

Αποδείξιμη Ασφάλεια Ανταλλαγή κλειδιού Diffie - Hellman

Παναγιώτης Γροντάς
ΕΜΠ
Κρυπτογραφία
2026 - 2027



Περιεχόμενα

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

Η έννοια της ασφάλειας – είδη
επιθέσεων

Σύγχρονη Κρυπτογραφία

- **Ορισμοί**

- Τυπικός (μαθηματικός) ορισμός του τι σημαίνει η ασφάλεια

- **Κατασκευές**

- Εργαλεία, Πρωτόκολλα που ελπίζουμε να ικανοποιούν τον ορισμό

- **Αποδείξεις**

- Τα (πολύπλοκα) σχήματα ικανοποιούν τον ορισμό
- Συσχέτιση με (αναγωγή σε) απλούστερα προβλήματα

Η έννοια της ασφάλειας

- 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 - $\exists$



Τυπικός 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

- $KGen(1^\lambda) \rightarrow (ek, dk) \in K^2$
- 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

Κρυπτογράφηση - Αποκρυπτογράφηση

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

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 κατηγορημα 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 $Enc("Midway") = "AF"$
 - 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: Ό,τι μπορεί να αποκαλυφθεί με το ciphertext μπορεί να αποκαλυφθεί και χωρίς αυτό.
- Λαμβάνουμε υπ' όψιν:
 - την υπολογιστική ισχύ του $\mathcal{A}$
 - την πιθανότητα επιτυχίας

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 $2^{59}sec$

Πρακτικά η ρητή προσέγγιση δεν χρησιμοποιείται:

- Δεν λαμβάνει υπ' όψιν 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 κατηγορημα για το μήνυμα: $Q: M \rightarrow \{0,1\}$

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

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

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

Πολλαπλασιάζουμε με 2 ώστε: $Adv_{\mathcal{A},Q}(\lambda) \in [0,1]$

- Αν $\mathcal{A}$ μαντέψει στην τύχη: $Adv_{\mathcal{A},Q}(\lambda) = 0$
- Αν $\mathcal{A}$ είναι παντοδύναμος / πανάσχετος: $Adv_{\mathcal{A},Q}(\lambda) = 1 = 2 \cdot (1 - \frac{1}{2})$ ή $Adv_{\mathcal{A},Q}(\lambda) = 1 = 2 \cdot (0 - \frac{1}{2})$ και όχι $\frac{1}{2}$

Εναλλακτικά:

$$Adv_{\mathcal{A},Q}(\lambda) \leq \frac{1}{2} + \Pr[\mathcal{A}(c) = Q(Dec_k(c))]$$

Σημασιολογική Ασφάλεια

Ένα κρυπτοσύστημα είναι **σημασιολογικά ασφαλές** αν για κάθε PPT αντίπαλο και για κάθε κατηγορία: $Adv_{\mathcal{A},Q}(\lambda) = negl(\lambda)$

Δύσχρηστος ορισμός:

- Δεν περιγράφει την επίθεση – αντίπαλο
- Δεν ορίζει το κατηγορία
- Αλλά ενσωματώνει την παράμετρο ασφάλειας

Αμελητέα Συνάρτηση

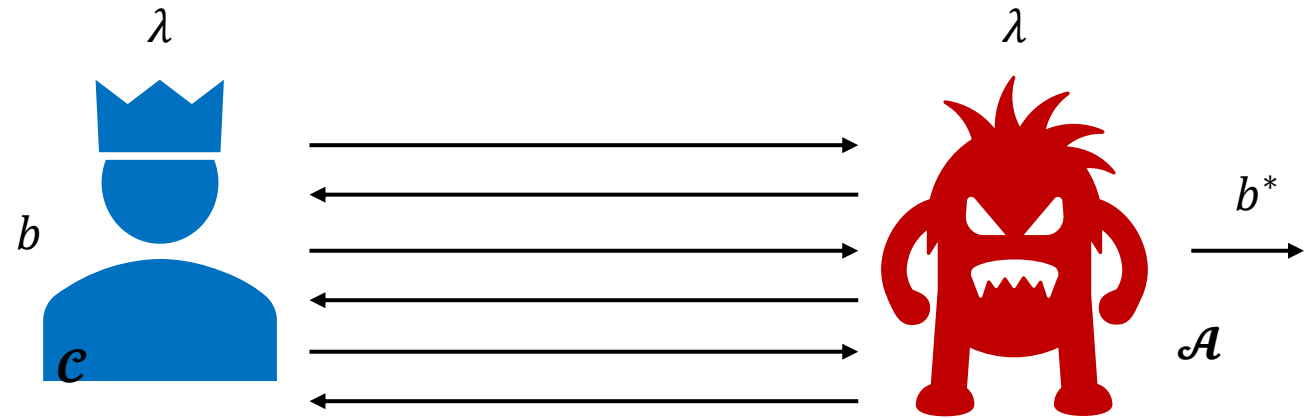
- Μεγαλώνει πιο αργά από αντίστροφο πολυώνυμο
- Παραδείγματα: 2^{-n} , $2^{-\sqrt{n}}$

Μια συνάρτηση f είναι αμελητέα αν για κάθε πολύωνυμο p υπάρχει n_0 :

$$\forall n > n_0: f(n) < \frac{1}{p(n)}$$

Μη-διακρισιμότητα (Indistinguishability)

