Αποδείξιμη Ασφάλεια – Ανταλλαγή κλειδιού Diffie - Hellman

Παναγιώτης Γροντάς
ΕΜΠ

Κρυπτογραφία
2025 - 2026

Περιεχόμενα

- Η έννοια της ασφάλειας – είδη επιθέσεων
- Μοντέλα ασφάλειας
- Αποδείξεις Ασφάλειας
- Ανταλλαγή κλειδιού Diffie - Hellman

Η έννοια της ασφάλειας – είδη επιθέσεων

Εισαγωγή

- **Χαρακτηρίζουμε ένα σύστημα ως ασφαλές. Τι εννοούμε;**
- **Πώς μπορούμε να είμαστε σίγουροι για τον χαρακτηρισμό μας;**
  - Ανάγκη για αυστηρότητα
- **Μια βασική ασυμμετρία:**
  - Ασφάλεια: Προστασία από κάθε απόπειρα παραβίασης $\forall$
  - Μη-ασφάλεια: Αρκεί να γίνει μία παραβίαση $\exists$

Ορισμός κρυπτοσυστήματος

- **Μια πλειάδα $CS = (M, C, K, KGen, Enc, Dec)$**
  - M: Σύνολο μηνυμάτων
  - C: Σύνολο κρυπτογραφημάτων
  - K: Σύνολο κλειδιών
  - $KGen$: Αλγόριθμος δημιουργίας κλειδιών
  - Enc: Αλγόριθμος κρυπτογράφησης
  - Dec: Αλγόριθμος αποκρυπτογράφησης

Δημιουργία κλειδιών

- $\boldsymbol{KGen}\left(\boldsymbol{1}^{\boldsymbol{\lambda}}\right) \rightarrow (\boldsymbol{ek}, \boldsymbol{dk}) \in \boldsymbol{K}^{\boldsymbol{2}}$
- **Πιθανοτικός αλγόριθμος; Επιλέγει κλειδιά ομοιόμορφα από K^2**
- **λ: Παράμετρος ασφάλειας (πλήθος bits του κλειδιού)**
  - Συμβολισμός στο μοναδιαίο σύστημα αρίθμησης
  - Χαρακτηρισμός ασφάλειας ως προς μέγεθος λ και όχι ως προς το πλήθος των ψηφίων της αναπαράστασής της.
  - Π.χ. για ασφάλεια 80 bits θέλουμε να έχουμε 80 ψηφία και όχι $\log_2 80 \approx 7$ ή $\log_{10} 80 \approx 2$

- **Σημασία λ για:**
  - χρόνο παραγωγής κλειδιών
  - χρόνο εκτέλεσης κρυπτογράφησης,
  - υπολογιστικής προσπάθειας / πιθανότητας επιτυχίας ’σπασίματος

Δημιουργία κλειδιών

- **Συμμετρικά κρυπτοσυστήματα**
  - $ek = dk$
- **Ασύμμετρα κρυπτοσυστήματα**
  - $ek \neq dk$
  - Το ek μπορεί να δημοσιοποιείται και όποιος θέλει θα δημιουργεί εύκολα κρυπτογραφήματα ή να επαληθεύει υπογραφές
    - Κρυπτογραφία δημοσίου κλειδιού
  - Το dk πρέπει να μείνει μυστικό

(Από)Κρυπτογράφηση

- $\boldsymbol{Enc(ek, m) \rightarrow c \in C}$
  - Ντετερμινιστικός αλγόριθμος: το μήνυμα αντιστοιχεί πάντα στο ίδιο κρυπτογράφημα
  - Πιθανοτικός αλγόριθμος: το μήνυμα αντιστοιχεί σε σύνολο από πιθανά κρυπτογραφήματα
- $\boldsymbol{Dec(dk, c) \rightarrow m \in M}$
  - Πάντα ντετερμινιστικός
  - Αν η κρυπτογράφηση είναι πιθανοτική πρέπει με κάποιον τρόπο να αναιρέσει την τυχαιότητα
- **Ορθότητα:**
  - $Dec\big(dk, Enc(ek, m)\big) = m, \forall m \in M, (ek, dk) \leftarrow KGen(1^{\lambda})$

Ο αντίπαλος $\mathcal{A}$

- **Οντότητα που μοντελοποιεί όλες τις επιθέσεις που μπορεί να γίνουν στο κρυπτοσύστημα**
- **Έχει πάντα στη διάθεσή του το κρυπτοκείμενο c και στα ασύμμετρα συστήματα και το key_{enc}**
- **Πιθανοί στόχοι:**
  - $Enc(ek, m) = m$ είναι άθραυστο (και άχρηστο)
  - Να μάθει το m?
  - Αν μάθει το 90%;
  - Να μάθει ένα κατηγόρημα του m?
    - Π.χ. ότι το τελευταίο bit είναι 1;

- **Χρειάζονται αυστηροί ορισμοί για:**
  - *Κριτήρια επιτυχίας $\mathcal{A}$*
  - *Τρόποι επίθεσης*
  - *Υπολογιστικές δυνατότητες*

Είδη επιθέσεων

- **Ciphertext-only Attack (CoA)**
  - Ο $\mathcal{A}$ διαθέτει μόνο το κρυπτοκείμενο
  - Ωτακουστής (Eve): Παθητικός αντίπαλος που παρακολουθεί το κανάλι επικοινωνίας (στιγμιαία)
- **Known Plaintext Attack (KPA)**
  - Παθητικός αντίπαλος
  - *Διαθέτει ζεύγη (m, c) μηνυμάτων – κρυπτοκειμένων*
  - **Ρεαλιστικό σενάριο**:
    - Κάποια μηνύματα δεν είναι απόρρητα (π.χ. handshakes, ACKs κλπ)
    - Μετά από καιρό κάποια κρυπτογραφημένα μηνύματα δημοσιοποιούνται
      - π.χ. μηνύματα πρόγνωσης καιρού Enigma

Είδη Επιθέσεων (2)

