# Κρυπτοσυστήματα Διακριτού Λογαρίθμου

Παναγιώτης Γροντάς - Άρης Παγουρτζής

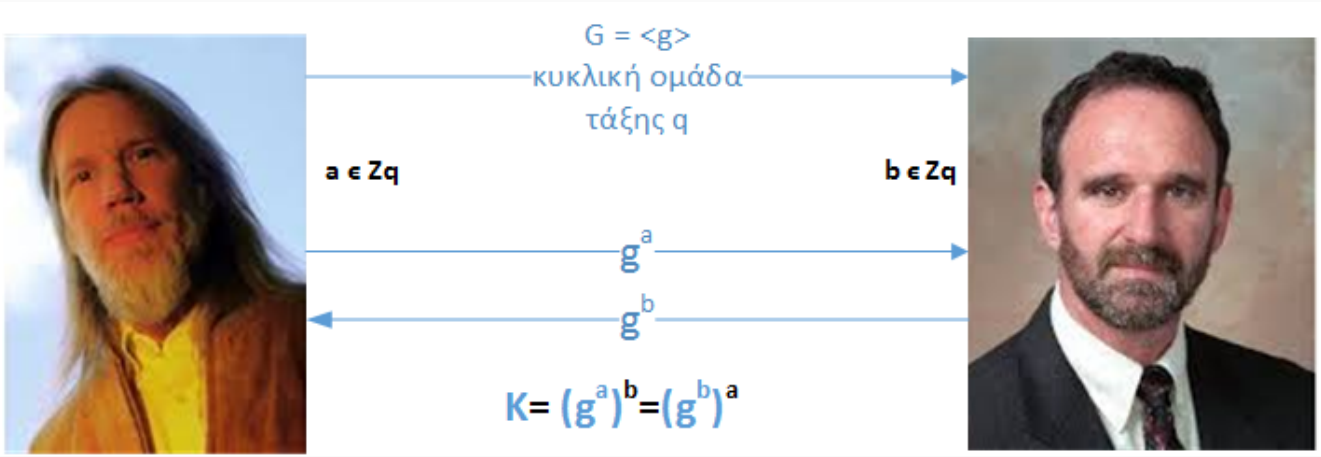
ΕΜΠ - Κρυπτογραφία

# Περιεχόμενα

# DLP

# Το πρωτόκολλο DHKE

Αντί για Alice και Bob...




Πρωτόκολλο **Δημιουργίας** Κλειδιού

**Απαιτήσεις**:

Ασφάλεια: Ύψωση σε δύναμη - μονόδρομη συνάρτηση στην $\mathbb{G}$

Συνήθως: $\mathbb{G}$ υποομάδα του $\mathbb{Z}_p^*$ με $p$ πρώτο ή ελλειπτικές καμπύλες

Εφαρμογές: SSL, TLS, IPSEC

# Ασφάλεια DHKE - Πρόβλημα DLP

**DLP - Το πρόβλημα του Διακριτού Λογάριθμου**
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 $log_g y \in \mathbb{Z}_q$

Αγνοούμε δεδομένα στο πρωτόκολλο DHKE

# Ασφάλεια DHKE - Πρόβλημα CDHP

$CDHP \leq^P DLP$

**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 $g^{x_1 \cdot x_2}$

# Ασφάλεια DHKE - Πρόβλημα DDHP

Μπορούμε να δοκιμάζουμε τυχαία στοιχεία

**DDHP - Το πρόβλημα απόφασης Diffie Hellman**
Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, δύο στοιχεία $y_1 = g^{x_1}, y_2 = g^{x_2}$ και κάποιο $y \in \mathbb{G}$

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

ή ισοδύναμα

**DDHP - Το πρόβλημα απόφασης Diffie Hellman**
Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, δύο στοιχεία $y_1 = g^{x_1}, y_2 = g^{x_2}$ και κάποιο $y \in \mathbb{G}$

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

# DDH σε μορφή παιγνίου *DDH – Game*

Κοινή είσοδος: παράμετρος ασφάλειας $\lambda$.

