An Introduction to Quantum Key Distribution

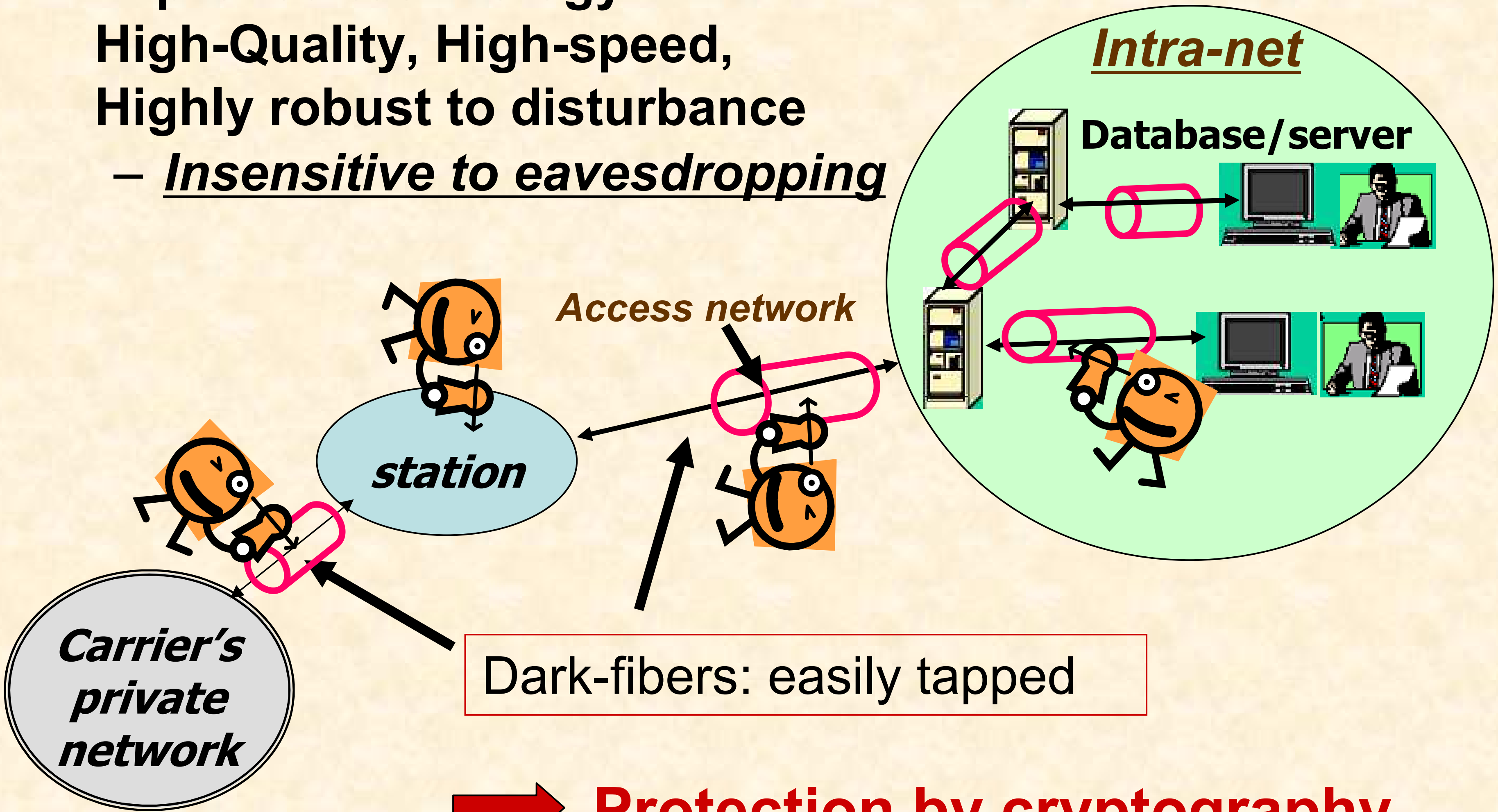
Akihisa Tomita

Quantum Computation and Information Project, ERATO-SORST, JST

Nano Electronics Research Laboratories, NEC Corp.

Security in optical communication networks

- **Improved technology:**
  High-Quality, High-speed,
  Highly robust to disturbance
  - ***Insensitive to eavesdropping***

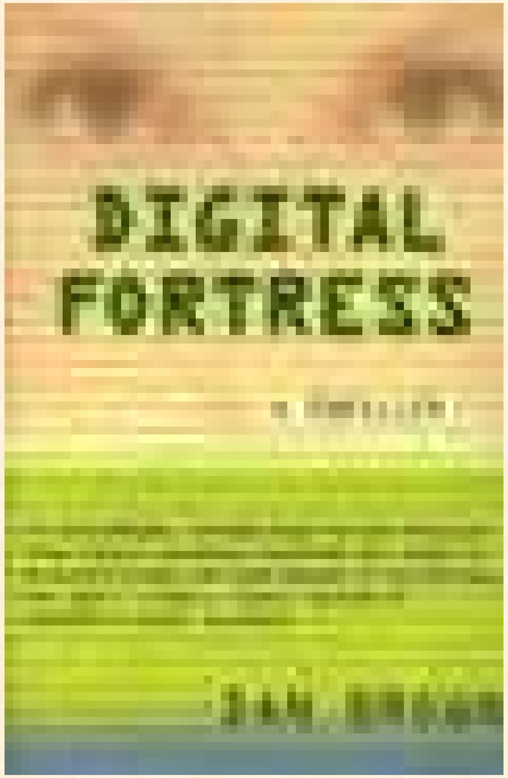


Protection by cryptography

Threat by innovating technologies

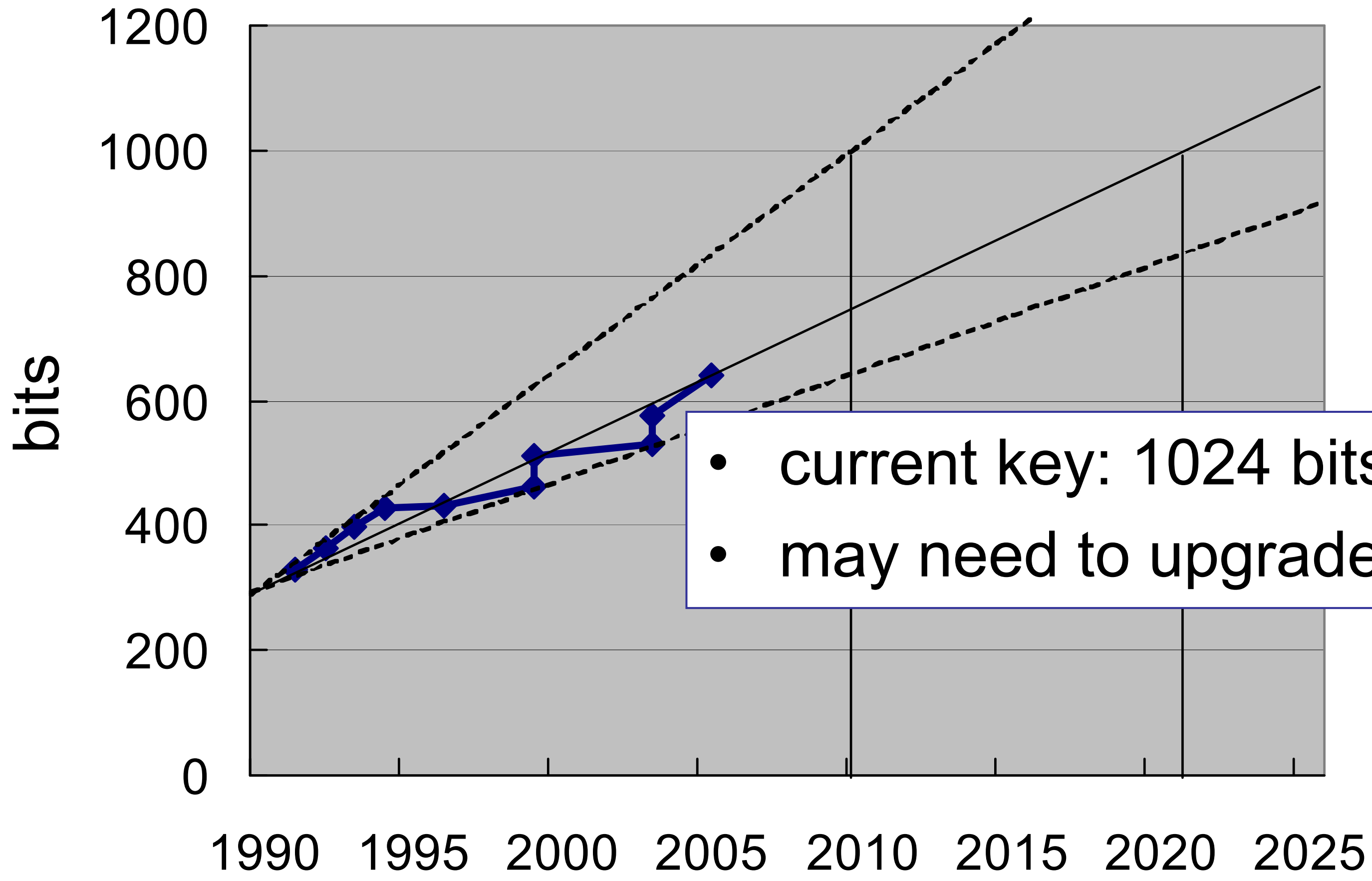
- Shor's and related quantum algorithms
  - Efficient solution for factorization, discrete log, ….
    (on which the security of public key cryptography relies)
- Grover algorithm for database search
- Progress in computers
  (reduces time to break codes)
- Invention of new algorithm
  - One-way has not been proved
  - Back doors may be exist in a certain implementation

Code breakers in the fictitious world



- 'TRANSLTR,' a huge computer in Dan Brown's novel "DIGITAL FORTRESS"
  - 5yrs. development period
  - $1.9 B cost
  - 3 M processors in parallel
  - 10,000 bit-key decrypted in an hour
  - quantum algorithm employed? in 1998? (Shor's algorithm appeared in 1994)

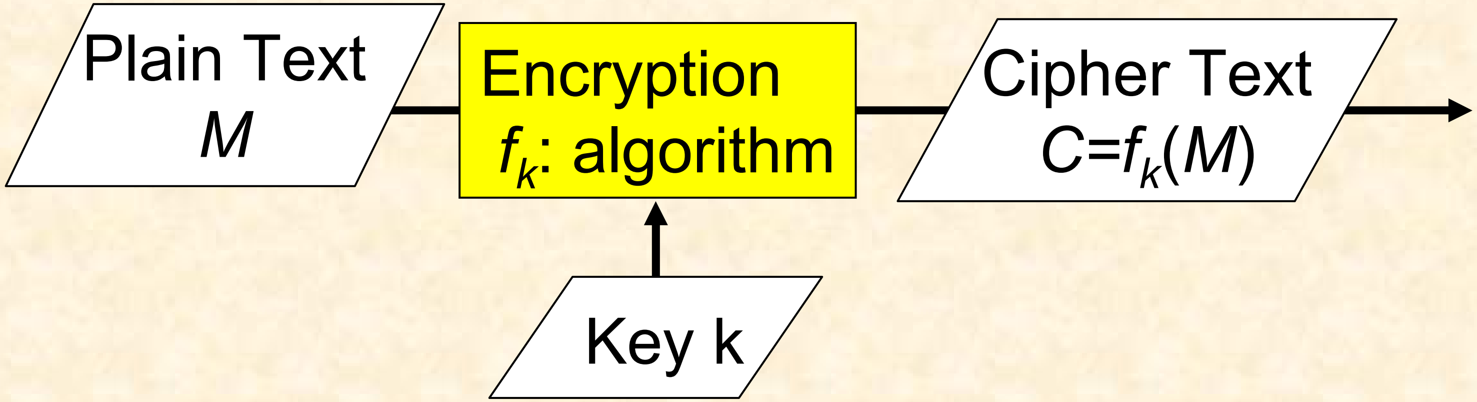
RSA Challenge (it's real)