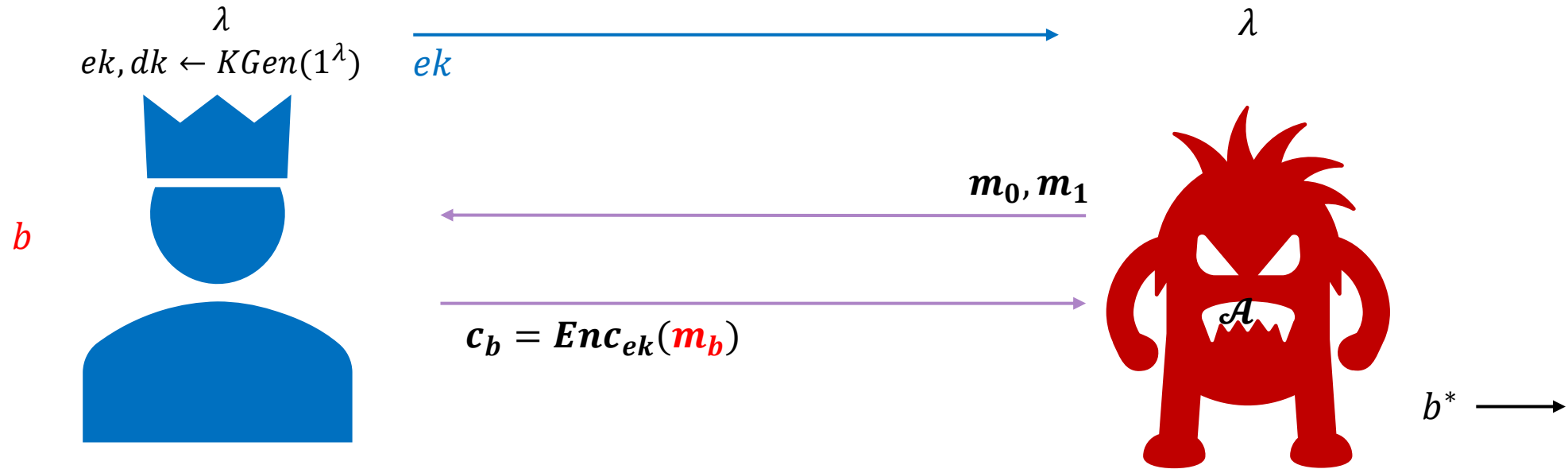
- Ορίζουμε την ασφάλεια μέσω ενός παιχνιδιού μεταξύ του **υπερασπιστή** (challenger) του κρυπτοσυστήματος $\mathcal{C}$ και του αντιπάλου $\mathcal{A}$
- Οι $\mathcal{C}$, $\mathcal{A}$ ανταλλάσσουν μηνύματα
- Κάποια στιγμή ο $\mathcal{C}$ θα κάνει μια τυχαία επιλογή $b \leftarrow \{0,1\}$
- Ο $\mathcal{A}$ 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 $\Leftrightarrow$
Μη-διακρισιμότητα

IND-CoA (Ciphertext only Attack)

