

QCrypt2015

30th, September 2015
Hitotsubashi-hall, Tokyo,
Japan



HOKKAIDO
UNIVERSITY

Toward a security certificated communication system

- How we are learning to stop worrying

Akihisa Tomita

Graduate School of Information Science
and Technology, Hokkaido University

Collaboration

Decoy BB84 QKD System development

NEC

TOSHIBA

Leading Innovation >>>

Security Certification

 **NTT**

MITSUBISHI
Changes for the Better



Application

 NAGOYA UNIVERSITY

 東京工業大学
Tokyo Institute of Technology

MITSUBISHI
Changes for the Better

NEC

CV QKD & Physical Layer Crypto

Secure Photonic Network

NEC



 学習院大学
GAKUSHUIN UNIVERSITY



東北大学
TOHOKU UNIVERSITY

This work has been supported by and collaborated with

NICT



HOKKAIDO UNIVERSITY

Plan of my talk

1. Introduction

- Increasing threat on the security in ICT
- QKD and its security proof

2. Security Certification and Software Development

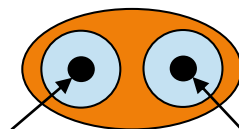
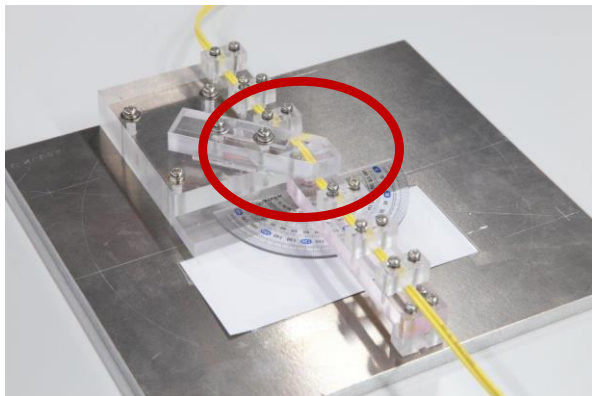
- Assumptions in security proof
- Requirements, design, evaluation
- Case study
 - phase correlation between pulses (experiment)
 - state preparation flaw (theory)

3. Toward quantum secure network



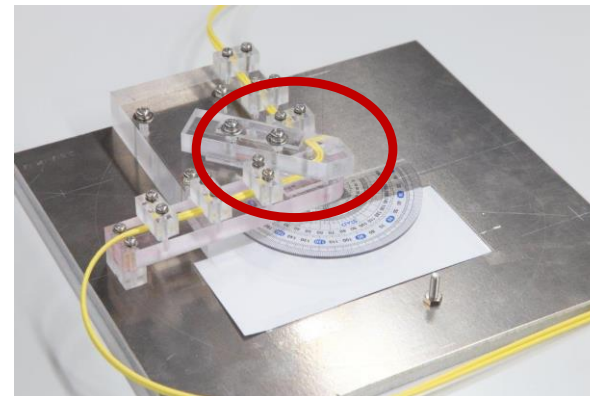
Eavesdropping on fiber communication


Light leakage in dual-core fiber



signal monitor

90deg. bend



signal

 monitor



– VPN Security only Virtual (Spiegel 1/2015)

- The NSA operates a large-scale VPN exploitation project to crack large numbers of connections, allowing it to intercept the data exchanged inside the VPN

Strengthened with Quantum key

– Lavabit

- US government ordered it to turn over its Secure Sockets Layer (SSL) private keys.
- All the collected email can be decrypted

– Logjam

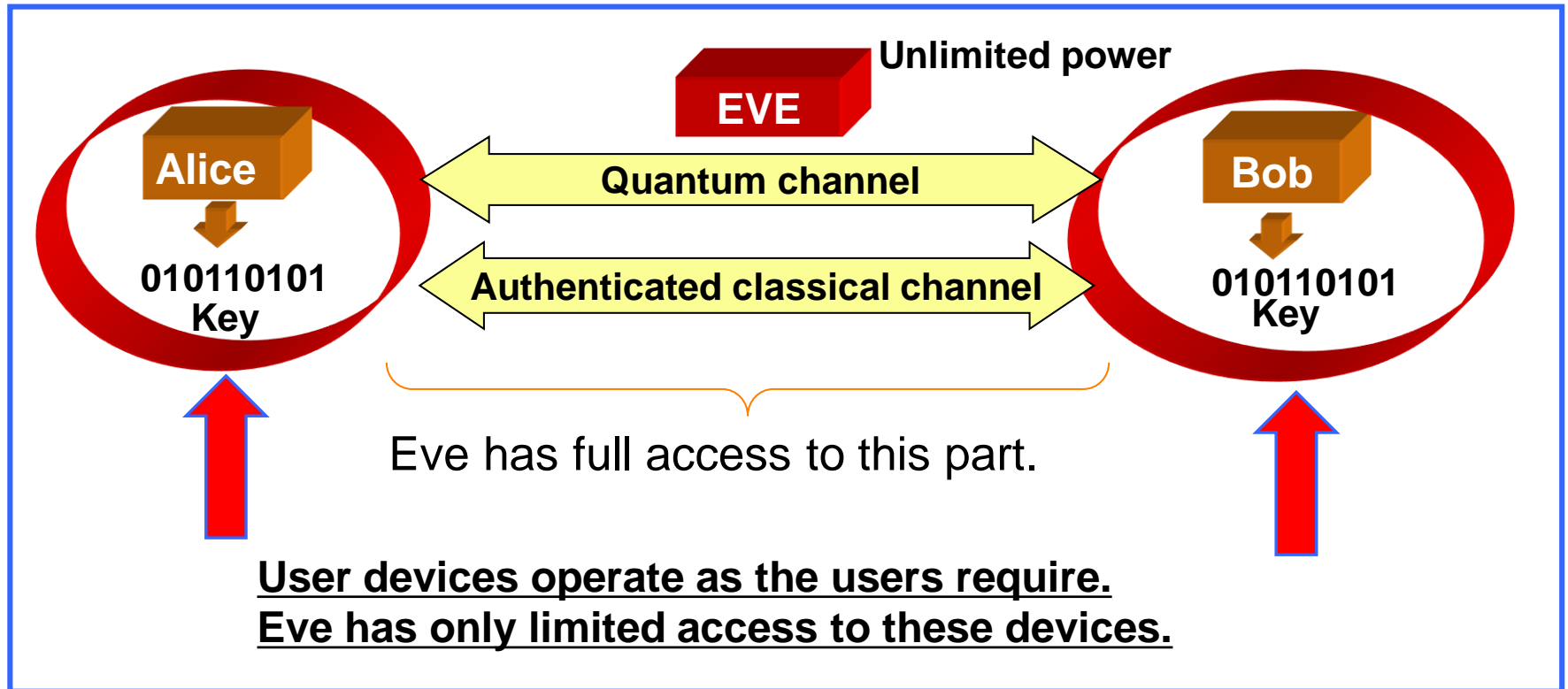
unconditional Forward Secrecy

Man-in-the-middle attack. Logjam persuades the server to use an old (weak) key exchange protocol in the negotiation phase.

No-update, no need to keep compatibility



QKD as a cryptographic primitive



- A QKD protocol provides **information theoretically secure key** shared by remote parties.
- It work as a supplier of shared key to other information-theoretically secure protocols



Feature of QKD

- Key generation procedure is composed of quantum communication and key distillation, *i.e.*, **physics** and **information theory**.
- **Information theoretical security**
= Key remains secure in the future, no matter how technology improved.
- **Quantitative guarantee of security** by estimating upper bound of leakage information from the statistics of quantum communication.
- Detection of eavesdropping
- **Universal Composability**.



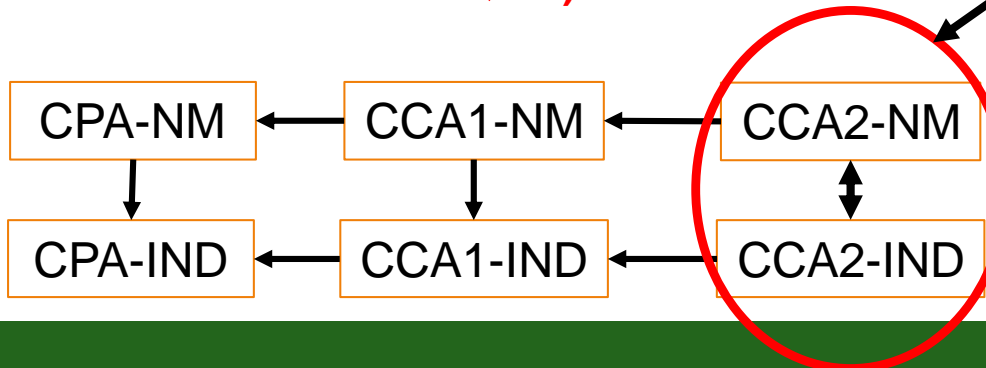
Security proof on modern crypt algorithms

Attacks

- **CPA** (Chosen Plaintext Attack) : cipher texts corresponding to the chosen plain texts are available.
- **CCA1** (Chosen Ciphertext Attack) : plain texts corresponding to the chosen cipher texts are available. (cipher texts are chosen before attack)
- **CCA2** (Adaptive Chosen Ciphertext Attack) : Cipher texts can be chosen during the attack, considering the information on plain-cipher pairs already obtained

Goal

- **perfect decryption** : whole plain text \Leftrightarrow **One-way (OW)**
- **partial decryption** : part of the plain text, or some information on the plain text \Leftrightarrow Semantic security = **IND: $E(m)$ is indistinguishable with $E(m')$ in poly-time**
- **falsification** : to create $C'=E(m')$ from $C=E(m)$ (A function F exists, s.t. $m'=F(m)$)
 \Leftrightarrow **non-malleable (NM)**



The strongest attack

- RSA-OAEP
 - OW-RSA and random oracle
- Cramer-Shoup
 - DH difficulty and universal one-way hash function



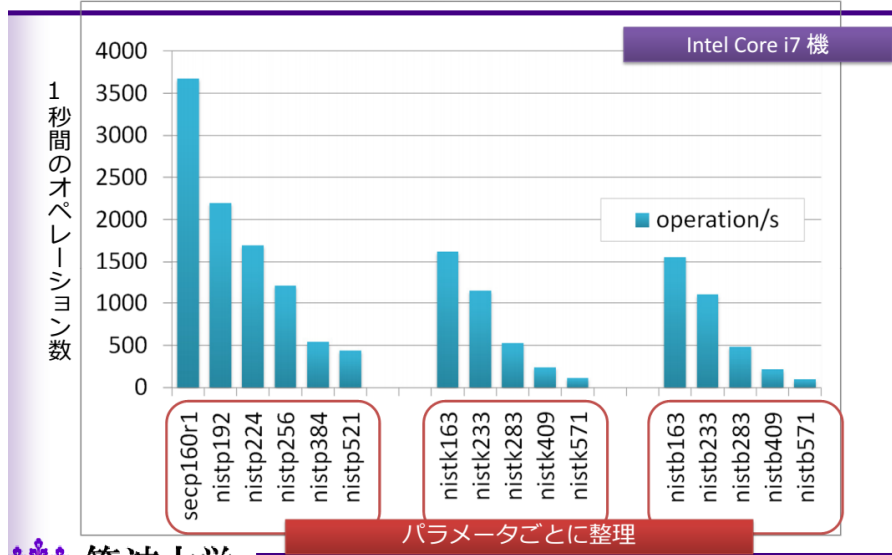
Universal composability

- QKD as a sub-protocol is secure,
 - if imperfection in key distribution (distinguishability to the ideal protocol) is not enhanced by the information from the upper-layer protocols
- ↔ ***The imperfection of the whole application is the sum of those of the component.***
 - equivalent to indistinguishability to the adoptive chosen cipher text attack (IND-CCA2) for public key crypt.
- Quantum information theory tells that ***trace norm distance will be never increased by any physically realizable processes (CPTP map)***
i.e., Eavesdropping cannot be improved = UC

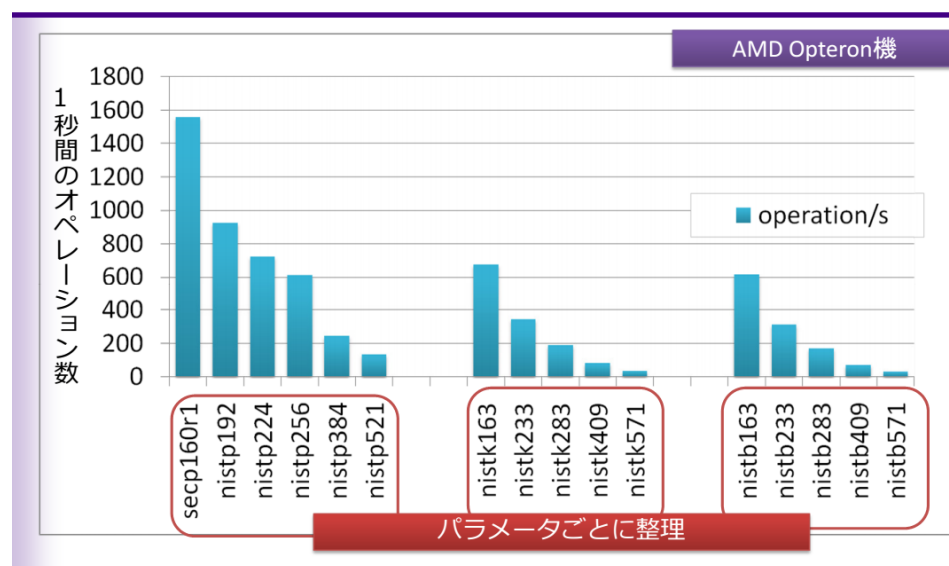


Did you think QKD is slow?

