Κρυπτοσυστήματα Διακριτού Λογαρίθμου

Παναγιώτης Γροντάς
ΕΜΠ

Κρυπτογραφία

2025 – 2026

Με βάση παλιότερες διαφάνειες Άρη Παγουρτζή

Περιεχόμενα

Αλγόριθμοι για το DLP

Το πρόβλημα του Διακριτού Λογάριθμου (DLP)

- Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, με τάξη q και στοιχείο $y \in \mathbb{G}$.
- Ζητείται $x \in \mathbb{Z}_q$ ώστε $y = g^x$

Το υπολογιστικό πρόβλημα Diffie-Hellman (CDHP)

- Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, με τάξη q και στοιχεία $g^\alpha, g^\beta \in \mathbb{G}$.
- Να υπολογιστεί το στοιχείο $g^{\alpha\beta}$

Το πρόβλημα απόφασης Diffie-Hellman (DDHP)

- Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, με τάξη q και στοιχεία $g^\alpha, g^\beta \in \mathbb{G}$ και στοιχείο $y \in \mathbb{G}$.
- Να αποφασιστεί αν $g^{\alpha\beta} = y$.

Μια υπενθύμιση

$$DDHP \leq CDHP \leq DLP$$

DLP Random Self-Reducibility

Δίνεται ομάδα $\mathbb{G}$ τάξης q και $g \in \mathbb{G}$. Έστω αλγόριθμος A ώστε:

$$\Pr[A(y) = DL(y) | y \leftarrow_{\$} \mathbb{G}] = \epsilon$$

Υπάρχει αλγόριθμος B τέτοιος ώστε:

$$\forall u \in \mathbb{G}: B(y) \in \{x, \perp\} \wedge \Pr[x = DLP(y)] = \epsilon$$

Ο αλγόριθμος B με είσοδο y δουλεύει ως εξής:

- $\alpha \leftarrow_{\$} \mathbb{Z}_q$
- $y' \leftarrow y \cdot g^{a}$
- $a' \leftarrow A(y')$
- **If** $g^{a'} = y'$ **then return** $a' - a$
- **return** $\perp$

Με $n \cdot \left\lceil \frac{1}{\epsilon} \right\rceil$ επαναλήψεις:

$$\Pr[B(y) = DLP(y)] = 1 - (1 - \epsilon)^{n \cdot \left\lceil \frac{1}{\epsilon} \right\rceil} \geq 1 - e^{-n}$$

Συμπέρασμα:

- Αν το DLP μπορεί να λυθεί για ***τυχαία*** στοιχεία της ομάδας, μπορεί να λυθεί για ***όλα*** τα στοιχεία της ομάδας.
- Η δυσκολία του DLP είναι **ομοιόμορφα** κατανεμημένη στην ομάδα και **δεν** περιορίζεται σε κάποια στιγμιότυπα αποκλειστικά.
- **Δυσκολία μέσης περίπτωσης και όχι μόνο δυσκολία χειρότερης περίπτωσης**
- Κατάλληλο πρόβλημα για κρυπτογραφία
- Κάτι τέτοιο δεν ισχύει για όλα τα NP-hard προβλήματα!

DLP Random Self-Reducibility

Brute-Force Επίλυση DLP

- Γενικευμένος αλγόριθμος – **Δεν εξαρτάται από τα χαρακτηριστικά της ομάδας!**
- Για την κυκλική ομάδα $\mathbb{G} = \langle g \rangle$ υπολογίζω για κάθε $x \in \mathbb{Z}_q$ το ζεύγος (x, g^x)
- Ταξινομώ με βάση το g^x
- Για είσοδο $y \in \mathbb{G}$ - Δυαδική Αναζήτηση μέχρι $y = g^x$
- Αν $|q| = \lambda$ bits τότε η πολυπλοκότητα του αλγορίθμου είναι $O(2^\lambda)$

Βασική ιδέα: Meet in the middle.

Γενικευμένος αλγόριθμος
Time complexity: $O(2^{\lambda/2})$
Space complexity: $O(2^{\lambda/2})$

1. Παρατήρηση: $\forall x \in \mathbb{Z}: \exists (k, a, b): x = ak + b$
2. $y = g^x = g^{ak+b} = g^{ak} g^b \Rightarrow g^b = y g^{-ak}$
3. Θα υπολογίζουμε τα $g^b, y g^{-ak}$ ανεξάρτητα μέχρι να συναντηθούν
    1. Ξεκινάμε από $k = \lceil \sqrt{q} \rceil$ (στη μέση)
    2. Baby steps (μέγεθος 1): $\left[g^b | b \in [0, \cdots, k-1] \right]$
    3. Giant steps (μέγεθος k): $y g^{-ak}: a \in [0, \cdots, k-1]$ και αναζήτηση στη λίστα $[g^b]$
    4. Όταν το βρούμε: $x = a^* k + b^*$

Αλγόριθμος Shanks (Baby Step – Giant Step)

Θέλουμε να βρούμε το $2^x = 17$ στην ομάδα $\mathbb{Z}_{29}^* = \langle 2 \rangle . k = \lceil \sqrt{28} \rceil = 6$

- $b \in [0 \cdots 5]$
- $2^0 = 1 \ (mod\ 29)$
- $2^1 = 2 \ (mod\ 29)$
- $2^2 = 4 \ (mod\ 29)$
- $2^3 = 8 \ (mod\ 29)$
- $2^4 = 16 \ (mod\ 29)$
- $2^5 = 3 \ (mod\ 29)$

- $a \in [0 \cdots 5]$
- $17 \cdot 2^{-0 \cdot 6} = 17 \ (mod\ 29)$
- $17 \cdot 2^{-1 \cdot 6} = 27 \ (mod\ 29)$
- $17 \cdot 2^{-2 \cdot 6} = 19 \ (mod\ 29)$
- $17 \cdot 2^{-3 \cdot 6} = 8 \ \ (mod\ 29)$ βρέθηκε

$$\boldsymbol{x = 6 \cdot 3 + 3 = 21}$$

Αλγόριθμος Shanks - Παράδειγμα (Baby Step – Giant Step)

Βασική ιδέα: Η δυσκολία του DLP σε μια ομάδα, εξαρτάται από τη δυσκολία του στις υποομάδες της. **Πώς:**

- **Παραγοντοποίηση της τάξης:** $q = \prod_i p_i^{e_i}$ *(όχι κατ' ανάγκη πλήρης).*
- **Προκύπτουν υποομάδες τάξης** $\frac{q}{p_i^{e_i}}$
- **Επίλυση μικρότερου DLP σε κάθε μία από αυτές**
  - Μας δίνει $x_i \ (mod\ p_i^{e_i})$
- **Συνδυασμός με CRT**

Αν η τάξη της ομάδας μπορεί να παραγοντοποιηθεί σε $B - smooth$ πρώτους (μικρότερους από κάποιο B δηλ), τότε το DLP γίνεται αρκετά πιο εύκολο.

Για ασφάλεια θέλουμε τάξη μεγάλο πρώτο.

Αλγόριθμος Pohlig - Hellman

1. Παραγοντοποιούμε την τάξη $q = \prod_i p_i^{e_i}$
2. Για κάθε p_i αναλύουμε το $x = x_0 + x_1 p_i + \cdots + x_{e_i-1} p_i^{e_i-1} \ (mod\ p_i^{e_i})$
3. Πρέπει να υπολογίσουμε τα $x_j, j \in [0 \cdots e_i - 1]$. Ακολουθούμε την παρακάτω επαναληπτική διαδικασία:
4. $y^{q/p_i} = (g^x)^{q/p_i} = \left(g^{x_0 + x_1 p_i + \cdots + x_{e_i-1} p_i^{e_i-1}}\right)^{q/p_i} = (g^{x_0 + k p_i})^{q/p_i} = g^{\frac{x_0 q}{p_i}}$
5. Υπολογίζουμε το x_0 με αλγόριθμο Shanks

Αλγόριθμος Pohlig - Hellman

Γενικεύουμε για υπολογισμό x_j:

- Δημιουργούμε ακολουθία y_j με $y_0 = y$ και
- Ορίζουμε: $y_j = y_{j-1}\, g^{-x_0 - x_1 p_i - \cdots - x_{j-1} p_i^{j-1}} \quad (j = 1, \dots)$
- $y_j^{q/p_i^{j+1}} = \left(g^{x - x_0 - x_1 p_i - \cdots - x_{j-1} p_i^{j-1}}\right)^{q/p_i^{j+1}} =$

  $\left(g^{x_j p_i^j + \cdots + x_{e_i - 1} p_i^{e_i - 1}}\right)^{q/p_i^{j+1}} = (g^{x_j p_i^j + k p_i^{j+1}})^{q/p_i^{j+1}} = g^{\frac{x_j q}{p_i}}$
- Υπολογίζουμε κάθε x_j
- Συνδυάζουμε με **CRT**.

Αλγόριθμος Pohlig - Hellman

Αλγόριθμος Pohlig – Hellman (Παράδειγμα)

- Θέλουμε να βρούμε το $2^x = 17$ στην ομάδα $\mathbb{Z}_{29}^* = \langle 2 \rangle$
- **Παραγοντοποιούμε** την τάξη: $29 = 2^2 7$
  - $x_2 = x_{20} + 2x_{21}\ (mod\ 4)$
  - $x_7 = x_{70}\ (mod\ 7)$
- **Υπολογισμός** x_{20}
  - $y^{q/2} = g^{x_{20} q/2} \Rightarrow 17^{28/2} = 2^{\frac{x_{20} 28}{2}} \Rightarrow 17^{14} = 2^{14 x_{20}} \Rightarrow 2^{14 x_{20}} = -1 \Rightarrow x_{20} = 1\ (mod\ 4)$
- **Υπολογισμός** x_{21}
  - $y_1 = \mathrm{yg}^{-\mathrm{x}_{20}} = 17 \cdot 2^{-1} = 17 \cdot 15 = 23\ (mod\ 29)$
  - $y_1^{q/4} = g^{x_{21} q/4} \Rightarrow 23^7 = 2^{14 x_{21}} \Rightarrow 1 = 2^{14 x_{21}} \Rightarrow x_{21} = 0\ (mod\ 4)$
- **Υπολογισμός** $\boldsymbol{x_2}$
  - $x_2 = x_{20} + 2x_{21}\ (mod\ 4) = 1\ (mod\ 4)$

- **Υπολογισμός** x_{70}
  - $y^{q/7} = g^{x_{70}q/7} \Rightarrow 17^{28/7} = 2^{\frac{x_{70}28}{7}} \Rightarrow 17^4 = 2^{4x_{70}} \Rightarrow 2^{4x_{70}} = 1$
    $\Rightarrow x_{70} = 0\ (mod\ 7)$
- **Εφαρμογή CRT**
  - $x_2 = 1\ (mod\ 4)$
  - $x_7 = 0\ (mod\ 7)$
  - $x = 21\ (mod\ 28)$

Αλγόριθμος Pohlig – Hellman (Παράδειγμα)

Αλγόριθμοι index calculus

- Οικογένεια πιθανοτικών αλγορίθμων που ισχύουν κυρίως στο $\mathbb{Z}_p^*$ για p πρώτο και σε λίγες περιπτώσεις ελλειπτικών καμπυλών
  - Χρειάζεται την έννοια του πρώτου.
  - Υποεκθετική πολυπλοκότητα – εξαρτάται από αλγόριθμο παραγοντοποίησης
- **Δημιουργοί:** Kraitchik (1922), Western and Miller (1968), Odlyzko (1984), Pomerance (1987)
- **Βασική ιδέα:**
  - Παραγοντοποιούμε στοιχεία της ομάδας.
  - Κάποιοι μικροί πρώτοι θα εμφανίζονται αρκετά συχνά στις παραγοντοποιήσεις.
  - Μπορούμε να βρούμε τους διακριτούς λογαρίθμους αυτών των πρώτων
  - Με συνδυασμό τους βρίσκουμε τον ζητούμενο διακριτό λογάριθμο

Είσοδος: Factor base - k μικροί πρώτοι $\{p_1, \cdots, p_k\}$ ή εναλλακτικά ένας ακέραιος B από τον οποίο υπολογίζουμε το factor base $(p_1, \cdots, p_k < B)$

Λειτουργία:

1. Εύρεση $l > k$ τιμών $\{x_1, \cdots, x_l\}$ ώστε $g_i = g^{x_i} \ (mod\ p)$ να είναι B −smooth.
2. Προκύπτουν l σχέσεις:

$$\left\{ g^{x_i} = \prod_{i=1\cdots k} p_i^{e_{il}} \ (mod\ p) \Rightarrow x_i = \sum_{i=1\cdots k} e_{il} \cdot \log_g p_i \ (mod\ p-1) \right\}_{i=1}^{l}$$

3. Επιλέγω ομοιόμορφα $\alpha \leftarrow \mathbb{Z}_{p-1}^*$ ώστε yg^a να είναι B −smooth

$$yg^a = \prod_{i=1\cdots k} p_i^{e_{il}} \ (mod\ p) \Rightarrow \alpha + x = \sum_{i=1\cdots k} e_{il} \cdot \log_g p_i \ (mod\ p-1)$$

- Επίλυση $l+1$ εξισώσεων με $\kappa + 1$ αγνώστους. Εύρεση x

Αλγόριθμοι index calculus

Παράδειγμα: Θέλουμε να βρούμε το $2^x = 17$ στην ομάδα $\mathbb{Z}_{29}^*$

Είσοδος: Οι μικροί πρώτοι $\{2, 3, 5, 7\}$

Επιλέγω x_i ώστε το 2^{x_i} να έχει παράγοντες στους πρώτους

- $2^1 = 2\ (mod\ 29) \Rightarrow x_1 = 1$
- $2^5 = 3\ (mod\ 29) \Rightarrow x_2 = 5$
- $2^{12} = 7\ (mod\ 29) \Rightarrow x_3 = 12$
- $2^{22} = 5\ (mod\ 29) \Rightarrow x_4 = 22$

Επιλέγω α ώστε το $2^\alpha \cdot 17$ να παραγοντοποιείται στο factor base

$$17 \cdot 2^1 = 5\ (mod\ 29) \Rightarrow \log_2 17 + \log_2 2 = \log_2 5\ (mod\ 28) \Rightarrow$$
$$x = 22 - 1\ (mod\ 28) \Rightarrow$$
$$\boldsymbol{x = 21}$$

Αλγόριθμοι index calculus

Ομάδες για κρυπτοσυστήματα DLP

Το DDHP δεν είναι δύσκολο στην $\mathbb{Z}_p^*$ με p πρώτο

Απόδειξη:

Θα κατασκευάσουμε **αποδοτικό** αλγόριθμο που μπορεί να ξεχωρίζει τις τριάδες (g^a, g^b, g^{ab}) και (g^a, g^b, g^c) με **μη αμελητέα** πιθανότητα χρησιμοποιώντας το σύμβολο **Legendre**.

