Bezznalostné dôkazy (Zero knowledge proofs)

Martin Stanek

2025

KI FMFI UK Bratislava

Úvod

- základný scenár bezznalostných (ZK) dôkazov
  - protokol s dvoma účastníkmi, dokazovateľ (P) a overovateľ (V)
  - dokázať tvrdenie bez prezradenie čohokoľvek okrem pravdivosti samotného tvrdenia
  - V nechce akceptovať nepravdivé tvrdenie & P chce úspešne dokázať pravdivé tvrdenie
  - *Prečo si to V nedokáže sám?* – P výpočtovo silnejší, resp. s dodatočnou informáciou
- rôznorodé aplikácie
  - vynútenie čestného správania účastníkov v protokoloch
  - identifikačné protokoly (autentifikácia na základe znalosti)
  - kryptomeny zamerané na súkromie, napr. Zcash, Monero (prostredníctvom Bulletproofs)
  - zk-SNARK (Succinct Non-Interactive ARguments of Knowledge)
  - zk-STARK (Scalable Transparent ARgument of Knowledge)

Cieľ: Vysvetliť vlastnosti ZK dôkazov, predstaviť základné konštrukcie.

„Tvrdenia“

- Čo vlastne dokazovateľ dokazuje?
- príslušnosť vstupu x do jazyka L – interaktívne dokazovacie systémy
  - výpočtovo neobmedzený P, pravdepodobnostný polynomiálny V
  - graf má Hamiltonovský cyklus, formula je splniteľná (SAT), …
- znalosť „svedka“ vo vhodnej relácii
  - dôkazy znalosti (proofs of knowledge) s výpočtovo neobmedzeným P
  - argumenty znalosti s výpočtovo efektívnym P (PPT algoritmus)
  - P pozná Hamiltonovský cyklus, splniteľné priradenie, diskrétny logaritmus, …

NP relácia

- $R \subseteq \{0,1\}^* \times \{0,1\}^*$ určená deterministickým polynomiálnym algoritmom $W(\cdot,\cdot)$
  - $R = \{(x,w) : W(x,w) \text{ akceptuje}\}$, w je svedkom x v relácii R
  - W je polynomiálny vzhľadom na dĺžku prvého vstupu, teda aj $|w| \leq p(|x|)$
- súvisiaci NP jazyk: $L_R = \{x : \exists w\ W(x,w) \text{ akceptuje}\}$, ľahko vidieť, že $L_R \in \text{NP}$

NP relácia a svedok

NP relácia

- $R \subseteq \{0,1\}^* \times \{0,1\}^*$ určená deterministickým polynomiálnym algoritmom $W(\cdot,\cdot)$
  - $R = \{(x,w) : W(x,w) \text{ akceptuje}\}$, w je svedkom x v relácii R
  - W je polynomiálny vzhľadom na dĺžku prvého vstupu, teda aj $|w| \leq p(|x|)$
- súvisiaci NP jazyk: $L_R = \{x : \exists w\ W(x,w) \text{ akceptuje}\}$, ľahko vidieť, že $L_R \in \text{NP}$

Príklady

- HAM: nech G je graf, π je permutácia vrcholov grafu
  - $W(G,\pi)$ akceptuje, ak poradie vrcholov v π je Hamiltonovskou kružnicou v G
  - L_R je jazyk obsahujúci Hamiltonovské grafy (NP-úplný)
- DL: nech $(G,\cdot)$ je grupa s generátorom g, nech $y \in G$
  - $W(y,w)$ akceptuje, ak $g^w = y$; svedok je diskrétny logaritmus
  - $L_R = G$, triviálny jazyk obsahujúci všetky prvky grupy
- pre každý NP jazyk L existuje NP relácia R taká, že $L_R = L$
- pre každú NP reláciu R je jazyk L_R v triede NP

Triviálne neinteraktívne dôkazy

- príslušnosť do jazyka $x \in L_R$
  - R je NP relácia
  - neobmedzený P, PPT V
- P pošle V svedka w pre x
  - V akceptuje, ak $W(x, w)$ akceptuje
- P pošle Hamiltonovskú kružnicu, splniteľné priradenie, … V overí, že je to správne
- pre triviálne jazyky by sme svedka nepotrebovali

