Αποδείξεις Μηδενικής Γνώσης

Παναγιώτης Γροντάς
ΕΜΠ

Κρυπτογραφία

2025 - 2026

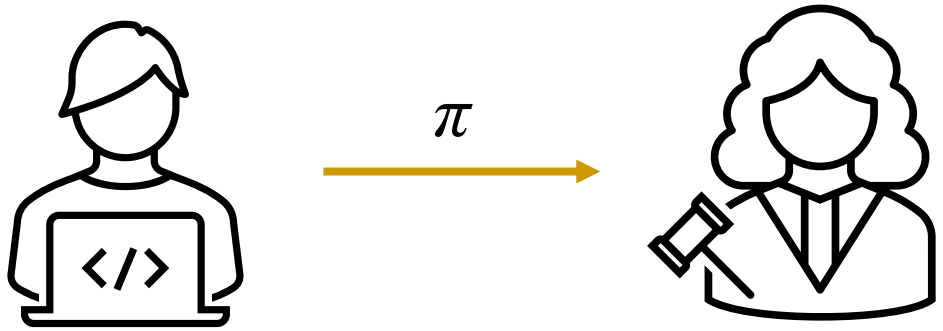
Περιεχόμενα

- Εισαγωγή
- Τυπικός Ορισμός
- Παραδείγματα από Θ. Πολυπλοκότητας
- Σ -Πρωτόκολλα

Εισαγωγή

Μαθηματικές Αποδείξεις

- Στατικά αντικείμενα
- Ντετερμινιστική Επαλήθευση
  - μόνο για αληθείς προτάσεις
- Διαρρέουν πληροφορία (για ενδιάμεσους συλλογισμούς)
- Μπορούμε να πειστούμε για την αλήθεια μιας πρότασης χωρίς διαρροή καμίας πληροφορίας;
- Πώς ορίζουμε κάτι τέτοιο τυπικά;



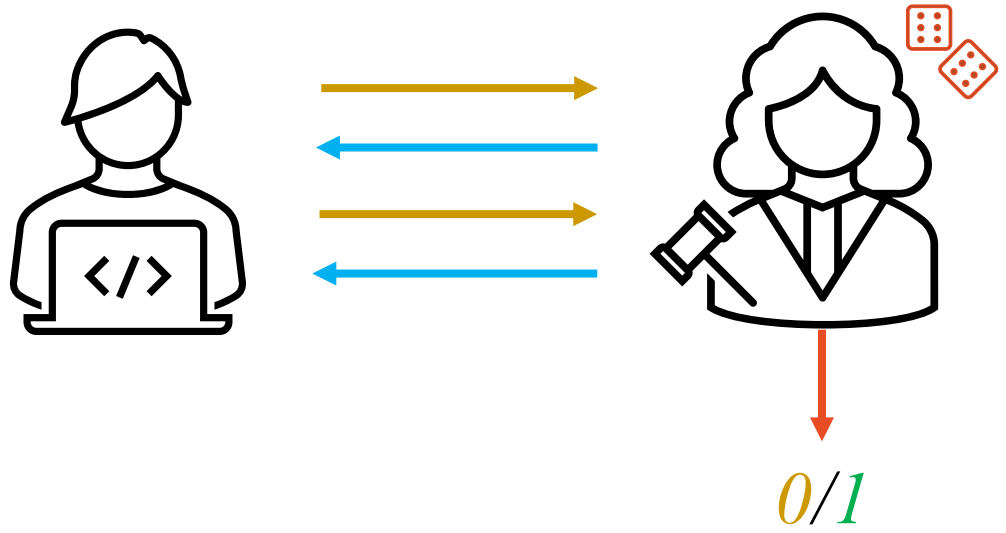
Παράδειγμα: Απόδειξη ότι ο χ **δεν** είναι πρώτος

Πώς: Αρκεί να δείξω έναν γνήσιο διαιρέτη

Διαρροή: Έμαθα ένα διαιρέτη του χ

Interactive Proof Systems (Διαλογικά Συστήματα Αποδείξεων)

- Αποδεικτική διαδικασία: Διάλογος μεταξύ δύο οντοτήτων ($\mathcal{P}$ και $\mathcal{V}$)
  - Ο $\mathcal{P}$ θέλει να αποδείξει μια πρόταση
  - Ο $\mathcal{V}$ συμμετέχει στην απόδειξη κάνοντας ερωτήσεις (ανάκριση)
  - Οι ερωτήσεις περιέχουν στοιχεία τυχαιότητας
  - **Transcript Απόδειξης:** ερωτήσεις – απαντήσεις
  - Ο $\mathcal{V}$ επαληθεύει την απόδειξη (αλλά και οποιοσδήποτε άλλος διαθέτει το transcript)
  - Ο $\mathcal{V}$ δέχεται με **(αμελητέα μικρή)** πιθανότητα λάθους.



Interactive Proof Systems
Τυπικός ορισμός

Ένα τυπικό σύστημα απόδειξης για μια γλώσσα L είναι ένα ζεύγος αλγορίθμων $(\mathcal{P}, \mathcal{V})$ όπου ο $\mathcal{V}$ είναι PPT με τις ιδιότητες:

- **Πληρότητα (completeness): κάθε αληθής πρόταση έχει επαληθεύσιμη απόδειξη**

$$x \in L, \forall\, \lambda: \Pr\left[\mathcal{V}\left(\left\langle \mathcal{P}\left(x, 1^{\lambda}\right), \mathcal{V}\left(x, 1^{\lambda}\right)\right\rangle\right) = 1\right] = 1$$

- **Ορθότητα (soundness): κάθε ψευδής πρόταση έχει επαληθεύσιμη απόδειξη με αμελητέα πιθανότητα**

$$x \notin L, \forall\, (\mathcal{P}^*, \lambda): \Pr\left[\mathcal{V}\left(\left\langle \mathcal{P}^*\left(x, 1^{\lambda}\right), \mathcal{P}\left(x, 1^{\lambda}\right)\right\rangle\right) = 1\right] \leq \mathrm{negl}(\lambda)$$

Αν και ο $\mathcal{P}^*$ είναι PPT τότε έχουμε Interactive **Argument** System

IP: το σύνολο των γλωσσών που έχουν σύστημα απόδειξης

$$NP \subseteq IP$$

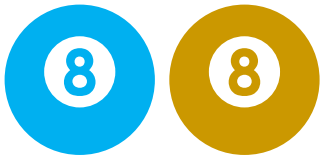
Μηδενική Γνώση (ZK)

- Ο $\mathcal{P}$ πείθει τον $\mathcal{V}$ χωρίς να διαρρέει καμία επιπλέον πληροφορία
- Shaffi Goldwasser, Silvio Micali και Charles Rackoff, 1985
- Μηδενική γνώση: Ιδιότητα που προστατεύει τον $\mathcal{P}$ από έναν κακό $\mathcal{V}^*$ που δεν θέλει απλά να επαληθεύσει την απόδειξη
- Πολλές θεωρητικές και πρακτικές εφαρμογές (*Βραβείο Turing 2013*)



S Goldwasser, S Micali, and C Rackoff. 1985. The knowledge complexity of interactive proof-systems. In Proceedings of the seventeenth annual ACM symposium on Theory of computing (STOC '85). Association for Computing Machinery, New York, NY, USA, 291–304. https://doi.org/10.1145/22145.22178

Παράδειγμα (ZK):

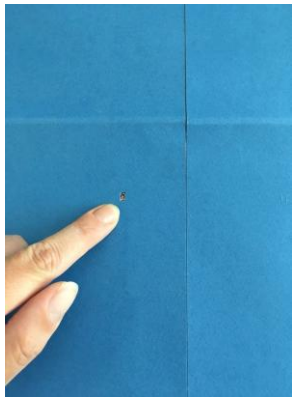


- **Commit (Δέσμευση)**
  - Ο $\mathcal{P}$ δίνει τις μπάλες στον $\mathcal{V}$
  - Ο $\mathcal{V}$ τις κρύβει πίσω από την πλάτη του μία ανά χέρι
  - Στην τύχη, αποφασίζει αν θα τις αντιμεταθέσει ή όχι
- **Challenge (Πρόκληση)**
  - Ο $\mathcal{V}$ παρουσιάζει τα χέρια στον $\mathcal{P}$
- **Response (Απάντηση)**
  - Ο $\mathcal{P}$ αποκρίνεται αν άλλαξαν χέρια ή όχι.
- **Verification (Επαλήθευση)**
  - Ο $\mathcal{V}$ αποδέχεται ή όχι.

- **Πληρότητα:** προφανής
- Ορθότητα:
  - Ο $\mathcal{P}^*$ έχει δύο μπάλες ίδιου χρώματος
  - Μπορεί να απαντήσει σωστά με πιθανότητα επιτυχίας $\frac{1}{2}$
  - Επανάληψη
    - Θα πρέπει να μαντέψει σωστά **κάθε** φορά
    - k επαναλήψεις $\frac{1}{2^k}$
- Μηδενική Γνώση: Αχρωματοψία
  - Το χρώμα δεν αλλάζει την όψη του πρωτοκόλλου για τον $\mathcal{V}$

https://www.wisdom.weizmann.ac.il/~/oded/poster03.html

Άλλα παραδείγματα ZK



https://www.wisdom.weizmann.ac.il/~naor/PAPERS/waldo_abs.html

https://pages.cs.wisc.edu/~mkowalcz/628.pdf

www.wisdom.weizmann.ac.il/~naor/PAPERS/sudoku_abs.htmles

Κρυπτογραφικές Εφαρμογές

Πρωτόκολλα ταυτοποίησης

- Αποφυγή μετάδοσης και αποθήκευσης
- Αντί για password
  - Απόδειξη γνώσης του

Ψηφιακές Υπογραφές

- Απόδειξη γνώσης ιδιωτικού κλειδιού

Anti – malleability

- Απόδειξη γνώσης κρυπτογραφημένου μηνύματος
- Αν το μήνυμα αλλάξει, δεν θα ισχύει

- **Απόδειξη** ότι ένα κρυπτογραφημένο μήνυμα εμπίπτει σε μια κατηγορία αποδεκτών μηνυμάτων (π.χ. ηλεκτρονικές ψηφοφορίες)
- **Απόδειξη** ότι κάποιος υπολογισμός σε ιδιωτικά δεδομένα έγινε σωστά.
- **Γενικά**, απόδειξη ότι οι παίκτες ακολουθούν ένα πρωτόκολλο χωρίς να αποκαλυφθούν ιδιωτικά δεδομένα.

