Θεωρία αριθμών και κρυπτογραφία
N. Lygeros

Θεωρία αριθμών και κρυπτογραφία

- Παράδειγμα της τυχαίας ακολουθίας 01010011000… και εμφάνιση των 100 και 111. Χρήση του τυχαίου ως παραπληροφόρηση.
- Οι ελλειπτικές καμπύλες επιτρέπουν την εφαρμογή νέων κρυπτοσυστημάτων. Ταυτόχρονα θέτουν σε κίνδυνο το κρυπτοσυστήματα, όπως το RSA. Η ιδέα του αλγόριθμου ανήκει στον Lenstra.

Υποθέτουμε ότι θέλουμε την παραγοντοποίηση ενός δεδομένου ακεραίου. Έστω p ένας πρώτος διαιρέτης του n (τον οποίο δεν γνωρίζουμε).

Στάδιο 1: Επιλογή μιας ελλειπτικής καμπύλης.

Επιλέγουμε το α και το b, έτσι ώστε $4a^3+27b^2$ να είναι πρώτο με το n. Εδώ τους επιλέξαμε τυχαία και δεν είναι πρώτο, ακόμα καλύτερα, διότι $\text{pgcd}(4a^3+27b^2, n)$ δίνει έναν απόλυτο διαιρέτη του n. Παρατηρούμε ότι, εφόσον $4a^3+27b^2$ είναι πρώτο με το n, είναι πρώτο και με το p και είναι αντίστροφο στο $\mathbb{Z}/p\mathbb{Z}$, την οποία γράφουμε $E(a,b,p)$.
(Εφόσον δεν ξέρουμε το p, δεν ξέρουμε και την ελλειπτική καμπύλη).

Στάδιο 2: Επιλογή ενός σημείου πάνω στην ελλειπτική καμπύλη.

Βρίσκουμε 2 ακέραιους x και y, ώστε $y^2 = x^3 + ax + b$. Συγκεκριμένα, είναι ένα σημείο της ελλειπτικής καμπύλης $E(a,b,p)$.

Στάδιο 3: Επιλογή ενός βοηθητικού ακεραίου.

Επιλέγουμε K ένας ακέραιος, όχι πολύ μεγάλος, ο οποίος έχει μικρούς πρώτους παράγοντες σε υψηλές δυνάμεις.

Στάδιο 4: Υπολογισμός στις ελλειπτικές συναρτήσεις.

Υπολογίζουμε τις συντεταγμένες του σημείου KP χρησιμοποιώντας τις κλασικές φόρμουλες*modulom*. Αυτοί οι υπολογισμοί περιέχουν διαιρέσεις οι οποίες δεν ισχύουν πάντα*modulon:* διότι ο παρανομαστής*d* πρέπει να είναι πρώτος με το n. Όμως ελπίζουμε ότι αυτό δεν θα γίνει. Διότι, αν ο d δεν είναι πρώτος με τον n, τότε $\text{pgcd}(d,n)$ δίνει ένα διαιρέτη (πρώτο) του n. Αν εκτελέσουμε ολοκληρωτικά όλους τους υπολογισμούς, ξαναρχίζουμε στο στάδιο 1, αλλάζοντας ελλειπτική καμπύλη.

Γιατί λειτουργεί ο αλγόριθμος;

Αν μια ελλειπτική καμπύλη $E(a,b,p)$ (p διαιρέτης του n) έχει m σημείο, ώστε m να είναι το γινόμενο μικρών πρώτων παραγόντων, τότε $m|K$. Το K είναι συνεπώς ένα πολλαπλάσιο του αριθμού της ομάδας της ελλειπτικής καμπύλης και με το θεώρημα του Lagrange KP=0 (σημείο στο άπειρο). Τότε, στον υπολογισμό KP θα συμβεί ένα λάθος (διαίρεση με 0) και θα βρούμε ένα διαιρέτη του n. Αρκεί να συμβεί για τον αριθμό της ελλειπτικής καμπύλης $E(a,b,p)$, όπως μπορούμε να επιλέξουμε ελεύθερα το α και το b, μπορεί να συμβεί. Και υπάρχει θεώρημα που λέει ότι πάντα συμβαίνει για μια ορισμένη επιλογή των α και b.
Στην πράξη, για να παραγοντοποιήσουμε τους ακέραιους RSA, ο αλγόριθμος είναι λιγότερο αποτελεσματικός από το quadratic κόσκινο μα είναι αποτελεσματικότατο για την παραγοντοποίηση ενός ακεραίου που έχει έναν σχετικά μικρό παράγοντα.

Ανταλλαγή κλειδιών μέσω ελλειπτικών καμπύλων.

Alice και Bob επιλέγουν ελεύθερα μια ελλειπτική καμπύλη $E(a,b,p)$, δηλαδή επιλέγουν ένα σώμα K και μια καμπύλη $y^2 = x^3 + ax^2 + b$.Και επιλέγουν μαζί ένα σημείο P στην καμπύλη.
Κρυφά η Alice επιλέγει έναν ακέραιο K_A και ο Bob έναν ακέραιο K_B . Η Alice στέλνει στον Bob το σημείο $K_A P$ και ο Bob στέλνει στην Alice $K_B P$. Έτσι, μπορούν να υπολογίσουν ο καθένας
$K_A(K_B P) = K_B(K_A P) = (K_A K_B P)$ ένα σημείο της καμπύλης που αποτελεί το μυστικό κλειδί τους.
Αν κάποιος ανακαλύψει τις ανταλλαγές τους, γνωρίζει $E(a,b,k), P, K_A P, K_B P$. Για να υπολογίσει όμως $K_A K_B P$ πρέπει να υπολογίσει K_A γνωρίζοντας P και $K_A P$. Δηλαδή πρέπει να λύσει το διακριτό λογάριθμο στην ελλειπτική καμπύλη. Ο διακριτός λογάριθμος είναι ήδη δύσκολος στις γνωστές ομάδες $(\mathbb{Z}/p\mathbb{Z})^x$. Για πιο δύσκολες ομάδες και διαφορετικές των ελλειπτικών καμπύλων είναι ακόμα πιο δύσκολα.

Πλεονεκτήματα και μειονεκτήματα.

+ Δύσκολος υπολογισμός του διακριτού λογάριθμου.

+ 200 bits (ECM) >> 1024 bits (RSA)

+ Εύκολοι υπολογισμοί καλό για τις πιστωτικές κάρτες (ελάχιστη ισχύ)

—› διότι υπάρχει εξάρτηση με το μέγεθος του κλειδιού.

- Η θεωρία είναι δύσκολη και νέα. Άρα μπορεί να υπάρχουν λύσεις που δεν χρησιμοποιούν τον διακριτό λογάριθμο. (Θεωρητικά).

- Πολλές πατέντες στην τεχνολογία της κρυπτογραφίας μέσω ελλειπτικών καμπύλων.