- **Chosen Plaintext Attack (CPA)**
  - Ενεργός αντίπαλος
  - Διαθέτει ζεύγη (m, c) μηνυμάτων – κρυπτοκειμένων
  - *Μπορεί να ζητήσει την **κρυπτογράφηση** μηνυμάτων της επιλογής του (πρόσβαση σε μαντείο κρυπτογράφησης)*
  - **Τετριμμένο σενάριο** για ασύμμετρα: Με το δημόσιο κλειδί μπορεί να κατασκευάσει c κατά βούληση
  - **Ιστορικό Παράδειγμα:** Σπάσιμο κρυπτοσυστήματος JN-25b στη ναυμαχία του Midway (Ιούνιος 1942)
    - Υποψία ότι $Enc(\text{"}Midway\text{"}) = \text{"}AF\text{"}$
    - Αποστολή Μηνυμάτων για επισκευή του συστήματος υδροδότησης του 'Midway'
    - Συλλογή Επικοινωνιών Ιαπώνων και συσχέτιση με χρονική στιγμή

Είδη Επιθέσεων 3

- **Chosen Ciphertext Attack (CCA)**
  - Ενεργός αντίπαλος
  - Διαθέτει ζεύγη (m, c) μηνυμάτων – κρυπτοκειμένων
  - Μπορεί να ζητήσει την κρυπτογράφηση μηνυμάτων της επιλογής του (πρόσβαση σε μαντείο κρυπτογράφησης)
  - *Μπορεί να ζητήσει την **αποκρυπτογράφηση** κρυπτοκειμένων της επιλογής του (πρόσβαση σε μαντείο αποκρυπτογράφησης)*
    - Ο αντίπαλος μπορεί να βγάλει έμμεσα συμπεράσματα από αντιδράσεις σε κρυπτογραφημένα μηνύματα (της επιλογής του)
      - Π.χ. αποστολή μη αποδεκτών μηνυμάτων σε πρωτόκολλο (Bleichenbacher RSA PKCS1 attack)
      - Ενέργεια στον πραγματικό κόσμο (πχ. αγορά μετοχών) ως αντίδραση σε κρυπτογραφημένα μηνύματα.

Μοντέλα Ασφάλειας

Οι κανόνες του Kerchoffs (1883)

Οι πρώτες προσπάθειες ορισμού ασφάλειας κρυπτοσυστημάτων

Αρχή 1: Το κρυπτοσύστημα θα πρέπει να είναι **πρακτικά** απρόσβλητο, αν δεν γίνεται απόλυτα .

Λόγοι:

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

Οι κανόνες του Kerchoffs (1883)

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)

- **Εμπειρικές Αρχές**
- **Αν και έχουν παράδοση αιώνων ακόμα και σήμερα δεν εφαρμόζονται πλήρως**
  - (Μεγάλες) εταιρίες δημιουργούν και χρησιμοποιούν δικούς τους μυστικούς αλγόριθμους/πρωτόκολλα
  - Crypto Snake Oil (Bruce Schneier) snake oil Archives - Schneier on Security

Αποδείξιμη Ασφάλεια

Μαθηματική (Λογική) **απόδειξη** ότι το κρυπτοσύστημα έχει κάποιες ιδιότητες ασφάλειας οι οποίες έχουν οριστεί τυπικά.

Παράδειγμα: Τέλεια μυστικότητα (Shannon)
Δυστυχώς όμως η τέλεια μυστικότητα δεν μπορεί να εφαρμοστεί στην κρυπτογραφία δημοσίου κλειδιού.

Γιατί;

Σημασιολογική Ασφάλεια

- **Goldwasser, Micali (1982)**
- **Βασική ιδέα: Χαλαρώνουμε τις απαιτήσεις ασφάλειας για να οδηγηθούμε σε έναν πρακτικό ορισμό**
- **Λαμβάνουμε υπ' όψιν:**
  - την υπολογιστική ισχύ του $\mathcal{A}$
  - την πιθανότητα επιτυχίας
  - το είδος των επιθέσεων
  - τον στόχο του $\mathcal{A}$

Ένας υπολογιστικά περιορισμένος $\mathcal{A}$ δεν μπορεί να επιτύχει στην επίθεση του παρά μόνο με αμελητέα πιθανότητα σε σχέση με την παράμετρο ασφάλειας

Ρητή προσέγγιση

Ορισμός: 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

Συνέπεια: Ένα κρυπτοσύστημα με παράμετρο ασφάλειας λ είναι $\left(\tau, \frac{\tau}{2^{\lambda}}\right)$-ασφαλές στην καλύτερη περίπτωση

Εξήγηση: Μια επίθεση brute-force σε χρόνο τ έχει πιθανότητα επιτυχίας $\frac{\tau}{2^{\lambda}}$

Πρακτικά:

Βραχυχρόνια ασφάλεια με:

$$\tau \in [2^{80}..2^{100}] \text{ και } \epsilon \approx 2^{-64}$$

Μακροχρόνια ασφάλεια με:

$$\tau \approx 2^{128} \text{ και } \epsilon \approx 2^{-128}$$

Quantum Computers:

$$\tau \approx 2^{256} \text{ (αλγόριθμος Grover)}$$

Ρητή προσέγγιση

Distributed.net RC5 brute force cracking	
56bits	250 days (1997)
64bits	5 years (2002)
72bits	36 years (…)
Bitcoin mining	
2022	2^{90} hashes
2023	2^{93} hashes
2024	2^{94} hashes

Εκτιμάται ότι από το Big Bang έχουν περάσει $2^{58} sec$

Πρακτικά η ρητή προσέγγιση δεν χρησιμοποιείται:

- Δεν λαμβάνει υπ’ οψιν το υπολογιστικό μοντέλο
- Δεν ασχολείται με το τι θα γίνει μετά το τ

Ασυμπτωτική προσέγγιση

- **Υπολογιστικά Περιορισμένος Αντίπαλος:**
  - Probabilistic Polynomial Time
- Οι ορισμοί ισχύουν για μεγάλες τιμές του λ
- Επιτρέπει προσαρμογή της ασφάλειας με αλλαγή του μήκους του κλειδιού