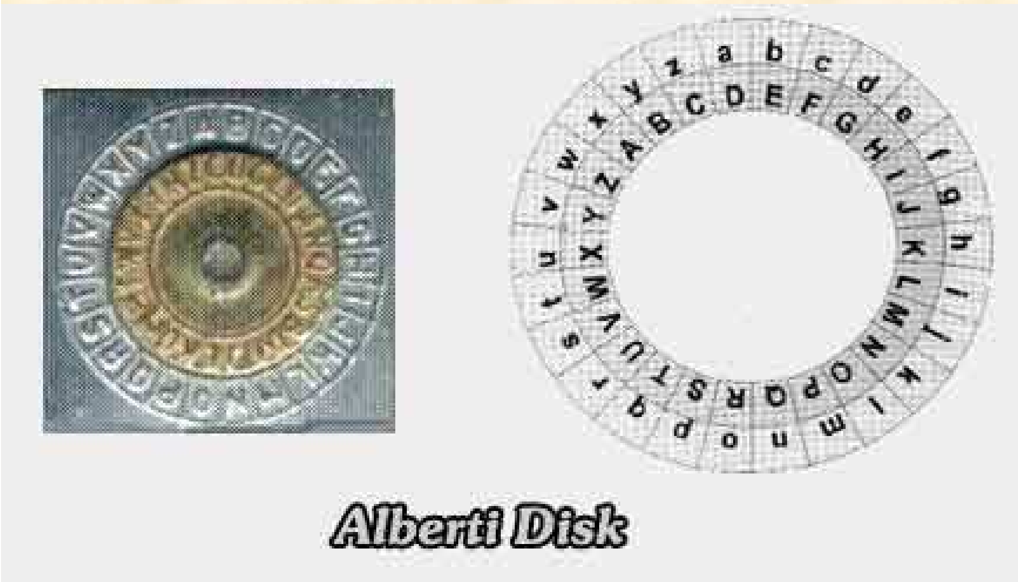
- current key: 1024 bits
- may need to upgrade

affordable resource ⟺ security

Secure communication

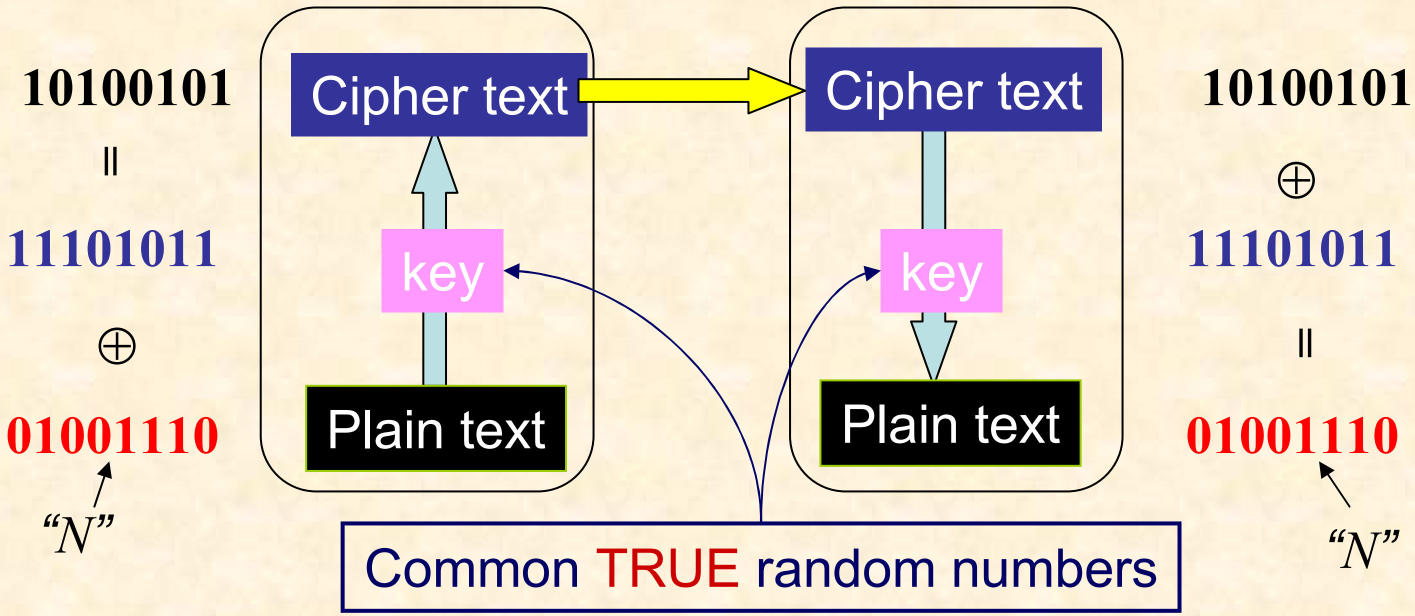


- Caesar's Cipher
  - algorithm: replace a character by the *k*-th one in the alphabet
  - Key: a number *k*
  - *example:*



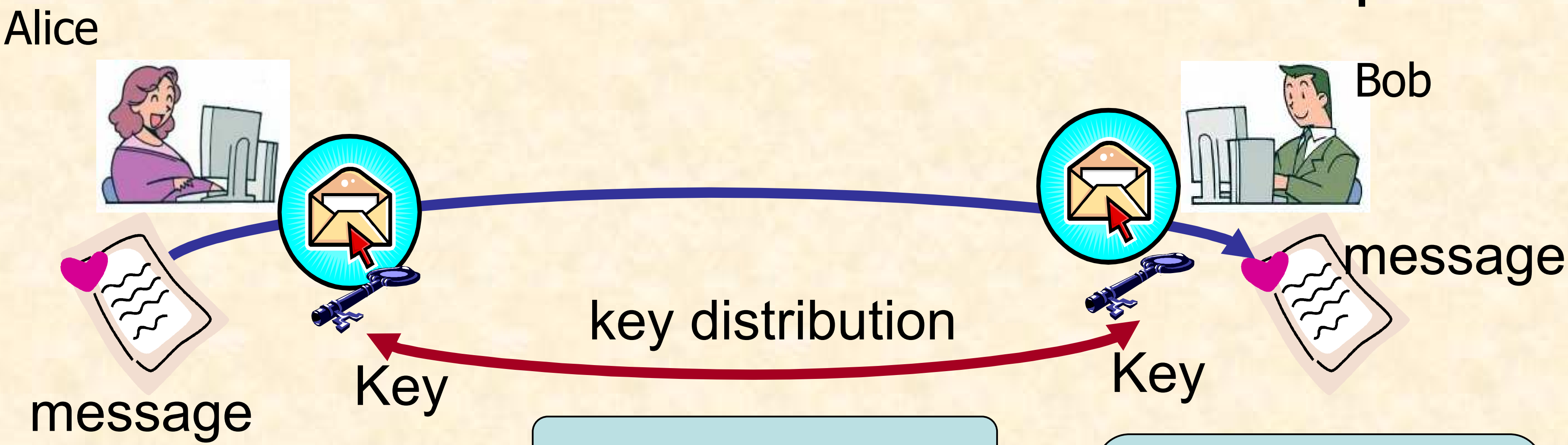
Perfectly secure cryptography

- Vernam cipher (One-time-pad)
  - $C = M \oplus K$
  - Fresh keys (used only once)
  - Length(M) = Length(K) = Length(C) = *const.*



Requirements for common keys

- Secure communication with Vernam cipher



error rate: ex. $<10^{-9}$

- shared by Alice and Bob
- negligible information for eavesdroppers
- statistically random

$\chi(K) \leq 2^{-\delta}$

ex. $\delta = 8$

Pass the RN tests:
ex. FIPS140-2
SP800-22

Adversaries

- Collect pairs of [plain texts] and cipher texts
- Guess key (cryptanalysis)
- Decode the following cipher texts

- impossible for one-time-pad
- only way is eavesdropping key distribution to know the key used in cipher

- try to get as much as information on the key

- If Adversaries' information on raw key is bounded, their information on final key can be reduced by Privacy Amplification

Quantum Key Distribution

～security based on laws of physics～

- A protocol to share random numbers (cryptographic key) between remote parties

- Everlasting, unconditional security guaranteed by quantum mechanics and Information theory, *i.e.*,
Any computers (incl. quantum) cannot draw key information

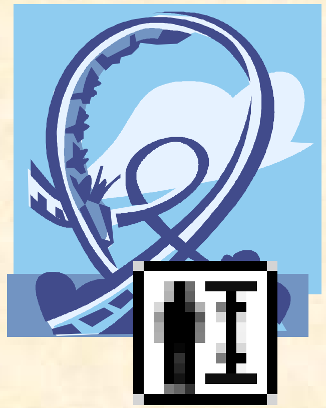
- **Detection of eavesdropping, or guaranteed security**

- **by limiting eavesdropper's information**

Mission impossible:

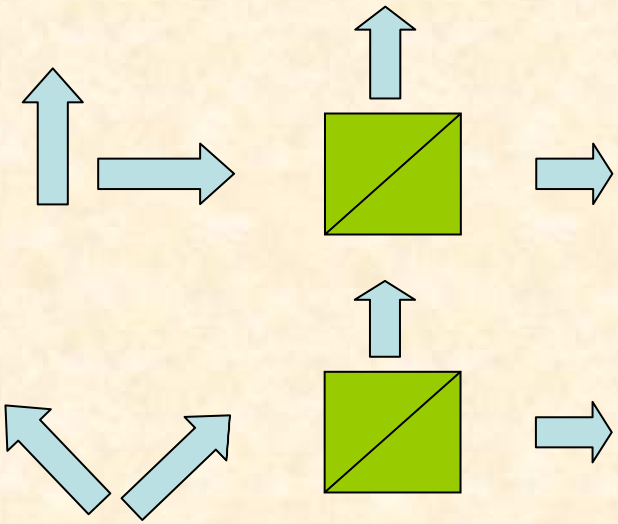
to distinguish two states with a single measurement

- classical states ＝ possible
- orthogonal states ＝ possible
- non-orthogonal states ＝ impossible



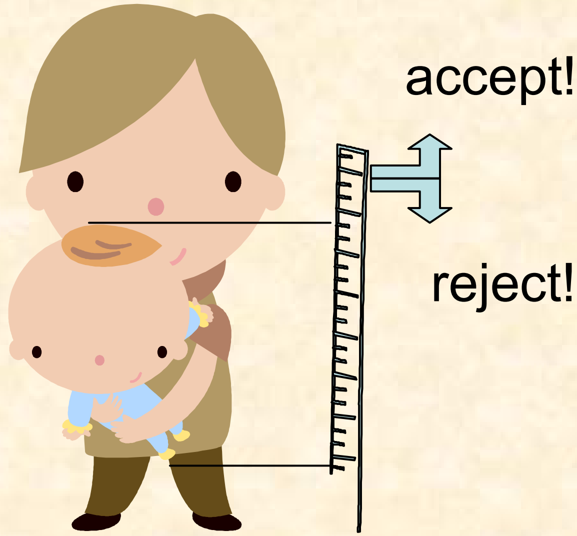
If you had many copies, it would be possible without a trace

