Αποδείξεις Μηδενικής Γνώσης και εφαρμογές

Παναγιώτης Γροντάς

17/12/2019

ΕΜΠ - Κρυπτογραφία (2019-2020)

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 ($\mathcal{P}$): Θέλει να αποδείξει ότι μία συμβολοσειρά ανήκει σε μία γλώσσα
  - 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 περισσότερο

Μηδενική γνώση: Ιδιότητα που προστατεύει τον $\mathcal{P}$

Πολλές θεωρητικές και πρακτικές εφαρμογές (Βραβείο Turing 2013)

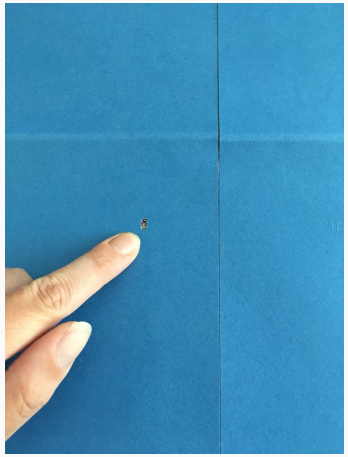
Ένα εύκολο παράδειγμα Oded Goldreich

- 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
- Μετατροπή πρωτοκόλλων με παθητική ασφάλεια σε ενεργή ασφάλεια

Συστήματα Αποδείξεων Μηδενικής Γνώσης

Διαλογικά Συστήματα Αποδείξεων

Συμβολισμός

- Γλώσσα $\mathcal{L} \in \mathtt{NP}$
- 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.

Απόδειξη: Κατασκευή Extractor $\mathcal{E}$: Ειδικός $\mathcal{V}$ που αν ολοκληρώσει το πρωτόκολλο θα βρει τον witness

Διαλογικά Συστήματα Αποδείξεων: Μηδενική Γνώση

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*

Διαλογικά Συστήματα Αποδείξεων: 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 κακόβουλο $\mathcal{P}^*$ (και οι δύο δεν διαθέτουν τον witness).

Ο $\mathcal{P}^*$

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

Ο $\mathcal{S}$

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

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

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 $\mathcal{P}_1$

Παραλλαγές Μηδενικής Γνώσης i

- **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 $\mathcal{P}, \mathcal{S}$ έχουν αμελητέα στατιστική απόσταση:

$$\Delta(X, Y) = \frac{1}{2} \sum_{u \in V} |Prob[X = u] - Prob[Y = u]| = negl(\lambda)$$

- **Computational Zero Knowledge** Οι κατανομές των συζητήσεων δεν μπορούν να διαχωριστούν από κάποιον αντίπαλο με πολυωνυμική υπολογιστική ισχύ.

Παραλλαγές Μηδενικής Γνώσης iii

- **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 ($\mathcal{P}$): 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 $\mathcal{P}$
4. Αν $b = 1$ ο $\mathcal{P}$ δημοσιοποιεί $\phi_b = \pi_1 : V_1 \to V_F$
5. Αν $b = 0$ ο $\mathcal{P}$ δημοσιοποιεί $\phi_b = \pi_1.\pi : V_0 \to V_F$ 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

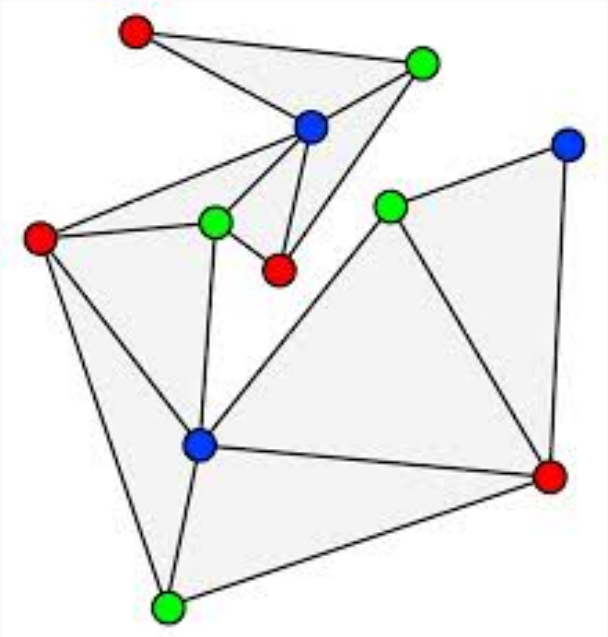
Κατασκευή simulator $\mathcal{S}$
Commitment: Επιλέγει b' και τυχαία μετάθεση π'
Υπολογίζει $F = \pi'(G_{b'})$

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

Πιθανότητα αποδοχής μετά από ακριβώς k rewinds: 2^{-k}

Αναμενόμενος χρόνος εκτέλεσης: $T_V \sum_{i=1}^{\infty} 2^{-k} = T_V$, πολυωνυμικός
(σημείωση: αναμενόμενο πλήθος rewinds $\sum_{i=1}^{\infty} k2^{-k} = 2$)

