CEMS
ZNANSTVENI CENTAR IZVRSNOSTI ZA NAPREDNE MATERIJALE I SENZORE

Kvantna kriptografija

Ljetna škola fizike 2019
12.09.2019.

dr. Mario Stipčević
Fotonika i kvantna optika
Centar izvrsnosti za napredne materijale i senzore
Institut Ruđer Bošković
http://cems.irb.hr

Projekt sufinancira Europska unija iz Europskog fonda za regionalni razvoj

INSTITUT ZA FIZIKU

Europska unija
Zajedno do fondova EU

Ministarstvo znanosti i obrazovanja

MINISTARSTVO REGIONALNOG RAZVOJA I FONDOVA EUROPSKE UNIJE

Operativni program KONKURENTNOST I KOHEZIJA

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

safu

Što je kriptografija

Područje kompjuterskih znanosti

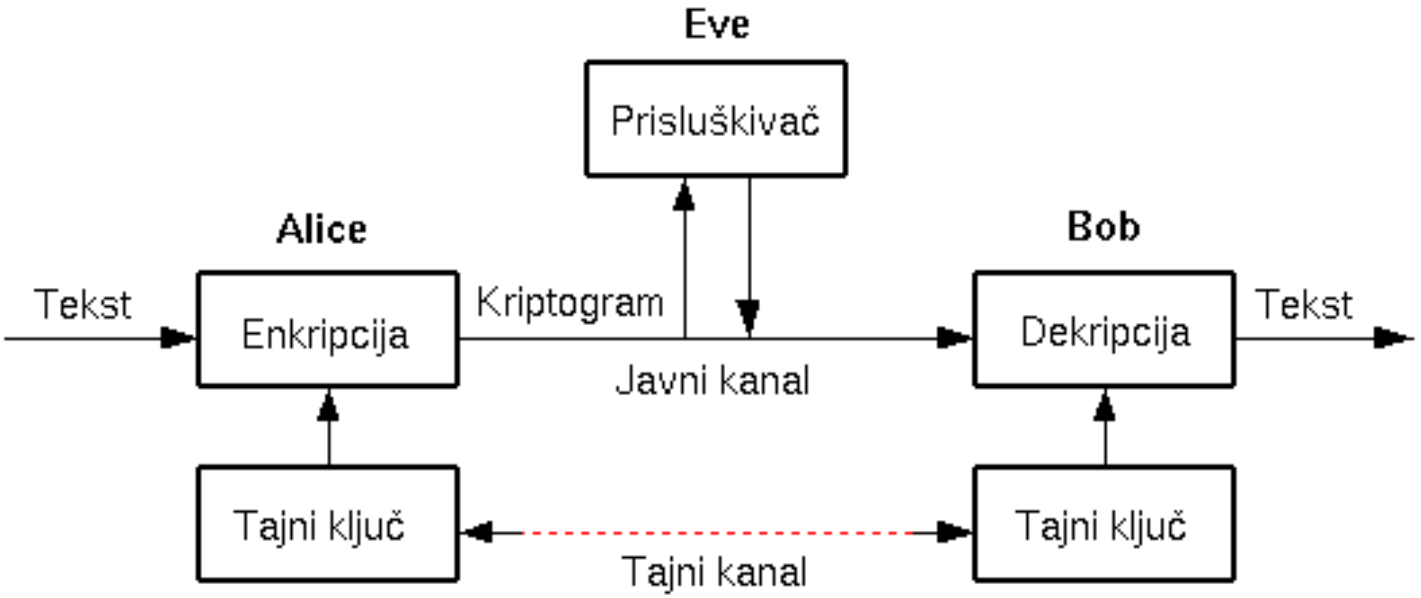
Osnovni zadaci:

- autentikacija
- generiranje tajnog ključa
- osiguravanje tajnosti poruke
- dokaz integriteta poruke
- dokaz neporecivosti

Složeni:

- sigurne komunikacije (mob.)
- elektroničko trgovanje i poslovanje (m,e-bankarstvo, kartice…)
- elektroničko potpisivanje
- anonimne bankovne transakcije
- elektroničko glasovanje
- elektronički novac
- e-država, …

Shannonov model kriptosustava



- Ovaj kriptosustav podrazumijeva da Eve iz javnog kanala prima istu informaciju kao Alice i Bob [1].

