Research and development of Tokyo QKD Network

Kiyoshi Tamaki

NTT basic research laboratories, Japan

NTT

NICT

NEC Empowered by Innovation

MITSUBISHI Changes for the Better

TOSHIBA Leading Innovation

HOKKAIDO UNIVERSITY

東京工業大学 Tokyo Institute of Technology

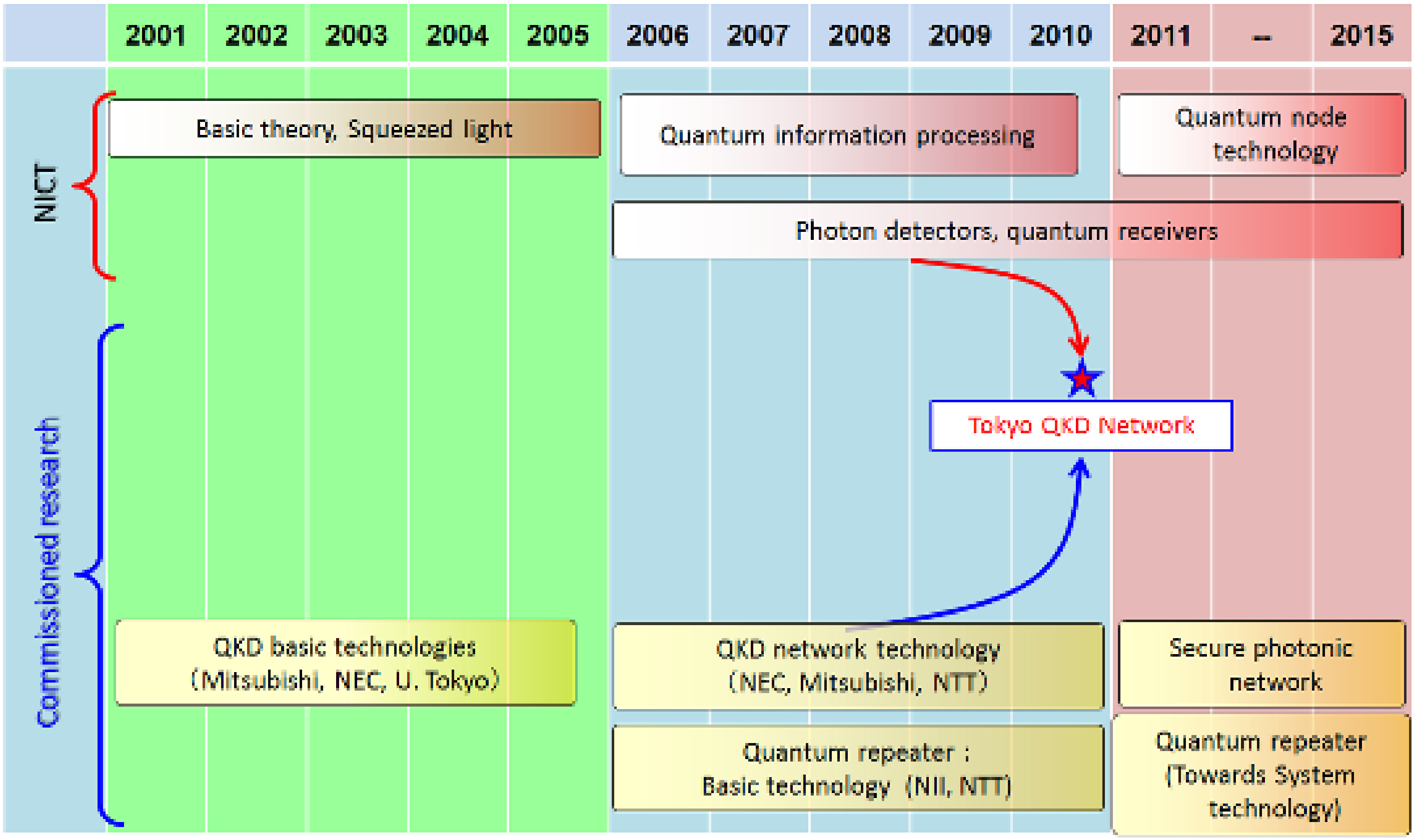
NAGOYA UNIVERSITY

東北大学 TOHOKU UNIVERSITY

GAKUSHUIN UNIVERSITY

Project overview of Tokyo QKD Network

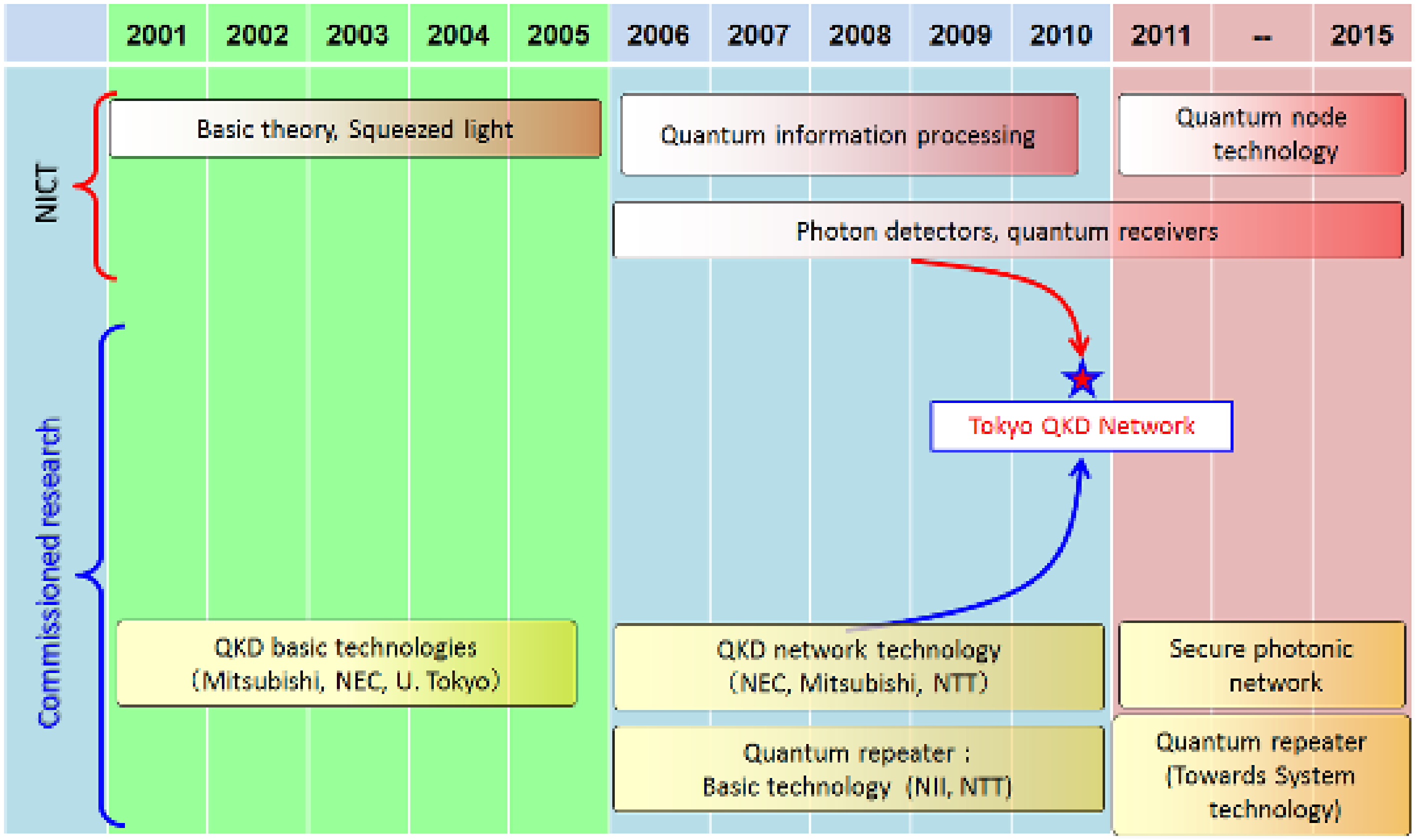
Main organization: National Institute of Information and Communications Technology (NICT): Research institute of Ministry of Internal Affairs and Communications, Japan



The project is based on the collaboration between NICT and commissioned research teams

Project overview of Tokyo QKD Network

NTT



List of the commissioned research organizations

NEC Empowered by Innovation

MITSUBISHI Changes for the Better

TOSHIBA Leading Innovation >>>

NTT

HOKKAIDO UNIVERSITY

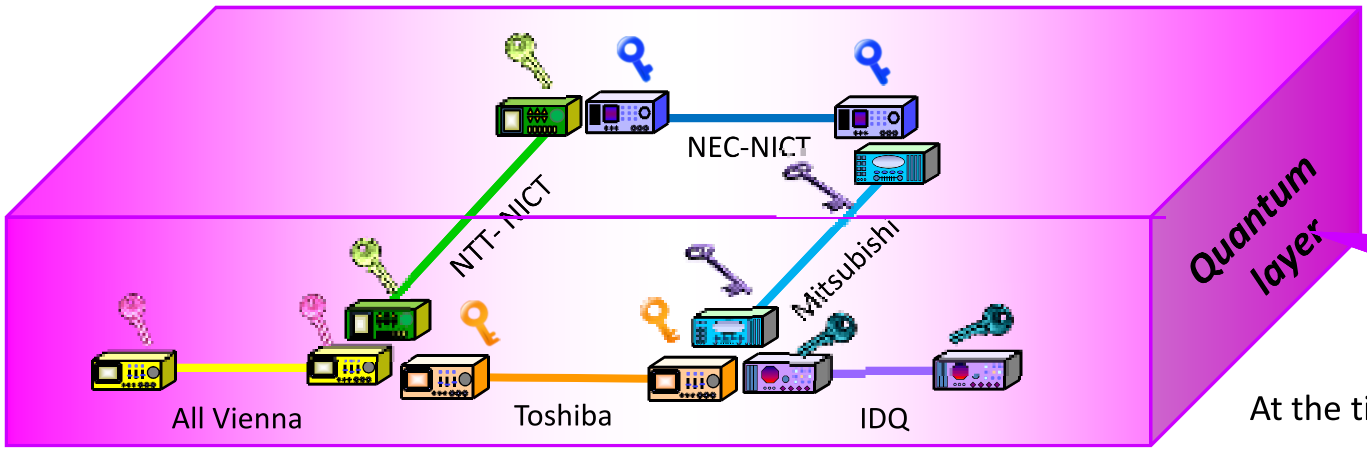
東京工業大学 Tokyo Institute of Technology

NAGOYA UNIVERSITY

東北大学 TOHOKU UNIVERSITY

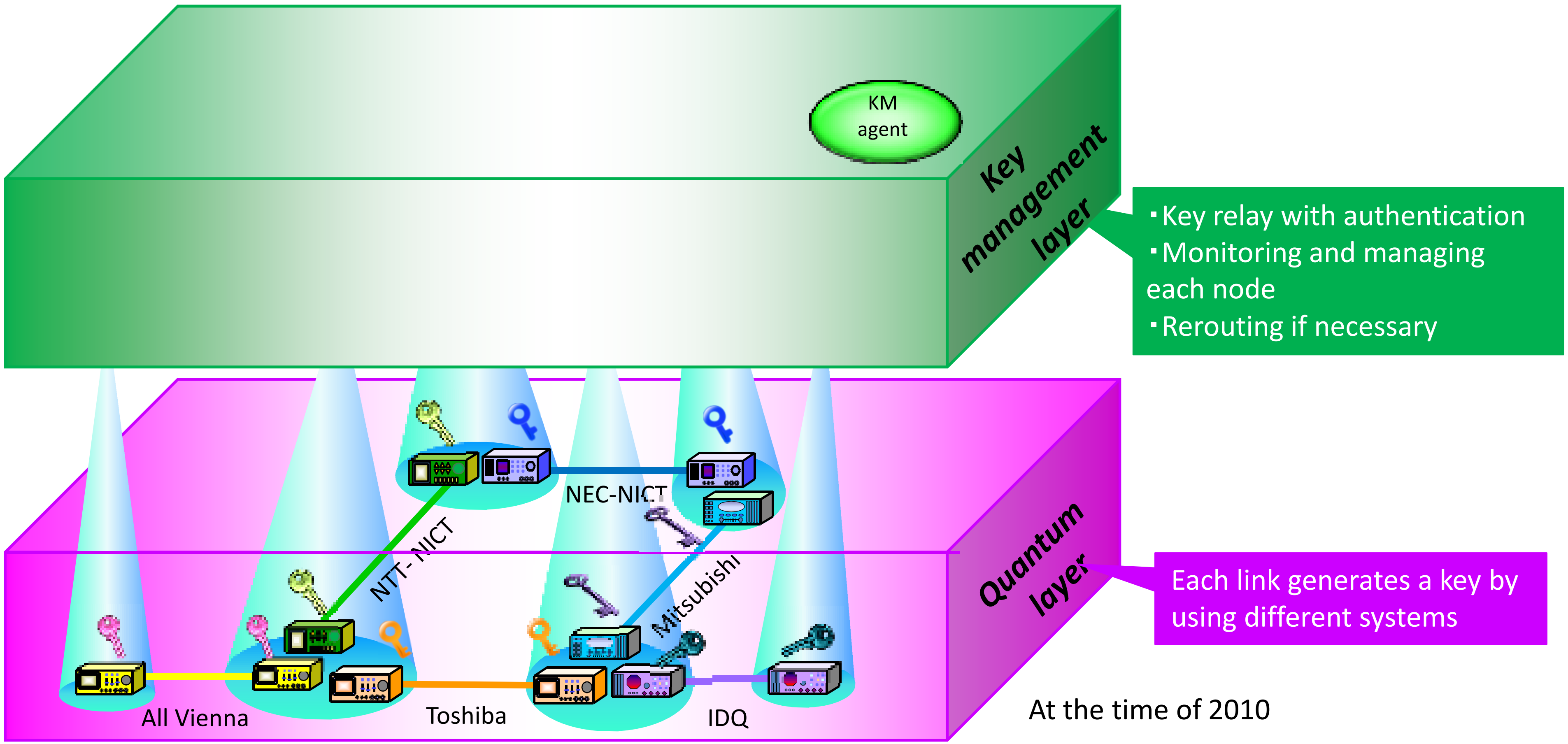
GAKUSHUIN UNIVERSITY

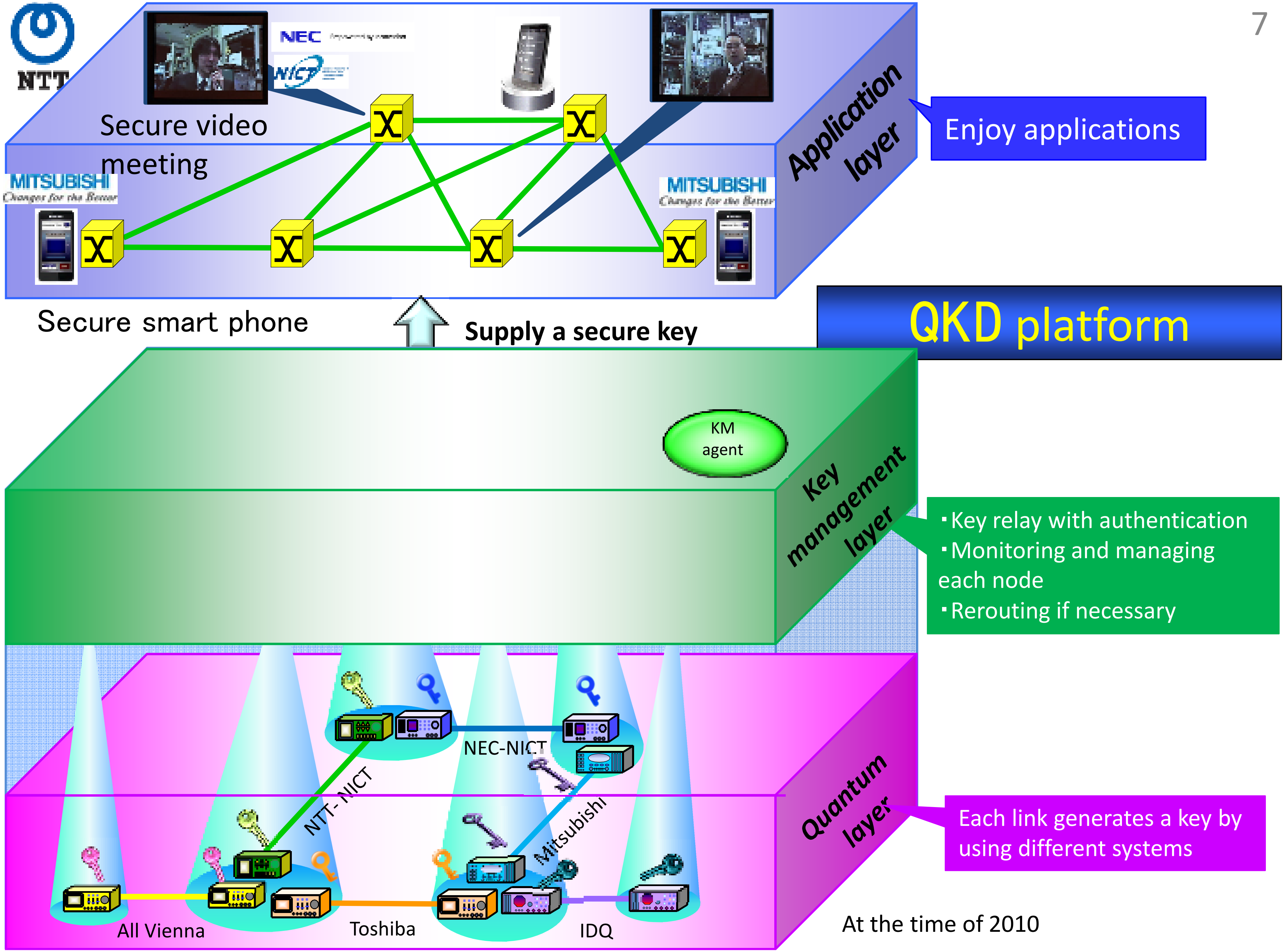
Tokyo QKD Network



Each link generates a key by using different systems

At the time of 2010


KM
agent
Key
management
layer
・Key relay with authentication
・Monitoring and managing each node
・Rerouting if necessary
NEC-NICT
NTT- NICT
Mitsubishi
All Vienna
Toshiba
IDQ
Quantum
layer
Each link generates a key by using different systems
At the time of 2010


NTT
NEC
Secure video meeting
MITSUBISHI
Changes for the Better
MITSUBISHI
Changes for the Better
Secure smart phone
Application layer
Enjoy applications
Supply a secure key
QKD platform
KM agent
Key management layer
・Key relay with authentication
・Monitoring and managing each node
・Rerouting if necessary
NEC-NICT
NTT- NICT
Mitsubishi
All Vienna
Toshiba
IDQ
Quantum layer
Each link generates a key by using different systems
At the time of 2010

NTT

In 2010, we performed live demonstration of Tokyo QKD Network

UQCC 2010

Updating Quantum Cryptography and Communications 2010

October 18 - 20, 2010, ANA INTERCONTINENTAL TOKYO

"See & touch the quantum-inspired future"

Conference Program

2010

日本語（解説付き）

- About UQCC
- Conference Program
- Exhibition
- Tokyo QKD Network
- Instructions for Speakers
- Accommodation
- Venue / Information
- Sponsors
- UQC2007, 2008 & Report
- Contact

Day 1 Monday 18 October

Time	Speaker	Title
9:30-9:35	Hideo Miyahara (President, NICT)	Welcome address
9:35-9:40	Hideki Imai (Director, AIST)	Opening remarks
Tokyo QKD network live demonstration:		
9:40-11:10	NICT, NEC, Mitsubishi Electric, NTT, TREL, ID Quantique,Mitsubishi Electric, NTT, TREL, ID Quantique, All Vienna	Demonstration of secure communication with QKD
11:10-11:50		Messages from team leaders, and Q&A
11:50-13:20	Lunch break (90min.)	
Session 1 Security for new generation network (chair: J. H. Shapiro)		
13:20-13:50	Tomonori Aoyama (Keio University/NICT)	Special talk ICT Paradigm Shift in 2010s and its impacts on the Information Society, 30min.

Project overview of Tokyo QKD Network

What can be improved in Tokyo QKD network after 2010 (phase II) ?

