Kryptologia kwantowa

Konrad Wojciechowski
Informatyka, Internet Przedmiotów
kwiecień 2021

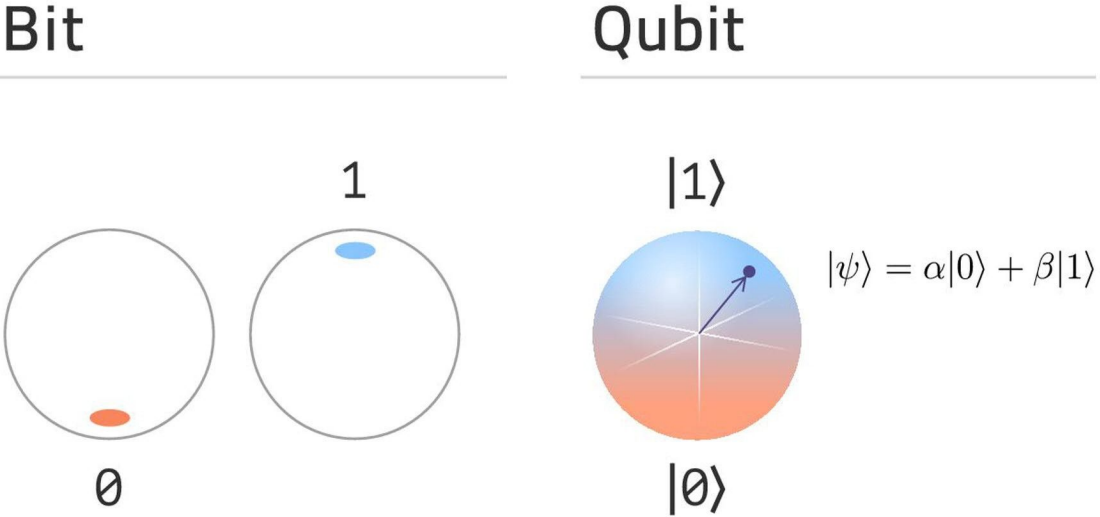
Plan prezentacji

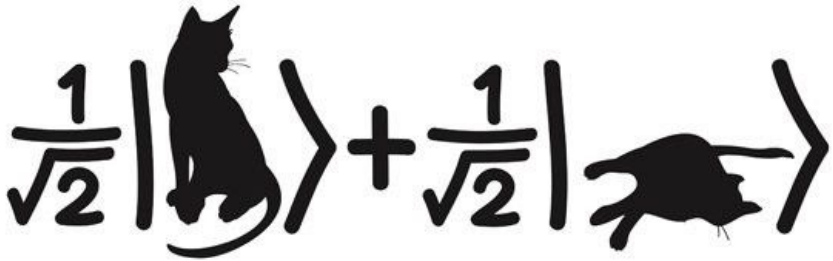
- Wstęp teoretyczny
- Kwantowa dystrybucja klucza
- Algorytm faktoryzacji Shora
- Kryptografia postkwantowa

