Quantum Communication and Quantum Algorithms

The Content

Introduction

1. Quantum Communication protocols,

2. Quantum algorithms

Basic Literature

1. Michael A. Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information Cambridge University Press, 2000
2. Gregg Jaeger, Quantum Information, An Overview, Springer Science+Business Media, LLC, 2007
3. Christopher Gerry, Peter Knight, Introductory Quantum Optics, Cambridge University Press, 2005
4. L. Mandel and E. Wolf, Optical Coherence and Quantum Optics, Cambridge University Press, 1995.
5. D. F. Walls, Gerard J. Milburn, Quantum Optics Springer Science & Business Media, 2008.
6. S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics,* Oxford, 1997
7. Anthony Sudbery. Quantum Mechanics and the Particles of Nature: An Outline for Mathematicians Cambridge University Press 1986

Quantum Algorithms

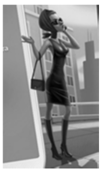
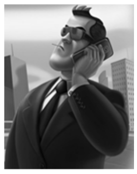
Charles Bennett

Bennett's laws of quantum information

- ✓ **1 qubit ⩾ 1 bit (classical),**
- ✓ **1 qubit ⩾ 1 ebit (entanglement bit),**
- ✓ **1 ebit + 1 qubit ⩾ 2 bits (i.e. superdense coding),**
- ✓ **1 ebit + 2 bits ⩾ 1 qubit (i.e. quantum teleportation),**

Quantum Teleportation (of unknown state)

Alice wants to send her qubit to Bob.
She does not know the quantum state of her qubit.

Alice  *classical communication* → Bob 

$|\Phi_C\rangle = a|0_C\rangle + b|1_C\rangle$ **Unknown qubit state!**

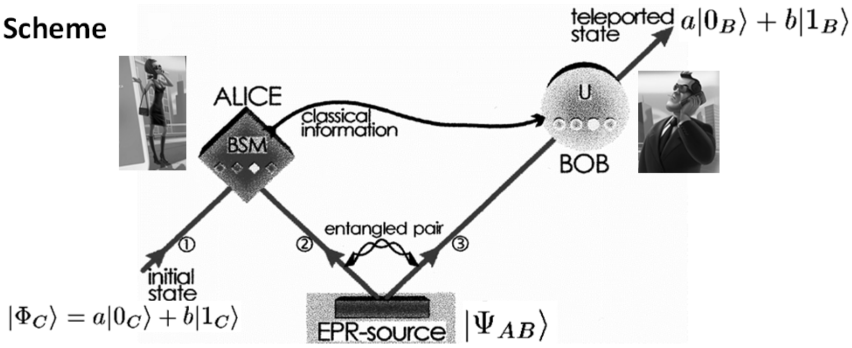
Suppose these bits contain information about $|\Phi_C\rangle$

Then Bob would have information about $|\Phi_C\rangle = a|0_C\rangle + b|1_C\rangle$

This would be a procedure for extracting information from $|\Phi_C\rangle$ without effecting the state

Quantum Teleportation Algorithm

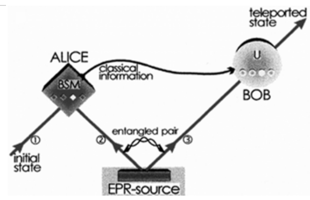
Scheme



1. To prepare entangled state $|\Psi_{AB}\rangle = \sqrt{1/2}\,(|0_A 0_B\rangle + |1_A 1_B\rangle)$

2. To share $|\Psi_{AB}\rangle$ with $|\Phi_C\rangle$

Quantum Teleportation Algorithm



2. To share $|\Psi_{AB}\rangle$ with $|\Phi_C\rangle$

$$|\Phi_{ABC}\rangle = |\Phi_C\rangle \otimes |\Psi_{AB}\rangle = \Big(a|0_C\rangle + b|1_C\rangle\Big) \otimes \sqrt{1/2}\Big(|0_A 0_B\rangle + |1_A 1_B\rangle\Big) =$$

$$= \frac{1}{2}\Big(|\Phi^+_{AC}\rangle \otimes \Big(a|0_B\rangle + b|1_B\rangle\Big) + |\Phi^-_{AC}\rangle \otimes \Big(a|0_B\rangle - b|1_B\rangle\Big) +$$