Úplnosť (Completeness)
$\forall x \in L_R$: V akceptuje

Korektnosť/zdravosť (Soundness)
$\forall x \notin L_R$: V neakceptuje

- P prezrádza „všetko“ (svedka)
- V sa dozvie niečo, čo by možno nevedel sám vypočítať
- dá sa dokazovať „viac“ (interakcia)
- dá sa dokazovať bezznalostne

Interaktívne dokazovacie systémy (príslušnosť do jazyka)

Interaktívny dokazovací systém (IDS)

Dvojica (P, V) je IDS pre jazyk L

- P a V spolu komunikujú
- neobmedzený P
- PPT V, teda aj polynomiálny počet kôl, dĺžky správ a pod.
- spoločný vstup x, V akceptuje/zamieta
  - $(P, V)(x) = 1/0$

Úplnosť

$\forall x \in L$: $\Pr[(P, V)(x) = 1] \geq 2/3$

Korektnosť/zdravosť

$\forall x \notin L \; \forall P^*$: $\Pr[(P^*, V)(x) = 1] \leq 1/3$

- pravdepodobnosti $2/3$ resp. $1/3$ možno opakovaním a „hlasovaním“ o výsledku stlačiť blízko k 1 resp. k 0
- úplnosť: P aj V sa správajú čestne
- korektnosť: V sa nenechá oklamať ľubovoľným P^*
- IP – trieda jazykov, pre ktoré existuje IDS
- IP = PSPACE

Príklad: GNI

- jazyk neizomorfných grafov
- GNI $= \{(G_1, G_2) : G_1 \not\simeq G_2\}$
- GNI $\in$ co-NP
- V volí náhodné izomorfné kópie G_1/G_2
- P počíta, z ktorého grafu kópia vznikla

Protokol – opakujeme k krát:

1. $V \to P$: H; $\quad H \simeq_R G_b$; $b \in_R \{1, 2\}$
2. $P \to V$: $b' \in \{1, 2, \perp\}$
3. V overí, či $b = b'$; ak nie, tak zamietne

V akceptuje po k úspešných kolách

Úplnosť ($G_1 \not\simeq G_2$)

- P uspeje vždy, lebo H môže byť izomorfné len s jedným G_b

Korektnosť/zdravosť ($G_1 \simeq G_2$)

- H je izomorfné s oboma grafmi
- P^* uspeje v jednom kole s pravd. $1/2$
- V akceptuje vstup s pravd. 2^{-k}

Bezznalostnosť (ZK) – intuícia

- znalosť ≈ niečo, čo nie je možné efektívne vypočítať (PPT)
- ZK IDS pre čestného overovateľa
  - V sa v interakcii s P nedozvie nič, čo by si nevedel sám vypočítať
- ZK IDS
  - ľubovoľný V^* (stále PPT) sa v interakcii s P nedozvie nič, čo by si nevedel sám vypočítať
- „nič sa nedozvedieť“
  - komunikácia s P je efektívne simulovateľná tak, že sa od skutočnej nedá odlíšiť
- predchádzajúci protokol pre GNI je ZK pre čestného overovateľa, ale nie je ZK vo všeobecnosti
  - V^* nemusí skonštruovať H ako izomorfnú kópiu G_1 alebo G_2 (vygeneruje náhodné H)
  - P mu vypočíta, či a s ktorým G_b je H izomorfný, pričom V^* si to nevie vypočítať sám

ZK formálnejšie

- view(P, V, x) – náhodná premenná obsahujúca komunikáciu $P \leftrightarrow V$ na vstupe x
- IDS (P, V) pre L je perfektne ZK pre čestného overovateľa, ak

$$\exists \text{ PPT } S \; \forall x \in L : \text{view}(P, V, x) = S(x)$$

- IDS (P, V) pre L je perfektne ZK, ak

$$\forall \text{ PPT } V^* \; \exists \text{ PPT } S \; \forall x \in L : \text{view}(P, V^*, x) = S(x)$$

- perfektne ZK $\approx$ simulovaná komunikácia je identická so skutočnou
- ZK je definovaná len pre $x \in L$

Simulátor pre čestného overovateľa v GNI protokole

- komunikácia P s čestným overovateľom V je sada k dvojíc
  - $\langle H_i, b_i \rangle_{i=1}^{k}$, kde $b_i \in_R \{1, 2\}$ a $H \simeq_R G_{b_i}$
- simulátor vygeneruje najskôr b_i a následne H_i
  - triviálne PPT
  - triviálne je komunikácia distribuovaná identicky so skutočnou komunikáciou

