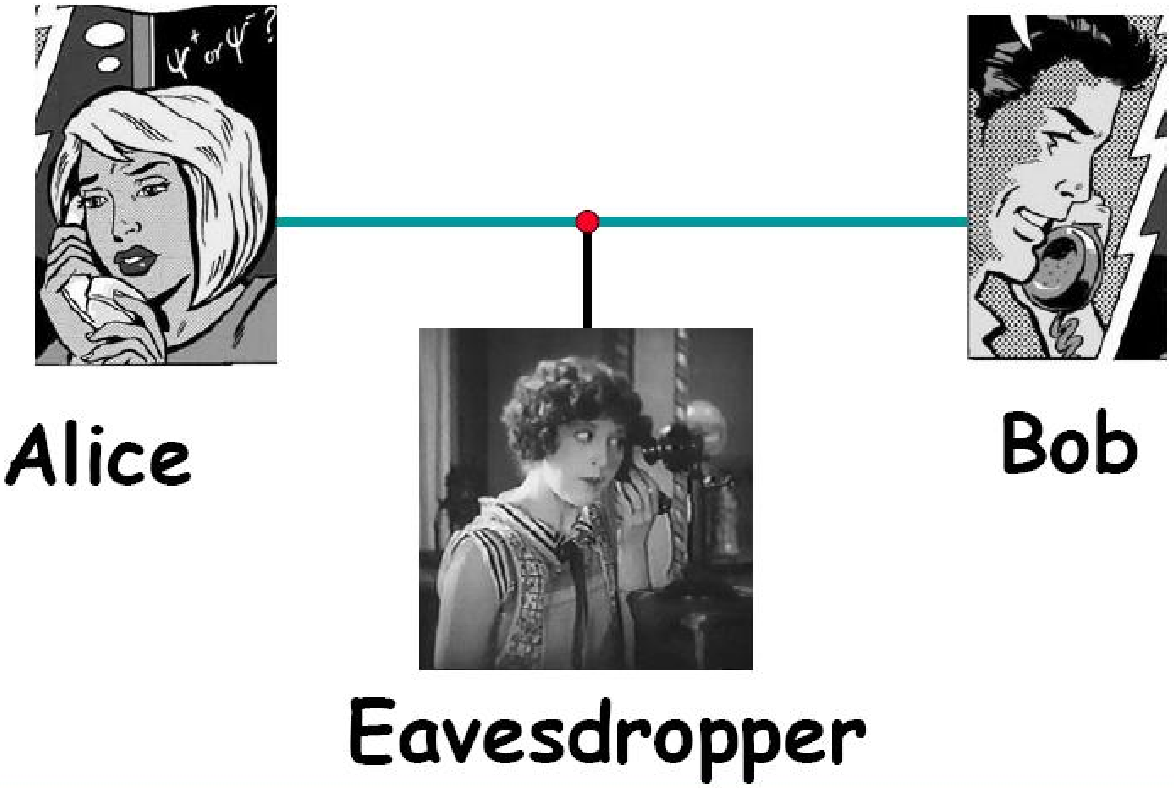
Lecture Note 2

Quantum Cryptography

Jian-Wei Pan

http://quantuminformation.physi.uni-heidelberg.de/

Scenario



Alice

Bob

Eavesdropper

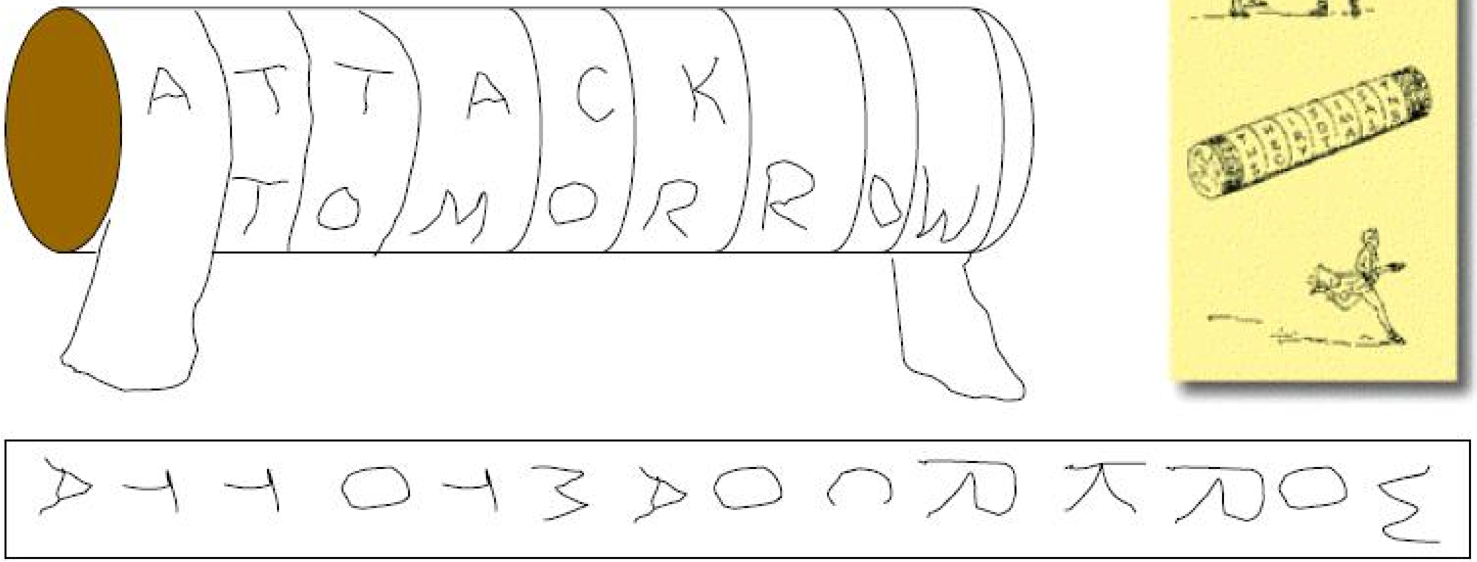
"Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve..."

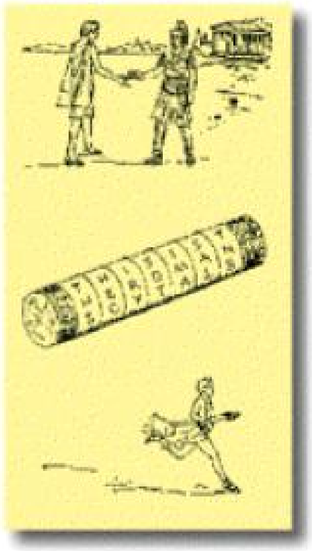
Edgar Alan Poe - "A few words on secret writing"; 1841