- U Shannonovom modelu javlja se problem distribucije tajnog ključa. Osnovno je pitanje: **kako dvije strane koje se nikada nisu vidjele ni čule mogu uspostaviti zajednički tajni ključ ?**

Kvantna kriptografija (Quantum Key Distribution – QKD)

Charles H.Bennett (IBM) i Gilles Brassard (U. Montreal) [5] objavili su 1984. godine prvi ***bezuvjetno siguran*** protokol za generiranje tajnog ključa između dvije strane koje inicijalno dijele malu prethodnu tajnu, baziran na zakonima **kvantne fizike**.

Taj je protokol poznat kao **BB84.**

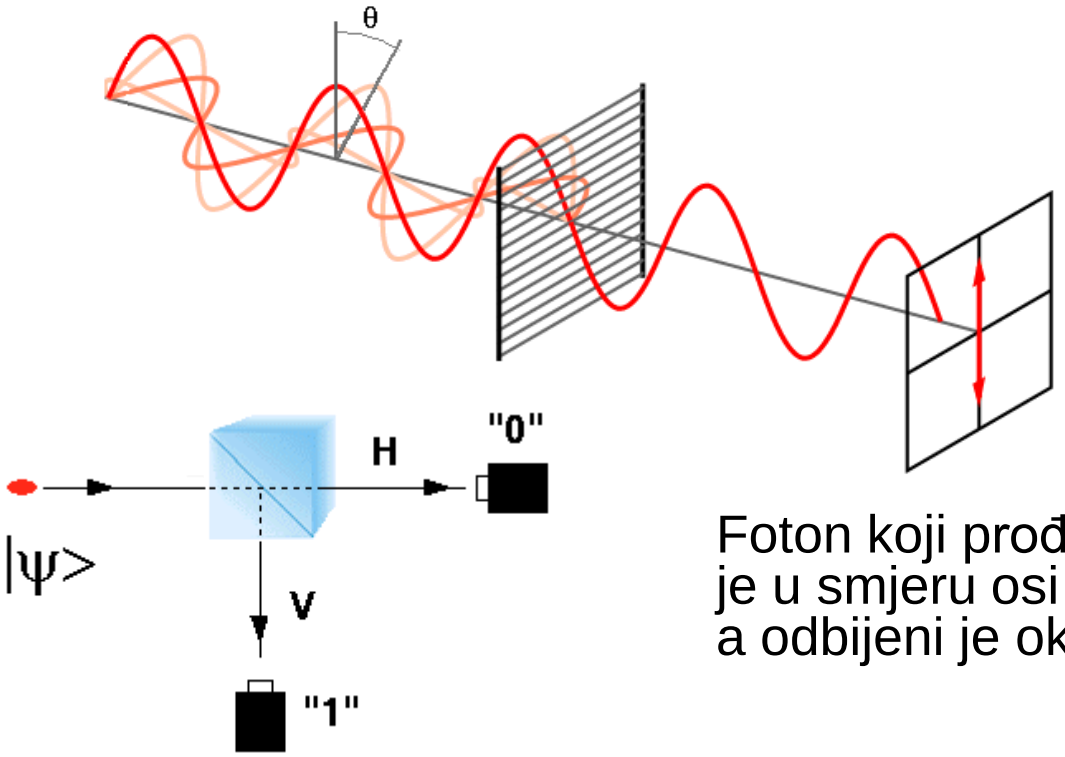
Foton i polarizator

Imamo linearno polarizirani ravni val intenziteta I_0 .

Na polarizatoru: dio prolazi: $I_0 \cos^2(\theta)$, a ostatak se odbija.

FOTON = Najmanji dio svjetlosne energije, ne može se dijeliti.

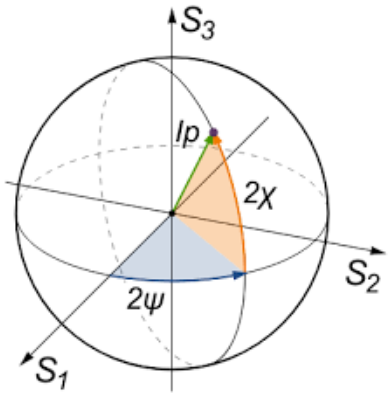
Zbog toga foton prolazi s VJEROJATNOŠĆU $\cos^2(\theta)$, SLUČAJNO!



Foton koji prođe polariziran je u smjeru osi polarizatora, a odbijeni je okomit na os.

