpha_1, \alpha_2, \dots \alpha_n\}$: για κάθε α_i $\sum_{i=1}^{k-1} a_i < a_k$
- Επιλέγω W, N με gcd(W,N)=1 και $N > \sum_{i=1}^{n} a_i$ Παίρνουμε αυτούς τους περιορισμούς για να μην έχουμε τον ίδιο αριθμό 2 φορές στη γενική ακολουθία (βλ. παράδειγμα παρακάτω)
- Υπολογίζω $b_i = wa_i \pmod N$ και ταξινομώ την ακολουθία b.

  Μυστικό κλειδί: α Δημόσιο κλειδί b

Κρυπτογράφηση

- βρίσκω δημόσιο κλειδί b του παραλήπτη
- σπάω το μήνυμα M σε n-άδες
- κάθε block του μηνύματος $m_i=\{m_1, m_2, \dots m_n\}$ το μετατρέπω σε $c_i = \sum_{j=1}^{n} b_j \cdot m_j$
- Μεταδίδω $c_1, c_2, \dots c_t$

Παράδειγμα: έστω b={1, 7, 8, 12, 15} και m=10101. Το αποτέλεσμα της κρυπτογράφησης είναι 1+8+15=24. Όπου έχουμε bit με την τιμή 1, προσθέτουμε τον αντίστοιχο αριθμό.

Αποκρυπτογράφηση

C_i --> $W^{-1} c \bmod N = c_1$ και λύνω τα c_i με την ακολουθία α.

Παράδειγμα

Έστω η superincreasing ακολουθία α={1, 2, 4, 9, 20, 38} και W=31, N=105

1: $31 \cdot 1 \bmod 105 = 31$

2: $31 \cdot 2 \bmod 105 = 62$

4: $31 \cdot 4 \bmod 105 = 19$

9: $31 \cdot 9 \bmod 105 = 69$

20: $31 \cdot 20 \bmod 105 = 95$

38: $31 \cdot 38 \bmod 105 = 23$

άρα b={19, 23, 31, 62, 69, 95}

Δεν μπορεί να έχουμε δύο ή παραπάνω ίδιους αριθμούς στη b λόγω των περιορισμών που έχουμε πάρει για τα W και N.

Έστω ότι το μήνυμα που θέλουν να μας στείλουν είναι το m=001100110100. Έχουμε 6 στοιχεία στην α άρα το χωρίζουμε σε εξάδες, δηλαδή m_1=001100 και m_2=110100. Τότε έχουμε c_1=31+62=93 και c_2=19+23+62=104.

Αποκρυπτογράφηση: $c_i \text{-->} w^{-1} c_1 \bmod N$

$31^{-1} \bmod 105 = 61$ -->$61 \cdot 93 \bmod 105 = 3$

$61 \cdot 104 \bmod 105 = 44$

ΠΡΟΣΟΧΗ θα πρέπει να αντιστρέψουμε την ταξινόμηση που κάναμε όταν φτιάξαμε τη b.

α	1	2	4	7	20	38
b	31	62	19	69	95	23
$\overline{b}$	19	23	31	62	69	95

Η νέα ταξινόμηση της b είναι στην πραγματικότητα: {4, 38, 1, 2, 9, 20} άρα το μήνυμα είναι : 3-->001100 44-->110100

Το πρωτόκολλο Merkle-Hellman έσπασε όταν ο Shamir απέδειξε ότι δεν χρειάζεται να βρούμε τα W και N, αρκεί να βρούμε κοντινά τους με τις ίδιες ιδιότητες.

Το πρώτο πιθανοτικό πρωτόκολλο

Τα πρωτόκολλα που έχουμε δει μέχρι τώρα είναι ντετερμινιστικά και υπάρχει περίπτωση το κρυπτογραφημένο μήνυμα να είναι ίδιο με το αρχικό. Το πρώτο πιθανοτικό πρωτόκολλο δημιουργήθηκε το δημιουργήθηκε το 1984 από τον ElGamal, το οποίο περιλαμβάνει τα εξής βήματα:

<u>Δημιουργία Κλειδιού</u>
Διαλέγω p πρώτο, g γεννήτορα και ακέραιο α.

Δημόσιο κλειδί: $(p, g, g^{\alpha} \bmod p)$

Μυστικό κλειδί: α

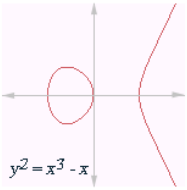
<u>Κρυπτογράφηση</u>
Έστω το μήνυμα m και διαλέγουμε τυχαίο k. Έτσι έχουμε $\gamma = \overline{g}^{k} \bmod p$ και $\delta = m(g^{\alpha k} \bmod p)$.

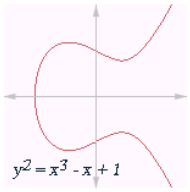
<u>Αποκρυπτογράφηση</u>
$m = \gamma^{-1} \delta \bmod p = g^{-\alpha k} m\, g^{\alpha k} \bmod p$

Παρατήρηση

Υπάρχουν προβλήματα που λύνονται σε εκθετικό χρόνο τα οποία περιμένουμε να πέσουν σε πολυωνυμικό στα επόμενα χρόνια. Γι' αυτό, πρωτόκολλα που βασίζονται σε αυτά θεωρούνται αναξιόπιστα.

Ελλειπτικές Καμπύλες





Οι καμπύλες αυτές λύνονται από σχέσεις της μορφής $y^2=x^3+Ax+B(modp)$.

Για να προσθέσουμε δύο σημεία σε αυτό το χώρο, πρέπει να πάρουμε την ευθεία που τα ενώνει και να βρούμε την τομή της με την καμπύλη. Η λύση θα είναι το αντισυμμετρικό σημείο αυτού του σημείου τομής.

Αν η ευθεία είναι κατακόρυφη, λύση είναι το "σημείο στο άπειρο" που συμβολίζεται με το 0. Δεν γίνεται να πολλαπλασιάσουμε δύο διαφορετικά σημεία σε αυτό το πεδίο, μπορούμε μόνο να παράγουμε πολλαπλάσια του ίδιο σημείου (ουσιαστικά με αλλεπάλληλες προσθέσεις).

Παράδειγμα

$y^2=x^3-3x+3$ (mod7)

x={0, 1, 2, 3, 4, 5, 6}

x=0: $y^2=3mod7$, δεν υπάρχει τέτοιο y

x=1: $y^2=0mod7$, 1, 0

x=2: $y^2=3mod7$, δεν υπάρχει τέτοιο y

....

Τελικά θα έχουμε 6 σημεία.

Αντιστοιχία πράξεων

Z	ελλειπτικές
Πολλαπλασιασμός	Πρόσθεση
Ύψωση σε δύναμη	Πολλαπλασιασμός

ElGamal σε ελλειπτικές καμπύλες

<u>Δημιουργία Κλειδιού</u>

Μήνυμα: $P_m=(x_m, y_m)$

δημόσιο κλειδί: $G=(x_g, y_g)$, $P_b=n_BBG$, A, B, P

μυστικό κλειδί: n_B

Κρυπτογράφηση

$C_m=(KG, P_m+kP_b)$