Sheme za zapriseganje

Marinka Žitnik

UNI LJ, FRI

5. junij 2012

Motivacija

- *Zaklenjena škatla* v vsakdanjem življenju.
  - Vsebina v škatli je skrita in nedostopna brez ključa.
  - Vsebino lahko razkrijemo le na en način.
- Poštena izmenjava informacij med strankami.
  - Nobena stranka ne sme izvedeti za izbrane vrednosti drugih vpletenih dokler sama ne razkrije svoje vrednosti.
  - Razkritje vrednosti je enolično in razkrije se lahko le vrednost, ki jo je stranka izbrala. Stranka se je k vrednosti **zavezala**, vrednost **zaprisegla**.

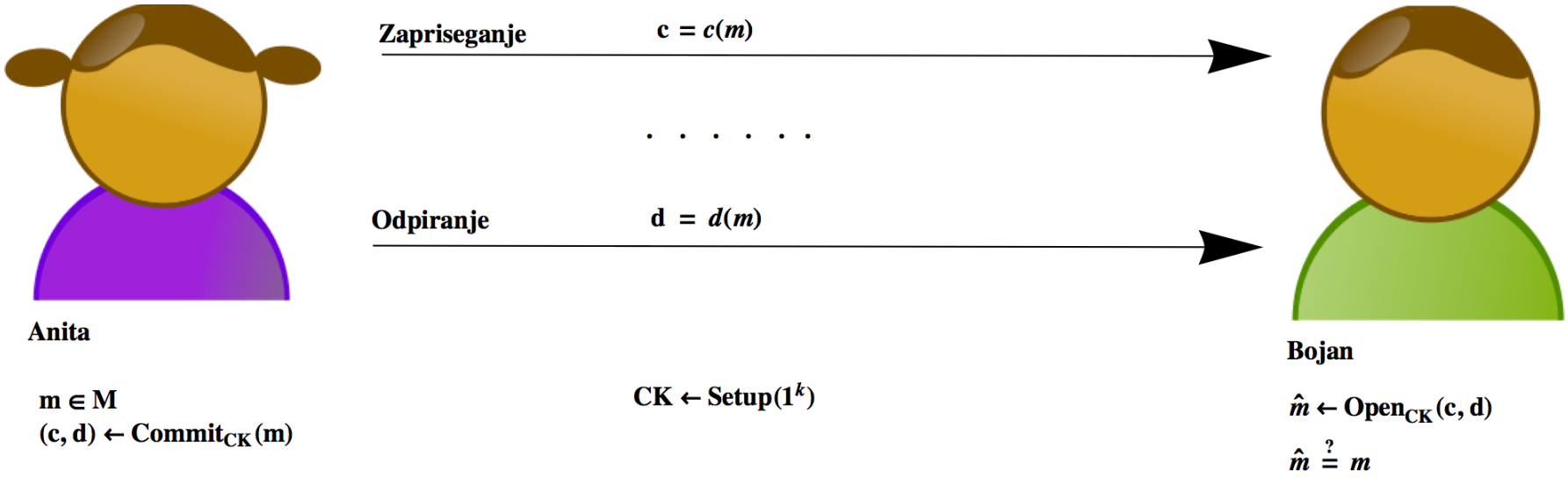
Sheme za zapriseganje

Definicija

Shema za zapriseganje je trojček $(\texttt{Setup}, \texttt{Commit}, \texttt{Open})$:

- $\texttt{CK} \leftarrow \texttt{Setup}(1^k)$ generira javni ključ za zapriseganje CK.
- $(c, d) \leftarrow \texttt{Commit}_{CK}(\text{m})$ za $m \in M$. $c = c(m)$ **zaprisežena vrednost** in $d = d(m)$ **vrednost odpiranja.**
- $\texttt{Open}_{CK}(\text{c,d}) \rightarrow \tilde{\text{m}} \in M \cup \{\perp\}$.
- Pravilnost. $\forall m \in M$, $\texttt{Open}_{CK}(\texttt{Commit}_{CK}(m)) = m$.

Sheme za zapriseganje



Slika: Shema za zapriseganje.

