Μοντέλα και Αποδείξεις Ασφάλειας στην Κρυπτογραφία

Παναγιώτης Γροντάς

ΕΜΠ - Κρυπτογραφία

09/10/2015

Περιεχόμενα

Κρυπτοσύστημα Ι

- $\mathcal{CS} = (\mathtt{M}, \mathtt{K}, \mathtt{C}, \mathtt{KeyGen}, \mathtt{Encrypt}, \mathtt{Decrypt})$
- $\mathtt{M}$: Σύνολο Μηνυμάτων
- $\mathtt{K}$: Σύνολο Κλειδιών
- $\mathtt{C}$: Σύνολο Κρυπτοκειμένων
- $\mathtt{KeyGen}(1^\lambda) = (key_{enc}, key_{dec}) \in \mathtt{K}^2$
  - Πιθανοτικός Αλγόριθμος
  - Το κλειδί συνήθως επιλέγεται *ομοιόμορφα* από το $\mathtt{K}$
  - λ : Παράμετρος ασφάλειας - πλήθος bits του κλειδιού
- $\mathtt{Encrypt}(key_{enc}, m) = c \in \mathtt{C}$
  - Ντετερμινιστικός Αλγόριθμος: Κάθε μήνυμα αντιστοιχεί σε ένα κρυπτοκείμενο
  - Πιθανοτικός Αλγόριθμος: Κάθε μήνυμα αντιστοιχεί σε ένα σύνολο πιθανών κρυπτοκειμένων
- $\mathtt{Decrypt}(key_{dec}, c) = m$

Κρυπτοσύστημα II

Παρατηρήσεις:

- Συμμετρικό Κρυπτοσύστημα $key_{enc} = key_{dec}$
- Ασύμμετρο Κρυπτοσύστημα $key_{enc} \neq key_{dec}$
  - Κρυπτογραφία Δημοσίου Κλειδιού
  - Το key_{enc} μπορεί να δημοσιοποιηθεί για την εύκολη ανταλλαγή μηνυμάτων
- Ορθότητα σε κάθε περίπτωση:
  $\mathtt{Decrypt}(key_{dec}, \mathtt{Encrypt}(key_{enc}, m)) = m, \forall m \in \mathtt{M}$

Ο αντίπαλος $\mathcal{A}$

- Στόχος: Να *σπάσει* το κρυπτοσύστημα
- Δηλαδή, με δεδομένο το c:
  - Να μάθει το κλειδί k;
    - Επίθεση Πυρηνικής Βόμβας
    - Θέλουμε να προστατεύσουμε το μήνυμα
    - $\text{Encrypt}(k, m) = m$ παρέχει ασφάλεια αλλά όχι μυστικότητα
  - Να μάθει ολοκληρο το αρχικό μήνυμα m;
    - Αν μάθει το 90%;
  - Να μάθει κάποια συνάρτηση του m;
    - Ναι αλλά ποια;
- Συμπέρασμα:Χρειάζονται ακριβείς ορισμοί
  - Για το τι σημαίνει ’σπασιμο’
  - Για τις δυνατότητες και τα μέσα του αντιπάλου.

Δυνατότητες και Μέσα (Ιστορικά) I

Επιθέσεις

- Επίθεση Μόνο Κρυπτοκειμένου - Ciphertext Only Attack (COA)
  - Παθητικός Αντίπαλος
  - Πολύ εύκολη: Χρειάζεται απλά πρόσβαση στο κανάλι επικοινωνίας

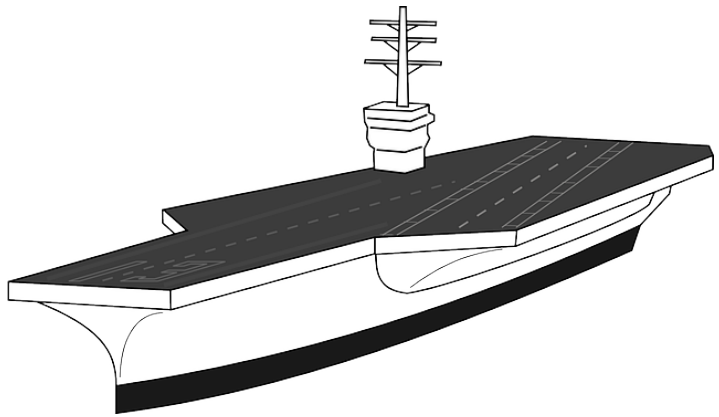
Δυνατότητες και Μέσα (Ιστορικά) II

- Επίθεση Γνωστού Μηνύματος - Known Plaintext Attack (KPA)
  - Παθητικός Αντίπαλος
  - Γνωρίζει ζεύγη μηνυμάτων - κρυπτοκειμένων
  - Ρεαλιστικό σενάριο
    - Ακόμα και τα απόρρητα πρωτόκολλα περιέχουν μη απόρρητα μηνύματα (handshakes, ack)
    - Enigma: Κρυπτοκείμενα πρόγνωσης καιρού
    - Κρυπτογραφημένα μηνύματα γίνονται κάποια στιγμή διαθέσιμα

Δυνατότητες και Μέσα (Ιστορικά) III

- Επίθεση Επιλεγμένου Μηνύματος - Chosen Plaintext Attack (CPA)

