Μοντέλα και Αποδείξεις Ασφάλειας στην Κρυπτογραφία - Ανταλλαγή Κλειδιού Diffie Hellman

Παναγιώτης Γροντάς - Άρης Παγουρτζής

ΕΜΠ - Κρυπτογραφία (2017-2018)

07/11/2017

Περιεχόμενα

- Ορισμός Κρυπτοσυστήματος
- Δυνατότητες Αντιπάλου - Επιθέσεις
- Εμπειρική Ασφάλεια (Kerckhoffs) - Σημασιολογική Ασφάλεια - Μη Διακρισιμότητα
- Γενική Μορφή Κρυπτογραφικών Αναγωγών
- Ανταλλαγή Κλειδιού Diffie Hellman

Κρυπτοσύστημα I

- $\mathcal{CS} = (\mathtt{M}, \mathtt{K}, \mathtt{C}, \mathtt{KeyGen}, \mathtt{Encrypt}, \mathtt{Decrypt})$
- $\mathtt{M}$: 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
    - $\texttt{Encrypt}(k, m) = m$ 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

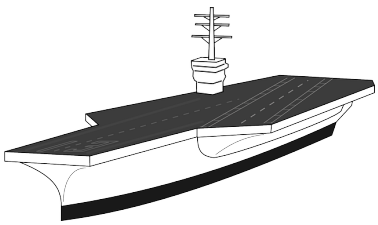
Δυνατότητες και Μέσα (Ιστορικά) II

- Επίθεση Γνωστού Μηνύματος - Known Plaintext Attack (KPA)
  - Παθητικός Αντίπαλος
  - Γνωρίζει ζεύγη μηνυμάτων - κρυπτοκειμένων
  - Ρεαλιστικό σενάριο για συμμετρικά
    - Ακόμα και τα απόρρητα πρωτόκολλα περιέχουν μη απόρρητα μηνύματα (handshakes, ack)
    - Enigma: Κρυπτοκείμενα πρόγνωσης καιρού
    - Κρυπτογραφημένα μηνύματα γίνονται κάποια στιγμή διαθέσιμα
  - Τετριμμένο σενάριο για ασύμμετρα
    - Ο $\mathcal{A}$ έχει το δημόσιο κλειδί
    - Μπορεί να κατασκευάσει μόνος του όσα ζεύγη θέλει

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'
  - Συσχέτιση με παλιότερες επικοινωνίες



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* συμπεράσματα 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

Οι πρώτες προσπάθειες ορισμού ασφάλειας κρυπτοσυστήματων και προστασίας

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

Οι κανόνες του Kerchoffs (1883) II

- Ανοικτό κρυπτοσύστημα: Εύκολη μελέτη
- (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 αντιστοιχίζονται σε κάτι απτό

Γενικά

Ιδέα

Μαθηματική (Λογική) απόδειξη ότι το κρυπτοσύστημα έχει κάποιες ιδιότητες ασφάλειας.

Παράδειγμα: Τέλεια μυστικότητα (Shannon)
Πρόβλημα: Μπορεί να εφαρμοστεί στην κρυπτογραφία δημοσίου κλειδιού; Γιατί;
Επαναχρησιμοποίηση δημοσίου κλειδιού

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 $q : \mathtt{M} \rightarrow \{0, 1\}$
- $Pr_{m \in \mathtt{M}}[q(m) = 0] = Pr_{m \in \mathtt{M}}[q(m) = 1] = \frac{1}{2}$
- 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: $c2^{-n}, 2^{-\sqrt{n}}, n^{-logn}$

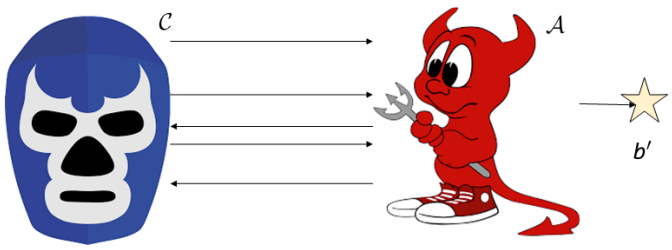
Παρατηρήσεις

- Ο τυπικός ορισμός ενσωματώνει την παράμετρο ασφαλείας
- Δύσχρηστος ορισμός
- Δεν ορίσαμε ακριβώς τη διαδικασία προς το '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 $c_b = \texttt{Encrypt}(m_b)$
- $\mathcal{A}$: 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

