From entanglement to quantum cryptography

马雄峰

xma@tsinghua.edu.cn

Center for Quantum Information

清華大學 交叉信息研究院

Tsinghua University Institute for Interdisciplinary Information Sciences

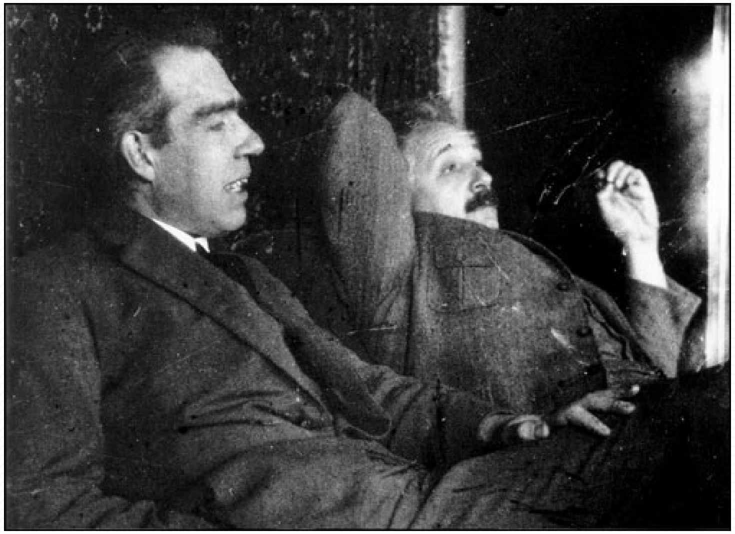
Outline

- Quantum entanglement
  - EPR pair
- Quantum cryptography
  - Cryptography
  - Why Quantum Cryptography
  - Why is it secure?
- *MDI QKD
- Some developments in quantum crypto

Quantum Entanglement

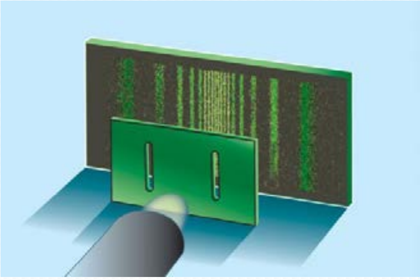
Quantum intrinsic randomness

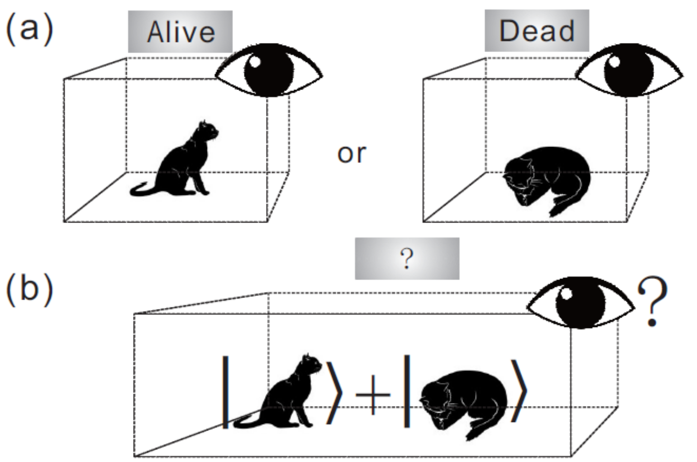
- Einstein, “God does not play dice!”
- Bohr, “Albert, stop telling God what to do!”



What is Coherence?

- Coherent interference
- Schrodinger's cat

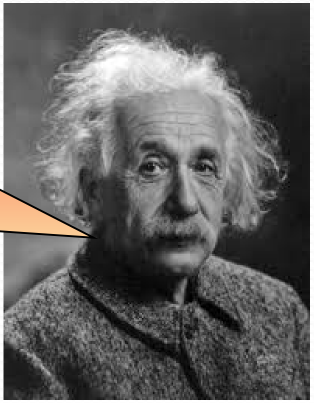




Einstein-Podolsky-Rosen Paradox

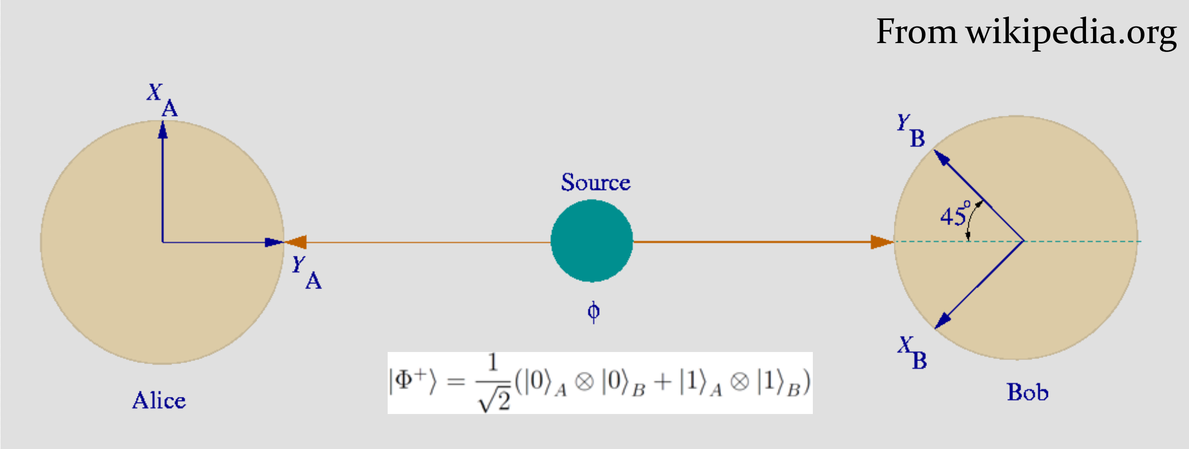
- Is Quantum Mechanics complete?
- Local hidden variable
- Entanglement
  - A pair of particles: measure on one particle would instantaneously affect the state of the other

Spooky action at a distance



Bell's inequality

- Quantum mechanics vs. local hidden variable



X_A
Y_A
Source
ϕ
Y_B
45°
X_B
Alice
$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$
Bob

From wikipedia.org

$$\begin{aligned} S &= -\langle x_a x_b \rangle + \langle x_a y_b \rangle + \langle y_a x_b \rangle + \langle y_a y_b \rangle \\ &= \langle (-x_a + y_a) x_b \rangle + \langle (x_a + y_a) y_b \rangle \\ &\leq |-x_a + y_a| + |x_a + y_a| \leq 2 \end{aligned}$$

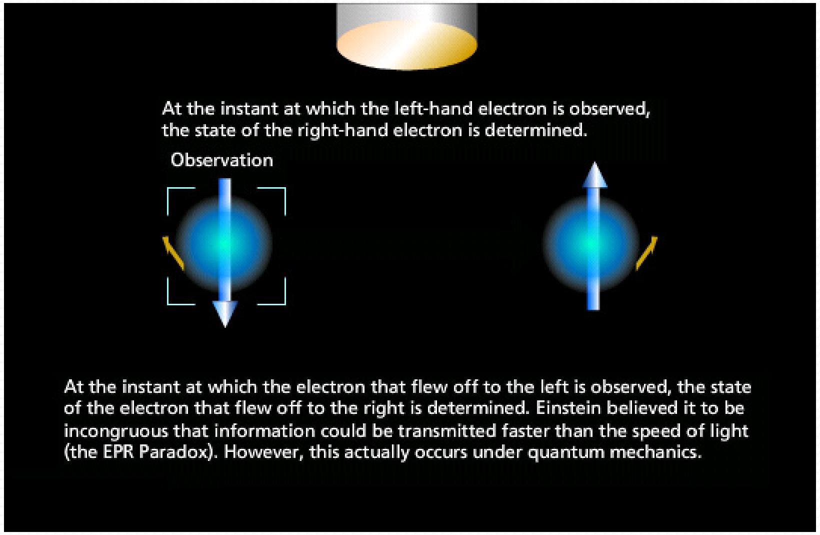
$$\langle x_a x_b \rangle = -\frac{1}{\sqrt{2}}$$

$$\langle x_a y_b \rangle = \langle y_a x_b \rangle = \langle y_a y_b \rangle = \frac{1}{\sqrt{2}}$$

$$S = 2\sqrt{2}$$

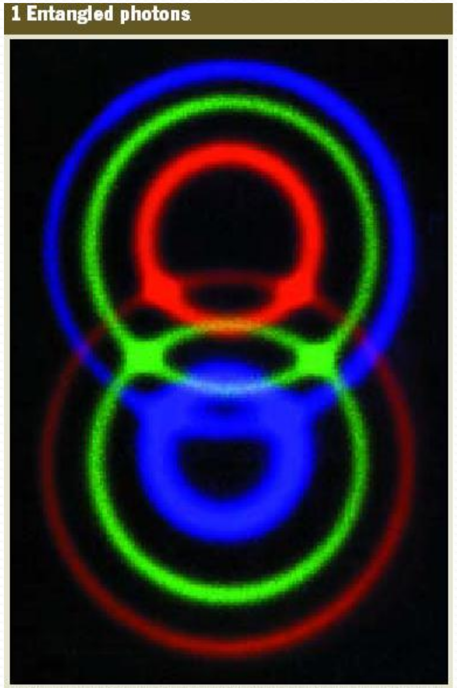
EPR pairs in reality

- Various physical systems



At the instant at which the left-hand electron is observed, the state of the right-hand electron is determined.

At the instant at which the electron that flew off to the left is observed, the state of the electron that flew off to the right is determined. Einstein believed it to be incongruous that information could be transmitted faster than the speed of light (the EPR Paradox). However, this actually occurs under quantum mechanics.



1 Entangled photons

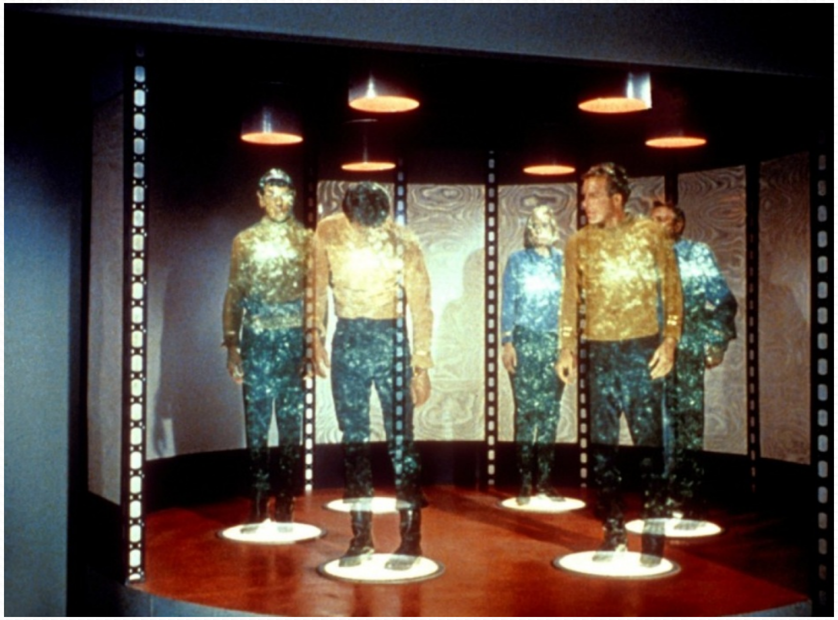
- Alain Aspect’81: Bell’s inequality experiment demo