Archaic Cryptography
----Permutation

Scytale

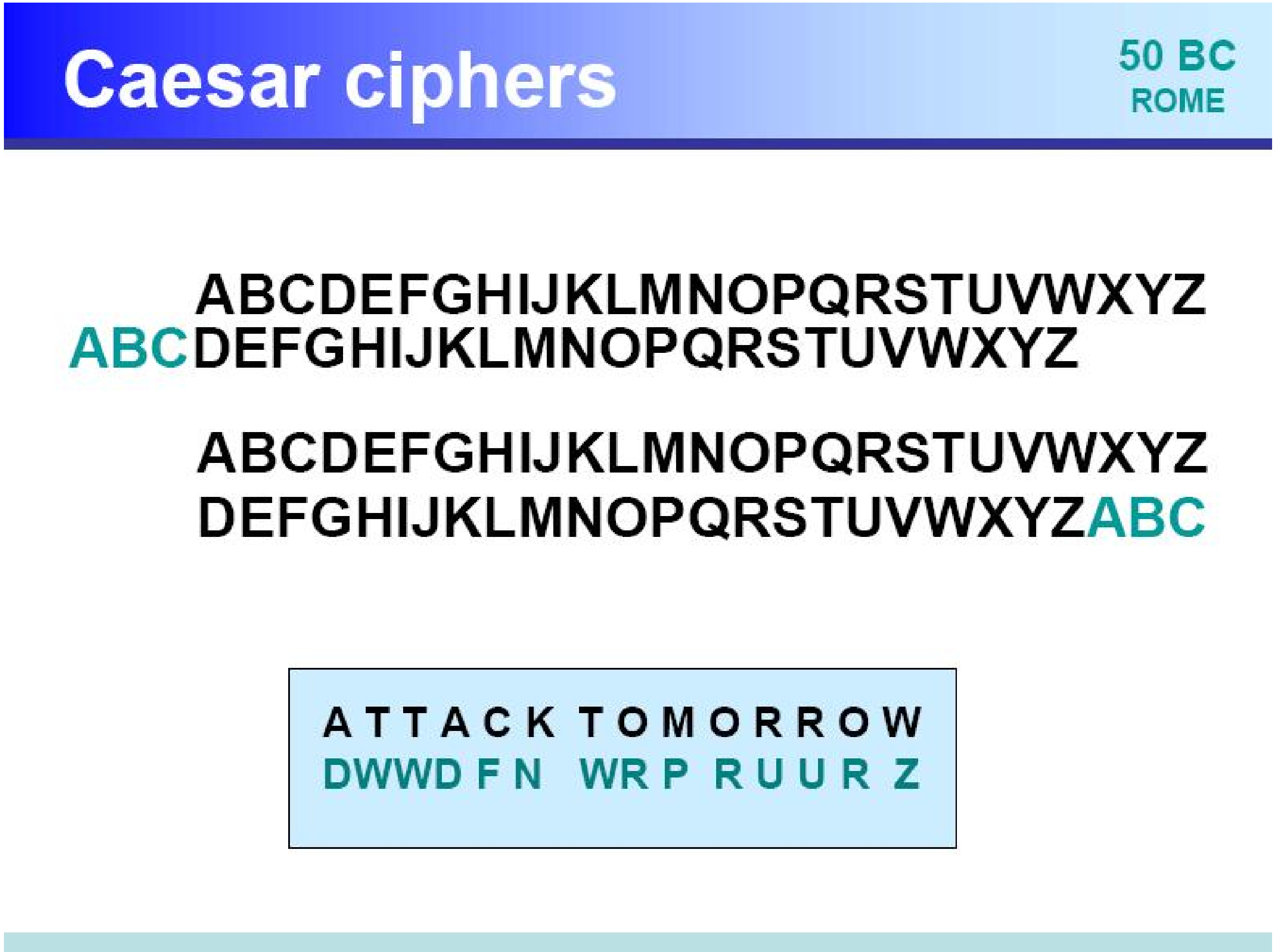
400 BC
SPARTA





Permutation of characters

Archaic Cryptography ----Substitution



Caesar ciphers

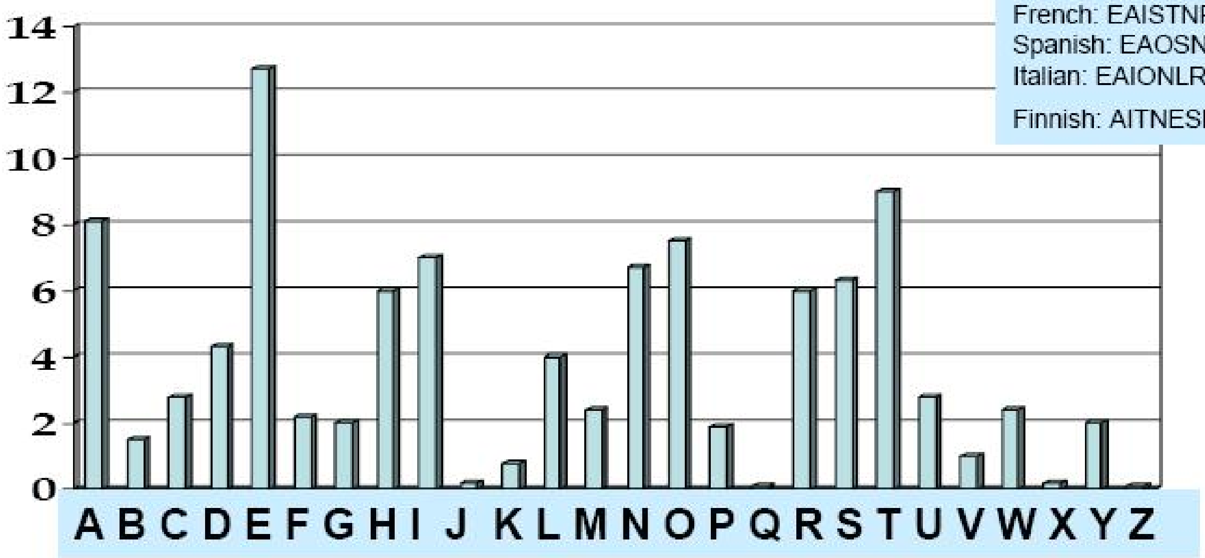
50 BC
ROME

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

ATTACK TOMORROW
DWWDFN WRPRUURZ

Frequency Problem

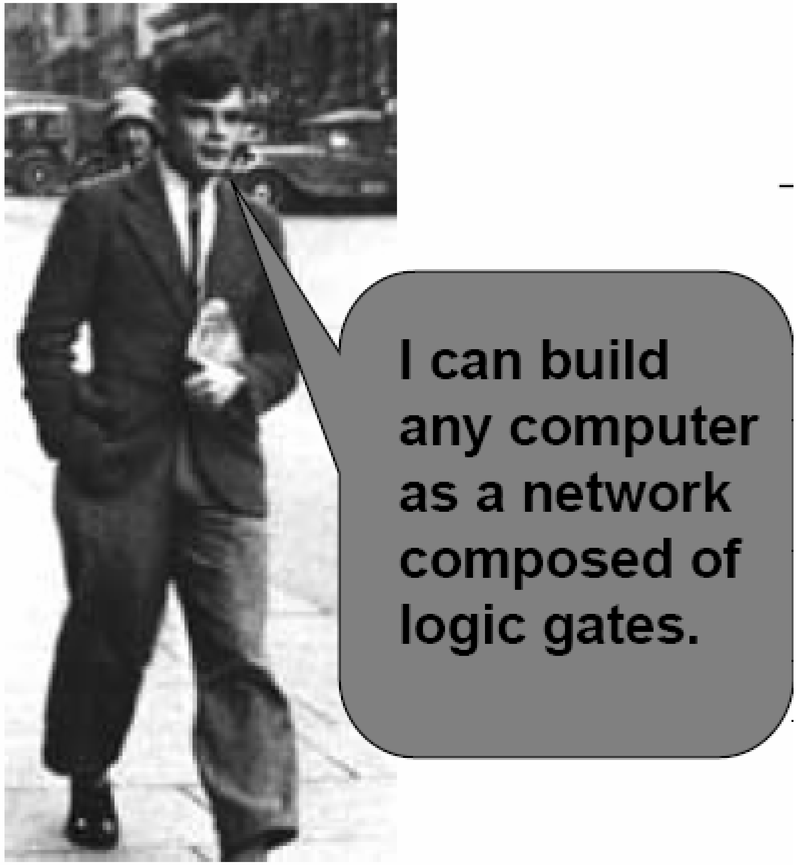


English: ETAOINSH
German: ENIRSATU
French: EAISTNRUL
Spanish: EAOSNRIL
Italian: EAIONLRTS
Finnish: AITNESLOK

Frequency of letters in a typical English text

Baghdad al-kindi

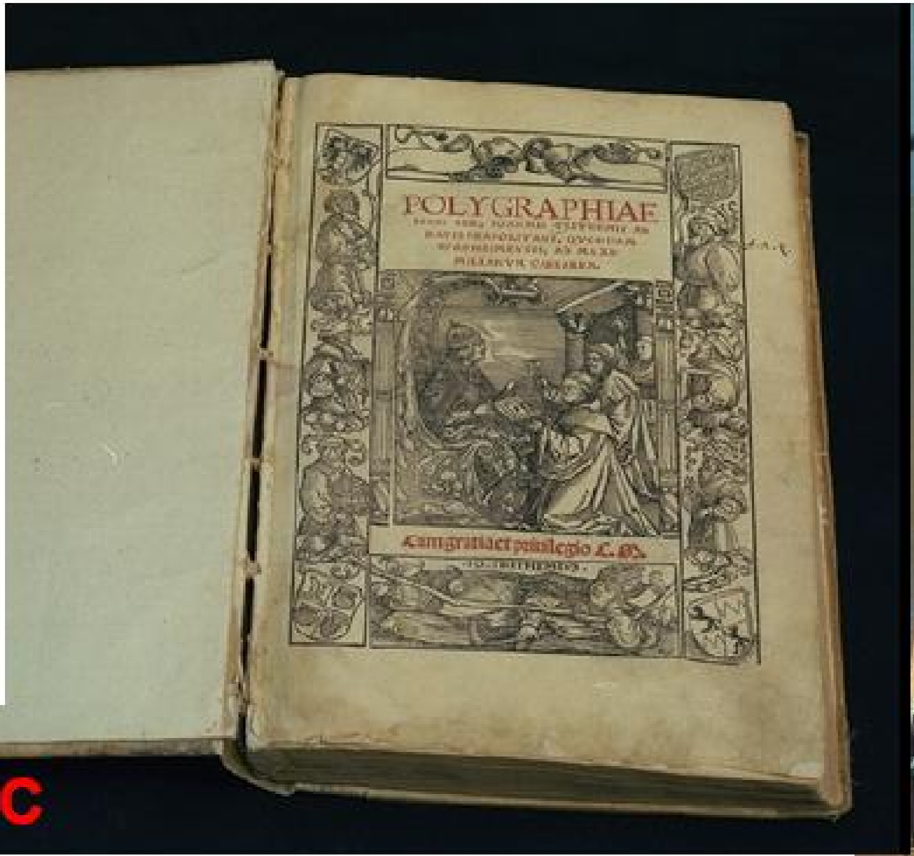
ENIGMA and COLOSSUS


I can build any computer as a network composed of logic gates.

Alan Turing, Cambridge 1935

Is there a perfect cipher?

