1 Αποδείξεις Μηδενικής Γνώσης

Μία ***απόδειξη (proof)*** είναι ένα πρωτόκολλο που επιτρέπει στη μία πλευρά μίας επικοινωνίας να πείσει την άλλη για την εγκυρότητα μιας πρότασης. Σε μια ***απόδειξη μηδενικής γνώσης (zero-knowledge proof)***, αυτό επιτυγχάνεται χωρίς την φανέρωση κάποιας πληροφορίας εκτός από την πιστότητα της απόδειξης. Θα εξετάσουμε διάφορα παραδείγματα αποδείξεων μηδενικής γνώσης πριν δώσουμε τον τυπικό ορισμό. Πρώτα εξετάζουμε το γενικό πλαίσιο.

Έχουμε δυο πλευρές, τον ***prover*** $\mathcal{P}$ και τον ***verifier (επαληθευτή)*** $\mathcal{V}$. Ο $\mathcal{P}$ πρέπει να πείσει τον $\mathcal{V}$ πως έχει κάποια γνώση σχετικά με μια δήλωση x χωρίς να αναφέρει ξεκάθαρα τι γνωρίζει. Ονομάζουμε τη γνώση αυτή ***witness (μάρτυρα)*** w. Και οι δύο πλευρές γνωρίζουν ένα κατηγόρημα R που θα επιβεβαιώσει ότι το w είναι ένας έγκυρος μάρτυρας για το x. Γενικά,

- Το κατηγόρημα R υποθέτουμε ότι είναι υπολογίσιμο σε πολυωνυμικό χρόνο: δεδομένου ενός w για μια πρόταση x, θα μπορούσαμε να ελέγξουμε αποτελεσματικά πως $R(x, w) = 1$.
- Ο prover $\mathcal{P}$ έχει τα R, x, και w τέτοια ώστε $R(x, w) = 1$. Θέλει να αποδείξει την κατοχή του w πραγματοποιώντας μια απόδειξη γνώσης π.
- Ο verifier $\mathcal{V}$ έχει τα R, x, και π.

Για να δείξουμε πως το παραπάνω πρωτόκολλο είναι χρήσιμο σε κρυπτογραφικές εφαρμογές, μπορούμε να κάνουμε τις εξής παραδοχές.

- Δεδομένου του R, είναι δύσκολο να βρούμε το αντίστοιχο w έτσι ώστε $R(x, w) = 1$.
- Ο prover $\mathcal{P}$ είναι απρόθυμος να αποκαλύψει το w; αλλιώς η απόδειξη είναι τετριμμένη.
- Ο verifier $\mathcal{V}$ μπορεί να επιβεβαιώσει αποτελεσματικά την εγκυρότητα του π.

Διαισθητικά οι ζητούμενες ιδιότητες για τις αποδείξεις μηδενικής γνώσεις είναι οι εξής:

(Πληρότητα) Ο $\mathcal{V}$ πάντα αποδέχεται αληθείς προτάσεις αν η απόδειξη γίνει σωστά από τον $\mathcal{P}$.

(Εγκυρότητα) Ο $\mathcal{V}$ δεν αποδέχεται ψευδείς προτάσεις (ακόμα και αν ο $\mathcal{P}$ προσπαθήσει να τον ξεγελάσει).

(Μηδενική Γνώση) Ο $\mathcal{V}$ δεν αποκομίζει τίποτα απο την απόδειξη, πέρα απο την ορθότητα της πρότασης.

1.1 Παραδείγματα Αποδείξεων Μηδενικής Γνώσης

Δίνουμε τα εξής χαρακτηριστικά παραδείγματα.

Παράδειγμα (Πού είναι ο Waldo)**.** Στο παιχνίδι *Πού είναι ο Waldo*, υπάρχει ένα μεγάλο ταμπλό που απεικονίζει μια σκηνή με πολλούς χαρακτήρες που μοιάζουν με τον «Waldo». Στόχος του παιχνιδιού είναι να βρούμε τον Waldo.

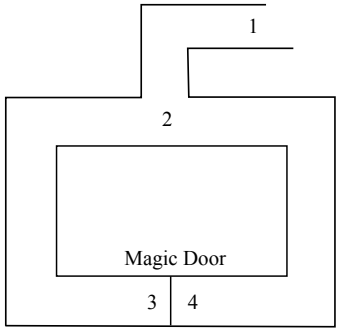
Υποθέτουμε ότι η Αλίκη και ο Βασίλης παίζουν αυτό το παιχνίδι. Η Αλίκη υποστηρίζει ότι έχει βρει που βρίσκεται ο Waldo αλλά δεν θέλει να το πει στο Βασίλη.

Η υπόθεση ότι ο Waldo υπάρχει είναι η πρόταση, οι συντεταγμένες (x, y) της θέσης του Waldo είναι ο μάρτυρας, και η διαδικασία λήψης των (x, y) και η επιβεβαίωση ότι ο Waldo είναι όντως εκεί σχετίζεται με το κατηγόρημα R.

Μια πιθανή λύση και όχι μοναδική είναι η Αλίκη να καλύψει το ταμπλό με ένα μεγάλο κομμάτι χαρτί και μια μικρή τρύπα στο κέντρο. Η Αλίκη θα τοποθετήσει το χαρτί στο ταμπλό έτσι ώστε να εμφανιστεί μόνο ο Waldo. Η λύση θα είναι αποτελεσματική αν το χαρτί έχει τουλάχιστον διπλάσιες διαστάσεις από το ταμπλό.

Παράδειγμα (Η Μαγική Πόρτα)**.** Το επόμενο παιχνίδι που θα μας απασχολήσει είναι το εξής.

1. Στο βάθος μιας σπηλιάς υπάρχει μια μαγική πόρτα που μπορεί να ανοίξει χρησιμοποιώντας ένα μυστικό κωδικό. Ο Βασίλης προσπαθεί να πείσει την Αλίκη ότι γνωρίζει τον κωδικό και συνεπώς πως μπορεί να ανοίξει την μαγική πόρτα.



Σχήμα 1: Η πόρτα μεταξύ των σημείων 3 και 4 μπορεί να ανοιχθεί χρησιμοποιώντας ένα μυστικό κωδικό.

1. Η Αλίκη κάθεται στο σημείο 1.
2. Ο Βασίλης μπαίνει στην σπηλιά και κάθεται στα σημεία 3 ή 4.
3. Όταν ο Βασίλης εξαφανίζεται, η Αλίκη προχωρά στο σημείο 2.
4. Η Αλίκη φωνάζει τον Βασίλη, ρωτώντας τον να βγει είτε από το αριστερό μονοπάτι είτε από το δεξί.
5. Ο Βασίλης δρα σύμφωνα με αυτό χρησιμοποιώντας τον μυστικό κωδικό αν είναι αναγκαίο.
6. Η Αλίκη και ο Βασίλης επαναλαμβάνουν τα βήματα 1-5 k φορές.

Αυτό το παιχνίδι μας δείχνει μια απόδειξη γνώσης μέσω μιας πιθανοτικής διαδικασίας. Συγκεκριμένα, μετά από k επαναλήψεις, ο Βασίλης μπορεί να πείσει την Αλίκη πως ξέρει τον μυστικό κωδικό με πιθανότητα $1 - 1/2^k$.

Στη συνέχει παρουσιάζουμε τρία πρακτικά παραδείγματα των αποδείξεων γνώσης.

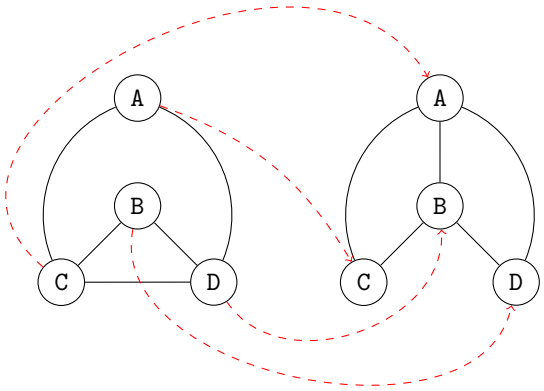
Παράδειγμα. Επιστρέφουμε στην κλάση NP: το σύνολο όλων των προβλημάτων, των οποίων μια υποψήφια λύση μπορεί να επαληθευτεί σε πολυωνυμικό χρόνο. Ονομάζουμε το σύνολο των συμβολοακολουθιών ***γλώσσα (language)***. Έστω x κάποια διατύπωση του προβλήματος και έστω R να είναι ένα κατηγόρημα πολυωνυμικού χρόνου. Τότε μια γλώσσα L είναι στο NP αν

$$\mathrm{L} = \{x \colon R(x, w) = 1 \text{ for some } w\}\,.$$

Θεωρούμε τη γλώσσα CLIQUE $= \{\langle G, k\rangle \colon G \text{ is a graph with a clique of size } k\}$. Οι μάρτυρες είναι τα σύνολα των k κόμβων που διαμορφώνουν μια κλίκα και το πολυωνυμικού χρόνου κατηγόρημα R που επαληθεύει ότι οι κόμβοι συνιστούν μια κλίκα.