OpenSSL speedコマンドでの比較 : ECDH



OpenSSL speedコマンドでの比較 : ECDH



Bench mark test on key exchange by public crypt presented by Kanaoka (U. Tsukuba) on PKI Day 2011.

Generation speed was measured with speed command in OpenSSL for two servers:

1. CPU: Intel Core i7 920 (2.6GHz), RAM: 8GB, OS: Linux (CentOS 5.6)
2. CPU: AMD Opteron 1216, RAM: 2GB, OS: Linux (CentOS 5.6)

A 256-bit key in 1ms = **256 kb/s**, almost the same rate as QKD

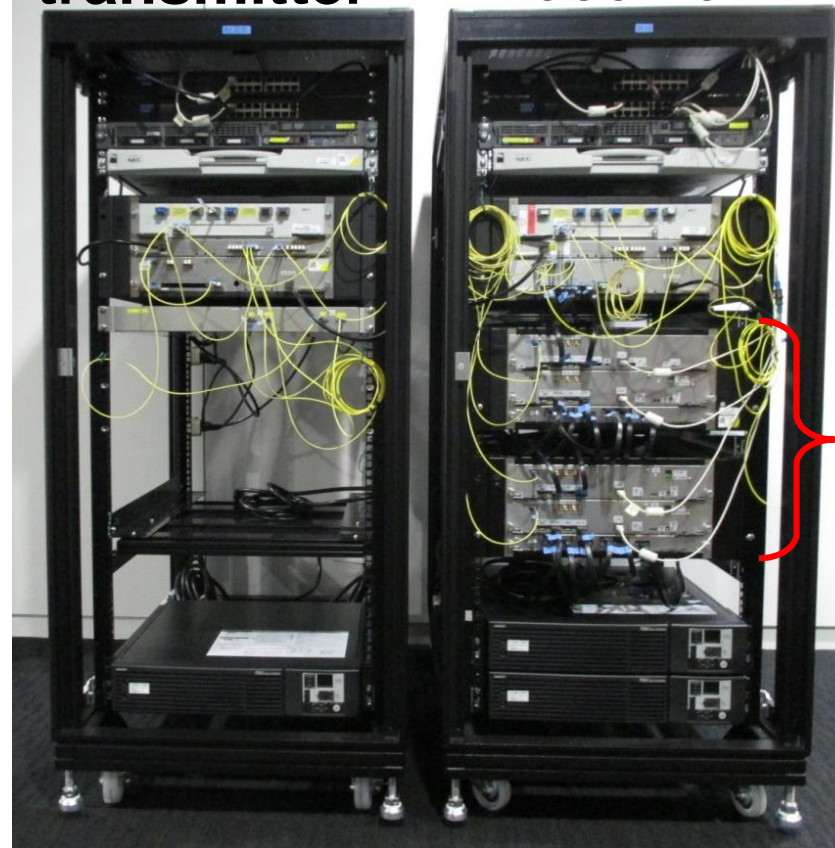
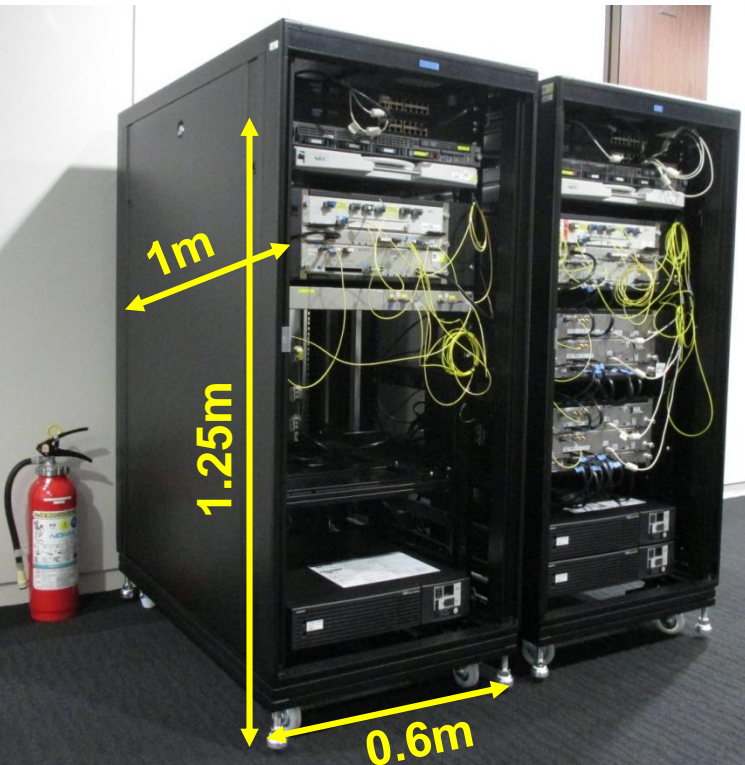


QKD equipment

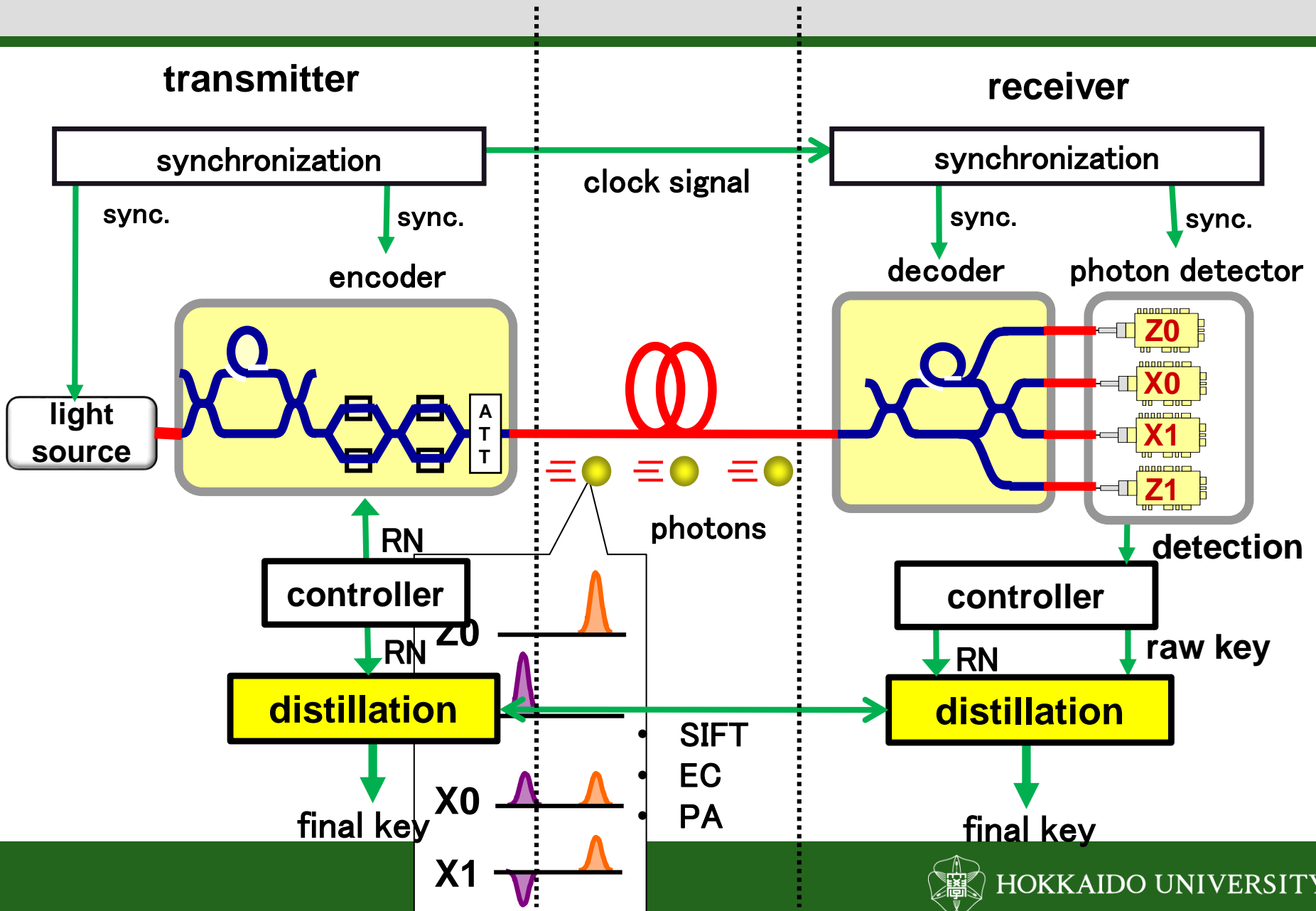
compatible with conventional lightwave communication equipment