- Ενεργός Αντίπαλος
- Γνωρίζει ζεύγη μηνυμάτων - κρυπτοκειμένων
- Μπορεί να ζητήσει την κρυπτογράφηση μηνυμάτων της επιλογής του (Μαντείο Κρυπτογράφησης)
- Ιστορικό Παράδειγμα: Η ναυμαχία του Midway (1942)
  - Αποστολή Πλαστών Μηνυμάτων Με Την Λέξη Midway
  - Συλλογή Επικοινωνιών Με Κρυπτοκείμενα AF



Δυνατότητες και Μέσα (Ιστορικά) IV

- Επίθεση Επιλεγμένου Κρυπτοκειμένου - Chosen Ciphertext Attack (CCA)
  - Ενεργός Αντίπαλος
  - Γνωρίζει ζεύγη μηνυμάτων - κρυπτοκειμένων
  - Μπορεί να ζητήσει την κρυπτογράφηση μηνυμάτων της επιλογής του (Μαντείο Κρυπτογράφησης)
  - Μπορεί να επιτύχει την αποκρυπτογράφηση μηνυμάτων της επιλογής του (Μαντείο Αποκρυπτογράφησης)
  - Ο αντίπαλος μπορεί να βγάλει *έμμεσα* her από αντιδράσεις σε κρυπτογραφημένα μηνύματα
    - Απόρριψη κρυπτογραφημένων ’σκουπιδιών’ από το πρωτόκολλο (Bleichenbacher RSA PKCS1 attack)
    - Ενέργεια στον πραγματικό κόσμο (πχ. αγορά μετοχών)

Οι κανόνες του Kerchoffs (1883) I

Αρχή 2

Ο αλγόριθμος(από)κρυπτογράφησης δεν πρέπει να είναι μυστικός. Πρέπει να μπορεί να πέσει στα χέρια του $\mathcal{A}$ χωρίς να δημιουργήσει κανένα πρόβλημα. Αντίθετα το κλειδί μόνο πρέπει να είναι μυστικό.

Λόγοι:

- Το κλειδί διανέμεται πιο εύκολα από τους αλγόριθμους (μικρότερο μέγεθος, απλούστερη δομή)
- Το κλειδί είναι πιο εύκολο να αλλαχθεί αν διαρρεύσει
- Πιο πρακτική χρήση για περισσότερους από έναν συμμετέχοντες
- Ανοικτό κρυπτοσύστημα: Εύκολη μελέτη

Οι κανόνες του Kerchoffs (1883) II

Παρατηρήσεις:
Αν και έχουν παράδοση ακόμα και σήμερα δεν εφαρμόζονται πλήρως

- (Μεγάλες) εταιρίες δημιουργούν και χρησιμοποιούν δικούς τους μυστικούς αλγόριθμους/πρωτόκολλα
  - Bruce Schneier Crypto Snake Oil

Οι κανόνες του Kerchoffs (1883) III

Αρχή 1

Το κρυπτοσύστημα θα πρέπει να είναι *πρακτικά* απρόσβλητο, αν δεν γίνεται θεωρητικά

- Διάρκεια Κρυπτανάλυσης > Διάρκεια Ζωής Μηνύματος
- Μικρή Πιθανότητα Επιτυχίας
- Υπολογιστική Ασφάλεια

Σε κάθε περίπτωση - Εμπειρικές Αρχές: Δεν παρέχουν εγγυήσεις ασφάλειας

Τέλεια μυστικότητα (Shannon, 1949) I

Υποθέσεις:

- αρχικό κείμενο $M \in \mathtt{M}$, το κλειδί $K \in \mathtt{K}$, κρυπτοκείμενο $C \in \mathtt{C}$ τυχαίες μεταβλητές
- M και K είναι ανεξάρτητες, ενώ η C εξαρτάται από τις άλλες δύο.
- Ο $\mathcal{A}$ μπορεί να έχει απεριόριστη υπολογιστική ισχύ

Τέλεια μυστικότητα (Shannon, 1949) II

Ο ορισμός του Shannon

$$\forall x \in \mathtt{M}, y \in \mathtt{C}: \quad \Pr_{M \in \mathtt{M}, K \in \mathtt{K}}[M = x \mid C = y] = \Pr_{M \in \mathtt{M}}[M = x]$$

Τέλεια μυστικότητα (Shannon, 1949) III

Ο ορισμός του Shannon

$$\forall x \in \mathtt{M}, y \in \mathtt{C}: \quad \Pr_{M \in \mathtt{M}, K \in \mathtt{K}}[M = x \mid C = y] = \Pr_{M \in \mathtt{M}}[M = x]$$

Το κρυπτοκείμενο δεν παρέχει καμμία νέα πληροφορία για το αρχικό κείμενο (*a posteriori* πληροφορία ίδια με την *a priori*).

Παράδειγμα:Random SHIFT Cipher

Ορισμός

- $\mathtt{M} = \mathtt{K} = \mathtt{C} = \{0, \ldots, 25\}$
  - Αναπαριστούμε κάθε γράμμα με τη θέση του στο αλφάβητο
  - Η $Pr[m = x]$ ορίζεται από τις στατιστικές συχνότητες των γραμμάτων της αγγλικής
  - Φυσικά $\sum_{x \in \mathtt{M}} \Pr[m = x] = 1$
- *Δημιουργία Κλειδιών*: Τυχαία επιλογή κλειδιού με ομοιόμορφη κατανομή.
  Δηλαδή $k \in \mathtt{K}$: $\Pr[k = i] = \frac{1}{26}, \ 0 \leq i \leq 25$
- *Κρυπτογράφηση*: $c = \mathtt{Encrypt}(k, m) = (m + k) \bmod 26$
- *Αποκρυπτογράφηση*: $\mathtt{Decrypt}(k, c) = (c - k) \bmod 26$

