

# Ψηφιακές Υπογραφές

Μοντέλα Ασφάλειας - Κατασκευές - Επιθέσεις

---

Παναγιώτης Γροντάς

02/03/2023

ΕΜΠ - Advanced Crypto (2022-2023)

# Ψηφιακές Υπογραφές

---

# Ορισμός Ψηφιακής Υπογραφής

Μια τριάδα αλγορίθμων  $DS = (KGen, Sign, Vf)$ :

- Πιθανοτικός αλγόριθμος  $KGen$  που παράγει κλειδιά υπογραφής και επαλήθευσης.

$$(sk, vk) := DS.KGen(1^\lambda)$$

Συνήθως χρησιμοποιείται σε συνδυασμό με αλγόριθμο  $Pgen$  ο οποίος παράγει τις κρυπτογραφικές παραμέτρους που χρησιμοποιούνται. Δηλ:

$$prms = (\mathbb{G}, H) := DS.Pgen(1^\lambda)$$

$$(sk, vk) := DS.KGen(prms)$$

- Αλγόριθμος υπογραφής μηνύματος  $m$  με κλειδί υπογραφής  $sk$ . Μπορεί να είναι πιθανοτικός.

$$\sigma := DS.Sign(sk, m)$$

- Αλγόριθμος επαλήθευσης υπογραφής  $\sigma$  με κλειδί  $vk$  στο μήνυμα  $m$ . Ντετερμινιστικός.

$$DS.Vf(vk, \sigma, m) \in \{0, 1\}$$

- No Message Attack: Ο αντίπαλος  $\mathcal{A}$  διαθέτει μόνο το  $vk$  (EUF-NMA)
- Known Message Attack: Ο αντίπαλος  $\mathcal{A}$  διαθέτει το  $vk$  και ζεύγη μηνυμάτων υπογραφών  $(m_i, \sigma_i)$  που είναι έγκυρες δηλ.

$$\forall i : Vf(vk, \sigma_i, m_i) = 1$$

Παραλλαγές:

- Plain:  $\mathcal{A}$  δεν διαλέγει τα μηνύματα
- Generic:  $\mathcal{A}$  διαλέγει μηνύματα μία φορά πριν δει το  $vk$  (chosen message attack)
- Oriented:  $\mathcal{A}$  διαλέγει μηνύματα μία φορά αφού δει το  $vk$  (chosen message attack)
- Adaptive:  $\mathcal{A}$  διαλέγει μηνύματα αφού δει το  $vk$  (chosen message attack) λαμβάνοντας υπόψιν και προηγούμενα ζεύγη μηνυμάτων υπογραφών

- Πλαστοπροσωπία: Ανάκτηση κλειδιού υπογραφής  $sk$
- Πλαστογράφηση: Δημιουργία έγκυρης υπογραφής χωρίς  $sk$ 
  - Universal: για οποιοδήποτε μήνυμα
  - Existential: για κάποιο μήνυμα (που μπορεί να μην έχει νόημα)

## EUF-CMA

Ασφάλεια: Αδυναμία επιτυχίας επίθεσης **EUF-CMA** για οποιοδήποτε υπολογιστικά περιορισμένο (PPT) αντίπαλο

- $\sigma := \mathcal{SO}(m)$  Εκφράζει το ότι ο  $\mathcal{A}$  μπορεί να αποκτά υπογραφές σε μηνύματα της επιλογής του.  
Υλοποιείται (στο παίγνιο) από τον  $\mathcal{C}$  με χρήση του  $sk$ .
- $h := \mathcal{RO}(m)$  Εκφράζει το ότι το σχήμα υπογραφών εφαρμόζεται σε  $m \in \{0, 1\}^*$ .  
Θεωρητικά υλοποιείται με ομοιόμορφη επιλογή, διατηρώντας τις ιδιότητες της συνάρτησης (ίδιο input - ίδιο output).  
Πρακτικά υλοποιείται με hash function  $H$ .  
Υπόθεση random oracle: Ισχυρότερη υπόθεση από (δηλ. implies) collision resistance, first, second preimage resistance

---

## Algorithm 1: $\text{Forge}_{\mathcal{A}, \Pi}$

---

Input :  $\lambda$

Output:  $\{0, 1\}$

$(\text{sk}, \text{vk}, \text{prms}) := \Pi.\text{KGen}(1^\lambda)$

$(m, \sigma) := \mathcal{A}^{\text{SO}, \mathcal{RO}}(\text{vk})$

if  $\Pi.\text{Vf}(\text{vk}, \sigma, m) = 1$  then

    return 1

else

    return 0

end

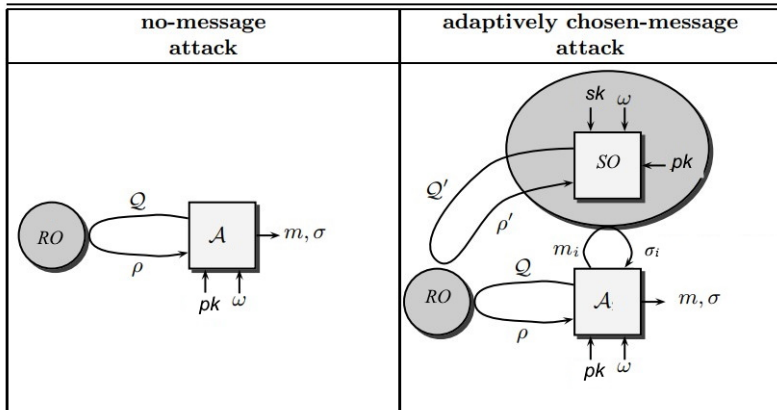
---

### Definition

Ένα σχήμα υπογραφών  $\Pi$  είναι **EUF-CMA unforgeable** αν για κάθε PPT αντίπαλο  $\mathcal{A}$

$$\Pr[\text{Forge}_{\Pi, \mathcal{A}}(1^\lambda) = 1] \leq \text{negl}(\lambda)$$

# Οι επιθέσεις σχηματικά



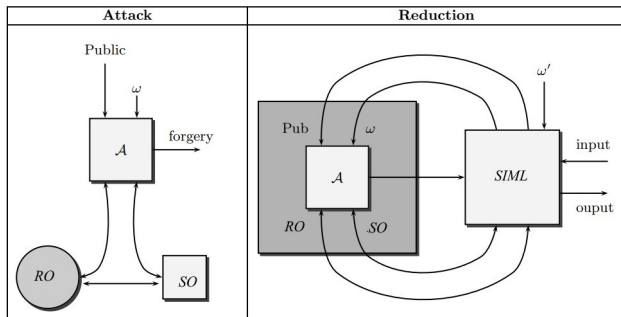


# Αποδείξεις ασφαλείας

Αναγωγή της ασφάλειας σχήματος υπογραφών σε δύσκολο υπολογιστικά πρόβλημα.