3-colorability



NP-Complete

Ορισμός

Γράφημα $G = (V, E)$

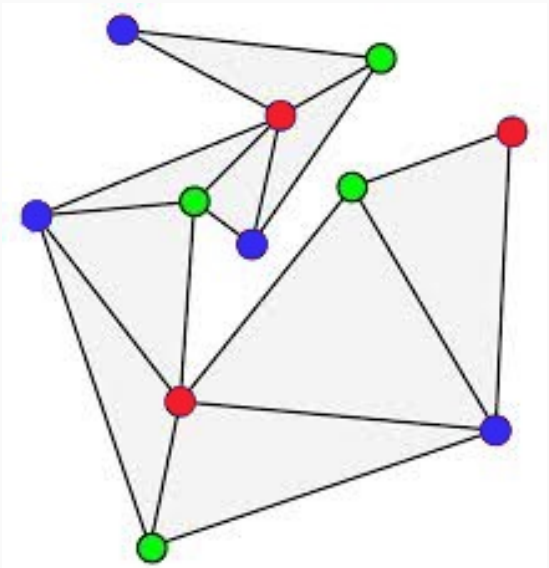
Ο $\mathcal{P}$ γνωρίζει ένα χρωματισμό

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

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. $\mathcal{P}$: 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 $|E|^2$ φορές



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 $\mathcal{V}$

ZKP for 3-colorability: Ιδιότητες (Ορθότητα)

- **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 επειδή

$$\forall x \in \mathbb{R}(1 + x) \leq e^x$$

  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)
  - Αναμενόμενο πλήθος δοκιμών για επιλογή 'καλής' ακμής: $3/2$
  - Για $|E|^2$ επιτυχημένες εκτελέσεις, αναμενόμενο συνολικό πλήθος δοκιμών: $\frac{3}{2}|E|^2$, πολυωνυμικός χρόνος

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

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

Στόχος

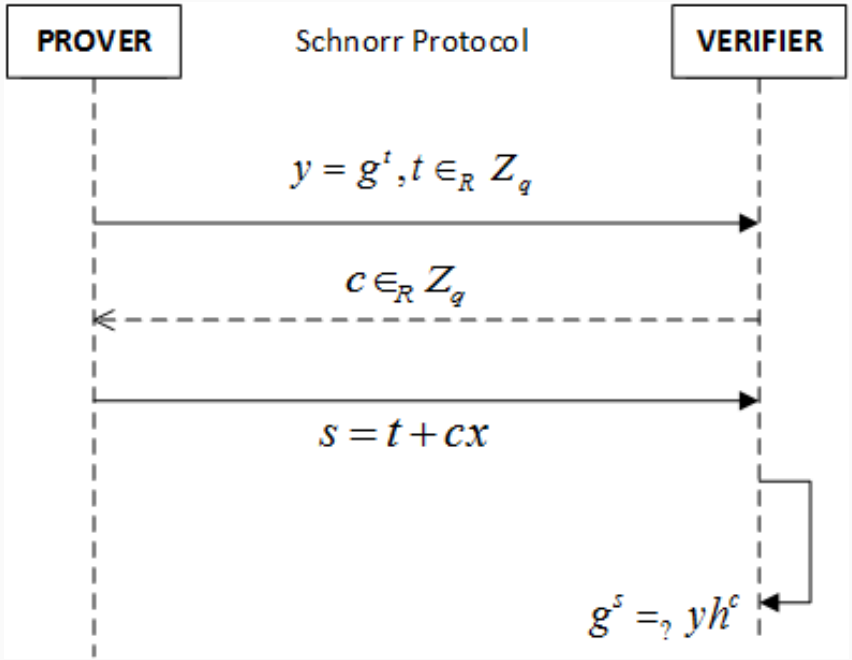
Απόδειξη κατοχής του x χωρίς να αποκαλυφθεί.

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')

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

  Αφού ο $\mathcal{P}$ 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 $\mathcal{V}$
  - 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

