

KAREL LEMR

KVANTOVÁ KRYPTOGRAFIE





Utajení je první zásadou
v záležitostech státu.

kardinál Richelieu

Když zpráva není pro všechny ...

Když zpráva není pro všechny ...



Když zpráva není pro všechny ...



Když zpráva není pro všechny ...



Když zpráva není pro všechny ...



... řešením je

KRYPTOGRAFIE

... řešením je



KRYPTO GRAFIE

kryptós – skrytý

gráphein – psát

... řešením je

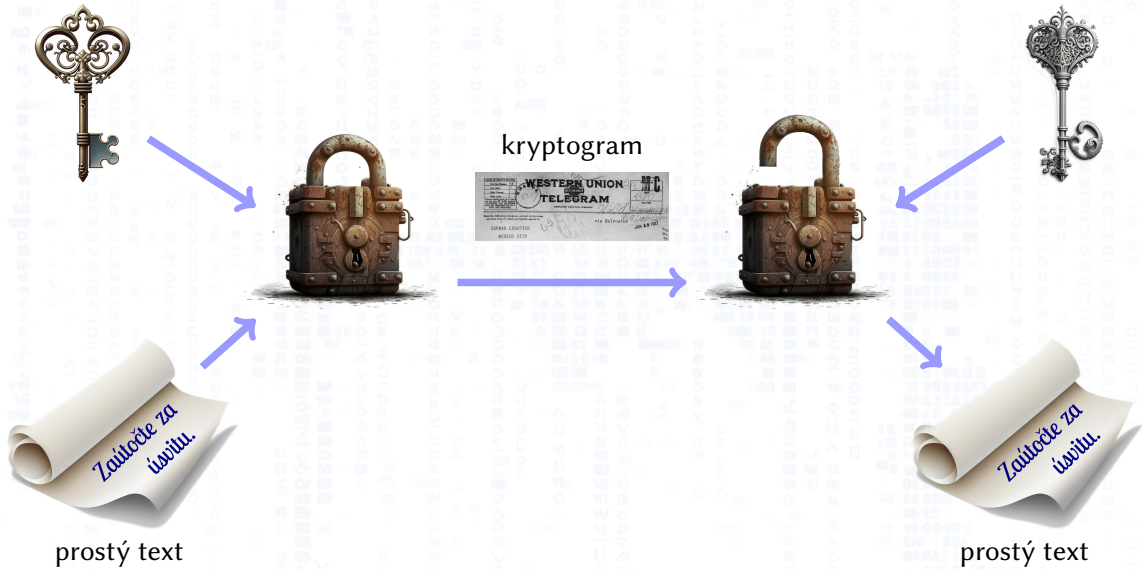


KRYPTO GRAFIE

kryptós – skrytý

gráphein – psát

- ▶ **kryptografie:** skrývá obsah zprávy (šifrováním)
- ▶ **steganografie:** skrývá existenci zprávy



starověk: Caesarova šifra



starověk: Caesarova šifra

prostý text: A B C D E ...

kryptogram: D E F G H ...



starověk: Caesarova šifra

↓

prostý text:	A	B	C	D	E	...
kryptogram:	D	E	F	G	H	...

- ▶ jednoduchá substituční šifra
- ▶ každý znak posuneme o určitý počet míst v abecedě
- ▶ příklad:
Caesar-D = posun o 3 ($A \rightarrow D$)
Caesar-F = posun o 5 ($A \rightarrow F$)





Kde je problém?



Kde je problém?

- ▶ délka abecedy: 26 znaků
- ▶ počet možných posunutí: 25 (Caesar-B až Caesar-Z)
- ▶ 25 klíčů lze prolomit hrubou silou!

řešení: šifra smíšené abecedy

prostý text:	A	B	C	D	E	...
kryptogram:	H	E	S	L	O	...



řešení: šifra smíšené abecedy

prostý text:	A	B	C	D	E	...
kryptogram:	H	E	S	L	O	...

- ▶ stále **monoalfabetická substituční šifra**
- ▶ možných klíčů = počet permutací = $26! = 4 \times 10^{26}$
- ▶ nelze zaútočit hrubou silou



Stále máme problém...



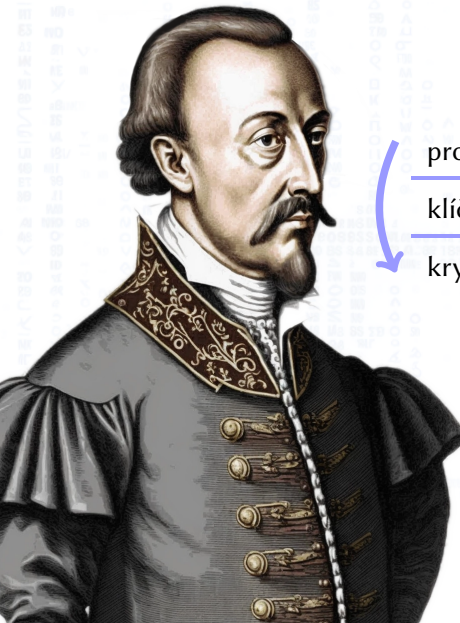


Stále máme problém ...

- ▶ **frekvenční analýza:**
zastoupení jednotlivých znaků v daném jazyce
(čeština: 7,7% e, 6,2% a, ...)
- ▶ porovnáme frekvenci znaků v kryptogramu
s frekvencí v daném jazyce
- ▶ prolomil: al-Kindī (9. století)



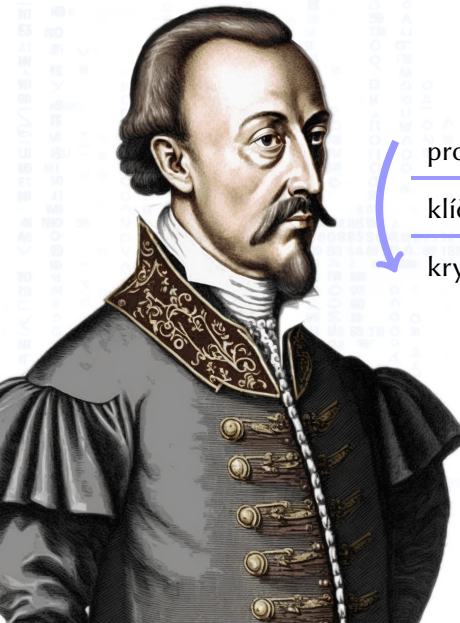
16. století: **Vigenèrova šifra**



16. století: Vigenèrova šifra

prostý text:	T	O	T	O	J	E	T	A	J	N	E
klíč:	K	L	I	C	K	L	I	C	K	L	I
kryptogram:	D	Z	B	Q	T	P	B	C	T	Y	M

(Caesarova-■ šifra, kde ■ je příslušný znak klíče)



16. století: Vigenèrova šifra

prostý text:	T	O	T	O	J	E	T	A	J	N	E
klíč:	K	L	I	C	K	L	I	C	K	L	I
kryptogram:	D	Z	B	Q	T	P	B	C	T	Y	M

(Caesarova-■ šifra, kde ■ je příslušný znak klíče)

- ▶ polyalfabetická substituční šifra
- ▶ stejný znak může být zakódován různě
→ nelze použít frekvenční analýzu
- ▶ skutečný objevitel: **Giovan Battista Bellaso**



... a problém trvá ...



