

Κρυπτοσυστήματα Διακριτού Λογαρίθμου

Παναγιώτης Γροντάς - Άρης Παγουρτζής

02/12/2022

ΕΜΠ - Κρυπτογραφία

- Διακριτός Λογάριθμος: Προβλήματα και Αλγόριθμοι
- Το κρυπτοσύστημα ElGamal (Ορισμός, Ασφάλεια, Παραλλαγές)
- Σχήματα Δέσμευσης με βάση το DLP
- Διαμοιρασμός απορρήτων - Shamir Secret Sharing - Threshold ElGamal

DLP

Προβλήματα Διακριτού Λογαρίθμου - (Υπενθύμιση)

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

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

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

$$\text{Δηλαδή: } DDHP \leq CDHP \leq DLP$$

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 $g^x = y$

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 $g^b, b \in \{0, 1, \dots, k-1\}$ και αποθηκεύουμε
 3. **Giant steps - μέγεθος k:**
Υπολογίζουμε $yg^{-ak}, a \in \{0, 1, \dots, k-1\}$ 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 $\mathbb{Z}_{29}^* = \langle 2 \rangle$, $\lceil \sqrt{29} \rceil = 6$

- $b \in \{0 \dots 5\}$
- $2^0 = 1 \pmod{29}$
- $2^1 = 2 \pmod{29}$
- $2^2 = 4 \pmod{29}$
- $2^3 = 8 \pmod{29}$
- $2^4 = 16 \pmod{29}$
- $2^5 = 3 \pmod{29}$
- $a \in \{0 \dots 5\}$
- $17 \cdot 2^{-0 \cdot 6} = 17 \pmod{29}$
- $17 \cdot 2^{-1 \cdot 6} = 27 \pmod{29}$
- $17 \cdot 2^{-2 \cdot 6} = 19 \pmod{29}$
- $17 \cdot 2^{-3 \cdot 6} = 8 \pmod{29}$
- Βρέθηκε

Άρα $x = 18 + 3 = 21$

Πράγματι: $2^{21} = 17 \pmod{29}$

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

Smooth Number

Μπορεί να παραγοντοποιηθεί σε μικρούς πρώτους - 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 $x = x_0 + x_1 p_i + \dots + x_{e_i-1} p_i^{e_i-1} \pmod{p_i^{e_i}}$ με $x_j \in \{0, \dots, p_i - 1\}$
- 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:

$$\begin{aligned} y^{\frac{p-1}{p_i}} &= (g^x)^{\frac{p-1}{p_i}} = g^{(x_0 + x_1 p_i + \dots + x_{e_i-1} p_i^{e_i-1}) \frac{p-1}{p_i}} = \\ &= g^{(x_0 + k p_i) \frac{p-1}{p_i}} = g^{x_0 \frac{p-1}{p_i}} g^{k p_i \frac{p-1}{p_i}} = \\ &= g^{x_0 \frac{p-1}{p_i}} \pmod{p} \end{aligned}$$

- 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
- $y_j = y_{j-1} \cdot g^{-(x_0+x_1p_i+\dots+x_{j-1}p_i^{j-1})} \pmod{p}$
- Γενικεύοντας την (1) έχουμε: $y_j^{\frac{p-1}{p_i^{j+1}}} = g^{x_j \frac{p-1}{p_i}}$

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

- Υπολογίζουμε το x_j

Συνδυασμός λύσεων με CRT

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

$$x_2 = x_{20} + 2x_{21} \pmod{4} \text{ και}$$

$$x_7 = x_{70} \pmod{7}$$

Υπολογισμός x_{20} για το x_2

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

$$\text{Άρα } x_{20} = 1$$

Υπολογισμός y_1 για το x_2

$$y_1 = yg^{-x_{20}} = 17 \cdot 2^{-1} = 17 \cdot 15 = 23 \pmod{29}$$

Υπολογισμός x_{21} για το x_2

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

$$\text{Άρα } x_{21} = 0$$

$$\text{Άρα } x_2 = 1 + 0 = 1 \pmod{4}$$

Υπολογισμός x_{70} για το x_7

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

$$\text{Άρα } x_{70} = 0$$

$$\text{Άρα } x_7 = 0 \pmod{7}$$

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

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

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

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

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

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

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

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

Algorithm 1 Ο αλγόριθμος διαχωρισμού

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

if $\left(\frac{g^c}{p}\right) = 1 \wedge \left(\left(\frac{g^a}{p}\right) = 1 \vee \left(\frac{g^b}{p}\right) = 1\right)$ **then**
| Επιστροφή "Τριάδα Diffie Hellman"

else

| Επιστροφή "Τυχαία Τριάδα"

end

Πλεονέκτημα: $\frac{3}{8}$ (γιατί;)