Μια άλλη γλώσσα είναι η SAT $= \{\langle \Phi\rangle \colon \Phi \text{ is a satisfiable boolean formula}\}$. Μπορούμε να επαληθεύσουμε σε πολυωνυμικό χρόνο πως ένα σύνολο μεταβλητών που εμπεριέχονται στο $\Phi \in SAT$ ικανοποιούν το Φ. Αποδείξεις μηδενικής γνώσης μπορούν να χρησιμοποιηθούν για να αποδείξουν πως ένα συγκεκριμένο στοιχείο ανήκει στη γλώσσα CLIQUE ή στη γλώσσα SAT. Αυτό θα το επεκτείνουμε στην ενότητα 1.5.

Παράδειγμα. Μια βασική εφαρμογή των αποδείξεων μηδενικής γνώσης βρίσκεται στα σχήματα ταυτοπροσωπίας. Στους παραδοσιακούς μηχανισμούς μυστικών κωδικών, ένας αντίπαλος που κρυφακούει την συνομιλία μπορεί να αντλήσει αρκετή πληροφορία για να αποκτήσει μη εγκεκριμένη πρόσβαση σε ένα σύστημα. Για να αντιμετωπίσουμε αυτό το πρόβλημα υποθέτουμε ότι το σύστημα περιλαμβάνει ένα δημόσιο κατάλογο που αναθέτει μια πρόταση ενός θεωρήματος σε κάθε χρήστη. Υποθέτοντας ότι μόνο ένα συγκεκριμένος χρήστης γνωρίζει ένα μάρτυρα για την απόδειξη, μια απόδειξη μηδενικής γνώσης μπορεί να πείσει το σύστημα για την αυθεντικότητά της. Αυτό είναι άμεσα συνδεδεμένο με το πρωτόκολλο του Schnorr, το οποίο θα εξετάσουμε στην ενότητα 1.3.



Σχήμα 2: Δυο ισομορφικά γραφήματα: Η αντιστοίχηση από ABCD σε CDAB αντιστοιχίζει το πρώτο γράφημα στο δεύτερο.

Παράδειγμα (Ισομορφισμός Γραφημάτων)**.** Ένα μη κατευθυνόμενο γράφημα αποτελείται από ένα σύνολο κορυφών V και ένα σύνολο ακμών E, όπου κάθε ακμή είναι ένα (μη διατεταγμένο) ζεύγος κορυφών. Δύο γραφήματα $G_0 = (V, E_0)$ και $G_1 = (V, E_1)$ είναι ισομορφικά αν υπάρχει μία μετάθεση κορυφών που απεικονίζει το ένα γράφημα στο άλλο, βλ. Σχήμα 2. Συγκεκριμένα λέμε ότι μια μετάθεση κορυφών $f : V \to V$ είναι ισομορφισμός από το G_0 στο G_1 αν για κάθε ζεύγος κορυφών, έχουμε $(u, v) \in E_1$ αν και μόνο αν $(f(u), f(v)) \in E_2$. Οι ισομορφισμοί γραφημάτων είναι μεταβατικοί, αν έχουμε δύο ισομορφισμούς $f : G_0 \to G_1$ και $g : G_1 \to G_2$ τότε ο $g \circ f : G_0 \to G_2$ είναι ισομορφισμός γραφημάτων από το G_0 στο G_2.

Για οποιαδήποτε δύο γραφήματα G_0, G_1 είναι εύκολο να ελέγξουμε αν μια μετάθεση κορυφών f είναι ισομορφισμός γραφημάτων. Από την άλλη, δεν υπάρχει γνωστός πολυωνυμικός αλγόριθμος ώστε για κάθε G_0 και G_1 να ελέγχθουμε αν είναι ισομορφικά. Θα ασχοληθούμε με προτάσεις που ισχυρίζονται ότι δύο γραφήματα είναι ισομορφικά μεταξύ τους. Ο prover γνωρίζει έναν ισομορφισμό μεταξύ τους αλλά θέλει να πείσει τον verifier, χωρίς όμως να φανερώσει τον ισομορφισμό. Πιο αυστηρά, θεωρούμε την γλώσσα των ισομορφικών γραφημάτων $L_R = \{(G_0, G_1)\}$ που ορίζεται από τη σχέση $R = \{((G_0, G_1), f) : G_1 = f(G_0)\}$.

Πρόταση: Δυο γραφήματα G_0, G_1 που έχουν το ίδιο σύνολο κορυφών V.

Witness για τον $\mathcal{P}$: Ένας ισομορφισμός f μεταξύ G_0 και G_1.

Προτόκολλο:

1. Ο $\mathcal{P}$ επιλέγει μια τυχαία μετάθεση κορυφών $h : V \to V$ και υπολογίζει $H = h(G_1)$. Αποθηκεύει την h και στέλνει το H στον $\mathcal{V}$.
2. Ο $\mathcal{V}$ επιλέγει μια τυχαία ερώτηση $b \xleftarrow{r} \{0, 1\}$.
3. Αν $b = 0$ ο $\mathcal{P}$ στέλνει $g = h \circ f$ στον $\mathcal{V}$.
   Αν $b = 1$ ο $\mathcal{P}$ στέλνει $g = h$ στον $\mathcal{V}$. Ο $\mathcal{V}$ αποδέχεται την απόδειξη αν $g(G_b) = H$.

Εύκολα ελέγχουμε ότι το πρωτόκολλο «δουλεύει». Αν τα G_0 και G_1 είναι ισομορφικά, τότε κάθε ένα είναι ισομορφικό και με το H. Επιπλέον, αν ο prover ξέρει τον ισομορφισμό f μπορεί επιλέον να υπολογίσει και τον ισομορφισμό ανάμεσα στα G_0 , H και αυτόν ανάμεσα στα G_1, H. Έτσι, μπορεί να απαντήσει σε κάθε ερώτηση $b \in \{0, 1\}$ και ο verifier πάντα αποδέχεται.

Αναφορικά με την ασφάλεια, το πρωτόκολλο έχει πιθανότητα 50% να αποκαλύψει ότι ένας prover «κλέβει». Αν τα G_0, G_1 δεν είναι ισομορφικά μεταξύ τους, τότε είναι αδύνατο το H να είναι ισομορφικό ως προς και τα δύο. Άρα, αν ο verifier διαλέξει το γράφημα που δεν είναι ισομορφικό ως προς το H, πράγμα που συμβαίνει με πιθανότητα 50%, η απάτη του prover αποκαλύπτεται.

Είναι απλό να αυξήσουμε την πιθανότητα εντοπισμού όσο χρειαζόμαστε: επαναλαμβάνουμε το πρωτοκολλο n φορές, για τα ίδια G_0, G_1 αλλά διαφορετικά H_i, b_i και g. Σε κάθε επανάληψη έχουμε 50% να πιάσουμε τον prover (εάν «κλέβει»), οπότε συνολικά, ένας ανέντιμος prover επιτυγχάνει με πιθανότητα μόλις 2^{-n}.

Η ιδιότητα της μηδενικής γνώσης είναι (τεχνικά) η πιο περίπλοκη. Τι σημαίνει οτι ο verifier δεν μαθαίνει κάτι που δεν ήξερε ήδη; Ένας τρόπος να το περιγράψουμε είναι μέσω προσομοίωσης: αν ο verifier έχει τη δυνατότητα να φτιάξει συνομιλίες πανομοιότυπες με αυτές που έχει με τον prover, τότε μάλλον και οι πραγματικές συνομιλίες είναι άχρηστες, αφού οι «ψευτικες» συνομιλίες είναι εξ ορισμού άχρηστες.

Θα δώσουμε μια απλή λύση που καλύπτει συνομιλίες με έναν τίμιο prover (ο οποίος επιλέγει το b ανεξάρτητα από τα G_i και το H). Επιλέγουμε τυχαία $b^* \leftarrow \{0,1\}$. Επιλέγουμε μια τυχαία αναδιάταξη h^*, και θέτουμε $H^* = h^*(G_b)$. Ισχυριζόμαστε ότι η συζήτηση (H^*, b^*, h^*) είναι πανομοιότυπη με μία πραγματική εκτέλεση του πρωτοκόλλου.