Random SHIFT Cipher και Τέλεια Μυστικότητα

1. $\forall y \in \mathtt{C}: \ \Pr[c = y] = \sum_{x \in \mathtt{M}} \Pr[m = x] \cdot \Pr[k = (y - x) \bmod 26] = \frac{1}{26} \sum_{x \in \mathtt{M}} \Pr[m = x] = \frac{1}{26}$
2. $\forall m \in \mathtt{M}, \ \ y \in \mathtt{C}: \Pr[C = y \mid M = x] = \Pr[k = (y - x) \bmod 26] = \frac{1}{26}$
3. Από τύπο Bayes: $\Pr[M = x \mid C = y] = \frac{\Pr[C=y|M=x] \Pr[M=x]}{\Pr[C=y]}$
4. Από (1),(2),(3):
   $\forall x \in \mathtt{M}, y \in \mathtt{C}: \Pr[M = x \mid C = y] = \frac{\frac{1}{26} \Pr[M=x]}{\frac{1}{26}} = \Pr[M = x]$

Τέλεια μυστικότητα! Μπορεί να επεκταθεί και για μέγεθος κειμένου n.

Ισοδύναμες Συνθήκες Τέλειας Μυστικότητας

1. $\forall x \in \mathtt{M}, y \in \mathtt{C}: \Pr[C = y] = \Pr[C = y \mid M = x]$

   (η πιθανότητα εμφάνισης ενός κρυπτοκειμένου είναι ανεξάρτητη από το αρχικό κείμενο)

2. $\forall x_1, x_2 \in \mathtt{M}, y \in \mathtt{C}: \Pr[C = y \mid M = x_1] = \Pr[C = y \mid M = x_2]$

   (συνθήκη χρήσιμη για *ανταπόδειξη* - perfect indistinguishability)

Τέλεια μυστικότητα: μήκος κλειδιού $\geq$ μήκος κειμένου

Αναγκαία συνθήκη για τέλεια μυστικότητα:

$$|\mathtt{M}| \leq |\mathtt{C}| \leq |\mathtt{K}|$$

- $|\mathtt{M}| \leq |\mathtt{C}|$:
  Αλλιώς, 2 μηνύματα δεν μπορούν να αντιστοιχούν στο ίδιο κρυπτοκείμενο (κρυπτογράφηση '1-1')
- $|\mathtt{C}| \leq |\mathtt{K}|$:
  Αλλιώς, για οποιοδήποτε μήνυμα δεν θα υπήρχαν αρκετά κλειδιά για να 'φθάσουμε' σε όλα τα κρυπτοκείμενα.
  $\forall x \in \mathtt{M}, \exists y \in \mathtt{C}, \Pr[C = y \mid M = x] = 0 \neq Pr[C = y]$.

(Υποθέτουμε ότι $Pr[C = y] > 0$, γιατί αλλιώς μπορούμε να αλλάξουμε το C ώστε να συμβαίνει)

Τέλεια μυστικότητα όταν $|\mathtt{M}| = |\mathtt{C}| = |\mathtt{K}|$ I

Θεώρημα

Έστω κρυπτοσύστημα με $|\mathtt{M}| = |\mathtt{C}| = |\mathtt{K}|$. Το σύστημα έχει τέλεια μυστικότητα *ανν* ισχύουν τα εξής:
(1) για κάθε $x \in \mathtt{M}, y \in \mathtt{C}$, υπάρχει μοναδικό $k \in \mathtt{K}$, ώστε $\mathtt{Encrypt}(k, x) = y$
(2) κάθε κλειδί επιλέγεται με την ίδια πιθανότητα, συγκεκριμένα $1/|\mathtt{K}|$

Τέλεια μυστικότητα όταν $|\mathtt{M}| = |\mathtt{C}| = |\mathtt{K}|$ II

Απόδειξη (ευθύ)

1. Παραβίαση της (1):
   $\exists(x, y, k_1, k_2) : y = \mathtt{Encrypt}(k_1, x) = \mathtt{Encrypt}(k_2, x)$
   Επειδή $|\mathtt{C}| = |\mathtt{M}| = |\mathtt{K}|$ $\exists y' : Pr[C = y'|M = x] = 0$
   Άτοπο λόγω τέλειας μυστικότητας
2. Από τέλεια μυστικότητα
   $\forall i \in \{1, \cdots, |\mathtt{M}|\}$: $Pr[M = m_i] = Pr[M = m_i|C = c] = \frac{Pr[M=m_i]Pr[C=c|M=m_i]}{Pr[C=c]}$
   Από (1): $Pr[C = c|M = m_i] = Pr[K = k_i]$
   Άρα $\forall i \in \{1, \cdots, |\mathtt{K}|\} : Pr[K = k_i] = Pr[C = c]$
   Όλα ισοπίθανα: $Pr[K = k_i] = \frac{1}{|\mathtt{K}|}$

Τέλεια μυστικότητα όταν $|\mathtt{M}| = |\mathtt{C}| = |\mathtt{K}|$ III

Απόδειξη (αντίστροφο)

$Pr[C = y] = \sum_k Pr[K = k]Pr[M = \mathtt{Decrypt}(k, y)] = \frac{1}{|K|} \sum_k Pr[M = \mathtt{Decrypt}(k, y)] = \frac{1}{|K|}$

$Pr[M = x|C = y] = \frac{Pr[M=x]Pr[C=y|M=x]}{Pr[C=y]} = \frac{Pr[M=x]Pr[K=k]}{Pr[C=y]} = Pr[M = x]$

Τέλεια μυστικότητα!