Απόδειξη: Αν το σχήμα υπογραφής δεν είναι ασφαλές σύμφωνα με τον τυπικό ορισμό (παίγνιο), τότε χρησιμοποιώντας την πλαστογράφιση μπορώ να λύσω το δύσκολο πρόβλημα.

Γενική μορφή αποδείξεων



# Ψηφιακές Υπογραφές RSA

---

Δημιουργία Κλειδιών:  $\text{KGen}(1^\lambda) = (d, (e, n))$

- $n := p \cdot q$ ,  $p, q$  πρώτοι αριθμοί  $\frac{\lambda}{2}$  bits
- Επιλογή  $e$  ώστε  $\text{gcd}(e, \phi(n)) = 1$
- $d := e^{-1} \pmod{\phi(n)}$  με EGCD
- Χρήση δημόσια διαθέσιμης τυχαίας συνάρτησης  $H : \{0, 1\}^* \rightarrow \mathbb{Z}_n^*$

Πρακτικά:  $\text{FDH}(m) = H(m||0)||H(m||1) \cdots [: \lambda]$  ( $\lambda \text{bits}$ )

ή μπορεί να υποστηρίζεται natively από την  $H$

## Υπογραφή

- Υπολογισμός  $H(m)$
- $\text{Sign}(d, m) \triangleq H(m)^d \bmod n$

## Επαλήθευση

- Υπολογισμός  $H(m)$
- $\text{Vf}((e, n), m, \sigma) \triangleq \sigma^e = H(m) \pmod{n}$

## Ορθότητα

$$\text{Vf}((e, n), m, H(m)^d) \triangleq (H(m)^d)^e = H(m) \pmod{n}$$

Υλοποίηση: συνάρτηση σύνοψης με δυσκολία εύρεσης συγκρούσεων

Πλεονέκτημα: Μπορεί να χρησιμοποιηθεί για υπογραφή τυχαίων συμβολοσειρών και όχι μόνο στοιχείων του  $\mathbb{Z}_n^*$

- Επίθεση χωρίς μήνυμα
  - Επιλογή τυχαίου  $\sigma \in \mathbb{Z}_n^*$
  - Η 'κρυπτογράφηση' δίνει τη σύνοψη  $h = \sigma^e \pmod n$  - όχι το μήνυμα
  - Για το μήνυμα πρέπει να βρεθεί  $m : H(m) = h$
  - Δυσκολία αντιστροφής

- Επίθεση επιλεγμένων μηνυμάτων
  - Ο  $\mathcal{A}$  έχει στη διάθεση του δημόσιο κλειδί  $(e, n)$  και θέλει να πλαστογραφήσει υπογραφή για  $m \in \mathbb{Z}_n^*$
  - Ο  $\mathcal{A}$  χρησιμοποιώντας το μαντρίο αποκτά τις υπογραφές 2 μηνυμάτων  $Q = \{(m_1, \sigma_1), (\frac{m}{m_1}, \sigma_2)\}$  με  $m_1 \in_R$
  - Υπολογισμός  $\sigma = \sigma_1 \sigma_2 = H(m_1)H(\frac{m}{m_1})$
  - Δεν ισχύουν οι ομομορφικές ιδιότητες.

## Θεώρημα

Αν το πρόβλημα RSA είναι δύσκολο, τότε οι υπογραφές RSA-FDH παρέχουν ασφάλεια έναντι υπαρξιακής πλαστογράφησης με επιλεγμένα μηνύματα **EUF-CMA** στο μοντέλο του τυχαίου μαντείου.

Θα αποδείξουμε το παρακάτω:

## Θεώρημα

Αν υπάρχει αντίπαλος  $\mathcal{A}$  που παράγει πλαστογράφηση στο RSA-FDH με πλεονέκτημα τουλάχιστον  $\text{Adv}_{\mathcal{A}}^{\text{forge}}(\lambda)$  μετά από  $Q_{\mathcal{RO}}$  ερωτήσεις στο τυχαίο μαντείο, τότε υπάρχει αντίπαλος  $\mathcal{B}$  που λύνει το πρόβλημα RSA με πιθανότητα  $\text{Adv}_{\mathcal{B}}^{\text{rsa}}(\lambda) \geq \frac{\text{Adv}_{\mathcal{A}}^{\text{forge}}(\lambda)}{Q_{\mathcal{RO}}}$ .

# Απόδειξη Ασφάλειας Hashed RSA: Κατασκευή $\mathcal{B}$

- Ο  $\mathcal{A}$  μπορεί να κατασκευάσει πλαστογράφηση υπογραφής
- Κατασκευή  $\mathcal{B}$  που με χρήση του  $\mathcal{A}$  και ενός τυχαίου μαντείου μπορεί να αντιστρέψει το RSA
- Είσοδος  $\mathcal{B}$ 
  - Δημόσιο κλειδί  $(e, n)$
  - Ομοιόμορφα επιλεγμένο  $y \in \mathbb{Z}_n^*$
- Έξοδος  $\mathcal{B}$ 
  - $x = y^{e^{-1}}$



# Απόδειξη Ασφάλειας Hashed RSA

## Επίθεση χωρίς μήνυμα $i$

### Υπόθεση

Για την πλαστογράφηση  $(m^*, \sigma^*)$  έχει προηγουμένως ερωτηθεί στο μαντείο το  $H(m^*)$

### Συνέπεια

Εφόσον η πλαστογράφηση είναι έγκυρη υπογραφή πρέπει  $\sigma^{*e} = H(m^*)$  Άρα  $\sigma^* = H(m^*)^{e^{-1}}$

### Πλήθος ερωτήσεων

Ο  $\mathcal{B}$  δεν γνωρίζει ακριβώς το  $Q_{\mathcal{RO}}$ , αλλά δεν έχει σημασία αφού  $\mathcal{A}$  είναι PPT. Άρα  $Q_{\mathcal{RO}} \leq \text{poly}(\lambda)$ .