Konjugirane baze kvantnih stanja

Kvantni kanal najčešće se realizira pomoću fotona dobro određene polarizacije. Moguće su tri ortogonalne baze polarizacija koje su međusobno konjugirane, npr:

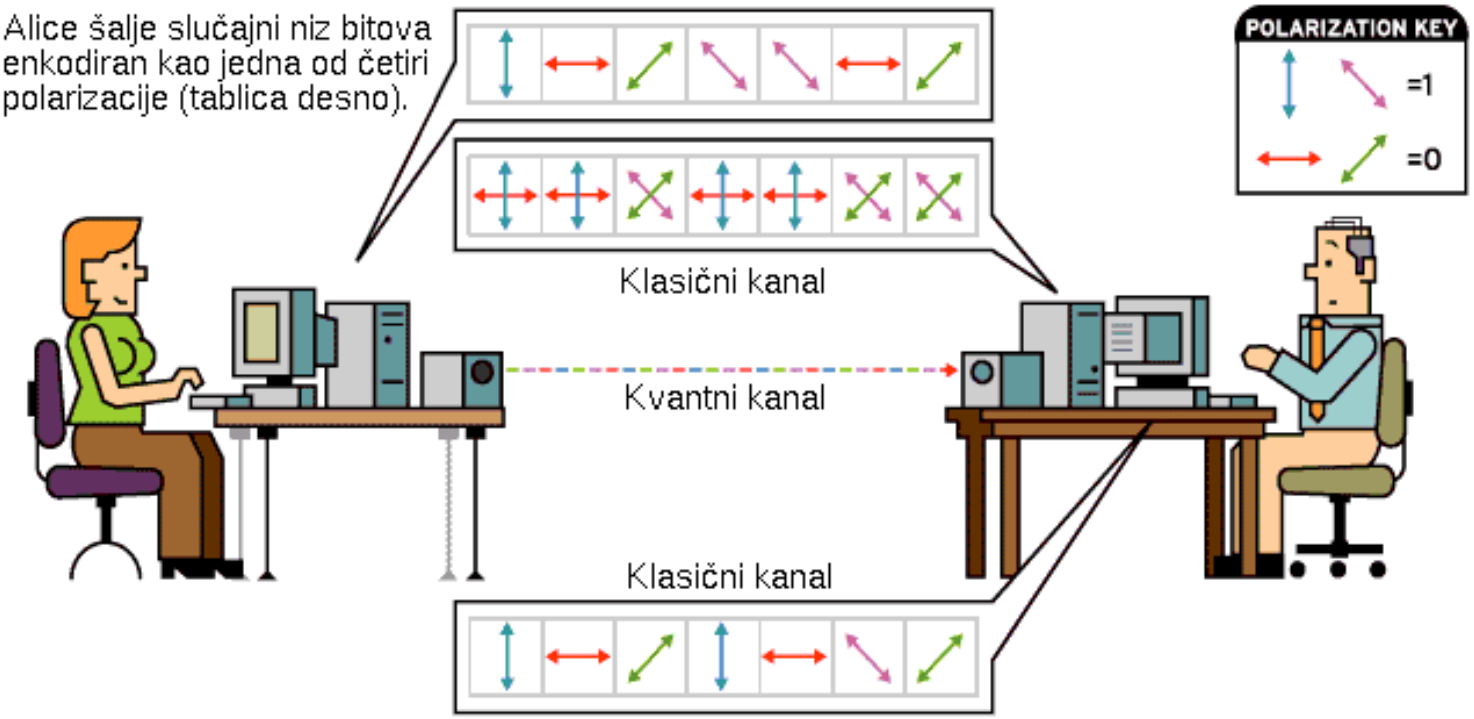


1. vertikalna linearna - horizontalna linearna
2. linearna 45 deg - linearna 135 deg
3. cirkularna lijeva - cirkularna desna