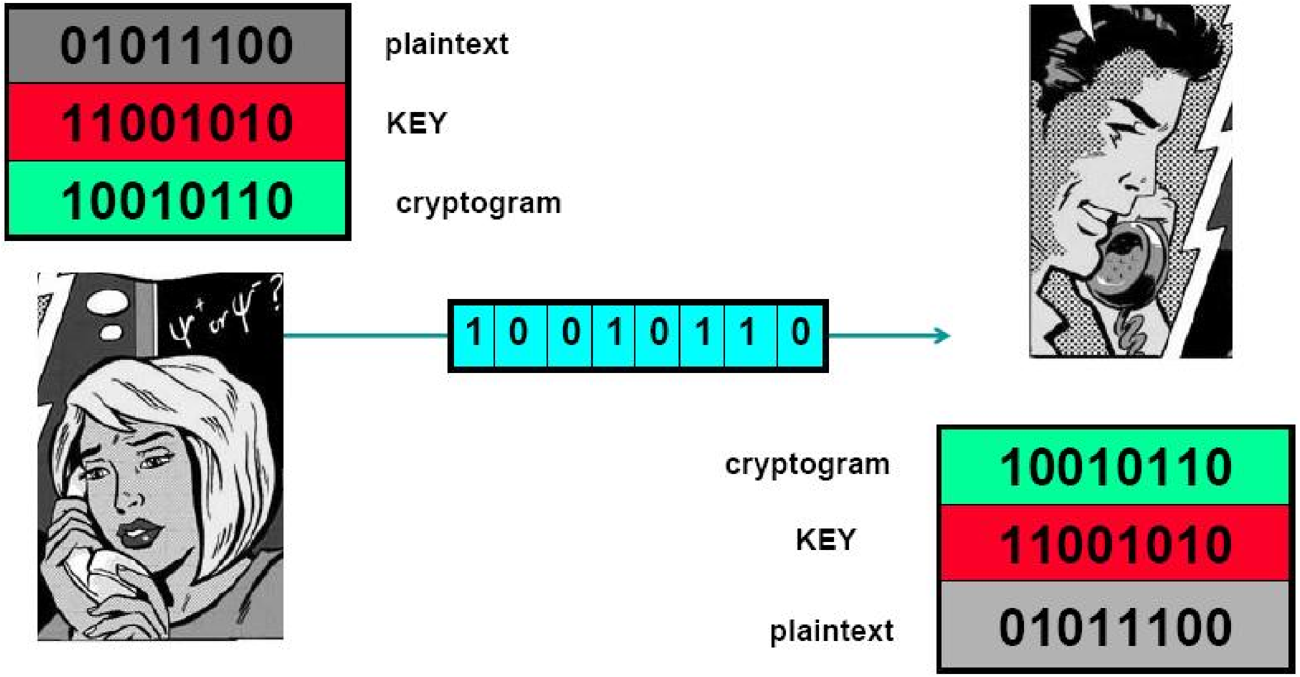
SCYTALE 400BC



POLYGRAPHIAE
1518

ENIGMA 1940

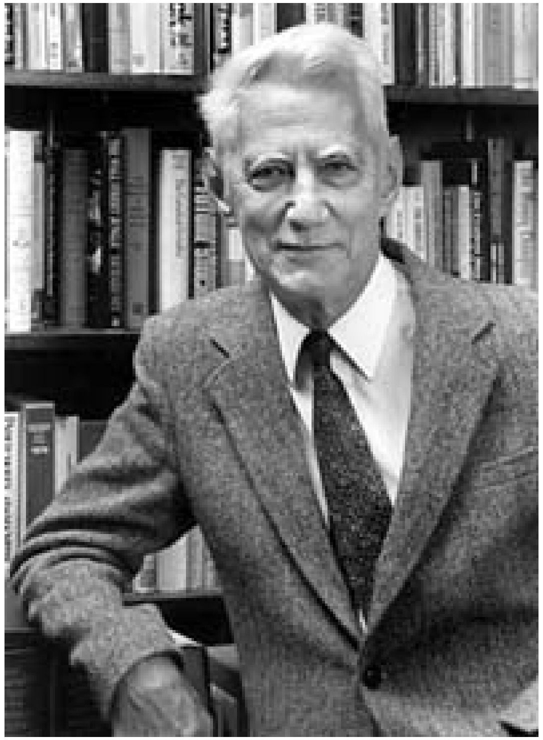
One-time pad



01011100	plaintext
11001010	KEY
10010110	cryptogram

1	0	0	1	0	1	1	0

cryptogram	10010110
KEY	11001010
plaintext	01011100



First Discovered by Gilbert Vernam

Security Proved by Claude Shannon

Bell Syst. Tech. J,28,656 (1949)

Key distribution problem

?

miles away

KEY	0	0	1	0	1	1	0

KEY	0	0	1	0	1	1	0

Public Key (Mathematical)

$$C = E_x (P)$$

$$P = D_k (C) = D_k (E_x (P))$$

X: Public Key; K: Private Key

P: Plain Text; E: Encryption; C: Ciphertext; D: Decryption.

- Based on certain mathematical operations are easier to do in one direction (public key or rule) than the other (without the private key).

- For Example: RSA Cryptosystem, Factor Large Integer

,

$$N = n_1 \times n_2$$

[R. Riverst, A. Shamir and L. Adleman, MIT/LCS/TR-212, Jan. 1979]

The Public Key method is only based on mathematical *assumption!*

- One side, some new decryption in classical cryptography

  [X.-Y. Wang, et al., SHA-0,Crypto 05]

- The other side, Quantum computation

Shor Algorithm makes $\sqrt{N} \Rightarrow \log N$

[P. Shor, Proc. Of 35th Annual Symposium on the Foundations of Computer Science (IEEE Computer Society, Los Alamitos).]

Classical：10 billion years   Quantum：1 minute！

" While quantum computation takes away with one hand, it returns with the other--Quantum Key Distribution!"

A. Ekert, et al., <The physics of quantum information>, 2001

Quantum No-Cloning Theorem

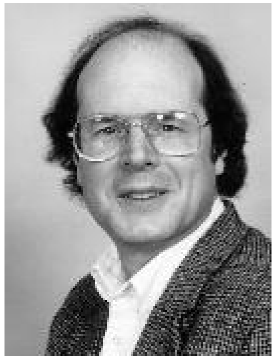
It is not possible to copy two non-orthogonal state together

[W. K. Wootters and W. H. Zurek, Nature 299 (1982), pp. 802-803]

[S. Wiesner, SIGACT News, 15, 78 (1983)]

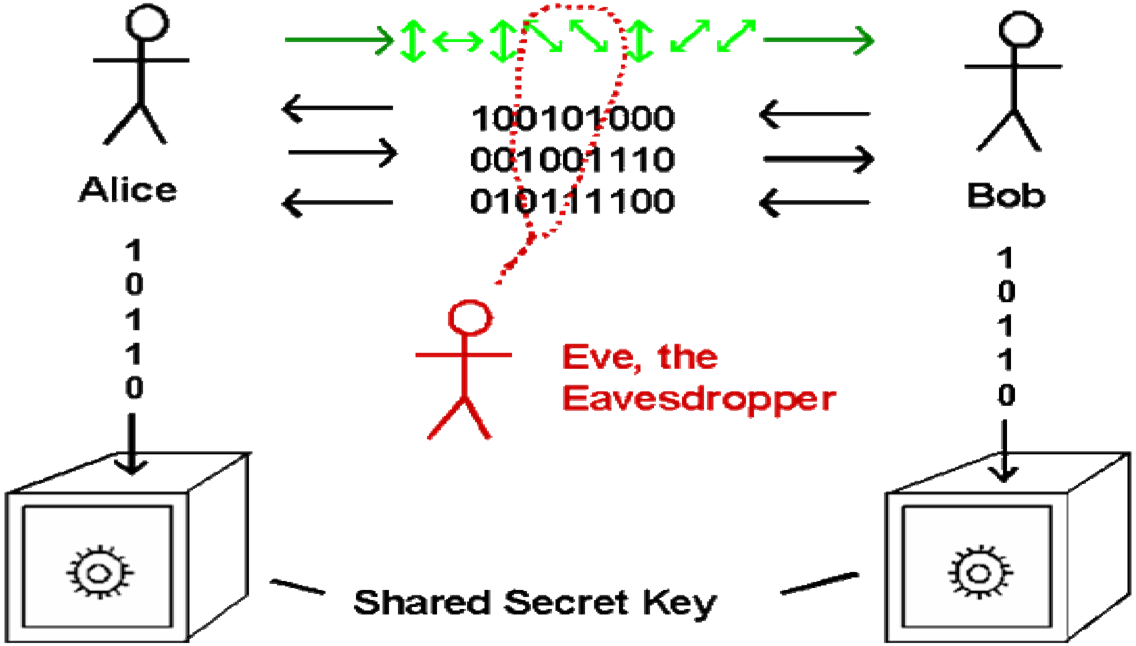
Single Particle Scheme

----Polarization



$$|H\rangle, \quad |+45^{\circ}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right)$$

$$|V\rangle, \quad |-45^{\circ}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right)$$



[C. H. Bennett & G. Brassard, BB84 protocol (1984)]

BB84 Protocol

1. Alice tosses a coin several times and notes out come each time (i.e. generates a random sequence of 0s and 1s.)

2. If it is head she decides to encode using a horizontal/verical basis. If it is a tail, she encodes in 45/135 basis.

3. Each bit is encoded as 0 or 1 in the chosen basis.

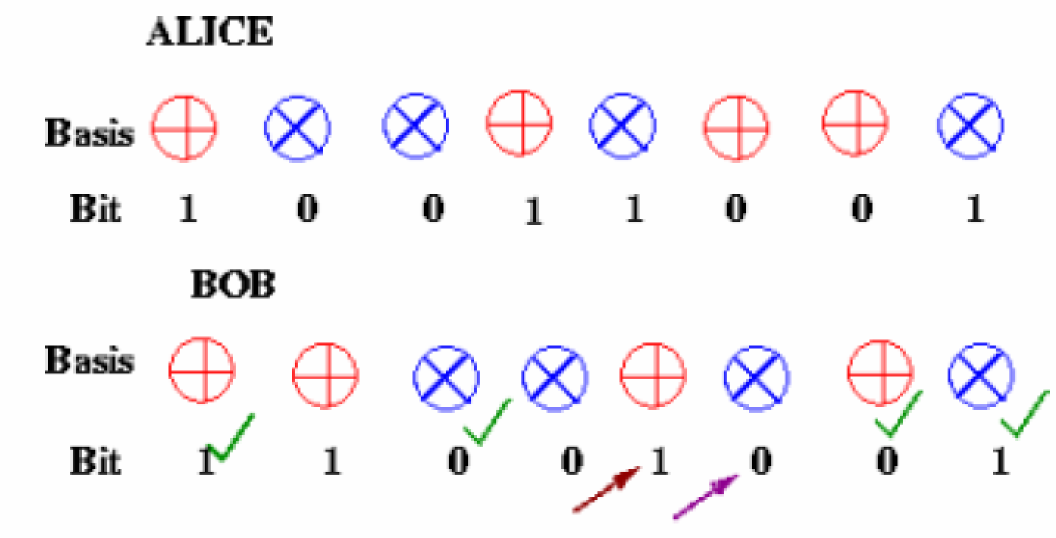
4. Bob receives each bit and does not know the basis used to encode. He also tosses a coin and decides to decode using the basis as decided by coin toss.

