Počítejme s kvantovou informací

Vojtěch Trávníček

Joint Laboratory of Optics, Palacky University
and Institute of Physics of Czech Academy of Sciences

vojtech.travnicek@upol.cz

Podpořeno z projektu OP VVV „Partnerská síť v oblasti výzkumu a vývoje zobrazovací a osvětlovací techniky a optoelektroniky pro optický a automobilový průmysl“, registrační číslo: CZ.02.1.01/0.0/0.0/17049/0008422.

6. 10. 2021

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

MULTIPHOTON QUANTUM LAB
@ RCPTM, PALACKÝ UNIVERSITY

Co to je kvantová informace

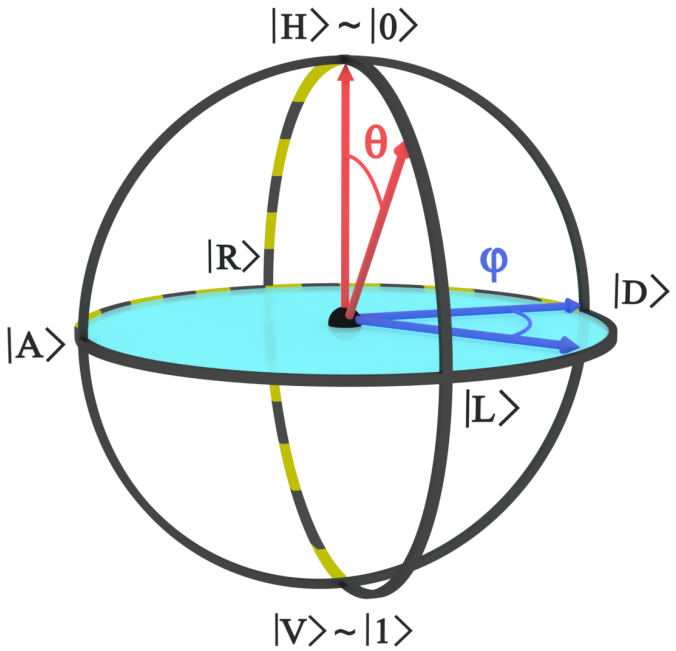
klasická informace

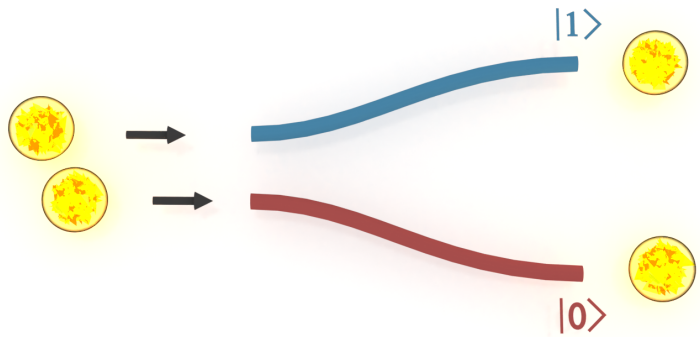
- Nejmenší jednotka je bit.
- Obvykle jeden bit nabývá hodnoty "1" nebo "0".
- Informace se zapisuje do elektrického napětí, proudu nebo do intenzity světla.
- Zpracování informace pomocí logických hradel.

kvantová informace

- Nejmenší jednotka je qubit.
- Qbit může být ve stavu $|1\rangle$ nebo $|0\rangle$ ale taká i libovolné superpozici těchto stavů.
- Informace se zapisuje do objektu podporující minimálně dvou-hladinový systém.
- Zpracování informace pomocí interakcí a měření.

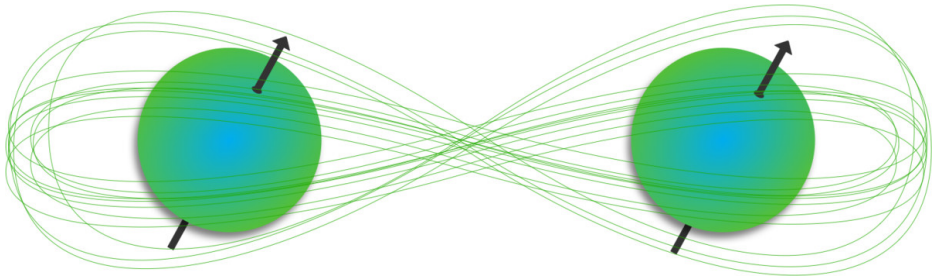
Reprezentace qubitu





$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1, \quad |\psi\rangle = \cos\frac{\theta}{2}|\mathrm{H}\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|\mathrm{V}\rangle$$

Kvantové provázání



- Čistě kvantový jev, kdy nelze stav nějakého většího systému rozdělit do stavů jednotlivých podsystémů.
- Výsledky měření na jednotlivých podsystémech jsou silně korelovány.
- Příkladem takového stavu je pro polarizační kódování tzv. Bellův stav $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\mathrm{HH}\rangle + |\mathrm{VV}\rangle)$
- Je to klíčový jev pro mnoho kvantových protokolů např. kvantovou teleportaci.