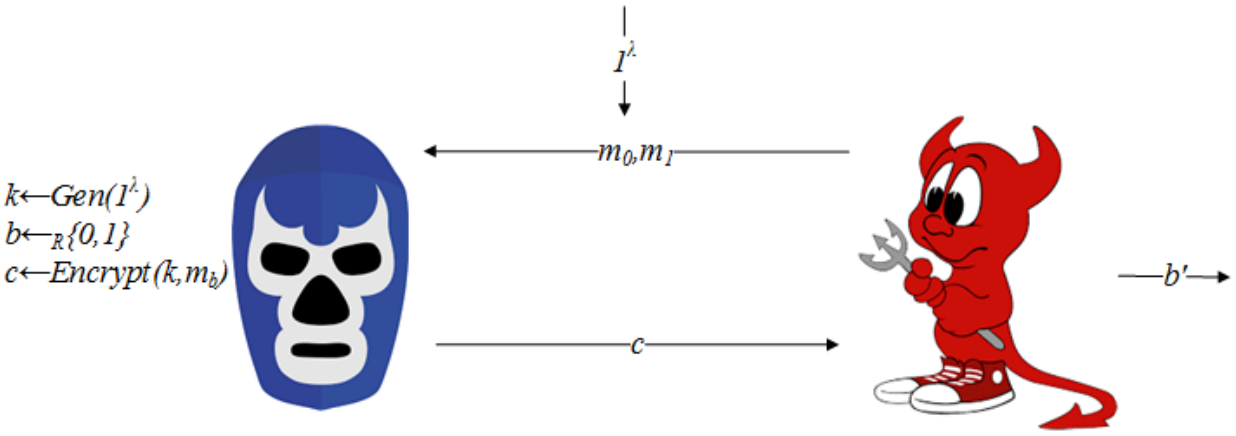
Ένα κρυπτοσύστημα διαθέτει την ιδιότητα της μη διακρισιμότητας όταν $\forall$ PPT $\mathcal{A}$:

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

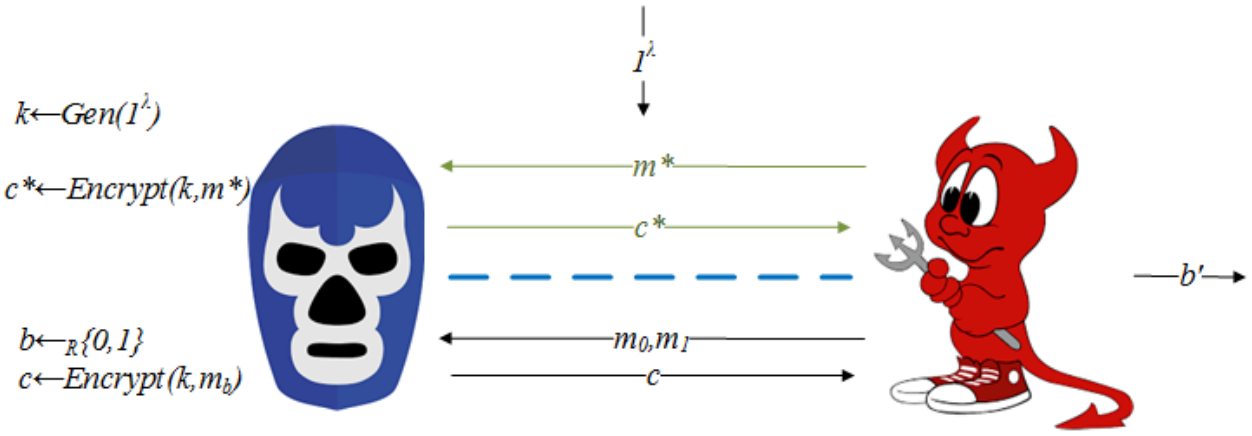
Θεώρημα

Σημασιολογική Ασφάλεια $\Leftrightarrow$ Μη-Διακρισιμοτητα

IND-EAV



IND-CPA



Παρατηρήσεις

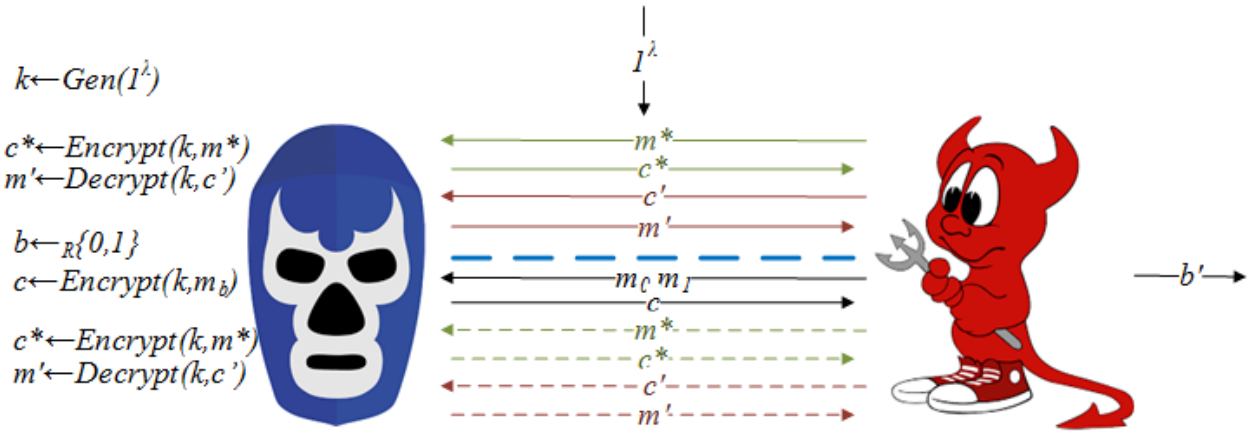
Θεώρημα

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



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 $c = \texttt{Encrypt}(m)$, ένα *έγκυρο* κρυπτοκείμενο $c' = \texttt{Encrypt}(h(m))$, 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 Ι

Γενική Μορφή

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

Αντιθετοαντιστροφή

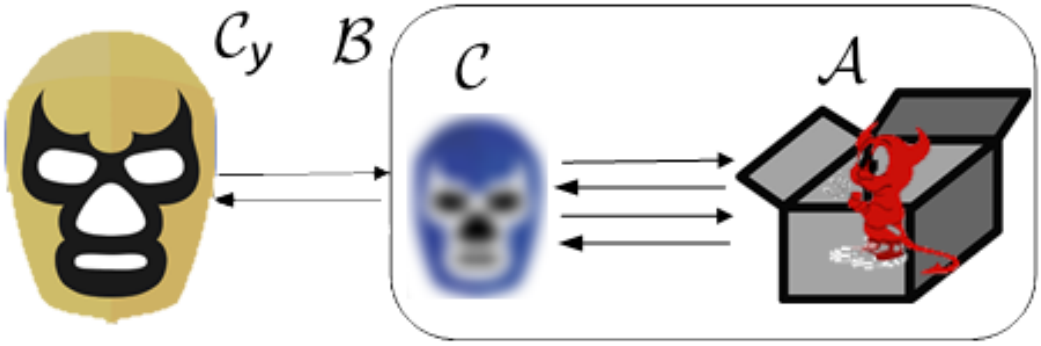
Αν το $\mathcal{CS}$ ΔΕΝ είναι ασφαλές (υπό συγκεκριμένο ορισμό), τότε δεν ισχύει η $\mathcal{Y}$.

Κατασκευαστική απόδειξη

Κρυπτογραφικές Αναγωγές ΙΙ

- $\mathcal{CS}$ 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 $\mathcal{CS}$

