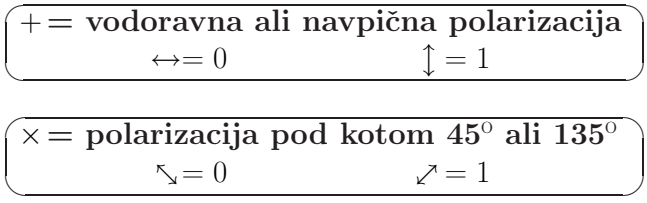
Kvantna kriptografija II. - varna izmenjava ključa

Marko Žnidarič

18. julij 2007

1 Kvantna kriptografija

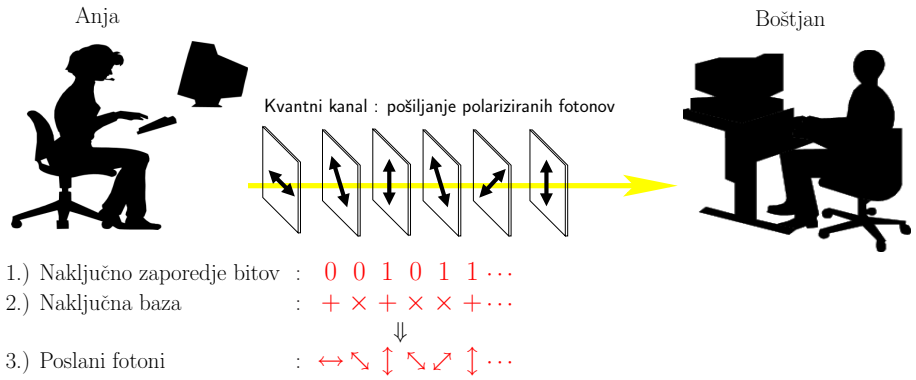
Osnovna ideja kvantne varne komunikacije oziroma natančneje kvantne izmenjave ključa je, da si Anja in Boštjan, še preden začneta s pošiljanjem šifriranih sporočil, po t.i. kvantnem kanalu izmenjata skrivni ključ. Kvantni kanal je povezava med Anjo in Boštjanom, po kateri si izmenjujeta kvantne delce. Kasneje si bomo podrobneje ogledali primer, pri katerem je kvantni kanal kar navadno telekomunikacijsko optično vlakno, po katerem Anja pošlje Boštjanu fotone, torej posebej oblikovane pulze svetlobe. Končni produkt tega prvega kvantnega dela komunikacije je ta, da imata oba enako skrivno geslo, pri čemer lahko absolutno zagotovita, da je le to res znano samo njima, četudi je pošiljanju fotonov nekdo "prisluškoval". Nadaljni postopek, po tem, ko imata skupni ključ, je popolnoma klasičen. Za šifriranje uporabita enega izmed algoritmov z zasebnim ključem, najboljše kar Vernamov postopek, ki je edini dokazano varen. Kot bomo videli, nam varnost prvega dela, torej kvantne izmenjave ključa, zagotavlja kvantna fizika. Varnost izmenjave ključa torej ne temelji na nekem nepreverjenem matematičnem dejstvu, npr. težavnosti faktorizacije, kot pri RSA, temveč na fizikalnih zakonih. Če lahko RSA zaščito zlomimo, če le imamo dovolj hiter računalnik, potem bi vdor v kvantno izmenjavo ključa zahteval kršenje fizikalnih zakonov. Kvantna varna komunikacija torej odpravi glavno pomanjkljivost Vernamovega šifriranja, to je problem varne izmenjave ključa. Oglejmo si podrobneje, kako je zagotovljena varnost kvantne izmenjave ključa.



Slika 1: Slovarček polarizacij.

Princip je enak, kot pri kvantnih bankovcih. Temelj je spoznanje, da kvantnih sistemov ni mogoče pomeriti, ne da bi jih pri tem zmotili. Temu je ekvivalentna izjava, da jih ni mogoče klonirati. Kloniranje kvantnega sistema bi pomenilo, da bi stanje sistema popolnoma verodostojno skopirali. Če bi bilo kloniranje mogoče, bi lahko opravljali meritve, ne da bi sistem zmotili. Sistem bi enostavno klonirali, potem pa opravili meritev