... a problém trvá ...

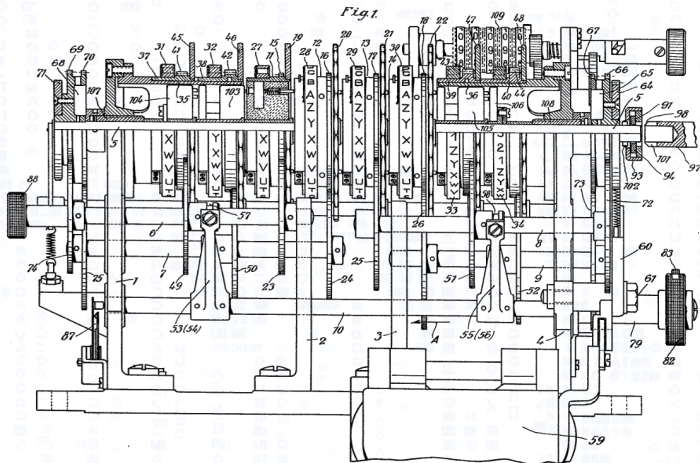
- ▶ délka zprávy $\gg$ délka klíče
- ▶ objeví se opakované sekvence znaků, **perioda opakování umožní určit délku klíče**
- ▶ známe-li délku klíče, **nasadíme frekvenční analýzu** zvláště pro jednotlivé znaky klíče
- ▶ prolomil: Friedrich Wilhelm Kasiski (19. století)

20. století:



Zu der Patentschrift 524754
Kl. 42n Gr. 14

Zu der Patentschrift 524754
Kl. 42n Gr. 14



20. století:



- ▶ po každém zašifrovaném znaku se stroj posune do nového nastavení
- ▶ výsledek: **polyalfabetická substituční šifra s velice dlouhým klíčem** (délka 26^3)
- ▶ množství počátečních nastavení zajišťuje **vyšoký počet možných klíčů**





Enigma neodolala matematice!



Enigma neodolala matematice!

- ▶ klíč **není náhodný**
je dán vnitřním fungováním Enigmy
- ▶ 1932: Marian Rejewski, Jerzy Różycki, Henryk Zygaliski prolamují Enigmu
- ▶ prolomena díky: nové matematice, špionáži a chybám operátorů
- ▶ během II. světové války v Bletchley Park Angličané úspěšně dešifrují

od 20. století: **Digitální kryptografie**



od 20. století: **Digitální kryptografie**

- ▶ využívá matematických výpočtů, které **mají výpočetně složitou inverzi**
- ▶ příklad: $11 \times 31 = ?$, $533 = ? \times ?$
- ▶ řešení:
- ▶ princip moderní kryptografie (RSA, AES, ...)



od 20. století: **Digitální kryptografie**

- ▶ využívá matematických výpočtů, které **mají výpočetně složitou inverzi**
- ▶ příklad: $11 \times 31 = ?$, $533 = ? \times ?$
- ▶ řešení: $11 \times 31 = 341$, $533 = 13 \times 41$
- ▶ princip moderní kryptografie (RSA, AES, ...)



od 20. století: **Digitální kryptografie**

- ▶ využívá matematických výpočtů, které **mají výpočetně složitou inverzi**
 - ▶ příklad: $11 \times 31 = ?$, $533 = ? \times ?$
 - ▶ řešení: $11 \times 31 = 341$, $533 = 13 \times 41$
 - ▶ princip moderní kryptografie (RSA, AES, ...)
-
- ▶ bezpečnost založena na **víře v náročnost výpočtu**
 - ▶ opravdu nelze spočítat snadněji?



Existuje vůbec dokonalá šifra?



Existuje vůbec dokonalá šifra?

Vernamova šifra



Existuje vůbec dokonalá šifra?

Vernamova šifra

- ▶ klíč o stejné délce jako zpráva
(řeší Vigenèrův problém)



Existuje vůbec dokonalá šifra?

Vernamova šifra

- ▶ **klíč o stejné délce jako zpráva**
(řeší Vigenèrův problém)
- ▶ **klíč je zcela náhodný**
(řeší problém Enigmy a digitální kryptografie)



Existuje vůbec dokonalá šifra?

Vernamova šifra

- ▶ **klíč o stejné délce jako zpráva**
(řeší Vigenèrův problém)
- ▶ **klíč je zcela náhodný**
(řeší problém Enigmy a digitální kryptografie)
- ▶ **klíč se použije pouze jedenkrát**
(aby platil první bod)



Existuje vůbec dokonalá šifra?

Vernamova šifra

- ▶ **klíč o stejné délce jako zpráva**
(řeší Vigenèrův problém)
- ▶ **klíč je zcela náhodný**
(řeší problém Enigmy a digitální kryptografie)
- ▶ **klíč se použije pouze jedenkrát**
(aby platil první bod)
- ▶ Jak zajistit **distribuci dlouhého a jednorázového klíče?**