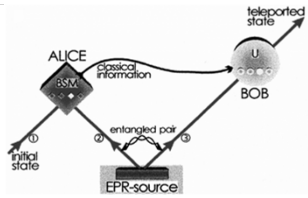
$$+|\Psi^+_{AC}\rangle \otimes \Big(a|1_B\rangle + b|0_B\rangle\Big) + |\Psi^-_{AC}\rangle \otimes \Big(a|1_B\rangle - b|0_B\rangle\Big)\Big),$$

where $|\Phi^\pm_{AC}\rangle = \sqrt{1/2}\Big(|0_A 0_C\rangle \pm |1_A 1_C\rangle\Big),$ ***are Bell states***

$$|\Psi^\pm_{AC}\rangle = \sqrt{1/2}\Big(|0_A 1_C\rangle \pm |1_A 0_C\rangle\Big)$$

•

Quantum Teleportation Algorithm



3. Alice perform Bell measurement with $|\Phi_{ABC}\rangle$

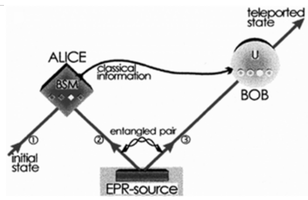
Output state

$$\boxed{\begin{aligned}|\Phi_{ABC}\rangle = \frac{1}{2}\Big(&|\Phi^+_{AC}\rangle \otimes \big(a|0_B\rangle + b|1_B\rangle\big) + |\Phi^-_{AC}\rangle \otimes \big(a|0_B\rangle - b|1_B\rangle\big) + \\ &+|\Psi^+_{AC}\rangle \otimes \big(a|1_B\rangle + b|0_B\rangle\big) + |\Psi^-_{AC}\rangle \otimes \big(a|1_B\rangle - b|0_B\rangle\big)\Big),\end{aligned}}$$

- ✓ ***Bob obtain qubit*** $a|0_B\rangle + b|1_B\rangle$ ***if Alice measures*** $\langle\Phi^+_{AC}|\Phi_{ABC}\rangle$
- ✓ ***Bob obtain qubit*** $a|0_B\rangle - b|1_B\rangle$ ***if Alice measures*** $\langle\Phi^-_{AC}|\Phi_{ABC}\rangle$
- ✓ ***Bob obtain qubit*** $a|1_B\rangle + b|0_B\rangle$ ***if Alice measures*** $\langle\Psi^+_{AC}|\Phi_{ABC}\rangle$
- ✓ ***Bob obtain qubit*** $a|1_B\rangle - b|0_B\rangle$ ***if Alice measures*** $\langle\Psi^-_{AC}|\Phi_{ABC}\rangle$

•

Quantum Teleportation Algorithm



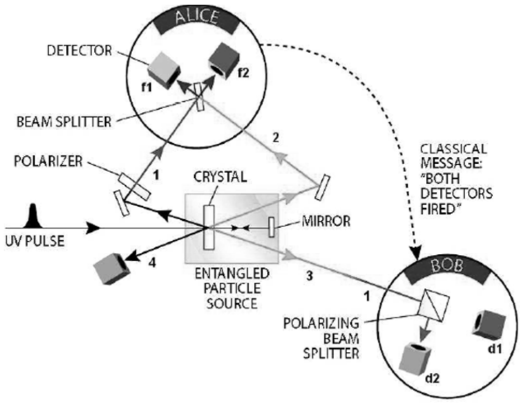
4. Alice tells Bob by classical channel (cell phone) what type of measurement he should do to recover initial qubit $a|0_B\rangle + b|1_B\rangle$