Ένας υπολογιστικά περιορισμένος $\mathcal{A}$ δεν μπορεί να επιτύχει στην επίθεση του παρά μόνο με αμελητέα πιθανότητα σε σχέση με την παράμετρο ασφάλειας

Σημασιολογική Ασφάλεια

Ο PPT $\mathcal{A}$ θέλει με είσοδο ένα κρυπτοκείμενο να υπολογίσει ένα **efficiently computable** κατηγόρημα για το μήνυμα: $Q: M \to \{0,1\}$

Γενικά: $\Pr_{m \in M}[Q(m) = 0] = \Pr_{m \in M}[Q(m) = 1] = \frac{1}{2}$

Ορίζουμε το πλεονέκτημα του $\mathcal{A}$ για κατηγόρημα q σε κρυπτοσύστημα με κλειδί k ως:

$$Adv_Q^A(\lambda) = \left| \Pr\left[\mathcal{A}(c) = Q\left(Dec_k(c)\right)\right] - \frac{1}{2} \right|$$

Αν ο $\mathcal{A}$ μαντέψει στην τύχη: $Adv_Q^A(\lambda) = 0$

Δύσχρηστος ορισμός:

- Δεν περιγράφει την επίθεση – αντίπαλο
- Μας ωθεί να ψάχνουμε κατηγόρημα
- Αλλά ενσωματώνει την παράμετρο ασφάλεια

Ένα κρυπτοσύστημα είναι σημασιολογικά ασφαλές αν για κάθε PPT αντίπαλο και για κάθε κατηγόρημα $Adv_Q^A(\lambda) = neql(\lambda)$

Αμελητέα Συνάρτηση

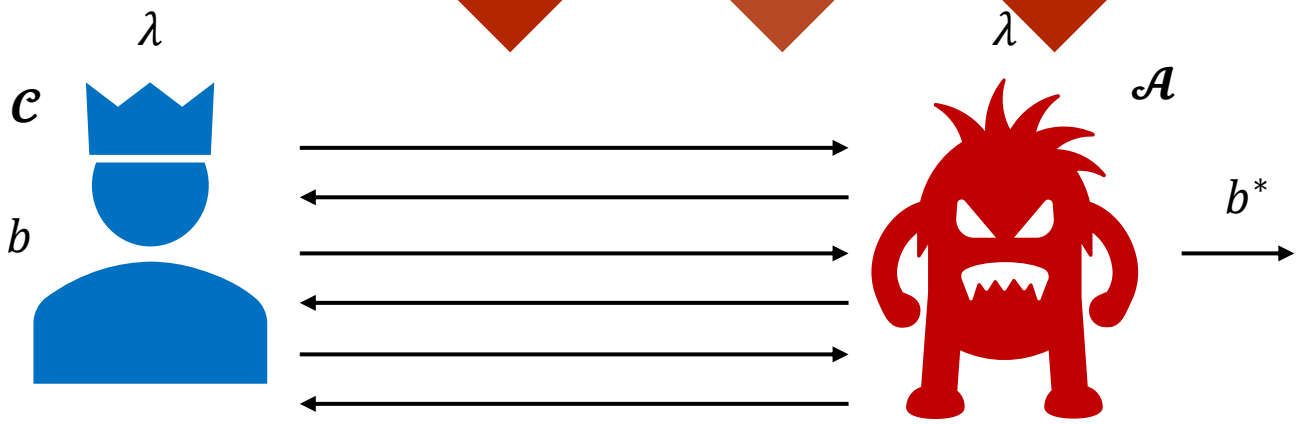
- Μεγαλώνει πιο αργά από αντίστροφο πολυώνυμο

Μια συνάρτηση f είναι αμελητέα αν για κάθε πολύωνυμο p υπάρχει n_0: $\forall n > n_0 : f(n) < \frac{1}{p(n)}$

- Παραδείγματα: $2^{-n}, 2^{-\sqrt{n}}$

Μη-διακρισιμότητα (Indistinguishability)

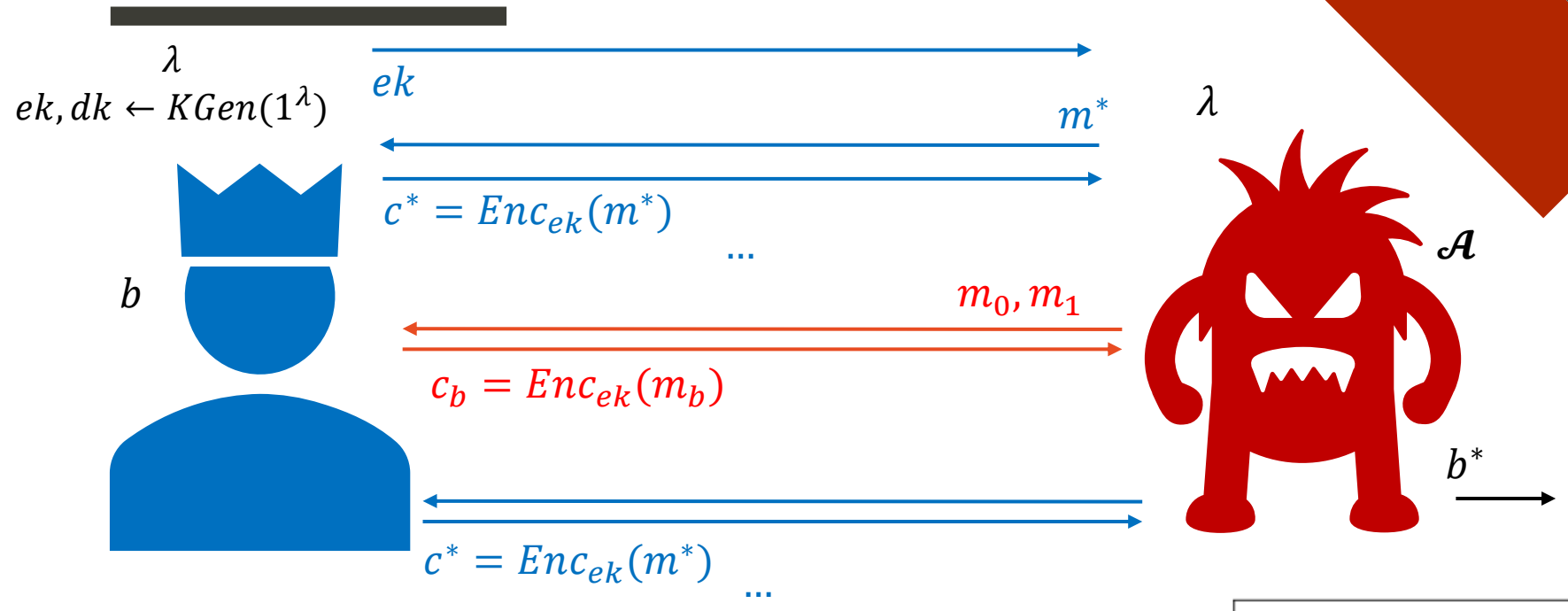
- Ορίζουμε την ασφάλεια μέσω ενός παιγνίου μεταξύ του υπερασπιστή (challenger) του κρυπτοσυστήματος $\mathcal{C}$ και του αντιπάλου $\mathcal{A}$
- Οι $\mathcal{C}, \mathcal{A}$ ανταλλάσσουν μηνύματα
- Κάποια στιγμή ο $\mathcal{C}$ θα κάνει μια τυχαία επιλογή $b \leftarrow \{0,1\}$
- Ο $\mathcal{A}$ μαντεύει b^* για το b
- Κερδίζει αν $b^* = b$
- Το κρυπτοσύστημα είναι **μη διακρίσιμο** αν η πιθανότητα να κερδίσει ο $\mathcal{A}$ είναι αμελητέα.