► Jak zajistit **distribuci dlouhého a jednorázového klíče?**



► Jak zajistit **distribuci dlouhého a jednorázového klíče?**



► Jak zajistit **distribuci dlouhého a jednorázového klíče?**

Zákony kvantové fyziky: Měření

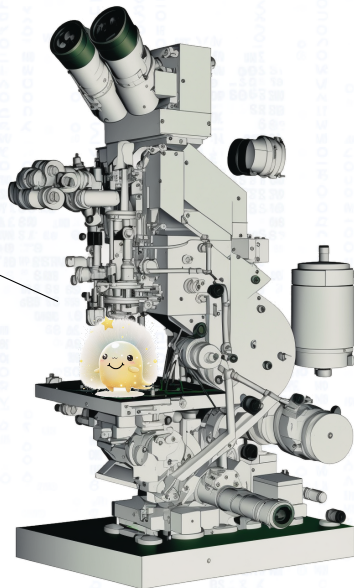
Zákony kvantové fyziky: Měření



foton:
příklad kvantového objektu

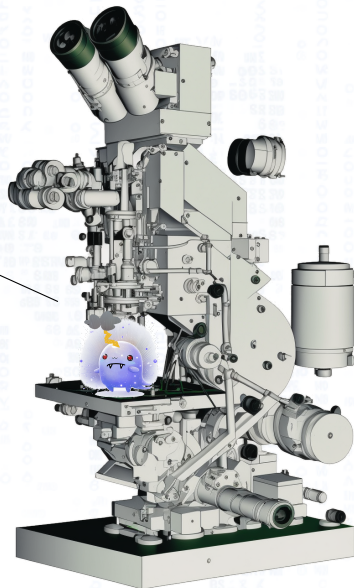
Zákony kvantové fyziky: **Měření**

měření kvantového stavu:
měříme vlastnosti fotonu



Zákony kvantové fyziky: **Měření**

měření podá informaci o
kvantovém stavu, ale
ovlivní měřený stav



Zákony kvantové fyziky: **Nemožnost klonovat**

Zákony kvantové fyziky: Nemožnost klonovat

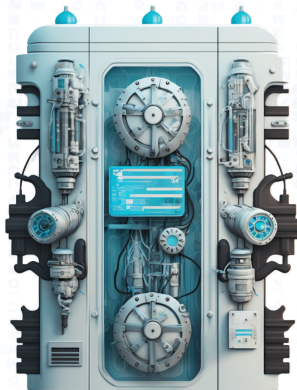


foton v neznámém
kvantovém stavu

Zákony kvantové fyziky: **Nemožnost klonovat**



foton v neznámém
kvantovém stavu



dokonalý kvantový kloner

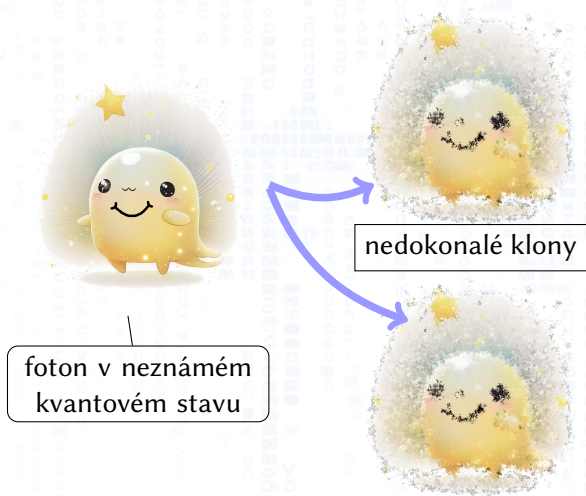


Zákony kvantové fyziky: Nemožnost klonovat

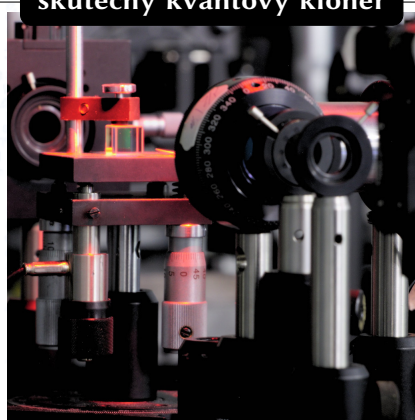
fotón v neznámém
kvantovém stavu

dokonalý kvantový kloner

Zákony kvantové fyziky: **Nedokonalé klonování**



skutečný kvantový kloner

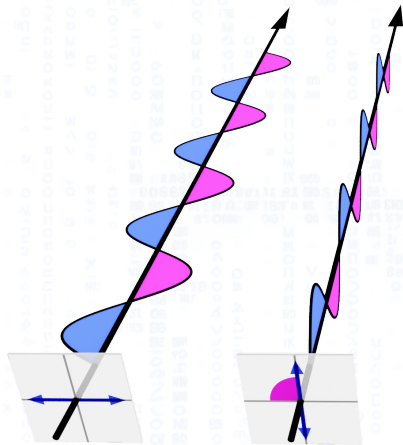


kódujeme do světla: **Polarizace**

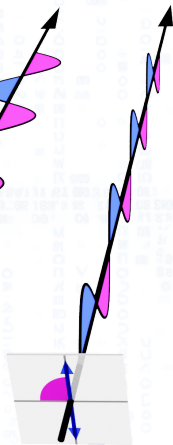
Jak poslat
informaci pomocí
jednotlivých fotonů?



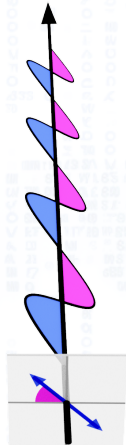
kódujeme do světla: Polarizace



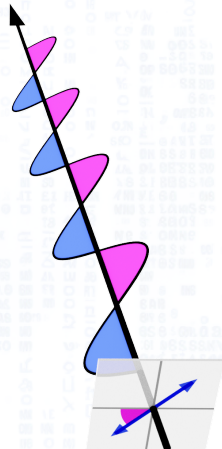
horizontální (0°)



vertikální (90°)



diagonální (45°)



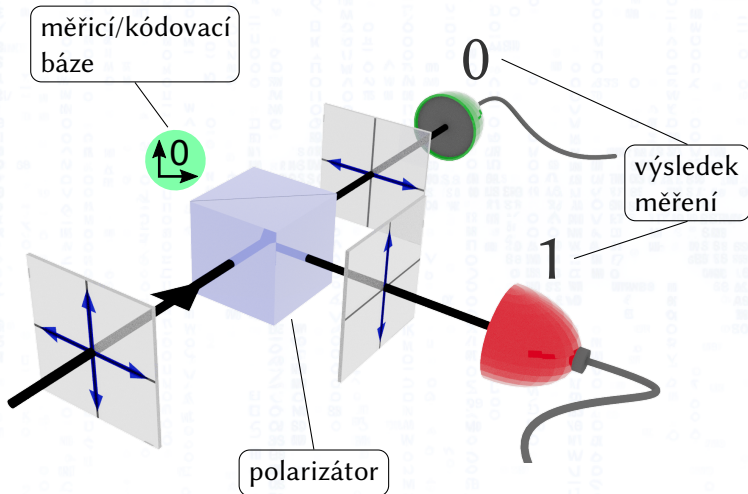
antidiagonální (-45°)

kódujeme do světla: Polarizace

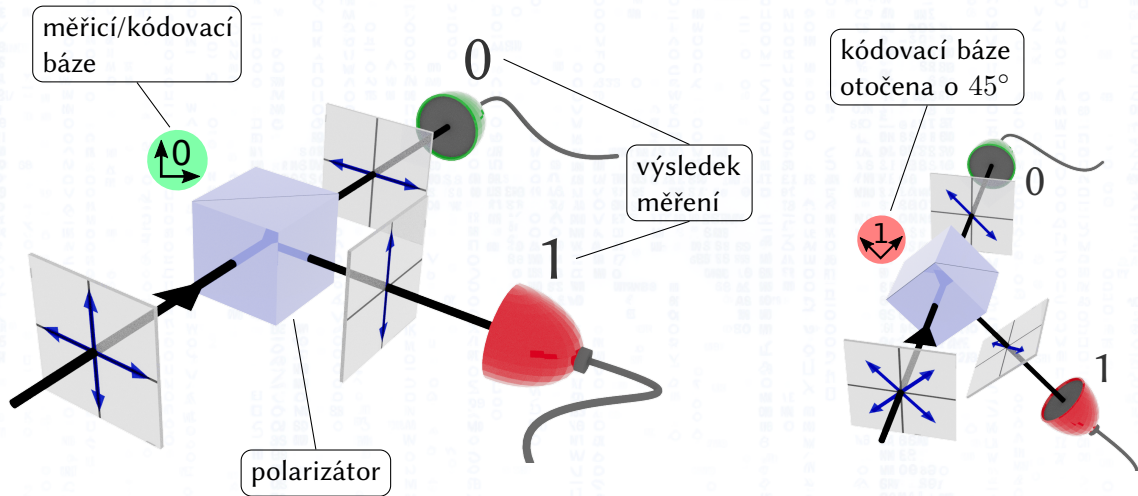


Jak změřit
polarizaci fotonů?