- ✓ ***If Alice measures*** $\langle\Phi^-_{AC}|\Phi_{ABC}\rangle$ ***, its OK for Bob***
- ✓ ***If Alice measures*** $\langle\Phi^-_{AC}|\Phi_{ABC}\rangle$ ***, she tells Bob to do*** $\widehat{\sigma}_z$: $|0\rangle \Rightarrow |0\rangle, |1\rangle \Rightarrow -|1\rangle$ ***operation with his qubit***
- ✓ ***If Alice measures*** $\langle\Psi^-_{AC}|\Phi_{ABC}\rangle$ ***, she tells Bob to do*** $\mathrm{NOT} = \widehat{\sigma}_x$: $0\rangle \Rightarrow |1\rangle, |1\rangle \Rightarrow |0\rangle$ ***operation with his qubit***
- ✓ ***If Alice measures*** $\langle\Psi^-_{AC}|\Phi_{ABC}\rangle$ ***, she tells Bob to do*** $\mathrm{NOT} = \widehat{\sigma}_x$ ***and*** $\widehat{\sigma}_z$

Alice uses 1ebit+2 bit (optional) information to teleport unknown state!

Experimental Realization

- UV pulse beam hits BBO crystal twice
- Photon 1 is prepared in initial state
- Photon 4 as trigger
- Alice looks for coincidences
- Bob knows that state is teleported and checks it.
- Threefold coincidence $f_1 f_2 d_1$(+45°) in absence of $f_1 f_2 d_2$ (-45°)
- Temporal overlap between photon 1,2



Dik Bouwmeester, Jian-Wei Pan, K. Mattle, M. Eibl, H. Weinfurter & A. Zeilinger , Experimental quantum teleportation Nature, 390, p. 575–579 (1997)

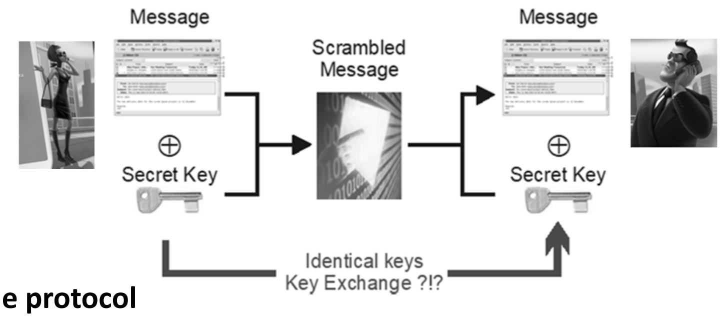
Quantum Teleportation: Outlook

- ***The teleportation process makes it possible to "reproduce" a qubit in a different location***
- ***But the original qubit is destroyed!***

$\boxed{\text{1 qubit = 1 ebit + 2 bits}}$

•

Secret Key Cryptography



Ernesto Che Guevara

The protocol

1. Alice encodes her message in numbers $M = \{73997\ 68279\ 65867\ldots\}$
2. Alice and Bob shares secret key $K = \{12793\ 41169\ 42357\ldots\}$
3. Alice creates scrambled message by **M+K=C,** $C = \{85680\ 09338\ 07114\ldots\}$

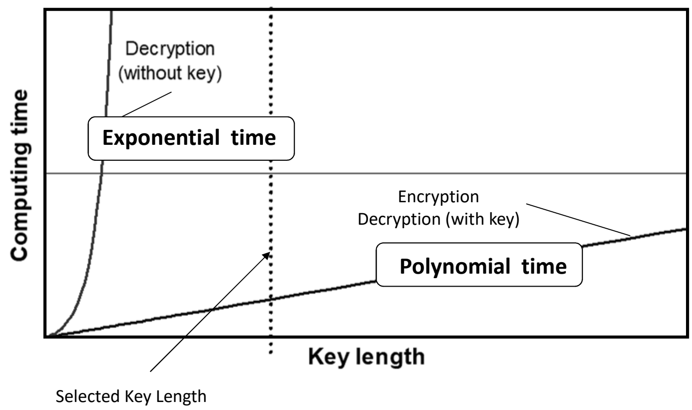
4. Alice submit **C** by public channel.

