Αποδείξεις Μηδενικής Γνώσης

Διαφάνειες: Παναγιώτης Γροντάς - Αλέξανδρος Ζαχαράκης

04/12/2018

ΕΜΠ - Κρυπτογραφία (2018-2019)

Περιεχόμενα

- Εισαγωγή
- Ορισμός - Εφαρμογές στην Θ. Πολυπλοκότητας
- Σ-πρωτόκολλα
- Witness Indistinguishable & Witness Hiding Πρωτόκολλα

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 - (κέρδος γνώσης);

Εισαγωγή

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

Μηδενική γνώση: Ιδιότητα που προστατεύει τον P Πολλές θεωρητικές και πρακτικές εφαρμογές (Βραβείο Turing 2013)

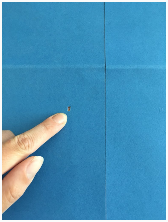
Ένα εύκολο παράδειγμα

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

Άλλα παραδείγματα

- Where's waldo 





- Η σπηλιά του Alladin 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
- Γενικά: Απόδειξη ότι παίκτης ακολουθεί κάποιο πρωτόκολλο χωρίς αποκάλυψη ιδιωτικών δεδομένων του

Συστήματα Αποδείξεων Μηδενικής Γνώσης

Συμβολισμός

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

Διαλογικά Συστήματα Αποδείξεων: Παράδειγμα

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

Διαλογικά Συστήματα Αποδείξεων: Πληρότητα

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

Πληρότητα - Completeness
Ο *τίμιος* $\mathcal{P}$, πείθει έναν *τίμιο* $\mathcal{V}$ με βεβαιότητα

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

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

Διαλογικά Συστήματα Αποδείξεων: Ορθότητα

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

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

Παρατήρηση:

Proof of Knowledge: Ο $\mathcal{P}^*$ δεν είναι PPT.

Argument of Knowledge: Ο $\mathcal{P}^*$ είναι PPT.

Διαίσθηση
Ο $\mathcal{V}$ δεν μαθαίνει τίποτε εκτός από το γεγονός ότι ο ισχυρισμός του $\mathcal{P}$ είναι αληθής.

Ό,τι μπορεί να υπολογίσει ο $\mathcal{V}$ μετά την συζήτηση με τον $\mathcal{P}$, μπορεί να το υπολογίσει και μόνος του

ή ισοδύναμα με μια συζήτηση με κάποια TM που δεν διαθέτει τον witness (προσομοίωση συζήτησης με simulator $\mathcal{S}$)

(δηλαδή ουσιαστικά χωρίς τη συζήτηση με τον πραγματικό $\mathcal{P}$) Άρα: η συζήτηση προσθέτει *μηδενική γνώση*

Ορισμός για (Τέλεια) Μηδενική Γνώση:
Για κάθε PPT $\mathcal{V}^*$ υπάρχει μία PPT $\mathcal{S}$: Αν $x \in \mathcal{L}$ και $M(x, w) = 1$ οι τυχαίες μεταβλητές

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

ακολουθούν ακριβώς την ίδια κατανομή.

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

Απόδειξη ιδιότητας ZK: Ο simulator

Δεν διαθέτει τον witness

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

Σχέση Ορθότητας - Μηδενικής Γνώσης

Ο $\mathcal{S}$ μοιάζει με κακό $\mathcal{P}^*$ (και οι δύο δεν διαθέτουν τον witness).

Ο $\mathcal{P}^*$

- Δεν γνωρίζει w
- Ορθότητα: Δεν πρέπει να πείσει τον V
- Μπορεί να μην είναι PPT

Ο $\mathcal{S}$

- Δεν γνωρίζει w
- ZK: Πρέπει να πείσει τον $\mathcal{V}^*$ με *rewinds*
- Πρέπει να είναι PPT

Για τον $\mathcal{V}$

- Στην ορθότητα πρέπει να είναι τίμιος
- Στην μηδενική γνώση όχι

Σύνθεση πρωτοκόλλων μηδενικής γνώσης

Σειριακή
Είναι δυνατή η εκτέλεση πολλών πρωτοκόλλων ZK το ένα μετά το άλλο Το αποτέλεσμα ΔΙΑΘΕΤΕΙ ZK

Παράλληλη
Γενικά δεν είναι δυνατή.

