Bezpečnosť podpisových schém

Martin Stanek

2025

KI FMFI UK Bratislava

Úvod

- podpisové schémy – často využívané v praxi
- formálny prístup k definícii bezpečnosti podpisových schém
- dôkazy redukciou na podkladový problém, „forking lemma“
- príklady:
  - RSA-FDH (Full Domain Hash)
  - Schnorrova podpisová schéma
- poddajnosť ECDSA schémy

Podpisová schéma

– podpisová schéma $\Pi = \langle \text{Gen}, \text{Sig}, \text{Vrf} \rangle$

Gen
– vstup: 1^k (k je bezpečnostný parameter)
– výstup: (pk, sk)
– pk je verejný (overovací) kľúč
– sk je súkromný (podpisový) kľúč

Sig
– vstup: sk, m (správa)
– výstup: podpis $\sigma \leftarrow \text{Sig}_{\text{sk}}(m)$

Vrf
– vstup: pk, σ, m
– výstup: 1 (korektný podpis), resp. 0 (nekorektný podpis m)

– všetky algoritmy sú polynomiálne vzhľadom na k
– Gen musí byť a Sig môže byť znáhodnený (pravdepodobnostný)
– Vrf je obvykle deterministický

Podpisová schéma $\Pi = \langle \mathrm{Gen}, \mathrm{Sig}, \mathrm{Vrf} \rangle$

- požadujeme korektnosť schémy:

$$\forall k \in \mathbb{N}\ \forall (\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}\left(1^k\right)\ \forall m : \mathrm{Vrf}_{\mathrm{pk}}(m, \mathrm{Sig}_{\mathrm{sk}}(m)) = 1$$

- praktické použitie – efektívnosť algoritmov (polynomiálne vzhľadom na k)
- priestor správ $\mathcal{M}$, obvykle $\mathcal{M} \subseteq \{0,1\}^+$
  - zrejmý z kontextu konkrétnej schémy
  - môže závisieť na verejnom kľúči pk, príp. použitej hašovacej funkcii
  - predpokladáme, že dĺžka správ je polynomiálna vzhľadom na k

Definícia bezpečnosti – čo nestačí

Nutné ale obvykle nepostačujúce prístupy:

- je ťažké vypočítať sk z verejného kľúča pk
  - nič to nehovorí o samotných podpisoch
- je ťažké pre dané m vypočítať σ: $\mathrm{Vrf}_{\mathrm{pk}}(m, \sigma) = 1$
  - útočník môže vypočítať m spolu so σ (napr. falšovanie náhodnej správy)
- je ťažké vypočítať dvojicu (m, σ): $\mathrm{Vrf}_{\mathrm{pk}}(m, \sigma) = 1$
  - útočník môže poznať nejaké korektne podpísané správy
- pre podpísané správy $\{(m_i, \sigma_i)\}_{i=1}^{n}$ je ťažké vypočítať dvojicu (m, σ): $m \notin \{m_1, \ldots, m_n\}$ a $\mathrm{Vrf}_{\mathrm{pk}}(m, \sigma) = 1$
  - útočník môže podpisujúceho presvedčiť o podpísaní inej vhodnej (pomocnej) správy

Ciele a schopnosti útočníka

- definície bezpečnosti kombinujú ciele a schopnosti útočníka
- ciele:
  - získať súkromný kľúč (úplné rozbitie schémy)
  - falšovať podpis ľubovoľnej správy (univerzálne falšovanie)
  - falšovať podpis nejakej vopred zvolenej správy (selektívne falšovanie)
  - falšovať podpis nejakej jednej správy (existenciálne falšovanie)
- schopnosti:
  - znalosť verejného kľúča
  - znalosť niekoľkých správ a ich podpisov
  - získavať podpisy k zvoleným správam (adaptívna voľba správ)
- najsilnejšia definícia = najslabší cieľ + najsilnejšie schopnosti