Είναι προφανές ότι το b και b^* έχουν την ίδια κατανομή αφού είναι τυχαία επιλεγμένα από το το $\{0,1\}$. Όταν $b^* = 1$, είναι προφανές ότι και τα H^*, g^* έχουν την ίδια κατανομή με τα H, g. Όταν $b^* = 0$, παρατηρούμε ότι $^* = (h \circ f^{-1})(G_0)$ και ότι $g = h \circ f^{-1} \circ f$, δηλαδή η προσομοίωση, όταν επιλέξουμε το h^* είναι ίδια με μία πραγματική εκτέλεση όπου ο prover επέλεξε $h = h^* \circ f^{-1}$).

Η παραπάνω ανάλυση ισχύει όταν ο verifier πράγματι ακολουθεί το πρωτόκολο, δηλαδή επιλέγει το b τυχαία, και ανεξάρτητα από οτιδήποτε άλλο. Αφού δώσουμε ορισμούς στην επόμενη ενότητα, είναι χρήσιμο να επιστρέψουμε και να δώσουμε ένα simulator για κάθε πιθανό verifier.

1.2 Τρεις βασικές ιδιότητες

Η διαμόρφωση του αυστηρού ορισμού μιας απόδειξης γνώσης είναι ένα πολύ λεπτό ζήτημα. Ο επόμενος ορισμός προέκυψε μετά από δεκαπέντε χρόνια δουλειάς και θεωρείται πνευματική κατάκτηση.

Ορισμός 1.2.1. Έστω $\langle \mathcal{P}, \mathcal{V} \rangle$ ένα ζεύγος αλληλεπιδρόντων προγραμμάτων. Ορίζουμε ως $\text{out}^{\mathcal{P}}_{\mathcal{P},\mathcal{V}}(x,w,z)$ να είναι η έξοδος του $\mathcal{P}$ όταν οι $\mathcal{P}$ και $\mathcal{V}$ εκτελούνται με τη δημόσια είσοδο x και τις ιδιωτικές εισόδους w και z (ο $\mathcal{P}$ καθορίζει το w και ο $\mathcal{V}$ διαλέγει το z). Το $\text{out}^{\mathcal{V}}_{\mathcal{P},\mathcal{V}}$ ορίζεται όμοια για το $\mathcal{V}$. Το PPT διαδραστικό πρωτόκολλο $\langle \mathcal{P}, \mathcal{V} \rangle$ είναι μια ***απόδειξη μηδενικής γνώσης (zero-knowledge proof)*** για μια γλώσσα $\text{L} \in NP$ με απόσταση μηδενικής γνώσης ε αν ισχύουν οι επόμενες ιδιότητες.

- **Πληρότητα (Completeness)**: Αν $x \in \text{L}$ και $R(x,w) = 1$ για κάποιο μάρτυρα w, τότε $\text{out}^{\mathcal{V}}_{\mathcal{P},\mathcal{V}}(x,w,z) = 1$ για κάθε συμβολοακολουθία z με συντριπτική πιθανότητα ν.

- **Εγκυρότητα (Soundness)**: Για κάθε πολυωνυμικού χρόνου πρόγραμμα $\mathcal{P}^*$ ορίζουμε

$$\pi_{x,w,z} = \text{Prob}[\text{out}^{\mathcal{V}}_{\mathcal{P}^*,\mathcal{V}}(x,w,z) = 1].$$

  Ένα πρωτόκολλο $\langle \mathcal{P}, \mathcal{V} \rangle$ ικανοποιεί την εγκυρότητα αν για κάθε $\mathcal{P}^*$ ισχύει ότι αν το $x \notin \text{L}$ τότε το $\pi_{x,w,z}$ είναι αμελητέο.

- **(Στατιστική) Μηδενική Γνώση ((Statistical) Zero-Knowledge)** (SZK): Για κάθε πολυωνυμικού χρόνου πρόγραμμα $\mathcal{V}^*$, υπάρχει ένα PTM πρόγραμμα S, που ονομάζεται ***simulator (προσομοιωτής)***, τέτοιο ώστε για κάθε x, w με $R(x,w) = 1$, οι τυχαίες μεταβλητές $S(x,z)$ και $\text{out}^{\mathcal{V}^*}_{\mathcal{P},\mathcal{V}^*}(x,w,z)$ είναι (στατιστικά) αδιαχώριστες για όλες τις συμβολοακολουθίες z:

$$\forall \mathcal{A} \left| \text{Prob}[\mathcal{A}(S(x,z)) = 1] - \text{Prob}[\mathcal{A}(\text{out}^{\mathcal{P}}_{\mathcal{P},\mathcal{V}^*}(x,w,z)) = 1] \right| < \varepsilon.$$

Εάν στον παραπάνω ορισμό περιοριστούμε μόνο στον $\mathcal{V}^*$, ο οποίος συμπεριφέρεται όπως ο $\mathcal{V}$ με μόνη διαφορά ότι στην τελική του έξοδο επισυνάπτει το σύνολο της συζήτησης, τότε μιλάμε για ***Μηδενική Γνώση Απέναντι σε Έντιμο Verifier (Honest Verifier Zero Knowledge – HVZK)***.

Η πληρότητα είναι όμοια με την σωστή λειτουργία του πρωτοκόλλου. Υποθέτοντας ότι ο prover και ο verifier ακολουθούν το πρωτόκολλο πιστά, η πληρότητα εγγυάται πως το πρωτόκολλο θα επιτύχει με ικανοποιητικά μεγάλη πιθανότητα.

Η διαισθητική ερμηνεία της εγκυρότητας διασφαλίζει πως το πρωτόκολλο θα αποτύχει όταν εκτελείται από έναν prover που χρησιμοποιεί έναν ψεύτικο μάρτυρα και από έναν τίμιο verifier.

Σημειώνεται ότι ο ορισμός της εγκυρότητας μας είναι πιο περιοριστικός (γι αυτό και απλούστερος) από προηγούμενους ορισμούς στη βιβλιογραφία, καθώς αποτυγχάνει σε πρωτόκολλα τα οποία επιτρέπουν μια σημαντική πιθανότητα ατιμίας από τον prover (π.χ. $1/2$). Στις πιο ενδιαφέρουσες περιπτώσεις τέτοια πρωτόκολλα μπορούν να κατασκευαστούν για να ικανοποιήσουν τον ορισμό μας μέσω παράλληλης ή ακολουθιακής επανάληψης.

Διαισθητικά, η στατιστική μηδενική γνώση είναι η ιδιότητα που απαγορεύει την εξαγωγή κάποιας γνώσης ενός verifier από έναν τίμιο prover. Αν ο verifier μπορεί να μάθει κάτι θα πρέπει να υπάρχει ένας αλγόριθμος που προσομοιώνει το πρωτόκολλο χωρίς πρόσβαση σε έναν μάρτυρα. Επιπλέον η εκτέλεση του αλγορίθμου είναι αδιαχώριστη από αυτή του πρωτοκόλλου.

Η μηδενική γνώση τίμιου verifier *(HVZK)* είναι ασθενέστερη εκδοχή της μηδενικής γνώσης. Σε αυτήν υποθέτουμε πως ο verifier εκτελεί το πρωτόκολλο τίμια, αλλά ενδεχομένως κάνει επιπλέον υπολογισμούς προς το συμφέρον του (honest but curious). Ειδικότερα, αυτό απεικονίζεται στον ορισμό μας περιορίζοντας τον V^* να προσομοιώνει τον verifier V και στο τέλος, να επιστρέφει ολόκληρη την επικοινωνία. Το να επιτύχουμε την ασθενέστερη ιδιότητα ονομάζεται μερικές φορές μηδενική γνώση *ημι-τίμιου (semi-honest)* verifier. Αν και αυτό χαλαρώνει τις προδιαγραφές του SZK, μπορεί να χρησιμοποιηθεί για να επιτύχουμε αποδείξεις μηδενικής γνώσεις σε καταστάσεις, χρησιμοποιώντας γενικές μεθόδους. Η απόδειξη μηδενικής γνώσης τίμιου verifier ανάγεται στην δημιουργία (από τον simulator) συνομιλιών αποδοχής του πρωτοκόλλου οι οποίες είναι αδιαχώριστες από τις συνομιλίες του πρωτοκόλλου μεταξύ τίμιου prover-verifier, χωρίς τη γνώση μάρτυρα.