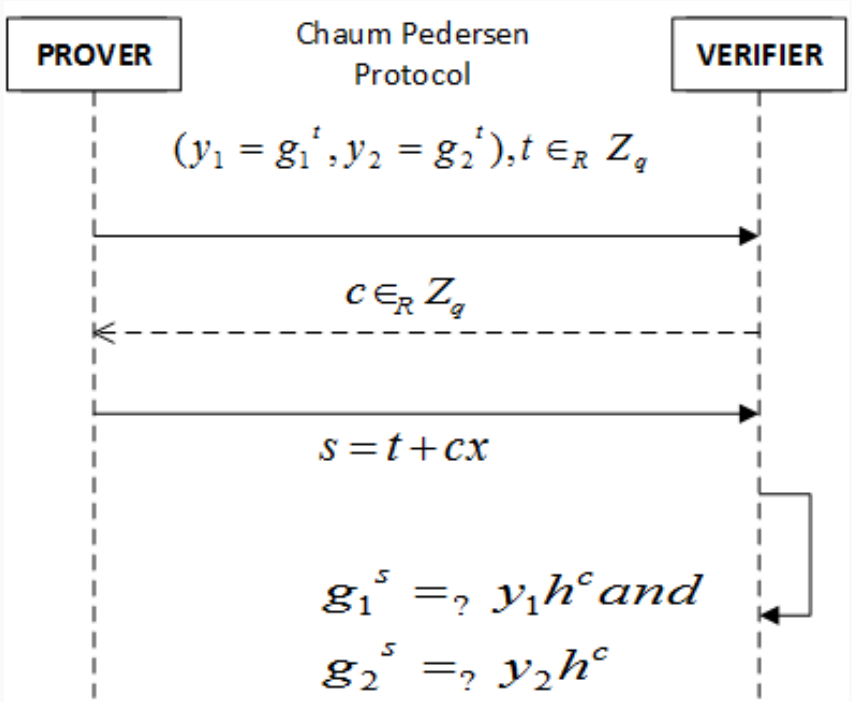
Απόδειξη γνώσης του x χωρίς να αποκαλυφθεί

Απόδειξη ισότητας διακριτών λογαρίθμων

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

Ισότητα DLOG:Το πρωτόκολλο Chaum Pedersen ii

- **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 $x = \frac{s-s'}{c'-c}$

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 (από)κρυπτογράφηση ενός (γνωστού) μηνύματος m.

Αν είναι έγκυρη τότε πρέπει

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

Ισοδύναμα:

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

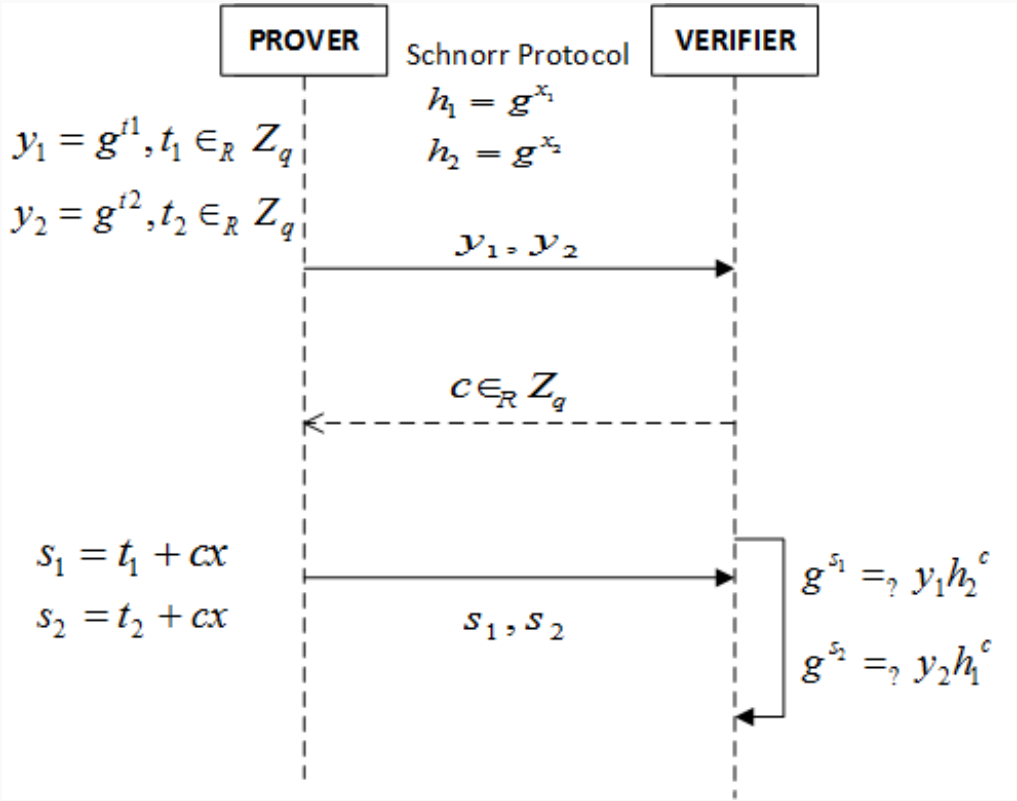
δηλ. ότι ο $\mathcal{P}$ είναι γνώστης της τυχαιότητας