Definícia bezpečnosti

- výpočtovo obmedzený PPT útočník A s prístupom k podpisovému orákulu
- cieľ: sfalšovať podpis k správe, na ktorú sa útočník orákula nepýtal
- hra (Q je množina správ, ktoré sa útočník pýtal orákula):

$\textbf{Sig-forge}_{A,\Pi}(\boldsymbol{k})$:

$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}\left(1^k\right)$

$(m, \sigma) \leftarrow A^{\mathrm{Sig}_{\mathrm{sk}}(\cdot)}(\mathrm{pk})$

if $\mathrm{Vrf}_{\mathrm{pk}}(m, \sigma) = 1 \ \wedge \ m \notin Q$: return 1 (A vyhral)

else: return 0 (A prehral)

Definícia bezpečnosti – EUF-CMA

Definicia. Podpisová schéma $\Pi = \langle \text{Gen}, \text{Sig}, \text{Vrf} \rangle$ je existenciálne nefalšovateľná pri útoku s možnosťou adaptívnej voľby správy (EUF-CMA), ak pre ľubovoľného PPT útočníka A existuje zanedbateľná funkcia $\text{negl}(\cdot)$ taká, že platí:

$$\Pr\left[\text{Sig-forge}_{A,\Pi}(k) = 1\right] \leq \text{negl}(k).$$

– $f : \mathbb{N} \to \mathbb{R}_0^+$ je (asymptoticky) zanedbateľná, ak pre ľubovoľný kladný polynóm p:

$$\exists n_0 \in \mathbb{N} : \forall n > n_0 : f(n) < \frac{1}{p(n)}$$

– *nejakú* zanedbateľnú funkciu označíme $\text{negl}(\cdot)$

Poznámky k definícii

- asymptotická definícia
  - často sa čas výpočtu útočníka (označme $t(k)$) a pravdepodobnosť úspechu (označme $\varepsilon(k)$) konkretizuje
  - $(t(k), \varepsilon(k))$-bezpečná schéma, ak pre ľubovoľného útočníka A pracujúceho v čase $t(k)$ platí, že $\Pr\left[\text{Sig-forge}_{A,\Pi}(k) = 1\right] \leq \varepsilon(k)$
  - ešte konkrétnejší prístup: $(t(k), \varepsilon(k), q_S)$-bezpečná schéma, kde q_S je počet otázok na podpisové orákulum
- RSA bez hašovacej funkcie nie je EUF-CMA
  - falšovanie náhodnej správy: $m = \sigma^e \bmod n$, pre ľub. $\sigma \in \mathbb{Z}_n$
  - pripomeňme RSA: $n = p \cdot q$, $ed \equiv 1 \bmod \varphi(n)$, $\text{pk} = (e, n)$, $\text{sk} = (d)$
  - verejná a súkromná transformácia ($\mathbb{Z}_n \to \mathbb{Z}_n$): $x \mapsto x^e \bmod n$, $x \mapsto x^d \bmod n$

RSA-FDH (Full Domain Hash)

- FDH: $H : \{0,1\}^* \to \mathbb{Z}_n$
- RSA-FDA: RSA podpisová schéma s FDH
  - $\mathrm{Sig}_{\mathrm{sk}}(m) = H(m)^d \bmod n$
  - $\mathrm{Vrf}_{\mathrm{pk}}(m, \sigma) = \left[\sigma^e \bmod n \stackrel{?}{=} H(m)\right]$
- pre bezpečnosť RSA-FDA je nutné (inak vieme úspešne útočiť):
  - RSA ťažko invertovateľné (RSA problém je ťažký)
  - H ťažko invertovateľná
  - H odolná vočí kolíziám
  - ťažké nájsť m_1, m_2, m_3: $H(m_1) \cdot H(m_2) \equiv H(m_3) \pmod n$
- Sú tieto požiadavky postačujúce? nemusia byť (!)
- H ako náhodné orákulum
- útočník s prístupom k orákulám $\mathrm{Sig}_{\mathrm{sk}}$ a H