disturbance ➡ upper bound of information

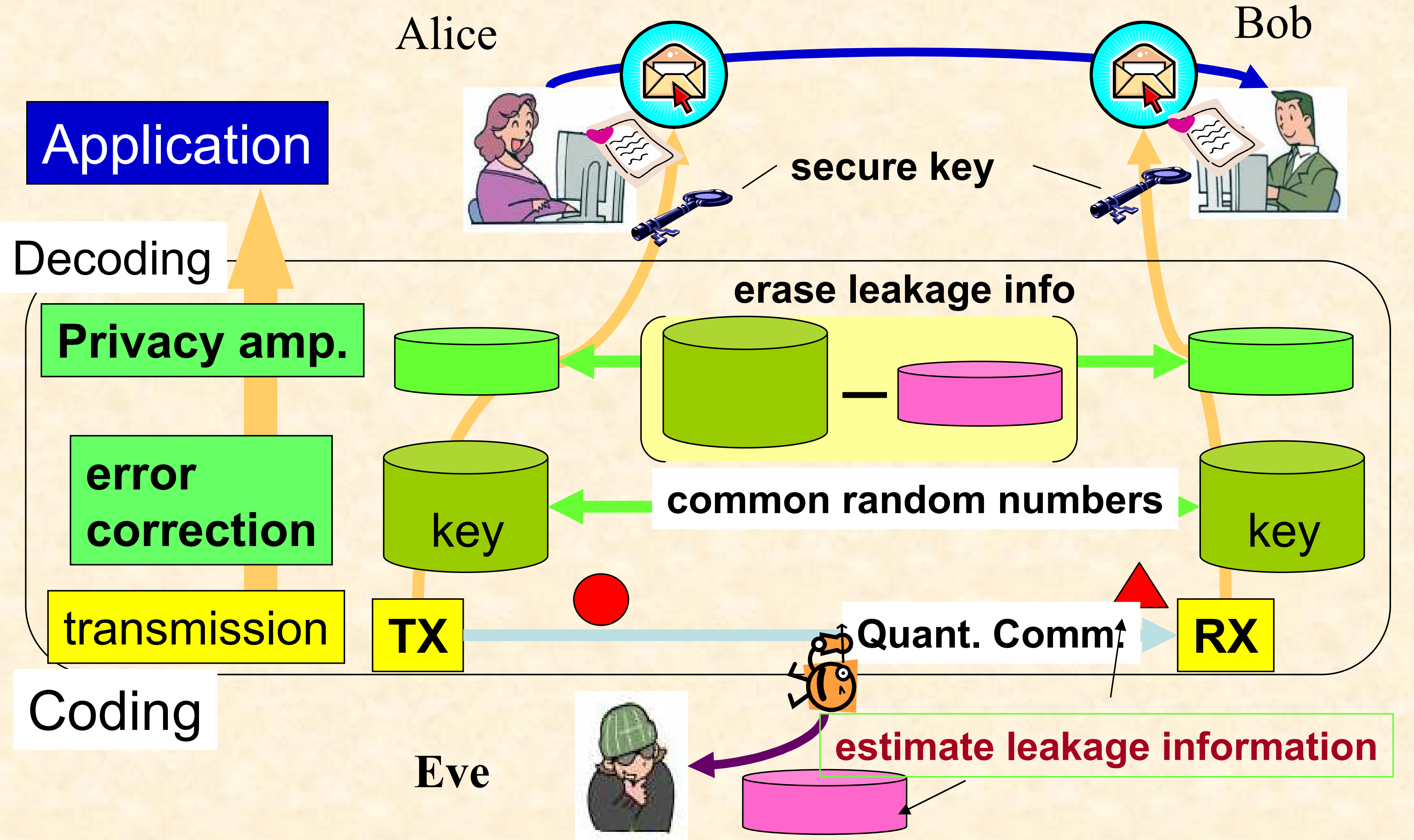


error free

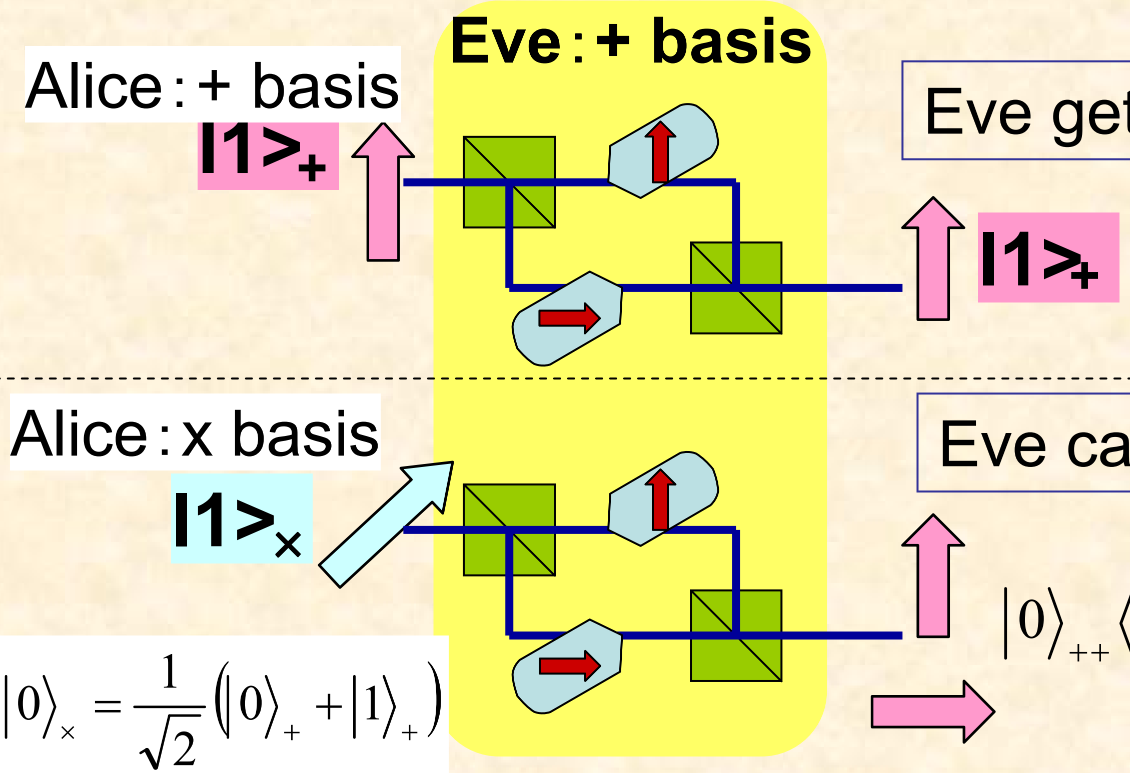
50% error



Secure key distribution with quantum communication



Errors and Eve's information



Eve gets information

Eve causes error

$|0\rangle_{++}\langle 0| + |1\rangle_{++}\langle 1|$

missing phase information

$$|0\rangle_\times = \frac{1}{\sqrt{2}}\left(|0\rangle_+ + |1\rangle_+\right)$$

$$|1\rangle_\times = \frac{1}{\sqrt{2}}\left(|0\rangle_+ - |1\rangle_+\right)$$

hat, after coding-decoding, for Alice's key [*Z*]

$$\max_{[Z]} \frac{1}{2}\left\|\rho_{[Z]} - \bar{\rho}^E\right\| \le P_{ph} \le 2^{N\bar{h}(n_e/N)-m}$$

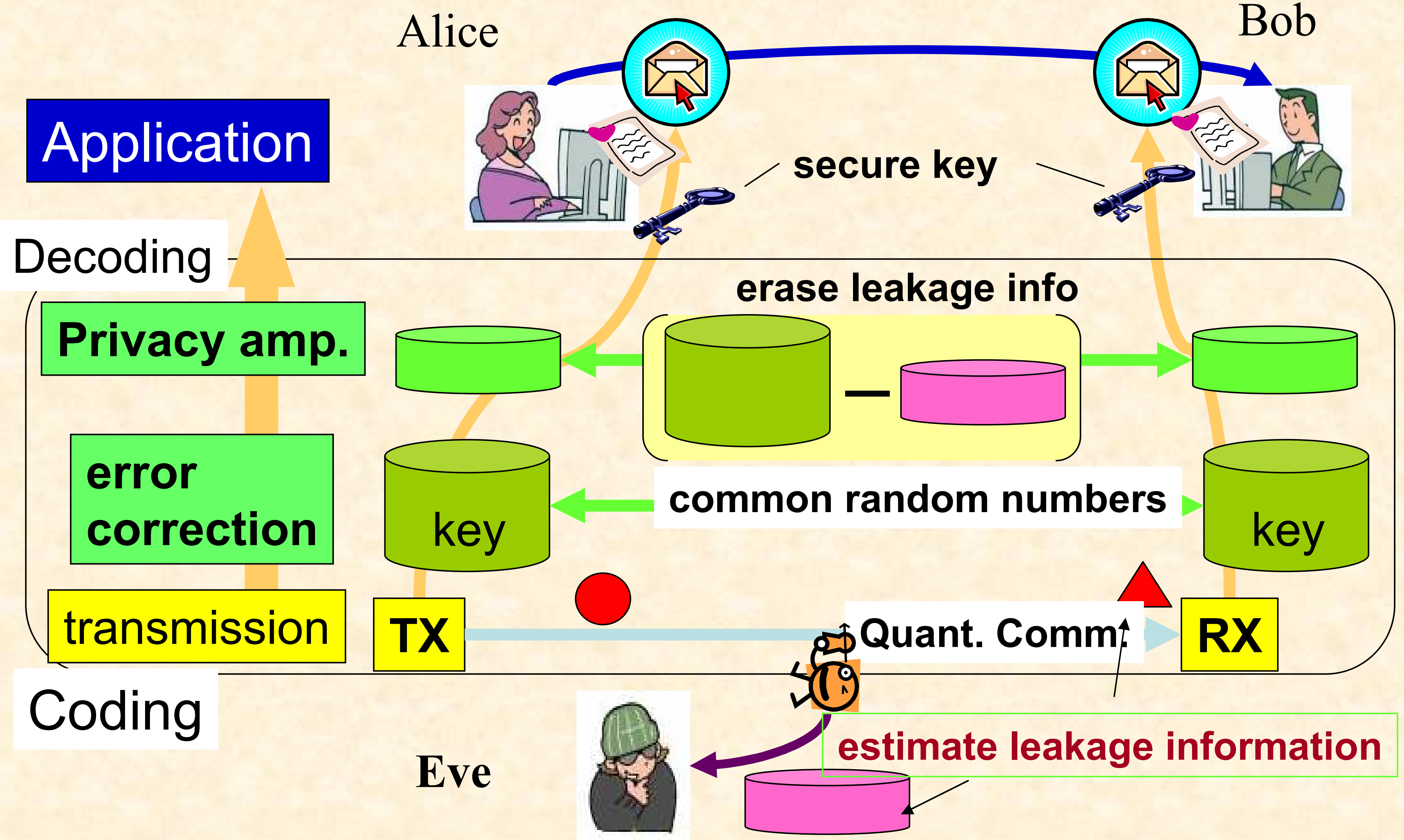
Eve's state

$$\bar{\rho}^E = \frac{1}{2^l}\sum_{[Z]} \rho^E_{[Z]}$$

$$\bar{h}(x) = -x\log_2 x - (1-x)\log_2(1-x)\ ;0 \le x \le 1/2$$

Alice's sent: l bits, final key: N bits

Secure key distribution with quantum communication



Error Correction Code

- Use redundancy to recover from error
- ex. correct one bit error

encoding : $0 \rightarrow (000)$; $1 \rightarrow (111)$

channel

$$\left\{\begin{matrix}(000)\\(100)\\(010)\\(001)\end{matrix}\right\} \qquad \left\{\begin{matrix}(111)\\(011)\\(101)\\(110)\end{matrix}\right\}$$

error correction

$(2^m\text{-}1, 2^m\text{-}1\text{-}m)$ Hamming code

- Parity check matrix $H=[I:P]$ $\quad m\mathrm{x}m: m\mathrm{x}(2^m\text{-}1\text{-}m)$
  - list 2^m-1 vectors of m bits $\quad$ ex. m=2

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

- Generator matrix $G=[{}^tP:I]$ $(2^m\text{-}1\text{-}m)\mathrm{x}m:(2^m\text{-}1\text{-}m)\mathrm{x}(2^m\text{-}1\text{-}m)$

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

- codeword $\quad \mathbf{c} = \mathbf{a}G \quad \mathbf{a} = \{0,1\}$

$$(000),(111)$$

- error $\quad \mathbf{v} = \mathbf{c} + \mathbf{e}$
- syndrome $\quad {}^t\mathbf{s} = H\,{}^t\mathbf{v} = H\,{}^t\mathbf{e}$

$$H\,{}^t\mathbf{c} = H{}^tG\,{}^t\mathbf{a} = \mathbf{0}$$

$$H{}^tG = \begin{bmatrix} I & P \end{bmatrix} \begin{bmatrix} P \\ I \end{bmatrix} = P + P = 0$$

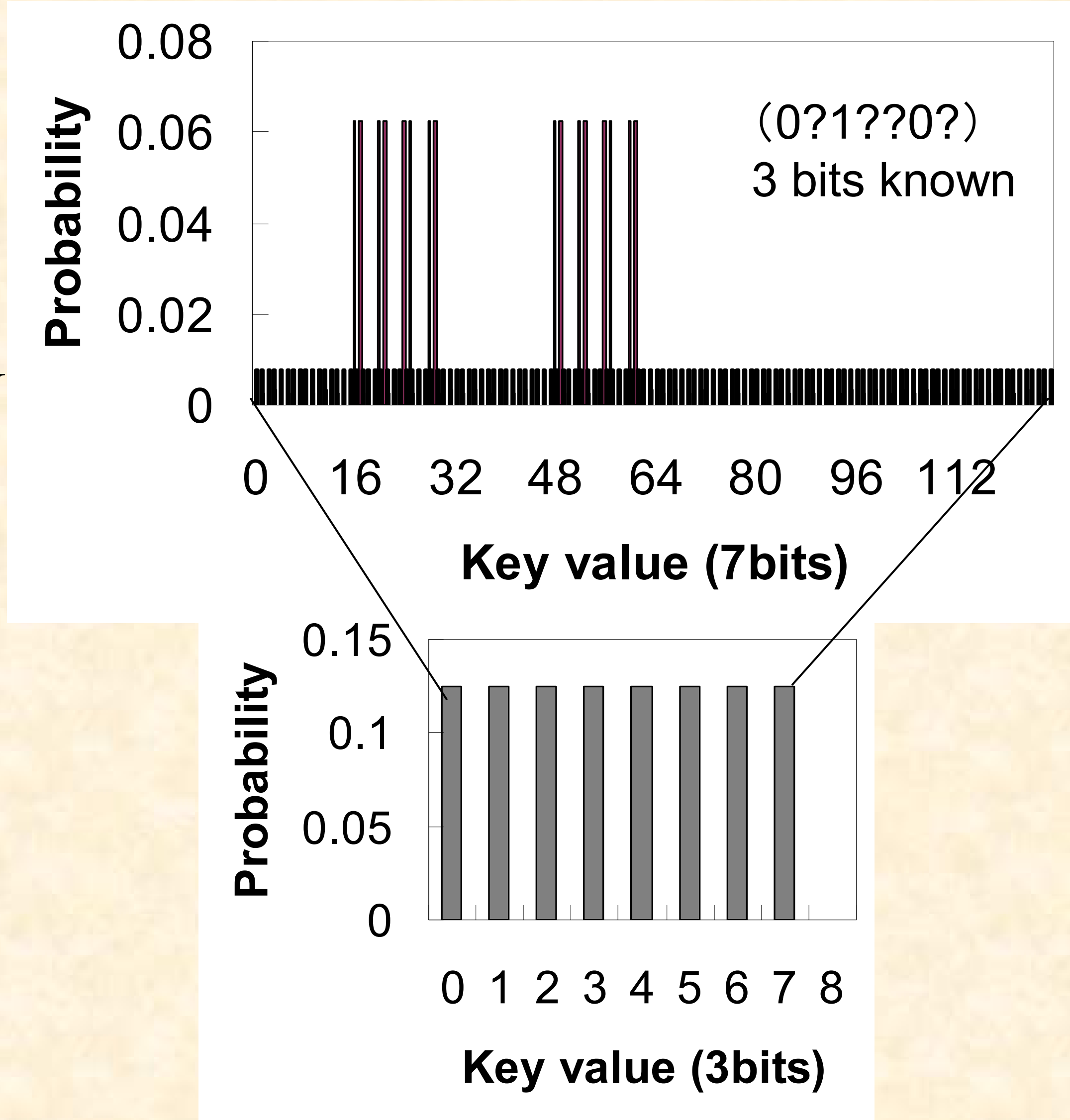
$$\mathbf{s}_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \mathbf{s}_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \mathbf{s}_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Privacy amplification

