

Κρυπτοσυστήματα Διακριτού Λογαρίθμου

Παναγιώτης Γροντάς - Άρης Παγουρτζής

ΕΜΠ - Κρυπτογραφία (2017-2018)

21/11/2017

Περιεχόμενα

- Διακριτός Λογάριθμος: Προβλήματα και Αλγόριθμοι
- Το κρυπτοσύστημα ElGamal
- Το κρυπτοσύστημα Cramer Shoup
- Σχήματα Δέσμευσης με βάση το DLP
- Ελλειπτικές Καμπύλες

Προβλήματα Διακριτού Λογαρίθμου I

DLP - Το πρόβλημα του Διακριτού Λογαρίθμου

Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$ τάξης q και ένα τυχαίο στοιχείο $y \in \mathbb{G}$

Να υπολογιστεί $x \in \mathbb{Z}_q$ ώστε $g^x = y$

δηλ. το $\log_g y \in \mathbb{Z}_q$

CDHP - Το υπολογιστικό πρόβλημα Diffie Hellman

Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, δύο στοιχεία

$y_1 = g^{x_1}, y_2 = g^{x_2}$

Να υπολογιστεί το $g^{x_1 \cdot x_2}$

Προβλήματα Διακριτού Λογαρίθμου II

DDHP - Το πρόβλημα απόφασης Diffie Hellman

Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, δύο στοιχεία

$y_1 = g^{x_1}, y_2 = g^{x_2}$ και κάποιο $y \in \mathbb{G}$

Να εξεταστεί αν $y = g^{x_1 \cdot x_2}$

ή ισοδύναμα

DDHP - Το πρόβλημα απόφασης Diffie Hellman

Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, δύο στοιχεία

$y_1 = g^{x_1}, y_2 = g^{x_2}$ και κάποιο $y \in \mathbb{G}$

Μπορούμε να ξεχωρίσουμε τις τριάδες $(g^{x_1}, g^{x_2}, g^{x_1 x_2})$ και (g^{x_1}, g^{x_2}, y) ;

Σχέσεις Προβλημάτων

$CDHP \leq DLP$

Αν μπορούμε να λύσουμε το DLP , τότε μπορούμε να υπολογίσουμε τα x_1, x_2 από τα y_1, y_2 και στην συνέχεια το $g^{x_1 \cdot x_2}$

$DDHP \leq CDHP$

Αν μπορούμε να λύσουμε το $CDHP$, υπολογίζουμε το $g^{x_1 \cdot x_2}$ και ελέγχουμε ισότητα με το y

Δηλαδή: $DDHP \leq CDHP \leq DLP$

Επιλογή Ομάδας

- Καθορίζει τη δυσκολία του προβλήματος
- Δύο επιλογές:
 - (\mathbb{Z}_p^*, \cdot) με p πρώτο (σε υποομάδα)
 - $(\mathcal{E}(\mathbb{F}_p), +)$
- Διαφορετική πράξη, παρά το όνομα
- Διαφορετική τιμή για παράμετρο ασφάλειας

Brute Force

Για ομάδα $\mathbb{G} = \langle g \rangle$ τάξης q λ bits

Δοκιμή όλων των $x \in \mathbb{Z}_q$ μέχρι να βρεθεί τέτοιο ώστε $g^x = y$

Πολυπλοκότητα $O(2^\lambda)$

Γενικευμένη μέθοδος - δεν εξαρτάται απο χαρακτηριστικά ομάδας

Αλγόριθμος Baby step - Giant Step (Shanks)

Αλγόριθμος Meet-In-The Middle

- Ισχύει $x = ak + b$, $k \in \mathbb{Z}$, $\forall x \in \mathbb{Z}$
- Για να μην χρειαστεί εύρεση αντιστρόφου: $x = ak - b$
- $y = g^{ak} \cdot g^{-b} \Rightarrow yg^b = g^{ak}$
- Θα υπολογίζουμε yg^b και g^{ak} μέχρι να συναντηθούν
 - 1 Ξεκινάμε στη 'μέση': $k = \lfloor \sqrt{q} \rfloor$
 - 2 **Giant steps - μέγεθος k :**
Υπολογίζουμε g^{ak} , $a \in \{0, \dots, \lfloor q/k \rfloor\}$ και αποθηκεύουμε σε πίνακα
 - 3 **Baby steps - μέγεθος 1:**
Υπολογίζουμε yg^b , $b \in \{0, \dots, \lfloor \sqrt{q} \rfloor\}$ και αναζητούμε στον πίνακα του Βημ. 2
 - 4 Όταν βρεθεί: $x = ak - b$

Πολυπλοκότητα χώρου και χρόνου: $O(2^{\frac{\lambda}{2}})$

Μείωση χώρου με αλγόριθμους Pollard (ρ , λ)

Παράδειγμα Baby step - Giant Step

Θέλουμε το $2^x = 17 \pmod{29}$ στο $\mathbb{Z}_{29}^* = \langle 2 \rangle$

$$\lfloor \sqrt{29} \rfloor = 5$$

- | | |
|----------------------------------|---------------------------------|
| ■ $a \in \{0 \dots 5\}$ | ■ $b \in \{0 \dots 5\}$ |
| ■ $2^{0 \cdot 5} = 1 \pmod{29}$ | ■ $17 \cdot 2^0 = 17 \pmod{29}$ |
| ■ $2^{1 \cdot 5} = 3 \pmod{29}$ | ■ $17 \cdot 2^1 = 5 \pmod{29}$ |
| ■ $2^{2 \cdot 5} = 9 \pmod{29}$ | ■ $17 \cdot 2^2 = 10 \pmod{29}$ |
| ■ $2^{3 \cdot 5} = 27 \pmod{29}$ | ■ $17 \cdot 2^3 = 20 \pmod{29}$ |
| ■ $2^{4 \cdot 5} = 23 \pmod{29}$ | ■ $17 \cdot 2^4 = 11 \pmod{29}$ |
| ■ $2^{5 \cdot 5} = 11 \pmod{29}$ | |

Άρα $x = 5 \cdot 5 - 4 = 21$
Πράγματι: $2^{21} = 17 \pmod{29}$

Αλγόριθμος Pohlig-Hellman - Ιδέα

Παρατήρηση

Η δυσκολία του DLP σε μια ομάδα \mathbb{G} εξαρτάται από τη δυσκολία του στις διάφορες υποομάδες της.