Η ανταλλαγή μηνυμάτων δίνει περισσότερη εκφραστικότητα στον ορισμό γιατί μπορεί να περιγράψει την επίθεση του $\mathcal{A}$

Σημασιολογική Ασφάλεια ⇔ Μη-διακρισιμότητα

IND-CPA



Χρήση encryption oracle

$$Adv^{\mathcal{A}}_{\text{INDCPA}}(\lambda) = \left|\Pr\left[\mathcal{A}^{\text{INDCPA}}(\lambda) = 1\right] - \frac{1}{2}\right| \leq negl(\lambda)$$

Game $\text{CPA}^{\text{A},b}_{\text{PKE}}(\lambda)$	Oracle $\text{Enc}(m_0, m_1)$
1 : $(\text{ek}, \text{dk}) \leftarrow \text{PKE.KeyGen}(1^\lambda)$	1 : $c \leftarrow \text{PKE.Enc}(\text{ek}, m_b)$
2 : $b' \leftarrow \text{A}^{\text{Enc}}(\text{ek})$	2 : **return** c
3 : **return** $(b = b')$	

IND-CPA

Θεώρημα

Ένα κρυπτοσύστημα που διαθέτει ντετερμινιστικό αλγόριθμο κρυπτογράφησης, δεν μπορεί να είναι ασφαλές σύμφωνα με τον ορισμό IND-CPA.

Απόδειξη

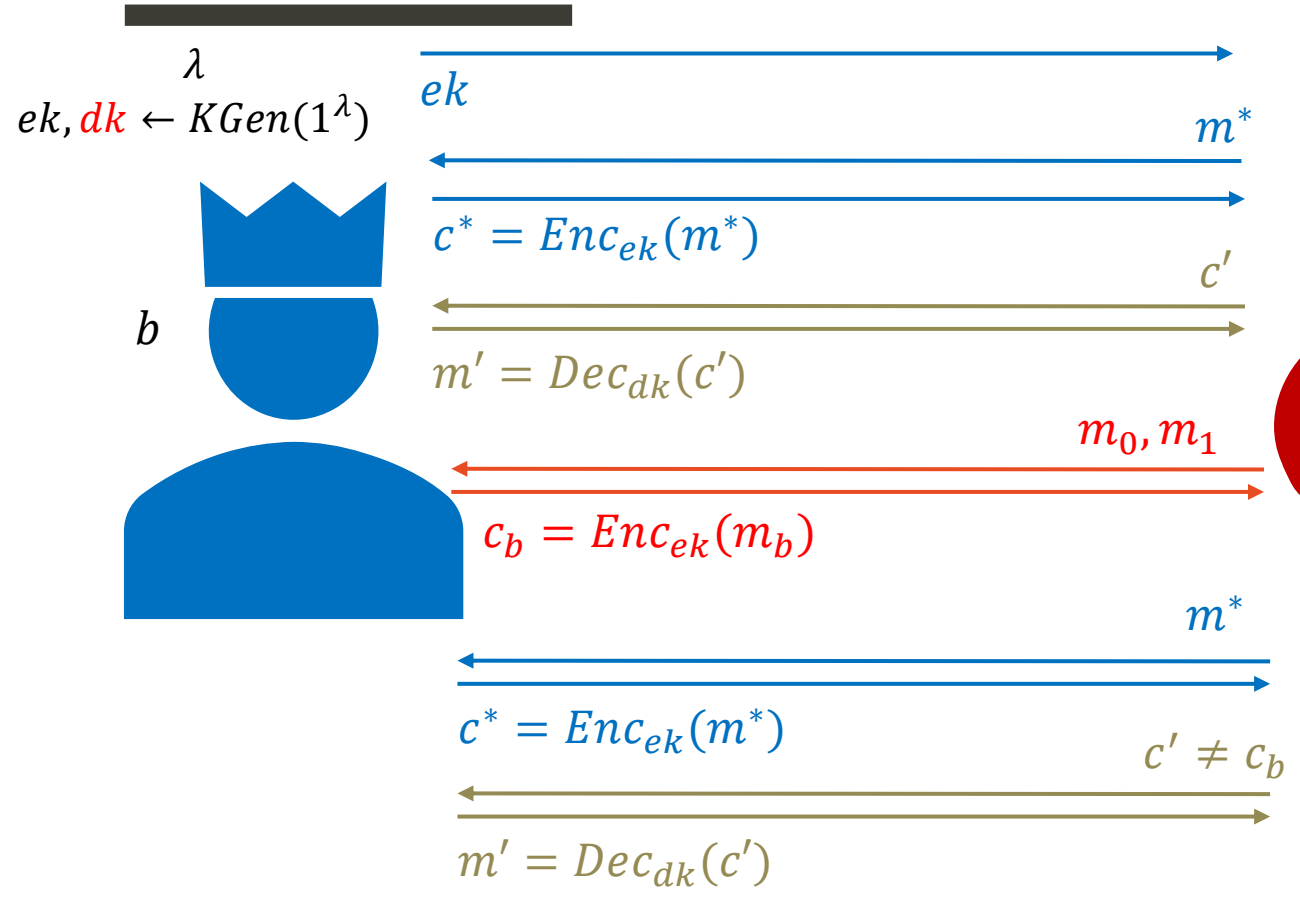
Ο αντίπαλος επιλέγει $m^* = m_0$. Λαμβάνει κρυπτογράφηση c^*.