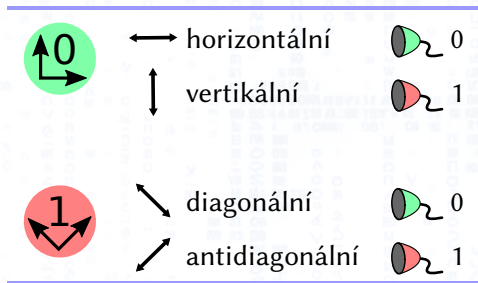
kódujeme do světla: Polarizace



kódujeme do světla: Polarizace

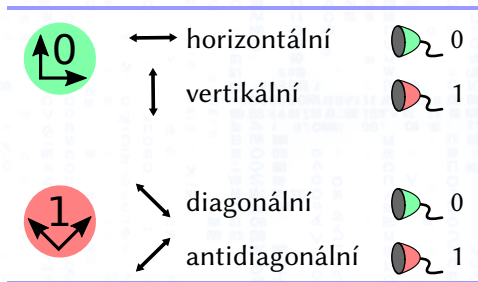


kódujeme do světla: Polarizace

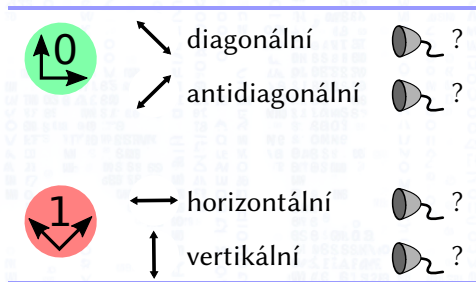


- ▶ když kódujeme **ve stejné bázi**,
jako měříme, je **výsledek jistý**

kódujeme do světla: Polarizace



- ▶ když kódujeme **ve stejné bázi**, jako měříme, je **výsledek jistý**



- ▶ když kódujeme **v nesprávné bázi**, je **výsledek náhodný**
- ▶ v tomto případě přesně 50:50

kvantová distribuce klíče: **protokol BB84**

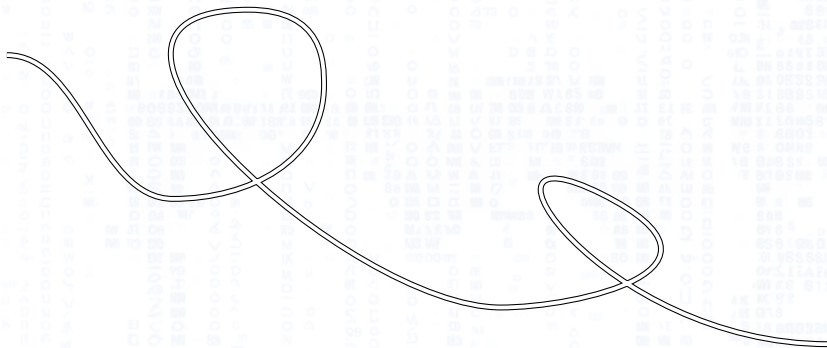
Jak distribuovat klíč
pomocí jednotlivých fotonů?



kvantová distribuce klíče: **protokol BB84**



ALICE



BOB



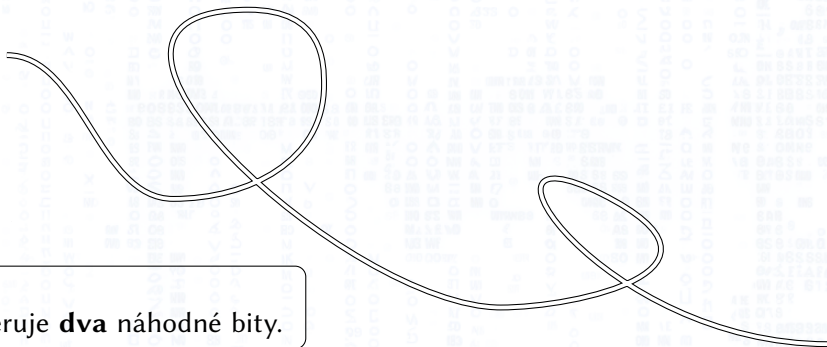
kvantová distribuce klíče: **protokol BB84**



ALICE

krok 1:

Alice vygeneruje **dva** náhodné bity.



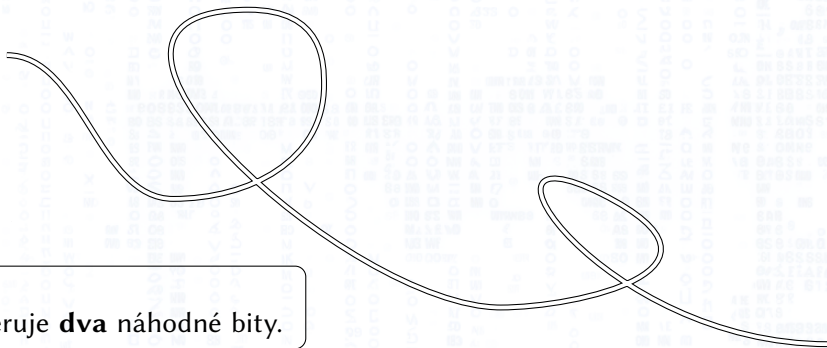
BOB



kvantová distribuce klíče: **protokol BB84**



ALICE



krok 1:

Alice vygeneruje **dva** náhodné bity.

krok 2:

První bit použije jako kódovací bázi, druhý jako hodnotu klíče.

Pošle Bobovi foton: 00 = $\leftrightarrow$, 01 = $\updownarrow$, 10 = $\swarrow \searrow$, 11 = $\nearrow \nwarrow$.

BOB



kvantová distribuce klíče: **protokol BB84**



ALICE

krok 1:

Alice vygeneruje **dva** náhodné bity.

krok 2:

První bit použije jako kódovací bázi, druhý jako hodnotu klíče.

Pošle Bobovi foton: 00 = $\longleftrightarrow$, 01 = $\updownarrow$, 10 = $\diagup \diagdown$, 11 = $\diagdown \diagup$.

krok 3:

Bob vygeneruje
jeden náhodný bit.