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

Σύνθεση Σ πρωτοκόλλων ii



Σύνθεση Σ πρωτοκόλλων iii

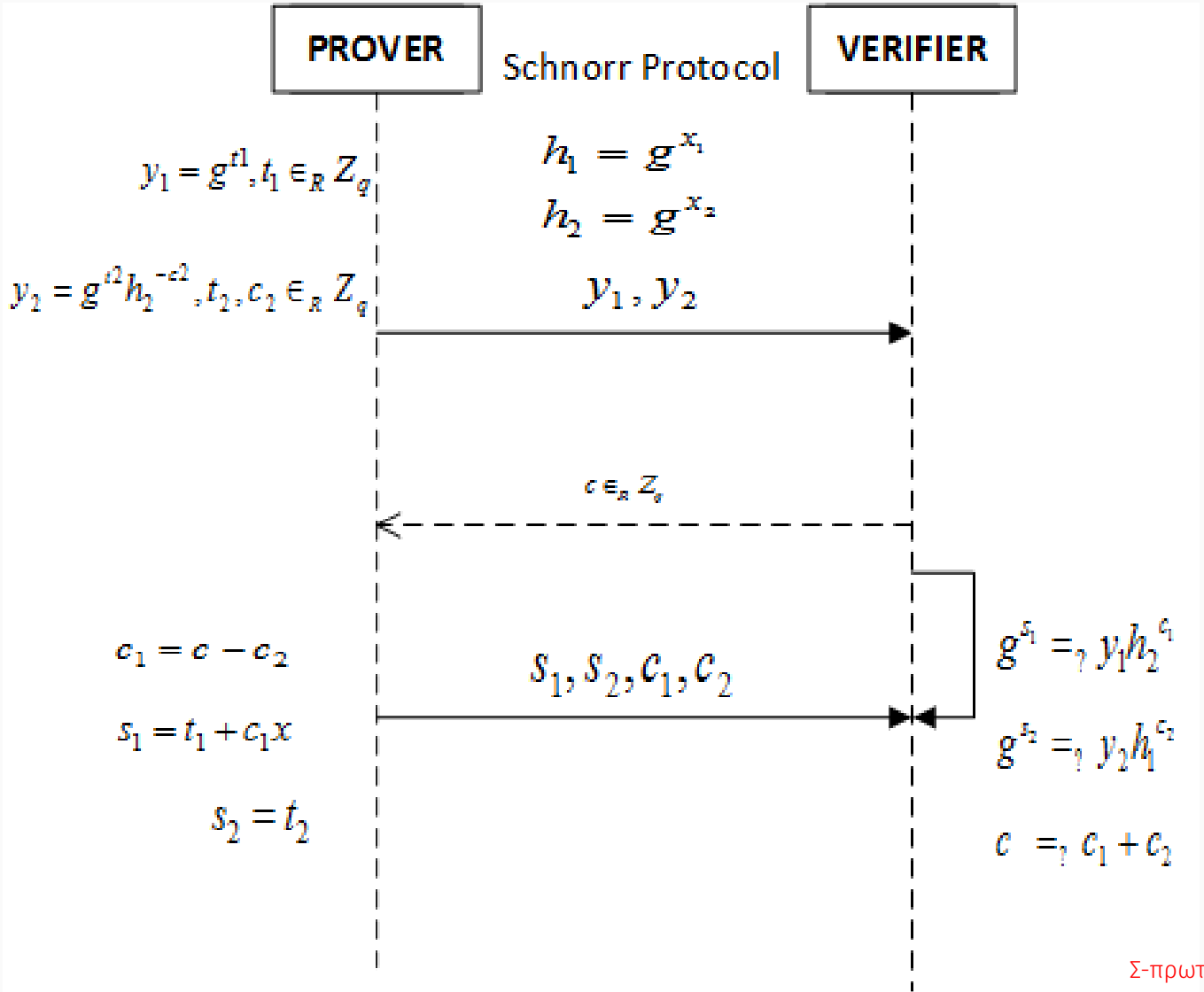
- Batch-AND
  Μαζική επαλήθευση πολλαπλών σχέσεων με ένα πρωτόκολλο. Για παράδειγμα:
  (g^a, g^b, g^{ab}) ΚΑΙ (g^c, g^d, g^{cd}) είναι τριάδες DH
  Μπορώ να εκτελέσω το Chaum Pedersen για $(g^{ac}, g^{bd}, g^{abcd})$
- EQ
  - Ο $\mathcal{P}$ γνωρίζει τον ίδιο w για διαφορετικές σχέσεις.
  - Chaum Pedersen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

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



Μη διαλογικές αποδείξεις

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) $c = \mathcal{H}(g^s h^{-c})$

Εφαρμογή: ηλεκτρονικές ψηφοφορίες

Ιδιότητες ηλεκτρονικών ψηφοφοριών

Ακεραιότητα: Το αποτέλεσμα των εκλογών πρέπει να αντανακλά τη βούληση των ψηφοφόρων

- Cast as intended
- Recorded as cast
- Tallied as recorded

Επιτυγχάνεται μέσω: *επαληθευσιμότητας*

- Ατομική (individual)
- Καθολική (universal)
- Δικαιώματος ψήφου (eligibility)
- Διαχειριστική (administrative)