Ορισμοί

Witness

- Witness w:
  - Μυστική είσοδος του $\mathcal{P}$ η οποία αποδεικνύει ότι $x \in L$
- Παράδειγμα:
  - L: το πρόβλημα του διακριτού λογαρίθμου (DLP) σε κυκλική ομάδα $\mathbb{G}$
  - $x = \{(g, q, Y) \mid \langle g \rangle = \mathbb{G}, , ord(\mathbb{G}) = q, \ Y \xleftarrow{\$} \mathbb{G}\}$
  - $w \in \mathbb{Z}_q$: $g^w = Y$
- **Trivial γλώσσα**: Για κάθε στοιχείο της $\mathbb{G}$ υπάρχει witness (διακριτός λογάριθμος) (αφού g γεννήτορας)

Τυπικός ορισμός συστημάτων ZK

- Έστω $L \in NP$ μια γλώσσα και R μια σχέση: $x \in L \Leftrightarrow (x, w) \in R$
- Μία απόδειξη μηδενικής γνώσης witness w ότι $x \in L$ είναι το transcript $\langle \mathcal{P}(x, w), \mathcal{V}(x) \rangle$ που παράγεται από ένα ζεύγος αλγορίθμων $(\mathcal{P}, \mathcal{V})$ όπου ο V PPT:
- **Πληρότητα (completeness):**
  - Ο τίμιος $\mathcal{P}$, πείθει έναν τίμιο $\mathcal{V}$ με βεβαιότητα
  - $x \in L: \Pr[\mathcal{V}(\langle \mathcal{P}(x, w), \mathcal{V}(x) \rangle) = 1] = 1$
- **Ορθότητα (soundness):**
  - Κανένας κακόβουλος $\mathcal{P}^*$ δεν μπορεί να πείσει τίμιο $\mathcal{V}$, παρά με αμελητέα πιθανότητα.
  - $x \notin L, \forall\, \mathcal{P}^*: \Pr[V(\langle \mathcal{P}^*(x), \mathcal{V}(x) \rangle) = 1] \leq \mathrm{negl}(\lambda)$

Knowledge Soundness – Proof of Knowledge (PoK)

- Η ορθότητα δεν είναι αρκετή
  - απόδειξη ύπαρξης w και όχι γνώσης w
- Πολλές φορές θέλουμε απόδειξη γνώσης w
  - Π.χ. σε trivial γλώσσες όπως το DLP
  - Για χρήση σε πρακτικές εφαρμογές

Απόδειξη Γνώσης:

Αν ο $\mathcal{P}$ πείσει έναν $\mathcal{V}$ να αποδεχθεί την απόδειξή με μη αμελητέα πιθανότητα τότε:

- Ο $\mathcal{P}$ ξέρει **συγκεκριμένο** witness, δηλ:
- Υπάρχει PPT αλγόριθμος $\mathcal{E}$, που:
  - εάν του δοθεί η δυνατότητα να αλληλεπιδρά επανειλημμένα με τον $\mathcal{P}$ μπορεί να εξάγει τον witness του $\mathcal{P}$.

Knowledge Soundness – Proof of Knowledge (PoK)

Το $\langle \mathcal{P}(x, w), \mathcal{V}(x) \rangle$ είναι **απόδειξη γνώσης (PoK)** για την L αν:

- $\forall\ \mathcal{P}^*, \exists$ expected **PPT knowledge extractor** $\mathcal{E}$ για $\boldsymbol{x} \in \{\mathbf{0}, \mathbf{1}\}^*$**:**
- $\{\langle \mathcal{P}^*(\mathrm{x}), \mathcal{V}(\mathrm{x}) \rangle\} = (\approx)\{\mathcal{E}^{\mathcal{P}^*}(x)\}$
- $\Pr\left[\ \mathcal{V}(\pi, x) = 1 \text{ AND } (x, w) \notin R \ | (\pi, w) \leftarrow \mathcal{E}^{\mathcal{P}^*}(x)\ \right] \leq \mathrm{negl}(\lambda)$

Ο extractor έχει oracle access στον $\mathcal{P}^*$. Μπορεί δηλαδή να κάνει ερωτήματα, να λαμβάνει απαντήσεις σε μορφή black – box.

Δεν υπάρχει αποδεκτό transcript το οποίο να μην αντιστοιχεί σε κάποιο witness

$=$ **Perfect** Knowledge Soundness
$\approx$ **Computational** Knowledge Soundness

Μηδενική Γνώση (Διαίσθηση)

- **Πώς** μπορούμε να ορίσουμε ότι 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 **χωρίς** την συζήτηση με τον $\mathcal{P}$.
  - Ο $\mathcal{V}$ δεν κέρδισε τίποτα από την συζήτηση
    - (π.χ. δεν έμαθε κάποιον διακριτό λογάριθμο)

Ισοδύναμα: Ό,τι μπορεί να υπολογίσει ο $\mathcal{V}$ από **την συζήτηση με τον $\mathcal{P}$**, μπορεί να το υπολογίσει από **από μια συζήτηση με PPT αλγόριθμο $\mathcal{S}$** που δεν διαθέτει τον witness.

Άρα: η συζήτηση με τον $\mathcal{P}$ προσθέτει μηδενική γνώση

Παρατήρηση: ο $\mathcal{V}$ είναι κακόβουλος ($\mathcal{V}^*$)

- Δεν αρκείται στην επαλήθευση
- Προσπαθεί επιπλέον να μάθει τον witness
- Συμπεριφέρεται αυθαίρετα

Μηδενική Γνώση (Ορισμός)

- Το $\langle \mathcal{P}(\mathrm{x}, \mathrm{w}), \mathcal{V}(\mathrm{x}) \rangle$ παρέχει **τέλεια μηδενική γνώση** αν:
  - $\forall PPT\ \mathcal{V}^*, \exists$ **expected** PPT simulator $\mathcal{S}$:
    - $\{\langle \mathcal{P}(x, w), \mathcal{V}^*(x) \rangle\} = \{\mathcal{S}^{\mathcal{V}^*}(x)\}$ για $\boldsymbol{x \in L}$
  - Οι συζητήσεις $\langle \mathcal{P}, \mathcal{V} \rangle$ και η έξοδος του S ακολουθούν **ίδια** κατανομή
- **Υπολογιστική μηδενική γνώση**:
  - $\{\langle \mathcal{P}(x, w), \mathcal{V}^*(x) \rangle\} \approx \{\mathcal{S}^{\mathcal{V}^*}(x)\}$ για $\boldsymbol{x \in L}$
  - Οι κατανομές των συζητήσεων $\langle \mathcal{P}, \mathcal{V} \rangle$ και εξόδου $\mathcal{S}$ δεν μπορούν να διαχωριστούν αποδοτικά

Συζήτηση

- Μπορεί να είναι ένα πρωτόκολλο **ταυτόχρονα και PoK και ZK**?
  - Ο $\mathcal{E}$ φαίνεται να παραβιάζει την μηδενική γνώση (παραγωγή witness)
  - Ο $\mathcal{S}$ φαίνεται να παραβιάζει την ορθότητα (αποδοχή χωρίς witness)
- **Ναι**, γιατί:
  - Ορθότητα: $\boldsymbol{x} \in \{\mathbf{0},\mathbf{1}\}^*$ **(μπορεί να μην υπάρχει witness - extractor)**
  - Μηδενική γνώση: $\boldsymbol{x} \in \boldsymbol{L}$ **(υπάρχει ορθότητα)**
  - Δεν κάνει extract τον witness ο $\mathcal{V}$ αλλά ο $\mathcal{E}$:
    - Αν υπάρχει ο witness, **ο $\mathcal{E}$ συμπεριφέρεται διαφορετικά από τον V**
    - Ο $\mathcal{E}$ έχει *oracle access* στον $\mathcal{P}^*$:
      - Δυνατότητα **Rewind**, αν δεν μπορεί να υπάρξει απάντηση σε κάποιο ερώτημα
      - Ο $\mathcal{V}$ δεν έχει αυτή τη δυνατότητα

Rewind (για ZK simulation)

- **Τα ίδια ισχύουν και για τον Simulator**
- Αν κάποια στιγμή ο $\mathcal{V}^*$ ρωτήσει κάτι που ο $\mathcal{S}$ δεν μπορεί να απαντήσει:
  - Ο $\mathcal{S}$ σταματά τον $\mathcal{V}^*$
  - Τον επαναφέρει πριν την ερώτηση
  - Προσπαθεί να απαντήσει ξανά
  - Αν όχι, επανάληψη κόκ
  - Πρέπει ο $\mathcal{S}$ να παραμείνει PPT.
- **Διαίσθηση**:
  - Μπορούμε να βλέπουμε τον $\mathcal{V}^*$ ως μια virtual machine που επαναφέρουμε σε προηγούμενο snapshot.
  - Ή και ως ένα παιχνίδι που κάνουμε save πριν μια δύσκολη μάχη.