Συγκεκριμένα

Παραγοντοποίηση της τάξης (πχ. στο \mathbb{Z}_p^* : $p - 1 = \prod_{i=1}^m p_i^{e_i}$ με p_i πρώτο)

Επίλυση σε κάθε υποομάδα και συνδυασμός με CRT

Smooth Number

Μπορεί να παραγοντοποιηθεί σε μικρούς πρώτους - Αν ισχύει για την τάξη επιτυγχύνει τον αλγόριθμο

Αλγόριθμος Pohlig-Hellman - Βήματα I

- Για κάθε p_i γράφουμε

$$x = a_0 + a_1 p_i + \dots + a_{e_i-1} p_i^{e_i-1} \pmod{p_i^{e_i}}$$

με

$$a_j \in \{0, \dots, p_i - 1\}$$

- Πχ. αν παράγοντας του $p - 1$ είναι το 4:

$$x = a_0 + a_1 * 2 \pmod{4}$$

- Με αντικατάσταση του x έχουμε:

$$\begin{aligned} y^{\frac{p-1}{p_i}} &= g^{x \frac{p-1}{p_i}} = g^{(a_0 + a_1 p_i + \dots + a_{e_i-1} p_i^{e_i-1}) \frac{p-1}{p_i}} = \\ &= g^{(a_0 + K p_i) \frac{p-1}{p_i}} = g^{a_0 \frac{p-1}{p_i}} \pmod{p} \end{aligned}$$

- Υπολογισμός a_0 (με αλγόριθμο Shanks)

DLP

DLP

11 / 62

Αλγόριθμος Pohlig-Hellman - Βήματα II

- Για υπολογισμό a_1, \dots δημιουργούμε ακολουθία y_j με $y_0 = y$

■

$$y_j = y_{j-1} \cdot g^{-(a_0 + a_1 p_i + \dots + a_{j-1} p_i^{j-1})} \pmod{p}$$

- Γενικεύοντας έχουμε :

$$y_j^{p_i^{j+1}} = g^{a_j \frac{p-1}{p_i}}$$

υπολογίζουμε το a_j με αλγόριθμο Shanks

- Υπολογισμός για κάθε p_i :

$$a_0, y_1, a_1, y_2, \dots, a_{e_i-1}$$

- Συνδυασμός λύσεων με CRT

DLP

DLP

12 / 62

Παράδειγμα Pohlig-Hellman I

Θέλουμε το $2^x = 17 \pmod{29}$ στο $\mathbb{Z}_{29}^* = \langle 2 \rangle$

$$28 = 2^{27}$$

$$x_2 = a_0 + 2a_1 \pmod{4} \text{ και } x_7 = a_0 \pmod{7}$$

Υπολογισμός a_0 για το x_2

$$y^{\frac{p-1}{2}} = g^{a_0 \frac{p-1}{2}} \Rightarrow 17^{14} = 2^{14a_0} \Rightarrow 2^{14a_0} = 28 = -1 \pmod{29}$$

$$\text{Άρα } a_0 = 1$$

Υπολογισμός y_1 για το x_2

$$y_1 = yg^{-a_0} = 17 \cdot 2^{-1} = 17 \cdot 15 = 23 \pmod{29}$$

Παράδειγμα Pohlig-Hellman II

Υπολογισμός a_1 για το x_2

$$y_1^{\frac{p-1}{4}} = g^{a_1 \frac{p-1}{2}} \Rightarrow 23^7 = 2^{14a_1} \Rightarrow 2^{14a_1} = 1 \pmod{29}$$

$$\text{Άρα } a_1 = 0$$

$$\text{Άρα } x_2 = 1 + 0 \pmod{4}$$

Υπολογισμός a_0 για το x_7

$$y^{\frac{p-1}{7}} = g^{a_0 \frac{p-1}{7}} \Rightarrow 17^4 = 2^{4a_0} \Rightarrow 2^{4a_0} = 1 \pmod{29}$$

$$\text{Άρα } a_0 = 0$$

$$\text{Άρα } x_7 = 0 \pmod{7}$$

$$\text{CRT: } x = 21$$

Δυσκολία DDHP I

Θεώρημα

Το DDHP δεν είναι δύσκολο στην \mathbb{Z}_p^*

Μπορεί να κατασκευαστεί αποδοτικός αλγόριθμος διαχωρισμού τριάδας DH g^a, g^b, g^{ab} από μια τυχαία τριάδα g^a, g^b, g^c .

Πώς: Χρησιμοποιώντας το **σύμβολο Legendre**.

Το σύμβολο Legendre διαρρέει το DLP parity

Από τον ορισμό: $(\frac{g^x}{p}) = (g^x)^{\frac{p-1}{2}}$

Όμως: $g^{p-1} = 1 \pmod{p}$

Άρα: $g^{\frac{p-1}{2}} = -1 \pmod{p}$

Δηλαδή: $(\frac{g^x}{p}) = (-1)^x$

Αν x μονός τότε $(\frac{g^x}{p}) = -1$ ($g^x \notin QR$)

Αν x ζυγός τότε $(\frac{g^x}{p}) = 1$ ($g^x \in QR$)

Δυσκολία DDHP II

Για τυχαία τριάδα $Prob[(\frac{g^c}{p}) = 1] = \frac{1}{2}$ ανεξάρτητο από τα $(\frac{g^a}{p}), (\frac{g^b}{p})$

Για τριάδα DH: $Prob[(\frac{g^{ab}}{p}) = 1] = \frac{3}{4}$

Ο αλγόριθμος

Υπολόγισε $(\frac{g^a}{p}), (\frac{g^b}{p}), (\frac{g^c}{p})$

Αν $(\frac{g^c}{p}) = 1$ και $((\frac{g^a}{p}) = 1 \text{ ή } (\frac{g^b}{p}) = 1)$ τότε