# Απόδειξη Ασφάλειας Hashed RSA

## Επίθεση χωρίς μήνυμα ii

- Ο  $\mathcal{B}$  προωθεί το  $(e, n)$  στον  $\mathcal{A}$
- Ο  $\mathcal{B}$  επιλέγει  $j \in_R [Q_{\mathcal{RO}}]$
- Ο  $\mathcal{A}$  όταν ρωτάει το μαντείο  $H$  για μηνύματα  $\{m_i\}_{i=1}^{Q_{\mathcal{RO}}}$  λαμβάνει τις απαντήσεις  $\{H(m_i)\}_{i=1}^{Q_{\mathcal{RO}}} \in_r$
- Ο  $\mathcal{B}$  ελπίζει ότι στο ερώτημα  $j$  θα γίνει η πλαστογράφιση
- Αν  $i = j$ , ο  $\mathcal{B}$  αντικαθιστά την απάντηση  $H(m_j^*)$  με το  $y$
- Αν έχει δίκιο, τότε ο  $\mathcal{A}$  εξάγει την πλαστογραφία  $(m_j^*, \sigma^*)$  με πιθανότητα  $p_F$
- Δηλαδή:  $\sigma^{*e} = y \Rightarrow \sigma^* = y^{e^{-1}}$
- Ο  $\mathcal{B}$  προωθεί το  $\sigma^*$  στην έξοδο
- Ο  $\mathcal{B}$  αντέστρεψε το RSA με πιθανότητα επιτυχίας  $\frac{\text{Adv}_{\mathcal{A}}^{\text{forge}}(\lambda)}{Q_{\mathcal{RO}}}$

# Απόδειξη Ασφάλειας Hashed RSA

## Επίθεση επιλεγμένου μηνύματος $i$

### Σενάριο

- $\mathcal{A}$  ζητάει συνόψεις και υπογραφές από τον  $\mathcal{B}$
- Συνόψεις: το τυχαίο μαντείο - προσομοίωση
- Υπογραφές: Πρέπει να τις απαντήσει ο  $\mathcal{B}$
- δηλ. να υπολογίσει το  $H(m)^d$  χωρίς το ιδιωτικό κλειδί...

# Απόδειξη Ασφάλειας Hashed RSA

## Επίθεση επιλεγμένου μηνύματος ii

Λύση

Ερώτηση  $\mathcal{A}^{\mathcal{RO}}(m)$ :

Επιλογή  $\sigma \leftarrow \mathbb{Z}_n^*$ ,

υπολογισμός  $\sigma^e$  και επιστροφή αντί  $H(m)$ ,

Αποθήκευση  $\sigma, \sigma^e, m$  για μετά

Ερώτηση  $\mathcal{A}^{\mathcal{SO}}(m)$ :

Επιστροφή  $\sigma$  από την αντίστοιχη απάντηση για  $H(m)$ .

Τετριμμένη επαλήθευση  $\sigma^e = H(m) = \sigma^e$

# Απόδειξη Ασφάλειας Hashed RSA

## Επίθεση επιλεγμένου μηνύματος iii

- Ο  $\mathcal{B}$  προωθεί το  $(e, n)$  στον  $\mathcal{A}$
- Ο  $\mathcal{B}$  επιλέγει  $j \in_R [Q_{\mathcal{RO}}]$
- Ο  $\mathcal{A}$  κάνει  $Q_{\mathcal{RO}} = O(\text{poly}(\lambda))$  ερωτήσεις στο μαντείο για μηνύματα  $\{m_i\}_{i=1}^{Q_{\mathcal{RO}}}$
- Κάθε ερώτηση του μαντείου  $H$  απαντάται από τον  $\mathcal{B}$  ως εξής:
  - Επιλέγει  $\sigma_i \leftarrow \mathbb{Z}_n^*$
  - Υπολογίζει  $\sigma_i^e = y_i$  και θέτει  $H(m_i) = y_i$
  - Επιστρέφει  $y_i$
  - Αποθηκεύει τις τριάδες  $\mathcal{T} = (y_i, \sigma_i, m_i)$
- Ο  $\mathcal{A}$  ζητάει υπογραφές από το μαντείο υπογραφών
  - Για κάθε σύνοψη  $y_i$  γίνεται αναζήτηση στον  $\mathcal{T}$  για την τριάδα που περιέχει το  $y$  και επιστρέφεται το  $\sigma_i$
  - Οι υπογραφές είναι έγκυρες αφού  $\sigma_i^e = y_i$
- Ο  $\mathcal{B}$  απαντάει το ερώτημα  $j$  στο  $H$  με  $y$

# Απόδειξη Ασφάλειας Hashed RSA

## Επίθεση επιλεγμένου μηνύματος iv

- Για το συγκεκριμένο δεν θα ζητηθεί υπογραφή, αλλά το  $\sigma^*$  θα παραχθεί από τον  $\mathcal{A}$  (πλαστογράφιση)
- Αφού πλαστογράφιση = έγκυρη υπογραφή θα ισχύει  $\sigma^{*e} = y$ , δηλαδή  $\sigma^* = y^{e^{-1}}$
- Άρα ο  $\mathcal{B}$  πέτυχε το στόχο του και αντέστρεψε το  $y$
- Πλεονέκτημα  $\mathcal{A}$   $\text{Adv}_{\mathcal{A}}^{\text{forge}}(\lambda)$  και πλεονέκτημα  $\mathcal{B}$

$$\text{Adv}_{\mathcal{B}}^{\text{rsa}}(\lambda) \geq \frac{\text{Adv}_{\mathcal{A}}^{\text{forge}}(\lambda)}{Q_{\mathcal{RO}}}$$

# Απόδειξη Ασφάλειας Hashed RSA

## Επίθεση επιλεγμένου μηνύματος $v$

Ασυμπτωτικά,  $\text{Adv}_B^{\text{rsa}}(\lambda) \leq \text{negl}(\lambda)$  και αφού  $Q_{\mathcal{RO}} \leq \text{poly}(\lambda)$  τότε και  $\text{Adv}_A^{\text{forge}}(\lambda) \leq \text{Adv}_B^{\text{rsa}}(\lambda) \cdot Q_{\mathcal{RO}} \leq \text{negl}(\lambda)$ .

### Παρατήρηση

Πρακτικά υπάρχει 'απώλεια' ασφάλειας  $Q_{\mathcal{RO}}$ .

Π.χ.: Αν  $\text{Adv}_B^{\text{rsa}}(\lambda) = 2^{-60}$  και  $Q_{\mathcal{RO}} = 2^{50}$  τότε  $\text{Adv}_A^{\text{forge}}(\lambda) = 2^{-10}$ .

## Πρωτόκολλα Ταυτοποίησης

---



## Το πρόβλημα της ταυτοποίησης

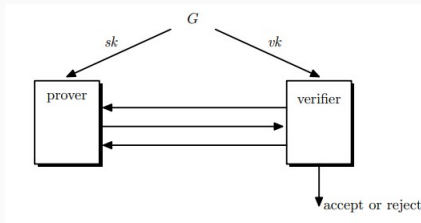
Μια οντότητα (P) θέλει να αποδείξει σε κάποια άλλη (V) ότι είναι αυτή που ισχυρίζεται ώστε να αποκτήσει δικαιώματα πρόσβασης σε κάποιους πόρους.