Λειτουργίες $\mathcal{C}$

- Παραγωγή: $\mathbb{G} = \langle g \rangle$ τάξης πρώτου $q$.
- Επιλογή τυχαίων $x_1, x_2 \in \mathbb{Z}_q$, $y \in G$
- Υπολογισμός $g^{x_1}, g^{x_2}, g^{x_1 x_2}$
- Επιλογή τυχαίου bit $b \in \{0, 1\}$
- Αν $b = 0$ τότε αποστολή $\mathbb{G}, g^{x_1}, g^{x_2}, y' = g^{x_1 x_2}$ στον $\mathcal{A}$
- Αν $b = 1$ τότε αποστολή $\mathbb{G}, g^{x_1}, g^{x_2}, y' = y$ στον $\mathcal{A}$

Ο $\mathcal{A}$ υπολογίζει $b'$.

Αν $b' \neq b$ τότε το αποτέλεσμα του παιχνιδιού είναι $0$, αλλιώς $1$

# DDH σε μορφή παιγνίου $DDH - Game$ (2)

Πλεονέκτημα $\mathcal{A}$ :

$$Adv_{\mathcal{A}}^{DDH-Game} =$$
$$|Pr[DDH - Game(\mathcal{A}(\mathbb{G}, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1)]$$
$$-Pr[DDH - Game(\mathcal{A}(\mathbb{G}, g^{x_1}, g^{x_2}, y) = 1)]|$$

Η υπόθεση DDH ισχύει αν $\forall$ PPT:

$\mathcal{A}$: $Adv_{\mathcal{A}}^{DDH}(\lambda) = negl(\lambda)$

# Σχέσεις Προβλημάτων

$CDHP \leq DLP$
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: $DDHP \leq CDHP \leq DLP$

Δεν γνωρίζουμε αν ισχύει η αντίστροφη σειρά - ισοδυναμία
Όμως: Υπάρχουν ομάδες όπου το *DDHP* έχει αποδειχθεί εύκολο, ενώ *CDHP* δεν έχει αποδειχθεί εύκολο
Μάλλον: $DDHP < CDHP$

# Ασφάλεια DHKE

Μοντέλο ασφάλειας: παθητικός αντίπαλος $\mathcal{A}$

**Διαίσθηση**
Ο $\mathcal{A}$ δεν αποκτά καμία χρήσιμη πληροφορία για το κλειδί που δημιουργείται.

Ισοδύναμα

Ο $\mathcal{A}$ δεν μπορεί να διακρίνει το κλειδί από ένα τυχαίο στοιχείο της ομάδας στην οποία ανήκει

# Παιχνίδι ανταλλαγής κλειδιού $KEG(\lambda, \mathcal{A}, \Pi)$

Κοινή είσοδος: $\lambda$. Λειτουργίες $\mathcal{C}$ :

- Δημιουργεί ομάδα $\mathbb{G}$
- Εκτελεί το πρωτοκόλλο $\Pi(1^\lambda)$
- Παράγεται: $(\tau, k)$
  - $\tau$: Τα μηνύματα που ανταλλάσσονται (δημόσια)
  - $k$: Το κλειδί που παράγεται (ιδιωτικό)
- Επιλογή τυχαίου $b \in \{0, 1\}$
- Αν $b = 0$ επιλογή τυχαίου $k'$ και αποστολή $(\tau, k')$ στον $\mathcal{A}$
- Αν $b = 1$ αποστολή $(\tau, k)$ στον $\mathcal{A}$

Ο $\mathcal{A}$ υπολογίζει $b'$. Αν $b' \neq b$ τότε το αποτέλεσμα του παιχνιδιού είναι $0$, αλλιώς $1$

Πλεονέκτημα $\mathcal{A}$ :
$Adv^{KEG}_{\mathcal{A},\Pi}(\lambda) = |Pr[KEG_\Pi(\mathcal{A}(\tau, k) = 1)] - Pr[KEG_\Pi(\mathcal{A}(\tau, k') = 1)]|$

# Ορισμός ασφάλειας DHKE

Ένα πρωτόκολλο ανταλλαγής κλειδιού $\Pi$ είναι ασφαλές, αν κάθε PPT *παθητικός* αντίπαλος $\mathcal{A}$ έχει αμελητέο πλεονέκτημα ως προς την παράμετρο ασφάλειας να επιτύχει στο *KEG*
$Adv^{KEG}_{\mathcal{A},\Pi}(\lambda) = negl(\lambda)$

# Απόδειξη ασφάλειας DHKE

Αν το DDHP είναι δύσκολο, τότε το πρωτόκολλο DHKE είναι ασφαλές (απέναντι σε παθητικό αντίπαλο)

**Απόδειξη - Σχεδιάγραμμα** DHKE μη ασφαλές: $\exists \mathcal{A}$ ώστε $Adv_{\mathcal{A}}^{KEG}(\lambda) = non - negl(\lambda)$

Θα κατασκευάσουμε αντίπαλο PPT $\mathcal{B}$ ο οποίος παραβιάζει την *DDH* με μη αμελητέο πλεονέκτημα.