K čemu potřebujeme kvantové počítání

Zrychlení určitých algoritmů

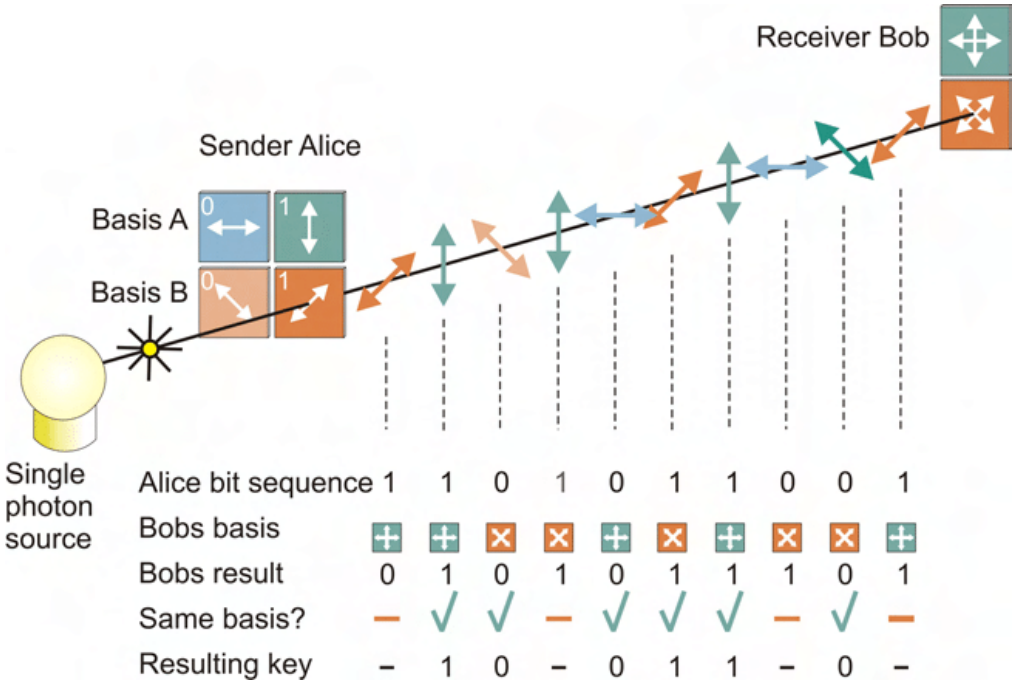
- V roce 1992 byl představen jeden z prvních algoritmů (Deutch-Jozsa algoritmus), kde kvantový přístup vykazoval výrazné zrychlení.
- V roce 1994 následoval P. Shor s jeho faktorizačním algoritmem.
  - Klasicky roste náročnost jako exp(N), kde N je délka čísla.
  - Kvantově však jen jako poly(N).
- A v roce 1996 představil L. Grover kvantový algoritmus pro vyhledání v neuspořádané databázi.
  - Klasicky roste s N, kvantově s $\sqrt{N}$.
- V poslední době je na vzestupu kvantové strojové učení.

