Quantum Key Distribution II Realization

Expository Quantum Lecture Series 3

Graduate School of Information Sciences, Tohoku University
Centre for Quantum Technologies (CQT), National University of Singapore
Masahito Hayashi（林　正人）

東北大学 大学院情報科学研究科
Graduate School of Information Sciences.TOHOKU University

GSIS
Graduate School of Information Sciences. TOHOKU University

TOHOKU UNIVERSITY

DEX-SMI

Contents

- Outline of our QKD system
- Security of known channel with finite-length code, imperfect resources, and threshold detector
- Estimation of channel with no statistical fluctuation
- How to realize QKD

Problems in realizable QKD systems

Real quantum channel has noise.

It is had to realize single photon state.

Key distillation protocol is required.

Real key distillation consists of finite-length code.

Our detector is imperfect.

Our implemented QKD system

Environment

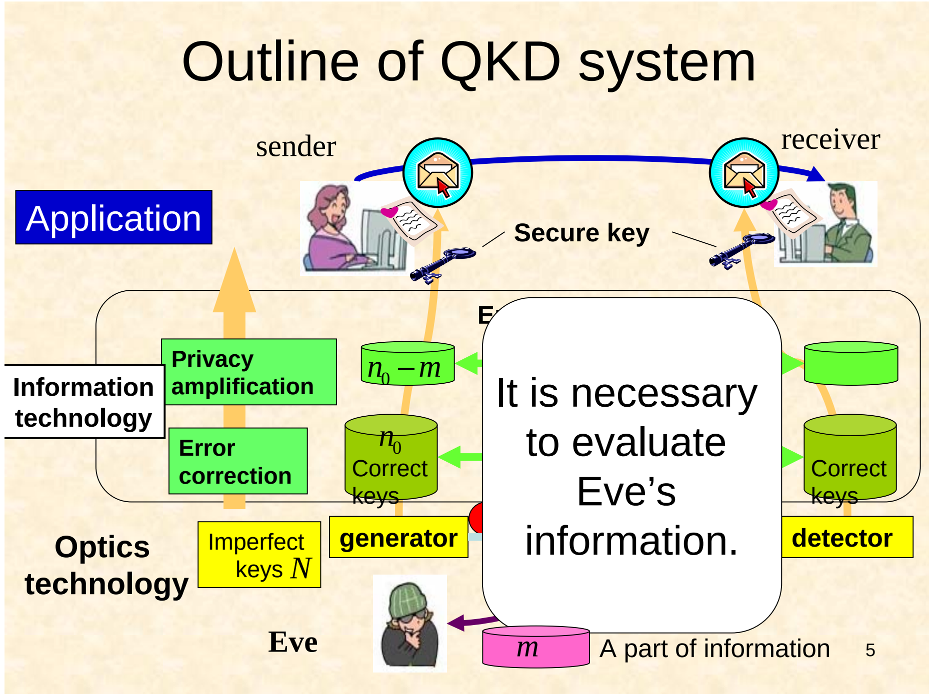
Optical fiber 20km
Usual business office
（Seminar room, ERATO-SORST, Tokyo office）

