

Skupinsko generirani podpisi

Tim Kalan

Mentor: doc. dr. Tilen Marc

27. maj 2024

Kaj je podpis?

Ročni podpis

- ▶ Vsakič (približno) enak
- ▶ Enostavno ponarediti
- ▶ Težko (zares) preveriti

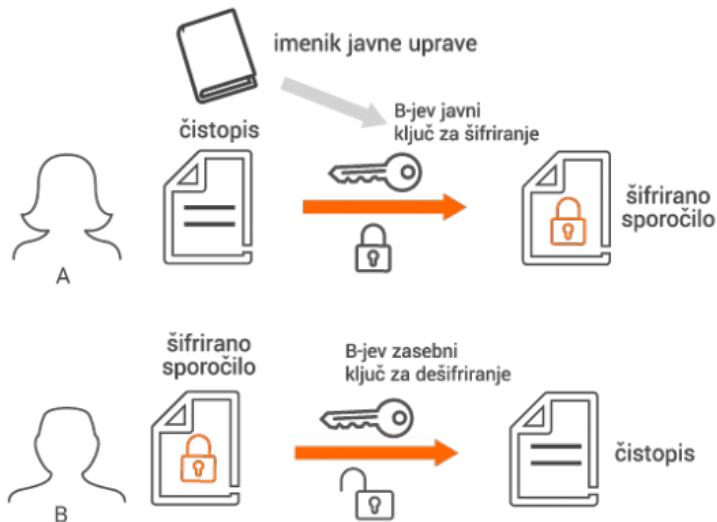
Digitalni podpis

- ▶ Vsakič unikaten
- ▶ Težko ponarediti
- ▶ Enostavno preveriti

Zakaj potrebujemo podpise?

- ▶ Mislim, da si lahko predstavljate ...
- ▶ Avtentikacija, integriteta
- ▶ Bančništvo, e-pošta, ssh, ...

Kriptografija javnega ključa 1



Kriptografija javnega ključa 2



Zgostitvene funkcije

- ▶ Psevdonaključne funkcije
- ▶ Enosmerne
- ▶ »Enostavno« izračunljive

```
SHA-256(Ljubljana) =  
b7f147d8b4a6703a951336654355071f  
9752385f85d0860379e99b484aee7a82  
SHA-256(Ljubljena) =  
995d2d8ffb40e1838219e65dd2c66570  
1ba34a90e11f7195a4b791838b6787fe
```

- ▶ Slučajni oraklji

Modularna aritmetika

- ▶ Kongruenca: $a \equiv b \pmod{m} \iff m \mid a - b$
- ▶ Grupa \mathbb{Z}_p^*
- ▶ Red elementa: $\text{ord}(g) = \min\{n \in \mathbb{N} \mid g^n \equiv 1 \pmod{p}\}$
- ▶ Diskretni logaritem: $g^x \equiv h \pmod{p}, x = ?$

$$2^1 \equiv 2 \pmod{11}$$

$$2^2 \equiv 4 \pmod{11}$$

$$2^3 \equiv 8 \pmod{11}$$

$$2^4 \equiv 5 \pmod{11}$$

$$2^5 \equiv 10 \pmod{11}$$

$$2^6 \equiv 9 \pmod{11}$$

$$2^7 \equiv 7 \pmod{11}$$

$$2^8 \equiv 3 \pmod{11}$$

$$2^9 \equiv 6 \pmod{11}$$

$$2^{10} \equiv 1 \pmod{11}$$

Primer digitalnega podpisa: Schnorrov podpis

Odličen primer za spoznavanje osnovnih konceptov:

- ▶ Generiranje ključev
- ▶ Podpisovanje
- ▶ Preverjanje

Schnorrov podpis

Generiranje ključev

- ▶ p, q **veliki** praštevili, $q \mid p - 1$
- ▶ $g \in \mathbb{Z}_p^*$, $\text{ord}(g) = q$, torej $g^q \equiv 1 \pmod{p}$
- ▶ $s \in [0, q - 1]$
- ▶ $I = g^s \pmod{p}$

Javni ključ: (p, q, g, I)

Zasebni ključ: s

Schnorrov podpis

Podpisovanje in preverjanje

- ▶ Podpis sporočila M je par (X, y)
 - ▶ $r \in [0, q - 1]$
 - ▶ $X = g^r \bmod p$
 - ▶ $e = H(X, M)$
 - ▶ $y = es + r \bmod q$
-
- ▶ Preverimo, če je (X', y') veljaven podpis za M
 - ▶ $e' = H(X', M)$
 - ▶ $g^{y'} \stackrel{?}{\equiv} X' \cdot I^{e'} \pmod{p}$
 - ▶ $g^{y'} \equiv g^{es+r} \pmod{p}$
 - ▶ $X' \cdot I^{e'} \equiv g^r \cdot (g^s)^e \pmod{p}$

Kako se skupina podpiše?