⇒ (1) Stability of key generation (few days)

(2) Theoretical investigation of the systems

Mission of phase III:

- More stable key generation
- Develop theory for more secure key generation

Organizations and people of QKD theory team

Hokkaido univ

Akihisa Tomita

Mitsubishi electric

Toyohiro Tsurumaru
Wataru Matsumoto
Takeshi Asai

Nagoya univ

Masahito Hayashi (NUS)

Tokyo inst. tech

Ryutaroh Matsumoto
Kenta Kasai

NTT

Koji Azuma
Go Kato
KT

Project overview of Tokyo QKD Network

What can be improved in Tokyo QKD network after 2010 (phase II) ?
⇒ (1) Stability of key generation (few days)
(2) Theoretical investigation of the systems

Mission of phase III:

- More stable key generation
- Develop theory for more secure key generation
- Come up with actual users case of QKD
- Start test service of QKD in NICT (2015)

Outline of the talk

BB84:

- ✓ Maintenance-free long term demonstration of NEC's QKD system
- ✓ Issues of imperfections of the devices

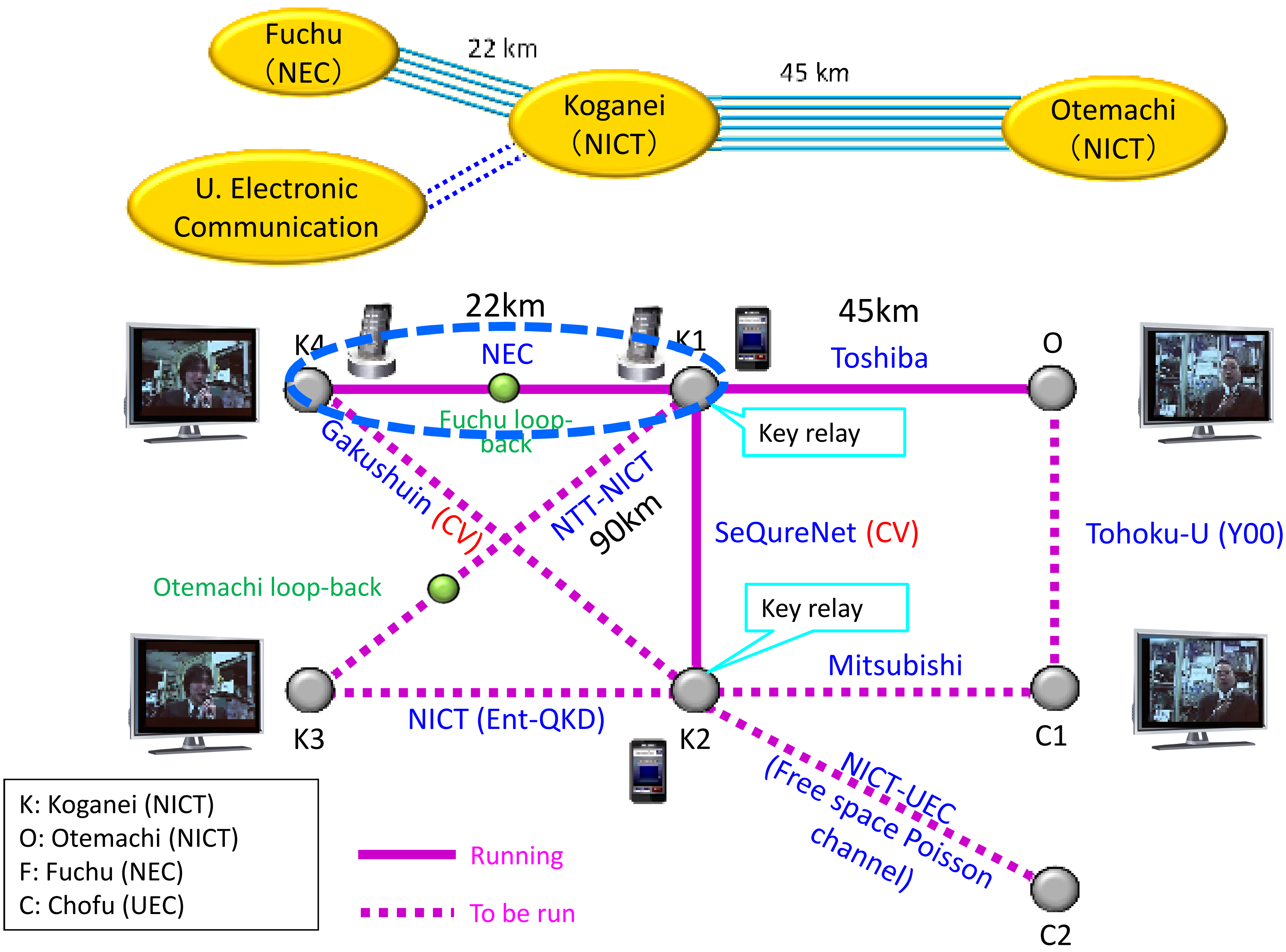
Differential phase shift QKD (DPS QKD):

- ✓ Field demonstration of NTT-NICT QKD system
- ✓ Unconditional security proof of DPS QKD

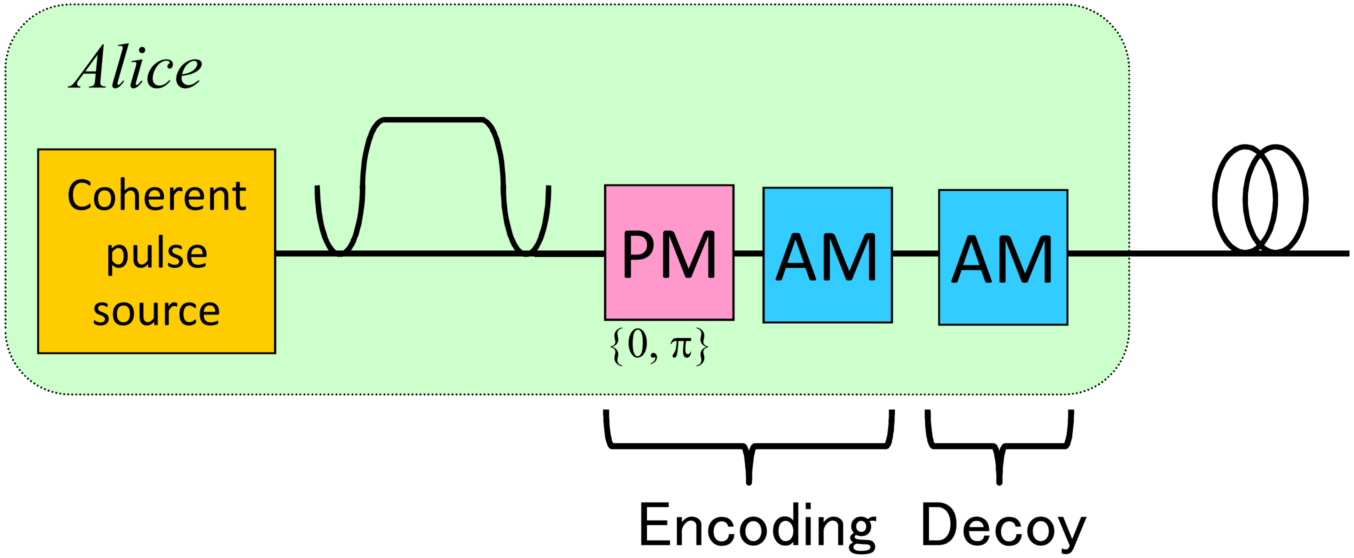
Continuous variable QKD (CV QKD):

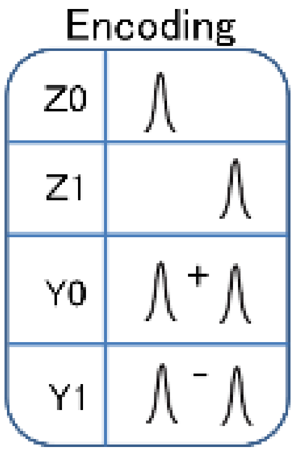
- ✓ Security proof against calibration attack on the local oscillator

Prototype of Tokyo QKD Network (2015)

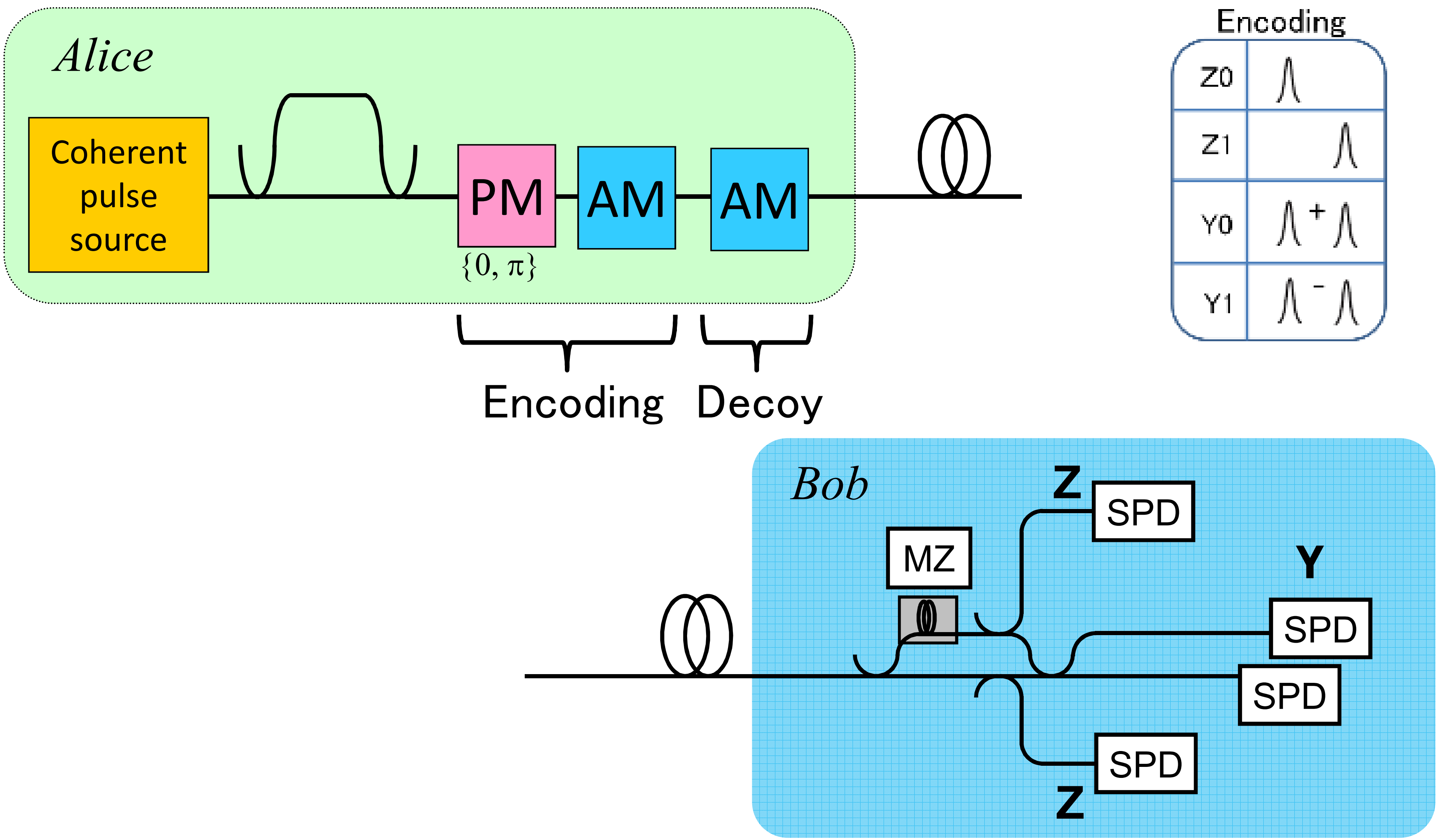


Basic concept of Passive BB84 with decoy and time-bin encoding





Basic concept of Passive BB84 with decoy and time-bin encoding

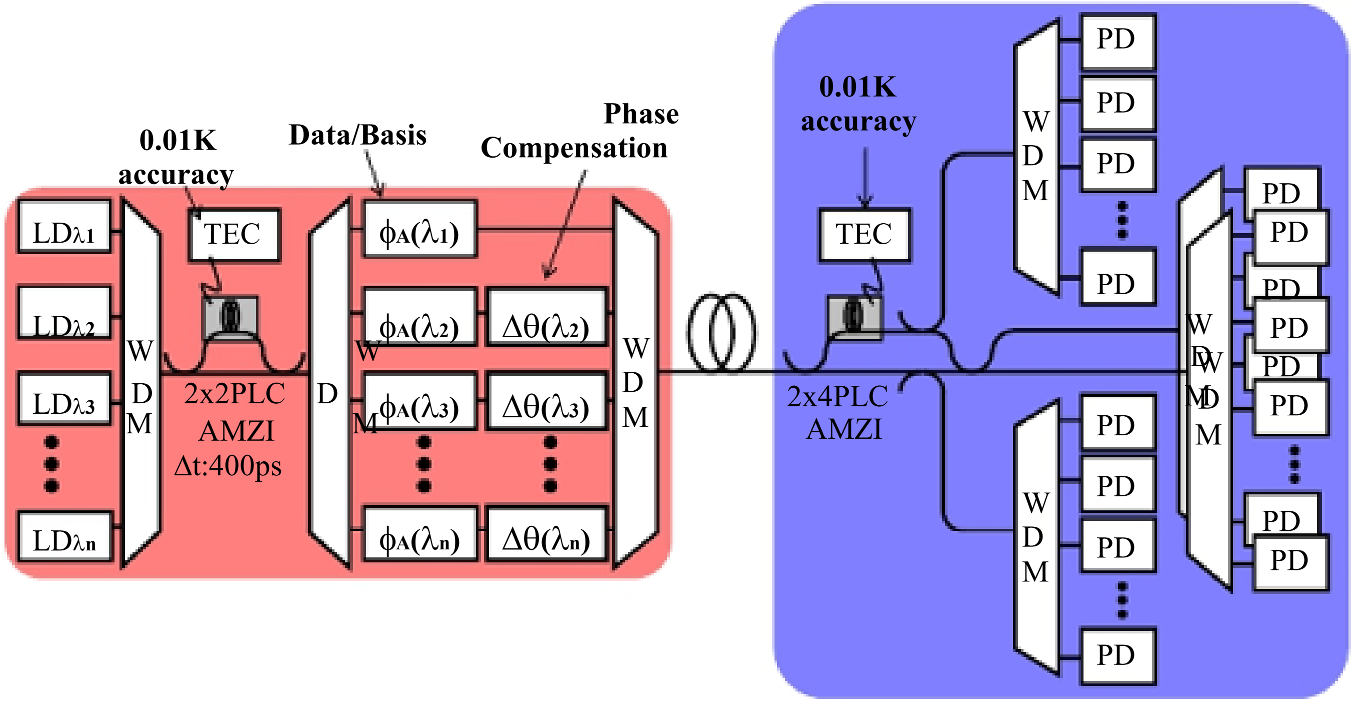


NEC's QKD system

- **WDM up to 8 channels with "Colorless interferometric technique"**
  - **The same Mach Zehnder interferometers for 8 channels**

    → Easy control, small size

A. Tanaka et al., ECOC2009, 1.4.2 (2009)



PD: photon detector

This slide is presented by the courtesy of NEC

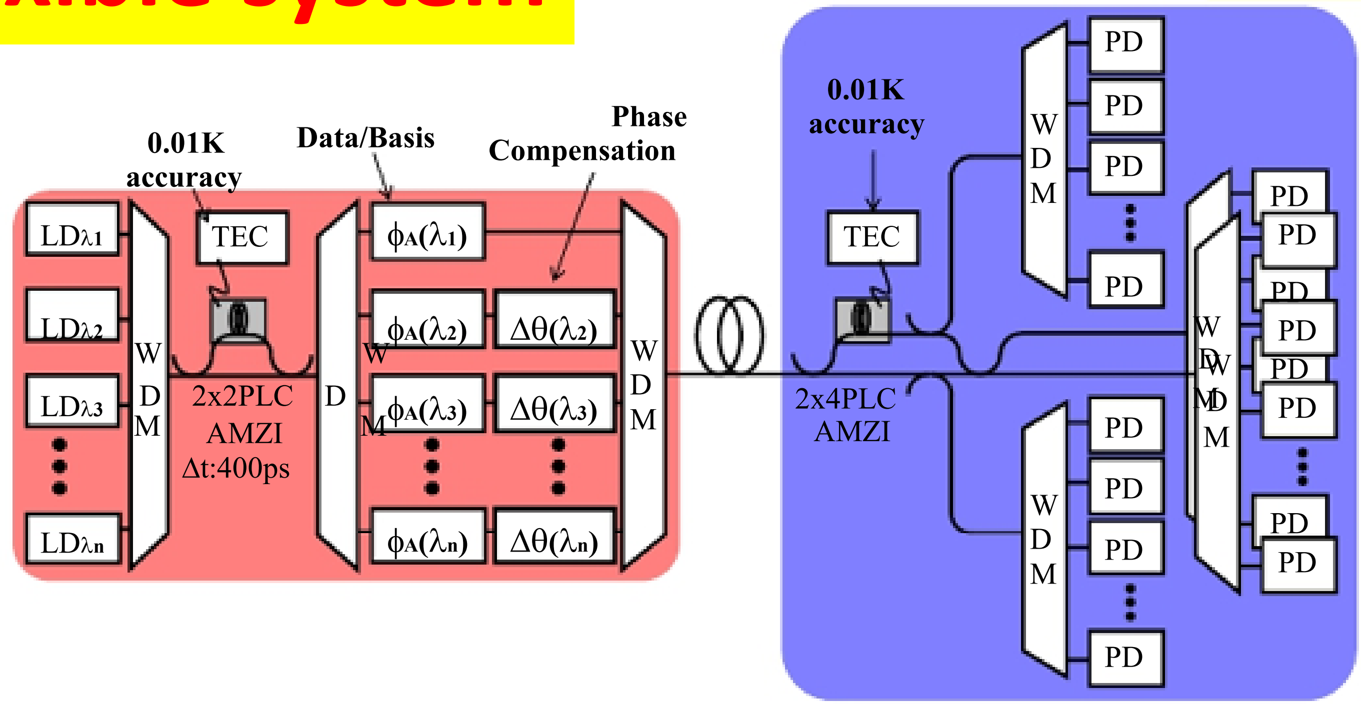
NEC's QKD system

- **WDM up to 8 channels with "Colorless interferometric technique"**
  - **The same Mach Zehnder interferometers for 8 channels**

  → Easy control, small size , save money

Flexible system

A. Tanaka et al., ECOC2009, 1.4.2 (2009)



PD: photon detector

This slide is presented by the courtesy of NEC

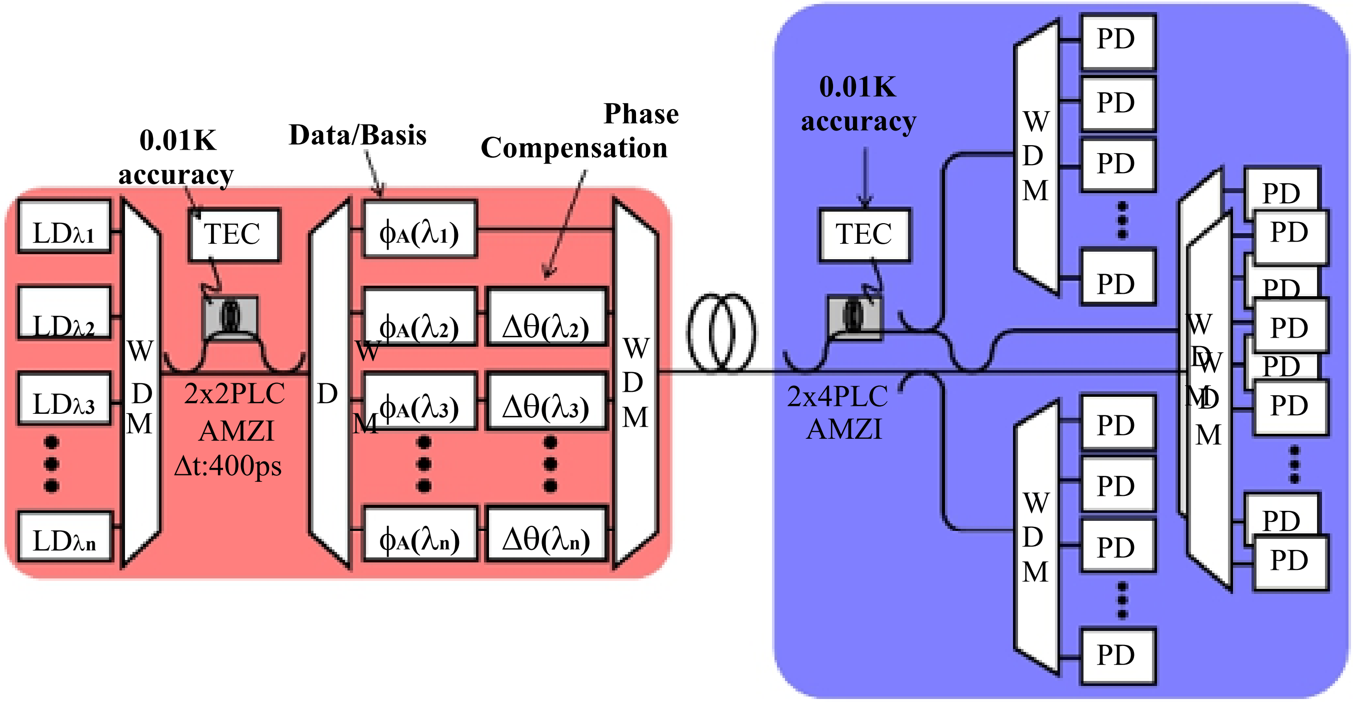
NEC's QKD system

- **WDM up to 8 channels with "Colorless interferometric technique"**
  - **The same Mach Zehnder interferometers for 8 channels**