Poznámky

- Typy ZK konštrukcií:
  - perfektne: simulovaná komunikácia je identická so skutočnou
  - výpočtovo: simulovaná komunikácia je nerozlíšiteľná od skutočnej v PPT (pravdepodobnosť rozlíšenia je zanedbateľná) … CZK
- CZK = IP (ak existuje jednosmerná funkcia)
- ukážeme NP ⊆ CZK
  - CZK pre jazyk HAM grafov obsahujúcich Hamiltonovskú kružnicu
  - HAM je NP-úplný

- použijeme záväzkovú schému
  - nech $\sigma(x)$ označuje záväzok x
  - záväzok matice: samostatné záväzky jednotlivých prvkov
- označenia:
  - M_G je incidenčná matica grafu G
  - $\pi(G)$ permutácia vrcholov grafu

Protokol – vstup je graf G

opakujeme k krát:

1. $P \to V$: $\boxed{\text{G}} = \sigma\left(M_{\pi(G)}\right)$
2. $V \to P$: $c \in_R \{0, 1\}$
3. $P \to V$:
   $c = 0$: π a odkrytie všetkých záväzkov z prvého kroku;
   $c = 1$: odkrytie len tých záväzkov, ktoré vytvárajú Hamiltonovskú kružnicu v $\boxed{\text{G}}$
4. V overí, či je odpoveď P v poriadku; ak nie, tak zamietne

V akceptuje po k úspešných kolách

Vlastnosti protokolu pre HAM

Úplnosť

- nech $G \in \text{HAM}$
- P dokáže uspieť v protokole vždy (stačí ho dodržať)

Korektnosť/zdravosť

- nech $G \notin \text{HAM}$
- predpokladajme σ s perfektnou záväznosťou
  - keďže P^* je výpočtovo neobmedzený
- P^* uspeje v jednom kole s pravd. $1/2$
  - potrebuje uhádnuť c predtým, ako sa zaviaže ku $\boxed{\text{G}}$
  - pravdepodobnosť celkovo: 2^{-k}

ZK

- black-box simulácia jedného kola $P \leftrightarrow V^*$:
  1. S zvolí $c' \in \{0, 1\}$
  2. ak $c = 0$, tak S vytvorí $\boxed{\text{G}}$ rovnako ako P v protokole
  3. ak $c = 1$, tak S zvolí náhodne Hamiltonovský graf H a namiesto $\boxed{\text{G}}$ použije $\sigma(H)$
  4. S simuluje V^* na vstupe $\boxed{\text{G}}$, resp. $\sigma(H)$ a získa c
  5. ak $c \neq c'$, tak S resetuje V^* do stavu pred 4. krokom a začne znova; inak vie S vypísať simul. komunikáciu

Poznámky

- simulátor S je PPT
- simulovaná komunikácia nie je identická so skutočnou
  - niekedy je záväzkom iný graf ako $\pi(G)$
  - keďže záväzková schéma má vlastnosť utajenia (hoci výpočtovo), v PPT nevieme skutočnú a simulovanú komunikáciu rozlíšiť
  - protokol je výpočtovo ZK (CZK)
- IDS, hoci aj ZK, nie sú prakticky príliš užitočné
  - zvyčajne nepotrebujeme dokazovať príslušnosť do jazyka
  - znalosť nejakého tajného alebo súkromného parametra, príp. vzťahov medzi viacerými parametrami
  - neobmedzene výpočtovo silný dokazovateľ je nerealistický koncept

Dôkazy / argumenty znalosti

Dôkazy / argumenty znalosti

- majme $x \in L$; a nech R je prislúchajúca NP-relácia, teda $L = L_R$
- niekedy chceme, aby P dokázal, že naozaj pozná svedka w: $W(x, w)$ akceptuje
  - neobmedzene výpočtový P nemá problém w zistiť
  - pre PPT P nie je schopnosť dokázať $x \in L$ to isté ako znalosť svedka, napr.
    $R = \{(n, p) : \ p, n \in \mathbb{N}, \ p \mid n, \ p \notin \{1, n\}\}$, L_R – množina zložených čísel
- triviálny dôkaz znalosti svedka je poslať w overovateľovi
  - V overí výpočtom $W(x, w)$
  - problém: vo všeobecnosti nie je ZK - pošleme Hamiltonovskú kružnicu, diskrétny log, …
- vlastnosti: úplnosť, ~~korektnosť/zdravosť~~ $\mapsto$ extraktor znalosti
  - následne môže/nemusí mať protokol aj vlastnosť ZK (formalizácia simuláciou)