Παρατήρηση:

Το σύμβολο **Legendre** διαρρέει το DL parity. $\left(\frac{g^x}{p}\right) = (\mathrm{g}^{\mathrm{x}})^{\frac{p-1}{2}}$

$(\mathrm{g}^{\mathrm{x}})^{\frac{p-1}{2}} = (-1)^{\mathrm{x}}$ αφού $\mathrm{g}^{\frac{p-1}{2}} = -1\ (mod\ p)$ καθώς λόγω Θ. Fermat: $\mathrm{g}^{p-1} = 1(mod\ p)$

Αν x **μονός** τότε: $\left(\frac{g^x}{p}\right) = -1$

Αν x **ζυγός** τότε: $\left(\frac{g^x}{p}\right) = 1$

Η $\mathbb{Z}_p^*$ με p πρώτο είναι ακατάλληλη

Το DDHP δεν είναι δύσκολο στην $\mathbb{Z}_p^*$ με p πρώτο

Αν (g^a, g^b, g^c) είναι τυχαία τριάδα: $\Pr\left[\left(\frac{g^c}{p}\right) = 1\right] = \frac{1}{2}$

Αν (g^a, g^b, g^{ab}) είναι τριάδα DH: $\Pr\left[\left(\frac{g^{ab}}{p}\right) = 1\right] = \frac{3}{4}$

Πλεονέκτημα: $\left|\frac{3}{4} - \frac{1}{2}\right| = \frac{1}{4}$

Μπορώ και καλύτερα αν χρησιμοποιήσω το πλήρες transcript

Αλγόριθμος διαχωρισμού

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

If $\left(\frac{g^c}{p}\right) = 1$ **and** $\left(\left(\frac{g^a}{p}\right) = 1$ **or** $\left(\frac{g^b}{p}\right) = 1\right)$

```
then
   return ‘DH’
else
   return ‘Random’
```

Πλεονέκτημα: $\frac{3}{8}$ (γιατί?)

Η $\mathbb{Z}_p^*$ με p πρώτο είναι ακατάλληλη

Ελλειπτικές καμπύλες

- ‘Λογάριθμος’ αφορά πρόσθεση σημείων
- Δεν υπάρχει η έννοια του πρώτου
- ίδια επίπεδα ασφάλειας με μικρότερο μέγεθος κλειδιών

Υποομάδα πρώτης τάξης q του $\mathbb{Z}_p^*$ με p πρώτο

- safe prime $p = 2q + 1$ *ή* Schnorr prime: $p = kq + 1$ με q πρώτο
- Υποομάδα τετραγωνικών υπολοίπων του $\mathbb{Z}_p^*$

Λόγοι:

- Όχι εύκολο DDHP
- Εύκολη εύρεση γεννήτορα
- Μεγάλη υποομάδα τάξης q

Όμως: Ευάλωτες στον υποεκθετικό index calculus

Επιλογή ομάδας

Ελλειπτικές καμπύλες (EC)

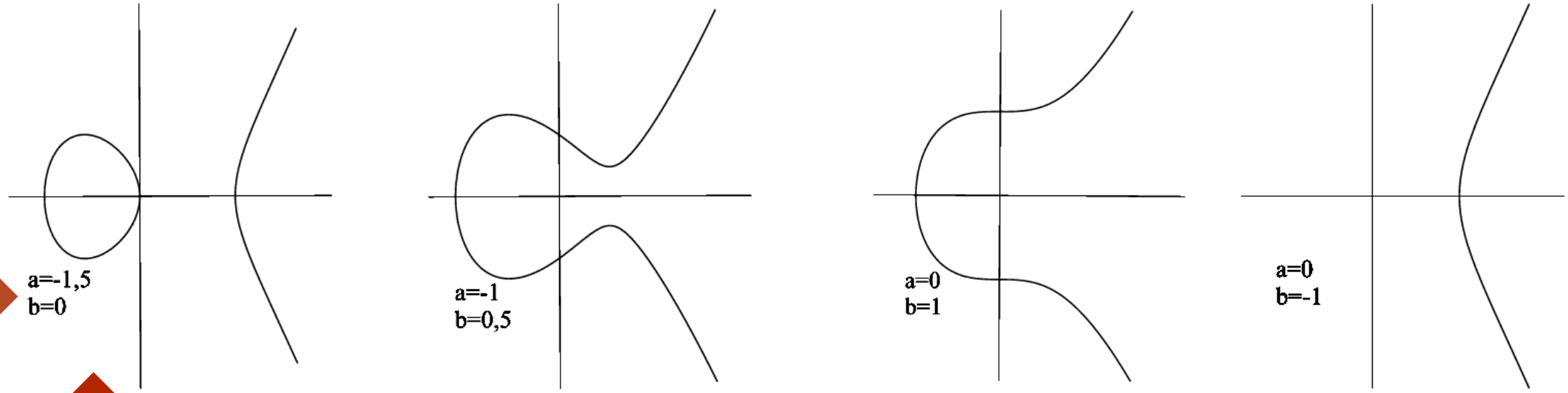
- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
  - Πρώτη εμφάνιση: 3ος πΧ αιώνας – Διόφαντος αναζήτηση ρητών ριζών της $y^2 = x^3 - x + 9$
  - Εκτενής μελέτη εδώ και 300 χρόνια
- Εφαρμογή στην Κρυπτογραφία: 80s (Neil Koblitz, Victor Miller)
- Επαναπροσδιορισμός του προβλήματος διακριτού λογάριθμου
  - Στοιχεία ομάδας – σημεία της καμπύλης
  - **Γενικευμένοι αλγόριθμοι μόνο (όχι index calculus).**
  - Ίδια επίπεδα ασφάλειας με μικρότερα κλειδιά και καλύτερη απόδοση!
    - Ενδεικτικά: **RSA** κλειδί **3072** bits παρέχει ίδια ασφάλεια με **EC** κλειδί **256** bits.

Έστω $\mathbb{F}$ ένα σώμα.

Μια ελλειπτική καμπύλη $\mathcal{E}(\mathbb{F})$ είναι το σύνολο των σημείων (x, y) που ικανοποιούν την εξίσωση: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + \alpha_6$ με $\alpha_1, \alpha_3, \alpha_2, \alpha_4, \alpha_6 \in \mathbb{F}$ και ένα στοιχείο $\mathcal{O}$ (σημείο στο άπειρο).

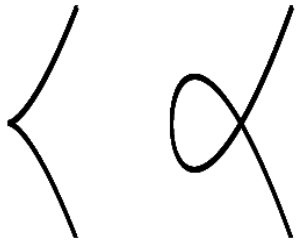
Πρακτικά η μορφή της καμπύλης ακολουθεί την εξίσωση:

$$y^2 = x^3 + \alpha x + \beta \quad \alpha, \beta \in \mathbb{F}$$



Γενική μορφή EC

- Συμμετρία ως προς άξονα x
  - Δυνατότητα συμπίεσης – αποθήκευση τετμημένη και 1 bit για το αν βρίσκεται *πάνω ή κάτω* από τον άξονα.
- Singular καμπύλες: Πολλαπλές ρίζες – προς αποφυγή
  - Πρέπει $4\alpha^3 + 27\beta^2 \neq 0$
- Δημιουργία ομάδας
  - Πράξη: Πρόσθεση σημείων (Poincare) με τη μέθοδο της εφαπτομένης (Διόφαντος) ή χορδής
  - Ουδέτερο στοιχείο: $\mathcal{O}$



Γενική μορφή EC

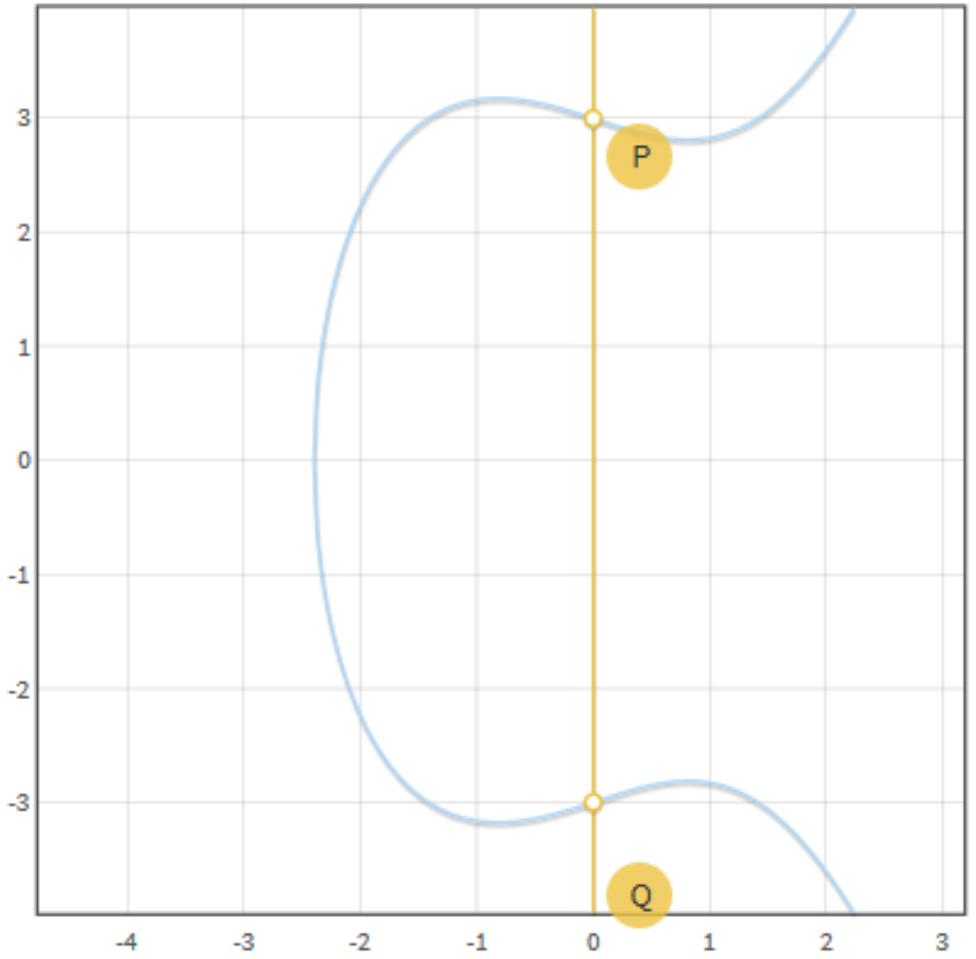
Έστω σημεία P, Q.