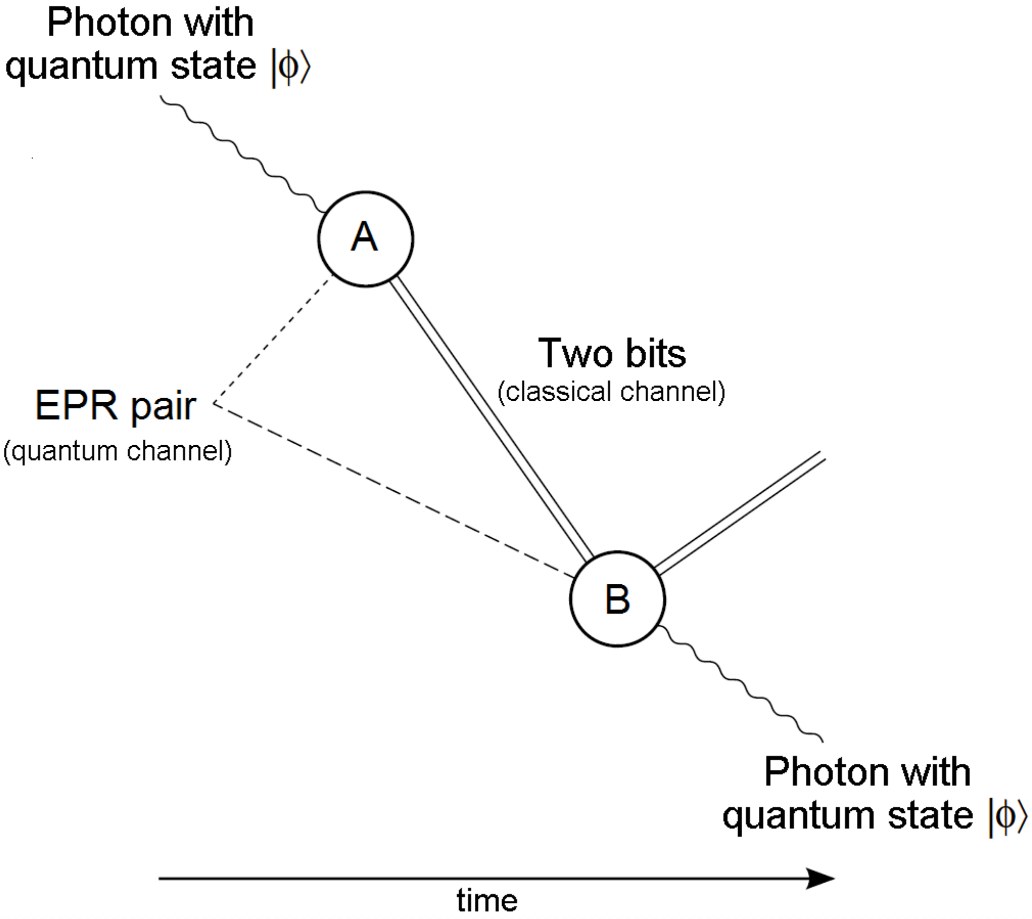
Entanglement

- EPR pair
  - |00>+|11> = |++>+|-->
- Non-locality --- Entanglement
  - Local hidden variable: been ruled out by Bell’s inequality test
  - Non-local correlation: why quantum mechanics is “weird”
- Natural source for secure key
  - Strong correlation
  - Randomness in nature
  - Cannot be eavesdropped --- no local hidden variable
- EPR pair means perfect key

Quantum Teleportation

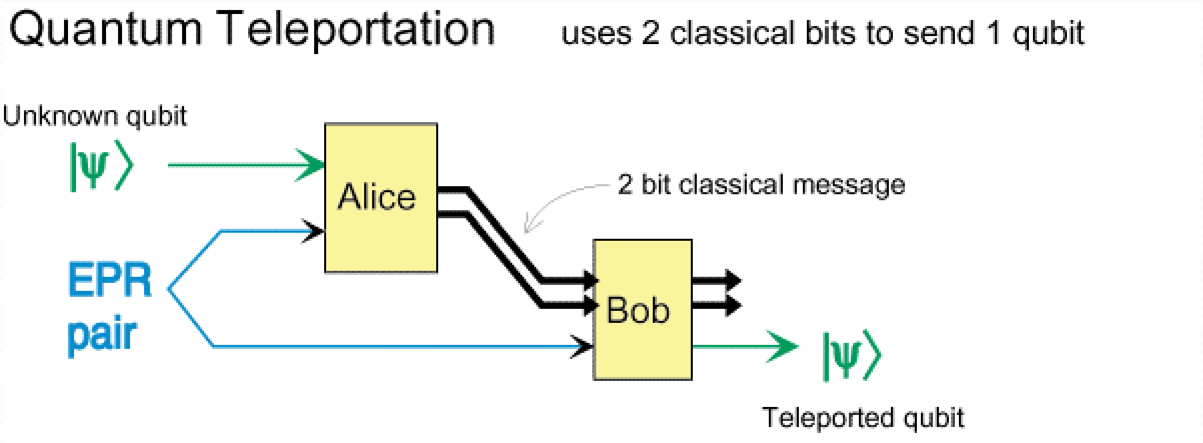
- Sci-Fi
  - Instant transportation
  - Teleport materials





Teleportation

- How to send a quantum state $a|1\rangle + b|1\rangle$ faithfully?
  - Classically, the values of a and b are continuous, so it requires a large amount of information transmission
  - Heisenberg's uncertainty principle
- What if Alice and Bob have a pre-shared entangled state?
  - Only needs to transfer 2 classical bits

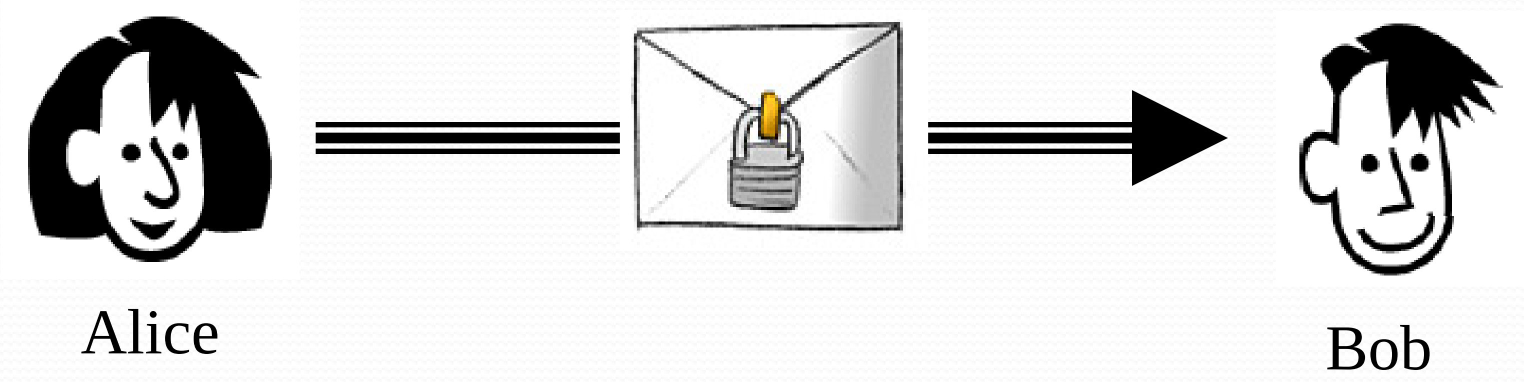


Quantum Cryptography

Information security

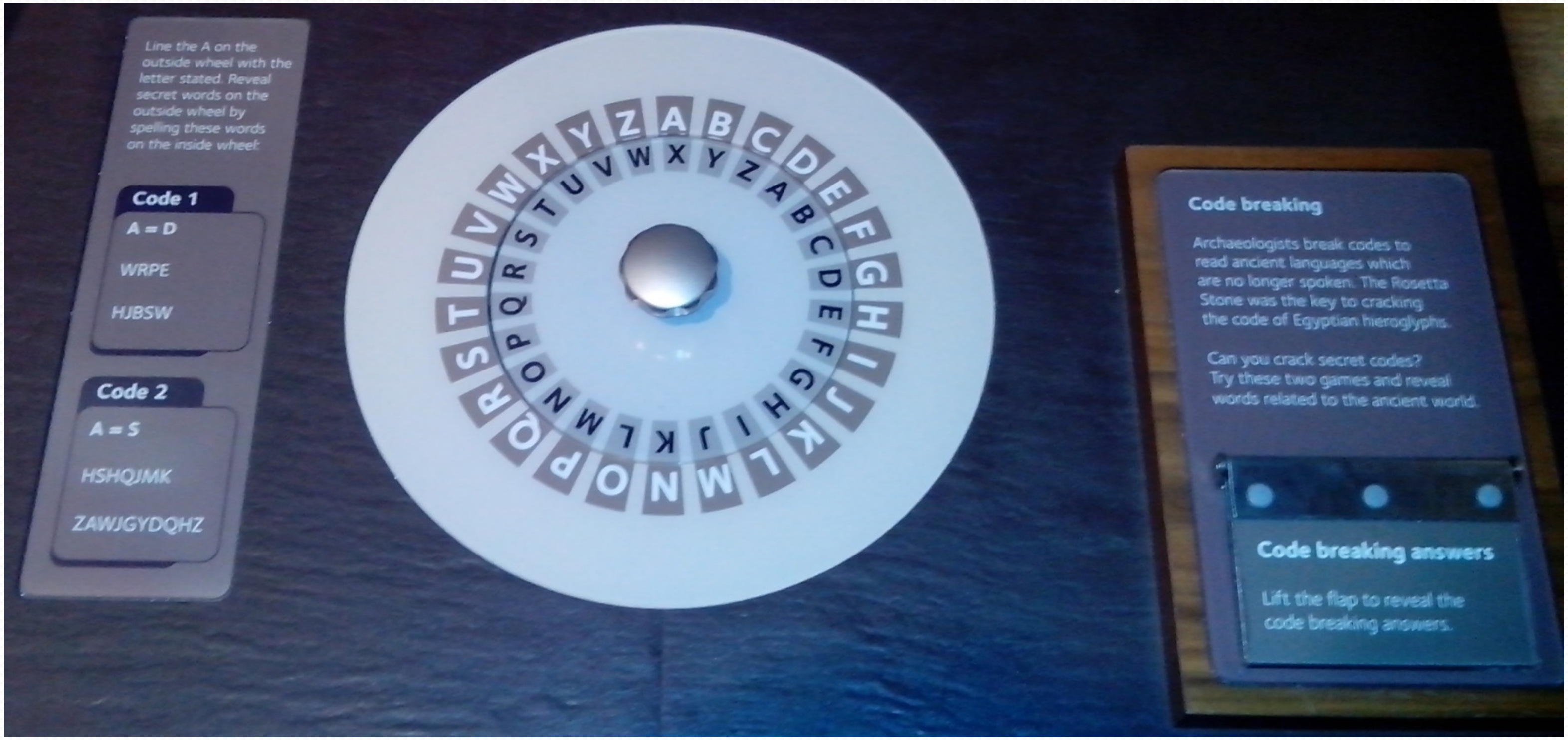
Cryptography

- Cryptography
  - The science of encoding and decoding secret messages.
- Cryptology
  - Public key cryptosystem (such as RSA, Diffie-Hellman)
- Cryptanalysis
  - Hacking



Cryptography in history

- 2000 BC
- War



Line the A on the outside wheel with the letter stated. Reveal secret words on the outside wheel by spelling these words on the inside wheel:

Code 1

A = D

WRPE

HJBSW

Code 2

A = S

HSHQJMK

ZAWJGYDQHZ

Code breaking

Archaeologists break codes to read ancient languages which are no longer spoken. The Rosetta Stone was the key to cracking the code of Egyptian hieroglyphs.

Can you crack secret codes? Try these two games and reveal words related to the ancient world.

Code breaking answers

Lift the flap to reveal the code breaking answers.

Objective

- Confidentiality
- Integrity
- Authenticity
- Nonrepudiation
- Access Control

Cryptographic Methods

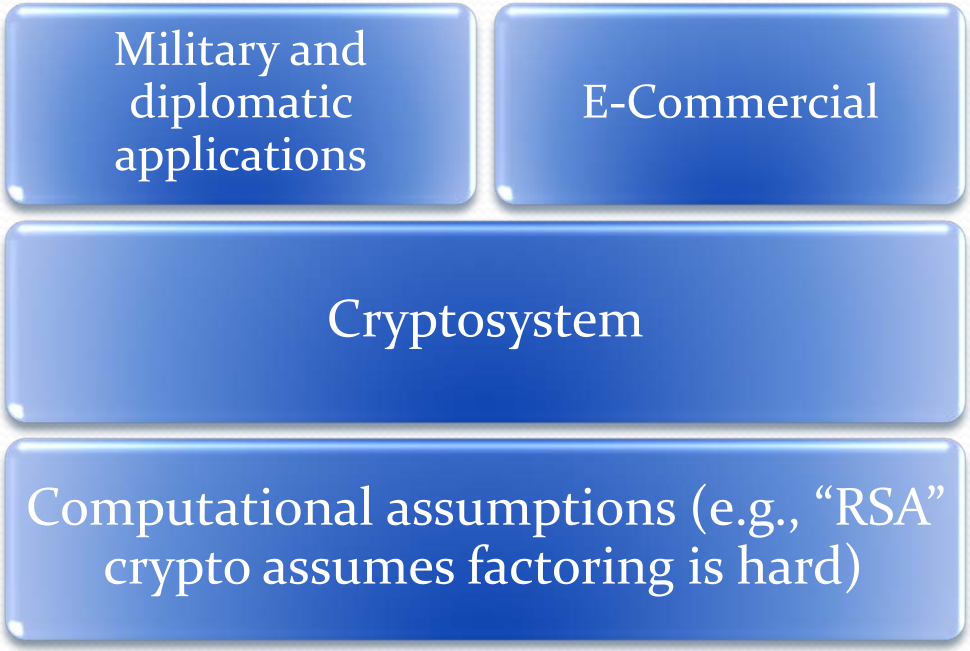
- Symmetric
  - Same key for encryption and decryption
  - Key distribution problem
  - E.g., DES, AES, IDEA, Blowfish, OTP, …
- Asymmetric
  - Mathematically related key pairs for encryption and decryption
  - Public and private keys
  - E.g., Diffie-Hellman, RSA, …
- Hybrid
  - Combines strengths of both methods
  - Asymmetric distributes symmetric key, also known as a session key
  - Symmetric provides bulk encryption
  - Example: SSL negotiates a hybrid method

Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active
- Kerckhoff’s Principle
  - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?
- Brute force
  - Trying all key values in the keyspace
- Dictionary Attack
  - Find plaintext based on common words
- Factoring Attacks
  - Find keys through prime factorization
  - Quantum computer

Conventional Cryptography

- Application framework



Military and diplomatic applications

E-Commercial

Cryptosystem

Computational assumptions (e.g., “RSA” crypto assumes factoring is hard)

What is wrong with conventional cryptography?