transmitter

receiver

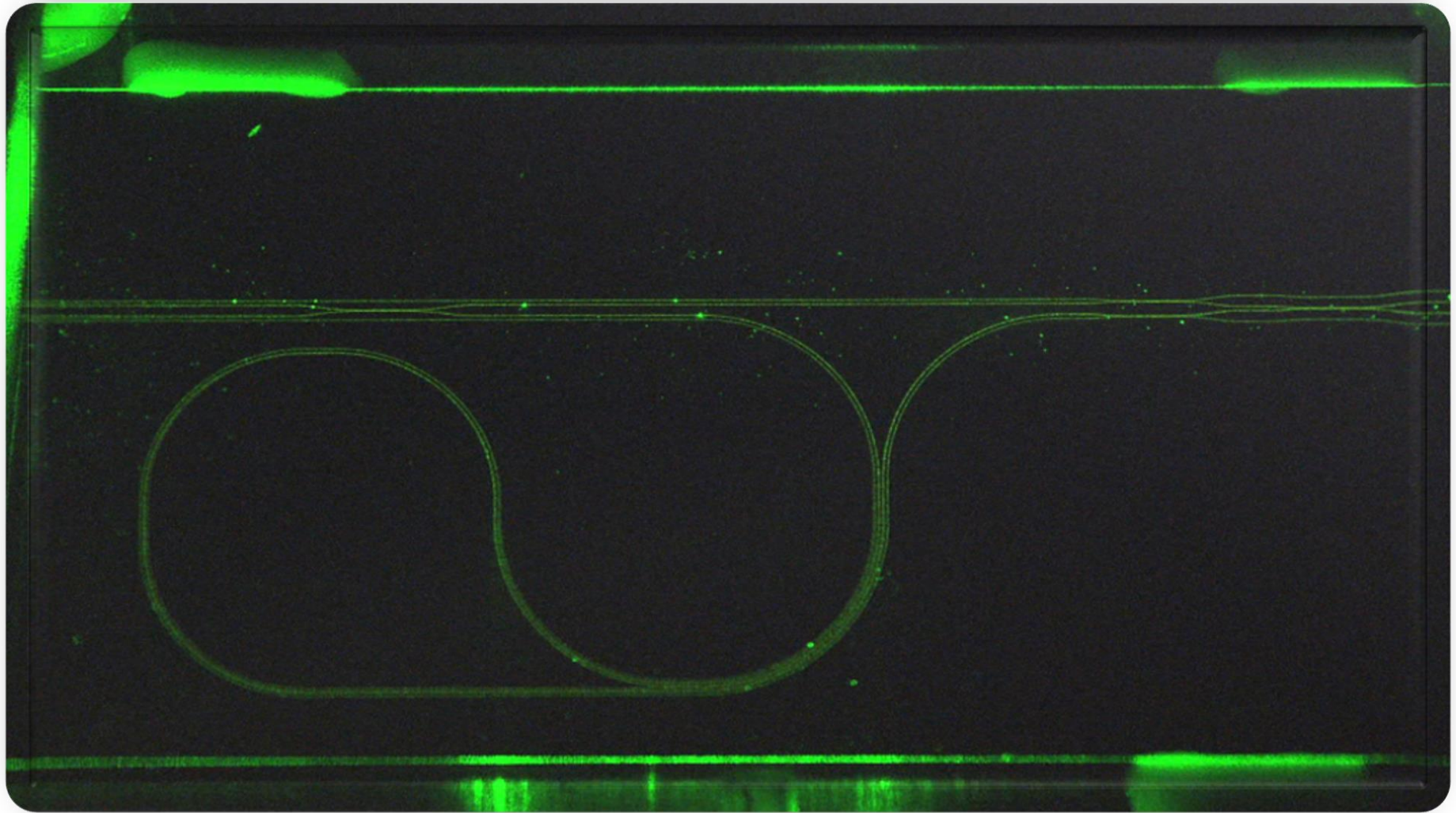


Construction of a QKD system



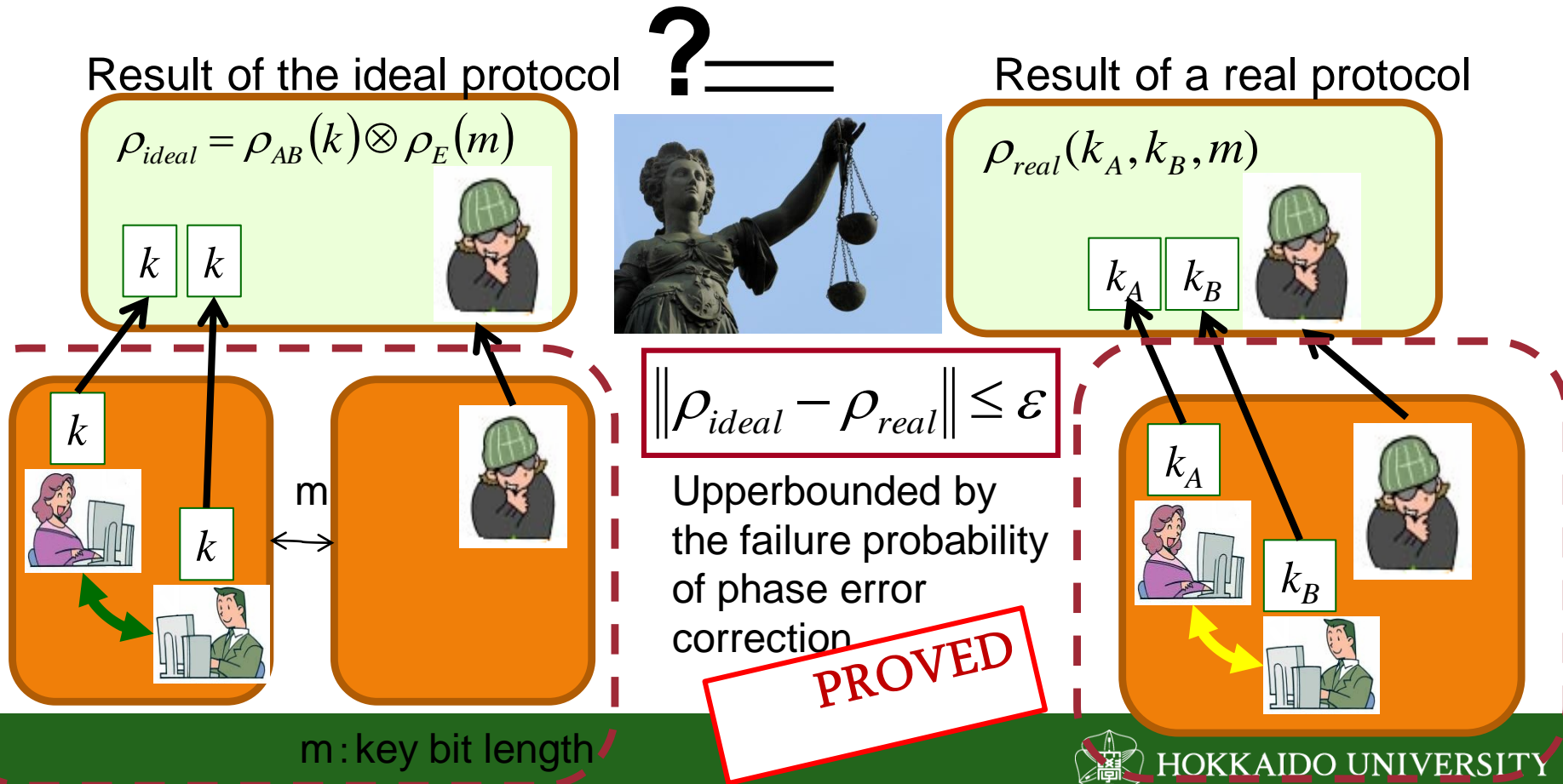
Asymmetric Mach-Zehnder interferometer

planar Lightwave Circuit on silica

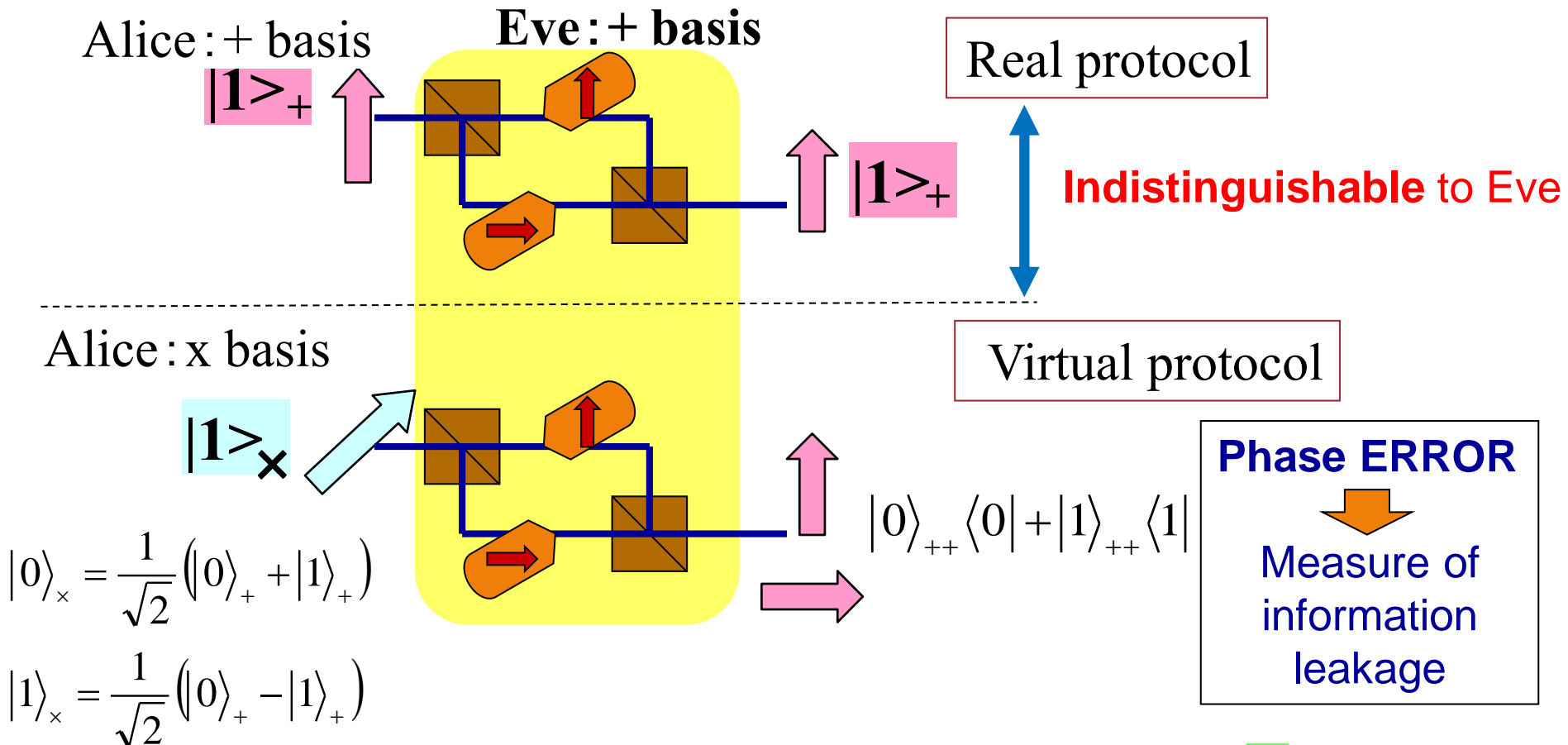


Security statement

A QKD system is secure, if an ideal (but virtual) judge tries to discriminate a real protocol from the ideal protocol with resulting density matrices but **fails**.



Physics behind the security



$$\|\rho_{A,E} - \rho_{ideal}\| \leq 2\sqrt{2}P_{ph} \leq 2^{N\bar{h}(n_e/N) - m + 3/2}$$