Wstęp teoretyczny

Pojęcia

- Kubit, superpozycja

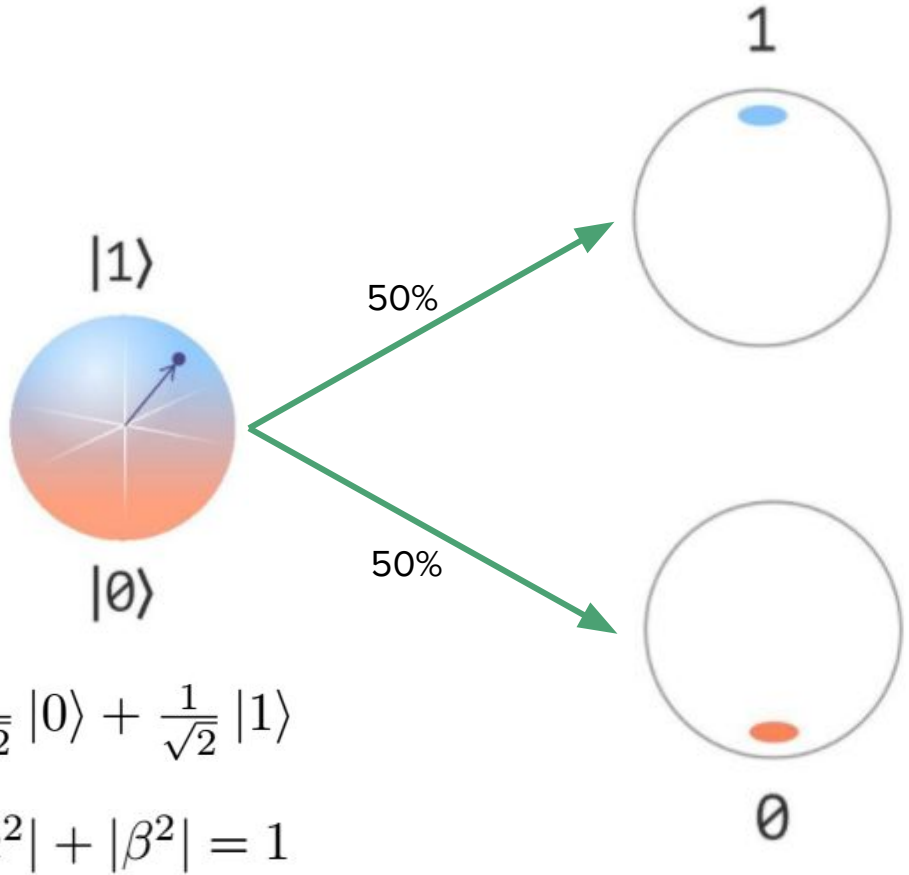




[https://towardsdatascience.com/grokking-quantum-computing-a-quirky-guide-for-curious-people-8cea6eb67803]

Pojęcia

- Kubit, superpozycja
- Pomiar kubitu

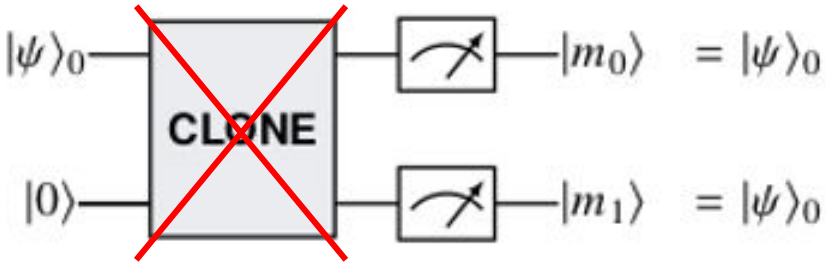


$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|\alpha^2| + |\beta^2| = 1$$

Pojęcia

- Kubit, superpozycja
- Pomiar kubitu
- Twierdzenie o nieklonowaniu (zakaz klonowania)



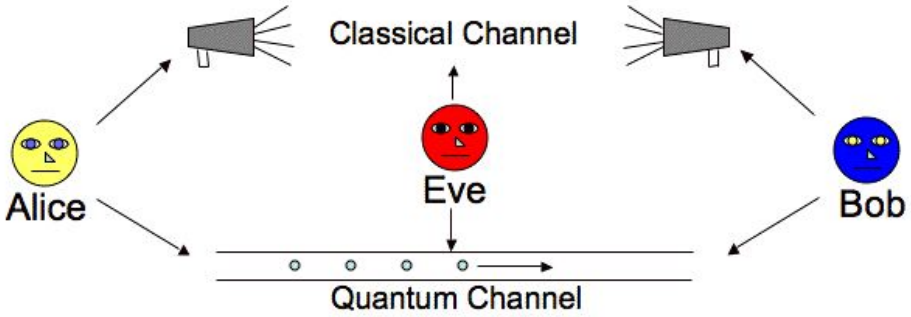
Nie można wykonać kopii nieznanego stanu kwantowego

[Wootters William, Zurek Wojciech, *A Single Quantum Cannot be Cloned,* 1982]

Jak technologie kwantowe zwiększają bezpieczeństwo?