Honest Verifier Zero Knowledge (HVZK)

- Ο $\mathcal{V}^*$ είναι τίμιος (κακός αλλά τίμιος)
  - Προσπαθεί μεν να μάθει το w, αλλά
  - **Ακολουθεί το πρωτόκολλο**
  - **Επιλέγει τα challenges ομοιόμορφα και ανεξάρτητα από τα μηνύματα του prover**
- Το simulation είναι πιο εύκολο
  - Στο rewind θα γίνει η ίδια ερώτηση
- **Χρησιμότητα:**
  - Μπορούμε να παραλείψουμε τον $\mathcal{V}$
  - Non-Interactive Zero Knowledge **(NIZK)**

Ειδική ορθότητα

- Ο knowledge extractor $\mathcal{E}$ δουλεύει ως εξής:
  - Μετά το challenge κάνει rewind τον $\mathcal{P}$ αμέσως μετά το commitment
  - Στέλνει ένα διαφορετικό challenge
  - Άρα έχει δύο απαντήσεις για το ίδιο commitment με διαφορετικά challenges
  - Extract τον witness

ΘΕΩΡΗΜΑ

Ειδική ορθότητα ⇒ Ορθότητα με πιθανότητα false positive $\frac{1}{|C|}$

όπου C είναι το challenge set

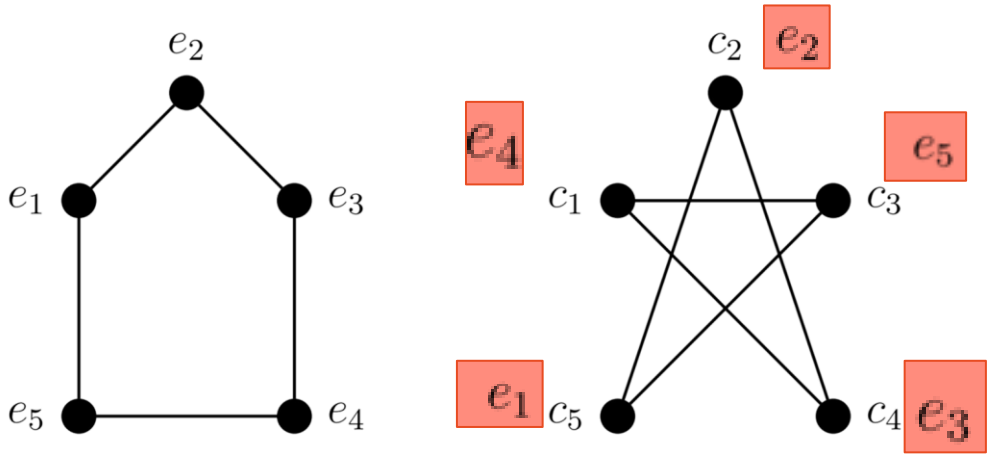
Witness Hiding/Indistinguishable ZK

- **Witness Hiding ZK**
  - Δεν μπορώ να μάθω ολόκληρο τον witness
  - Αλλά μπορώ να μάθω το 99%
- **Witness Indistinguishable ZK**
  - Δεν μπορώ να προσδιορίσω ποιος από εναλλακτικούς witnesses χρησιμοποιήθηκε

Παραδείγματα

ZK για Ισομορφισμό Γραφημάτων

- Ισομορφικά Γραφήματα
- $G_0 = (V_0, E_0), G_1 = (V_1, E_1)$ με $|V_0| = |V_1|$
- $G_0 \cong G_1 \Leftrightarrow \exists\, \varphi: V_0 \to V_1$ ώστε $(v_i, v_j) \in E_0 \Leftrightarrow (\varphi(v_i), \varphi(v_j)) \in E_1$



ZK για Ισομορφισμό Γραφημάτων

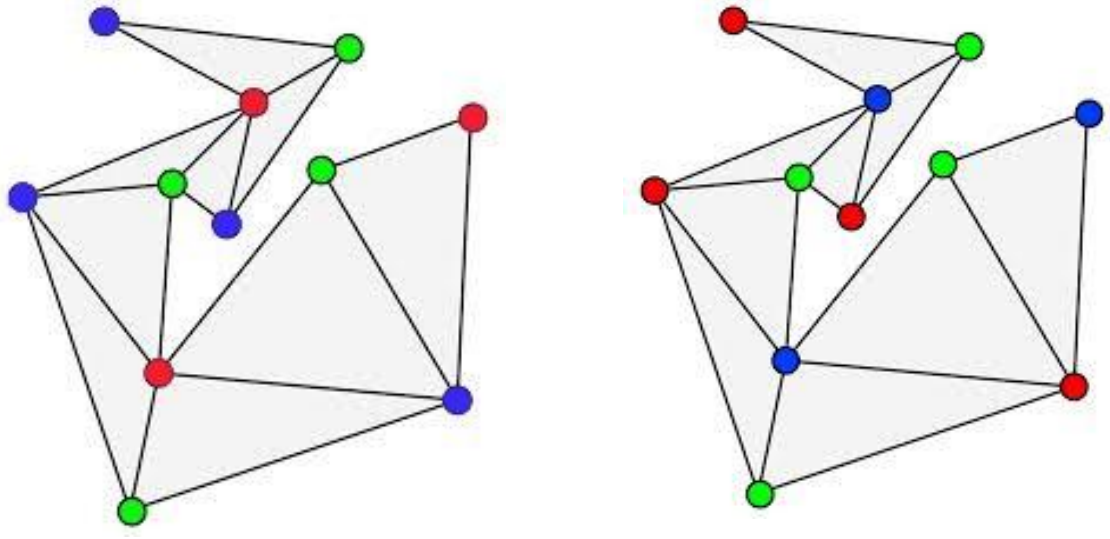
- Το πρωτόκολλο
  - Δημόσια Είσοδος G_0, G_1
  - Witness φ
- **Commit $(\mathcal{P})$**
  - Επιλογή τυχαίας μετάθεσης
    - $\psi: V_1 \to V_1$
  - $F = \psi(V_1)$
  - Αποστολή F στον $\mathcal{V}$
- **Challenge $(\mathcal{V})$**
  - Αποστολή $b \xleftarrow{\$} \{0,1\}$
- **Response $(\mathcal{P})$**
  - Αν $b = 1$ αποστολή $\chi = \psi$
  - Αν $b = 0$ αποστολή $\chi = \psi.\varphi$
- **Επαλήθευση**
  - Αποδοχή ανν $\chi(G_b) = F$
- **Επανάληψη k φορές**

ZK για Ισομορφισμό Γραφημάτων

- Πληρότητα
  1. Αν $b = 1$ όντως $\chi(G_1) = \psi(G_1) = F$
  2. Αν $b = 0$ όντως $\chi(G_1) = (\psi.\varphi)(G_0) = \psi(G_1) = F$
- Ορθότητα (κλασικός ορισμός)
  1. Αν $\nexists\varphi$: $\boldsymbol{G_0} \cong \boldsymbol{G_1}$ τότε $\Pr[\mathcal{V}(F,\chi) = 1] = \frac{1}{2}$ (μπορεί να απαντήσει για $b = 1$)
  2. Σε $k = \text{poly}(n)$ επαναλήψεις $\Pr[\mathcal{V}(F,\chi)^k = 1^k] = 2^{-\text{poly}(n)}$
- Μηδενική Γνώση - Κατασκευή $\mathcal{S}$
  1. **Commit:** Επιλογή $b' \xleftarrow{\$} \{0,1\}$ και τυχαίας μετάθεσης $\boldsymbol{\psi'}$. Υπολογισμός $\boldsymbol{\psi'(G_{b'}) = F'}$
  2. **Κλήση** $\mathcal{V}(\boldsymbol{F'}) \rightarrow \boldsymbol{b}$
  3. **Response:** Αν $b = b'$ κλήση $\mathcal{V}(F', \chi')$ αλλιώς rewind πριν την κλήση
  4. Αναμενόμενος χρόνος εκτέλεσης $\mathcal{S}$: διπλάσιος του $\mathcal{P}$

ZK για 3-colorability

- Δίνεται γράφημα $\boldsymbol{G = (V, E)}$ και $\boldsymbol{c: V \rightarrow \{1, 2, 3\}}$
- Έγκυρος χρωματισμός: $\boldsymbol{(v_i, v_j) \in E \Rightarrow c(v_i) \neq c(v_j)}$
  - Γειτονικές κορυφές έχουν διαφορετικό χρώμα
- Ύπαρξη c: πρόβλημα NP-complete



ZK για 3-colorability

- Το πρωτόκολλο
  - Δημόσια Είσοδος $G = (V, E)$
  - Witness c (έγκυρος 3-χρωματισμός)
- Commit $(\mathcal{P})$
  - Επιλογή τυχαίας μετάθεσης $\psi: \{1,2,3\} \to \{1,2,3\}$
  - Νέος χρωματισμός $\psi.c$
  - Δέσμευση στον $\psi.c$
    - $\forall v_i \in V: com_i = \mathbf{commit}(\psi.c(v_i), r_i)$
  - Αποστολή δεσμεύσεων στον V
- Challenge $(\mathcal{V})$
  - $(v_i, v_j) \overset{\$}{\leftarrow} E$
- Response $(\mathcal{P})$
  - Αποκάλυψη $\psi.c(v_i), \mathrm{r_i}, \psi.c(v_j), \mathrm{r_j}$
- Επαλήθευση
  - Αποδοχή ανν $\psi.c(v_i) \neq \psi.c(v_j)$ και οι δεσμεύσεις επαληθεύονται
- Επανάληψη k φορές

ZK για 3-colorability

- Πληρότητα
  1. Αν c είναι έγκυρος 3-χρωματισμός και $\psi.c$ έγκυρος 3-χρωματισμός.
  2. Όλες οι δεσμεύσεις θα επαληθευτούν
- Ορθότητα (κλασικός ορισμός)
  1. Αν c δεν είναι έγκυρος 3-χρωματισμός τότε υπάρχουν τουλάχιστον δύο γειτονικές κορυφές με το ίδιο χρώμα
  2. Πιθανότητα επιλογής τους = $1/|E|$ (= Πιθανότητα ανίχνευσης εξαπάτησης από $\mathcal{P}^*$)
  3. Πιθανότητα επιτυχούς εξαπάτησης από $\mathcal{P}^* = 1 - 1/|E|$
  4. Με $|E||V|$ επαναλήψεις:
     - Πιθανότητα επιτυχίας του $\mathcal{P}^* = \left(1 - 1/|E|\right)^{|E||V|} \leq e^{-|V|}$ αφού $\left(1 + \frac{t}{n}\right)^n \leq e^t$
     - Αμελητέα στο μέγεθος του γραφήματος

ZK για 3-colorability

- Μηδενική γνώση - Κατασκευή $\mathcal{S}$
  1. **Commit:**
     - Επιλογή $e_i \leftarrow_{\$} E$ και χρωματισμός κορυφών με διαφορετικό χρώμα
     - Στις υπόλοιπες ακμές οι κορυφές χρωματίζονται με το ίδιο χρώμα
     - Δέσμευση στον χρωματισμό – Αποστολή Δεσμεύσεων
  2. Κλήση $\mathcal{V}(G, \{com_i\}) \rightarrow e_j$
  3. **Response:**
     1. Αν $e_i = e_j$ τότε αποκάλυψη χρωμάτων
     2. Αν $e_i \neq e_j$ τότε rewind
     3. Αναμενόμενος αριθμός επαναλήψεων για επιτυχία: $|E|$