Sacrifice bits

M. Hayashi and T. Tsurumaru, New J. Phys. **14**, 093014 (2012)



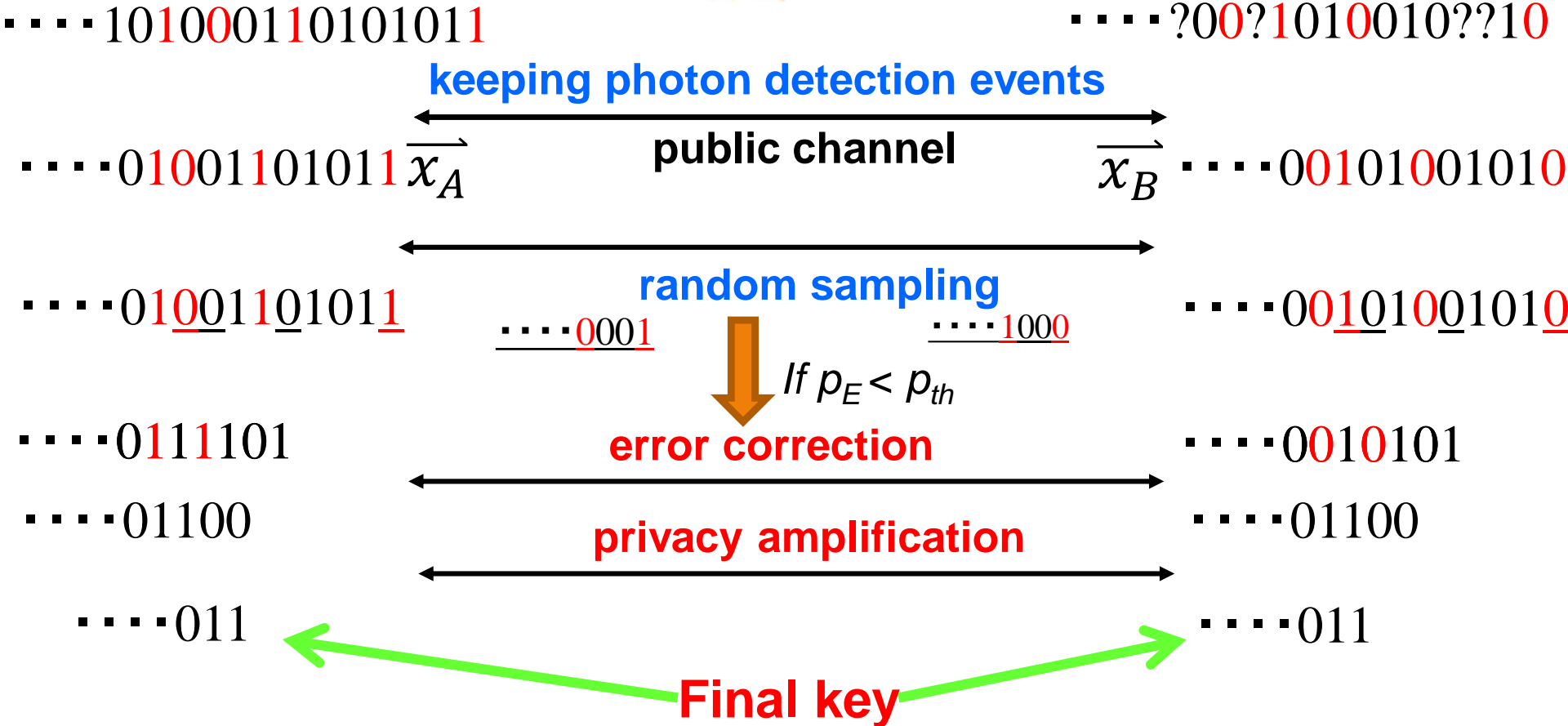
Key Distillation



Alice



Bob



Key Distillation



Alice



Bob



... 101000110101011

... ?00?1010010??10

← keeping photon detection events →

... 01001101011 $\overrightarrow{x_A}$

public channel

$\overrightarrow{x_B}$... 00101001010

... 010011010111

... 0001

← random sampling →

... 1000

... 00101001010

Failure in error rate estimation results in **INSECURE** final key

For a true value e , $\Pr\{e \in (p_E - \delta, p_E + \delta)\} \geq 1 - \varepsilon$

$\varepsilon = e^{-N\delta^2}$: $N = |\overrightarrow{x_A}|$ Long code length decreases error probability

Ex. $\delta=0.5\%$: $N=1\text{Mbit}$ (10Mbit) $\Rightarrow \varepsilon=10^{-11}$ (10^{-109})



Key Distillation

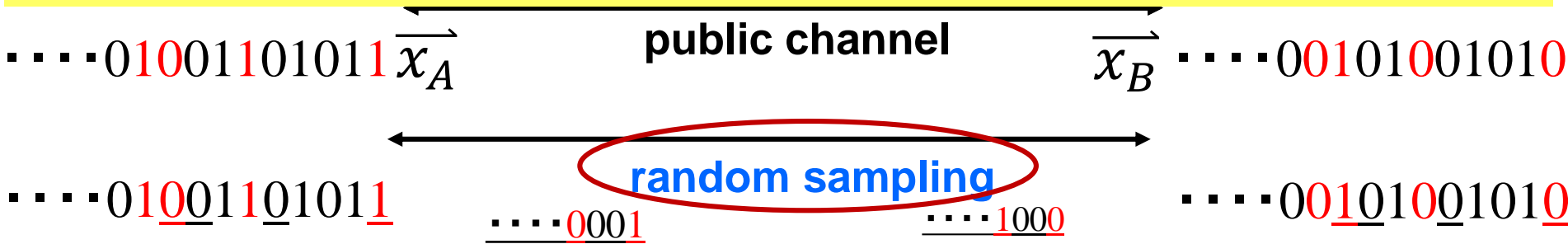


Alice



Bob

Ex: $\epsilon=10^{-11}$ \Rightarrow Suppose we generate one final key per second, the key will leak only once in 3000 years in average.



Failure in error rate estimation results in **INSECURE** final key
 For a true value e , $\Pr\{e \in (p_E - \delta, p_E + \delta)\} \geq 1 - \epsilon$

$\epsilon = e^{-N\delta^2}$: $N = |\vec{x}_A|$ Long code length decreases error probability

Ex. $\delta=0.5\%$: $N=1\text{Mbit}$ (10Mbit) $\Rightarrow \epsilon=10^{-11}$ (10^{-109})

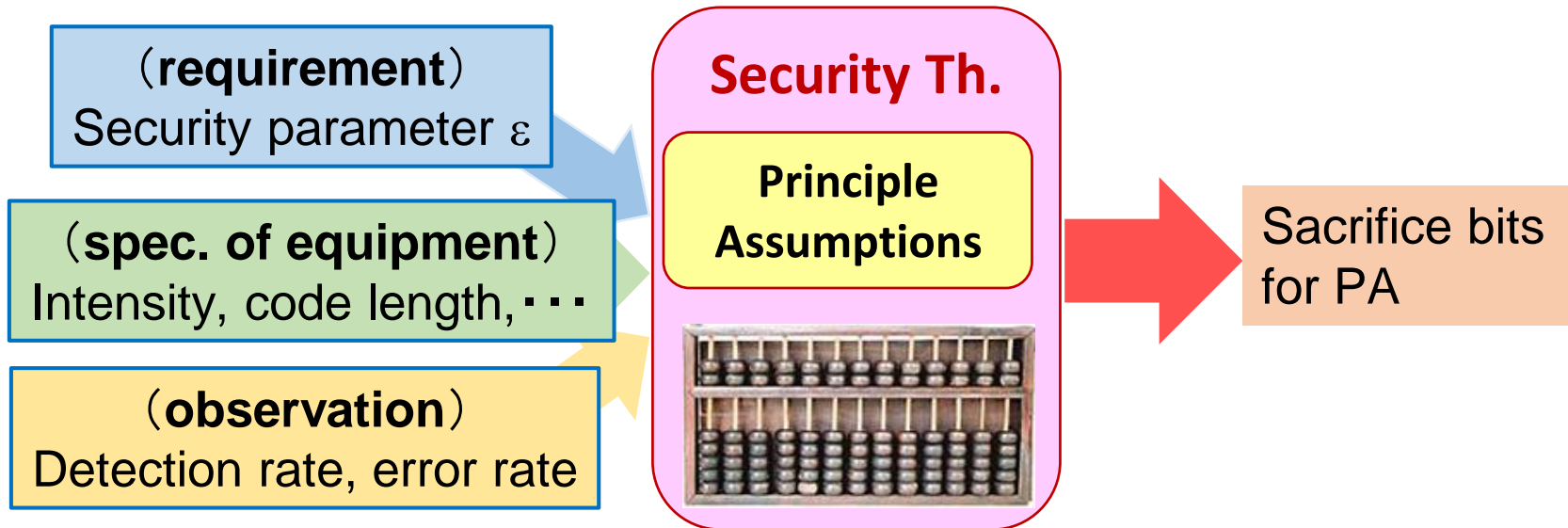


Final key rate and sacrifice bits

$$R = K\eta(1 - EC - PA)$$

Directly calculated from bit error rate:
rate: $fH(\delta_x)$

Indirectly calculated with
estimated phase error rate: $H(\delta_y')$



Each theory (Mayers, Ben-or, Shor-Preskill, Renner, Koashi, Hayashi,...) yields different estimation.



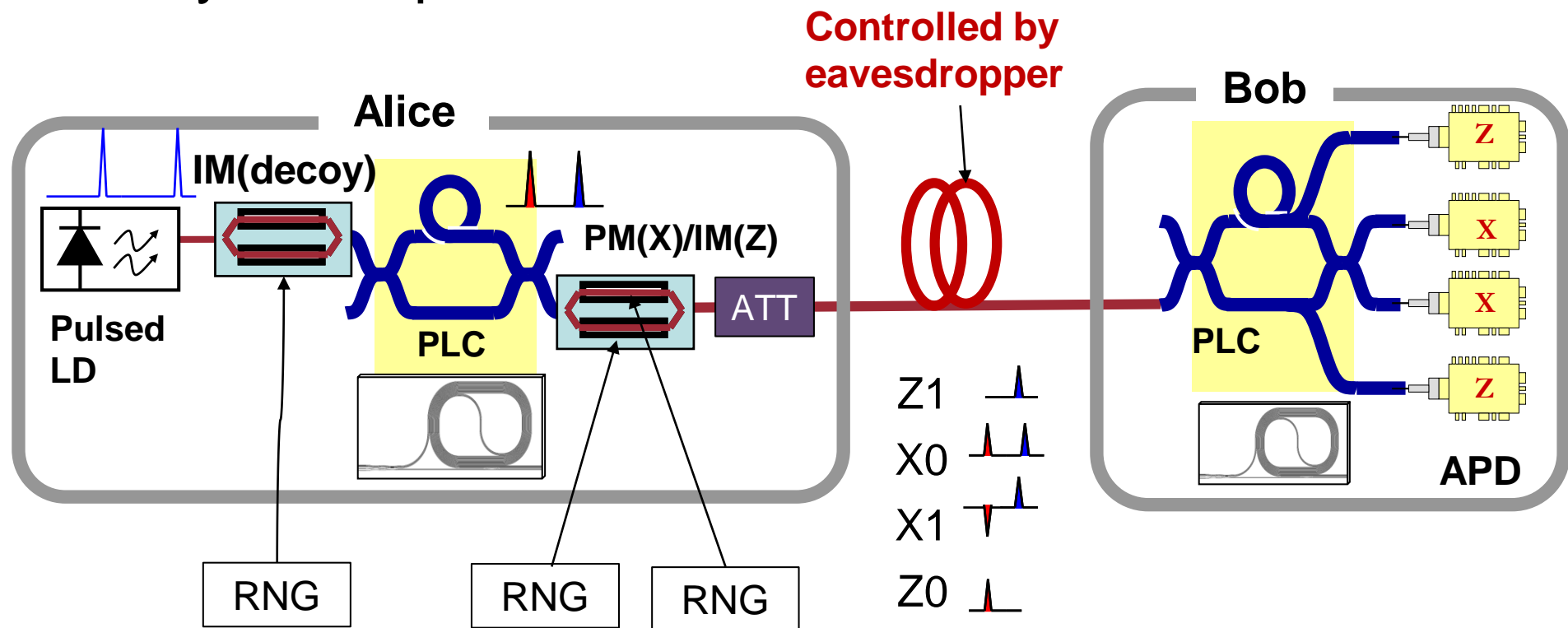
Process of security certification

1. Describe of the protocol and used devices.
2. List the assumptions for the security proof.
3. Evaluate the discrepancy from the assumptions.
Estimate the effects of the discrepancy.
4. Improve the implementation:
 - devices and system design.
 - Introduce new model.
 - Modify the security proof to include the discrepancy.



Model system

Decoy-BB84 protocol



$$\mu_0 \approx 0 < \mu_1 < \mu_2$$

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

Indistinguishability, a key for security

If the states are indistinguishable to Eve, she applies the same eavesdropping strategy to all the states.

- The strategy is not optimal to some states, so that eavesdropping disturbs the states.
- Eve's information on key is upper-bounded as a function of phase error rate.