5. Half the time Bob's basis will be the same as Alice's in which case the qubit received will be the same provided Eve is not intercepting.

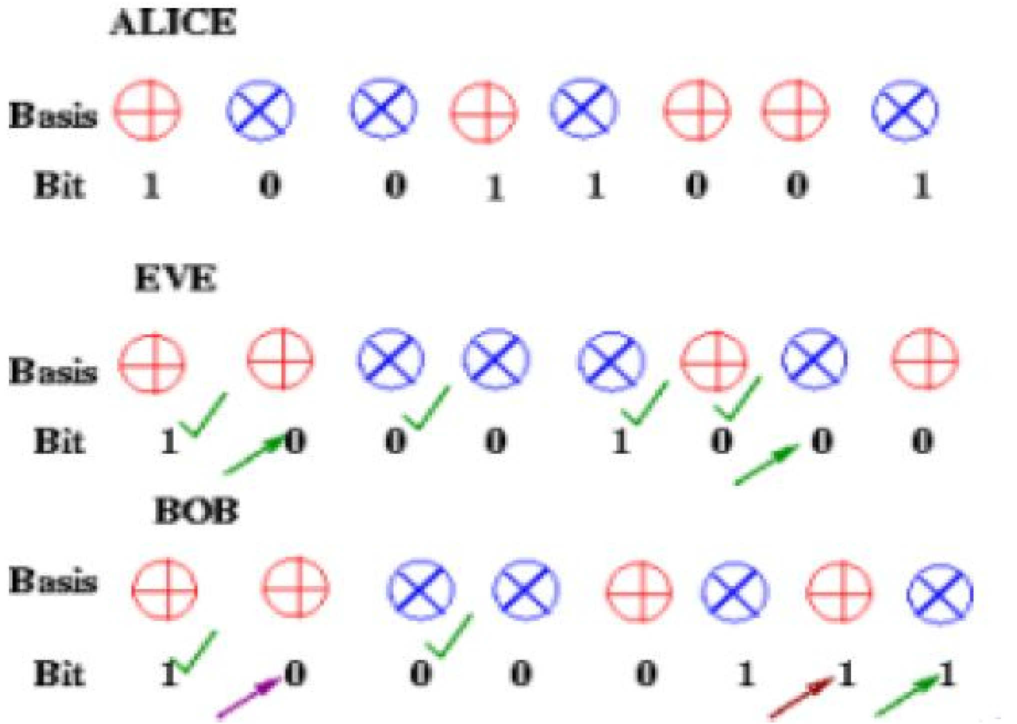
6. Alice now uses a classical channel to announce the basis that she used each time. Bob discards those where the bases are different. The remained bits are called raw key (with an efficiency of 50%).

8. Bob now announces a part of the qubits. Alice can conclude whether an eve is present.

No Eve



With Eve

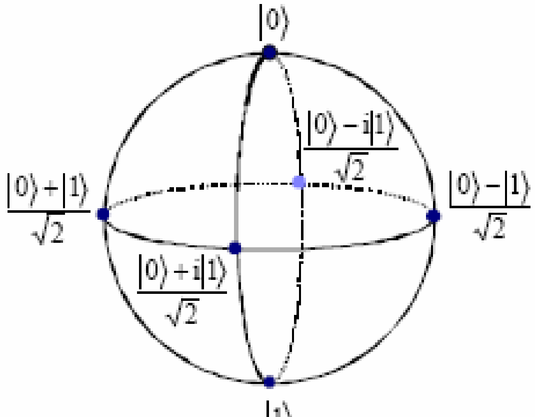


If Eve is present, the probability that Alice and Bob can not find is $(0.25)^N$ after they compare N raw key's value!

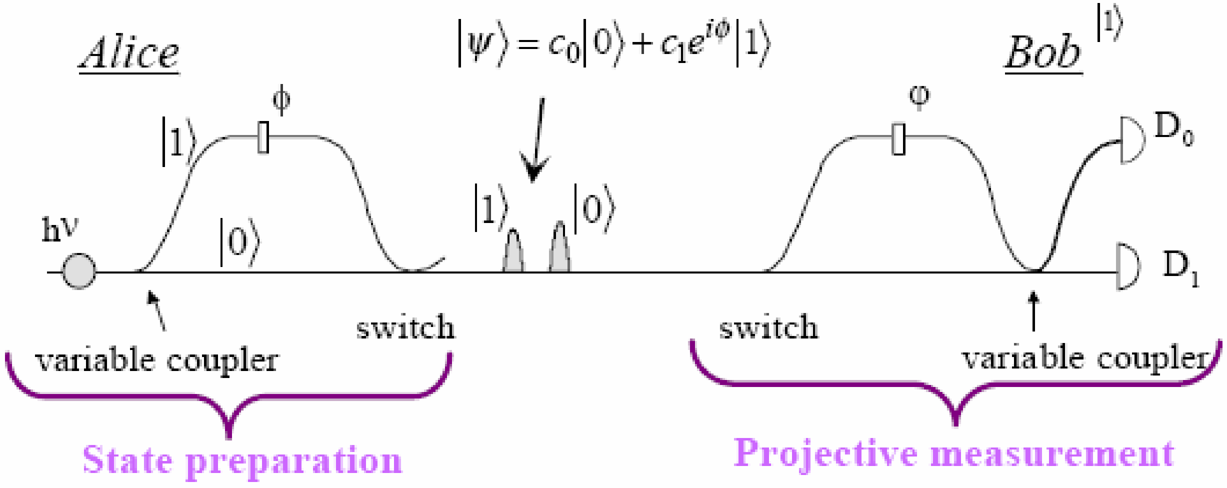
Single Particle Scheme
----Phase

- qubit : $|\psi\rangle = c_0|0\rangle + c_1 e^{i\phi}|1\rangle$

- any qubit state can be created and measured in any basis



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



[C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992)]

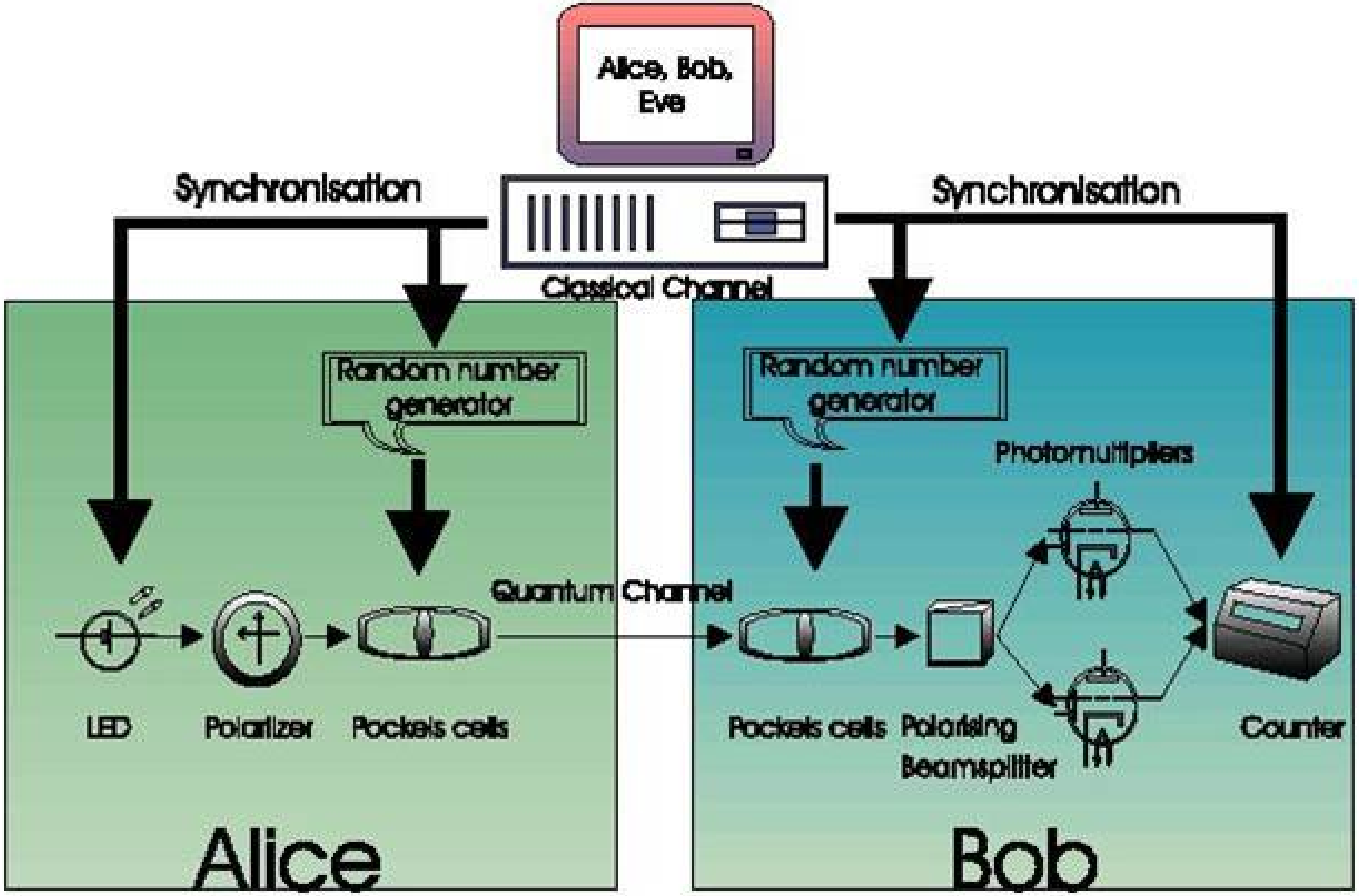
BB84 Security

	one-way communication	two-way communication
Upper bound	14.6%	1/4
Lower bound	11.0%	18.9%