Skupina:

$$G = P_1, P_2, \dots, P_L$$

$$S \subseteq G$$

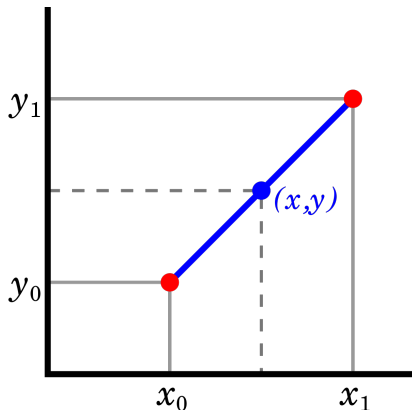
- ▶ **Prilagodljivost** (angl. *flexibility*)
- ▶ **Odgovornost** (angl. *accountability*)

Skupinski podpisi (angl. *group signatures*)

- ▶ Anonimen podpis v imenu skupine
- ▶ Ni prilagodljivosti
- ▶ Delna odgovornost (vodja skupine)
- ▶ Primer: Upravni odbor, kjer je generalni direktor vodja

Pragovni podpisi (angl. *threshold signatures*)

- ▶ t -od- L shema
- ▶ Zmerna prilagodljivost
- ▶ Ni odgovornosti
- ▶ Primer: Sef, ki ga lahko odklene nekaj lastnikov



Naivni pristop

- ▶ Želimo si prilagodljivost in odgovornost
- ▶ Vsak član S podpiše $(M, S) \rightarrow \sigma_i$
- ▶ Kot na papirju
- ▶ Primer: Ponudniki cen na omrežju Flare

Težava?

$\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \dots$

Večstranski podpisi (angl. *multisignatures*)

- ▶ Skupina vrne samo en podpis
- ▶ Prilagodljivost in odgovornost
- ▶ Naivna ideja + učinkovitost
- ▶ Primer: Podpisovanje peticij

Začetna ideja

Osnovni pojmi

- ▶ Skupina $G = P_1, P_2, \dots, P_L$
- ▶ Podmnožica podpisnikov S je znana vnaprej, poljubna
- ▶ Vsi v skupini imajo dostop do slučajnega oraklja H
- ▶ Napadalec:
 - ▶ Ima dostop do H
 - ▶ Kontrolira vse komunikacijske kanale
 - ▶ Cilj: ponarediti podpis

Začetna ideja

Generiranje ključev

- ▶ Vsi v skupini poznajo p, q in g
- ▶ Vsak podpisnik P_i :

$$s_i \in [0, q - 1]$$

$$I_i = g^{s_i} \bmod p$$

Javni ključi: (p, q, g, I_i)

Zasebni ključi: s_i

Začetna ideja

Podpisovanje

$$r_i \in [0, q - 1]$$

$$X_i = g^{r_i} \bmod p$$

↓

$$\tilde{X} = \prod_{P_i \in S} X_i \bmod p$$

↓

$$e = H(\tilde{X}, M, S)$$

$$y_i = es_i + r_i \bmod q$$

↓

$$\tilde{y} = \sum_{P_i \in S} y_i \bmod q$$

Začetna ideja

Preverjanje

- ▶ Preverimo, če je (\tilde{X}', \tilde{y}') veljaven podpis za M
- ▶ $e' = H(\tilde{X}', M, S)$
- ▶ $g^{\tilde{y}'} \stackrel{?}{\equiv} \tilde{X}' \cdot (\prod_{P_i \in S} I_i)^{e'} \pmod{p}$

Problem 1

Skupni parametri

- ▶ Kako generiramo p, q, g ?
- ▶ Če si pomagamo z orakljem, to pozna tudi napadalec
- ▶ **Rešitev:** Del DLP, varna praštevila

Generiranje skupnih parametrov p, q, g

- ▶ Vsem je dostopen orakelj H in varnostni parameter k
- ▶ Za naključno generiranje $H^*(2^k), H^*(2^k + 1), H^*(2^k + 2), \dots$

while True do

$q \leftarrow$ random k -bit string

$p \leftarrow 2q + 1$

if p is prime and q is prime **then return** p, q

- ▶ Preverjanje praštevil?