If distinguishable, Eve can directly measure the key bit values, or improve the eavesdropping

- Security analysis doesn't work



Assumptions behind security proof

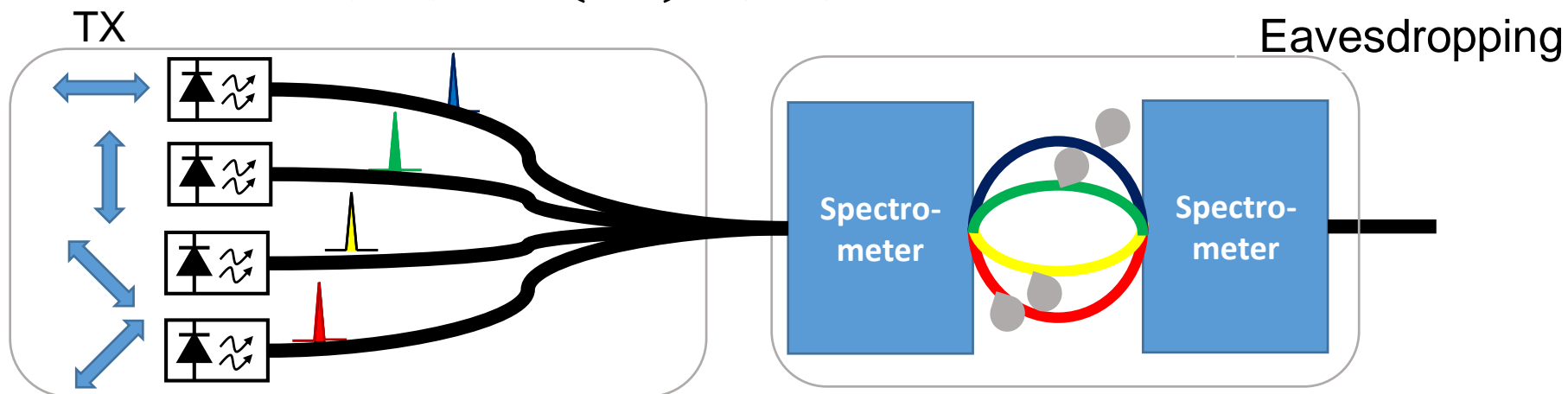
1. **No disclosure of the secret**: choice of bit values, bases, decoy pulses, test bits, and hash functions
2. **No external observation or control** (side channels) allowed
 - information gain only through the quantum channel.
3. **Security theory works**
 - ✓ Quantum mechanics is correct
 - ✓ Information theoretically secure authenticated channel
 - Devices work as expected (ex. Koashi's security proof)
 - *Independent pulses (no phase correlation)*
 - *Known photon number distribution in emitted pulses*
 - *Basis-independent detection probability*



1. No Disclosure of the secret

- Random choice = TRUE random numbers
- Apparatus should reflect the random choice faithfully
- The random choice should not affect the other characteristics of photons: polarization, amplitude, phase, frequency, pulse shape, timing, spatial mode

$$E(\mathbf{r}, t) = \mathbf{e}(\mathbf{r}, t)A(\mathbf{r}, t)e^{i\omega t - i\mathbf{k} \cdot \mathbf{r} + \varphi(\mathbf{r}, t)}$$



Side channel attacks in conventional systems

Probing: direct tapping on signal lines in chips, etc.

Power Analysis: measuring variation of power consumption during encryption/decryption

Timing Analysis: measuring time variation during encryption/decryption

Failure Attack: Applying signals or clocks out of spec to induce errors, and comparing normal processing

Tempest Attack: collecting electromagnetic wave

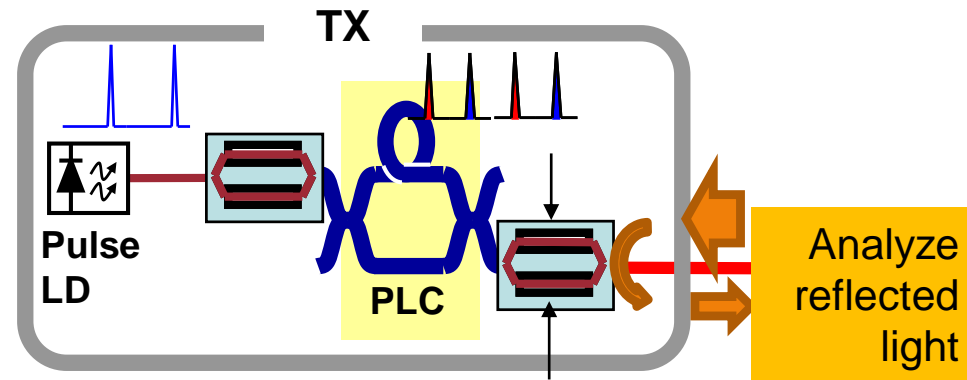
- Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation <http://www.tau.ac.il/~tromer/radioexp/>
 - an AM radio can receive leaked EM wave from computers
-
- Eco-design makes the above analysis, because of significant difference in power consumption between tasks
 - Side channel attacks are effective for processing with high load



2. Side channel attack in quantum comm.

TX: Trojan horse attack

- power monitor
- attenuators
- isolator



RX: photon detectors controlled by external light

- appropriate filters
- time gate
- identical detectors (efficiency, time response)
- single mode optical fiber
- polarization independence
- excessive input monitor



Requirement for QKD equipment

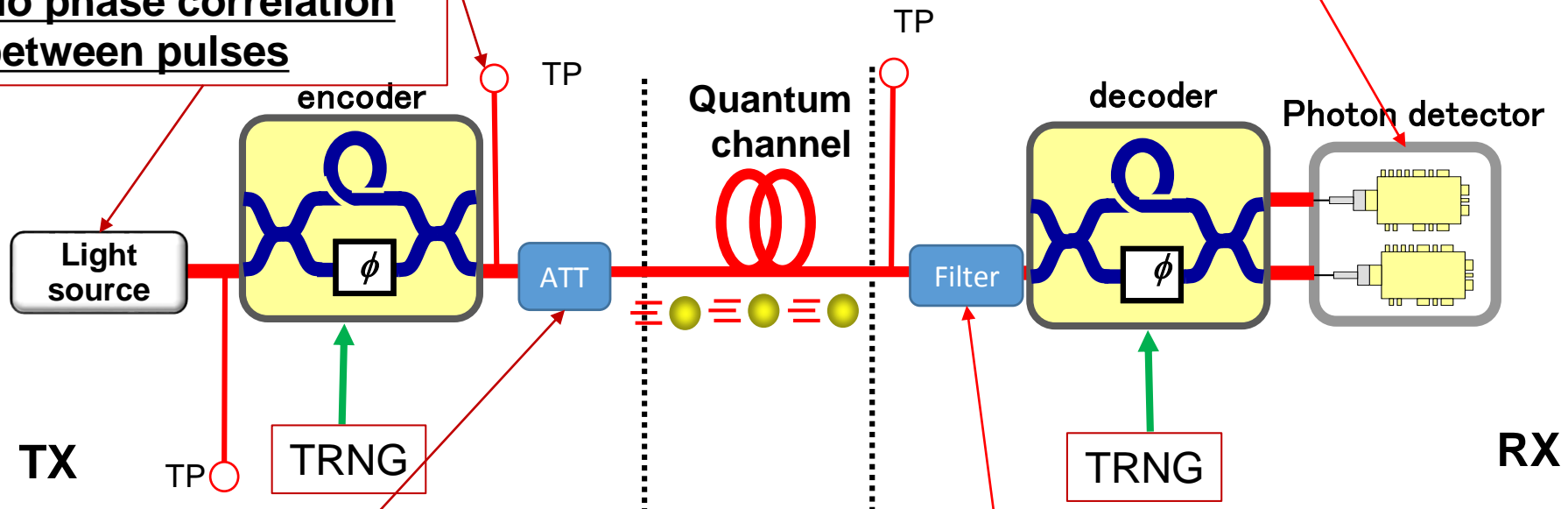
Unpredictability of selection

- identical properties-pulse shape, spectrum, polarization, spatial mode-for all the quantum states
- identical properties for signal and decoy
- faithful photon states

Identical detection

- detection efficiency
- dark count probability for all the photon detectors

No phase correlation between pulses



Known photon number distribution

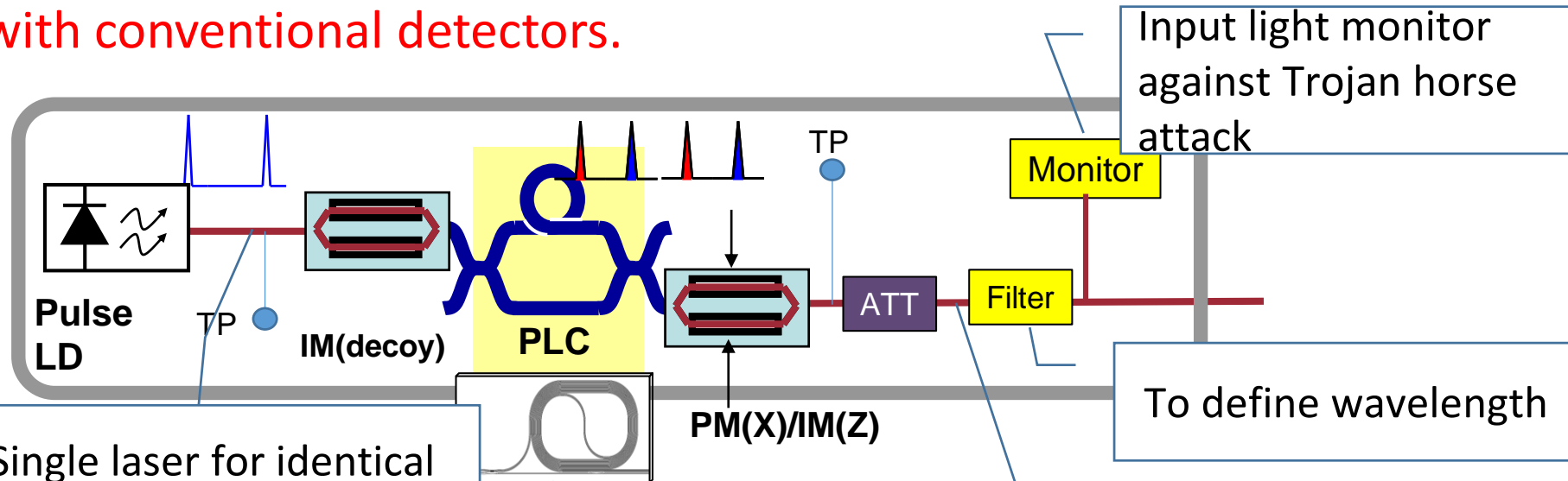
- Intensity
- Photon statistics (Poisson?)

Only detect the expected mode of light



Design consideration on transmitters

Light is rather strong before attenuator, so that we can monitor with conventional detectors.



- Single laser for identical characteristics
- Gain-switching for phase randomization

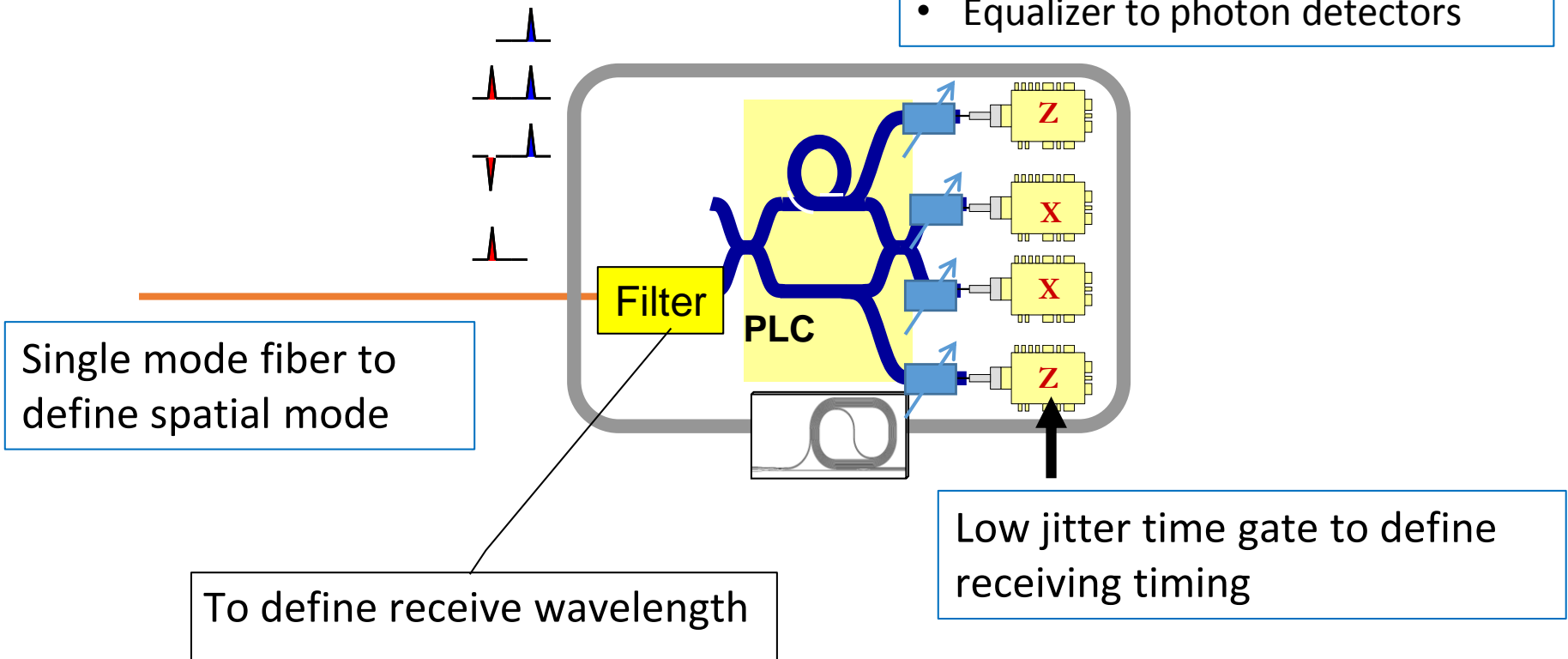
- Stable PLC interferometer
- Precise control of drive signal
- Optimal modulation



