Αποδείξεις Μηδενικής Γνώσης και εφαρμογές

Παναγιώτης Γροντάς

16/12/2022

ΕΜΠ - Κρυπτογραφία

Περιεχόμενα

Εισαγωγή

Αποδείξεις

Αποδείξεις στα μαθηματικά

- Στόχος: η αλήθεια μας πρότασης
- με ενδιάμεσους συλλογισμούς
- οι οποίοι δίνουν όμως επιπλέον πληροφορίες

Πχ. απόδειξη με Αντί-Παράδειγμα
Ο 15 δεν είναι πρώτος

...γιατί διαιρείται από το 3 και το 5

Ερώτημα: Μπορούμε να πειστούμε για την αλήθεια χωρίς διαρροή επιπλέον πληροφοριών (μεταφορά γνώσης);

Εισαγωγή

- Shaffi Goldwasser, Silvio Micali και Charles Rackoff, 1985
- Διαλογικά συστήματα αποδείξεων
  - Υπολογισμός ως διάλογος
  - Prover (P): Θέλει να αποδείξει ότι μία συμβολοσειρά ανήκει σε μία γλώσσα
  - Verifier (V): Θέλει να ελέγξει την απόδειξη
    - Μια σωστή απόδειξη πείθει τον V με πολύ μεγάλη πιθανότητα
    - Μια λάθος απόδειξη πείθει τον V με πολύ μικρή πιθανότητα
- Απόδειξη μηδενικής γνώσης
  - Ο V πείθεται χωρίς να μαθαίνει τίποτε περισσότερο

Μηδενική γνώση: Ιδιότητα που προστατεύει τον P

Πολλές θεωρητικές και πρακτικές εφαρμογές (Βραβείο Turing 2013)

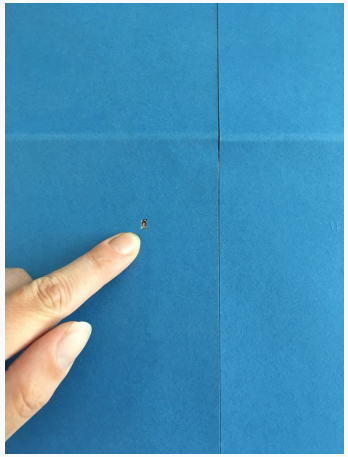
Ένα εύκολο παράδειγμα (Oded Goldreich)

- Ο V έχει αχρωματοψία
- Ο P έχει δύο ταυτόσημες μπάλες, διαφορετικού χρώματος
- Μπορεί να πειστεί ο V για το ότι οι μπάλες έχουν διαφορετικό χρώμα (αφού δεν μπορεί να το μάθει);
- Ναι
    - Ο P δίνει τις μπάλες στον V (commit)
    - Ο V κρύβει τις μπάλες πίσω από την πλάτη του (1 ανά χέρι)
    - Στην τύχη, αποφασίζει να τις αντιμεταθέσει (ή όχι)
    - Ο V παρουσιάζει τα χέρια με τις μπάλες στον P (challenge)
    - Ο P απαντάει αν άλλαξαν χέρια (response)
    - Ο V αποδέχεται ή όχι
    - Αν οι μπάλες δεν έχουν διαφορετικό χρώμα (κακόβουλος P): Πιθανότητα απάτης 50%
    - Επανάληψη: Μείωση πιθανότητας απάτης (πρέπει να μαντέψει σωστά όλες τις φορές)

Άλλα παραδείγματα

- Where’s waldo 





- Η σπηλιά του Aladdin How to explain zero-knowledge protocols to your children
- Γνώση λύσης sudoku

Εφαρμογές στην κρυπτογραφία

- Σχήματα αυθεντικοποίησης αντί για passwords
  - Αντί για κωδικό: Απόδειξη ότι ο χρήστης τον γνωρίζει
  - Αποφεύγεται η μετάδοση και η επεξεργασία
  - Secure Remote Password protocol (SRP - RFC 2945)
- Απόδειξη ότι το κρυπτοκείμενο περιέχει μήνυμα συγκεκριμένου τύπου
- Ψηφιακές υπογραφές
- Άντι-malleability
- Απόδειξη ότι έγινε κάποιος υπολογισμός σε μια ιδιωτική βάση δεδομένων
- Γενικά: Απόδειξη ότι παίκτης ακολουθεί κάποιο πρωτόκολλο χωρίς αποκάλυψη ιδιωτικών δεδομένων του
- Μετατροπή πρωτοκόλλων με παθητική ασφάλεια σε ενεργή ασφάλεια

Συστήματα Αποδείξεων Μηδενικής Γνώσης

Διαλογικά Συστήματα Αποδείξεων

Συμβολισμός

- Γλώσσα $\mathcal{L} \in \boldsymbol{NP}$
- Πολυωνυμική Μηχανή Turing $\mathcal{M}$
- $x \in \mathcal{L} \Leftrightarrow \exists w \in \{0,1\}^{p(|x|)} : M(x,w) = 1$
- Δύο μηχανές Turing P, V
- $\langle \mathrm{P}(x,w), \mathrm{V}(x) \rangle$ είναι το transcript του πρωτοκόλλου μεταξύ P, V με κοινή (δημόσια είσοδο) το x και ιδιωτική είσοδο του P το w.
- $out_{\mathrm{V}} \langle \mathrm{P}(x,w), \mathrm{V}(x) \rangle$ η έξοδος του V στο τέλος του πρωτοκόλλου

Διαλογικά Συστήματα Αποδείξεων: Παράδειγμα

- $\mathcal{L}$ η γλώσσα του προβλήματος του διακριτού λογαρίθμου
- x ένα στιγμιότυπο του προβλήματος $x = (g : \langle g \rangle = \mathbb{G}, b \in_R \mathbb{G})$
- w ο 'μάρτυρας', δηλ. $w : b = g^w$

Διαλογικά Συστήματα Αποδείξεων

Ένα πρωτόκολλο μηδενικής γνώσης για την $\mathcal{L}$ είναι μία αλληλεπίδραση $\langle \mathrm{P}(x, w), \mathrm{V}(x) \rangle$ με τις εξής ιδιότητες:

Πληρότητα - Completeness
Ο *τίμιος* P, πείθει έναν *τίμιο* V με βεβαιότητα

Αν $x \in \mathcal{L}$ και $M(x, w) = 1$

$$Pr[out_{\mathrm{V}} \langle \mathrm{P}(x, w), \mathrm{V}(x) \rangle = 1] = 1$$

Διαλογικά Συστήματα Αποδείξεων: Ορθότητα

Ορθότητα - Soundness
Κανένας *κακόβουλος* P (σμβ. με P*), δεν μπορεί να πείσει *τίμιο* V, παρά με αμελητέα πιθανότητα.
Αν $x \notin \mathcal{L}$ τότε $\forall(\mathrm{P}^*, w^*)$:

$$Pr[out_{\mathrm{V}}\langle \mathrm{P}^*(x, w^*), \mathrm{V}(x)\rangle = 1] = negl(\lambda)$$

Παρατηρήσεις:
Proof: Ο P είναι unbounded - statistical / information theoretic soundness
Argument of Knowledge: Ο P είναι PPT / computational soundness

Διαλογικά Συστήματα Αποδείξεων: Μηδενική Γνώση

Διαίσθηση
Ο V δεν μαθαίνει τίποτε εκτός από το γεγονός ότι ο ισχυρισμός του P είναι αληθής.

Ό,τι μπορεί να υπολογίσει ο V μετά την συζήτηση με τον P, μπορεί να το υπολογίσει και μόνος του

ή ισοδύναμα με μια συζήτηση με κάποια PPT TM που δεν διαθέτει τον witness (προσομοίωση συζήτησης με simulator Sim)

(δηλαδή ουσιαστικά χωρίς τη συζήτηση με τον πραγματικό P)

Άρα: η συζήτηση προσθέτει *μηδενική γνώση*

Διαλογικά Συστήματα Αποδείξεων: Μηδενική Γνώση

Ορισμός για (Τέλεια) Μηδενική Γνώση:

Υπάρχει μία PPT Sim ώστε για κάθε PPT V*: Αν $x \in \mathcal{L}$ και $M(x, w) = 1$ οι τυχαίες μεταβλητές

$$out_{V*}\langle P(x, w), V^*(x)\rangle \text{ και}$$
$$out_{V*}\langle Sim(x)^{V^*(x)}\rangle$$

ακολουθούν ακριβώς την ίδια κατανομή.

κακόβουλος verifier προσπαθεί να μάθει κάποιο κατηγόρημα για το w είτε παθητικά είτε χωρίς να ακολουθεί το πρωτόκολλο

Απόδειξη ιδιότητας ZK: Ο simulator

Δεν διαθέτει τον witness αλλά δουλεύει στην γλώσσα $\mathcal{L}$

- Προσομοίωση απόδειξης στη θέση του P
- Αλληλεπιδρά με τον V
- Οι αλληλεπιδράσεις $\langle \text{Sim}, \text{V} \rangle$ και $\langle \text{P}, \text{V} \rangle$ είναι μη διακρίσιμες
- Επιτρέπουμε και rewinds:
  - Αν κάποια στιγμή ο V 'ρωτήσει' κάτι που δεν μπορεί να απαντήσει ο Sim τότε stop - rewind
- Μηδενική γνώση αν ο V κάποια στιγμή αποδεχτεί (έστω και με rewinds)
- Γιατί: Δεν μπορεί να ξεχωρίσει τον P (που διαθέτει witness) από τον Sim (που δεν διαθέτει)
- Αρκεί ο Sim να παραμείνει PPT
- Συγκεκριμένα: Ένας V που εξάγει πληροφορία από τον P θα εξάγει την ίδια πληροφορία και από τον Sim (όπου δεν υπάρχει κάτι να εξαχθεί)

Σχέση Ορθότητας - Μηδενικής Γνώσης

Ο Sim μοιάζει με κακό P* (και οι δύο δεν διαθέτουν τον witness). Μήπως θα μπορούσε να χρησιμοποιηθει ο Sim για να σπάσει η ορθότητα:

ΟΧΙ

Το rewind απορρίπτει αυτή την δυνατότητα, γιατί:

Επιτρέπει στον Sim να αντιδρά μόνο σε γνωστά μηνύματα του V

Ο P* δεν έχει αυτή τη δυνατότητα, μαθαίνει το μήνυμα και πρέπει να απαντήσει στη διάρκεια του πρωτοκόλλου

Αν δεν υπήρχε η δυνατότητα rewind τότε θα ήταν αδύνατο να ισχύει ταυτόχρονα soundness και ZK

Παρατήρηση: Sim ορίζεται για $x \in \mathcal{L}$

Φυσική ερμηνεία rewind: snapshot VM - εκτέλεση - επιστροφή

Παραλλαγές Μηδενικής Γνώσης i

- **Almost Perfect (Statistical) Zero Knowledge** Οι κατανομές των συζητήσεων με έχουν αμελητέα στατιστική απόσταση.
- **Computational Zero Knowledge** Οι κατανομές των συζητήσεων δεν μπορούν να διαχωριστούν από κάποιον αντίπαλο με πολυωνυμική υπολογιστική ισχύ.

Παραλλαγές Μηδενικής Γνώσης ii

- **Honest Verifier Zero Knowledge**
  - Ο V είναι τίμιος δηλ:
  - ακολουθεί το πρωτόκολλο
  - τα μηνύματα του προέρχονται από την ομοιόμορφη κατανομή - δεν εξαρτώνται από τα μηνύματα του P
  - μοντελοποιεί και παθητικό αντίπαλο

  Πρακτικά: ο Sim παράγει συζητήσεις οι οποίες έχουν ίδια κατανομή με αυθεντικές $\langle P(x, w), V(x) \rangle$
- **Witness hiding - Witness Indistinguishable proofs**
  - WH - δεν μπορεί να γίνει γνωστός ολόκληρος ο μάρτυρας
  - WI - δεν μπορεί να γίνει διάκριση μεταξύ ισοδύναμων μαρτύρων

Διαφορά ZK - HVZK

... είναι στον V

- Σε HVZK:
  - Τα μηνύματα του V είναι τυχαία
  - Μπορούν να προετοιμαστούν εκ των προτέρων από τον P(και τον Sim
  - Άρα ο V *δεν χρειάζεται* (non interactive)
- Σε ZK:
  - Ο αντίπαλος είναι οποιοσδήποτε verifier
  - Μπορεί να μην ακολουθήσει το πρωτόκολλο
  - Τα μηνύματα του V εξαρτώνται από τα μηνύματα του P

Παραλλαγές Ορθότητας

Ειδική ορθότητα (special soundness)
Υπάρχει ένας PPT αλγόριθμος (Knowledge Extractor), $\mathcal{E}$ ο οποίος αν δεχθεί *πολλά επιτυχή* transcripts του πρωτοκόλλου με το ίδιο αρχικό μήνυμα από τον P αλλά διαφορετικές προκλήσεις από τον V μπορεί να εξάγει τον witness.