BOB



kvantová distribuce klíče: **protokol BB84**



ALICE

krok 1:

Alice vygeneruje **dva** náhodné bity.

krok 2:

První bit použije jako kódovací bázi, druhý jako hodnotu klíče. Pošle Bobovi foton: 00 = $\longleftrightarrow$, 01 = $\updownarrow$, 10 = $\diagup \diagdown$, 11 = $\diagdown \diagup$.

krok 3:

Bob vygeneruje **jeden** náhodný bit.

krok 4:

Bob provede měření v bázi podle jeho bitu. Pokud se jeho báze shoduje s bazí Alice, Bob získá hodnotu bitu klíče.

BOB



kvantová distribuce klíče: **protokol BB84**



ALICE

opakujeme kroky 1–4

krok 1:

Alice vygeneruje **dva** náhodné bity.

krok 2:

První bit použije jako kódovací bázi, druhý jako hodnotu klíče.
Pošle Bobovi foton: 00 = $\longleftrightarrow$, 01 = $\uparrow$, 10 = $\searrow$, 11 = $\swarrow$.

krok 3:

Bob vygeneruje **jeden** náhodný bit.

krok 4:

Bob provede měření v bázi podle jeho bitu. Pokud se jeho báze shoduje s bazí Alice, Bob získá hodnotu bitu klíče.

BOB



kvantová distribuce klíče: **protokol BB84**



ALICE

Aliciny bity

Odeslaný foton

Bobova báze

Bobovo měření

BOB



kvantová distribuce klíče: protokol BB84



ALICE

Aliciny bity	10	00	11	00	01	00	10	10	11	11
Odeslaný foton										
Bobova báze										
Bobovo měření										

BOB



kvantová distribuce klíče: **protokol BB84**



ALICE

	1. bit – báze		2. bit – klíč							
Aliciny bity	10	00	11	00	01	00	10	10	11	11
Odeslaný foton										
Bobova báze										
Bobovo měření										

BOB



kvantová distribuce klíče: protokol BB84



ALICE

Aliciny bity	10	00	11	00	01	00	10	10	11	11
Odeslaný foton										
Bobova báze										
Bobovo měření										

BOB



kvantová distribuce klíče: protokol BB84



ALICE

Aliciny bity	10	00	11	00	01	00	10	10	11	11
Odeslaný foton										
Bobova báze										
Bobovo měření										

BOB



kvantová distribuce klíče: protokol BB84



ALICE

Aliciny bity	10	00	11	00	01	00	10	10	11	11
Odeslaný foton										
Bobova báze										
Bobovo měření	1	0	1	0	1	0	0	1	0	1

BOB



kvantová distribuce klíče: **protokol BB84**

Alice a Bob si **až nyní** sdělí měřicí báze, vyloučí neshodné případy



ALICE

Aliciny bity	10	00	11	00	01	00	10	10	11	11
Odeslaný foton										
Bobova báze										
Bobovo měření	1	0	1	0	1	0	0	1	0	1

BOB



kvantová distribuce klíče: **protokol BB84**



ALICE

Alice a Bob si **až nyní** sdělí měřicí báze, vyloučí neshodné případy

Aliciny bity	10	00	11	00	01	00	10	10	11	11
Odeslaný foton										
Bobova báze										
Bobovo měření	1	0	1	0	1	0	0	1	0	1

zbylé případy tvoří klíč **01011** sdílený Alicí a Bobem

BOB



kvantová distribuce klíče: **protokol BB84**



ALICE

EVA



BOB



► Co když je linka odposlouchávaná?

Jaké má Eva možnosti odposlechu?



Jaké má Eva možnosti odposlechu?

- ▶ Eva měří přenášené fotony
→ měření změní stav
- ▶ Eva klonuje fotony
→ klonování zašumí fotony



Jaké má Eva možnosti odposlechu?

- ▶ Eva měří přenášené fotony
→ měření změní stav
- ▶ Eva klonuje fotony
→ klonování zašumí fotony
- ▶ výsledek: Eva svou činností
způsobí chyby v přenosu
- ▶ Alice s Bobem obětují
(sdělí si) část klíče
a ověřují, zda je přenesen
bezchybně



Chyby v přenosu klíče Evu odhalí!

**ODPOSLECH
ODHALEN**



Chyby v přenosu klíče Evu odhalí!

**ODPOSLECH
ODHALEN**

- ▶ Alice s Bobem přenesený klíč zahodí a nepoužijí
- ▶ zatím nešifrovali zprávu, odposlechnutý klíč není důvěrný

od nápadu po praxi: **vybrané milníky protokolu BB84**



od nápadu po praxi: vybrané milníky protokolu BB84



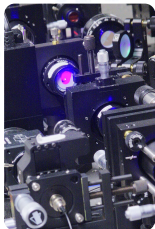
1984:
C. Bennett a
G. Brassard
navrhují protokol
pro kvantovou
distribuci klíče

od nápadu po praxi: vybrané milníky protokolu BB84



1989:
první
experimentální
implementace
BB84

1984:
C. Bennett a
G. Brassard
navrhují protokol
pro kvantovou
distribuci klíče



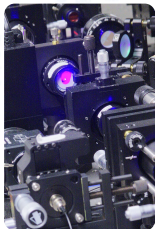
od nápadu po praxi: vybrané milníky protokolu BB84



1989:
první
experimentální
implementace
BB84



1984:
C. Bennett a
G. Brassard
navrhují protokol
pro kvantovou
distribuci klíče



2004:
první praktické
využití:
bankovní
komunikace
(Vídeň)

od nápadu po praxi: vybrané milníky protokolu BB84

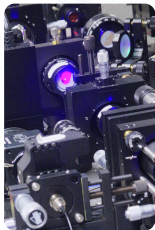


1989:
první
experimentální
implementace
BB84



2007:
přenos klíče
vzduchem
na 144 km
(Kanárské ostrovy)

1984:
C. Bennett a
G. Brassard
navrhují protokol
pro kvantovou
distribuci klíče



2004:
první praktické
využití:
bankovní
komunikace
(Vídeň)



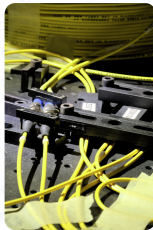
od nápadu po praxi: vybrané milníky protokolu BB84



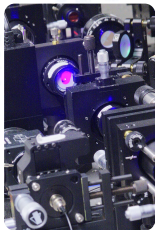
1989:
první
experimentální
implementace
BB84



2007:
přenos klíče
vzduchem
na 144 km
(Kanárské ostrovy)



1984:
C. Bennett a
G. Brassard
navrhují protokol
pro kvantovou
distribuci klíče



2004:
první praktické
využití:
bankovní
komunikace
(Vídeň)



2016:
rekord přenosu
optickým vláknem
na 404 km
(Čína)

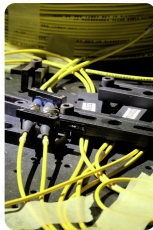
od nápadu po praxi: vybrané milníky protokolu BB84



1989:
první
experimentální
implementace
BB84



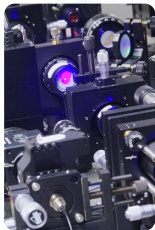
2007:
přenos klíče
vzduchem
na 144 km
(Kanárské ostrovy)