    → Easy control, small size , save money

- **1.25GHz clock x 8 channels = 10GHz system in total**

A. Tanaka et al., ECOC2009, 1.4.2 (2009)



PD: photon detector

This slide is presented by the courtesy of NEC

Key distillation hardware engine

Requirements

key distillation HW

This slide is presented by the courtesy of NEC

Key distillation hardware engine

Requirements

- 50Gbps random number input
  - 10GHz photon transmission x 5 bit

    5 bit: Basis (1bit), Data (1bit), Decoy (2bit), EC&PA (1bit)
- Large size matrix multiplication for EC & PA processes

  code length: 1M bit
- Real-time processing

key distillation HW

This slide is presented by the courtesy of NEC

Key distillation hardware engine

Requirements

- 50Gbps random number input
  - 10GHz photon transmission x 5 bit
    5 bit: Basis (1bit), Data (1bit), Decoy (2bit), EC&PA (1bit)
- Large size matrix multiplication for EC & PA processes
  code length: 1M bit
- Real-time processing

key distillation HW

Key features

- 6 FPGAs for high speed data processing
- 5 Gb (= 40Gbit) memory in total
- 9 XFPs for high speed interface

This slide is presented by the courtesy of NEC

Key distillation hardware engine

Requirements

- 50Gbps random number input
  - 10GHz photon transmission x 5 bit

    5 bit: Basis (1bit), Data (1bit), Decoy (2bit), EC&PA (1bit)
- Large size matrix multiplication for EC & PA processes

  code length: 1M bit
- Real-time processing

key distillation HW

Key features

- 6 FPGAs for high speed data processing
- 5 Gb (= 40Gbit) memory in total
- 9 XFPs for high speed interface

Flexible hardware

This slide is presented by the courtesy of NEC

Key distillation hardware engine

Requirements

- 50Gbps random number input
  - 10GHz photon transmission x 5 bit
    5 bit: Basis (1bit), Data (1bit), Decoy (2bit), EC&PA (1bit)
- Large size matrix multiplication for EC & PA processes
  code length: 1M bit
- Real-time processing

key distillation HW

Key features

- 6 FPGAs for high speed data processing
- 5 Gb (= 40Gbit) memory in total
- 9 XFPs for high speed interface

Processing time < 300ms for each 1Mbit block

⇨ real-time processing

This slide is presented by the courtesy of NEC

Toward stable key generation

Source: Google map

Loss: 13dB
(Corresponds to about 50km of a typical good fiber)
Round trip: 22km

This slide is presented by the courtesy of NEC

Toward stable key generation

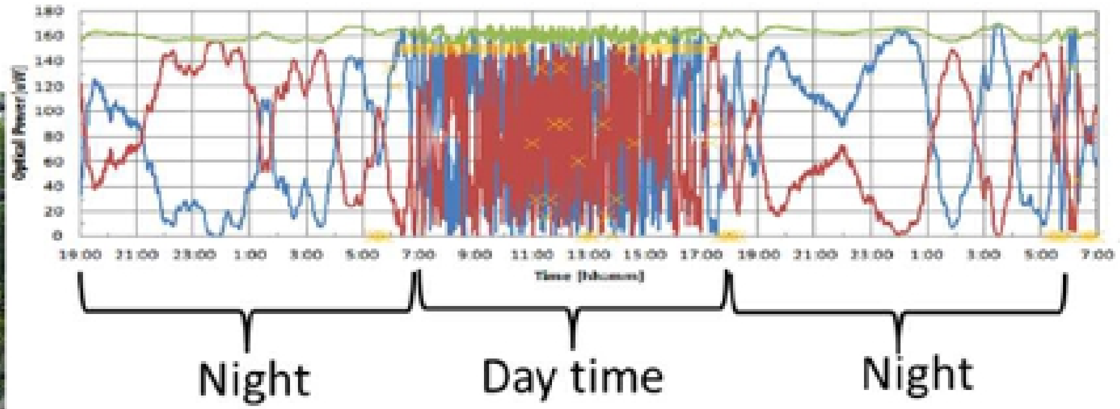
More than 95% of the line: overhead

This slide is presented by the courtesy of NEC

Toward stable key generation

More than 95% of the line: overhead

Polarization fluctuation in time (29th -31st Aug)

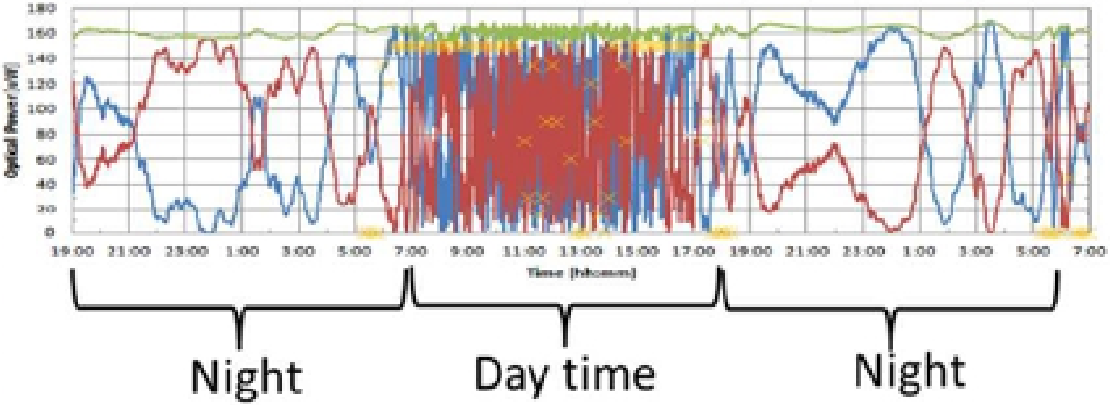


This slide is presented by the courtesy of NEC

Toward stable key generation

More than 95% of the line: overhead

Polarization fluctuation in time (29th -31st Aug)



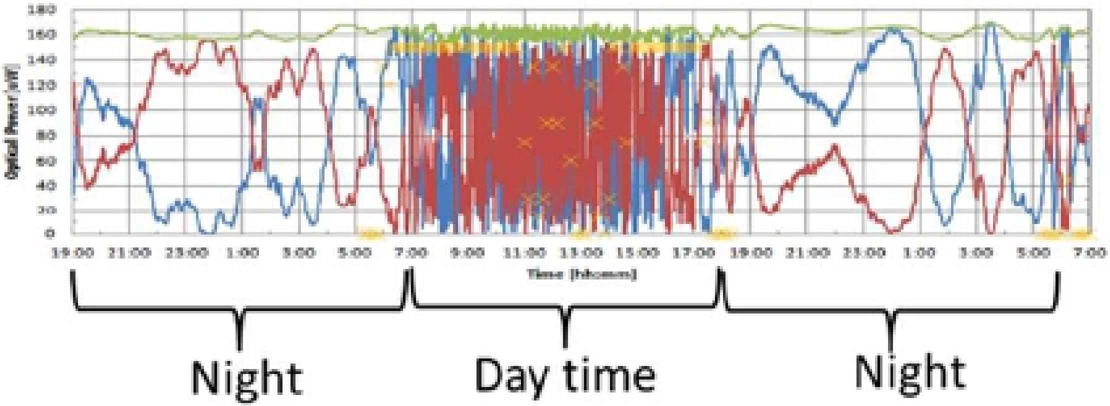
Lesson: Keep your system polarization independent

This slide is presented by the courtesy of NEC

Toward stable key generation

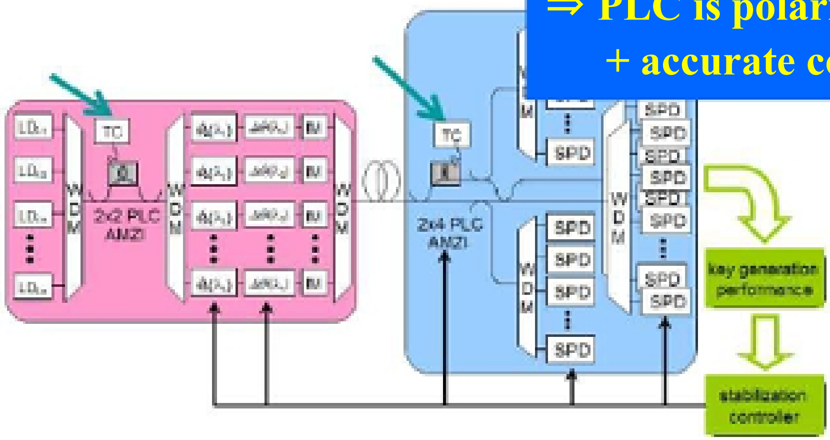
More than 95% of the line: overhead

Polarization fluctuation in time (29th -31st Aug)



Lesson: Keep your system polarization independent

⇒ PLC is polarization independent for some temperature regime
+ accurate control of interferometer for low QBER

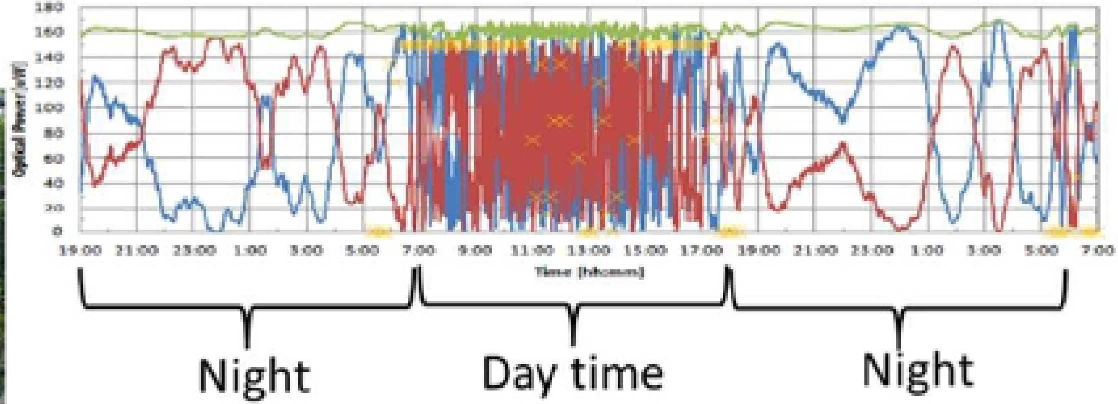


This slide is presented by the courtesy of NEC

Toward stable key generation

More than 95% of the line: overhead

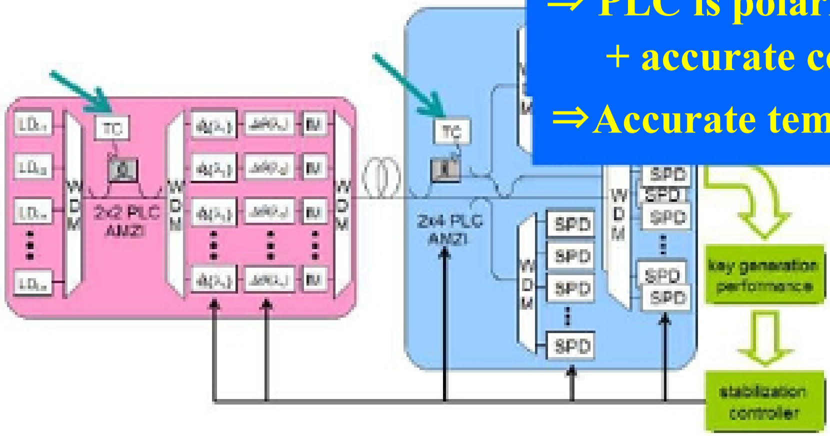
Polarization fluctuation in time (29th -31st Aug)



Lesson: Keep your system polarization independent

⇒ **PLC is polarization independent for some temperature regime**
+ accurate control of interferometer for low QBER

⇒**Accurate temperature of PLC (~0.01K)**



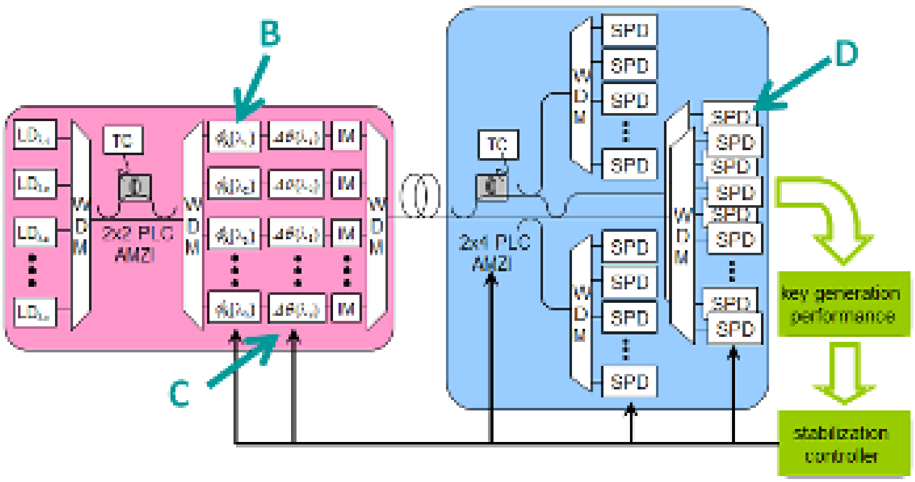
This slide is presented by the courtesy of NEC

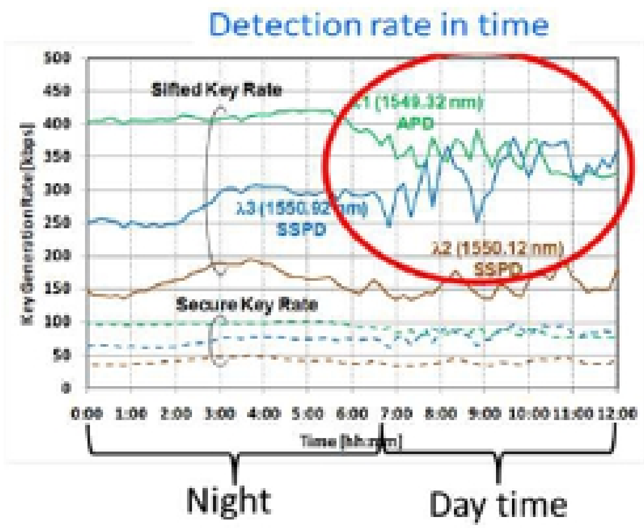
Toward stable key generation

A) Accurate temperature of PLC (~0.01K) for low QBER and polarization independence

Key points : Control of other components

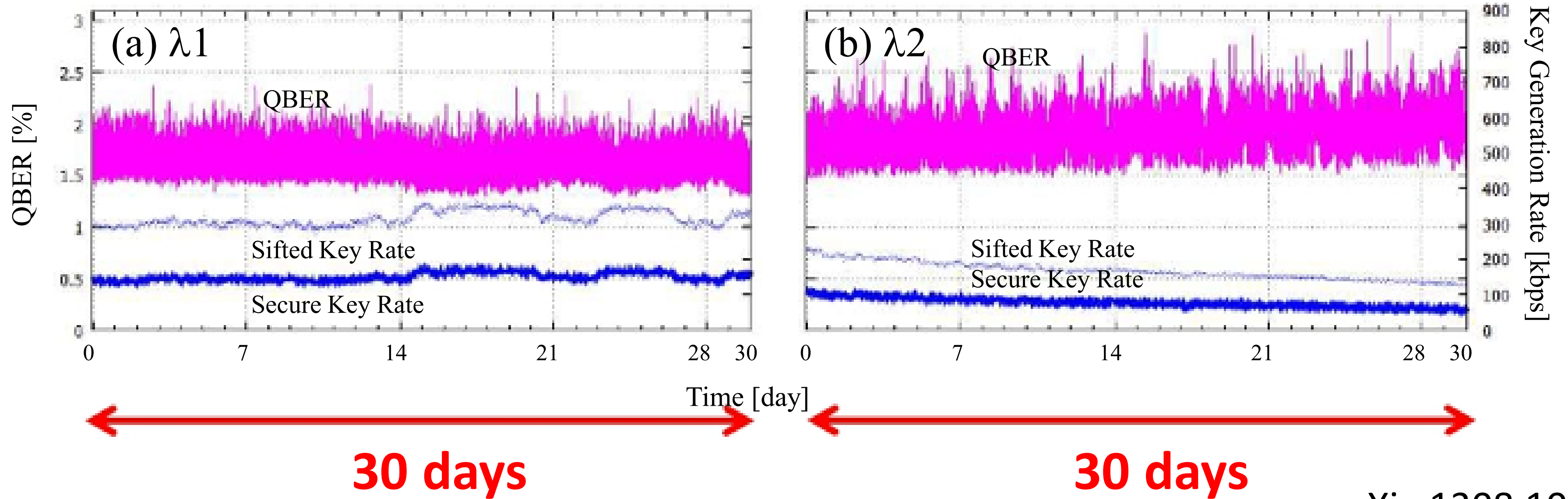
B) Modulator bias voltage
C) Modulation amplitude of phase compensation
D) Gate pulse timing for APDs





This slide is presented by the courtesy of NEC

Maintenance-free long-term field demonstration



arXiv:1308.1011

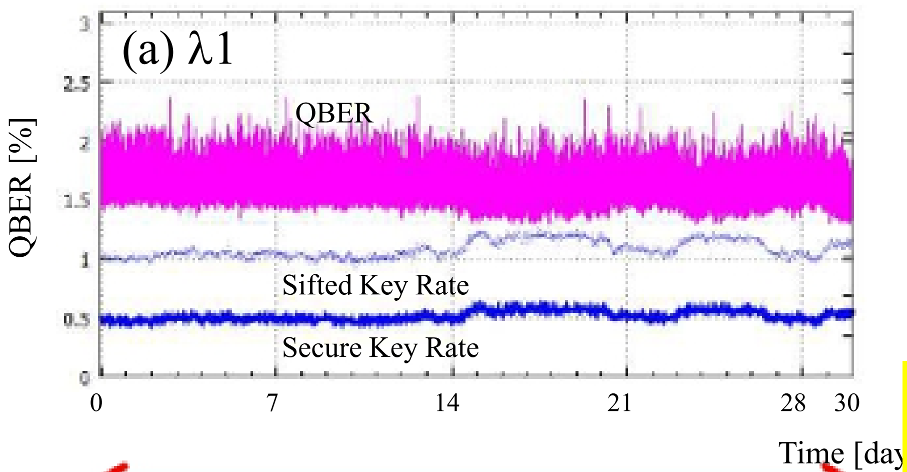
Wavelength[nm]	QBER[%]	Siftedkey[kbps]	Securekey[kbps]
λ1:1547.72	1.61	315.3	151.5
λ2:1550.92	1.86	168.0	78.3
Total	**1.70 (av)**	**483.3**	**229.8**