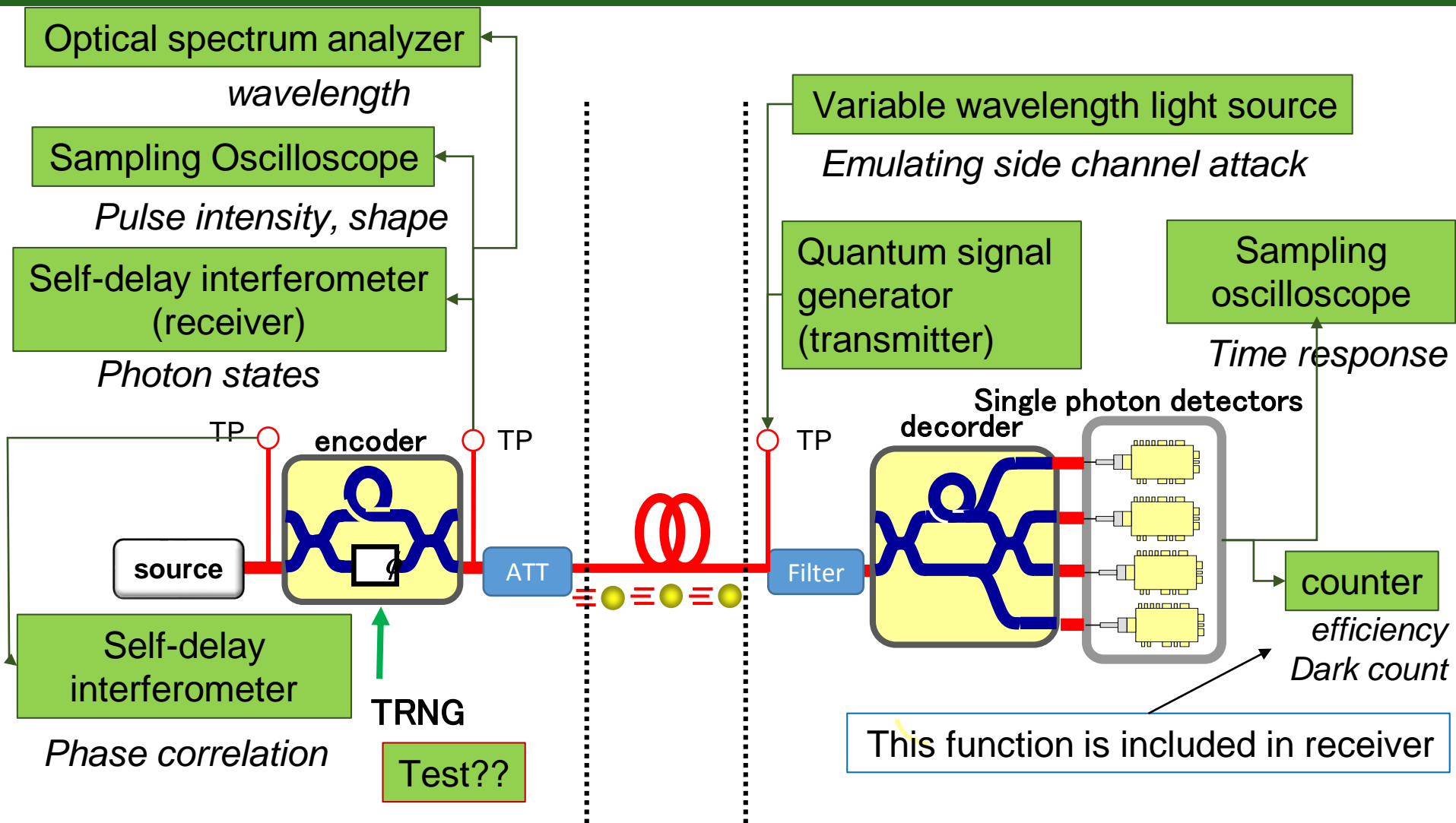
Design consideration on receivers

We need to consider *any* input photon states;
Restrict the mode by filtering

- Dark count monitor and auto-bias control
- Equalizer to photon detectors

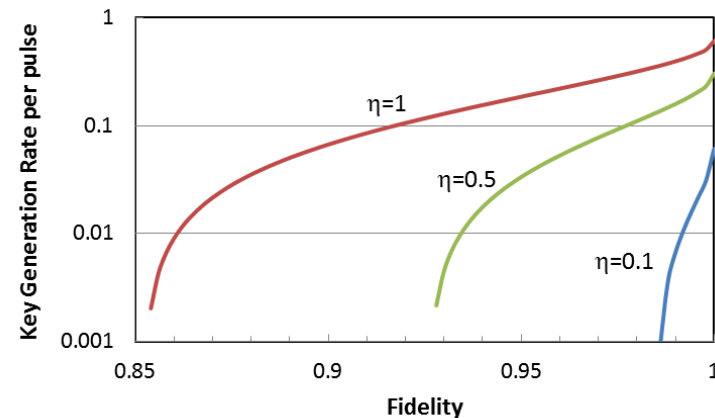


We have tools for evaluation



We need Quantitative criteria

- Idea: no information=random choice +indistinguishability
- Random choice : TRNG
- Indistinguishability between states A and B : *quantified with $F(A,B)$*
 - Modify theory to include the effect of $1-F>0 \rightarrow$ practically acceptable lower bound of F .
 - Theories provide different effects (better theory should be developed)
- Recent development (case studies)
 - **Phase randomization: measurement and evaluation of the effect**
 - **State preparation flaw: robust three-state protocol**



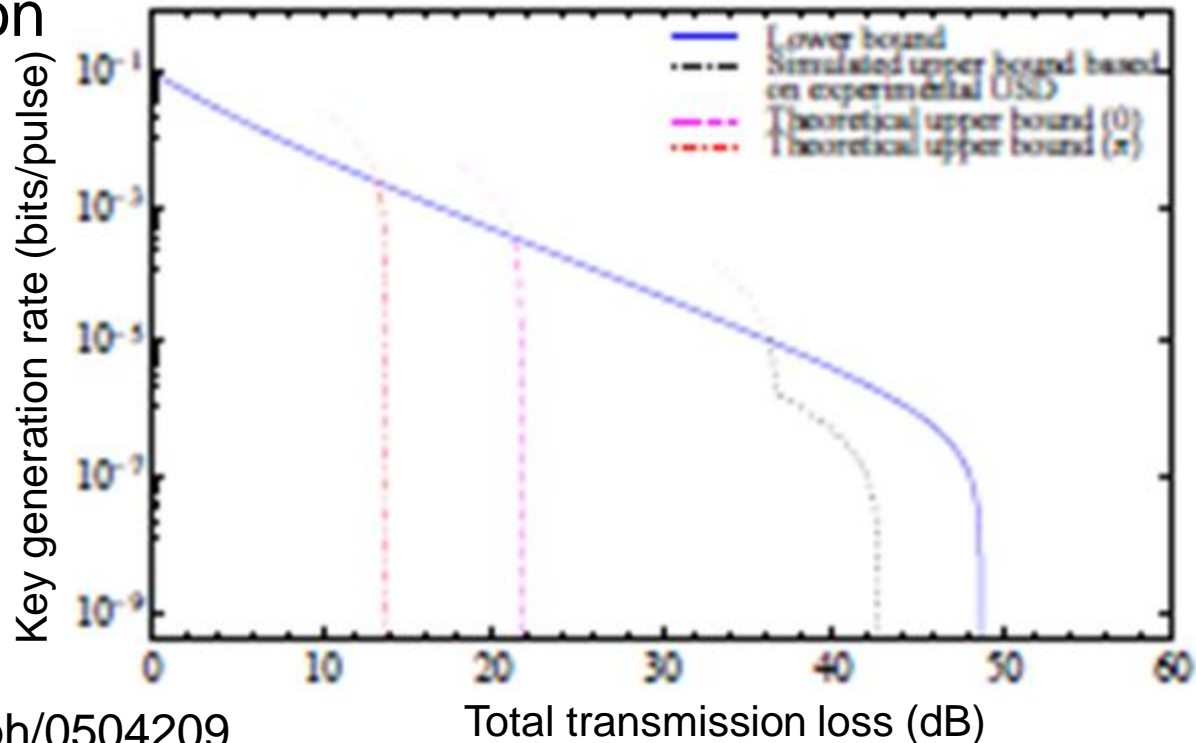
Effect of inter-pulse phase correlation

Current security proof of Decoy-BB84 assumes phase randomization

$$\rho = e^{-\mu} \sum_{n=1}^{\infty} \frac{\mu^n}{n!} |n\rangle \langle n|$$

→ phase correlation provides security holes (USD+PNS)

- Distinguishability on
 - Basis
 - Decoy/Signal



H.K. Lo and J. Preskill, quant-ph/0504209

Y.L. Tang, et al., ArXiv:1304.2541



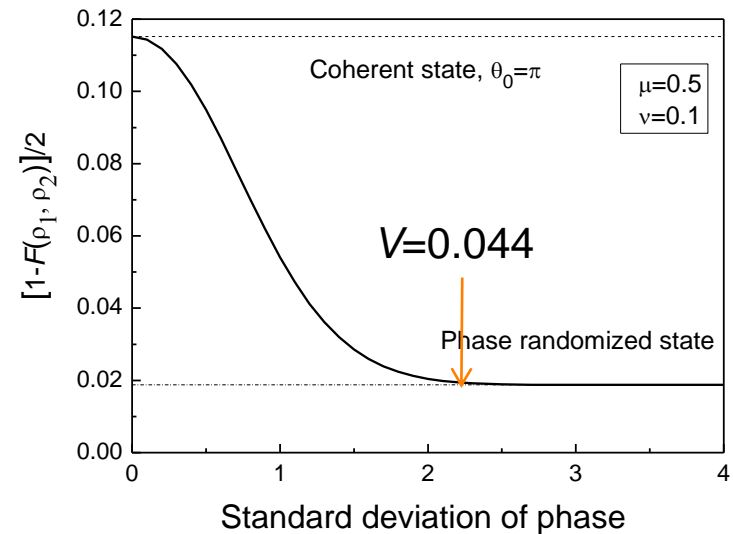
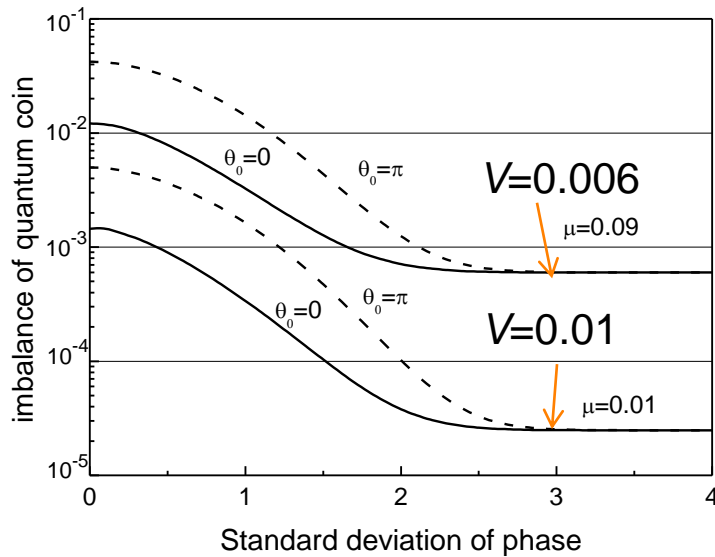
Criteria for phase randomization