2017:
přenos klíče
pomocí satelitu
na oběžné dráze
(Čína&Rakousko)



1984:
C. Bennett a
G. Brassard
navrhují protokol
pro kvantovou
distribuci klíče

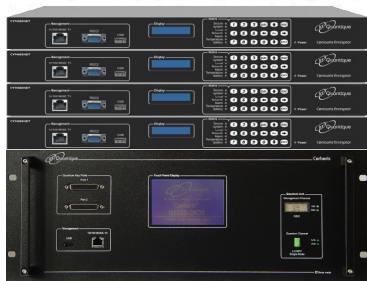


2004:
první praktické
využití:
bankovní
komunikace
(Vídeň)

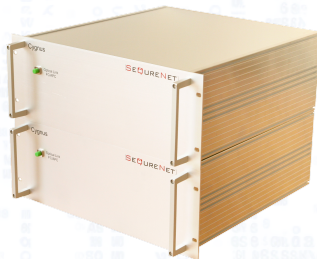


2016:
rekord přenosu
optickým vláknem
na 404 km
(Čína)

kvantová distribuce klíče pro všechny: **komerční řešení**



Cerberis (ID Quantique)



Cygnus (SeQureNet)

- typická cena za pár zařízení (pro Alici a Boba): € 250 000

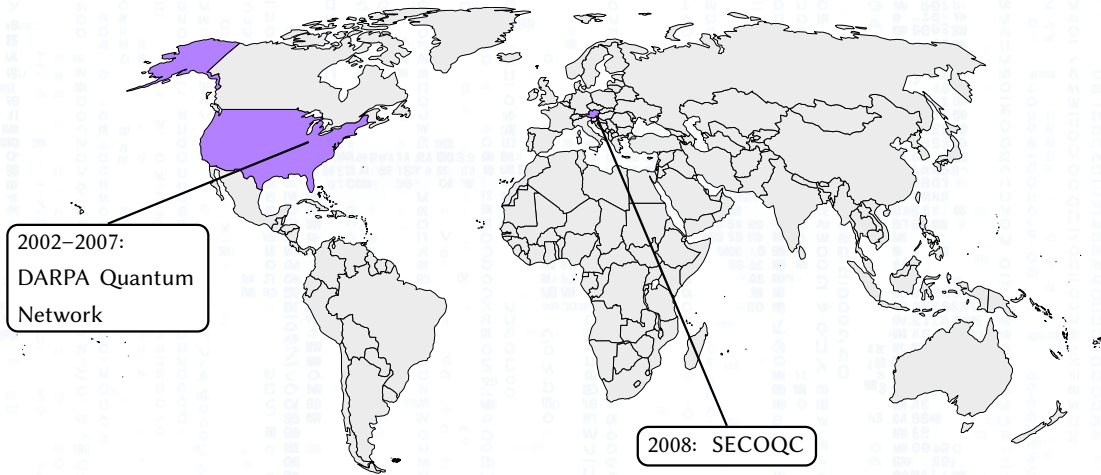
propojujeme uživatele: **kvantové kryptografické sítě**



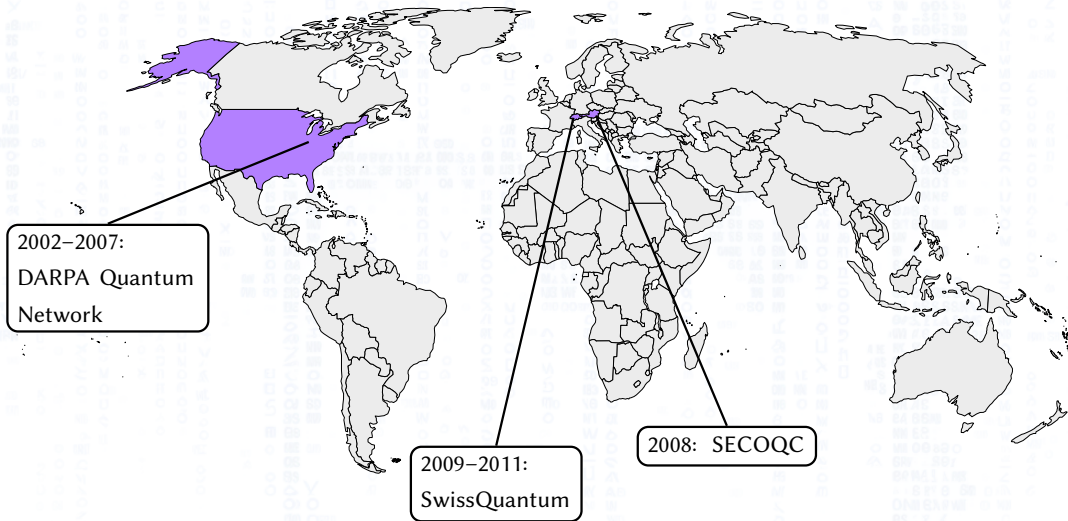
propojujeme uživatele: **kvantové kryptografické sítě**



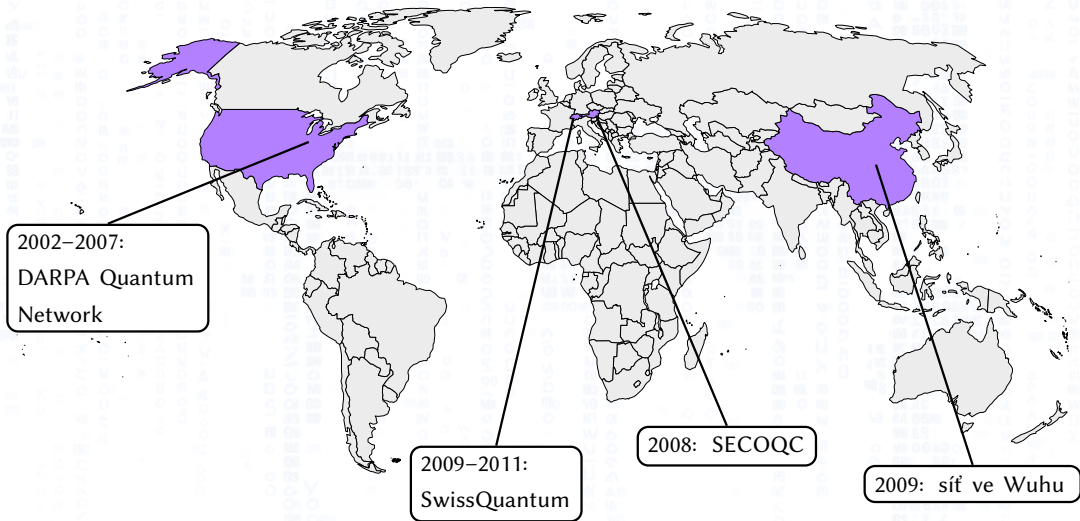
propojujeme uživatele: kvantové kryptografické sítě