K čemu potřebujeme kvantové počítání

Kvantová kryptografie

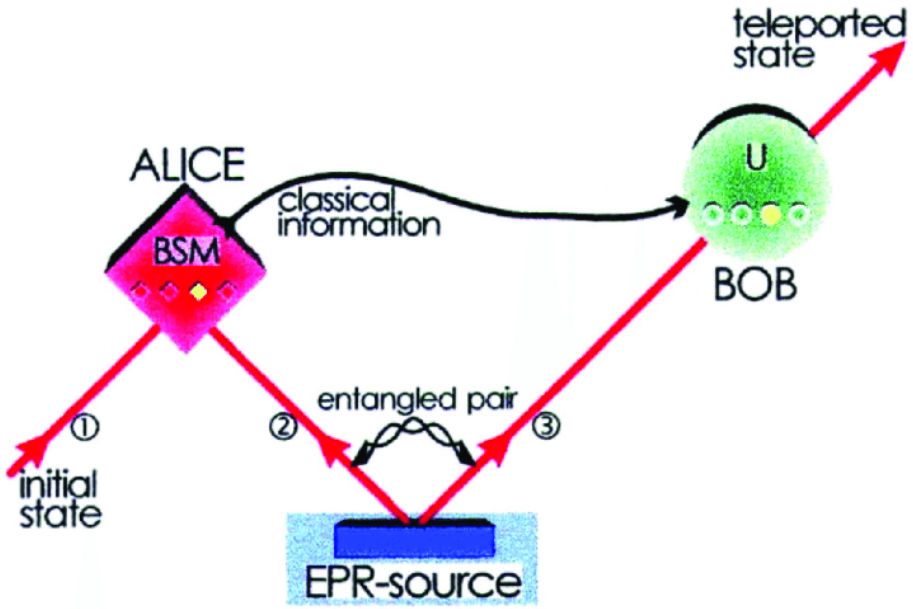
- Kvantové algoritmy díky své efektivitě představují hozbu (i když zatím jen teoreticky) pro klasickou kryptografii.
- Jak tomu čelit?
  - Prodloužit délku klíče.
  - Postkvantová kryptografie.
  - Kvantová kryptografie.
- Distribuce kvantového klíče.
  - Protokoly BB84 a E91.

BB84



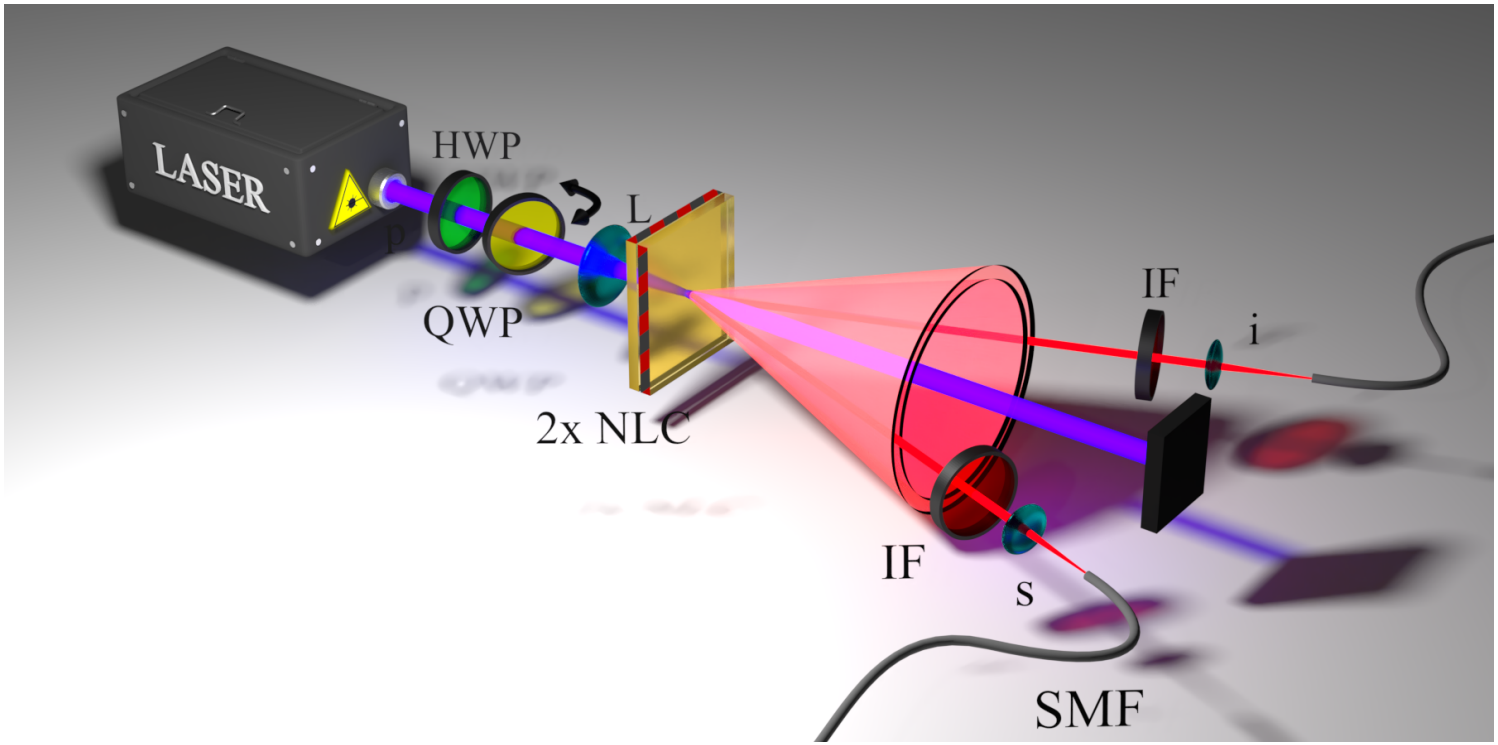
- Alice náhodně vygeneruje bit a poté podle náhodně zvolené báze připravý jeden ze čtyř možných polarizačních stavů.
- Bob tento stav změří opět v náhodné bázi a zaznamená výsledek.
- Po skončení přenosu Alice a Bob porovnají báze, které použili pro každý jednotlivý bit. Pokud se báze shodují je bit použit pro klíč.
- Odposlouchávání může být odhaleno tím, že se porovná určitá část klíče. Pokud část vykazuje příliš mnoho chyb klíč se zahodí.

