# Επιθέσεις και Ασφάλεια Κρυπτοσυστημάτων

January 31, 2014

# Επιθέσεις ενεργητικού αντιπάλου $\mathcal{A}$

## Chosen Plaintext Attack

- Ικανότητα: Ο $\mathcal{A}$ μπορεί να κρυπτογραφεί μηνύματα της αρεσκείας του
- Στόχος: Ο $\mathcal{A}$ θέλει να μάθει την αποκρυπτογράφηση ενός κρυπτοκειμένου

## Chosen Ciphertext Attack

- Ικανότητα: Ο $\mathcal{A}$ μπορεί να κρυπτογραφεί μηνύματα της αρεσκείας του
- Ικανότητα: Ο $\mathcal{A}$ μπορεί να αποκρυπτογραφεί κάποια μηνύματα της αρεσκείας του
- Στόχος: Ο $\mathcal{A}$ θέλει να μάθει την αποκρυπτογράφηση ενός συγκεκριμένου διαφορετικού μηνύματος

# Indistinguishability under Chosen Plaintext Attack (IND-CPA)

## CPA Game

- Δημιουργία ζεύγους κλειδιών (PK,SK)
- Δημοσίευση PK
- Ο $\mathcal{A}$ μπορεί να κρυπτογραφεί πολυωνυμικό πλήθος μηνυμάτων
- Τελικά υποβάλλει δύο μηνύματα $M_0, M_1$ στο σύστημα
- Το σύστημα διαλέγει τυχαία 1 bit $b$ και αποστέλλει το $C = Enc(M_b)$ στον $\mathcal{A}$
- Ο $\mathcal{A}$ μπορεί να συνεχίσει να κρυπτογραφεί πολυωνυμικό πλήθος μηνυμάτων και να κάνει οποιονδηποτε υπολογισμό θέλει.
- Τελικά μαντεύει το $b$

## Ορισμός ασφάλειας

Το κρυπτοσύστημα έχει την ιδιότητα IND-CPA αν κάθε PPT $\mathcal{A}$ έχει αμελητέο πλεονέκτημα στον υπολογισμό του $b$ από το να μαντέψει τυχαία.

# Indistinguishability under Chosen Ciphertext Attack (IND-CCA) I

CCA Game

- Δημιουργία ζεύγους κλειδιών (PK,SK)
- Δημοσίευση PK
- Ο $\mathcal{A}$ μπορεί να κρυπτογραφεί πολυωνυμικό πλήθος μηνυμάτων
- Ο $\mathcal{A}$ χρησιμοποιεί το σύστημα ως *decryption oracle* και μπορει να αποκρυπτογραφήσει συγκεκριμένα μηνύματα
- Τελικά υποβάλλει δύο μηνύματα $M_0, M_1$ στο σύστημα, διαφορετικά από αυτα που μπορει να αποκρυπτογραφήσει
- Το σύστημα διαλέγει τυχαία 1 bit $b$ και αποστέλλει το $C = Enc(M_b)$ στον $\mathcal{A}$
- Ο $\mathcal{A}$ μπορεί να συνεχίσει να κρυπτογραφεί πολυωνυμικό πλήθος μηνυμάτων και να κάνει οποιονδηποτε υπολογισμό θέλει

# Indistinguishability under Chosen Ciphertext Attack (IND-CCA) II

- Προαιρετικά ο $\mathcal{A}$ μπορει να συνεχίσει να χρησιμοποιεί το *decryption oracle*
- Τελικά μαντεύει το $b$

### Ορισμός ασφάλειας

Το κρυπτοσύστημα έχει την ιδιότητα IND-CCA1 αν κάθε PPT $\mathcal{A}$ έχει αμελητέο πλεονέκτημα στον υπολογισμό του $b$ από το να μαντέψει τυχαία. Αν ισχύει το προαιρετικό βήμα το κρυπτοσύστημα είναι IND-CCA2 (adaptive IND-CCA)

### Malleability:Μια σχετική ιδιότητα

Οποιαδηποτε αλλαγή στο ciphertext οδηγεί σε αντίστοιχη αλλαγή στο plaintext. Κάποιες φορές είναι επιθυμητή και κάποιες όχι.

# Παραδείγματα με *παραδοσιακό* RSA I

### Το παραδοσιακό RSA δεν είναι IND-CPA γιατί είναι deterministic

Αν τα πιθανά μηνύματα είναι:

- $m_1$ = "Buy IBM"
- $m_2$ = "Sell IBM"

τότε ο $\mathcal{A}$ μπορεί να τα κρυπτογραφήσει και να τα συγκρίνει με το νόμιμο ciphertext

### Το παραδοσιακό RSA είναι malleable

- Στόχος: Αλλοίωση του $c = m^e \pmod n$
- $c' = c(\frac{9}{10})^e \pmod n = (m\frac{9}{10})^e \pmod n$
- Η αποκρυπτογράφηση δίνει το $m\frac{9}{10}$
- Ο $\mathcal{A}$ μπορεί να *αλλοιώσει* κάποιο μήνυμα χωρίς να το γνωρίζει

# Παραδείγματα με *παραδοσιακό* RSA II

**Το παραδοσιακό RSA δεν είναι IND-CCA**

Ο $\mathcal{A}$ μπορεί να αποκρυπτογραφήσει μηνύματα επιλογής του

- Στόχος: Αποκρυπτογράφηση του $c = m^e \pmod n$
- Μπορεί να αποκρυπτογραφήσει το $c' = cx^e \pmod n$ όπου το $x$ είναι δικής του επιλογής
- Ανακτά το $m = \frac{m'}{x}$