- Φυσική πρόσβαση σε αντικείμενο
- Πρόσβαση σε τοπικό υπολογιστή
- Πρόσβαση σε απομακρυσμένο υπολογιστή

## Ορισμός ii

Ένα πρωτόκολλο ταυτοποίησης είναι μια τριάδα  $ID = (KGen, P, V)$ :

- $(vk, sk) = KGen(1^\lambda)$
- $\langle P(sk, vk), V(vk) \rangle$  είναι ένα πρωτόκολλο μεταξύ των αλγορίθμων  $P, V$  τέτοιο ώστε μετά την εκτέλεσή του  $V(vk) \in \{0, 1\}$



**Πληρότητα:** Αν ο  $P$  εκτελεστεί με είσοδο το  $sk$  του  
 $(sk, vk) \leftarrow KGen(1^\lambda)$  τότε  $V(vk) = 1$

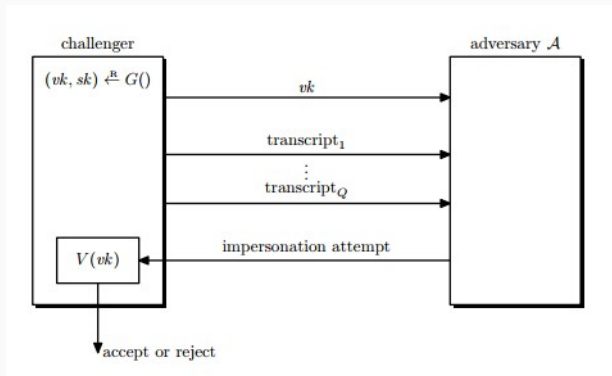
- **Direct (Impersonation) Attacks:** Ο  $\mathcal{A}$  αλληλεπιδρά με τον  $V$  χωρίς το  $sk$ , δηλ.
  - Τοπική πρόσβαση στον verifier
  - Δεν υπάρχει δυνατότητα eavesdropping
  - Το τελευταίο στάδιο οποιασδήποτε επίθεσης

$$ID_{DA} = \langle \mathcal{A}(vk), V(vk) \rangle$$

- **Eavesdropping Attacks:** Ο  $\mathcal{A}$  μπορεί να ζητήσει ένα σύνολο από  $Q$  πραγματικά transcripts  $T = \langle P(sk, vk), V(vk) \rangle_{i=1}^Q$  πριν προβεί σε direct attack.
  - Παρακολούθηση δικτύου

$$ID_{EVE} = \langle \mathcal{A}(T, vk), V(vk) \rangle$$

## Μοντέλο Ασφάλειας ii



- ***r*-Impersonation Attacks:** Ο αντίπαλος έχει δυνατότητα eavesdropping

**Αλλά**, κατά τη διάρκεια του direct attack, ο  $\mathcal{A}$  μπορεί να αλληλεπιδράσει ταυτόχρονα με  $r$  verifiers.

Κερδίζει αν τουλάχιστον ένας από αυτούς δεχθεί.

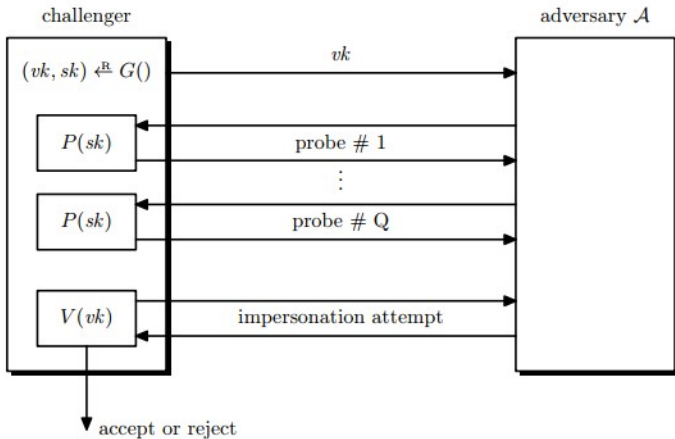
$$ID_{r-EVE} = \langle \mathcal{A}(T, vk), V^r(vk) \rangle$$

- **Active Attacks** Ο  $\mathcal{A}$  αλληλεπιδρά με τον  $P$  στη θέση του verifier χωρίς κατ'ανάγκη να ακολουθεί το πρωτόκολλο, πριν προβεί σε direct attack.

- Χρήση fake verifier
- Phishing attacks

$$ID_{ACT} = \langle P(sk), \mathcal{A}(vk) \rangle$$

# Μοντέλο Ασφάλειας iv



- **Concurrent (Active) Attacks** Ο αντίπαλος μπορεί να δημιουργήσει πολλά ταυτόχρονα sessions με τον prover παριστάνοντας τον verifier και να χρησιμοποιήσει τα μηνυμάτά τους ώστε στη συνέχεια να κάνει direct attack.

Ο  $\mathcal{A}$  αλληλεπιδρά με  $l$  prover - clones.

Κάθε  $P$  clone διαθέτει το ίδιο  $sk$ , αλλά έχει ξεχωριστό random tape και ξεχωριστή κατάσταση.

$$ID_{CC} = \langle P^l(sk), \mathcal{A}(vk) \rangle$$

## Λήμμα

Έστω πρωτόκολλο ταυτοποίησης ID. Για κάθε αντίπαλο  $\mathcal{A}$  στο μοντέλο  $ID_{r-EVE}$  υπάρχει αντίπαλος  $\mathcal{B}$  στο  $ID_{EVE}$  ώστε:

$$\text{Adv}_{\mathcal{B}}^{\text{id}_{eve}}(\lambda) \geq \frac{1}{r} \text{Adv}_{\mathcal{A}, r}^{\text{id}_{r-eve}}(\lambda)$$

## Απόδειξη

Guessing argument

Ο  $\mathcal{B}$  μαντεύει για ποιον ( $j$ ) από τους verifiers του  $ID_{r-EVE}$  κερδίζει ο  $\mathcal{A}$ .

Για αυτόν παίζει το παιχνίδι  $ID_{EVE}$  ως challenger, ενώ προσομοιώνει τους υπόλοιπους.

Κερδίζει αν μάντεψε σωστά, δηλαδή αν ο  $\mathcal{A}$  κάνει επιτυχή direct attack στον  $V_j$ .



## Κατασκευές

---

# Το πρωτόκολλο του Schnorr [?]

- $(q, g, \mathbb{G}) := \text{Pgen}(1^\lambda)$  με  $\mathbb{G} = \langle g \rangle$  ομάδα τάξης  $q$
- $(x, Y) \leftarrow \text{KGen}(\text{prms})$  με  $x \leftarrow \mathbb{Z}_q, Y = g^x$
- $T \leftarrow \text{P}(Y, x)$  με  $t \leftarrow \mathbb{Z}_q, T := g^t$
- $c \leftarrow \text{V}(Y, T)$  με  $c \leftarrow \mathbb{Z}_q$
- $s \leftarrow \text{P}(x, (T, c))$  με  $s = t + cx \bmod q$
- $\text{V}(Y, (T, c, s)) = 1 \Leftrightarrow g^s = TY^c$

Αρχική έκδοση:  $c \in \{0, 1\}^k \subseteq \mathbb{Z}_q$

## Θεώρημα

Αν το DLP είναι δύσκολο στην  $\mathbb{G}$  τότε το πρωτόκολλο ταυτοποίησης του Schnorr παρέχει ασφάλεια σε direct attacks.

