

# Dôkazy znalosti a identifikačné protokoly

Martin Stanek

Department of Computer Science  
Comenius University  
`stanek@dcs.fmph.uniba.sk`

Cryptology 1 (2020/21)

# Obsah

Dôkaz znalosti diskrétného logaritmu

Schnorrov identifikačný protokol

Fiatova-Shamirova heuristika

Identifikačný protokol z RSA

# Úvod

- ▶ IPS (Interactive Proof System) predpokladá neobmedzene výpočtovo silného dokazovateľa  $P$
- ▶ praktické použitie: PPT dokazovateľ s pomocným vstupom (tajná/súkromná informácia)
- ▶ napr. ak  $P$  pozná izomorfizmus  $G_1 \simeq G_2$ , tak vie realizovať ZK IPS pre GI v polynomiálnom čase
- ▶ identifikačná schéma
  - ▶ dvaja účastníci  $P$  (dokazovateľ) a  $V$  (overovateľ)
  - ▶  $P$  vygeneruje svoj súkromný a verejný kľúč
  - ▶  $P$  dokáže svoju identitu účastníkovi  $V$  prostredníctvom znalosti súkromného kľúča
  - ▶ pritom  $V$  nevie o identite  $P$  presvedčiť niekoho ďalšieho (o súkr. kľúči sa nedozvie nič)
  - ▶ konštrukčný prvok pre podpisové schémy

# Dôkaz znalosti diskretného logaritmu

- ▶  $(G, \cdot)$  – grupa prvočíselného rádu  $q$ ; generátor  $g \in G$
- ▶ spoločný vstup  $P$  a  $V$  (verený kľúč):  $x \in G$
- ▶  $P$  pozná hodnotu  $w \in \mathbb{Z}_q$  (súkromný kľúč, svedok, witness):  $g^w = x$

Protokol:

1.  $P \rightarrow V: z = g^r$  pre  $r \xleftarrow{\$} \mathbb{Z}_q$
  2.  $V \rightarrow P: c \xleftarrow{\$} \{0, 1\}$
  3.  $P \rightarrow V: a = r + cw \bmod q$
  4.  $V$  overí, či platí  $g^a = z \cdot x^c$
- ▶ protokol viackrát opakujeme
  - ▶  $V$  akceptuje práve vtedy, keď  $P$  uspeje vo všetkých opakovaníach

# Vlastnosti protokolu

- ▶ úplnosť (*completeness*): triviálne, pri znalosti  $w$  vie  $P$  uspieť vždy,  
$$g^a = g^{r+cw} = g^r \cdot (g^w)^c = z \cdot x^c$$
- ▶ bezznalostnosť (*zero-knowledge*): pomocou black-box simulácie:
  - ▶ simulátor  $S$  má k dispozícii  $x$  a  $V^*$
  - ▶  $S$  zvolí  $c' \xleftarrow{\$} \{0, 1\}$
  - ▶  $S$  simuluje  $V^*$  na vstupe  $z = g^a \cdot x^{-c'}$ , pre  $a \xleftarrow{\$} \mathbb{Z}_q$
  - ▶ ak  $V^*$  vygeneruje výzvu  $c = c'$ , tak trojica  $\langle z, c, a \rangle$  je korektnou trojicou pre simulovanú komunikáciu; v opačnom prípade resetuje  $V^*$  do predchádzajúceho stavu
- ▶ korektnosť (*soundness*): keďže  $\forall x \exists w : g^w = x$ , tak pojem korektnosti ako pre IPS nemá veľký zmysel
  - ▶ pripomeňme, že pri IPS korektnosť bola o situácii, keď vstup nie je z jazyka
  - ▶ tu nás zaujíma situácia, keď  $P$  nepozná  $w$

## Úspešný beh $\Rightarrow$ znalosť $w$

- ▶ namiesto korektnosti požadujeme, aby z úspešného behu protokolu vyplývala znalosť  $w$  k danému  $x$
- ▶ neformálne:  $P$  vie správne odpovedať na každú výzvu
  - ▶  $c = 0$ :  $g^a = z$
  - ▶  $c = 1$ :  $g^{a'} = z \cdot x$
  - ▶ odtiaľ  $g^{a'-a} = x$  a teda pozná  $w = a' - a$
- ▶ samozrejme, uspieť by  $P$  mohol aj bez  $w$ , ak by vopred vedel hodnotu  $c$ 
  - ▶ vhodná príprava  $z$  podľa predpokladaného  $c$
  - ▶  $c = 0$ :  $z = g^a$  pre  $a \xleftarrow{\$} \mathbb{Z}_q$
  - ▶  $c = 1$ :  $z = g^a \cdot x^{-1}$  pre  $a \xleftarrow{\$} \mathbb{Z}_q$
  - ▶ problém nastane, ak výzva bude  $1 - c$
  - ▶ šanca uspieť pri  $k$  opakovaníach je  $2^{-k}$