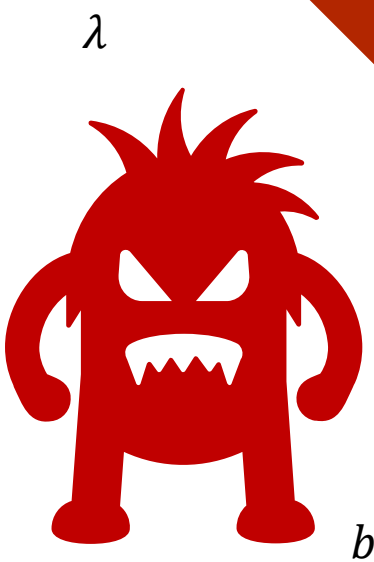
Αν $c_b = c^*$ τότε $b' = 0$ αλλιώς $b^* = 1$.

Με αυτή τη στρατηγική κερδίζει πάντα.

Πώς θα επηρέαζε η πιθανοτική κρυπτογράφηση την στρατηγική αυτή?

IND-CCA





Χρήση encryption decryption oracle

$$Adv^{\mathcal{A}}_{\text{INDCCA}}(\lambda) = \left|\Pr\left[\mathcal{A}^{\text{INDCCA}}(\lambda) = 1\right] - \frac{1}{2}\right|$$

IND-CCA

- **IND-CCA1**
  - Ο $\mathcal{A}$ δεν μπορεί να χρησιμοποιήσει το decryption oracle αφού έχει λάβει το c_b
  - *Προσωρινή δυνατότητα αποκρυπτογράφησης*
  - Θεωρητικό μόνο ενδιαφέρον
- **IND-CCA2 (adaptive CCA)**
  - Ο $\mathcal{A}$ μπορεί να χρησιμοποιήσει το decryption oracle αφού έχει λάβει το c_b
  - Τότε όμως δεν μπορεί να ρωτήσει το c_b
  - Μπορεί όμως να ρωτήσει μια ‘πειραγμένη’ εκδοχή του c_b
  - *Μόνιμη δυνατότητα αποκρυπτογράφησης*
  - **Το επιθυμητό επίπεδο ασφάλειας για κρυπτοσυστήματα δημοσίου κλειδιού**

Malleability

Για κρυπτοκείμενο $c = Enc(m)$, υπάρχουν συναρτήσεις f, g τέτοιες ώστε $f(c) = Enc(g(m))$ όπου η g είναι εύκολα αντιστρέψιμη.

Αν ένα κρυπτοσύστημα είναι malleable, δεν μπορεί να είναι ασφαλές κατά IND-CCA2

Γιατί;

Τα malleable κρυπτοσυστήματα όμως έχουν πολλές χρήσιμες εφαρμογές γιατί επιτρέπουν πράξεις στα κρυπτοκείμενα που μεταφράζονται σε πράξεις στα μηνύματα (χρήσιμο στις ηλεκτρονικές ψηφοφορίες κ.α.)

Πλήρως ομομορφική κρυπτογραφία (Gentry 2010): Επιτρέπονται οποιεσδήποτε πράξεις μεταξύ κρυπτοκειμένων.