[D.Gottesman and H.K.Lo, quant-ph/0105121]

We take all the error rates as being brought by the eavesdropping and when the error rate is lower than the lower bound, we can utilize some classical cryptography method to let the Eve know nothing about the key. If the error rate is higher than the upper bound, the key is insecure*!*

Experimental realization
----Single Photon Polarization



[C. H. Bennett et al., J. Cryptol. 5, 3 (1992)]

The problem of single photon polarization

- No Perfect Single Photon Source

  Solution: Weak Coherent Light

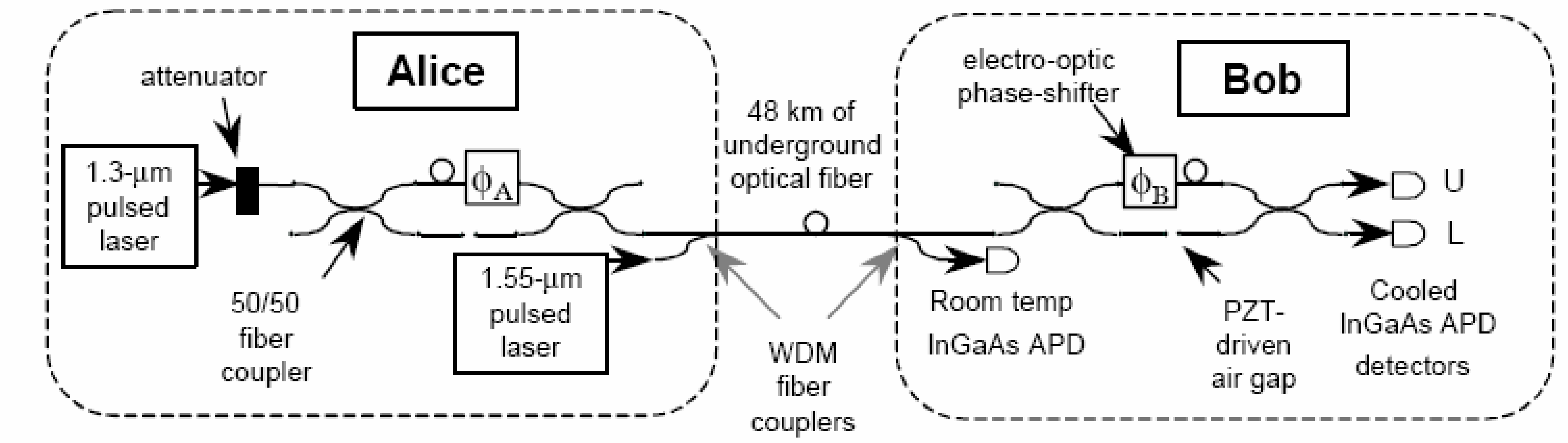
- Needs sharing the same reference frame

  Solution: Two Photon BB84…

- Stress induced birefringence and polarization-mode dispersion in Fiber.

  Solution: Free Space…

Experimental realization
----Single Photon Phase



As the two coherent contributions are separated by a few nanoseconds but propagating along the same fiber, the are essentially no temperature or stress induced fluctuation.

[R. J. Hughes et al., Advances in Cryptology – Proceeding of Crypto’96, Springer, (1996)]

The problem of single photon phase

- No Perfect Single Photon Source

  Solution: Weak Coherent Light

- The unbalanced Mach-Zehnder interferometer must be stable on the sub-wavelength scale.

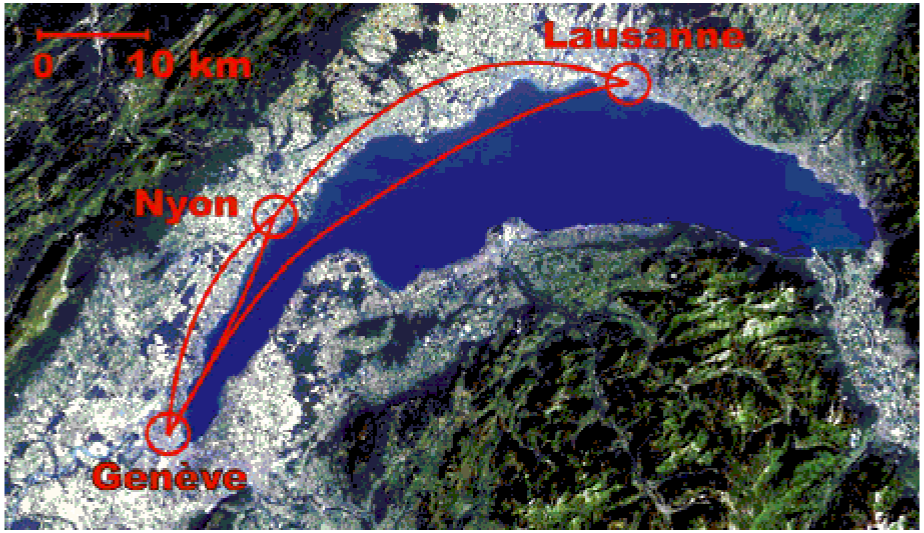
  Solution: Local stability is enough

- The Phase Modulators is sensitive to polarization.

  Solution: Plug and Play system?

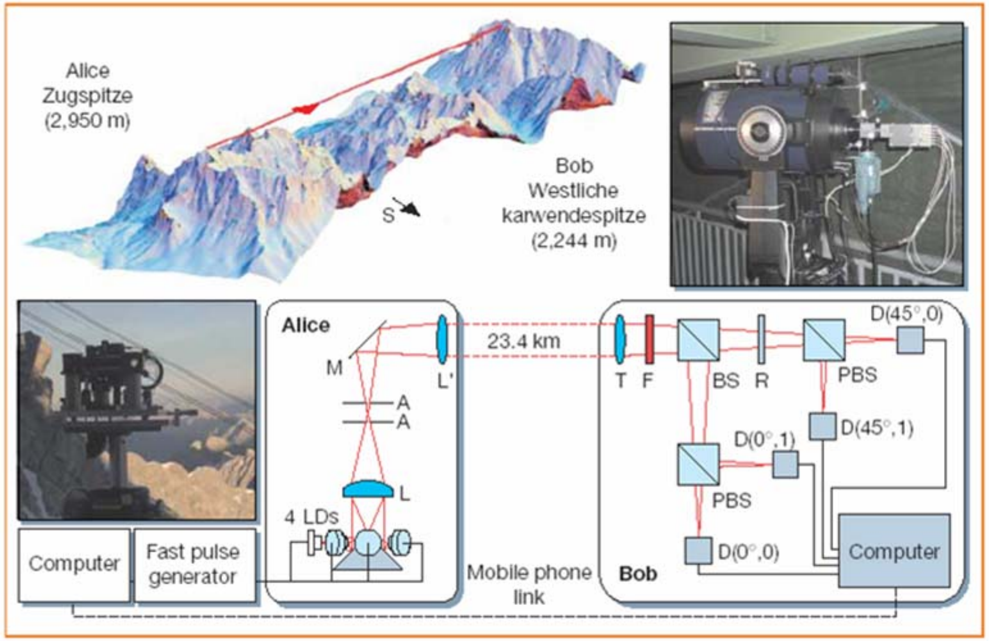
- The detection efficiency for the telecom wavelength photon is too low.

Single Photon QKD Status
----Weak Coherent Light

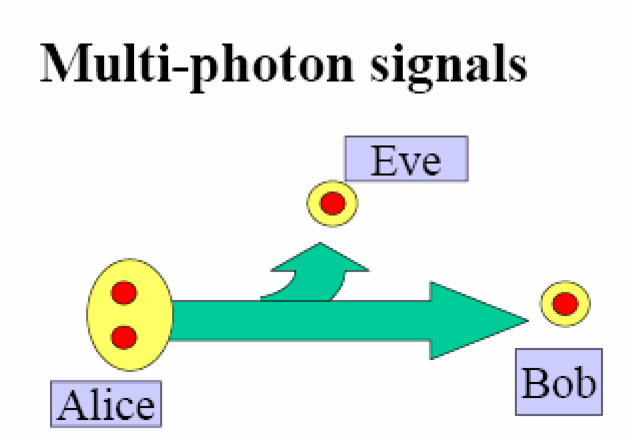


Phase; Fiber; 67KM
[D. Stucki et al., New J. Phys. 4, 41(2002)]

Polarization; Free Space; 23.4KM
[C. Kurtsiefer et al., Nature 419, 450 (2002)]



Drawback and PNS Attack



a) still unconditional security for Poissonian photon-number statistics
b) photon number is second-quantization language (only optional, relevant is signal overlap structure)
c) public announcement of basis is crucial for problem!