Συνολικά: E2E (End To End) Verifiability

Μυστικότητα: Ο ψηφοφόρος πρέπει να εκφράσει την πραγματική του επιλογή

- Ανωνυμία - Αδυναμία σύνδεσης ψήφου - ψηφοφόρου
- Εναντίον:
  - Των καταμετρητών (privacy)
  - Άλλων ψηφοφόρων (coercion)
  - Του ίδιου του ψηφοφόρου (vote selling)
- Το ίδιο το αποτέλεσμα διαρρέει πληροφορία

Εκλογές και Υπολογιστές

- Ψηφοφορία μέσω αντιπροσώπου
- Μη έμπιστου (κακόβουλο λογισμικό, προγραμματιστικά λάθη)
- Ανοιχτό λογισμικό, μεθοδολογίες πιστοποίησης δεν επαρκούν
    - Αναγκαίες αλλά όχι ικανές συνθήκες

Software/System Independence (Rivest)

- Τα σφάλματα του συστήματος δεν πρέπει να επηρεάζουν τα αποτελέσματα
- Επαλήθευση: και αυτή μέρος του συστήματος
- VVPAT (Voter Verifiable Paper Trail)
- Κρυπτογραφία: Επαλήθευση με μαθηματικά

Κρυπτογραφία και Εκλογές: Μυστικότητα αλλά κυρίως **εμπιστοσύνη**

Συστατικά - Συμμετέχοντες

Bulletin Board

- Αποθετήριο **όλων** των δεδομένων που παράγονται σε κάθε φάση μιας ψηφοφορίας για επαληθευσιμότητα
- Πρόσβαση από όλους τους εμπλεκόμενους: Read / Append
- Θεωρητικά: Broadcast channel with memory

Οντότητες - Ρόλοι

- Ψηφοφόροι
- Registration authorities: καταχωρούν στοιχεία των ψηφοφόρων και δίνουν τα αντίστοιχα tokens
- Talliers: Εξάγουν μερικά ή πλήρη αποτελέσματα
- Verifiers: Επαλήθευση της διαδικασίας (ολόκληρης ή τμηματικά)

Ομομορφικά Συστήματα

- Οι ψήφοι:
  - κρυπτογραφούνται με το δημόσιο κλειδί των ΤΑ
  - εισάγονται στο ΒΒ
  - διατηρούνται μυστικοί καθ' όλη τη διάρκεια της διαδικασίας
- Το αποτέλεσμα υπολογίζεται στα κρυπτοκείμενα με βάση τις ομομορφικές ιδιότητες του κρυπτοσυστήματος
- Για παράδειγμα στο Lifted El Gamal:

$$\begin{aligned}\texttt{Encrypt}(v_1) \cdot \texttt{Encrypt}(v_2) = \\ (g^{r_1}, g^{v_1} \cdot y^{r_1}) \cdot (g^{r_2}, g^{v_2} \cdot y^{r_2}) = \\ (g^{r_1+r_2}, g^{v_1+v_2} \cdot y^{r_1+r_2})\end{aligned}$$

- Αποκρυπτογραφείται **μόνο** το αποτέλεσμα

Ομομορφικά Συστήματα

- Ακεραιότητα - Εγκυρότητα της ψήφου:
  Πώς επαληθεύεις μία κρυπτογραφημένη ψήφο
  Λύση: Απόδειξη μηδενικής γνώσης *(non interactive)* για την εγκυρότητα
  Κατάθεση μαζί με την ψήφο
  Επαλήθευση από όλους
- Μυστικότητα / Δικαιοσύνη
  Αποκρυπτογράφηση μεμονωμένων ψήφων - ενδιάμεσων αποτελεσμάτων
  Λύση: Threshold cryptosystems

Cramer, Genaro, Schoenmakers (CGS97)