Partial phase randomization modeled with Gaussian Prob. distribution:

$$P(\theta) = \exp \left[-\frac{(\theta - \theta_0)^2}{2\sigma^2} \right]$$

Visibility of interference between adjacent pulses:

$$V = \exp \left[-\frac{\sigma^2}{2} \right]$$

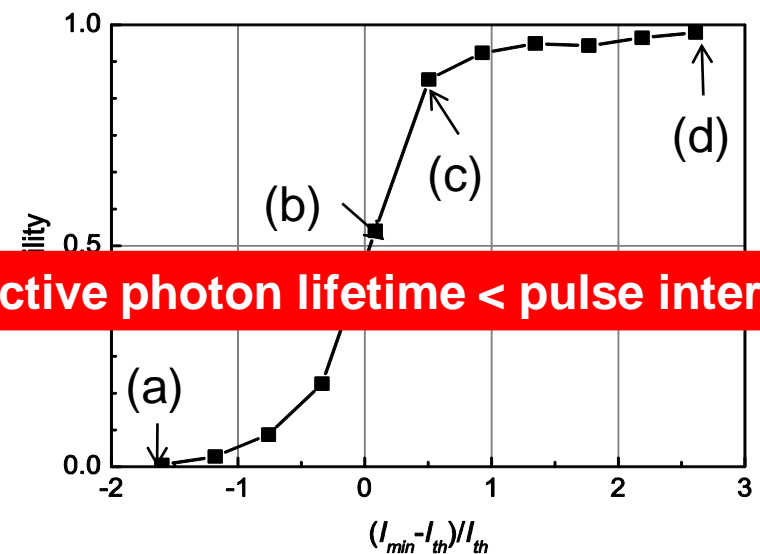
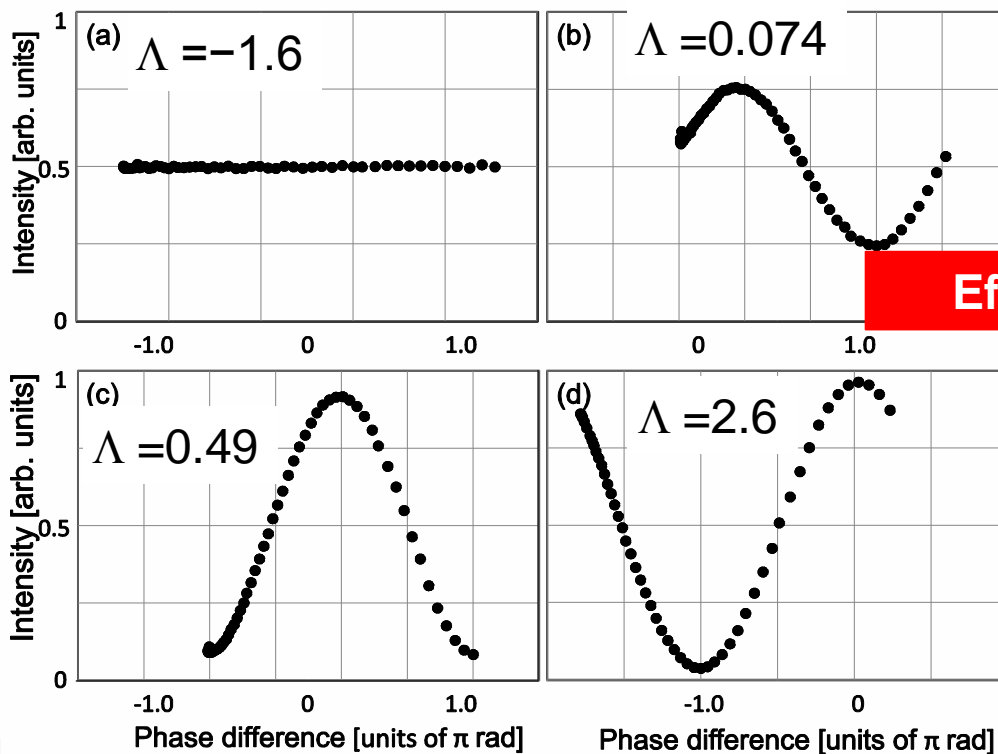
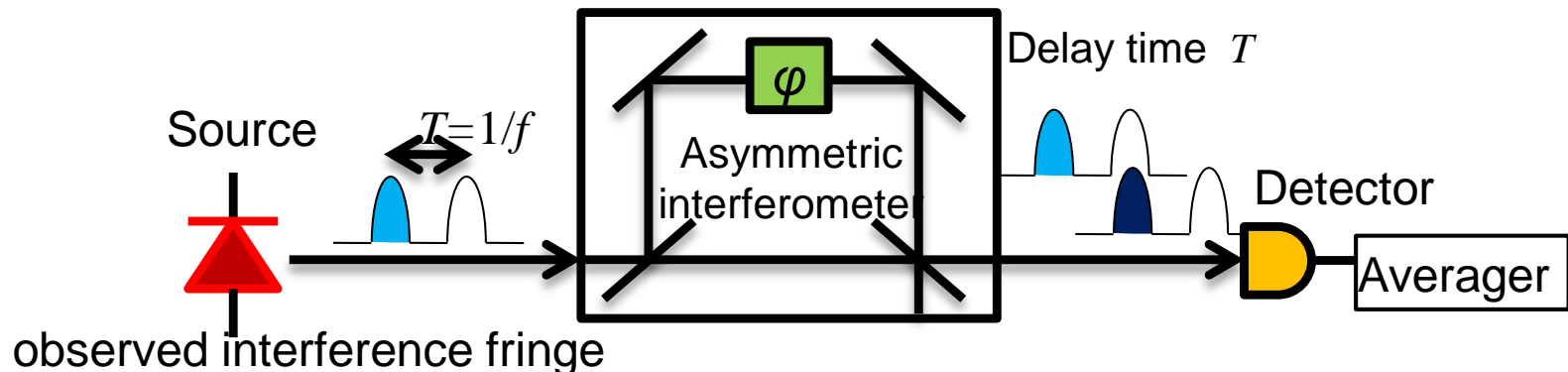


distinguishability between X- and Z- coding

distinguishability between signal and decoy

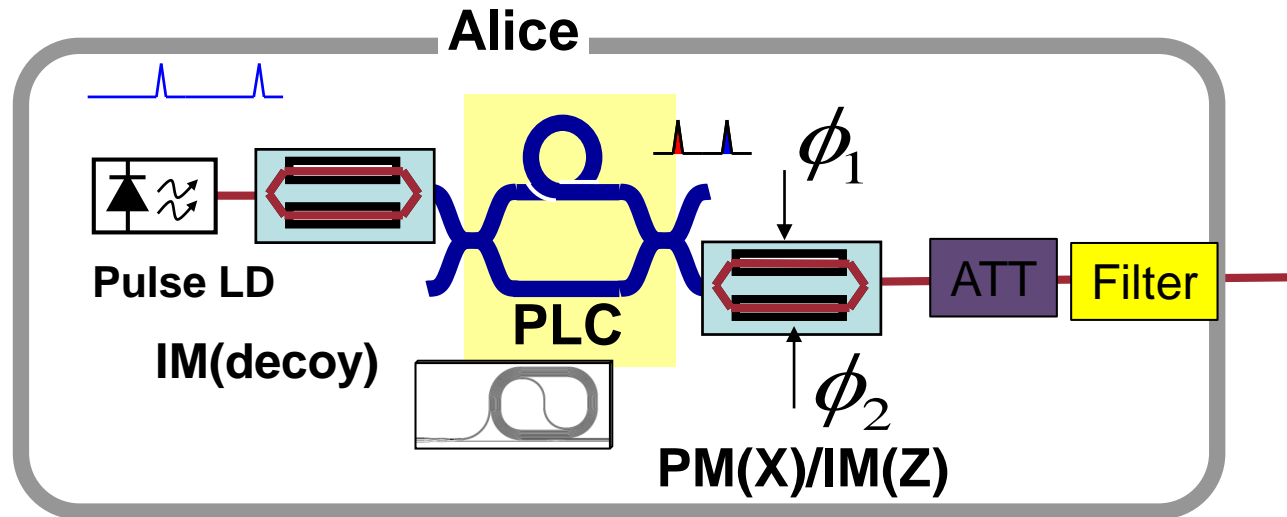


Inter-pulse phase correlation for 10 GHz



Visibility as a function of normalized excitation $\Lambda = (I_{\min} - I_{th})/I_{th}$

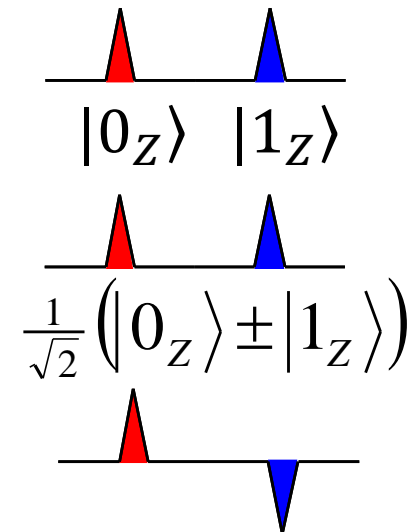
State preparation flow 1



Superposition of temporally separated pulse

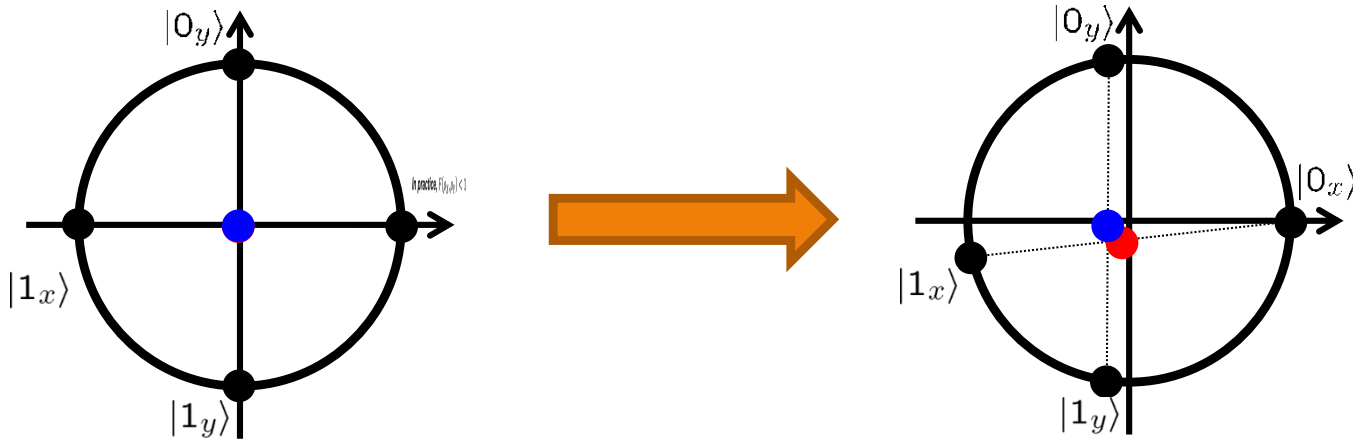
- precision of divided amplitude/timing in the interferometer (**PLC**)
- precision and fluctuation of modulation

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



State preparation flaw 2

If Bases are partially distinguishable



Ideally, $F(\rho_X, \rho_Y) = 1$

In practice, $F(\rho_X, \rho_Y) < 1$

GLLP:

$$R \propto 1 - h(\delta_x) - h(\delta'_y)$$

$$\left[\begin{array}{l} \delta'_y \leq \delta_y + 4\Delta + 4\sqrt{\Delta\delta_y} \\ \Delta = [(1 - F(\rho_Y, \rho_X)) / 2] / \eta_{\text{detection}} \end{array} \right.$$