Η παράλληλη εκτέλεση δύο πρωτοκόλλων ZK δεν παράγει πρωτόκολλο ZK. Αιτία - Ιδέα

- $\mathcal{P}_1, \mathcal{P}_2$ (unbounded) zero knowledge provers
- $\mathcal{V}^*$: PPT δεν μπορεί να διακρίνει τις απαντήσεις
- Σε παράλληλη εκτέλεση: Με βάση τις απαντήσεις του $\mathcal{P}_1$ κατασκευάζει ερωτήσεις για τον $\mathcal{P}_2$ από τις οποίες εξάγει γνώση για το statement του $\mathcal{P}_1$

- Black-Box Zero Knowledge
  $\exists$ PPT $\mathcal{S}$, $\forall \mathcal{V}^*$
  $out_{\mathcal{V}^*}\langle \mathcal{P}(x,w), \mathcal{V}^*(x)\rangle(x)$ και $out_{\mathcal{V}^*}\langle \mathcal{S}^{\mathcal{V}^*}(x), \mathcal{V}^*(x)\rangle(x)$ να ακολουθούν ακριβώς την ίδια κατανομή.
  Παρατηρήσεις: Ο $\mathcal{S}$
    - ισχύει για όλους τους $\mathcal{V}$
    - έχει oracle access στον $\mathcal{V}$
    - δηλ. ελέγχει το input, rewind αλλά όχι το output

Παραλλαγές Μηδενικής Γνώσης ii

- **Almost Perfect (Statistical) Zero Knowledge** Οι κατανομές των συζητήσεων με $\mathcal{P}$,S

  .

  $\Delta(X,Y) = \frac{1}{2}\sum_{u \in V} |Prob_[X = u] - Prov[Y = u]| = negl(\lambda), \Lambda = |x|$
- **Computational Zero Knowledge** Οι κατανομές των συζητήσεων δεν μπορούν να διαχωριστούν από κάποιον αντίπαλο με πολυωνυμική υπολογιστική ισχύ.

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

  Πρακτικά: ο $\mathcal{S}$ παράγει συζητήσεις οι οποίες έχουν ίδια κατανομή με αυθεντικές $\langle\mathcal{P}(x,w),\mathcal{V}(x)\rangle$
- Witness hiding - Witness Indistinguishable proofs
    - WH - δεν μπορεί να γίνει γνωστός ολόκληρος ο μάρτυρας
    - WI - δεν μπορεί να γίνει διάκριση ποιου μάρτυρα από κάποιες επιλογές

  Ισχύει παράλληλη σύνθεση και έχουν καλύτερη απόδοση

Διαφορά ZK - HVZK

... είναι στον $\mathcal{V}$

- Σε HVZK:
  - Τα μηνύματα του $\mathcal{V}$ είναι τυχαία
  - Μπορούν να προετοιμαστούν εκ των προτέρων από τον $\mathcal{S}$
  - Άρα ο $\mathcal{V}$ *δεν χρειάζεται* (non interactive)
- Σε ZK:
  - Τα μηνύματα του $\mathcal{V}$ εξαρτώνται από τα μηνύματα του $\mathcal{P}$

Παραλλαγές Ορθότητας

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

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

Ειδική ορθότητα $\Rightarrow$ απόδειξη γνώσης

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 ZKP

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

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

GI ZKP: Ιδιότητες

Πληρότητα
Αν $\mathcal{P}, \mathcal{V}$ έντιμοι και ακολουθούν το πρωτόκολλο τότε σίγουρη αποδοχή

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

Ορθότητα
Αν $\mathcal{P}$ δεν έχει π ώστε $G_0 \cong G_1$ τότε σε κάθε επανάληψη:

- ο $\mathcal{V}$ δέχεται με πιθανότητα $\frac{1}{2}$ γιατί ο $\mathcal{P}^*$ δεν μπορεί να γνωρίζει και ϕ_0 και ϕ_1

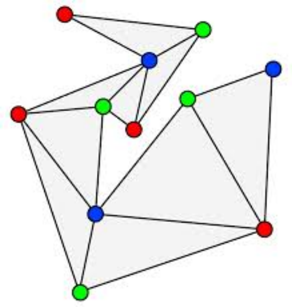
GI ZKP: Μηδενική Γνώση

Κατασκευή simulator $\mathcal{S}$
Commitment: Επιλέγει b' και τυχαία μετάθεση π'
Υπολογίζει $F = \pi'(G_{b'})$

Challenge: Αν $b = b'$ τότε αποστολή π' αλλιώς rewind

Πιθανότητα αποδοχής σε k επαναλήψεις 2^{-k}

Αναμενόμενος χρόνος εκτέλεσης: $T_V \sum_{i=1}^{\infty} 2^{-k} = T_V$ που είναι πολυωνυμικός

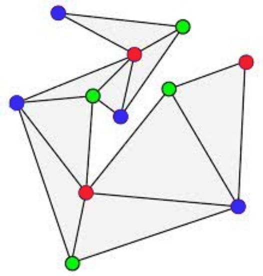


NP-Complete

Ορισμός
Γράφημα $G = (V, E)$
Ο $\mathcal{P}$ γνωρίζει ένα χρωματισμό $c : V \rightarrow \{1, 2, 3\}$
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. $\mathcal{P}$: 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 $\mathcal{V}$
2. $\mathcal{V}$: επιλέγει μία τυχαία ακμή $(v_i, v_j) \in E$ και την στέλνει στον $\mathcal{P}$.
3. $\mathcal{P}$: ανοίγει τις δεσμεύσεις - αποκαλύπτει τις τιμές $\pi.c(v_i), \pi.c(v_j)$ και r_i, r_j
4. $\mathcal{V}$: ελέγχει αν $\pi.c(v_i) \neq \pi.c(v_j)$ και οι δεσμεύσεις είναι έγκυρες
5. Επανάληψη



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 $\mathcal{V}$

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

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

  Πιθανότητα επιτυχίας του $\mathcal{P}^*$:

$$(1 - \frac{1}{|E|})^{|E|^2} \leq e^{-|E|}$$ αμελητέα ως προς το μέγεθος του γραφήματος

ZKP for 3-colorability: Ιδιότητες (Μηδενική Γνώση)

- Μηδενική Γνώση
  - Χρήση $\mathcal{S}$ χωρίς γνώση έγκυρου χρωματισμού
  - Ο $\mathcal{S}$ επιλέγει τυχαίο χρωματισμό
  - Πιθανότητα επιλογής από $\mathcal{V}$ ακμής με διαφορετικά χρώματα κορυφών $\frac{2}{3}$
  - Πιθανότητα επιλογής από $\mathcal{V}$ ακμής με ίδια χρώματα κορυφών $\frac{1}{3}$
  - Αν ο $\mathcal{V}$ επιλέγει 'κακή' ακμή, rewind (και εκτέλεση από την αρχή)
  - Για k επιτυχείς επιλογές χρειάζονται κατά μέσο όρο $2k$ εκτελέσεις

ZKP for 3-colorability: Ιδιότητες (Μηδενική Γνώση)

Συμπέρασμα: Ο $\mathcal{S}$ δεν απαιτεί πολύ περισσότερο χρόνο από έναν $\mathcal{P}$ με γνώση του c

Όμως οι συζητήσεις δεν είναι πανομοιότυπες! (Γιατί;)

Τα commitments του $\mathcal{P}$ είναι έγκυροι χρωματισμοί, ενώ του $\mathcal{S}$ όχι!