- Unanticipated Advances in Hardware and Algorithms.
- Quantum Code-breaking
- “Cryptographers do not sleep well.”
- Cryptography is for the paranoid.
- In history, every advance in code-making has been defeated by advances in code-breaking with disastrous consequences to users.

Unanticipated Advances in Hardware and Algorithms

- Code-breaking of Enigma led to fore-runners of computers!

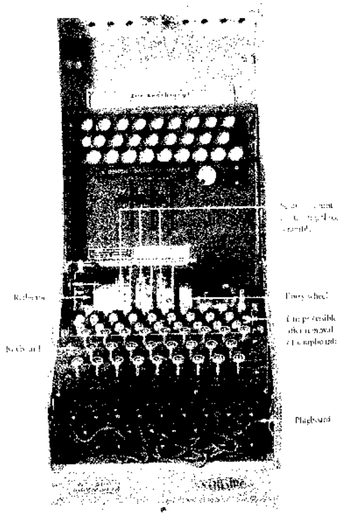


Figure [illegible] three scramblers

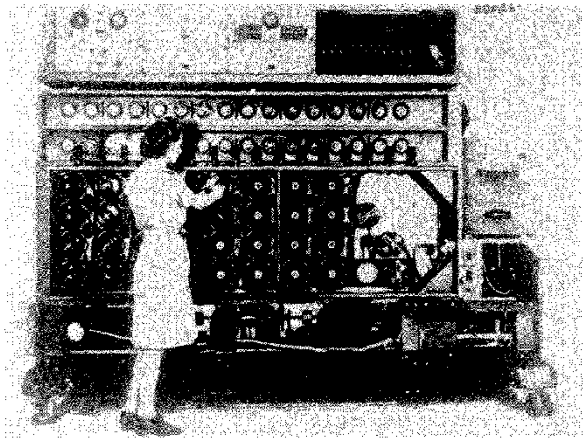


Figure 50 A Bletchley Park bombe in action.

German Enigma Machine
10 million billion possible combinations!
Looked unbreakable.

Allied code-breaking machine “bombe”.
Enigma Broken!

Quantum Code-breaking

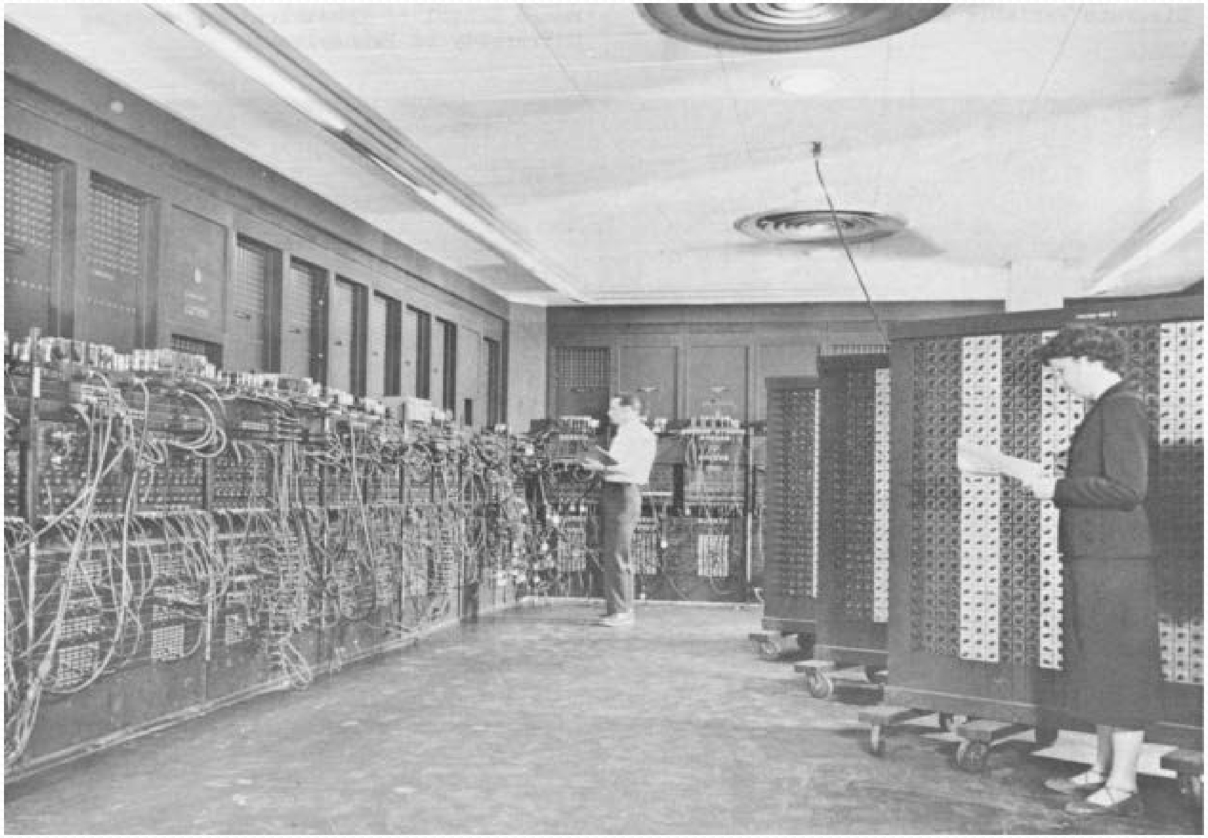
- Shor's algorithm: Factoring is easy with a quantum computer!
- Quantum computing can efficiently break:
  - RSA
  - Discrete logarithm problem: Diffie-Hellman key exchange
  - Elliptic-curve cryptographic systems
- "If a quantum computer is ever built, much of conventional Cryptography will fall apart!" (Brassard)

Forward security?

- Trade secrets and government secrets are kept as secrets for decades (say 70 years).
- A Big Problem RIGHT NOW:
  - If adversary can factor in 2086, she can then decrypt all traffic sent in 2016. (She can save all communications in 2016.)
- Was there any computer 70 years ago?
- What will a computer look like 70 years from now?
- It is ridiculous to think that we know the future 70 years from now.

ENIAC 1946

- The world's first electronic digital computer



Cell phone 2016

Computer in 2086

Private key cryptosystem

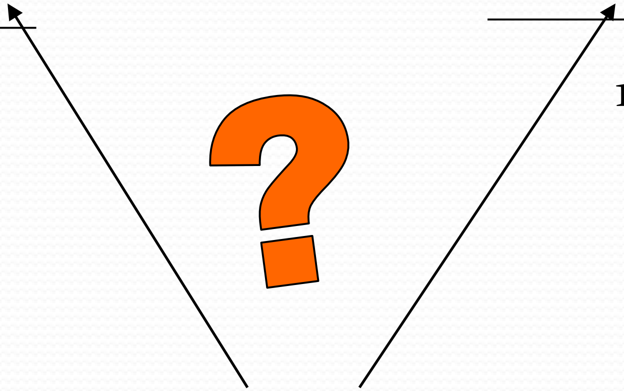
- One-time pad (OTP): proven secure by Shannon
- Alice and Bob share two identical keys secretly.

Encode

Decode

Counter Example: like it or not?

Message	10010110101		10101100001	Code
XOR			XOR	
Key	00111010100		00111010100	Key
Code	10101100001		10010110101	Message



Alice

Bob

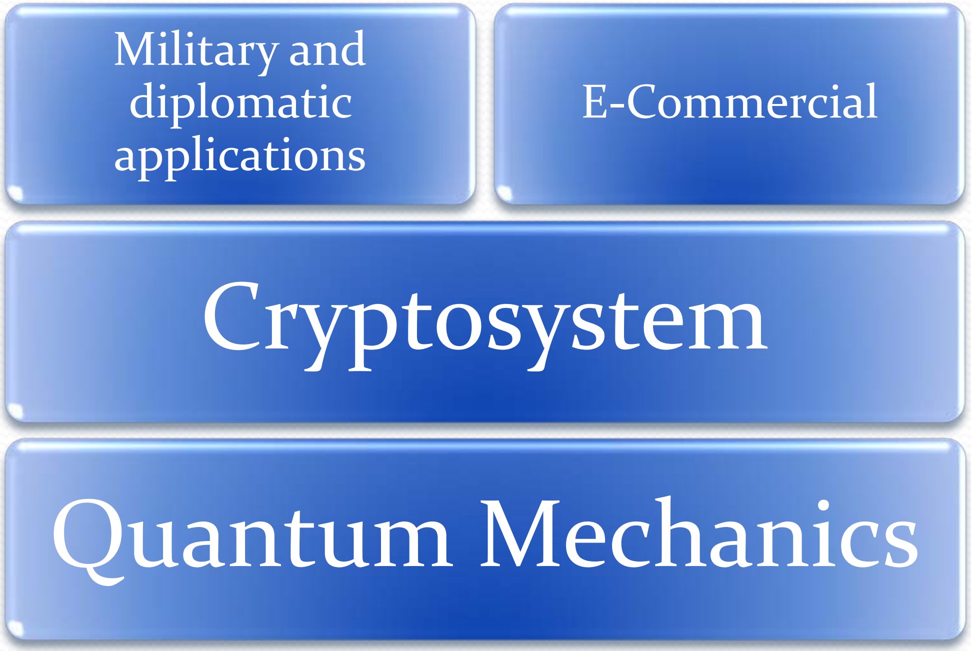
Key Distribution

Cryptographic Key

- Identical
  - Faithful decryption
- Private
  - Secure communication
- At least a long as the message
  - An efficient way to distribute key

