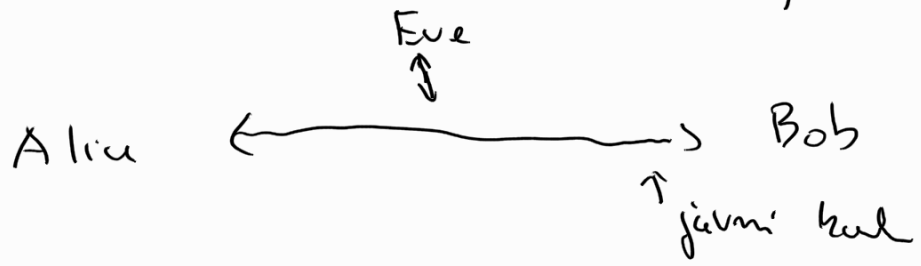
Kvantna kriptografija

· protokol za razmjenu ključeva BB 84

(Bennet, Brassard, 1984)



1. Alice dva stringa: $x = x_1 \dots x_n$ i $y = y_1 \dots y_n$ (slučajno gen.)

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{x_i y_i}\rangle \quad \text{gdje}$$

y_i odredio bazu

$|\psi_{00}\rangle = |0\rangle \qquad |\psi_{10}\rangle = |1\rangle$

$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; $|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

2. Alice pošalje tih n qubita Bobu.

3. Bob generira slučajan string $y' \in \{0,1\}^n$ i

svaki primljen qubit mjeri

i) ako $y'_i = 0$ ... $\{|0\rangle, |1\rangle\}$

ii) ako $y'_i = 1$ ... $\{|+\rangle, |-\rangle\}$

... → ako je $y_i = y'_i$ onda Bob mjeri qubit u "istoj" bazi kao i Alice.

$x' \in \{0,1\}^n$ string rezultata ishoda

$|0\rangle, |+\rangle \rightsquigarrow$ bilježi s 0, $|1\rangle, |-\rangle \dots \rightsquigarrow 1$

4. Alice i Bob objave stringove y i y' te iz stringova x i x' izbace sve one bitove za koje je $y_i \neq y'_i$

$\rightsquigarrow$ ono što je preostalo je njihov "polu-privatni" ključ.

U idealnom slučaju, kad nije bilo greške, zbog konst. vrijedi da $y_i = y'_i \Rightarrow x_i = x'_i$

$$\left(y_i = y'_i = 0 \rightsquigarrow \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \rightsquigarrow \{|0\rangle, |1\rangle\} \rightsquigarrow \begin{matrix} |0\rangle \rightsquigarrow x \\ \searrow |1\rangle \end{matrix} \right)$$

Što ako je Eve prisluškivala?

Jedna vrsta "napada". Pretp. da Eve presreće qubit koji je Alice poslala Bobu i taj qubit izmjeri u bazi $\{|\phi_0\rangle, |\phi_1\rangle\}$

gdje su $|\phi_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$; $|\phi_1\rangle = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle$

$(y_i = y'_i) \rightsquigarrow$ Eve presreće taj qubit.

$\overset{\shortparallel}{0}$ A ako je Eve izmjerila $|\phi_0\rangle$, koja je vjerojatnost da je $x_i = 0$ (uzmimo da je Alice poslala $|0\rangle$)

[Koji inf. o x_i Eve dobije svojom mjerenjem?]

Računamo uvjetnu vjerojatnost $P(|0\rangle \mid |\phi_0\rangle)$ koristimo Bayesov teorem:

$$P(|0\rangle \mid |\phi_0\rangle) = \frac{\overset{\cos^2\frac{\pi}{8}}{P(|\phi_0\rangle \mid |0\rangle)} \cdot \overset{\frac{1}{2}}{P(|0\rangle)}}{\underset{\frac{1}{2}}{P(|\phi_0\rangle)}} = \cos^2\frac{\pi}{8} \approx 0.85$$

$P(|0\rangle) = \frac{1}{2}$ $\quad P(|\phi_0\rangle) = P(|\phi_0\rangle \mid |0\rangle) \cdot \overset{\frac{1}{2}}{P(|0\rangle)} + P(|\phi_0\rangle \mid |1\rangle) \cdot \underset{\frac{1}{2}}{P(|1\rangle)}$

$= \cos^2\frac{\pi}{8} \cdot \frac{1}{2} + \sin^2\frac{\pi}{8} \cdot \frac{1}{2} = \frac{1}{2}$

Vrijedi $|0\rangle = \cos\frac{\pi}{8}|\phi_0\rangle < \sin\frac{\pi}{8}|\phi_1\rangle$ $\rightarrow$ u bazi $\{|\phi_0\rangle, |\phi_1\rangle\}$

$\cos^2\frac{\pi}{8}$ $\sin^2\frac{\pi}{8}$

U 85% slučajeva Eve će saznati X_i, ali

nakon toga će se qubit nalaziti u stanju $|\phi_0\rangle$ pa kad ga

Bob bude mjerio u bazi $\{|0\rangle, |1\rangle\}$ s vjerojatnost

od 15% će izmjeriti $|1\rangle$, odnosno za taj i

$X_i \neq X_i'$ $\Rightarrow$ uplitanje od Eve će biti vidljivo

u stringovi X i X'

5. Alice i Bob moraju procijeniti koliko Eve zna

o X i X'?

