Κρυπτοσυστήματα Διακριτού Λογαρίθμου

Παναγιώτης Γροντάς - Άρης Παγουρτζής

28/11/2023

ΕΜΠ - Κρυπτογραφία

DLP

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 $g^{x_1 \cdot x_2}$

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 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 - (Υπενθύμιση)

$CDHP \leq DLP$
Αν μπορούμε να λύσουμε το DLP, τότε μπορούμε να υπολογίζουμε 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: $DDHP \leq CDHP \leq DLP$

Θεώρημα
Έστω ομάδα $\mathbb{G}$ τάξης q και $g \in \mathbb{G}$. Έστω $\mathcal{A}$ PPT αλγόριθμος με την εξής ιδιότητα:

$$u \leftarrow\$ \mathbb{G} : \Pr[\mathcal{A}(u) = DLP(u)] = \epsilon$$

Υπάρχει PPT αλγόριθμος $\mathcal{B}$ με την ιδιότητα:

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

Απόδειξη
Ο αλγόριθμος $\mathcal{B}$ είναι ο εξής:

Algorithm 1 DLP Self Reducibility

Είσοδος $u \in \mathbb{G}$

$a \leftarrow\$ \mathbb{Z}_q$

$u_1 \leftarrow u \cdot g^a$

$a_1 \leftarrow \mathcal{A}(u_1)$

if $g^{a_1} \neq u_1$ **then**

  return fail

else

  return $a_1 - a$

end

DLP Random Self - Reducibility (Παρατηρήσεις)

Με $n_0 \cdot \lceil \frac{1}{\epsilon} \rceil$ επαναλήψεις η πιθανότητα επιτυχίας είναι:

$$\Pr[\mathcal{B}(u) = DLP(u)] = 1 - (1-\epsilon)^{n_0 \cdot \lceil \frac{1}{\epsilon} \rceil} \geq 1 - e^{-n_0}$$

Συμπέρασμα: Εύκολο DLP για μη αμελητέο ποσοστό τυχαίων στοιχείων, εύκολο για όλα τα στοιχεία της ομάδας *Συνέπεια*: Κάθε random self - reducible πρόβλημα το οποίο είναι δύσκολο στη χειρότερη περίπτωση θα είναι και δύσκολο στη μέση περίπτωση.

Κατάλληλα 'Δύσκολα" προβλήματα για κρυπτογραφία Δεν ισχύει για όλα τα NP-hard προβλήματα

Αλγόριθμοι επίλυσης DLP

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 $g^x = y$ Εναλλακτικά:

Precomputation όλων των τιμών (x, g^x) $\forall x \in \mathbb{Z}_q$
Ταξινόμηση ως προς g^x
Δυαδική αναζήτηση
Σε κάθε περίπτωση: Πολυπλοκότητα $O(2^\lambda)$ Γενικευμένη μέθοδος - δεν εξαρτάται απο χαρακτηριστικά ομάδας

Αλγόριθμος Baby step - Giant Step (Shanks)

Αλγόριθμος Meet-In-The Middle

- Στόχος: εύρεση $x : y = g^x$
- Βασική ιδέα: $\forall x \in \mathbb{Z}, \exists k, a, b \in \mathbb{Z} : \;\; x = ak + b$,
- $y = g^x \Rightarrow y = g^{ak} \cdot g^b \Rightarrow yg^{-ak} = g^b$
- Θα υπολογίζουμε g^b και yg^{-ak} μέχρι να συναντηθούν
    1. Ξεκινάμε στη 'μέση': $k = \lceil \sqrt{q} \rceil$
    2. **Baby steps - μέγεθος** 1:
       Υπολογίζουμε $g^b, b \in \{0, 1, \cdots, k-1\}$ και αποθηκεύουμε
    3. **Giant steps - μέγεθος** k:
       Υπολογίζουμε $yg^{-ak}, a \in \{0, 1, \cdots, k-1\}$ και το αναζητούμε στα αποτελέσματα του Βημ. 2
    4. Όταν βρεθεί υπολογίζουμε: $x = ak + b$

Πολυπλοκότητα Χρόνου: $O(2^{\frac{\lambda}{2}})$ - Βέλτιστη για γενικευμένο

Πολυπλοκότητα Χώρου: $O(2^{\frac{\lambda}{2}})$ - Βέλτιστη αυτή του Pollard rho σταθερή

Παράδειγμα Baby step - Giant Step

Θέλουμε το $2^x = 17 \pmod{29}$ στο $\mathbb{Z}_{29}^* = \langle 2 \rangle$, $\lceil \sqrt{29} \rceil = 6$

- $b \in \{0 \cdots 5\}$
- $2^0 = 1 \pmod{29}$
- $2^1 = 2 \pmod{29}$
- $2^2 = 4 \pmod{29}$
- $2^3 = 8 \pmod{29}$
- $2^4 = 16 \pmod{29}$
- $2^5 = 3 \pmod{29}$

- $a \in \{0 \cdots 5\}$
- $17 \cdot 2^{-0 \cdot 6} = 17 \pmod{29}$
- $17 \cdot 2^{-1 \cdot 6} = 27 \pmod{29}$
- $17 \cdot 2^{-2 \cdot 6} = 19 \pmod{29}$
- $17 \cdot 2^{-3 \cdot 6} = 8 \pmod{29}$
- Βρέθηκε

Άρα $x = 18 + 3 = 21$

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 DLP σε κάθε υποομάδα (εύρεση $x \pmod{p_i^{e_i}}$)

Συνδυασμός με CRT

(B) - Smooth Number
Μπορεί να παραγοντοποιηθεί σε μικρούς πρώτους ($< B$)- Αν ισχύει για την τάξη επιταχύνει σημαντικά τον αλγόριθμο - κάνει το DLP πιο εύκολο.

Αλγόριθμος Pohlig-Hellman

- Παραγοντοποιούμε την τάξη: $p - 1 = \prod_{i=1}^{m} p_i^{e_i}$
- Για κάθε p_i γράφουμε $x = x_0 + x_1 p_i + \cdots + x_{e_i-1} p_i^{e_i-1} \pmod{p_i^{e_i}}$ με $x_j \in \{0, \cdots, p_i - 1\}$
- Θα υπολογίσουμε τους συντελεστές ως εξής:
- Για το x_0 ισχύει: $y^{\frac{p-1}{p_i}} = g^{x_0 \frac{p-1}{p_i}} \pmod{p}$ (1) επειδή:

$$y^{\frac{p-1}{p_i}} = (g^x)^{\frac{p-1}{p_i}} = g^{(x_0 + x_1 p_i + \cdots + x_{e_i-1} p_i^{e_i-1}) \frac{p-1}{p_i}} =$$
$$g^{(x_0 + K p_i) \frac{p-1}{p_i}} = g^{x_0 \frac{p-1}{p_i}} g^{K p_i \frac{p-1}{p_i}} =$$
$$g^{x_0 \frac{p-1}{p_i}} \pmod{p}$$

- Υπολογισμός x_0 (πχ. είτε με brute force (συνήθως) είτε με αλγόριθμο Shanks για πιο μεγάλες τιμές)

Αλγόριθμος Pohlig-Hellman (2)