- Several copies of signal state
- Eve can single out a copy (Jaynes-Cummings dynamics)
- No errors are caused in polarization
- Announcement of basis:

Delayed measurement gives full information to Eve

Solution to PNS

- SARG04 Protocol

  [Scarani, Acin, Ribordy, Gisin, PRL **92**, 057901 (2004)]

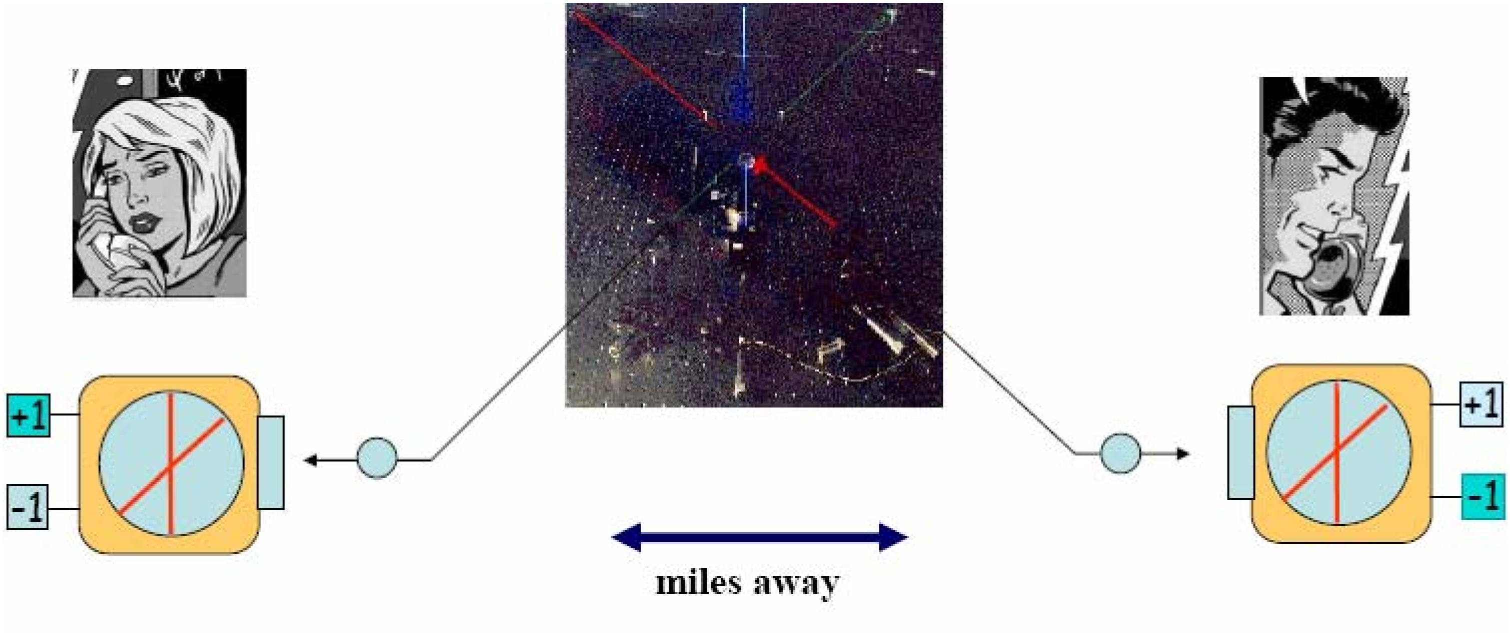
- Decoy State Method

  [Hwang, PRL **91**, 057901 (2003)]
  [Wang, PRL **94**, 230503 (2005)]
  [Lo, Ma and Chen PRL **94**, 230504 (2005)]

- Strong Reference Pulse Scheme

  [Huttner, Imoto, Gisin, Mor, PRA **51**, 1863 (1995)]

Entanglement QKD Scheme



$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$$

$$= \frac{1}{\sqrt{2}}(|H'\rangle_1|V'\rangle_2 - |V'\rangle_1|H'\rangle_2)$$

Where $|H'\rangle, |V'\rangle$ are the 45 degree polarization

$$|H'\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

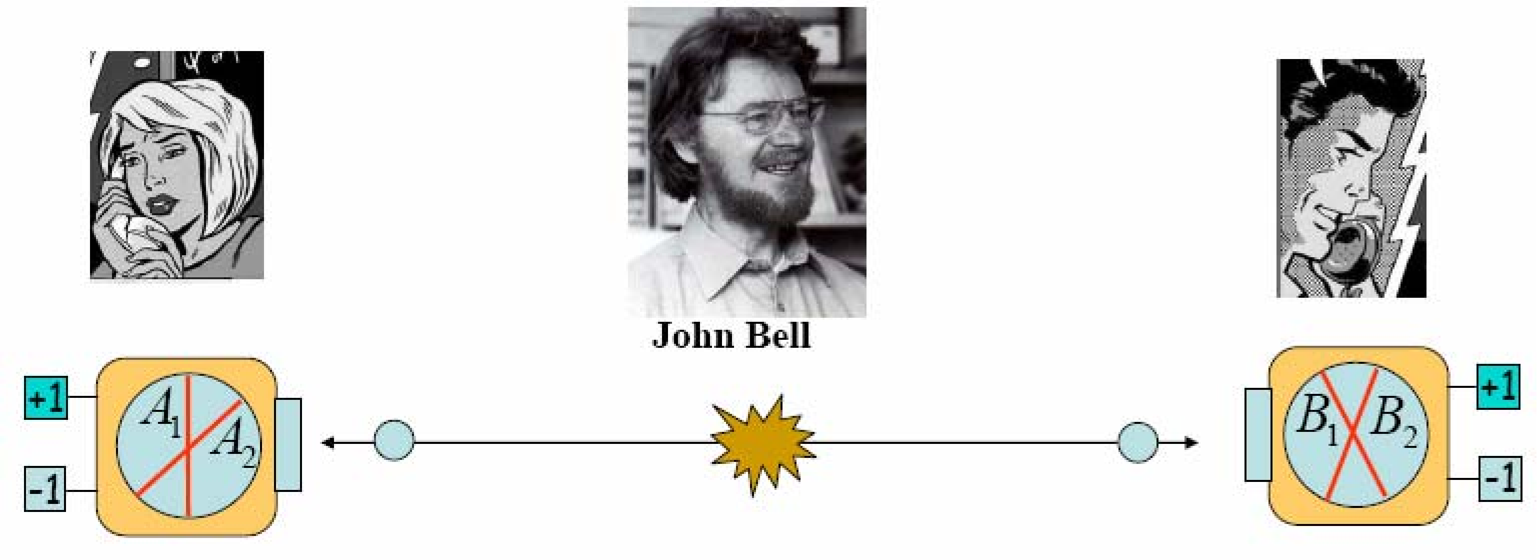
$$|V'\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

[A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991)]

Entanglement Scheme and Bell Inequality

“If Eve knows precisely which particle is in which state, the entanglement can be concluded from the local reality theory.”

----A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991)



$$S = \left| E(\phi_A \phi_B) - E(\phi_A \phi_B^{'}) + E(\phi_A^{'} \phi_B) + E(\phi_A^{'} \phi_B^{'}) \right|$$

Local Reality prediction: $S_{MAX} \leq 2$

Quantum Mechanical prediction: $S_{MAX} = 2\sqrt{2}$

Ekert 91 Protocol

1. Alice and Bob share an entangled photon pair in the state $\left|\Psi^{-}\right\rangle$;

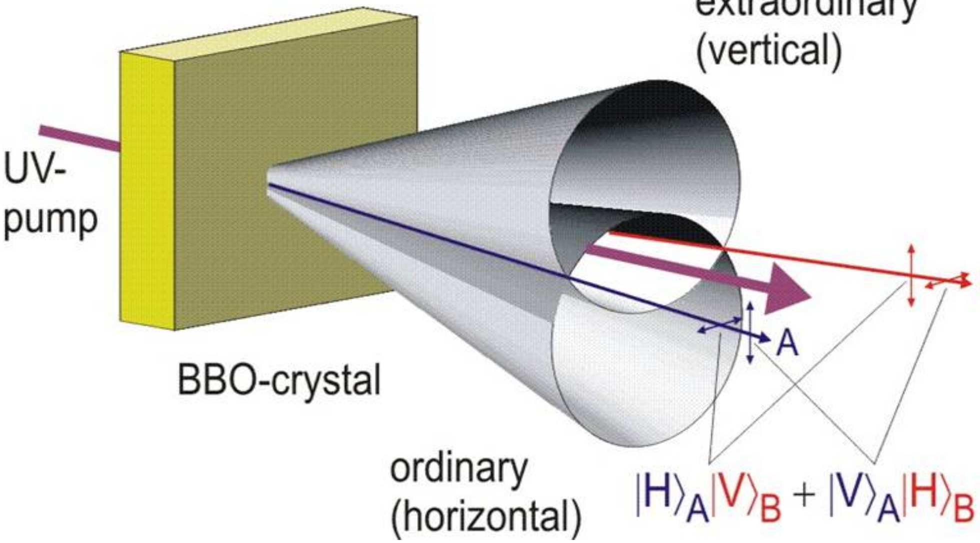
2. Alice and Bob perform measurements and register the outcomes of the measurements in one of three bases, obtained by rotating the basis around the z-axis by angles $\left|\Phi_1^a\right\rangle = 0$, $\left|\Phi_2^a\right\rangle = \frac{1}{4}\pi$, $\left|\Phi_3^a\right\rangle = \frac{1}{8}\pi$ for Alice and by angles, $\left|\Phi_1^b\right\rangle = 0$ $\left|\Phi_2^b\right\rangle = -\frac{1}{8}\pi,$ $\left|\Phi_3^b\right\rangle = \frac{1}{8}\pi$ for Bob.

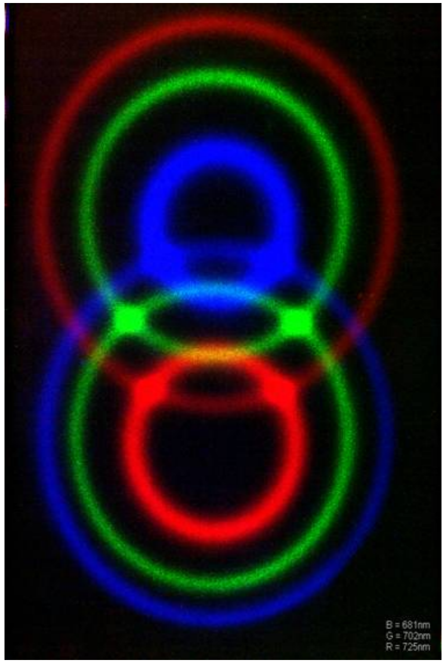
3. The users choose their bases randomly and independently for each pair.