Extraktor znalosti

- znalosť nemusí byť explicitná, kde P používa priamo w
- znalosť definujeme ako schopnosť w efektívne vypočítať (extrahovať) z P
- PPT E nazývame extraktor znalosti, ak $\forall\, P^*\ \forall x \in L_R$:

$$\Pr\left[(x,w) \in R :\ w \leftarrow E^{P^*}(x)\right] \geq \Pr[(P^*, V)(x) = 1]$$

  - neformálne: ak P^* uspeje v protokole, dokážeme z interakcie s ním získať w
  - extraktor vie „resetovať“ P^*
  - extrakcia definovaná len pre $x \in L_R$ (v opačnom prípade svedok neexistuje)
  - niekedy je vzťah medzi pravdepodobnosťami voľnejší
  - E vie overiť či je w správne a vie spúšťať extrakciu viackrát (znížiť pravd. neúspechu)

Schnorrov protokol – dôkaz znalosti diskrétneho logaritmu

- $(G, \cdot)$ grupa prvočíselného rádu p s generátorom g
- spoločný vstup: $x \in G$
- P pozná $w \in \mathbb{Z}_p$: $g^w = x$

Protokol

1. $P \to V$: $a = g^r$, $r \in_R \mathbb{Z}_p$
2. $V \to P$: $c \in_R \mathbb{Z}_p$
3. $P \to V$: $z = r + cw$
4. V akceptuje práve vtedy, keď $g^z = ax^c$

Úplnosť

$$g^z = g^{r+cw} = a \cdot (g^w)^c = ax^c$$

Extraktor znalosti

- nech P^* uspeje v protokole
- E zbehne protokol s P^* (a, c, z) a po úspešnom dobehnutí resetuje P^* do stavu v kroku 2, kde zvolí $c' \neq c$
- ak P^* uspeje, máme dva úspešné behy:

$$g^z = ax^c \wedge g^{z'} = ax^{c'} \Rightarrow w = \frac{z - z'}{c - c'}$$

Perfektne ZK pre čestného overovateľa (HVZK)

- čestný overovateľ ⇒ c je volené uniformne náhodne
- simulátor S:
  - zvolí $c \in_R \mathbb{Z}_p$, $z \in_R \mathbb{Z}_p$
  - vypočíta $a = g^z / x^c$
  - výstup je trojica (a, c, z)
- výstup distribuovaný rovnako ako komunikácia $P \leftrightarrow V$
- nie je ZK pre nečestného overovateľa
  - V^* môže zvoliť c akokoľvek, nedá sa simulovať ako black-box (pravd., že trafíme c je zanedbateľná)
- varianty protokolu pre ZK:
  - výzva $c \in \{0, 1\}$ a opakujeme k krát black-box simulácia ako pri HAM
  - V pošle záväzok k zvolenému c predtým, ako sa dozvie a (aplikovateľné nielen pre Schnorrov protokol)
- nečestný V^* nevadí v neinteraktívnych dôkazoch/argumentoch

Σ-protokol pre NP reláciu R:
vstupy účastníkov: $P(x, w)$; $V(x)$

1. $P \to V$: a (oznámenie/záväzok)
2. $V \to P$: $c \in_R C$ (výzva)
3. $P \to V$: z (odpoveď)

V zamietne alebo akceptuje, deterministicky v PT zo vstupu a komunikácie: (x, a, c, z)

Vlastnosti

- perfektná úplnosť ($x \in L_R$): V vždy akceptuje
- špeciálna korektnosť/zdravosť: existuje PPT extraktor, ktorý z $x \in L_R$ a dvojice akceptujúcich komunikácií (a, c, z), (a, c', z') s $c \neq c'$ vypočíta w také, že $(x, w) \in R$
- špeciálna HVZK: existuje PPT simulátor S
  - $\forall x \in L_R \; \forall c \in C$: $S(x, c)$ vygeneruje akceptačnú komunikáciu (a, c, z), distribuovanú rovnako ako v skutočnej komunikácii (kde V použije c)