Knowleldge Extractor
Αν $x \in \mathcal{L}$ και $M(x, w) = 1$ τότε υπάρχει PPT αλγόριθμος $\mathcal{E}$

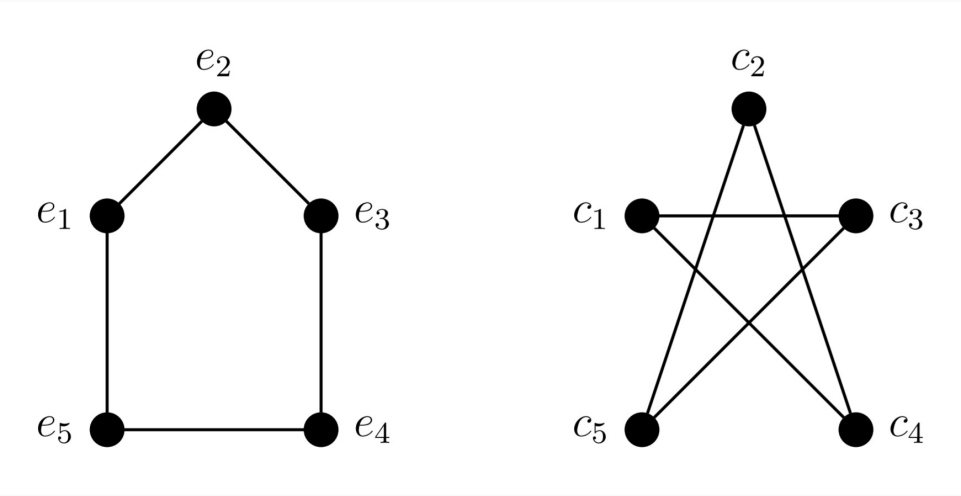
$$Pr[\mathcal{E}(\langle \mathrm{P}(x, w), \mathrm{V}(x) \rangle) = w] \geq 1 - negl(\lambda)$$

Θεώρημα
Ειδική ορθότητα $\Rightarrow$ ορθότητα με πιθανότητα false-positive $\frac{1}{|C|}$ όπου:
C: το σύνολο προέλευσης των μηνυμάτων του V

Ειδική ορθότητα $\Rightarrow$ απόδειξη γνώσης συγκεκριμένου witness

Graph Isomorphism

Ορισμός
Γραφήματα $G_0 = (V_0, E_0)$ και $G_1 = (V_1, E_1)$ με $|V_0| = |V_1|$
Ισχύει ο ισομορφισμός $G_0 \cong G_1$ ανν υπάρχει $\pi : V_0 \to V_1$ ώστε
$(v_i, v_j) \in E_0 \Leftrightarrow (\pi(v_i), \pi(v_j)) \in E_1$



GI HV-ZKP

Δημόσια είσοδος: Τα γραφήματα G_0, G_1
Witness (P): π

1. P: εφαρμόζει τυχαία μετάθεση π_1 στο V_1
2. Προκύπτει γράφημα F ($G_1 \cong F$) το οποίο δημοσιοποιείται στον V (δέσμευση)
3. V: Επιλέγει ένα τυχαίο bit b και το στέλνει στον P
4. Αν $b = 1$ ο P δημοσιοποιεί $\phi_1 = \pi_1 : V_1 \to V_F$
5. Αν $b = 0$ ο P δημοσιοποιεί $\phi_0 = \pi_1.\pi : V_0 \to V_F$ ώστε $G_0 \cong F$
6. Ο V δέχεται ανν $\phi_b(G_b) = F$
7. Επανάληψη k φορές

GI HV-ZKP: Ιδιότητες

Πληρότητα
Αν P, V έντιμοι και ακολουθούν το πρωτόκολλο τότε σίγουρη αποδοχή

- $b = 1 : \phi_1(G_b) = \pi_1(G_1) = F$
- $b = 0 : \phi_0(G_b) = \pi_1.\pi(G_0) = \pi_1(G_1) = F$

Ορθότητα
Αν $\nexists \pi$ ώστε $G_0 \cong G_1$ τότε σε κάθε επανάληψη:

- ο V δέχεται με πιθανότητα $\frac{1}{2}$ $(b = 1)$

Με επανάληψη k φορές: Πιθανότητα επιτυχούς απάτης 2^{-k}

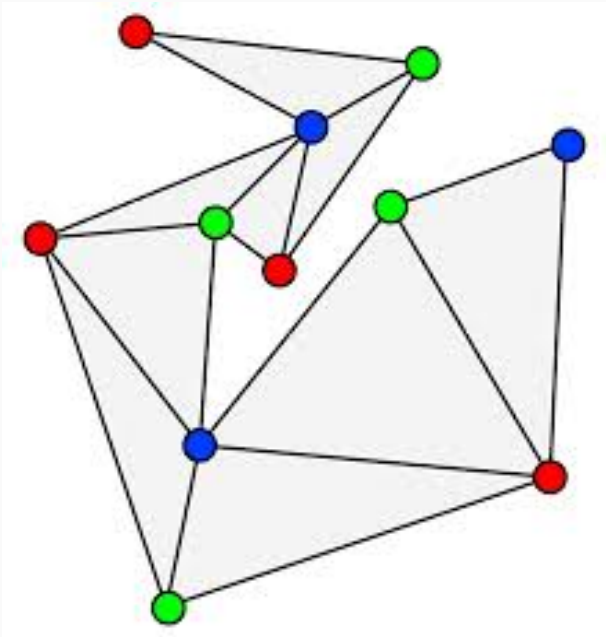
GI HV-ZKP: Μηδενική Γνώση

Κατασκευή simulator Sim (V^*)