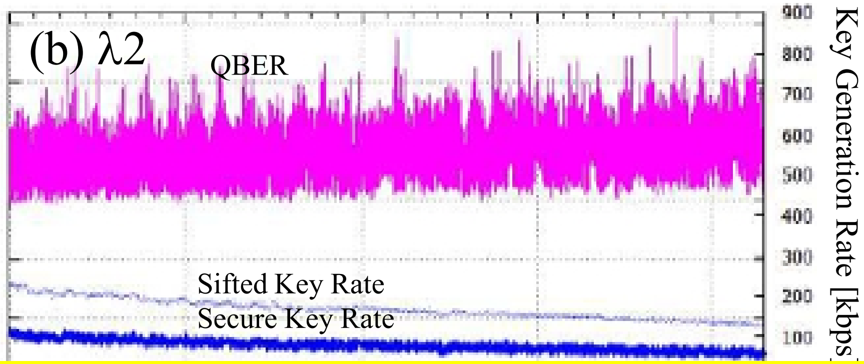
Loss: 13dB, 22km, Overhead ratio 95%

c.f. IP phone: 100kbps
Video meeting: 800kbps

This slide is presented by the courtesy of NEC

Maintenance-free long-term field demonstration





Degradation of the APD's cooling system due to imperfect sealing

30 days

30 days

arXiv:1308.1011

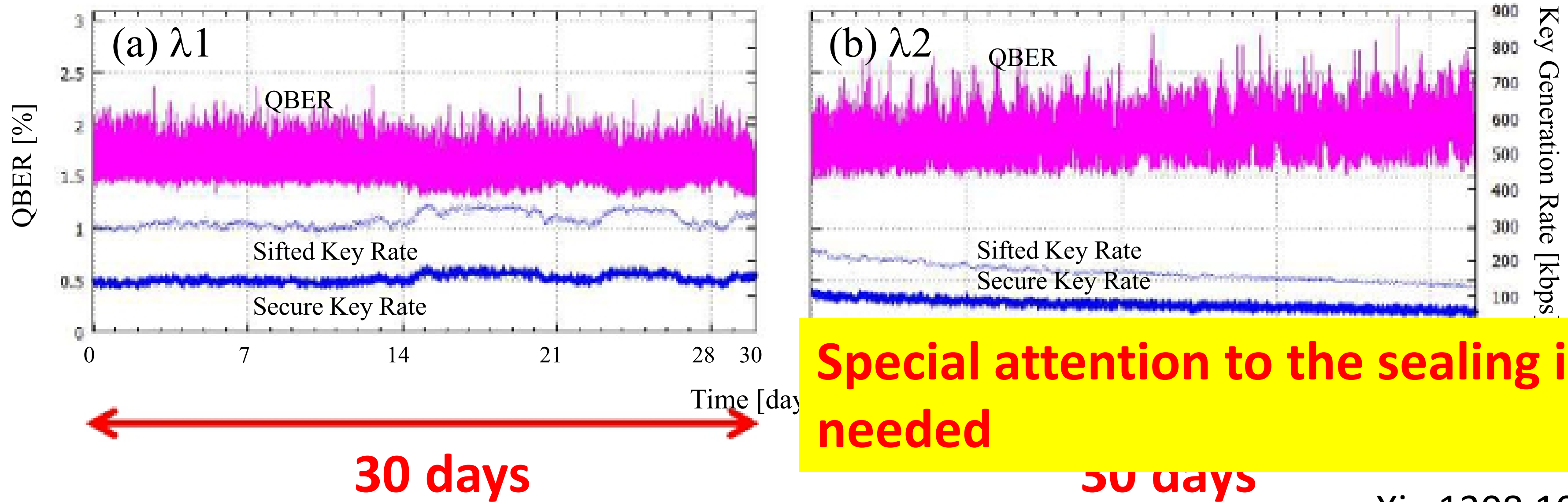
Wavelength[nm]	QBER[%]	Siftedkey[kbps]	Securekey[kbps]
λ1:1547.72	1.61	315.3	151.5
λ2:1550.92	1.86	168.0	78.3
Total	**1.70 (av)**	**483.3**	**229.8**

Loss: 13dB, 22km, Overhead ratio 95%

c.f. IP phone: 100kbps
Video meeting: 800kbps

This slide is presented by the courtesy of NEC

Maintenance-free long-term field demonstration



Special attention to the sealing is needed

arXiv:1308.1011

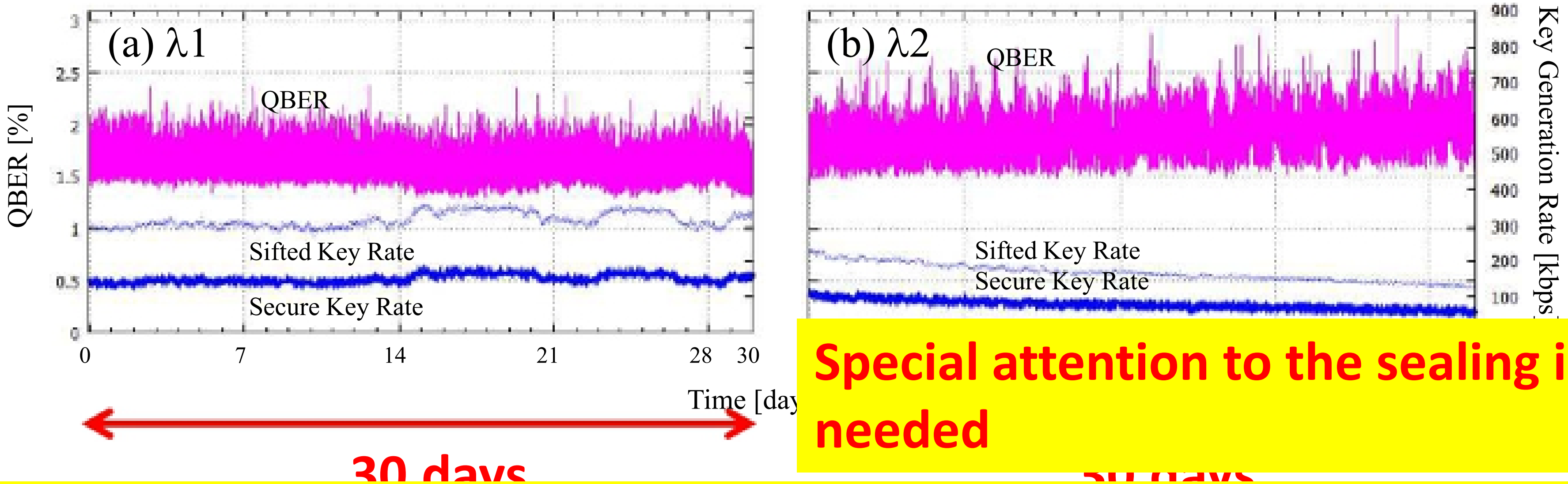
Wavelength[nm]	QBER[%]	Siftedkey[kbps]	Securekey[kbps]
λ1:1547.72	1.61	315.3	151.5
λ2:1550.92	1.86	168.0	78.3
Total	**1.70 (av)**	**483.3**	**229.8**

Loss: 13dB, 22km, Overhead ratio 95%

c.f. IP phone: 100kbps
Video meeting: 800kbps

This slide is presented by the courtesy of NEC

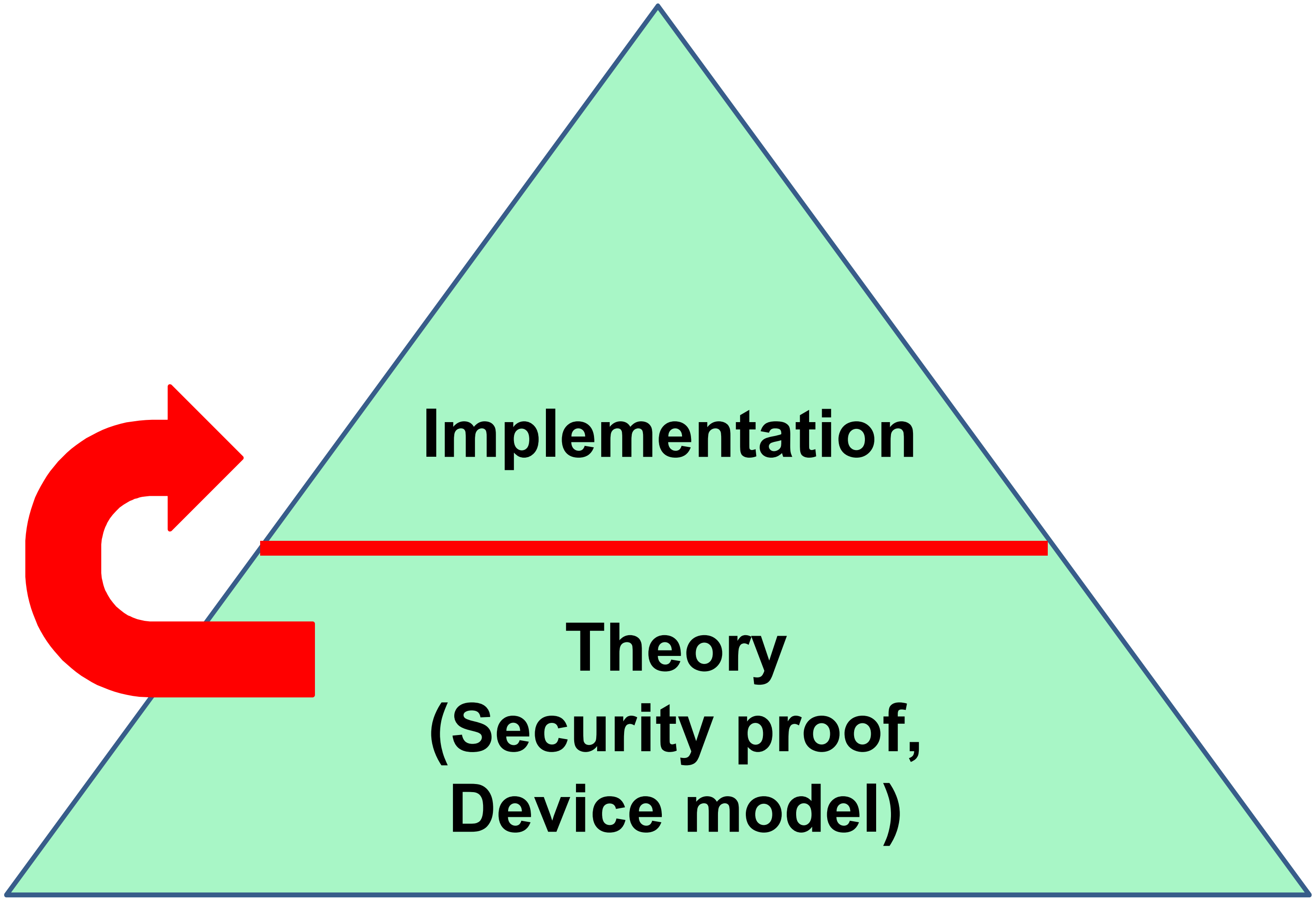
Maintenance-free long-term field demonstration

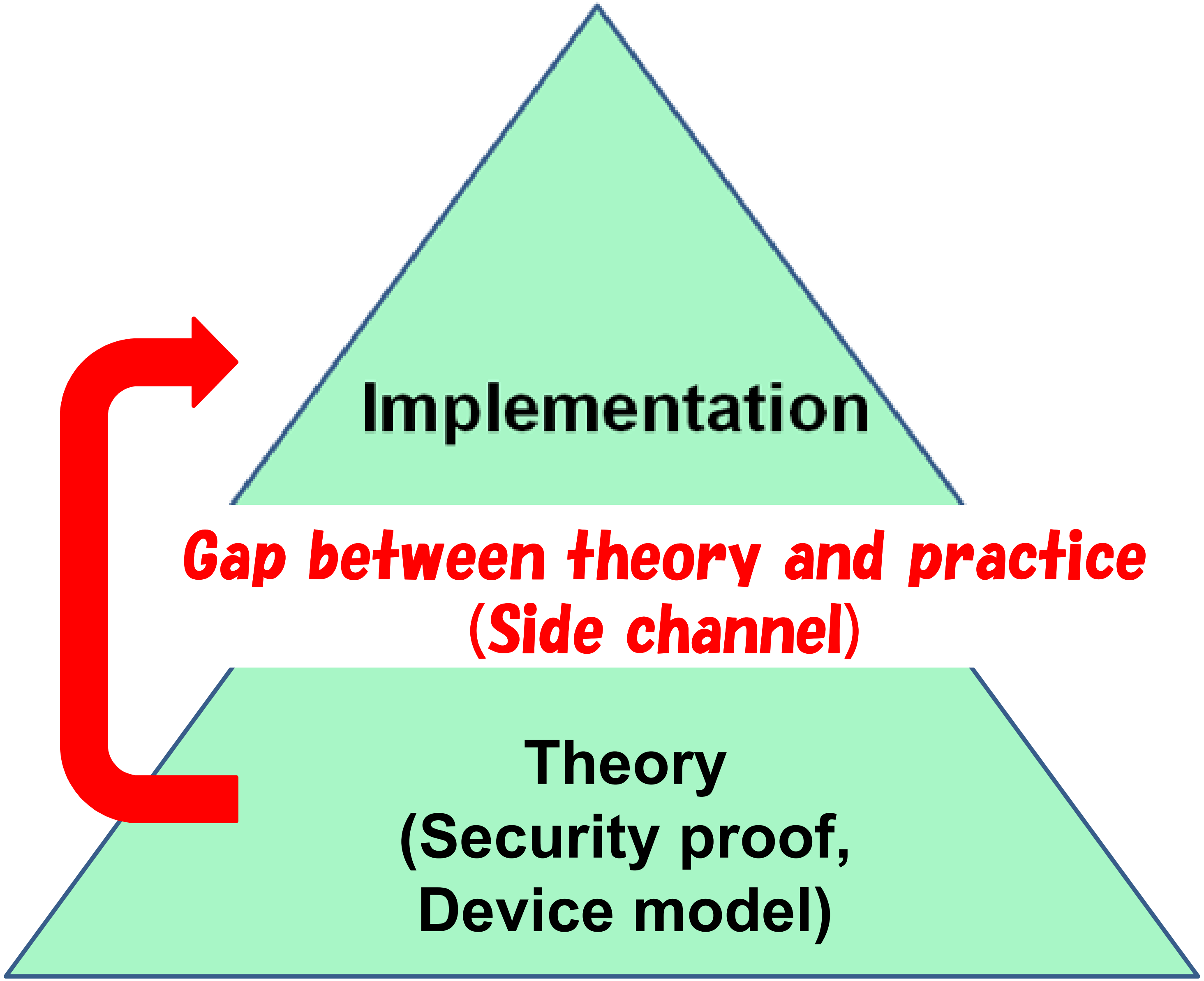


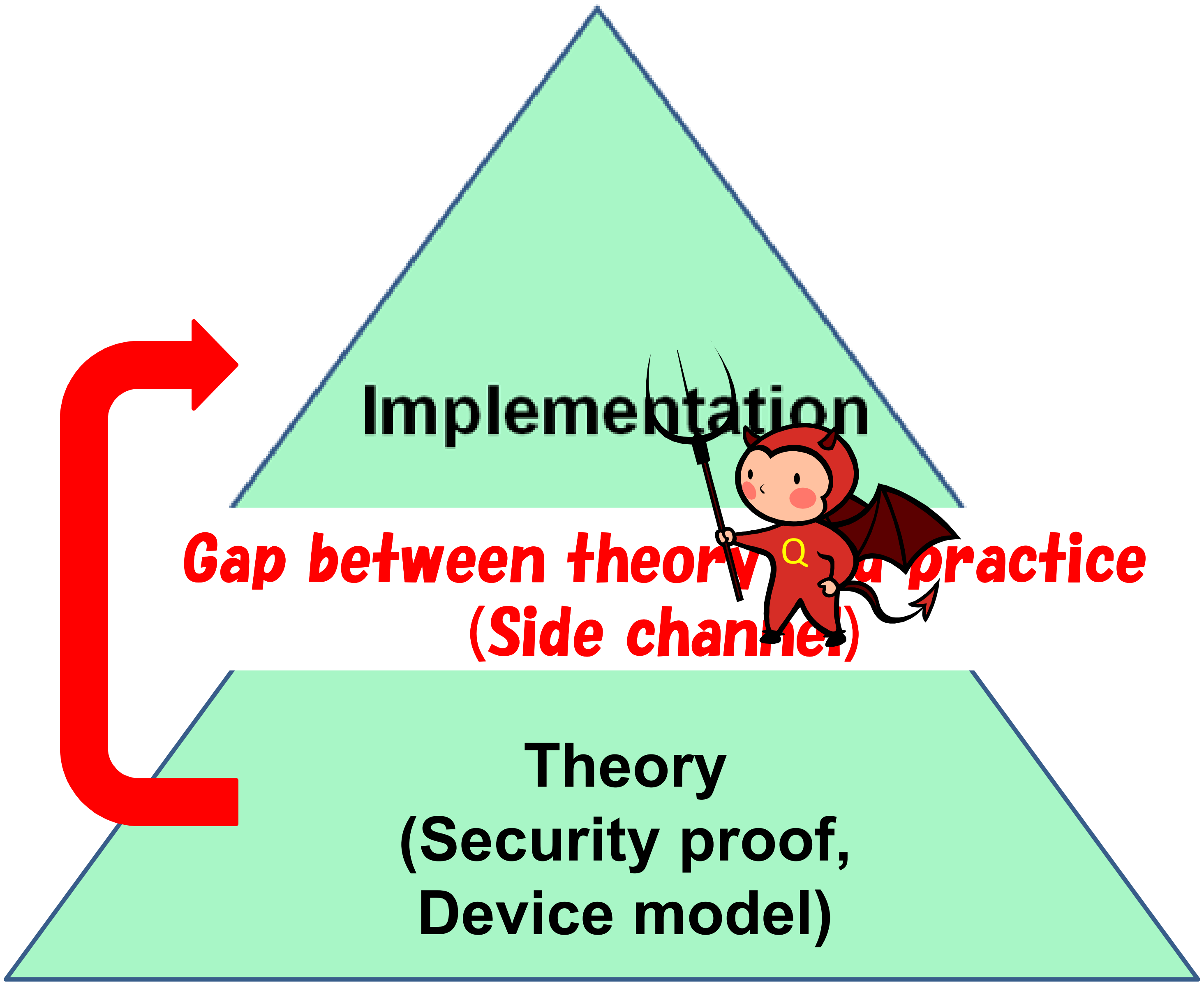
Special attention to the sealing is needed

Past: we worry about the stability.
Now, it is time to

- **Seriously investigate the life time of each component device to construct a reliable QKD system**
- **Consider implementations of countermeasures against side channels**


Implementation
Theory
(Security proof,
Device model)


Implementation
Gap between theory and practice
(Side channel)
Theory
(Security proof,
Device model)


Implementation
Gap between theory
practice
(Side chan
Theory
(Security proof,
Device model)

Two approaches to combat side-channels

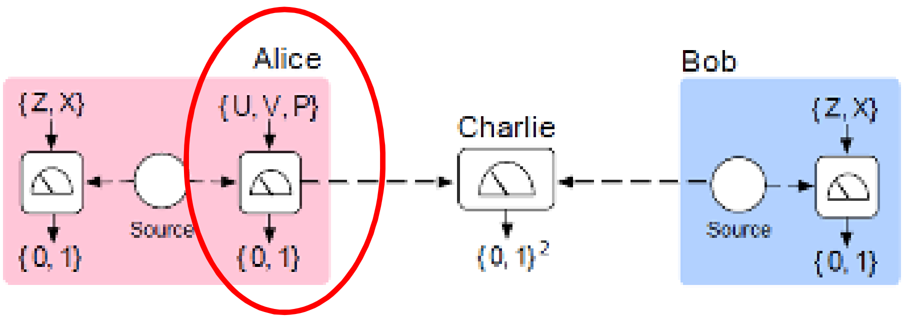
Device independent QKD

- ✓ Few assumptions (independence of the state & measurement, etc) ☺
- ✓ You do not need to fully characterize your device ☺
- ✓ Technologically challenging and impractical

Security based on physical assumptions

- ✓ More assumptions ☹
- ✓ Trust your device ☹
- ✓ Longer distance and practical☺

Local Bell test

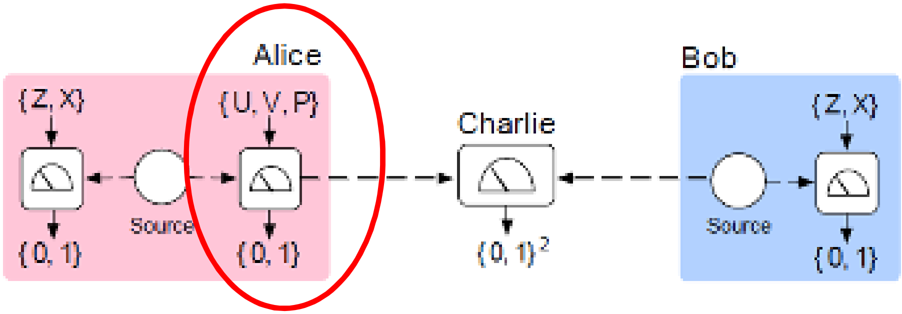


C. C. Wen Lim, C. Portmann, et.al., arXiv:1208.0023

Two approaches to combat side-channels

Device independent QKD	*Security based on physical assumptions*
✓ Few assumptions (independence of the state & measurement, etc) ☺	✓ More assumptions ☹
✓ You do not need to fully characterize your device ☺	✓ Trust your device ☹
✓ Technologically challenging and impractical	✓ Longer distance and practical☺

Local Bell test

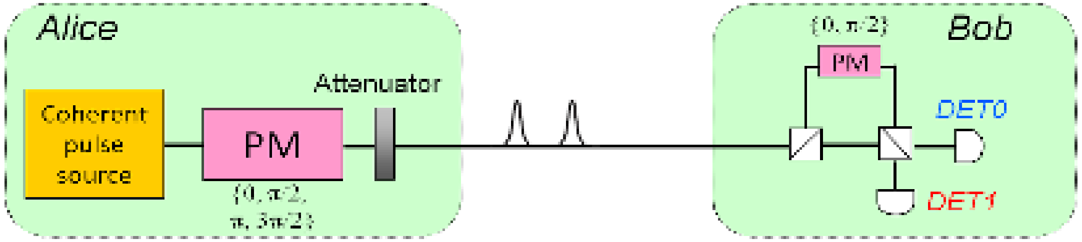


C. C. Wen Lim, C. Portmann, et.al., arXiv:1208.0023

What does the theory require to the QKD system?