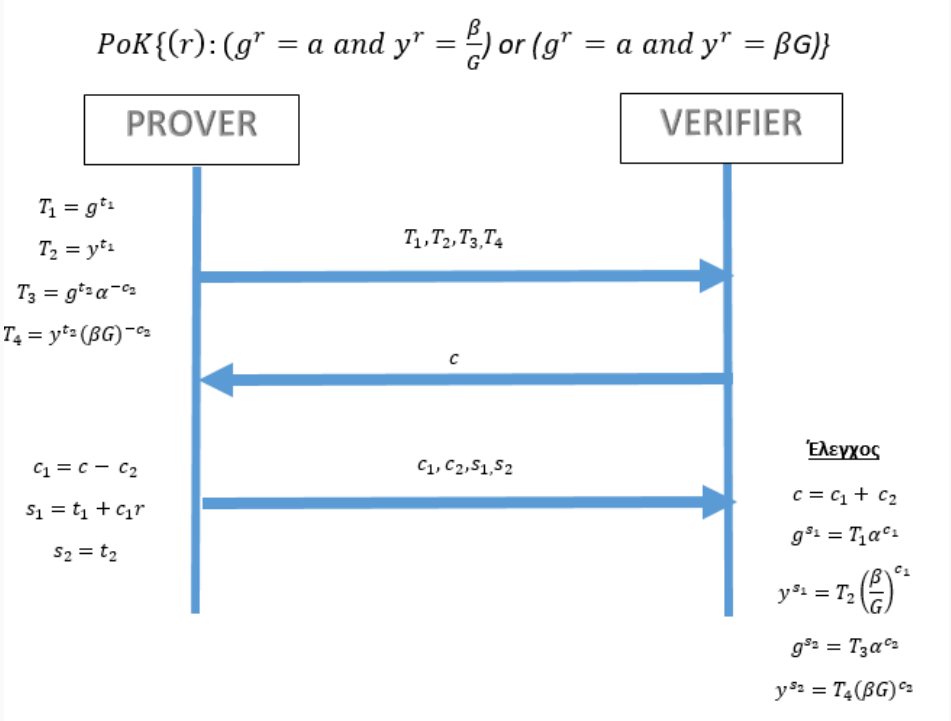
- Το βασικό πρωτόκολλο για ομομορφικά συστήματα
- Υλοποιείται στο σύστημα Helios
- Κρυπτογράφηση ψήφων με εκθετικό ElGamal
- Αποκρυπτογράφηση αποτελέσματος: Υπολογισμός *μικρού* διακριτού λογαρίθμου
- 3 αποδείξεις μηδενικής γνώσης:
  - Εγκυρότητα ψήφου
  - Γνώση ιδιωτικού κλειδιού που αντιστοιχεί σε δημόσιο (Schnorr)
  - Έγκυρη Αποκρυπτογράφηση (Chaum - Pedersen)

Cramer, Genaro, Schoenmakers (CGS97):Λεπτομέρειες

- Ψήφος $b \in \{1, -1\}$ (yes-no)
- Κρυπτογράφηση: $(g^r, G^b \cdot y^r)$
- Απόδειξη εγκυρότητας:
  - $b = 1 : (\alpha, \beta) = (g^r, G \cdot y^r) \Rightarrow log_g \alpha = log_y(\beta / G)$
  - $b = -1 : (\alpha, \beta) = (g^r, \frac{y^r}{G}) \Rightarrow log_g \alpha = log_y(\beta \cdot G)$
  - Παραλλαγή OR πρωτοκόλλου Chaum - Pedersen
- Στο BB: ψήφος με μη διαλογική απόδειξη
- Καταμέτρηση
  - Επαλήθευση αποδείξεων
  - Πολλαπλασιασμός ψηφοδελτίων με έγκυρες αποδείξεις
  - $(A, B) = (\prod_{i=1}^{n} g^{r_i}, \prod_{i=1}^{n} g^{b_i} y^{r_i})$
  - Threshold Decryption δίνει το $g^{(\#yes - \#no)}$
  - Απόδειξη ορθής αποκρυπτογράφησης (άσκηση)
  - Επίλυση μικρού διακριτού λογαρίθμου δίνει το: $(\#yes - \#no)$

Cramer, Genaro, Schoenmakers (CGS97):Η απόδειξη μηδενικής γνώσης

Έστω ότι ο ψηφοφόρος έχει ψηφίσει yes (απόδειξη για no άσκηση)