5. Bob decodes the message starting from 4 item and moving to the 1th.

Shannon proves that this protocol is absolutely secure if Alice and Bob use secret key only one time

Security of public key cryptography

Complexity of the Problem



How is your Credit Card Safe?

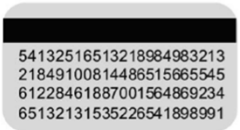
In our life public-key cryptosystem, like RSA protect s data transmission , coding, etc

R. **R**ivest, A. **S**hamir, and L. **A**delmann, "A method for Obtaining Digital Signatures and Publik-Key cryptosystems" (1977)

This protocol uses asymmetry in solution of two problems

Simple problem: 77236 **x** 42231 **=** 3261753516

Hard problem is factorizatio 48151623427 **=** ▭ **x** ▭ **?**



Credit card contains
Large number Z – "Public key"

+

We introduce PIN –
"Private Key"

ATM checks the result of

$$\frac{\text{"Public key"}}{\text{"Private Key"}} = ?$$

Factorization

1881988129206079638386972394616504 3
9807163563379417382700763356422988 8
5971523466548531906060650474304531 7
3880113033967161996923212057340318 7
9550656996221305168759307650257059

=

Euclid

prime numbers

398075086424064937397 1
255005503864911990643 6
234252670840638518957 5
946388957261768583317

×

472772146107435302536 2
230719730482246329146 9
530209711645985217113 0
520711256363590397527