Ορίζουμε το άθροισμα ως $P + Q$

- Αν $P = \mathcal{O}$ τότε $P + Q = Q$
- Αν $Q = -P$ τότε $P + Q = \mathcal{O}$
- **Το $\mathcal{O}$ υπάρχει σε κάθε κατακόρυφη**

Αντίθετο σημείου

- Αν $P = \mathcal{O}$ τότε $-P = \mathcal{O}$
- Αν $P = (x, y)$ τότε $-P = (x, -y)$



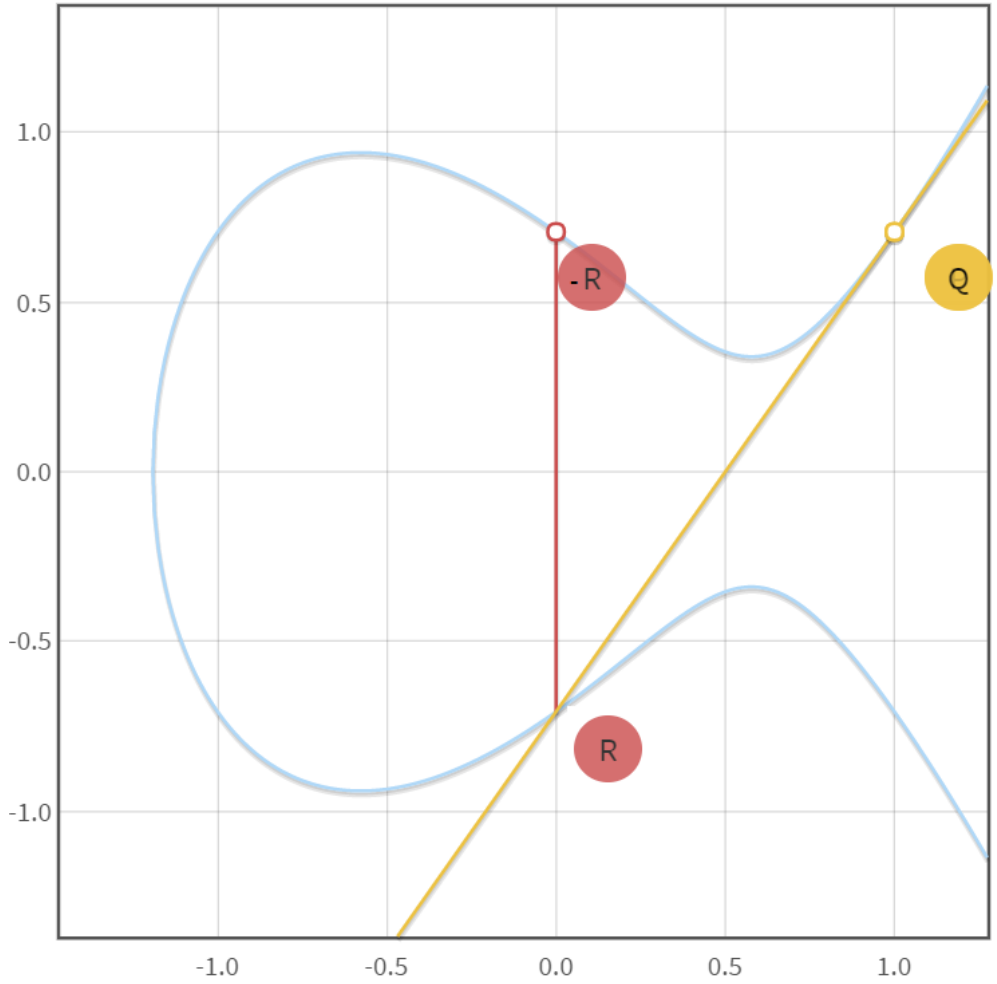
Πρόσθεση σημείων EC Γεωμετρική ερμηνεία

Πηγή εικόνων:
Elliptic Curve point addition ($\mathbb{R}$)

Πρόσθεση σημείων EC Γεωμετρική ερμηνεία

Αν $P = Q$ τότε το $P + Q$ υπολογίζεται ως εξης:

- Θεωρούμε την εφαπτομένη στο P
- Βρίσκουμε το σημείο τομής R με την καμπύλη
- Βρίσκουμε το αντίθετο

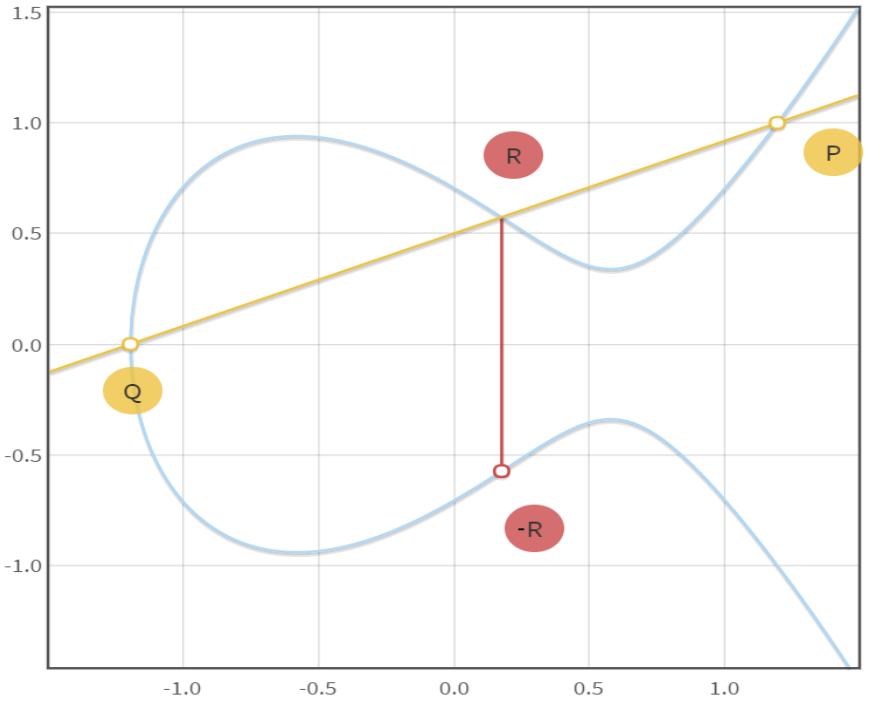


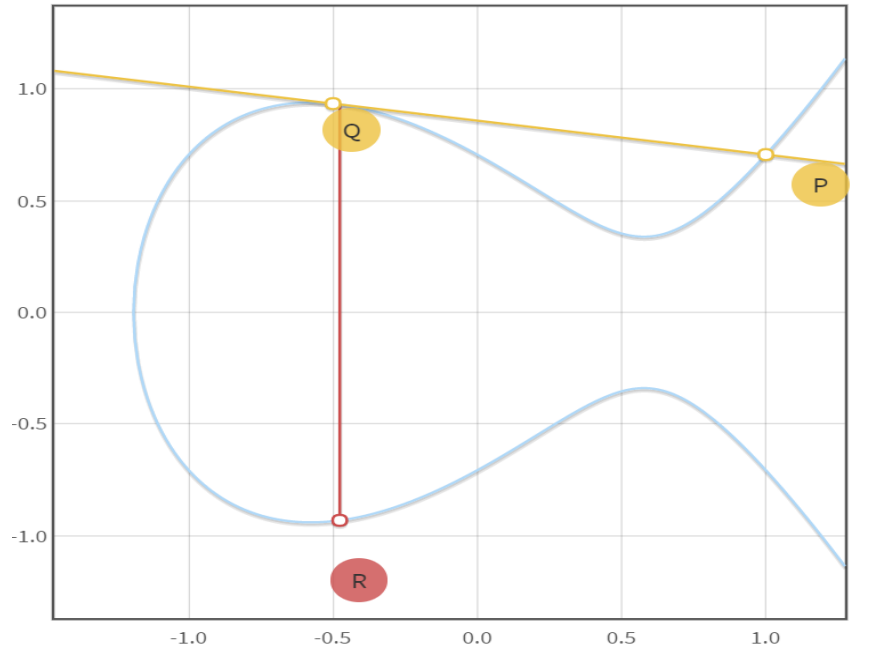
Πηγή εικόνων:
Elliptic Curve point addition ($\mathbb{R}$)

Αν $P \neq Q$ τότε το $P + Q$ υπολογίζεται ως εξης:

- Θεωρούμε το ευθύγραμμο τμήμα $\overline{PQ}$
- Βρίσκουμε το αντίθετο του σημείου τομής του R με την καμπύλη
- Αν δεν υπάρχει σημείο τομής, τότε σε ένα εκ των P, Q το $\overline{PQ}$ θα εφάπτεται της καμπύλης. Το άθροισμα είναι το αντίθετο.

Πρόσθεση σημείων EC Γεωμετρική ερμηνεία





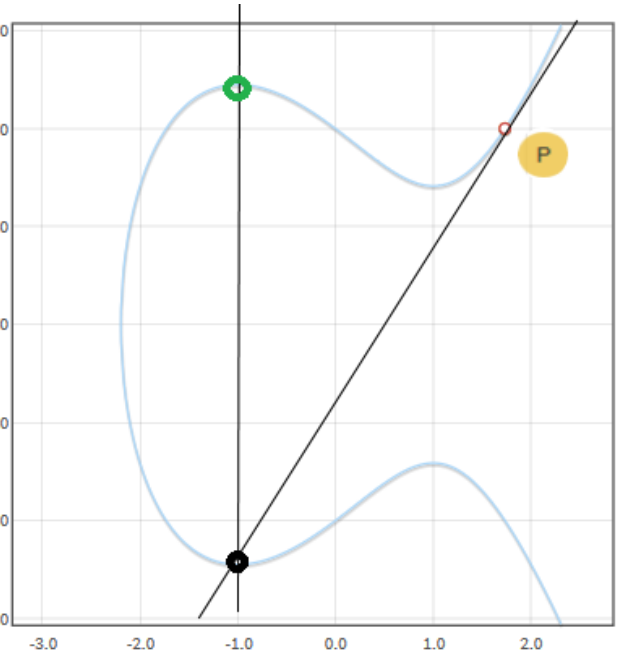
Πηγή εικόνων: Elliptic Curve point addition ($\mathbb{R}$)

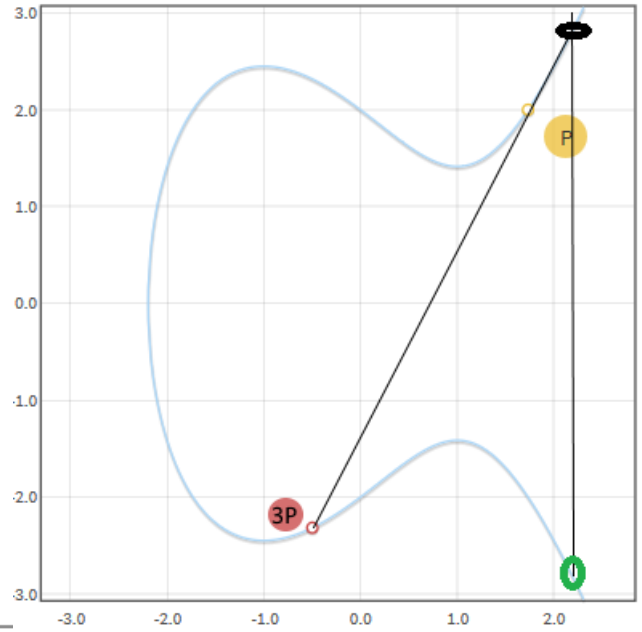
Αλγεβρική ερμηνεία

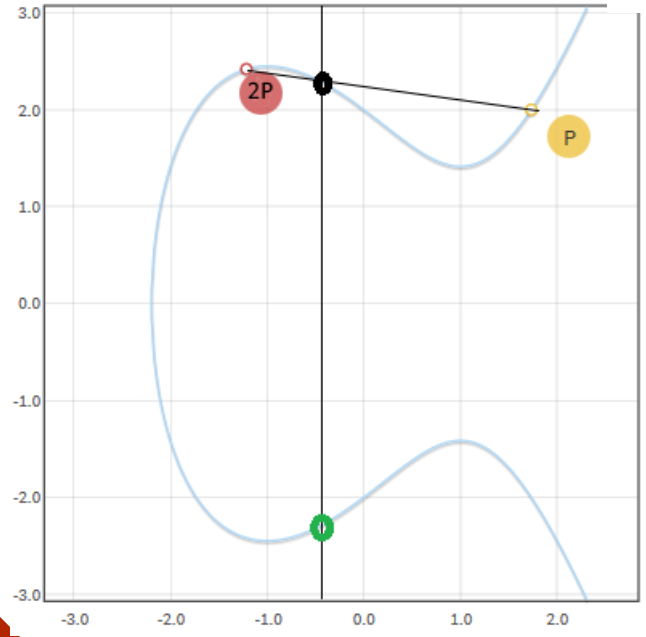
- Συντελεστής ευθείας $\overline{\mathrm{PQ}}$: $\frac{y_P - y_Q}{x_P - x_Q}$
- Εύρεση σημείου τομής του R με την ελλειπτική καμπύλη
- Επίλυση τριτοβάθμιας εξίσωσης.

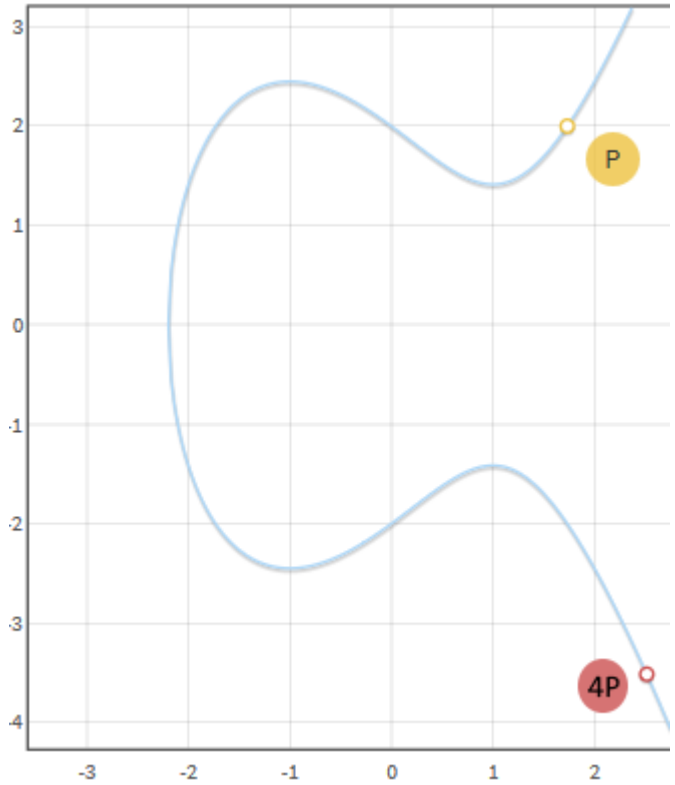
Πρόσθεση σημείων EC

Υπολογισμός $nP = P + P + P + \cdots + P$









Πολλαπλασιασμός σημείου με ακέραιο

Αντί για $n-1$ προσθέσεις μπορούμε να κάνουμε $logn$ προσθέσεις. Π.χ.