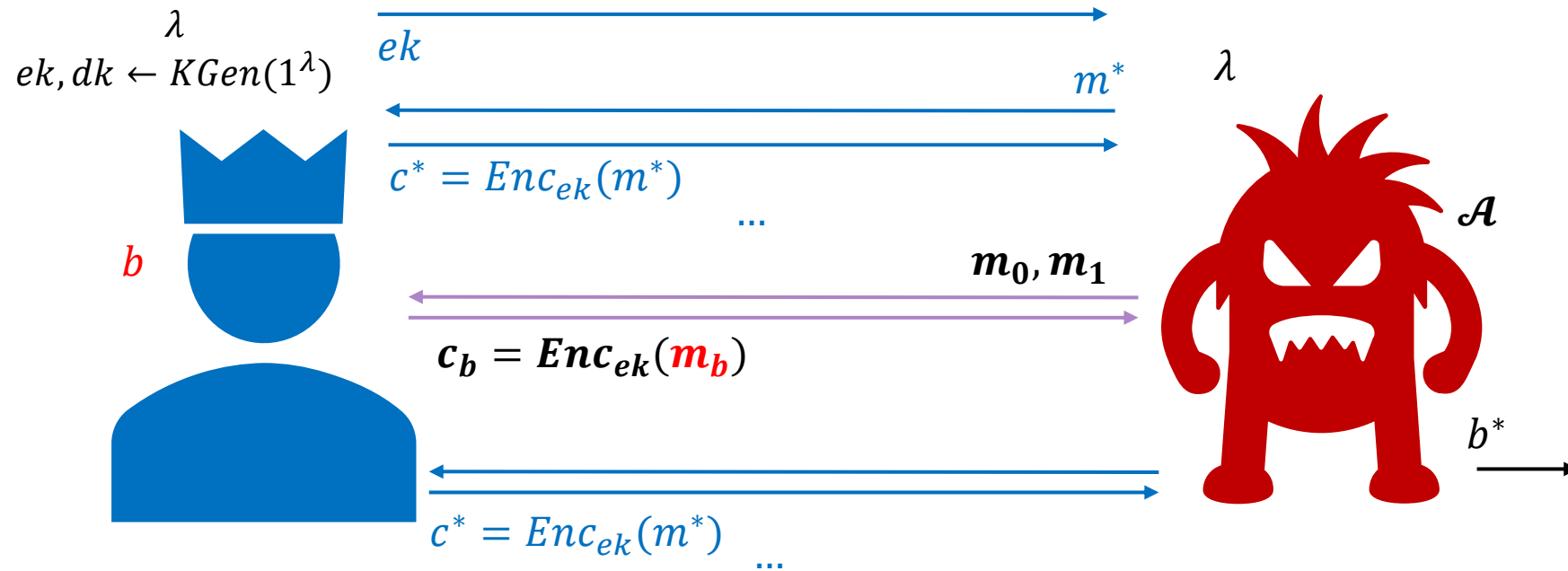


$$Adv_{\mathcal{A}, IND-CoA}(\lambda) \leq \frac{1}{2} + \Pr[IND-CoA(\lambda) = 1]$$

Αν $b = b'$ το παίγνιο επιστρέφει **1** (νίκη) αλλιώς **0** (ήττα)

$$\Pr[IND-CoA(\lambda) = 1] \triangleq \Pr[\mathcal{A} \text{ wins in IND-CoA}]$$

IND-CPA



$$Adv_{\mathcal{A}, \text{IND-CPA}}(\lambda) \leq \frac{1}{2} + \Pr[\text{IND-CPA}(\lambda) = 1]$$

IND-CPA

Χρήση Encryption Oracle

Game $\text{CPA}_{\text{PKE}}^{A,b}(\lambda)$	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 : $b' \leftarrow A^{\text{Enc}}(\text{ek})$	2 : return c
3 : return $(b = b')$	

IND-CPA και ντετερμινιστική κρυπτογράφηση

Θεώρημα

Ένα κρυπτοσύστημα που διαθέτει ντετερμινιστικό αλγόριθμο κρυπτογράφησης, δεν μπορεί να είναι ικανοποιεί την ιδιότητα IND-CPA.

Απόδειξη

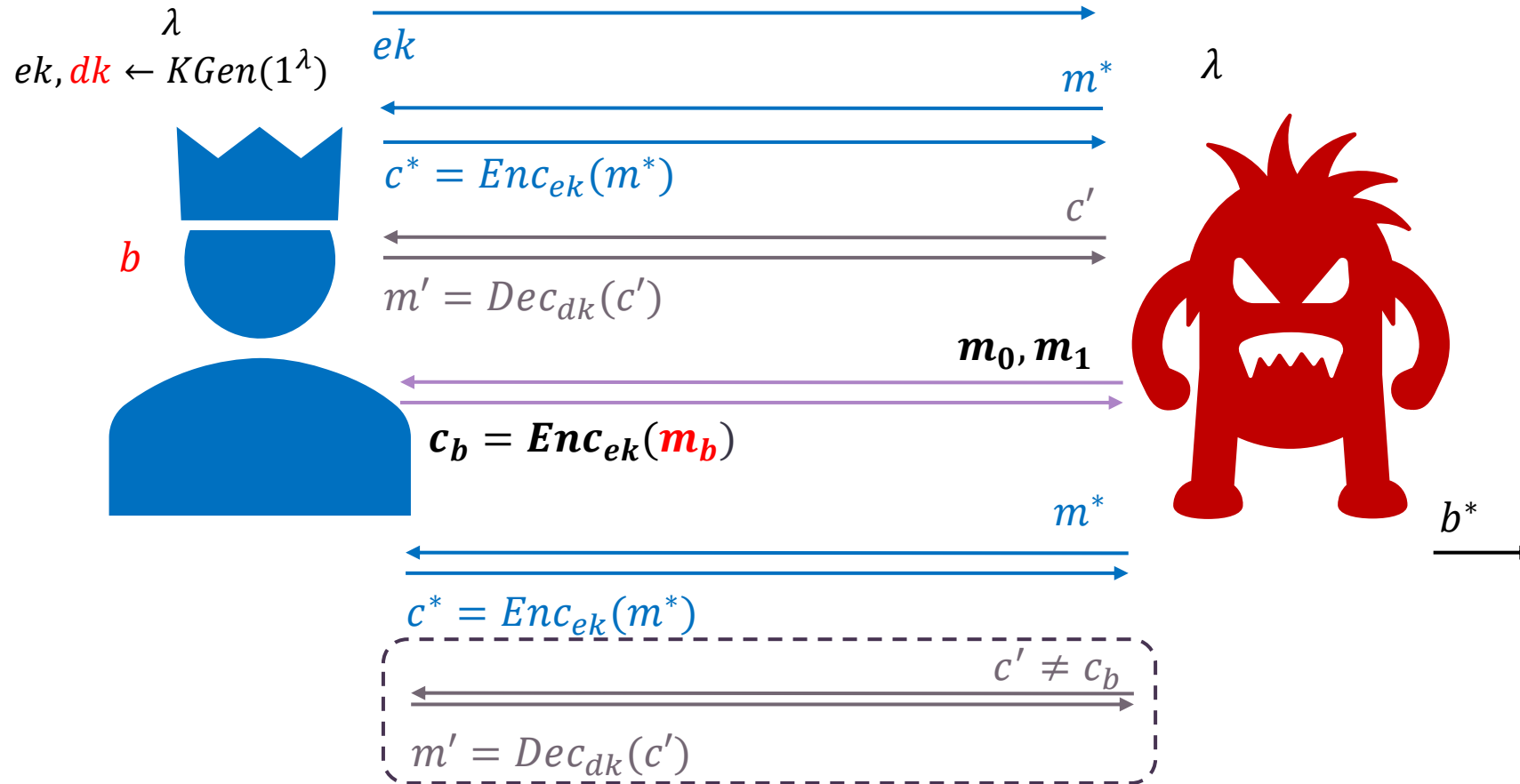
Ο αντίπαλος επιλέγει $m^* = m_0$. Λαμβάνει κρυπτογράφηση c^* .

