

Πώς προσθέτουμε σημεία?

Αν $P=(x_1, y_1)$ και $Q=(x_2, y_2) \in E(F_p)$ τότε:

(1) Αν $x_2=x_1$ και $y_2=-y_1$ τότε $P+Q=0$ αλλιώς

$$(2) P+Q=(x_3, y_3) \text{ όπου } \begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \text{ και } \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{ αν } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, \text{ αν } P = Q \end{cases}$$

Αρα $2a=(2, 7) \oplus (2, 7) = (x_3, y_3)$. Υπολογίζουμε $\lambda=(3*2^2+1)(2*7)^{-1} \text{ mod } 11 = 2*3^{-1} \text{ mod } 11 = 2*4=8$. Οπότε $x_3=8^2-2-2 \text{ mod } 11 \Rightarrow x_3=5$ και $y_3=8(2-5)-7 \text{ mod } 11 \Rightarrow y_3=2$. (Από τους τύπους παραπάνω).

Αρα τελικά \Rightarrow ότι $2a=(5,2)$

Συνεχίζουμε με τον ίδιο τρόπο και σχηματίζουμε τον ακόλουθο πίνακα:

$a=(2,7)$	$5a=(3,6)$	$9a=(10,9)$
$2a=(5,2)$	$6a=(7,9)$	$10a=(8,8)$
$3a=(8,3)$	$7a=(7,2)$	$11a=(5,9)$
$4a=(10,2)$	$8a=(3,5)$	$12a=(2,4)$

Το 13α είναι το ουδέτερο αφού προκύπτει ως το άθροισμα του a και του $12a$ τα οποία έχουν $x_1 = x_{12}$ και $y_1 = -y_{12}$ ($4+7 = 0 \text{ mod } 11$)

Από το παράδειγμα φαίνεται ότι $\#E(F_p) \sim P$. Πράγματι ισχύει το Θεώρημα του Hasse:

$p+1-2\sqrt{p} \leq \#E(F_p) \leq p+1+2\sqrt{p}$. Υπάρχει αλγόριθμος του Schoof που υπολογίζει επακριβώς το $\#E(F_p)$.

Υποθέτουμε ότι υπολογίσαμε το $\#E(F_p)$. Θα πρέπει να βρούμε κατάλληλη κυκλική υποομάδα της $E(F_p)$ όπου το DLP να είναι δύσκολο. Χρειαζόμαστε κάτι παραπάνω από τη δομή της $E(F_p)$. Ισχύει το:

Θεώρημα:

$E =$ ελλειπτική καμπύλη $|_{F_p}$ ($p > 3$). Υπάρχουν φυσικοί n_1 και n_2 τέτοιοι ώστε $E(F_p) \approx Z_{n_1} \times Z_{n_2}$ όπου ισχύει επιπλέον $n_2 | n_1$ και $n_2 | (p-1)$.

- Αν επομένως μπορούμε να υπολογίσουμε τα n_1 και n_2 τότε γνωρίζουμε ότι υπάρχει κυκλική υποομάδα $\approx Z_{n_1}$. Αυτή αποτελεί πιθανό υποψήφιο για το κρυπτοσύστημα El Gamal.

Ειδικές Περιπτώσεις

- Αν $n_2=1 \Rightarrow E(F_p)$ κυκλική επίσης, αν $\#E(F_p)$ πρώτος αριθμός ή γινόμενο δύο διακεκριμένων πρώτων $\Rightarrow E(F_p)$ κυκλική.
- $E(F_p) \approx Z_{n_1} \times Z_{n_2}$ όπου n_2 / n_1 και $n_2 / p-1$. Αν $n_2 = 1 \Rightarrow Z_{n_2} = \{1\} \Rightarrow E(F_p) \approx Z_{n_1}$ κυκλική τάξης n_1 και είναι υποψήφια για το DLP πρόβλημα.

Είναι γνωστό από θεωρία ομάδων ότι, αν G αβελιανή ομάδα τάξης $p \cdot q$ όπου $p, q \in \mathbb{P}$ με $p \neq q$ τότε η ομάδα G είναι κυκλική.

Παράδειγμα Κρυπτογράφησης κατά El Gamal με χρήση ελλειπτικών καμπύλων.

Υποθέτουμε ότι $a = (2, 7)$ και ο μυστικός εκθέτης του Bob είναι $\alpha = 7$, άρα $\beta = 7 \cdot a = (7, 2)$ από πίνακα. Η συνάρτηση κρυπτογράφησης είναι $e_k(x, k) = (k \cdot (2, 7), x + k \cdot (7, 2))$ και η συνάρτηση αποκρυπτογράφησης είναι $d_k(y_1, y_2) = y_2 - 7y_1$.