Kvantová teleportace



- Jeden foton z provázaného páru interaguje na děliči s neznámým stavem, ketrý chceme teleportovat. Provede se tzv. projekce na Bellův stav.
- Díky provázanosti se stav druhého fotonu z páru změní a to na neznámý vstupní stav s pravděpodobností 25%.
- V ostatních případech je potřeba na Bobově fotonu provést transformaci, jež převede foton do vstupního stavu. Tato transformace je závyslá na výsledku měření u Alice.

Fotony pro kvantové zpracování informace



- Zdroj jednotlivých a provázaných fotonů.
- Pro interferenci je důležité aby byly fotony co nejméně rozlišitelné.
- Fotony se převážně generují pomocí procesu sponntání sestupné parametrické konverze.

Vybrané výsledky publikované skupinou kvantové informace

npj | Quantum Information

ARTICLE OPEN

Experimental quantum forgery of quantum optical money

Karol Bartkiewicz[1,2,3], Antonín Černoch[4], Grzegorz Chimczak[1], Karel Lemr[2], Adam Miranowicz[1,3] and Franco Nori[3,5]

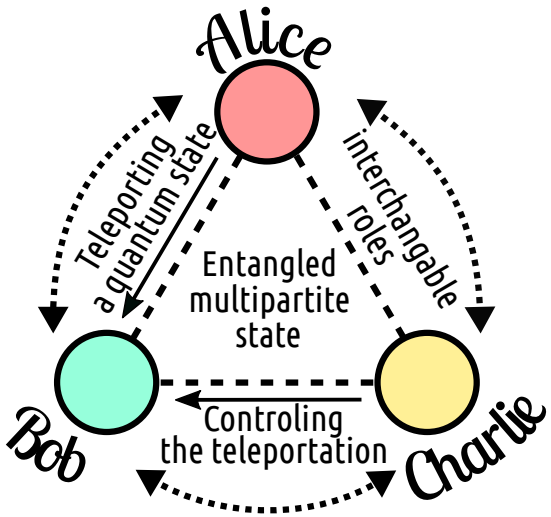
- V roce 1970 Weisen předložil návrh kvantových peněz.
- Kolegové ukazali, že je možné za použití kvantových stavů takovéto bankovky implementovat a také, že je lze padělat.
- V návaznosti navrhly postupy jak celý proces zabezpečit proti podobným útokům.

Vybrané výsledky publikované skupinou kvantové informace

PHYSICAL REVIEW LETTERS **122,** 170501 (2019)

Demonstration of Controlled Quantum Teleportation for Discrete Variables on Linear Optical Devices

Artur Barasiński,[1,2,*] Antonín Černoch,[3,†] and Karel Lemr[1,‡]



- Experimentální provedení kontrolované kvantové teleportace.
- První krok ke kvantové teleportační síti.

Vybrané výsledky publikované skupinou kvantové informace

PHYSICAL REVIEW LETTERS **123,** 260501 (2019)

Experimental Measurement of the Hilbert-Schmidt Distance between Two-Qubit States as a Means for Reducing the Complexity of Machine Learning

Vojtěch Trávníček,[1,*] Karol Bartkiewicz,[1,2,†] Antonín Černoch,[3,‡] and Karel Lemr[1,§]

- Výzkum se věnoval měření vzdáleností mezi kvantovými stavy.
- Zajímavé pro kvantové strojové učení. Hlavně pro klasifikační algoritmy.

Výhled do budoucna

- V dohledné době kvantové počítače nenahradí ty klasické.
- Budou se objevovat zařízení pro jednotlivé úlohy.
- Možný nástup kvantové komunikace a šifrování ve vetším měřítku. Je však potřeba lepších zdrojů fotonů.
- Velkým tématem je kvantové strojové učení.
- Rozšíření cloudových služeb jako je IBMQ.

Děkuji za pozornost