1. Επιλέγει ομοιόμορφα $b' \in \{0, 1\}$ και μετάθεση π'_1
2. Υπολογίζει $F' = \pi'_1(G_{b'})$
3. Κλήση V^*: $b \leftarrow V^*(F')$
4. Αν $b = b'$ τότε κλήση $V^*(F', \pi'_1)$ αλλιώς rewind

Αφού G_0, G_1 είναι ισομορφικά: $\pi'_1(G_0), \pi'_1(G_1)$ έχουν ίδια κατανομή για τυχαίο π'_1
Αναμενόμενος χρόνος εκτέλεσης του Sim για επιτυχία: διπλάσιος του V

3-colorability



NP-Complete

Ορισμός

Γράφημα $G = (V, E)$

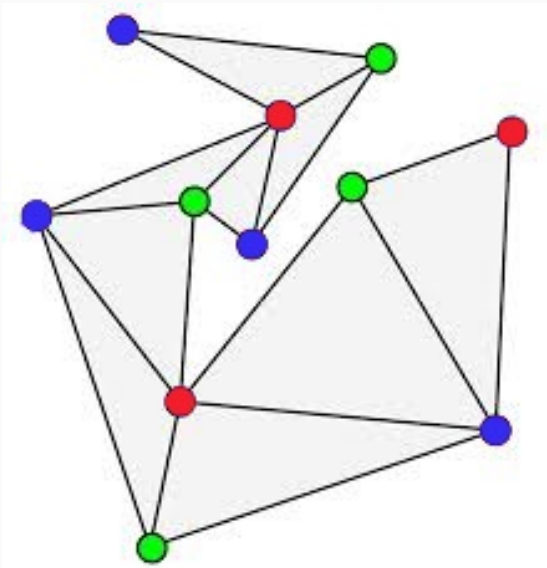
Ο P γνωρίζει ένα χρωματισμό

$c : V \to \{1, 2, 3\}$

Έγκυρος χρωματισμός: Γειτονικές κορυφές έχουν διαφορετικό χρώμα $(v_i, v_j) \in E \Rightarrow c(v_i) \neq c(v_j)$

ZKP for 3-colorability

1. P: επιλέγει μια τυχαία μετάθεση π του $\{1, 2, 3\}$.
   - Προκύπτει εναλλακτικός έγκυρος 3 - χρωματισμός $\pi.c$ του G.
   - Χρήση σχήματος δέσμευσης για τον εναλλακτικό χρωματισμό
   - Υπολογίζει $commit((\pi.c)(v_i), r_i) \forall v_i \in V$
   - Αποστολή δεσμεύσεων στον V
2. V: επιλέγει μία τυχαία ακμή $(v_i, v_j) \in E$ και την στέλνει στον P.
3. P: ανοίγει τις δεσμεύσεις - αποκαλύπτει τις τιμές $\pi.c(v_i), \pi.c(v_j)$ και r_i, r_j
4. V: ελέγχει αν $\pi.c(v_i) \neq \pi.c(v_j)$ και οι δεσμεύσεις είναι έγκυρες
5. Επανάληψη $|V| \mid E \mid$ με νέο randomness κάθε φορά



ZKP for 3-colorability: Ιδιότητες (Πληρότητα)

- **Πληρότητα**
  Αν ο c είναι έγκυρος χρωματισμός τότε και ο $\pi.c$ είναι έγκυρος χρωματισμός
  Το άνοιγμα των δεσμεύσεων θα γίνει αποδεκτό από V

ZKP for 3-colorability: Ιδιότητες (Ορθότητα)

- **Ορθότητα**

  Έστω P* με μη έγκυρο χρωματισμό για κάποιο γράφημα:
  Δηλ. τουλάχιστον 2 γειτονικές κορυφές με το ίδιο χρώμα:
  Πιθανότητα ανίχνευσης εξαπάτησης από V = Πιθανότητα επιλογής 'κακής' ακμής = $\frac{1}{|E|}$
  Πιθανότητα επιτυχούς εξαπάτησης από P* = $1 - \frac{1}{|E|}$
  Σε $|V||E|$ επαναλήψεις και εφόσον

  $$(1 + \frac{t}{n})^n \leq e^t$$

  Πιθανότητα επιτυχίας του P*:

  $$(1 - \frac{1}{|E|})^{|V||E|} \leq e^{-|V|}$$ αμελητέα

ZKP for 3-colorability: Ιδιότητες (Μηδενική Γνώση)

- Κατασκευή simulator
  - Ο Sim επιλέγει μια ακμή e_i^* και χρωματίζει τις κορυφές με διαφορετικό χρώμα
  - Για τις υπόλοιπες ακμές χρωματίζει τις κορυφές με το ίδιο χρώμα
  - Δέσμευση στον χρωματισμό
  - Κλήση $e_i \leftarrow \mathrm{V}^*(G, \{commit_i\}_{i=1}^{|V|})$
  - Αν $e_i = e_i^*$ αποκάλυψη χρωμάτων
  - Αν $e_i \neq e_i^*$, restart
  - Αναμενόμενος αριθμός rewinds για επιτυχία $|E|$

ZKP for 3-colorability: Ιδιότητες (Μηδενική Γνώση)

Όμως οι συζητήσεις δεν είναι πανομοιότυπες! (Γιατί;)

Τα commitments του P είναι έγκυροι χρωματισμοί, ενώ του Sim όχι!

Η ιδιότητα ZK εξαρτάται από το πόσο καλά κρύβουν τα commitments τους χρωματισμούς!

Αλλά 3-colorability NP-Complete

Συνέπεια [GMW91]
Αν υπάρχουν ασφαλή σχήματα δέσμευσης τότε όλο το NP έχει αποδείξεις μηδενικής γνώσης

Σ-πρωτόκολλα

Σ-πρωτόκολλα

Χαλάρωση ZK με τίμιο verifier

Ορισμός
Ένα πρωτόκολλο 3 γύρων με honest verifier και special soundness

1. **Commit** Ο P δεσμεύεται σε μία τιμή.
2. **Challenge** Ο V διαλέγει μία τυχαία πρόκληση. Εφόσον είναι τίμιος θεωρούμε ότι η πιθανότητα επιλογής πρόκλησης είναι ομοιόμορφα κατανεμημένη.
3. **Response** Ο P απαντάει χρησιμοποιώντας τη δέσμευση, το μυστικό και την τυχαία τιμή.