Quantum Cryptography

- Application framework

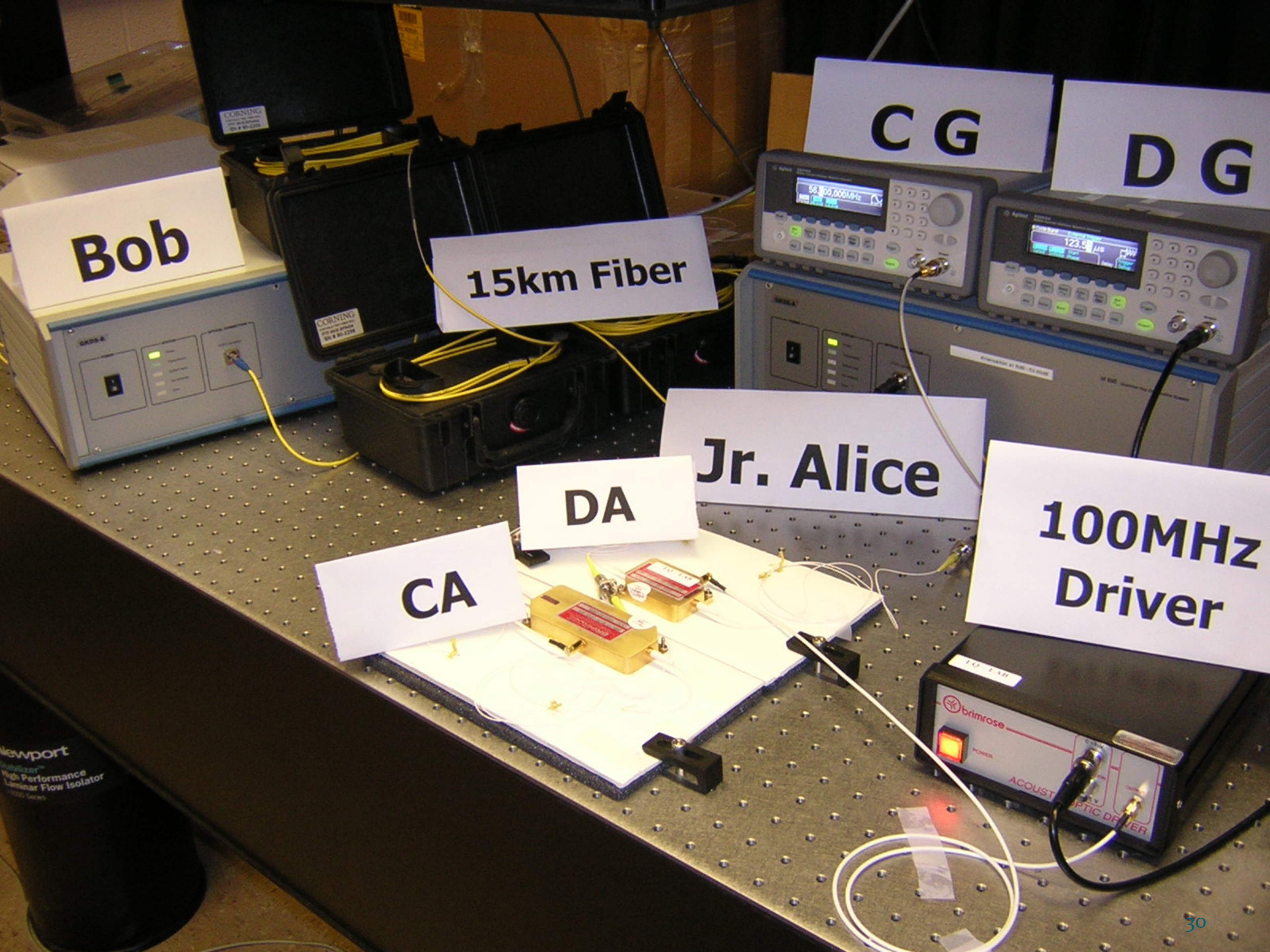


Military and diplomatic applications

E-Commercial

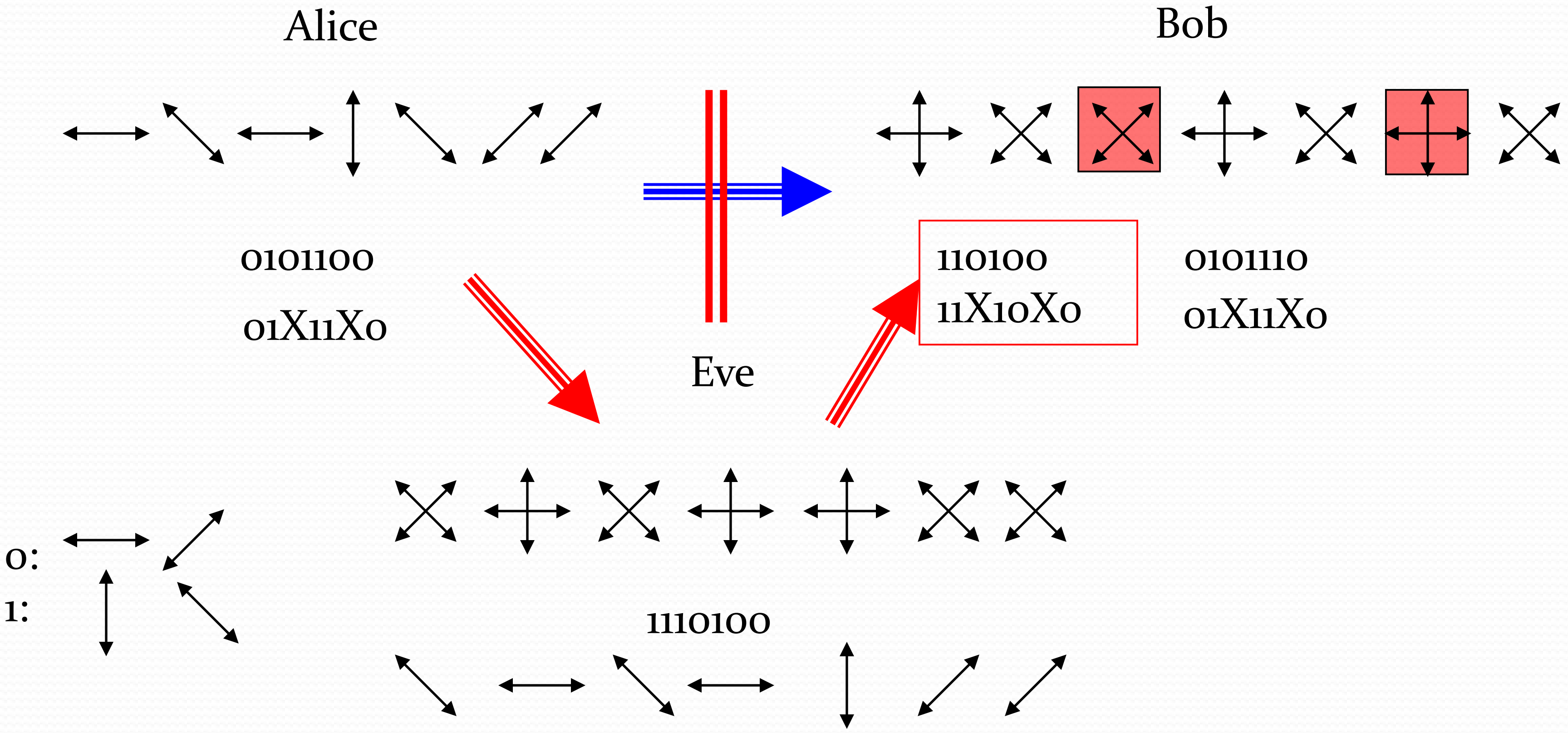
Cryptosystem

Quantum Mechanics


C G
D G
Bob
15km Fiber
Jr. Alice
DA
CA
100MHz
Driver
CORNING
56.100,000MHz
123.5 µs
brimrose
POWER
ACOUSTO-OPTIC DRIVER
Newport
Stabilizer
High Performance
Laminar Flow Isolator

Quantum key distribution (QKD)

- BB84 (Bennett & Brassard 1984)



Alice

Bob

0101100

01X11X0

110100

11X10X0

0101110

01X11X0

Eve

1110100

0:

1:

A few observations

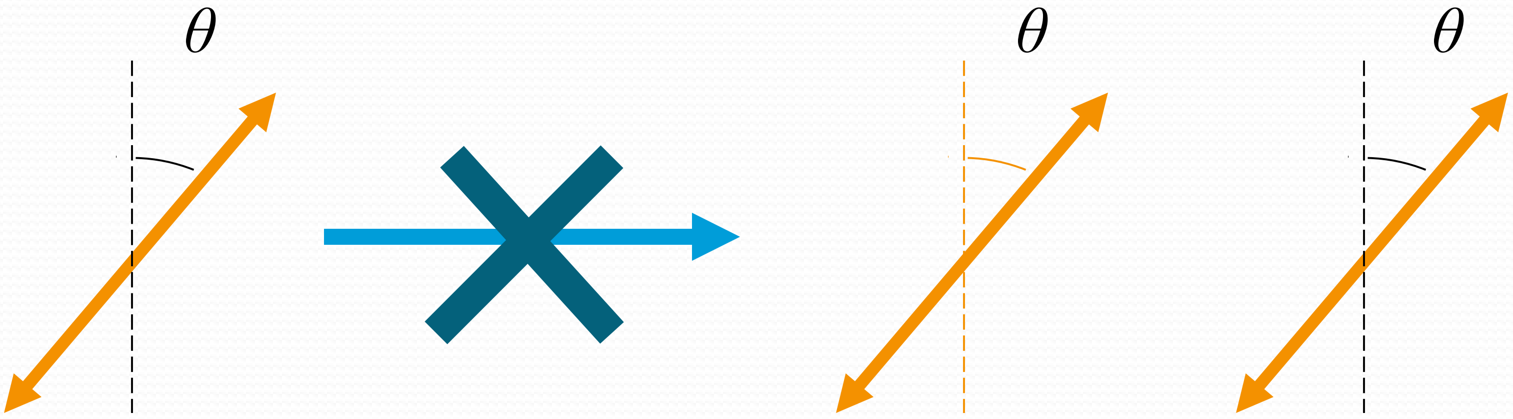
- Random keys are distributed via QKD systems
  - Alice does not send messages directly
  - Users can safely discard keys if they feel the channel is insecure without causing any security problem
  - Secure keys are used in later cryptosystems: composable
- A successful attack by Eve
  - Eve obtains non-trivial amount of information about the final key without Alice and Bob's notice
  - If Alice and Bob do not end up with any secure key, the attack is a failure
- Channel is totally insecure
  - Classical channel: authentication

Summary (take home message)

- QKD systems distribute keys
- QKD does not replace all the current cryptosystems
- QKD does not replace current communication systems
- An ideal private key
  - Identical: Alice and Bob share the same key
  - Private: Eve has no (or up to trivial amount of) information about the final key
- Post processing
  - Error correction: all classical, e.g., Cascade, LDPC
  - Privacy amplification: shorten the key so that Eve's information is eliminated; the focus of all security proofs

Quantum No-Cloning Theorem

- The polarization of a single photon cannot be cloned. Therefore, eavesdropper CANNOT have the same quantum information that Bob has.

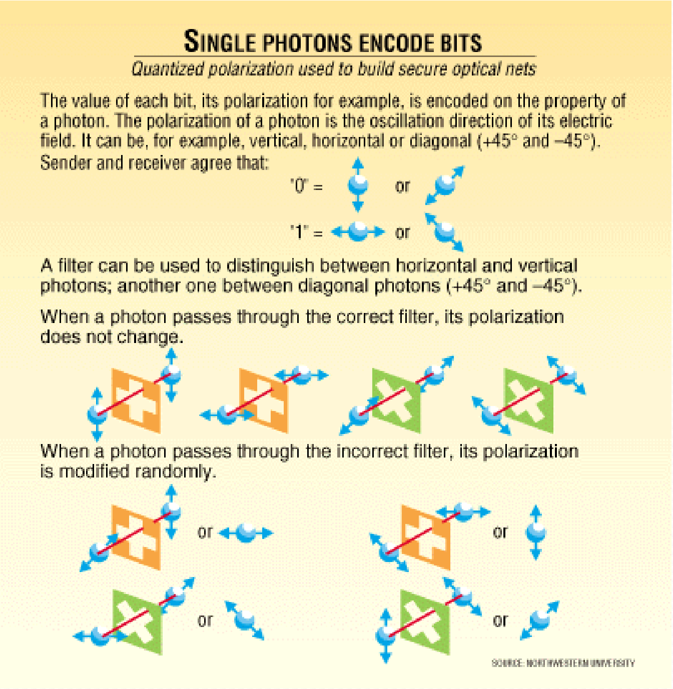


IMPOSSIBLE

- Information gain means disturbance

A quick review

- Prepare-and-measure protocols
  - BB84, six-state…
- Entanglement based protocols
  - Ekert91, BBM92
- Unconditional security proof
  - Mayers (1996)
  - Lo and Chau (1999)
  - Shor and Preskill (2000)
  - Devetak and Winter (2003), Renner (2005)
- Security analysis for QKD with imperfect devices
  - E.g. Mayers, Lütkenhaus, ILM
  - Koashi-Preskill
  - Gottesman-Lo-Lütkenhaus-Preskill (GLLP)



SINGLE PHOTONS ENCODE BITS

Quantized polarization used to build secure optical nets

The value of each bit, its polarization for example, is encoded on the property of a photon. The polarization of a photon is the oscillation direction of its electric field. It can be, for example, vertical, horizontal or diagonal (+45° and –45°).

Sender and receiver agree that:

A filter can be used to distinguish between horizontal and vertical photons; another one between diagonal photons (+45° and –45°).

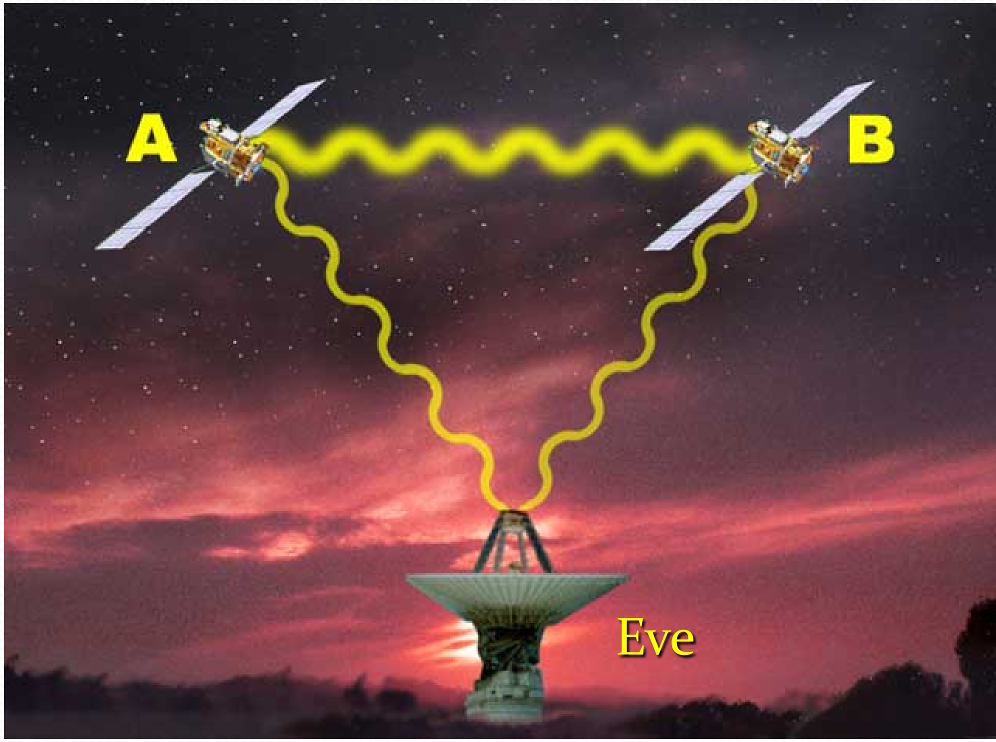
When a photon passes through the correct filter, its polarization does not change.