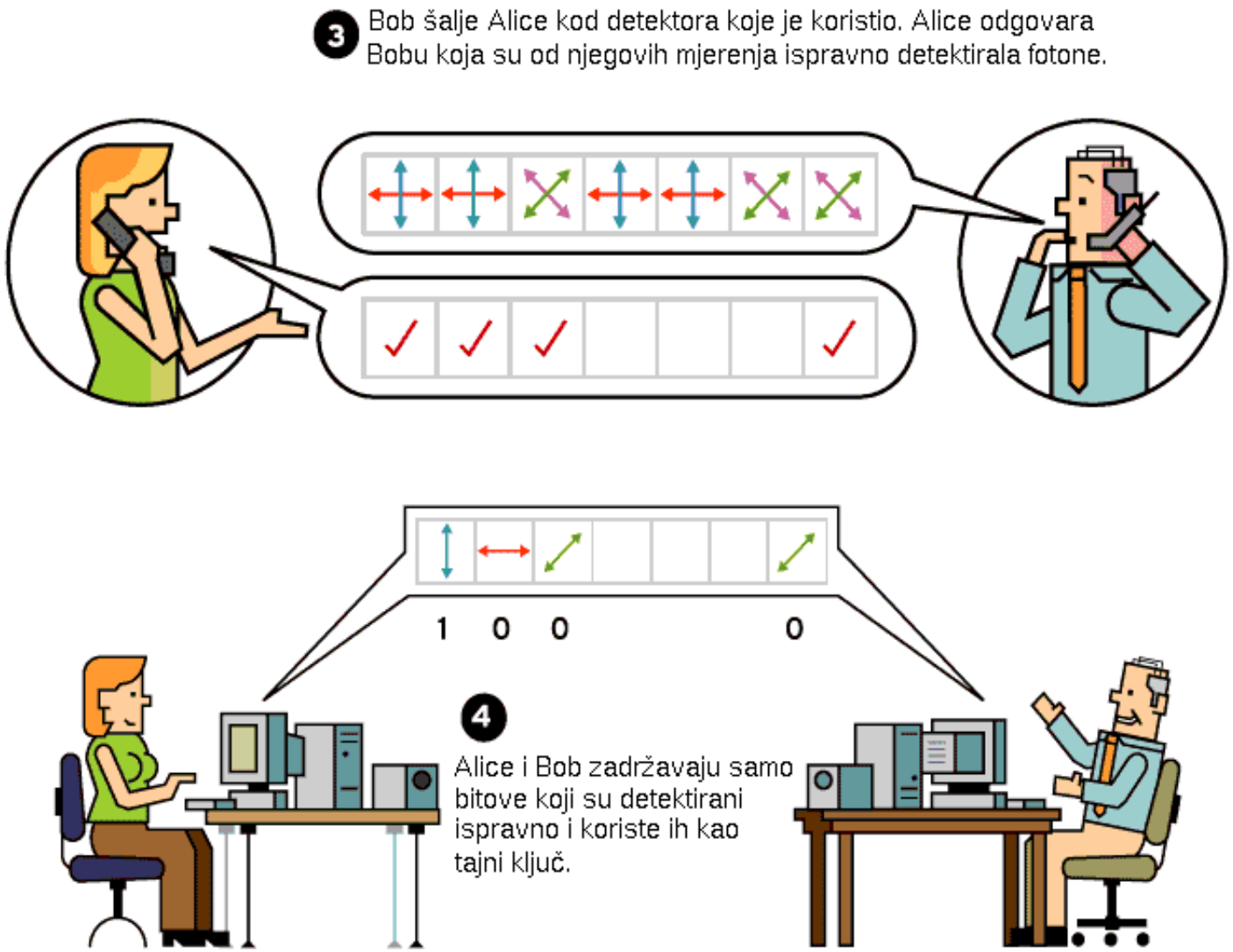
Bilo koje dvije polarizacije iz različitih baza su **konjigirane** tj. ne mogu se razlikovati sa samo jednim polarizatorom (mjerenjem).

Kvantna kriptografija je moguća ako se nule i jedinice enkodiraju međusobno konjugiranim stanjima.

1/3 BB84 protokol – inicijalna faza



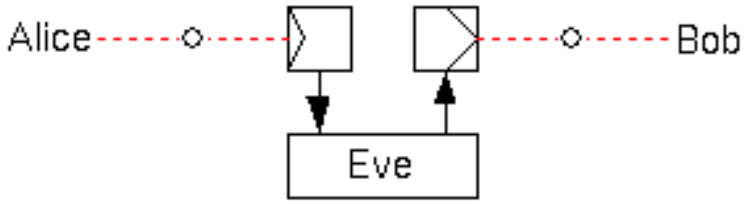
2 Bob odabire na slučajan način jedan od dva tipa detektora: jedan precizno detektira fotone s horizontalnom ili vertikalnom polarizacijom, a drugi one polarizirane pod ±45 stupnjeva. Kad detektor odgovara polarizaciji fotona, oni bivaju detektirani ispravno. No zakoni kvantne mehanike dopuštaju da i fotoni koji ne odgovaraju orijentaciji detektora svejedno mogu biti detektirani kao oni koji odgova–raju i stoga Bob ne zna koje je bitove primio ispravno.


3
Bob šalje Alice kod detektora koje je koristio. Alice odgovara Bobu koja su od njegovih mjerenja ispravno detektirala fotone.
1 0 0 0
4
Alice i Bob zadržavaju samo bitove koji su detektirani ispravno i koriste ih kao tajni ključ.

Sigurnost - napadi na BB84 protokol

Idealno, BB84 se radi tako da se kroz kvantni kanal puštaju samo pojedinačni fotoni. U tom slučaju jedini mogući napad je:

- presretni / pošalji (intercept / resend)



No-cloning teorem onemogućuje da se izvorni foton kopira radi neometanog mjerenja i slanja Bobu.