$$\text{Adv}_{\mathcal{B}}^{\text{dlp}}(\lambda) \geq \text{Adv}_{\mathcal{A}}^{\text{id}_{\text{da}}}(\lambda)^2 - \frac{\text{Adv}_{\mathcal{A}}^{\text{id}_{\text{da}}}(\lambda)}{q}$$

ή ισοδύναμα:

$$\text{Adv}_{\mathcal{A}}^{\text{id}_{\text{da}}}(\lambda) \leq \frac{1}{q} + \sqrt{\text{Adv}_{\mathcal{B}}^{\text{dlp}}(\lambda)}$$

Για ευκολία θέτουμε:

$$\epsilon = \text{Adv}_{\mathcal{A}}^{\text{id}_{\text{da}}}(\lambda) \text{ και } \epsilon' = \text{Adv}_{\mathcal{B}}^{\text{dlp}}(\lambda)$$

## Tightness

Πλαστοπροσωπία με πιθανότητα  $\epsilon$

Επίλυση διακριτού λογάριθμου με πιθανότητα  $\epsilon^2$

## Βασική ιδέα απόδειξης

Αν ο  $\mathcal{A}$  μπορεί να απαντήσει για  $Y = g^x$  στο  $ID_{DA}$  για ένα challenge  $c_1$  με πιθανότητα  $\epsilon$ , θα μπορεί να απαντήσει για δύο challenges  $c_1, c_2 (c_1 \neq c_2)$  με πιθανότητα  $\epsilon^2$ .

Μετά την πρώτη επιτυχία ο  $\mathcal{B}$  κάνει rewind τον  $\mathcal{A}$  στο σημείο πριν την παραγωγή του challenge.

Δύο accepting transcripts  $(T, c_1, s_1 = t + c_1x)$  και  $(T, c_2, s_2 = t + c_2x)$

Δηλαδή:  $T \cdot Y^{c_1} = g^{s_1}$  και  $T \cdot Y^{c_2} = g^{s_2}$

Άρα:

$$g^{s_1} Y^{-c_1} = g^{s_2} Y^{-c_2} \Rightarrow$$

$$g^{s_1 - s_2} = Y^{c_1 - c_2} \Rightarrow$$

$$s_1 - s_2 = x(c_1 - c_2) \Rightarrow$$

$$x = \frac{s_1 - s_2}{c_1 - c_2}$$

# Rewinding/Splitting/Resetting/Forking Lemma [?, ?]

## Rewinding Lemma

Έστω πεπερασμένα, μη κενά σύνολα  $S, T$  με  $|T| = n$  και  $f : S \times T \rightarrow \{0, 1\}$ .

Έστω τυχαία μεταβλητή  $X$  με τιμές από το  $S$  και τυχαίες μεταβλητές  $Y, Y'$  που παίρνουν τιμές στο  $T$  ομοιόμορφα οι οποίες είναι ανεξάρτητες μεταξύ τους.

Αν  $\Pr[f(X, Y) = 1] = \epsilon$  τότε ισχύει

$$\Pr[f(X, Y) = 1 \wedge f(X, Y') = 1 \wedge Y \neq Y'] \geq \epsilon^2 - \frac{\epsilon}{n}$$

Αντιστοιχία:

$$S = \mathbb{G}$$

$$Y = \mathbb{Z}_q^2 \quad (c, s) = y \in Y$$

και  $f$  είναι η επαλήθευση από τον  $V$

# Απόδειξη Splitting Lemma i

Θεωρούμε  $g(s) = \Pr[f(s, Y) = 1]$  για  $s \in S$ . Ισχύει  $\mathbb{E}[g(X)] = \epsilon$  γιατί:

$$\begin{aligned}\mathbb{E}[g(X)] &= \sum_{s \in S} g(s) \Pr[X = s] = \\ &= \sum_{s \in S} \Pr[f(s, Y) = 1] \Pr[X = s] \\ &= \sum_{s \in S} \Pr[f(s, Y) = 1 \wedge X = s] \quad \text{Ανεξαρτησία} \\ &= \Pr[f(X, Y) = 1] \quad \text{Ολική Πιθανότητα} \\ &= \epsilon\end{aligned}$$

## Απόδειξη Splitting Lemma ii

Έστω το event

$$G_s = f(s, Y) = 1 \wedge f(s, Y') = 1 \wedge Y \neq Y'$$

και

$$n_s = |\{t \in T : f(s, t) = 1\}|$$

Τότε  $g(s) = \frac{n_s}{n}$

$$\Pr[G_s] \geq \frac{n_s}{n} \frac{n_s - 1}{n} = \left(\frac{n_s}{n}\right)^2 - \frac{n_s}{n^2} = g(s)^2 - \frac{g(s)}{n}$$



## Απόδειξη Splitting Lemma iii

Έστω το event  $G : f(X, Y) = 1 \wedge f(X, Y') = 1 \wedge Y \neq Y'$

$$\begin{aligned}\Pr[G] &= \sum_{s \in S} \Pr[G \wedge X = s] \\ &= \sum_{s \in S} \Pr[G_s] \Pr[X = s] \\ &\geq \sum_{s \in S} \left( g(s)^2 - \frac{g(s)}{n} \right) \Pr[X = s] \\ &= \mathbb{E}[g(X)^2] - \frac{\mathbb{E}[g(X)]}{n} \\ &\geq \mathbb{E}[g(X)]^2 - \frac{\mathbb{E}[g(X)]}{n} \quad \text{Jensen's inequality} \\ &= \epsilon^2 - \frac{\epsilon}{n}\end{aligned}$$

## Ασφάλεια σε direct attacks (απόδειξη)

Για  $\mathcal{A}$  που επιτυγχάνει στο  $\text{ID}_{\text{DA}}$  με  $\text{vk} = Y \in \mathbb{G}$ ,  $\text{sk} = x \in \mathbb{Z}_q$  κατασκευάζουμε  $\mathcal{B}$  που λύνει το DLP στην  $\mathbb{G}$  για το  $Y$ .

Ο  $\mathcal{B}$  θα υπολογίσει το  $x$  μέσω δύο αποδεκτών συζητήσεων  $(T, c_1, s_1 = t + c_1x)$  και  $(T, c_2, s_2 = t + c_2x)$  με  $c_1 \neq c_2$ .

Τα  $c_1, c_2$  επιλέγονται τυχαία από τον  $\mathcal{B}$  (που παίζει το ρόλο του  $V$ ).