One Time Pad (Vernam, 1917)

Ορισμός

- Plaintext: $x = (x_0, x_1, \ldots, x_{n-1}), \quad x_i \in \{0,1\}$
- Key: $k = (k_0, k_1, \ldots, k_{n-1}), \quad k_i \in \{0,1\}$
- Ciphertext: $y = (y_0, y_1, \ldots, y_{n-1}), \quad y_i \in \{0,1\}$
- Κρυπτογράφηση: $y_i = x_i \oplus k_i = x_i + k_i \bmod 2$
- Αποκρυπτογράφηση: $x_i = y_i \oplus k_i$

Ασφάλεια: αν για κάθε bit k_i του κλειδιού ισχύει $\Pr[k_i = 0] = \Pr[k_i = 1] = 1/2$, τότε το κρυπτοσύστημα έχει τέλεια μυστικότητα (γιατί;).

Συμπεράσματα

- Τέλεια Μυστικότητα: Θεωρητικά Εφικτή, αλλά...
  - Πρακτικά μη πραγματοποιήσιμη
    - Παραγωγή Κλειδιού: Αποδείξιμα Τυχαίες Ακολουθίες
    - Ανταλλαγή Κλειδιού: Μόνο σε κλειστούς οργανισμούς (πχ. στρατός, μυστικές υπηρεσίες)
  - Ασύμβατη με κρυπτογραφία δημοσίου κλειδιού (πολλαπλή χρήση δημοσίου κλειδιού)
- Ανάγκη για νέες μορφές αποδείξιμης ασφάλειας

Σημασιολογική Ασφάλεια I

Βασική ιδέα (Goldwasser, Micali): Χαλαρώνουμε τις υποθέσεις για να οδηγηθούμε σε έναν πιο χρήσιμο ορισμό, λαμβάνοντας υπόψιν:

- την υπολογιστική ισχύ του $\mathcal{A}$
- την πιθανότητα επιτυχίας
- το είδος των επιθέσεων

Διαίσθηση

Ένας υπολογιστικά περιορισμένος $\mathcal{A}$ δεν μπορεί να μάθει τίποτε χρήσιμο από το κρυπτοκείμενο παρά μόνο με αμελητέα πιθανότητα

Σημασιολογική Ασφάλεια II

Ρητή Προσέγγιση

Ένα κρυπτοσύστημα είναι (τ, ϵ) ασφαλές αν οποιοσδήποτε $\mathcal{A}$ σε χρόνο το πολύ τ, δεν μπορεί να το σπάσει με πιθανότητα καλύτερη από ϵ

Για συμμετρικά κρυπτοσυστήματα σήμερα $\tau = 2^{80}$ και $\epsilon = 2^{-64}$
Δεν χρησιμοποιείται γιατί

- Δεν ασχολείται με το υπολογιστικό μοντέλο (κατανεμημένοι υπολογιστές, εξειδικευμένο HW κτλ.)
- Δεν ασχολείται με το τι θα γίνει μετά το τ
- Για τους ίδιους λόγους με Υπολογιστική Πολυπλοκότητα

Σημασιολογική Ασφάλεια III

Ασυμπτωτική Προσέγγιση

Ένα κρυπτοσύστημα είναι ασφαλές αν οποιοσδήποτε PPT $\mathcal{A}$ έχει αμελητέα πιθανότητα να το σπάσει (σε σχέση με την παράμετρο ασφάλειας)

Παρατηρήσεις:

- Ισχύει για μεγάλες τιμές του λ
- Συνέπεια του $|\mathtt{K}| < |\mathtt{M}|$
- Επιτρέπει προσαρμογή της ασφάλειας με αλλαγή του μήκους του κλειδιού

Σημασιολογική Ασφάλεια IV

Τυπικός Ορισμός: Υποθέσεις

- Ο $\mathcal{A}$ θέλει να υπολογίσει το κατηγόρημα $q : \mathtt{M} \to \{0, 1\}$
- $Pr_{m \in \mathtt{M}}[q(m) = 0] = Pr_{m \in \mathtt{M}}[q(m) = 1] = \frac{1}{2}$
- Το μήκος των κρυπτοκειμένων είναι το ίδιο (δεν διαρρέει πληροφορία)

Το πλεονέκτημα του $\mathcal{A}$

$$Adv(\mathcal{A}) = |Pr[\mathcal{A}(c) = q(\mathtt{Decrypt}(key, c))] - \tfrac{1}{2}|$$

Παρατήρηση: Αν ο $\mathcal{A}$ μαντέψει στην τύχη έχει $Adv(\mathcal{A}) = 0$

Σημασιολογική Ασφάλεια V

Ορισμός

Ένα κρυπτοσύστημα είναι σημασιολογικά ασφαλές όταν $\forall$ PPT $\mathcal{A}$, $\forall q$:

$$Adv(\mathcal{A}) = negl(\lambda)$$

Αμελητέα συνάρτηση: Μεγαλώνει με πιο αργό ρυθμό από αντίστροφο πολυώνυμο

Σημασιολογική Ασφάλεια VI

Αμελητέα συνάρτηση

Οποιαδήποτε συνάρτηση για την οποία για κάθε πολυώνυμο p υπάρχει n_0 ώστε $\forall n \geq n_0 : negl(n) < \frac{1}{p(n)}$