Εκτός από την εγκυρότητα, σε ορισμένες περιπτώσεις θα χρησιμοποιήσουμε μια ισχυρότερη ιδιότητα, την ***εγκυρότητα γνώσης (knowledge soundness)***. Συγκεκριμένα:

Ορισμός 1.2.2. Εγκυρότητα Γνώσης (Knowledge Soundness): Για κάθε πολυωνυμικού χρόνου πρόγραμμα $\mathcal{P}^*$ ορίζουμε

$$\pi_{x,w,z} = \text{Prob}[\text{out}^{\mathcal{V}}_{\mathcal{P}^*,\mathcal{V}}(x,w,z) = 1].$$

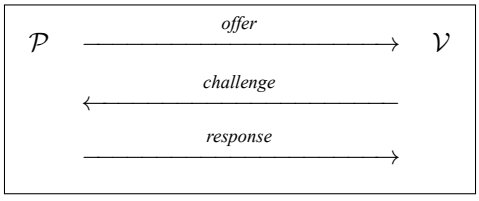
Ένα πρωτόκολλο $\langle \mathcal{P}, \mathcal{V} \rangle$ ικανοποιεί την εγκυρότητα αν για κάθε $\mathcal{P}^*$ υπάρχει πρόγραμμα , μια πιθανοτική Turing machine (PTM), που ονομάζεται ***knowledge extractor (εξαγωγέας γνώσης)*** με την ακόλουθη ιδιότητα. Έστω ότι

$$\tilde{\pi}_{x,w,z} = \text{Prob}[K(x,w,z) = w' : R(x,w') = 1].$$

Τότε ισχύει ότι αν το $\pi_{x,w,z}$ είναι μη αμελητέο, τότε και το $\tilde{\pi}_{x,w,z}$ είναι μη αμελητέο.

1.3 Το πρωτόκολλο του Schnorr

Ένα κλασικό πρωτόκολλο τριών κινήσεων που ικανοποιεί τις ιδιότητες μιας απόδειξης μηδενικής γνώσης είναι το πρωτόκολλο του Schnorr, ένα Σ-πρωτόκολλο (Σ-Protocol, από το διάγραμμα της ροής μηνυμάτων κατά την εκτελεσή του).



Το πρωτόκολλο του Schnorr λειτουργεί πάνω σε μία κυκλική ομάδα $G = \langle g \rangle$ τάξης q. Από την προηγούμενη συζήτησή μας, οι $\mathcal{P}$ και $\mathcal{V}$ έχουν γεννήτορες ομάδας $\langle \mathbb{G}, g, q \rangle$. Ο prover $\mathcal{P}$ διαλέγει ένα witness $w \in \mathbb{Z}_q$ τέτοιον ώστε $h = g^w$ για κάποιο $h \in \langle g \rangle$. Ο verifier $\mathcal{V}$ δέχεται $\mathbb{G}, g, q$ και h, και πρέπει να επιβεβαιώσει ότι $w = \log_g h$.

Αυτό μπορεί να περιγραφεί και σαν γλώσσα. Ορίζουμε το

$$\text{DLOG} = \{\langle \langle \mathbb{G}, g, q \rangle, h \rangle : h = g^w \text{ for some } w \in \mathbb{Z}_q\}$$

(το DLOG σημαίνει "discrete logarithm".) Υπό του πρωτοκόλλου του Schnorr, υπάρχει ένας αποδοτικός τρόπος να αποδείξουμε πως οποιαδήποτε πρόταση $\langle \langle \mathbb{G}, g, q \rangle, h \rangle$ ανήκει στο DLOG χωρίς να φανερώσουμε το $w = \log_g h$.

1. Ο $\mathcal{P}$ διαλέγει $t \xleftarrow{r} \mathbb{Z}_q$ και στέλνει το $y = g^t$ στον $\mathcal{V}$.
2. Ο $\mathcal{V}$ διαλέγει μια πρόκληση $c \xleftarrow{r} \mathbb{Z}_q$ και την στέλνει στον $\mathcal{P}$.
3. Ο $\mathcal{P}$ υπολογίζει το $s = t + wc \bmod q$ και στέλνει το s στον $\mathcal{V}$. Ο $\mathcal{V}$ ελέγχει και αποδέχεται αν και μόνο αν $g^s = yh^c$.

1.3.1 Ανάλυση

Πληρότητα Αν ο prover και ο verifier είναι τίμιοι τότε ισχύει ότι

$$g^s = g^{t+wc} = g^t (g^w)^c = yh^c.$$

Το πρωτόκολλο του Schnorr ικανοποιεί συνεπώς την πληρότητα και μπορεί πάντα να πείσει έναν τίμιο verifier.

Εγκυρότητα Το πρωτόκολλο (όπως και κάθε Σ-προτόκολλο) ικανοποιεί μια ειδική (ισχυρότερη) περίπτωση της εγκυρότητας.

Υποθέτουμε ότι μπορούμε να δημιουργήσουμε δύο αποδεκτές συνομιλίες από τον $\mathcal{P}$ με τιμές πρόκλησης $c \neq c'$: $\langle y, c, s \rangle$ και $\langle y, c', s' \rangle$. Αν τα s και s' είναι έγκυρα, τότε $g^s = yh^c$ and $g^{s'} = yh^{c'}$. Λύνοντας ως προς y τις δύο εξισώσεις υπολογίζεται ο διακριτός λογάριθμος.

$$\begin{aligned} y = g^s h^{-c} &= g^{s'} h^{-c'} \\ h^{c-c'} &= g^{s-s'} \\ h &= g^{(s-s')/(c-c')} \end{aligned}$$

Γενικότερα, ορίζουμε:

Ορισμός 1.3.1 (Ειδική Εγκυρότητα (Special Soundness)). Ένα προτόκολλο 3 κινήσεων (με πρώτη κίνηση από τον prover) είναι ειδικά έγκυρο αν: Υπάρχει PTM E τέτοιο ώστε για οποιαδήποτε πρόταση x και οποιεσδήποτε 2 αποδεκτές συνομιλίες της μορφής (a, c, s), (a, c', s') όπου $c \neq c'$, το $w \leftarrow E(x, a, c, c', s, s')$ αποτελεί μάρτυρα για το x, δηλαδή $R(x, w) = 1$.

Η ειδική εγκυρότητα είναι ισχυρότερη από την εγκυρότητα. Η απόδειξη αφήνεται ως άσκηση.

Εγκυρότητα και Εγκυρότητα Γνώσης Σε κάθε περίπτωση, η εγκυρότητα του προτοκόλλου του Schnorr είναι συχνά τετριμμένη: το να εξακριβώσουμε $\langle \langle \mathbb{G}, g, q \rangle, h \rangle$ ανήκει στο DLOG είναι ισοδύναμο με το αν $h \in \langle g \rangle$, το οποίο εξακριβώνεται εύκολα π.χ. αν ο p είναι πρώτος. Για αυτό το λόγο, θα καταφύγουμε στην εγκυρότητα γνώσης: δε μας αρκεί ο prover να δείξει ότι ο λογάριθμος του h υπάρχει, αλλά και ότι τον γνωρίζει

(Σε αντίθεση με την περίπτωση πχ των ισομορφικών γραφημάτων, όπου η ύπαρξη και μόνο του ισομορφισμού είναι μη τετριμμένη).

Για να δείξουμε ότι το προτόκολλο ικανοποιεί την εγκυρότητα γνώσης, θα βασιστούμε στην ειδική εγκυρότητα ώστε να κατασκευάσουμε τον εξαγωγέα K (ο οποίος λειτουργεί με πρόσβαση στον $\mathcal{P}$) βασιζόμενοι στον εξαγωγέα E ο οποίος λειτουργεί με πρόσβαση σε δύο συνομιλίες.

Αν και το παραπάνω δεν μας δικαιολογεί πώς μπορούμε να "αποσυμπιλήσουμε" τον $\mathcal{P}$ για να αποκτήσουμε την δεύτερη συζήτηση, μας δείχνει πώς να εξάγουμε έναν μάρτυρα ως $(s-s')/(c-c') \bmod q$. Υποθέτουμε πως έχουμε πρόσβαση στον $\mathcal{P}$ κατά τρόπο τέτοιον ώστε να μπορούμε να σταματήσουμε σε οποιοδήποτε σημείο και να επιστρέψουμε σε ένα προηγούμενο βήμα της εκτέλεσης προσομοιώνοντας ξανά την εκτέλεση.