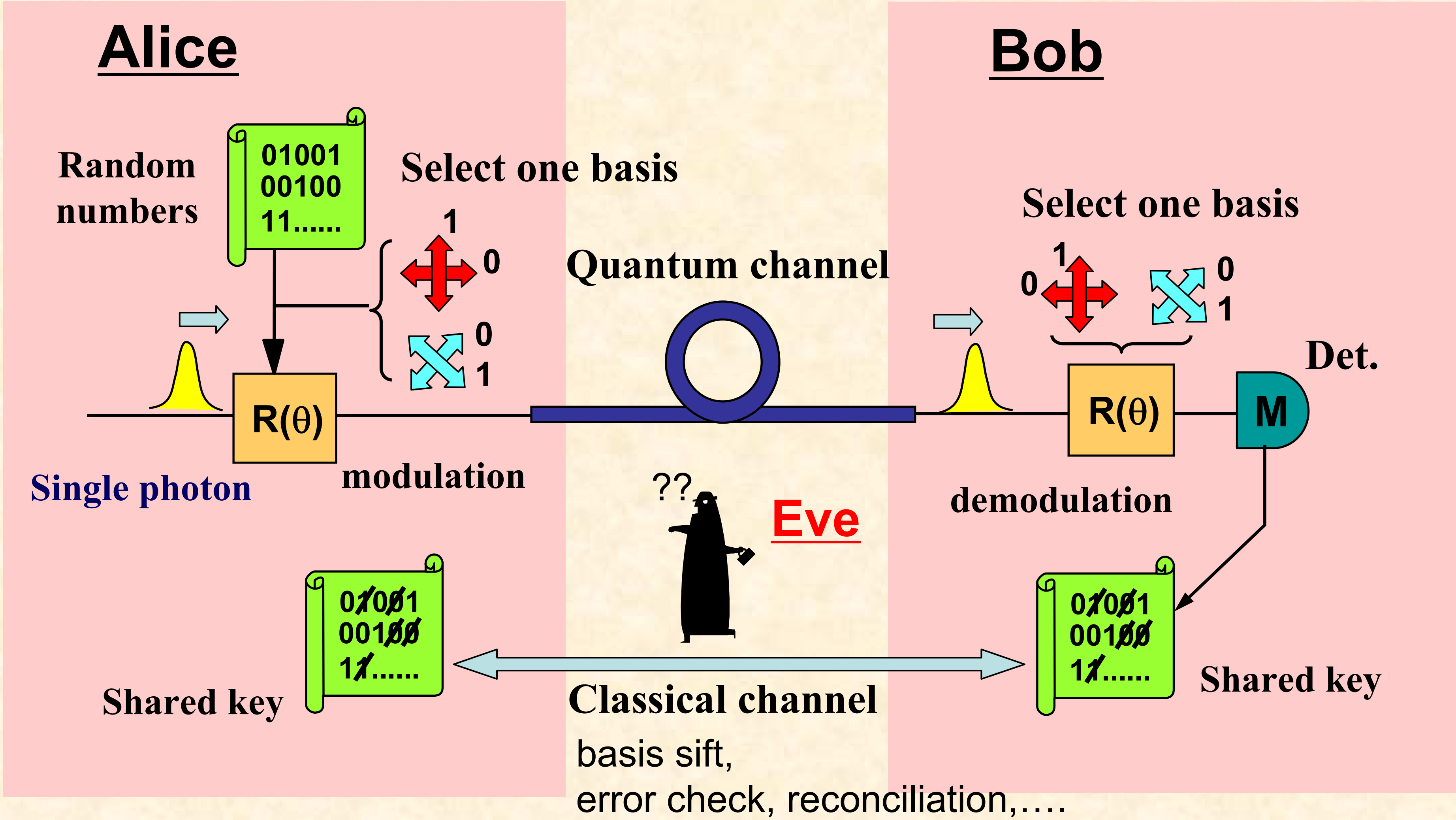
- Alice and Bob share N random bits W
- If Eve's knowledge about W is at most $\Theta < N$
- Alice and Bob can distill $N-m$ bits of secure key K, which satisfies

$$I(K) \le 2^{-\delta} \quad (\delta = m - \Theta),$$

with a random choice of universal hash function G (N-m x N) random matrix: $K=GW$



BB84 protocol



Assumptions on security proof of BB84

- Quantum mechanics is correct
- An authenticated classical communication channel exists
  - Eve can hear, but cannot modify
- Legitimated users are isolated from outside
  - eavesdropping is allowed only on the channel

Security proof of BB84 by Shor and Preskill

Shor & Preskill, PRL **85**, 441 (2000)

- A CSS code (quantum error correction code) to achieve unconditional security:

$\chi_E(R) \to 0$ with the rate $R = 1 - h(e_\times) - h(e_+)$

- assuming perfect devices (single photon source and single photon detector*)

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x)$$

* Mayers proved the unconditional security with imperfect photon detectors before Shor-Preskill (1996)

Improvement of security proof

- Classical error correction and privacy amplification (Koashi & Preskill)
- The above holds for finite length code in the sense that Holevo information is bounded by:
  $\chi_E \leq 2^{-\delta}$ (Hayashi)
- Imperfect photon detectors (Mayers, Koashi, ILM)
- Eve's information should be measured with Hoelvo information or distance norm to guarantee the universal composability (Renner & others)

Assumptions on BB84 protocol

ideal

- single photon source
  - one photon for one bit
- infinite computational resource
  - infinite code length (asymptotic)
- infinite code length, infinite time to measure
  - no estimation error
  - no fluctuation

practical

- weak coherent light
  - 0,1,2,.. photons for one bit
- finite memory capacity, execution time
  - finite code length
- finite code length, finite time
  - sampling error
  - fluctuation

Can we extract secure keys under the practical assumptions?

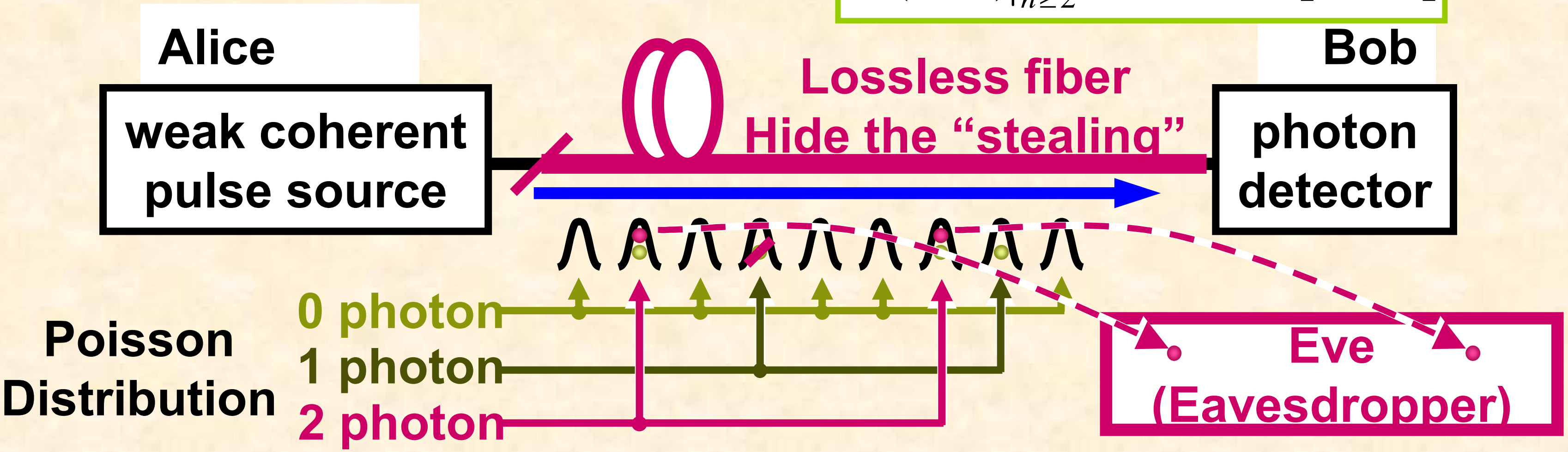
Yes, with decoy method.

PNS (Photon Number Splitting) Attack

➢ Effective attack on weak coherent pulse

Average Photon Number μ

$$\left.P(n,\mu)\right|_{n\geq 2} \geq 1-\exp[-T\mu]$$

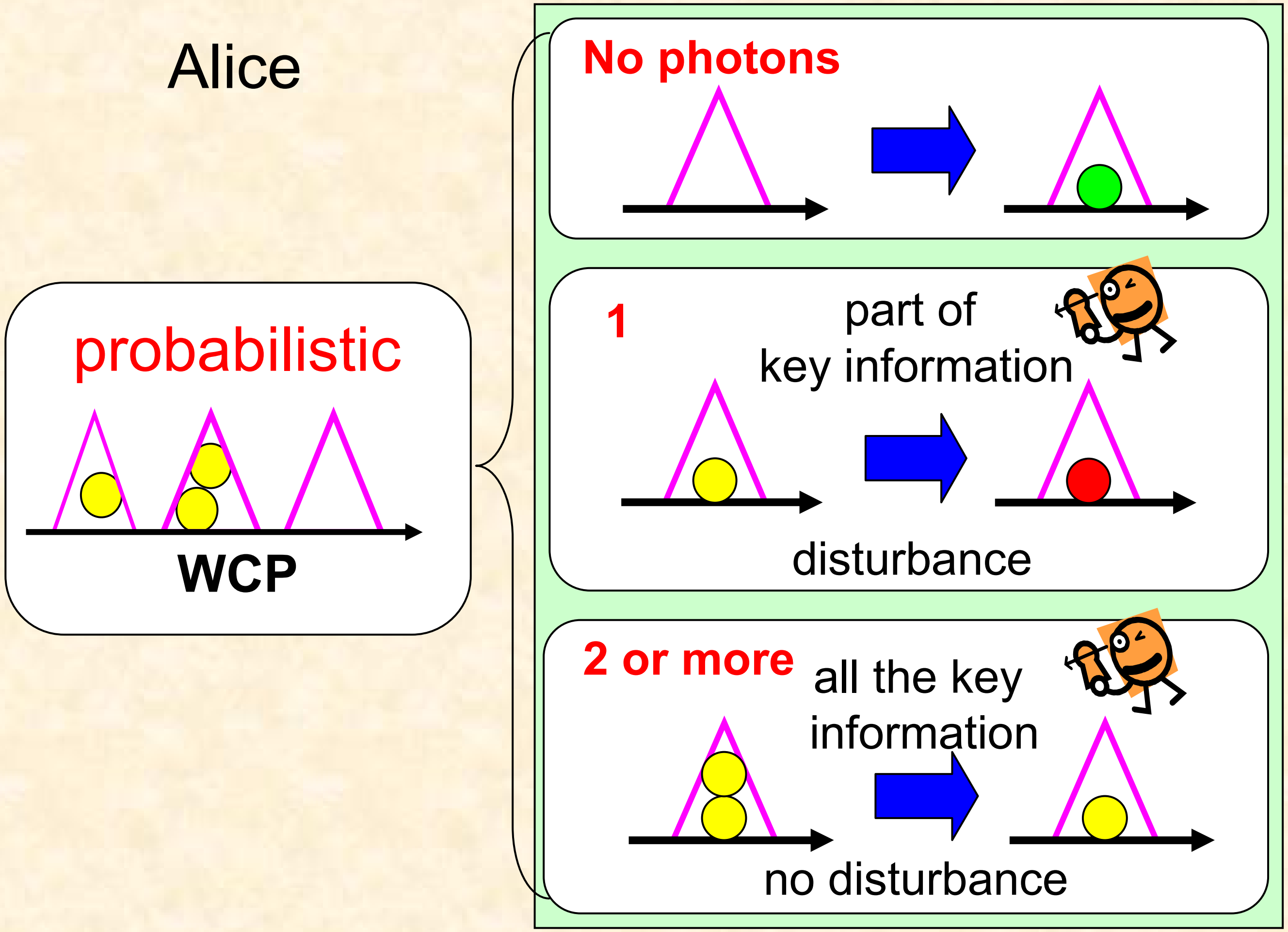


- If more than two photons in a pulse, take one and keep it. If one photon, cut the line.
- Measure the photon after the basis is open, and
- get full information.
- For large channel loss, Eve is not detected.