Zaveza in skrivanje

1. **Skrivanje.** Računsko težko izvedljivo je, da nasprotnik A_1 generira dve sporočili $m_0, m_1 \in M$, tako da A_2 lahko razlikuje med zapriseženima vrednostima c_0, c_1. To pomeni, da $c(m)$ ne razkrije nobene informacije o sporočilu m.
2. **Zaveza.** Računsko težko izvedljivo je, da nasprotnik A izračuna *trčenje* (c, d, d'), tako da sta (c, d) in (c, d') veljavna para za zapriseganje za sporočili m in m', $m \neq m'$.

Katera stranka požene `Setup` algoritem?

- Center zaupanja. *Sheme za zapriseganje z javnimi parametri.*
- Prejemnik. *Informatično-teoretsko skrivanje.*
- Pošiljatelj *Informatično-teoretska zaveza.*
- Prejemnik generira nov ključ `CK` za vsako sporočilo. *Interaktivna shema.*

Brezpogojno ... računsko

Brezpogojna zaveza Anita ne more spremeniti zaprisežene vrednosti, tudi če bi imela neomejeno računsko moč.

Računska zaveza $P^* \in \mathcal{RP}$. Naj bo $\epsilon(k)$ verjetnost, s katero P^* vrne c z $\mathtt{Open_C K}(c, d), m' \leftarrow \mathtt{Open_{CK}}(c, d'), m' \neq m$. $\epsilon(k)$ je zanemarljiva v k.

Brezpogojno skrivanje Porazdelitvi $\mathtt{Commit}_{CK}(0)$ in $\mathtt{Commit}_{CK}(1)$ sta statistično neločljivi.

Računsko skrivanje Bojan s polinomsko računsko močjo težko ugotovi m iz objavljene zaprisežene vrednosti.

Brezpogojno skrivanje in zaveza

Lema

Sheme za zapriseganje z lastnostmi brezpogojnega skrivanja in brezpogojne zaveze ne obstajajo.

Dokaz.

Recimo, da obstaja taka shema $\mathfrak{C}$ in Anita z njo zapriseže sporočilo $m = 0$, $c = \mathtt{Commit}_{CK}(r, 0)$. Obstaja r', da velja $c = \mathtt{Commit}_{CK}(r', 1)$, sicer zaprisežena vrednost zagotovo ni $m = 0$. (**skrivanje**)
Anita z neomejeno računsko močjo poišče ustrezni r' in spremeni zapriseženo vrednost m na $m' = 1$, ne da bi to lahko ugotovil Bojan. (**zaveza**) □