Συνέπεια [GMW91]
Αν υπάρχουν computationally hiding bit commitment schemes τότε όλο το NP έχει αποδείξεις μηδενικής γνώσης (black box computational)

Σ-πρωτόκολλα

Σ-πρωτόκολλα

Χαλάρωση ZK με τίμιο verifier

Ορισμός
Ένα πρωτόκολλο 3 γύρων με honest verifier και special soundness

1. **Commit** Ο $\mathcal{P}$ δεσμεύεται σε μία τιμή.
2. **Challenge** Ο $\mathcal{V}$ διαλέγει μία τυχαία πρόκληση. Εφόσον είναι τίμιος θεωρούμε ότι η πιθανότητα επιλογής πρόκλησης είναι ομοιόμορφα κατανεμημένη.
3. **Response** Ο $\mathcal{P}$ 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

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 $\mathcal{P}$ έχει ένα witness $x \in \mathbb{Z}_q^*$ ώστε $h = g^x \pmod{p}$

Στόχος

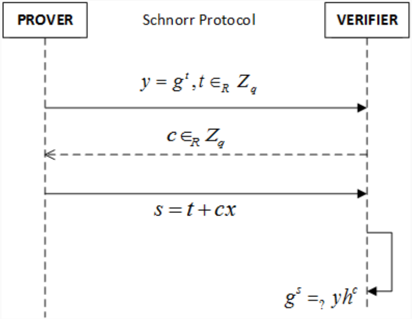
Απόδειξη κατοχής του x χωρίς να αποκαλυφθεί.

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 ($\mathcal{P} \rightarrow \mathcal{V}$):**
  - Τυχαία επιλογή $t \in_R \mathbb{Z}_q^*$
  - Υπολογισμός $y = g^t \bmod p$.
  - Αποστολή y στον $\mathcal{V}$.
- **Challenge ($\mathcal{V} \rightarrow \mathcal{P}$):** Τυχαία επιλογή και αποστολή $c \in_R \mathbb{Z}_q^*$
- **Response ($\mathcal{P} \rightarrow \mathcal{V}$):** Ο $\mathcal{P}$ υπολογίζει το $s = t + cx \bmod q$ και το στέλνει στον $\mathcal{V}$
- Ο $\mathcal{V}$ 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 $\mathcal{P}^*$ να ξεγελάσει τίμιο verifier: $\frac{1}{q}$ - αμελητέα - επανάληψη για μεγαλύτερη σιγουριά
- **Special soundness**
  Έστω 2 επιτυχείς εκτελέσεις του πρωτοκόλλου (y, c, s) και (y, c', s')

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

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

Πρωτόκολλο Schnorr: HVZK

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

Ενίσχυση για μηδενική γνώση:

- Προσθήκη δέσμευσης από τον $\mathcal{V}$ στην τυχαιότητα *πριν* το πρώτο μήνυμα του $\mathcal{P}$ ή
- Challenge space $\{0, 1\}$ (γιατί;)
- Ο $\mathcal{V}$ έχει δύο επιλογές μόνο για επιλογή πρόκλησης.
- Αν αλλάξει, ο $\mathcal{S}$ 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 $\mathcal{P}$ έχει ένα witness $x \in \mathbb{Z}_q$ ώστε $h_1 = g_1^x \bmod p$, $h_2 = g_2^x \bmod p$

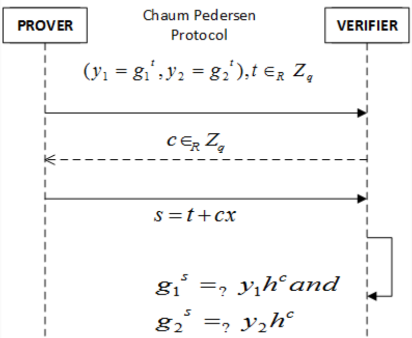
Στόχος

Απόδειξη γνώσης του x χωρίς να αποκαλυφθεί

Απόδειξη ισότητας διακριτών λογαρίθμων

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

- Commit:
    - Ο $\mathcal{P}$ 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 $\mathcal{V}$
- Challenge:
  Ο $\mathcal{V}$ διαλέγει και αποστέλλει
  $c \in_R \mathbb{Z}_q$
- Response:
  Ο $\mathcal{P}$ υπολογίζει $s = t + cx \bmod q$
  και το στέλνει στον $\mathcal{V}$