Επιστροφή "Diffie Hellman"

Αλλιώς

Επιστροφή "Τυχαία"

Πλεονέκτημα: $\frac{3}{8}$ (γιατί;)

ΜΗ ΑΜΕΛΗΤΕΟ

Επιλογή του \mathbb{G}

Συνέπειες

Δουλεύουμε σε μεγάλη υποομάδα του \mathbb{Z}_p^* με τάξη πρώτο q

Για παράδειγμα:

Επιλογή safe prime: $p = 2q + 1$ με q πρώτο

Δουλεύουμε στην υποομάδα τετραγωνικών υπολοίπων τάξης q

Επιλογή schnorr primes $p = k \cdot q + 1$ με q πρώτο

Παρ' όλα αυτά: Υποεκθετικοί αλγόριθμοι (index calculus)

Μεγέθη

Symmetric Security	$ p $	$ q $
80 bits	1024	160
112 bits	2048	224
128 bits	3072	256

Εναλλακτικά: Ελλειπτικές καμπύλες

Ορισμός ElGamal

Δημιουργία Κλειδιών: $KeyGen(1^\lambda) = (y = g^x, x)$

- Επιλογή δύο μεγάλων πρώτων p, q ώστε $q \mid (p - 1)$
- \mathbb{G} υποομάδα τάξης q του \mathbb{Z}_p^* - γεννήτορας g
- Ιδιωτικό κλειδί: τυχαίο $x \in \mathbb{Z}_q$
- Δημόσιο κλειδί: $y = g^x \bmod p$
- Επιστροφή (y, x)

Κρυπτογράφηση

- Επιλογή τυχαίου $r \in \mathbb{Z}_q$
- $Encrypt_y(r, m) = (g^r \bmod p, m \cdot y^r \bmod p)$

Αποκρυπτογράφηση

- $Decrypt_x(a, b) = \frac{b}{a^x}$

Ορθότητα

$$Decrypt_x(Encrypt_y(r, m)) = \frac{m y^r}{(g^r)^x} = m$$

Πιθανοτική Κρυπτογράφηση: Ένα μήνυμα έχει πολλά πιθανά κρυπτοκείμενα

Message expansion Κρυπτοκείμενο διπλάσιο του μηνύματος

Επιτάχυνση Κρυπτογράφησης

Κόστος: 2 υψώσεις σε δύναμη - 1 πολλαπλασιασμός
Ύψωση σε δύναμη: Δεν εξαρτάται από το μήνυμα
(precomputation)

Ασφάλεια Κρυπτογράφησης

Μυστικότητα ElGamal \equiv CDHP

Αντιστοιχία δημοσίων στοιχείων

$$\begin{aligned}g^{x_1} &\equiv g^r \\g^{x_2} &\equiv y = g^x \\g^{x_1 x_2} &\equiv y^r\end{aligned}$$

$EG \leq CDHP$ Υπολογισμός $g^{x_1 x_2} \rightarrow$ αποκρυπτογράφηση (με εύρεση αντιστρόφου)

$CDHP \leq EG$ αποκρυπτογράφηση (g^r, b) (χωρίς το κλειδί) \rightarrow υπολογισμός $\frac{b}{m} \rightarrow$ επίλυση CDFH

Επανάληψη τυχειότητας → Επίθεση ΚΡΑ

ΚΡΑ: Γνωρίζουμε ζεύγη μηνυμάτων - κρυπτοκειμένου για τα οποία έχει χρησιμοποιηθεί η ίδια τυχειότητα

Επίθεση

$$(c_r, c_1) = \text{Encrypt}_y(r, m_1) = (g^r \bmod p, m_1 \cdot y^r \bmod p)$$

$$(c_r, c_2) = \text{Encrypt}_y(r, m_2) = (g^r \bmod p, m_2 \cdot y^r \bmod p)$$

Αν γνωρίζω το (m_1, c_1) : $c_1 = m_1 \cdot y^r \bmod p \Rightarrow y^r = c_1 \cdot m_1^{-1}$

Μπορώ να υπολογίσω το m_2 ως: $m_2 = \frac{c_2}{y^r} = \frac{c_2}{c_1 \cdot m_1^{-1}}$

Ασφάλεια σε επιθέσεις CPA I

Θεώρημα

Αν το DDHP είναι δύσκολο, τότε το κρυπτοσύστημα El Gamal διαθέτει ασφάλεια IND-CPA.

Απόδειξη:

Έστω ότι το ElGamal δεν διαθέτει ασφάλεια IND-CPA.

Άρα $\exists \mathcal{A}$, ο οποίος μπορεί να νικήσει στο παιχνίδι CPA με μη αμελητέα πιθανότητα.

Κατασκευή \mathcal{B} :

- Είσοδος: τριάδα στοιχείων
- Εσωτερικά: Προσομοίωση του \mathcal{C} στο παιχνίδι CPA και χρήση \mathcal{A}
- Αποτέλεσμα: Ξεχωρίζει DH τριάδα από τυχαία