Poznámky k Σ-protokolom

- Σ-protokol pre reláciu R je zároveň dôkaz/argument znalosti pre R
- Schnorrov protokol je Σ-protokol
- Σ-protokoly je možné skladať, pričom výsledný protokol je opäť Σ-protokol, napr.
  - nech (P_0, V_0) je Σ-protokol pre R_0
  - nech (P_1, V_1) je Σ-protokol pre R_1
  - $R_{\text{AND}} = \{((x_0, x_1), (w_0, w_1)) : (x_0, w_0) \in R_0, (x_1, w_1) \in R_1\}$
  - $R_{\text{OR}} = \{((x_0, x_1), (b, w_b)) : (x_b, w_b) \in R_b, b \in \{0, 1\}\}$

Σ-protokol pre R_{AND}

$\boldsymbol{R_{\text{AND}}}$ (paralelný beh s rovnakým c):

1. $P \to V$: (a_0, a_1), kde a_i je oznámenie P_i
2. $V \to P$: c (predpokladáme rovnaký priestor výziev v oboch protokoloch)
3. $P \to V$: (z_0, z_1), kde z_i je odpoveď P_i

V akceptuje práve vtedy, keď $V_0(x_0, a_0, c, z_0)$ akceptuje $\wedge$ $V_0(x_1, a_1, c, z_1)$ akceptuje

- spôsob ako vyrobiť neinteraktívny protokol
  - argument znalosti, príp. Σ-protokol
  - V posiela „iba“ náhodné výzvy a overuje odpovede P (*public coins*)
- Σ-protokol
  - nahradíme náhodnú výzvu c výstupom hašovacej funkcie: $H(x, a)$
  - H má vhodný obor hodnôt
  - model s náhodným orákulom

Schnorrov protokol – neinteraktívna verzia

Protokol (výpočet P)

1. $a = g^r$, $r \in_R \mathbb{Z}_p$
2. $c = H(x, a)$
3. $z = r + cw$
4. dôkaz: (a, z)

V akceptuje práve vtedy, keď $g^z = ax^{H(x,a)}$

- alternatívny dôkaz (c, z) a overenie:

$$c \stackrel{?}{=} H(x, a), \text{ kde } a = g^z \cdot x^{-c}$$

Podpisová schéma zo Schnorrovho protokolu

- zakomponovaním správy m do predchádzajúceho protokolu získame podpisovú schému:
  - súkromný kľúč: w, verejný kľúč: $x = g^w$
  - Podpisovanie správy m:
    1. $a = g^r$, $r \in_R \mathbb{Z}_p$
    2. $c = H(m, a)$
    3. podpis $\sigma = (c, r + cw)$
  - Overenie podpisu $\sigma = (c, z)$ pre správu m:
    1. $a = g^z \cdot x^{-c}$
    2. podpis je korektný vtedy, keď $c = H(m, a)$
- porovnajte so Schnorrovou podpisovou schémou

Dôkaz/argument znalosti otvoreného textu v RSA schéme

- RSA:
  - $n = p \cdot q$, $e \cdot d \equiv 1 \pmod{\varphi(n)}$
  - $E(m) = m^e \bmod n$
  - $D(c) = c^d \bmod n$
  - dostatočne veľké prvočíselné e (podmienka navyše)
- Σ-protokol pre reláciu $R = \{(y, w) : w^e = y \bmod n\} \subseteq \mathbb{Z}_n^* \times \mathbb{Z}_n^*$
  - $L_R = \mathbb{Z}_n^*$ (triviálny jazyk)
  - spoločný vstup y
  - P pozná navyše w
  - P nemusí v protokole poznať d ani faktorizáciu n, stačí verejný kľúč

Protokol (Guillou, Quisquater)

1. $P \to V$: $a = r^e$, $r \in_R \mathbb{Z}_n^*$
2. $V \to P$: $c \in_R \mathbb{Z}_e$
3. $P \to V$: $z = rw^c$
4. V akceptuje práve vtedy, keď $z^e = a \cdot y^c$