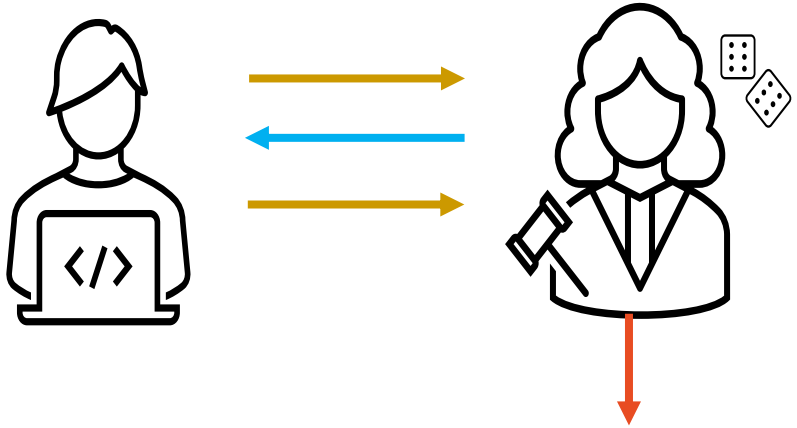
ZK για 3-colorability

- Είναι πανομοιότυπες οι συζητήσεις
- ΟΧΙ!
  - Οι δεσμεύσεις του P αντιστοιχούν σε έγκυρο χρωματισμό
  - Οι δεσμεύσεις του S αντιστοιχούν σε μη έγκυρο χρωματισμό
- Η ιδιότητα ZK εξαρτάται από το πόσο καλά 'κρύβουν' τα commitments τον χρωματισμό
- Επίσης 3-colorability είναι NP-Complete.
- **Συμπέρασμα:** Αν υπάρχουν ασφαλή σχήματα δέσμευσης τότε όλο το NP έχει αποδείξεις μηδενικής γνώσης

Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. J. ACM, 38(3), 1991.

Σ-πρωτόκολλα

Σ-πρωτόκολλα



- **Ένα πρωτόκολλο 3 γύρων με <u>ειδική ορθότητα</u> και <u>honest verifier</u>**
- **Commit**
  - Ο $\mathcal{P}$ δεσμεύεται σε μία τιμή
- **Challenge**
  - Ο $\mathcal{V}$ διαλέγει μία τυχαία πρόκληση.
  - Εφόσον είναι τίμιος θεωρούμε ότι η πιθανότητα επιλογής πρόκλησης είναι ομοιόμορφα κατανεμημένη.
- **Response**
  - Ο $\mathcal{P}$ απαντάει χρησιμοποιώντας τη δέσμευση, το μυστικό και την τυχαία τιμή

Το πρωτόκολλο του Schnorr

- **Απόδειξη Γνώσης Διακριτού Λογαρίθμου**

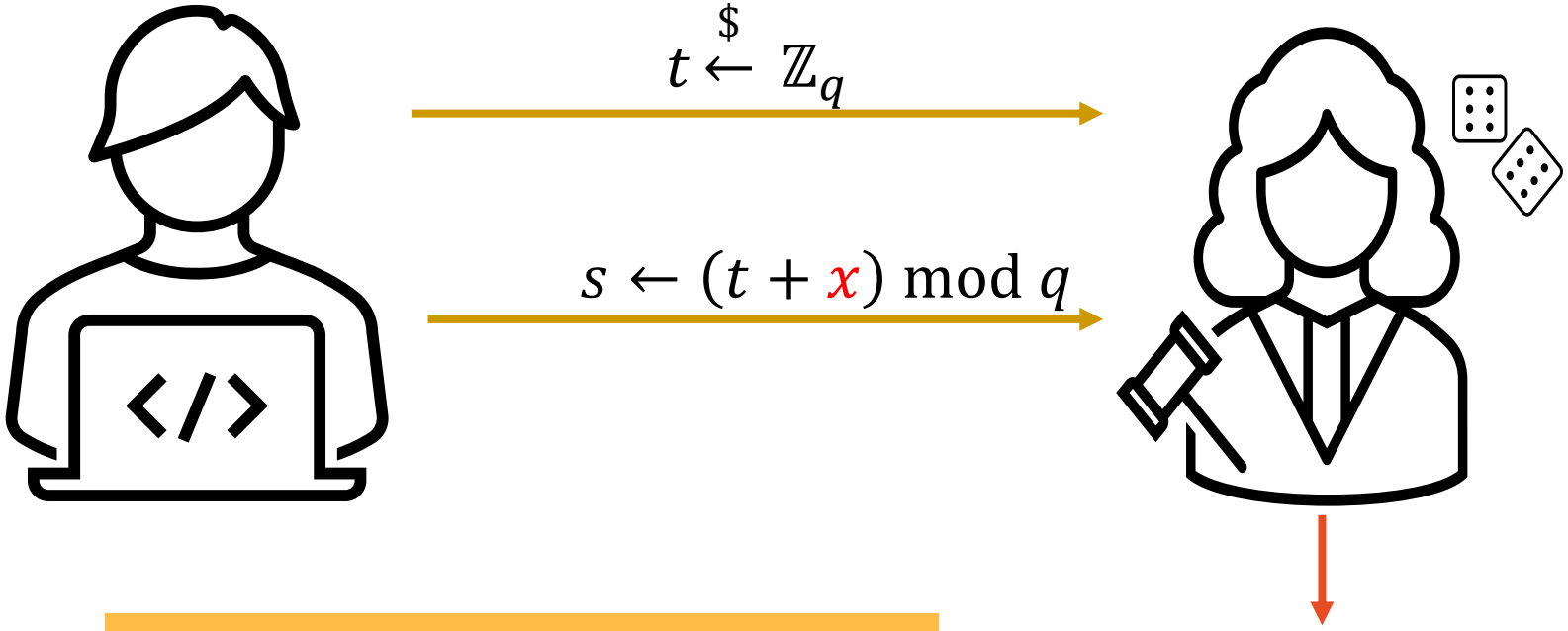
$$PoK\{x: g^x = Y, Y, g \in \mathbb{G}\}$$

- **Δημόσια είσοδος**
  - $\mathbb{G}$ είναι κυκλική ομάδα τάξης πρώτου q με γεννήτορα g
  - Στοιχείο $Y \in \mathbb{G}$
- **Witness**
  - $x \in \mathbb{Z}_q$

Schnorr, C. P. (1990). "Efficient Identification and Signatures for Smart Cards". In Gilles Brassard (ed.). *Advances in Cryptology*. Conference on the Theory and Application of Cryptographic Techniques. Proceedings of CRYPTO '89. Lecture Notes in Computer Science. Vol. 435. pp. 239–252.