# Formálnejší prístup

- ▶ NP relácia  $R \subseteq \{0, 1\}^* \times \{0, 1\}^*$  je určená DPT algoritmom  $W(\cdot, \cdot)$ 
  - ▶  $R = \{(x, w) : W(x, w) \text{ akceptuje}\}$
  - ▶  $W$  je polynomiálny vzhľadom na dĺžku prvého vstupu ( $|w| \leq p(|x|)$ )
- ▶ súvisiaci NP jazyk  $L_R = \{x : \exists w W(x, w) \text{ akceptuje}\}$ 
  - ▶ ľahko vidieť, že  $L_R \in \text{NP}$
- ▶ množina svedkov pre  $x$ :  $R(x) = \{w : W(x, w) \text{ akceptuje}\}$
- ▶ pre predchádzajúci dlog problém/protokol:
  - ▶  $R = \{(x \in G, w \in \mathbb{Z}_q) : g^w = x\}$
  - ▶  $L_R = G$

# Extraktor znalosti

- ▶ knowledge extractor  $\sim$  spôsob naplnenia korektnosti (soundness, special soundness)
- ▶ PPT algoritmus  $K$ , ktorý pre ľubovoľný  $P^*$  taký, že uspeje na vstupe  $x \in L_R$ , vypočíta svedka, teda  $K(P^*, x) \in R(x)$
- ▶ potrebné formalizovať “uspeje”, t.j. vzťah medzi pravdepodobnosťami
- ▶ týka sa len  $x \in L_R$ , lebo v inak je  $R(x) = \emptyset$  a  $K$  nemá čo vypočítať
- ▶ extraktor znalosti pre predchádzajúci (dlog) protokol:
  1.  $K$  simuluje  $P^*$  a získa  $z \in G$
  2.  $K$  si zapamätá stav  $P^*$
  3.  $K$  poskytne  $P^*$  výzvu  $c = 0$  a získa odpoveď  $a_0$
  4.  $K$  resetuje  $P^*$  do stavu v kroku 2
  5.  $K$  poskytne  $P^*$  výzvu  $c = 1$  a získa odpoveď  $a_1$
  6. následne  $a_1 - a_0 = \text{dlog}_g(zx) - \text{dlog}_g z = \text{dlog}_g x$
- ▶  $K$  vie overiť správnosť získaného  $w$  a vie skúšať postup extrakcie viackrát (redukcia pravdepodobnosti neúspechu), ak  $P^*$  neuspeje vždy

# Schnorrov identifikačný protokol

- ▶  $(G, \cdot)$ ,  $|G| = q$ ,  $g$  – ako predtým
- ▶ dokazujeme znalosť  $\text{dlog}_g x = w$ , pre nejaké  $x \in G$
- ▶ výzva nie je bit ale ľubovoľná hodnota zo  $\mathbb{Z}_q$

Protokol:

1.  $P \rightarrow V: z = g^r$ , pre  $r \xleftarrow{\$} \mathbb{Z}_q$
2.  $V \rightarrow P: c \xleftarrow{\$} \mathbb{Z}_q$
3.  $P \rightarrow V: a = r + cw$
4.  $V$  akceptuje práve vtedy, keď  $g^a = z \cdot x^c$

# Schnorrov identifikačný protokol – vlastnosti

- ▶ úplnosť:  $g^a = g^{r+cw} = g^r \cdot (g^w)^c = z \cdot x^c$
- ▶ extraktor znalosti:
  - ▶ postupujeme podobne ako pre bitovú výzvu
  - ▶ resetujeme  $P^*$  pre výzvy  $c \neq c'$
  - ▶ po získaní príslušných odpovedí  $a, a'$  spĺňajúcich  $g^a = zx^c$  a  $g^{a'} = zx^{c'}$ , dostaneme:  $g^{a-a'} = x^{c-c'}$
  - ▶ teda  $a - a' = w(c - c') \Rightarrow w = (a - a') / (c - c')$
- ▶ (perfektná) bezznalosť pre čestného overovateľa:
  - ▶ čestný  $\sim$  výzva  $c$  je volená uniformne náhodne zo  $\mathbb{Z}_q$
  - ▶ simulátor  $S$  zvolí  $c \xleftarrow{\$} \mathbb{Z}_q$
  - ▶  $S$  dopočíta  $z = g^a / x^c$ , pre  $a \xleftarrow{\$} \mathbb{Z}_q$
  - ▶ simulovaná komunikácia:  $\langle z, c, a \rangle$
  - ▶ pre nečestného overovateľa nevieme spraviť efektívnu black-box simuláciu