Για τον υπολογισμό των υπόλοιπων συντελεστών:

- Δημιουργούμε ακολουθία $\{y_j\}$ με $y_0 = y$ και
- $y_j = y_{j-1} \cdot g^{-(x_0 + x_1 p_i + \cdots + x_{j-1} p_i^{j-1})} \pmod{p}$
- Γενικεύοντας την (1) έχουμε: $y_j^{\frac{p-1}{p_i^{j+1}}} = g^{x_j \frac{p-1}{p_i}}$

$$
\begin{aligned}
y_j^{\frac{p-1}{p_i^{j+1}}} &= (g^{x-(x_0+x_1p_i+\cdots+x_{j-1}p_i^{j-1})})^{\frac{p-1}{p_i^{j+1}}} \\
&= (g^{x_j p_i^j + \cdots + x_{e_i-1} p_i^{e_i-1}})^{\frac{p-1}{p_i^{j+1}}} = (g^{x_j p_i^j + K p^{j+1}})^{\frac{p-1}{p_i^{j+1}}} \\
&= (g^{x_j p_i^j})^{\frac{p-1}{p_i^{j+1}}} (g^{K p^{j+1}})^{\frac{p-1}{p_i^{j+1}}} = (g^{x_j})^{\frac{p-1}{p_i}}
\end{aligned}
$$

- Υπολογίζουμε το x_j

Συνδυασμός λύσεων με CRT

Pohlig-Hellman - παράδειγμα

Θέλουμε το $2^x = 17 \pmod{29}$ **στο** $\mathbb{Z}_{29}^* = \langle 2 \rangle$
Παραγοντοποιούμε την τάξη: $28 = 2^2 7$

$x_2 = x_{20} + 2x_{21} \pmod 4$ και

$x_7 = x_{70} \pmod 7$

Υπολογισμός x_{20} **για το** x_2
$y^{\frac{p-1}{2}} = g^{x_{20}\frac{p-1}{2}} \Rightarrow 17^{14} = 2^{14x_{20}} \Rightarrow 2^{14x_{20}} = 28 = -1 \pmod{29}$

Άρα $x_{20} = 1$

Υπολογισμός y_1 **για το** x_2
$y_1 = yg^{-x_{20}} = 17 \cdot 2^{-1} = 17 \cdot 15 = 23 \pmod{29}$

Pohlig-Hellman - παράδειγμα

Υπολογισμός x_{21} **για το** x_2

$y_1^{\frac{p-1}{4}} = g^{x_{21}\frac{p-1}{2}} \Rightarrow 23^7 = 2^{14x_{21}} \Rightarrow 2^{14x_{21}} = 1 \pmod{29}$

Άρα $x_{21} = 0$

Άρα $x_2 = 1 + 0 = 1 \pmod 4$

Υπολογισμός x_{70} **για το** x_7

$y^{\frac{p-1}{7}} = g^{x_{70}\frac{p-1}{7}} \Rightarrow 17^4 = 2^{4x_{70}} \Rightarrow 2^{4x_{70}} = 1 \pmod{29}$

Άρα $x_{70} = 0$

Άρα $x_7 = 0 \pmod 7$

Από $x_2 = 1 + 0 = 1 \pmod 4$ και $x_7 = 0 \pmod 7$ με CRT προκύπτει $x = 21$

Οικογένεια πιθανοτικών αλγορίθμων που ισχύουν μόνο στο $\mathbb{Z}_p^*$ - στενή σχέση με παραγοντοποίηση

Βήμα 1
Εύρεση k μικρών πρώτων $\{p_1, \cdots, p_k\}$ ($p_i \leq B\, \forall i$) και

$l > k$ τιμών $\{x_1, \cdots, x_l\}$ ώστε $g_i = g^{x_i} \pmod{p}$ να είναι B-smooth.

Προκύπτουν οι παρακάτω l σχέσεις:

$$\left\{ g^{x_i} = \prod_{i=1}^{k} p_i^{e_{i,l}} \pmod{p} \Rightarrow x_i = \sum_{i=1}^{k} e_{i,l} \cdot log_g p_i \pmod{p-1} \right\}_{i=1}^{l}$$

Παρατήρηση: Ανεξάρτητο βήμα από το $y = g^x$ (για το οποίο θέλουμε να βρούμε διακριτό λογάριθμο).

Βήμα 2
Για το y επιλέγουμε ομοιόμορφα a ώστε $g^a \cdot y$ να είναι B-smooth.

Άρα:

$$g^a \cdot y = \prod_{i=1}^{k} p_i^{e_i} \pmod{p} \Rightarrow a + x = \sum_{i=1}^{k} e_i \cdot log_g p_i \pmod{p-1}$$

Σύστημα $l+1$ εξισώσεων με $k+1$ αγνώστους $x, log_g p_i$.
Επίλυση και εύρεση x. Πολυπλοκότητα: $2^{\sqrt{\lambda log \lambda}}$ Υπογραμμική
Παρατήρηση: Χρειάζεται την έννοια του πρώτου. Δεν λειτουργεί σε όλες τις ομάδες.

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

Απόδειξη 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

$(\frac{g^x}{p}) = (g^x)^{\frac{p-1}{2}}$ και $g^{p-1} = 1 \pmod p$ (FLT)

g γεννήτορας: $g^{\frac{p-1}{2}} = -1 \pmod p \Rightarrow (\frac{g^x}{p}) = (-1)^x$

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

Αλγόριθμοι Διαχωρισμού με βάση Legendre

Για τυχαία τριάδα: $\Pr\left[(\frac{g^c}{p}) = 1\right] = \frac{1}{2}$

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

Πλεονέκτημα: $\mid \frac{1}{2} - \frac{3}{4} \mid = \frac{1}{4}$

Χρήση πλήρους transcript διαχωρισμός με μεγαλύτερο πλεονέκτημα:

Algorithm 2 Ο αλγόριθμος διαχωρισμού

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

if $(\frac{g^c}{p}) = 1 \wedge ((\frac{g^a}{p}) = 1 \vee (\frac{g^b}{p}) = 1)$ **then**

  Επιστροφή "Τριάδα Diffie Hellman"

else

  Επιστροφή "Τυχαία Τριάδα"

end

Πλεονέκτημα: $\frac{3}{8}$ (γιατί;)

ΜΗ ΑΜΕΛΗΤΕΟ σε κάθε περίπτωση

Επιλογή Ομάδας $\mathbb{G}$

Καθορίζει τη δυσκολία του προβλήματος

- Υποομάδα πρώτης τάξης q του $(\mathbb{Z}_p^*, \cdot)$ με p πρώτο
- safe prime $p = 2q + 1$ υποομάδα τετραγωνικών υπολοίπων του $\mathbb{Z}_p^*$
- Λόγοι:
    - Όχι εύκολο DDHP
    - Εύκολη εύρεση γεννήτορα
- Επίσης p Schnorr prime: $p = kq + 1$ με q πρώτο
- Όμως: Ευάλωτες στον υποεκθετικό index calculus