Είναι χρήσιμο να δούμε το πιθανοτικό πρόγραμμα $\mathcal{P}$ σε δύο φάσεις:

1. Ο $\mathcal{P}(\text{first}, \langle \mathbb{G}, g, q \rangle, h)$ επιστρέφει $\langle y, \text{aux} \rangle$
2. Ο $\mathcal{P}(\text{second}, \langle \mathbb{G}, g, q \rangle, c, \text{aux})$ επιστρέφει $\langle s \rangle$

όπου aux αναπαριστά την εσωτερική πληροφορία που χρησιμοποιεί ο $\mathcal{P}$, χωρίς να την δημοσιεύει. Χρησιμοποιώντας αυτό, μπορούμε να κατασκευάσουμε έναν εξαγωγέα γνώσης K με την ακόλουθη δομή:

1. Έστω $\rho_1 \xleftarrow{\text{r}} \{0,1\}^{\lambda_1}$ οι ρίψεις νομισμάτων που απαιτούνται από το πρώτο βήμα του $\mathcal{P}$. Φιξάρουμε την τυχαιότητα του $\mathcal{P}$ με ρ_1 και προσομοιώνουμε $\mathcal{P}(\text{first}, \langle \mathbb{G}, g, q \rangle, h)$ για να λάβουμε y.
2. Διαλέγουμε $c \xleftarrow{\text{r}} \mathbb{Z}_q$.
3. Έστω $\rho_2 \xleftarrow{\text{r}} \{0,1\}^{\lambda_2}$ οι ρίψεις νομισμάτων που απαιτούνται από το δεύτερο βήμα του $\mathcal{P}$. Προσομοιώνουμε τον $\mathcal{P}(\text{second}, \langle \mathbb{G}, g, q \rangle, c, \text{aux})$ με φιξαρισμένη τυχαιότητα ρ_2 για να πάρουμε το s.
4. Διαλέγουμε $c' \xleftarrow{\text{r}} \mathbb{Z}_q$ και $\rho_2' \xleftarrow{\text{r}} \{0,1\}^{\lambda_2}$. Επαναλαμβάνουμε τα βήματα 2 και 3 για να πάρουμε το s'; Επιστρέφουμε τα $\langle y, c, s \rangle$ και $\langle y, c', s' \rangle$.

Αν ο εξαγωγέας γνώσης αποκτήσει δύο αποδεκτές συνομιλίες, μπορούμε να αναδημιουργήσουμε τον μάρτυρα όπως περιγράψαμε. Παραμένει να δείξουμε ότι ο εξαγωγέας γνώσης δημιουργεί δύο αποδεκτές συνομιλίες με σημαντική πιθανότητα. Για την απόδειξη χρειαζόμαστε το ακόλουθο λήμμα.

Λήμμα 1.3.1 (Splitting Lemma)**.** *Έστω X και Y πεπερασμένα σύνολα. Έστω $A \subseteq X \times Y$ το σύνολο των **καλών στοιχείων (good elements)** του $X \times Y$. Υποθέτουμε πως υπάρχει ένα κάτω φράγμα στον αριθμό των καλών αντικειμένων τέτοιο ώστε*

$$|A| \geq \alpha |X \times Y| .$$

*Ορίζουμε το σύνολο των **πολύ καλών στοιχείων (super-good elements)** A' να είναι το υποσύνολο του A τέτοιο ώστε*

$$A' = \left\{ (x,y) \in A \colon k_x > \frac{\alpha}{2} |Y| \right\}$$

όπου k_x είναι ο αριθμός των $y \in Y$ τέτοιο ώστε $(x,y) \in A$ για κάποιο φιξαρισμένο x. Τότε

$$|A'| \geq \frac{\alpha}{2} |X \times Y| .$$

Απόδειξη. Η απόδειξη γίνεται με εις άτοπον απαγωγή. Θεωρούμε πως $|A'| / |X \times Y| < \alpha/2$. Συνεπώς ισχύει ότι

$$|A| = |A'| + |A \setminus A'| < \frac{\alpha}{2} |X \times Y| + |A \setminus A'| . \tag{1}$$

Για κάθε $(x,y) \in A \setminus A'$, έχουμε ότι $k_x \leq (\alpha/2)|Y|$. Αφού υπάρχουν μόνο $|X|$ διαφορετικά x, ισχύει ότι $|A \setminus A'| \leq (\alpha/2)|X||Y|$. Από την (1) έχουμε ότι

$$|A| < \frac{\alpha}{2}|X \times Y| + \frac{\alpha}{2}|X||Y|.$$

Αυτό έρχεται σε αντίθεση με το κάτω φράγμα $|A|$, συνεπώς καταλήγουμε στο $|A'| \geq \alpha/2\,|X \times Y|$.

■

Επιστρέφουμε στην αποτελεσματική κατασκευή του εξαγωγέα γνώσης K. Ορίζουμε

$$X \times Y = \left\{(\rho_1, (c, \rho_2))\colon \rho_1 \in \{0,1\}^{\lambda_1},\ (c, \rho_2) \in \mathbb{Z}_q \times \{0,1\}^{\lambda_2}\right\}.$$

Αν ο prover είναι πειστικός με πιθανότητα τουλάχιστον α, ορίζουμε το A ναι είναι το σύνολο από $(\rho_1, (c, \rho_2))$ τα οποία αποδέχεται ο verifier. Τότε ισχύει ότι $|A| \geq \alpha\,|X \times Y|$. Αυτό σημαίνει πως μπορούμε να φιξάρουμε μια καλή ακολουθία $(\rho_1, (c, \rho_2))$ στο A τέτοια ώστε η συζήτηση που καταλήγουμε με τον K να είναι αποδεκτή. Από το Λήμμα 1.3.1, ο K βρίσκει μια πολύ καλή ακολουθία στα βήματα 1 εώς 3 με πιθανότητα $\alpha/2$.

Υποθέτουμε οτι ο εξαγωγέας γνώσης βρίσκει μια πολύ καλή ακολουθία. Τότε υπάρχει ξανά πιθανότητα $\alpha/2$ ο K να βρει μια άλλη καλή ακολουθία στο βήμα 4. Η πιθανότητα και οι δύο συζητήσεις να είναι αποδεκτές είναι $\alpha^2/4$. Επιπλέον, υπάρχει μόνο $1/m$ πιθανότητα ο K να παράγει την ίδια τιμή πρόκλησης $c = c'$.

Θεωρούμε το εξής: Έστω S το γεγονός ότι ο εξαγωγέας γνώσης είναι πειστικός. Έστω C το γεγονός $c \neq c'$ στην δεύτερη επιλογή, D το γεγονός η ακολουθία $(\rho_1, (c, \rho_2))$ να είναι πολύ καλή και E το γεγονός η ακολουθία $(\rho_1, (c', \rho_2'))$ να είναι καλή.

Συνεπάγεται ότι

$$\text{Prob}[S] \geq \text{Prob}[C \wedge D \wedge E] \geq \text{Prob}[D \wedge E] - \text{Prob}[\neg C] = \frac{\alpha^2}{4} - \frac{1}{q}.$$

Αυτό αποδεικνύει πως το πρωτόκολο του Schnorr ικανοποιεί την ιδιότητα της εγκυρότητας γνώσης.

Μηδενική Γνώση Το πρωτόκολλό τριών κινήσεων που είδαμε ικανοποιεί την μηδενική γνώση για τον τίμιο verifier. Για να το δείξουμε αυτο παρουσιάζουμε εναν αλγόριθμο ικανό να προσομοιώσει μια αποδεκτή συζήτηση μεταξύ ενός τίμιου prover και ενός (ημί) τίμιου verifier. Υποθέτουμε πως όταν έχει δοθεί η δημόσια πληροφορία του κατηγορήματος $\langle\langle \mathbb{G}, g, q\rangle, h\rangle$, τότε ο προσομοιωτής S διαλέγει τυχαια c και s από το $\mathbb{Z}_q$ και επιστρέφει $\langle g^s h^{-c}, c, s\rangle$. Θυμίζουμε ότι η έξοδος για το τίμιο μοντέλο είναι $\langle g^t, c, t + wc \bmod q\rangle$ όπου $t, c \xleftarrow{r} \mathbb{Z}_q$. Μπορούμε έυκολα να επαληθεύσουμε ότι οι δύο πιθανοτικές κατανομές είναι όμοιες, συνεπώς η HVZK ισχύει.