High quality random numbers

Classical side channel

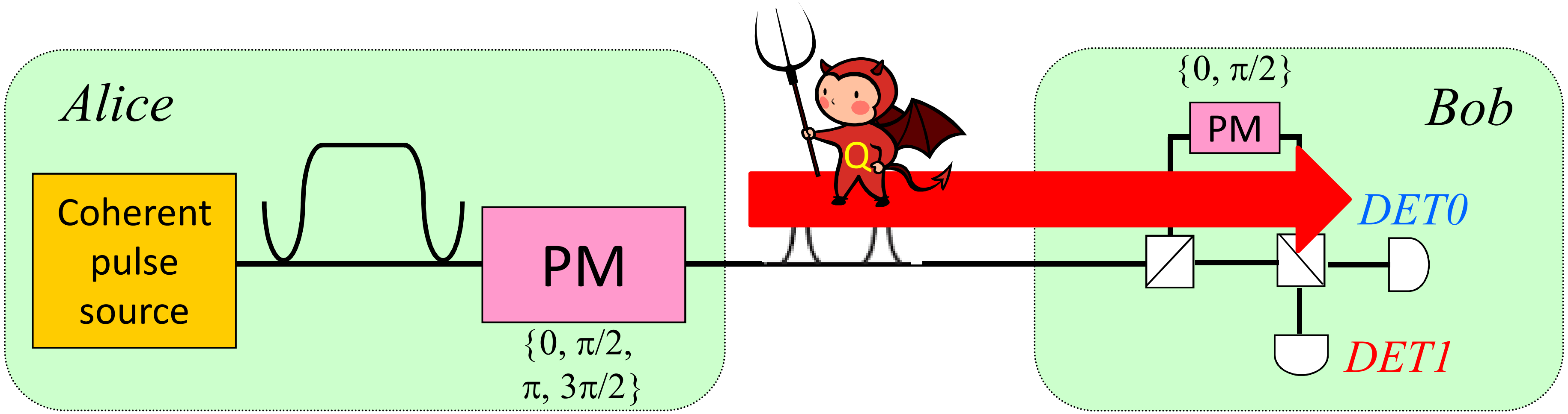


Precise state preparation

Precise measurement

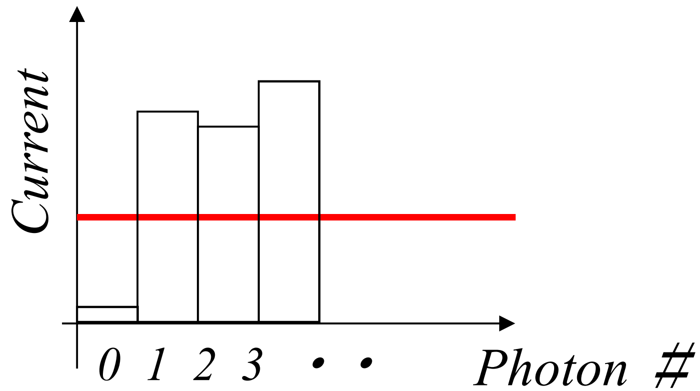
Detection unit is most fragile

Blight pulse illumination attack

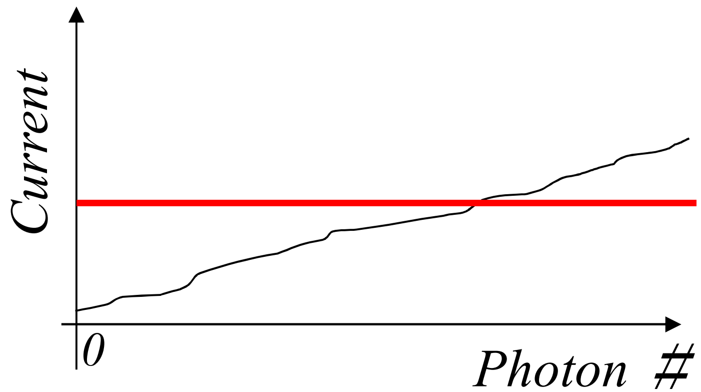


L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics 4, 686 (2010). L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs.

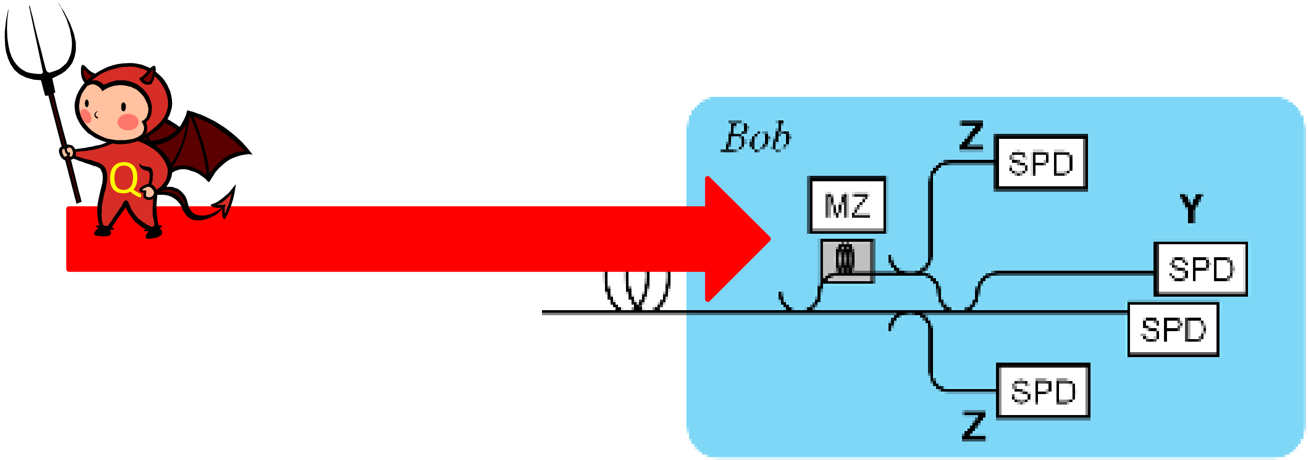
Normal mode



Linear mode



Countermeasure against bright pulse illumination attack

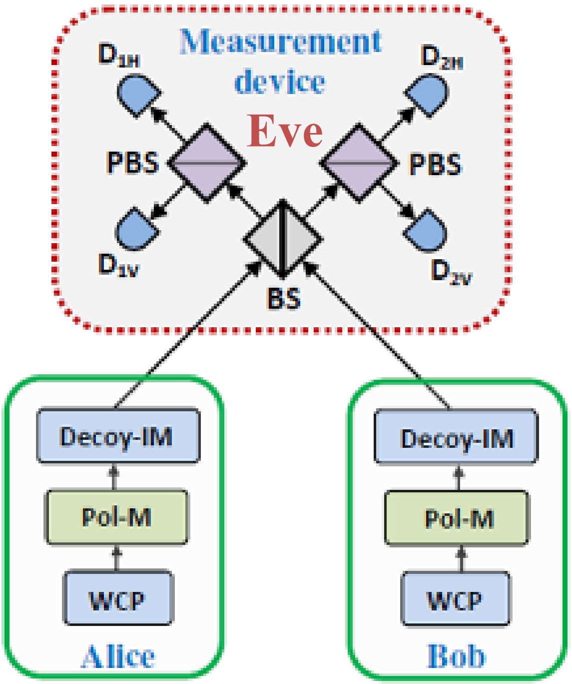


- **If more than 2 detectors click, then we discard the block, reset the SPDs and restart (8000 photons are needed to blind a SSPD*)**

Can we *completely* close all the side channel of *the detectors*?

*M. Fujiwara, et. al, Optics Express, 21, 5, pp. 6304 (2013)

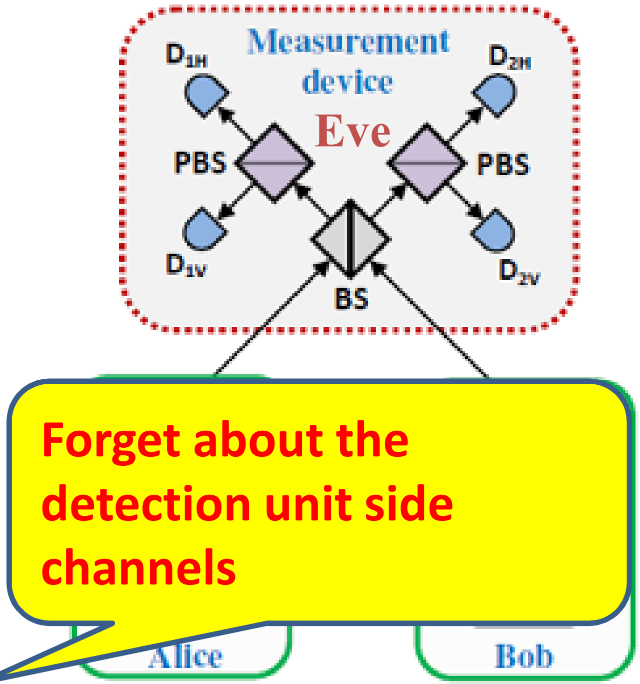
Measurement device independent QKD (MDIQKD)



H-K. Lo, M. Curty, and B. Qi, PRL. **108**, 130503 (2012)
Experiment: A. Rubenok, J. A. Slater, et.al., arXiv:1304.2463
T. F. da Silva, D. Vitoreti, et.al., arXiv:1207.6345
Y. Liu, T-Y Chen, et.al., arXiv:1209.6178
Z. Tang, Z. Liao, et.al., arXiv:1306.6134
F. Xu, B. Qi, et.al., arXiv:1306.5814

- ✓ **Completely free from any possible security loophole in the detectors!**
- ✓ **The security is based on time reversal of quantum swapping**

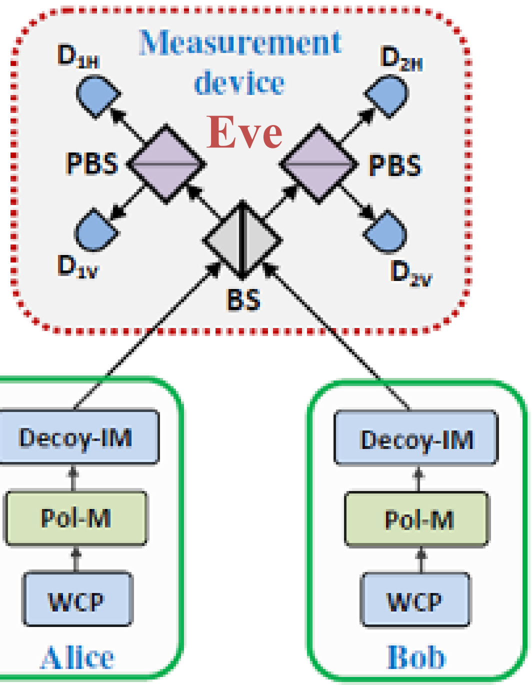
Measurement device independent QKD (MDIQKD)



H-K. Lo, M. Curty, and B. Qi, PRL. **108**, 130503 (2012)
Experiment: A. Rubenok, J. A. Slater, et.al., arXiv:1304.2463
T. F. da Silva, D. Vitoreti, et.al., arXiv:1207.6345
Y. Liu, T-Y Chen, et.al., arXiv:1209.6178
Z. Tang, Z. Liao, et.al., arXiv:1306.6134
F. Xu, B. Qi, et.al., arXiv:1306.5814

- ✓ **Completely free from any possible security loophole in the detectors!**
- ✓ **The security is based on time reversal of quantum swapping**

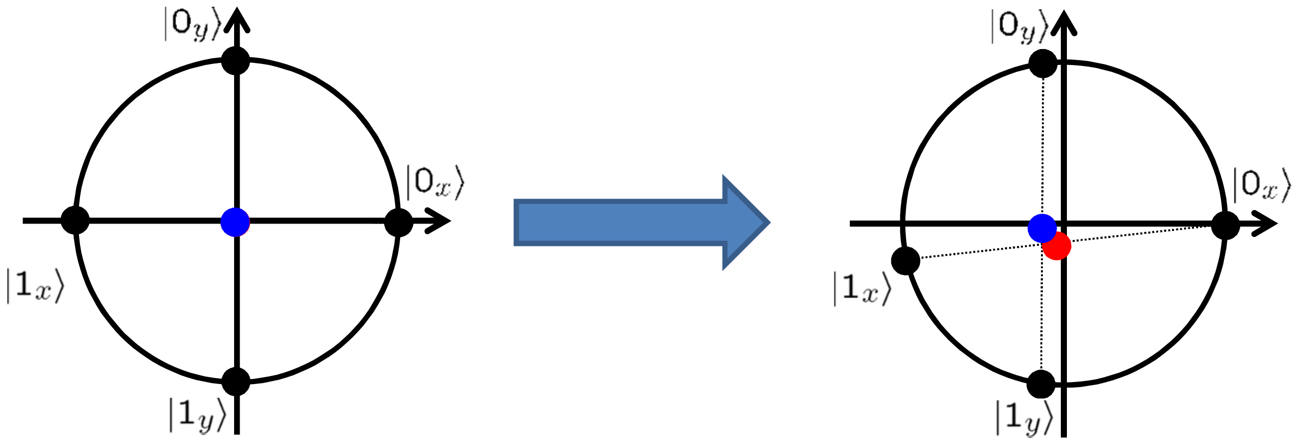
Measurement device independent QKD (MDIQKD)



As far as we can characterize the source, we can generate a key

Hmm, I can exploit the imperfect state !! PM is NOT perfect!!

Basis dependent flaw



Ideally ***In practice***

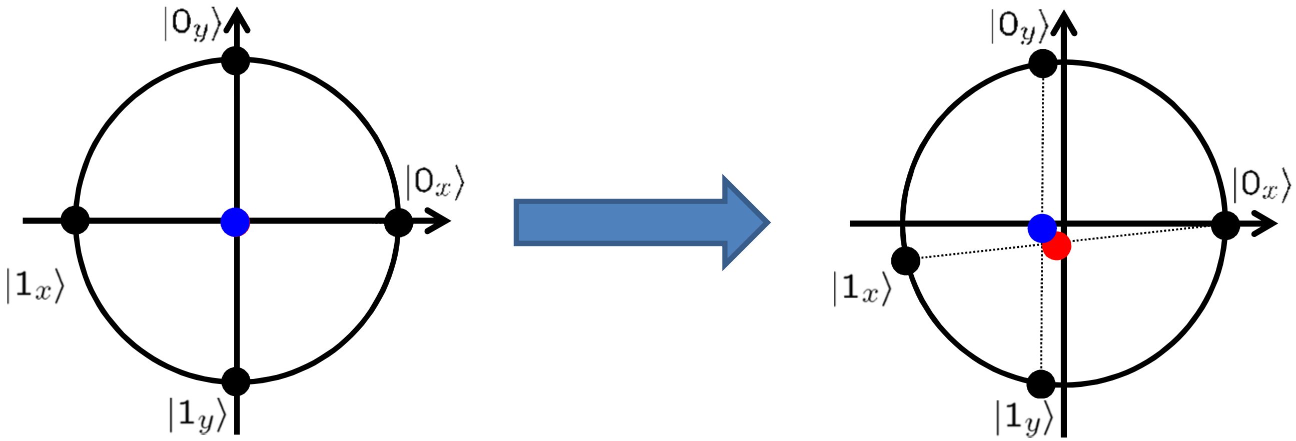
$$R \propto 1 - h(\delta_x) - h(\delta'_y)$$

$$\begin{cases} \delta'_y \le \delta_y + 4\Delta + 4\sqrt{\Delta\delta_y} \\ \Delta = \left(1 - F\left(\rho_Y, \rho_X\right)\right)/2 \end{cases}$$

D. Gottesman, H. K. Lo, N. Luetkenhaus, and J. Preskill, Quant. Inf. Comput. 5, 325 (2004).
M. Koashi, arXiv:quant-ph/0505108.

Qubit ⇒ Loss independent

Basis dependent flaw



Ideally ***In practice***

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

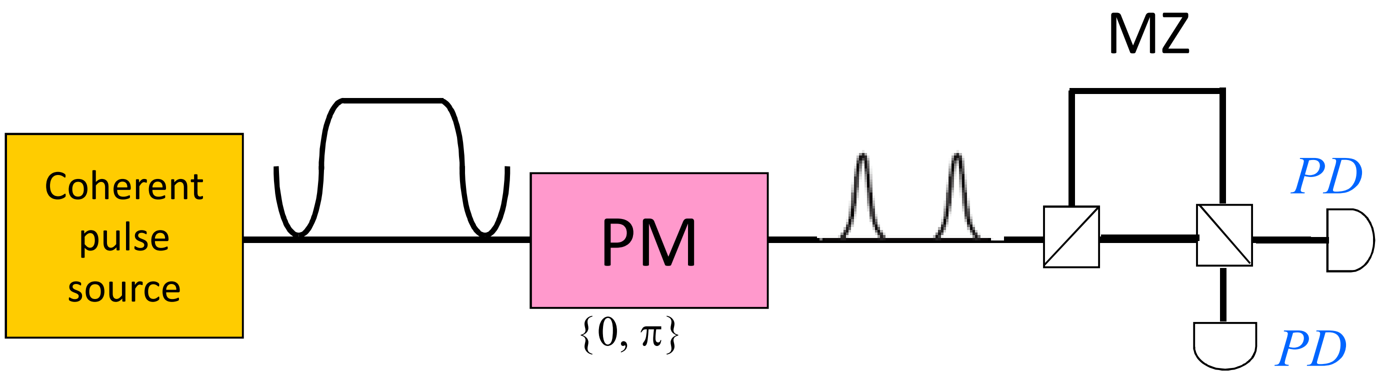
$$\begin{cases} \delta'_y \leq \delta_y + 4\Delta + 4\sqrt{\Delta \delta_y} \\ \Delta = \left(1 - F\left(\rho_Y, \rho_X\right)\right)/2 \end{cases}$$

D. Gottesman, H. K. Lo, N. Luetkenhaus, and J. Preskill, Quant. Inf. Comput. 5, 325 (2004).
M. Koashi, arXiv:quant-ph/0505108.

You have to estimate of the precision of PM

Towards precise and real time monitoring of PM

Standard measurement of the precision of PM

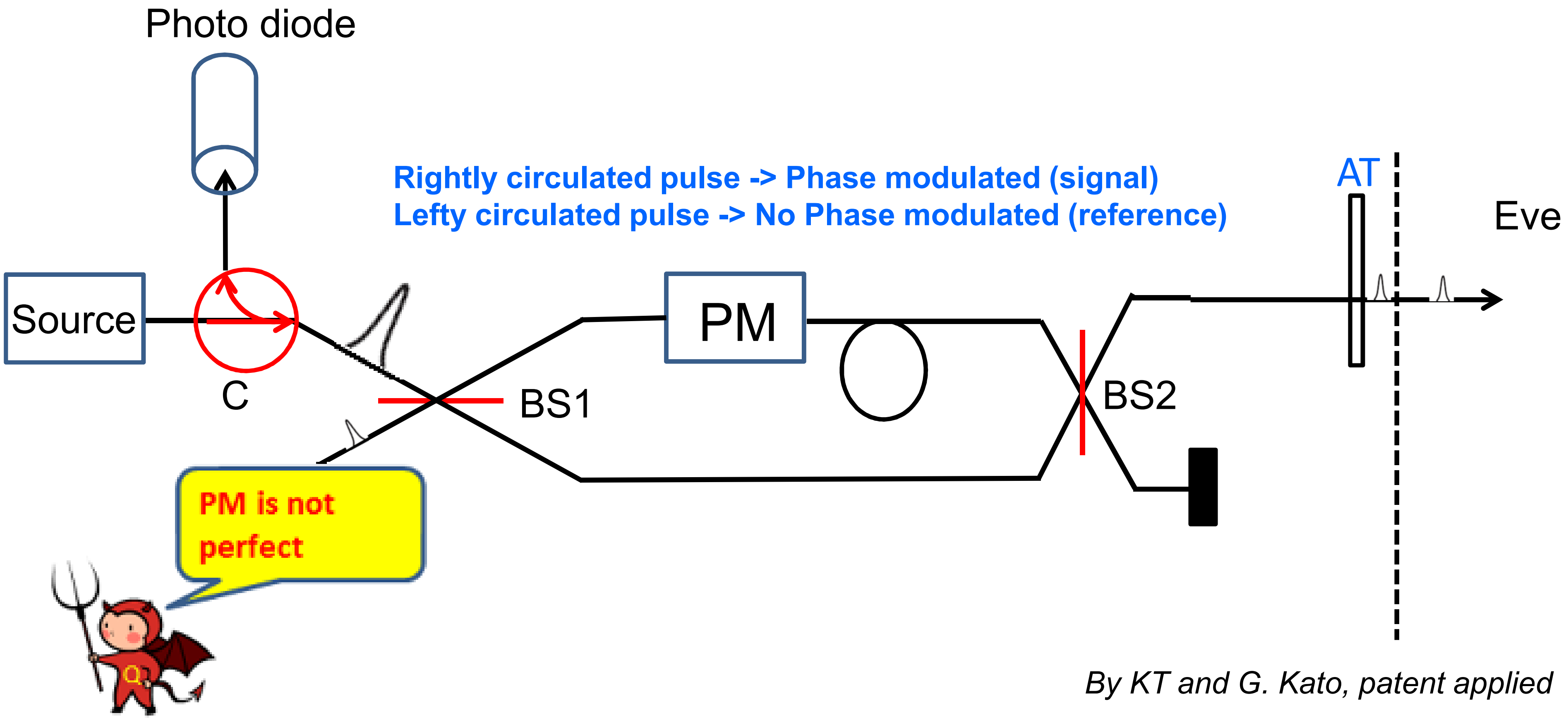


Observe extinction ratio

PM is not perfect

Is it PM or MZ that causes an error?