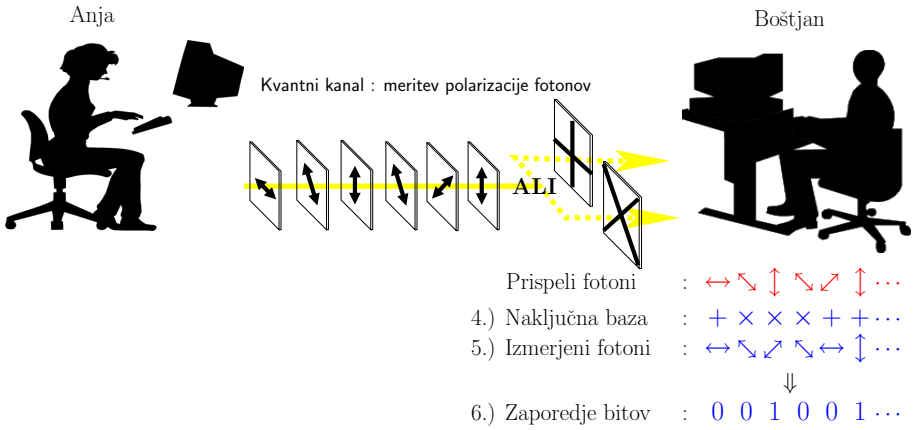
na podvojeni kopiji. Stanje te kopije bi se ob meritvi sicer spremenilo, vendar pa bi stanje prvega sistema ostalo nedotaknjeno. To pa je v nasprotju z zakoni kvantne fizike. Pri kvantni varni komunikaciji za izmenjavo ključa ponavadi uporabimo fotone, ki jih pošiljamo po optičnem vlaknu. Fotoni so lahko v dveh osnovnih ortogonalnih stanjih, ki ju določa smer linearne polarizacije. Dve različni polarizaciji fotona nam pri kvantni komunikaciji predstavljata dve različni vrednosti bita, torej 0 in 1. Dogovoriti se je seveda potrebno, katera smer polarizacije bo pomenila katero vrednost. Npr., vodoravna polarizacija nam pomeni vrednost 0, navpična pa 1. Izkaže se, da za uspešno kvantno izmenjavo ključa ni dovolj, da pošiljamo le vodoravno ali navpično polarizirane fotone. Anja mora pošiljati tudi fotone, ki so polarizirani pod kotom 45^o ali 135^o. Z drugimi besedami, potrebujemo dve bazi, v katerih bomo pošiljali fotone. Anja bo izbirala med navpično bazo, to bomo označili na kratko s $+$, in bo pomenila fotone z navpično ali vodoravno polarizacijo, in diagonalno bazo, na kratko $\times$, ki bo pomenila fotone polarizirane v diagonalni smeri pod kotom 45^o ali 135^o, glej sliko 1. Izbira, katero bazo bo Anja uporabila za posamezni foton, mora biti naključna. Na drugi strani optičnega vlakna mora Boštjan te fotone detektirati, ter, če hoče ugotoviti ali dani foton predstavlja stanje 0 ali 1, tudi ugotoviti, v kateri smeri so ti fotoni polarizirani. Polarizacijo fotona ugotovimo na enostaven način. Če je Anja poslala foton v $+$ bazi, potem Boštjan ta foton enostavno pošlje skozi polarizator, ki prepušča le svetlobo polarizirano v navpični smeri. Če je polarizator foton prepustil, potem je bila polarizacije fotona navpična , torej 1, sicer pa 0. Podobna zgodba je tudi v primeru, da Anja uporabi $\times$ bazo, Boštjan pa ima polarizator obrnjen v diagonalni smeri. Zanimivo vprašanje pa je, kaj se zgodi, če smer Boštjanovega polarizatorja ni kompatibilna z Anjino izbiro baze. Npr., Anja pošlje foton v $\times$ bazi, Boštjanov polarizator pa je obrnjen v navpični smeri. Kvantni račun pokaže, da bo v tem primeru Boštjan v polovici primerov izmeril 0, v polovici pa 1! Kaj bo izmeril za konkretni foton ne moremo napovedati, vse kar vemo so verjetnosti. Ta nedoločenost je ključna za varnost kvantne izmenjave ključa. Eden izmed bolj znanih kvantnih protokolov za izmenjavo ključa se imenuje BB84 po odkriteljih Brassardu in Bennettu ter letu objave 1984.



Slika 2: Anja generira naključni niz bitov. Vsak foton pošlje v naključno izbrani bazi.

1.1 Protokol BB84

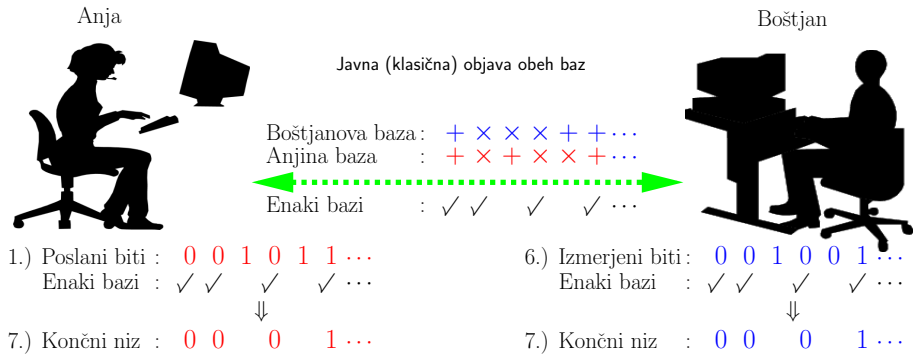
Postopek izmenjave ključa poteka v več korakih. Anja pošilja polarizirane fotone Boštjanu, ta pa meri njihovo polarizacijo.



Slika 3: Boštjan detektira Anjine fotone. Ker ne pozna njene izbire baze, jo tudi sam izbira naključno.