D. Gottesman, H. K. Lo, N. Luetkenhaus, and J. Preskill,
Quant. Inf. Comput. 5, 325 (2004).

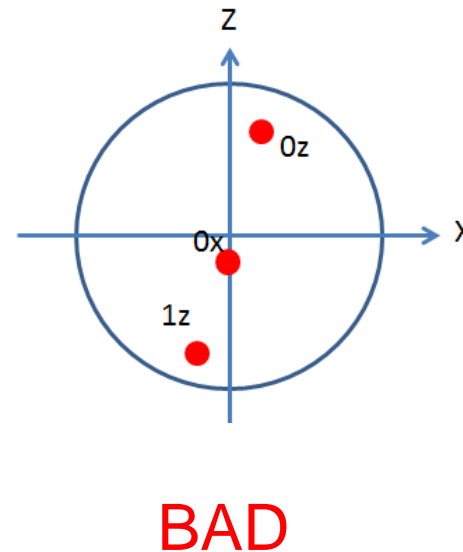
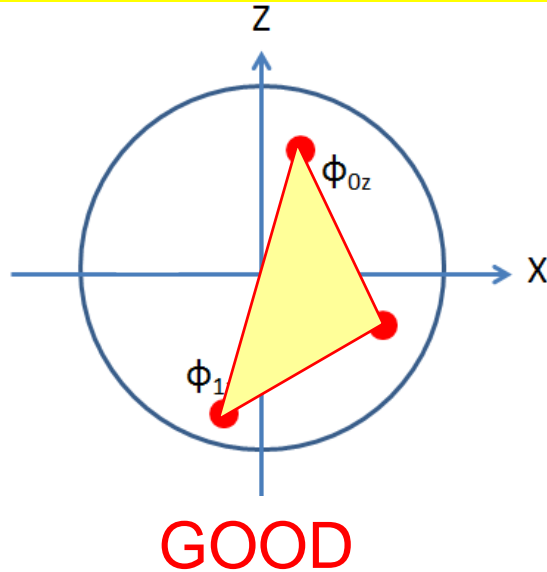
M. Koashi, arXiv:quant-ph/0505108.

Exponential increase of the flaw!



A protocol immune to state preparation flaw

As long as three states form a triangle, we can obtain the exact phase error rate



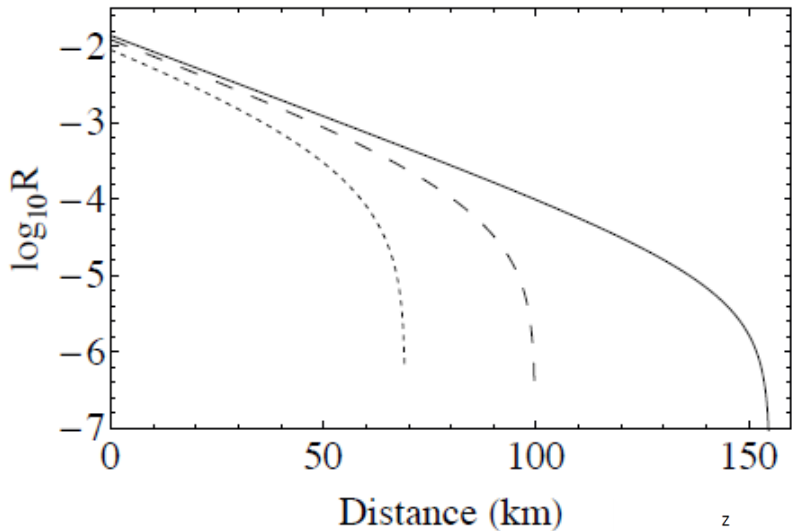
- Three-state protocol can estimate **exact phase error rate** by utilizing **basis mismatch events**.
- The states should be **known**.

K.Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. **A 90**, 052314 (2014)

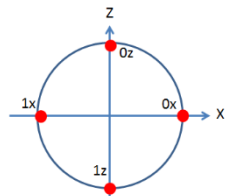


Key rate of the three-state protocol

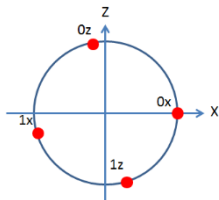
b Decoy-state BB84 protocol based on GLLP



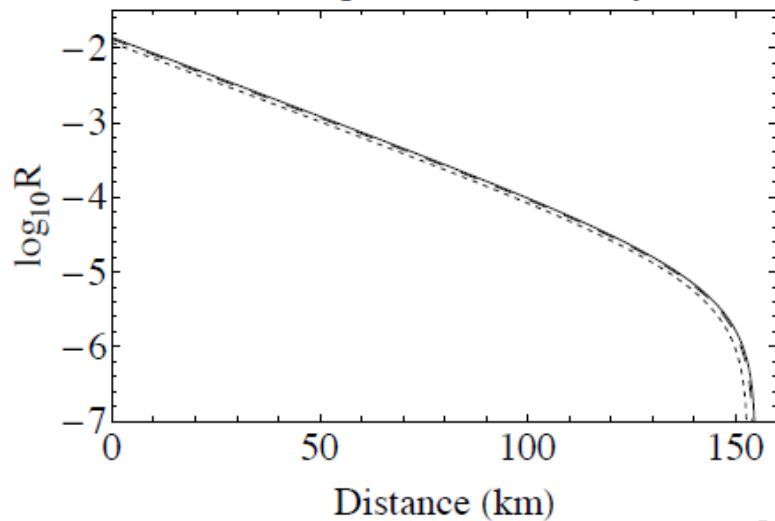
— : Ideal state preparation



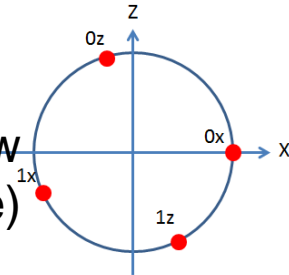
--- : State preparation flaw (about $3.6 \cdot \theta / 180$ degree)



a Three-state protocol with decoy states



..... : State preparation flaw (about $7.2 \cdot \theta / 180$ degree)



The state preparation flaw is almost negligible!



Open issues

Nothing overlooked?

- Requirements are clear
- Photon pulses are defined with finite number of characteristics

$$\mathbf{E}(\mathbf{r}, t) = \mathbf{e}(\mathbf{r}, t)A(\mathbf{r}, t)e^{i\omega t - i\mathbf{k}\cdot\mathbf{r} + \varphi(\mathbf{r}, t)}$$

- But, new side channels may be found in the future
 - MDI will help us. Further studies on the implementation required.

Measurements accurate enough?

- Results are affected by error, fluctuation, and drift.
- Measurement devices may contain imperfection

Effects of imperfections treated well?

- Conservative theory will yield low (or zero) final key rate



Random number generator

High speed generation required:

$$1 \text{ GHz (clock)} \times (1+1+2) = 4 \text{ Gb/s}$$

Large number of bits:

$$100 \text{ Mb (code length)} / 0.004 \text{ (detection rate)} = 25 \text{ Gb}$$

Classical tests are not sufficient

- Quantum mechanics may help
- How to evaluate non-classicality with required high accuracy?

Remark

- Different requirements for different use of random numbers: key bits and others



Security certification in practical systems⁴⁰

Dialogues between theorists and engineers

Description of the protocol and used devices.

List assumptions for the security proof

Check the assumptions on the real machine

Evaluate the security against attacks

NO

OK?

NO

YES

Change model
Create new proof

Improve the implementation

security
certification



For deployment of QKD secure network

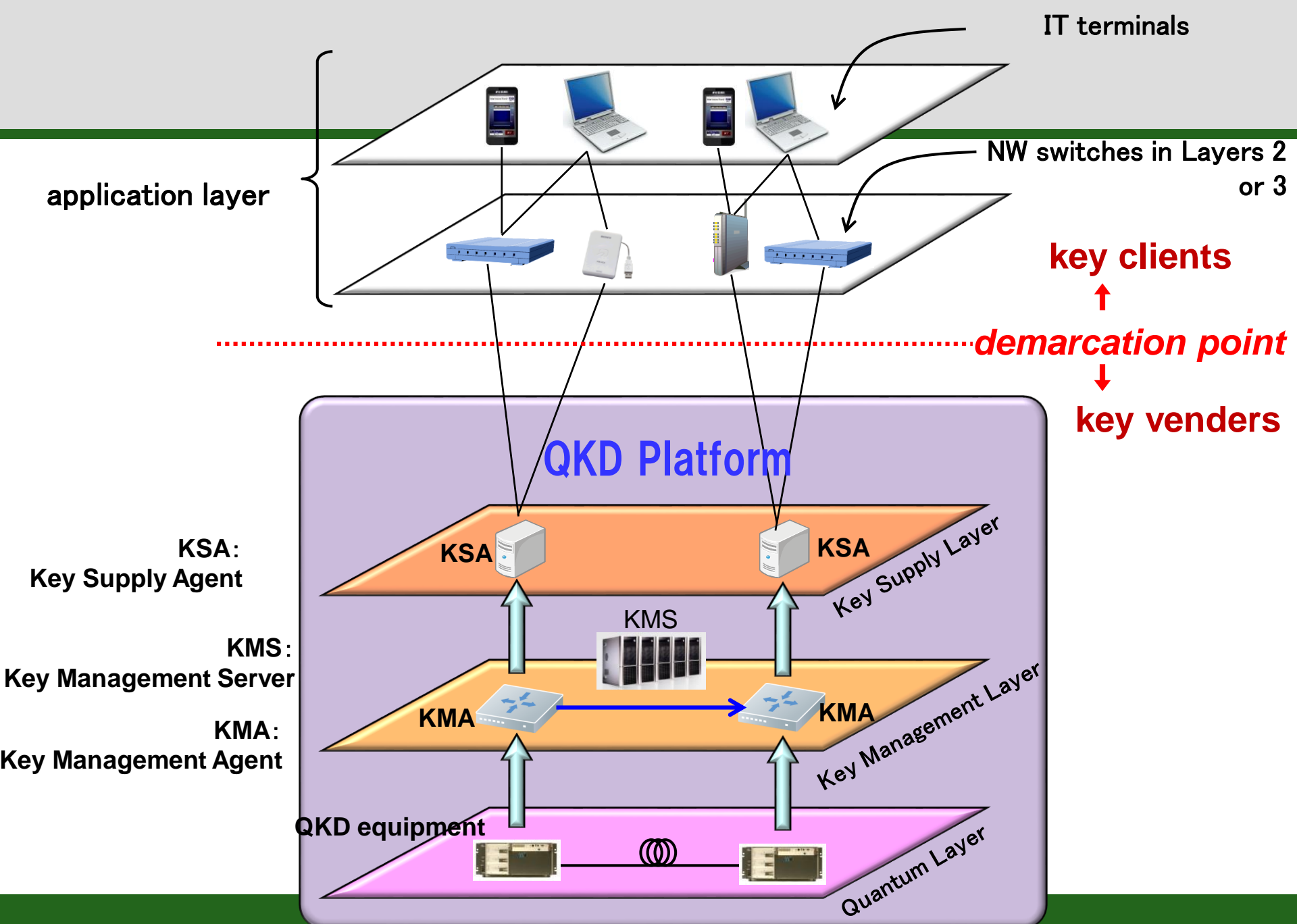
More sophistication of the QKD technology

- Further performance improvement
 - Quantum communication
 - Key distillation
- Security
 - counter-measurement to side channel
 - Refine/Improve security analysis
 - **Quantify criteria for secure QKD systems**
- Integrated network
 - Connection between QKD-platform and layer 4 or upper

Next generation quantum secure technology

- **QKD based on novel principles**
 - for ex. loss-tolerant
- **Harnessing quantum technology other than QKD**
- **Merging with modern (information theoretically secure) cryptography**





Summary

QKD enables remote parties to share information theoretically secure key.

QKD provides universal composability (stronger than most of the public key crypt from this view)

Security certification on the practical system

- Process
- Assumptions
- Design
- Evaluation of imperfections and its effects
- **Still on going: both theoretical and experimental**

Practical QKD network demonstrations