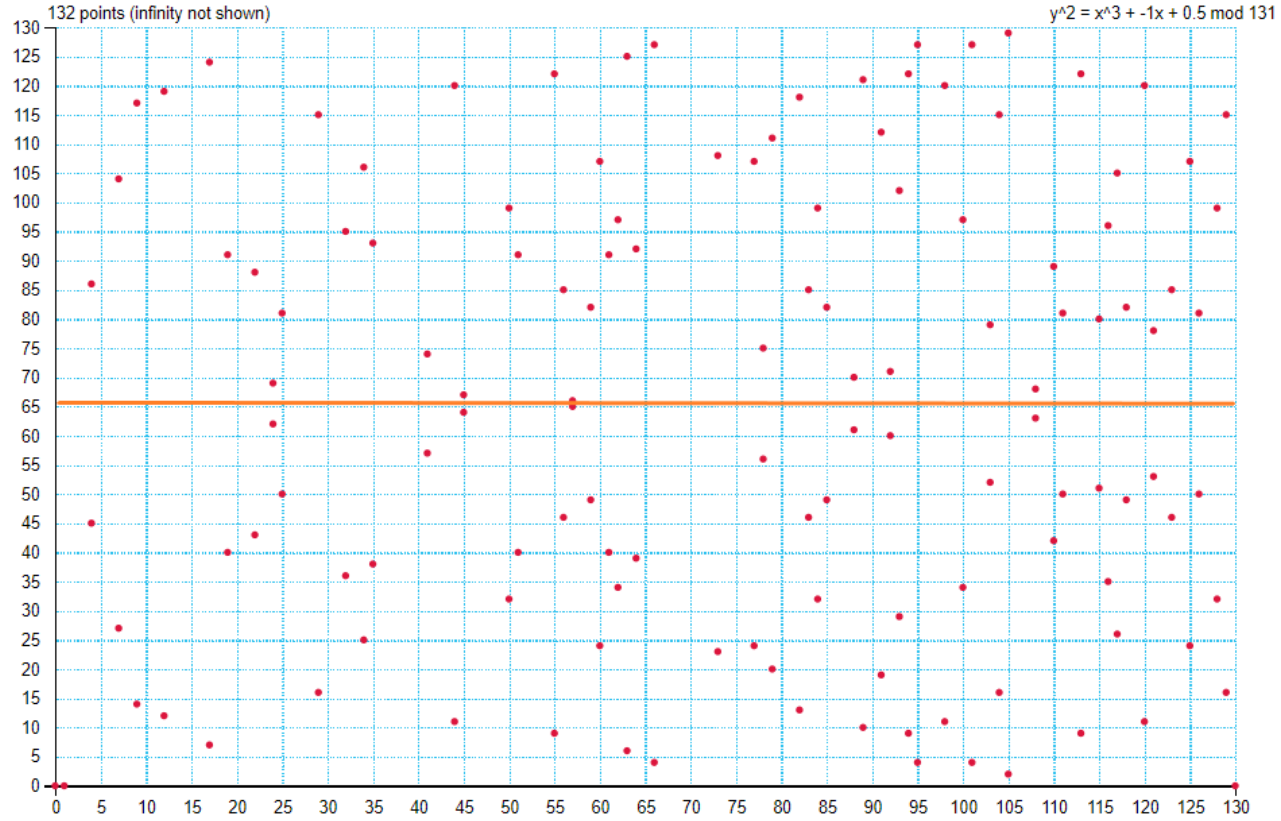
$$17P = P + 16P$$
$$2P = P + P$$
$$4P = 2P + 2P$$
$$8P = 4P + 4P$$
$$16P = 8P + 8P$$

Double and Add

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

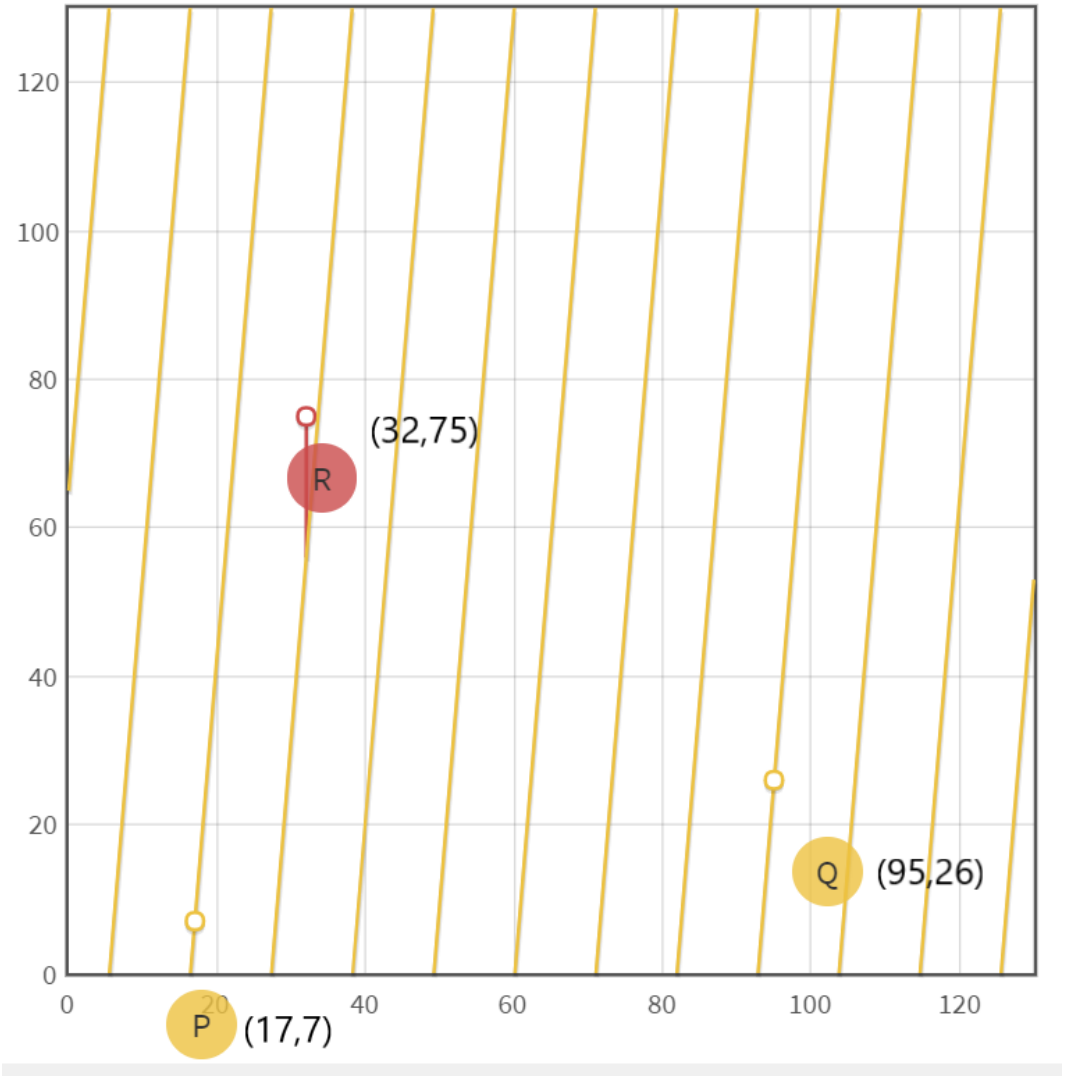
Elliptic curve plotter:
Elliptic Curves over Finite Fields

$$\mathcal{E}(\mathbb{F}_p): y^2 = x^3 - x + \frac{1}{2} \ (mod\ p)$$



Ελλειπτικές Καμπύλες στο $\mathbb{F}_p$

Η ευθεία που συνδέει τα P, Q, R για τα οποία $P + Q + R = 0$ επαναλαμβάνεται.



Πρόσθεση σημείων στο $\mathbb{F}_p$

- Επιλογή τάξης ομάδας:
  - Αλγόριθμοι Schoof, SEA
  - Hasse bound
  - Θεώρημα Lagrange: Η τάξη κάθε υποομάδας διαιρεί την τάξη της ομάδας
- Μπορούμε αποδοτικά να υπολογίσουμε την τάξη και γεννήτορες μιας ομάδας σημείων της ελλειπτικής καμπύλης.

Η ομάδα της καμπύλης $(\mathcal{E}(\mathbb{F}_p), +)$

Δίνονται:

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

Ζητείται:

- Να βρεθεί **ακέραιος** $x \in \mathbb{Z}_q$ τέτοιος ώστε $\boldsymbol{xG = Y}$

Ομοίως ορίζουμε και EC-CDH, EC-DDH

Το πρόβλημα ECDLP

Το πρόβλημα ECDLP

Υπόθεση: Το πρόβλημα ECDLP είναι **υπολογιστικά απρόσιτο.**

Προσοχή: Δεν ισχύει σε κάθε καμπύλη.

- Supersingular curves $\mathcal{E}(\mathbb{F}_p)$ όπου
  - Υπάρχει υποομάδα $\mathbb{G}_r$ τάξης r με $r \mid p^k - 1$ για **μικρά k**
  - Υποεκθετικό DLP – MOV's attack:
    - Μεταφορά DLP στο $\mathbb{F}_{P^k}$
    - Επίλυση με index calculus
- Anomalous curves
  - $\#\mathcal{E}(\mathbb{F}_p) = p$ – γραμμικό DLP – Smart's attack

Δεν προτείνεται η αυθαίρετη παραγωγή καμπυλών αλλά η χρήση έτοιμων

$\alpha \xleftarrow{\$} \mathbb{Z}_q$

$(p, a, b, \#\mathcal{E}, q, G)$

$b \xleftarrow{\$} \mathbb{Z}_q$

aG

bG

$K = abG$

$K = baG$

Το κοινό κλειδί είναι ένα σημείο της δημόσιας επιλεγμένης καμπύλης

ECDH

Πρότυπες Καμπύλες

Πρότυπο **NIST FIPS186-3**

- **NIST P-256**

$$y^2 = x^3 - 3x + b \; mod \; (2^{256} - 2^{224} + 2^{192} + 2^{96} - 1)$$

με $b = 41\,058\,363\,725\,152\,142\,129\,326\,129\,780\,047\,268\,409\,114\,441\,015\,993\,725\,554\,835\,256\,314\,039\,467\,401\,291$

Η πιο δημοφιλής ελλειπτική καμπύλη στο Internet - υποχρεωτική σε όλες τις υλοποιήσεις του πρωτοκόλλου TLS

- **NIST P-384**

$$y^2 = x^3 - 3x + b \; mod \; (2^{384} - 2^{128} - 2^{96} + 2^{32} - 1)$$

με $b = 27\,580\,193\,559\,959\,705\,877\,849\,011\,840\,389\,048\,093\,056\,905\,856\,361\,568\,521\,428\,707\,301\,988\,689\,241\,309\,860\,865\,136\,260\,764\,883\,745\,107\,765\,439\,761\,230\,575$

- **Δεν ξέρουμε πώς έχει επιλεγεί το b – Φόβοι για υπονόμευση**
- **Χρήση σε** Dual_EC_DRBG – broken NIST pseudorandom generator

Πρότυπες καμπύλες

- **Ισχυρισμός NIST:** Το b προήλθε από ένα τυχαίο seed s, το οποίο όμως δεν διευκρινίζεται πώς δημιουργήθηκε.
- **Πρόβλημα:** Δίνεται μια καμπύλη $y^2 = x^3 + ax + b\ \mathcal{E}(\mathbb{F}_p)$ ορισμένη στο $\mathbb{F}_p$ $(p, a, b, \#\mathcal{E}, q, G)$.

Πώς ξέρουμε ότι είναι ασφαλής;

- **Επαληθευσιμότητα:** Εγγύηση ότι δεν είναι *πειραγμένη* (nothing up my sleeve)
  - Επιλογή random seed από δημόσια διαθέσιμα δεδομένα s.
    - Υπολογισμός $h = H(s)$
    - Παραγωγή των a, b από το h με δημόσια διαθέσιμες συναρτήσεις
      - $\alpha = f(h), b = g(h)$
    - Επαληθευσιμότητα υπό την υπόθεση preimage resistance
      - (γιατί αλλιώς πρώτα επιλογή των a, b) και μετά επιλογή h

Εναλλακτικές καμπύλες

- **secp256k1 (OpenSSL, Bitcoin)**

$$y^2 = x^3 + 7 \; mod \; (2^{256} - 2^{32} - 977)$$

- **Curve25519 (OpenSSH)**

$$y^2 = x^3 + 486662 \cdot x^2 + x \; mod \; (2^{255} - 19)$$

- **Άλλες μορφές:**
  - **Koblitz curves:** $y^2 + xy = x^3 + ax^2 + 1, a \in \{0,1\}$
  - **Binary curves:** $y^2 + xy = x^3 + x^2 + b, b \in \mathbb{Z}$
  - **Edwards curves:** $y^2 + x^2 = 1 + dx^2y^2, d \in \{0,1\}$

Πρότυπες καμπύλες

Pairings

Δίνονται τρεις πεπερασμένες κυκλικές ομάδες: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$

Ζεύξη (Pairing) είναι μια **αποδοτικά υπολογίσιμη** συνάρτηση

$$e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

Διγραμμική (bilinear)

$$e(G_1 + G_2, H_1) = e(G_1, H_1) \cdot e(G_2, H_1)$$
$$e(G_1, H_1 + H_2) = e(G_1, H_1) \cdot e(G_1, H_2)$$

ή ισοδύναμα:

$$e(aG, bH) = e(G, H)^{ab} = e(bG, aH)$$

Μη-εκφυλισμένη (non-degenerate)

$$\mathbb{G}_1 = \langle \mathrm{G} \rangle, \mathbb{G}_2 = \langle \mathrm{H} \rangle \Rightarrow \mathbb{G}_\mathrm{T} = \langle e(G, H) \rangle$$