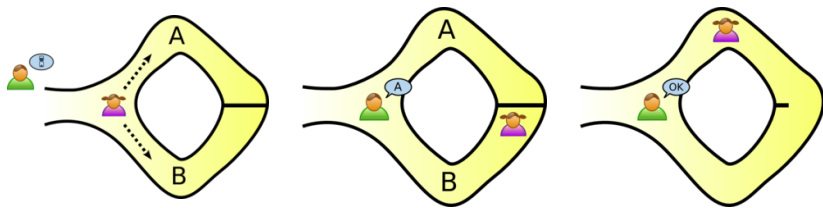
Problem 2

$$I_A = g^{s_A} \bmod p$$

- ▶ Napadalec goljufa pri izračunu javnega ključa I_A
- ▶ Lahko podpisuje v imenu skupine
- ▶ **Rešitev:** Dokaz brez razkritja znanja, potrebno preverjanje vsakega javnega ključa

Dokazi brez razkritja znanja

- ▶ Dokaz, da nekaj vemo, ne da bi razkrili kaj vemo
- ▶ Interaktivni protokol



Fiat-Shamirjeva hevrastika

- ▶ Pretvorba interaktivnega dokaza v neinteraktivnega
- ▶ Interaktivnost zamenja slučajni orakelj
- ▶ Če oraklji ne obstajajo, hevrastika ni varna

(Ne)interaktivni dokaz

- ▶ A: Pozna x , da $y \equiv g^x \pmod{q}$
- ▶ A: Naključni v , da $t \equiv g^v \pmod{q}$
- ▶ A: Pošlje t

- ▶ B: Naključni c , pošlje A
- ▶ A: Izračuna $c = H(g, y, t)$

- ▶ A: Pošlje $r = v - cx \pmod{\varphi(q)}$ B
- ▶ B: Preveri $t \stackrel{?}{\equiv} g^r y^c \pmod{q}$

Problem 3

Preverjanje dokazov

- ▶ Kdo preverja dokaze brez razkritja znanja?
- ▶ Kje so sploh dostopni?

- ▶ **Rešitev:** Dokaz brez razkritja znanja del javnega ključa (daljši ključi, dražje preverjanje podpisov)

Problem 4

Velikost S

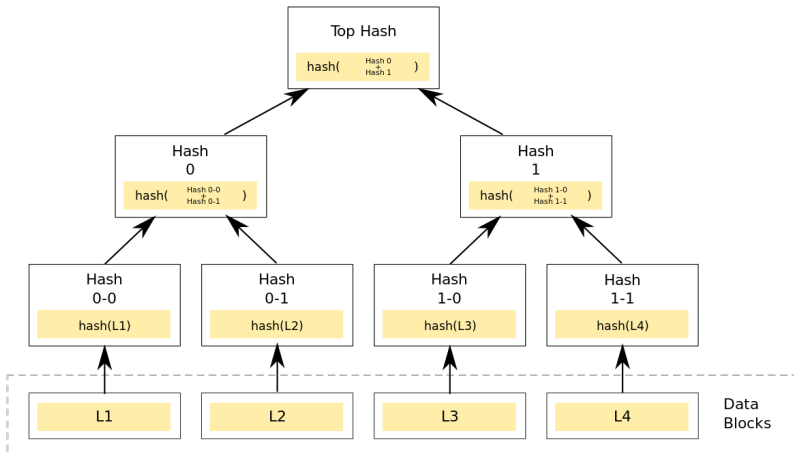
- ▶ Število podpisnikov omejeno
- ▶ Tehnikalije v dokazu varnosti
- ▶ **Rešitev:** Podpis σ_i sporočila $H(X_1, I_1, X_2, I_2, \dots, X_L, I_L)$

Problem 5

Velikost ključa

- ▶ V ključ moramo torej dati σ_i in $X_1, I_1, X_2, I_2, \dots, X_L, I_L$
- ▶ Predolg ključ, proporcionalen velikosti G
- ▶ **Rešitev:** Merklovo drevo z listi I_1, I_2, \dots, I_L , v ključu samo I_i in avtentikacijska pot

Merklova drevesa



Problem 6

Sočasno podpisovanje

- ▶ Dokaz varnosti uporablja previjanje (angl. *rewinding*)
- ▶ Previjanje je potovanje nazaj v času

- ▶ **Rešitev:** Ne dovolimo sočasnega podpisovanja