Information Leakage

Eve

Bob



detection events: J^0

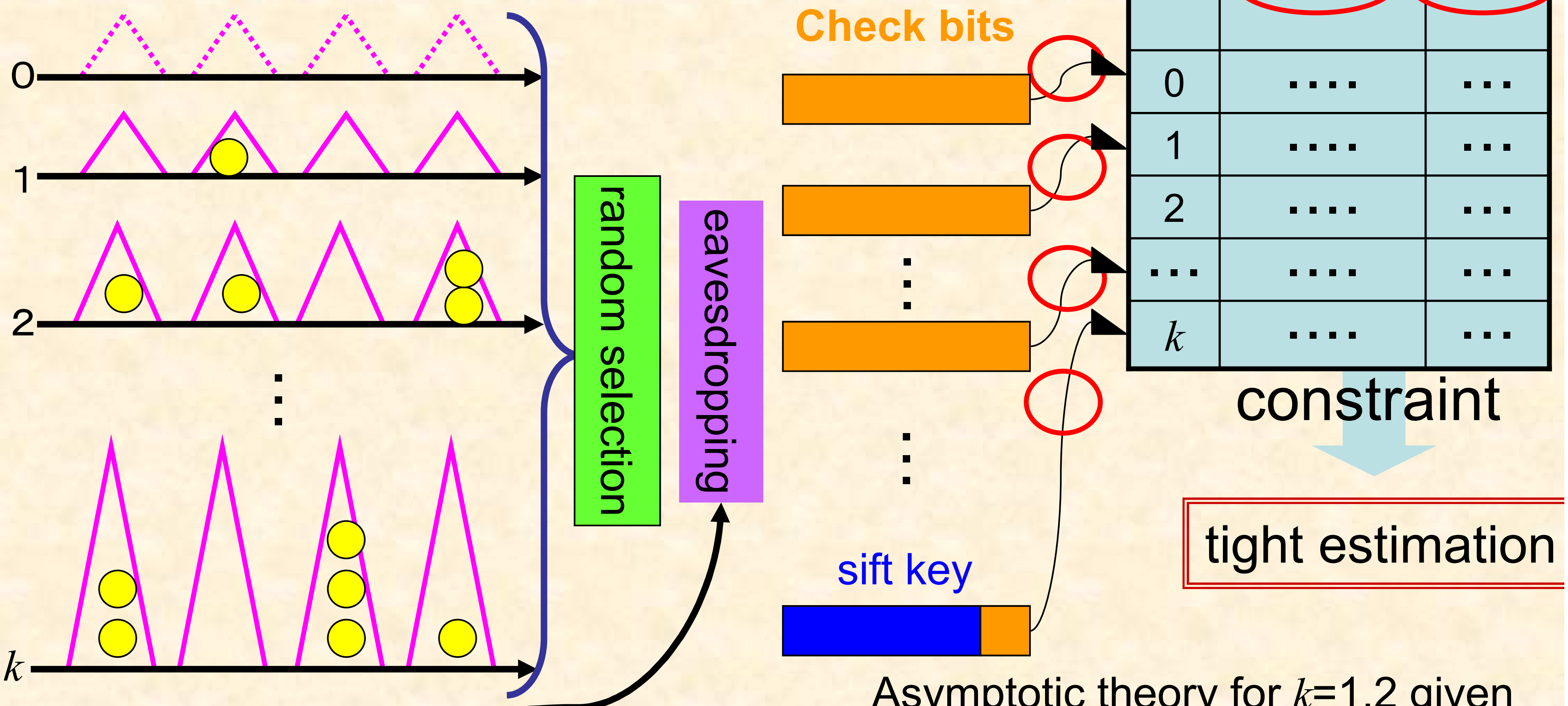
detection events: J^1
disturbed bits: t

detection events: J^2

Information on Bob's sift bit: $J^0 + J^1 \overline{h}\left(t/J^1\right) + J^2$ (GLLP04)

Idea of Decoy method

Decoy method [Hwang PRL **91** 057901(03)]



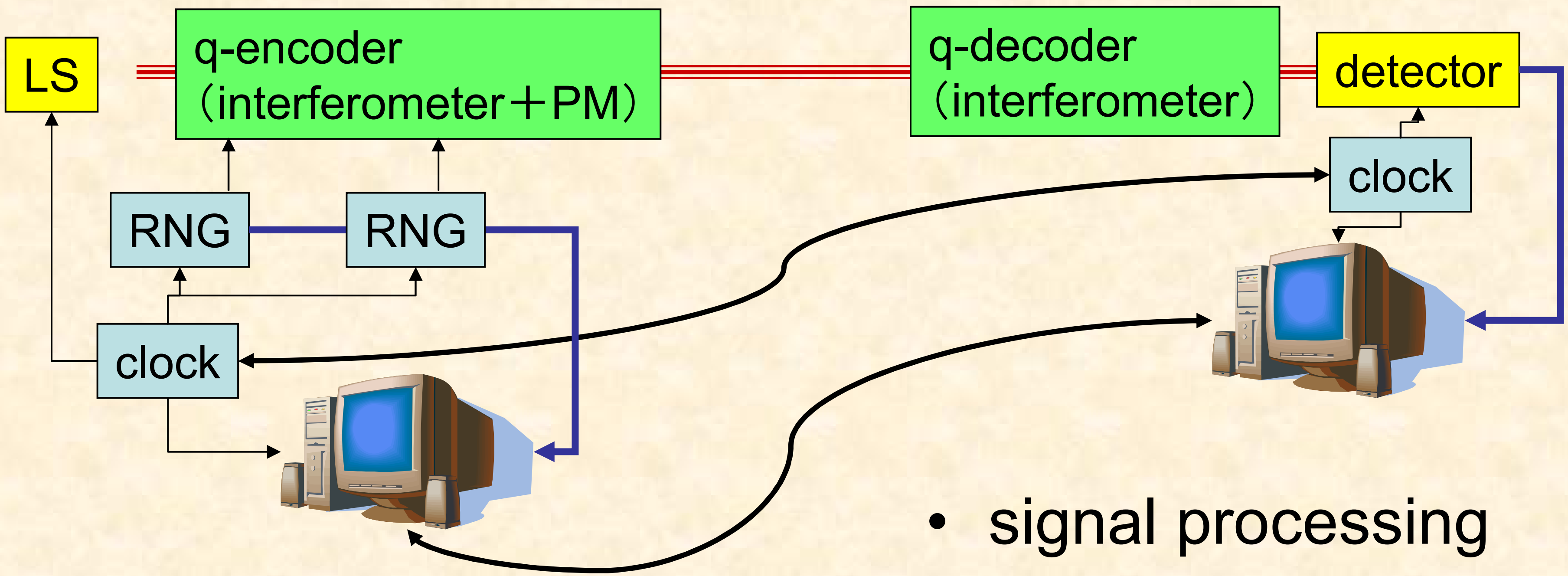
Photon number: known
Ave. photon number: unknown

Asymptotic theory for k=1,2 given by Wang PRL **94** 230503 (05) and Lo, et al PRL **94** 230504 (05)

Implementation: How to certificate security?

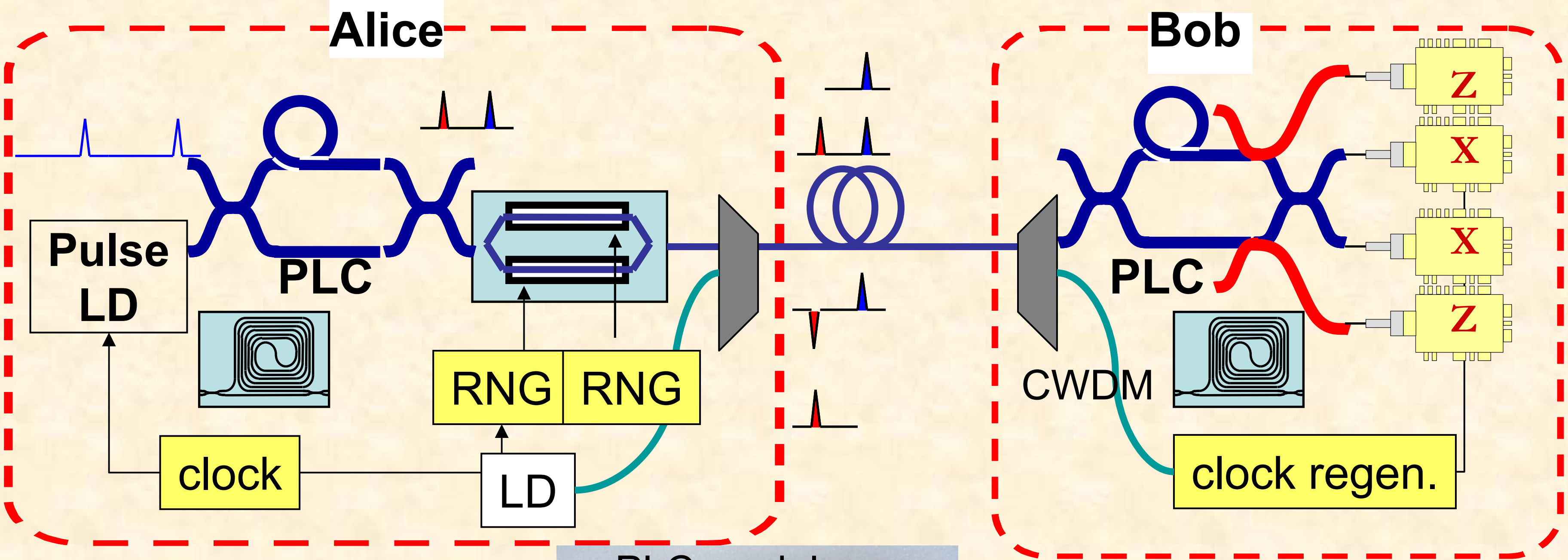
- Ingredients
- protocol
- process
- calibration/test
- qualification
- transport
- storage
- usage

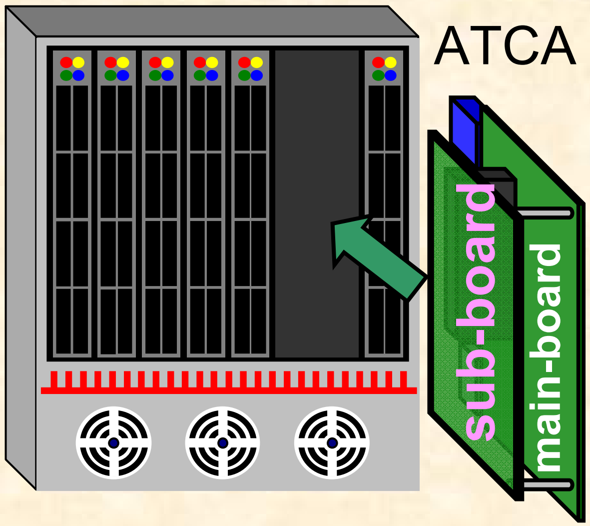
Making QKD equipment



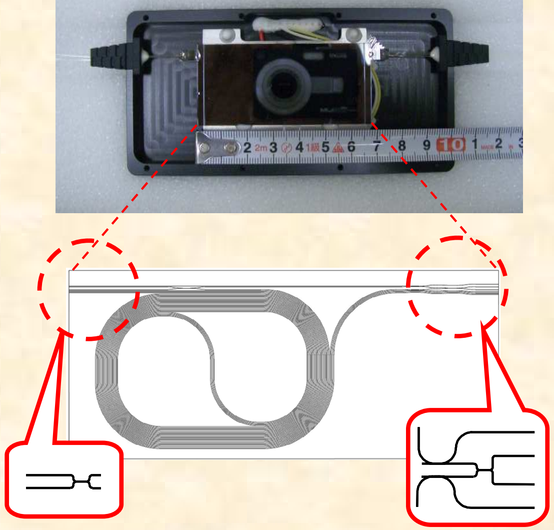
- q-commun.
  - Light Source
  - encode/ decode
  - detector
- control
  - clock sync.
  - RNG
  - frame sync.
  - temp.
- signal processing
  - raw key
  - sift
  - channel estimation (leakage information)
  - error correction
  - privacy amplification