# Παραδείγματα με *παραδοσιακό* ElGamal I

Το ElGamal *είναι* IND-CPA *αν* ισχύει η DDH assumption

Το παραδοσιακό El Gamal *είναι* malleable

- Στόχος: Αλλοίωση του $c = (G, M) = (g^r, mh^r)$
- $c' = (G', M') = (Gg^{r'}, M\frac{9}{10}h^{r'}) = (g^{r+r'}, m\frac{9}{10}h^{r+r'})$
- Η αποκρυπτογράφηση $\frac{M'}{G'^x}$ δίνει το $m\frac{9}{10}$
- Ο $\mathcal{A}$ μπορεί *να αλλοιώσει* κάποιο μήνυμα χωρίς *να* το *γνωρίζει*

# Παραδείγματα με *παραδοσιακό* ElGamal II

**Το παραδοσιακό El Gamal δεν είναι IND-CCA**

Ο $\mathcal{A}$ μπορεί να αποκρυπτογραφήσει μηνύματα επιλογής του

- Στόχος: Αποκρυπτογράφηση του $c = (G, M) = (g^r, mh^r)$
- $c' = (G', M') = (Gg^{r'}, M\alpha h^{r'}) = (g^{r+r'}, m\alpha h^{r+r'})$ όπου το $\alpha$ επιλέγεται από τον $\mathcal{A}$
- Η αποκρυπτογράφηση $\frac{M'}{G'^x}$ δίνει το $am$ και κατά συνέπεα το $m$
- Ο $\mathcal{A}$ μπορεί να *αλλοιώσει* κάποιο μήνυμα χωρίς να το γνωρίζει

# Λύσεις RSA I

## Randomised Encryption

- Αντί για κρυπτογράφηση $m$ κρυπτογράφηση $f(m, r)$ όπου $r$ random
- Η $f$ είναι εύκολα αντιστρέψιμη από οποιονδήποτε
- Μια απλή υλοποίηση της $f$: random padding
- Χρήση στο SSL μέχρι πρόσφατα: PKCS1

# Λύσεις RSA II

Η επίθεση του Bleichenbacher (1998) [Ble98]

- Στόχος: Αποκρυπτογράφηση του $c = f(m, r)^e \pmod n$
- Αποστολή πολλών μηνυμάτων της μορφής $c' = cx^e \pmod n$ με τυχαια $x$
- Ο $\mathcal{A}$ προσπαθεί να βρει μηνύματα $m'$ για τα οποία $f(m', r) = (c')^d \pmod n$
- Ανακτά το $m = \frac{m'}{x}$
- Πρακτικά: χρήση *SSL* error codes ως decryption oracle
- Με 300.000 εως 2.000.000 $c'$ μπορεί να αποκρυπτογραφηθεί το $c$
- **Λύση**: RSA - OAEP secure in the random oracle model [BR95]

# Λύσεις El Gamal:Cramer Shoup cryptosystem [CS98] I

- Ronald Cramer, Victor Shoup, Crypto 1998
- Επέκταση του El Gamal
- Χρηση συνάρτησης σύνοψης $H$
- Αν ισχυει η υπόθεση DDH, τότε παρέχει IND-CCA2

# Λύσεις El Gamal:Cramer Shoup cryptosystem [CS98] II

### Δημιουργία Κλειδιών

- Επιλογή πρώτων $p, q$ με $p = 2q + 1$
- $G$ ειναι η υποομάδα ταξης $q$ στον $\mathbb{Z}_p^*$
- Επιλογή random generators $g_1, g_2$
- Επιλογή τυχαίων στοιχείων $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$
- $c = g_1^{x_1} g_2^{x_2} d = g_1^{y_1} g_2^{y_2}, h = g_1^z$
- Δημόσιο Κλειδί: $(c, d, h)$
- Μυστικό Κλειδί: $(x_1, x_2, y_1, y_2, z)$

# Λύσεις El Gamal:Cramer Shoup cryptosystem [CS98] III

## Κρυπτογράφηση

- Μετατροπή μηνύματος $m$ στο $G$
- Επιλογή τυχαίου $r \in \mathbb{Z}_q$
- 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: $(u_1, u_2, e, v)$

# Λύσεις El Gamal:Cramer Shoup cryptosystem [CS98] IV

**Αποκρυπτογράφηση**

- Υπολογισμός $\alpha = H(u_1, u_2, e)$
- Έλεγχος αν $u_1^{x1} u_2^{x2} (u_1^{y1} u_2^{y2})^{\alpha} = v$. Σε περίπτωση αποτυχίας έξοδος χωρίς αποκρυπτογράφηση
- Σε περιπτωση επιτυχίας υπολογισμός $m = \frac{e}{u_1^z}$

# Λύσεις El Gamal:Cramer Shoup cryptosystem [CS98] V

### Παρατηρήσεις

- $h, z$ αντιστοιχούν σε δημόσιο - ιδιωτικό κλειδί El Gamal
- $u_1, e$ αντιστοιχούν στο κρυπτογράφημα του El Gamal
- Η $H$ μπορεί να αντικατασταθεί για αποφυγή του random oracle
- $u_2, v$ λειτουργεί ως έλεγχος ακεραιότητας, ώστε να μπορεί να αποφευχθεί το malleability
- Διπλάσια πολυπλοκότητα από ElGamal τόσο σε μέγεθος κρυπτοκειμένου, όσο και σε υπολογιστικές απαιτήσεις

# References I

[Ble98] Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the rsa encryption standard pkcs1. pages 1–12. Springer-Verlag, 1998.

[Bon12] Dan Boneh. Cryptography i. Coursera Online Course, November 2012.

[BR95] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption – how to encrypt with rsa. pages 92–111. Springer-Verlag, 1995.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *Advances in Cryptology — CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer Berlin Heidelberg, 1998.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.

[Sho98] Victor Shoup. Why chosen ciphertext security matters, 1998.