

Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία

Επιθέσεις και Ασφάλεια Κρυπτοσυστημάτων

Διδάσκοντες: Άρης Παγουρτζής – Στάθης Ζάχος

Αρχικές διαφάνειες: Παναγιώτης Γροντάς
Τροποποιήσεις: Άρης Παγουρτζής

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Επιθέσεις ενεργητικού αντιπάλου (adversary) $\mathcal{A}$

Chosen Plaintext Attack

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

Chosen Ciphertext Attack

- Ικανότητα 1: Ο $\mathcal{A}$ μπορεί να κρυπτογραφεί μηνύματα της επιλογής του
- Ικανότητα 2: Ο $\mathcal{A}$ μπορεί να αποκρυπτογραφεί κρυπτοκείμενα της επιλογής του
- Στόχος: Ο $\mathcal{A}$ θέλει να μάθει την αποκρυπτογράφηση ενός κρυπτοκειμένου, αλλά δεν μπορεί να χρησιμοποιήσει την Ικανότητα 2 απευθείας στο κρυπτοκείμενο αυτό.

Indistinguishability under Chosen Plaintext Attack (IND-CPA) I

CPA Game

- Ο προκαλών (challenger) $\mathcal{C}$ δημιουργεί ζεύγος κλειδιών (PK, SK) και δημοσιεύει το PK
- Ο αντίπαλος $\mathcal{A}$ κρυπτογραφεί έως και πολυωνυμικό πλήθος μηνυμάτων της επιλογής του
- Τελικά υποβάλλει δύο μηνύματα M_0, M_1 στο σύστημα
- Ο προκαλών $\mathcal{C}$ διαλέγει τυχαία 1 bit b και στέλνει το $C = Enc(M_b)$ στον $\mathcal{A}$
- Ο $\mathcal{A}$ κρυπτογραφεί (το πολύ) πολυωνυμικό πλήθος μηνυμάτων της επιλογής του και κάνει οποιονδήποτε άλλο υπολογισμό μπορεί
- Τελικά “μαντεύει” το b

Indistinguishability under Chosen Plaintext Attack (IND-CPA) II

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 εντελώς τυχαία.

Indistinguishability under Chosen Ciphertext Attack (IND-CCA1) I

Indistinguishability under Chosen Ciphertext Attack (IND-CCA1) II

CCA Game

- Ο προκαλών $\mathcal{C}$ δημιουργεί ζεύγος κλειδιών (PK, SK) , δημοσιεύει PK
- Ο αντίπαλος $\mathcal{A}$ κρυπτογραφεί έως πολυωνυμικό πλήθος μηνυμάτων της επιλογής του
- Ο $\mathcal{A}$ χρησιμοποιεί το *decryption oracle* και αποκρυπτογραφεί έως πολυωνυμικό πλήθος κρυπτοκειμένων της επιλογής του
- Τελικά υποβάλλει δύο μηνύματα M_0, M_1 στον προκαλούντα $\mathcal{C}$
- Ο προκαλών $\mathcal{C}$ διαλέγει τυχαία 1 bit b και στέλνει το $C = Enc(M_b)$ στον $\mathcal{A}$
- Ο $\mathcal{A}$ κρυπτογραφεί έως πολυωνυμικό πλήθος μηνυμάτων της επιλογής του και κάνει οποιονδήποτε άλλο υπολογισμό μπορεί
- Τελικά “μαντεύει” το b

Indistinguishability under Chosen Ciphertext Attack (IND-CCA1) I

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 εντελώς τυχαία.

Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2) I

Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2) II

CCA Game

- Ο προκαλών $\mathcal{C}$ δημιουργεί ζεύγος κλειδιών (PK, SK) , δημοσιεύει PK
- Ο αντίπαλος $\mathcal{A}$ κρυπτογραφεί έως πολωνυμικό πλήθος μηνυμάτων της επιλογής του
- Ο $\mathcal{A}$ χρησιμοποιεί το *decryption oracle* και αποκρυπτογραφεί έως πολωνυμικό πλήθος κρυπτοκειμένων της επιλογής του
- Τελικά υποβάλλει δύο μηνύματα M_0, M_1 στον προκαλούντα $\mathcal{C}$
- Ο $\mathcal{C}$ διαλέγει τυχαία 1 bit b και στέλνει το $C = Enc(M_b)$ στον $\mathcal{A}$
- Ο $\mathcal{A}$ κρυπτογραφεί έως πολωνυμικό πλήθος επιλ. μηνυμάτων
- Ο $\mathcal{A}$ αποκρυπτογραφεί έως πολωνυμικό πλήθος επιλ. κρυπτοκειμένων, διαφορετικών από το C και κάνει οποιονδήποτε άλλο υπολογισμό μπορεί
- Τελικά “μαντεύει” το b

Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2) I

Ορισμός ασφάλειας

Το κρυπτοσύστημα έχει την ιδιότητα IND-CCA2 αν κάθε PPT $\mathcal{A}$ έχει αμελητέο πλεονέκτημα στον υπολογισμό του b από το να μαντέψει εντελώς τυχαία.

