Kvantna enkripcija (BB84)

Kvantna računala (SI)

9. listopada 2020.

Protokoli za kvantnu razmjenu ključa (QKD)

QKD = Quantum Key Distribution

Protokoli šifrirane komunikacije koji koriste tzv. *tajni ključ* zahtijevaju da tajni ključ bude poznat isključivo pošiljatelju i primatelju šifrirane poruke te da ga oni dovoljno jednostavno i često mogu zamijeniti novim tajnim ključem.

Kritična faza svakog takvog protokola je ona u kojoj dvije stranke razmijenjuju tajne ključeve. Prisluškivanje komunikacije u fazi razmjene ključa može omogućiti trećoj stranci dešifriranje svih daljnjih poruka.

Oslanjajući se na temeljna načela kvantne fizike, moguće je osmisliti protokol za razmjenu tajnog ključa koji dozvoljava provjeru je li komunikacija bila prisluškivana.

Najpoznatiji protokoli za kvantnu razmjenu ključa

- BB84 (Bennett i Brassard, 1984): koristi se komplementarnost baza u pripremi i mjerenju stanja qubitova.

  `http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf`

- E91 (Eckert, 1991): oslanja se na spregnuta stanja qubitova (ovaj protokol ovdje za sada ne obrađujemo).

Fizičke realizacije koriste stanja polarizacije fotona s pomoću kojih se odvija komunikacija.

Osnovne pretpostavke

Protokol BB84 služi za uspostavljanje tajnog enkripcijskog ključa odnosno ključa koji je poznat isključivo dvjema strankama koje zovemo Alice (pošiljateljica) i Bob (primatelj).

Stranku koja pokušava prisluškivati komunikaciju između Alice i Boba i na taj način steći uvid tajni enkripcijski ključ zovemo Eve.

Protokol BB84 omogućuje provjeru tajnosti komunikacije između Alice i Boba. Pokaže li se da je komunikacija bila prosluškivana, uspostavljeni ključ se odbacuje.

Osnovne pretpostavke su:

- Alice može poslati Bobu niz fotona u različitim stanjima linearne polarizacije.
- Bob može mjeriti stanje polarizacije fotona koje prima.
- Eve može presresti fotone koje je poslala Alice, izmjeriti njihovo stanje polarizacije, kreirati nove (zamjenske) fotone i poslati ih Bobu.

Nulti korak: Alice i Bob odabiru dvije baze koje će koristiti pri pripremi i pri mjerenju stanja polarizacije fotona. Neka su to:

- baza B_+ koju čine stanja $|x\rangle$ i $|y\rangle$ (linearna polarizacija u smjeru osi x i y) te
- baza $B_\times$ koju čine stanja stanja $|\pi/4\rangle$ i $|-\pi/4\rangle$ (linearna polarizacija pod kutevima $\pm 45^\circ$ u donosu na os x).

Dogovor uključuje pridruživanje vrijednosti 0 i 1 stanjima baze:

Baza	Stanja baze	Vrijednost	Nova oznaka
B_+	$\|x\rangle$	0	$\|0_+\rangle$
	$\|y\rangle$	1	$\|1_+\rangle$
$B_\times$	$\|\pi/4\rangle = 1/\sqrt{2}\,(\|x\rangle + \|y\rangle)$	0	$\|0_\times\rangle$
	$\|-\pi/4\rangle = 1/\sqrt{2}\,(\|x\rangle - \|y\rangle)$	1	$\|1_\times\rangle$

Eve također zna za taj dogovor.

Koraci uspostavljanja ključa

Prvi korak: Alice šalje Bobu niz fotona pri čemu stanje polarizacije pojedinog fotona proizlazi iz

- slučajnog niza vrijednosti klasičnog bita 0 ili 1
- i slučajnog niza odabira baze B_+ ili $B_\times$.

Alice pamti, ali za sada ne objavljuje slučajne nizove koje je koristila. U nizu fotona koji putuju prema Bobu pojavljuju se četiri različita stanja polarizacije:

Alice:	Vrijednost bita	0		1	
	Baza	B_+	$B_\times$	B_+	$B_\times$
	Stanje polarizacije	$\|0_+\rangle$	$\|0_\times\rangle$	$\|1_+\rangle$	$\|1_\times\rangle$

Drugi korak: Bob mjeri stanja polarizacije fotona pritom slučajno odabirući bazu. (Za sada pretpostavljamo da Eve ne prisluškuje.)