When a photon passes through the incorrect filter, its polarization is modified randomly.

SOURCE: NORTHWESTERN UNIVERSITY

Entanglement-based protocols BBM92

- Alice (or Eve) prepares an EPR pair
  - $|\Psi\rangle_{AB} = |00\rangle + |11\rangle$
  - Alice and Bob each measures one half of the pair
- Z basis measure (bit)
  - $|0\rangle$ or $|1\rangle$
- X basis measure (phase)
  - $|0\rangle + |1\rangle$ or $|0\rangle - |1\rangle$



Lo-Chau security proof I

- Lo and Chau, 1999
- Entanglement distillation
  - Distill perfect EPR pairs from imperfect ones
  - Bell basis: |00>+|11>, |01>+|10>, |00>-|11>, |01>-|10>
  - Objective: |00>+|11>
- Bit errors (Z)
  - |01>+|10>
- Phase errors (X)
  - |00>-|11>
- Both bit and phase errors (Y)
  - |01>-|10>

Lo-Chau security proof II

- Bit error correction (Z: 0,1)
  - Bit errors: |01>+|10> and |01>-|10>
  - After bit error correction: |00>+|11> or |00>-|11>
- Phase error correction (X: +,-)
  - Phase errors: |00>-|11> or |01>-|10>
  - After phase error correction: |00>+|11> or |01>+|10>
- Share (almost) pure EPR pairs
  - |00>+|11>
- Measure in Z basis to get final key
  - Almost perfect privacy (randomness)
- Security: think of teleportation

Shor-Preskill security proof I

- Shor and Preskill, 2000
- Problem with Lo-Chau proof
  - Requires quantum computers
- Reduce to prepare-and-measure schemes
- Put the final key measurement ahead before error corrections
  - Commute operations in quantum mechanics
- Error correction: classical methods
- Privacy amplification: key point of all security proofs

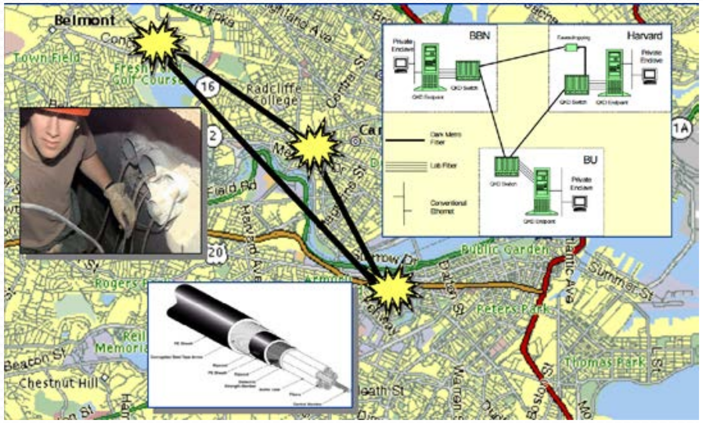
Shor-Preskill security proof II

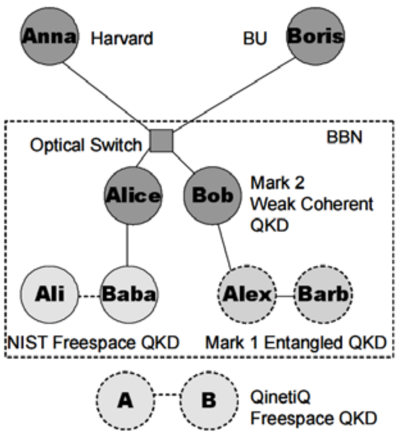
- Bit error correction becomes regular error correction
  - Enables Alice and Bob shares identical keys
  - H(bit error rate): Shannon entropy
- Phase error correction becomes privacy amplification
  - Enables Alice and Bob shares private keys
  - H(phase error rate): Shannon entropy
- Final key rate
  - 1-H(bit error rate)-H(phase error rate)
- Symmetry of BB84
  - Between X and Z basis
  - Basis-independent source: bit error rate=phase error rate
- 1-2H(QBER)
  - Not optimal: can be enhanced by two-way LOCC

Some developments in quantum crypto

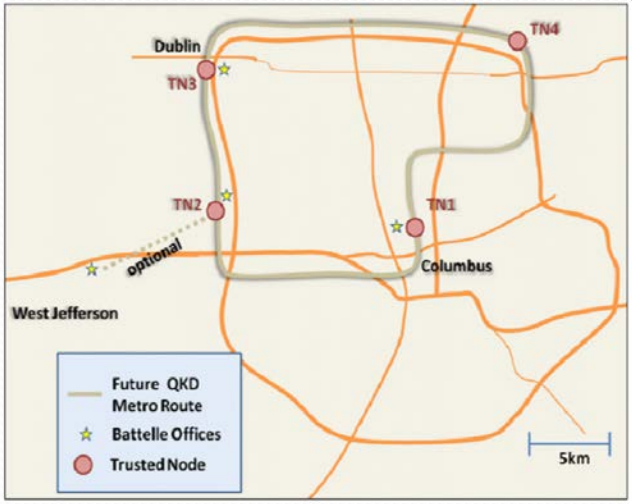
USA QKD network

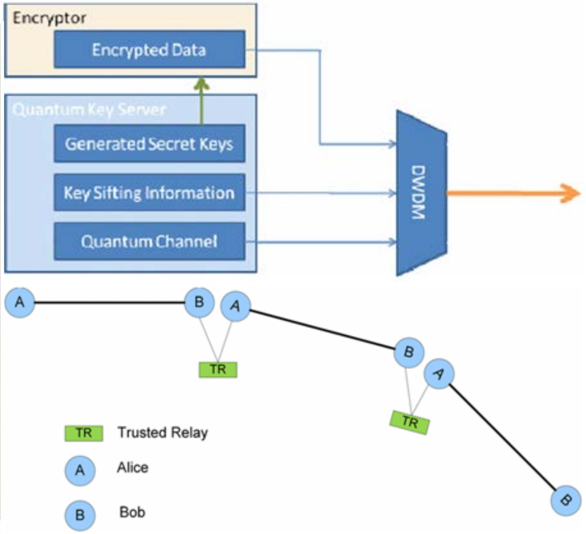
- DARPA
- Battelle
- Smart grid





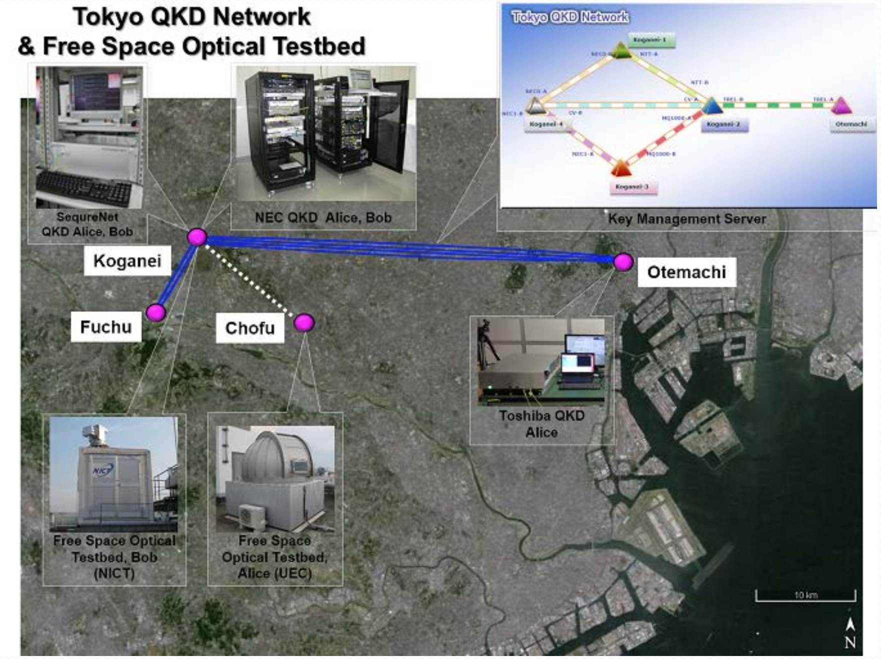
First field test of QKD network (2004)





Japan: Tokyo network

- The Tokyo QKD network is constructed in a part of the NICT open test-bed network "Japan Giga Bit Network 2 plus“ by the project teams consisting of nine research group from Japan and Europe

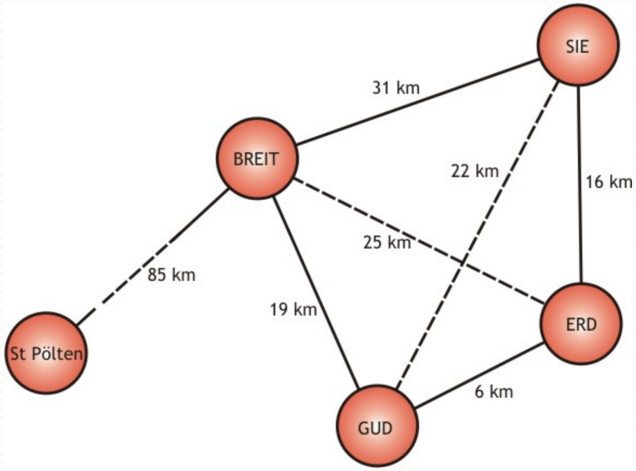


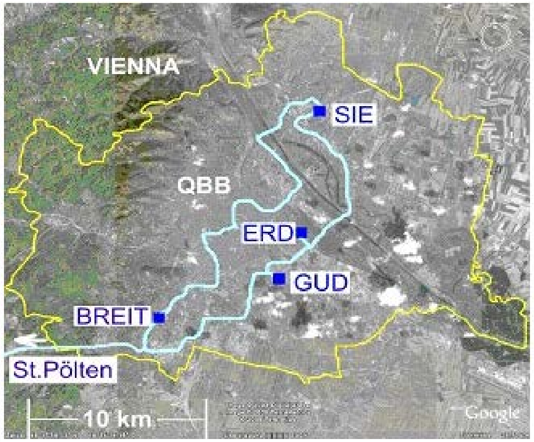
(2015)

Europe SECOQC

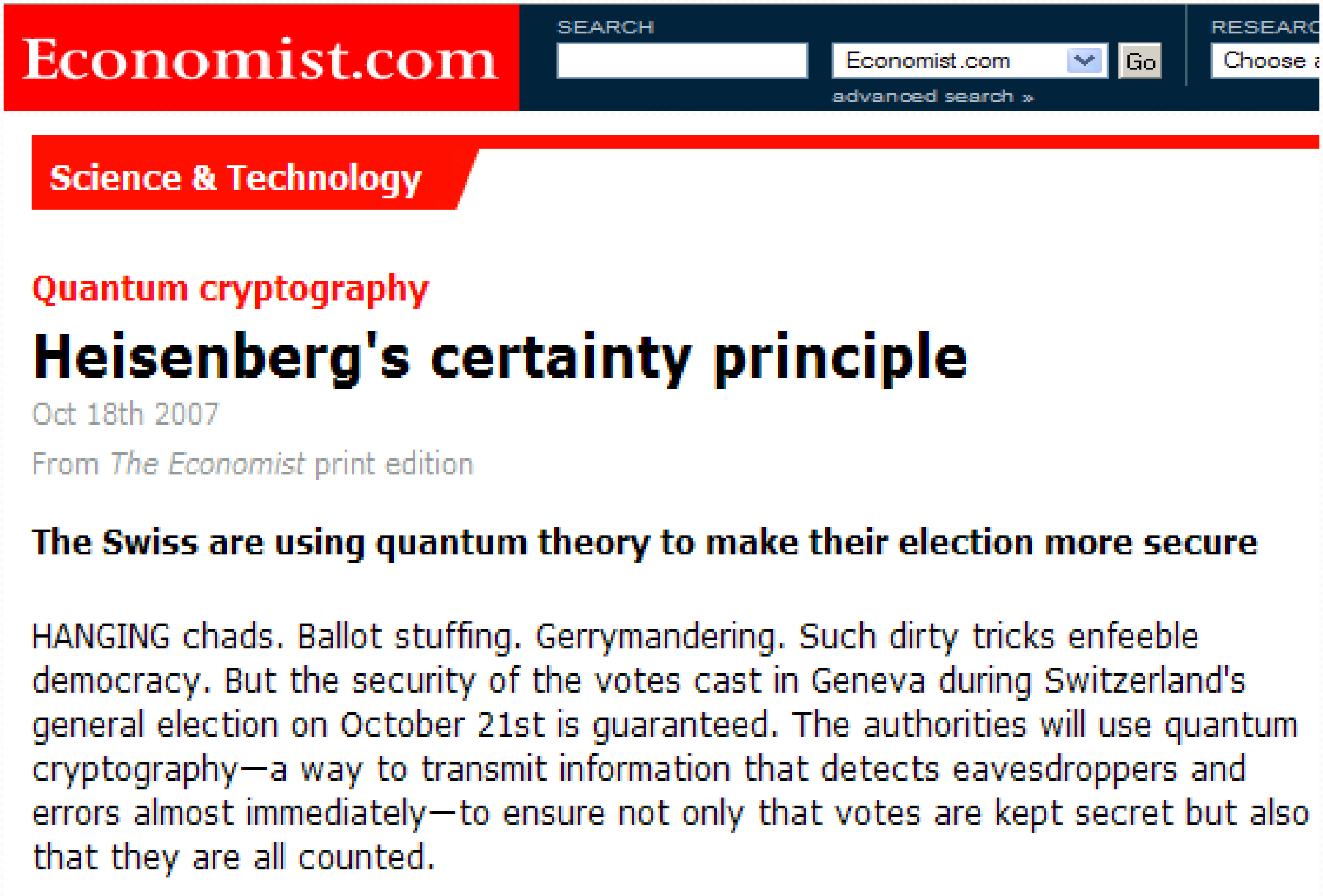
SECOQC

- Focused on development of a global network for secure communication based on quantum cryptography (2008)