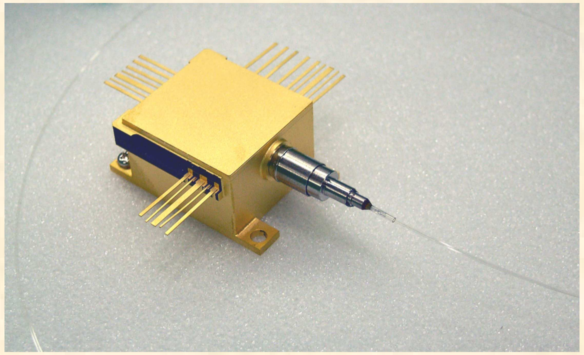
A QKD system under development





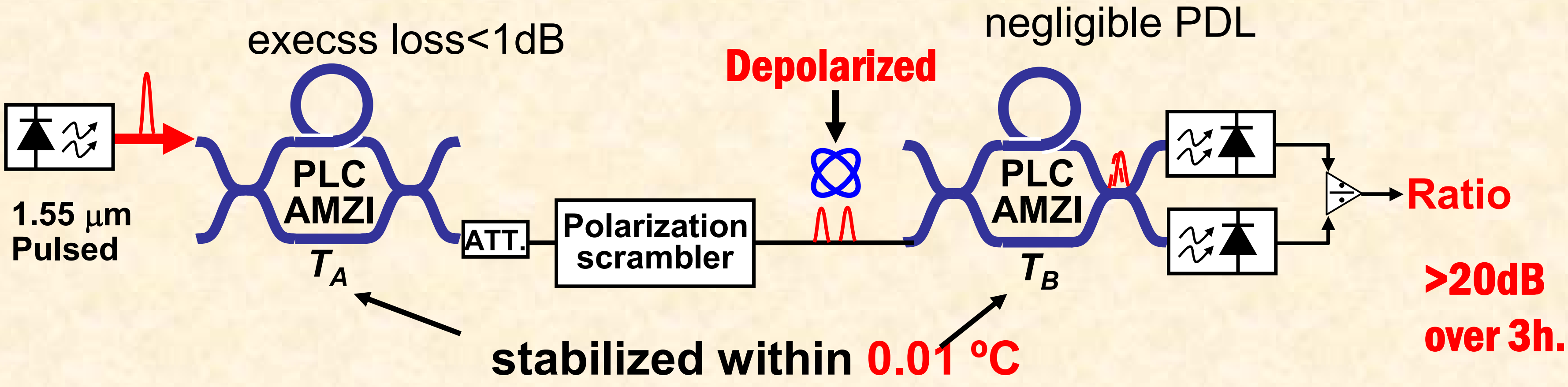
PLC module



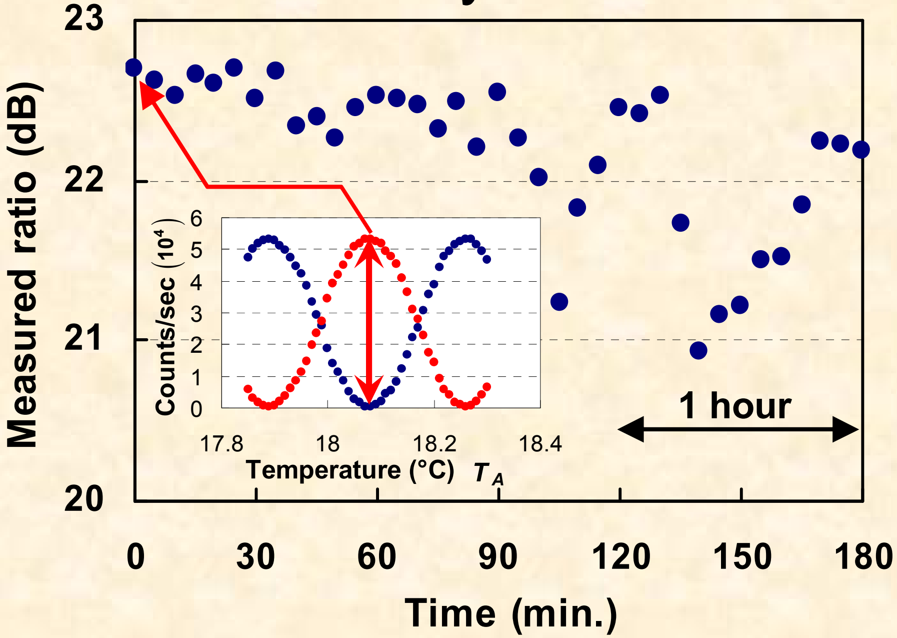


compact APD module

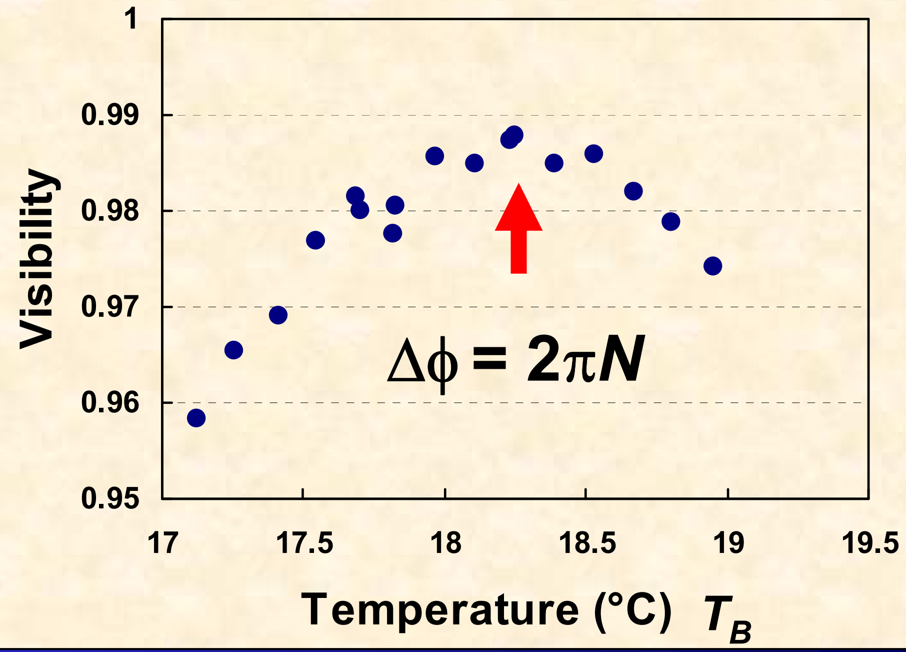
PLC characteristics



stability



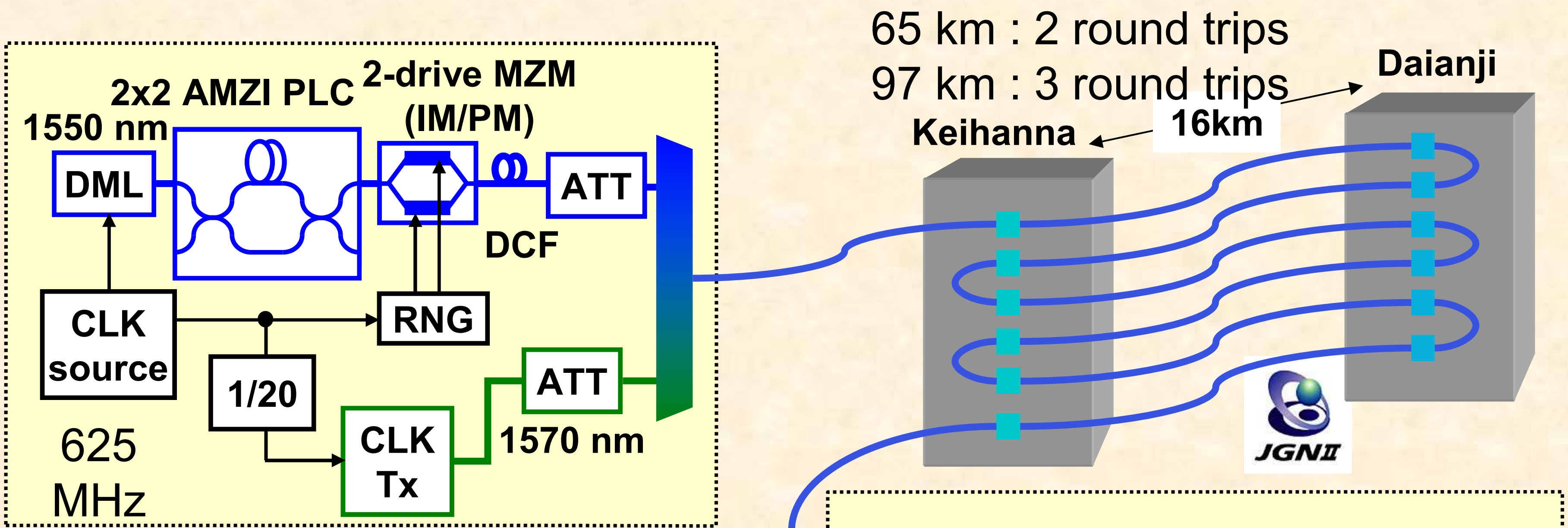
polarization independence



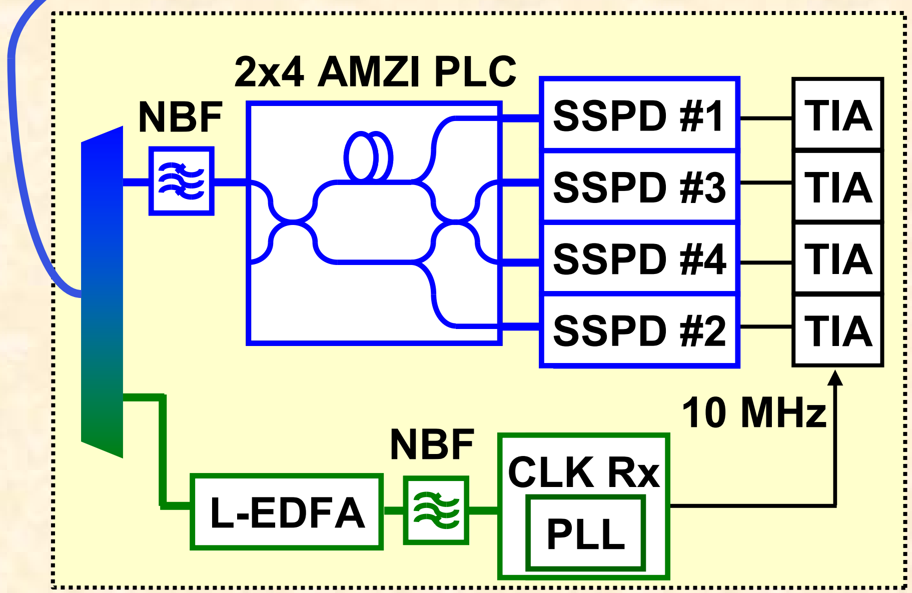
Issues for high speed operation

- high speed photon detector
  - APD (afterpulse, RF circuit)
  - SSPD
- True random number generator
  - LSI's
  - entanglement-based (built-in randomness)
- Signal processing circuit
  - high clock frequency, large memory, code length～1Mbit)
  - development of special purpose circuit board

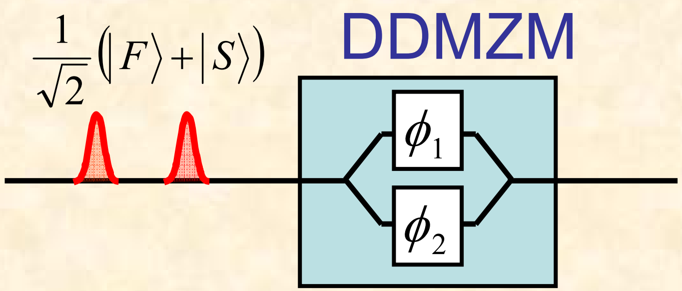
Field experiment of fast QKD transmission



Transmitter (Alice)



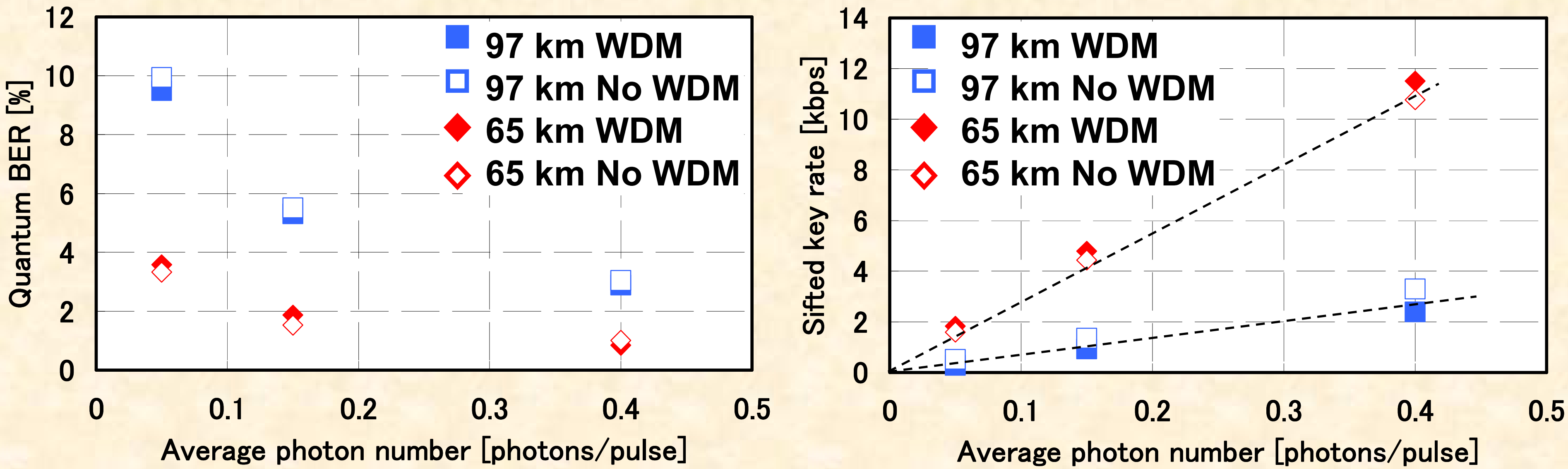
Receiver (Bob)



$$E_{out} = E_{in} \cos\left(\frac{\phi_1 - \phi_2}{2}\right) \cdot \exp\left(i \frac{\phi_1 + \phi_2}{2}\right)$$