Special Soundness
Δύο εκτελέσεις του πρωτοκόλλου με το ίδιο commitment, οδηγούν στην αποκάλυψη του witness

Γνώση DLOG:Το πρωτόκολλο του Schnorr i

Γνωστά Στοιχεία

- **Δημόσια:** Γεννήτορας g μιας (υπό)ομάδας τάξης q του $\mathbb{Z}_p^*$ με δύσκολο DLP και στοιχείο $h \in \mathbb{Z}_p^*$
- **Ιδιωτικά:** Ο P έχει ένα witness $x \in \mathbb{Z}_q^*$ ώστε $h = g^x \pmod{p}$

Στόχος

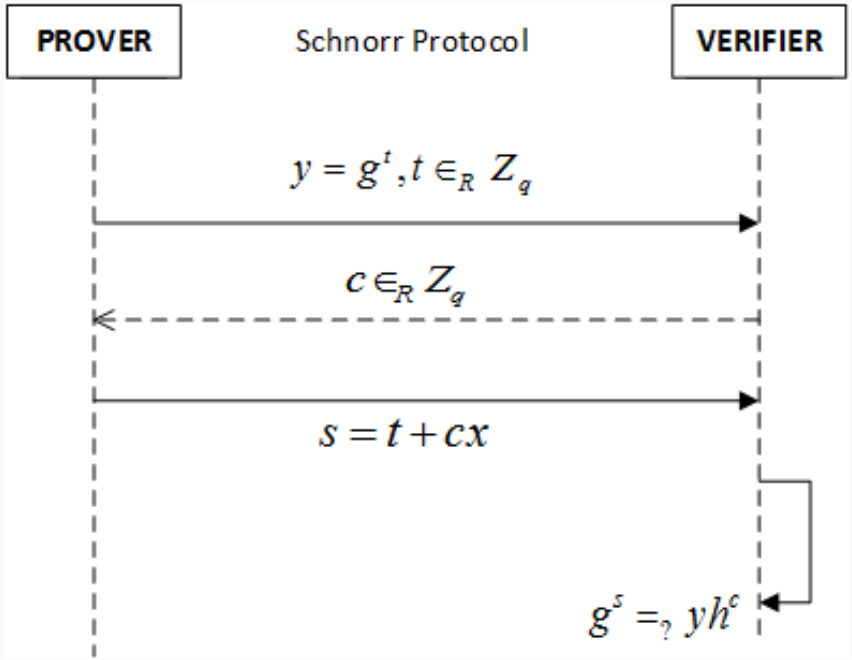
Απόδειξη κατοχής του x χωρίς να αποκαλυφθεί.

Συμβολισμός Camenisch-Stadler

$PoK\{(x) : g^x = h \pmod{p}, h, g \in_R \mathbb{Z}_p^*\}$

Γνώση DLOG:Το πρωτόκολλο του Schnorr ii

- **Commit** ($\mathsf{P} \to \mathsf{V}$)**:**
  - Τυχαία επιλογή $t \in_R \mathbb{Z}_q^*$
  - Υπολογισμός $y = g^t \bmod p$.
  - Αποστολή y στον V.
- **Challenge** ($\mathsf{V} \to \mathsf{P}$)**:**
  Τυχαία επιλογή και αποστολή
  $c \in_R \mathbb{Z}_q^*$
- **Response** ($\mathsf{P} \to \mathsf{V}$)**:**
  Ο P υπολογίζει το
  $s = t + cx \bmod q$ και το στέλνει
  στον V
- Ο V αποδέχεται αν
  $g^s = yh^c \pmod p$



Πρωτόκολλο Schnorr: Πληρότητα

- Πληρότητα

$$g^s = g^{t+cx} = g^t g^{cx} = yh^c \pmod{p}$$

Πρωτόκολλο Schnorr: Ορθότητα

- **Ορθότητα** Πιθανότητα ο P* να ξεγελάσει τίμιο verifier: $\frac{1}{q}$ - αμελητέα
- **Special soundness**
  Έστω 2 επιτυχείς εκτελέσεις του πρωτοκόλλου (y, c, s) και (y, c', s')

$$g^s = yh^c \text{ και } g^{s'} = yh^{c'} \Rightarrow g^s h^{-c} = g^{s'} h^{-c'} \Rightarrow$$
$$g^{s-xc} = g^{s'-xc'} \Rightarrow s - xc = s' - xc' \Rightarrow$$
$$x = \frac{s' - s}{c' - c}$$

  Αφού ο P μπορεί να απαντήσει 2 τέτοιες ερωτήσεις ξέρει το DLOG (ορθότητα και γνώση)

Πρωτόκολλο Schnorr: HVZK

- Διαθέτει Honest Verifier Zero Knowledge
  Έστω Sim που δεν γνωρίζει το x και τίμιος V
  - Αρχικά ο Sim δεσμεύεται κανονικά στο $y = g^t, t \in_R \mathbb{Z}_q^*$
  - Ο V επιλέγει $c \in_R \mathbb{Z}_q^*$
  - Αν ο Sim μπορεί να απαντήσει (αμελητέα πιθανότητα) το πρωτόκολλο συνεχίζει κανονικά
  - Αλλιώς γίνεται rewind ο V
  - Στη δεύτερη εκτέλεση ο Sim δεσμεύεται στο $y = g^t h^{-c}, t \in_R \mathbb{Z}_q^*$
  - Ο V επιλέγει ίδιο $c \in_R \mathbb{Z}_q^*$ (ίδιο random tape)
  - Ο Sim στέλνει $s = t$
  - Ο V θα δεχτεί αφού
    $yh^c = g^t h^{-c} h^c = g^t = g^s$

Δηλαδή:
Η συζήτηση $(t \in_R \mathbb{Z}_q; g^t h^{-c}, c \in_R \mathbb{Z}_q, t)$ και η $(t, c \in_R \mathbb{Z}_q; g^t, c, t + xc)$ ακολουθούν την ίδια κατανομή

Πρωτόκολλο Schnorr: ZK

Μηδενική Γνώση: Δε διαθέτει

- Ένας cheating verifier δε διαλέγει τυχαία
- Βασίζει κάθε challenge στο προηγούμενο commitment του Sim
- Στη simulated εκτέλεση δεν θα επιλέξει το ίδιο challenge
- Αμελητέα πιθανότητα να μπορεί να απαντηθεί από τον Sim

Ενίσχυση για μηδενική γνώση:

- Προσθήκη δέσμευσης από τον V στην τυχαιότητα *πριν* το πρώτο μήνυμα του P ή
- Challenge space $\{0, 1\}$ (γιατί;)
- Ο V έχει δύο επιλογές μόνο για επιλογή πρόκλησης.
- Αν αλλάξει, ο Sim μπορεί να προετοιμαστεί και για τις δύο περιπτώσεις.

