Κρυπτοσυστήματα Διακριτού Λογαρίθμου

Παναγιώτης Γροντάς - Άρης Παγουρτζής

27/11/2018

ΕΜΠ - Κρυπτογραφία (2018-2019)

Περιεχόμενα

- 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

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: $DDHP \leq CDHP \leq DLP$

Random Self - Reducibility

Θεώρημα

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

$$u \in_R \mathbb{G} : Pr[A(u) = DL(u)] = \epsilon$$

Υπάρχει PPT αλγόριθμος B με την ιδιότητα:

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

Απόδειξη
Ο αλγόριθμος B είναι ο εξής:

Είσοδος $u \in \mathbb{G}$

$\sigma \leftarrow_R \mathbb{Z}_q$

$u_1 \leftarrow u \cdot g^{\sigma}$

$a_1 \leftarrow A(u_1)$

if $g^{a_1} \neq u_1$ **then**
  return fail
else
  return $a_1 - \sigma$
end

Random Self - Reducibility (Παρατηρήσεις)

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

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

Συμπέρασμα: Εύκολο DLP για μη αμελητέο ποσοστό τυχαίων στοιχείων, εύκολο για όλα τα στοιχεία της ομάδας

Συνέπεια: Κατάλληλα 'Δύσκολα" προβλήματα για κρυπτογραφία: Δύσκολα στη χειρότερη περίπτωση και Random Self - Reducible (δύσκολα στη μέση περίπτωση)

Δεν ισχύει για όλα τα NP-hard προβλήματα

Επιλογή Ομάδας

- Καθορίζει τη δυσκολία του προβλήματος
- Δύο επιλογές:
  - $(\mathbb{Z}_p^*, \cdot)$ με p πρώτο (σε υποομάδα)
  - Λόγοι:
    - Δυσκολότερο το DLP
    - Τετριμμένη εύρεση γεννήτορα (όλα τα στοιχεία εκτός από το 1)
    - Εύκολη εύρεση αντίστροφου
  - $(\mathcal{E}(\mathbb{F}_p), +)$ (Ελλειπτικές καμπύλες: 'Λογάριθμος' αφορά πρόσθεση)
    - ίδια επίπεδα ασφάλειας με μικρότερη τιμή παραμέτρου ασφάλειας

Αλγόριθμοι DL

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 $g^b, b \in \{0, 1, \cdots, k-1\}$ 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 $\mathbb{Z}_{29}^* = \langle 2 \rangle$, $\lceil \sqrt{29} \rceil = 6$

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

- $a \in \{0 \cdots 5\}$
- $17 \cdot 2^{-0 \cdot 6} = 17 \pmod{29}$
- $17 \cdot 2^{-1 \cdot 6} = 37 \pmod{29}$
- $17 \cdot 2^{-2 \cdot 6} = 19 \pmod{29}$
- $17 \cdot 2^{-3 \cdot 6} = 8 \pmod{29}$
- 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 και συνδυασμός με CRT

Smooth Number
Μπορεί να παραγοντοποιηθεί σε μικρούς πρώτους - Αν ισχύει για την τάξη επιταχύνει σημαντικά τον αλγόριθμο

Αλγόριθμος Pohlig-Hellman

- Παραγοντοποιούμε την τάξη: $p-1=\prod_{i=1}^{m} p_i^{e_i}$
- Για κάθε p_i γράφουμε $x=a_0+a_1p_i+\cdots+a_{e_i-1}p_i^{e_i-1} \pmod{p_i^{e_i}}$ με $a_j\in\{0,\cdots,p_i-1\}$
- Θα υπολογίσουμε τους συντελεστές ως εξής:
- Για το a_0 ισχύει: $y^{\frac{p-1}{p_i}}=g^{a_0\frac{p-1}{p_i}} \pmod{p}$ (1) επειδή:

$$\begin{aligned} y^{\frac{p-1}{p_i}}=(g^x)^{\frac{p-1}{p_i}}=g^{(a_0+a_1p_i+\cdots+a_{e_i-1}p_i^{e_i-1})\frac{p-1}{p_i}} &= \\ g^{(a_0+Kp_i)\frac{p-1}{p_i}}=g^{a_0\frac{p-1}{p_i}}g^{Kp_i\frac{p-1}{p_i}} &= \\ g^{a_0\frac{p-1}{p_i}} \pmod{p} \end{aligned}$$