Slučajno će odabrati "pola" bitova u svojim stringovi

i usporediti. Ako je nepodudarnost mala ($< 10\%$)

onda će nastaviti dalje s protokolom, inače će krenuti

iz početka.

6. U ovom trenutku Alice i Bob ima stringova koji se

podudaraju u 90% bitova.

i) podudaraju na svim mjestima s velikom vjerojatnosti.

ii) Eve nema skoro nikakvu inform. o stringovima

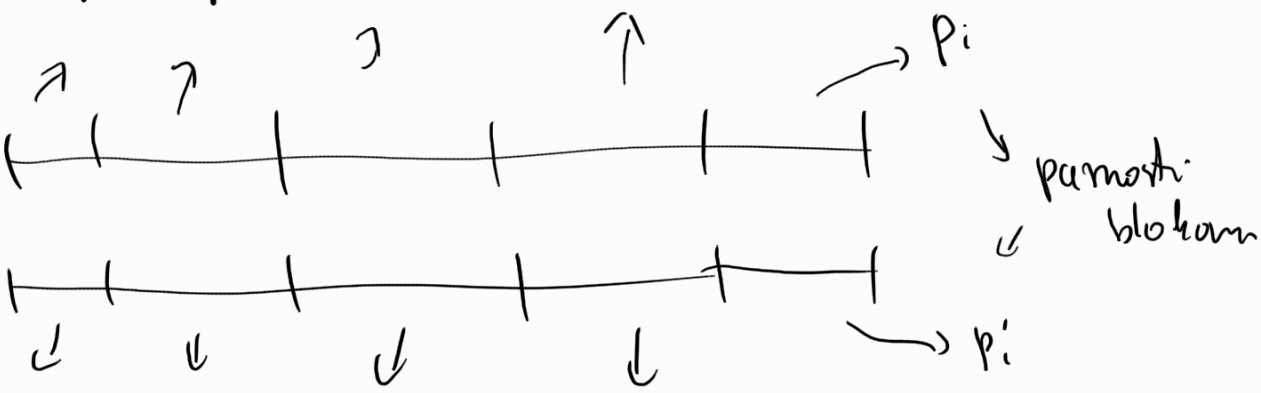
1. informatiom reconciliation

i) Alice i Bob primijeni slučajnu permutaciju na

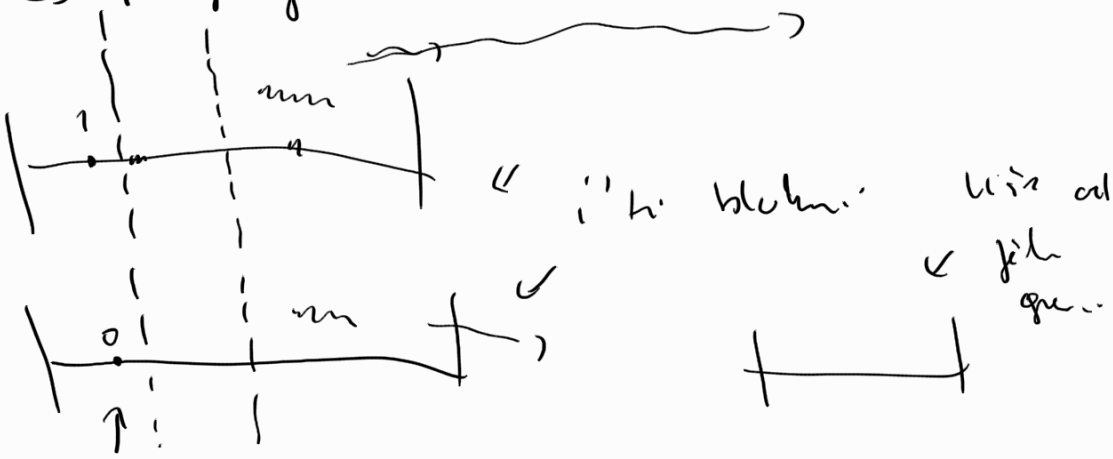
svoje stringovi kako bi greške ravnomjerno preraspodijelili

ii) Svoje string. podijeli u blokovi od po b bitova

tako da je malo vjerojatno da blok duljine b ima više od jedne greške



Ako $p_i \neq p_i'$ => postoji greška u bloku i



- izbace zadnji bit iz svakog bloka koji su obrađeni

=> ponovno pretraži postoje li

U ovom trenutku, stringovi x i x' se gotovo sigurno podudaraju u svim bitovima.

Problem je što Eve možda zna neke bitove tog ključa.

(privacy amplification)

Alice i Bob se dogovore oko hash funkcije koja će primijeniti na svoj string.

hash fn.

$$f: \{0,1\}^m \to \{0,1\}^k \qquad k < m$$

$x, x' \in \{0,1\}^m$

kompresija

Hash funk. ima svojstvo da se reprezentacija ponaša na kliknu strizanje.

$k < n$

$$\underbrace{|0\ 1\ 0\ 1\ 0|}_{|0\ 1\ 1\ 1\ 0|} \xrightarrow{f} \text{"potpun" razlikuje stran. l.d.}$$

razlikuje se u 3. kl.

$$x \approx x' \xrightarrow{f} f(x) = f(x')$$

Eve.

$\Rightarrow f(x) = f(x')$ = privatni ključ koji su Alice i Bob zamijenili.