- $(\mathcal{E}(\mathbb{F}_q), +)$ - Ελλειπτικές καμπύλες
- 'Λογάριθμος' αφορά πρόσθεση σημείων
- Δεν υπάρχει η εννοια του πρώτου
- ίδια επίπεδα ασφάλειας με μικρότερο μέγεθος κλειδιών

Μεγέθη

Symmetric Security	$\lvert p \rvert$	$\lvert q \rvert$
80 bits	1024	160
112 bits	2048	224
128 bits	3072	256
192 bits	7680	384
256 bits	15360	512

Ελλεπτικές καμπύλες

Γενικά

- Πλούσιο σε ιστορία μαθηματικό αντικείμενο
  - Πρώτη εμφάνιση Διόφαντος 3 αιώνας πΧ (ρητές ρίζες της $y^2 = x^3 - x + 9$)
  - Μελέτη εδώ και 300 έτη
- Κρυπτογραφία: 80s (Neil Koblitz, Victor Miller)
- Βασίζεται στο πρόβλημα του Διακριτού Λογάριθμου
  - 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 - καλύτερη απόδοση

RSA	EC
1024	160
2048	224
3072	256

Γενική μορφή

Έστω $\mathbb{F}$ ένα σώμα.

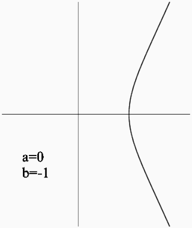
Ορισμός $\mathcal{E}(\mathbb{F})$
Μια ελλειπτική καμπύλη $\mathcal{E}$ πάνω από το $\mathbb{F}$ είναι το σύνολο των σημείων $(x, y) \in \mathbb{F}^2$, που ικανοποιούν την εξίσωση Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{F}$$

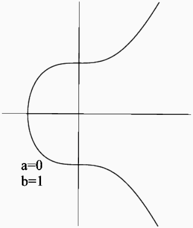
και ένα στοιχείο $\mathcal{O}$, (- *σημείο στο άπειρο*)

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

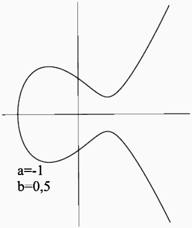
Ελλειπτικές καμπύλες στο $\mathbb{R}$ (μορφή)



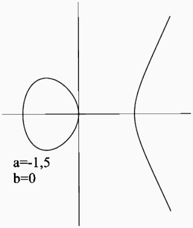
$y^2 = x^3 - 1$



$y^2 = x^3 + 1$



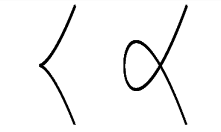
$y^2 = x^3 - x + \frac{1}{2}$



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

Παρατηρήσεις στη μορφή ελλειπτικών καμπυλών

- Συμμετρία ως προς άξονα x
- Συμπίεση σημείου: Αποθηκεύουμε τετμημένη και 1 bit για πάνω ή κάτω από τον άξονα των x (δηλ. $(x, 0)$ ή $(x, 1)$)
- Προς αποφυγή Singular καμπύλες: Πολλαπλές ρίζες, σημεία τομής



Πρέπει $4a^3 + 27b^2 \neq 0$

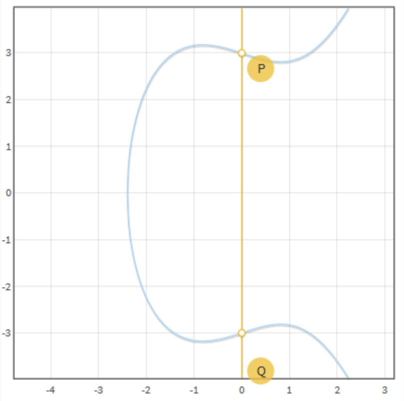
Ομάδα Σημείων Ελλειπτικής καμπύλης

Πράξη Ομάδας: Μέθοδος εφαπτομένης (Διόφαντος) ή χορδής - Πρόσθεση (Poincaré)
Τα σημεία μιας ελλειπτικής καμπύλης αποτελούν αβελιανή ομάδα ως προς την *πρόσθεση σημείων*

- ουδέτερο στοιχείο $\mathcal{O}$
- αντίθετο σημείου P στην $\mathcal{E}(\mathbb{R})$:
  - Αν $P = \mathcal{O}$, τότε $-P = \mathcal{O}$
  - Αν $P = (x, y)$ τότε $-P = (x, -y)$ (ανήκει στην $\mathcal{E}$ λόγω συμμετρίας)
- πρόσθεση: Για τρία σημεία P, Q, R στην ίδια ευθεία: $P + Q + R = \mathcal{O}$
- πρόσθεση: προσεταιριστική και αντιμεταθετική

(Γεωμετρική) Ερμηνεία

Το άθροισμα $P + Q$



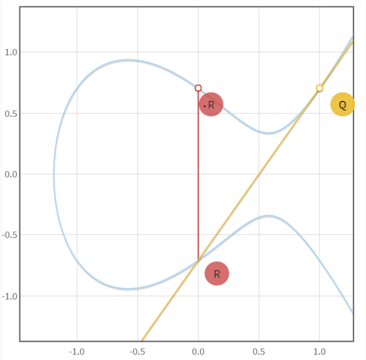
Αν $P = \mathcal{O}$, τότε $\mathcal{O} + Q = Q$

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

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

Αν $P = Q$ τότε:

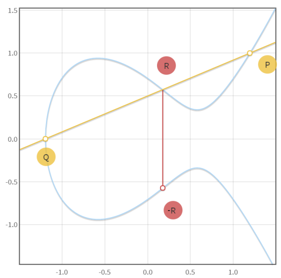
- Θεωρούμε την εφαπτομένη στο P
- Βρίσκουμε το σημείο τομής R με την $\mathcal{E}$.
- Βρίσκουμε το αντίθετο

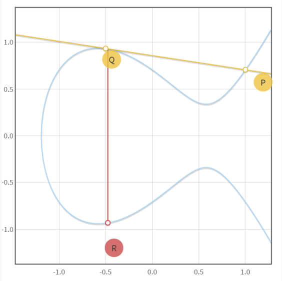


Elliptic Curve point addition

Αν $P \neq Q$ τότε:

- Θεωρούμε το $\overline{PQ}$
- Αν υπάρχει σημείο τομής R με την $\mathcal{E}$:
    - Βρίσκουμε το αντίθετο
- Αν δεν υπάρχει σημείο τομής:
    - Σε ένα εκ των P, Q η $\overline{PQ}$ θα εφάπτεται με την $\mathcal{E}$
    - Βρίσκουμε το αντίθετο