- Υπολογισμός a_0 (πχ. με αλγόριθμο Shanks)

Αλγόριθμος Pohlig-Hellman

- Για τον υπολογισμό των υπόλοιπων συντελεστών:
  - Δημιουργούμε ακολουθία $\{y_j\}$ με $y_0 = y$ και
  - $y_j = y_{j-1} \cdot g^{-(a_0 + a_1 p_i + \cdot + a_{j-1} p_i^{j-1})} \pmod{p}$
  - Γενικεύοντας την (1) έχουμε: $y_j^{\frac{p-1}{p_i^{j+1}}} = g^{a_j \frac{p-1}{p_i}}$
  - Υπολογίζουμε το a_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: $28 = 2^2 7$

$x_2 = a_0 + 2a_1 \pmod 4$ και

$x_7 = a_0 \pmod 7$

Υπολογισμός a_0 **για το** x_2
$y^{\frac{p-1}{2}} = g^{a_0 \frac{p-1}{2}} \Rightarrow 17^{14} = 2^{14a_0} \Rightarrow 2^{14a_0} = 28 = -1 \pmod{29}$

Άρα $a_0 = 1$

Υπολογισμός y_1 **για το** x_2
$y_1 = yg^{-a_0} = 17 \cdot 2^{-1} = 17 \cdot 15 = 23 \pmod{29}$

Pohlig-Hellman - παράδειγμα

Υπολογισμός a_1 **για το** x_2
$y_1^{\frac{p-1}{4}} = g^{a_1 \frac{p-1}{2}} \Rightarrow 23^7 = 2^{14a_1} \Rightarrow 2^{14a_1} = 1 \pmod{29}$
Άρα $a_1 = 0$

Άρα $x_2 = 1 + 0 = 1 \pmod{4}$

Υπολογισμός a_0 **για το** x_7
$y^{\frac{p-1}{7}} = g^{a_0 \frac{p-1}{7}} \Rightarrow 17^4 = 2^{4a_0} \Rightarrow 2^{4a_0} = 1 \pmod{29}$
Άρα $a_0 = 0$

Άρα $x_7 = 0 \pmod{7}$

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

Δυσκολία DDHP

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

Μπορεί να κατασκευαστεί αποδοτικός αλγόριθμος διαχωρισμού τριάδας DH g^a, g^b, g^{ab} από μια τυχαία τριάδα g^a, g^b, g^c.
Πώς: Χρησιμοποιώντας το σύμβολο Legendre.

Το σύμβολο Legendre διαρρέει το DLP parity
Από τον ορισμό: $(\frac{g^x}{p}) = (g^x)^{\frac{p-1}{2}}$
Όμως: $g^{p-1} = 1 \pmod p$
Άρα: $g^{\frac{p-1}{2}} = -1 \pmod p$
Δηλαδή: $(\frac{g^x}{p}) = (-1)^x$
Αν x μονός τότε $(\frac{g^x}{p}) = -1$
Αν x ζυγός τότε $(\frac{g^x}{p}) = 1$

Δυσκολία DDHP

Για τυχαία τριάδα: $Prob[(\frac{g^c}{p}) = 1] = \frac{1}{2}$
Για τριάδα DH: $Prob[(\frac{g^{ab}}{p}) = 1] = \frac{3}{4}$

Algorithm 1 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

Συνέπειες

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

Για παράδειγμα:

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

Δουλεύουμε στην υποομάδα τετραγωνικών υπολοίπων τάξης q

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

Παρ’ όλα αυτά: Υποεκθετικοί αλγόριθμοι (index calculus)