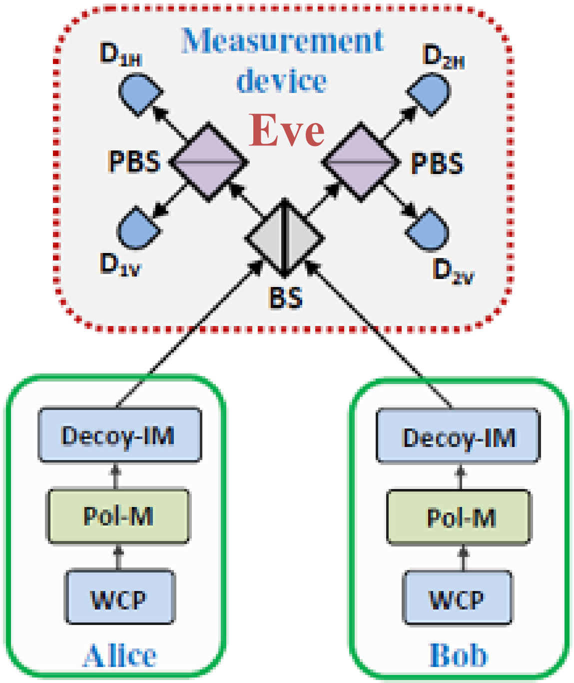
Towards precise and real time monitoring of PM



By KT and G. Kato, patent applied

- ✓ *Interferometer-independent* accuracy
- ✓ Real time monitoring
- ✓ This device can be used for standard BB84 and MDI BB84

Measurement device independent QKD (MDIQKD)

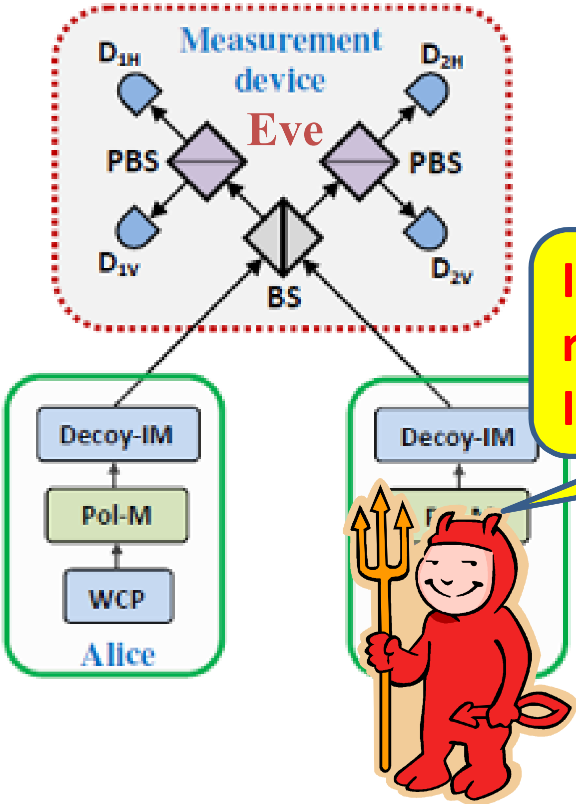


Look, we have the theory, and the phase modulation is OK

Hmm, I can exploit the imperfect state !! PM is NOT perfect!!

NTT

Measurement device independent QKD (MDIQKD)

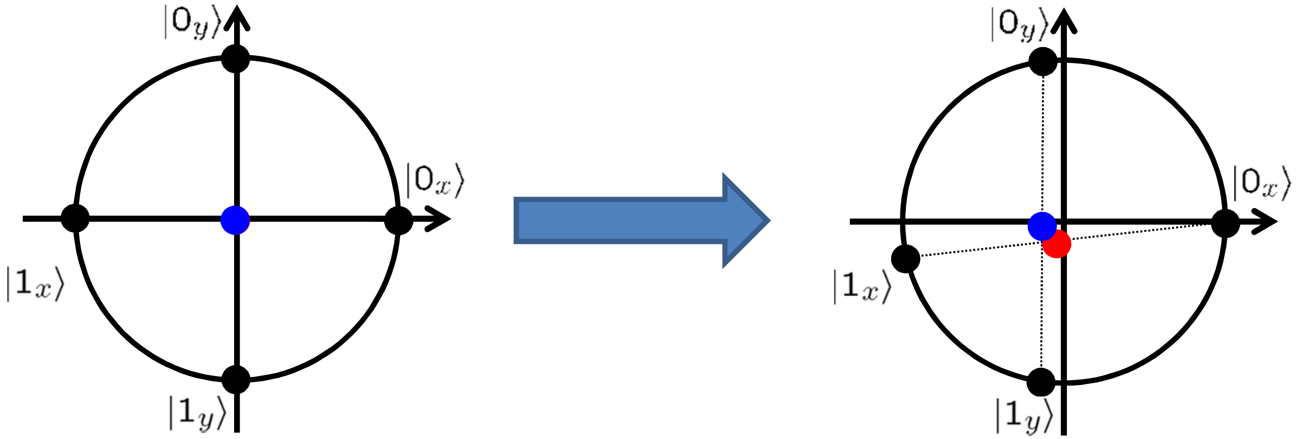


Is it really a qubit? Is it really phase randomized? I can still hack!

Look, we have the theory, and the phase modulation is OK

Hmm, I can exploit the imperfect state !! PM is NOT perfect!!

Basis dependent flaw



Ideally ***In practice***

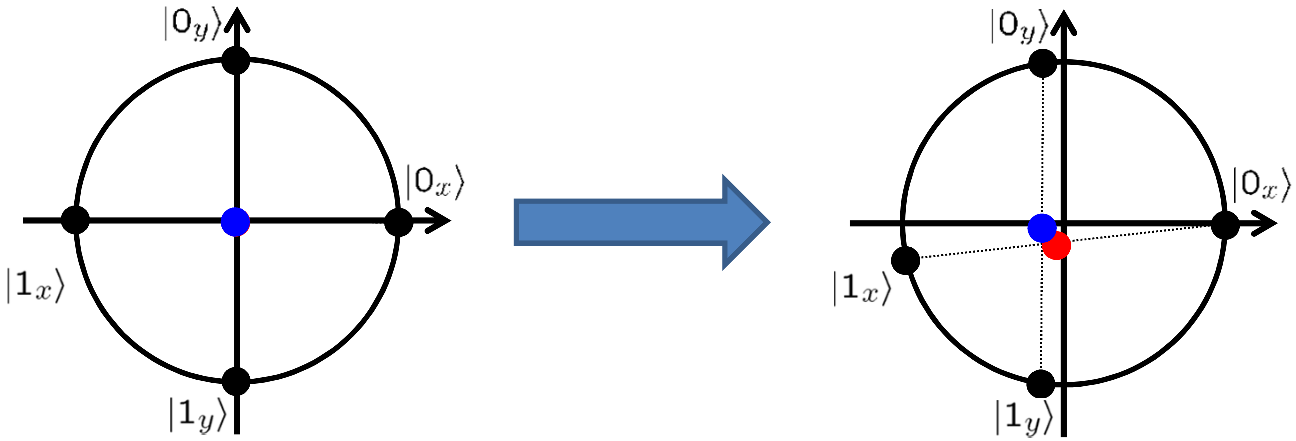
$$R \propto 1 - h(\delta_x) - h(\delta'_y)$$

$$\begin{cases} \delta'_y \leq \delta_y + 4\Delta + 4\sqrt{\Delta \delta_y} \\ \Delta = \left(1 - F\left(\rho_Y, \rho_X\right)\right)/2 \end{cases}$$

D. Gottesman, H. K. Lo, N. Luetkenhaus, and J. Preskill, Quant. Inf. Comput. 5, 325 (2004).
M. Koashi, arXiv:quant-ph/0505108.

Qubit ⇒ Loss independent

Basis dependent flaw



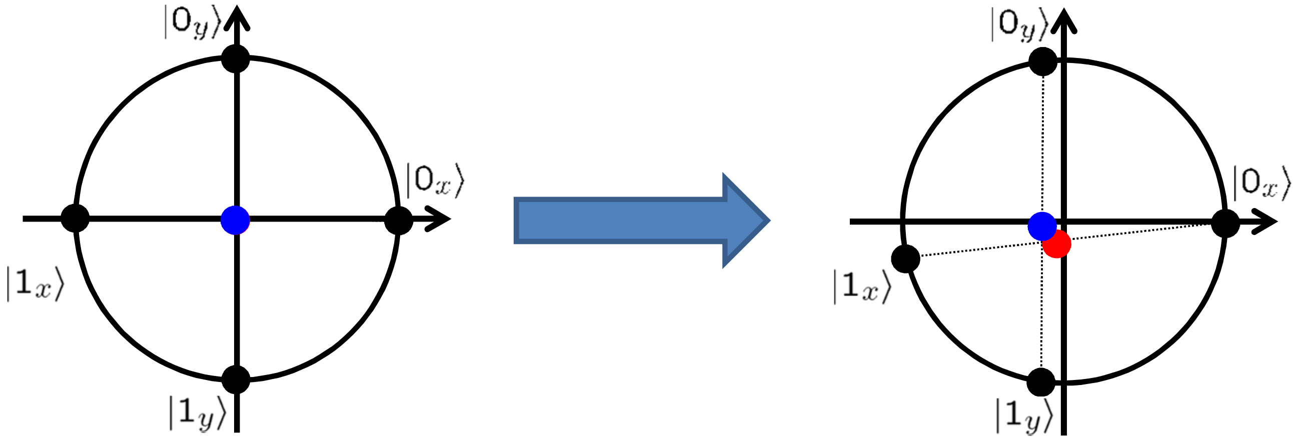
Ideally ***In practice***

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

$$\begin{cases} \delta'_y \leq \delta_y + 4\Delta + 4\sqrt{\Delta\delta_y} \\ \Delta = \left(1 - F\left(\rho_Y, \rho_X\right)\right)/2 \end{cases}$$

If the state is NOT in a qubit

Basis dependent flaw



Ideally ***In practice***

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

$$\begin{cases} \delta'_y \leq \delta_y + 4\Delta + 4\sqrt{\Delta\delta_y} \\ \Delta = \left(1 - F\left(\rho_Y, \rho_X\right)\right)/2 \end{cases}$$

Pessimistic

$$\Delta = \left[\left(1 - F\left(\rho_Y, \rho_X\right)\right)/2\right]/\eta_{\mathrm{detection}}$$

Exponential increase of the flaw!

NTT

Basis dependent flaw

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

$$\begin{cases} \delta'_y \leq \delta_y + 4\Delta + 4\sqrt{\Delta \delta_y} \\ \Delta = \left(1 - F\left(\rho_Y, \rho_X\right)\right)/2 \end{cases}$$

Pessimistic

$$\Delta = \left[\left(1 - F\left(\rho_Y, \rho_X\right)\right)/2\right]/\eta_{\mathrm{detection}}$$

Exponential increase of the flaw!

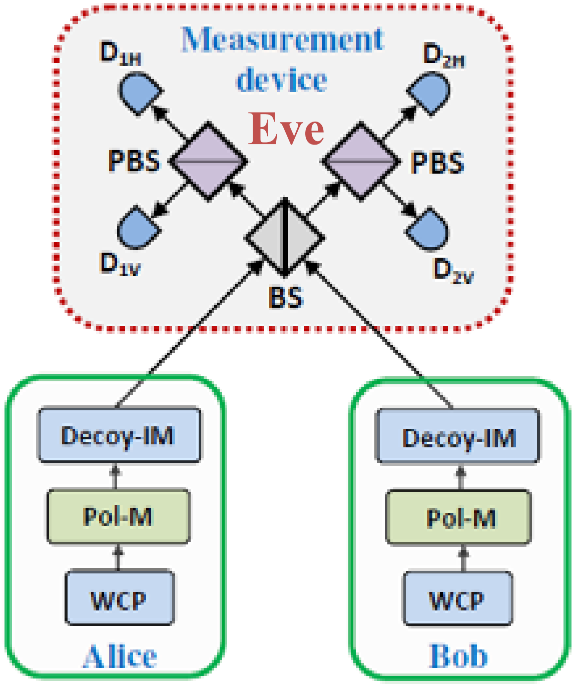
Qubit: **The signal states are linearly dependent**

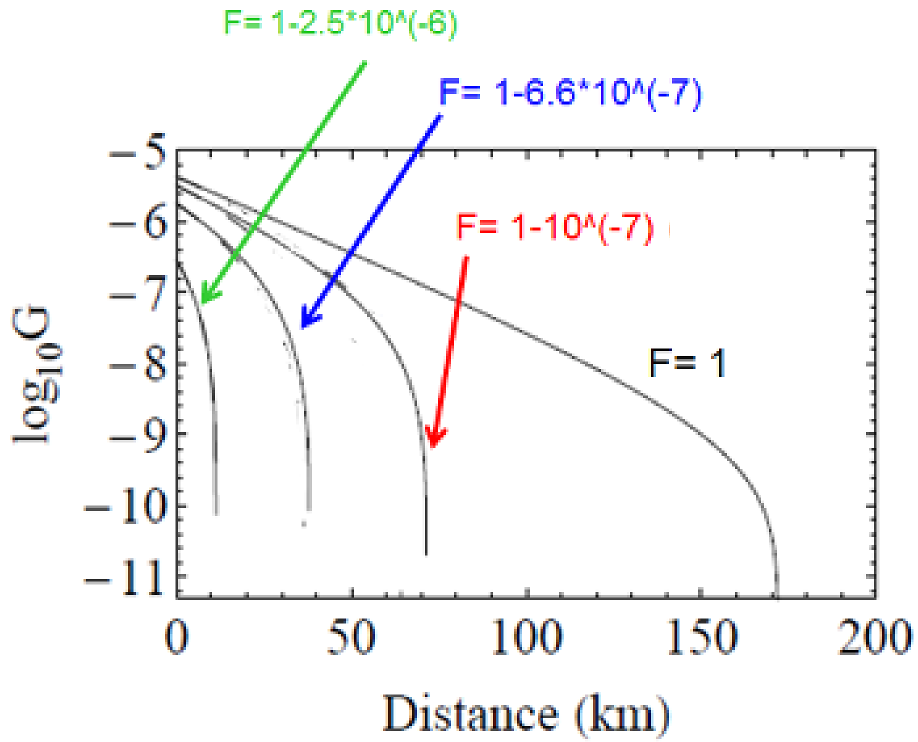
Multi mode: **The signal states are linearly **independent****

→ ***Unambiguous state discrimination***

Basis dependent flaw

If the state is in multi mode, pessimistically we have



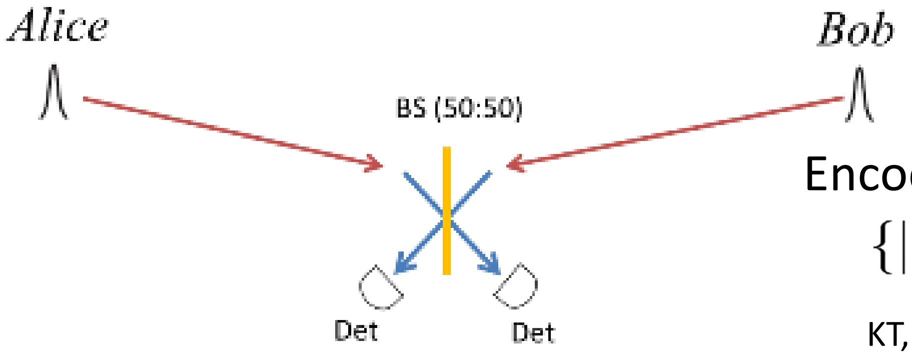


KT, H-K. Lo, C-H. F. Fung, B. Qi, Phys. Rev. A 85, 042307 (2012) (arXiv:1111.3413)

M. Sasaki, M. Fujiwara, et al, Optics Express **19**, 10387 (2011)

$F\left(\rho_Y, \rho_X\right)$ is determined only by the accuracy of PM

Phase encoding scheme for MDIQKD



Encoding: phase non-randomized BB84 state

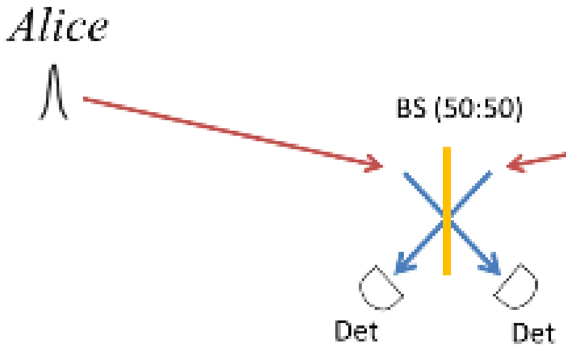
$$\{|\alpha\rangle, |-\alpha\rangle, |i\alpha\rangle, |-i\alpha\rangle\}$$

KT, H-K. Lo, C-H. F. Fung, B. Qi, Phys. Rev. A 85, 042307 (2012) (arXiv:1111.3413)

- ***The fidelity depends on the precision of PM as well as the intensity α***

$$\rho_X = \frac{1}{2}\left[|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right] \quad \rho_Y = \frac{1}{2}\left[|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right]$$

Phase encoding scheme for MDIQKD



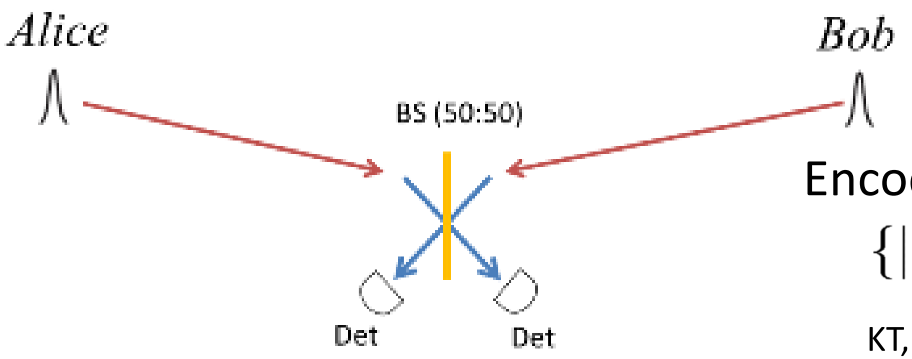
Encoding: phase non-randomized BB84 state

$$\{|\alpha\rangle, |-\alpha\rangle, |i\alpha\rangle, |-i\alpha\rangle\}$$

KT, H-K. Lo, C-H. F. Fung, B. Qi, Phys. Rev. A 85, 042307 (2012) (arXiv:1111.3413)

- **The fidelity depends on the precision of PM as well as the intensity α** $\rho_X = \frac{1}{2}[|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|]$ $\rho_Y = \frac{1}{2}[|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|]$
- **Essentially, this scheme is based on multiple modes**
  The signal states are linearly **independent*: Essentially multi mode*

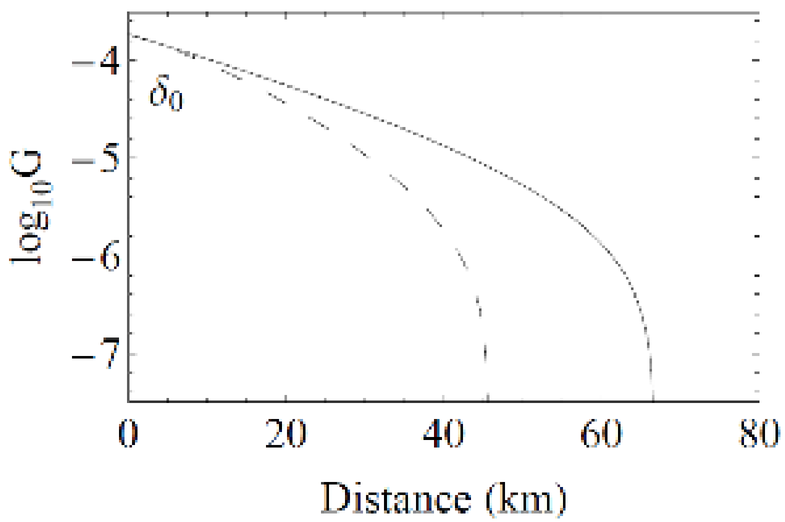
Phase encoding scheme for MDIQKD



Encoding: phase non-randomized BB84 state

$$\{|\alpha\rangle, |-\alpha\rangle, |i\alpha\rangle, |-i\alpha\rangle\}$$

KT, H-K. Lo, C-H. F. Fung, B. Qi, Phys. Rev. A 85, 042307 (2012)
(arXiv:1111.3413)