Συνήθως: $n^{-c}, c2^{-n}$

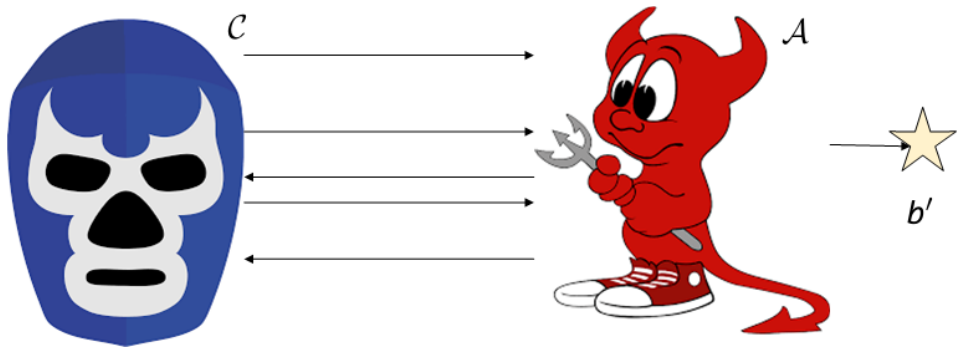
Παρατηρήσεις

- Ο τυπικός ορισμός ενσωματώνει την παράμετρο ασφαλείας
- Δύσχρηστος ορισμός
- Και πάλι δεν ορίσαμε ακριβώς τι σημαίνει 'σπάσιμο'

Μη Διακρισιμότητα(Indistinguishability) I

Παίγνιο Μη Διακρισιμότητας μεταξύ των $\mathcal{A}$, $\mathcal{C}$ (αναπαριστά το κρυπτοσύστημα)

- Ανταλλαγή Μηνυμάτων μεταξύ $\mathcal{A}$, $\mathcal{C}$
- $\mathcal{A}$: Παράγει δύο μηνύματα m_0, m_1
- $\mathcal{C}$: Διαλέγει ένα τυχαίο bit b
- $\mathcal{C}$: Παράγει και απαντά με το $c_b = \mathrm{Encrypt}(m_b)$
- $\mathcal{A}$: Μαντεύει ένα bit b'



$$IND - Game(\mathcal{A}) = \begin{cases} 1, b' = b \\ 0, \text{αλλιώς} \end{cases}$$

Μη Διακρισιμότητα(Indistinguishability) II

Πλεονέκτημα

$$Adv_{IND}(\mathcal{A}) = |Pr[IND - Game(\mathcal{A}) = 1] - \frac{1}{2}|$$

Ορισμός

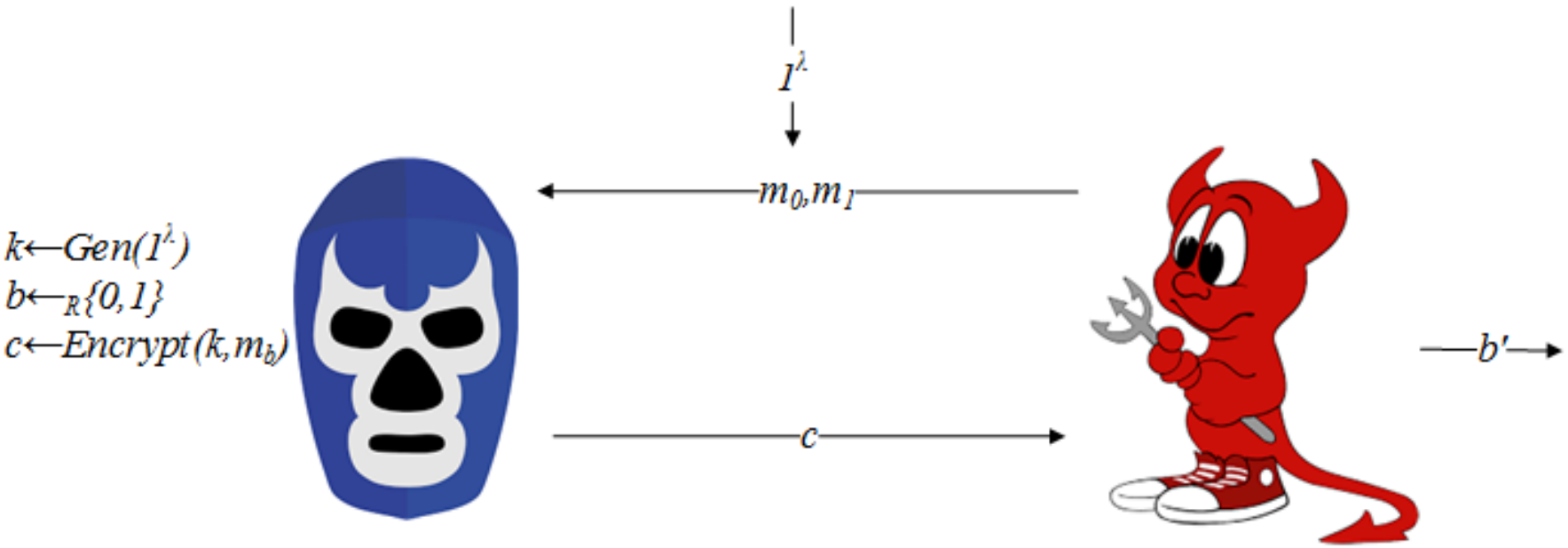
Ένα κρυπτοσύστημα διαθέτει την ιδιότητα της μη διακρισιμότητας όταν $\forall$ PPT $\mathcal{A}$:

$$Adv_{IND}(\mathcal{A}) = negl(\lambda)$$

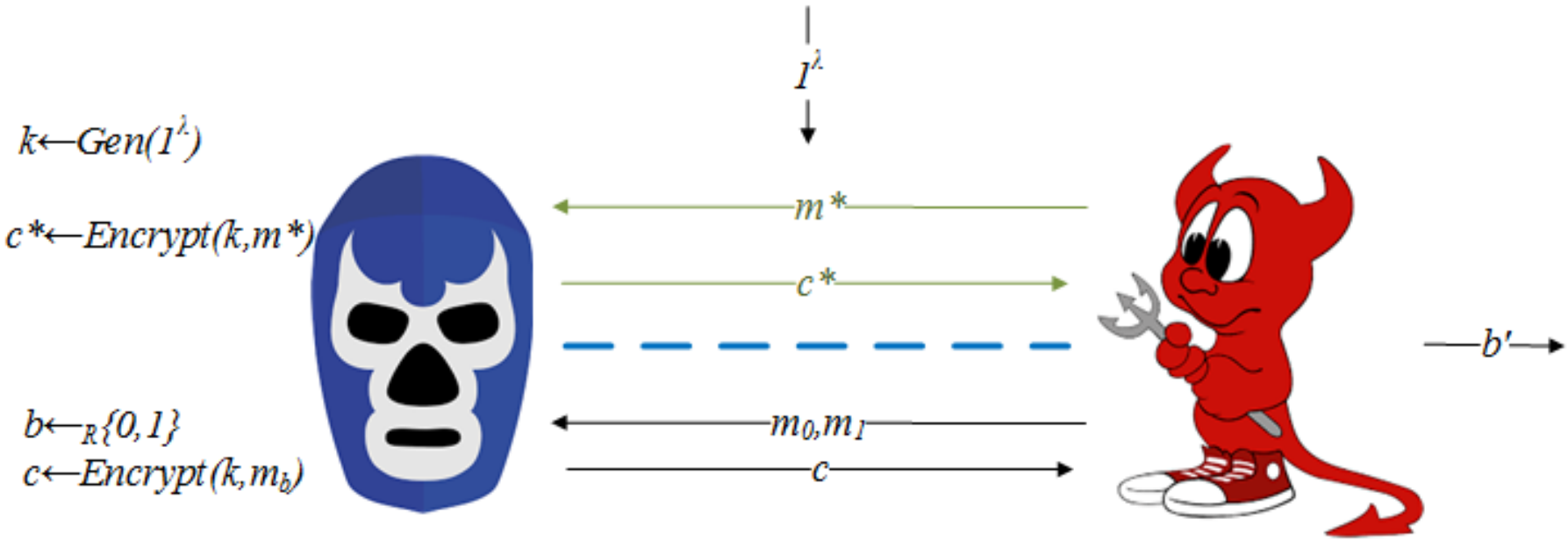
Θεώρημα

Σημασιολογική Ασφάλεια $\Leftrightarrow$ Μη-Διακρισιμοτητα

IND-EAV


1^λ
m_0, m_1
$k \leftarrow Gen(1^\lambda)$
$b \leftarrow_R \{0,1\}$
$c \leftarrow Encrypt(k, m_b)$
c
b'

IND-CPA


1^λ
$k \leftarrow Gen(1^\lambda)$
m^*
$c^* \leftarrow Encrypt(k, m^*)$
c^*
b'
$b \leftarrow_R \{0,1\}$
m_0, m_1
$c \leftarrow Encrypt(k, m_b)$
c