Από Rewinding Lemma  $\mathcal{B}$  επιτυγχάνει με πλεονέκτημα τουλάχιστον  $\epsilon^2 - \frac{\epsilon}{q}$  αν ο  $\mathcal{A}$  καταφέρει impersonation με πλεονέκτημα  $\epsilon \geq \frac{1}{q}$ .

$$\epsilon' \geq \epsilon^2 - \frac{\epsilon}{q} = \epsilon^2 - 2\frac{\epsilon}{q} + \frac{\epsilon}{q} \geq \epsilon^2 - 2\frac{\epsilon}{q} + \frac{1}{q^2} = \left(\epsilon - \frac{1}{q}\right)^2$$

Άρα

$$\epsilon' \geq \left(\epsilon - \frac{1}{q}\right)^2 \Rightarrow \epsilon \leq \sqrt{\epsilon'} + \frac{1}{q}$$

# Υπενθύμιση: Πρωτόκολλα HVZK

## HVZK

Ένα πρωτόκολλο μεταξύ ενός  $P$  και ενός  $V$  είναι Honest Verifier Zero Knowledge αν υπάρχει αλγόριθμος  $PPT$   $Sim$  τέτοιος ώστε για κάθε  $(vk, sk) \leftarrow KGen(1^\lambda)$  οι κατανομές πιθανότητας των transcripts μεταξύ  $P(sk, vk), V(vk)$  είναι ίδιες με αυτές μεταξύ  $Sim(vk), V(vk)$

## Το πρωτόκολλο Schnorr είναι HVZK

Ο  $Sim$  παράγει τα μήνυμα με αντίστροφη σειρά

Τα transcripts

$\mathcal{T}_1 = \langle P(Y, x), V(Y) \rangle = (T = g^t, c, s = t + cx)$  και

$\mathcal{T}_2 = \langle Sim(Y), V(Y) \rangle = (T = g^s Y^{-c}, c, s)$

γίνονται αποδεκτά από τον  $V$  και έχουν ταυτόσημες κατανομές.

## Θεώρημα

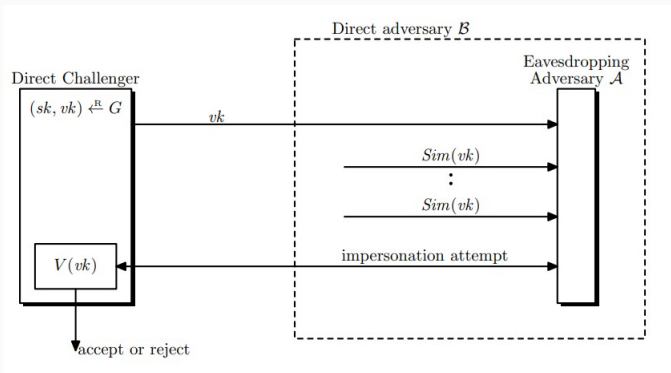
Αν το πρωτόκολλο ταυτοποίησης ID είναι HVZK, τότε:

$$\text{Adv}_{\mathcal{B}, \text{ID}}^{\text{id}_{\text{eve}}}(\lambda) = \text{Adv}_{\mathcal{A}, \text{ID}}^{\text{id}_{\text{da}}}(\lambda)$$

## Απόδειξη

Στο Eavesdropping παίγνιο  $ID_{\text{EVE}}$  ο  $\mathcal{B}$  παράγει τα transcripts μόνος του αντί να τα πάρει από τον challenger του direct παίγνιου  $ID_{\text{DA}}$ .

# Eavesdropping attacks και HVZK ii



## Fiat-Shamir Heuristic

Αντικατάσταση verifier από random oracle  $H : \mathcal{M} \times \mathbb{G}^2 \rightarrow \mathbb{Z}_q$

## Υπογραφές Schnorr

- $(q, g, \mathbb{G}) := \text{Pgen}(1^\lambda)$  με  $\mathbb{G} = \langle g \rangle$  ομάδα τάξης  $q$  και  $H : \mathcal{M} \times \mathbb{G}^2 \rightarrow \mathbb{Z}_q$
- $(x, Y) := \text{KGen}(\text{prms})$  με  $x \leftarrow \mathbb{Z}_q, Y = g^x$
- $\text{Sign}(x, m) = (T, s)$  με:
  - $T := g^t$  και  $t \leftarrow \mathbb{Z}_q$
  - $s := t + cx \bmod q$  με  $c := H(m, T, Y)$
- $\text{Vf}(Y, (T, s), m) = 1 \Leftrightarrow g^s = TY^{H(m, T, Y)}$

## Υπογραφές Schnorr - Εναλλακτική Υλοποίηση

- $(q, g, \mathbb{G}) := \text{Pgen}(1^\lambda)$  με  $\mathbb{G} = \langle g \rangle$  ομάδα τάξης  $q$  και  $H : \mathcal{M} \times \mathbb{G}^2 \rightarrow \mathbb{Z}_q$
- $(x, Y) := \text{KGen}(\text{prms})$  με  $x \leftarrow \mathbb{Z}_q, Y = g^x$
- $\text{Sign}(x, m) = (c, s)$  με:
  - $c := H(m, T, Y)$  και  $T := g^t$  με  $t \leftarrow \mathbb{Z}_q$
  - $s := t + cx \bmod q$
- $\forall (Y, (T, s), m) = 1 \Leftrightarrow c = H(m, g^s Y^{-c}, Y)$

Μείωση μεγέθους:

Κανονική υπογραφή  $\sigma \in \mathbb{G} \times \mathbb{Z}_q$

Εναλλακτική υπογραφή  $\sigma \in \mathbb{Z}_q^2$

## Θεώρημα

Έστω αντίπαλος  $\mathcal{A}$  ο οποίος επιτυγχάνει σε επίθεση **EUFCMA** εναντίον των υπογραφών Schnorr με το πολύ  $Q_{SO}$  signing queries και το πολύ  $Q_{RO}$  random oracle queries.

Τότε υπάρχει αντίπαλος  $\mathcal{B}$  ο οποίος νικάει στο  $ID_{r-EVE}$  με πλεονέκτημα:

$$\text{Adv}_{\mathcal{B}, Q_{RO}+1}^{\text{id}_{r-\text{eve}}}(\lambda) \geq \text{Adv}_{\mathcal{A}, \text{EUFCMA}}^{\text{schnorr}}(\lambda) - \frac{Q_{SO}(Q_{SO} + Q_{RO} + 1)}{q}$$



## Βασική Ιδέα

Θα κατασκευάσουμε  $\mathcal{B}$  ο οποίος απαντάει στα queries στο  $\mathcal{RO}$  και  $\mathcal{SO}$  τα οποία κάνει ο  $\mathcal{A}$  για να βγάλει πλαστογράφιση. Χρησιμοποιώντας την πλαστογράφιση θα πρέπει να κάνει έναν από τους verifiers του  $r$  impersonation game να αποδεκτούν.

**Πρόβλημα** Η αναγωγή θα πρέπει να προσομοιώσει υπογραφές για το  $\mathcal{SO}$  χωρίς το  $sk$

**Πώς;** Χρησιμοποιώντας τα transcripts από το eavesdropping game  $\mathcal{T} = \{(T_i, c_i, s_i)\}$  για να προγραμματίσει το  $\mathcal{RO}$ .