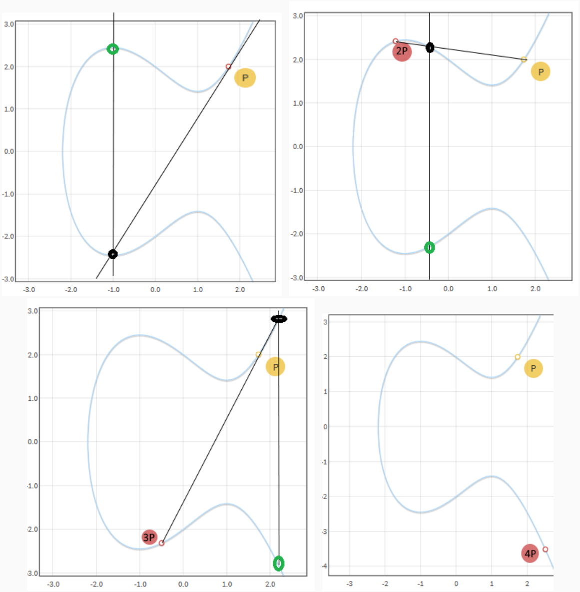




Αλγεβρική αναπαράσταση

- Συντελεστής ευθείας $\overline{PQ}$: $m = \frac{y_P - y_Q}{x_P - x_Q}$
- Εύρεση σημείου τομής (x_R, y_R) με ελλειπτική καμπύλη
- Επίλυση τριτοβάθμιας εξίσωσης

Πολλαπλασιασμός σημείου με ακέραιο $nP = P + P + \cdots + P$



Double and add

Υπολογισμός nP

Απαιτούνται $n-1$ προσθέσεις

Λύση: Square and multiply - Double and add

$$\begin{aligned} 17P &= P + 16P \\ 2P &= P + P \\ 4P &= 2P + 2P \\ 8P &= 4P + 4P \\ 16P &= 8P + 8P \end{aligned}$$

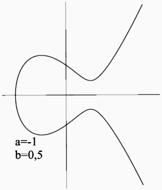
Ελλειπτικές καμπύλες στο $\mathbb{F}_p$

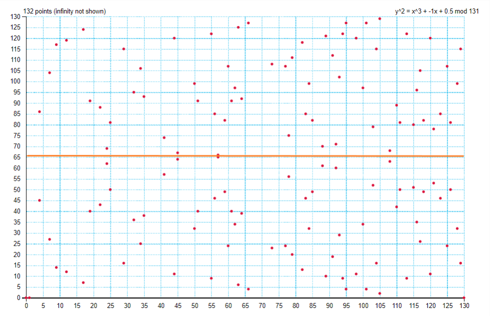
Ορισμός $\mathcal{E}(\mathbb{F}_p)$

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

Παράδειγμα: $y^2 = x^3 - x + \frac{1}{2} \pmod{131}$

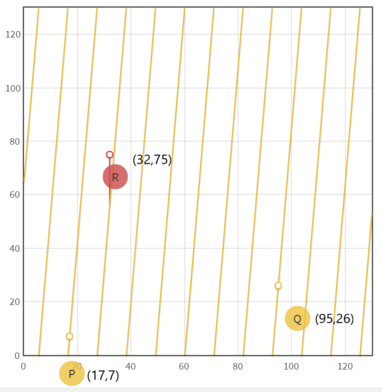
Discrete Elliptic Curve Plotter





Πρόσθεση σημείων στο $\mathbb{F}_p$

Η ευθεία που συνδέει τα P, Q, R επαναλαμβάνεται



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

Εύρεση τάξης ομάδας: Το πολύ $2p+1$ σημεία (συμμετρία +)

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

Ισοδύναμα: $|\mathcal{E}(\mathbb{F}_p)| = p+1-t$ με $|t| \leq 2\sqrt{p}$
t: trace της καμπύλης.

Υπολογισμός
Αλγόριθμος Schoof σε $O(log(p))$ με βελτιώσεις Elkiens, Atkin (SEA)

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

Υπολογισμός Σημείου Καμπύλης

- Επιλογή ομοιόμορφου $x_0 \xleftarrow{\$} \mathbb{Z}_p$
- Αντικατάσταση στην εξίσωσης καμπύλης $y_0^2 = f(x_0) \bmod p$
- Έλεγχος αν $f(x_0)$ τετραγωνικό υπόλοιπο - όπως στο $\mathbb{Z}_p$
- Αν ναι, υπολογισμός τετραγωνικής ρίζας $f(x_0)$

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

Ομάδα για κρυπτογραφικές εφαρμογές: Θέλουμε να έχει πρώτη τάξη
Αν $|\mathcal{E}(\mathbb{F}_p)|$ πρώτος δουλεύουμε σε αυτήν
Αλλιώς ψάχνουμε μεγάλη υποομάδα πρώτης τάξης

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

Υπολογισμός τάξης υποομάδας σημείου στην $\mathcal{E}(\mathbb{F}_p)$
Θεώρημα Lagrange: Η τάξη κάθε υποομάδας διαιρεί την τάξη της ομάδας

Υπολογισμός τάξης υποομάδας με σημείο βάσης (γεννήτορα) G

- Εύρεση τάξη ομάδας με αλγόριθμο Schoof
- Εύρεση των διαιρετών της τάξης, d
- Επιστροφή $min\{d : dG = \mathcal{O}\}$

Εύρεση σημείων βάσης
Θέλουμε γεννήτορες μεγάλων υποομάδων

- Επιλογή τάξης υποομάδας (μεγάλος πρώτος q): $q \mid |\mathcal{E}|$
- Υπολογισμός cofactor $h = \frac{|\mathcal{E}|}{q}$
- Επιλογή τυχαίου σημείου P
- Υπολογισμός $G = hP$
- Αν $G = \mathcal{O}$ επανάληψη

Ισοδύναμες μορφές ελλειπτικών καμπυλών

Βελτιστοποίηση πρόσθεσης σημείων και πολλαπλασιασμού σημείου με ακέραιο

- 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: $y^2 + x^2 = 1 + dx^2y^2, d \in \{0, 1\}$ (προστασία από side channels)

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!

- $\#\mathcal{E}(\mathbb{F}_p) \mid p^k - 1$ για μικρά k - υποεκθετικό DLP - MOV's attack (pairings)
- $\#\mathcal{E}(\mathbb{F}_p) = p$ - πολυωνυμικό DLP - Smart's attack

Συνέπεια: Δεν προτείνεται η παραγωγή καμπυλών, αλλά η χρήση έτοιμων

Πρότυπες καμπύλες ii

Πρότυπο NIST FIPS186-3
15 ελλειπτικές καμπύλες. Οι πιο γνωστές:

- **NIST P-256** ή **secp256r1**
  $y^2 = x^3 - 3x + b \bmod (2^{256} - 2^{224} + 2^{192} + 2^{96} - 1)$
  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** $y^2 = x^3 - 3x + b \bmod (2^{384} - 2^{128} - 2^{96} + 2^{32} - 1)$
  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

Πώς επιλέχτηκε το b - Δεν γνωρίζουμε Φόβοι για υπονόμευση

Στο πρότυπο NIST FIPS186-3 αναφέρεται ότι το b προήλθε από ένα seed s το οποίο όμως δεν αναφέρεται πώς δημιουργήθηκε.