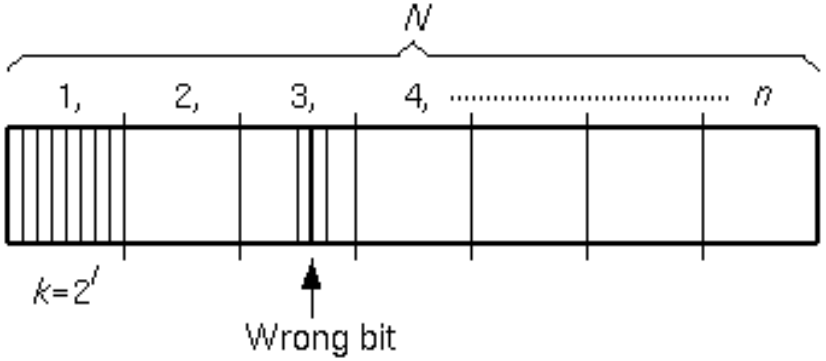
Bilo kakvo mjerenje (prisluškivanje) uništava kvantno stanje Alicinog fotona te neizostavno povećava broj pogrešno primljenih bitova.

Zbog nesavršenosti u aparaturi (nejednakost osi baza, konačna efikasnost detektora, šum) Alice i Bob ipak nemaju posve isti niz.

2/3 Protokol za izjednačenje podataka

Protokol za izjednačenje podataka je u stvari error-correction protokol, pri čemu se pretpostavi da npr. Alice ima “ispravan”, a Bob “oštećeni” niz, pa se protokol svodi na to da se Bobovi podaci usuglase s Alicinim.

- Alice i Bob podijele svatko svoj niz na *n* blokova pa usporede paritete. U blokovima koji imaju različite paritete binarnom pretragom pronalaze različiti bit i odbacuju zadnji bit. Bob invertira “krivi” bit.
- Alice i Bob randomiziraju položaj svih bitova u nizovima javnim protokolom (matricom) te ponavljaju oba koraka nekoliko puta.



Budući da se protokol vodi putem javnog kanala bitan zahtjev jest što manje curenje informacija.

Hash ili digest funkcije

Hash funkcije su varijanta one-way funkcija čiji je argument u skupu nizova bilo koje duljine, a vrijednost u skupu svih nizova jedne određene duljine:

$$H(x):\{0,1\}^{*}\rightarrow\{0,1\}^{r}$$

i za koje vrijedi:

1. Collision resistance:
   za dani *x*, vrlo je teško naći *y* takav da je *H*(*x*) = *H*(*y*)

2. Univerzalnost (Wegman 1979 [9]):

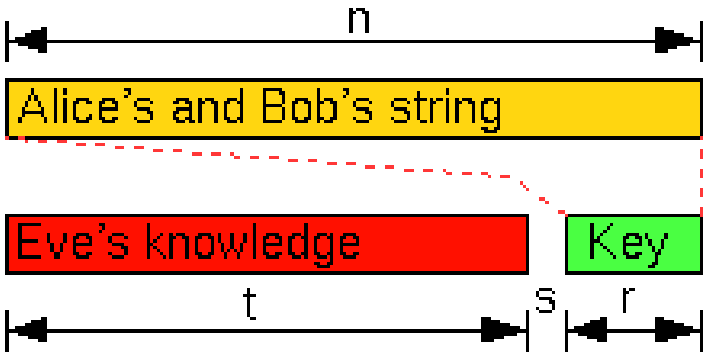
$$x_1 \neq x_2 \Rightarrow p(H(x_1)=H(x_2))<2^{-r}$$

kolokvijalno rečeno, minimalna promjena *x* uzrokuje drastičnu promjenu *H*(*x*).

Najpoznatije hash funkcije su MD5 (*r*=128) i SHA familija (*r*=160-1024).

3/3 Protokol za povećanje privatnosti

Postupak kojim se djelomično tajni niz (kakvog na kraju 2. faze imaju Alice i Bob) može putem javne komunikacije pretvortiti u kraći, vrlo tajni niz - odnosno konačni ključ.



Teorem. Ako se niz duljine *n* o kojem Eve ima *t* bitova informacije hashira na duljinu *r*, onda o rezultirajućem nizu duljine *r* Eve ima manje od

$$2^{-S} / \ln 2$$

bitova informacije, gdje je *s* = *n*–*t*–*r* tzv. *security factor*. Hash funkcija može biti poznata Eve.