Ασφάλεια σε επιθέσεις CPA II

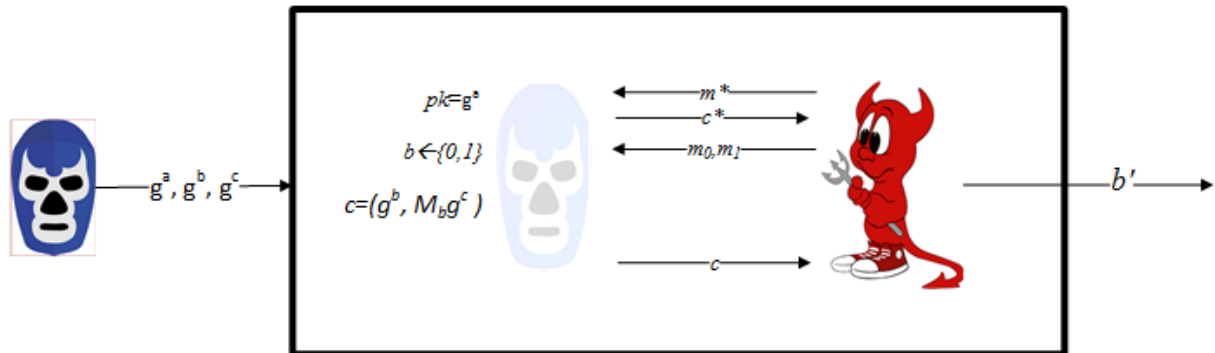
- Είσοδος: g^α, g^β, g^c
- Στο CPA-GAME δημόσιο κλειδί $y = g^\alpha$
- Ο \mathcal{B} απαντά στις κρυπτογραφήσεις του \mathcal{A}
- Όταν ο \mathcal{A} προκαλέσει με δύο μηνύματα
 - ο \mathcal{C} διαλέγει τυχαίο $bit \in \{0, 1\}$,
 - κρυπτογραφεί το M_b με τυχαιότητα το g^β και πολλαπλασιάζει με g^c
 - Τελικά στέλνει το: $(g^\beta, M_b \cdot g^c)$
- Ο \mathcal{A} επιστρέφει την τιμή του bit^*
- Ο \mathcal{B} εξάγει το bit^*

Ασφάλεια σε επιθέσεις CPA III

Ανάλυση

- Για τριάδα DH: $g^c = (g^\alpha)^\beta = y^\beta$
- ο \mathcal{A} θα λάβει ένα έγκυρο κρυπτοκείμενο ElGamal.
- Η πιθανότητα να μαντέψει σωστά είναι τουλάχιστον: $1/2 + \text{non-negl}(\lambda)$.
- Για τυχαία τριάδα: ο \mathcal{A} θα πρέπει να μαντέψει τυχαία
- Πιθανότητα επιτυχίας: $\frac{1}{2}$.
- Τελική πιθανότητα επιτυχίας για \mathcal{B} τουλάχιστον $\text{non-negl}(\lambda)$
- Μπορεί να ξεχωρίσει μία DH τριάδα από μία τυχαία με μη αμελητέα πιθανότητα.

Ασφάλεια σε επιθέσεις CPA IV



Ομομορφικές Ιδιότητες I

Πολλαπλασιαστικός Ομομορφισμός

$$\begin{aligned} \text{Encrypt}_y(r_1, m_1) \cdot \text{Encrypt}_y(r_2, m_2) &= \\ (g_1^{r_1}, m_1 y^{r_1}) \cdot (g_2^{r_2}, m_2 y^{r_2}) &= \\ (g^{r_1+r_2}, (m_1 \cdot m_2) \cdot y^{r_1+r_2}) &= \\ \text{Encrypt}_y(r_1 + r_2, m_1 m_2) & \end{aligned}$$

Ομομορφικές Ιδιότητες II

Reencryption

$$\begin{aligned}\text{Encrypt}_y(r_1, m) \cdot \text{Encrypt}_y(r_2, 1) &= \\ (g^{r_1}, my^{r_1}) \cdot (g^{r_2}, y^{r_2}) &= \\ (g^{r_1+r_2}, my^{r_1+r_2}) &= \text{Encrypt}_y(r_1 + r_2, m)\end{aligned}$$

Αλλαγή της τυχαιότητας - Αλλαγή της μορφής του μηνύματος
...χωρίς γνώση του ιδιωτικού κλειδιού
Malleability

Ομομορφικές Ιδιότητες III

Προσθετικός Ομομορφισμός - Εκθετικό ElGamal

Κρυπτογράφηση του g^m

$$\text{Encrypt}_y(, r, m) = (g^r, g^m y^r)$$

$$\begin{aligned}\text{Encrypt}_y(r_1, m_1) \cdot \text{Encrypt}_y(r_2, m_2) &= \\ (g^{r_1}, g^{m_1} y^{r_1}) \cdot (g^{r_2}, g^{m_2} y^{r_2}) &= \\ (g^{r_1+r_2}, g^{m_1+m_2} \cdot y^{r_1+r_2}) &= \\ \text{Encrypt}_y(r_1 + r_2, (m_1 + m_2))\end{aligned}$$

Αποκρυπτογράφηση: Λαμβάνουμε το g^m
Επίλυση 'εύκολου' διακριτού λογαρίθμου.

Το παραδοσιακό ElGamal δεν διαθέτει CCA-security

Έστω ότι ο \mathcal{A} μπορεί να αποκρυπτογραφήσει μηνύματα επιλογής του, εκτός του c .

- Στόχος: Αποκρυπτογράφηση του $c = (G, M) = (g^r, m_b y^r)$
- Κατασκευή
 $c' = (G', M') = (G \cdot g^{r'}, M \cdot a y^{r'}) = (g^{r+r'}, a \cdot m_b \cdot y^{r+r'})$, όπου a επιλέγεται από τον \mathcal{A}
- Η αποκρυπτογράφηση του M' ($\frac{M'}{G'^x}$) δίνει το $a m_b$ και κατά συνέπεια το m_b
- Αν $m_b = m_0$ επιστρέφει $b^* = 0$ αλλιώς επιστρέφει $b^* = 1$

ElGamal CCA2: Cramer-Shoup cryptosystem I

- Ronald Cramer, Victor Shoup, Crypto 1998
- Επέκταση του ElGamal
- Χρήση συνάρτησης σύνοψης \mathcal{H} με collision resistance (δεν είναι απαραίτητη)
- Αν ισχύει η υπόθεση DDH, τότε παρέχει IND-CCA2

EIGamal CCA2: Cramer-Shoup cryptosystem II

Δημιουργία Κλειδιών

- Επιλογή πρώτων p, q με $p = 2q + 1$
- G είναι η υποομάδα τάξης q στο \mathbb{Z}_p^*
- Επιλογή random generators g_1, g_2
- Επιλογή τυχαίων στοιχείων $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$
- Υπολογισμός
 - $c = g_1^{x_1} g_2^{x_2}$
 - $d = g_1^{y_1} g_2^{y_2}$
 - $h = g_1^z$
- Δημόσιο Κλειδί: (c, d, h)
- Μυστικό Κλειδί: (x_1, x_2, y_1, y_2, z)