Ο $\mathcal{V}$ 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 $x = \frac{s-s'}{c'-c}$

- **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 $\mathsf{CP}(g_1 = g, g_2 = g^b, h_1 = g^a, h_2 = g^{ab} = g^{b^a})$ 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:

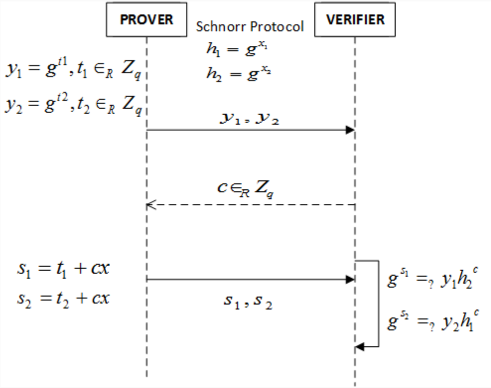
$$log_g c_1 = log_h(\frac{c_2}{m})$$

δηλ. ότι ο $\mathcal{P}$ είναι γνώστης της τυχαιότητας

Σύνθεση Σ πρωτοκόλλων i

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

- AND
    - Ο $\mathcal{P}$ γνωρίζει 2 διαφορετικά w για διαφορετικές σχέσεις.
    - Απόδειξη: 2 παράλληλες εκτελέσεις του Σ πρωτόκολλου με ίδιο challenge


PROVER
Schnorr Protocol
VERIFIER
$h_1 = g^{x_1}$
$h_2 = g^{x_2}$
$y_1 = g^{t1}, t_1 \in_R Z_q$
$y_2 = g^{t2}, t_2 \in_R Z_q$
y_1, y_2
$c \in_R Z_q$
$s_1 = t_1 + cx$
$s_2 = t_2 + cx$
s_1, s_2
$g^{s_1} =_? y_1 h_2^c$
$g^{s_2} =_? y_2 h_1^c$

Σύνθεση Σ πρωτοκόλλων iii

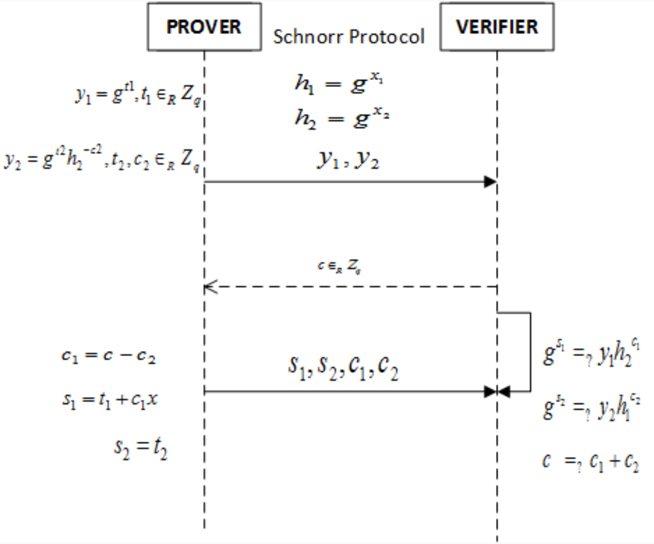
- Batch-AND
  Μαζική επαλήθευση πολλαπλών σχέσεων με ένα πρωτόκολλο. Για παράδειγμα:
  (g^a, g^b, g^{ab}) ΚΑΙ (g^c, g^d, g^{cd}) είναι τριάδες DH
  Μπορώ να εκτελέσω το Chaum Pedersen για $(g^{ac}, g^{bd}, g^{abcd})$
- EQ
  - Ο $\mathcal{P}$ γνωρίζει τον ίδιο w για διαφορετικές σχέσεις.
  - Chaum Pedersen
- OR
  - Ο $\mathcal{P}$ 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 $\mathcal{P}$ ακολουθεί το πρωτόκολλο
- Για τους υπόλοιπους ο $\mathcal{P}$ καλεί τον $\mathcal{S}$ ο οποίος υπολογίζει τις δεσμεύσεις που θα έκαναν τον $\mathcal{V}$ να δεχθεί σε μία προσομοιωμένη συζήτηση
  - Πρόβλημα: Ο $\mathcal{S}$ δεν ξέρει το challenge
  - Λύση: Το επιλέγει τυχαία
- Όλες οι δεσμεύσεις αποστέλλονται στον $\mathcal{V}$
- Ο τελευταίος απαντάει με *μία* τυχαία πρόκληση
- Ο $\mathcal{P}$ ερμηνεύει την πρόκληση ως ένα μυστικό που πρέπει να χωριστεί
- Κάθε μερίδιο θα χρησιμοποιείται στις απαντήσεις του $\mathcal{P}$ στο στάδιο Response
- Ο $\mathcal{V}$ αποδέχεται αν όλες τις απαντήσεις που έλαβε στο τελευταίο βήμα είναι έγκυρες.