Πρόβλημα: Δίνεται μια καμπύλη $(p, a, b, \#\mathcal{E}, q, G)$ - Πώς γνωρίζουμε ότι είναι ασφαλής (;)

Επαληθευσιμότητα: Εγγύηση ότι δεν είναι 'πειραγμένη' (nothing up my sleeve)

- Επιλογή τυχαίου αριθμού s και δημοσιοποίησή του
- Υπολογισμός $h = \mathcal{H}(s)$
- Παραγωγή των a, b από το h, δηλ. $f(h) = a$ και $g(h) = b$
- Επαληθεύσιμο υπό την υπόθεση του preimage resistance (γιατί αλλιώς πρώτα επιλογή των a,b) και μετά επιλογή h

Πρότυπες καμπύλες iv

NIST Curves: Κακή φήμη και λόγω χρήσης στην γεννήτρια τυχαιότητας Dual_EC_DRBG (NIST)

Dual_EC_DRBG
Δίνεται η καμπύλη NIST P-256, γεννήτορας P, σημείο Q, seed s

Θέσε $r = x_{sP}$

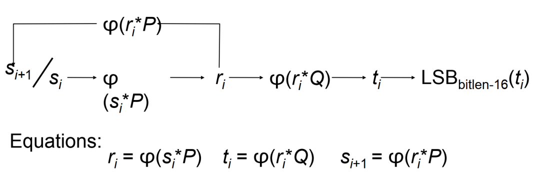
Θέσε $s' = x_{rP}$

Θέσε $t = x_{rQ}$

Επιστροφή $LSB_{-16}(t)$

Επανάληψη με $s = s'$

Πρότυπες καμπύλες v



Προβλήματα (Shumow - Ferguson 2007)

- Δεν αιτιολογείται η χρήση του Q
- Πολλά bits ως έξοδο τα οποία μπορούν να χρησιμοποιηθούν για την εύρεση του τελικού σημείου (2^{16} έλεγχοι στην εξίσωση της καμπύλης)
- Πρόβλεψη των επόμενων εξόδων με βάση την σχέση $Q = eP$ (e backdoor)

Πρότυπες καμπύλες vi

Εναλλακτικά:

secp256k1 (OpenSSL, Bitcoin)

$y^2 = x^3 + 0x + 7 \bmod (2^{256} - 2^{32} - 977)$

Curve25519 (OpenSSH)

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

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

Ανταλλαγή Κλειδιού ECDH ii

Πρωτόκολλο

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

Εφαρμογή: Pairing Based Cryptography

- Η επίθεση MOV (Menezes - Okamoto - Vanstone)
- Επίλυση ECDLP $\mathcal{E}(\mathbb{F}_p)$
- Με μεταφορά του στο $\mathbb{F}_p^k$
- k: embedding degree της καμπύλης $min\{k : |\langle G \rangle| \mid p^k - 1\}$
- Το DLP γίνεται ευκολότερο (υποεκθετικοί αλγόριθμοι), όχι όμως εύκολο
- Χρήση συνάρτηση μεταφοράς

Ορισμός Pairing

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

Ζεύξη (pairing-bilinear map): Μία *αποδοτικά* υπολογίσιμη συνάρτηση

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

1) Διγραμμική (bilinear):

$$e(G_1 + G_2, H_1) = e(G_1, H_1) \cdot e(G_2, H_1)\text{και}$$

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

ή ισοδύναμα $e(aG, bH) = e(G, H)^{ab} \quad \forall G \in \mathbb{G}_1, H \in \mathbb{G}_2\ a, b \in \mathbb{Z}$

2) Μη εκφυλισμένη (non-degenerate):
Αν $\mathbb{G} = \langle G \rangle$ τότε $\mathbb{G}_T = \langle e(G, G) \rangle$

Ορισμός Pairing (2)

Μπορεί και $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$

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

Συνέπεια ορισμού: Συμμετρία $e(aG, bG) = e(G, G)^{ab} = e(bG, aG)$

Ένα απλό παράδειγμα
$e(x, y) = 2^{xy}$ Τότε:
$e(a, b + c) = 2^{a(b+c)}$ και: $e(a, b) \cdot e(a, c) = 2^{ab} \cdot 2^{ac} = 2^{a(b+c)}$

Τα πιο γνωστά pairings: Weil, Tate, Ate

Ζεύξεις στην κρυπτογραφία

- Στο $\mathbb{G}$ κάποια προβλήματα είναι δύσκολα, αλλά στο $\mathbb{G}_T$ μπορεί να είναι εύκολα
- Λόγω της απεικόνισης e μπορούμε να μεταβούμε αποδοτικά από την δύσκολη εκδοχή στην εύκολη
- Χρήσιμη ασυμμετρίας για την κατασκευή κρυπτογραφικών πρωτοκόλλων
- Bonus: 'Πολλαπλασιασμός' σε lifted τιμές.
- Αρνητικές συνέπειες: Κάποια προβλήματα γίνονται ευκολότερα αν όχι εύκολα

Αν υπάρχει pairing

Το DDHP γίνεται εύκολο: Θέλουμε να ελέγξουμε αν $cG = (ab)G$, με δεδομένα τα aG, bG, cG.

Αποδοτικός υπολογισμός μέσω ζεύξης: $e(aG, bG) = e(G, G)^{ab}$

Σύγκριση με το $e(G, cG) = e(G, G)^c$

Το DLP γίνεται ευκολότερο: Αντί για εύρεση x από G, xG στην $\mathbb{G}$ (ελλειπτική καμπύλη)

εύρεση x από $e(G, G), e(G, xG)$ στην $\mathbb{G}_T$ (πεπερασμένο σώμα)

Διγραμμικό Πρόβλημα Απόφασης Diffie-Hellman
Δίνονται: δύο στοιχεία $H, G \in \mathbb{G}$ και τα στοιχεία $\alpha G, \beta G, e(G, G)^c$.

Ζητείται: Ισχύει $c = \alpha\beta$;

Τριμερής ανταλλαγή κλειδιού

Έστω κυκλική ομάδα με $\mathbb{G} = \langle g \rangle$

Τρεις οντότητες A, B, C με ζευγάρια ιδιωτικών - δημοσίων κλειδιών $(x_A, Y_A = x_A G), (x_B, Y_B = x_B G), (x_C, Y_C = x_C G)$.

Μπορεί να συμφωνηθεί ένα κοινό κλειδί μεταξύ τους;

Χωρίς pairings - σε 3 γύρους

1. Ο A στέλνει το Y_A στον B, ο B στέλνει το Y_B στον C, ο C στέλνει το Y_C στον A (κυκλικά).
2. Ο A υπολογίζει το $T_A = x_A Y_C = x_C x_A G$, ο B υπολογίζει το $T_B = x_B y_A = x_B x_A G$ και ο C υπολογίζει το $T_C = x_C Y_B = x_B x_C G$
3. Ο A στέλνει το T_A στον B, ο B στέλνει το T_B στον C, ο C στέλνει το T_C στον A (πάλι κυκλικά).
4. Όλοι υπολογίζουν το κοινό κλειδί ως εξής:
    - Ο A με $x_A T_C = x_B x_C x_A G$
    - Ο B με $x_B T_A = x_C x_A x_B G$
    - Ο C με $x_C T_B = x_A x_B x_C G$

Με pairings - σε 1 γύρο (Joux-2000)

Υποθέτουμε δύο ομάδες $\mathbb{G}$, $\mathbb{G}$ με τάξη ένα πρώτο q και μία συμμετρική διγραμμική ζεύξη $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.