Το πρωτόκολλο του Schnorr – Αποτυχημένη Πρόταση 1

$$PoK\{x: g^x = Y, Y, g \in \mathbb{G}\}$$

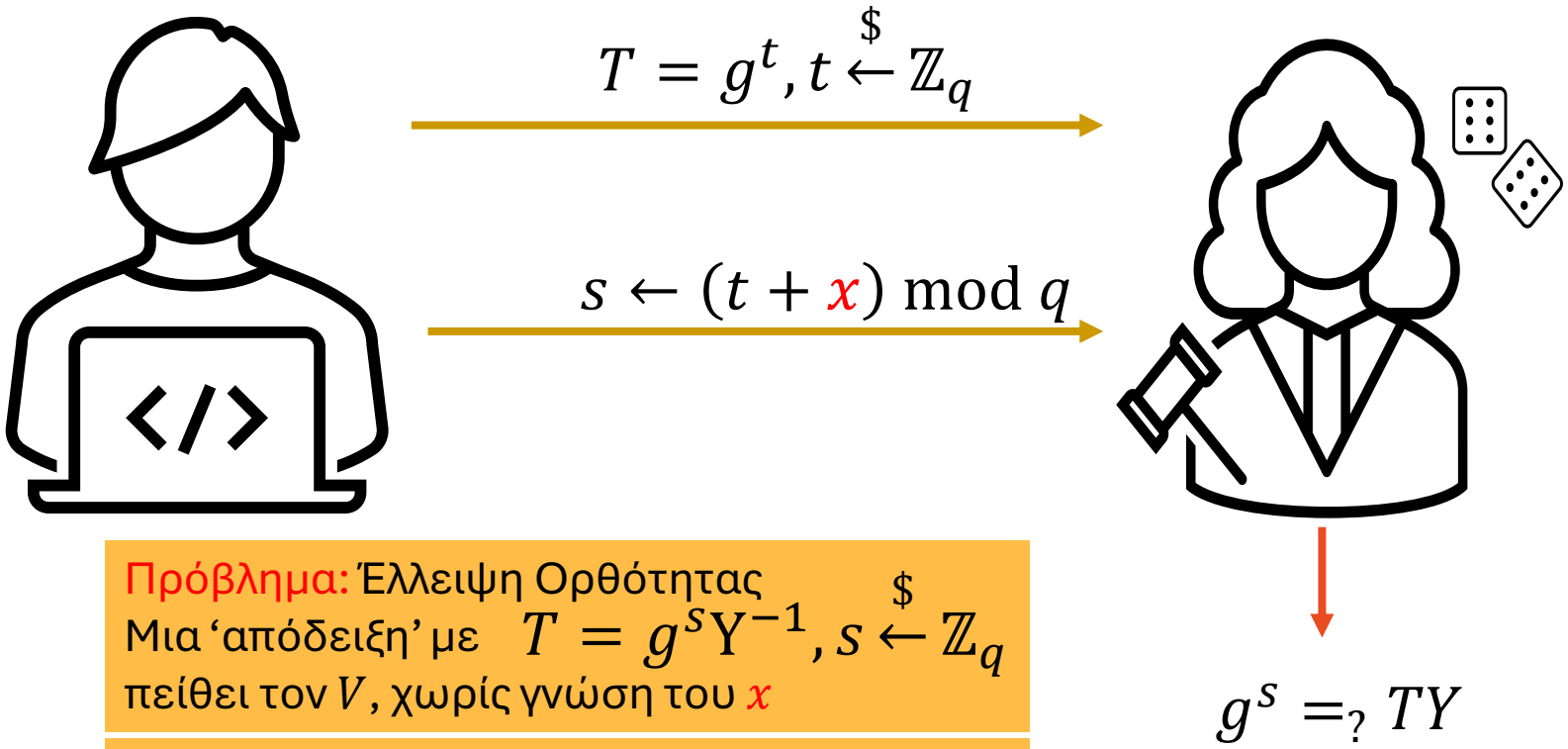


Πρόβλημα: Έλλειψη Μηδενικής Γνώσης

$x = (s - t) \bmod q$ t

Το πρωτόκολλο του Schnorr – Αποτυχημένη Πρόταση 2

$$PoK\{x: g^x = Y, Y, g \in \mathbb{G}\}$$

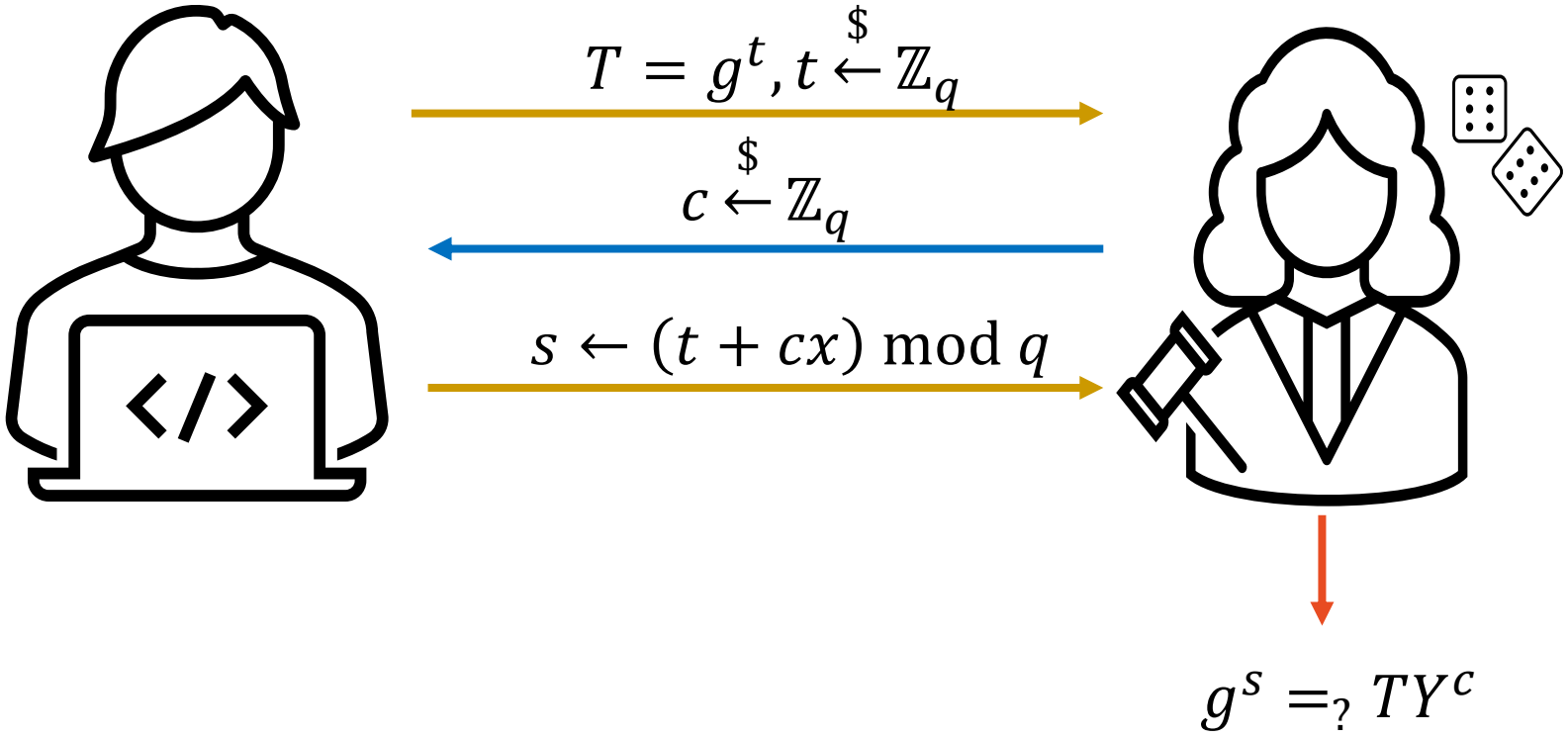


Πρόβλημα: Έλλειψη Ορθότητας
Μια 'απόδειξη' με $T = g^s Y^{-1}, s \xleftarrow{\$} \mathbb{Z}_q$ πείθει τον V, χωρίς γνώση του x

Λύση: Χρειάζεται και η συμμετοχή του V

Το πρωτόκολλο του Schnorr

$$PoK\{x: g^x = Y, Y, g \in \mathbb{G}\}$$



Διαίσθηση

- Το μυστικό είναι η κλίση της ευθείας $y = ax + b$
- Υπάρχει σε ‘κρυμμένη’ μορφή $\boxed{\alpha}$
- Σε κάθε εκτέλεση του πρωτοκόλλου ο $\mathcal{P}$ επιλέγει νέο b - νέα ευθεία
- Το στέλνει σε ‘κρυμμένη’ μορφή $\boxed{b}$
- Ο $\mathcal{V}$ έχει την ευθεία σε ‘κρυμμένη’ μορφή
- Ο $\mathcal{V}$πιλέγει να την αποτιμήσει στο $\mathrm{x}_0 = c$
- Ο $\mathcal{P}$ υπολογίζει το $y_0 = ax_0 + b = s$
- Ο $\mathcal{V}$ μπορεί να ελέγξει μέσω των κουτιών αν το (x_0, y_0) όντως ανήκει στην ευθεία
- Ειδική ορθότητα: Αν επιλεγούν δύο σημεία της ίδιας ευθείας, τότε θα αποκαλυφθεί.
- Μηδενική γνώση: Από ένα σημείο διέρχονται άπειρες ευθείες.

https://x.com/ChrisPeikert/status/1547187811538829312

Ανάλυση

- **Πληρότητα:**
  - Αν είναι γνωστός ο διακριτός λογάριθμος του Y, τότε ο $\mathcal{V}$ θα επαληθεύσει τη σχέση με επιτυχία.
  - $g^s = g^{t+cx} = g^t(g^x)^c = TY^c$
- **Ειδική ορθότητα:**
  - Έστω δύο επιτυχή transcript του πρωτοκόλλου (T, c, s) και (T, c', s') με το ίδιο commitment
  - Λόγω επιτυχίας $g^s = TY^c$ και $g^{s'} = TY^{c'}$
  - Άρα $g^s Y^{-c} = g^{s'} Y^{-c'} \Rightarrow g^{s-xc} = g^{s'-xc'}$
  - Άρα $s - xc = s' - xc'$
  - Εύρεση witness $x = \frac{s-s'}{c-c'}$

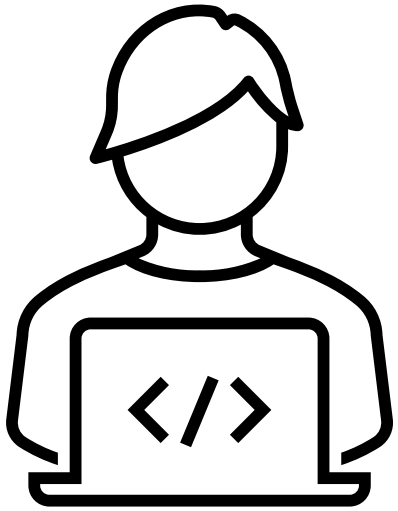
Ανάλυση

- Honest Verifier Zero Knowledge
- Κατασκευή simulator $\mathcal{S}$:
  - Commit $T = g^t, t \xleftarrow{\$} \mathbb{Z}_q$
  - Με αμελητέα πιθανότητα ο $\mathcal{S}$ μπορεί να απαντήσει σε challenge $c \xleftarrow{\$} \mathbb{Z}_q$
  - Rewind τον $\mathcal{V}$
  - Commit σε $T' = g^s Y^{-c}, \ s \xleftarrow{\$} \mathbb{Z}_q$
  - Ο $\mathcal{V}$ επειδή είναι honest και έχει το ίδιο random tape θα ρωτήσει το ίδιο $c \xleftarrow{\$} \mathbb{Z}_q$
  - Ο $\mathcal{S}$ απαντάει με s
  - Επαλήθευση $g^s = T' Y^c$ (λόγω κατασκευής)
- Οι συζητήσεις $\left(\boldsymbol{T} = g^t, t \xleftarrow{\$} \mathbb{Z}_q, \boldsymbol{c}, c \xleftarrow{\$} \mathbb{Z}_q, \boldsymbol{s} = t + c\text{x}\right)$ και $\left(\boldsymbol{T'} = g^s Y^{-c}, s \xleftarrow{\$} \mathbb{Z}_q, \boldsymbol{c}, c \xleftarrow{\$} \mathbb{Z}_q, \boldsymbol{s}\right)$ έχουν την ίδια κατανομή

Ανάλυση

- Δε διαθέτει μηδενική γνώση
  - Ένας cheating verifier $\mathcal{V}^*$ δεν διαλέγει ομοιόμορφα
  - Οι απαντήσεις του εξαρτώνται από τα μηνύματα του $\mathcal{P}$
  - Μετά το rewind δεν διαλέγει το ίδιο c
    - αφού ο $\mathcal{S}$ έστειλε T' αντί για T
  - Ο $\mathcal{S}$ κάθε φορά μπορεί να απαντήσει με αμελητέα πιθανότητα
- Τροποποίηση για μηδενική γνώση
  - Challenge space $\{0,1\}$ (γιατί?)
  - Προσθήκη commitment του $\mathcal{V}^*$ στο c πριν το πρώτο μήνυμα του $\mathcal{P}$

Μη διαλογικές αποδείξεις



- Μπορούμε να καταργήσουμε τον $\mathcal{V}$;
  - Ο $\mathcal{P}$ παράγει την απόδειξη μόνος του.
  - Επαληθεύεται από οποιονδήποτε $\mathcal{V}$.
- **Common Reference String (CRS)**
  - Μία ομοιόμορφα επιλεγμένη ακολουθία από bits που είναι διαθέσιμη και σε $\mathcal{P}, \mathcal{V}$ σαν επιπλέον είσοδος του πρωτοκόλλου.
  - Χρησιμεύει για την παραγωγή των μηνυμάτων $\mathcal{P}, \mathcal{V}$
  - Ποιος το παράγει; **Αν δεν είναι έμπιστος, μπορεί να σπάσει το soundness**.
- **FIAT-Shamir Heuristic**
  - Αντικατάσταση challenge με αποτέλεσμα μιας ψευδοτυχαίας συνάρτησης (π.χ. hash function)
  - Ασφάλεια στο μοντέλο του τυχαίου μαντείου.