OR-Schnorr

Υποθέτουμε ότι ο $\mathcal{P}$ ξέρει το x_1



Ερώτηση
Μπορούμε να καταργήσουμε τον $\mathcal{V}$;

Ο $\mathcal{P}$ 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 $\mathcal{P}, \mathcal{V}$
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 $\mathcal{P}$ έχει ένα witness $x \in \mathbb{Z}_q^*$ ώστε $h = g^x \bmod p$

Ο $\mathcal{P}$:

- 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 (h, c, s)
- Επαλήθευση (από οποιονδήποτε) $c = \mathcal{H}(g^s h^{-c})$

Witness Indistinguishable - Witness Hiding Protocols

Witness Indistinguishability & Witness Hiding

Χαλάρωση ZK για βελτίωση απόδοσης και composability

Υποθέτουμε cheating verifier $\mathcal{V}^*$

- Ορίζουμε ως $W(x) = \{w : R(x, w) = 1\}$
- Στις αποδείξεις γνώσης ο $\mathcal{P}$ θέλει να πείσει τον $\mathcal{V}$ ότι ξέρει έναν μάρτυρα $w \in W(x)$.
- ZK: Ο $\mathcal{V}^*$ δεν μαθαίνει *οτιδήποτε* για το w.
- WH: Ο $\mathcal{V}^*$ δεν μαθαίνει *ολόκληρο* $w \in W(x)$.
- WI: Ο $\mathcal{V}^*$ δεν μαθαίνει τίποτα για *ποιο* $w \in W(x)$ ξέρει ο $\mathcal{P}$.

Σχέση

- ZK $\rightarrow$ WH και ZK $\rightarrow$ WI (όχι όμως αντίστροφα)
- HVZK $\rightarrow$ WI
- Υπο συνθήκες WI $\rightarrow$ WH
- WH $\nrightarrow$ WI

Witness Indistinguishability

- Πολλά μυστικά κλειδιά αντιστοιχούν στο ίδιο δημόσιο κλειδί.
- Αποδείξεις με διαφορετικά κλειδιά είναι μη διακρίσιμες.
- Γνώση δύο κλειδιών οδηγούν σε εξαγωγή ενός μυστικού.

Ορισμός
Ένα διαλογικό σύστημα αποδείξεων είναι WI αν $\forall \mathcal{V}^*$ ισχύει

$$\{\langle \mathcal{P}(w), \mathcal{V}^*(z)\rangle(x)\}_{x \in L, w \in W(x)} \equiv \{\langle \mathcal{P}(w'), \mathcal{V}^*(z)\rangle(x)\}_{x \in L, w' \in W(x)}$$

Αναπαράσταση στοιχείου σε ομάδα

Ορισμός
Έστω $\mathbb{G}$ ομάδα τάξης q και $g_1, g_2 \in \mathbb{G}$. Αναπαράσταση του $h \in \mathbb{G}$ ως προς g_1, g_2 ονομάζεται κάθε ζεύγος $x_1, x_2 \in \mathbb{Z}_q$ τέτοιο ώστε $h = g_1^{x_1} g_2^{x_2}$.