Pairings

Συμμετρικά pairings: $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$

Συνήθως: $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G} \subseteq \mathcal{E}(\mathbb{F}_p), \mathbb{G}_T \subseteq \mathbb{F}_{p^a}$

Γνωστά pairings: Weil, Tate, Ate

Παράδειγμα με φυσικούς:

$$e: \mathbb{N} \times \mathbb{N} \to \mathbb{N} \text{ με } e(x, y) = 2^{xy}$$

Bilinearity:

$$e(a + b, c) = 2^{(a+b)c} = 2^{ac+bc} = e(ac) \cdot e(bc)$$
$$e(a, b + c) = 2^{a(b+c)} = 2^{ab+ac} = e(ab) \cdot e(ac)$$
$$e(ab, cd) = 2^{ab \cdot cd} = 2^{cb \cdot ad} = e(cb) \cdot e(ad)$$

- Στις $\mathbb{G}_1, \mathbb{G}_2$ ή $\mathbb{G}$ κάποια προβλήματα μπορεί να είναι δύσκολα.
- Στην $\mathbb{G}_T$ όμως μπορεί να είναι εύκολα (Gap Diffie-Hellman groups)
- Η απεικόνιση e όμως μας επιτρέπει να μεταβούμε αποδοτικά στην $\mathbb{G}_T$ παρακάμπτοντας έτσι τη δυσκολία.
- Η ασυμμετρία αυτή μπορεί να έχει θετικά αποτελέσματα (νέα πρωτόκολλα) ή αρνητικά αποτελέσματα (σπάσιμο ασφάλειας)
- Bonus: Ένας πολλαπλασιασμός στον εκθέτη
- Πρόβλημα: Σπάσιμο υπόθεσης DDH

Pairings στην κρυπτογραφία

Ύπαρξη Pairing – Εύκολο DDHP

- Θέλουμε να ελέγξουμε αν $ab = c$ με δεδομένα aG, bG, cG
- Αν υπάρχει συμμετρικό pairing τότε:
  - $e(aG, bG) = e(G, G)^{ab}$
  - $e(cG, G) = e(G, G)^{c}$
  - Αν $e(G, G)^{ab} = e(G, G)^{c}$ τότε $ab = c$

Bilinear Decisional Diffie-Hellman (BDDHP)

- Δίνονται (aG, bG, cG) σε μια κυκλική ομάδα $\mathbb{G} = \langle G \rangle$ με τάξη q για την οποία υπάρχει pairing σε $\mathbb{G}_T$ και $d \in \mathbb{Z}_q$
- Να εξεταστεί αν $d = abc$.

Έστω κυκλική ομάδα $\mathbb{G} = \langle G \rangle$ με τάξη q και οντότητες με κλειδιά

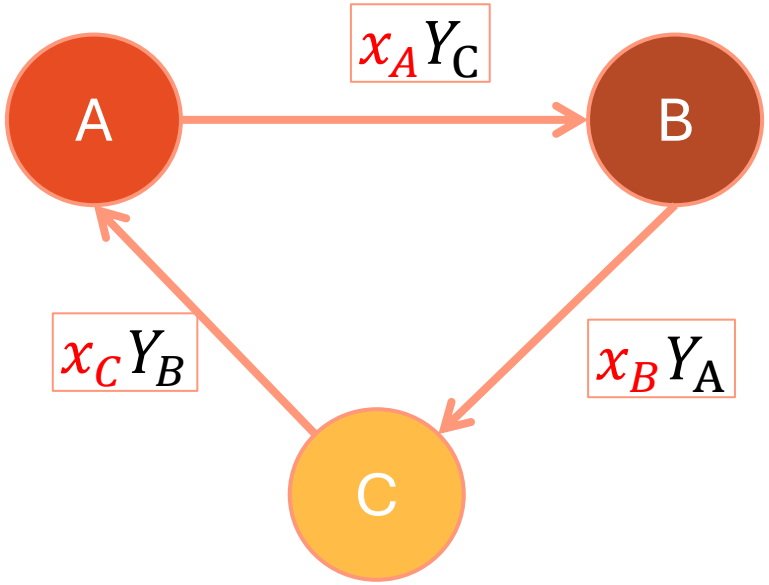
- *A*: $(x_A, Y_A = x_A \mathrm{G})$
- *B*: $(x_B, Y_B = x_B \mathrm{G})$
- *C*: $(x_C, Y_C = x_C \mathrm{G})$

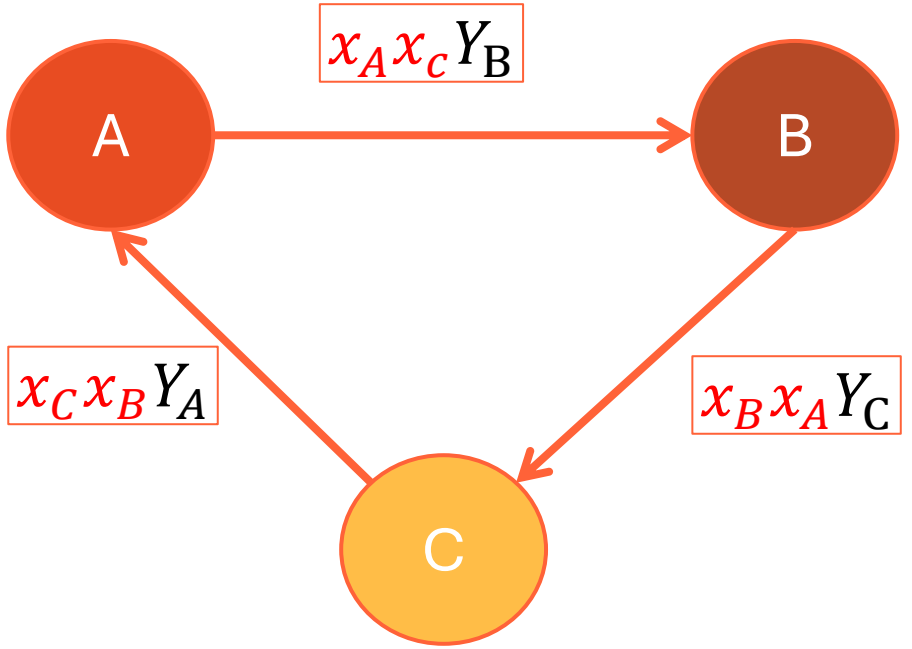
Πώς μπορούν να συμφωνήσουν ένα κοινό κλειδί μεταξύ τους;

Σε πόσους γύρους;

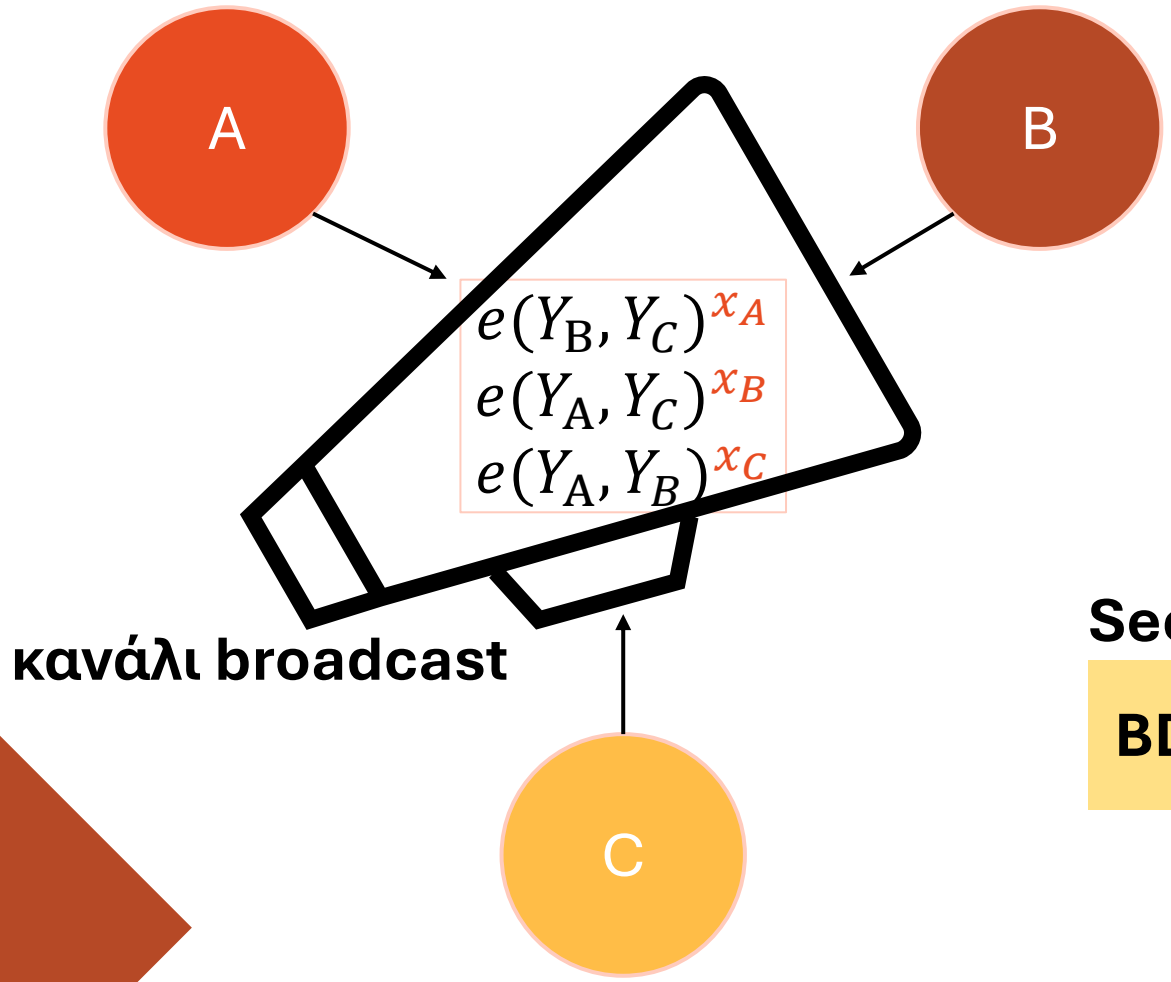
Τριμερής ανταλλαγή κλειδιού

$$x_C x_B Y_A = x_C x_A Y_B = x_A x_B Y_c = x_C x_B x_A G$$





Τριμερής ανταλλαγή κλειδιού (2 γύροι)



$$e(Y_B, Y_C)^{x_A} = e(Y_A, Y_C)^{x_B} = e(Y_A, Y_B)^{x_C} = e(G, G)^{x_A x_B x_C}$$

Security (Passive Adversaries)

BDDP is hard ⇒ Joux key exchange is secure

Τριμερής ανταλλαγή κλειδιού (1 γύρος- Joux 2000)

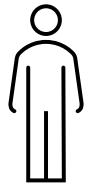
Identity Based Encryption (IBE)

- Αρχική ιδέα: Shamir 1984
- Μια λύση στο πρόβλημα αυθεντικότητας κλειδιού
  - Δεν απαιτεί διανομή κλειδιού
  - Δημόσιο κλειδί = δημόσιο ψευδώνυμο χρήστη (π.χ. email)
  - Ιδιωτικό κλειδί προκύπτει από το ψευδώνυμο
- Σχήμα Boneh-Franklin (2001) – μετά από πολλά χρόνια προσπαθειών
  - Απαιτεί ύπαρξη **TTP**
  - **Απαιτεί ύπαρξη pairing**

- **Δημιουργία Κλειδιών TTP**
  - Επιλογή κυκλικών ομάδων $\mathbb{G}$, $\mathbb{G}_T$ τάξης q με δύσκολο DLP με pairing $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
  - Συναρτήσεις σύνοψης: $\mathrm{H}_{\mathbb{G}}: \{0,1\}^* \rightarrow \mathbb{G}$, $\mathrm{H}_{\mathbb{G}_T}: \mathbb{G}_T \rightarrow \{0,1\}^*$
  - Ιδιωτικό κλειδί TTP: $x \leftarrow_{\$} \mathbb{Z}_q$
  - Δημόσιο κλειδί TTP: $y \leftarrow g^x$

- **Δημιουργία Κλειδιών χρήστη με ψευδώνυμο ID (από TTP)**

  Δημόσιο κλειδί: $y_{ID} \leftarrow \mathrm{H}_{\mathbb{G}}(ID)$
  Ιδιωτικό κλειδί: $x_{ID} \leftarrow y_{ID}^{x}$
- **Κρυπτογράφηση για χρήστη ID**
  - Επιλογή **εφήμερου** κλειδιού $r \leftarrow_{\$} \mathbb{Z}_q$
  - Υπολογισμός $t \leftarrow e(y, y_{ID})^r$
  - $m \in \{0,1\}^*$
  - $Enc_{y_{ID}}(m, r) = (g^r, m \oplus \mathrm{H}_{\mathbb{G}_T}(t))$



- **Αποκρυπτογράφηση**

$$Dec_{x_{ID}}(c_1, c_2) = c_2 \oplus H_{\mathbb{G}_T}\left(e(c_1, x_{ID})\right)$$

Identity Based Encryption (IBE)

Ορθότητα:

- $t = e(y, y_{ID})^r = e(g^x, h)^r = e(g, h)^{xr}$
- $e(c_1, x_{ID}) = e(g^r, y_{ID}^x) = e(g, h)^{xr}$
- $c_2 \oplus H_{\mathbb{G}_T}\left(e(c_1, x_{ID})\right) = m \oplus H_{\mathbb{G}_T}(t) \oplus H_{\mathbb{G}_T}\left(e(c_1, x_{ID})\right) = m$

