

# Kako se skupina podpiše?

Tim Kalan

Mentor: doc. dr. Tilen Marc

27. maj 2024

# Zakaj potrebujemo podpise?

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

# Kaj je podpis?

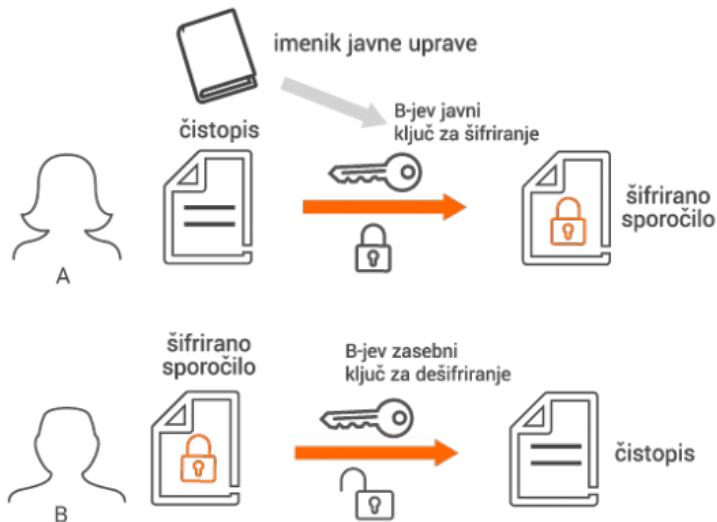
## **Ročni podpis**

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

## **Digitalni podpis**

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

# 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
```

- ▶ Naključni orakliji

# Primer digitalnega podpisa: RSA

Odličen primer za spoznavanje osnovnih konceptov:

- ▶ Generiranje ključev
- ▶ Podpisovanje
- ▶ Preverjanje

# RSA

## Generiranje ključev

- ▶ Izberemo dve **veliki** praštevili  $p$  in  $q$  (kako?)
- ▶ Izračunamo  $n = pq$  in  $\phi(n) = (p - 1)(q - 1)$
- ▶ Izberemo  $e$  tako, da je  $1 < e < \phi(n)$  in  $\gcd(e, \phi(n)) = 1$
- ▶ Izračunamo  $d$  tako, da je  $ed \equiv 1 \pmod{\phi(n)}$

**Javni ključ:**  $(n, e)$

**Zasebni ključ:**  $d$



# RSA

## Podpisovanje in preverjanje

- ▶ Sporočilo  $m$  podpišemo tako, da izračunamo  $s = m^d \bmod n$
- ▶ Podpis je par  $(m, s)$
  
- ▶ Preverimo tako, da izračunamo  $m' = s^e \bmod n$
- ▶ Podpis je pravilen, če je  $m' = m$

# RSA

## Primer

# Kako se skupina podpiše?

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

**Skupina:**

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

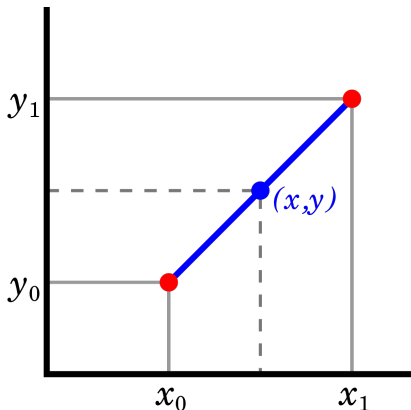
$$S \subseteq G$$

## 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- $n$  shema
- ▶ Zmerna prilagodljivost
- ▶ Ni odgovornosti
- ▶ Primer: Sef, ki ga lahko odklene nekaj lastnikov



# Naivna ideja

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

# Naivna ideja

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

Težava?

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

# Skupni podpisi (angl. *multisignatures*)

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



# Schnorrov podpis

## Generiranje ključev

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

**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  $M$
  - ▶  $e' = H(X', M)$
  - ▶  $g^{y'} \stackrel{?}{\equiv} X' \cdot I^{e'} \pmod{p}$

# 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 naključnega 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

## Problem 2

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

- ▶ Napadalec goljufa pri izračunu  $I_A$
- ▶ 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

# Problem 3

## Preverjanje dokazov

- ▶ Kdo preverja dokaze brez razkritja znanja?
- ▶ **Rešitev:** Dokaz brez razkritja znanja del javnega ključa

# Problem 4

Velikost  $S$

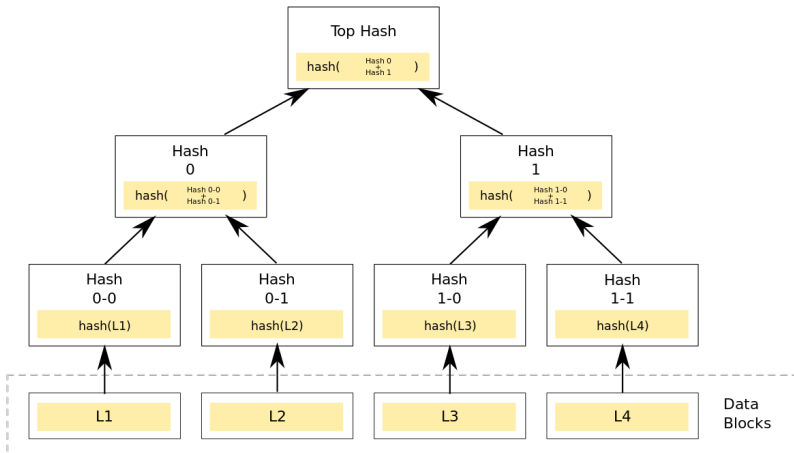
- ▶ Število podpisnikov omejeno
- ▶ Tehnikalije v dokazu varnosti
- ▶ **Rešitev:** Podpis  $\sigma_i$  sporočila  $H(X_1, I_1, X_2, I_2, \dots, X_L, I_L)$

# Problem 5

Velikost ključa

- ▶ V ključ moramo torej dati  $\sigma_i$  in  $X_1, I_1, X_2, I_2, \dots, X_L, I_L$
- ▶ Predolg ključ, proporcionalen velikosti  $G$
- ▶ **Rešitev:** Merklovo drevo z listi  $I_1, I_2, \dots, I_L$

# Merklova drevesa



# Problem 6

## Sočasno podpisovanje

- ▶ Dokaz varnosti uporablja previjanje (angl. *rewinding*)
- ▶ **Rešitev:** Ne dovolimo sočasnega podpisovanja

# Končna shema



# Varnost