Αποδείξεις Ασφάλειας

Κρυπτογραφικές αναγωγές

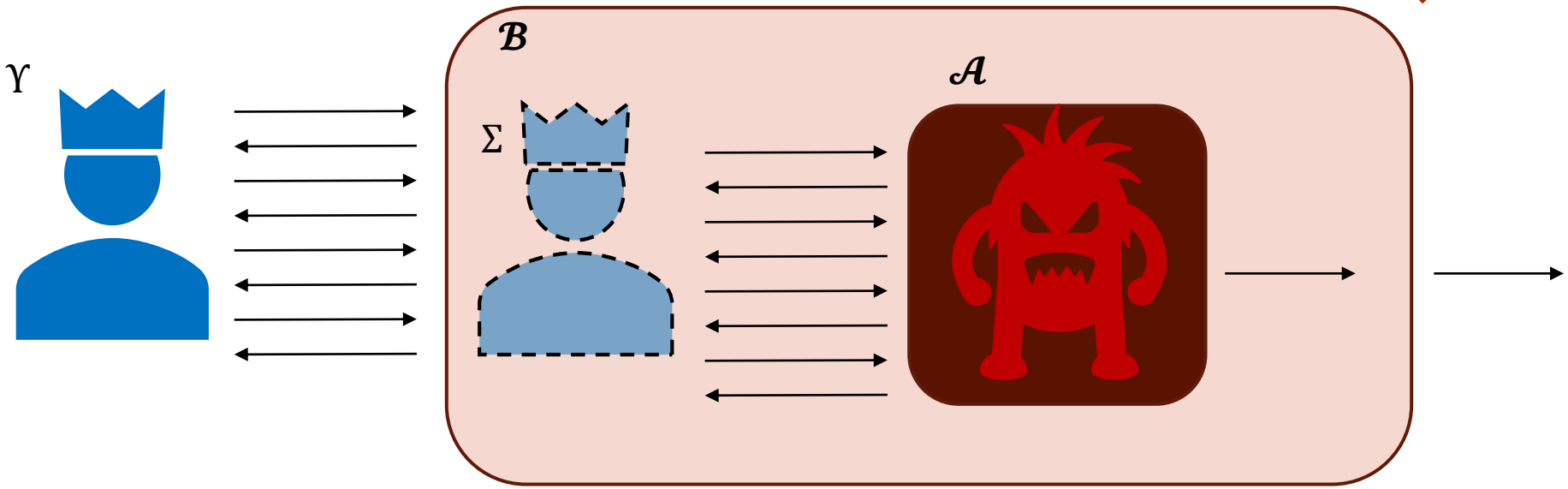
- Η ασφάλεια ενός πρωτοκόλλου ανάγεται στη δυσκολία ενός δύσκολου προβλήματος.
- **Αν ισχύει η υπόθεση Υ, τότε το σύστημα Σ είναι ασφαλές.**
- Ισοδύναμα (αντιθετοαντιστροφή):
- **Αν το σύστημα Σ ΔΕΝ είναι ασφαλές, τότε ΔΕΝ ισχύει η υπόθεση Υ.**
- **Παραδείγματα Υ:**
  - Δυσκολία Παραγοντοποίησης,
  - Δυσκολία Εύρεσης Διακριτού Λογαρίθμου, …

Κρυπτογραφικές αναγωγές

- Κατασκευαστική απόδειξη:
- Αφού το Σ δεν είναι ασφαλές, τότε υπάρχει ένας αντίπαλος $\mathcal{A}$ ο οποίος επιτυγχάνει με μη αμελητέα πιθανότητα στην επίθεση που ορίζεται στο παίγνιο ασφάλειας.
- Χρησιμοποιούμε τον $\mathcal{A}$ ως black-box και με τα μηνύματα που ανταλλάσουμε με αυτόν κατασκευάζουμε αντίπαλο$\mathcal{B}$ που σπάει την υπόθεση Υ στο παίγνιο που την ορίζει.
- **ΆΤΟΠΟ:** γιατί **δεχόμαστε** ότι η υπόθεση είναι δύσκολη.

Κρυπτογραφικές Αναγωγές

Σχηματικά:



Παρατηρήσεις

- Ο $\mathcal{B}$ θα πρέπει να είναι PPT.
  - Δηλαδή η επεξεργασία που κάνει πέρα από την αλληλεπίδρασή με τον A, θα πρέπει να είναι περιορισμένη.
  - Επιθυμητά και **tight**: Δηλαδή ο χρόνος του $\mathcal{B}$ και η πιθανότητα επιτυχίας του (μη αμελητέα) θα πρέπει να είναι **κοντά** στου $\mathcal{A}$
- Η αλληπίδραση του $\mathcal{A}$ με τον challenger της Υ θα πρέπει να είναι μη διακρίσιμη από την αλληλεπίδραση με τον challenger του κρυπτοσυστήματος.
  - Π.χ. τα μηνύματα θα πρέπει είναι από τις ίδιες κατανομές.

Συζήτηση

- Η απόδειξη ασφάλειας παρέχει **σχετικές**

και όχι απόλυτες εγγυήσεις.

  - Ισχύει με την υπόθεση της δυσκολίας του προβλήματος αναγωγής
- Αποτελεί ευκαιρία για καλύτερο ορισμό του πρωτοκόλλου / συστήματος.
  - Σημαντικό για πολύπλοκα συστήματα
- Εντείνει τις κρυπταναλυτικές προσπάθειες στο πρόβλημα της αναγωγής και όχι σε κάθε πρωτόκολλο / σύστημα ξεχωριστά.
- Ρυθμίζει την παράμετρο ασφάλειας
- Είναι τόσο καλή όσο το μοντέλο ασφάλειας (**KRACK Attacks: Breaking WPA2**)
- Δεν αποκλείει πρόβλημα στην υλοποίηση

Ανταλλαγή κλειδιού Diffie - Hellman

New Directions in Cryptography (1976)

DHKE

$\mathbb{G} = \langle g \rangle, q$

$\alpha \xleftarrow{\$} \mathbb{Z}_q$

$b \xleftarrow{\$} \mathbb{Z}_q$

g^a

g^b

$K = g^{ba}$

$K = g^{ab}$

- Ανταλλαγή Κλειδιού Diffie – Hellman (DHKE)
  - Καλύτερα **κατανεμημένη δημιουργία** κλειδιού
- Απαιτεί ομάδα τάξης πρώτου q (Ελλειπτική καμπύλη, υποομάδα $\mathbb{Z}_p^*$)
- Σημαντικό συστατικό πρωτοκόλλων Internet (TLS, SSL, IPSec, Signal)

Ασφάλεια DHKE

Το πρόβλημα του Διακριτού Λογάριθμου (DLP)

- Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, με τάξη q και στοιχείο $y \in \mathbb{G}$.
- Ζητείται $x \in \mathbb{Z}_q$ ώστε $y = g^x$

Το υπολογιστικό πρόβλημα Diffie-Hellman (CDHP)

- Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, με τάξη q και στοιχεία $g^\alpha, g^\beta \in \mathbb{G}$.
- Να υπολογιστεί το στοιχείο $g^{\alpha\beta}$

Το πρόβλημα απόφασης Diffie-Hellman (DDHP)

- Δίνεται μια κυκλική ομάδα $\mathbb{G} = \langle g \rangle$, με τάξη q και στοιχεία $g^\alpha, g^\beta \in \mathbb{G}$ και στοιχείο $y \in \mathbb{G}$.
- Να αποφασιστεί αν $g^{\alpha\beta} = y$.