Swiss election uses quantum cryptography



Science & Technology

Quantum cryptography

Heisenberg's certainty principle

Oct 18th 2007

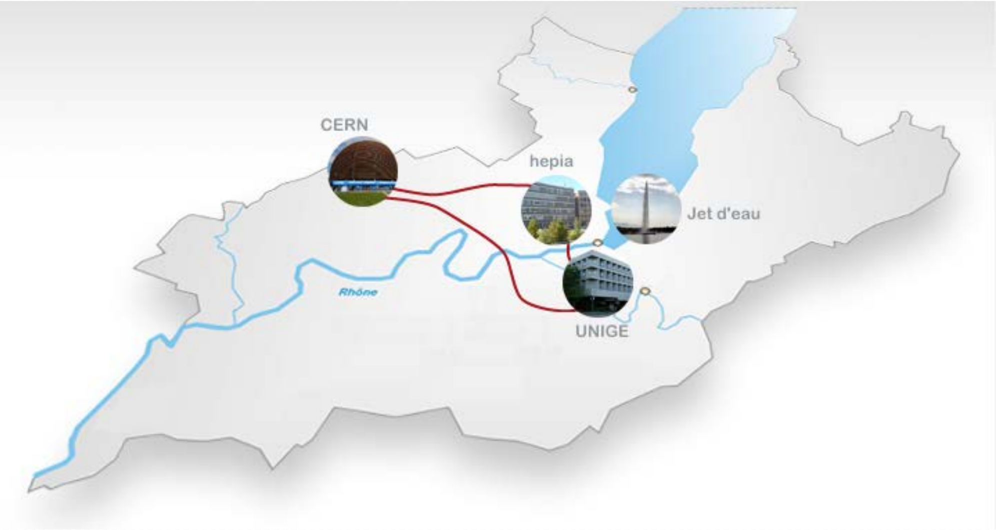
From *The Economist* print edition

The Swiss are using quantum theory to make their election more secure

HANGING chads. Ballot stuffing. Gerrymandering. Such dirty tricks enfeeble democracy. But the security of the votes cast in Geneva during Switzerland's general election on October 21st is guaranteed. The authorities will use quantum cryptography—a way to transmit information that detects eavesdroppers and errors almost immediately—to ensure not only that votes are kept secret but also that they are all counted.

Switzerland Geneva network

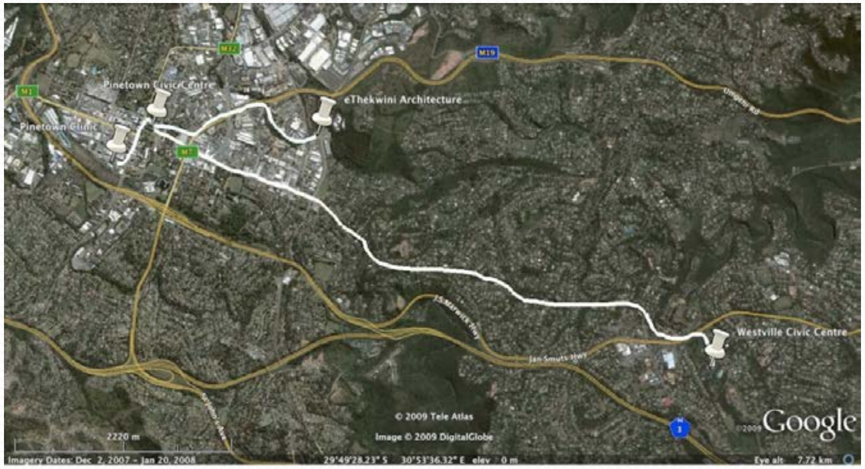
- N. Gisin



(2009)

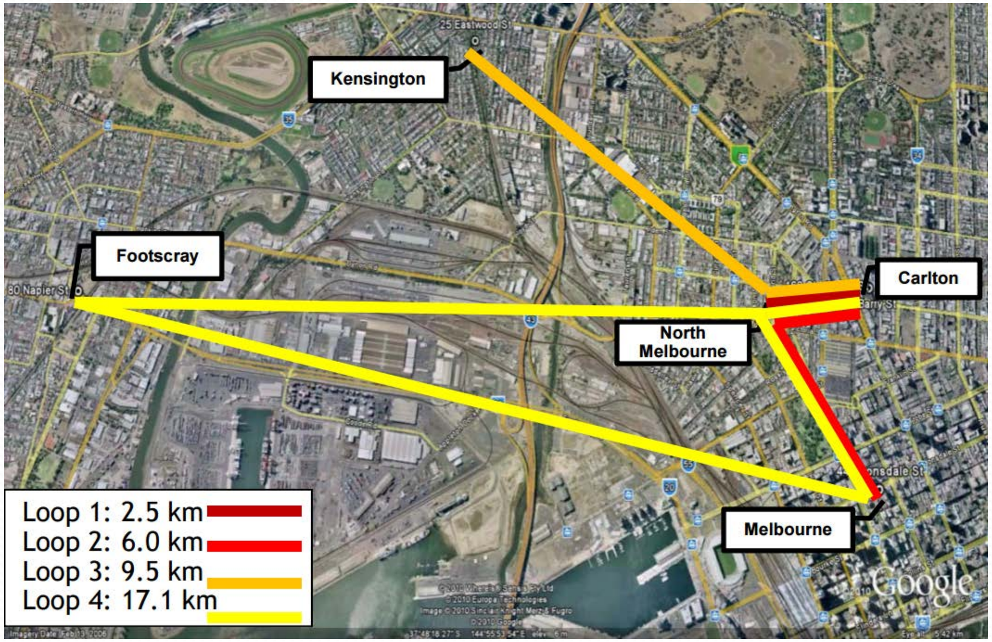
South Africa Durban Quantum Network

- Distance 2.6 km~27 km
- First Quantum Network in Africa (2009)



Melbourne Quantum Network

- Melbourne established commercial Quantum Network
- Establish the network between space and ground Collaborate with NASA / JPL



(2010)

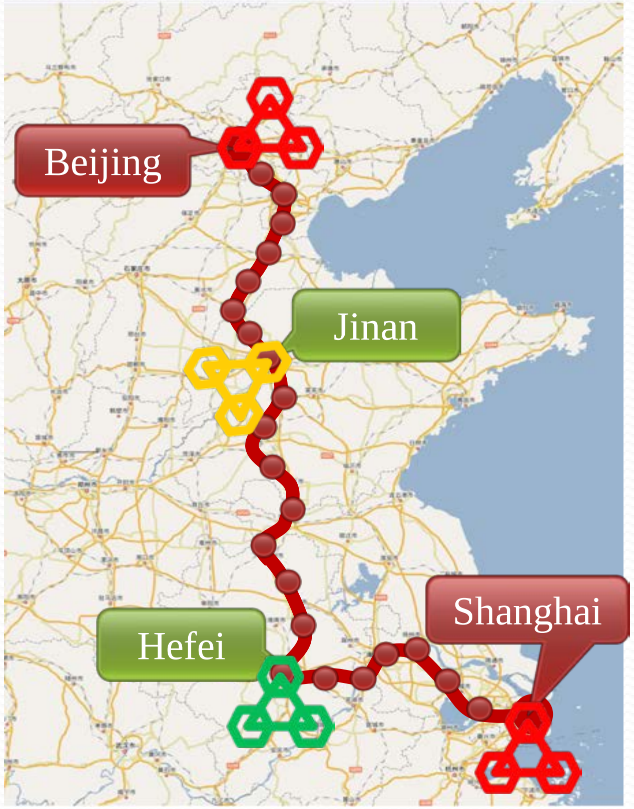
China’s Quantum Secure Backbone project

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes

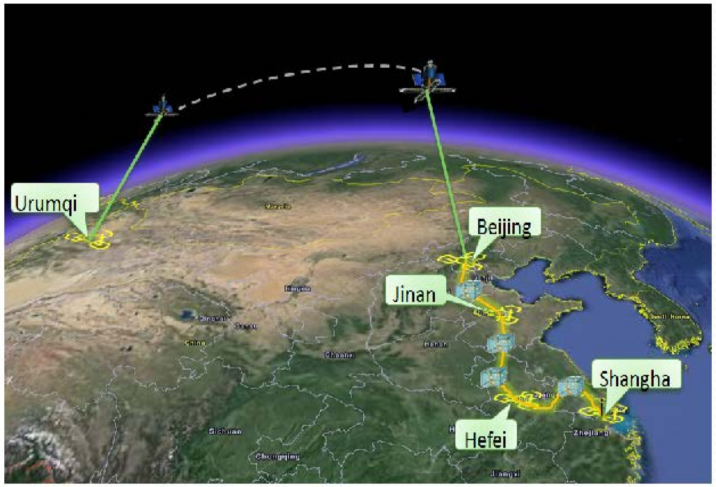
  31 fiber links
- Metropolitan networks

  Existing: Hefei, Jinan

  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; China Banking Regulatory Commission …
- GDP 35.6% ($3 trillion)
- Population 25.8% (0.3 billion)