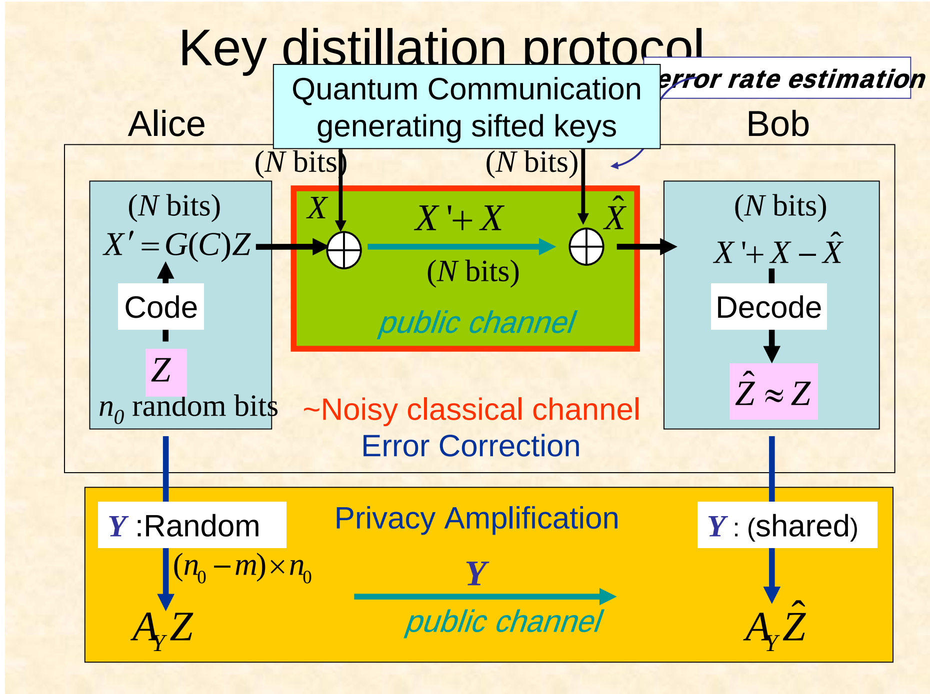
Optical device

Modification of QKD system developed by NEC
（4 intensities）
wave length　1.55 μm
System clock 62.5 MHz
Plug and Play method

Error correction & Privacy Amplification

PC（LINUX)
CPU: Pentium(R)4(3GHz)
Memory: 2GB





Detail of privacy amplification

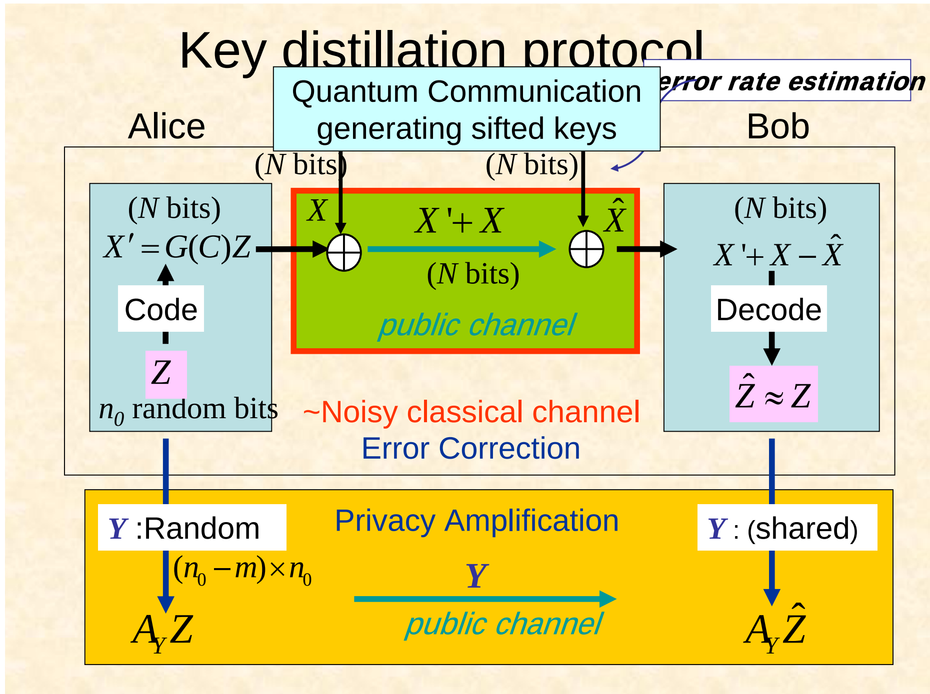
Toeplitz matrix: Same element in diagonal array.