- **Υπόθεση DLP**
  - Το DLP είναι δύσκολο.
- **Υπόθεση CDH (CDH Assumption)**
  - Το CDHP είναι δύσκολο.
- **Υπόθεση DDH (DDH Assumption)**
  - Το DDHP είναι δύσκολο.

Σχέσεις προβλημάτων

$$\boldsymbol{DDHP \leq CDHP \leq DLP}$$

$\boldsymbol{DDHP \leq CDHP}$

Αν μπορούμε να λύσουμε το CDHP, τότε μπορούμε να υπολογίσουμε από τα g^{α}, g^{β} το $g^{\alpha\beta}$ και στη συνέχεια να ελέγξουμε αν $y = g^{\alpha\beta}$.

$\boldsymbol{CDHP \leq DLP}$

Αν μπορούμε να λύσουμε το DLP, τότε μπορούμε να υπολογίζουμε τα α, β από τα g^{α}, g^{β} και κατά συνέπεια να υπολογίσουμε το $\alpha\beta$ και στη συνέχεια το $g^{\alpha\beta}$.

$$\boldsymbol{DDHA \Rightarrow CDHA \Rightarrow DLPA}$$

- Δεν γνωρίζουμε αν ισχύει η αντίστροφη σειρά (**ισοδυναμία**).
- Σε συγκεκριμένες ομάδες ισχύει μάλλον ότι $\boldsymbol{DDHP < CDHP}$
  - Εύκολο $\boldsymbol{DDHP}$
  - Μάλλον Δύσκολο $\boldsymbol{CDHP}$ (δηλ. δεν έχει αποδειχθεί εύκολο)

Τριάδες Diffie - Hellman

- $(g^{\alpha}, g^{\beta}, g^{a\beta})$ είναι μια τριάδα Diffie – Hellman
- $(g^{\alpha}, g^{\beta}, g^{\gamma})$ είναι μια τυχαία τριάδα στοιχείων της ομάδας $\mathbb{G}$.

Το πρόβλημα απόφασης Diffie-Hellman (DDHP)

Μπορούμε να ξεχωρίσουμε αποδοτικά σε μια ομάδα $\mathbb{G}$ να ξεχωρίσουμε τριάδες **Diffie – Hellman** από **τυχαίες** τριάδες;

DDHP σε μορφή παιγνίου

Input : security parameter λ
Output: $\{0,1\}$

$(\mathbb{G}, g, q) \leftarrow Gen(1^\lambda)$
$\mathfrak{b} \leftarrow\$ \{0,1\}$
$a, b, c \leftarrow\$ \mathbb{Z}_q$
if $b = 0$ **then**
  $y := g^{ab}$
else
  $y := g^c$
end
$\mathfrak{b}' \leftarrow \mathcal{A}(\textbf{guess}, \mathbb{G}, g, q, g^a, g^b, y)$
if $\mathfrak{b} = \mathfrak{b}'$ **then**
  return 1
else
  return 0
end

- Ο challenger παράγει την ομάδα και διαλέγει ένα τυχαίο bit
- Επίσης διαλέγει ομοιόμορφα 3 δείκτες.
- Αν $b = 0$ τότε θέτει $y = g^{a\beta}$ αλλιώς $y = g^c$
- Ο αντίπαλος λαμβάνει όλα τα στοιχεία και καλείται να μαντέψει το b
- Αν το βρει **σωστά κερδίζει**, αλλιώς **χάνει**.
- Πλεονέκτημα αντιπάλου:
  - $Adv^{\mathcal{A}}_{\mathrm{DDH}}(\lambda) = \left|\Pr\left[\mathcal{A}\left(g, g^\alpha, g^\beta, g^{a\beta}\right) = 1\right] - \Pr\left[\mathcal{A}\left(g, g^\alpha, g^\beta, g^c\right) = 1\right]\right|$
    - Η υπόθεση DDH ισχύει αν $Adv^{\mathcal{A}}_{\mathrm{DDH}}(\lambda) \leq negl(\lambda)$

DHKE σε μορφή παιγνίου

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

Ισοδύναμα

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

- Ο challenger παράγει την ομάδα και διαλέγει ένα τυχαίο bit
- Εκτελεί το πρωτόκολλο DHKE το οποίο παράγει ένα transcript τ και ένα κλειδί K
  - transcript τ: τα δημόσια μηνύματα που ανταλλάσσονται
  - κλειδί K: ιδιωτικό αποτέλεσμα
- Αν $b = 0$ τότε ο $\mathcal{A}$ λαμβάνει (τ, K) με σωστό K αλλιώς $K \leftarrow_{\$} \mathbb{G}$
- Ο αντίπαλος μαντεύει b'. Αν $b = b'$ κερδίζει, αλλιώς χάνει.
- Πλεονέκτημα αντιπάλου:
  - $Adv^{\mathcal{A}}_{\mathrm{DHKE}}(\lambda) = \left|\Pr[\mathcal{A}(\tau, K) = 1] - \frac{1}{2}\right|$
- Το πρωτόκολλο DHKE είναι ασφαλές αν $Adv^{\mathcal{A}}_{\mathrm{DHKE}}(\lambda) \leq negl(\lambda)$

Απόδειξη Ασφάλειας DHKE

Θεώρημα **Αν ισχύει η DDHA, τότε το πρωτόκολλο DHKE είναι ασφαλές απέναντι σε παθητικό αντίπαλο.**