Kwantowa dystrybucja klucza (QKD)

- Kryptografia kwantowa ≠ QKD
- Teoretycznie umożliwia **w pełni bezpiecz** wymianę klucza
- Próba podsłuchu powoduje **zakłócenia**, które mogą zostać wykryte
- Wymaga bezpiecznego kanału klasycznego - **uprzednia wymiana kluczy**
- Protokoły **BB84**, E91
- Czy warto?



	Koszty	**Bezpieczeństwo**
QKD	Wysokie	Całkowite (teoretycznie)
Klasyczne rozwiązania	Niskie	Bardzo wysokie

Sieci QKD

- 2001, USA - DARPA Quantum Network
- 2003, UE - sieć QKD w Wiedniu w ramach projektu SECOQC
- 2009, Japonia - sieć QKD w Tokio
- 2009, Chiny - hierarchiczna sieć w Wuhu
- 2010, Szwajcaria - SwissQuantum w Genewie - połączenie CERN z uniwersytetami
- 2016, Chiny - Quantum Experiments at Space Scale - pierwszy “kwantowy” satelita, wymiana kluczy między Pekinem a Wiedniem (dystans 7500 km)
- 2017, Chiny - połączenie między Pekinem a Szanghajem o długości 2000 km
- 2021, Chiny - połączenie sieci ponad 700 światłowodów z dwoma satelitami - zasięg 4600 km

OPEN QKD

Otwarta europejska platforma testowa dla technologii Kwantowej Dystrybucji Klucza

[https://openqkd.eu/partners/]

Plany PCSS

- **High performance computing** - With use case #01 we intend to connect the PSNC datacenters (primary and backup) in Poznań.
- **High performance computing** - With use case #06 we intend to connect the VSB and PSNC datacenters in Ostrava and Poznań.
- **Healthcare** - With use case #07 we intend to connect the PSNC datacenter in Poznań and hospital where PSNC delivers a number of IT services.
- **e-Government** - With use case #08 we intend to connect the PSNC datacenter in Poznań and Poznan city hall branches that provide critical IT services for citizens.
- **Banking** - With use case #09 we intend to connect the PSNC datacenter in Poznań and banking datacenter that provide critical digital banking services for citizens.
- **Police** - With use case #10 we intend to connect the PSNC datacenter in Poznań and local police datacenter that provide critical services for police infrastructure.
- **Time signal reference distribution** - With use case #11 we intend to connect one of the PSNC nodes and PoPs that include devices and infrastructure for the distribution of the reference time and frequency signals.

[https://openqkd.eu/]

POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE

Zestawienie złożonych ofert

Dot. postępowania **PN 10/05/2020 – system transmisyjny QKD o zasięgu miejskim**

Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia: **5.596.500,00 złotych brutto**