When we generate n_0 bit from $n_0 - m$ bit number $Z \in \mathbf{F}_2^{n_0}$,

$$
A_Y :=
\begin{pmatrix}
a_{n_0-m} & a_{n_0-m+1} & \cdots & a_{n_0-2} & a_{n_0-1} & 1 & & & \\
a_{n_0-m-1} & a_{n_0-m} & \cdots & a_{n_0-3} & a_{n_0-2} & & 1 & 0 & \\
\vdots & \vdots & \ddots & \vdots & \vdots & & & \ddots & \\
a_2 & a_3 & \cdots & a_{n_0-(n_0-m)} & a_{n_0-(n_0-m)+1} & & 0 & 1 & \\
a_1 & a_2 & \cdots & a_{n_0-(n_0-m)-1} & a_{n_0-(n_0-m)} & & & & 1
\end{pmatrix}
$$

Apply this matrix to $Z \in \mathbf{F}_2^{n_0}$

Only $n_0 - 1$ random bit Y is required.



Components of QKD system

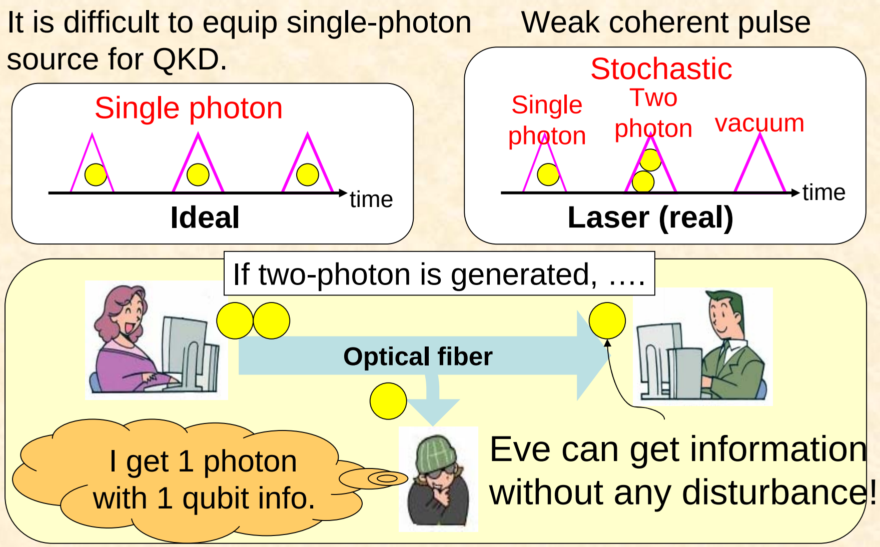
- Quantum optics technology with weak coherent light
- Information processing technology
  - –Error correction code (LDPC code)
  - –Privacy amplification (Toeplitz matrix)
  - –Evaluation of eavesdropper's information
    - •Security of known channel with finite-length code
    - •Estimation of channel with no-statistical fluctuation
    - •Estimation of channel with statistical fluctuation

Contents

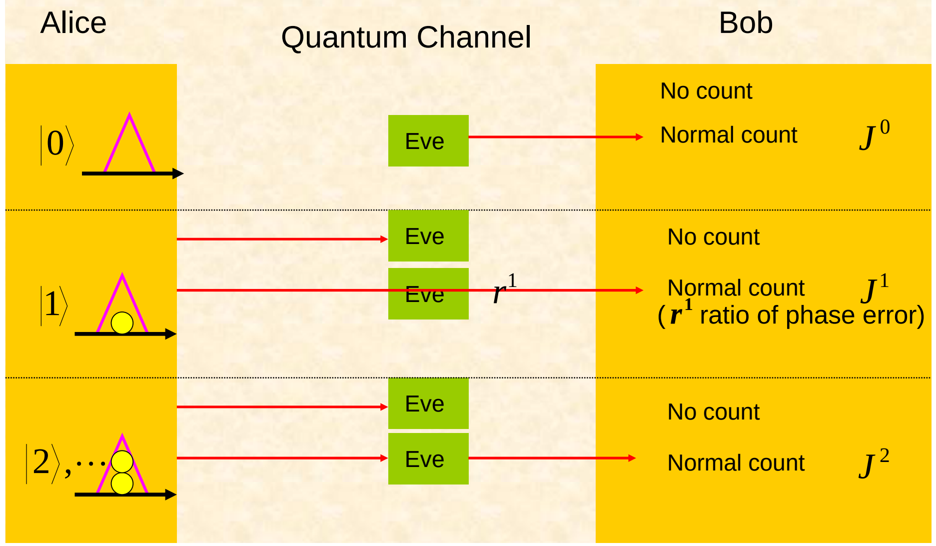
- Outline of our QKD system
- Security of known channel with finite-length code, imperfect resources, and threshold detector
- Estimation of channel with no statistical fluctuation
- How to realize QKD

Single-photon and Laser

It is difficult to equip single-photon source for QKD.



