Kvantna enkripcija

Kvantna računala (SI)

19. studenog 2018.

Protokoli za kvantnu razmjenu ključa (QKD)

QKD = Quantum Key Distribution

Protokoli enkriptirane komunikacije koji koriste tzv. *tajni ključ* zahtijevaju da on bude poznat isključivo dvjema strankama (pošiljatelju i primatelju enkriptirane poruke) te da ga se dovoljno jednostavno i dovoljno često može zamijeniti novim tajnim ključem.

Kritična faza svakog takvog protokola je ona u kojoj dvije stranke razmijenjuju tajne ključeve. Prisluškivanje komunikacije u fazi razmjene ključa omogućilo bi 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.

Osnovni protokoli za kvantnu razmjenu ključa

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

Podrazumijeva se postojanje dogovora između Alice i Boba o odabiru dviju komplementarnih baza koje će Alice koristiti u pripremi stanja polarizacije fotona i koje će Bob koristiti pri mjerenju stanja polarizacije fotona.

Neka su to baza $\oplus$ sa stanjima $\circ$ i $\ominus$ te njoj komplementarna baza $\otimes$ sa stanjima $\diagdown$ i $\diagup$. Dogovor također uključuje pridruživanje vrijednosti 0 i 1 baznim stanjima:

Baza	Polarizacija	Vrijednost
$\oplus$	$\circ$	0
	$\ominus$	1
$\otimes$	$\diagdown$	0
	$\diagup$	1

Eve također zna za taj dogovor.

Koraci uspostavljanja ključa

Prvi korak: Alice šalje Bobu niz fotona čije stanje polarizacije odgovara slučajnom nizu vrijednosti 0 ili 1 te slučajnom odabiru baze $\oplus$ ili $\otimes$.

Tablica pokazuje primjer fotona koje Alice šalje Bobu:

Alice:							
	Vrijednost	0	1	0	0	1	...
	Baza	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	...
	Polarizacija	$\diagdown$	$\diagup$	$\vert$	$\diagdown$	$-$	...

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

Tablica pokazuje primjer vrijednosti koje Bob dobiva mjerenjem:

Alice:	Vrijednost	0	1	0	0	1	...
	Baza	⊗	⊗	⊕	⊗	⊕	...
	Polarizacija	⦸	⊘	◐	⦸	⊖	...
Bob:	Baza	⊕	⊗	⊗	⊗	⊗	...
	Vrijednost	1	1	0	0	0	...

Važno je uočiti da u onim mjerenjima u kojima Bob koristi različitu bazu od one koju je koristila Alice, on dobiva slučajnu vrijednost 0 ili 1, odnosno vrijednosti koja ne ovisi o vrijednosti koju je koristila Alice.

Treći korak: Bob objavljuje niz baza koje je koristio pri mjerenju, ali ne i rezultate samog mjerenja. Alice uspoređuje Bobov niz s nizom koji je ona koristila te javlja bobu na kojim se mjestima njihovi nizovi podudaraju. Nakon toga Alice i Bob izgrađuju tajni ključ samo od onih vrijednosti 0 i 1 kod kojih su koristili iste baze. (Ostale vrijednosti se odbacuju.)

Primjer:

Alice:	0	1	1	0	1	1	0	0	0	...
	⊕	⊕	⊗	⊕	⊗	⊗	⊗	⊕	⊗	...
	◐	⊖	⊘	◐	⊘	⊘	⦸	◐	⦸	...
Bob:	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊕	⊗	...
	0	0	1	0	1	1	0	0	0	...
Ključ:	0	-	-	0	1	1	-	0	0	...

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 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.

Tablica pokazuje primjer prisluškivane komunikacije i odstupanja u ključu koja su izazvana prisluškivanjem:

Alice:	0	1	1	0	1	1	0	0	0	...
	⊕	⊕	⊗	⊕	⊗	⊗	⊗	⊕	⊗	...
	◑	⊖	⊘	◑	⊘	⊘	⊘	◑	⊘	...
Eve:	⊗	⊕	⊕	⊗	⊗	⊕	⊕	⊗	⊕	...
	1	1	1	1	1	1	1	0	0	...
	⊘	⊖	⊖	⊘	⊘	⊖	⊖	⊘	◑	...
Bob:	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊕	⊗	...
	1	0	1	0	1	1	1	1	0	...
Ključ A:	0	-	-	0	1	1	-	0	0	...
Ključ B:	1	-	-	0	1	1	-	1	0	...