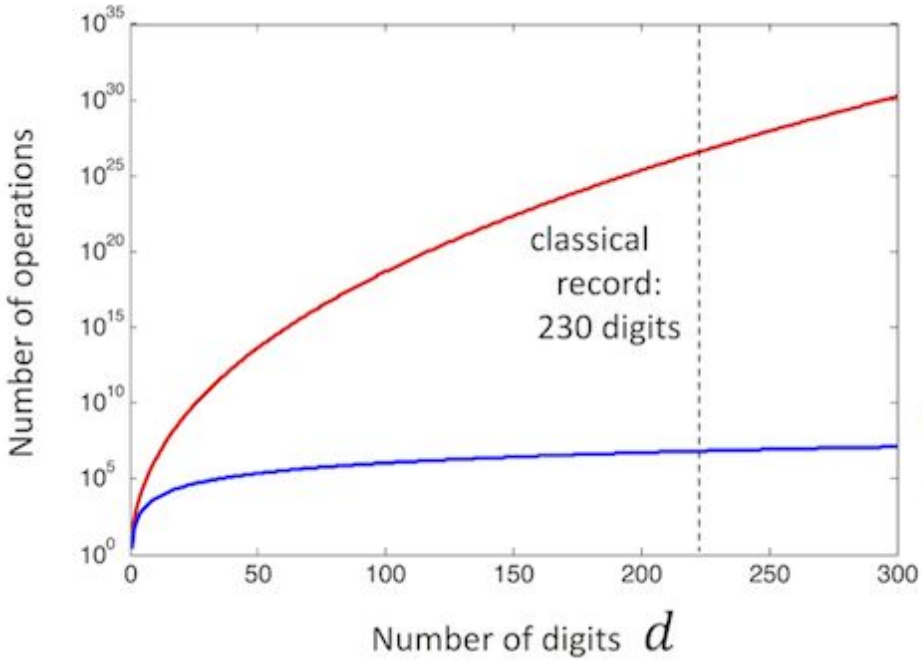
Lp.	Nazwa (firma) oraz adres Wykonawcy	Cena PLN brutto	Okres gwarancji i wsparcia technicznego	Termin Realizacji	Warunki płatności
1.	Konsorcjum firm: ICsec Spółka Akcyjna – lider konsorcjum ul. Wichrowa nr 1a 60-449 Poznaniu ALMA S.A. – członek konsorcjum ul. Wichrowa nr 1a 60-449 Poznaniu	4.922.460,00 zł	60 miesięcy	Zgodnie z SIWZ	Zgodnie z SIWZ

[http://wwwold.man.poznan.pl/online/zampub.php?co=offers&za_id=13047&wydzial=pcss]

Jak technologie kwantowe zagrażają bezpieczeństwu?

Algorytm faktoryzacji Shora

- Peter W. Shor, A*lgorithms for quantum computation: discrete logarithms and factoring*, **1994**
- **Faktoryzacja** liczb całkowitych, **logarytmy dyskretne**
- Niemalże **wykładniczy** przyrost wydajności względem najlepszego algorytmu klasycznego



Algorytm Shora a kryptografia

RSA	Faktoryzacja dużych liczb	
DSA	Logarytmy dyskretne	
ECDSA	Logarytmy dyskretne na krzywych eliptycznych	
AES	Szyfr blokowy	
SHA	Funkcje jednokierunkowe	

* Pod warunkiem korzystania z wersji 256-bitowej - algorytm Grovera

Czy komputery kwantowe zagrażają kryptografii?

Klucz RSA-2048	**Największa liczba rozłożona na czynniki pierwsze za pomocą algorytmu Shora**
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357	21

Czy komputery kwantowe zagrażają kryptografii?

- Wystarczająco zaawansowane komputery kwantowe - **co najmniej 20 lat**
- Kwantowe wyżarzanie - faktoryzacja liczby 1005973, ale **brak dowodów** na większą wydajność
- Złamanie RSA, DSA, ECDSA ≠ koniec kryptografii

Kryptografia postkwantowa

- Algorytmy kryptograficzne oparte na kratach (ang. *lattice-based cryptography*) - **NTRU**
- Algorytmy oparte na kodach korekcyjnych (ang. *code-based cryptography)* - **Algorytm McEliece'a**
- Kryptografia wielu zmiennych (ang. *multivariate cryptography*) - **HFE**
- Algorytmy oparte na funkcji skrótu (ang. *hash-based cryptography*) - **Drzewo hash**
- Kryptografia symetryczna - **AES**

Bibliografia

- https://towardsdatascience.com/grokking-quantum-computing-a-quirky-guide-for-curious-people-8cea6eb67803
- Bernstein D.J., *Introduction to post-quantum cryptography.* [w:]: Bernstein D.J., Buchmann J., Dahmen E., *Post-Quantum Cryptography,* 2009
- https://en.wikipedia.org/wiki/Quantum_cryptography
- https://en.wikipedia.org/wiki/Quantum_key_distribution
- https://en.wikipedia.org/wiki/Quantum_network
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- https://en.wikipedia.org/wiki/Post-quantum_cryptography
- https://jakubmielczarek.com/2019/11/25/technologie-kwantowe-a-cyberbezpieczenstwo/
- https://openqkd.eu/

Dziękuję za uwagę