Υποθέτουμε ότι η Αλίκη επιθυμεί να κρυπτογραφήσει το $x = (10, 9)$ το οποίο ανήκει $E(F_{11})$. Έστω ότι διαλέγει $k = 3$ και υπολογίζει $y_1 = 3(2, 7) = (8, 3)$ και $y_2 = (10, 9) + 3(7, 2) =$

$(10, 9) + (3, 5) = (10, 2)$. Σημειώνουμε ότι η πρόσθεση μεταξύ των δύο σημείων γίνεται με το τρόπο που δόθηκε παραπάνω και ΟΧΙ με το καθιερωμένο τρόπο πρόσθεσης σημείων.

Άρα το $y = ((8, 3), (10, 2))$.

Στην συνέχεια ο Βασιλάκης αποκρυπτογραφεί το μήνυμα y και παίρνει:

$$x = (10, 2) - (7(8, 3)) = (10, 2) - (3, 5) = (10, 2) + (8, 6) = (10, 9).$$

Παρατήρηση:

1. Το El Gamal, σε ελλειπτική καμπύλη έχει μερικές παραπάνω δυσκολίες από ότι στο F_p . Στο F_p έχουμε απεικόνιση από το $x \rightarrow y = (y_1, y_2)$. Στις ελλειπτικές καμπύλες έχουμε παράγοντα 4 δηλαδή $x = (x_1, x_2) \rightarrow ((-, -), (-, -))$.
2. Πολύ πιο σοβαρό είναι το πρόβλημα ότι το Plaintext P αποτελείται από σημεία πάνω στο $E(F_p)$ και δεν υπάρχει γενική (deterministic = με κάποιο τρόπο να καθορίζεται πλήρως) μέθοδος που να δίνει τα ρητά σημεία.

Η μέθοδος του Menezes και Vanstone χρησιμοποιεί «μάσκα» τόσο το plaintext όσο και το Cipher text. Επιτρέπεται να είναι διατεταγμένα ζεύγη (μη μηδενικά) στοιχεία ενός σώματος. (Όχι κατ' ανάγκη σημεία της Ελλειπτικής Καμπύλης)

Κρυπτοσύστημα Menezes – Vanstone

$E|_{F_p}$, $p \in P$, $p > 3$ τέτοιο ώστε να περιέχει κυκλική υποομάδα H της $E(F_p)$ όπου το πρόβλημα να είναι δύσκολο.

$P : F_p^* \times F_p^*$, $l = E \times F_p^* \times F_p^*$, $K = \{(E, a, a, \beta) \mid \beta = a \alpha\}$, όπου $a \in E(F_p)$. a, β δημοσιοποιημένα, a μυστικό.

Για $K = (E, a, a, \beta)$ και τυχαίο $k \in Z_{|H|}$ και $x = (x_1, x_2) \in F_p^* \times F_p^*$ ορίζουμε $e_k(x, k) = (y_0, y_1, y_2)$, όπου $y_0 = ka$, $y_1 = c_1 x_1 \bmod p$, $y_2 = c_2 x_2 \bmod p$.

Για $y = (y_0, y_1, y_2)$ αποκωδικοποιούμε $d_k(y) = (y_1 c_1^{-1} \bmod p, y_2 c_2^{-1} \bmod p)$ όπου $a y_0 = (c_1, c_2)$.

Παρατήρηση:

Το κρυπτοσύστημα επιτρέπει $10 \times 10 = 100$ δυνατά Plaintext σε αντίθεση με τα 13 του αρχικού συστήματος.

Παράδειγμα :

Υποθέτουμε ότι $a = (2, 7)$ και ο μυστικός εκθέτης του Βασιλή είναι $\alpha = 7$. Αυτό σημαίνει ότι το $\beta = 7(2, 7) = (7, 2)$. Υποθέτουμε ότι η Αλίκη θέλει να στείλει το κρυπτοσύστημα $x = (x_1, x_2) = (9, 1) \notin E(F_{11})$. Η Αλίκη διαλέγει $k = 6$. Υπολογίζει $y_0 = k a = 6(2, 7) = (7, 9)$ και $ka = k \beta = a y_0 = 6(7, 2) = (8, 3)$. Επομένως $c_1 = 8$ και $c_2 = 3$. Στην συνέχεια υπολογίζει τα y_1 και y_2 .

- $y_1 = c_1 x_1 \bmod p = 8 \times 9 \bmod 11 = 6$
- $y_2 = c_2 x_2 \bmod p = 3 \times 1 \bmod 11 = 3$

Άρα το cipher text $y = (y_0, y_1, y_2) = ((7, 9), (6, 3))$.

Ο Βασιλής παίρνει το μήνυμα y και υπολογίζει $(c_1, c_2) = 7(7, 9) = (8, 3)$.

Στην συνέχεια εκτελεί της παρακάτω πράξεις προκειμένου να αποκρυπτογραφήσει το μήνυμα.

$$x \equiv (y_1 c_1^{-1} \bmod p, y_2 c_2^{-1} \bmod p) = (6 \times 8^{-1} \bmod 11, 3 \times 3^{-1} \bmod 11) = (6 \times 7 \bmod 11, 3 \times 4 \bmod 11) = (9, 1).$$