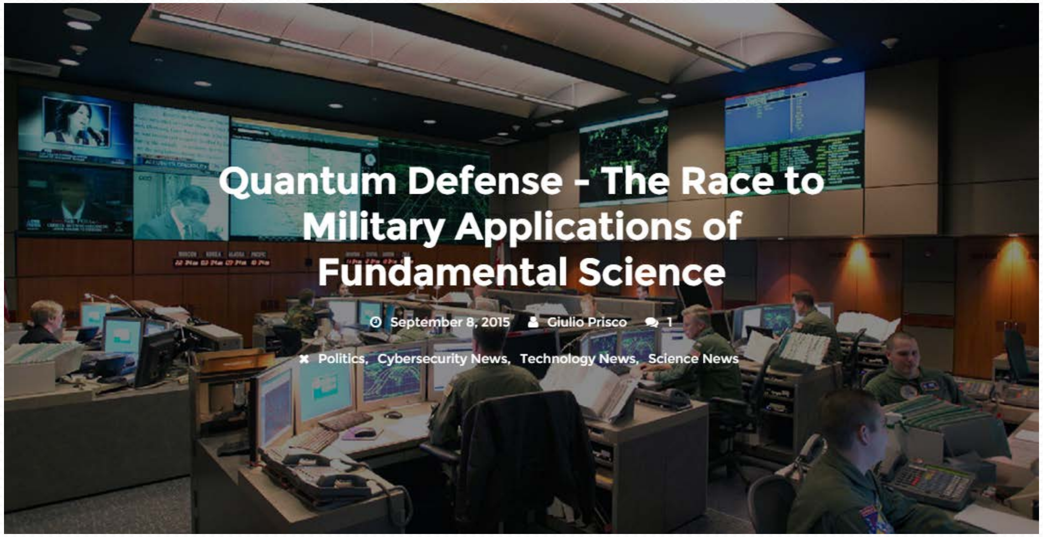


Quantum Satellite



First quantum satellite, “Mozi”
1:40am, August 16, 2016

The race between US and China



Quantum Defense - The Race to Military Applications of Fundamental Science

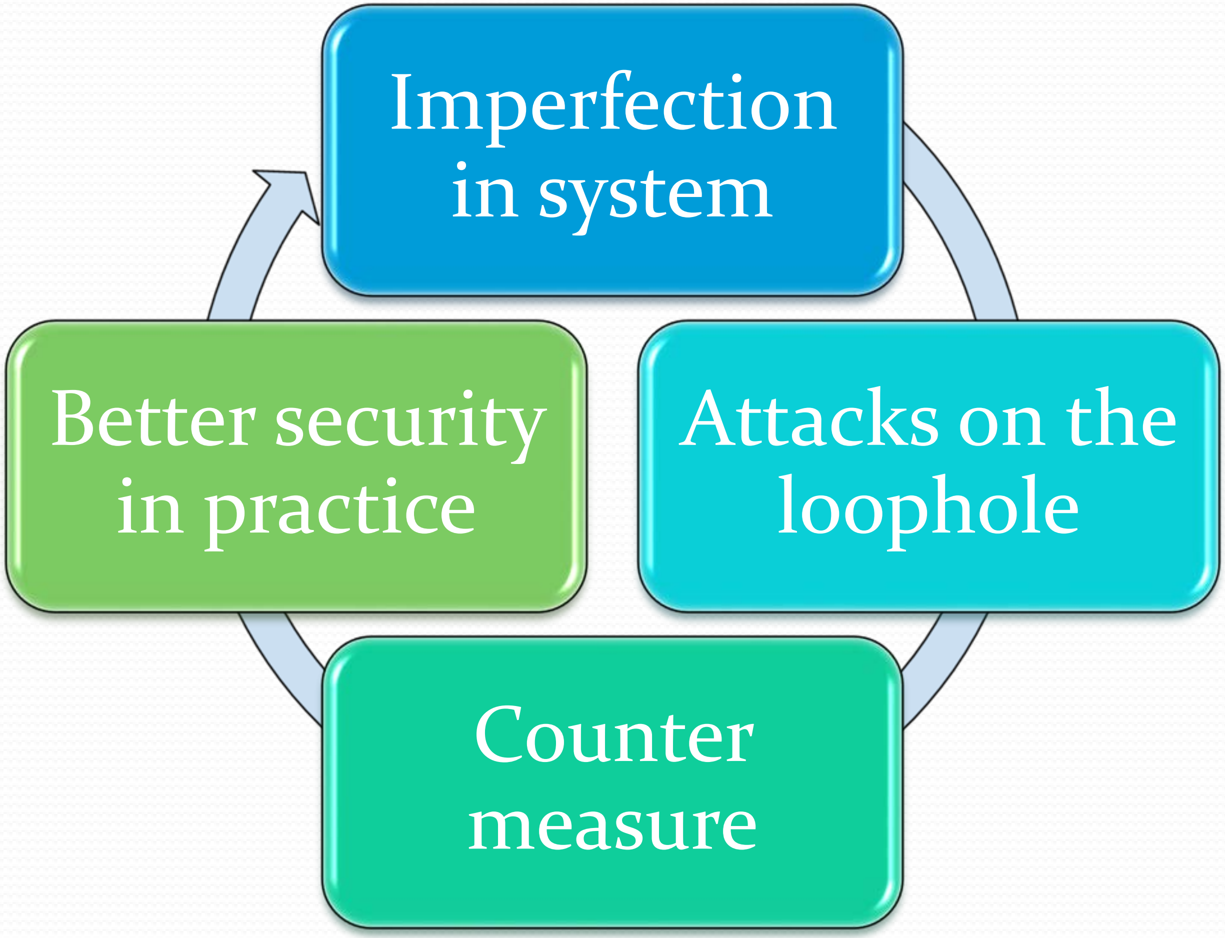
September 8, 2015 Giulio Prisco 1

Politics, Cybersecurity News, Technology News, Science News

Unbreakable communication security, and quantum supercomputers much more powerful than today's machines. As usual, the race is between the US and China.

Measurement-device-independent QKD (MDIQKD)

Objective for hacking


Imperfection in system

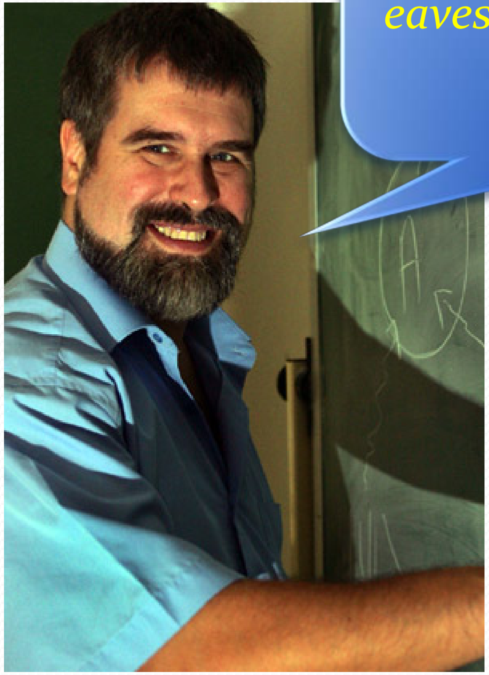
Attacks on the loophole

Counter measure

Better security in practice

Side information

- Basis (or bit) information may be contained in other degrees of freedom
  - Timing of the pulse
  - Frequency
- Source
  - Multi photons
  - Decoy state
  - Phase randomization
- Loopholes in detection
  - Gated detectors
  - Polarization sensitive
  - Deadtime



… was unconditionally secure against any eavesdropper who happened to be deaf!

G. Brassard, IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, pp.19 (2005) arXiv:quant-ph/0604072

QKD scenario

- The channels are not sure, but Alice and Bob’s labs are
  - Alice and Bob characterize their devices well and trust them

Alice

00111010100…

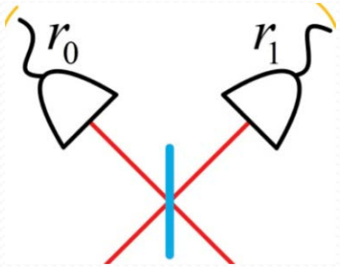
Bob

00111010100…

- What if Alice and Bob are not too sure about the devices?
  - For instance, the products are bought from the market ar built up by unknown manufacture

Question from practical side

- Detection efficiency mismatch
  - The numbers of 0's and 1's are different
- Time-shift attack



A typical measurement with two detectors

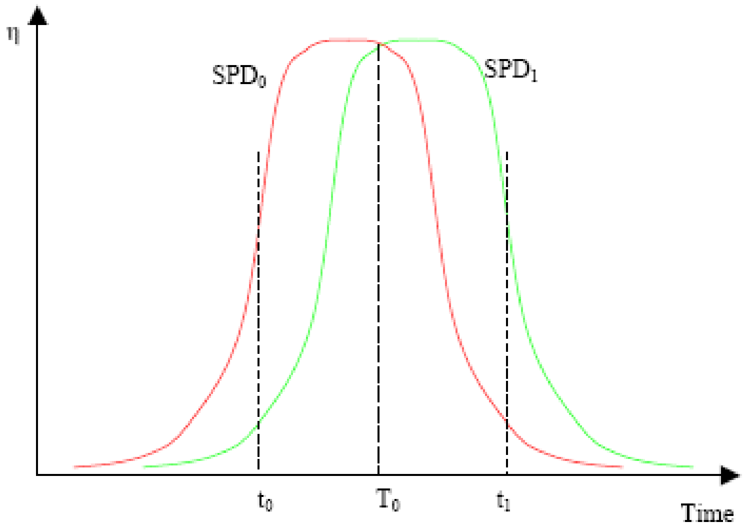


Fig. 1. The time-dependence efficiencies of SPDs.

Detection device-independent QKD

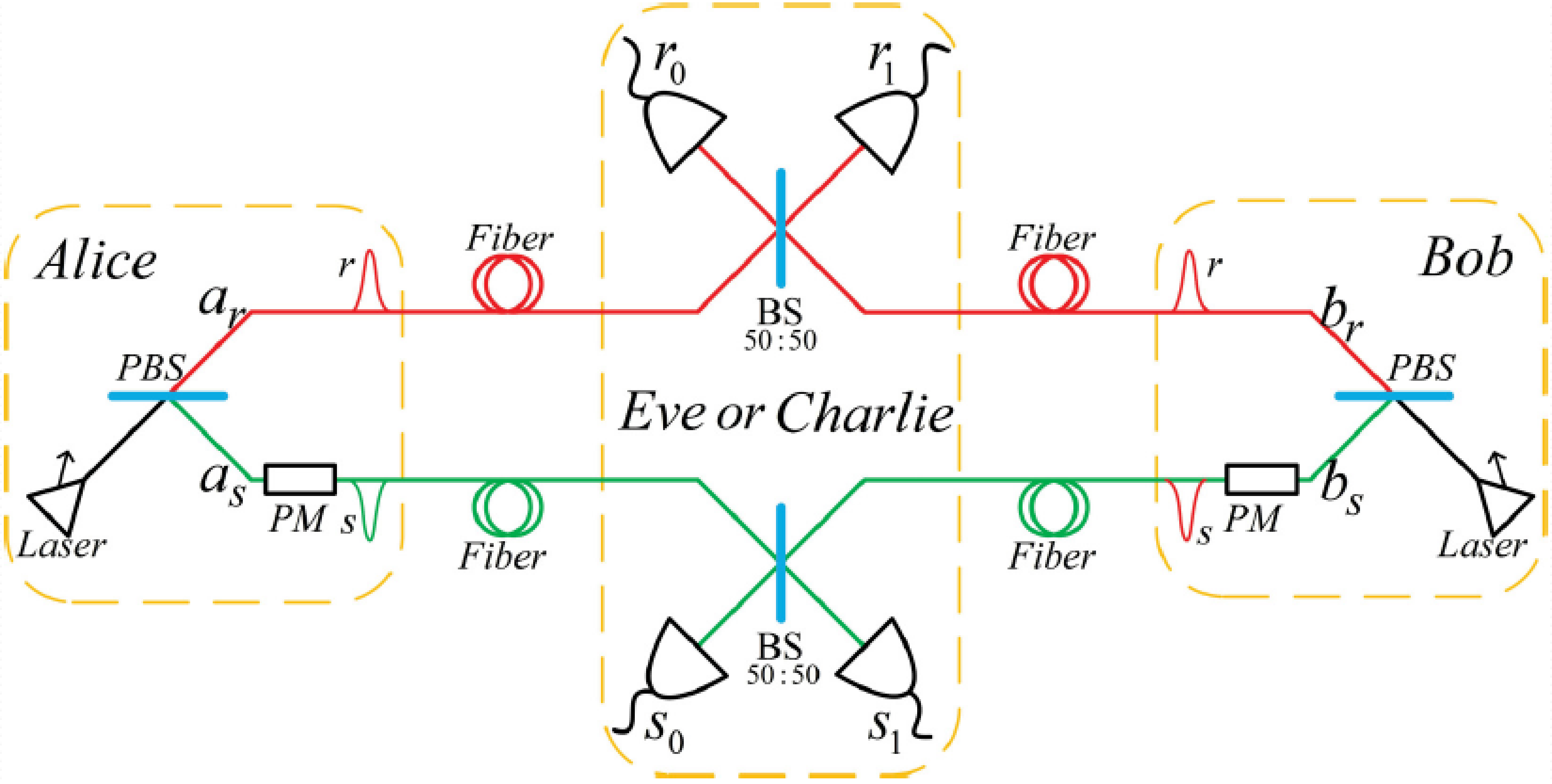
- Random assignment for no clicks
  - Detection efficiency: 65.9%
  - Error tolerance: 11%
- Partially self-testing schemes
- Experimental realization
  - Minimum requirements

X. Ma, T. Moroder and N. Lütkenhaus, arXiv:0812.4301, (2008).
X. Ma and N. Lütkenhaus, Quant. Info. Comp. 12, 0203 (2012).