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



Παραλλαγές IND-CCA

- IND-CCA1

- Ο $\mathcal{A}$ **δεν μπορεί** να χρησιμοποιήσει το decryption oracle αφού έχει λάβει το c_b
- Προσωρινή δυνατότητα αποκρυπτογράφησης
- Διαρρέει η αποκρυπτογράφηση **κάτι** για το κρυπτοσύστημα/κλειδί;

- 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;

Όμως:

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

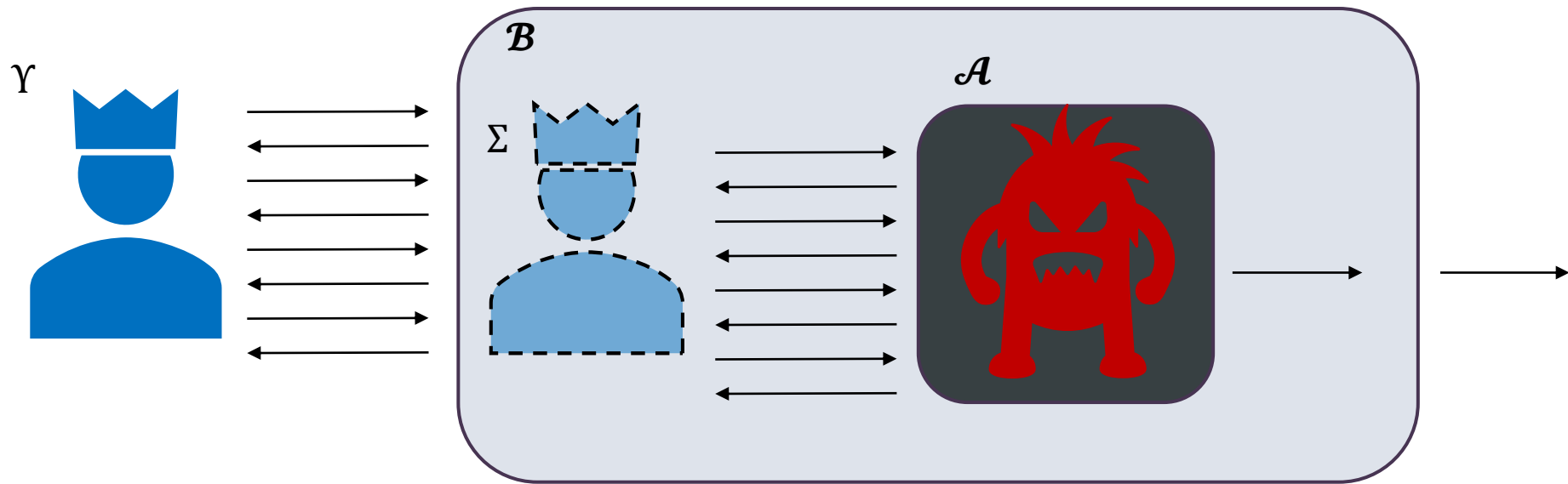
- Η ασφάλεια ενός πρωτοκόλλου ανάγεται στη δυσκολία ενός δύσκολου προβλήματος.
- **Αν ισχύει η υπόθεση $Υ$, τότε το σύστημα Σ είναι ασφαλές.**
- Ισοδύναμα (αντιθετοαντιστροφή):
- **Αν το σύστημα Σ ΔΕΝ είναι ασφαλές, τότε ΔΕΝ ισχύει η υπόθεση $Υ$.**
- Παραδείγματα $Υ$:
 - Δυσκολία Παραγοντοποίησης,
 -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

Κρυπτογραφικές αναγωγές

- **Διαδικασία απόδειξης:**
- 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 ανταλλάσσουμε 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:



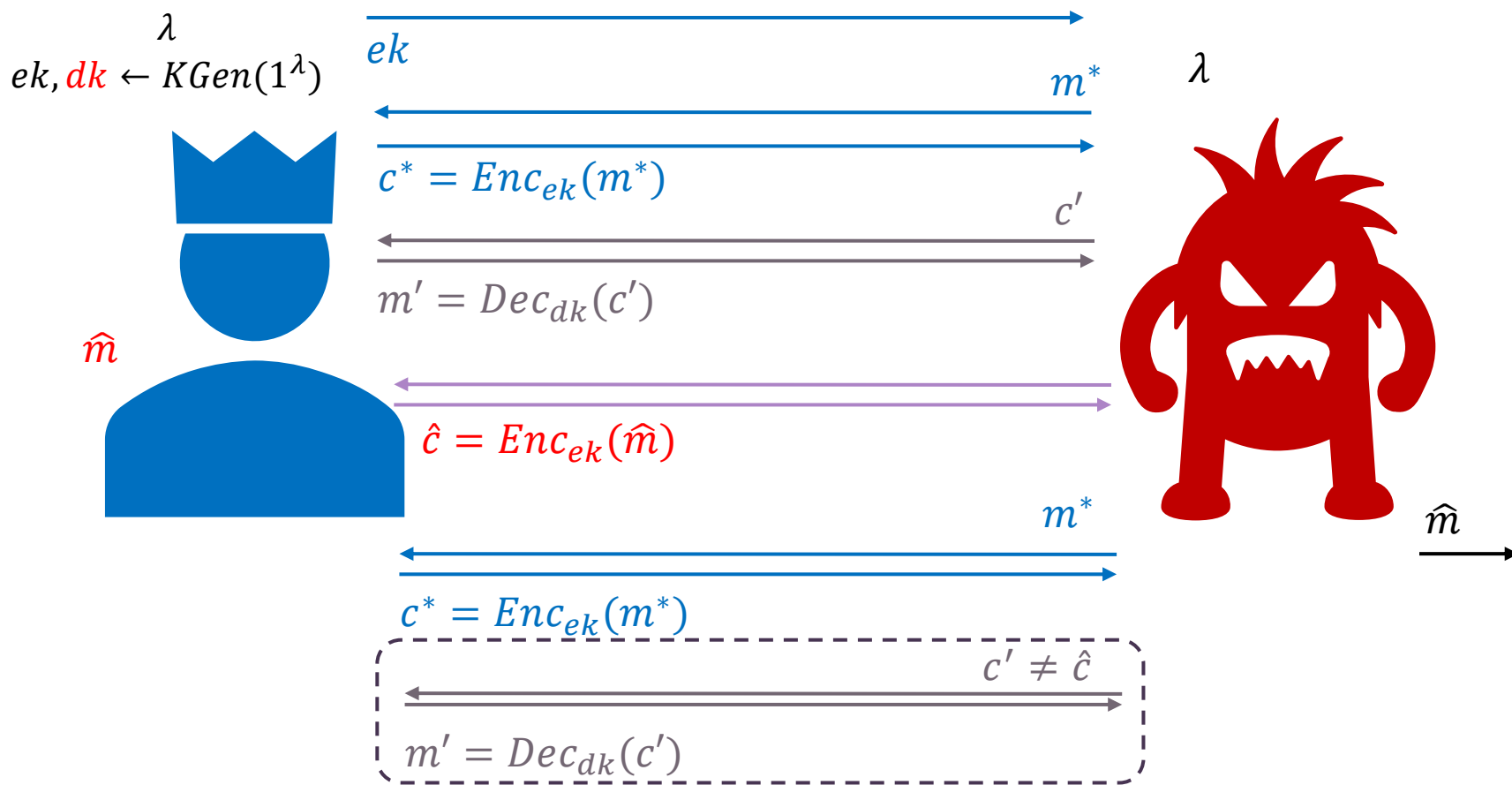
Παρατηρήσεις

- Ο $\mathcal{B}$ θα πρέπει να είναι PPT.
 - Δηλαδή η επεξεργασία που κάνει πέρα από την αλληλεπίδρασή με τον $\mathcal{A}$, 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 αλληλεπίδραση του $\mathcal{A}$ με τον challenger της $\mathcal{Y}$ 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
- Συγκεντρώνει τις κρυπταναλυτικές προσπάθειες **στο πρόβλημα της αναγωγής** και όχι σε κάθε πρωτόκολλο / σύστημα ξεχωριστά.
- Ρυθμίζει την **παράμετρο ασφάλειας**
- Είναι τόσο χρήσιμη όσο το μοντέλο ασφάλειας ([KRACK Attacks: Breaking WPA2](#))
- Δεν αποκλείει πρόβλημα στην υλοποίηση