ΜΗ ΑΜΕΛΗΤΕΟ

Επιλογή Ομάδας 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:
 - Δύσκολο DDHP
 - Εύκολη εύρεση γεννήτορα
- Επίσης p Schnorr prime:
 $p = kq + 1$ με q πρώτο
- Όμως: Υποεκθετικοί αλγόριθμοι (index calculus)
- $(\mathcal{E}(\mathbb{F}_q), +)$ (Ελλειπτικές καμπύλες: 'Λογάριθμος' αφορά πρόσθεση)
 - ίδια επίπεδα ασφάλειας με μικρότερη τιμή κλειδιών

Μεγέθη

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

Το κρυπτοσύστημα ElGamal

Ορισμός ElGamal

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

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

Κρυπτογράφηση

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

Αποκρυπτογράφηση

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

Ορθότητα $Dec_x(Enc_y(r, m)) = (my^r)((g^r)^x)^{-1} = mg^{rx-rx} = m \pmod p$

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

Επιτάχυνση Κρυπτογράφησης:

Κόστος: 2 υψώσεις σε δύναμη - 1 πολλαπλασιασμός

Ύψωση σε δύναμη: **Δεν εξαρτάται** από το μήνυμα

Μπορεί να προεπιλεγθούν 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

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

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

Γενίκευση: Key encapsulation primitives

Επανάληψη τυχαιότητας → Επίθεση ΚΡΑ

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

Επίθεση

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

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

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

$$g^{x_1} \leftrightarrow g^r$$

$$g^{x_2} \leftrightarrow y = g^x$$

$$g^{x_1 x_2} \leftrightarrow y^r$$

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 $a \in_R \mathbb{G}$
4. Έξοδος $m \in \mathbb{G} : a = m \cdot g^{x_1 x_2}$
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 IND-CPA

Θεώρημα

Αν το DDHP είναι δύσκολο στην \mathbb{G} , τότε το κρυπτοσύστημα ElGamal διαθέτει ασφάλεια IND-CPA.

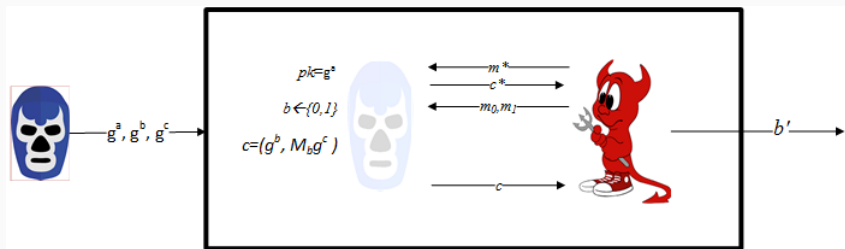
Απόδειξη:

Έστω ότι το ElGamal δεν διαθέτει ασφάλεια IND-CPA.

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

- Είσοδος: τριάδα στοιχείων
- Εσωτερικά: Προσομοίωση του $\mathcal{C}_{\text{IND-CPA}}$ 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^α, g^β, 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 $b \in_R \{0, 1\}$,
 - 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: $g^c = (g^a)^b = y^b$
 - 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 - αφού η κρυπτογράφηση δεν είναι σωστή.
- Πιθανότητα επιτυχίας: $\frac{1}{2}$.
- Άρα πλεονέκτημα \mathcal{B} :
$$\Pr[\mathcal{B}(g^a, g^b, g^{ab}) = 1] - \Pr[\mathcal{B}(g^a, g^b, g^c) = 1] \geq \text{non-negl}(\lambda)$$
- 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}

Πολλαπλασιαστικός Ομομορφισμός

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

Reencryption

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

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

Προσθετικός Ομομορφισμός - Εκθετικό ElGamal

Κρυπτογράφηση του g^m αντί για m : $\text{Enc}_y(r, m) = (g^r, g^m y^r)$

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

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 $|m| \ll |q|$

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

- 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 IND-CCA2

Δημιουργία Κλειδιών

- Επιλογή πρώτων p, q με $p = 2q + 1$
- \mathbb{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)

Κρυπτογράφηση

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

Αποκρυπτογράφηση

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

Ορθότητα

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

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

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
 - $ck \leftarrow \text{KGen}(1^\lambda)$
Δημιουργία δημόσιου commitment key ck
 - $(c, o) := \text{Commit}_{ck}(m)$
Δέσμευση στο m με το ck και παραγωγή τιμής ανοίγματος o
 - $\{0, 1\} := \text{Open}_{ck}(c, o, m)$
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 : $(c_A, o_A) = \text{Commit}_{ck}(b_A)$
- Η Alice στέλνει c_A
- Ο Bob στέλνει b_B
- Η Alice στέλνει b_A, o_A
- Ο Bob επαληθεύει αν $\text{Open}_{ck}(c_A, o_A, b_A) = 1$
- Αποφασίζουν ανάλογα με το αν $b_A = b_B$
- Προβλήματα (ξανά);

- 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 (ή $x \in \mathbb{Z}_q$ 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:
 $c \stackrel{?}{=} g^m \cdot h^r$

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

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

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

Ασφάλεια - Computationally Binding

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 είναι 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