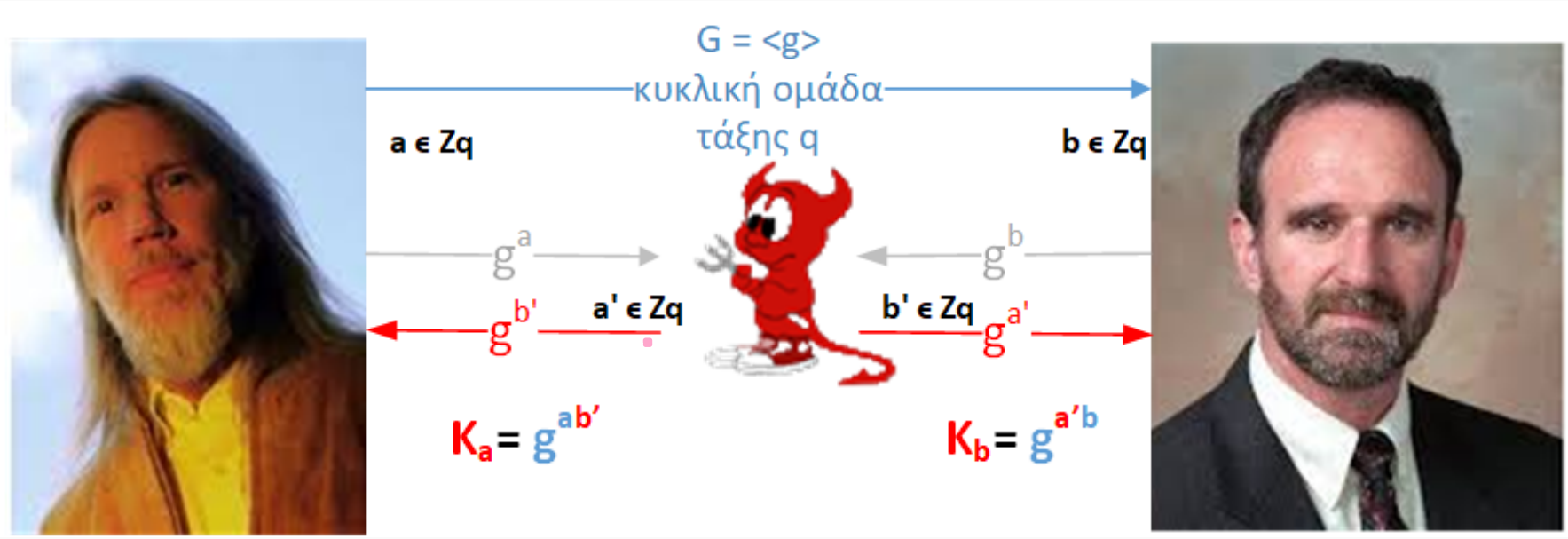
Ο $\mathcal{B}$ λειτουργεί ως εξής:

- Όταν λάβει το μήνυμα από τον $\mathcal{C}_{DDH}$ το προωθεί στον $\mathcal{A}$
- Μορφή μηνύματος $(\tau, k') = ((\mathbb{G}, g^{X_1}, g^{X_2})), y')$
- Όταν ο $\mathcal{A}$ απαντήσει, προωθεί το $b'$.

$$Adv_{\mathcal{B}}^{DDH-Game} = |Pr[DDH - Game(\mathcal{B}(\mathbb{G}, g^{X_1}, g^{X_2}, g^{X_1 X_2}) = 1)] - Pr[DDH - Game(\mathcal{B}(\mathbb{G}, g^{X_1}, g^{X_2}, y) = 1)] =$$
$$|Pr[KEG_{DHKE}(\mathcal{A}(\tau, k) = 1)] - Pr[KEG_{DHKE}(\mathcal{A}(\tau, k') = 1)]| = non - negl(\lambda)$$