Identity Based Encryption (IBE)

Το κρυπτοσύστημα ElGamal

ElGamal

- Taher ElGamal (1985)
- Ένα κρυπτοσύστημα με βάση την ανταλλαγή κλειδιού Diffie-Hellman
  - Κρυπτογράφηση = Ανταλλαγή (**εφήμερου**) κλειδιού με τον παραλήπτη του μηνύματος
- Χρήση και για υπογραφές
  - Βάση για το σχήμα υπογραφών (**EC)DSA**

Το κρυπτοσύστημα ElGamal

- **Δημιουργία Κλειδιών**
  - Επιλογή κυκλικής ομάδας $\mathbb{G}$ τάξης q με δύσκολο DLP
    - Υποομάδα πρώτης τάξης q του $\mathbb{Z}_p^*$
    - Ελλειπτική καμπύλη
  - Ιδιωτικό κλειδί: $x \leftarrow_{\$} \mathbb{Z}_q$
  - Δημόσιο κλειδί: $y \leftarrow g^x$
- **Κρυπτογράφηση**
  - Κωδικοποίηση m σε $\mathbb{G}$
  - Επιλογή **εφήμερου** κλειδιού $r \leftarrow_{\$} \mathbb{Z}_q$
  - $Enc_y(m, r) = (g^r, m \cdot y^r)$
- **Αποκρυπτογράφηση**
  - $\mathrm{Dec}_x(c_1, c_2) = c_2 \cdot c_1^{-x}$
- **Ορθότητα:**
  - $Dec(g^r, m \cdot y^r) = m \cdot y^r \cdot (g^r)^{-x} = m \cdot y^{r-r} = m$

Παρατηρήσεις

- **Παράμετροι κρυπτογράφησης είναι ίδιες για όλες τις κρυπτογραφήσεις**
  - Σύγκριση με RSA (κάθε δημόσιο κλειδί ορίζει τη δική του ομάδα)
  - **Δημιουργία παραμέτρων 1 φορά για όλους τους χρήστες**.
- Συνήθη ασφαλή μεγέθη: $(|p| = 3072)\ |q| = 256$
- **Πιθανοτική κρυπτογράφηση:**
  - Ένα μήνυμα έχει πολλά πιθανά κρυπτοκείμενα!
- **Διπλασιασμός χώρου:**
  - Ένα στοιχείο της ομάδας κρυπτογραφείται με δύο στοιχεία της ομάδας.

- **Το μήνυμα πρέπει να μετατραπεί σε στοιχείο της ομάδας**
- Όμως θα θέλαμε $m \in \{0,1\}^*$
- Σε κάποιες περιπτώσεις μπορούμε να ορίσουμε αντιστοίχιση στην ομάδα
- Γενικότερα Key Encapsulation schemes:
  - Για να κρυπτογραφήσουμε $m \in \{0,1\}^*$
  - Επιλέγουμε $m_{\mathbb{G}} \leftarrow_{\$} \mathbb{G}$
  - $k \leftarrow H(m_{\mathbb{G}})$ π.χ. με SHA-256
  - Αποστολή $(Enc_{EG,pk}(m_G, r), Enc_{AES,k}(m))$

Παρατηρήσεις

Επίθεση KPA είναι επιτυχής αν έχει χρησιμοποιηθεί **η ίδια τυχαιότητα** σε περισσότερα από 1 μηνύματα.

$$(c_r, c) = (g^r, m \cdot y^r) = Enc_y(m, r)$$

$$(c_r, c') = (g^r, m' \cdot y^r) = \mathrm{Enc_y}(m', \mathrm{r})$$

Αν γνωρίζω $(m, (c_r, c))$ τότε:

$$y^r = c \cdot m^{-1}$$

και

$$m' = c' \cdot (y^r)^{-1} = c' \cdot (c \cdot m^{-1})^{-1} = c' \cdot c^{-1} \cdot m$$

Συμπέρασμα: Αυστηρά **νέα** τυχαιότητα σε κάθε κρυπτογράφηση!

Ασφάλεια ElGamal: Επανάληψη τυχαιότητας

Μυστικότητα ElGamal (OW-CPA)

Η μυστικότητα ElGamal (αποκάλυψη ολόκληρου του μηνύματος) είναι ισοδύναμη με το CDHP.

Απόδειξη:

Αντιστοιχία παραμέτρων:

$$g^a \leftrightarrow g^r$$
$$g^b \leftrightarrow g^x = y$$
$$g^{ab} \leftrightarrow y^r = g^{xr}$$

Ευθύ: $ElGamal \leq CDHP$

1. $CDHP$ oracle: Επίλυση $CDHP(g^r, g^x) \rightarrow g^{xr} (= y^r)$
2. Εύρεση αντίστροφου y^r
3. Αποκρυπτογράφηση

Μυστικότητα ElGamal

Η μυστικότητα ElGamal (αποκάλυψη ολόκληρου του μηνύματος) είναι ισοδύναμη με το CDHP.

Απόδειξη:

Αντίστροφο: $CDHP \leq ElGamal$

1. ElGamal oracle: Μπορώ να υπολογίζω μηνύματα ElGamal από κρυπτογραφήσεις με δημόσιο κλειδί y (χωρίς το ιδιωτικό). $EG(c_1, c_2) \rightarrow m$
2. Αντιστοιχία: $y = g^b$, $c_1 = g^a$ και επιλέγουμε $h \leftarrow_{\$} \mathbb{G}$
3. Καλούμε: $EG(c_1, h)$
4. Λαμβάνουμε $m \in \mathbb{G}$ ώστε: $h = m \cdot y^r = m \cdot g^{ab}$
5. Υπολογίζουμε $g^{ab} = h \cdot m^{-1}$

Αν το DDHP είναι δύσκολο στην $\mathbb{G}$, τότε το κρυπτοσύστημα ElGamal έχει την ιδιότητα IND-CPA.

Απόδειξη: Έστω ότι το ElGamal δεν διαθέτει ασφάλεια IND-CPA.

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

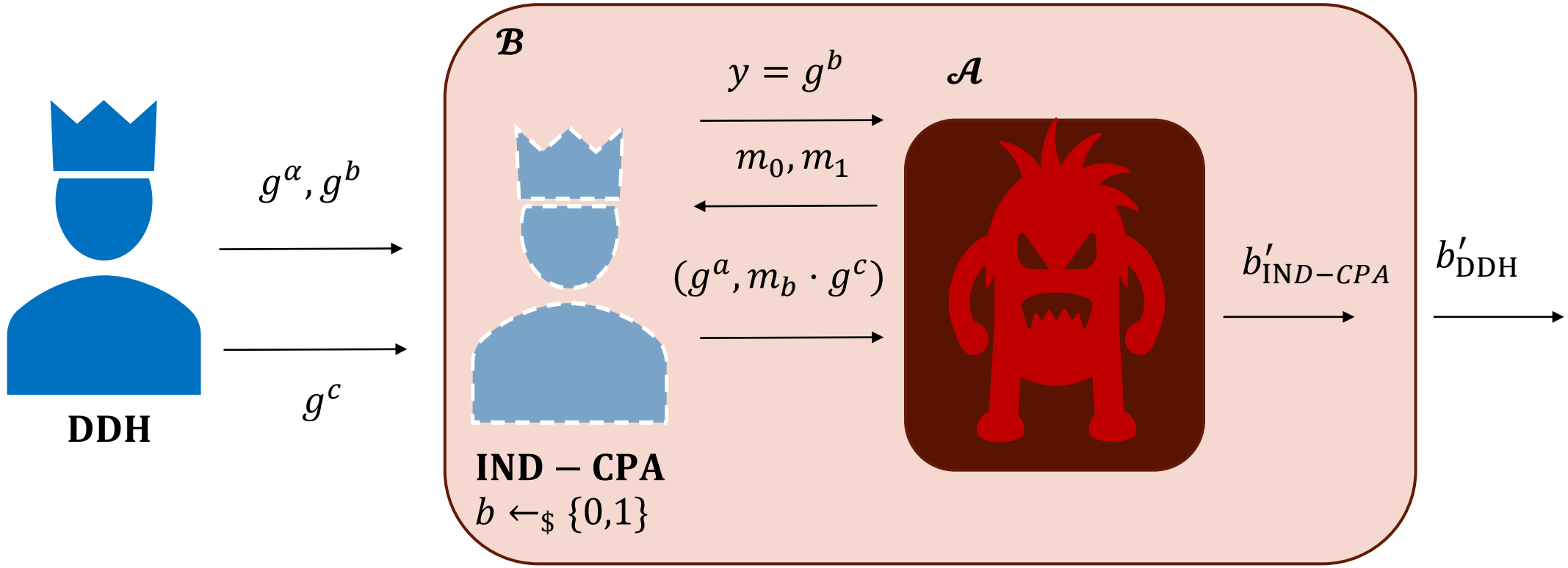
Θα τον χρησιμοποιήσουμε για να κατασκευάσουμε νέο αντίπαλο $\mathcal{B}$ με:

Είσοδο: τριάδα στοιχείων

Εσωτερικά: Προσομοίωση του challenger στο παιχνίδι IND-CPA και χρήση $\mathcal{A}$ ως μαύρο κουτί

Αποτέλεσμα: Διαχωρισμός DH - τυχαίας τριάδας με μη αμελητέα πιθανότητα

IND-CPA για ElGamal



IND-CPA για ElGamal

Αν το DDHP είναι δύσκολο στην $\mathbb{G}$, τότε το κρυπτοσύστημα ElGamal έχει την ιδιότητα IND-CPA.

Είσοδος $\mathcal{B}$: τριάδα στοιχείων (g^a, g^b, g^c) όπου $c = ab$ ή $c \leftarrow_{\$} \mathbb{Z}_q$

Εσωτερικά:

- Ο challenger κάνει setup ένα ElGamal σύστημα με $y = g^b$.
- Με το y απαντά στις κρυπτογραφήσεις του $\mathcal{A}$, κρυπτογραφώντας τα μηνύματα που θέλει.
- Όταν σταλεί το challenge m_0, m_1 ο challenger επιλέγει m_b και παράγει το ζεύγος: $(g^a, m_b \cdot g^c)$

Αποτέλεσμα:

- Ο $\mathcal{A}$ εξάγει b' το οποίο επιστρέφεται αυτούσιο από τον B.

IND-CPA για ElGamal

Αν το DDHP είναι δύσκολο στην $\mathbb{G}$, τότε το κρυπτοσύστημα ElGamal έχει την ιδιότητα IND-CPA.

Αν $c = ab$ τότε η κρυπτογράφηση ElGamal είναι έγκυρη **(γιατί?)**

Άρα το πλεονέκτημα του $\mathcal{A}$ είναι **πραγματικό,** και μαντεύει το σωστό b στο παιχνίδι IND-CPA με **μη αμελητέα πιθανότητα**.

Αν c είναι τυχαίο τότε η κρυπτογράφηση ElGamal είναι άκυρη **(γιατί?)**

Άρα το πλεονέκτημα του $\mathcal{A}$ στο παίγνιο IND-CPA δεν τον βοηθάει οπότε η καλύτερη **στρατηγική είναι να μαντέψει στην τύχη**.

Άρα κερδίζει το παίγνιο IND-CPA με πιθανότητα $\frac{1}{2}$

$$Adv^{\mathcal{B}}_{\mathrm{DDH}}(\lambda) = \left|\Pr\left[\mathcal{B}\left(g, g^{\alpha}, g^{\beta}, g^{\alpha\beta}\right) = 1\right] - \Pr\left[\mathcal{B}\left(g, g^{\alpha}, g^{\beta}, g^{c}\right) = 1\right]\right|$$
$$\geq \frac{1}{2} + negl(\lambda) - \frac{1}{2} \geq negl(\lambda)$$ **ΜΗ ΑΜΕΛΗΤΕΟ (ΆΤΟΠΟ)**

IND-CPA για ElGamal

Πολλαπλασιασμός κρυπτοκειμένων – κρυπτοκείμενο γινομένου

$$Enc_y(m_1, r_1) \odot Enc_y(m_2, r_2) = (g^{r_1}, m_1\, y^{r_1}) \odot (g^{r_2}, m_2\, y^{r_2}) =$$

$$(g^{r_1+r_2}, m_1 \cdot m_2 \cdot y^{r_1+r_2}) = Enc_y(m_1 \cdot m_2, r_1 + r_2)$$

Reencryption: Αλλαγή μορφής κρυπτοκειμένου χωρίς ιδιωτικό κλειδί, μέσω αλλαγής τυχαιότητας

$$Enc_y(m, r_1) \odot Enc_y(1, r_2) = Enc_y(m, r_1 + r_2)$$

Malleability!