Πώς πετυχαίνουμε περισσότερα από την HVZK. Ενώ η HVZK είναι σχετικά μια αδύναμη ιδιότητα, είναι χρήσιμη ως ενδιάμεσο βήμα στην επέκταση των πρωτοκόλλων για την ικανοποίηση της (πλήρους) SZK. Υπάρχουν δυο γενικοί τρόποι που χρησιμοποιούν δύο είδη σχημάτων δέσμευσης, από τα οποία και τα δύο βασίζονται στην απαραίτηση σημασία της ανεξάρτητης επιλογής του y από το c.

Στην πρώτη μέθοδο, ο verifier είναι ο πρώτος που θα στείλει μήνυμα. Πριν λάβει το y, ο $\mathcal{V}$ διαλέγει το c και υπολογίζει το $(c', \sigma) \leftarrow \text{Commit}(c)$. Τότε ο $\mathcal{V}$ στέλνει c' στον prover. Όταν ο $\mathcal{P}$ στείλει y, τότε ο verifier επιστρέφει το (c, σ) για να ανοιχτεί η δέσμευση. Αν $\text{Verify}(c, c', \sigma) = 0$, ο prover σταματά το πρωτόκολλο. Αλλιώς το πρωτόκολλο ολοκληρώνεται χρησιμοποιώντας την πρόκληση c.

Επειδή το σχήμα δέσμευσης ικανοποιεί την ιδιότητα binding, οπότε ο $\mathcal{V}$ δεν μπορεί να αλλάξει το c. Γι' αυτό η στατιστική μηδενική γνώση ισχύει. Λόγω της ιδιότητας hiding , ο $\mathcal{P}$ δεν μπορεί να αντλήσει καμία πληροφορία για το t c και η εγκυρότητα δεν παραβιάζεται. Ένας προσομοιωτής για την ιδιότητα της μηδενικής γνώσης πρέπει να μπορεί να εξάγει το c από το c'. Αυτό ονομάζεται ***εξαγωγική (extractable)*** ιδιότητα για μια δέσμευση.

Στη δεύτερη μέθοδο ο πρώτος που θα μιλήσει θα είναι ο prover. Αφού υπολογίσει το y, ο $\mathcal{P}$ υπολογίζει το $(y', \sigma) \leftarrow \text{Commit}(y)$ και στέλνει το y' στον $\mathcal{V}$. Όταν ο $\mathcal{V}$ επιστρέψει το c, τότε ο $\mathcal{P}$ στέλνει το (y, σ, s) για να ανοιχτεί η δέσμευση. Αν $\text{Verify}(y, y', \sigma) = 0$, τότε ο verifier σταματά το πρωτόκολλο.

Αφού το σχημα δέσμευσης ικανοποιεί την ιδιότητα hiding, το y' δεν περιέχει καμία χρήσιμη πληροφορία για το y. Για το λόγο αυτό ο $\mathcal{V}$ αναγκάζεται να διαλέξει το c ανεξάρτητα από το y όπως είναι επιθυμητό. Οπότε το σχήμα ικανοποιεί την ιδιότητα της μηδενικής γνώσης.

Σημειώνουμε ότι η εγκυρότητα δεν παραβιάζεται υπό αυτού του σχήματος γιατί η ιδιότητα binding αποτρέπει τον $\mathcal{P}$ να ανοίξει το y με δύο διαφορετικούς τρόπους. Στην περίπτωση αυτή, ο προσομοιωτής μπορεί να προσπεράσει την ιδιότητα binding της δέσμευσης. Αυτό σημαίνει πως αν ο προσομοιωτής έχει δεσμευτεί για ένα αυθαίρετο y^*, αφού έχει λάβει την πρόκληση c, μπορεί να διαλέξει $y = g^s h^{-c}$. Δεσμεύσεις που επιτρέπουν τέτοια παραβίαση ονομάζονται ***διφορούμενες (equivocal)***.

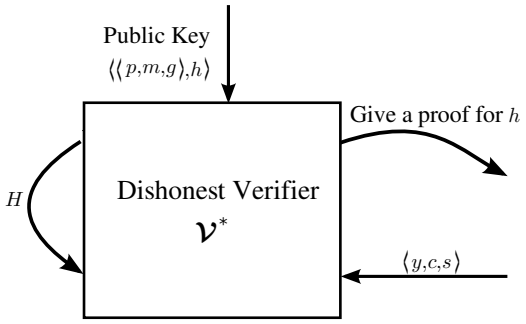
Παρατηρούμε ότι το πρώτο σχημα προσέθεσε μια νέα κίνηση στο πρωτόκολλο, ενώ το δεύτερο διατήρησε τη δομή των τριών κινήσεων. Για αυτόν το λόγο προτιμάται συνήθως το δεύτερο σχήμα. Όμως η παραπάνω συζήτηση ουσιαστικά ανάγει το πρόβλημα στο σχεδιασμό ενός σχήματος δέσμευσης που είτε είναι διφορούμενο ή επιτρέπει την εξαγωγική ιδιότητα του προσομοιωτή.

1.4 Μη Διαδραστικές Αποδείξεις Μηδενικής Γνώσης

Τώρα εισάγουμε μια μη διαδραστική έκδοση του πρωτοκόλλου του Schnorr, βασισμένοι στο γνωστό και ως ***Fiat-Shamir Heuristic***.

Για να φτιάξουμε μια μη διαδραστική απόδειξη χρησιμοποιούμε μια συνάρτηση κατακερματισμού $H: \{0,1\}^* \longrightarrow \mathbb{Z}_q$ τέτοια ώστε η συζήτηση $\langle y, c, s\rangle = \langle g^t, H(g^t), t + H(g^t)w \bmod q\rangle$. Αυτό υποχρεώνει το c να επιλέγεται μετά το y, εξαρτόμενο άμεσα απο τις ιδιότητες της συνάρτησης κατακερματισμού.

Για να δείξουμε ότι ισχύει η SZK, υποθέτουμε πως το H είναι ένα τυχαίο μαντείο που το ελέγχει ο προσομοιωτής. Στο μοντέλο τυχαίου μαντείου, ένας μη τίμιος verifier $\mathcal{V}^*$ μπορεί να κάνει ερωτήσεις στο τυχαιο μαντείο. Στο Σχήμα 3 φαίνεται πώς ο $\mathcal{V}^*$ αλληλεπιδρά με το H.



Σχήμα 3: Η προσομοίωση ενός μη τίμιου verifier $\mathcal{V}^*$ στο Μοντέλο Τυχαίου Μαντείου.

Όταν ο verifier ρωτήσει για την απόδειξη του $h = g^w$, τότε ο προσμοιωτής επιλέγει τυχαία τα c και s για να υπολογίσει τα $y = g^s h^{-c}$. Θέτει το (y, c) στο *History* και επιστρέφει $\langle y, c, s\rangle$. Ο μη τίμιος verifier δεν μπορεί να διαχωρίσει έναν τίμιο prover απο έναν εξομοιωτή εκτός αν $(y, c') \in History$ με $c \neq c'$. Τότε ο $\mathcal{V}^*$ επιτυγχάνει με πιθανότητα $(1/m)q_H$, όπου q_H είναι ο αριθμός των ερωτήσεων στο τυχαίο μαντείο.

Στη συνέχεια αποδεικνύουμε την εγκυρότητα γνώσης στο Μοντέλο Τυχαίου Μαντείου. Όπως και στο πρωτόκολλο του Schnorr, θέλουμε να παράξουμε δυο συζητήσης που καταλήγουν σε αποδοχή με το ίδιο y αλλά με διαφορετικές τιμές πρόκλησης. Χρησιμοποιώντας αυτές τις δύο συζητήσεις μπορούμε να εξάγουμε εναν μάρτυρα. Σημειώνουμε πως $c = H(y)$. Αν ένας μη τίμιος prover $\mathcal{P}^*$ κάνει μια μοναδική ερώτηση στο τυχαίο μαντείο πριν παράξει το $\langle y, c, s\rangle$, τότε η ανάλυση είναι η ίδια όπως με το διαδραστικό πρωτόκολλο. Τα προβλήματα εμφανίζονται όταν ο $\mathcal{P}^*$ κάνει παραπάνω από μια ερώτηση.