Παρατηρήσεις

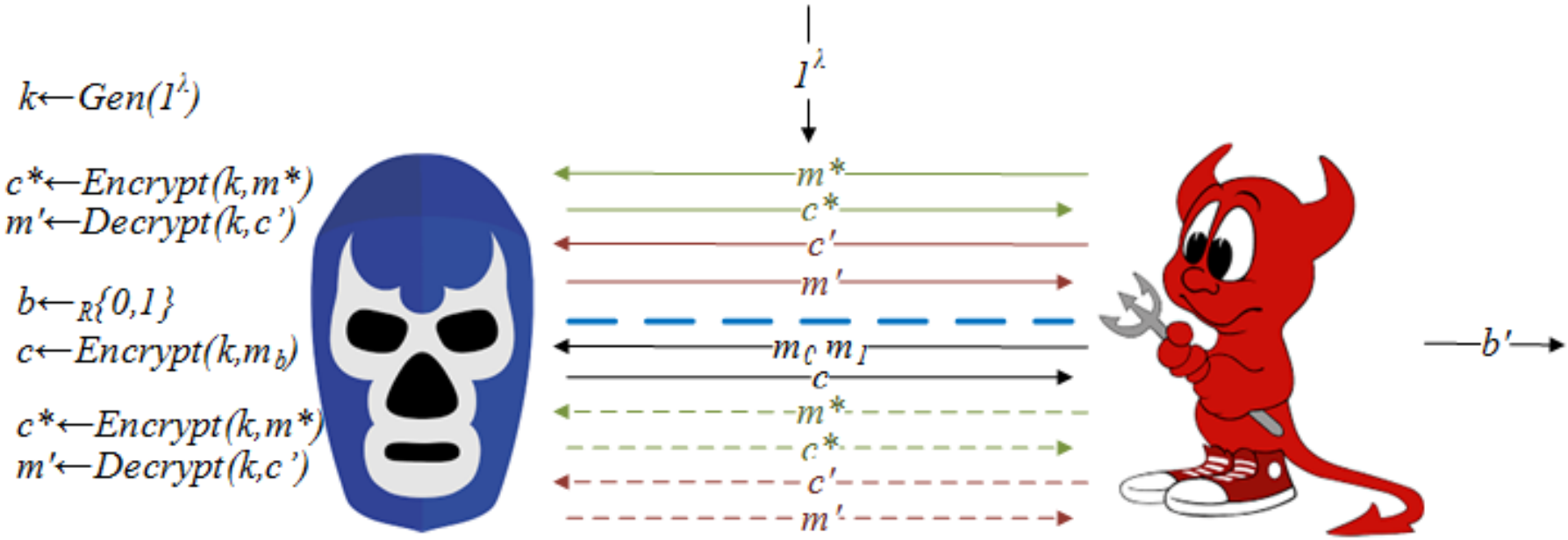
Θεώρημα

Ένα κρυπτοσύστημα με ντετερμινιστικό αλγόριθμο κρυπτογράφησης δεν μπορεί να έχει την ιδιότητα IND-CPA.

Απόδειξη

- Ο $\mathcal{A}$ θέτει $m^* = m_0$ και λαμβάνει την κρυπτογράφηση c^*
- Η απάντηση του είναι $b' = \begin{cases} 0, c^* = c \\ 1, \text{αλλιώς} \end{cases}$
- Ο $\mathcal{A}$ κερδίζει πάντα $Pr[IND - CPA(\mathcal{A}) = 1] = 1$

IND-CCA


$k \leftarrow Gen(1^\lambda)$
$c^* \leftarrow Encrypt(k, m^*)$
$m' \leftarrow Decrypt(k, c')$
$b \leftarrow_R \{0,1\}$
$c \leftarrow Encrypt(k, m_b)$
$c^* \leftarrow Encrypt(k, m^*)$
$m' \leftarrow Decrypt(k, c')$
1^λ
m^*
c^*
c'
m'
m_0, m_1
c
m^*
c^*
c'
m'
b'

Παρατηρήσεις

- Στο παίγνιο IND-CCA ο $\mathcal{A}$ δεν μπορεί να ρωτήσει τον C για την αποκρυπτογραφήση του c
- Μπορεί όμως να:
  - Μετατρέψει το c σε $\hat{c}$
  - Ζητήσει την αποκρυπτογράφηση του $\hat{c}$ σε $\hat{m}$
  - Να μετατρέψει το $\hat{m}$ σε m, κερδίζοντας με πιθανότητα 1
- IND-CCA2: Επιτρέπεται χρήση του μαντείου αποκρυπτογράφησης μετά το c (adaptive IND-CCA)
- IND-CCA1: αλλιώς

Malleability I

Malleable (εύπλαστο) Κρυπτοσύστημα

Επιτρέπει στο $\mathcal{A}$ να φτιάξει, γνωρίζοντας μόνο το κρυπτοκείμενο $c = \mathrm{Encrypt}(m)$, ένα *έγκυρο* κρυπτοκείμενο $c' = \mathrm{Encrypt}(h(m))$, για κάποια, συνήθως πολυωνυμικά αντιστρέψιμη, συνάρτηση h γνωστή σε αυτόν.

Σημαντική ιδιότητα

Non-malleability $\Leftrightarrow$ IND-CCA2

Malleability II

Κάποιες φορές είναι επιθυμητή και κάποιες όχι.

- Ομομορφικά Κρυπτοσυστήματα: Αποτίμηση μερικών πράξεων στα κρυπτοκείμενα (ηλ. ψηφοφορίες)
- Πλήρως Ομομορφικά Κρυπτοσυστήμα (Gentry 2010): Αποτίμηση οποιουδήποτε κυκλώματος στα κρυπτοκείμενα
- Δεν μπορούν να είναι IND-CCA2, ... αλλά είναι πολύ χρήσιμα