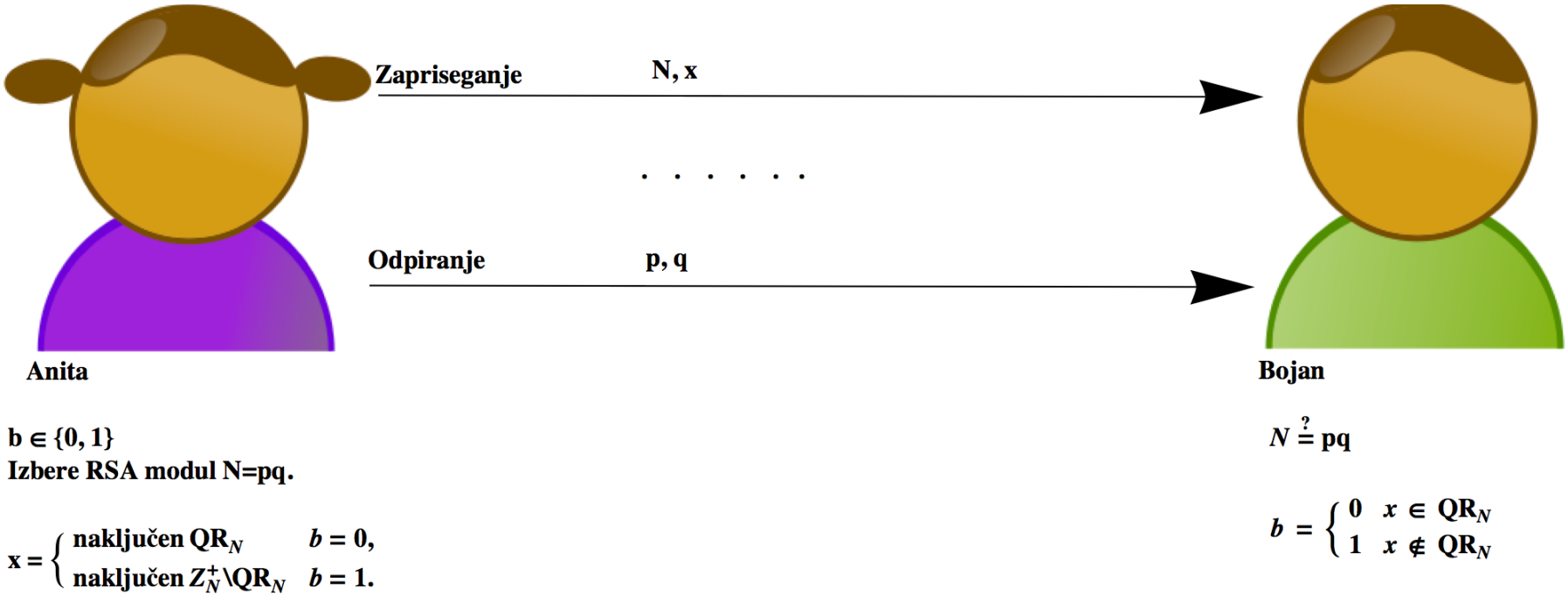
Opis in varnost ... v projektu

- Kriptografski sistem z zaprisego.
- Enobitna shema s PRG.
- Enobitna shema z OWP.
- Sheme z uporabo CRHF.
- Pedersenova shema.

Sestavljanje novih shem iz obstoječih

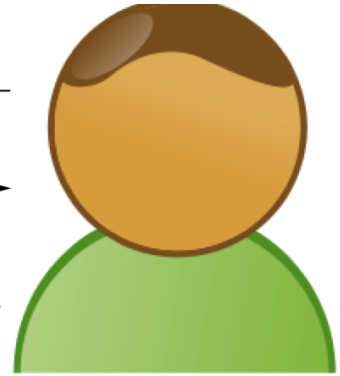
- Bit-by-bit.
- Hash-then-commit.
- Sproščena zaveza (vzporedno šifriranje z avtentikacijo).

Metanje kovanca preko telefona (prvič)



Slika: Konstrukcija sheme za varno metanje kovanca na osnovi QRA.

Metanje kovanca preko telefona (drugič)



p, g, s

Zapriseganje x

. . . . . .

Odpiranje y

Anita

$p \stackrel{?}{=}$ praštevilo

$g \stackrel{?}{\in} QR_p$

$s \stackrel{?}{\in} QR_p$

$b \in \{0, 1\}$

Izbere naključen $y \in Z_{(p-1)/2}$.