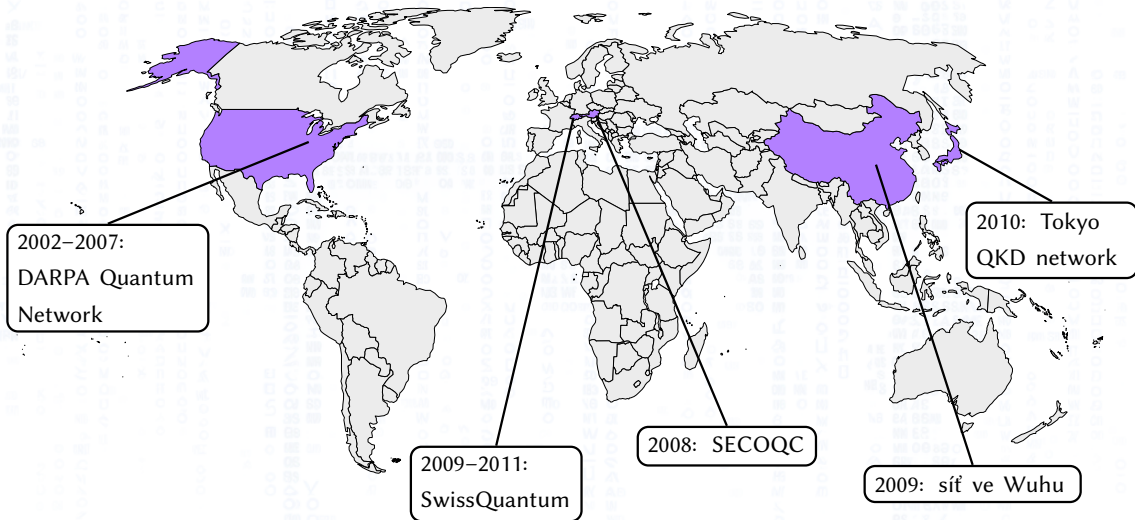
propojujeme uživatele: kvantové kryptografické sítě



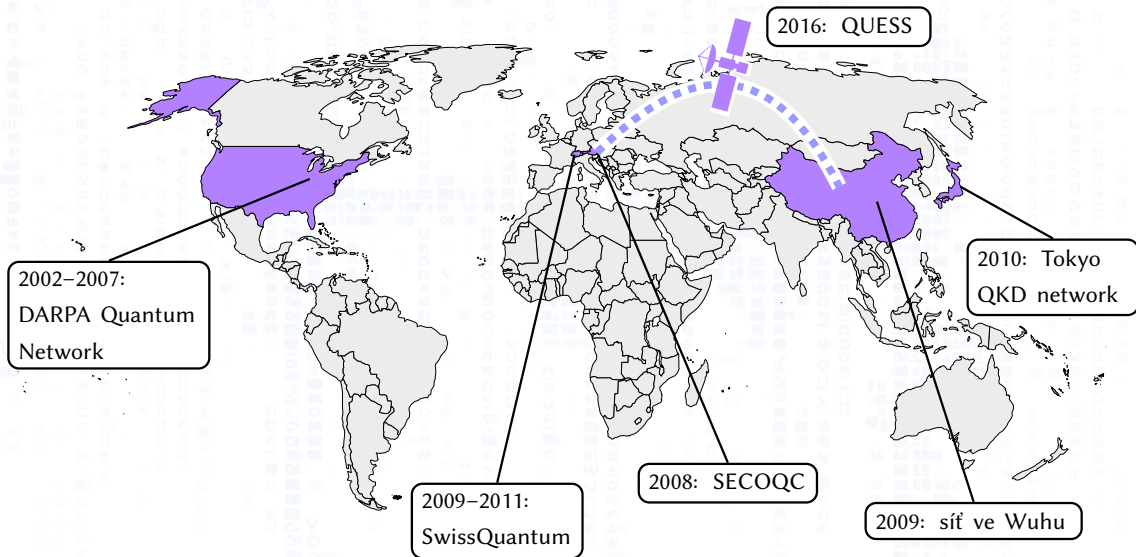
propojujeme uživatele: kvantové kryptografické sítě



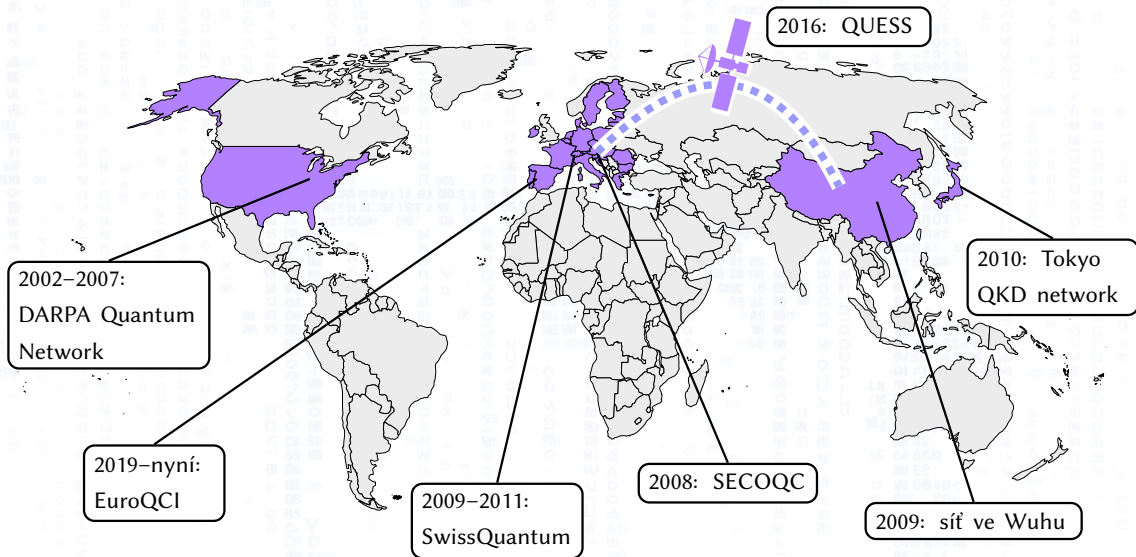
propojujeme uživatele: kvantové kryptografické sítě



propojujeme uživatele: kvantové kryptografické sítě



propojujeme uživatele: kvantové kryptografické sítě



Nic není dokonalé ani reálné technické řešení





Nic není dokonalé technologické nedokonalosti

- ▶ Alice pošle více fotonů naráz místo jednoho
→ Eva si jeden foton odkloní
- ▶ nastavení Aliciny báze lze pozorovat
→ Eva ví, jak Alice kóduje
- ▶ Bobův detektor lze manipulovat
→ Eva ovládá, co Bob změří

Nic není dokonalé technologické nedokonalosti



- ▶ technologické nedostatky
se snažíme odstraňovat
- ▶ vývoj technik proti jejich zneužití

Může být ještě hůř!