Κρυπτογραφικές Αναγωγές III



Παρατηρήσεις

Κανόνες Ορθότητας

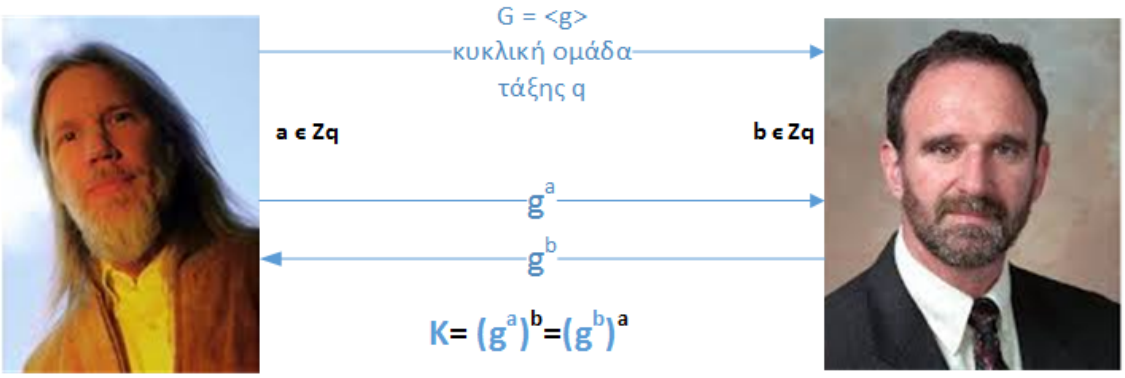
- Προσομοίωση: Ο $\mathcal{A}$ δεν θα πρέπει να ξεχωρίζει τον $\mathcal{B}$ από οποιονδήποτε άλλο εισηγητή.
- Πιθανότητα επιτυχίας: Αν ο $\mathcal{A}$ έχει μη αμελητέα πιθανότητα επιτυχίας τότε και ο $\mathcal{B}$ θα πρέπει να έχει μη αμελητέα πιθανότητα
- Πολυπλοκότητα: Ο $\mathcal{B}$ θα πρέπει να 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
- Αποδεικνύουν την ασφάλεια του μοντέλου
  - Πόσο αναπαριστά το μοντέλο την πραγματικότητα; KRACK
  - Δεν σημαίνει ότι οποιαδήποτε υλοποίηση θα είναι ασφαλής

Το πρωτόκολλο DHKE



Πρωτόκολλο **Δημιουργίας** Κλειδιού
Απαιτήσεις:
Ορθότητα: Αντιμεταθετική ιδιότητα
Ασφάλεια: Ύψωση σε δύναμη - μονόδρομη συνάρτηση στην $\mathbb{G}$
Συνήθως: $\mathbb{G}$ υποομάδα του $\mathbb{Z}_p^*$ με p πρώτο
Εφαρμογές: SSL, TLS, IPSEC

Σχετιζόμενα Προβλήματα Ι

DLP - Το πρόβλημα του Διακριτού Λογαρίθμου

Δίνεται μια κυκλική ομάδα $\mathbb{G} =< g >$ 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

Σχετιζόμενα Προβλήματα ΙΙ

CDHP - Το υπολογιστικό πρόβλημα Diffie Hellman

Δίνεται μια κυκλική ομάδα $\mathbb{G} =< g >$, δύο στοιχεία
$y_1 = g^{x_1}, y_2 = g^{x_2}$
Να υπολογιστεί το $g^{x_1 \cdot x_2}$

Σχετιζόμενα Προβλήματα III

Μπορούμε να δοκιμάζουμε τυχαία στοιχεία

DDHP - Το πρόβλημα απόφασης Diffie Hellman

Δίνεται μια κυκλική ομάδα $\mathbb{G} =< g >$, 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 $\mathbb{G} =< g >$, 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);

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 I

Διαίσθηση

Ένας (παθητικός) αντίπαλος δεν αποκτά καμία χρήσιμη πληροφορία για το κλειδί που δημιουργείται.

Ισοδύναμα

Ένας (παθητικός) αντίπαλος δεν μπορεί να διακρίνει το κλειδί από ένα τυχαίο στοιχείο της ομάδας στην οποία ανήκει

Ασφάλεια DHKE II

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

- Εκτέλεση πρωτοκόλλου $\Pi(1^\lambda) \rightarrow (\tau, k)$
- τ: Τα μηνύματα που ανταλλάσσονται (δημόσια)
- k: Το κλειδί που παράγεται (ιδιωτικό)
- Επιλογή τυχαίου $b \in \{0, 1\}$
- Αν $b = 0$ επιλογή τυχαίου k' αλλιώς $k' = k$
- Εκτέλεση $\mathcal{A}\ (\tau, k') \rightarrow b'$
- Αν $b' \neq b$ τότε το αποτέλεσμα του παιχνιδιού είναι 0, αλλιώς 1

Ασφάλεια DHKE III

Ορισμός ασφάλειας

Ένα πρωτόκολλο ανταλλαγής κλειδιού Π είναι ασφαλές, αν κάθε PPT *παθητικός* αντίπαλος $\mathcal{A}$ έχει αμελητέα πιθανότητα ως προς την παράμετρο ασφάλειας να επιτύχει στο *KEG*