$$x = \begin{cases} g^y & b = 0 \\ s\,g^y & b = 1 \end{cases}$$

Bojan

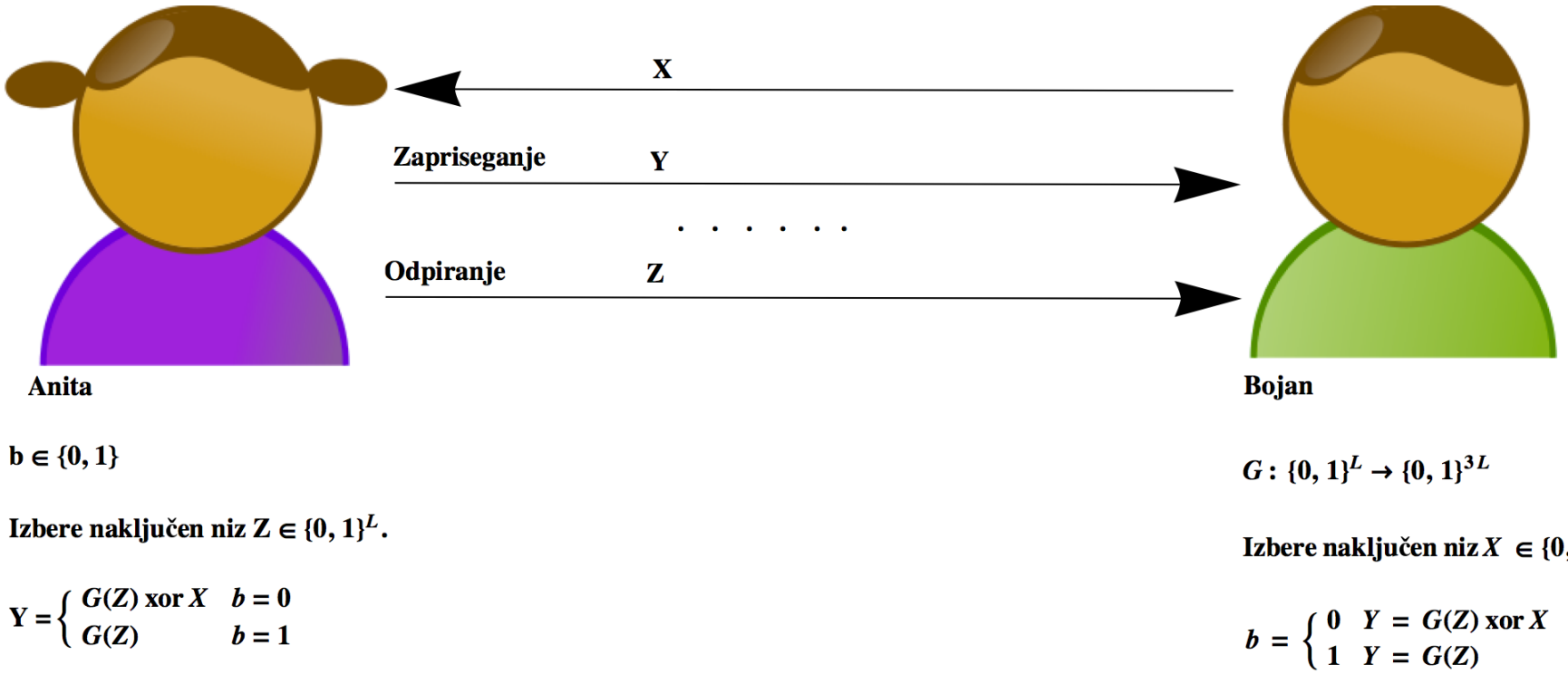
Izbere

– praštevilo p,
– generator $g \in QR_p$,
– naključen $s \in QR_p$.

$$b = \begin{cases} 0 & x = g^y \\ 1 & x = s\,g^y \end{cases}$$

Slika: Konstrukcija sheme za varno metanje kovanca na osnovi DLP.

Metanje kovanca preko telefona (tretjič)



Slika: Konstrukcija sheme za varno metanje kovanca na osnovi PRG (Naor, 91).

Dokazi brez razkritja znanja

Izrek

Če obstajajo enosmerne permutacije, potem ima vsak jezik v $\mathcal{NP}$ dokaz brez razkritja znanja.

??? Ali obstoj enosmernih funkcij implicira obstoj shem za zapriseganje z brezpogojnim skrivanjem. **???**

Dokazi brez razkritja znanja

Dokaz.

Najprej podamo dokaz brez razkritja znanja za problem 3COLOR (**Shema za zapriseganje**). Nato reduciramo originalni jezik L na 3COLOR z uporabo Cook-ove redukcije.

1. Dokazovalnik P enakomerno izbere naključno permutacijo π nad $\{1, 2, 3\}$. Za $i = 1, 2, \ldots, n$, P pošlje zaprisego $\mathfrak{C}(\pi(\phi(i)))$ preverjevalniku V.
2. V enakomerno izbere naključno povezavo $e \in E$.
3. Ob sprejemu $e = (i, j) \in E$, P razkrije i-ti in j-ti vrednosti.
4. V preveri, da sta razkrita $\phi(i), \phi(j)$ različna elementa iz $\{1, 2, 3\}$ in da se ujemata z zaprisegami iz 1.