Manuel Blum, Paul Feldman, and Silvio Micali. Non-Interactive Zero-Knowledge and Its Applications. Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988). 103–112. 1988

Fiat, Amos; Shamir, Adi (1987). "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". Advances in Cryptology — CRYPTO' 86. Lecture Notes in Computer Science. Vol. 263. Springer Berlin Heidelberg. pp. 186–194. doi:10.1007/3-540-47721-7_12. ISBN 978-3-540-18047-0.

Non-interactive Schnorr

- Δημόσια Είσοδος: $g \in \mathbb{G},\ ord(\mathbb{G}) = q, Y \in \mathbb{G}$
- Ιδιωτική Είσοδος : $x \in \mathbb{Z}_q : Y = g^x$

Τα βήματα του $\mathcal{P}$

Επιλογή $t \xleftarrow{\$} \mathbb{Z}_q$ και υπολογισμός $T = g^t$

1. **Υπολογισμός $c \leftarrow H(g, Y, T)$**
2. Υπολογισμός $s \leftarrow t + cx$
3. Η απόδειξη είναι: $\pi = (c, s)$
4. Επαλήθευση (**από οποιονδήποτε**) αν
$$c = H(g, Y, g^s Y^{-c})$$

Υπογραφές Schnorr

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

Δημόσια Είσοδος: $g \in \mathbb{G},\ ord(\mathbb{G}) = q, pk \in \mathbb{G}$

Ιδιωτική Είσοδος: $sk \in \mathbb{Z}_q : Y = g^{sk}$

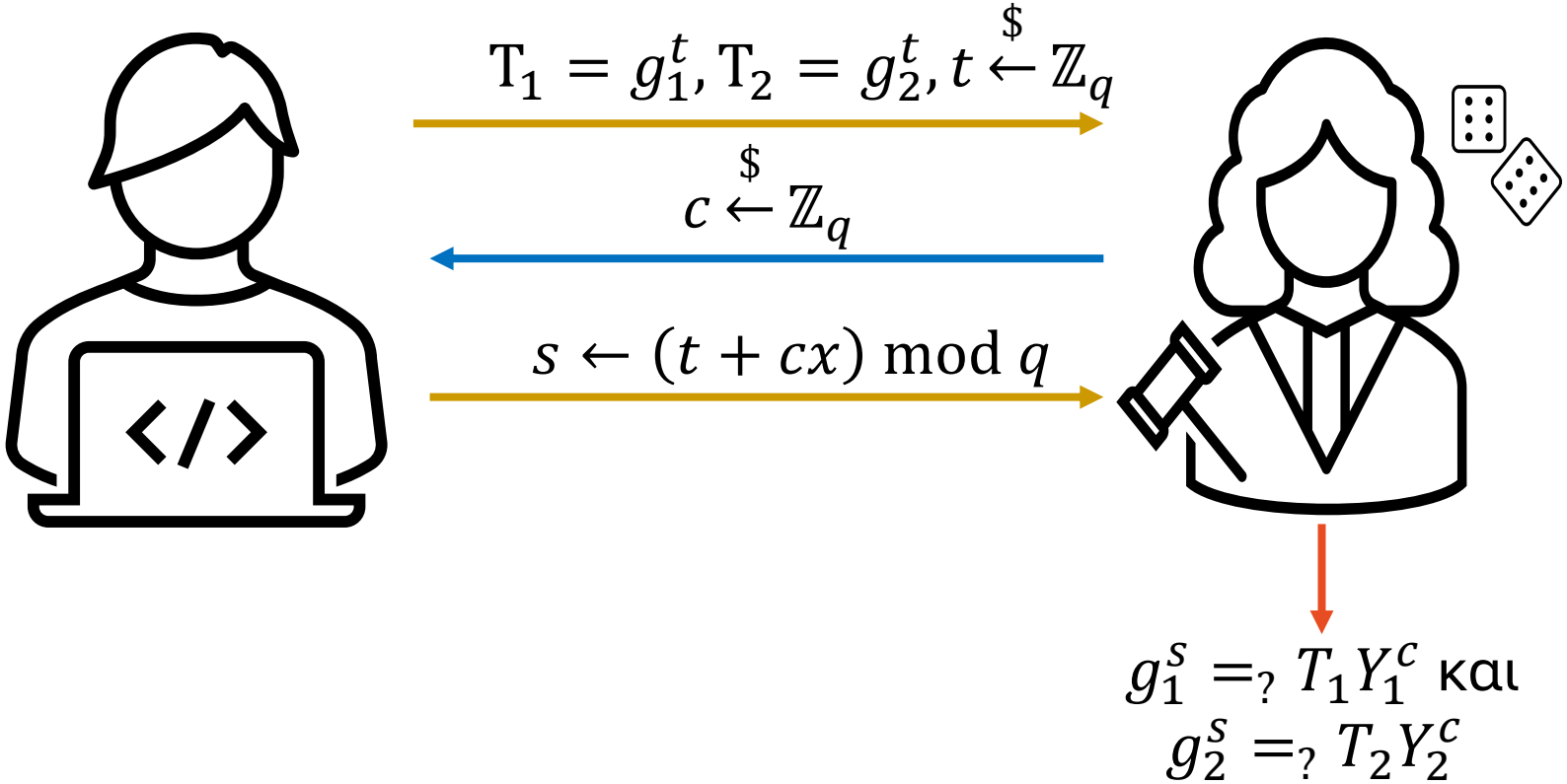
Τα βήματα του $\mathcal{P}$

1. Επιλογή $t \xleftarrow{\$} \mathbb{Z}_q$ και υπολογισμός $T = g^t$
2. **Υπολογισμός $\boldsymbol{c \leftarrow H(g, pk, T, m)}$**
3. Υπολογισμός $s \leftarrow t + c \cdot sk$
4. Η απόδειξη είναι: $\sigma = (c, s)$
5. Επαλήθευση (**από οποιονδήποτε**) αν

$$c = H(g, pk, g^s pk^{-c}, m)$$

Πρωτόκολλο Chaum - Pedersen

- Απόδειξη γνώσης και ισότητας δύο διακριτών λογάριθμων
- $PoK\{x: g_1^x = Y_1 \; και \; g_2^x = Y_2, \; Y_1, Y_2, g_1, g_2 \in \mathbb{G}\}$



Ανάλυση

- **Πληρότητα:**
  - Αν είναι γνωστοί και ταυτίζονται οι διακριτοί λογάριθμοι των Y_1, Y_2 τότε επαληθεύονται και οι δύο σχέσεις:
  - $g_1^s = g_1^{t+cx} = g_1^t (g_1^x)^c = T_1 Y_1^c$
  - $g_2^s = g_2^{t+cx} = g_2^t (g_2^x)^c = T_2 Y_2^c$
- **Ειδική ορθότητα:**
  - Έστω δύο επιτυχή transcript του πρωτοκόλλου (T_1, T_2, c, s) και (T_1, T_2, c', s') με το ίδιο commitment
  - Λόγω επιτυχίας $g_1^s = T_1 Y_1^c$ και $g_1^{s'} = T_1 Y_1^{c'}$
  - Άρα $g_1^s Y_1^{-c} = g_1^{s'} Y_1^{-c'} \Rightarrow g_1^{s-xc} = g_1^{s'-xc'}$
  - Άρα $s - xc = s' - xc'$
  - Εύρεση witness $x = \frac{s-s'}{c-c'}$
  - Τον ίδιο witness θα λάβουμε και από το T_2.
- **Honest Verifier Zero-Knowledge:**
  - Οι συζητήσεις $\left(\boldsymbol{T_1} = g_1^t, \boldsymbol{T_2} = g_2^t, \overset{\$}{\leftarrow} \mathbb{Z}_q, \boldsymbol{c}, c \overset{\$}{\leftarrow} \mathbb{Z}_q, \boldsymbol{s} = t + c\mathrm{x}\right)$ και $\left(\boldsymbol{T_1}' = g_1^s Y_1^{-c}, \boldsymbol{T_2}' = g_2^s Y_2^{-c}, s \overset{\$}{\leftarrow} \mathbb{Z}_q, \boldsymbol{c}, c \overset{\$}{\leftarrow} \mathbb{Z}_q, \boldsymbol{s}\right)$ έχουν την ίδια κατανομή

Εφαρμογές Chaum - Pedersen

- Η τριάδα (g^a, g^b, g^c) είναι τριάδα Diffie – Hellman

Κλήση $CP\langle g_1 = g, g_2 = g^b, Y_1 = g^a, Y_2 = g^{ab} = (g^b)^a \rangle$ με witness a

- Δίνεται ένα κρυπτοκείμενο $c = (c_1, c_2)$ με $(c_1, c_2) \in \mathbb{G}$. Αποδείξτε ότι αποτελεί έγκυρο κρυπτογράφημα με δημόσιο κλειδί Y ενός μηνύματος $m \in \mathbb{G}$, χωρίς να διαρρεύσει το ιδιωτικό κλειδί και η τυχαιότητα.