$Prob[KEG(\lambda, \Pi, \mathcal{A}) = 1] \leq \frac{1}{2} + negl(\lambda)$

Απόδειξη ασφάλειας DHKE

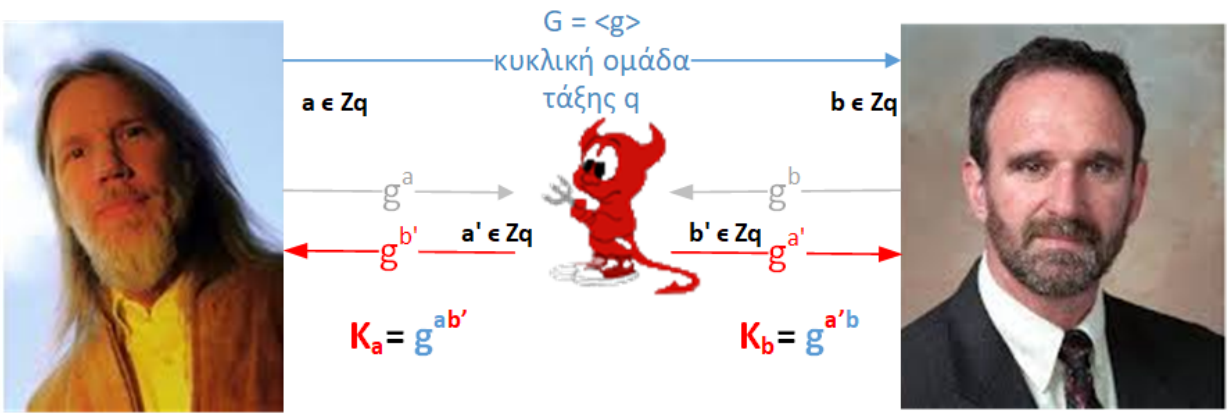
$DDH \implies DHKE$

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

Απόδειξη - Σχεδιάγραμμα Έστω ότι το DHKE δεν είναι ασφαλές.
$\exists \mathcal{A}$ ώστε $Prob[KEG(\lambda, \Pi, \mathcal{A}) = 1] > \frac{1}{2} + non - negl(\lambda)$
Θα κατασκευάσουμε αντίπαλο PPT $\mathcal{B}$ ο οποίος παραβιάζει την *DDH*.
Τα μηνύματα που ανταλλάσσονται είναι τα $\tau = (\mathbb{G}, g, g^{x_1}, g^{x_2})$
Εκτελούμε τον $\mathcal{A}$ με είσοδο $(\tau, g^{x_1 x_2})$
Επειδή το $g^{x_1 x_2}$ είναι έγκυρο κλειδί:
$Prob[KEG(\lambda, \Pi, \mathcal{A}(\tau, g^{x_1 x_2})) = 1] > \frac{1}{2} + non - negl(\lambda)$
Εκτελούμε τον $\mathcal{A}$ με είσοδο (τ, y) με $y \in_R \mathbb{G}$
Επειδή το y είναι τυχαίο στοιχείο:
$Prob[KEG(\lambda, \Pi, \mathcal{A}(\tau, y))=1]=1_{\frac{1}{2}}$
Άρα ο $\mathcal{B}$ μπορεί να σπάσει την DDH γιατί μπορεί να ξεχωρίσει με μη αμελητέα πιθανότητα το y από το g^{x_1, x_2} ΑΤΟΠΟ

Ενεργοί Αντίπαλοι

Man In The Middle Attacks



Superfish - Lenovo (02/2015)
DELL - 10/2015

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

- W. Diffie and M. Hellman. New directions in cryptography. IEEE Trans. Inf. Theor., 22(6):644-654, September 1976
- Ivan Damgard, A proof reading of some issues in cryptography
- Neil Koblitz, Alfred Menezes Another Look at "Provable Security"
- Dan Boneh (1998). "The Decision Diffie–Hellman Problem". ANTS-III: Proceedings of the Third International Symposium on Algorithmic Number Theory. Springer-Verlag: 48–63. doi:10.1007/bfb0054851
- 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

Βιβλιογραφία III

- Bristol Cryptography Blog
- Kerckhoffs Wikipedia Entry (`https://goo.gl/SHnu8K`)