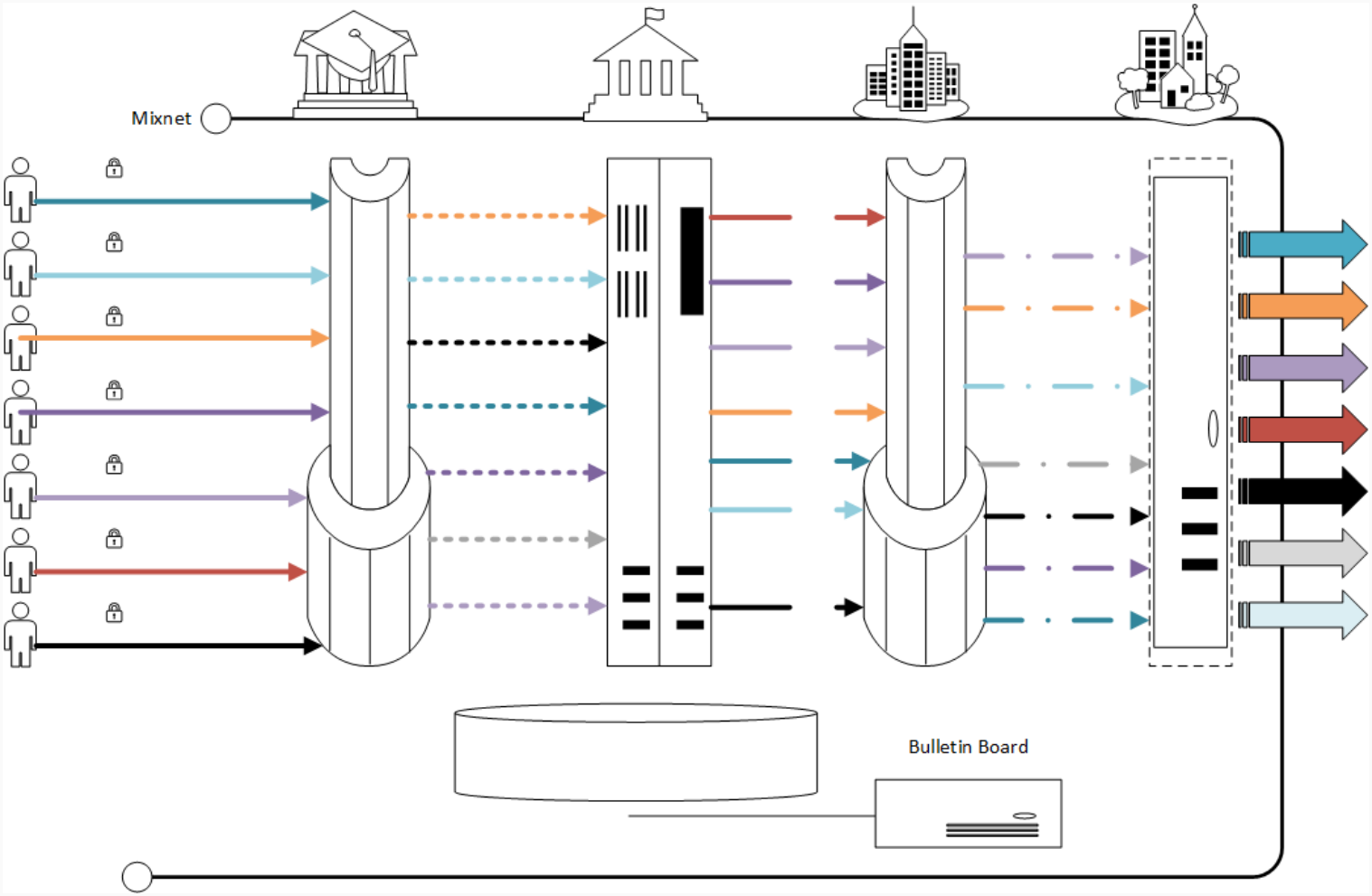
Στην πραγματικότητα: non interactive με Fiat-Shamir heuristic

Εφαρμογή: δίκτυα μίξης

Ψηφοφορίες με Δίκτυα Μίξης

- Γενικό δομικό στοιχεία για εφαρμογές ανωνυμίας
- Προτάθηκε από τον David Chaum (1981)
- Αποτελείται από ένα σύνολο από **μίκτες**. Κάθε ένας:
  - λαμβάνει ένα σύνολο από μηνύματα (BB)
  - αλλάζει τη μορφή τους
  - εφαρμόζει μια τυχαία μετάθεση
- Δύο μορφές λειτουργίας
  - Σειριακά (κάθε μίκτης σε όλα τα μηνύματα)
  - Παράλληλα (κάθε μίκτης σε ένα υποσύνολο από τα μηνύματα)
- Στις ψηφοφορίες: τα μηνύματα είναι οι ψήφοι (ανακάτεμα της κάλπης)
- BB: παρέχει είσοδο και λαμβάνει έξοδο από κάθε μίκτη

Γενική Μορφή Δίκτυου Μίξης



Decryption Mixnets (RSA)

- Κάθε μίκτης i έχει ένα ζεύγος κλειδιών RSA (pk_i, sk_i)
- Ψηφοφόρος: κρυπτογράφηση ψήφου με δημόσια κλειδιά των μικτών *σε αντίστροφη σειρά*.

$$L_0 = \{\texttt{Encrypt}_{pk_1}(\texttt{Encrypt}_{pk_2}(\cdots \texttt{Encrypt}_{pk_m}(v_i, r_i) \cdots, r_2), r_1)\}_{i=1}^{n}$$

- Μίκτης: Αλλαγή Μορφής
  - αφαιρεί ένα επίπεδο κρυπτογράφησης χρησιμοποιώντας με το ιδιωτικό του κλειδί (ξεφλούδισμα)
  - αφαιρεί την τυχαιότητα που περιέχει
  - αλλάζει την μορφή.
- Μίκτης: Ανακάτεμα
  - Επιλογή τυχαίας μετάθεσης και εφαρμογή στα μηνύματα
  - Το αποτέλεσμα γράφεται στο BB
  - Για παράδειγμα ο πρώτος μίκτης θα γράψει:

$$L_1 = \{\texttt{Encrypt}_{pk_2}(\cdots \texttt{Encrypt}_{pk_k}(v_i, r_i) \cdots, r_2)\}_{i=\pi_1^{-1}(1)}^{\pi_1^{-1}(n)}$$

Decryption Mixnets (RSA)