Security analysis with known channel



Eve's information among pulses detected by Bob.

Concerning Alice's information

Number of bits completely eavesdropped by Eve J^2

Number of bits non-eavesdropped by Eve J^0

Number of bits partially ($h(r^1)$) eavesdropped by Eve J^1

Eve knows $h(r^1)J^1 + J^2$ bits information concerning Alice's bit.

Eve's information after key distillation

Eve's Holevo information for final key

m : Number of sacrifice bits

$n_0 - m$: Size of final key

$P_{av,\times}$: Average of virtual phase error ratio

$$\mathrm{E}_Y \chi_E([Z]) \le (1 + n_0 - m - \log P_{av,\times}) P_{av,\times}$$

$$P_{av,\times} \le \mathrm{E}_{r^1,J^1,J^2} 2^{-(m-h(r^1)J^1-J^2)_+}$$

Exponential evaluation!

Size of sacrifice bits is determined by estimating the random variables r^1, J^1, J^2.

MH PRA, **76**, 012329 (2007)

$$m = h(r^1)J^1 + J^2 + \delta$$

Eve's distinguishability after key distillation

m : Number of sacrifice bits

$\rho_{[Z]}$: Eve's state with Alice's final key $[Z]$

ρ_E : Eve's average state

$$\mathrm{E}_Y \left\| \rho_{AE} - \rho_A \otimes \rho_E \right\|_1 \le \mathrm{E}_Y \max_{[Z]} \left\| \rho_{[Z]} - \rho_E \right\|_1$$
$$\le 2\mathrm{E}_{r^1,J^1,J^2} 2^{-(m-h(r^1)J^1-J^2)_+}$$

Exponential evaluation!

MH PRA, **76**, 012329 (2007)

Asymptotic key generation rate per sent pulse

$$R = \frac{\mu e^{-\mu} q^1 (1 - h(r^1)) + e^{-\mu} p_0 - p_\mu h(s_\mu)}{2}$$

μ : Signal intensity

p_μ : Counting rate of signal pulse

s_μ : Bit error rate of signal pulse

p_0 : Counting rate of vacuum

mentioned by Lo

Contents

- Outline of our QKD system
- Security of known channel with finite-length code, imperfect resources, and threshold detector
- Estimation of channel with no statistical fluctuation
- How to realize QKD

17

Estimation of channel parameters

Decoy-state method
(We send pulses with different intensities.)

We estimate the possible range of parameters r^1, J^0, J^1, J^2 based on the counting rates and error rates of individual intensities.

1.Estimation with no-statistical fluctuation.

2.Estimation with statistical fluctuation.

normal approximation of

$$h(r^1)J^1 + J^0 + J^2 - \Theta$$

Θ: Estimator of Eve's info. $h(r^1)J^1 + J^0 + J^2$

18

Estimation of channel parameter with no statistical fluctuation

$$e^{-\mu_i}\sum_{n=0}^{\infty}\frac{\mu_i^n}{n!}|n\rangle\langle n|$$ Phase-randomized coherent light

p_i : counting rate with intensity μ_i

$\tilde{q}^n \in [0,1]$: counting rate of n-particle state (unknown parameter)

$$e^{-\mu_i}\sum_{n=0}^{\infty}\frac{\mu_i^n \tilde{q}^n}{n!} = p_i,$$

Do we have to treat infinite number of parameters based on finite-number of constraints?