Πρέπει να μαντέψουμε ποιο  $\mathcal{RO}$  query θα οδηγήσει στην πλαστογράφιση.

**Υποθέσεις** Αν ο  $\mathcal{A}$  βγάλει μια πλαστογράφιση  $(m^*, (T^*, s^*))$  σημαίνει ότι:

- δεν έχει ζητήσει υπογραφή για το  $m^*$  στο  $\mathcal{SO}$ .
- έχει κάνει το ερώτημα  $(m^*, T^*, Y)$  στο  $\mathcal{RO}$ .

Ένα επιπλέον ερώτημα στο  $\mathcal{RO}$  :  $Q_{\mathcal{RO}} + 1$

## Αρχικοποίηση $\mathcal{B}$

- Είσοδος:  $Y, \mathcal{T} = \{(T_i, c_i, s_i)\}_{i=1}^{Q_s}$  τα οποία είναι έγκυρα
- Αποστολή  $Y$  στον  $\mathcal{A}$
- Αρχικοποίηση  $\mathcal{RO}$  ως άδειο λεξικό

## Προσομοίωση $\mathcal{SO}(m_i)$

- Ο  $\mathcal{B}$  δεν διαθέτει το ιδιωτικό κλειδί.
- Το ερώτημα αφορά το μήνυμα  $m_i$ .
- Ανάκτηση  $i$ -οστού transcript  $(T_i, c_i, s_i)$
- Θέτουμε  $\mathcal{RO}(m_i, T_i, Y) = c_i$  (για μελλοντική χρήση)
- Η υπογραφή  $\sigma_i = (T_i, s_i)$  είναι έγκυρη ( $T_i, s_i$  προέρχονται από τον challenger του  $\text{ID}_{\text{r-EVE}}$ )
- Επιστροφή  $\sigma_i$

## Προσομοίωση $\mathcal{RO}(m_j, T_j, Y)$

Το  $\mathcal{RO}$  ερωτάται είτε από τον  $\mathcal{A}$ , είτε εσωτερικά από τον  $\mathcal{B}$ .

Συνολικά το πολύ  $Q_{SO} + Q_{RO} + 1$  φορές.

Για το ερώτημα  $(m_j, T_j)$ :

- Αν  $\mathcal{RO}(m_j, T_j, Y) \neq \perp$ , επιστροφή του  $c_j$
- Αν  $\mathcal{RO}(m_j, T_j, Y) = \perp$ , τότε προώθηση  $T_j$  στον challenger-verifier  $V_j$  του  $\text{ID}_{r\text{-EVE}}$
- Λήψη  $c_j$  και προώθηση στον  $\mathcal{A}$
- Αποθήκευσε  $((m_j, T_j), j)$  για να θυμηθείς σε ποιον  $V_j$  θα στείλεις την απάντηση  $s_j$ .

## Λήψη forgery $m^*, (T^*, s^*)$

- Θα έχει ρωτηθεί το  $\mathcal{RO}(m^*, T^*)$
- Δηλαδή  $T^* = T_j$  για κάποιο  $j$
- Ανάκτηση  $j$  από λίστα και αποστολή  $s^*$  στον  $V_j$

## Πρόβλημα: Ύπαρξη συγκρούσεων

Κάποιο από τα  $T_i$  τα οποία ερωτούνται στο  $\mathcal{SO}$  έχει ερωτηθεί νωρίτερα στο  $\mathcal{RO}$ .

Γιατί; ο  $\mathcal{B}$  'χαραμίζει' ένα transcript από αυτά που δόθηκαν από το eavesdropping.

Πιθανότητα το πολύ  $Q_{\mathcal{SO}} \frac{Q_{\mathcal{SO}} + Q_{\mathcal{RO}} + 1}{q}$

# Συνολικά - Αναγωγή στο διακριτό λογάριθμο

$$\sqrt{\text{Adv}_{\mathcal{B}}^{\text{dlp}}(\lambda)} \geq \text{Adv}_{\mathcal{A}}^{\text{id}_{\text{da}}}(\lambda) - \frac{1}{q} \quad (\text{DLP} \Rightarrow \text{ID}_{\text{DA}})$$

$$\text{Adv}_{\mathcal{B}, \text{ID}}^{\text{id}_{\text{eve}}}(\lambda) = \text{Adv}_{\mathcal{A}, \text{ID}}^{\text{id}_{\text{da}}}(\lambda) \quad (\text{ID}_{\text{EVE}} \Leftrightarrow \text{ID}_{\text{DA}})$$

$$\text{Adv}_{\mathcal{B}, \text{ID}}^{\text{id}_{\text{eve}}}(\lambda) \geq \frac{1}{Q_{\mathcal{RO}} + 1} \text{Adv}_{\mathcal{A}, \text{ID}, Q_{\mathcal{RO}} + 1}^{\text{id}_{\text{r-eve}}}(\lambda) \quad (\text{ID}_{\text{EVE}} \Rightarrow \text{ID}_{\text{r-EVE}})$$

$$\text{Adv}_{\mathcal{B}, Q_{\mathcal{RO}} + 1}^{\text{id}_{\text{r-eve}}}(\lambda) \geq \text{Adv}_{\mathcal{A}, \text{EUF-CMA}}^{\text{schnorr}}(\lambda) - \frac{Q_{\mathcal{SO}}(Q_{\mathcal{SO}} + Q_{\mathcal{RO}} + 1)}{q} \quad (\text{ID}_{\text{r-EVE}} \Rightarrow \text{DS}_{\text{Schnorr}})$$

Άρα:

$$\sqrt{\text{Adv}_{\mathcal{B}}^{\text{dlp}}(\lambda)} \geq -\frac{1}{q} + \frac{1}{Q_{\mathcal{RO}} + 1} \cdot \left( \text{Adv}_{\mathcal{A}, \text{EUF-CMA}}^{\text{schnorr}}(\lambda) - \frac{Q_{\mathcal{SO}}(Q_{\mathcal{SO}} + Q_{\mathcal{RO}} + 1)}{q} \right) +$$

Τελικά:

$$\text{Adv}_{\mathcal{A}, \text{EUF-CMA}}^{\text{schnorr}}(\lambda) \leq \frac{Q_{\mathcal{RO}} + 1}{q} + \frac{Q_{\mathcal{SO}}(Q_{\mathcal{SO}} + Q_{\mathcal{RO}} + 1)}{q} + (Q_{\mathcal{RO}} + 1) \cdot \sqrt{\text{Adv}_{\mathcal{B}}^{\text{dlp}}(\lambda)}$$

# One-More Discrete Log (OMDL) [?] i

DL oracle το οποίο για  $Y_i \in \mathbb{G}$  επιστρέφει  $x_i \in \mathbb{Z}_q : Y_i = g^{x_i}$

Χρήση το πολύ  $Q = \text{poly}(\lambda)$  φορές.