Zašto to funkcionira ?

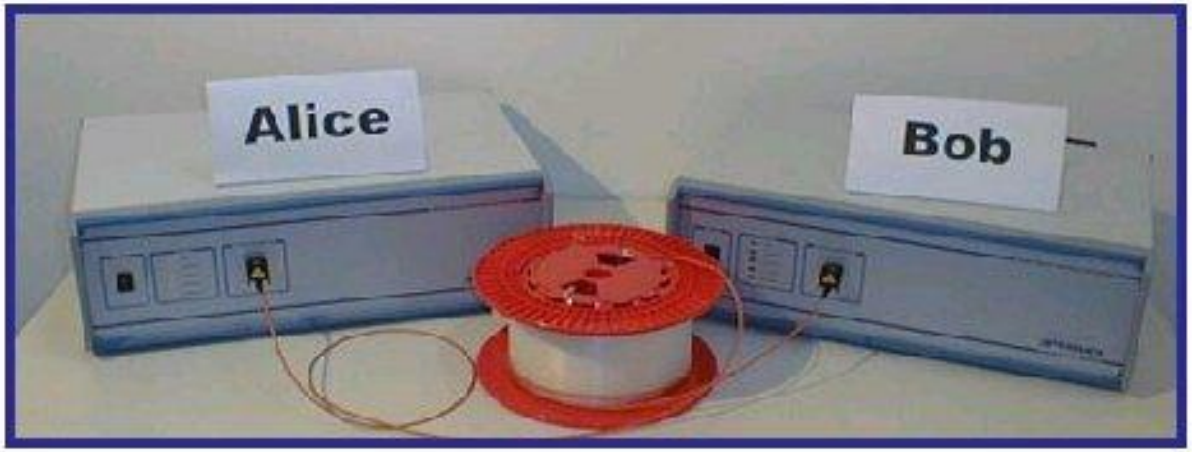
Već smo vidjeli da najmanja razlika između nizova *E* i *A* vodi gotovo sigurno na na različite hash vrijednosti: $H(E) \neq H(A)$. Ako se *E* razlikuje od *A* za *r* bitova, to znači da nam (po definiciji) treba *r* bitova informacije da bismo *E* mogli svesti (transformirati) na *A*. Takovih transformacija ima 2^*r* i vjerojatno je da bi svaki *E* (koji odgovara jednoj od tih transformacija) imao drugačiji $H(E)$.

Uzmimo da *H* preslikava u nizove duljine *r.* Dakle je $H(A)$ jedan određeni niz duljine *r.* S druge strane, za slučajno odabrani *E* je $H(E)$ jedan uniformno distribuirani slučajni broj duljine *r*.

Drugim riječima $H(E)$ nema nikakve veze s $H(A)$. Upravo to (malo preciznije) govori izrečeni Teorem.

Prvi komercijalni uređaj za kvantnu kriptografiju

Sredinom 2002. godine Švicarska spin-off firma idQuantique prikazala je prvi komercijalni uređaj za kvantnu kriptografiju s dometom od 67 kilometara. Trenutni rekord je 400 km.



Main features

- First commercial quantum key distribution system
- Key distribution distance: up to 60 km
- Key distribution rate: up to 1000 bits/s
- Compact and reliable

No-cloning QKD protokoli

- **BB84** (Bennett, Brassard 1984) - originalno koristi 4 neortog. stanja
- **EPR** (Ekert 1991) - koristi EPR parove u 3 baze
- **B92** (Bennet 1992) - koristi samo 2 neortogonalna kvantna stanja
- **BBM92** (Bennet, Brassard, Mermin 1992) – kao EPR ali 2 baze

Pokazuje se da su ti protokoli **ekvivalentni** te da se svode na BB84 !

Postoje i brojne manje modifikacije aparature ili protokola čija je svrha povećanje otpornosti na pojedine napade.

Općenito, kaže se da je QKD protokol **siguran** ako Alice i Bob mogu odabrati parametre $s > 0$ i $l > 0$ tako da za bilo koju strategiju prisluškivanja protokol uspjeva s vjerojatnošću barem $1-O(2^{-S})$ i pri tom je prisluškivačeva zajednička informacija s konačnim ključem < 2^{-l}.