Primjer: Isječak komunikacije bez prisluškivanja

Alice:	Vrijednost	...	0	1	0	1	1	...
	Baza	...	$B_\times$	$B_\times$	B_+	$B_\times$	B_+	...
	Stanje	...	$\|0_\times\rangle$	$\|1_\times\rangle$	$\|0_+\rangle$	$\|1_+\rangle$	$\|1_+\rangle$	...
Bob:	Baza	...	$B_\times$	B_+	B_+	B_+	B_+	...
	Mjerenje	...	0	$0/1$	0	$0/1$	1	...

U mjerenjima u kojima Bob koristi istu bazu koju je koristila Alice, on dobiva onu vrijednost bita koju je Alice poslala.

U mjerenjima u kojima Bob koristi različitu bazu od one koju je koristila Alice, on mjerenjem dobiva vrijednosti bita 0 ili 1 s jednakom vjerojatnošću (oznaka $0/1$).

Treći korak: Alice i Bob objavljuju nizove baza koje su koristili i uspoređuju ih. Iz niza vrijednosti bitova oni izbacuju one vrijednosti bitova kod kojih su koristili različite baze (približno 50% slučajeva), dok ostale vrijednosti zadržavaju kao tajni ključ.

Primjer: Isječak iz komunikacije bez prisluškivanja s uspostavljenim ključem

Alice:	$\cdots$	0	1	1	0	1	0	0	$\cdots$
	$\cdots$	B_+	B_+	$B_\times$	B_+	$B_\times$	$B_\times$	B_+	$\cdots$
	$\cdots$	$\lvert 0_+\rangle$	$\lvert 1_+\rangle$	$\lvert 1_\times\rangle$	$\lvert 0_+\rangle$	$\lvert 1_\times\rangle$	$\lvert 0_\times\rangle$	$\lvert 0_+\rangle$	$\cdots$
Bob:	$\cdots$	B_+	$B_\times$	B_+	B_+	$B_\times$	B_+	B_+	$\cdots$
	$\cdots$	0	$0/1$	$0/1$	0	1	$0/1$	0	$\cdots$
Ključ:	$\cdots$	0	-	-	0	1	-	0	$\cdots$

Koraci provjere privatnosti

Četvrti korak: Alice i Bob javno razmijenjuju uzorak (maleni dio) uspostavljenog tajnog ključa te ga uspoređuju.

Ako je komunikacija za vrijeme uspostave ključa bila prisluškivana, pojavit će se odstupanje ključeva u približno 25% bitova. Uoče li Alice i Bob takvo odstupanje, oni napuštaju ključ jer je moguće da je do odstupanja došlo zbog prisluškivanja.

Prisluškivanje dovodi do odstupanja u ključu zbog toga što Eve, s obzirom da ne zna koju je bazu Alice odabrala za dani foton, bazu koju koristi za mjerenje stanja polarizacije i slanje zamjenskog fotona odabire slučajno. Odabere li bazu koja se razlikuje od one koju je koristila Alice, mjerenjem stanja polarizacije i slanjem zamjenskog fotona ona mijenja njegovo stanje polarizacije.

Primjer: Isječak iz komunikacije s prisluškivanjem i pogreškama u uspostavljenom ključu

Alice:	$\cdots$	0	1	1	1	0	$\cdots$
	$\cdots$	B_+	B_+	$B_\times$	$B_\times$	B_+	$\cdots$
	$\cdots$	$\|0_+\rangle$	$\|1_+\rangle$	$\|1_\times\rangle$	$\|1_\times\rangle$	$\|0_+\rangle$	$\cdots$
Eve:	$\cdots$	$B_\times$	B_+	B_+	$B_\times$	B_+	$\cdots$
	$\cdots$	$0/1$	1	$0/1$	1	0	$\cdots$
	$\cdots$	$\|0_\times\rangle/\|1_\times\rangle$	$\|1_+\rangle$	$\|0_+\rangle/\|1_+\rangle$	$\|1_\times\rangle$	$\|0_+\rangle$	$\cdots$
Bob:	$\cdots$	B_+	$B_\times$	B_+	$B_\times$	$B_\times$	$\cdots$
	$\cdots$	$0/1$	$0/1$	$0/1$	1	$0/1$	$\cdots$
Ključ:	$\cdots$	$0/1$	-	-	1	-	$\cdots$