EIGamal CCA2: Cramer-Shoup cryptosystem III

Κρυπτογράφηση

- Κωδικοποίηση μηνύματος m στο G
- Επιλογή τυχαίου $r \in \mathbb{Z}_q$
- Υπολογισμός
 - $u_1 = g_1^r, u_2 = g_2^r$
 - $e = mh^r$
 - $\alpha = \mathcal{H}(u_1 || u_2 || e)$
 - $v = c^r d^{r\alpha}$
- Κρυπτογράφημα: (u_1, u_2, e, v)

EIGamal CCA2: Cramer-Shoup cryptosystem IV

Αποκρυπτογράφηση

- Υπολογισμός $\alpha = \mathcal{H}(u_1 || u_2 || e)$
- Έλεγχος αν $u_1^{x_1} u_2^{x_2} (u_1^{y_1} u_2^{y_2})^\alpha = v$. Σε περίπτωση αποτυχίας έξοδος χωρίς αποκρυπτογράφηση
- Σε περίπτωση επιτυχίας υπολογισμός $m = \frac{e}{u_1^z}$

EIGamal CCA2: Cramer-Shoup cryptosystem V

Ορθότητα

$$\frac{e}{u_1^z} = \frac{mh^r}{u_1^z} = m \cdot \frac{g_1^{zr}}{g_1^{rz}} = m$$

- h, z αντιστοιχούν σε δημόσιο - ιδιωτικό κλειδί EIGamal
- u_1, e αντιστοιχούν στο κρυπτογράφημα του EIGamal

Παρατηρήσεις

- u_2, v λειτουργούν ως έλεγχος ακεραιότητας, ώστε να μπορεί να αποφευχθεί το malleability
- Διπλάσια πολυπλοκότητα από EIGamal τόσο σε μέγεθος κρυπτοκειμένου, όσο και σε υπολογιστικές απαιτήσεις

DLP-based Commitment Schemes

Coin Flipping over the telephone

- Η Alice και ο Bob διαφωνούν (τηλεφωνικά) για το πού θα πάνε
- Αποφασίζουν να ρίξουν δύο νομίσματα (απομακρυσμένα)
- Ίδιο αποτέλεσμα: διαλέγει η Alice
- Διαφορετικό Αποτέλεσμα: διαλέγει ο Bob
- Προβλήματα;

DLP-based Commitment Schemes

Λύση: Commitment Schemes

- Ιδιότητες
 - **Hiding** - Προστατεύει αποστολέα - καθώς δεν μπορεί να διαρρεύσει η τιμή του
 - **Binding** - Προστατεύει παραλήπτη - καθώς ο αποστολέας δεν μπορεί να αλλάξει την τιμή του εκ των υστέρων
- Χρήση randomisation για προστασία από brute-force επιθέσεις

Pedersen commitment

- Επιλογή ομάδας με δύσκολο DLP από TTP
 - Επιλογή πρώτου q ώστε $p = 2q + 1$ πρώτος
 - $\mathbb{G} = \langle g \rangle$ υπομάδα τάξης q του \mathbb{Z}_p^*
 - Επιλογή $x \in \mathbb{Z}_q$ και $h = g^x$
 - Δημοσιοποίηση g, \mathbb{G}, p, q, h
- Δέσμευση: $c = \text{commit}(m, r) = g^m \cdot h^r \bmod p$
- Αποκάλυψη: Αποστολή m, r
- Επαλήθευση: $c \stackrel{?}{=} g^m \cdot h^r$

Ιδιότητες I

Information Theoretically Hiding

$$c = g^m \cdot h^r \bmod p = g^{m+xr} \bmod p$$

Ακόμα και ένας παντοδύναμος αντίπαλος να μπορεί να λύσει το DLP θα έχει μία εξίσωση της μορφής

$$d = m + xr \pmod{q}$$

(2 άγνωστοι m, r - 1 εξίσωση)

Computationally Binding αν το DLP είναι δύσκολο

Έστω $c = \text{commit}(m, r) = \text{commit}(m', r')$ με $m \neq m'$

$$\begin{aligned}g^m \cdot h^r &= g^{m'} \cdot h^{r'} \Rightarrow \\g^{m+xr} &= g^{m'+xr'} \Rightarrow \\m + xr &= m' + xr' \pmod{q} \Rightarrow \\x &= \frac{m' - m}{r - r'}\end{aligned}$$

ΑΤΟΠΟ

Ελλειπτικές καμπύλες

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο (200 έτη)
 - Κρυπτογραφία: 80s
 - Βασίζονται στο πρόβλημα DLP
 - Αντικατάσταση του \mathbb{Z}_p με σημεία τους
 - Μόνο γενικευμένοι αλγόριθμοι DLP $O(2^{\frac{\lambda}{2}})$ - όχι υποεκθετικοί
 - Ίδια επίπεδα ασφάλειας με μικρότερη παράμετρο ασφάλειας και καλύτερη απόδοση
- | | |
|------|-----|
| RSA | EC |
| 1024 | 160 |
| 2048 | 224 |
| 3072 | 256 |

Γενική μορφή

Έστω \mathbb{F} ένα σώμα.

Ορισμός $\mathcal{E}(\mathbb{F})$

Μια ελλειπτική καμπύλη \mathcal{E} πάνω από το \mathbb{F} είναι το σύνολο των σημείων $(x, y) \in \mathbb{F}$, που ικανοποιούν την εξίσωση Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

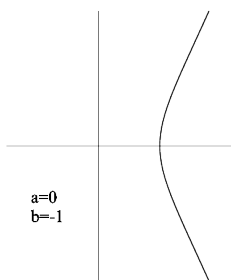
$$a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{F}$$