- Κλήση $CP\langle g_1 = g, g_2 = Y, Y_1 = c_1, Y_2 = c_2 m^{-1} \rangle$ με witness r
- Δείχνουμε δηλ. ότι έχει χρησιμοποιηθεί κοινή τυχαιότητα και ο P τη γνωρίζει

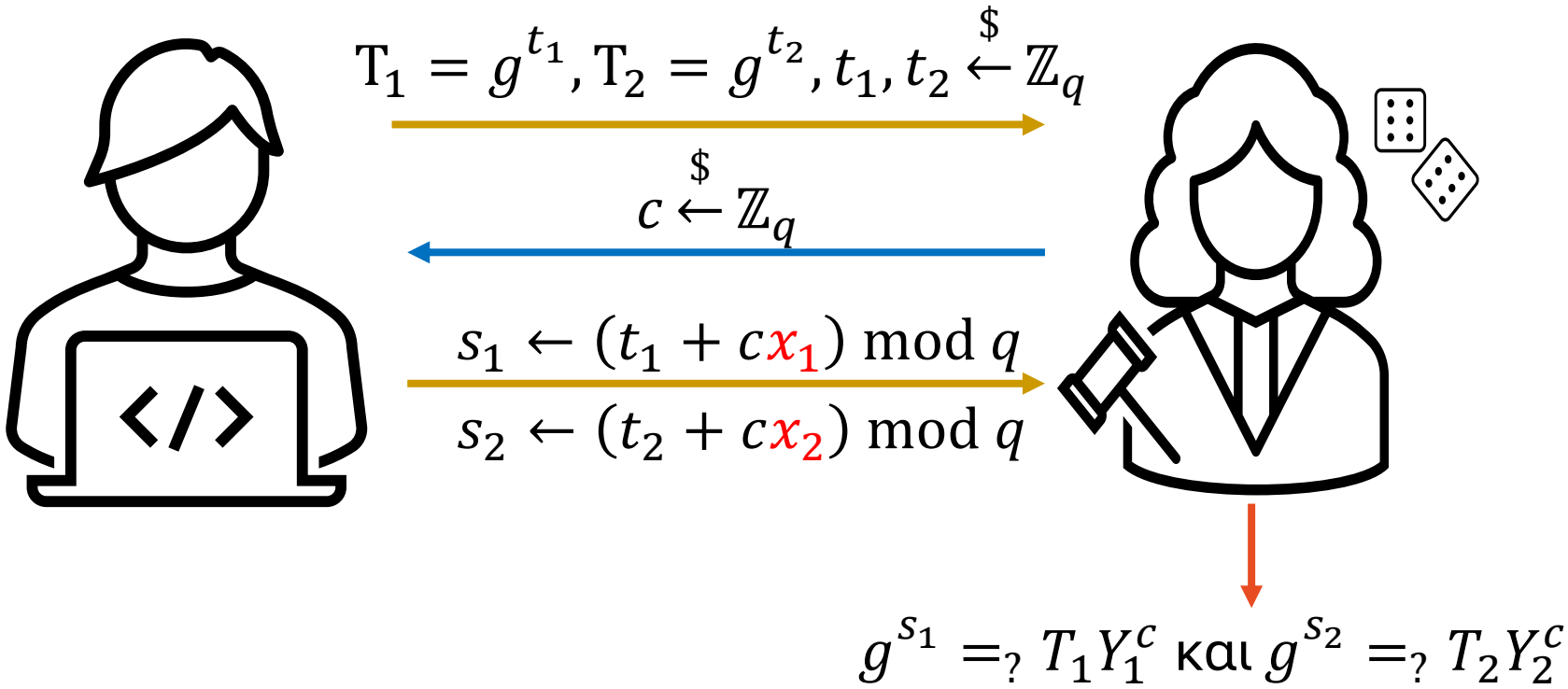
Σύνθεση Σ-πρωτοκόλλων

- Τι αποδεικνύουμε στο πρωτόκολλο Chaum-Pedersen;
  - Ότι δύο διαφορετικές σχέσεις $g_1^x = Y_1 \; και \; g_2^x = Y_2$ έχουν τον **ίδιο** witness x?
  - Πρόκειται για μία σύνθεση **EQ**.
  - Υπάρχουν και άλλα είδη σύνθεσης (με διατήρηση των ιδιοτήτων των Σ-πρωτοκόλλων)
  - Μπορούμε δηλ. με δεδομένα δύο ή περισσότερα Σ-πρωτόκολλα να φτιάξουμε ένα **νέο Σ-πρωτόκολλο (διατηρώντας δηλαδή τις ιδιότητες HVZK και Special Soundness);**
    - **NAI [CDS94]**
    - Οι πιο ενδιαφέρουσες είναι οι συνθέσεις **AND, OR**

Cramer, R., Damgård, I., Schoenmakers, B. (1994). Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In: Desmedt, Y.G. (eds) Advances in Cryptology — CRYPTO '94. CRYPTO 1994. Lecture Notes in Computer Science, vol 839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48658-5_19

Σύνθεση AND

- Απόδειξη γνώσης δύο διακριτών λογάριθμων
- $PoK\{(x_1, x_2): g^{x_1} = Y_1 \textbf{ AND } g^{x_2} = Y_2,\ Y_1, Y_2, g \in \mathbb{G}\}$

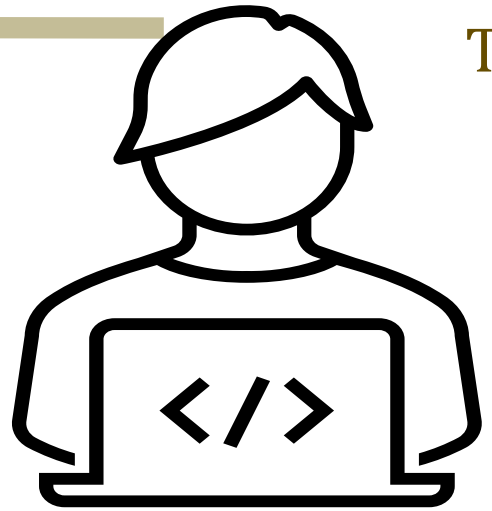


Σύνθεση OR

- Μπορούμε να αποδείξουμε ότι γνωρίζουμε τουλάχιστον ένα $w_i \in W = \{w_1, \cdots, w_n\}$
- Γενικευμένη στρατηγική:
  - Για τον witness που γνωρίζουμε: εκτελούμε κανονικά το Σ-πρωτόκολλο
  - Για τους υπόλοιπους: χρήση simulator με challenges επιλεγμένα από τον P
  - Υπολογισμός responses
    - Με βάση το challenge του V
    - Και τα δεσμευμένα challenges του P
- **Πάρα πολλές εφαρμογές**

OR Schnorr

- Απόδειξη γνώσης **ενός** από δύο διακριτούς λογάριθμους
- $PoK\{(x_1, x_2): g^{x_1} = Y_1 \textbf{ OR } g^{x_2} = Y_2,\ Y_1, Y_2, g \in \mathbb{G}\}$



$T_1 = g^{t_1}, T_2 = g^{t_2} Y_2^{-c_2}, t_1, c_2, t_2 \xleftarrow{\$} \mathbb{Z}_q$

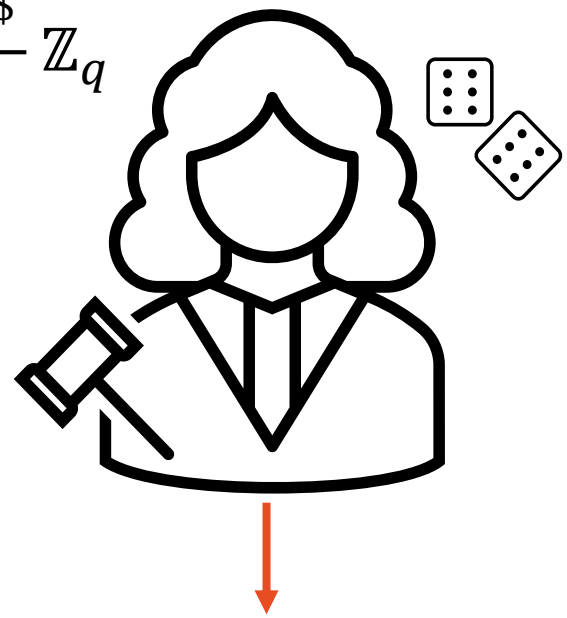
$c \xleftarrow{\$} \mathbb{Z}_q$

c_1, c_2, s_1, s_2

$s_1 \leftarrow (t_1 + c_1 x_1) \bmod q$

$s_2 \leftarrow t_2$

$c_1 \leftarrow c - c_2$



$g^{s_1} =_? T_1 Y_1^{c_1}$ και $g^{s_2} =_? T_2 Y_2^{c_2}$

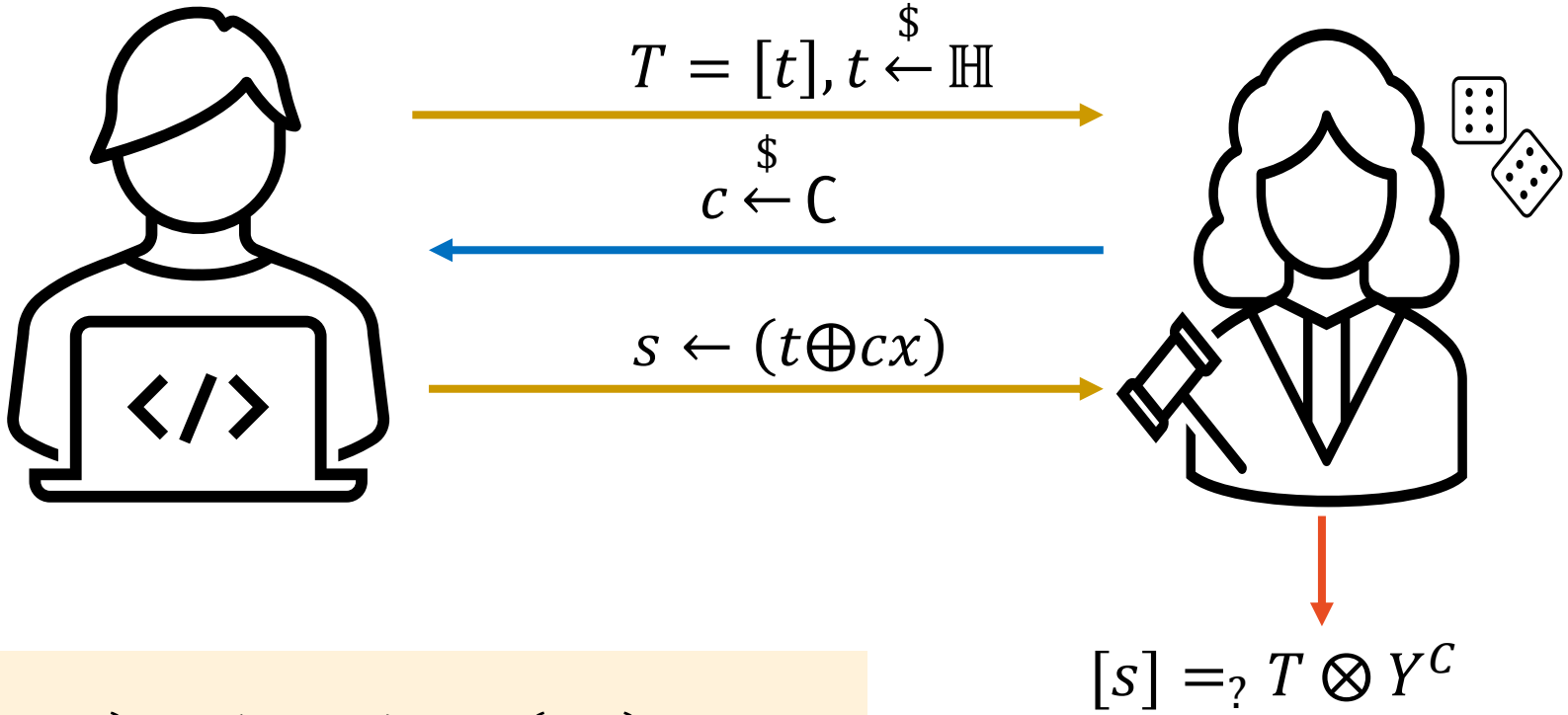
και $c = c_1 + c_2$

Maurer, Ueli. "Unifying zero-knowledge proofs of knowledge." International Conference on Cryptology in Africa. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