# Fiatova-Shamirova heuristika

- ▶ Schnorrov protokol je interaktívny
- ▶ neinteraktívna verzia:  $P$  pošle dáta a  $V$  overí
- ▶ Fiatova-Shamirova heuristika:
  - ▶ výzva konštruovaná z prvej správy pomocou h.f.  $c = H(z)$
  - ▶ predpokladáme vhodný obor hodnôt  $H$  (tu  $\mathbb{Z}_q$ )
  - ▶ idea:  $P$  nevie  $c$ , kým nezvolí  $z$ , ani k  $c$  nevie dopočítať vhodné  $z$
- ▶ FS heuristika – transformácia trojkolového HVZK dôkazu znalosti s verejnými hodmi mincou do schémy pre digitálne podpisy

# FS heuristika pre Schnorrov protokol

- ▶ predpoklad  $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q$  je náhodné orákulum
- ▶ podpisovanie správy  $m$ :
  1.  $z = g^r$ , pre  $r \xleftarrow{\$} \mathbb{Z}_q$
  2.  $c = H(m || z)$
  3. podpis  $\sigma = (c, \underbrace{r + wc}_s)$
- ▶ overenie podpisu:
  1.  $z = g^s \cdot x^{-c}$
  2. overenie  $c = H(m || z)$
- ▶ porovnajte so Schnorrovou podpisovou schémou

# Identifikačný protokol z RSA

- ▶ Guillou-Quisquater
- ▶ inštancia RSA:  $n = p \cdot q$ ,  $e$  nesúdeliteľné s  $\varphi(n)$ 
  - ▶ požadujeme dostatočne veľké prvočíselné  $e$
- ▶ pre  $y \in \mathbb{Z}_n$  dokazujeme znalosť  $x$ :  $x^e = y \bmod n$
- ▶ počítame mod  $n$

Protokol:

1.  $P \rightarrow V$ :  $z = r^e$ , pre  $r \xleftarrow{\$} \mathbb{Z}_n$
2.  $V \rightarrow P$ :  $c \xleftarrow{\$} \mathbb{Z}_e$
3.  $P \rightarrow V$ :  $a = rx^c$
4.  $V$  akceptuje práve vtedy, keď  $a^e = zy^c$

# Identifikačný protokol z RSA – vlastnosti (1)

- ▶ úplnosť:  $a^e = (rx^c)^e = r^e \cdot (x^e)^c = zy^c$
- ▶ (perfektná) bezznalosť pre čestného overovateľa:
  - ▶ čestný ~ výzva  $c$  je volená uniformne náhodne zo  $\mathbb{Z}_e$
  - ▶ simulátor  $S$  zvolí  $c \xleftarrow{\$} \mathbb{Z}_e$
  - ▶  $S$  dopočíta  $z = a^e / y^c$ , pre  $a \xleftarrow{\$} \mathbb{Z}_n$
  - ▶ simulovaná komunikácia:  $\langle z, c, a \rangle$
- ▶ simulácia nečestného overovateľa vs. efektívnosť
  - ▶ malé  $e$  – black-box simulácia, potreba iterovať protokol
  - ▶ veľké  $e$  – jeden beh stačí, nevieme spraviť efektívnu black-box simuláciu

# Identifikačný protokol z RSA – vlastnosti (2)

## ▶ extraktor znalosti:

- ▶ nech  $P$  uspeje v protokole pre dve výzvy  $c \neq c'$  s rovnakým  $z$
- ▶ teda máme  $a, a'$ :  $a^e = zy^c$  a  $a'^e = zy^{c'}$
- ▶ dostávame  $(a/a')^e = y^{c-c'}$  (★)
- ▶  $\text{nsd}(e, c - c') = 1$ , lebo  $c \neq c' \in \mathbb{Z}_e$  a  $e$  je prvočíslo
- ▶ (rozšírený Euklidov algoritmus) nájdeme  $u, v \in \mathbb{Z}$ :  $ue + v(c - c') = 1$
- ▶ umocnením (★) na  $v$  máme:

$$(a/a')^{ve} = y^{v(c-c')} = y^{1-ue} = y \cdot y^{-ue} \Rightarrow y = \underbrace{(y^u \cdot (a/a')^v)}_x^e$$

# Identifikačný protokol z RSA – poznámky

- ▶ FS heuristika – neinteraktívny protokol voľbou  $c = H(z)$
- ▶ konštrukcia podpisovej schémy analogicky ako pre Schnorrov protokol
- ▶  $P$  pri realizácii protokolu nepotrebuje poznať súkromný RSA exponent  $d$
- ▶ identity-based ~ schémy založené na identite, verejný kľúč je verejná informácia (napr. e-mailová adresa)
  - ▶  $y_A = H^*(\text{id}_A)$ ;  $x_A = y_A^d$
  - ▶ potrebná dôveryhodná tretia strana generujúca súkromné kľúče
  - ▶ nie je potrebné podpisovať certifikáty