- Όλοι οι συμμετέχοντες εκπέμπουν τα δημόσια κλειδιά τους $Y_A = x_A G, Y_B = x_B G, Y_C = x_C G$.
- Με την βοήθεια της ζεύξης το κοινό κλειδί μπορεί να υπολογιστεί ως εξής:
  - $e(Y_B, Y_C)^{x_A} = e(G, G)^{x_B x_C x_A}$
  - $e(Y_A, Y_C)^{x_B} = e(G, G)^{x_A x_C x_B}$
  - $e(Y_A, Y_B)^{x_C} = e(G, G)^{x_A x_B x_C}$

Το κρυπτοσύστημα ElGamal

Ορισμός ElGamal

Δημιουργία Κλειδιών: $\mathsf{KGen}(1^\lambda) = (y = g^x, x)$

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

Κρυπτογράφηση

- Επιλογή $r \leftarrow\$ \mathbb{Z}_q$
- $\mathsf{Enc}_y(r, m) = (g^r \bmod p, (m \cdot y^r) \bmod p)$

Αποκρυπτογράφηση

- $\mathsf{Dec}_x(a, b) = b \cdot (a^x)^{-1} \bmod p$

Ορθότητα $\mathsf{Dec}_x(\mathsf{Enc}_y(r, m)) = (my^r)((g^r)^x)^{-1} = mg^{rx-rx} = m \pmod p$

Παρατηρήσεις: Πρακτικά Θέματα

Παράμετροι κρυπτογράφησης: p, q δεν χρειάζεται να αλλάζουν ανά χρήστη όπως στο RSA

Εκτέλεση KGen μια φορά για όλους τους χρήστες

Συνήθως: $|p| = 2048, |q| = 256$

Πιθανοτική Κρυπτογράφηση: Ένα μήνυμα έχει πολλά πιθανά κρυπτοκείμενα

Message expansion: Κρυπτοκείμενο διπλάσιο του μηνύματος

Παρατηρήσεις: Πρακτικά Θέματα (2)

Επιτάχυνση Κρυπτογράφησης:

Κόστος: 2 υψώσεις σε δύναμη - 1 πολλαπλασιασμός

Ύψωση σε δύναμη: Δεν εξαρτάται από το μήνυμα

Μπορεί να προεπιλεχθούν r και να προϋπολογιστούν οι δυνάμεις g^r, y^r

Επιτάχυνση Αποκρυπτογράφησης:

$(a^x)^{-1} = (a^x)^{-1} a^{p-1} = a^{p-x-1} \pmod{p}$

1 ύψωση σε δύναμη - 1 πολλαπλασιασμός

ElGamal στην πράξη

Το μήνυμα πρέπει να είναι στοιχείο της ομάδας: $m \in \mathbb{G}$.

Όμως θα θέλαμε: $m \in \{0,1\}^*$

Σε κάποιες περιπτώσεις μπορεί να οριστεί κωδικοποίηση $f : \mathbb{G} \mapsto \{0,1\}^l$

Γενική Λύση: Hybrid Encryption

- $m \in \{0,1\}^*$
- $m_G \leftarrow\$ \mathbb{G}$
- $k = \mathsf{H}(m_G)$ με H κατάλληλη συνάρτηση σύνοψης
- Αποστολή $(\mathsf{Enc}_{EG,\mathsf{pk}}(m_G), \mathsf{Enc}_{AES,k}(m))$

Γενίκευση: Key encapsulation primitives

KPA: Γνωρίζουμε ζεύγη μηνυμάτων - κρυπτοκειμένου για τα οποία έχει χρησιμοποιηθεί η ίδια τυχαιότητα

Επίθεση

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

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

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

Μπορώ να υπολογίσω το m_2 ως:

$m_2 = c_2 \cdot (y^r)^{-1} = c_2 \cdot (c_1 \cdot m_1^{-1})^{-1}$

Μυστικότητα ElGamal $\equiv$ $CDHP$

Αντιστοιχία δημοσίων στοιχείων

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

Ευθύ: $EG \leq CDHP$:

1. Επίλυση $CDHP$
2. Υπολογισμός $g^{x_1 x_2} = y^r$
3. Εύρεση αντιστρόφου του y^r
4. Αποκρυπτογράφηση

Αντίστροφα: $CDHP \leq EG$:

1. Αποκρυπτογράφηση EG (χωρίς ιδιωτικό κλειδί)
2. $\forall a \in \mathbb{G}$ μπορώ να χρησιμοποιήσω το EG ως oracle
3. Είσοδος: $y = g^{x_2}, c = (g^{x_1}, a)$ για $a \leftarrow\$ \mathbb{G}$
4. Έξοδος: κάποιο $m \in \mathbb{G}$ ώστε $a = m \cdot g^{x_1 x_2}$
5. Άρα: $g^{x_1 x_2} = a \cdot m^{-1} \pmod{p}$

Αποδείξαμε ότι η συνάρτηση El-Gamal διαθέτει την ιδιότητα **OW-CPA (One-Wayness under Chosen Plaintext Attack)**

Ασφάλεια Κρυπτογράφησης $\mathrm{IND\text{-}CPA}$

Θεώρημα
Αν το DDHP είναι δύσκολο στην $\mathbb{G}$, τότε το κρυπτοσύστημα El Gamal διαθέτει ασφάλεια $\mathrm{IND\text{-}CPA}$.

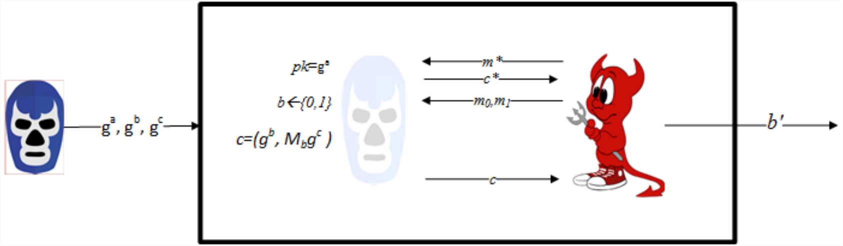
Απόδειξη:

Έστω ότι το ElGamal δεν διαθέτει ασφάλεια $\mathrm{IND\text{-}CPA}$.

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 $\mathcal{C}_{\mathrm{IND\text{-}CPA}}$ στο παιχνίδι CPA και χρήση $\mathcal{A}$ ως μαύρο κουτί
- Αποτέλεσμα: Διαχωρισμός DH - τυχαίας τριάδας με μη αμελητέα πιθανότητα

Ασφάλεια Κρυπτογράφησης IND-CPA



Ασφάλεια Κρυπτογράφησης IND-CPA

- Είσοδος: $g^{\alpha}, g^{\beta}, g^{c}$
- Στο CPA-GAME δημόσιο κλειδί $y = g^{\alpha}$
- Ο $\mathcal{B}$ απαντά στις κρυπτογραφήσεις του $\mathcal{A}$ (προσομοιώνει $\mathcal{C}_{\text{IND-CPA}}$)
- Όταν ο $\mathcal{A}$ προκαλέσει με δύο μηνύματα m_0, m_1
    - ο $\mathcal{C}_{\text{IND-CPA}}$ διαλέγει ομοιόμορφα bit $b \xleftarrow{\$} \{0, 1\}$,
    - 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 b^*
- Ο $\mathcal{B}$ εξάγει το b^*