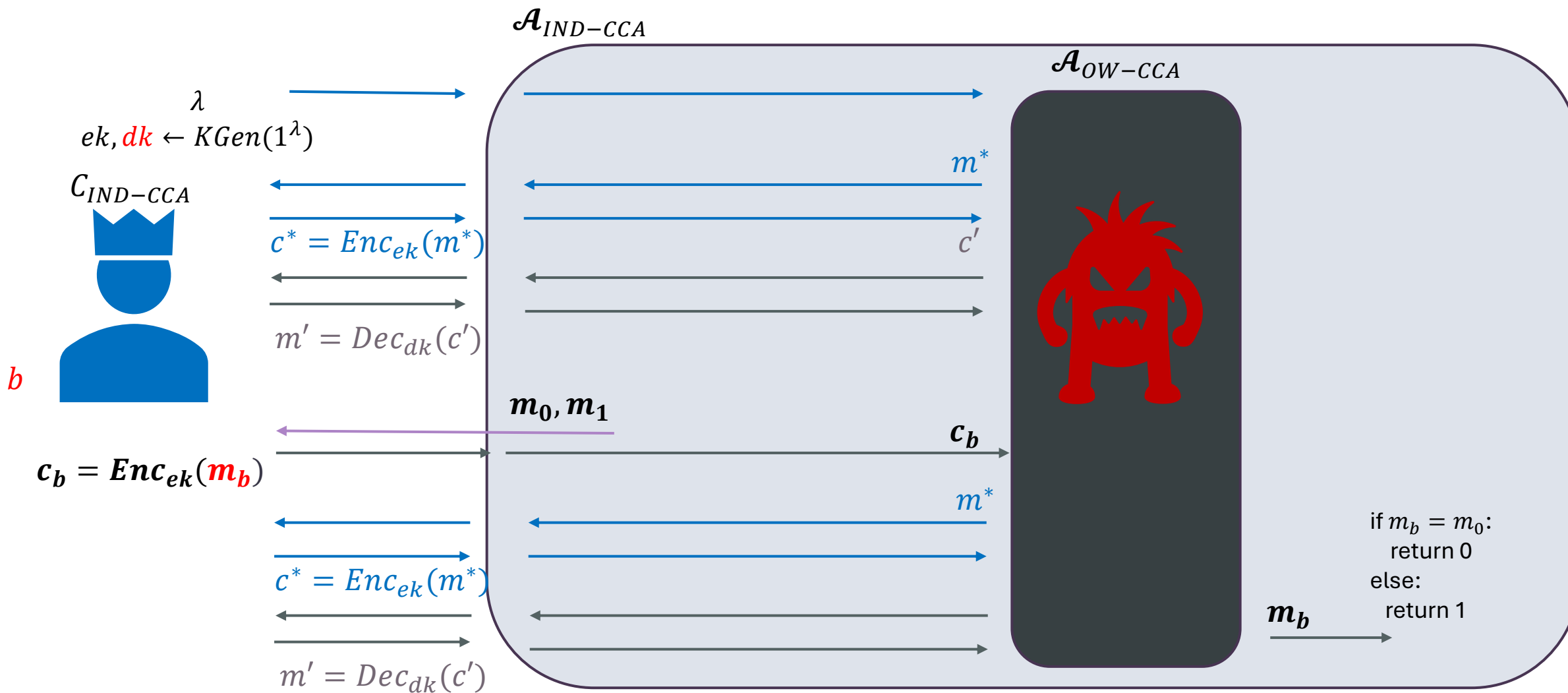
Παράδειγμα: IND-CCA $\Rightarrow$ OW-CCA



OW-CCA: One Way CCA

Αντί να μαντέψει ένα κατηγορημα για το μήνυμα, πρέπει να μαντέψει ολόκληρο το μήνυμα. Θδο: **ασφάλεια IND-CCA ισχυρότερη ασφάλειας OW-CCA.**

Παράδειγμα: IND-CCA $\Rightarrow$ OW-CCA



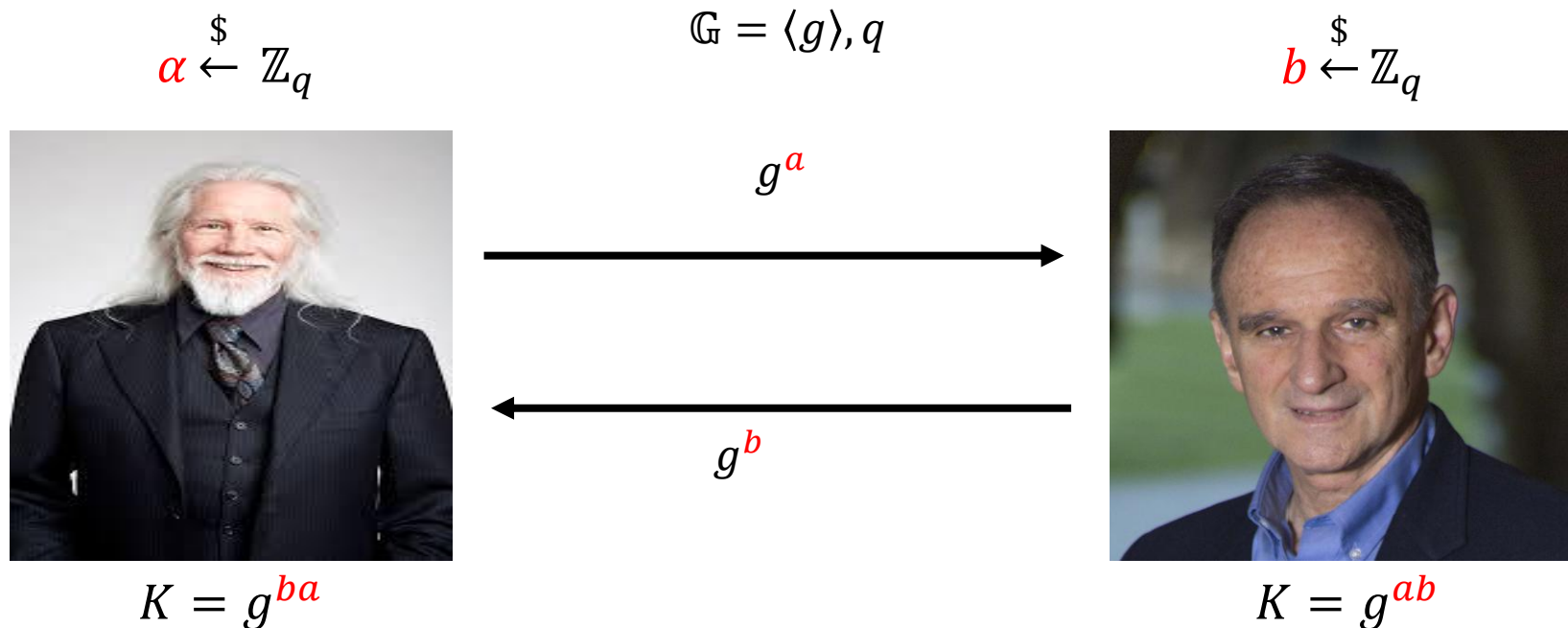
Εξάσκηση

- $OW-CCA \Rightarrow OW-CPA \Rightarrow OW-CoA$
- $IND-CCA \Rightarrow IND-CPA \Rightarrow IND-CoA$
- $IND-CPA \Rightarrow OW-CPA$
- $IND-CoA \Rightarrow OW-CoA$

Ανταλλαγή κλειδιού Diffie - Hellman

New Directions in Cryptography (1976)

- 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

$$DDHP \leq CDHP \leq DLP$$

$$CDHP \leq DLP$$

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

$$DDHP \leq CDHP$$

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 $y = g^{\alpha\beta}$.