Υποθέτουμε πως στον αρχικό γύρο ο $\mathcal{P}^*$ κάνει q_H ερωτήσεις πριν τερματίσει την συζήτηση. Τότε ο εξαγωγέας γνώσης επιστρέφει τον $\mathcal{P}^*$ σε ένα προηγούμενο βήμα, χωρίς να υπάρχει εγγύηση πως ο $\mathcal{P}^*$ θα κάνει ξανά q_H ερωτήσεις. Όταν ο $\mathcal{P}^*$ τερματισει, θα επιστρέψει $\langle y', c', s'\rangle$ με $c' = H(y')$ και ενδεχομένως $y \neq y'$. Αυτό μειώνει την ικανότητά μας να εξάγουμε έναν μάρτυρα, οπότε θα πρέπει να τροποποιήσουμε καταλληλα την πιθανότητα λήψης δύο συζητήσεων αποδοχής με το ίδιο y.

Υποθέτουμε πως αφού κάνει q_H ερωτήσεις, ο $\mathcal{P}^*$ επιλέγει μια ερώτηση που έκανε και χρησιμοποιεί την αντίστοιχη απάντηση που πήρε για αυτήν από το τυχαίο μαντείο στην έξοδό του. Έστω $\text{Prob}[A] = \alpha$ η πιθανότητα πως η συζήτηση καταλήγει σε αποδοχή. Έστω $\text{Prob}[Q_i] = \beta_i$ η πιθανότητα ότι ο μη τίμιος prover χρησιμοποιεί την iοστη απάντηση, c_i όπου $1 \leq i \leq q_H$. Οριζουμε το $\text{Prob}[A \cap Q_i] = \alpha_i$. Αντίστοιχα, για την επανάλληψη του πειράματος γράφουμε A', Q'_j, c'_i Τότε ισχύει

$$\sum_{i=1}^{q_H} \alpha_i = \alpha \qquad \text{and} \qquad \sum_{i=1}^{q_H} \beta_i = 1.$$

Ορίζουμε ως $\text{Prob}[E]$ την πιθανότητα εξαγωγής ενός μάρτυρα από το $\mathcal{P}^*$, και έχουμε:

$$\text{Prob}[E] = \text{Prob}[A \cap A' \cap (i = j) \cap (c_i \neq c'_j)]$$

Ισοδύναμα, έχουμε: $\text{Prob}[E] \geq \text{Prob}[A \cap A' \cap (i = j)] - \text{Prob}[(c_i = c'_j)]$, δηλαδή:

$$\begin{aligned}\text{Prob}[E] &\geq \text{Prob}[A \cap A'] - \frac{1}{q} \\ &= \sum_{i=1}^{q_H} \text{Prob}[A_{\cap} Q_i \cap A' \cap Q_i'] - \frac{1}{q} \\ &= \sum_{i=1}^{q_H} \text{Prob}[A_i \cap A_i'] - \frac{1}{q}\end{aligned}$$

Απο τον ορισμό του εξαγωγέα τους υπολογισμούς μας στην ενότητα 1.3, γνωρίζουμε ότι:

$$\text{Prob}[A_i \cap A_i'] \geq \frac{\text{Prob}[A_i]^2}{4} = \frac{\alpha_i^2}{4}.$$

Η συνολική πιθανότητα υπολογίζεται ως εξής.

$$\begin{aligned}\text{Prob}[E] &\geq \sum_{i=1}^{q_H} \text{Prob}[A_i \cap A_i'] - \frac{1}{q} \\ &= \frac{1}{4} \sum_{i=1}^{q_H} \alpha_i^2 - \frac{1}{q}\end{aligned}$$

Από τη στατιστική γνωρίζουμε ότι $\frac{\sum(\alpha_i^2)}{q_H} \geq (\frac{\alpha}{q_H})^2$, και άρα $\sum(\alpha_i^2) \geq \frac{\alpha}{q_H}$, για οποιουσδήποτε πραγματικούς α_i έχουν μέσο όρο $\frac{\alpha}{q_H}$. Καταλήγουμε λοιπόν στο ότι δεδομένου ενός πειστικού prover, μπορούμε να εξάγουμε εναν μάρτυρα με πιθανότητα:

$$\frac{\alpha^2}{4q_H} - \frac{1}{q}.$$

1.5 Μηδενική Γνώση Τίμιου Verifier για όλο το NP

Τα πάντα στο NP μπορούν να αποδειχθούν με ένα πρωτόκολλο μηδενικής γνώσης τριών κινήσεων. Θεωρούμε τη γλώσσα HC όλων των Hamlitonian γραφημάτων. Θυμίζουμε πως ένας ***κύκλος Hamiltion (Hamiltonian cycle)*** π είναι ένα μονοπάτι στο γράφημα G που επισκέφτεται κάθε κόμβο ακριβώς μια φορά πριν επιστρέψει στο αρχικό σημείο. Το HC είναι NP-complete, οπότε μια απόδειξη γνώσης για το HC θα έδινε μια απόδειξη γνώσης για ολα τα προβλήματα στο NP: Δεδομένου ενός στιγμιοτύπου το προβλήματος στο NP, μπορούμε να το μεταμορφώσουμε σε ενα γράφημα κύκλο Hamilton αν και μόνο αν είναι ένα στιγμιότυπο αποδοχής για το πρόβλημα. Τότε μπορούμε να χρησιμοποιήσουμε την απόδειξη της HC για οποιοδήποτε πρόβλημα στο NP.

Ένα γραφημα με n κόμβους μπορεί να αναπαρασταθεί με εναν $n \times n$ δυαδικό πίνακα που ονομάζεται ο ***πίνακας πρόσπτωσης (adjacency matrix)*** του γραφήματος. Αν ο i-οστός κόμβος συνδέεται με τον jοστό, τοτε το στοιχείο του πίνακα ij είναι 1, διαφορετικά είναι 0. Δεδομένης μιας αναδιάταξης π στο $\{1, ..., n\}$ και ενός γραφήματος G που ορίζεται από τον πίνακα πρόσπτωσης (a_{ij}), ορίζουμε το αναδιαταγμένο γράφημα G^{π} ως το γράφημα που έχει πίνακα πρόσπτωσης $(a'_{ij}) = (a_{\pi^{-1}(i)\pi^{-1}(j)})$. Ένας κύκλος Hamiltonin είναι ένα γράφημα που μπορεί να αναπαρασταθεί από μια αναδιάταξη π των κόμβων με την ειδική ιδιότητα πως το γράφημα G^{π} συμπεριλαμβάνει τις ακμές $(1, 2), (2, 3), ..., (n-1, n), (n, 1)$.

Αν το π είναι κύκλος Hamilton για ένα γράφημα G και π' είναι μια αυθαίρετη αναδιάταξη τότε το $\pi'^{-1} \circ \pi$ είναι ένας κύκλος Hamilton για ενα γράφημα $G^{\pi'}$.

Οι αποδειξεις HVZK μπορούν να χρησιμοποιηθούν για να επαληθεύσουμε ότι ένας κύκλος Hamilton υπάρχει σε ενα γράφημα χωρίς να αποκαλύψουμε τον κύκλο. Το Σχήμα 4 παρουσιάζει πώς μια απόδειξη

HVZK μπορεί να υλοποιηθεί. Σημειώνουμε πως ένας μη τίμιος prover μπορεί να μην φανερωθεί με πιθανότητα $\kappa = 1/2$. Υποθέτουμε πως ο prover δεσμεύεται σε έναν λάθος πίνακα πρόσπτωσης με τον οποίον κατασκευάζει τον κύκλο Hamliton. Αν ο verifier επιστρέψει $c = 0$, τότε ο verifier μαθαίνει πως ο prover δεν δεσμεύθηκε σε σωστή αναδιάταξη του γραφήματος. Σε k επαναλήψεις όμως, μπορεί να μειώσει την πιθανότητα του λάθους του σε $\kappa = 1/2^k$ και έτσι να ικανοποιήσει την ιδιότητα της εγκυρότητας.