Může být ještě hůř!

zařízení nelze věřit



- ▶ Eva naprogramovala zařízení, aby podvádělo
- ▶ Alice záměrně vyšle více fotonů naráz
- ▶ Bobův detektor tajně přebírá signál od Evy

řešením je kvantová provázanost: **protokol E91**

řešením je kvantová provázanost: **protokol E91**

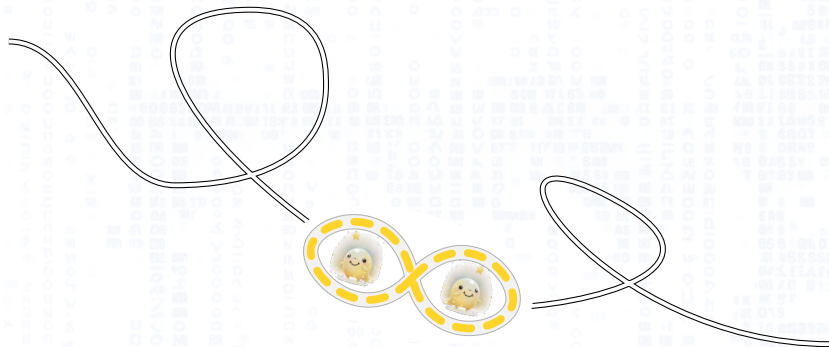


- ▶ lze připravit **kvantově provázané** páry fotonů
- ▶ změříme-li oba fotony z páru ve stejné bázi, **vždy obdržíme stejný výsledek:**
($\leftarrow, \leftarrow$) nebo ($\uparrow, \uparrow$) ($\searrow, \searrow$) nebo ($\nearrow, \nearrow$)
- ▶ nevíme předem jaký výsledek, ale víme, že u obou fotonů stejný
- ▶ **nelze dosáhnout klasicky bez kvantové provázanosti**

řešením je kvantová provázanost: **protokol E91**



ALICE



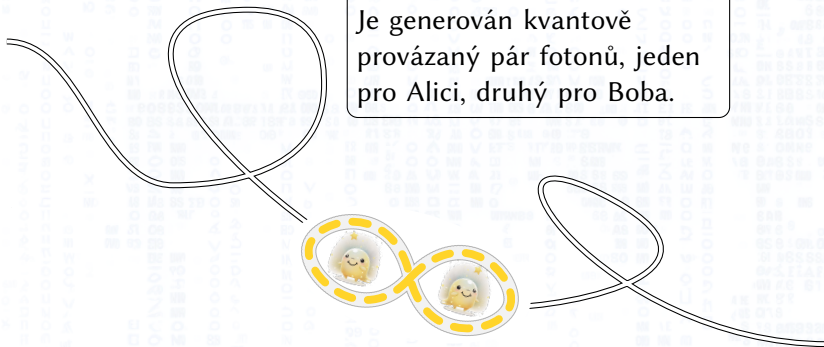
BOB



řešením je kvantová provázanost: **protokol E91**



ALICE



krok 1:

Je generován kvantově provázaný pár fotonů, jeden pro Alici, druhý pro Boba.

BOB



řešením je kvantová provázanost: **protokol E91**



ALICE

krok 2:

Alice a Bob nastaví nezávisle náhodné měřicí báze.

krok 1:

Je generován kvantově provázaný pár fotonů, jeden pro Alici, druhý pro Boba.



BOB



řešením je kvantová provázanost: protokol E91



ALICE

krok 2:

Alice a Bob nastaví nezávisle náhodné měřicí báze.

krok 3:

Alice a Bob provedou měření. Pokud zvolili stejné báze a výsledky se liší, pak **něco není v pořádku**. Klíč vyhodí.

krok 1:

Je generován kvantově provázaný pár fotonů, jeden pro Alici, druhý pro Boba.



BOB



Eva nemá šanci: **protokol E91**

Eva nemá šanci: **protokol E91**

► **Alice ani Bob nic neposílají**

→ Eva nemůže zneužít vysílání více fotonů naráz

Eva nemá šanci: **protokol E91**

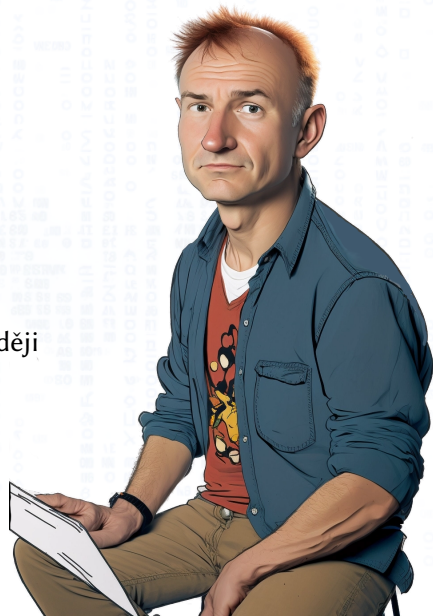
- ▶ **Alice ani Bob nic neposílají**
→ Eva nemůže zneužít vysílání více fotonů naráz
- ▶ **Alice a Bob nastaví měření až po vyslání páru fotonů**
→ Eva neví, co nastavili včas, aby jim signálem vnutila výsledek

Eva nemá šanci: **protokol E91**

- ▶ **Alice ani Bob nic neposílají**
→ Eva nemůže zneužít vysílání více fotonů naráz
- ▶ Alice a Bob nastaví **měření až po vyslání páru fotonů**
→ Eva neví, co nastavili včas, aby jim signálem vnutila výsledek
- ▶ Alice a Bob ověří, že **výsledky měření odpovídají kvantově provázanému stavu** (správná statistika stejné/rozdílné výsledky podle jejich voleb bazí)
→ Eva nemůže podvrhnout vlastní pár fotonů

Eva nemá šanci: **protokol E91**

- ▶ **kryptografie nezávislá na zařízení**
→ odstraňuje požadavek na důvěru k výrobci
- ▶ **Artur Ekert 1991**
→ význam jeho návrhu si fyzici uvědomili až později



klasická fyzika vrací úder:

postkvantová kryptografie



A composite image of Isaac Newton, a prominent figure in classical physics, depicted with his characteristic long, curly white hair and a dark, buttoned coat. He is holding a modern handgun in his right hand, pointing it towards the viewer. The background is dark and textured.

klasická fyzika vrací úder:

postkvantová kryptografie

- ▶ klasická digitální kryptografie
→ víra v náročnost výpočtu
- ▶ používá úlohy, pro které ZATÍM není známý účinný kvantový algoritmus
→ nelze zaútočit kvantovým počítačem (?)

Děkuji za pozornost.



@KvantovyKarel

Obrazové zdroje: ilustrační obrázky – Midjourney AI | Enigma patent – Scherbius a Korn | Enigma fotografie – A. Nassiri | Cerberis – ID Quantique | Cygnus – SeQureNet | mapa světa – simplemaps.com