Ισότητα DLOG:Το πρωτόκολλο Chaum Pedersen i

Γνωστά Στοιχεία

- **Δημόσια:** Γεννήτορες g_1, g_2 μιας (υπό)ομάδας τάξης q του $\mathbb{Z}_p^*$ με δύσκολο DLP και 2 στοιχεία $h_1, h_2 \in \mathbb{Z}_p^*$
- **Ιδιωτικά:** Ο P έχει ένα witness $x \in \mathbb{Z}_q$ ώστε $h_1 = g_1^x \bmod p$, $h_2 = g_2^x \bmod p$

Στόχος

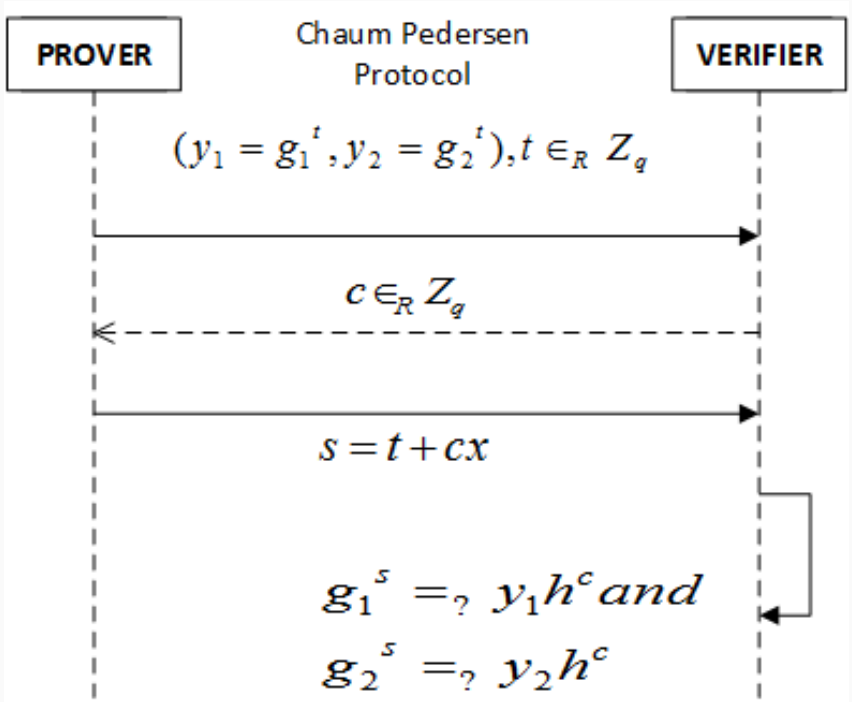
Απόδειξη γνώσης του x χωρίς να αποκαλυφθεί

Απόδειξη ισότητας διακριτών λογαρίθμων

$$PoK\{(x) : h_1 = g_1^x \pmod p \wedge h_2 = g_2^x \pmod p, h_1, g_1, h_2, g_2 \in_R \mathbb{Z}_p^*\}$$

Ισότητα DLOG:Το πρωτόκολλο Chaum Pedersen ii

- **Commit:**
  - Ο P διαλέγει $t \in_R \mathbb{Z}_q$
  - Υπολογίζει $y_1 = g_1^t \bmod p$
    $y_2 = g_2^t \bmod p$
  - Αποστέλλει y_1, y_2 στον V
- **Challenge:**
  Ο V διαλέγει και αποστέλλει
  $c \in_R \mathbb{Z}_q$
- **Response:**
  Ο P υπολογίζει $s = t + cx \bmod q$
  και το στέλνει στον V



Ο V δέχεται αν $g_1^s = y_1 h_1^c \pmod p$ και $g_2^s = y_2 h_2^c \pmod p$

Ιδιότητες Chaum-Pedersen i

- **Πληρότητα**
  Αν $h_1 = g_1^x$ και $h_2 = g_2^x$ τότε:

$$g_1^s = g_1^{t+xc} = y_1 h_1^c$$
$$g_2^s = g_2^{t+xc} = y_2 h_2^c$$

- **Special soundness**
  Έστω δύο αποδεκτά transcripts με το ίδιο commitment $((y_1, y_2), c, s)$ και $((y_1, y_2), c', s')$

$$g_1^s = y_1 h_1^c \text{ και } g_1^{s'} = y_1 h_1^{c'} \Rightarrow g_1^s h_1^{-c} = g_1^{s'} h_1^{-c'}$$
$$g_2^s = y_2 h_2^c \text{ και } g_2^{s'} = y_2 h_2^{c'} \Rightarrow g_2^s h_2^{-c} = g_2^{s'} h_2^{-c'}$$

  Όπως σε Schnorr $x = \frac{s'-s}{c'-c}$

Ιδιότητες Chaum-Pedersen ii

- **Honest verifier zero knowledge**

  Πραγματικό transcript με $c \in_R \mathbb{Z}_q$:

  $$(t \in_R \mathbb{Z}_q; (g_1^t, g_2^t), \quad c \in_R \mathbb{Z}_q, \quad t + xc \bmod q)$$

  Simulated transcript με $c \in_R \mathbb{Z}_q$:

  $$(t, c \in_R \mathbb{Z}_q; (g_1^t h_1^{-c}, g_2^t h_2^{-c}), \quad c, \quad t)$$

  Ίδιες κατανομές αν $x = log_{g_1} h_1 = log_{g_2} h_2$

Εφαρμογές

Έλεγχος για τριάδες DH

Η τριάδα (g^a, g^b, g^c) είναι τριάδα DH (δηλ. $g^c = g^{ab}$)

Εκτελούμε $CP(g_1 = g, g_2 = g^b, h_1 = g^a, h_2 = g^{ab} = g^{b^a})$ με witness a

Εγκυρότητα κρυπτογράφησης El-Gamal

Δίνεται ένα ζεύγος στοιχείων του $\mathbb{Z}_p^*$ τα (c_1, c_2).