# Ενεργοί Αντίπαλοι

Η σημασία του μοντέλου ασφάλειας - Man In The Middle Attacks




Πώς είμαι σίγουρος ότι μιλάω με αυτόν που *νομίζω* ότι μιλάω;
Λύση: ψηφιακές υπογραφές - ψηφιακό πιστοποιητικό (εγγύηση 'έμπιστου' τρίτου)

# 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 $q$ $\lambda$ 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**

1. Παραγοντοποίηση της τάξης
   (πχ. στο $\mathbb{Z}_p^*$: $p-1 = \prod_{i=1}^{m} p_i^{e_i}$ με $p_i$ πρώτο)
2. 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:

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

- 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

# Επιλογή του $\mathbb{G}$

## Συνέπειες

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

## Για παράδειγμα:

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

Δουλεύουμε στην υποομάδα τετραγωνικών υπολοίπων τάξης $q$

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

Παρ' όλα αυτά: Υποεκθετικοί αλγόριθμοι (index calculus)

## Μεγέθη

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

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

## Αποκρυπτογράφηση

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

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

# 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)

# Ασφάλεια Κρυπτογράφησης

**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 $g^{x_1 x_2} = \frac{c}{m}$

# Επανάληψη τυχαιότητας → Επίθεση KPA

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:

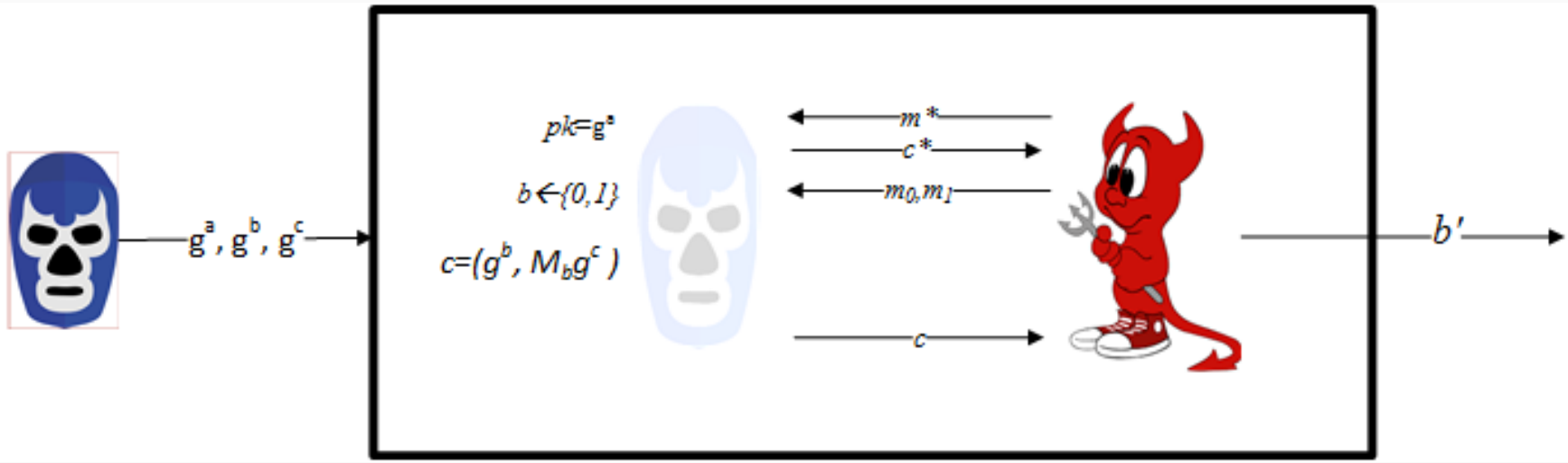
Έστω ότι το ElGamal δεν διαθέτει ασφάλεια IND-CPA.

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 $g^{\beta}$ 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($\lambda$)
- Μπορεί να ξεχωρίσει μία DH τριάδα από μία τυχαία με μη αμελητέα πιθανότητα.

# Ομομορφικές Ιδιότητες

## Πολλαπλασιαστικός Ομομορφισμός

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

# Ομομορφικές Ιδιότητες

## Reencryption

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

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

# Ομομορφικές Ιδιότητες

**Προσθετικός Ομομορφισμός - Εκθετικό ElGamal**
Κρυπτογράφηση του $g^m$ αντί για $m$

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

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

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 $b^* = 1$

# 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

DLP-based collision resistance

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

# 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