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 μη αμελητέα ($> 1/2 + \mathsf{negl}(\lambda)$).
- Για τυχαία τριάδα: ο $\mathcal{A}$ θα πρέπει να μαντέψει τυχαία - αφού η κρυπτογράφηση δεν είναι σωστή.
- Πιθανότητα επιτυχίας: $\frac{1}{2}$.
- Άρα πλεονέκτημα $\mathcal{B}$:
  $\Pr\left[\mathcal{B}(g^a, g^b, g^{ab}) = 1\right] - \Pr\left[\mathcal{B}(g^a, g^b, g^c) = 1\right] > \mathsf{negl}(\lambda)$
- Συμπέρασμα: Ο $\mathcal{B}$ μπορεί να ξεχωρίσει μία DH τριάδα από μία τυχαία με μη αμελητέα πιθανότητα.
- ΑΤΟΠΟ, αν ισχύει η υπόθεση DDH στο $\mathbb{G}$

Ομομορφικές Ιδιότητες

Πολλαπλασιαστικός Ομομορφισμός

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

Ομομορφικές Ιδιότητες

Reencryption

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

Αλλαγή της τυχαιότητας - Αλλαγή της μορφής του μηνύματος

...χωρίς γνώση του ιδιωτικού κλειδιού

Malleability

Ομομορφικές Ιδιότητες

Προσθετικός Ομομορφισμός - Εκθετικό ElGamal
Κρυπτογράφηση του g^m αντί για m: $\mathrm{Enc}_y(r, m) = (g^r, g^m y^r)$

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

Αποκρυπτογράφηση: Λαμβάνουμε το g^m

Επίλυση διακριτού λογαρίθμου

Δεν αποτελεί πρόβλημα για κάποιες εφαρμογές

πχ. e-voting: Το m είναι το άθροισμα των ψήφων για κάποιο υποψήφιο $|m| << |q|$

Το ElGamal δεν διαθέτει CCA-security

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

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

Cramer-Shoup cryptosystem

ElGamal CCA2: Cramer-Shoup cryptosystem

- Ronald Cramer, Victor Shoup, Crypto 1998
- Επέκταση του ElGamal
- Χρήση συνάρτησης σύνοψης H (υπάρχουν εκδόσεις και χωρίς)
- Αν ισχύει η υπόθεση DDH στο $\mathbb{G}$, τότε παρέχει ασφάλεια $\mathrm{IND\text{-}CCA2}$

Δημιουργία Κλειδιών

- Επιλογή πρώτων p, q με $p = 2q + 1$
- $\mathbb{G}$ ειναι η υποομάδα ταξης 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)

ElGamal CCA2: Cramer-Shoup cryptosystem

Κρυπτογράφηση

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

ElGamal CCA2: Cramer-Shoup cryptosystem

Αποκρυπτογράφηση

- Υπολογισμός $\alpha = \mathrm{H}(u_1||u_2||e)$
- 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 $m = \frac{e}{u_1^z}$

ElGamal CCA2: Cramer-Shoup cryptosystem

Ορθότητα

- $u_1^{x_1} u_2^{x_2} \cdot (u_1^{y_1} u_2^{y_2})^{\alpha} = (g_1^{x_1} g_2^{x_2})^r \cdot (g_1^{y_1} g_2^{y_2})^{r\alpha} = c^r d^{r\alpha} = v$
- $\frac{e}{u_1^z} = \frac{mh^r}{u_1^z} = m \cdot \frac{g_1^{zr}}{g_1^{rz}} = m$

Παρατηρήσεις

- h, z αντιστοιχούν σε δημόσιο - ιδιωτικό κλειδί ElGamal
- u_1, 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

DLP-based Commitment Schemes

Coin Flipping over the telephone

Manuel Blum (1981)

- 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;

Commitment Schemes

- Σύνταξη
  - $\mathsf{ck} \leftarrow \mathsf{KGen}(1^\lambda)$
    Δημιουργία δημόσιου commitment key ck
  - $(c, o) := \mathsf{Commit}_{\mathsf{ck}}(m)$
    Δέσμευση στο m με το ck και παραγωγή τιμής ανοίγματος o
  - $\{0, 1\} := \mathsf{Open}_{\mathsf{ck}}(c, o, m)$
    Επαληθεύει αν η δέσμευση c αντιστοιχεί στο m
- Ιδιότητες
  - **Hiding** - Προστατεύει αποστολέα - καθώς δεν μπορεί να διαρρεύσει το μήνυμά του
  - **Binding** - Προστατεύει παραλήπτη - καθώς ο αποστολέας δεν μπορεί να αλλάξει την τιμή του εκ των υστέρων
- opening key = randomization για προστασία από brute-force επιθέσεις

Coin Flipping over the telephone με commitment schemes

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

Pedersen commitment

- Επιλογή ομάδας με δύσκολο DLP από TTP (trusted setup)
  - Επιλογή πρώτου p ώστε $p = 2q + 1$ πρώτος
  - $\mathbb{G} = \langle g \rangle$ υπομάδα τάξης q του $\mathbb{Z}_p^*$
  - Επιλογή τυχαίου $h \leftarrow_\$ \mathbb{G}$
  - 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:
  $c =_? g^m \cdot h^r$

Pedersen commitment (2)

Generalized Pedersen Commitments - Vector commitments
Δίνεται vector $\mathbf{m} = (m_1, \cdots, m_n)$ και $h \leftarrow\$ \mathbb{G}$ και

$\mathbf{g} = (g_1, \cdots, g_n) \leftarrow\$ \mathbb{G}^n$.

$\mathrm{Commit}(\mathbf{m}, r) = h^r \prod_{i=1}^n g_i^{m_i}$

Ομομορφικές Ιδιότητες
Πολλαπλασιασμός commitments - άθροισμα committed values

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

Ασφάλεια - Information Theoretically Hiding

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

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

Για κάθε m υπάρχει r που την επαληθεύει

Αν το DLP είναι δύσκολο τότε το σχήμα δέσμευσης είναι binding

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

DLP-based collision resistance

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

Απόδειξη (Διαισθητικά)
Αν ειναι perfectly hiding τότε $\forall c$ υπάρχουν τουλάχιστον 2 διαφορετικά m που παράγουν το ίδιο c.

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

και αντίστροφα...