MDIQKD

- Alice randomly chooses bit {0,1} and basis {X, Z} and sends the state to an untrusted party, could be Eve
  - The source is the same as BB84
- Bob does the same
- Eve projects the two qubits into one of four Bell states
  - Bell state measurement (BSM)
- Eve announces the BSM results
- Alice and Bob run postprocessing
- Security relies on a “time-reversed” EPR distribution QKD protocol (BBM92)

MDIQKD



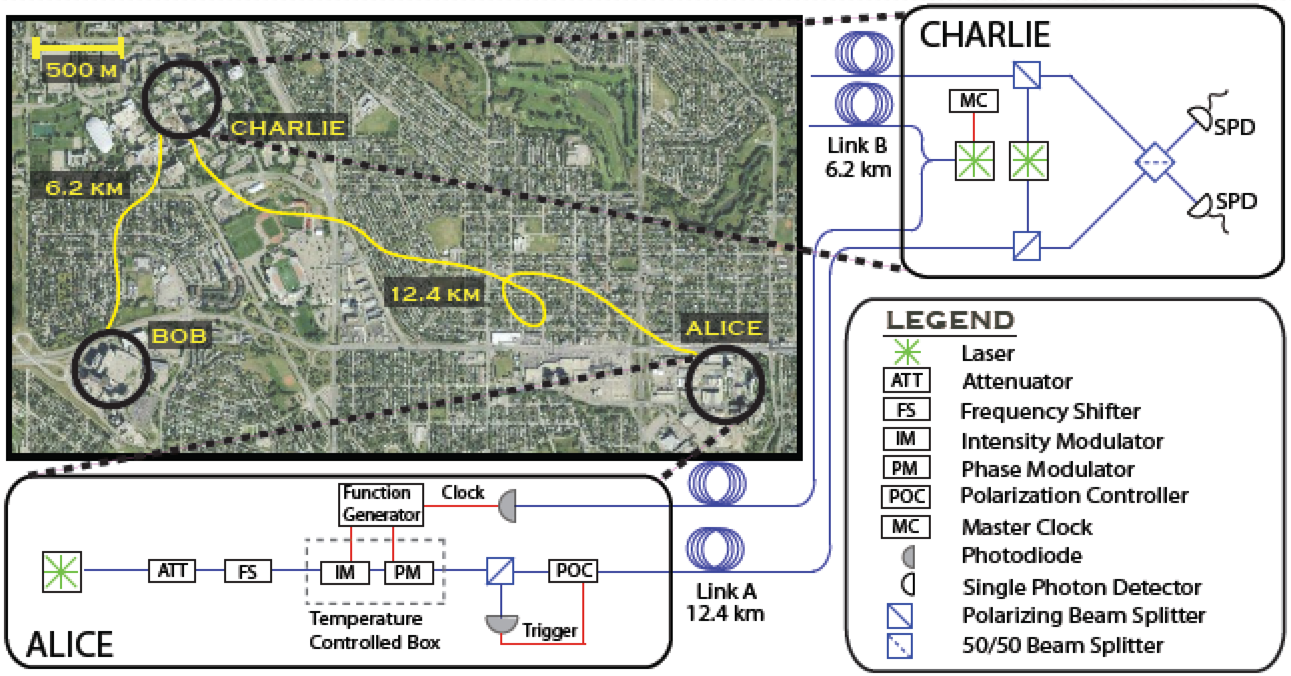
H.-K. Lo, M. Curty and B. Qi, PRL 108, 130503 (2012).
X. Ma, C.-H. F. Fung and M. Razavi, PRA 86, 052305 (2012)
X. Ma, and M. Razavi, PRA 86, 062319 (2012)

Key advantages

- Measurement device independent
  - The measurement devices are assumed to be held by an untrusted party
- Two quantum channels
  - Like entanglement based protocol, the effects of background counts can be reduced

Field test

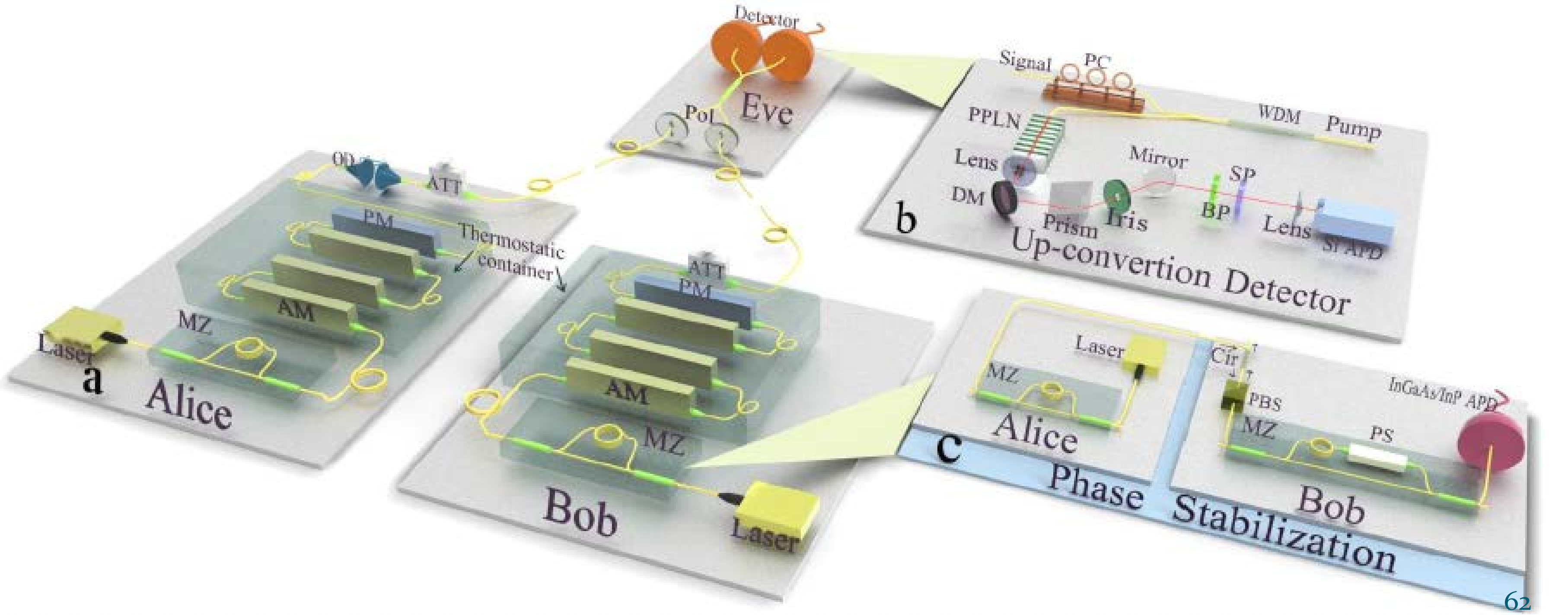
- Calgary: W. Tittel's group
  - Rubenok et al., Phys. Rev. Lett. 111, 130501 (2013).



Implementation

APS Highlights of the Year 2013

- Shanghai
  - Liu et al., Phys. Rev. Lett. 111, 130502 (2013)
  - 60 hour experiment: 25 kbit secure key over a 50 km



MDIQKD over 200km fiber

- Y.-L. Tang, et al., “Measurement-Device-Independent Quantum Key Distribution over 200 km”, PRL 113, 190501 (2014)

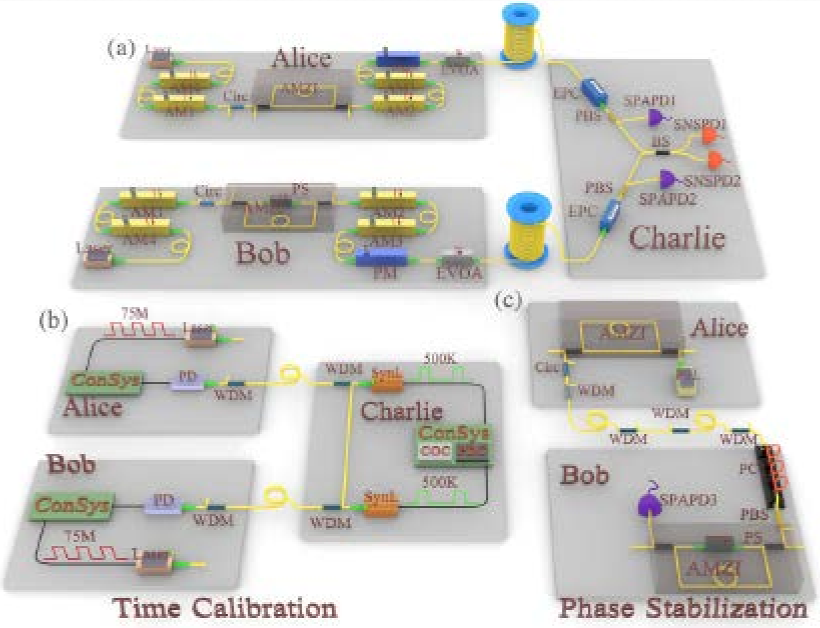
两院院士评选
2014中国十大科技进展新闻
入选纪念

量子通信安全传输创世界纪录

a

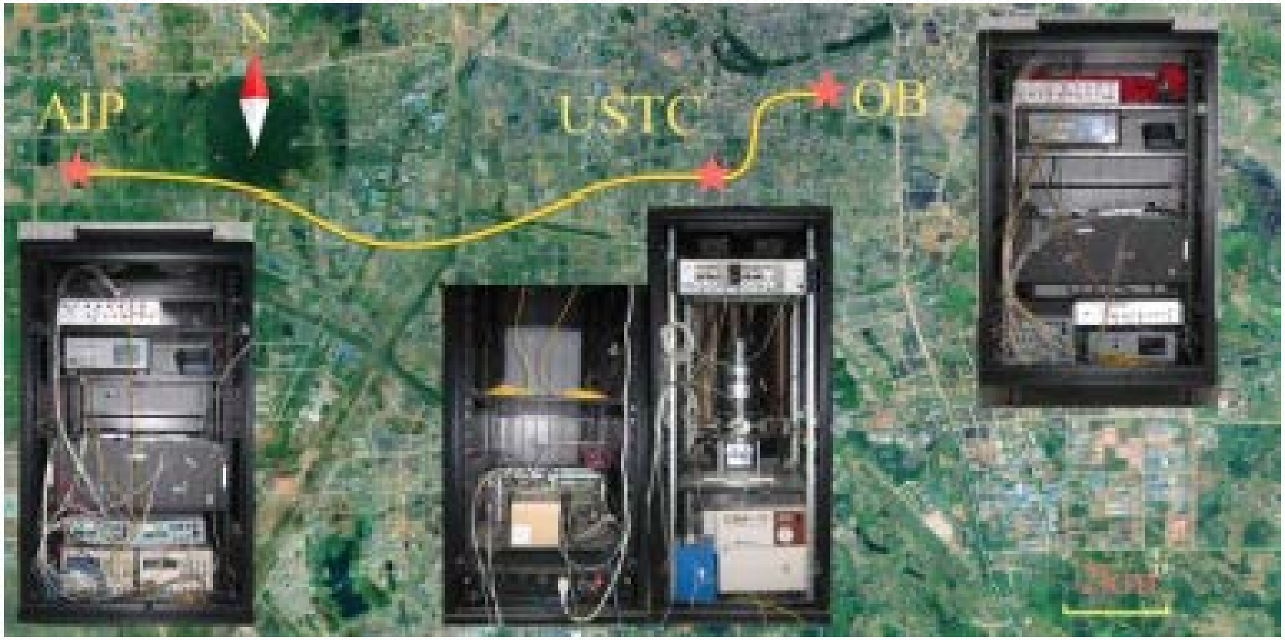
b

主办：中国科学院 中国工程院
承办：中国科学院学部工作局
中国工程院办公厅
中国科学报社



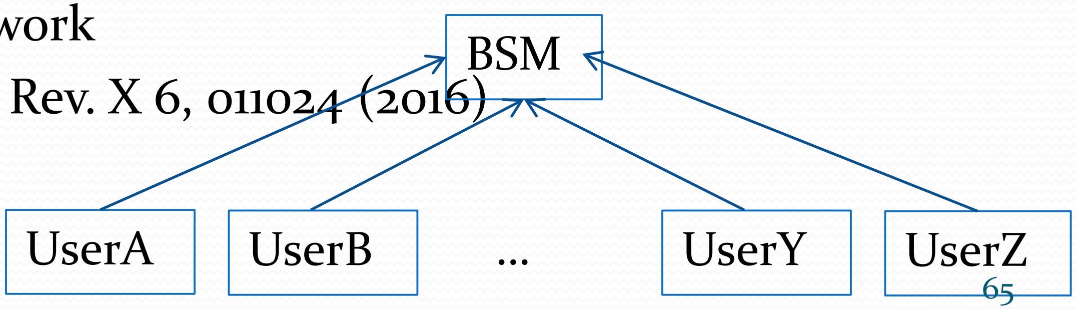
Full field test of MDIQKD

- Y.-L. Tang, et al., “Field Test of Measurement-Device-Independent Quantum Key Distribution”, IEEE Journal of Selected Topics in Quantum Electronics, 21, 1, 1077-260X (2014)



Untrusted relay network

- Detection devices are normally much more expensive than sources
  - Users only need to purchase cheap source devices
  - All users hold the same source devices
- Memories can be added to the relay to enhance the performance
  - C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus, New Journal of Physics 16 (2014) 043005
  - S. Abruzzo, H. Kampermann, D. Bruß, Phys. Rev. A 89, 012301 (2014)
- Implemented for regular QKD
  - Fröhlich, et al., Nature 501, 69-72 (2013)
- Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network
  - Yan-Lin Tang, et al., Phys. Rev. X 6, 011024 (2016)


BSM
UserA
UserB
…
UserY
UserZ