RSA predpoklad

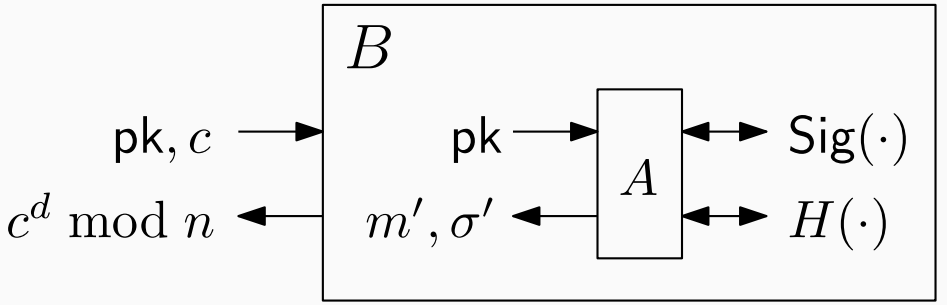
- RSA problém (problém invertovania RSA): pre $\text{pk} = (n, e)$ a náhodne zvolené $c \in \mathbb{Z}_n$ vypočítať $x \in \mathbb{Z}_n$: $x^e \equiv c \pmod{n}$ (alebo inak: $x = c^d \bmod n$).
- RSA predpoklad: pre ľubovoľný PPT algoritmus A je $\Pr\left[A(\text{pk}, c) = \left(c^d \bmod n\right)\right]$ zanedbateľná

Bezpečnosť RSA-FDH

Veta. Nech Π je RSA-FDH podpisová schéma, H je náhodné orákulum a nech platí RSA predpoklad. Potom Π je existenciálne nefalšovateľná pri útoku s možnosťou adaptívnej voľby správy.

Bezpečnosť RSA-FDH – dôkaz (hlavná myšlienka)

- A uspeje v Sig-forge s nezanedbateľnou pravdepodobnosťou ε_A
  - označme (m', σ') výstup úspešného A
- skonštruujeme B invertujúci RSA s nezanedbateľnou pr. ε_B
  - vstup: $\mathsf{pk} = (n, e)$, $c \in_R \mathbb{Z}_n$
  - výstup: $m \in \mathbb{Z}_n$: $m^e \equiv c \pmod{n}$
- B simuluje A s verejným pk
- B musí korektne simulovať obe orákulá



Redukcia Sig-forge na invertovanie RSA

Pozorovania

- ak sa A nespýta orákula na hodnotu $H(m')$, tak σ' bude korektné len so zanedbateľnou pravdepodobnosťou
- q_H počet otázok A na orákulum H
  - počítajú sa aj nepriame otázky cez simuláciu Sig_{sk} orákula
- B tipne, ktorou otázkou (označme r) sa bude A pýtať na hodnotu $H(m')$
  - pravdepodobnosť, že uhádne je $1/q_H$

Simulácie orákul – H

- B si pamätá všetky otázky aj odpovede
- otázka $H(m_i)$, pre $i \neq r$:
  1. $\sigma_i \in_R \mathbb{Z}_n$
  2. definujeme $H(m_i) \leftarrow \sigma_i^e \bmod n$
  3. zapamätáme si trojicu $(m_i, H(m_i), \sigma_i)$
- otázka $H(m_i)$, pre $i = r$:
  1. definujeme $H(m_i) \leftarrow c$
  2. zapamätáme si trojicu $(m_i, H(m_i), \_)$
- v oboch prípadoch je výstup, hodnota $H(m_i)$, uniformne distribuovaná v $\mathbb{Z}_n$
  - presne ako pre náhodné orákulum
- drobnosti:
  - konzistentné odpovede (ak sme už takú otázku simulovali)
  - viacnásobné otázky na m_r
    - položené neskôr
    - ak sa m_r už vyskytlo predtým
  - ak existuje úspešný A, tak existuje rovnako úspešný A^*, ktorý sa nepýta opakovane