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 $s_1, \dots, s_{n-1} \in_R \mathbb{G}$
- 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

$$s_n = s \oplus \left(\bigoplus_{i=1}^{n-1} s_i \right)$$

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

Πρόβλημα: Ένας παίκτης μπορεί να ακυρώσει την ανακατασκευή

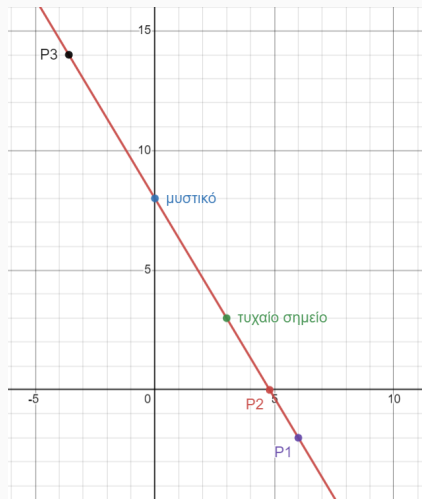
Παραλλαγή για ευελιξία: (t, n) threshold secret sharing

- Ένα μυστικό s πρέπει να μοιραστεί σε n παίκτες P_1, P_2, \dots, 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 πολυώνυμο 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

- Έστω ένα πολυώνυμο βαθμού $t - 1$:
$$p(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$$
- Μπορεί να ανακατασκευαστεί από t σημεία $(x_i, p(x_i))$ με διαφορετικές τετμημένες (με μοναδικό τρόπο)
- Υπάρχουν άπειρα πολυώνυμα βαθμού t που περνούν από t σημεία
- Υπάρχει μοναδικό πολυώνυμο βαθμού $t - 1$ που περνά από t σημεία
- Κατασκευή με συντελεστές Lagrange
- $$\lambda_i(x) = \prod_{k=1, k \neq i}^t \frac{x - x_k}{x_i - x_k}$$
- Προκύπτει το
$$L(x) = \sum_{i=1}^t p(x_i) \lambda_i(x) = p(x_1) \lambda_1(x) + \dots + p(x_t) \lambda_t(x)$$

Shamir secret sharing: Διανομή

Υποθέτουμε ότι διαθέτουμε έναν έμπιστο διανομέα:

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

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

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)

$$s_1 + s_2 = f(0) + g(0) = (f + g)(0)$$

- 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

Υποθέσεις

- Ομάδα \mathbb{G} τάξης q με γεννήτορα g με δύσκολο DLP
- Υπολογιστικά περιορισμένος αντίπαλος
- Για απλότητα χρήση συνάρτησης σύνοψης H για δέσμευση
- Για ασφάλεια: Απαιτείται έντιμη πλειοψηφία (το πολύ $t - 1$ **corrupted** / **τουλάχιστον** t honest)
 - Οποιοδήποτε σύνολο από t honest θα ανακατασκευάσει το μυστικό
 - Για έντιμο διανομέα: το μυστικό είναι το σωστό
 - Οι corrupted δεν μαθαίνουν τίποτα για το s

Ο διανομέας:

- Επιλογή $a_0 \in_R \mathbb{Z}_q$
- Διαμοιρασμός του a_0 με Shamir Secret Sharing
 - Επιλογή $a_1, \dots, a_{t-1} \in_R \mathbb{Z}_q$
 - Ορισμός $p(x) = a_0 + \sum_{j=1}^{t-1} a_j \cdot x^j$
 - Αποστολή $s_i = p(i)$ στον P_i
- Broadcast: $\{A_j = g^{a_j}\}_{j=0}^{t-1}$ και
- $c = H(a_0) \oplus s$

- Κάθε παίκτης P_i υπολογίζει:

$$c_i = \prod_{j=0}^{t-1} (A_j)^{i^j} = \prod_{j=0}^{t-1} (g^{a_j})^{i^j} = \prod_{j=0}^{t-1} g^{a_j \cdot i^j} = g^{\sum_{j=0}^{t-1} a_j \cdot i^j} = g^{P(i)}$$

- Αν ο διανομέας είναι έμπιστος θα ισχύει: $c_i = g^{P(i)} = g^{S_i}$
- Επαλήθευση σχέσης: Αν δεν ισχύει ο P_i τερματίζει ανεπιτυχώς
- Αν τερματίσουν πάνω από t χρήστες, ο διανομέας δεν είναι έμπιστος: τερματισμός
- Αν τερματίσουν λιγότεροι από t χρήστες: Φταίει ο P_i - επανάληψη S_i

- Συγκέντρωση τουλάχιστον t μεριδίων - υπολογισμός a_0
- Υπολογισμός $s = \mathcal{H}(a_0) \oplus c$

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
 $\text{KGen}(1^\lambda) = (y, \{i, p(i)\}_{i=1}^n)$
- Κρυπτογράφηση
 - Κανονικά
 $\text{Enc}(y, m) = (G, M) = (g^r, m \cdot y^r)$

- 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:

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

όπου λ_i οι συντελεστές Lagrange

- Αποκρυπτογράφηση ως: $\frac{M}{C}$

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