4. The measurements with the same angle are used as keys and the others are used to check the Bell inequality.

5. If the inequality is violated, there is no eve and the key can be used. Otherwise, they discard all the keys.

Experimental realization
----Polarization entanglement





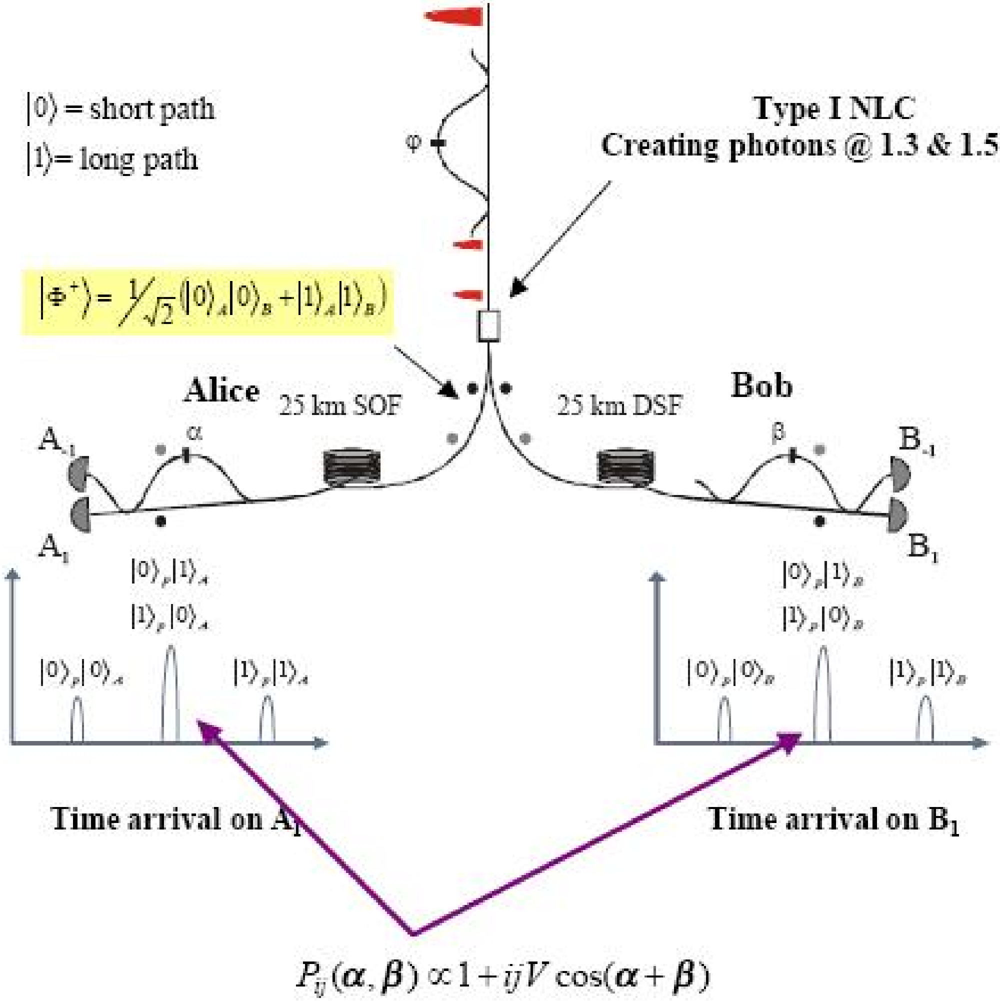
$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2\right)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2\right)$$

[P. G. Kwiat et al., Phys. Rev. Lett. 75, 4337 (1995).]

Experimental realization

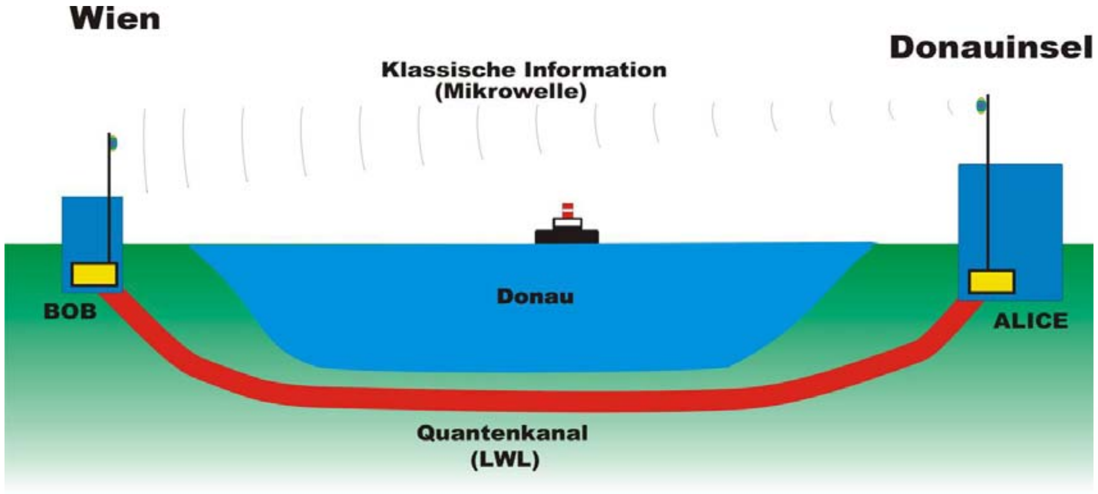
----Time bin entanglement



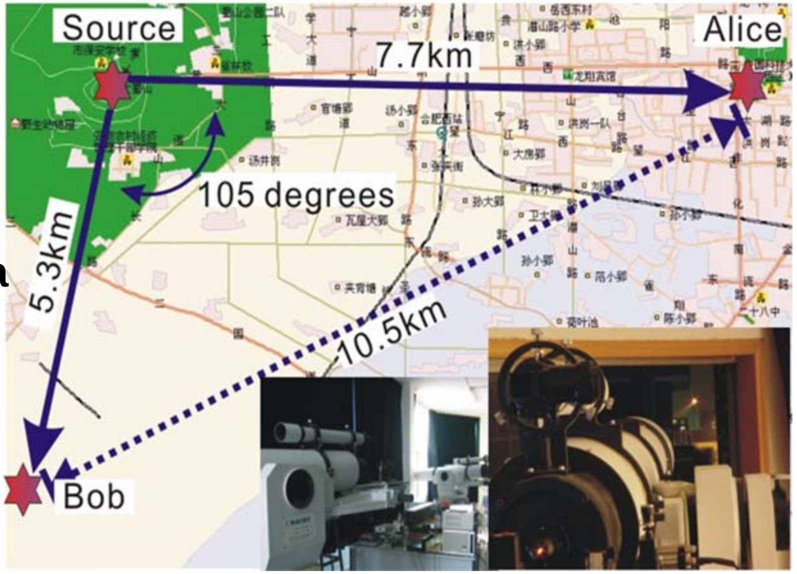
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

$$P_{ij}(\alpha,\beta) \propto 1 + ijV\cos(\alpha+\beta)$$

Experimental realization
----Entanglement



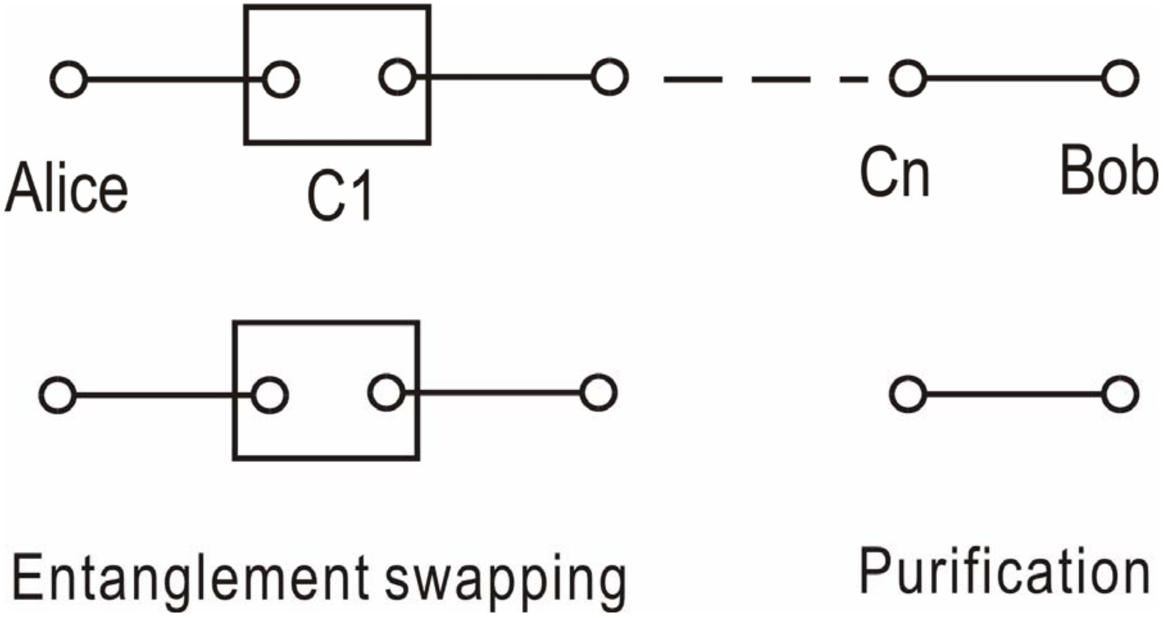
- Time bin entanglement; Fiber; 8.5KM; Switzerland
[G. Robordy, et al., Phys. Rev. A, 63, 012309 (2001)]
- Polarization entanglement; Free Space; 600M; Austria
[M. Aspelmeyer et al., Science 301, 621 (2003).]
- Polarization entanglement; Free Space; 13KM; China
[C. Z. Peng et al., Phys. Rev. Lett. . 94 , 150501 (2005)]