Simulácie orákul – Sig

- $\mathrm{Sig}_{\mathrm{sk}}(m)$:
  1. ak sa A ešte nepýtal na $H(m)$, simulujeme: získame $(m_i, H(m_i), \sigma_i)$, kde $m_i = m$
  2. ak $m = m_r$, tak B skončí neúspechom
  3. výstup simulácie: σ_i
- podpisy sú konzistentné s odpoveďami v simulácii H
- ak zároveň
  - A uspeje: (m', σ'), kde $(\sigma')^e \bmod n = H(m')$ a
  - B uhádol r: teda $m' = m_r$,

  tak $(\sigma')^e \bmod n = c$ a B úspešne invertoval c v RSA

RSA-FDH – záver a poznámky

- ak A je PPT, tak aj B je PPT
- pravdepodobnosť úspechu B je $\varepsilon_B \approx \varepsilon_A / q_H$ (inak: $\varepsilon_A \approx \varepsilon_B \cdot q_H$)
  - ε_B je nezanedbateľné, ak ε_A je nezanedbateľné
- konkrétnejšie:
  - nech $q_H = 2^{50}$ a chceme 128-bitovú bezpečnosť, teda $\varepsilon_A \approx 2^{-128}$
  - odtiaľ $\varepsilon_B \approx 2^{-178}$
  - potom podľa RFC 3766 by sme mali použiť n dĺžky 6722 bitov
- **tesná redukcia**: ak $\varepsilon_B \approx \varepsilon_A$ (aj čas)
  - napr. RSA-PSS (Probabilistic Signature Scheme)
  - rovnako ako RSA-FDH model s náhodným orákulom
  - nevýhoda: potreba náhodného generátora

Schnorrova podpisová schéma

- $\mathrm{Gen}(1^k)$
  - vygenerujeme grupu G prvočíselného rádu q (kde $|q| = k$) a jej generátor g
  - $\mathrm{sk} = x \in_R \mathbb{Z}_q$
  - $\mathrm{pk} = (g, y)$, kde $y = g^x$
- hašovacia funkcia $H : \{0,1\}^* \to \mathbb{Z}_q$

- $\mathrm{Sig}_{\mathrm{sk}}(m) = \sigma = (c, s)$, kde
  1. $R = g^r$, pre $r \in_R \mathbb{Z}_q$
  2. $c = H(R, m)$
  3. $s = xc + r \pmod q$
- $\mathrm{Vrf}_{\mathrm{pk}}(m, (c, s)) = \left[c \stackrel{?}{=} H(R, m)\right]$, kde
  - $R = g^s \cdot y^{-c}$
- korektnosť schémy:
  $R = g^s \cdot y^{-c} = g^{xc+r} \cdot g^{-xc} = g^r$

DL predpoklad

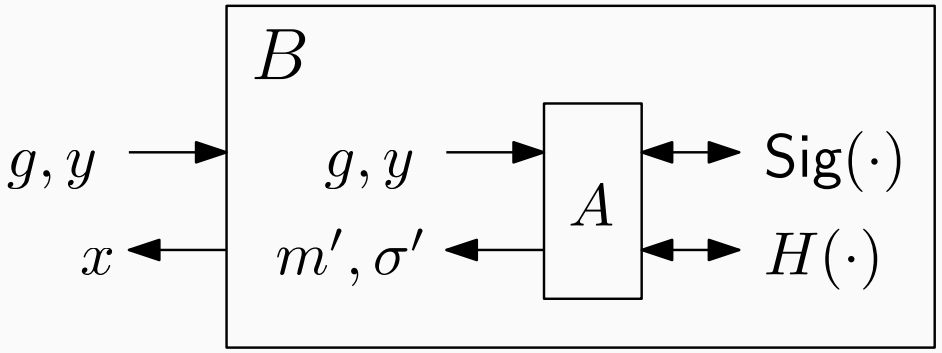
- problém diskrétneho logaritmu (problém výpočtu DL):
  pre dané g a $y \in_R G$ vypočítať $x \in \mathbb{Z}_q$: $g^x = y$
- DL predpoklad:
  pre ľubovoľný PPT algoritmus A je $\Pr[A(g, y) = x : g^x = y]$ zanedbateľná

Bezpečnosť Schnorrovej schémy

Veta. Nech Π je Schnorrova podpisová schéma, H je náhodné orákulum a nech platí DL predpoklad. Potom Π je EUF-CMA.