Malleability: μια σχετική ιδιότητα

Ένας ορισμός

Ένα κρυπτοσύστημα λέγεται *malleable* (εύπλαστο) εάν είναι δυνατόν ένας αντίπαλος να φτιάξει, γνωρίζοντας μόνο το κρυπτοκείμενο $c = E(m)$, δηλαδή το κρυπτογράφημα ενός μηνύματος m , ένα έγκυρο κρυπτοκείμενο $c' = E(h(m))$, για κάποια, συνήθως πολυωνυμικά αντιστρέψιμη, συνάρτηση h γνωστή σε αυτόν.

Μπορεί δηλαδή να αλλοιώσει οποιοδήποτε κρυπτοκείμενο, ώστε να αντιστοιχεί σε μήνυμα που είναι το αρχικό μήνυμα αλλαγμένο με γνωστό και αντιστρέψιμο τρόπο.

Malleability: μια σχετική ιδιότητα

Ένας ορισμός

Ένα κρυπτοσύστημα λέγεται *malleable* (εύπλαστο) εάν είναι δυνατόν ένας αντίπαλος να φτιάξει, γνωρίζοντας μόνο το κρυπτοκείμενο $c = E(m)$, δηλαδή το κρυπτογράφημα ενός μηνύματος m , ένα έγκυρο κρυπτοκείμενο $c' = E(h(m))$, για κάποια, συνήθως πολυωνυμικά αντιστρέψιμη, συνάρτηση h γνωστή σε αυτόν.

Μπορεί δηλαδή να αλλοιώσει οποιοδήποτε κρυπτοκείμενο, ώστε να αντιστοιχεί σε μήνυμα που είναι το αρχικό μήνυμα αλλαγμένο με γνωστό και αντιστρέψιμο τρόπο.

Κάποιες φορές είναι επιθυμητή και κάποιες όχι.

Malleability: μια σχετική ιδιότητα

Ένας ορισμός

Ένα κρυπτοσύστημα λέγεται *malleable* (εύπλαστο) εάν είναι δυνατόν ένας αντίπαλος να φτιάξει, γνωρίζοντας μόνο το κρυπτοκείμενο $c = E(m)$, δηλαδή το κρυπτογράφημα ενός μηνύματος m , ένα έγκυρο κρυπτοκείμενο $c' = E(h(m))$, για κάποια, συνήθως πολυωνυμικά αντιστρέψιμη, συνάρτηση h γνωστή σε αυτόν.

Μπορεί δηλαδή να αλλοιώσει οποιοδήποτε κρυπτοκείμενο, ώστε να αντιστοιχεί σε μήνυμα που είναι το αρχικό μήνυμα αλλαγμένο με γνωστό και αντιστρέψιμο τρόπο.

Κάποιες φορές είναι επιθυμητή και κάποιες όχι.

Σημαντική ιδιότητα

Non-malleability $\Leftrightarrow$ IND-CCA2

Παράδειγμα 1: παραδοσιακό RSA I

Το παραδοσιακό RSA δεν είναι IND-CPA γιατί είναι deterministic

Αν τα δύο μηνύματα του $\mathcal{A}$ είναι:

- $m_0 = \text{"Buy IBM"}$
- $m_1 = \text{"Sell IBM"}$

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

Παράδειγμα 1: παραδοσιακό RSA II

Το παραδοσιακό RSA δεν είναι CCA-secure

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

- Στόχος: Αποκρυπτογράφιση του $c = m_b^e \pmod{n}$
- Μπορεί να αποκρυπτογραφήσει το $c' = c_b x^e \pmod{n}$ όπου το x είναι δικής του επιλογής
- Ανακτά το $m_b = \frac{m'}{x}$
- Αν $m_b = m_0$ επιστρέφει $b^* = 0$ αλλιώς επιστρέφει $b^* = 1$

Παράδειγμα 2: παραδοσιακό ElGamal

Το ElGamal είναι IND-CPA αν ισχύει η DDH assumption: απόδειξη στον πίνακα.

Παράδειγμα 2: παραδοσιακό ElGamal

Το ElGamal είναι IND-CPA αν ισχύει η DDH assumption: απόδειξη στον πίνακα.

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

Παράδειγμα 2: παραδοσιακό ElGamal I

Το παραδοσιακό El Gamal δεν είναι CCA-secure ούτε IND-CCA2-secure

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

- Στόχος: Αποκρυπτογράφηση του $c = (G, M) = (g^r, m_b h^r)$
- Κατασκευή $c' = (G', M') = (Gg^{r'}, Mah^{r'}) = (g^{r+r'}, m_b ah^{r+r'})$, 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 $b^* = 1$

Λύσεις για το 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 για το 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 τυχαία 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 έως 2.000.000 c' μπορεί να αποκρυπτογραφηθεί το c
- **Λύση:** RSA - OAEP secure in the random oracle model [BR95]

Λύσεις για το 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 για το El Gamal: Cramer-Shoup cryptosystem [CS98] II

Δημιουργία Κλειδίων

- Επιλογή πρώτων p, q με $p = 2q + 1$
- G είναι 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 για το 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 για το El Gamal: Cramer-Shoup cryptosystem [CS98] IV

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 $m = \frac{e}{u_1^{\bar{e}}}$

Λύσεις για το 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 λειτουργούν 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.