Best classical algorithm takes time $O(\exp(n^{1/3}))$

Shor's quantum algorithm takes time $O(n^3 \log n)$

An efficient algorithm for factoring breaks the RSA public key cryptosystem

•

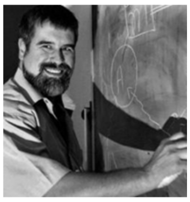
Quantum Cryptography BB84 protocol

- 2 conjugate basis
- Information encoded in photon's polarization

  → **'0'** ≡ ↔ & ⤡

  → **'1'** ≡ ↕ & ⤢
- Quantum & classical channels used for key exchange

Charles Bennett

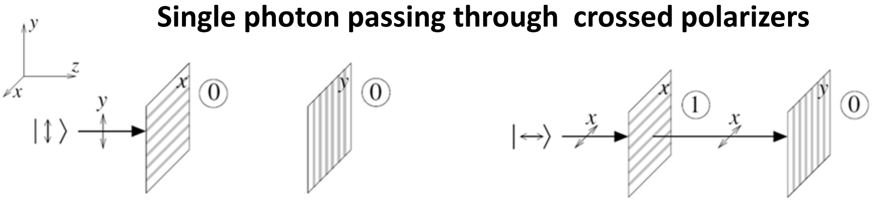


Gilles Brassard

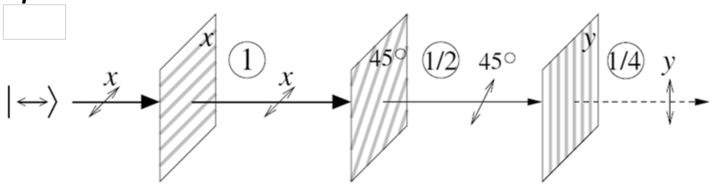
•

Single photon polarization: vital peculiarities

Single photon passing through crossed polarizers

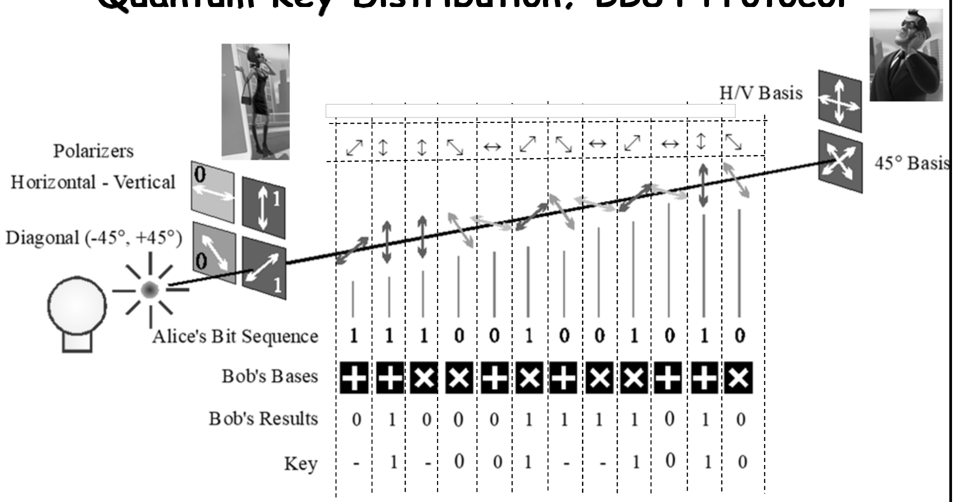


Neither a vertically nor a horizontally polarized photon can go through two crossed polarizers



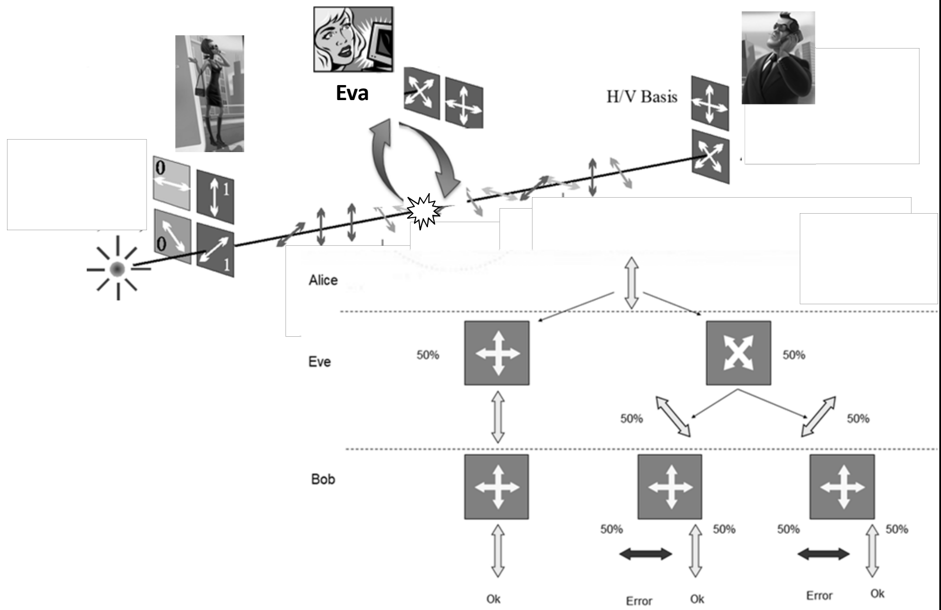
Inserting between the crossed polarizers another polarizer at 45◦ allows the horizontally polarized photon to pass with probability 1/4 .