Αν ξέρω δύο αναπαραστάσεις του h ως προς g_1, g_2 τότε ξέρω διακριτό λογάριθμο του g_2 ως προς g_1 (βλ. Pedersen commitments)

Πρωτόκολλο Okamoto Schnorr: WI Proof of Knowledge of Representation

$$PoK\{(x_1, x_2) : h = g_1^{x_1} g_2^{x_2}, \mathbb{G}, q,\ g_1, g_2, h \in \mathbb{G}, \}$$

- $\mathcal{P}$: $r_1, r_2 \leftarrow_R \mathbb{Z}_q$;
  $a \leftarrow g_1^{r_1} g_2^{r_2}$;
  Στέλνει a.
- $\mathcal{V}$: $c \leftarrow_R \mathbb{Z}_q$;
  Στέλνει c.
- $\mathcal{P}$: $s_1 = r_1 + x_1 c$; $s_2 = r_2 + x_2 c$;
  Στέλνει s_1, s_2.
- $\mathcal{V}$: Αποδέχεται αν $g_1^{s_1} g_2^{s_2} = a h^c$.

Πρωτόκολλο Okamoto Schnorr:Ιδιότητες

Ιδιότητες Πληρότητα και Ειδική Ορθότητα προφανείς.

WI: Έστω $h = g_1^{x_1} g_2^{x_2} = g_1^{x_1'} g_2^{x_2'}$
Τότε

$$g_1^{x_1 - x_1'} g_2^{x_2 - x_2'} = hh^{-1} = 1$$

Για κάθε transcript (a, c, s_1, s_2) με witness x_1, x_2 και τυχαιότητα r_1, r_2 στο πρώτο βήμα υπάρχουν r_1', r_2' που δίνουν ακριβώς την ίδια συζήτηση για x_1', x_2'. Πράγματι:

$$\begin{aligned}
r_1' &= r_1 + c(x_1 - x_1') \\
r_2' &= r_2 + c(x_2 - x_2') \\
a' &= g_1^{r_1'} g_2^{r_2'} = g_1^{r_1 + c(x_1 - x_1')} g_2^{r_2 + c(x_2 - x_2')} = \\
&= g_1^{r_1} g_2^{r_2} g_1^{c(x_1 - x_1')} g_2^{c(x_2 - x_2')} = \\
&= a
\end{aligned}$$

Πηγές

Βιβλιογραφία i

1. Παγουρτζής, Α., Ζάχος, Ε., ΓΠ, 2015. Υπολογιστική κρυπτογραφία. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
2. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. Chapman and Hall/CRC, 2007
3. Oded Goldreich, The Foundations of Cryptography - Volume 1, Cambridge University Press, 2001
4. Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science-Business Media, 2009.
5. Kiayias, Aggelos Cryptography primitives and protocols, UoA, 2015
6. Nigel Smart. Introduction to cryptography
7. Berry Schoenmakers. Cryptographic protocols, 2015.
8. D. Chaum and T. P. Pedersen. Wallet databases with observers. CRYPTO '92.
9. U. Feige and A. Shamir. 1990. Witness indistinguishable and witness hiding protocols. In STOC '90.
10. R. Cramer, I. Damgard, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In CRYPTO '94.
11. A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. CRYPTO '86.
12. O.Goldreich,S.Micali, and A.Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. J. ACM, 38(3):690–728, July 1991.
13. S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. STOC '85
14. Jean-Jacques Quisquater, Louis Guillou, Marie Annick, and Tom Berson. 1989. How to explain zero-knowledge protocols to your children. CRYPTO '89
15. Mike Rosulek, Zero-Knoweldge Proofs, with applications to Sudoku and Where's Waldo
16. C.P. Schnorr. Efficient signature generation by smart cards. Journal of Cryptology, 4(3):161–174, 1991
17. Online Lectures by Susan Hohenberger, Rafael Pass
18. Matthew Green, Zero knowledge proofs: An illustrated primer
19. Jeremy Kuhn Zero Knowledge Proofs — A Primer