19

How to recover parameters r^1, J^0, J^1, J^2 !

$$\tilde{q}^0 = p^0 \quad (\mu_0 = 0)$$

$J^0 = \tilde{q}^0 N$ $\quad$ N:Number of detected pulses by Bob

$$J^1 = \tilde{q}^1 N$$

$$J^2 = (1 - \tilde{q}^0 - \tilde{q}^1)N$$

For r^1, we apply the same method to error events.

$$r^1 = \frac{\tilde{q}^1_{\mathrm{error}} N_{\mathrm{error}}}{\tilde{q}^1 N}$$

20

If a good expansion exists,…..

(Vacuum＋k intensities)

$$\sum_{n=0}^{\infty} e^{-\mu_i}\frac{\mu_i^n}{n!}|n\rangle\langle n|$$

$$= e^{-\mu_i}|0\rangle\langle 0| + e^{-\mu_i}\mu_i|1\rangle\langle 1| + \sum_{n=2}^{k+1} P_i^n \rho_n$$

$$q^1 \triangleq \tilde{q}^1$$

$$q^m \triangleq \mathrm{Tr}\rho_m \sum_{n=2}^{\infty} \tilde{q}^n |n\rangle\langle n| \ (m \ge 2)$$

Finite constraints

$$e^{-\mu_i}q^0 + e^{-\mu_i}\mu_i q^1 + \sum_{n=2}^{k+1} P_i^n q^n = p_i$$

k constraints and k+1 unknown parameters

$1 \ge q^j \ge 0$ Lower bound of q^1

Vacuum＋2 intensities $(0 < \mu_1 < \mu_2)$

Wang2005

$$\rho_2 := \frac{1}{\Omega_2}\sum_{n=2}^{\infty}\frac{\mu_1^{n-2}}{n!}|n\rangle\langle n|$$

$$\rho_3 := \frac{1}{\Omega_3}\sum_{n=3}^{\infty}\frac{\mu_2^{n-2}-\mu_1^{n-2}}{(\mu_2-\mu_1)n!}|n\rangle\langle n|$$

$$\sum_{n=0}^{\infty} e^{-\mu_1}\frac{\mu_1^n}{n!}|n\rangle\langle n| = e^{-\mu_1}|0\rangle\langle 0| + e^{-\mu_1}\mu_1|1\rangle\langle 1| + e^{-\mu_1}\mu_1^2\Omega_2\rho_2$$

$$\sum_{n=0}^{\infty} e^{-\mu_2}\frac{\mu_2^n}{n!}|n\rangle\langle n| = e^{-\mu_2}|0\rangle\langle 0| + e^{-\mu_2}\mu_2|1\rangle\langle 1| + e^{-\mu_2}\mu_2^2\Omega_2\rho_2 + e^{-\mu_2}\mu_2^2(\mu_2-\mu_1)\Omega_3\rho_3$$

Expansion with Arbitrary number of intensities

Generalize "difference"

$$e^{-\mu_i}\sum_{n=2}^{\infty}\frac{\mu_i^n}{n!}|n\rangle\langle n| = \sum_{l=1}^{i} e^{-\mu_i}\mu_i^2\prod_{t=1}^{l-1}(\mu_i-\mu_t)\Omega_{l+1}\rho_{l+1}$$

$$\rho_{l+1} := \frac{1}{\Omega_{l+1}}\sum_{n=l+1}^{\infty}\sum_{j=1}^{l}\frac{\mu_j^{n-2}}{\prod_{t=1,\neq j}^{l}(\mu_j-\mu_t)}\frac{1}{n!}|n\rangle\langle n|$$

$$q^m \triangleq \mathrm{Tr}\rho_m \sum_{n=2}^{\infty} \tilde{q}^n |n\rangle\langle n|$$

$$e^{-\mu_i}q^0 + e^{-\mu_i}\mu_i q^1 + \sum_{n=2}^{i+1} e^{-\mu_i}\mu_i^2\prod_{t=1}^{n}(\mu_i-\mu_t)\Omega_n q^n = p_i$$

$1 \ge q^j \ge 0$ Lower bound of q^1

Estimation of counting rate q^1

$$q_{\min}^{1,k} \triangleq \min\left\{ q^1 \,\middle|\, \begin{array}{l}\text{previous condition} \\ 1 \ge q^1, q^{k+1} \ge 0\end{array} \right\}$$