Bezpečnosť Schnorovej schémy – dôkaz (hlavná myšlienka)

- A uspeje v Sig-forge s nezanedbateľnou pravdepodobnosťou ε_A
- skonštruujeme B počítajúci DL s nezanedbateľnou pravd. ε_B
  - vstup: g a $y \in_R G$
  - výstup: $x \in \mathbb{Z}_q$: $g^x = y$
- B simuluje A s pk $= (y, g)$
- B musí korektne simulovať obe orákulá



Redukcia Sig-forge na počítanie DL

Simulácia H

- simulácia $H(R, m)$:
  - odpoveď h volíme náhodne uniformne zo $\mathbb{Z}_q$
  - páry $((R, m), h)$ si pamätáme v zozname Q
  - konzistencia – na rovnaké otázky sú rovnaké odpovede

Simulácia Sig

- B simuluje orákulum $\mathrm{Sig}_{\mathrm{pk}}(m)$ takto:
  1. $c \in_R \mathbb{Z}_q$ a $s \in_R \mathbb{Z}_q$, podpis je (c, s)
  2. vypočíta $R = g^s \cdot y^{-c}$
  3. zapamätá si $Q \leftarrow Q \cup \{((R, m), c)\}$, aby hodnota $H(R, m)$ bola korektná k vygenerovanému podpisu
     - ak sa už A na $H(R, m)$ predtým pýtal (zanedbateľná pravdepodobnosť), môže B voliť nové s
- podpis je korektný (verifikácia uspeje)
- hodnoty c, s sú uniforme distribuované v $\mathbb{Z}_q$
  - pre A neodlíšiteľné od skutočných podpisov

Výpočet DL pomocou A

- nech $R = g^s \cdot y^{-c}$ pre dvojicu hodnôt (c, s)
- ak sa A nespýta orákula na hodnotu $H(R, m)$, tak sfalšuje podpis pre m a R len so zanedbateľnou pravdepodobnosťou
- q_H počet rôznych otázok A na orákulum H
  - aj nepriame otázky na cez simuláciu Sig orákula
- ak A uspeje (pravd. ε_A)
  - nech t. otázka na H obsahuje správnu dvojicu (R_t, m_t)
  - potom B získa korektný podpis (c_t, s_t) pre m_t, kde $R_t = g^{s_t} \cdot y^{-c_t}$
  - navyše sa A nikdy nepýtal $\mathrm{Sig}_{\mathrm{sk}}(m_t)$

Výpočet DL pomocou A (2)

- B resetuje A a opäť ho simuluje od začiatku
  - rovnaká náhodná páska a
  - rovnaké odpovede z H a $\mathrm{Sig}_{\mathrm{sk}}$ orákul ako predtým
- až po otázku $H(R_t, m_t)$
  - tentoraz zvolí B ako odpoveď náhodné $c'_t \neq c_t$
  - z pohľadu A stále korektné
  - B pokračuje v simulácii A
- pravd., že A uspeje a navyše sfalšuje znova podpis pre m_t a $R_t \approx \varepsilon_A / q_H$
- *forking lemma*: presná analýza pravd., že A uspeje v oboch behoch

$$\text{forking} \geq \varepsilon_A \cdot \left(\frac{\varepsilon_A}{q_H} - \frac{1}{|H|} \right)$$

Výpočet DL pomocou A (3)