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

$$DDHA \Rightarrow CDHA \Rightarrow DLPA$$

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 **ομοιόμορφα επιλεγμένες** τριάδες;

DDHP σε μορφή παιχνιδιού

- Ο challenger παράγει την ομάδα και διαλέγει ένα τυχαίο bit
- Επίσης διαλέγει ομοιόμορφα 3 δείκτες.
- Αν $b = 0$ τότε θέτει $y = g^{ab}$ 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:
 - $Adv_{\text{DDH}}^{\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(g, g^a, g^b, g^{ab}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c) = 1]|$
 - Η υπόθεση DDH ισχύει αν $Adv_{\text{DDH}}^{\mathcal{A}}(\lambda) \leq \text{negl}(\lambda)$

```
Input  : security parameter  $\lambda$   
Output:  $\{0, 1\}$   
 $(G, g, q) \leftarrow \text{Gen}(1^\lambda)$   
 $b \leftarrow \{0, 1\}$   
 $a, b, c \leftarrow \mathbb{Z}_q$   
if  $b = 0$  then  
   $y := g^{ab}$   
else  
   $y := g^c$   
end  
 $b' \leftarrow \mathcal{A}(\text{guess}, G, g, q, g^a, g^b, y)$   
if  $b = b'$  then  
  return 1  
else  
  return 0  
end
```

DHKE σε μορφή παιγνίου $KE_{\mathcal{A}, DHKE}$

- 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 (αποτέλεσμα παιγνίου **1**), αλλιώς χάνει (αποτέλεσμα παιγνίου 0).
- Πλεονέκτημα αντιπάλου:
 - $Adv_{DHKE}^{\mathcal{A}}(\lambda) = \left| \Pr[KE_{\mathcal{A}, DHKE}(\tau, K) = 1] - \frac{1}{2} \right|$
- Το πρωτόκολλο DHKE είναι ασφαλές αν $Adv_{DHKE}^{\mathcal{A}}(\lambda) \leq negl(\lambda)$

$\mathcal{A}$ wins $KE(\tau, K)$

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.

Απόδειξη Ασφάλειας DHKE

Θεώρημα

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

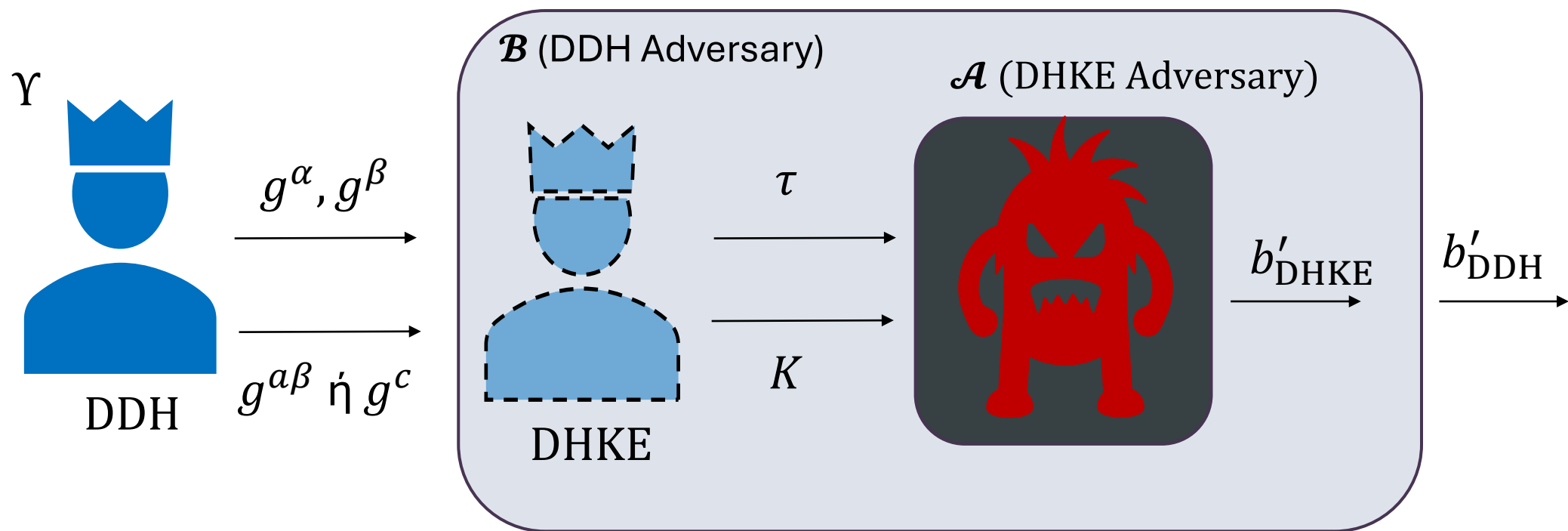
Απόδειξη Έστω ότι DHKE μη ασφαλές. Τότε υπάρχει αντίπαλος $\mathcal{A}$ για τον οποίον