1. Anja ima zaporedje naključnih bitov, ki jih želi poslati Boštjanu.
2. Anja za vsak bit naključno izbere + ali × bazo. Izbira, katero bazo uporabi za posamezni foton, je naključna in znana samo njej (Boštjan ne ve, ali je dani foton poslan v + ali × bazi).
3. Glede na vrednost bita in izbrano bazo Anja pošlje ustrezno polariziran foton, slika 2.
4. Ker Boštjan ne ve, v kateri bazi je poslan posamezni foton, lahko le ugiba. Tako za vsak foton naključno izbere bazo, v kateri bo opravil meritev.
5. Boštjan izmeri foton v izbrani bazi.
6. Iz rezultatov meritev dobi Boštjan niz bitov, slika 3. Ker je v polovici primerov izbral bazo, ki ni kompatibilna z Anjino, ta niz ni enak Anjinemu.
7. Anja in Boštjan po javnem kanalu, npr. telefonu, objavita v katerih bazah sta pošiljala oz. detektirala fotone. Nato oba obdržita le tiste bite, za katere sta izbrala enako bazo, slika 4.

Ker je v polovici primerov Boštjanova izbira baze napačna, je dobljeni niz bitov krajši, kot pa začetni Anjin. V povprečju bo pol krajši. Če bi Anja in Boštjan primerjala njun niz bitov, preden sta zavrgla nekompatibilne, bi ugotovila, da se razlikujeta v 25% primerov (polovici napačnih izbir baz). Kako je z varnostjo? Recimo, da je pošiljanju fotonov prisluškovala Eva. Njena strategija je, da pomeri vse Anjine fotone, in nato Boštjanu pošlje foton v stanju, kot ga je izmerila. Ker tudi Eva ne pozna Anjine izbire baze, tudi sama le to izbira naključno. V polovici primerov bo pravilna, v polovici pa ne. Verjetnost,



Slika 4: Anja in Boštjan javno objavita svoji izbiri baz. Obdržita le tiste bite, za katere sta izbrala enako bazo. Na koncu imata oba enak naključni niz bitov, v prikazanem primeru 0001 . . ..

da bo Boštjan izmeril enako vrednost bita, kot ga je poslala Anja, je sedaj enaka 62.5% (ko Eva izbere kompatibilno bazo, je ta verjetnost 75%, sicer pa 50%). Končna Anjina in Boštjanova niza se bosta torej v primeru Evinega prisluškovanja razlikovala v 37.5% bitov. Verjetnost za različne bite se je ob prisluškovanju povečala iz 25% na 37.5%. To povečanje napak pa lahko Anja in Boštjan zaznata in temu ustrezno ukrepata. Dejstvo je, da Eva ne more prisluškovati, ne da bi bila pri tem odkrita. Kvantna mehanika namreč pravi, da bodo Evine meritve spremenile stanja fotonov in tako vnesla dodatne napake, ki jih lahko zaznamo. Po koncu celotnega kvantnega protokola imata Anja in Boštjan niz naključnih bitov, ki so znani samo njima, in ki potem služijo za Vernamovo šifriranje.

1.2 Tehnologija

Kvantna kriptografija, za razliko od kvantnih računalnikov in kvantne teleportacije, ni samo domena laboratorijskih poskusov, temveč je že komercialno dostopna. Pred nekaj leti je podjetje idQuantique iz Ženeve ponudilo prvi plug&play sistem za kvantno izmenjavo ključev. Podobne izdelke ponuja tudi ameriški MagicQ, svoje pa razvija tudi NEC. Vsi ti sistemi delujejo na principu pošiljanja fotonov po optičnih vlaknih. Za sedaj so razdalje, na katerih delujejo omejene pod 100 km. Da zagotovimo 100% varnost morajo biti izpolnjeni določeni tehnični pogoji, ki potem omejujejo razdaljo, na kateri zadeva še deluje. Problem je v neidealnih polarizatorjih, izkoristku merilcev fotonov, absorbciji svetlobe v optičnih vlaknih... Polprevodniški detektorji fotonov so danes sposobni detektirati posamezni foton z nekaj 10% učinkovitostjo, poleg tega imajo tudi lastni šum, kar pomeni, da včasih zaznajo foton, ko le tega sploh ni bilo. Pulzi svetlobe, ki jih pošiljamo po optičnih vlaknih, morajo biti zelo šibki. V posameznem pulzu namreč ne sme biti več kot le en foton. Če bi imeli v pulzu dva fotona, bi lahko Eva enega pomerila, drugega pa nemotenega poslala naprej Boštjanu. V tem primeru Evinega prisluškovanja ne bi mogli odkriti. Ker je v uporabljenih pulzih le en samcat foton, se le ta slej ko prej absorbira v optičnem vlaknu. Vse te težave skupaj nam omejijo končni doseg na okoli 100 km.

Slika 5: Komercialni sistem za kvantno kriptografijo Vectis podjetja IdQuantique. Slika: © id Quantique SA.