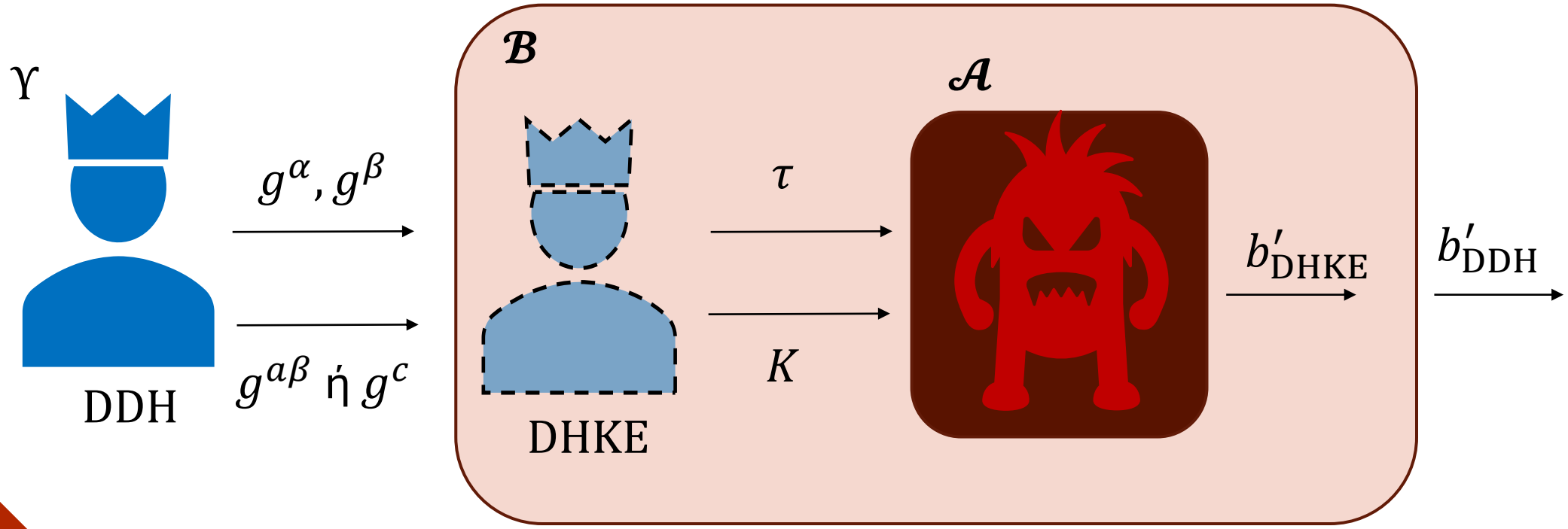
Απόδειξη Έστω ότι DHKE μη ασφαλές. Τότε υπάρχει αντίπαλος $\mathcal{A}$ για τον οποίον

$$Adv^{\mathcal{A}}_{\mathrm{DHKE}}(\lambda) > negl(\lambda)$$

Θα χρησιμοποιήσουμε τον $\mathcal{A}$, ώστε να κατασκευάσουμε αντίπαλο $\mathcal{B}$ ώστε

$$Adv^{\mathcal{B}}_{\mathrm{DDH}}(\lambda) > negl(\lambda)$$

Απόδειξη Ασφάλειας DHKE



Απόδειξη Ασφάλειας DHKE

$$Adv^{\mathcal{A}}_{\mathrm{DHKE}}(\lambda) = \left|\Pr[\mathcal{A}(\tau, K) = 1] - \frac{1}{2}\right| =$$

$$\left|\frac{1}{2}\Pr[\mathcal{A}(\tau, K) = 1 | b = 0] + \frac{1}{2}\Pr[\mathcal{A}(\tau, K) = 1 | b = 1] - \frac{1}{2}\right| =$$

$$\left|\frac{1}{2}\Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{\alpha\beta}) = 0] + \frac{1}{2}\Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{c}) = 1] - \frac{1}{2}\right| =$$

$$\left|\frac{1}{2}\left(1 - \Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{\alpha\beta}) = 1]\right) + \frac{1}{2}\Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{c}) = 1] - \frac{1}{2}\right| =$$

$$\left|\frac{1}{2} - \frac{1}{2}\Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{\alpha\beta}) = 1] + \frac{1}{2}\Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{c}) = 1] - \frac{1}{2}\right| =$$

$$\frac{1}{2}\left|\Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{\alpha\beta}) = 1] - \Pr[\mathcal{B}(g^{\alpha}, g^{\beta}, g^{c}) = 1]\right| = \frac{1}{2} Adv^{\mathcal{B}}_{\mathrm{DDH}}(\lambda)$$

Αν $Adv^{\mathcal{A}}_{\mathrm{DHKE}}(\lambda) > negl(\lambda)$ τότε και $Adv^{\mathcal{B}}_{\mathrm{DDH}}(\lambda) > negl(\lambda)$

ΑΤΟΠΟ

Η σημασία του μοντέλου – Man in the middle attacks

Ο αντίπαλος είναι ενεργός!

$\alpha \xleftarrow{\$} \mathbb{Z}_q \qquad g^a$

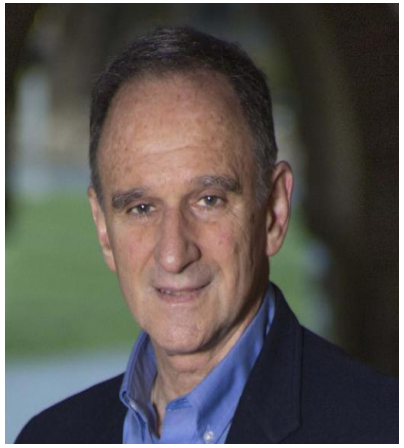
$g^{b'}, b' \xleftarrow{\$} \mathbb{Z}_q$

$K_1 = g^{b'a}$

$g^b \qquad b \xleftarrow{\$} \mathbb{Z}_q$

$g^{a'}, a' \xleftarrow{\$} \mathbb{Z}_q$

$K_2 = g^{a'b}$



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

Πραγματικές επιθέσεις

- **Man-in-the-Middle Attacks on Lenovo Computers - Schneier on Security**
  - Προεγκατεστημένο λογισμικό Visual Discovery: προσπάθεια για εμφάνιση διαφημίσεων όχι με βάση κείμενο αλλά με βάση εικόνες
  - Παρακολούθηση δικτυακής κίνησης και μέσω https
  - Λογισμικό proxy που λειτουργεί ως MiTM Εγκατάσταση (self signed) ψηφιακού πιστοποιητικού
- **Dell apologizes for HTTPS certificate fiasco, provides removal tool - Ars Technica**