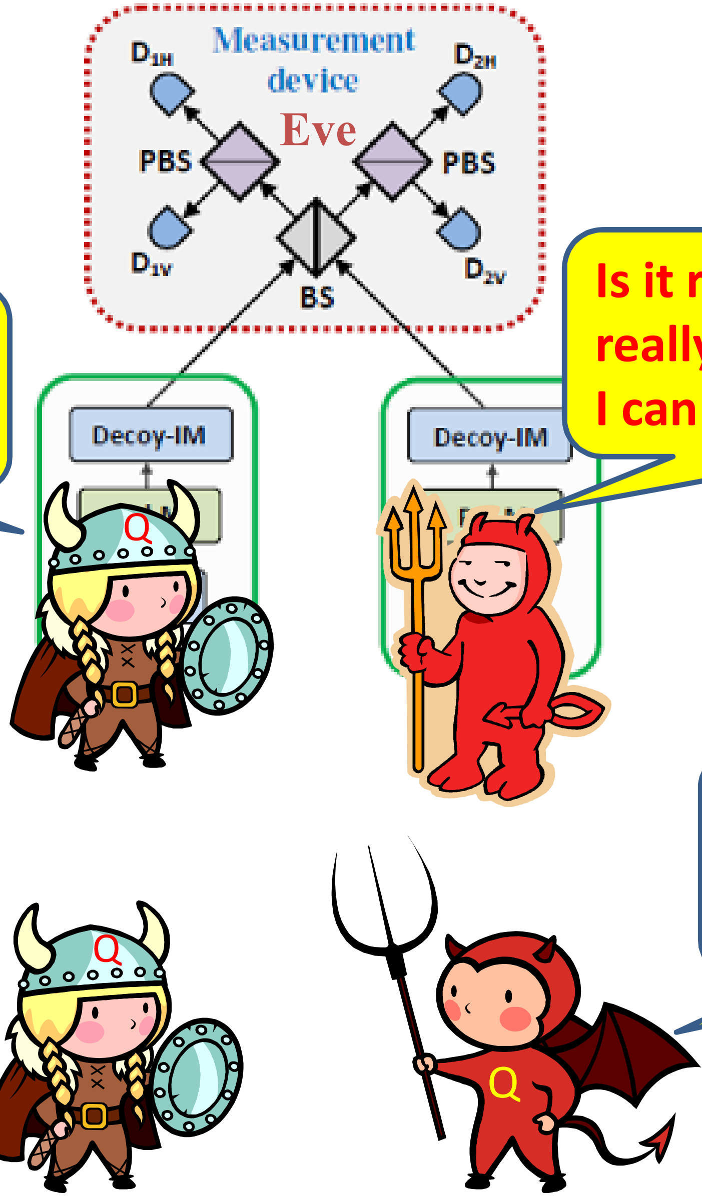
δ_0: 3.6deg (reasonable experimental value) of PM error

Even if we take into account the PM error, we can generate the key over 65km!

f(δx) = 1.22, eali = 0.0075, pdark = 1.0 × 10^−7, η = 0.15, ηch =0.21dB/km

M. Sasaki, M. Fujiwara, et al, Optics Express **19**, 10387 (2011)

Measurement device independent QKD (MDIQKD)



Well, we have MDI with phase non-randomized BB84

Is it really a qubit? Is it really phase randomized? I can still hack!

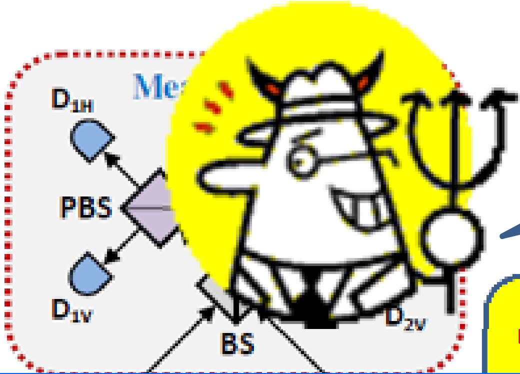
Look, we have the theory, and the phase modulation is OK

Hmm, I can exploit the imperfect state !! PM is not perfect!!

Measurement device independ

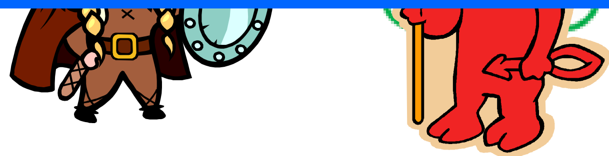
Measurement device independ

Oh, I've found another flaw!!



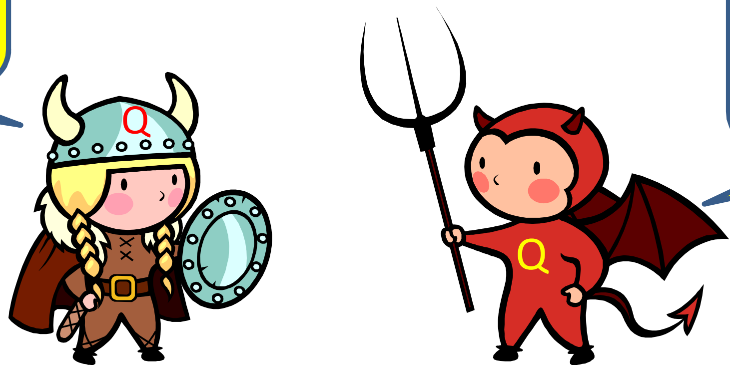
Is it really a qubit? Is it

Never ending, but by repeating this cycle we can have an almost perfectly secure QKD system



Look, we have the theory, and the phase modulation is OK

Hmm, I can exploit the imperfect state !! PM is not perfect!!



DPS QKD protocol

Outline of the talk

BB84:

- ✓ Maintenance-free long term demonstration of NEC's QKD system
- ✓ Issues of imperfections of the devices

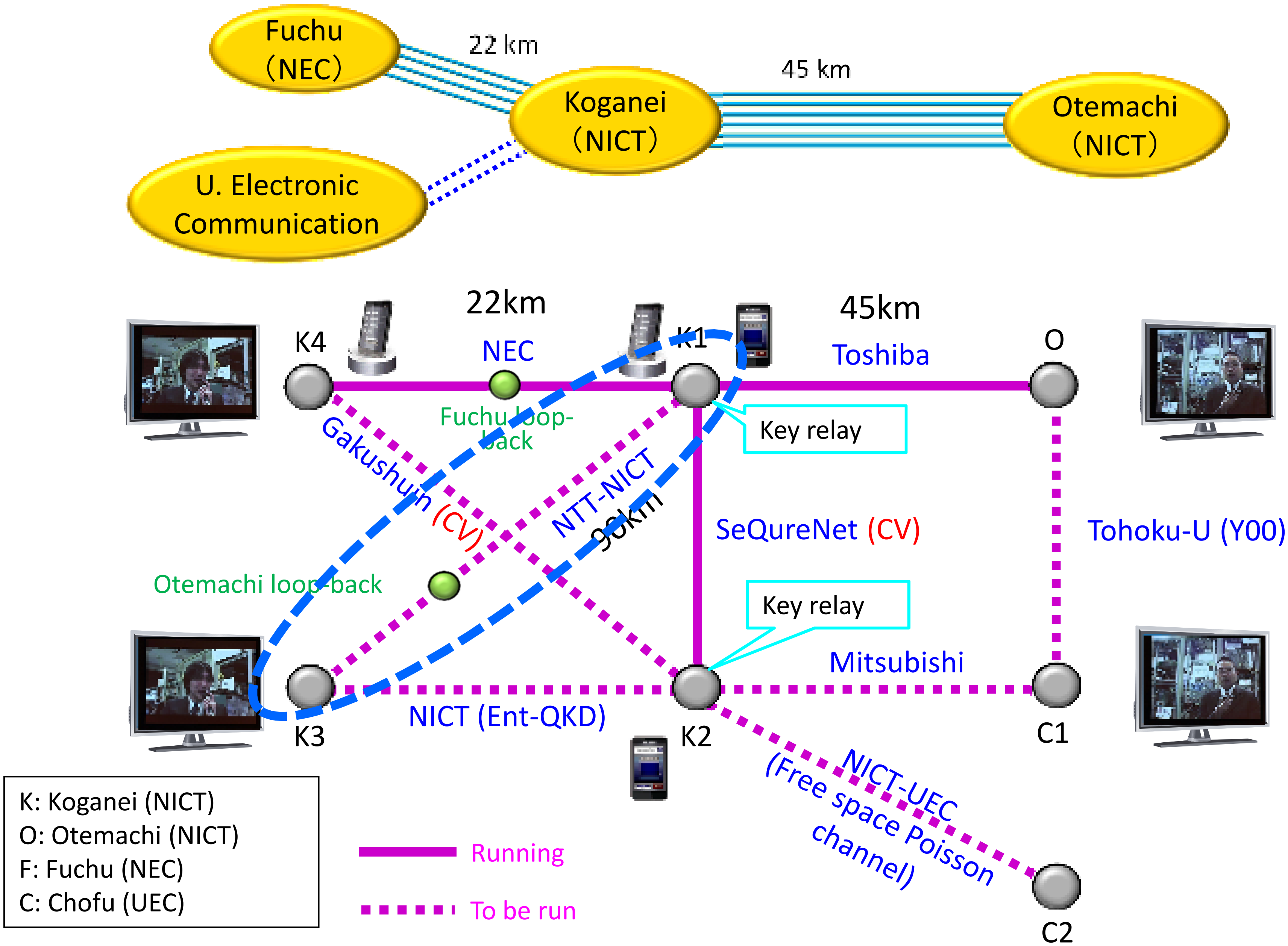
Differential phase shift QKD (DPS QKD):

- ✓ Field demonstration of NTT-NICT QKD system
- ✓ Unconditional security proof of DPS QKD

Continuous variable QKD (CV QKD):

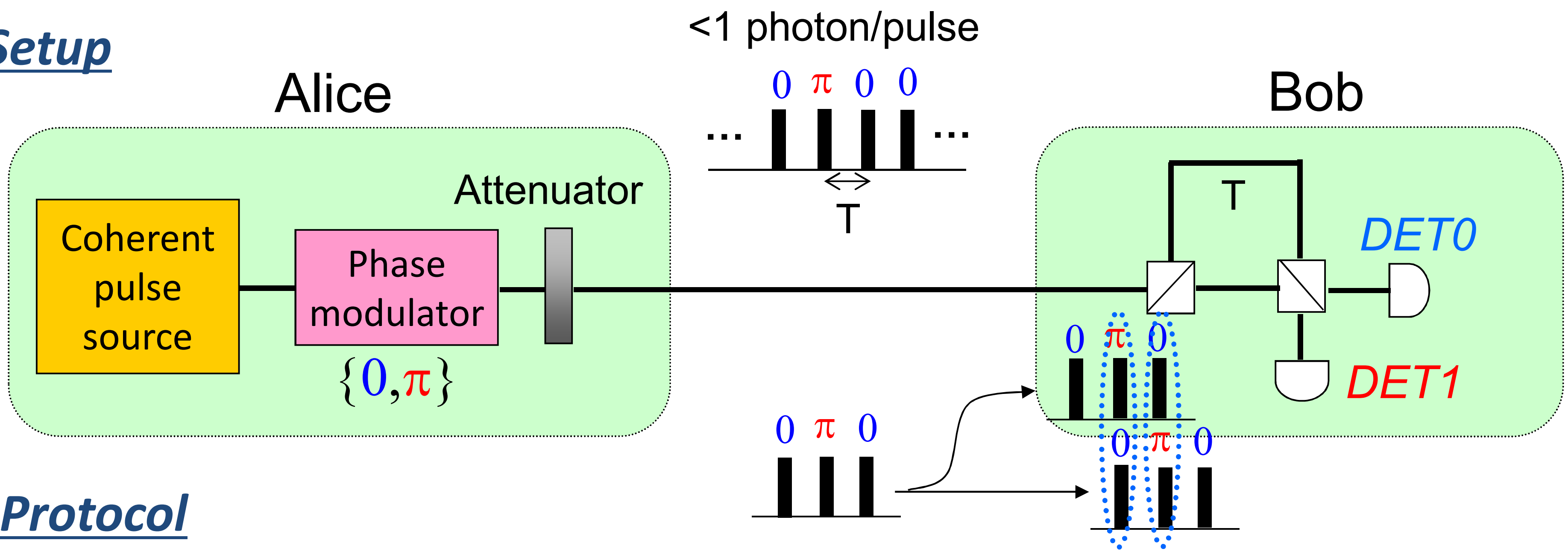
- ✓ Security proof against calibration attack on the local oscillator

Prototype of Tokyo QKD Network (2015)



Differential-phase-shift QKD (DPS QKD)

Setup



Protocol

Alice

Time	t1	t2	t3	t4	t5	t6	t7
Ph. Diff.	0	π	0	0	0	π	0

Time	t2	t4	t6
Sifted key	1	0	1

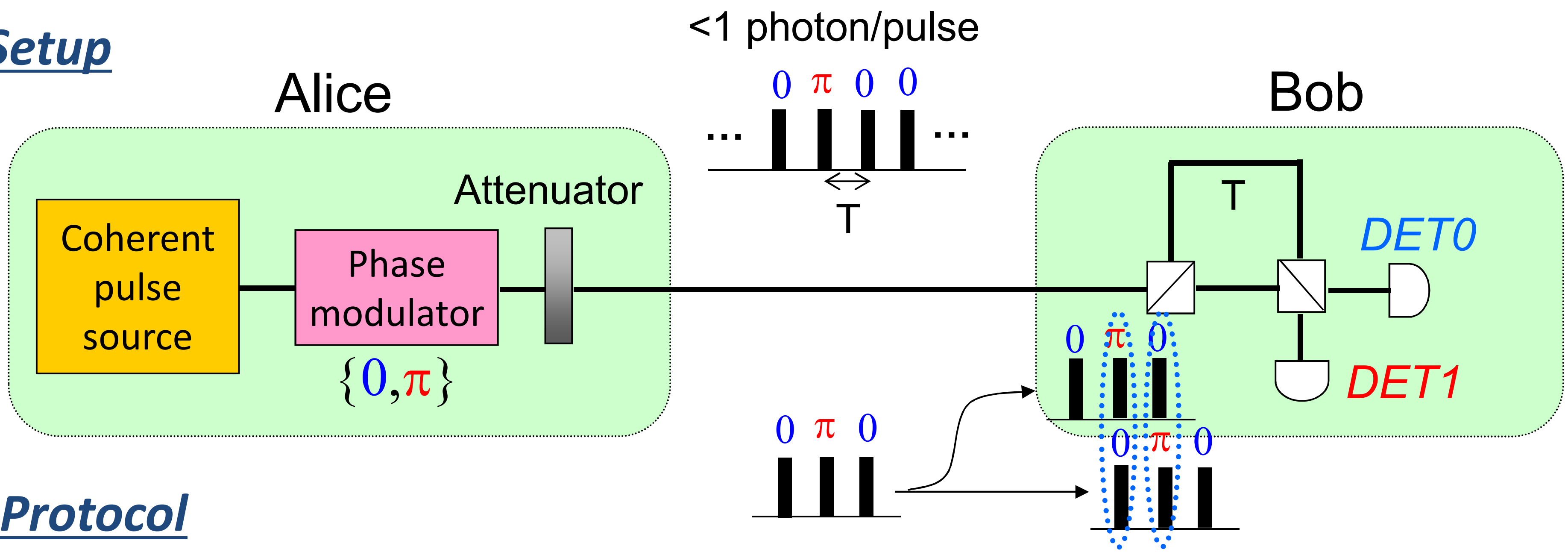
Bob

Time	t2	t4	t6
Det	Det1	Det0	Det1
Ph. Diff.	π	0	π
Sifted key	1	0	1

K. Inoue et al. Phys. Rev. A **68**, 022317 (2003).

DPS QKD

Setup

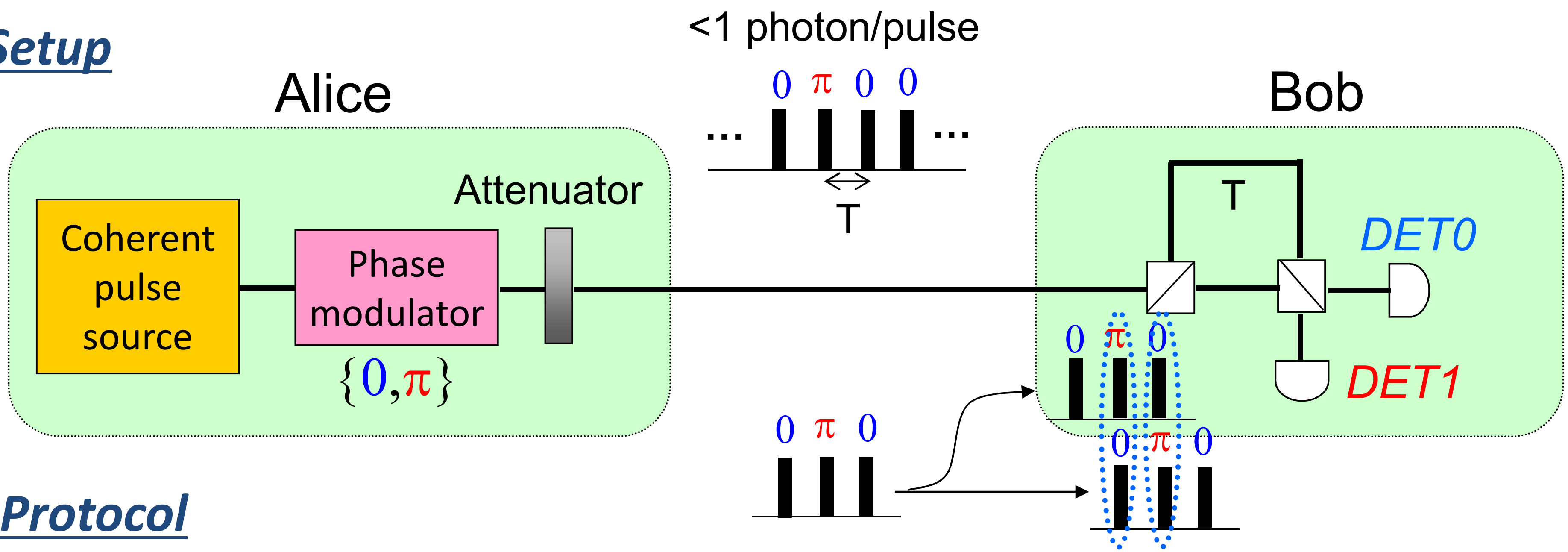


Protocol

- DPS QKD is simple to implement

DPS QKD

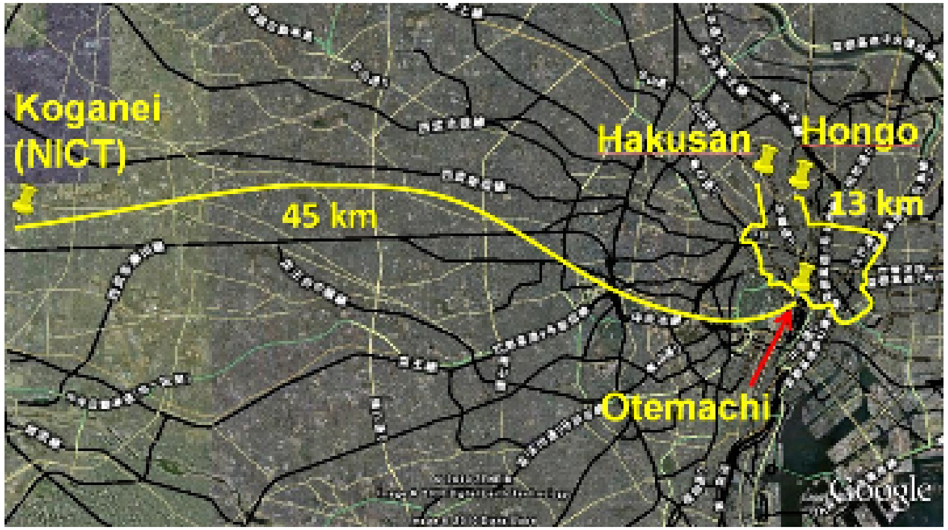
Setup

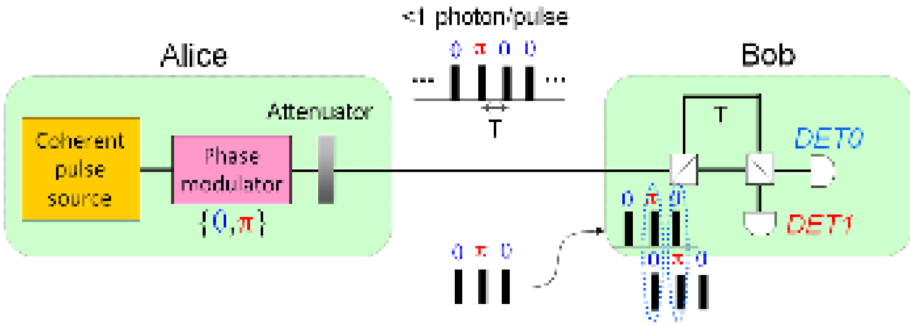


Protocol

- DPS QKD is simple to implement
- DPS QKD is expected to generate a key even from multi-photon emission by Alice (robust against PNS attack)
- The security only against particular attacks is known