Tanaka, et al; Opt. Ex. **16**, 11354 (2008)

Sift key transmission performance



- No degradation caused by WDM

  Nonlinear noise can be successfully suppressed
- Stable for more than 6 h
- Final key rate estimation using decoy

  μ = 0.4 photon/pulse
  μ' = 0.15 photon/pulse
  μ'' = 0.0 photon/pulse

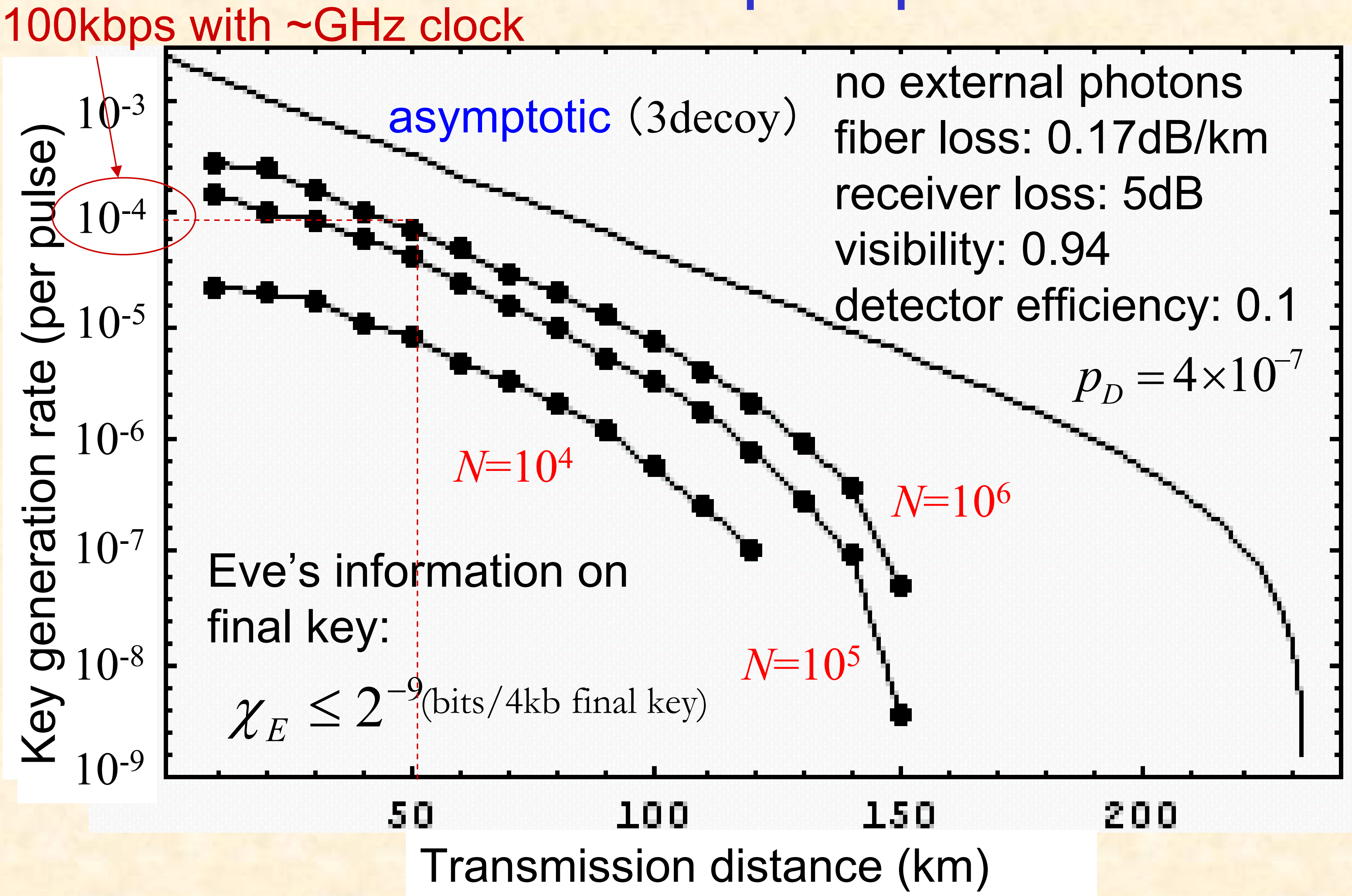
  ⇨ **Final key rate : 0.78 ~ 0.82 kbps** (asymptotic)

We could have claimed "secure QKD experiment," if done in 2002

What’s the problem?

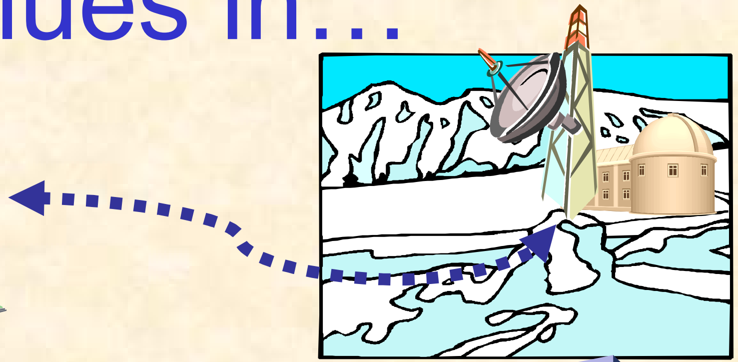
- Transmitter
  - PRNG
    - should be replaced by high speed TRNG
  - fixed intensities
    - should be change pulse-to-pulse
  - phase correlation between pulses?
    - no, we drove the laser in gain-switch mode.
- Receiver
  - different detector efficiencies
    - should be calibrated
  - passive basis choice
    - probably no problem
- Post processing
  - finite key
    - not yet
  - off-line
    - high speed electronics (hardware logic) under development

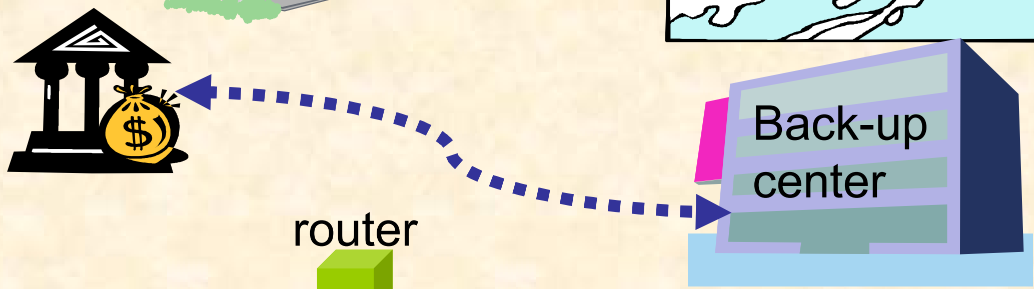
Performance prospect

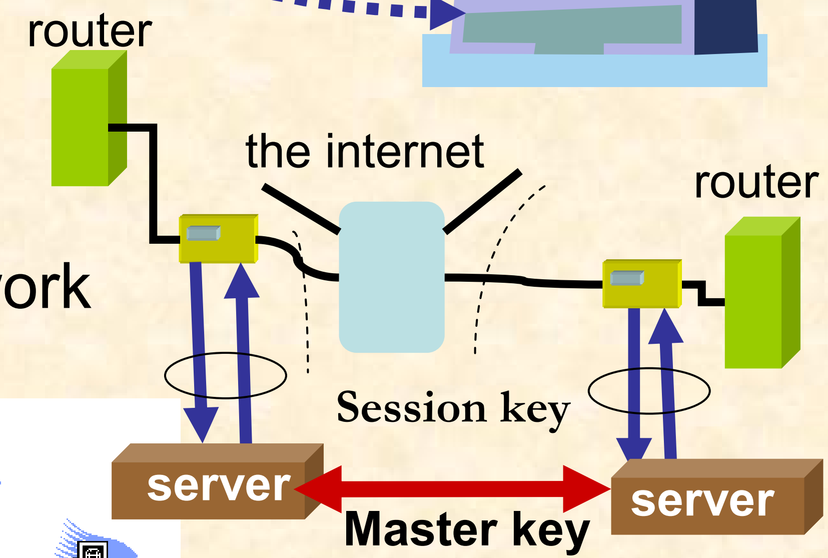


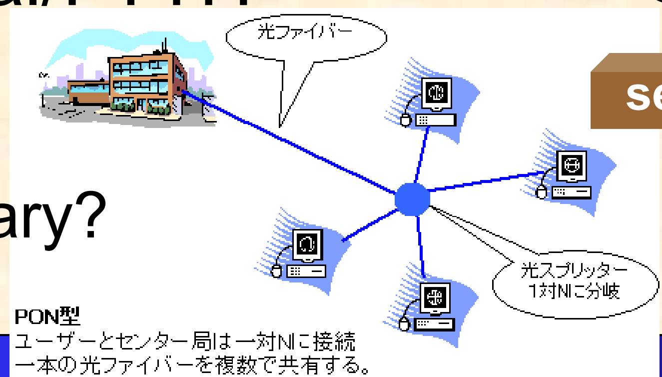
QKD provides Values in…

- Strategic information link
  - Extreme security (one-time-pad)
  - long distance
  - small market
- Key Infrastructure
  - Replacement of PKI (D-H key exchange)
  - compatibility with existing network
- ad-hoc/terminal/FTTH
  - weakest link
  - cost
  - really necessary?