Μεγέθη

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

Το κρυπτοσύστημα ElGamal

Ορισμός ElGamal

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

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

Κρυπτογράφηση

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

Αποκρυπτογράφηση

- $\mathtt{Decrypt}_x(a, b) = \frac{b}{a^x}$

Ορθότητα $\mathtt{Decrypt}_x(\mathtt{Encrypt}_y(r, m)) = \frac{my^r}{(g^r)^x} = m$

Πρακτικά Θέματα

Πιθανοτική Κρυπτογράφηση: Ένα μήνυμα έχει πολλά πιθανά κρυπτοκείμενα

Message expansion Κρυπτοκείμενο διπλάσιο του μηνύματος

Επιτάχυνση Κρυπτογράφησης
Κόστος: 2 υψώσεις σε δύναμη - 1 πολλαπλασιασμός

Ύψωση σε δύναμη:Δεν εξαρτάται από το μήνυμα (precomputation)

Μυστικότητα ElGamal $\equiv CDHP$
Αντιστοιχία δημοσίων στοιχείων

$$g^{x_1} \equiv g^r$$
$$g^{x_2} \equiv y = g^x$$
$$g^{x_1 x_2} \equiv y^r$$

$EG \leq CDHP$: $CDHP \Rightarrow$ Υπολογισμός $g^{x_1 x_2} = y^r \Rightarrow$ αποκρυπτογράφηση (με εύρεση αντιστρόφου του y^r)
$CDHP \leq EG$: $EG \Rightarrow$
Για οποιοδήποτε $c \in \mathbb{G}$:
εύρεση m που αντιστοιχεί στο $g^{x_2}, (g^{x_1}, c)$ (χρήση EG ως oracle αποκρυπτογράφησης με δημόσιο κλειδί g^{x_2})
Υπολογισμός $g^{x_1 x_2} = \frac{c}{m}$

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

Επίθεση

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

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

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

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

Ασφάλεια σε επιθέσεις CPA

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

Απόδειξη:

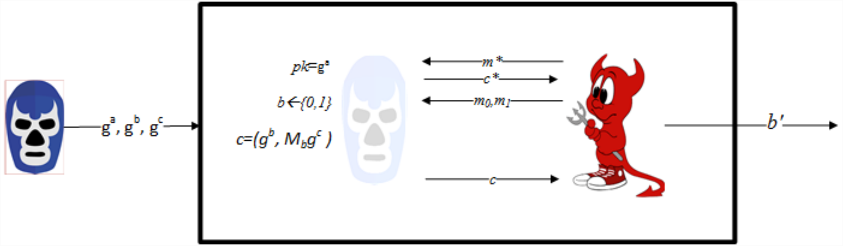
Έστω ότι το ElGamal δεν διαθέτει ασφάλεια IND-CPA.

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

Κατασκευή $\mathcal{B}$:

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

Ασφάλεια σε επιθέσεις CPA



Ασφάλεια σε επιθέσεις CPA

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

Ασφάλεια σε επιθέσεις CPA

Ανάλυση

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

Πολλαπλασιαστικός Ομομορφισμός

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

Ομομορφικές Ιδιότητες

Reencryption

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

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

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

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

Αποκρυπτογράφηση: Λαμβάνουμε το g^m

Επίλυση διακριτού λογαρίθμου ('εύκολου').

Ασφάλεια σε επιθέσεις CCA

Το textbook ElGamal δεν διαθέτει CCA-security

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

- Στόχος: Αποκρυπτογράφηση του $c = (G, M) = (g^r, m_b y^r)$
- Κατασκευή $c' = (G', M') = (G \cdot g^{r'}, M \cdot a y^{r'}) = (g^{r+r'}, a \cdot m_b \cdot y^{r+r'})$, όπου a επιλέγεται από τον $\mathcal{A}$
- Η αποκρυπτογράφηση του M' ($\frac{M'}{G'^x}$) δίνει το am_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 $\mathcal{H}$ (υπάρχουν εκδόσεις και χωρίς)
- Αν ισχύει η υπόθεση DDH, τότε παρέχει IND-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)