EPR paradoks

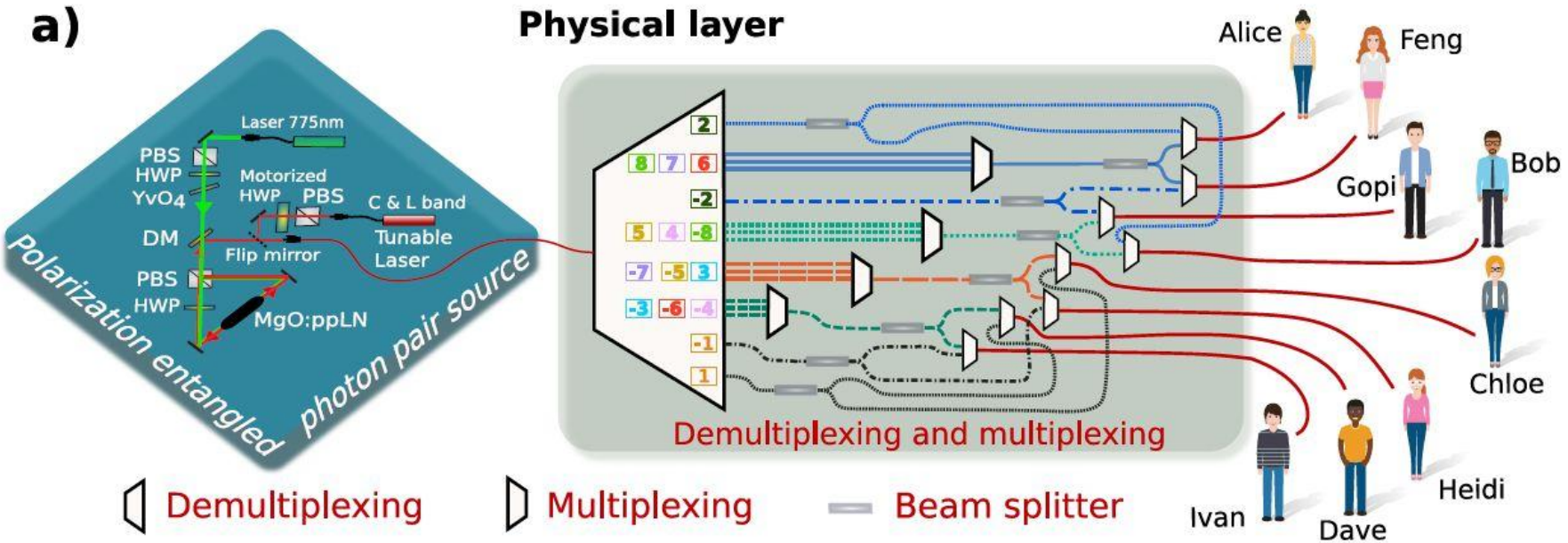
Einstein nije vjerovao u kvantnu fiziku pa je pokušavao raznim paradoksima dokazati njenu kontradiktornost ili nepotpunost. Pokazalo se, međutim, da je svaki puta bio u krivu te da su njegovi paradoksi doveli do novih uvida i čudesnih dokaza valjanosti kvantne fizike. Najpoznatiji je tzv. EPR paradoks [4] koji ukazuje na ne-lokalnost kv. fizike.

Određenim postupkom moguće je proizvesti par “isprepletenih” (entangled) fotona. Ako se jednom od njih na put stavi polarizator, vjerojatnost prolaska je 0.5, a njegova polarizacija odgovara smjeru polarizatora (prolaz) ili je okomita. Istovremeno, na ma kojoj udaljenosti, drugi foton poprima ortogonalnu polarizaciju. Paradoks je u tome što se drugi foton “orijentira” momentalno.

Činjenica da se ne može utjecati na orijentaciju prvog fotona može se iskoristiti za kvantnu kriptografiju.