- potom B má dva falšované podpisy pre správu m_t a vie vypočítať súkromný kľúč x:

$$\begin{aligned} R_t &= g^{s_t} \cdot y^{-c_t} \\ R_t &= g^{s'_t} \cdot y^{-c'_t} \end{aligned} \qquad \Longrightarrow \qquad g^{s_t - s'_t} = y^{c_t - c'_t}$$

- následne $x = (s_t - s'_t)(c_t - c'_t)^{-1} \bmod q$
- B vypočíta DL y s nezanedbateľnou pravd. $\varepsilon_B \approx \varepsilon_A^2 / q_H$
- redukcia opäť nie je tesná

ECDSA

- $\mathrm{Gen}(1^k)$
  - $(E, +)$ grupa bodov eliptickej krivky
  - krivka nad $\mathrm{GF}(p)$ (prvočíslo p)
  - $G \in E$, kde n – rád G – je dostatočne veľké, obvykle prvočíslo
  - $\mathrm{sk} = d \in_R \{1, \ldots, n-1\}$
  - $\mathrm{pk} = Q$, kde $Q = dG$
- $\mathrm{Sig}_{\mathrm{sk}}(m) = \sigma = (r, s)$, kde
  1. $(x_1, y_1) = kG$, pre $k \in_R \{1, \ldots, n-1\}$
  2. $r = x_1 \bmod n$ (ak $r = 0$, opakuj znova)
  3. $s = k^{-1}(H(m) + dr) \bmod n$ (ak $s = 0$ opakuj znova)
- $\mathrm{Vrf}_{\mathrm{pk}}(m, (r, s))$:
  1. over $r, s \in \{1, \ldots, n-1\}$
  2. $w = s^{-1} \bmod n$
  3. $u_1 = H(m)w \bmod n$, $u_2 = rw \bmod n$
  4. $(x_1, y_1) = u_1 G + u_2 Q$
  5. akceptuj $\Leftrightarrow x_1 \bmod n = r$

korektnosť schémy:

$k \equiv s^{-1}(H(m) + dr) \equiv u_1 + u_2 d \pmod n$

$\Rightarrow u_1 G + u_2 Q = (u_1 + u_2 d)G = kG$ ■

EUF-CMA s DL predpokladom a v modeli s náhodným orákulom

Podpisy v ECDSA sú „poddajné“ (malleable)

- nahraďme podpis (r, s) dvojicou $(r, -s \bmod n)$
- overenie:
  - $w^* = (-s)^{-1} = -s^{-1} = -w$
  - $u_1^* = H(m)w^* = -H(m)w = -u_1$
  - $u_2^* = rw^* = -rw = -u_2$
  - $u_1^* G + u_2^* Q = -(u_1 G + u_2 Q) = -kG = (x_1, -y_1)$
  - teda $x_1 \bmod n = r$ a podpis je korektný

prečo to môže byť problém:

- Bitcoin „transaction malleability“
- TXID (ID transakcie) závislé na podpise
- iné TXID, platná transakcia
- Mt. Gox (najväčšia Bitcoinová burza, 2014) duplicitné výbery

Silná existenciálna nefalšovateľnosť

- SUF-CMA (sEUF-CMA), silnejšia definícia ako EUF-CMA
- hra (Q je množina dvojíc: správy, ktoré sa útočník pýtal orákula, *a príslušné odpovede*):

$$\textbf{Sig-forge}^{\textbf{suf}}_{A,\Pi}(\boldsymbol{k}):$$

$$(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Gen}\left(1^k\right)$$

$$(m, \sigma) \leftarrow A^{\mathrm{Sig}_{\mathrm{sk}}(\cdot)}(\mathrm{pk})$$

$$\text{if } \mathrm{Vrf}_{\mathrm{pk}}(m, \sigma) = 1 \ \wedge \ (m, \sigma) \notin Q : \text{return } 1 \quad (A \text{ vyhral})$$

$$\text{else: return } 0 \quad (A \text{ prehral})$$