If the counting rate is independent of basis, …

$$q_{\min}^{1,k} = \min\{q_{1,\min},\ldots,q_{k,\min}\}$$

$$q_{j,\min} \triangleq \sum_{i=1}^{j}\beta_i^j(p_i - p_0 e^{-\mu_i}) - \frac{1-(-1)^j}{2}\mu_1\cdots\mu_j\Omega_{j+1}$$

$$\beta_i^j \triangleq (-1)^{j-1}\frac{\mu_1\cdots\mu_j e^{\mu_i}}{\mu_i^2\prod_{t=1,\neq i}^{j}(\mu_i-\mu_t)}$$

Estimation of counting rate q^1 (with dependence of basis)

$$e^{-\mu_i}q^0 + e^{-\mu_i}\mu_i q^1 + \sum_{n=2}^{i+1} e^{-\mu_i}\mu_i^2 \prod_{t=1}^{n}(\mu_i-\mu_t)\Omega_n q^{n,\times} = p_i^\times$$

$$e^{-\mu_i}q^0 + e^{-\mu_i}\mu_i q^1 + \sum_{n=2}^{i+1} e^{-\mu_i}\mu_i^2 \prod_{t=1}^{n}(\mu_i-\mu_t)\Omega_n q^{n,+} = p_i^+$$

$$q^{1,k}_{\min} \triangleq \min_{1\ge q^1, q^{2,\times},\ldots,q^{k+1,\times},q^{2,+},\ldots,q^{k+1,+}\ge 0} q^1$$

$$= \min\left\{q^\times_{1,\min},\ldots,q^\times_{k,\min},q^+_{1,\min},\ldots,q^+_{k,\min}\right\}$$

$$q^x_{j,\min} \triangleq \sum_{i=1}^{j} \beta_i^j \left(p_i^x - p_0 e^{-\mu_i}\right) - \frac{1-(-1)^j}{2}\mu_1\cdots\mu_j\Omega_{j+1}$$

$$\beta_i^j \triangleq (-1)^{j-1}\frac{\mu_1\cdots\mu_j e^{\mu_i}}{\mu_i^2\prod_{t=1,\ne i}^{j}(\mu_i-\mu_t)} \qquad x=\times,+$$

Asymptotic key generation rate

Estimating r^1 as well as q^1, we substitute them into the following:

$$R = \frac{\mu e^{-\mu}q^1(1-h(r^1)) + e^{-\mu}p_0 - p_\mu h(s_\mu)}{2}$$

μ : Signal intensity

p_μ : Counting rate of signal pulse

s_μ : Bit error rate of signal pulse

p_0 : Counting rate of vacuum

When there is no Eve, ……

The counting rate with intensity μ_i

$$p_i = 1 - e^{-\alpha\mu_i} + p_0$$

$$q_{j,\min}$$

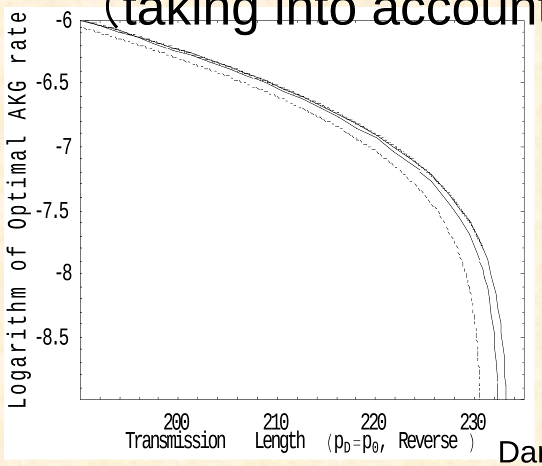
Usually $q^{1,k}_{\min} = q_{k,\min}$

$$= \alpha + p_0 - (-1)^j\left(\varepsilon_\alpha^j(\vec{\mu}) + p_0\varepsilon_\alpha^1(\vec{\mu})\right) - \frac{1-(-1)^j}{2}\varepsilon_\alpha^1(\vec{\mu})$$

$$\varepsilon_\alpha^j(\vec{\mu}) \triangleq (-1)^{j-1}\mu_1\cdots\mu_j\Delta_f^j(\vec{\mu})$$

where $$f(x) = \frac{e^x - e^{(1-\alpha)x} - \alpha x}{x^2}$$

Key generation rate (taking into account dark count)