Višestrani QKD - kvantni internet

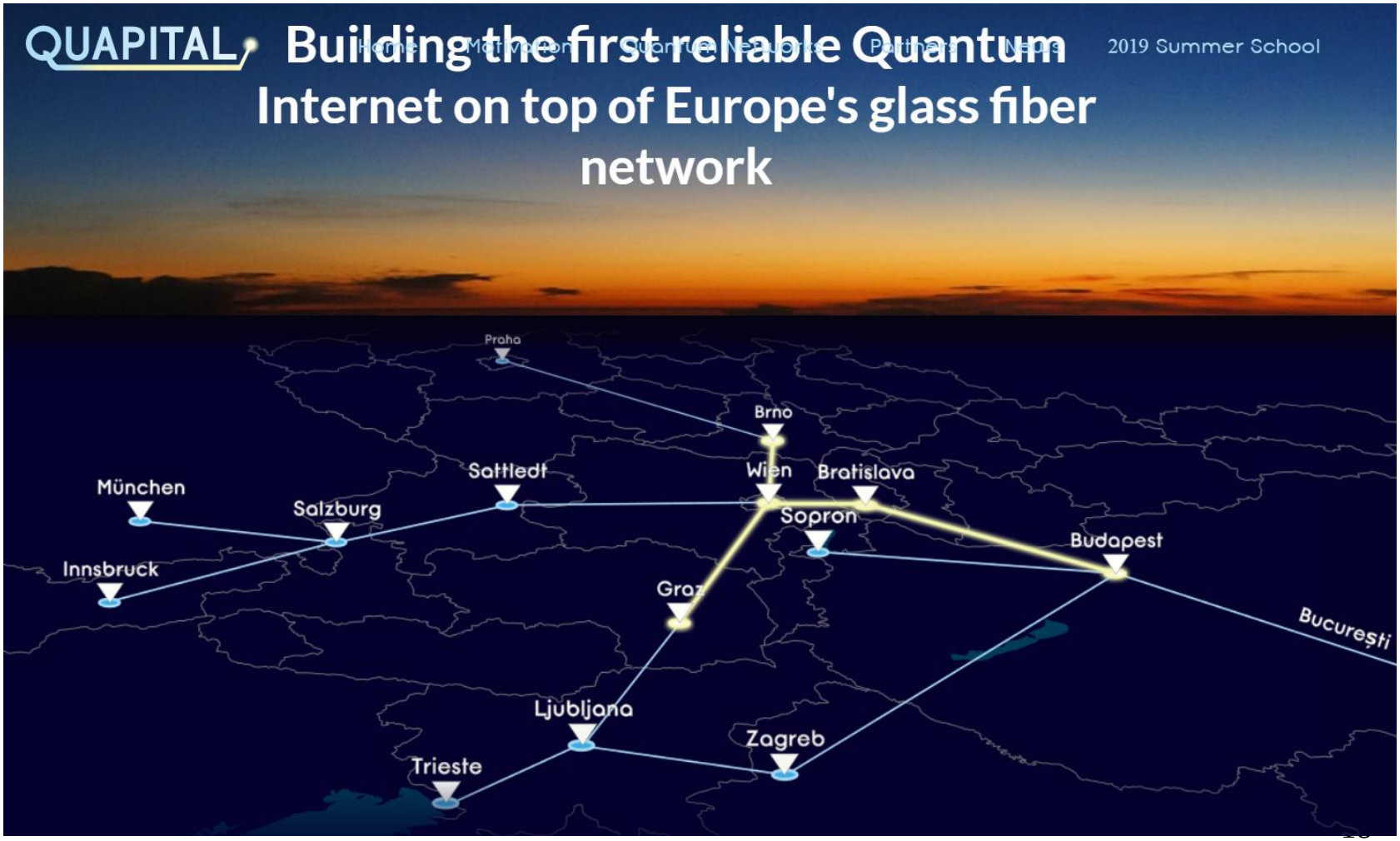
U suradnji University of Bristol (UK), IQOQI (Beč) i IRB CEMS-Fotonika sagradili smo najveću mreži kvantne kriptografije do sada, s 8 komunikacijskih čvorova.



Projekt: Q-NET.

Quapital – EU-wide kvantni internet

Projekt QUAPITAL http://quapital.eu



Bibliografija

[1] C. Shannon, Communication Theory of Secrecy Systems, Interna publikacija Bell Systems, 1946 (zabrana tajnosti skinuta 1949)

[2] D. Knuth, The art of computer programming, Vol 2. Seminumerical algorithms, Addison-Wesley 1998

[3] U. Maurer, Secret Key Agreement by Public Discussion, IEEE Trans. Inform. Theor. **39**(1993)733-742

[4] A. Einstein, B. Podolski, N. Rosen, Phys. Rev. **41**(1935)777

[5] C.H.Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 1984, pp 175-179

[6] A. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**(1991)661-663

[7] I. Csiszar, J. Koerner, Broadcast channels with confidential messages, IEEE Trans. Inform. Theor. **24**(1978)339-348

[8] W.K. Wooters, W.H. Zurek, A Single Quantum Cannot be Cloned, Nature, **299**(1982)802-803

[9] J.L Carter, M.N.Wegman, Universal Classes of Hash Functions, J. Compututer and System Sciences **18**(1979)143-154

[10] C.H.Bennett, F.Besette, G.Brassard, L.Savail, J.Smolin, Experimental Quantum Cryptography, Proc. Eurocrypt 1980, pp. 253-265

[11] C.H.Bennet, G.Brassard, J-M.Robert, Privacy amplification by public discussion, SIAM J. on Computing **17**(1988)210-229

[12] http://www.quantum.univie.ac.at/research/crypto/index.html