Drawbacks and Quantum Repeater

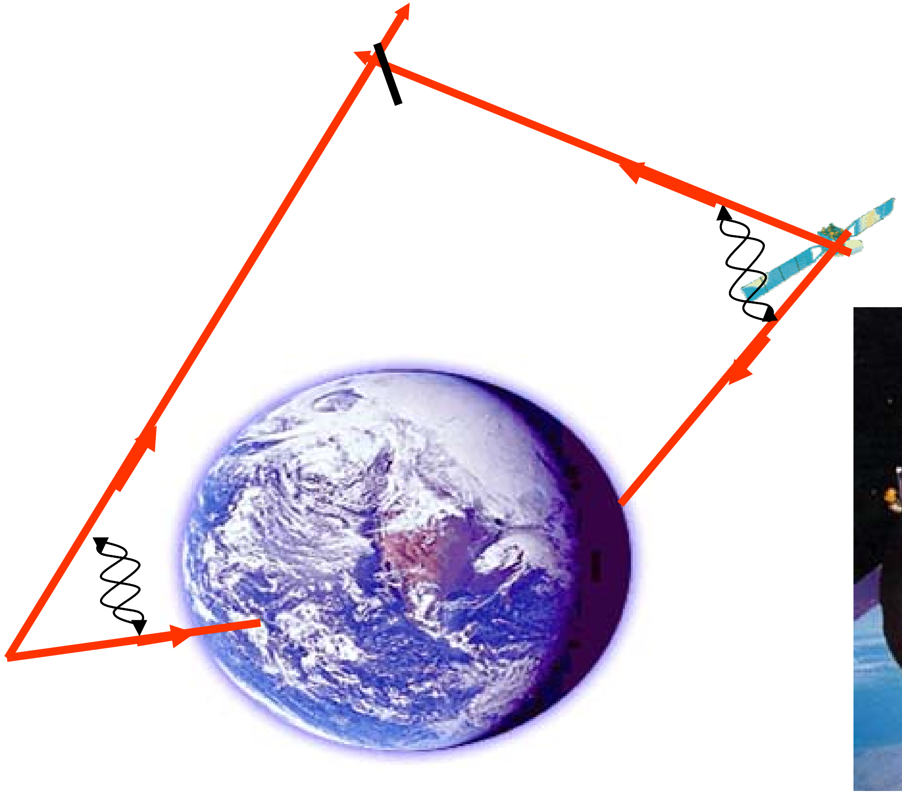
Decoherence → Quantum Entanglement Purification
Background Noise → Quantum Entanglement Swapping

} **Quantum Repeater**

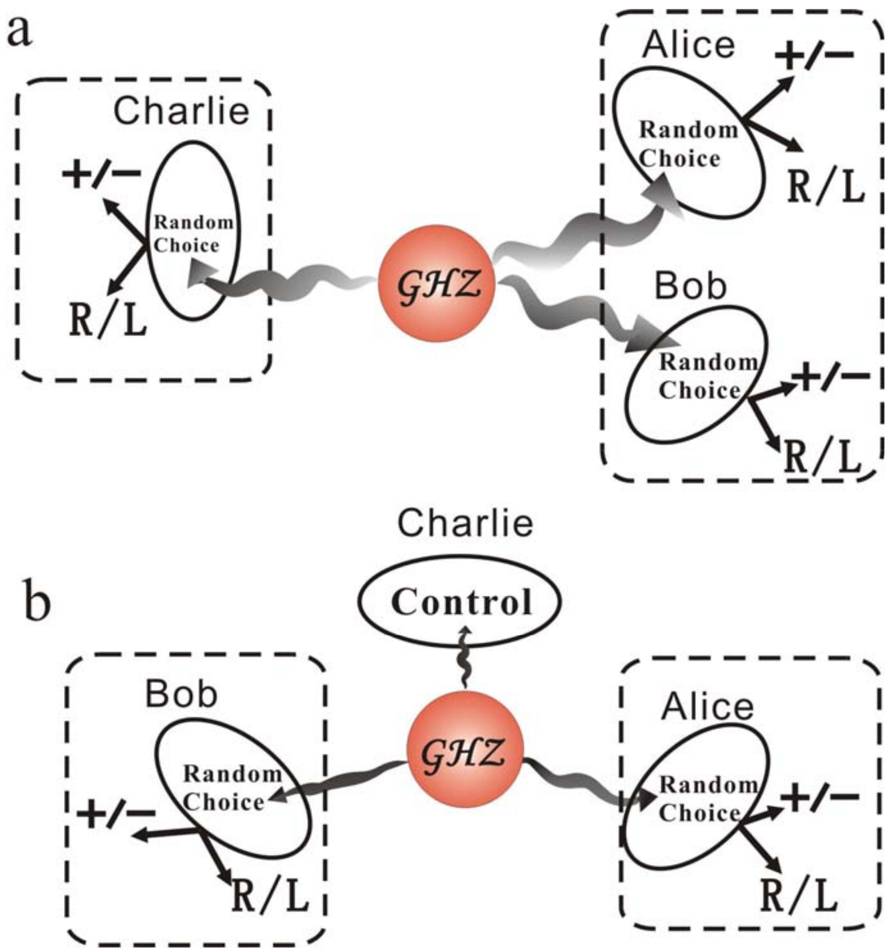


H.-J. Briegel, et al., Phys. Rev. Lett. 81, 5932, 1998.

Global quantum key distribution based on entanglement



Other quantum cryptography
Quantum Secret Sharing and Third-Man Quantum Cryptography



$$|\Psi^+\rangle_{abc} = \frac{1}{\sqrt{2}}\left(|H\rangle_a|H\rangle_b|H\rangle_c + |V\rangle_a|V\rangle_b|V\rangle_c\right)$$

$$|x_\pm\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle \pm |V\rangle\right),$$

$$|y_\pm\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle \pm i|V\rangle\right)$$

A *xxx* measurement

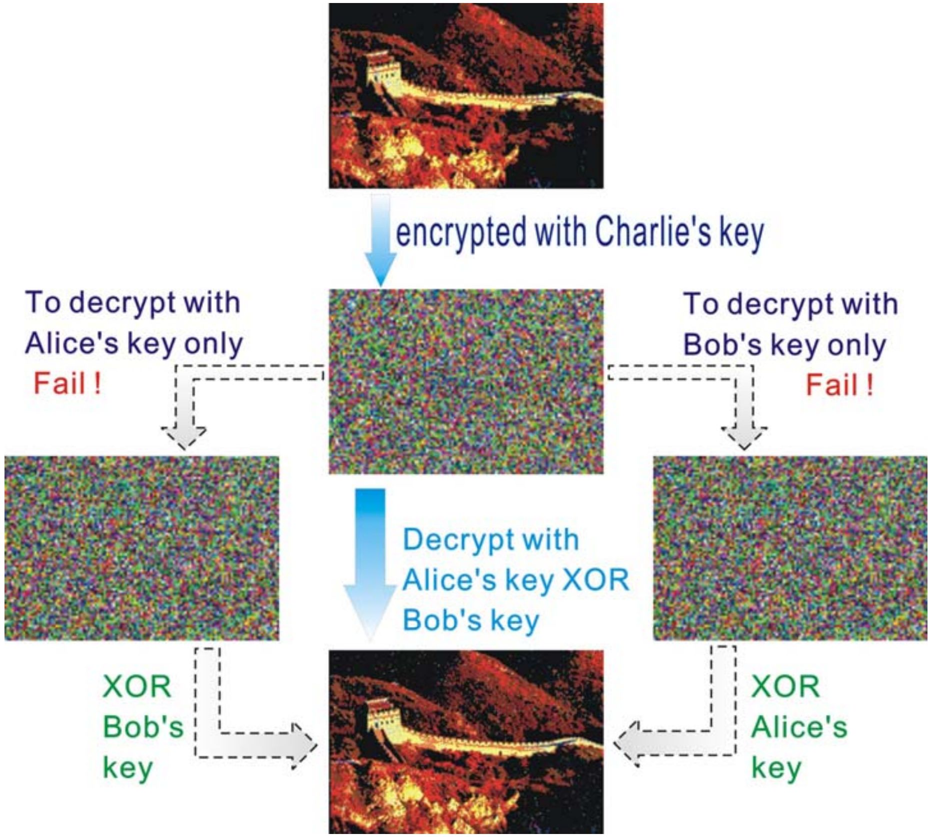
$$|\Psi^+\rangle_{abc} = \frac{1}{\sqrt{2}}((|x_+\rangle_a|x_+\rangle_b + |x_-\rangle_a|x_-\rangle_b)|x_+\rangle_c$$

$$+ (|x_+\rangle_a|x_-\rangle_b + |x_-\rangle_a|x_+\rangle_b)|x_-\rangle_c)$$

xxx, xyy, yxy, yyx

xyx, yxx, xxy, xyx

Other quantum cryptography
Quantum Secret Sharing and Third-Man Quantum Cryptography



In QSS, from 327 579 bits of raw key with a QBER of 12.9%, after security check and error reduction, Alice and Bob jointly generate 87□666 bits cured key with Charlie□ with a QBER of 0□3□□

In TQC□ with the permission of Charlie□ after security check and error reduction Alice can generate a 87,666 bits cured key with Bob, with the same QBER□ Otherwise, even after twice error reduction, the QBER remains 49.999%

[Y.-A. Chen et al., PRL, 95, 200502 (2005)]

Some References

Here we only present basic knowledge to Quantum Cryptography.

Deeply reading is suggested to

[N. Gisin, et al., Rev. Mod. Phys. 74, 145, 2002];

or www.qubit.org