Γενίκευση

$PoK\{x \in \mathbb{H}: [x] = Y, Y \in \mathbb{G}\}$

Δίνονται ομάδες $(\mathbb{H}, \oplus)$ και $(\mathbb{G}, \otimes)$ και **μονόδρομος** ομομορφισμός $[\,]: \mathbb{H} \to \mathbb{G}$ ώστε: $[g_1 \oplus g_2] = [g_1] \otimes [g_2]$



Schnorr: $(\mathbb{H}, \oplus) = (\mathbb{Z}_q, +)$ και $(\mathbb{G}, \cdot)$ με δύσκολο DLP και $[x] = g^x$

Ανάλυση

- **Πληρότητα:**

$$[s] = [t \oplus cx] = [t] \otimes [cx] = [t] \otimes [x]^c = T \otimes Y^c$$

- **Ειδική ορθότητα:**

Ισχύει αν υπάρχουν τιμές $l \in \mathbb{N}$ και $u \in \mathbb{H}$ ώστε:

$$\gcd(c_1 - c_2, l) = 1 \ \ \forall c_1, c_2 \in \mathbb{C} \text{ και } [u] = Y^l.$$

Τότε:

$$[s] =_? T \otimes Y^c \text{ και } [s'] =_? T \otimes Y^{c'}$$

Υπάρχει witness $x' = u^a \oplus (s'^{-1} \oplus s)^b$ ώστε $[x'] = Y$

με α, b από τον EGCD αλγόριθμο για $la + (c - c')b = 1$.

$[s'^{-1} \oplus s] = [s'^{-1}] \otimes [s] = Y^{-c'} \otimes T^{-1} \otimes T \otimes Y^c = Y^{-c'} \otimes Y^c = Y^{c-c'}$

Πράγματι:

$$[x'] = [u^a \oplus (s'^{-1} \oplus s)^b] = [u]^a \otimes [s'^{-1} \oplus s]^b =$$
$$(Y^l)^a \otimes (Y^{c-c'})^b = Y^{la+(c-c')b} = Y$$

- **Honest Verifier Zero-Knowledge**

Για δεδομένα Y, c και τυχαία επιλεγμένο s: $T = [s] \otimes Y^{-c}$

Schnorr:

$l = q$ (πρώτος)

$u = 0$

ZK Γενικού σκοπού

- **Υπενθύμιση:** Όλο το NP έχει αποδείξεις μηδενικής γνώσης
- Μπορούμε να αποδείξουμε περισσότερα και πιο ενδιαφέροντα πράγματα από τη γνώση ενός DL
- **Για παράδειγμα:** Ότι ένα πρόγραμμα εκτελέστηκε σωστά ακόμα και αν δεν δείξουμε κάποια inputs ή/και outputs!
- **Motivation:** Privacy / Performance on the blockchain
  - Η μεγαλύτερη συνεισφορά του blockchain στην ανθρωπότητα! *#sarcasm*

(ZK-)SNARKs

- **ZK**: Zero-Knowledge.
- **Succinct**: Η απόδειξη είναι πολύ σύντομη (σε μέγεθος και χρόνο επαλήθευσης) σε σχέση με τον υπολογισμό.
- **Non-Interactive:** Δεν χρειάζεται η συμμετοχή του verifier. Δημόσια επαληθεύσιμη απόδειξη.
- **Arguments:** Ο Prover είναι PPT.
- of **Knowledge.** Απόδειξη κατοχής.

Αποτελούνται από:

- **Σύστημα απόδειξης (δέσμευση γνώσης πολυωνύμου)**
- **Μεταγλωττιστή** του προγράμματος σε κάτι που μπορεί να χειριστεί το σύστημα απόδειξης (**πολυώνυμο**) - **Arithmetization**

Arithmetization (Γενικά)

```
function calc(w, a, b)
    if w then
        return a × b
    else
        return a + b
    end if
end function
```

$$f(w, a, b) = w \cdot a \cdot b + (1 - w)(a + b) = v$$

Πρόκειται για αριθμητικό κύκλωμα

Μετατροπή σε R1CS: $L \cdot R = O$

$$a \cdot b = m$$
$$w \cdot (m - a - b) = v - a - b$$
$$w \cdot w = w$$

Ευρεση πολυωνύμου P ώστε:

$$P(1) = a \cdot b - m$$
$$P(2) = w \cdot (m - a - b) - v + a + b$$
$$P(3) = w \cdot w - w$$

- Κρατώντας κάποιο inputs μυστικά
- Σε συνεργασία με τον verifier

Aniket **Kate**, Gregory M. **Zaverucha**, and Ian **Goldberg**. Constant-size commitments to polynomials and their applications. In Masayuki Abe, editor, Advances in Cryptology - ASIACRYPT pages 177–194. Springer, 2010

KZG Commitments

- Δέσμευση και απόδειξη γνώσης πολυωνύμου
- **Computationally** binding – **Computationally** Hiding
- **Σταθερό μέγεθος:** 1 group element *ανεξάρτητα* από το μέγεθος του πολυωνύμου.
  - **Schwartz-Zippel Lemma:** Δύο διαφορετικά πολυώνυμα P, Q βαθμού το πολύ d συμφωνούν το πολύ σε ποσοστό d/q σημεία. Δηλαδή $\Pr\left[[P(r) = Q(r)] \middle| r \leftarrow_{\$} \mathbb{F}_q^d\right] \leq \frac{d}{q}$
  - Συνήθως $d \ll q$
- Γρήγορη επαλήθευση
- Ενσωμάτωση στο Ethereum
- Μειονέκτημα: trusted setup.

KZG Commitments

$\boldsymbol{KeyGen(1^{\lambda}, d)}$

- Επιλογή πρώτου q και σώματος $\mathbb{F}_q^d$
- Επιλογή ομάδων $\mathbb{G}, \mathbb{G}_T$ τάξης q ώστε να υπάρχει συμμετρικό pairing μεταξύ τους e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
- Επιλογή $g \leftarrow_{\$} \mathbb{G}$ και $\tau \leftarrow_{\$} \mathbb{Z}_q$
- Υπολογισμός powers-of-tau $\boldsymbol{g^{\tau}, g^{\tau^2}, \ldots, g^{\tau^d}}$
- Διαγραφή τ (trusted setup)
- Επιστροφή $(e, \mathbb{F}_q^d, \mathbb{G}, \mathbb{G}_T, \boldsymbol{g^{\tau}, g^{\tau^2}, \ldots, g^{\tau^d}})$ – structured reference string (SRS)

Commitment σε πολυώνυμο $-$ $\boldsymbol{Commit(P)}$

Αν $P(x) = \sum_{i=0\ldots d} \alpha_i x^i$ τότε:

- $C_p = g^{P(\tau)} = g^{\sum_{i=0\ldots d} \alpha_i \tau^i} = \prod_{i=0\ldots d} g^{\alpha_i \tau^i} = \prod_{i=0\ldots d} (g^{\tau^i})^{a_i}$
  - Μπορεί να γίνει χωρίς το τ, μόνο με βάση το SRS

- Το commitment είναι μόνο ένα στοιχείο της $\mathbb{G}$ ανεξάρτητα από τον βαθμό του P $-$ Σταθερό μέγεθος.

Challenge - Response

Απόδειξη αποτίμησης

- Ο $\mathcal{V}$ επιλέγει u
- Ο $\mathcal{P}$ πρέπει να δείξει ότι $P(u) = v$ μέσω των commitments (χωρίς να αποκαλύψει το πολυώνυμο)
- $P(u) = v \Leftrightarrow \exists W\colon (x - u) \cdot W(x) = P(x) - v$
- Ο $\mathcal{P}$ υπολογίζει το W και δεσμεύεται σε αυτό υπολογίζοντας το $C_W = g^{W(\tau)}$

Επαλήθευση

- Ο $\mathcal{V}$ γνωρίζει C_P, C_W, v, u
- Πρέπει να ελέγξει ότι $(\tau - u) \cdot W(\tau) = P(\tau) - v$
- Δεν γνωρίζει το τ όμως.
- Μπορεί να το παρακάμψει μέσω του pairing.
- Ελέγχει ότι:

$$e(C_P \cdot g^{-v}, g) = e(g^{\tau}/g^{u}, C_W) \Leftrightarrow$$

$$e\left(g^{P(\tau)-v}, g\right) = e\left(g^{\tau-u}, g^{W(\tau)}\right) \Leftrightarrow$$

$$e(g, g)^{P(\tau)-v} = e(g, g)^{W(\tau)(\tau-u)}$$

Soundness

- Αν $P(u) \neq v$ τότε ο $\mathcal{P}^*$ πρέπει να βρει $W(\tau)$ ώστε: $e(g,g)^{P(\tau)-v} = e(g,g)^{W(\tau)(\tau-u)}$
- Για να υπολογιστεί το $W(\tau)$ θα πρέπει να μπορεί να 'διαιρεθεί' το $P(u) - v$ με το $(\tau - u)$ στον εκθέτη λόγω SRS ($g^{W(\tau)} = g^{\frac{P(\tau)-v}{\tau-u}}$).
- **Υπόθεση q-SDH** (*q-strong Diffie-Hellman)*
  - Με δεδομένα το **SRS** $(e, \mathbb{F}_q^d, \mathbb{G}, \mathbb{G}_T, \boldsymbol{g}^{\tau}, \boldsymbol{g}^{\tau^2}, \ldots, \boldsymbol{g}^{\tau^d})$ είναι **δύσκολο** να υπολογιστεί οποιοδήποτε ζεύγος $u, g^{\frac{1}{(\tau-u)}}$.
  - Πιστεύεται ότι είναι υπολογιστικά δύσκολη.