Secret Sharing - Threshold Cryptosystems

Διαμοιρασμός απορρήτων - Εισαγωγή

Το πρόβλημα

Κλειδιά: κρίσιμα κρυπτογραφικά δεδομένα (όχι τα μόνα)

Για παράδειγμα: ιδιωτικό κλειδί

- Δύναμη αποκρυπτογράφησης
- Δύναμη υπογραφής

Λύση

Δεν θέλουμε να είναι στην φυσική κατοχή μίας οντότητας (μόνο)

Βασικό συστατικό Secure Multi Party Computation

Additive secret sharing

Έστω $(\mathbb{G}, +)$ μια ομάδα και $s \in \mathbb{G}$ το μυστικό το οποίο θέλουμε να μοιράσουμε σε n παίκτες

- Διαλέγουμε ομοιόμορφα $s_1, \cdots s_{n-1} \leftarrow\$ \mathbb{G}$
- Θέτουμε $s_n = s - \sum_{i=1}^{n-1} s_i$
- Μοιράζουμε τα $\{s_i\}_{i=1}^{n}$ στους παίκτες
- Ανακατασκευή $s = \sum_{i=1}^{n} s_i$

Παραλλαγή: Αν $s \in \{0,1\}^l$ τότε υλοποίηση με XOR $s_n = s \oplus (\bigoplus_{i=1}^{n-1} s_i)$

Ασφάλεια: Κανένα υποσύνολο από $n-1$ παίκτες δεν μπορεί να ανακατασκευάσει το s

Πρόβλημα: Ένας παίκτης μπορεί να ακυρώσει την ανακατασκευή

Threshold Secret Sharing

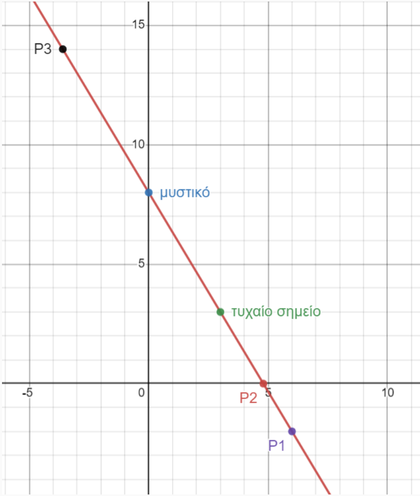
Παραλλαγή για ευελιξία: (t, n) threshold secret sharing

- Ένα μυστικό s πρέπει να μοιραστεί σε n παίκτες $P_1, P_2, \cdots P_n$ ώστε:
    - Οποιοδήποτε υποσύνολο από τουλάχιστον t παίκτες να μπορεί να το ανακτήσει
    - Κανένα υποσύνολο με $t - 1$ παίκτες να μην μπορεί
- Υπόθεση Εμπιστευόμαστε τον διανομέα D και τους παίκτες

Λύση: Shamir secret sharing - Βασίζεται σε πολυώνυμα σε πεπερασμένο σώμα $\mathbb{F}_p$ με $s \in \mathbb{F}_p, |\mathbb{F}_p| > n, p$ πρώτος

Διαισθητικά...

- Από 2 σημεία $(x_1, y_1), (x_2, y_2)$ διέρχεται μοναδική ευθεία
- Από 1 σημείο (x_1, y_1) διέρχονται άπειρες
- Το 1 σημείο είναι το $(0, s)$
- Διαλέγω το 2 τυχαία
- Ορίσαμε μια ευθεία
- Μοιράζω σημεία της στους διαφορους παίκτες
- Οποιοιδήποτε 2 μπορούν να ανακατασκευάσουν την ευθεία και να ανακτήσουν το μυστικό.
- Κανένας παίκτης μόνος του δεν μπορεί



Πολυωνυμική παρεμβολή

- 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 από t σημεία $(x_i, p(x_i))$ με διαφορετικές τετμημένες (με μοναδικό τρόπο)
- Κατασκευή με συντελεστές Lagrange
- $\lambda_i(x) = \prod_{k=1, k\neq i}^{t} \frac{x - x_k}{x_i - x_k}$
  - $\lambda_i(x) = 1$ αν $x = x_i$
  - $\lambda_i(x) = 0$ αν $x \neq x_i$
- Προκύπτει το $p(x) = L(x) = \sum_{i=1}^{t} p(x_i)\lambda_i(x) = p(x_1)\lambda_1(x) + \cdots + p(x_t)\lambda_t(x)$

Shamir secret sharing: Διανομή

Υποθέτουμε ότι διαθέτουμε έναν έμπιστο διανομέα:

- Επιλέγει και δημοσιοποιεί ένα πρώτο p
- Επιλέγει $t-1$ συντελεστές ενός πολυωνύμου βαθμού t $\{a_{t-1}, \cdots, a_1\} \leftarrow\$ \mathbb{Z}_p$
- Θέτει ως σταθερό όρο το μυστικό s
- Προκύπτει το πολυώνυμο $p(x) = a_{t-1} \cdot x^{t-1} + \cdots + a_1 \cdot x + s \pmod p$
- $p(0) = s$
- Μοιράζει στον παίκτη i την τιμή $(i, p(i))$ (ή $(x_i, p(x_i)), x_i \leftarrow\$ \mathbb{Z}_p$)

Shamir secret sharing: Ανακατασκευή

- Παρατήρηση: Δεν μας ενδιαφέρει να υπολογίσουμε το πολυώνυμο p αλλά το μυστικό $p(0) = s$
- Κάθε παίκτης i υπολογίζει τους συντελεστές Lagrange
- $\lambda_i(0) = \prod_{k=1, k \neq i}^{t} \frac{-k}{i-k} \mod p$
- t παίκτες μπορούν να υπολογίσουν το $p(0)$ ως: $\sum_{i=1}^{t} p(i)\lambda_i(0) \mod p$

Παρατηρήσεις I

- Πληροφοριοθεωρητική ασφάλεια αν ο αντίπαλος διαθέτει λιγότερα 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 ΙΙ

- Μειονεκτήματα: 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

Εφαρμογή: Threshold ElGamal I

- Δημιουργία Κλειδιών από (trusted) dealer
- Οι παίκτες είναι 'αρχές' που συνεργάζονται στην αποκρυπτογράφηση
    - Επιλογή δύο μεγάλων πρώτων p, q ώστε $q \mid (p-1)$
    - Επιλογή της υποομάδας τάξης q του $\mathbb{Z}_p^*$ και γεννήτορα g
    - Επιλογή τυχαίου $x \in \mathbb{Z}_q$
    - Κανονικός υπολογισμός δημοσίου κλειδιού $y = g^x \bmod p$
    - Χρήση σχήματος Shamir για διαμοιρασμό του ιδιωτικού $x \pmod q$
    - Αποτέλεσμα: Δημόσιο κλειδί και μερίδια $\mathsf{KGen}(1^\lambda) = (y, \{i, p(i)\}_{i=1}^n)$
- Κρυπτογράφηση
    - Κανονικά $\mathsf{Enc}(y, m) = (G, M) = (g^r, m \cdot y^r)$

Εφαρμογή: Threshold ElGamal II

- Αποκρυπτογράφηση: Σε δύο βήματα
  1. **’Αποκρυπτογράφηση’ μεριδίων**
     - Κάθε παίκτης υπολογίζει και δημοσιοποιεί το $c_i = G^{p(i)} \bmod p$
  2. **Συνδυασμός**
     - Συγκεντρώνονται t ‘αποκρυπτογραφημένα’ μερίδια (i, c_i) τα οποία συνδυάζονται ως:

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

       όπου λ_i οι συντελεστές Lagrange
     - Αποκρυπτογράφηση ως:$M \cdot C^{-1}$

Παρατηρήσεις

- Υπολογιστική ασφάλεια ως προς τα c_i
- Ίδια κρυπτογράφηση
- Αποκρυπτογράφηση χωρίς ανακατασκευή του ιδιωτικού κλειδιού (δυνατότητα επαναχρησιμοποίησης)