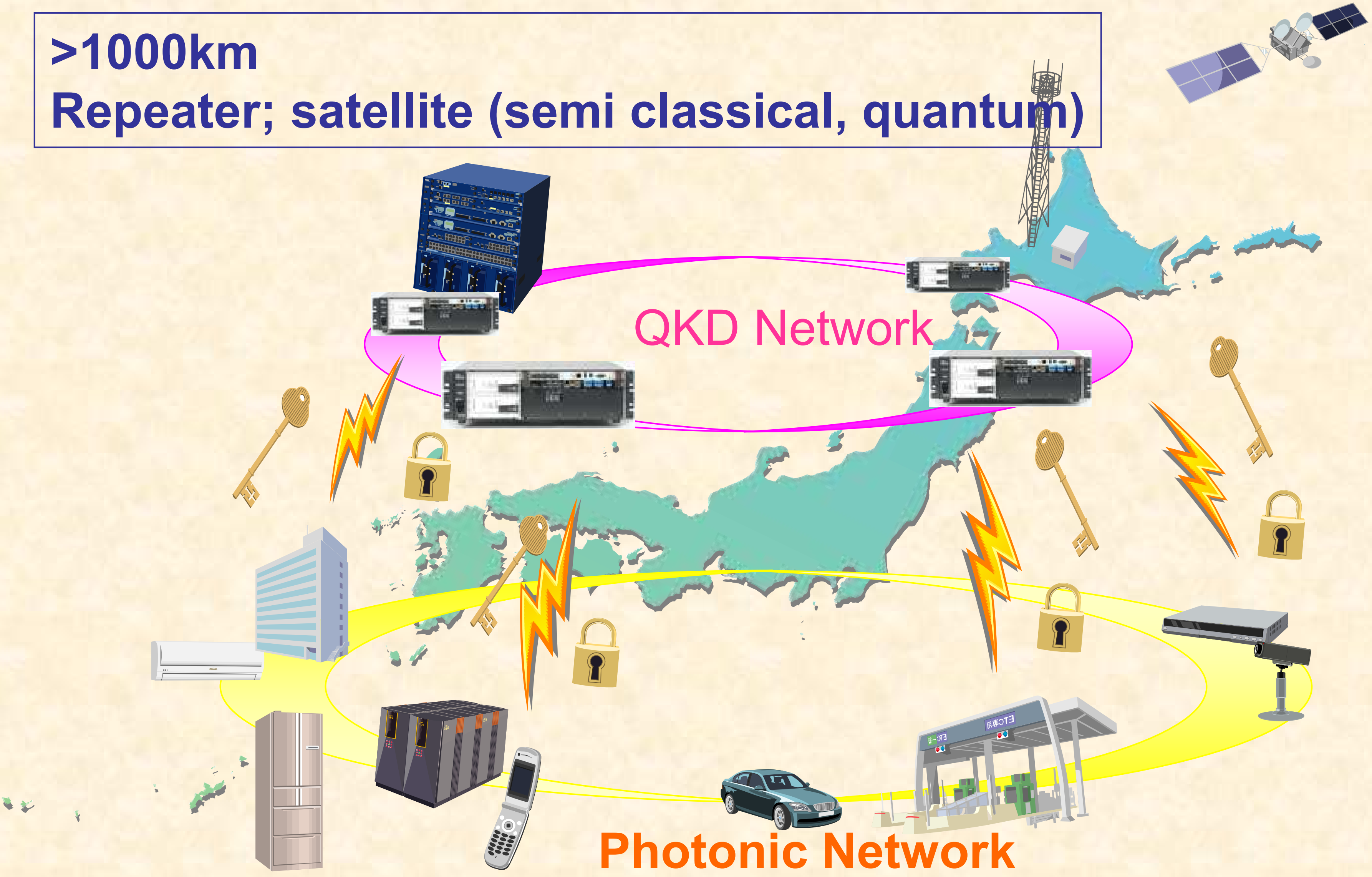




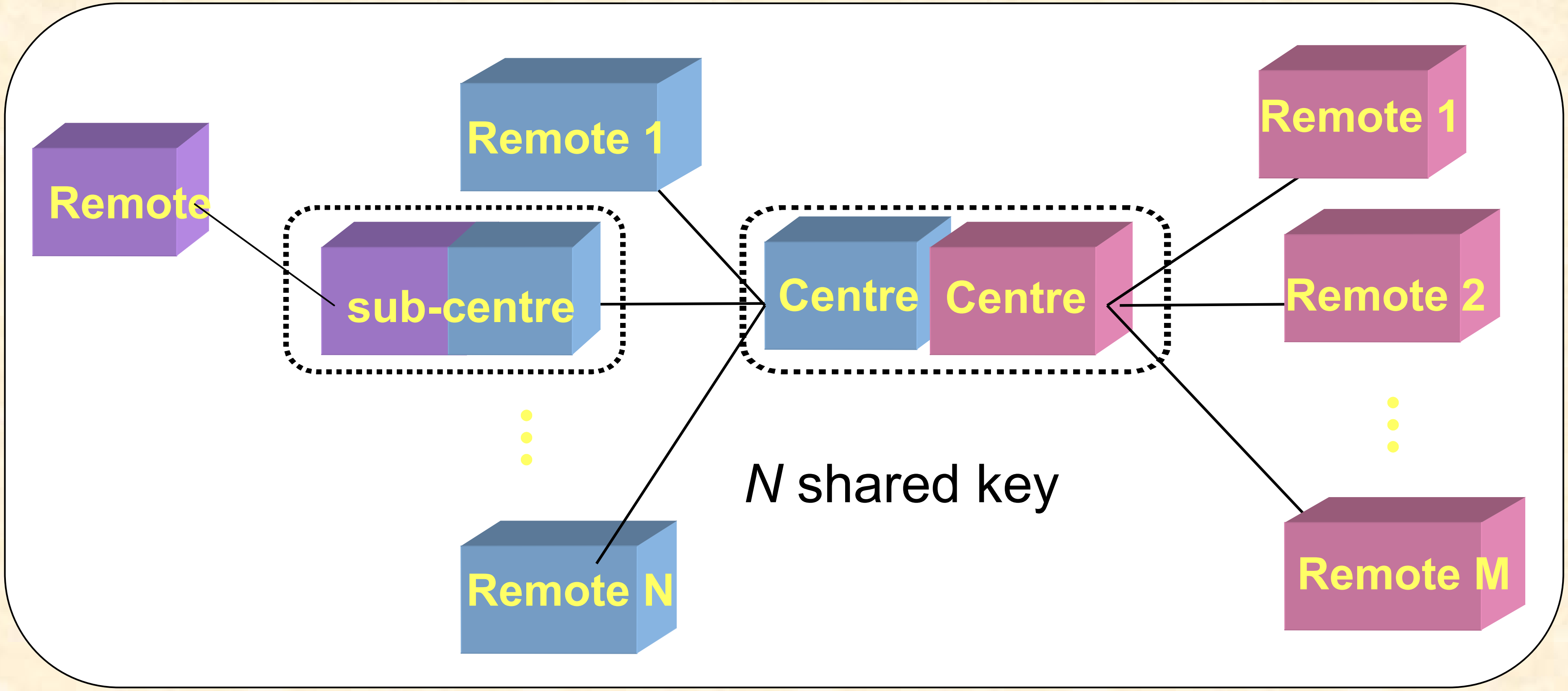


Highly secure network

>1000km
Repeater; satellite (semi classical, quantum)



QKD Network



- transmission (1:1, 1:N, N:M)
- relay
- key sharing
- monitor
- path-control
- buffer

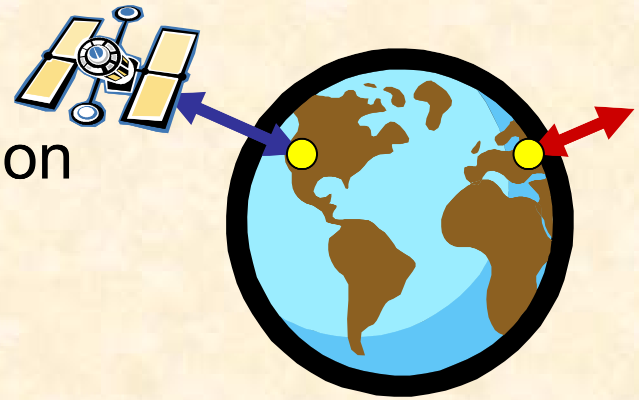
Interconnectivity

1. Functions
   - Interface between different venders' equipment
   - Common key file structures
2. Compatibility between systems
   - photon transmission
   - error correction (data exchange)
   - privacy amplification (data exchange)
3. Key synchronization
   - encryption/decryption
   - compensation of the difference on the specification
     - error rate
     - key (clock) rate

"classical" connection would be a practical solution

Satellite scenario for long distance transmission

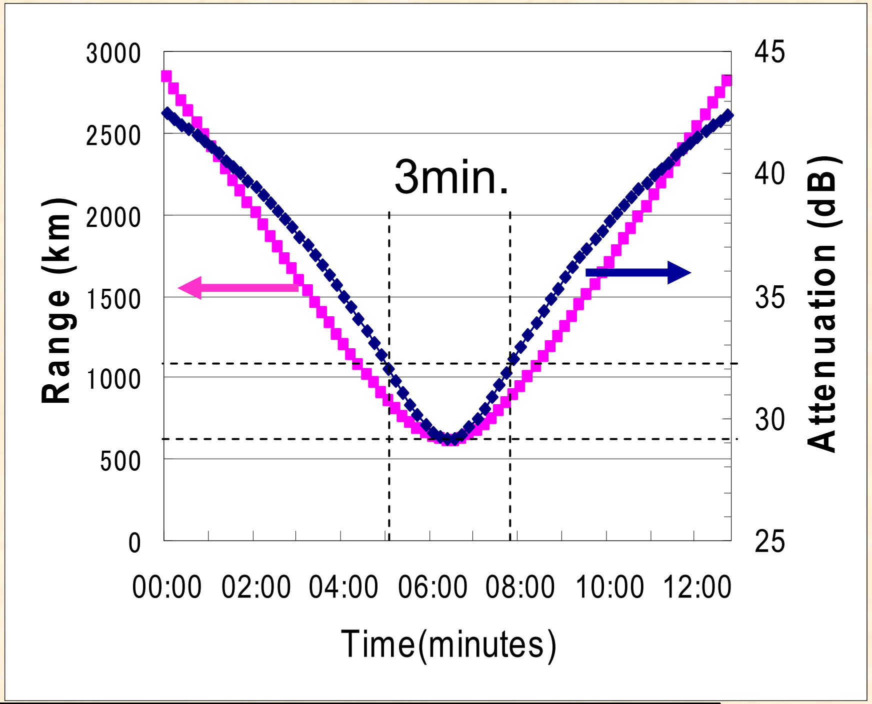
- Satellite as a trusted repeater
  - no limitation on transmission distance
- QKD experiments in free space (EU)
  - La Palma-Tenerife (144km)
  - entangled photons / WCP (decoy method)
    Nature Phys. **3,** 481 (2007)
    Phys. Rev. Lett. **98**, 010504 (2007)



Rapid intensity change from LEO

OICETS (Kirari) Circular orbit, altitude~610km

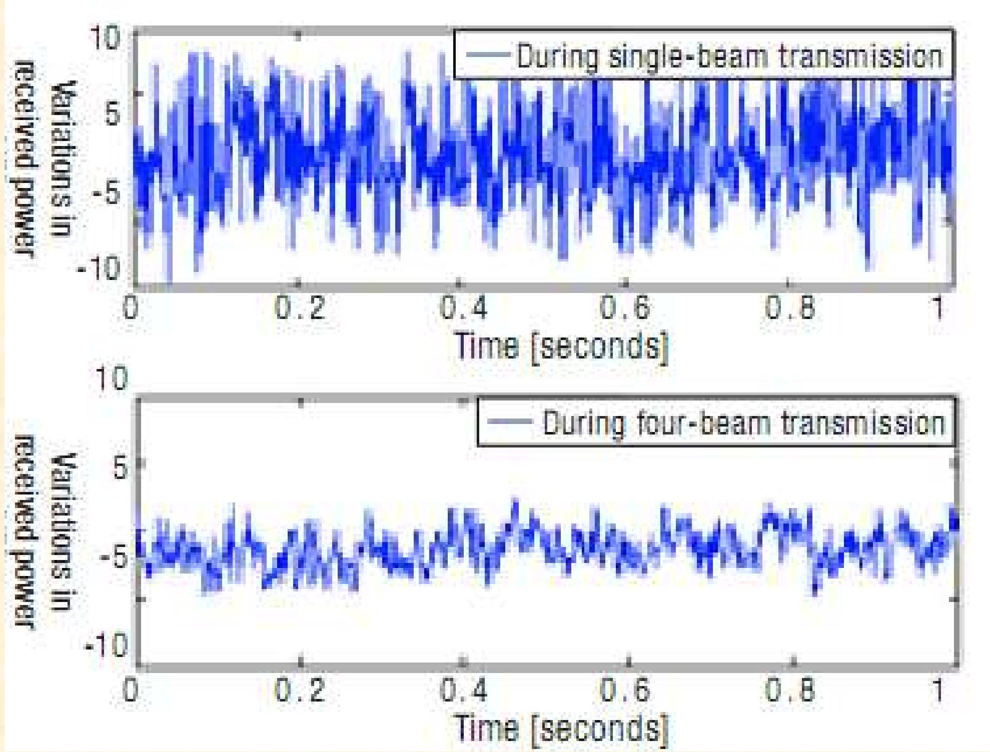
- Short time window ~3min
  - tracking
  - # of bits (not enough for good statistics)
  - timing (clock synchronization)
    - Δt~5ns demonstrated by Villoresi, et al (NJP**10** 033038 (2008))
    - higher clock?
- Intensity change by range, thickness of atmosphere
- can be compensated using orbital data.
  - Security? (Eve also knows it)



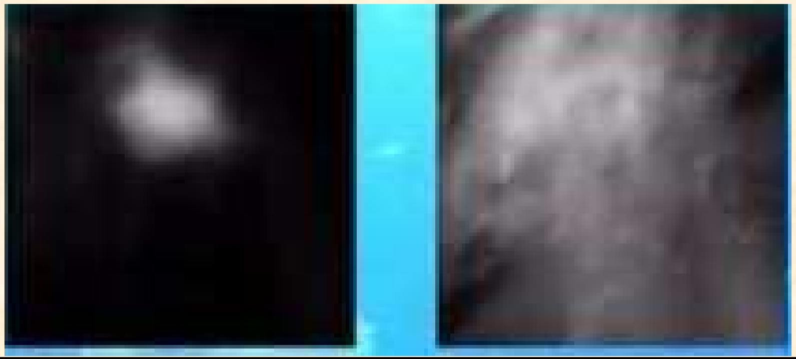
ground aperture(m)	0.3
LEO aperture(m)	0.1
wavelength	800
pointing loss	0.2
A_{atm} (dB)	1
Fried parameter	0.2
Transmission	0.8

Fluctuation by atmosphere

- Intensity/phase
  - wind, turbulences
    - distorted wavefront
  - temperature
    - refraction angle
  - scattering, diffraction by small particles
- Difficult to use decoy;
  - E91, or other protocols
    - key rate, statistics



Beam spot from the satellite (NICT)



LEO-Ground optical communication experiment by NICT (March & May, 2006)

Cryptography

- not complete with secure key distribution
- Functions of cryptography
  - Confidentiality
  - Integrity
  - Authentication

QKD may have crossed the Valley of Death

to get into the Darwinian Sea….

“Struggle for Life” in a Sea of Technical and Entrepreneurship Risk

Prof. Lewis M. Branscomb, Harvard University

conch shell

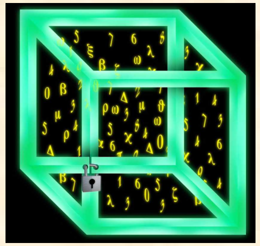
- Symbol of communication, security (Native American)
- ~~Symbol of tall talking~~ (Japanese)

To clarify what we can promise to the costumers

Conclusion

- Security proof on QKD has been almost established
- Successful proto-types have proved feasibility
- To survive in Darwinian sea
  - Propose business models
    - application
    - cost/value
  - Define specification
  - improve performance
  - system integration

collaborators



JST QCI pj.

- M. Hayashi (moved to Tohoku U.)
- J. Hasegawa
- T. Hiroshima

NICT

- M. Sasaki
- M. Fujiwara
- S. Miki
- Z. Wang
- M. Toyoshima

NEC

- A. Tajima
- A. Tanaka
- W. Maeda
- S. Takahashi
- Y. Nambu
- K. Yoshino

NIST National Institute of Standards and Technology

- S.-W. Nam
- B. Beak

NEC's work has been partly supported by NICT