Κρυπτογράφηση

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

Αποκρυπτογράφηση

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

ElGamal CCA2: Cramer-Shoup cryptosystem

Ορθότητα

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

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

Παρατηρήσεις

- 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

- 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;

Λύση: Commitment Schemes

- 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
- Χρήση randomization για προστασία από brute-force επιθέσεις

Pedersen commitment

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

Ιδιότητες - 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

Ιδιότητες - Computationally Binding

Αν το DLP είναι δύσκολο τότε το σχήμα δέσμευσης είναι binding

Έστω $c = commit(m, r) = commit(m', r')$ 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 DL-based collision resistance

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 τυχαία $s_1, \cdots s_{n-1} \in \mathbb{G}$
- 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 $\mathbb{F}$ με $s \in \mathbb{F}, |\mathbb{F}| > n$

Πολυωνυμική παρεμβολή

- 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)
- Υπάρχουν άπειρα πολυώνυμα βαθμού t που περνούν από t σημεία
- Υπάρχει μοναδικό πολύωνυμο 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
  $L(x) = \sum_{i=1}^{t} p(x_i)\lambda_i(x) = p(x_1)\lambda_1(x) + \cdots + p(x_t)\lambda_t(x)$

Shamir secret sharing: Διανομή

Υποθέτουμε ότι διαθέτουμε έναν έμπιστο διανομέα:

- Επιλέγει και δημοσιοποιεί ένα πρώτο p
- Επιλέγει $t-1$ συντελεστές ενός πολυωνύμου βαθμού t $\{a_{t-1}, \cdots, a_1\} \in_R \mathbb{Z}_p$
- 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 $(x_i, p(x_i)), x_i \in_R \mathbb{Z}_p$)

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
- $\lambda_i(0) = \prod_{k=1,k\neq i}^{t} \frac{-k}{i-k} \bmod p$
- t παίκτες μπορούν να υπολογίσουν το $p(0)$ ως: $\sum_{i=1}^{t} p(i)\lambda_i(0) \bmod p$

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

Feldman Verifiable Secret Sharing

Υποθέσεις

- Ομάδα $\mathbb{G}$ τάξης q με γεννήτορα g με δύσκολο DLP
- Υπολογιστική Ασφάλεια
- Για απλότητα χρήση συνάρτησης σύνοψης $\mathcal{H}$ 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

Feldman Verifiable Secret Sharing: Διαμοιρασμός s

Ο διανομέας:

- Επιλογή $a_0 \in_R \mathbb{Z}_q$
- Διαμοιρασμός του a_0 με Shamir Secret Sharing
  - Επιλογή $a_1, \cdots, a_{t-1} \in_R \mathbb{Z}_q$
  - 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
- $c = \mathcal{H}(a_0) \oplus s$

Feldman Verifiable Secret Sharing: Φάση επαλήθευσης

- 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

Feldman Verifiable Secret Sharing: Φάση ανακατασκευής

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

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: $\frac{M}{C}$

Παρατηρήσεις

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

Πηγές

Βιβλιογραφία i

- Παγουρτζής, Α., Ζάχος, Ε., ΓΠ, 2015. Υπολογιστική κρυπτογραφία. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
- Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography (Chapman and Hall/Crc Cryptography and Network Security Series). Chapman and Hall/CRC, 2007
- Nigel Smart. Introduction to cryptography
- Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science-Business Media, 2009.
- Kiayias, Aggelos Cryptography primitives and protocols, UoA, 2015
- Dan Boneh, Introduction to cryptography, online course
- Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In CRYPTO ’91, pages 129–140, 1991
- Victor Shoup Why chosen ciphertext security matters, 1998
- Adi Shamir, How to share a secret. Communications of the ACM 22.11 (1979): 612-613.
- Helger Lipmaa, 79.159 Cryptography and Data Security, 24.03.2004 Lecture 9: Secret Sharing, Threshold Cryptography, MPC
- J. Kuhn The Mathematics of Secret Sharing