- Η διαδικασία επαναλαμβάνεται.
- Τελικά στην έξοδο του δικτύου μίξης:

$$L_k = \{v_i\}_{i=\pi_k^{-1} \circ \cdots \circ \pi_1^{-1}(1)}^{\pi_k^{-1} \circ \cdots \circ \pi_1^{-1}(n)}$$

- Ακολουθεί η καταμέτρηση
- Παρατηρήσεις:
  - Αρκεί ένας 'τίμιος' μίκτης απέναντι σε παθητικό αντίπαλο
  - Ο τελευταίος μίκτης έχει πρόσβαση στο plaintext
  - Το πλήθος των κρυπτογραφήσεων και το μέγεθος του κρυπτοκειμένου είναι ανάλογο του αριθμού των μικτών.

Reencryption Mixnets (ElGamal)

Ιδιότητα El Gamal: Reencryption

$$\texttt{Encrypt}(v, r_1) \cdot \texttt{Encrypt}(1, r_2) = \texttt{Encrypt}(v, r_1 + r_2)$$

Η μορφή των μηνυμάτων αλλάζει με reencryption
Δύο παραλλαγές:

- (Decryption) Reencryption και Permutation
- Λαμβάνει από το BB την είσοδο

$$L_{j-1} = \{\texttt{Encrypt}(v_i, r_{j-1,i})\}_{i=1}^{n} = \{(g^{r_{j-1,i}}, v_i \cdot y^{r_{j-1,i}})\}_{i=1}^{n}$$

- Εισάγει νέα τυχαιότητα με reencryption:

$$L'_{j-1} = \{\texttt{Encrypt}(v_i, r_{j-1,i}) \cdot \texttt{Encrypt}(1, r_{j,i})\}_{i=1}^{n} = \{(g^{r_{j-1,i}+r_{j,i}}, v_i \cdot y^{r_{j-1,i}+r_{j,i}})\}_{i=1}^{n}$$

- Εφαρμόζει μία τυχαία μετάθεση π_j
- Γράφει τα αποτελέσματα στο BB

Mixnets για ψηφοφορίες

Επαληθευσιμότητα των ενεργειών ψηφοφόρων και μικτών

- Ψηφοφόρος: Απόδειξη γνώσης της ψήφου ώστε
  - να **μην** βάλει ετικέτα σε κάποια ψήφο
  - να **μην** αντιγράψει μια ψήφο
  - … όπως στα ομομορφικά συστήματα
- Μίκτης: Απόδειξη μετάθεσης (proof of shuffle)
  - Η μετάθεση είναι έγκυρη
  - χωρίς να αλλάξει κάποια ψήφο
  - χωρίς να παραλείψει κάποια ψήφο

Παράδειγμα i

- Έισοδος:
  - $C_1 = \texttt{Encrypt}(m_1, r_1)$
  - $C_2 = \texttt{Encrypt}(m_2, r_2)$.
- Reencryption
  - $C'_1 = Reenc(C_1) = \texttt{Encrypt}(m_1, r_1 + r'_1)$
  - $C'_2 = Reenc(C_2) = \texttt{Encrypt}(m_2, r_2 + r'_2)$
- Τυχαία επιλογή bit $b \in_R \{0, 1\}$.
- Αν $b = 0$ έξοδος (C'_1, C'_2)
- Αν $b = 1$ έξοδος (C'_2, C'_1)

Παράδειγμα ii

Βήμα 1 Απόδειξη ορθότητας reencryption

Δηλαδή
Το κρυπτογράφημα $C' = (G', M') = (g^u, m' \cdot y^u)$ είναι reencryption του $C = (G, M) = (g^t, m \cdot y^t)$

Βασική ιδέα: Το C' είναι reencryption του C ανν και τα δύο κρυπτογραφούν το ίδιο μήνυμα, δηλ. $m' = m$.

Διαιρούμε τα δύο μέρη και έχουμε:

$$\frac{G'}{G} = \frac{g^u}{g^t} = g^{u-t} \text{ και } \frac{M'}{M} = \frac{m'y^u}{my^t} = y^{u-t}$$

Αρκεί νδο ότι $log_g \frac{G'}{G} = log_y \frac{M'}{M}$

Χρήση non interactive Chaum Pedersen

Παράδειγμα iii

Βήμα 2 Απόδειξη ορθότητας μετάθεσης
Πρέπει νδο $\{C'_1, C'_2\}$ είναι reencryption μια μετάθεσης του $\{C_1, C_2\}$ χωρίς να την φανερώσουμε την αντιστοιχία.

Ισοδύναμα:

$$(C'_1 = Reenc(C_1) \wedge C'_2 = Reenc(C_2)) \bigvee (C'_1 = Reenc(C_2) \wedge C'_2 = Reenc(C_1))$$

Λύση: Σύνθεση 4 πρωτοκόλλων Chaum-Pedersen

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. (link)
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