Εξαγωγή ενός επιπλέον Discrete Log που δεν έχει ρωτηθεί στο DL oracle

Ισχυρότερη υπόθεση από DLP ( $\text{DLP} = \text{OMDL}_0$ )

Χρήση για απόδειξη ασφάλειας Schnorr Identification για active - concurrent sessions [?].



# One-More Discrete Log (OMDL) [?] ii

---

Algorithm 2:  $\text{OMDL}_n$

---

Input :  $\lambda$

Output:  $\{0, 1\}$

$(\mathbb{G}, q, g) \leftarrow \text{Pgen}(1^\lambda)$

$\{x_i\}_{i=1}^n \leftarrow \mathbb{Z}_q$

for  $i \leftarrow 0$  to  $n$  do

$Y_i := g^{x_i}$

end

$(\pi, \{z_i\}_{i=1}^{Q+1}) \leftarrow \mathcal{A}^{\text{DL}}(\mathbb{G}, q, g, (Y_i)_{i=1}^n)$

if  $\forall i \in Q + 1 : y_i = g^{z_{\pi(i)}} \wedge Q \leq n$  then

  return 1

else

  return 0

end

---

## Θεώρημα [?]

$$\text{Adv}_{\mathcal{A}, \text{ID}_{CC}}^{\text{schnorr}}(\lambda) \leq \frac{1}{q} + \sqrt{\text{Adv}_{\mathcal{B}}^{\text{omdl}}(\lambda)}$$

Αν το OMDL είναι δύσκολο, τότε το σχήμα ταυτοποίησης schnorr είναι ασφαλές εναντίον active - concurrent impersonation attacks.

Έστω  $\mathcal{A}$  που νικά στο  $ID_{CC}$ .

Θα κατασκευάσουμε  $\mathcal{B}$  που νικάει στο OMDL. Δηλ. πρέπει να έχει ως έξοδο  $Q + 1$  διακριτούς λογάριθμους, ενώ έχει κάνει  $Q$  ερωτήσεις στο DL oracle.

Αρχικά ο  $\mathcal{A}$  θα χρειαστεί να αλληλεπιδράσει με prover clones ως *verifier*. Ο  $\mathcal{B}$  θα τους προσομοιώσει με τη βοήθεια του DL.

Δηλαδή:

- $\mathcal{B}$  prover
- $\mathcal{A}$  verifier

## Απόδειξη ii

Ο  $\mathcal{B}$  επιλέγει  $Y \leftarrow \mathbb{G}$ . Για κάθε session με τον  $\mathcal{A}$ , ο  $\mathcal{B}$  επιλέγει  $T_i \leftarrow \mathbb{G}$ . Όταν ο  $\mathcal{A}$  (V) στείλει το challenge  $c_i$  ο  $\mathcal{B}$  κάνει query to DL oracle με την τιμή  $T_i \cdot Y^{c_i}$  και προωθεί την απάντησή του ως  $s_i$ .

Ορθότητα:

$$\begin{aligned} \text{DL}(T_i \cdot Y^{c_i}) &= \\ \text{DL}(T_i) + \text{DL}(Y^{c_i}) &= \\ t_i + cx_i &= \\ s_i \end{aligned}$$

Αλλαγή ρόλων. Δηλαδή:

- $\mathcal{B}$  verifier
- $\mathcal{A}$  prover

Στη συνέχεια ο  $\mathcal{A}$  κάνει την direct attack στέλνοντας commitment  $T$ .

Ο  $\mathcal{B}$  επιλέγει τυχαίο challenge  $c$  και το στέλνει στον  $\mathcal{A}$ . Λαμβάνει το response  $s$  και ελέγχει αν  $g^s = TY^c$  (επιτυχές με πιθανότητα  $\epsilon$ )

Rewind

Ο  $\mathcal{B}$  επιλέγει τυχαίο challenge  $c'$  και το στέλνει στον  $\mathcal{A}$ . Λαμβάνει το response  $s'$  και ελέγχει αν  $g^{s'} = TY^{c'}$ . (επιτυχές με πιθανότητα  $\epsilon$ ).

Ο  $\mathcal{B}$  ανακτά το  $x, Y = g^x$  ως:  $x = \frac{s-s'}{c-c'}$

Στη συνέχεια υπολογίζει τους υπόλοιπους  $Q$  λογάριθμους για τα  $T_i$  που ζήτησε από το DL ως  $t_i = s_i - c_i x$

Τελικά επιστρέφει  $(x, t_1, \dots, t_Q)$ .

Ιδανικά Straight Line Reductions: Δεν χρειάζεται το rewinding

Δεν υπάρχουν στο standard model

## Algebraic Group Model [?]

Ο  $\mathcal{A}$  κάθε φορά που επιστρέφει ένα στοιχείο  $T \in \mathbb{G}$  επιστρέφει και την αναπαράσταση του σχετικά με τα στοιχεία που έχει δει μέχρι τώρα.

Δηλαδή:

$$(T, (a_0, a_1, \dots, a_n)) \leftarrow \mathcal{A}(g, Y_1, \dots, Y_n)$$

με

$$= g^{a_0} Y_1^{a_1} \dots Y_n^{a_n}$$

## Υπολογισμός DLP χωρίς rewinding

Όταν εξαχθεί το forgery  $\sigma^* = (T^*, s^*)$  εξάγονται και  $(a_0, a_1)$  ώστε  $= g^{a_0} Y^{a_1}$

Όμως:  $g^{s^*} = TY^{c^*}$  έχουμε:

$$\begin{aligned} g^{s^*} Y^{c^*} &= g^{a_0} Y^{a_1} \Rightarrow \\ s^* + xc^* &= a_0 + xa_1 \Rightarrow \\ x &= \frac{a_0 - s^*}{c^* - a_1} \end{aligned}$$



Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko, *The one-more-rsa-inversion problems and the security of chaum's blind signature scheme*, J. Cryptol. **16** (2003), no. 3, 185–215.



Mihir Bellare and Adriana Palacio, *Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks*, Advances in Cryptology — CRYPTO 2002 (Berlin, Heidelberg) (Moti Yung, ed.), Springer Berlin Heidelberg, 2002, pp. 162–177.



Georg Fuchsbauer, Eike Kiltz, and Julian Loss, *The algebraic group model and its applications*, Advances in Cryptology – CRYPTO 2018 (Cham) (Hovav Shacham and Alexandra Boldyreva, eds.), Springer International Publishing, 2018, pp. 33–62.





David Pointcheval and Jacques Stern, *Security arguments for digital signatures and blind signatures*, J. Cryptol. **13** (2000), no. 3, 361–396.



Claus-Peter Schnorr, *Efficient identification and signatures for smart cards*, Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 1989, Proceedings (Gilles Brassard, ed.), Lecture Notes in Computer Science, vol. 435, Springer, 1989, pp. 239–252.