Ομομορφισμός - Malleability

Αντί για $m \in \mathbb{G}$ κρυπτογραφούμε το $g^m, m \in \mathbb{Z}_q$: $Enc_y(m, r) = (g^r, g^m \cdot y^r)$

Γιατί: Επειδή προσφέρει **προσθετικό** ομομορφισμό.

$$Enc_y(m_1, r_1) \odot Enc_y(m_2, r_2) = (g^{r_1}, g^{m_1} y^{r_1}) \odot (g^{r_2}, g^{m_2} y^{r_2}) =$$

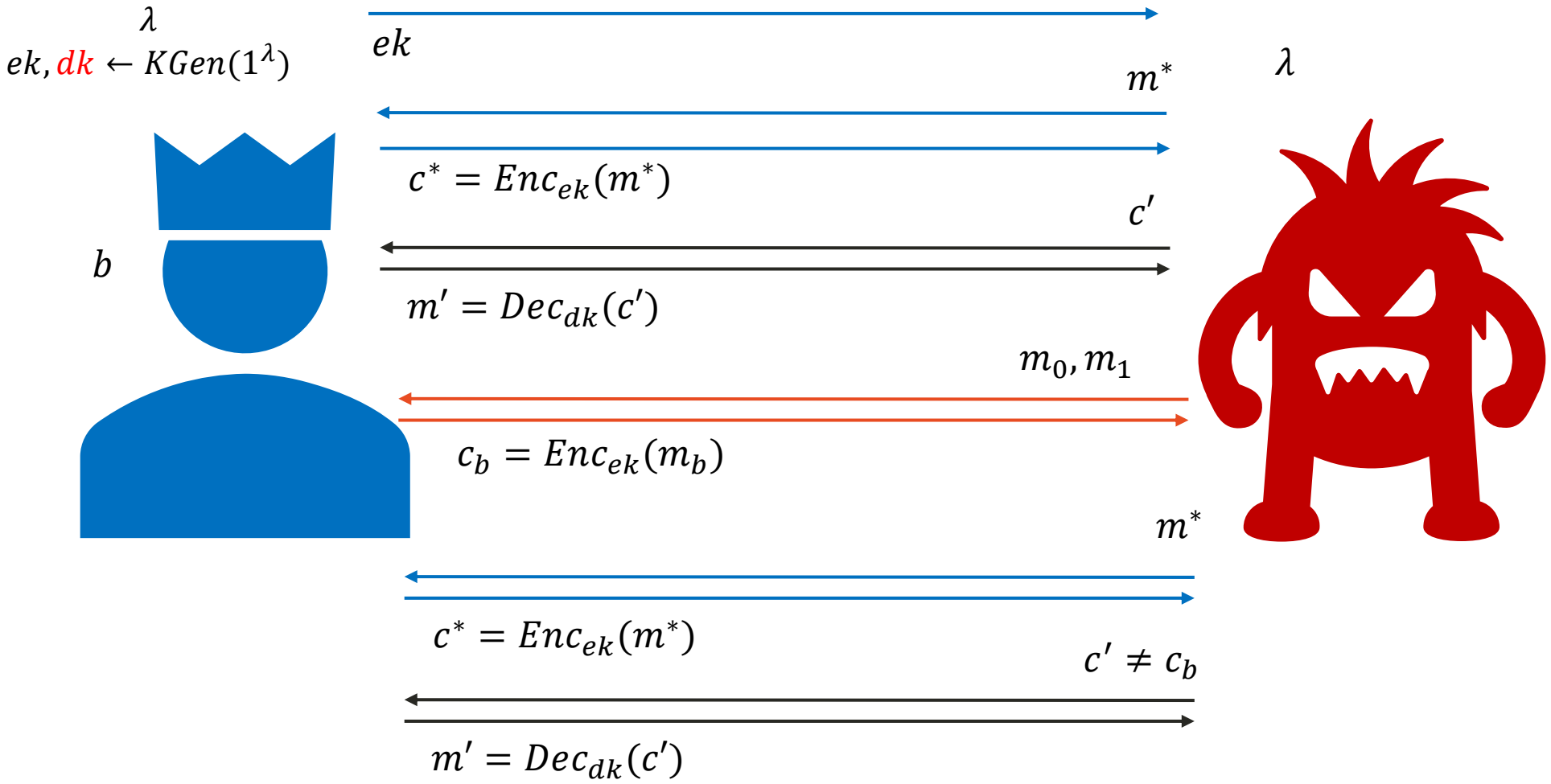
$$(g^{r_1+r_2}, g^{m_1+m_2} \cdot y^{r_1+r_2}) = Enc_y(m_1 + m_2, r_1 + r_2)$$

Πρόβλημα: Η αποκρυπτογράφηση δίνει το g^m. Χρειάζεται επίλυση DLP.

Σε αρκετές εφαρμογές δεν είναι πρόβλημα γιατί $|m| \ll |q|$

Παράδειγμα: Ηλεκτρονικές ψηφοφορίες μια κωδικοποίηση υποψήφιων χρειάζεται π.χ. $8\ bits$ και όχι 256, ενώ μας βολεύει να μπορούμε να αθροίζουμε ψήφους

Εκθετικό (Lifted ElGamal)


λ
$ek, dk \leftarrow KGen(1^{\lambda})$
ek
m^*
λ
$c^* = Enc_{ek}(m^*)$
c'
b
$m' = Dec_{dk}(c')$
m_0, m_1
$c_b = Enc_{ek}(m_b)$
m^*
$c^* = Enc_{ek}(m^*)$
$c' \neq c_b$
$m' = Dec_{dk}(c')$

IND-CCA

- Πώς μπορεί να αποκρυπτογραφηθεί το $c_b = (g^r, m_b \cdot y^r)$;
- Υπενθύμιση: δεν μπορεί να σταλεί απευθείας στο μαντείο κρυπτογράφησης.
- Επιλογή $h \in \mathbb{G}$ και υπολογισμός του $c = (g^{r'}, h \cdot y^{r'})$
- Αποστολή του $c \odot c_b \neq c_b$
- Λήψη $h \cdot m_b$
- Υπολογισμός m_b με χρήση h^{-1}
- Σίγουρη νίκη!

IND-CCA για ElGamal

- ElGamal με IND-CCA2
- Επέκταση του ElGamal
- Χρήση συνάρτησης σύνοψης H (υπάρχουν εκδόσεις και χωρίς)
- **Αν ισχύει η υπόθεση DDH στην $\mathbb{G}$, τότε παρέχει ασφάλεια IND-CCA2**

Cramer - Shoup

Δημιουργία κλειδιών

- Επιλογή ομάδας $\mathbb{G}$ τάξης q
- Επιλογή $g_1, g_2 \in \mathbb{G}$
- Επιλογή $x_1, x_2, y_1, y_2, z \leftarrow_{\$} \mathbb{Z}_q$
- Υπολογισμός
  - $c \leftarrow g_1^{x_1} g_2^{x_2}$
  - $d \leftarrow g_1^{y_1} g_2^{y_2}$
  - $h \leftarrow g_1^{z}$
- Δημόσιο κλειδί (c, d, h)
- Ιδιωτικό κλειδί (x_1, x_2, y_1, y_2, z)

Cramer - Shoup

Κρυπτογράφηση

- Κωδικοποίηση μηνύματος m στο $\mathbb{G}$
- Επιλογή $r \leftarrow_{\$} \mathbb{Z}_q$
- Υπολογισμός
  - $\boldsymbol{u_1 \leftarrow g_1^r}, u_2 \leftarrow g_2^r$
  - $\boldsymbol{e \leftarrow m \cdot h^r}$
  - $a \leftarrow H(u_1 || u_2 || e)$
  - $v \leftarrow c^r d^{ra}$
- Επιστροφή: $(\boldsymbol{u_1}, u_2, \boldsymbol{e}, v)$

- **Αποκρυπτογράφηση**$(\boldsymbol{u_1}, u_2, \boldsymbol{e}, v)$
- Υπολογισμός
  - $a \leftarrow H(u_1 || u_2 || e)$
- Έλεγχος αν:
  - $u_1^{x_1} u_2^{x_2} \left(u_1^{y_1} u_2^{y_2}\right)^{\alpha} = v$
- Σε περίπτωση αποτυχίας **έξοδος**
- Σε περίπτωση επιτυχίας
  - $m = \boldsymbol{e} \cdot \boldsymbol{u_1}^{-z}$

Cramer - Shoup

Ορθότητα

- $u_1^{x_1}\, u_2^{x_2}\left(u_1^{y_1}\, u_2^{y_2}\right)^{\alpha} = (g_1^{x_1} g_2^{x_2})^{r}\ (g_1^{y_1} g_2^{y_2})^{ra} = cd^{a}$
- $e \cdot u_1^{-z} = m \cdot h^{r}\, u_1^{-z} = m \cdot g_1^{zr} g_1^{-zr} = m$

- $\boldsymbol{h}, \boldsymbol{z}$ αντιστοιχούν σε δημόσιο - ιδιωτικό κλειδί ElGamal
- $\boldsymbol{u_1}, \boldsymbol{e}$ αντιστοιχούν στο κρυπτογράφημα του ElGamal
- u_2, v λειτουργούν ως έλεγχος ακεραιότητας, ώστε να μπορεί να αποφευχθεί το malleability
- Διπλάσια πολυπλοκότητα από ElGamal τόσο σε μέγεθος κρυπτοκειμένου, όσο και σε υπολογιστικές απαιτήσεις

Cramer - Shoup

Σχήματα δέσμευσης

Coin Flipping over the telephone

- Η **Alice** και ο **Bob** διαφωνούν τηλεφωνικά για το πού θα πάνε και πρέπει να αποφασίσουν απομακρυσμένα
- Αποφασίζουν να ρίξουν νόμισμα μέσω τηλεφώνου
- Ίδια αποτελέσματα – επιλέγει η Alice.
- Διαφορετικά αποτελέσματα – επιλέγει ο Bob.
- Τι προβλήματα μπορεί να προκύψουν;
- Λύση: Σχήμα δέσμευσης.

Manuel Blum (1981)

Σύνταξη: Μια τριάδα αλγορίθμων $KGen, Commit, Open$

- $KGen(1^{\lambda}) \rightarrow ck$: Δημιουργία **δημοσίου κλειδιού δέσμευσης**
- $Commit_{ck}(m) \rightarrow (cm, ok)$
  - Παραγωγή δέσμευσης cm και **κλειδιού ανοίγματος** ok.
  - ok:Προστατεύει από επιθέσεις brute force (παρέχει randomization)
- $Open(cm, ok, m) \rightarrow \{0,1\}$
  - Επιστρέφει 1 αν $(cm, ok) = Commit_{ck}(m)$, αλλιώς 0

Σχήματα δέσμευσης

Hiding - Προστατεύει αποστολέα - καθώς δεν μπορ να διαρρεύσει το μήνυμά τοι

$$\left|\Pr\left[b' = b \;\middle|\; \begin{array}{c}(\vec{m}_1, \vec{m}_2) \leftarrow \mathcal{A}, \\ r \xleftarrow{\$} \mathcal{R}, b \xleftarrow{\$} \{1,2\}, \\ c \leftarrow \mathrm{Cm}(\vec{m}_b; r), b' \leftarrow \mathcal{A}[c]\end{array}\right] - \frac{1}{2}\right| \leq \mathrm{negl}(\lambda)$$

Binding - Προστατεύει παραλήπτη - καθώς ο αποστολέας δεν μπορεί να αλλάξει την τιμή του εκ των υστέρων.

$$\Pr\left[\begin{array}{l}(\mathrm{Cm}(\vec{m}_1; r_1) = \mathrm{Cm}(\vec{m}_2; r_2)) \\ \wedge\ \vec{m}_1 \neq \vec{m}_2\end{array} \;\middle|\; \begin{array}{c}\vec{m}_1 \xleftarrow{\$} \mathcal{M}, \vec{r}_1 \xleftarrow{\$} \mathcal{R}, \\ (\vec{m}_2, r_2) \leftarrow \mathcal{A}[\vec{m}_1, r_1]\end{array}\right] \leq \mathrm{negl}(\lambda)$$

Ιδιότητες Ασφάλειας

- Η Alice ρίχνει το νόμισμα και αποκτά b_A
- Ο Bob ρίχνει το νόμισμα και αποκτά b_B
- Η Alice δεσμεύεται στο $b_A : (c_A, o_A) = Commit_{ck}(b_A)$
- Η Alice στέλνει c_A
- Ο Bob στέλνει b_B
- Η Alice στέλνει b_A, o_A
- Ο Bob επαληθεύει αν $Open_{ck}(c_A, o_A, b_A) = 1$
- Αποφασίζουν ανάλογα με το αν $b_A = b_B$
- Προβλήματα;

Coin flipping over the telephone

Pedersen commitments

- Επιλογή κυκλικής ομάδας $\mathbb{G}$ τάξης q με δύσκολο DLP
  - Επιλογή τυχαίων generators $g, h \leftarrow_{\$} \mathbb{G}$
  - Trusted setup: Τα g, h πρέπει να επιλέγονται ομοιόμορφα και ανεξάρτητα
- **Δέσμευση**: Για μήνυμα $m \in \mathbb{Z}_q$ υπολογισμός:
  - $c \leftarrow Commit(m, r) = g^m h^r$ με $r \leftarrow_{\$} \mathbb{Z}_q$
- **Άνοιγμα:**
  - Αποστολή c, m, r
  - Επαλήθευση αν $c = g^m h^r$

Generalized Pedersen Commitments - Vector commitments

- Δέσμευση σε vector $\boldsymbol{m} = (m_1, \dots, m_n) \in \mathbb{Z}_q^n$
- Επιλογή $\{g_i\}_{i=1}^n, h \leftarrow_{\$} \mathbb{G}$
- Υπολογισμός $c \leftarrow (\prod_{i=1\dots n} g_i^{m_i}) \cdot h^r$

Ομομορφικές Ιδιότητες

Πολλαπλασιασμός commitments - άθροισμα committed values

$$c_1 \cdot c_2 = Commit(m_1, r_1) \cdot Commit(m_2, r_2) =$$
$$g^{m_1} h^{r_1} \cdot g^{m_2} h^{r_2} = g^{m_1+m_2} h^{r_1+r_2} =$$
$$Commit(m_1 + m_2, r_1 + r_2)$$

Pedersen commitments

Ιδιότητες: Binding

Αν το DLOG είναι δύσκολο στην $\mathbb{G}$, τότε το σχήμα Pedersen διαθέτει την ιδιότητα της (υπολογιστικής) δέσμευσης **(computational binding)**.