και ένα στοιχείο \mathcal{O} , - σημείο στο άπειρο

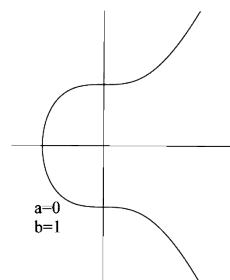
Πρακτικά

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}$$

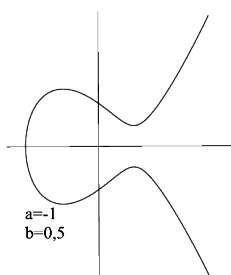
Ελλειπτικές καμπύλες στο \mathbb{R} I



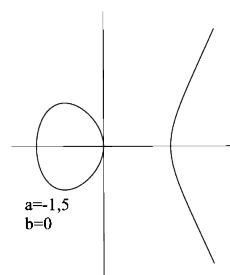
$$y^2 = x^3 - 1$$



$$y^2 = x^3 + 1$$



$$y^2 = x^3 - x + \frac{1}{2}$$



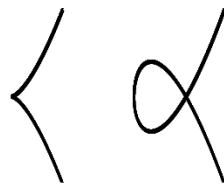
$$y^2 = x^3 - \frac{3}{2}x$$

Ελλειπτικές καμπύλες στο \mathbb{R} II

Παρατηρήσεις:

- Συμμετρία ως προς άξονα x
- Συμπίεση σημείου $(x, 0)$ ή $(x, 1)$ για πάνω ή κάτω από τον άξονα των x

Προς αποφυγή Singular καμπύλες: Πολλαπλές ρίζες, σημεία τομής



Πρέπει $4a^3 + 27b^2 \neq 0$

Αντίθετο Σημείου

P σημείο στην $\mathcal{E}(\mathbb{R})$.

Το αντίθετο σημείο $-P$

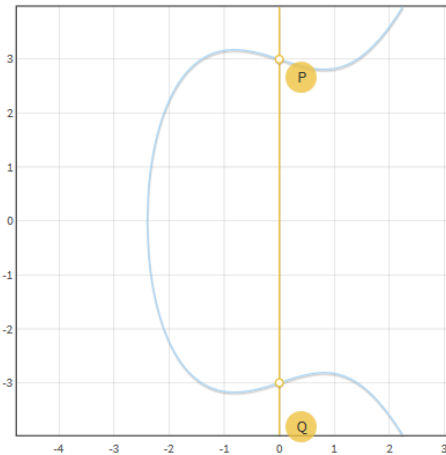
- 1 Αν $P = \mathcal{O}$, τότε $-P = \mathcal{O}$
- 2 Αλλιώς αν $P = (x, y)$ τότε $-P = (x, -y)$
(ανήκει στην \mathcal{E} λόγω συμμετρίας)

(Γεωμετρική) Πρόσθεση Σημείων I

Το άθροισμα $P + Q$

Αν $P = \mathcal{O}$, τότε $\mathcal{O} + Q = Q$

Αν $Q = -P$, τότε $P + Q = \mathcal{O}$.

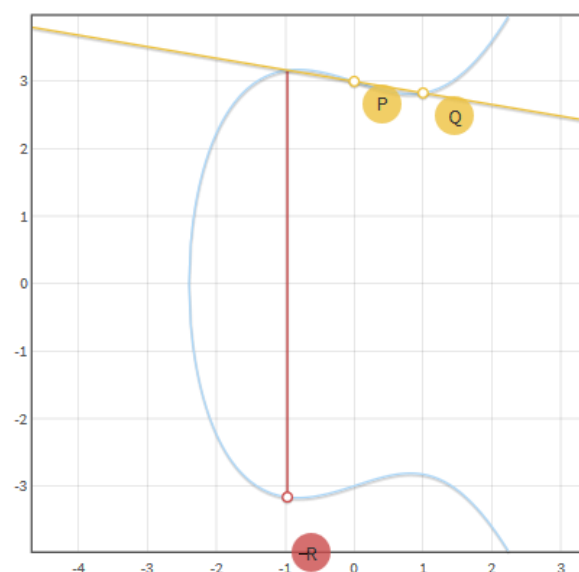


Το σημείο \mathcal{O} . υπάρχει σε **κάθε κατακόρυφη**

(Γεωμετρική) Πρόσθεση Σημείων II

Αν $P \neq Q$ τότε:

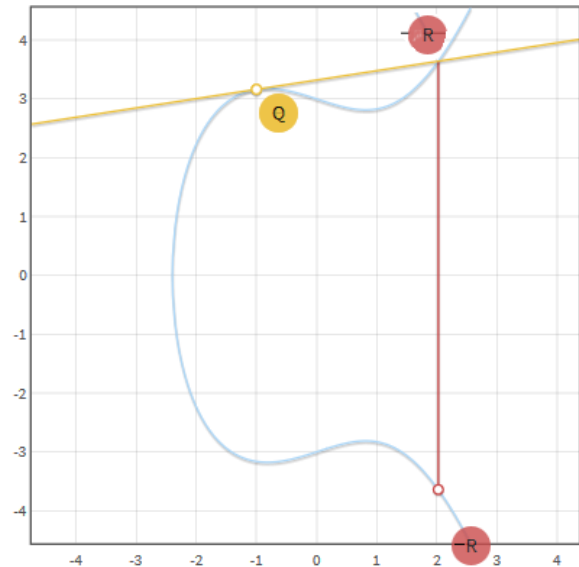
- Θεωρούμε την \overline{PQ}
- Βρίσκουμε το σημείο τομής R με την \mathcal{E} .
- Βρίσκουμε το αντίθετο



(Γεωμετρική) Πρόσθεση Σημείων III

Αν $P = Q$ τότε:

- Θεωρούμε την εφαπτομένη στο P
- Βρίσκουμε το σημείο τομής R με την \mathcal{E} .
- Βρίσκουμε το αντίθετο