Perfektná úplnosť

$z^e = (rw^c)^e = r^e \cdot (w^e)^c = a \cdot y^c$

Špeciálna korektnosť/zdravosť

- nech (a, c, z) a (a, c', z') pre $c \neq c'$ sú dve akceptujúce komunikácie
- teda $z^e = a \cdot y^c$, $(z')^e = a \cdot y^{c'}$, odkiaľ

$$\frac{z^e}{y^c} = \frac{(z')^e}{y^{c'}} \quad \Rightarrow \quad \left(\frac{z}{z'}\right)^e = y^{c-c'}$$

- $\mathrm{nsd}(e, c - c') = 1$, teda $\exists s, t : \; se + t(c - c') = 1$ (rozšírený Euklidov algoritmus)

$$\left(\frac{z}{z'}\right)^{te} = y^{t(c-c')} = y^{1-se} \quad \Rightarrow \quad (\underbrace{y^s \cdot (z/z')^t}_{w})^e = y \qquad \text{... získame } w$$

Vlastnosti GQ protokolu (2)

Špeciálna HVZK

- nech $y \in \mathbb{Z}_n^*$ a nech $c \in \mathbb{Z}_e$
- $S(y, c)$ vygeneruje akceptačnú komunikáciu (a, c, z) takto:
  1. $z \in_R \mathbb{Z}_n^*$
  2. $a = z^e / y^c$
- triviálne je trojica (a, c, z) akceptačná – overovacia rovnica sedí
- rovnaká distribúcia:
  - a je uniformne distribuované v $\mathbb{Z}_n^*$ (lebo z^e je takto distribuované)
  - c a y a teda aj y^c sú fixné ($y^c \in \mathbb{Z}_n^*$)
  - z je potom jednoznačne určené overovacou rovnicou

Neinteraktívna verzia GQ protokolu (FS heuristika)

– FS heuristika: výpočet výzvy $c = H(y, a)$
  ▫ H s oborom hodnôt $\mathbb{Z}_e$

Protokol (výpočet P)

1. $a = r^e$, $r \in_R \mathbb{Z}_n$
2. $c = H(y, a)$
3. $z = rw^c$
4. dôkaz: (a, z)

V akceptuje práve vtedy, keď $z^e = a \cdot y^{H(y,a)}$

– alternatívny dôkaz (c, z) a overenie:

$$c \stackrel{?}{=} H(y, a), \text{ kde } a = z^e \cdot y^{-c}$$

Neinteraktívna verzia GQ protokolu (FS heuristika)

- FS heuristika: výpočet výzvy $c = H(y, a)$
  - H s oborom hodnôt $\mathbb{Z}_e$

Protokol (výpočet P)

1. $a = r^e$, $r \in_R \mathbb{Z}_n$
2. $c = H(y, a)$
3. $z = rw^c$
4. dôkaz: (a, z)

V akceptuje práve vtedy, keď $z^e = a \cdot y^{H(y,a)}$

- alternatívny dôkaz (c, z) a overenie:

$$c \stackrel{?}{=} H(y, a), \text{ kde } a = z^e \cdot y^{-c}$$

Podpisová schéma

- súkromný kľúč: w, verejný kľúč y
- podpis správy m: $\sigma = (c, z)$
  - $r \in_R \mathbb{Z}_n$, $a = r^e$, $c = H(m, a)$, $z = rw^c$
- podpis $\sigma = (c, z)$ pre m je korektný, keď:
  - $c = H(m, a)$, kde $a = z^e \cdot y^{-c}$

- schémy založené na identite
- verejný kľúč ≈ identita (mailová adresa)
  - $y_A = H^*(\mathrm{id}_A)$
- nie sú potrebné certifikáty, PKI
- potrebná je však dôveryhodná tretia strana
  - výpočet súkromného kľúča, $w_A = y_A^d$

Úlohy

1. Ukážte, že Schnorrov protokol pre diskrétny logaritmus je Σ-protokol.
2. Ukážte, že nasledujúci variant Schnorrovho protokolu má vlastnosti úplnosti, špeciálnej korektnosti a HVZK, avšak je úplne neodolný voči nečestnému overovateľovi (vstupy ako v pôvodnom protokole, $P(x, w)$, $V(x)$):
    1. $P \to V$: $a = g^r$, $r \in_R \mathbb{Z}_p^*$
    2. $V \to P$: $c \in_R \mathbb{Z}_p$
    3. $P \to V$: $z = w + cr$
    4. V akceptuje práve vtedy, keď $g^z = xa^c$