Έστω ότι μπορούν να βρεθούν $m, m', \mathrm{r}, \mathrm{r}'$ με $c = g^m h^r$ και $\mathrm{c} = g^{m'} h^{r'}$ και $m \neq m'$. Τότε:

$$g^m h^r = g^{m'} h^{r'} \Rightarrow$$

$$g^{m-m'} = h^{r'-r} = g^{x(r'-r)} \Rightarrow$$

$$m - m' = x(r' - r) \pmod q \Rightarrow$$

$$x = \frac{r' - r}{m - m'}$$

Ποιες είναι οι συνέπειες για τη διαδικασία παραγωγής κλειδιών?

Ιδιότητες: Hiding

Το σχήμα Pedersen διαθέτει την ιδιότητα της τέλειας απόκρυψης **(perfect hiding)**.

Έστω ότι $c = g^m h^r = g^{m+xr}$

Ακόμα και ένας αντίπαλος που μπορεί να επιλύσει το DLP θα έρθει αντιμέτωπος με μια εξίσωση:

$$d = m + xr$$

με m, r άγνωστα.

- **Μία σχέση – δύο άγνωστοι**
- **Για κάθε m υπάρχει r για το οποίο $d = m + xr$**

Ένα σχήμα δέσμευσης δεν μπορεί να είναι ταυτόχρονα και **perfectly hiding** και **perfectly binding**.

Αν ειναι perfectly hiding τότε $\forall c$ υπάρχουν **τουλάχιστον** 2 διαφορετικά m που το παράγουν.

Άρα ο αντίπαλος του binding (unbounded) θα μπορούσε να τα βρει και έτσι να αλλάξει το μήνυμα στο οποίο έχει κάνει commit. και αντίστροφα...

Συμβατότητα ιδιοτήτων

Σχήματα Διαμοιρασμού Μυστικών

Δεν θέλουμε κρίσιμα κρυπτογραφικά δεδομένα να βρίσκονται στην κατοχή μιας μόνο οντότητας.

- Κλειδί αποκρυπτογράφησης
- Κλειδί υπογραφής

- Πρωτόκολλα διαμοιρασμού κλειδιών σε μερίδια και απόδοσης τους σε παίκτες
- Πρωτόκολλα κοινής υπογραφής
- Πρωτόκολλα κοινής κρυπτογράφησης

Εισαγωγή

Ορισμός: Ένα σχήμα διαμοιρασμού μυστικών αποτελείται από δύο αλγόριθμους.

- $\boldsymbol{Share(s, t, n) \rightarrow (s_1, s_2, \ldots, s_n)}$
  - Δημιουργεί n μερίδια του μυστικού
  - Πιθανοτικός
- $\boldsymbol{Reconstruct(s_1, s_2, \ldots, s_t) \rightarrow s}$
  - Ανακατασκευάσει το μυστικό από $t \leq n$ μερίδια.
  - Ντετερμινιστικός

Σχήματα Διαμοιρασμού Μυστικών

- Μοιράζουμε το μυστικό s σε n παίκτες $P_1, \dots, P_n$ ώστε
  - Οποιοδήποτε υποσύνολο από t παίκτες να μπορεί να το ανακτήσει (**ορθότητα**).
  - Κανένα υποσύνολο από $t-1$ παίκτες να μην μπορεί. (**ασφάλεια**).

  Formally:
  - Για κάθε s, s' και για κάθε υποσύνολο από το πολύ $t-1$ μερίδια οι κατανομές των $Share(s,t,n)$ και $Share(s',t,n)$ είναι μη διακρίσιμες.
  - Unconditional ορισμός

Ο διαμοιρασμός γίνεται από μια οντότητα η οποία ονομάζεται **διανομέας** D την οποία εμπιστευόμαστε (**αρχικά**)

(t,n)Threshold secret sharing

Additive secret sharing

Έστω $(\mathbb{G}, +)$ μια ομάδα και $s \in \mathbb{G}$ ένα στοιχεία της. Θέλουμε να το μοιράσουμε σε n παίκτες:

- Διαλέγουμε ομοιόμορφα $s_1, s_2, \cdots, s_{n-1} \leftarrow_{\$} \mathbb{G}$
- Θέτουμε $s_n \leftarrow s - \sum_{i=1 \cdots n-1} s_i$
- Μερίδια: $\{s_i\}_{i=1}^{n}$
- Ανακατασκευή: $s = \sum_{i=1 \cdots n} s_i$

Θέλουμε να μοιράσουμε $s \in \{0,1\}^l$ σε n παίκτες:

- Διαλέγουμε ομοιόμορφα $s_1, s_2, \cdots, s_{n-1} \leftarrow_{\$} \{0,1\}^l$
- Θέτουμε $s_n \leftarrow s \oplus (\oplus_{i=1 \ldots n-1} s\_i)$
- Μερίδια: $\{s_i\}_{i=1}^{n}$
- Ανακατασκευή: $s = \oplus_{i=1 \ldots n} s_i$

Πρόβλημα: Ένας παίκτης μπορεί να εμποδίσει την ανακατασκευή

Oops. Cryptographers cancel election results after losing decryption key.

Shamir Secret Sharing (1979)

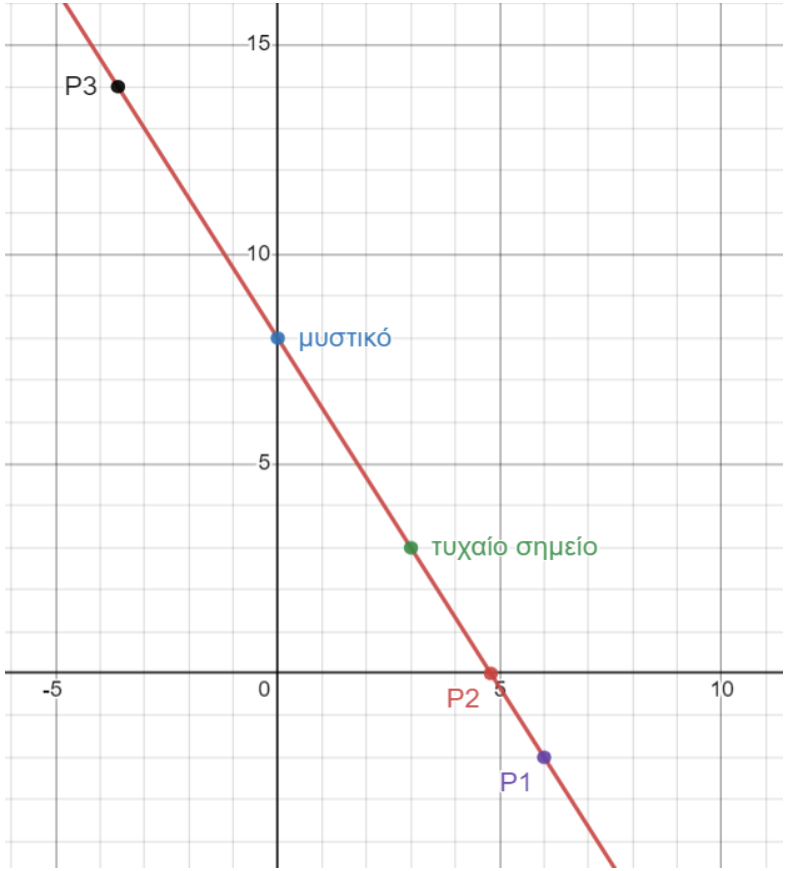
Βασίζεται σε πολυώνυμα σε πεπερασμένο σώμα $\mathbb{F}_p$ με $s \in \mathbb{F}_p$, $|\mathbb{F}_p| > n$, p πρώτος

Διαίσθηση

- Από 2 σημεία διέρχεται μοναδική ευθεία.
- Από 1 σημείο διέρχονται άπειρες.

$(2, n)$ secret sharing του s

- Ορίζουμε μια ευθεία $y = ax + s$.
- Δίνουμε στους n παίκτες τυχαία σημεία της (μερίδια).
- Οποιοιδήποτε 2 παίκτες μπορούν να το ανακατασκευάσουν.
- 1 παίκτης μόνος του δεν μπορεί.



Shamir Secret Sharing

- Υπάρχουν άπειρα πολυώνυμα βαθμού t που περνούν από t σημεία
- Υπάρχει μοναδικό πολυώνυμο βαθμού $t - 1$ που περνά από t σημεία

Έστω ένα πολυώνυμο βαθμού $t - 1$:

$$p(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$

- Μπορεί να ανακατασκευαστεί με **μοναδικό** τρόπο από t σημεία $(x_i, p(x_i))$ με διαφορετικές τετμημένες.
- Συντελεστές Lagrange
  - $\lambda_i(x) = \prod_{\substack{k=1 \\ k \neq i}}^{t} \frac{x - x_k}{x_i - x_k}$ ώστε $\lambda_i(x_i) = 1$ και $\lambda_i(x) = 0 \; \forall x \neq \mathrm{x}_i$.
- Πολυώνυμο Lagrange

$$p(x) = L(x) = \sum_{i=1}^{t} \lambda_i(x) p(x_i)$$

Πολυωνυμική Παρεμβολή

Διανομή

Ο διανομέας (TTP) που θέλει να μοιράσει ένα μυστικό s:

- Επιλέγει και δημοσιοποιεί έναν πρώτο p
- Επιλέγει τυχαία $t-1$ συντελεστές $\{a_1, \cdots, a_{t-1}\}$ και θέτει $\alpha_0 = s$
- Προκύπτει $p(x) = s + a_1 x + \cdots + a_{t-1} x^{t-1} \, mod \, p \; (p(0) = s)$
- Μερίδιο παίκτη P_i το σημείο $(i, p(i))$

Shamir Secret Sharing

Ανακατασκευή από t παίκτες

- Κάθε παίκτης P_i υπολογίζει: $\lambda_i(0) = \prod_{\substack{k=1 \\ k \neq i}}^{t} \frac{-k}{i-k}$
- Ενώνουν τα μερίδια τους:

$$p(0) = \sum_{i=1}^{t} \lambda_i(0) p(i)$$

- Δεν μας ενδιαφέρει το πολυώνυμο αλλά το $p(0)$

Shamir Secret Sharing

- Πληροφοριοθεωρητική ασφάλεια αν ο αντίπαλος διαθέτει λιγότερα από t μερίδια
- Μπορούν να προστεθούν εύκολα καινούρια μερίδια, χωρίς να αλλάξουν τα παλιά: Υπολογισμός νέων σημείων
- Εύκολη αντικατάσταση μεριδίων: Υπολογισμός νέων σημείων (πρέπει να γίνει ασφαλής καταστροφή των παλιών)
- Σημαντικοί παίκτες: περισσότερα από ένα μερίδια
- Αλλαγή Μεριδίων: Τροποποίηση πολυωνύμου χωρίς να αλλάξει το μυστικό
- Ομομορφικές ιδιότητες (άθροισμα πολυωνύμων είναι πολυώνυμο)
  - $s_1 + s_2 = f(0) + g(0) = (f + g)(0)$

Παρατηρήσεις

Μειονεκτήματα: Απαιτείται Εμπιστοσύνη

- **Κακόβουλος διανομέας:** Λανθασμένα μερίδια σε τμήμα των παικτών
- **Κακόβουλος παίκτης:** Παροχή λανθασμένων μεριδίων κατά τη διάρκεια της ανακατασκευής

Λύση: Συνδυασμός με σχήμα δέσμευσης (**Verifiable Secret Sharing**)

- Ο διανομέας μαζί με τα μερίδια παρέχει και δεσμεύσεις για τους συντελεστές
- Οι παίκτες επαληθεύουν ότι οι δεσμεύσεις δίνουν το σημείο τους

Παρατηρήσεις

Δημιουργία Κλειδιών από (trusted) dealer

- Οι παίκτες είναι ’αρχές’ που συνεργάζονται στην αποκρυπτογράφηση
- Επιλογή κατάλληλης ομάδας τάξης q
- Κανονικός υπολογισμός δημοσίου κλειδιού $y = g^x$
- Χρήση σχήματος Shamir για διαμοιρασμό του ιδιωτικού $x \ (mod\ q)$
- Αποτέλεσμα: Δημόσιο κλειδί και μερίδια

$$KGen(1^\lambda) = (y, \left(i, p(i)\right)_{i=1})$$

- Κρυπτογράφηση: Κανονικά

$$Enc_y(m) = (G_1, G_2) = (g^r, m \cdot y^r)$$

Threshold ElGamal

Αποκρυπτογράφηση: Σε τρία βήματα

1.‘Αποκρυπτογράφηση’ μεριδίων

Κάθε παίκτης υπολογίζει και δημοσιοποιεί το $c_i = G_1^{p(i)}$

2.Συνδυασμός

Συγκεντρώνονται t ‘αποκρυπτογραφημένα’ μερίδια (i, c_i) τα οποία συνδυάζονται ως:

$$C = \prod_i c_i^{\lambda_i(0)} = \prod_i G_1^{p(i)\lambda_i(0)} = G_1^{\sum_i p(i)\lambda_i(0)} = G_1^{p(0)} = G_1^{x}$$

3. Αποκρυπτογράφηση

$$m = G_2 \cdot C^{-1}$$

Παρατήρηση:

Το ανακατασκευασμένο κλειδί δεν εμφανίζεται πουθενά.

Threshold ElGamal