Να δειχθεί ότι αποτελούν έγκυρη κρυπτογράφηση ενός μηνύματος m.

Αν είναι έγκυρη τότε πρέπει

$$(c_1, c_2) = (g^r, m \cdot h^r)$$

Ισοδύναμα:

$$log_g c_1 = log_h(\frac{c_2}{m})$$

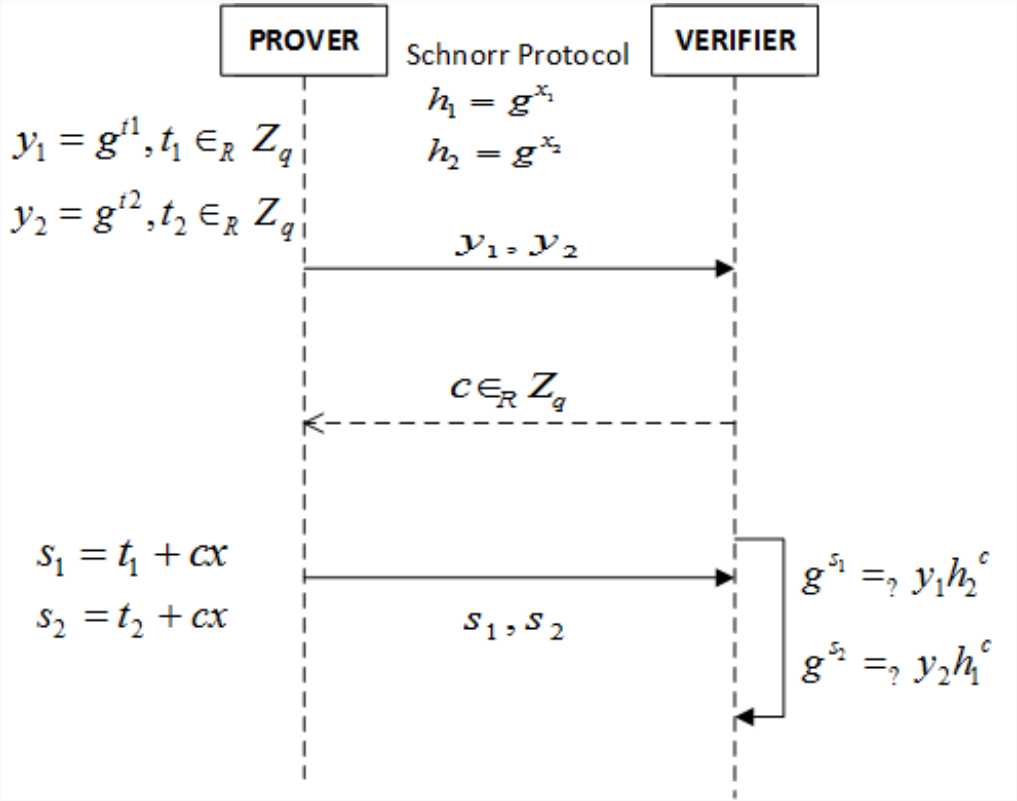
δηλ. ότι έχει χρησιμοποιηθεί κοινή τυχαιότητα και ο P τη γνωρίζει

Σύνθεση Σ πρωτοκόλλων i

Θέωρημα
Τα Σ πρωτόκολλα διατηρούν τις ιδιότητες τους αν συνδυαστούν με τις παρακάτω σχέσεις:

- *AND*
  - Ο P γνωρίζει 2 διαφορετικά *w* για διαφορετικές σχέσεις.
  - Απόδειξη: 2 παράλληλες εκτελέσεις του Σ πρωτόκολλου με ίδιο challenge

Σύνθεση Σ πρωτοκόλλων ii



Σύνθεση Σ πρωτοκόλλων iii

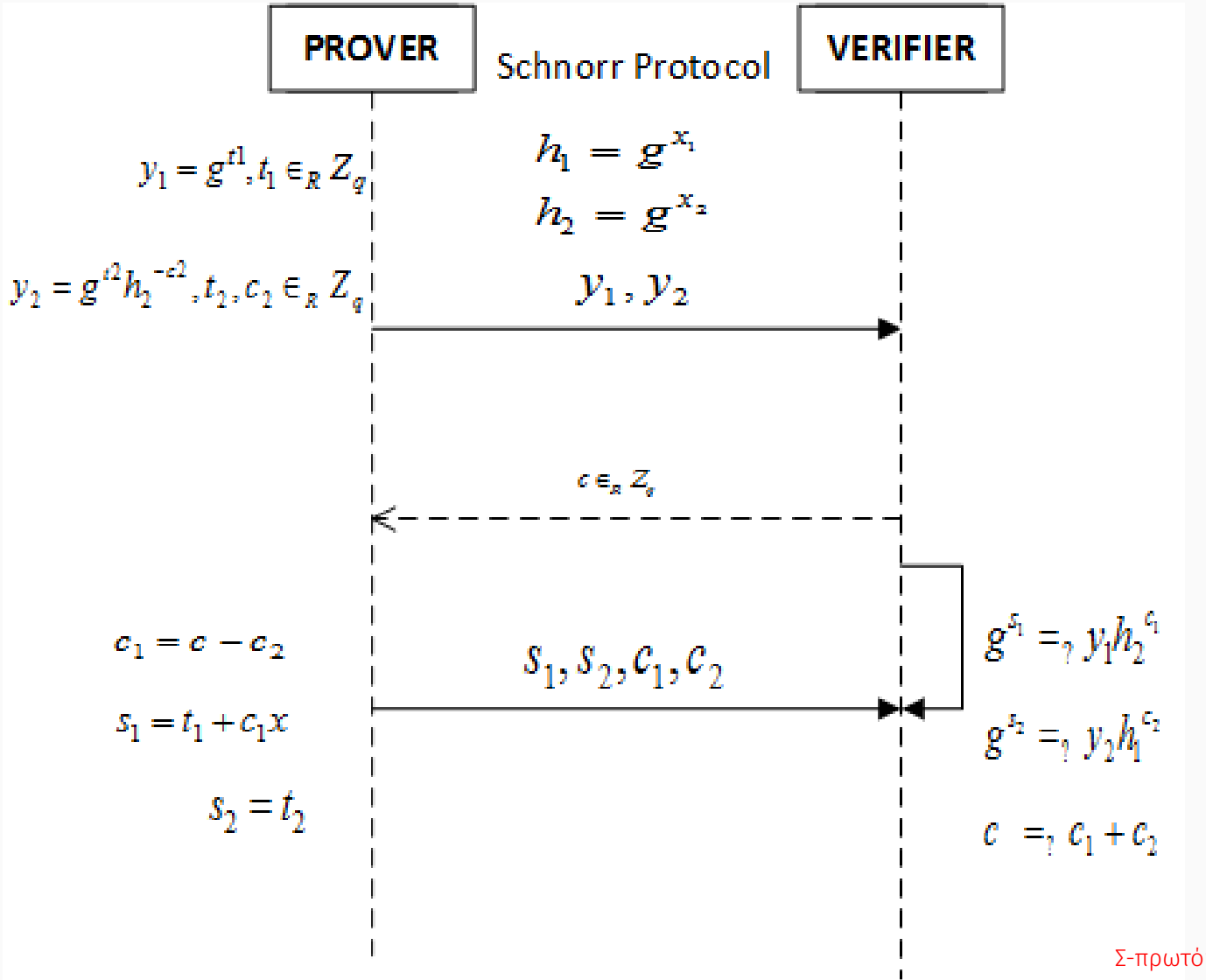
- Batch-AND
  Μαζική επαλήθευση πολλαπλών σχέσεων με ένα πρωτόκολλο. Για παράδειγμα:
  (g^a, g^b, g^{ab}) ΚΑΙ (g^c, g^d, g^{cd}) είναι τριάδες DH
  Μπορώ να εκτελέσω το Chaum Pedersen για $(g^{ac}, g^{bd}, g^{abcd})$
- *EQ*
  - Ο P γνωρίζει τον ίδιο *w* για διαφορετικές σχέσεις.
  - Chaum Pedersen
- *OR*
  - Ο P γνωρίζει *κάποιο w* για διαφορετικές σχέσεις.
  - Εφαρμογή: Απόδειξη ότι ο *w* ανήκει σε ένα σύνολο