Quantum Key Distribution; BB84 Protocol

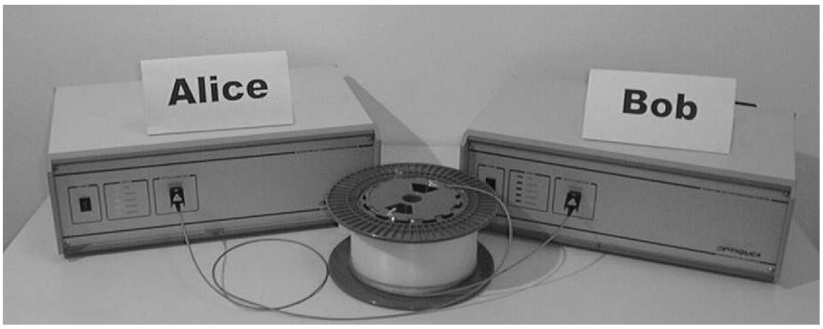


Use quantum physics to force spy to introduce errors in the communication

Eavesdropping Effect

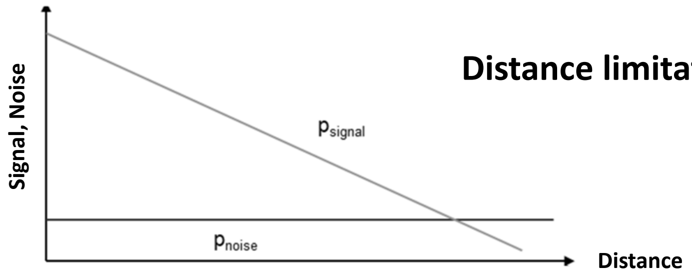


Quantum Cryptography nowadays



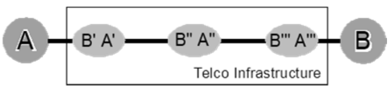
This is what the actual device looks like. The coil is of ordinary optical fiber.

Extending the key Distribution Distance

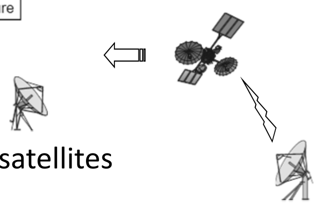


Distance limitation < 300 km

- Chaining links



- Better components



- Free space links to low-earth-orbit (LEO) satellites
- Quantum relays and repeaters

Literature

- Bennett, C. H., G. Brassard and A. K. Ekert. "Quantum Cryptography", Scientific American. October 1992: pp. 752 – 753.
- Brassard, Gilles. "A Bibliography of Quantum Cryptography" (April 24,2002). [Online] Available at: www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html, April 13, 2004.
- DeJesus, Edmund. "Cryptography : Quantum Leap". Information Security Magazine (Aug 2001). [Online] Available at: www.infosecuritymag.com/articles/august01/features_crypto.shtml, May 8, 2004.
- Hammond, Andrew. MagiQ. [Online] Available at: http://www.magiqtech.com/press/Magiq_Navajo_Launch.pdf, May 11, 2004.
- Kahn, David. "The Codebreakers". Macmillan, 1967.
- Nickels, Ian. Informal in-person interviews conducted in May 2004 at SRJC.
- The European Information Society Group. "Briefing 16 Annex 1 : What is Cryptography?". [Online] Available at: www.eurim.org/briefings/brief16a.htm, April 15, 2004.
- Thornton, Stephen T. and Andrew Rex. "Modern Physics For Scientists and Engineers". Second Edition. United States of America: Thomson Learning, 2002.
- Unsigned. "Quantum leap for secret codes" BBC News (June 5, 2003). [Online] Available at: www.bbc.co.uk/1/hi/technology/2963138.stm, April 13, 2004.

Search Problem

In data base we have $N = 2^n$ **entries**

Variable ***x = 0, ….., N*** enumerates ***N*** entries

Our goal it to find entry with that fulfill to Eq. **x=** ω

Moscow phone book , 1928

Then we introduce function that

$$f_\omega(x) = \begin{cases} 0, & \text{if } x \neq \omega \\ 1, & \text{if } x = \omega \end{cases},$$

Our Goal is to find **x** for which $f_\omega(x) = 1$.

Grover Quantum Search Algorithm

Lov Grover

- Quantum search algorithm provides a ***quadratic speedup*** over best classical algorithm

Classical: N steps   Quantum: $N^{1/2}$ steps

- Maybe there is a better quantum search algorithm
- Imagine one that requires **log *N*** steps:
  - Quantum search would be exponentially faster than any classical algorithm
  - Used for **NP** problems: could reduce them to **P** by searching all possible solutions

NO: Quantum search algorithm is "optimal"
Any search- based method for **NP** problems is slow

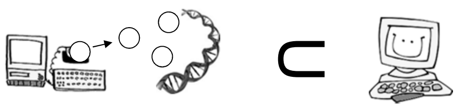
Some Important Conclusions about QC

Reversibility

In ideal QC the simulations are reversible

Quantum Supremacy

Al calculations that can be realized in classical Computer are realizable on QC



No Cloning Theorem

Unknown quantum state cannot be cloned

The End