Κρυπτογραφικές Αναγωγές I

Γενική Μορφή

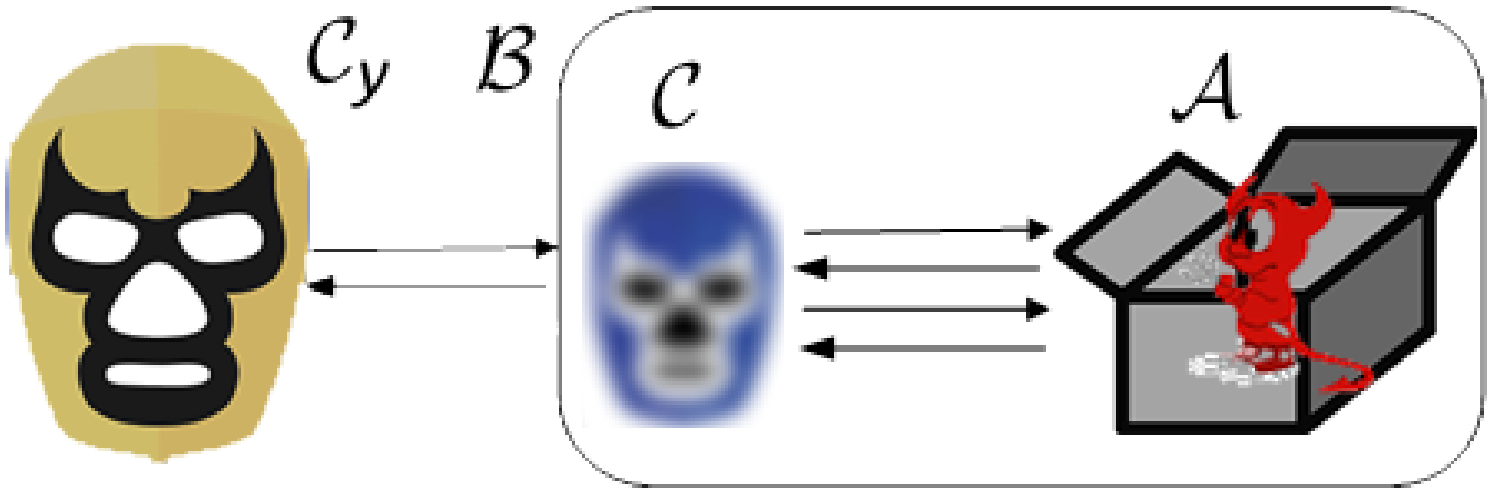
Αν ισχύει η υπόθεση $\mathcal{Y}$, τότε και το κρυπτοσύστημα $\mathcal{CS}$ είναι ασφαλές (υπό συγκεκριμένο ορισμό).

Αντιθετοαντιστροφή

Αν το $\mathcal{CS}$ ΔΕΝ είναι ασφαλές (υπό συγκεκριμένο ορισμό), τότε δεν ισχύει η $\mathcal{Y}$.

Κατασκευαστική απόδειξη

Κρυπτογραφικές Αναγωγές II



Κρυπτογραφικές Αναγωγές III

- $\mathcal{CS}$ μη ασφαλές $\Rightarrow \exists$ PPT $\mathcal{A}$ ο οποίος παραβιάζει τον ορισμό ασφάλειας
- *Κατασκευάζουμε* PPT αλγόριθμο $\mathcal{B}$, ο οποίος αλληλεπιδρά με τον $\mathcal{C}_y$ ο οποίος προσπαθεί να 'υπερασπιστεί' την $\mathcal{Y}$
- Ο $\mathcal{B}$ για να καταρρίψει την $\mathcal{Y}$ χρησιμοποιεί εσωτερικά σαν υπορουτίνα τον $\mathcal{A}$ (black box access) παριστάνωντας τον $\mathcal{C}$ στο παίγνιο μη διακρισιμότητας του $\mathcal{CS}$

Παρατηρήσεις

Κανόνες Ορθότητας

- Προσομοίωση: Ο $\mathcal{A}$ δεν θα πρέπει να ξεχωρίζει τον $\mathcal{B}$ από οποιονδήποτε άλλο εισηγητή.
- Πιθανότητα επιτυχίας: Αν ο $\mathcal{A}$ έχει μη αμελητέα πιθανότητα επιτυχίας τότε και ο $\mathcal{B}$ θα πρέπει να έχει μη αμελητέα πιθανότητα
- Πολυπλοκότητα: Ο $\mathcal{B}$ θα πρέπει να είναι PPT. Αυτό πρακτικά σημαίνει ότι όποια επιπλέον εσωτερική επεξεργασία πρέπει να είναι πολυωνυμική
- Πρέπει να είναι όσο πιο tight γίνεται ($t_{\mathcal{B}} \approx t_{\mathcal{A}}$ και $\epsilon_{\mathcal{B}} \approx \epsilon_{\mathcal{A}}$)

Συμπεράσματα-Συζήτηση

Κρυπτογραφικές Αναγωγές

- Παρέχουν σχετικές εγγυήσεις (Δύσκολο Πρόβλημα, Μοντέλο Ασφάλειας)
- Δίνουν ευκαιρία να ορίσουμε καλύτερα το κρυπτοσύστημα/πρωτόκολλο
- Πρακτική Χρησιμότητα: Ρύθμιση Παραμέτρου Ασφάλειας
- Συγκέντρωση Κρυπταναλυτικών Προσπαθειών στο Πρόβλημα Αναγωγής και όχι σε κάθε κρυπτοσύστημα ξεχωριστά
- Πιο σημαντικές όσο πιο πολύπλοκο γίνεται το πρωτόκολλο
- Δεν σημαίνει ότι οποιαδήποτε υλοποίηση θα είναι ασφαλής

Βιβλιογραφία I

- St. Zachos and Aris Pagourtzis. Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία. Πανεπιστημιακές Σημειώσεις
- 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
- Alptekin Kupcu. Proofs In Cryptography
- S. Goldwasser and S. Micali. Probabilistic encryption. Journal of Computer and System Sciences, 28(2):270–299, 1984.
- S. Micali, C. Rackoff, and B. Sloan. The notion of security for probabilistic cryptosystems. SIAM J. Computing, 17(2):412–426, 1988.

Βιβλιογραφία II

- Ivan Damgard, A proof reading of some issues in cryptography
- Neil Koblitz, Alfred Menezes Another Look at “Provable Security”
- Bruce Schneier’s Blog
  - Memo to the Amateur Cipher Designer (https://goo.gl/92TW36)
  - Crypto Snake Oil (https://goo.gl/FaFoSK)
- A Few Thoughts on Cryptographic Engineering
- Bristol Cryptography Blog
- Kerckhoffs Wikipedia Entry (https://goo.gl/SHnu8K)