Γενικευμένη κατασκευή αποδείξεων OR

- Έστω $W = \{w_1, ..., w_n\}$ οι εναλλακτικοί μάρτυρες
- Για αυτόν που κατέχει ο P ακολουθεί το πρωτόκολλο
- Για τους υπόλοιπους ο P καλεί τον Sim ο οποίος υπολογίζει τις δεσμεύσεις που θα έκαναν τον V να δεχθεί σε μία προσομοιωμένη συζήτηση
  - Πρόβλημα: Ο Sim δεν ξέρει το challenge
  - Λύση: Το επιλέγει τυχαία
- Όλες οι δεσμεύσεις αποστέλλονται στον V
- Ο τελευταίος απαντάει με *μία* τυχαία πρόκληση
- Ο P ερμηνεύει την πρόκληση ως ένα μυστικό που πρέπει να χωριστεί
- Κάθε μερίδιο θα χρησιμοποιείται στις απαντήσεις του P στο στάδιο Response
- Ο V αποδέχεται αν όλες τις απαντήσεις που έλαβε στο τελευταίο βήμα είναι έγκυρες.

OR-Schnorr

$PoK\{(x_1, x_2) : h_1 = g_1^{x_1} \pmod p \vee h_2 = g_2^{x_2} \pmod p\}$ Υποθέτουμε ότι ο P ξέρει το x_1



Μη διαλογικές αποδείξεις

Ερώτηση
Μπορούμε να καταργήσουμε τον V ;

Ο P παράγει την απόδειξη μόνος του

Η απόδειξη είναι επαληθεύσιμη από οποιονδήποτε

Common Reference String
Μία ομοιόμορφα επιλεγμένη ακολουθία bits (από κάποια έμπιστη οντότητα) ως κοινή είσοδος σε P, V
Χρησιμεύει για την επιλογή των μηνυμάτων που ανταλλάσσονται

Μετασχηματισμός Fiat Shamir
Αντικατάσταση της τυχαίας πρόκλησης με το αποτέλεσμα μιας ψευδοτυχαίας συνάρτησης με είσοδο τη δέσμευση (τουλάχιστον)

Συνήθως συνάρτηση σύνοψης - $\mathcal{H}$ (τυχαίο μαντείο)

Non-interactive Schnorr

Γνωστά Στοιχεία

- **Δημόσια:** Γεννήτορας g μιας (υπό)ομάδας τάξης q του $\mathbb{Z}_p^*$ με δύσκολο DLP και στοιχείο $h \in \mathbb{Z}_p^*$
- **Ιδιωτικά:** Ο P έχει ένα witness $x \in \mathbb{Z}_q^*$ ώστε $h = g^x \bmod p$

Ο P:

- Τυχαία επιλογή $t \in_R \mathbb{Z}_q$,
- Υπολογισμός $y = g^t \bmod p$
- Υπολογισμός $c = \mathcal{H}(y)$ όπου $\mathcal{H}$ είναι μια συνάρτηση σύνοψης που δίνει τιμές στο $\mathbb{Z}_q$
- Υπολογισμός $s = t + cx \bmod q$
- Δημοσιοποίηση του (c, s)
- Επαλήθευση (από οποιονδήποτε) $c = \mathcal{H}(g^s h^{-c})$

Υπογραφές Schnorr

Αποδείξεις μηδενικής γνώσης (ιδιωτικού) κλειδιού υπογραφής που λαμβάνουν υπ' όψιν και το μήνυμα

Ο υπογράφων:

- Τυχαία επιλογή $t \in_R \mathbb{Z}_q$,
- Υπολογισμός $y = g^t \bmod p$
- Υπολογισμός $c = \mathcal{H}(y||m)$ όπου $\mathcal{H}$ είναι μια συνάρτηση σύνοψης που δίνει τιμές στο $\mathbb{Z}_q$
- Υπολογισμός $s = t - cx \bmod q$ (για να μην χρειαστεί αντίστροφος μετά)
- Δημοσιοποίηση του (c, s)
- Επαλήθευση (από οποιονδήποτε) $c = \mathcal{H}(g^s h^c||m)$