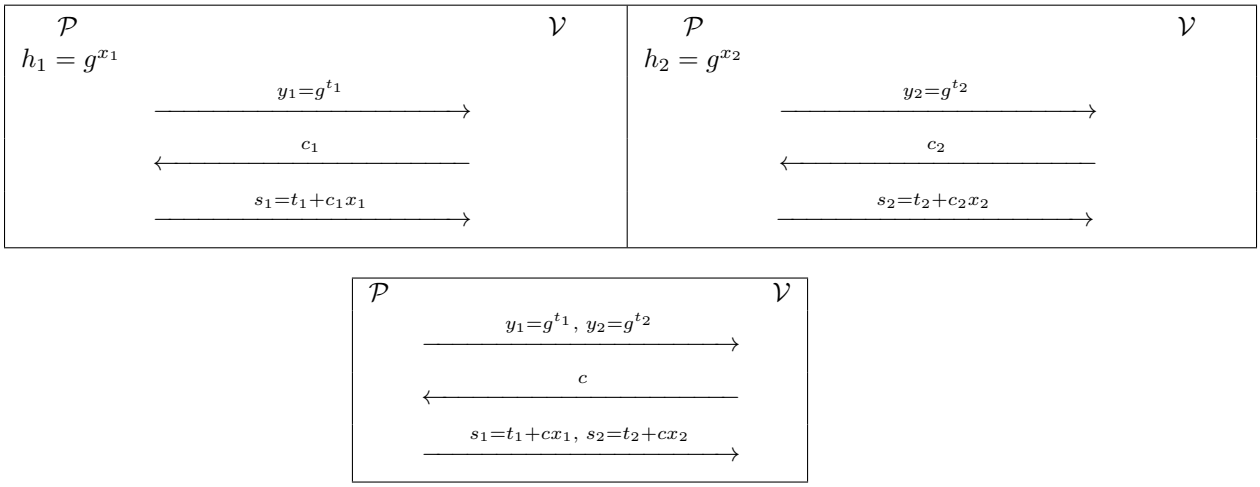
$\mathcal{P}$(προσωπική είσοδος π)		$\mathcal{V}$
	Το γράφημα G	
Διαλέγουμε μια τυχαία αναδιάταξη π' του γραφήματος G. Δεσμευόμαστε στον πίνακα πρόσπτωσης του γραφήματος $G^{\pi'}$	$\begin{bmatrix} \text{com}_{11} & \cdots & \text{com}_{1n} \\ \vdots & \ddots & \vdots \\ \text{com}_{n1} & \cdots & \text{com}_{nn} \end{bmatrix}$ $\longrightarrow$	
		$c \xleftarrow{\text{r}} \{0,1\}$
	$\longleftarrow$ c	
Αν $c = 0$, τότε ανοίγουμε όλες τις δεσμεύσεις και στέλνουμε το π'^{-1}. Αν $c = 1$, τότε σε κάθε γραμμή λέμε ποιές δεσμεύσεις χρειάζεται να ανοικτούν (εξαρτάται από το π)		
	Ανοίγουμε το com βασιζόμενοι στο c $\longrightarrow$	
		Επαληθεύουμε τις δεσμεύσεις: Αν $c = 0$, ελέγχουμε αν ο πίνακας ισούται με $G^{\pi'}$; Αν $c = 1$, ελέγχουμε αν αποκαλύπτεται ο κύκλος

Σχήμα 4: Μια απόδειξη γνώσης ενός κύκλου Hamilton. Επιπρόσθετα με την δέσμευση στον πίνακα πρόσπτωσης $G^{\pi'}$, ο prover πρέπει να κάνει μια ξεχωριστή δέσμευση com_{ij} σε κάθε στοιχείο του πίνακα.

1.6 Η Σύζευξη δύο Αποδείξεων Μηδενικής Γνώσης

Υπάρχουν στιγμιότυπα στα οποία ένας prover θέλει να ελέγξει διάφορες προτάσεις με μια αλληλεπίδραση, είτε λόγω αποτελεσματικότητας είτε λόγω ιδιωτικότητας. Στα Σ-πρωτόκολλα, αυτό μπορεί να γίνει χρησιμοποιώντας μια μοναδική πρόκληση διατηρώντας την δομή τριών κινήσεων. Όταν λάβει την πρόκληση ο prover συνδυάζει τις απαντήσεις όπως φαίνεται στο Σχήμα 5.

Θεώρημα 1.6.1. *Η σύζευξη δύο αποδειξεων μηδενικής γνώσης τίμιου verifier ικανοποιεί την ιδιότητα της (ειδικής) εγκυρότητας και της HVZK.*



Σχήμα 5: Η σύζευξη δύο αποδείξεων μηδενικής γνώσης για το διακριτό λογάριθμο.

1.7 Η διάζευξη δύο αποδείξεων μηδενικής γνώσης (Disjunction of ZK Proofs)

Στην ενότητα 1.1 αναφέραμε πως κάποια σχήματα ταυτοποίησης χρήστη περιέχουν λεξικά με διάφορες προτάσεις θεωρημάτων που αντιστοιχίζονται σε κάθε χρήστη. Σε τετοια σχήματα, μπορεί να εμφανιστούν προβλήματα ιδιωτικότητας όταν οι χρήστες θέλουν να έχουν πρόσβαση χωρίς να φανερώσουν τους εαυτούς τους. Με τη σύζευξη δύο αποδείξεων μηδενικής γνώσης, ένα πρωτόκολλο ταυτοποίησης ρωτά τον χρήστη $\mathcal{P}$ να δώσει έναν μάρτυρα σε δύο προτάσεις. Ο χρήστης προφανώς γνωρίζει τον μάρτυρα για μια απο τις προτάσεις, αλλά δεν χρειάζεται να αποκαλύψει σε ποιά. Το σύστημα $\mathcal{V}$ στέλνει μια μοναδική τιμή πρόκλησης c την οποία ο χρήστης μπορεί να διαχωρίσει σε δύο επιμέρους προκλήσεις για κάθε πρόταση με τον όρο ότι το άθροισμά τους πρέπει να είναι αυτό που διάλεξε το σύστημα.

Αναφορικά με την πρόταση που δεν γνωρίζει μάρτυρα, ο $\mathcal{P}$ χρησιμοποιεί τον simulator. Για να είναι έγκυρη η συζήτηση του simulator, ο $\mathcal{P}$ θα αναγκαστεί να μοιράσει την πρόκληση ώστε η πρόταση που δεν γνωρίζει να έχει ως τιμή αυτήν που χρησιμοποίησε ο simulator. Στην πρόταση για την οποία γνωρίζει ένα μάρτυρα θα αναγκαστεί να χρησιμοποιήσει ως πρόκληση τη διαφορά. Αυτό δεν είναι πρόβλημα αφού γνωρίζοντας το μάρτυρα μπορεί να απαντήσει σε κάθε πρόκληση.

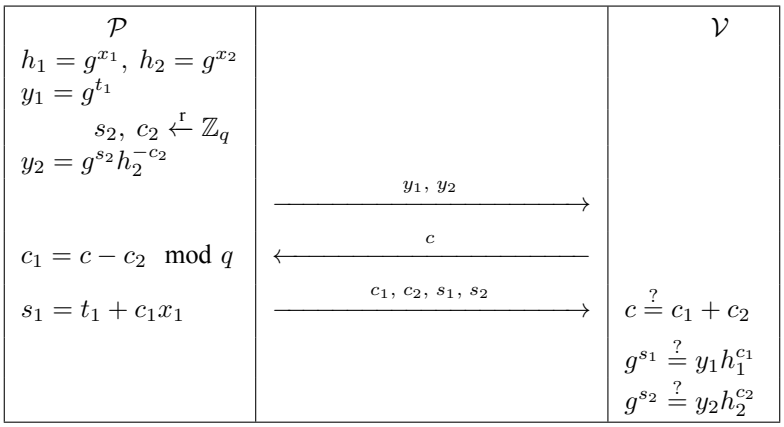
Παρατηρούμε ότι εάν ο $\mathcal{P}$ αποπειραθεί να προσομοιώσει τις αποδείξεις και των δύο προτάσεων (αντί μίας), δε θα έχει τρόπο να εξασφαλίσει ότι το άθροισμα των προκλήσεων θα ταυτίζεται με την τιμή που υπέδειξε το σύστημα $\mathcal{V}$.

Στο Σχήμα 6 αναπαρίσταται η εκτέλεση μιας διάζευξης.

Στο Σχήμα 6 αναπαρίσταται η εκτέλεση μιας διάζευξης για Σ-πρωτόκολλα.

Θεώρημα 1.7.1. *Η διάζευξη δύο αποδείξεων μηδενικής γνώσης τίμιου verifier ικανοποιεί την ιδιότητα της (ειδικής) εγκυρότητας και της HVZK.*

Notes by S. Pehlivanoglu, J. Todd, & H.S. Zhou. Edits by Pyrros Chaidos



Σχήμα 6: Η διάζευξη δύο αποδείξεων μηδενικής γνώσης για τον διακριτό λογάριθμο δείχνοντας πως ο prover μπορεί να πείσει τον verifier πως γνωρίζει έναν από τους δύο διακριτούς λογαριθμους f h_1, h_2 (χωρίς να αποκαλύπτει ποιον). Σε αυτή την περίπτωση ο prover $\mathcal{P}$ γνωρίζει τον μάρτυρα r h_1.