Distance (km)

$$p_i = 1 - e^{-\alpha\mu_i} + p_0,$$

$$\alpha = 0.1\times 10^{-\frac{0.17\times L+5}{10}}$$

No interfusion in channel (assumption)

$$p_0 = p_D$$

Error rate of single photon in channel 0.03

Dark count rate p_D 4.0×10^{-7}

$$k = 2,3,4,\infty$$

Channel performance from T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, *Jpn. J. Appl. Phys.*, **43**, L1217 (2004).

Security guaranteed QKD system

Environment

Optical fiber 20km
Usual business office
（Seminar room, ERATO-SORST, Tokyo office）

Optical device

Modification of QKD system developed by NEC
（4 intensities）
wave length　1.55 μm
System clock 62.5 MHz
Plug and Play method

Error correction & Privacy Amplification

PC （LINUX)
CPU: Pentium(R)4(3GHz)
Memory: 2GB

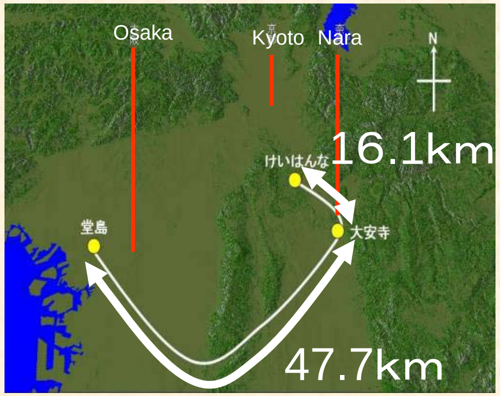
Contents

How to realize QKD?

- Optical fiber communication
- Free space transmission
- Satellite communication
- All of them require
  weak photon source.

QKD with Metropolitan fiber network

Longest distance



47.7km
+3×16.1km
=96km　Mitsubishi

3Returns (16.1km)
+0.4km
=97km　NEC

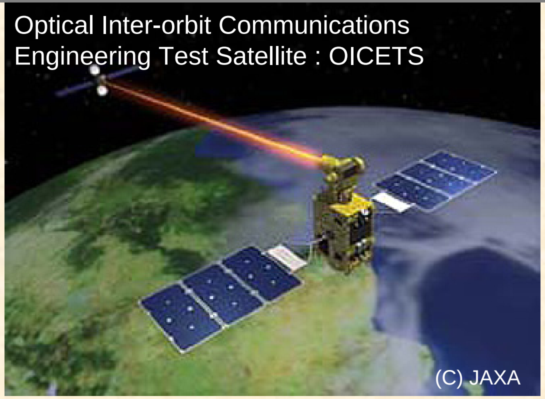
Mitsubishi (2004) and NEC (2008) with NICT.
Similar experiment is demonstrated in USA and Swiss.

清水克宏(三菱電機)「JGN2光テストベッドを用いた 量子暗号システム試験」
JGNIIシンポジウム2005in大阪. http://www.jgn.nict.go.jp/sympo2005/

QKD with free space

By National University of Singapore
Similar experiment is done by Wien Univ.

Satellite communication with QKD



NICT(JAPAN) OICETS and ESA (EU) Artemis will demonstrate satellite communication with QKD. Cosmic space has no air obstructing communication.

When QKD is used in practice?

Swiss considers to use QKD for voting.

Science & Technology

Quantum cryptography

Un

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.

Summary

- If two photons are sent, Eve can get a part of information without disturbing.
- Eve can also get a part of information when the channel has noise.
- By sacrificing bits, Alice and Bob can generate secure key, which is almost independent of Eve's information.
- Many realization experiment have been done by several groups.
- QKD is close to real application.