Αλγεβρική αναπαράσταση: Τριτοβάθμιες εξισώσεις με συντεταγμένες

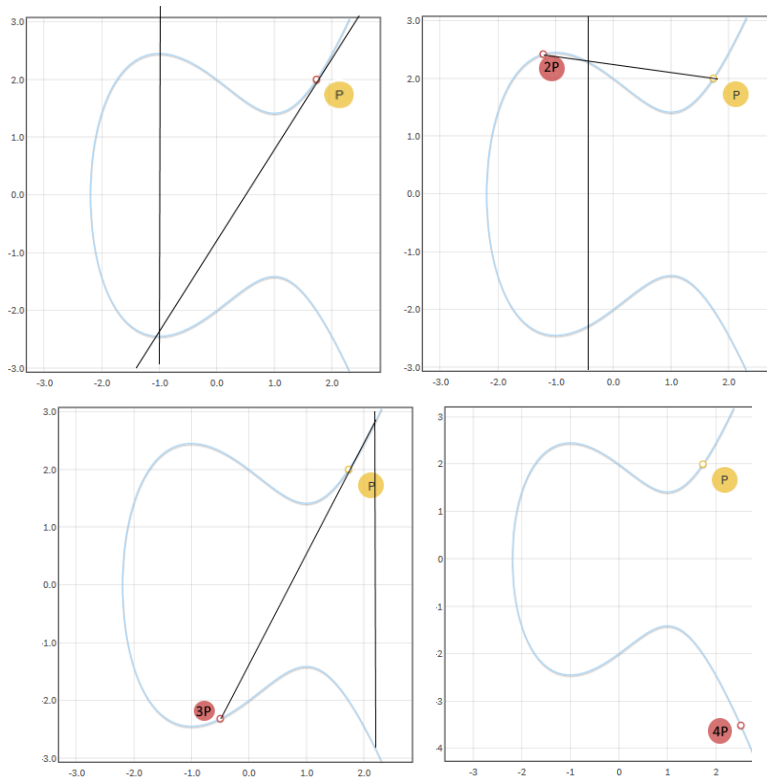
Ομάδα Σημείων Ελλειπτικής καμπύλης

Τα σημεία μιας ελλειπτικής καμπύλης αποτελούν αβελιανή ομάδα ως προς την πρόσθεση

- ουδέτερο στοιχείο \mathcal{O}
- αντίθετο στοιχείο $-P$
- πρόσθεση προσεταιριστική και αντιμεταθετική

Πολλαπλασιασμός σημείου με ακέραιο

$$nP = P + P + \dots + P$$



DLP

Ελλειπτικές κομπύλες

49 / 62

Double and add

Υπολογισμός nP

Απαιτούνται $n - 1$ προσθέσεις

Λύση: Square and multiply - Double and add

$$17P = P + 16P$$

$$2P = P + P$$

$$4P = 2P + 2P$$

$$8P = 4P + 4P$$

$$16P = 8P + 8P$$

DLP

Ελλειπτικές κομπύλες

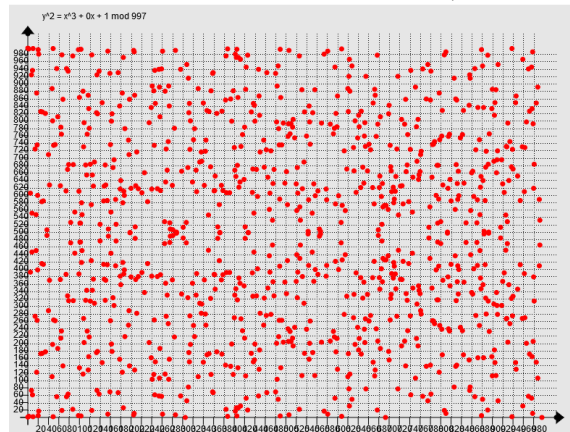
50 / 62

Ελλειπτικές καμπύλες πάνω από το \mathbb{F}_p

Ορισμός $\mathcal{E}(\mathbb{F}_p)$

$$\mathcal{E} = \mathcal{O} \cup \{y^2 = x^3 + ax + b \pmod{p}, \\ (x, y) \in \mathbb{F}_p^2, (a, b) \in \mathbb{F}_p^2 : 4a^3 + 27b^2 \neq 0 \pmod{p}\}$$

Παράδειγμα: $y^2 = x^3 + 1 \pmod{997}$



από [Discrete Elliptic Curve Plotter](#)

DLP

Ελλειπτικές καμπύλες

51 / 62

Η ομάδα των σημείων $\mathcal{E}(\mathbb{F}_p)$ I

Εύρεση τάξης ομάδας

Εκθετικός αλγόριθμος

Δοκιμές όλων των $x \in \{0, \dots, p-1\}$

Έλεγχος ποια ικανοποιούν την εξίσωση της καμπύλης

Θ. Hasse

$$p + 1 - 2\sqrt{p} \leq |\mathcal{E}(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$$

Υπολογισμός: αλγόριθμος Schoof $\in P$ με βελτιώσεις Elkies, Atkin (SEA)

DLP

Ελλειπτικές καμπύλες

52 / 62

Η ομάδα των σημείων $\mathcal{E}(\mathbb{F}_p)$ II

Κυκλικές υποομάδες

Κάθε σημείο μιας καμπύλης $\mathcal{E}(\mathbb{F}_p)$ παράγει μια κυκλική υποομάδα

Υπολογισμός τάξης υποομάδας $\mathcal{E}(\mathbb{F}_p)$

Θεώρημα Lagrange: Η τάξη κάθε υποομάδας διαιρεί την τάξη της ομάδας

Τάξη υποομάδας με σημείο βάσης (γεννήτορα) P

- Εύρεση τάξη ομάδας με αλγόριθμο Schoof
- Εύρεση των διαιρετών της τάξης, d
- Για σημείο βάσης P εύρεση $\min\{d : dP = \mathcal{O}\}$

Η ομάδα των σημείων $\mathcal{E}(\mathbb{F}_p)$ III

Εύρεση σημείων βάσης

Θέλουμε γεννήτορες μεγάλων υποομάδων

- Εύρεση μεγάλου πρώτου $q \mid |\mathcal{E}|$
- Υπολογισμός $h = \frac{|\mathcal{E}|}{q}$
- Επιλογή τυχαίου σημείου P
- Υπολογισμός $G = hP$
- Αν $G = \mathcal{O}$ επανάληψη

Πρόβλημα ECDLP

Δίνονται:

- Μία ελλειπτική καμπύλη \mathcal{E} ορισμένη πάνω από το \mathbb{F}_p ($p, a, b, \#\mathcal{E}$)
- Μία μεγάλη υποομάδα της με τάξη q
- ένα σημείο βάσης G και
- ένα σημείο Y .