$$Adv_{\text{DHKE}}^{\mathcal{A}}(\lambda) > \text{negl}(\lambda)$$

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

$$Adv_{\text{DDH}}^{\mathcal{B}}(\lambda) > \text{negl}(\lambda)$$

Απόδειξη Ασφάλειας DHKE



Απόδειξη Ασφάλειας DHKE

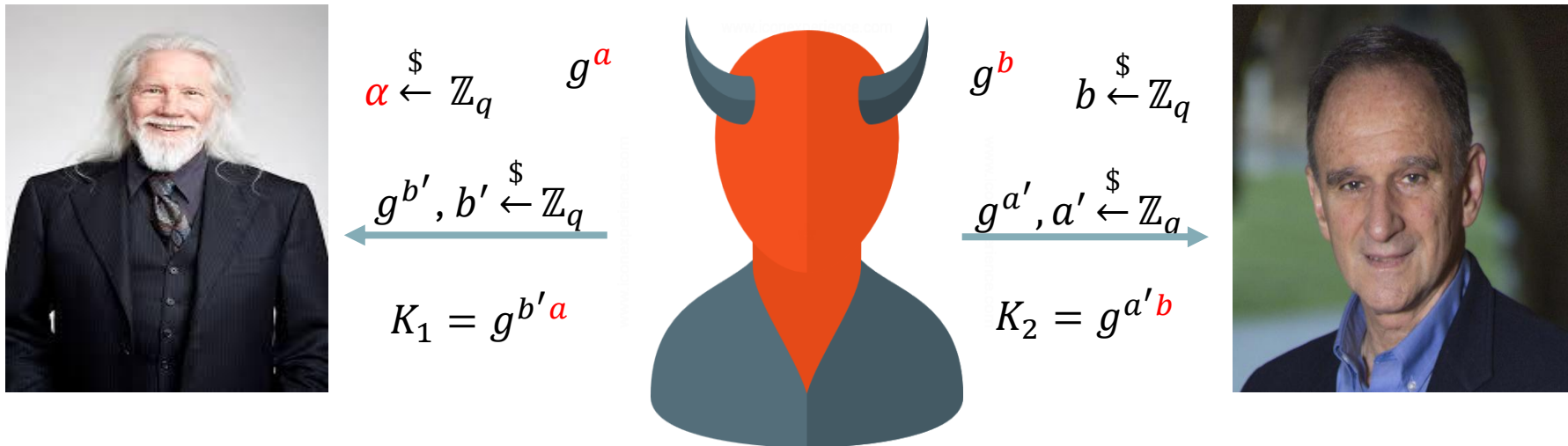
$$\begin{aligned} Adv_{\text{DHKE}}^{\mathcal{A}}(\lambda) &= \left| \Pr[\mathcal{A} \text{ wins } KE(\tau, K)] - \frac{1}{2} \right| = \\ &= \left| \left(\frac{1}{2} \Pr[\mathcal{A} \text{ wins } KE(\tau, K) | b = 0] + \frac{1}{2} \Pr[\mathcal{A} \text{ wins } KE(\tau, K) | b = 1] \right) - \frac{1}{2} \right| = \\ &= \left| \frac{1}{2} \Pr[\mathcal{A}((g^\alpha, g^\beta), g^{a\beta}) = 0] + \frac{1}{2} \Pr[\mathcal{A}((g^\alpha, g^\beta), g^c) = 1] - \frac{1}{2} \right| = \\ &= \left| \frac{1}{2} (1 - \Pr[\mathcal{A}((g^\alpha, g^\beta), g^{a\beta}) = 1]) + \frac{1}{2} \Pr[\mathcal{A}((g^\alpha, g^\beta), g^c) = 1] - \frac{1}{2} \right| = \\ &= \left| \frac{1}{2} - \frac{1}{2} \Pr[\mathcal{A}((g^\alpha, g^\beta), g^{a\beta}) = 1] + \frac{1}{2} \Pr[\mathcal{A}((g^\alpha, g^\beta), g^c) = 1] - \frac{1}{2} \right| = \\ &= \frac{1}{2} \left| \Pr[\mathcal{A}(g^\alpha, g^\beta, g^{a\beta}) = 1] - \Pr[\mathcal{A}(g^\alpha, g^\beta, g^c) = 1] \right| \\ &= \frac{1}{2} \left| \Pr[\mathcal{B}(g^\alpha, g^\beta, g^{a\beta}) = 1] - \Pr[\mathcal{B}(g^\alpha, g^\beta, g^c) = 1] \right| = \frac{1}{2} Adv_{\text{DDH}}^{\mathcal{B}}(\lambda) \end{aligned}$$

Αν $Adv_{\text{DHKE}}^{\mathcal{A}}(\lambda) > \text{negl}(\lambda)$ τότε και $Adv_{\text{DDH}}^{\mathcal{B}}(\lambda) > \text{negl}(\lambda)$

ΑΤΟΠΟ

Η σημασία του μοντέλου – Man in the middle attacks

Ο αντίπαλος είναι ενεργός!



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](#)