Ζητείται: Να βρεθεί, αν υπάρχει, ακέραιος x τέτοιος ώστε $xG = Y$.

Εικασία

Το πρόβλημα ECDLP είναι υπολογιστικά απρόσιτο (όχι σε κάθε καμπύλη)

Ανταλλαγή Κλειδιού ECDH I

Στόχοι

- Κατασκευή κοινού κλειδιού πάνω από δημόσιο κανάλι επικοινωνίας
- Σε EC: Το κοινό κλειδί είναι σημείο της καμπύλης
- Δημόσια επικοινωνία και συμφωνία σε σημείο P μιας ελλειπτικής καμπύλης \mathcal{E}

Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \#\mathcal{E}, q, G)$

Πρωτόκολλο

- Η Alice επιλέγει έναν ακέραιο $a \in \{1, \dots, q-1\}$
- Υπολογίζει το $aG \in \mathcal{E}$ και το δημοσιοποιεί.
- Ο Bob επιλέγει έναν ακέραιο $b \in \{1, \dots, q-1\}$ και δημοσιοποιεί το $bG \in \mathcal{E}$
- Το δημόσιο κλειδί που θα χρησιμοποιούν στη συνέχεια είναι το $P = a(bG) = b(aG) \in \mathcal{E}$

Κρυπτογραφία Δημοσίου Κλειδιού

Παραλλαγή Κρυπτοσυστήματος ElGamal

Δημιουργία κλειδιών

- Δημόσια Διαθέσιμες Παράμετροι: $(p, a, b, \# \mathcal{E}, q, G)$
- Ιδιωτικό κλειδί: Ένας τυχαίος ακέραιος $x \in \{1, \dots, q-1\}$
- Δημόσιο κλειδί: Το σημείο $Y = xG \in \mathcal{E}$

Κρυπτογράφηση

- Κωδικοποίηση μηνύματος ως σημείο P_m της \mathcal{E}
- Επιλέγεται ένας τυχαίος ακέραιος $k \in \{1, \dots, q-1\}$
- Κρυπτογράφημα: $\text{Encrypt}(Y, P_m) = (kG, P_m + kY)$

Αποκρυπτογράφηση

- Υπολογισμός

$$P_m + kY - x(kG) = P_m$$

Κωδικοποίηση μηνύματος σε σημείο

- Hashed Elgamal
 - 1ος τρόπος
 - Χρήση συνάρτησης $\mathcal{H} : \mathcal{E} \Rightarrow \mathcal{M}$
 - Κρυπτογράφηση: $\text{Encrypt}(Y, P_m) = (kG, m \oplus \mathcal{H}(kY))$
 - 2ος τρόπος
 - Επιλογή τυχαίου a και αντικατάσταση των bits χαμηλής τάξης του με το m
 - Επιλογή ενός από τα δύο πιθανά σημεία της καμπύλης

Πρότυπες καμπύλες

Πρότυπο NIST FIPS186-3

15 ελλειπτικές καμπύλες. Για παράδειγμα:

- **NIST P-256** $y^2 = x^3 - 3x + 41\ 058\ 363\ 725\ 152\ 142\ 129\ 326\ 129\ 780\ 047\ 268\ 409\ 114\ 441\ 015\ 993\ 725\ 554\ 835\ 256\ 314\ 039\ 467\ 401\ 291 \pmod{(2^{256} - 2^{224} + 2^{192} + 2^{96} - 1)}$

Χρήση στην γεννήτρια τυχειότητας Dual_EC_DRBG.

- **NIST P-384** $y^2 = x^3 - 3x + 27\ 580\ 193\ 559\ 959\ 705\ 877\ 849\ 011\ 840\ 389\ 048\ 093\ 056\ 905\ 856\ 361\ 568\ 521\ 428\ 707\ 301\ 988\ 689\ 241\ 309\ 860\ 865\ 136\ 260\ 764\ 883\ 745\ 107\ 765\ 439\ 761\ 230\ 575 \pmod{(2^{384} - 2^{128} - 2^{96} + 2^{32} - 1)}$

Φόβοι για υπονόμηση

Εναλλακτικά:

Secp256k1 (OpenSSL, Bitcoin) $y^2 = x^3 + 0x + 7 \pmod{(2^{256} - 2^{32} - 977)}$

Curve25519 (OpenSSH) $y^2 = x^3 + 486662 \cdot x^2 + x \pmod{(2^{255} - 19)}$

Επιλογή Καμπύλης

Το ECDLP δεν είναι δύσκολο σε όλες τις καμπύλες

Δίνεται μια καμπύλη $(p, a, b, \#E, q, G)$

Πρόβλημα: Είναι ασφαλής (;)

Επαληθευσιμότητα

- Επιλογή τυχαίου αριθμού s
- Υπολογισμός $h = \mathcal{H}(s)$
- Παραγωγή των a, b από το h
- Επαληθευσιμο, αλλιώς a, b από αντιστροφή της σύνοψης

Αλλά: Πρέπει το s να είναι πραγματικά τυχαίο!

Nothing up my sleeve

Το s προέρχεται από ψηφία του π , ε,τριγωνομετρικών αριθμών

Βιβλιογραφία I

- St. Zachos and Aris Pagourtzis. Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία. Πανεπιστημιακές Σημειώσεις
- Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography (Chapman and Hall/Crc Cryptography and Network Security Series). Chapman and Hall/CRC, 2007
- Nigel Smart. [Introduction to cryptography](#)
- Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science-Business Media, 2009.
- Kiayias, Aggelos [Cryptography primitives and protocols](#), UoA, 2015
- Dan Boneh, Introduction to cryptography, online course
- Neal Koblitz and Alfred J. Menezes, [A riddle wrapped in an enigma](#)
- Jeremy Kun [Introducing Elliptic Curves](#)
- Andrea Corbellini [Elliptic Curve Cryptography: a gentle introduction](#)
- Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In CRYPTO '91, pages 129–140, 1991
- Victor Shoup [Why chosen ciphertext security matters](#), 1998
- DR Stinson [The Pohlig - Hellman Algorithm](#)