Field demonstration of DPS QKD

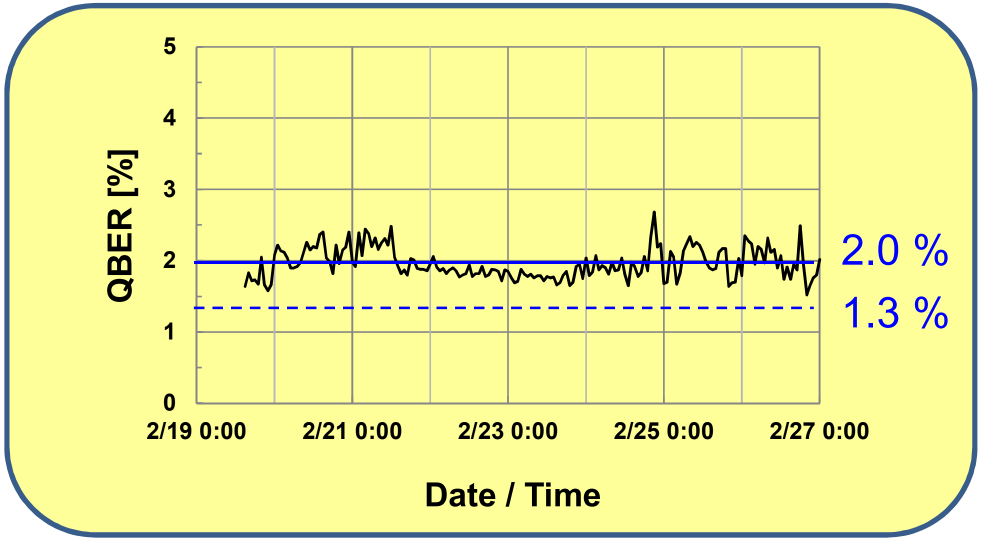




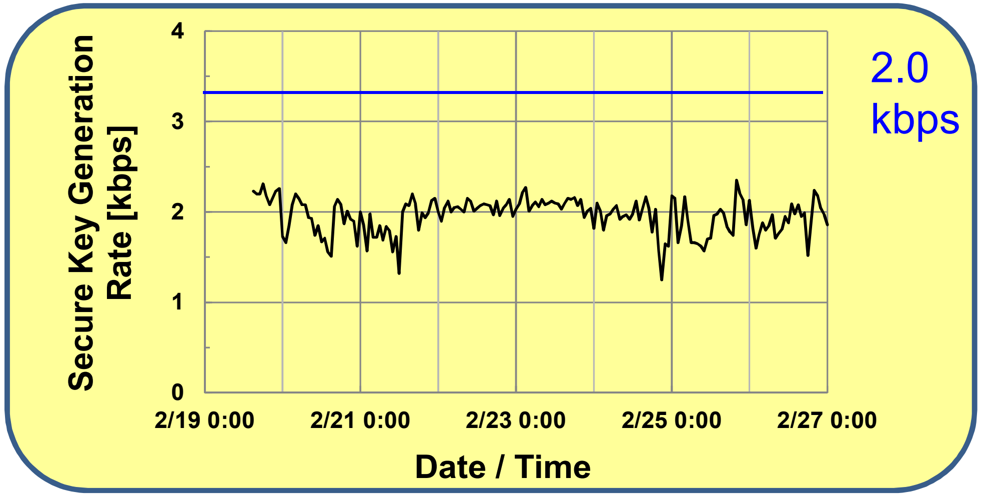
- 90-km loopback fiber link (26.5dB loss) between Koganei and Otemachi
- Overhead ratio: 50%
- Join work between NTT and NICT

Field demonstration of DPS QKD

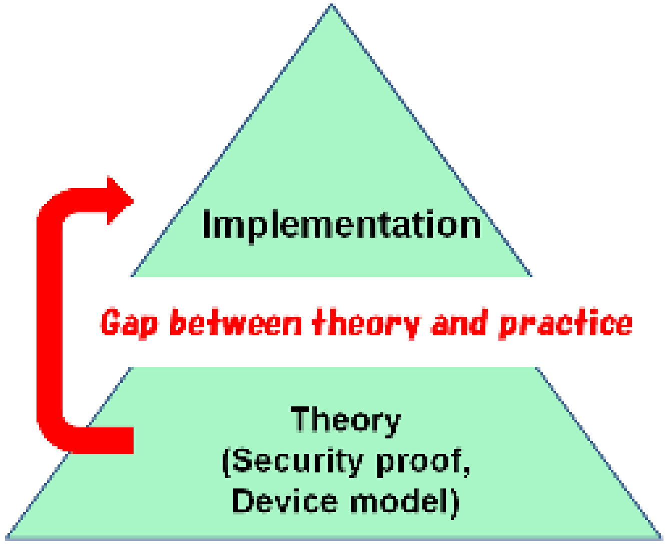
QBER

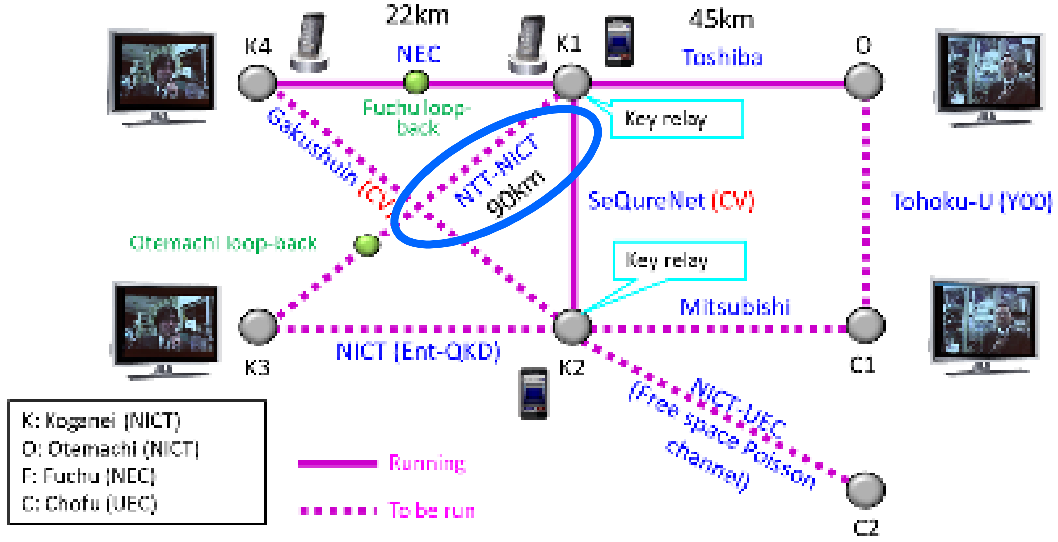


Secure key rate
(assuming individual attacks)



QBER～ 2%, Secure key rate～2 kbps, 7.5days



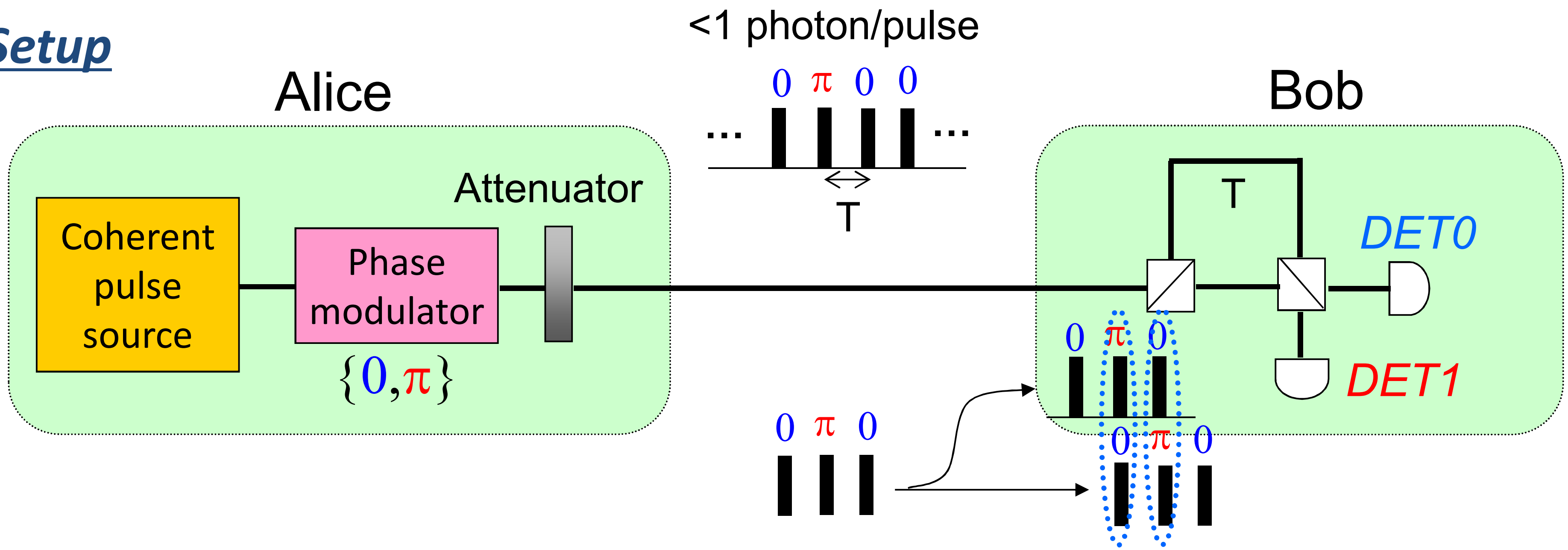


Protocol	Organization in charge of system	Status of the Theory
DPS QKD	NTT-NICT	・We need theory (Unconditionally security was ***not*** proven yet)
CV QKD	Gakushuin Univ SeQureNet	・We need theory (Imperfect local oscillator)
BB84	NEC, Toshiba, Mitsubishi	・Unconditionally secure ・The gap exists

Unconditional security of DPS

Why is it difficult to prove the security of DPS?

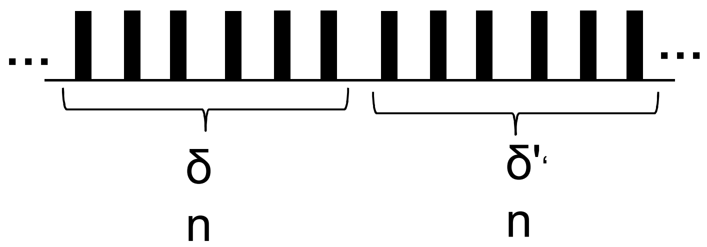
Setup



The information is encoded between signals and one cannot work only on each pulse separately like in BB84!!

Outline of the proof

1. Alice performs block-wise phase randomization



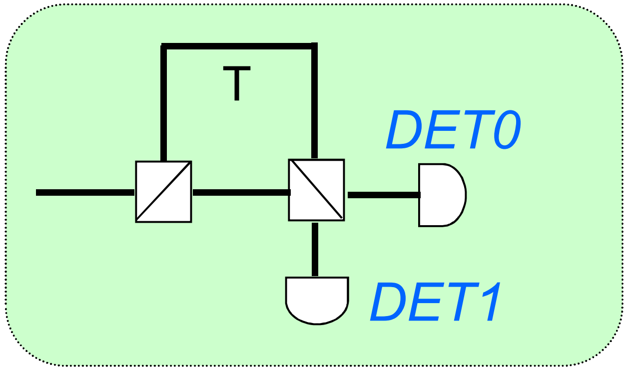
$0 \leqq \delta, \delta', \ldots < 2\pi$

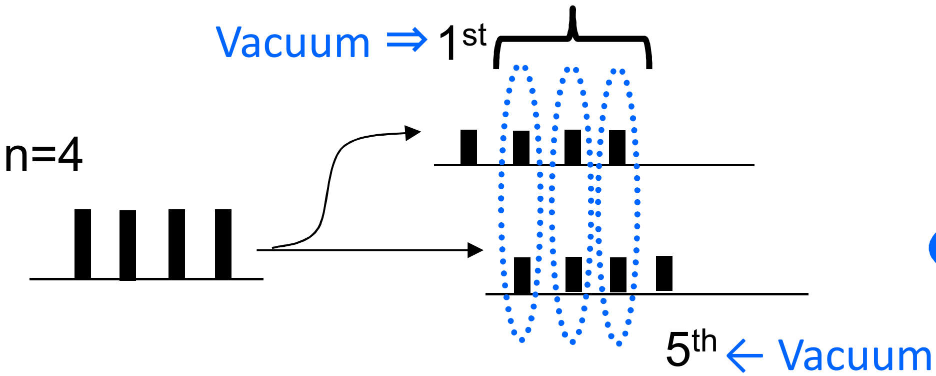
⇒ Work on each photon number space separately and combine them with the worst case scenario to maximize Eve's information (GLLP argument)

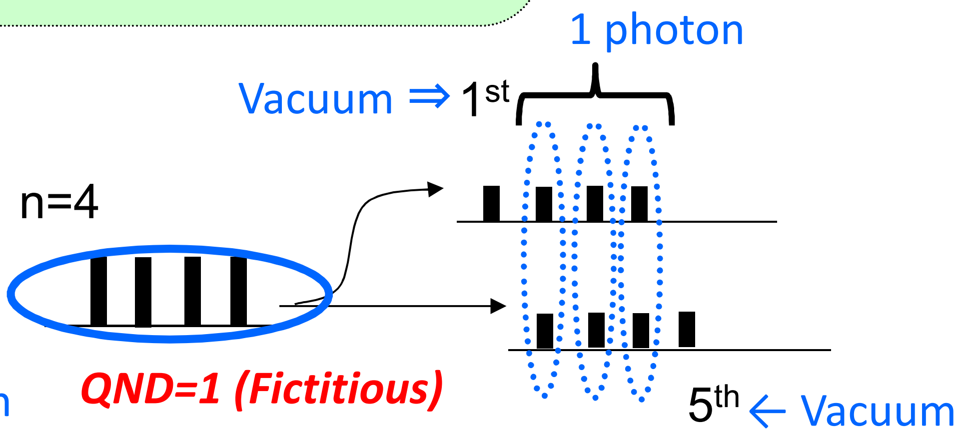
D. Gottesman, H.-K. Lo, N. Luetkenhaus, and J. Preskill, Quantum Information and Computation 5, 325 (2004).

Outline of the proof

2. Bob's detector is photon number resolving (among the vacuum, a single-photon, and multiple photons)



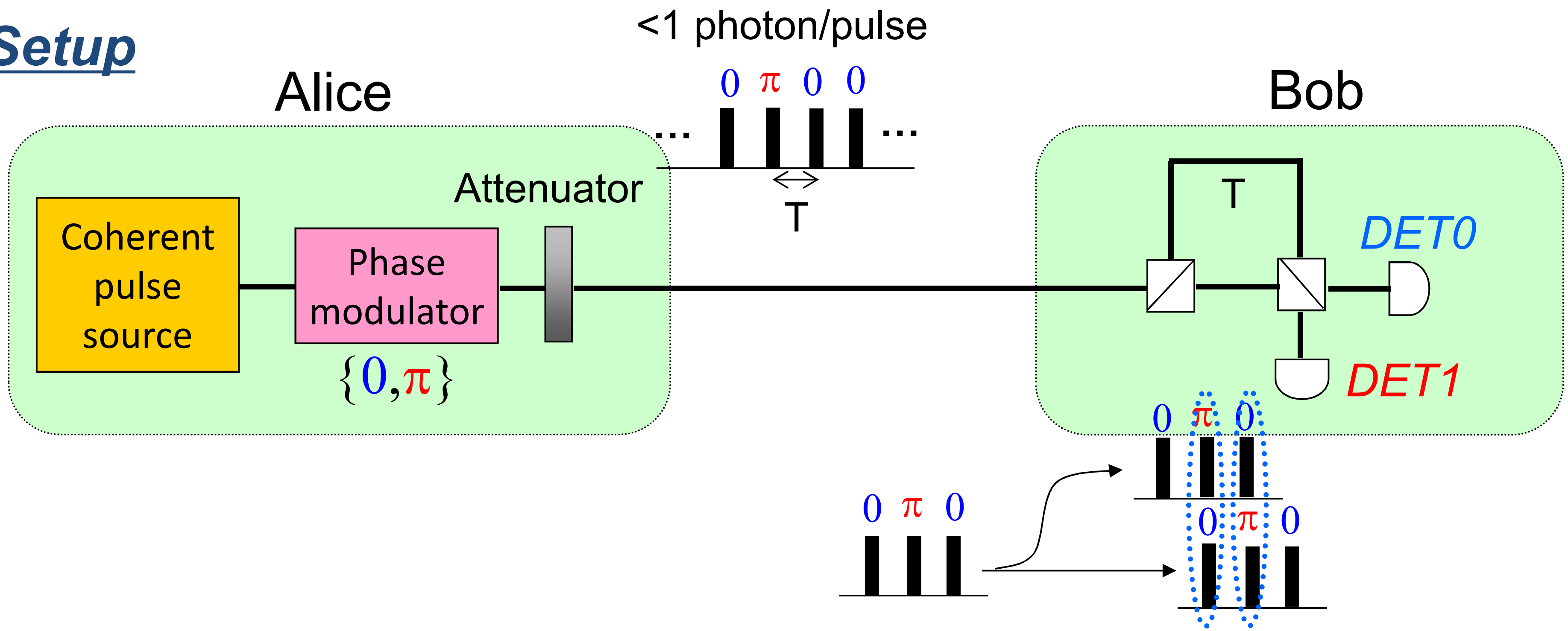




Bob's basis:

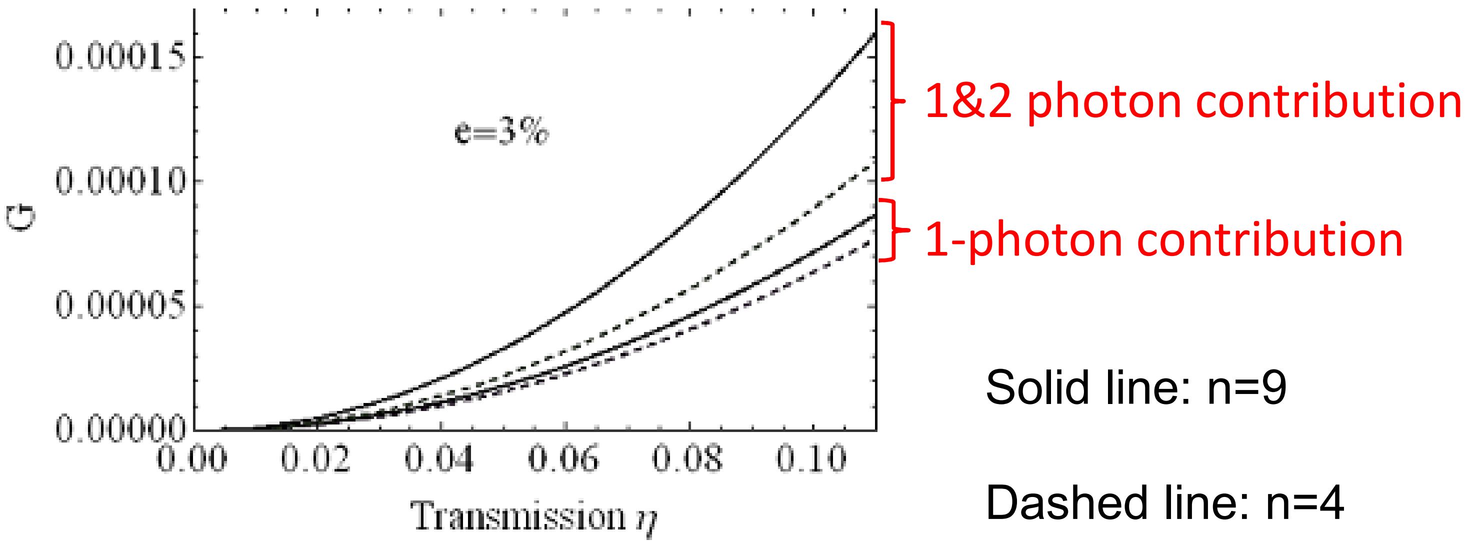
$$\{|\vec{b}\rangle\}:\{|1000\rangle, |0100\rangle, |0010\rangle, |0001\rangle\}$$

Setup



3. We employ the symmetry of the protocol to reduce the size of the density matrix shared by Alice and Bob, i.e., invariance under joint application of random phase flip

Key distillation rate



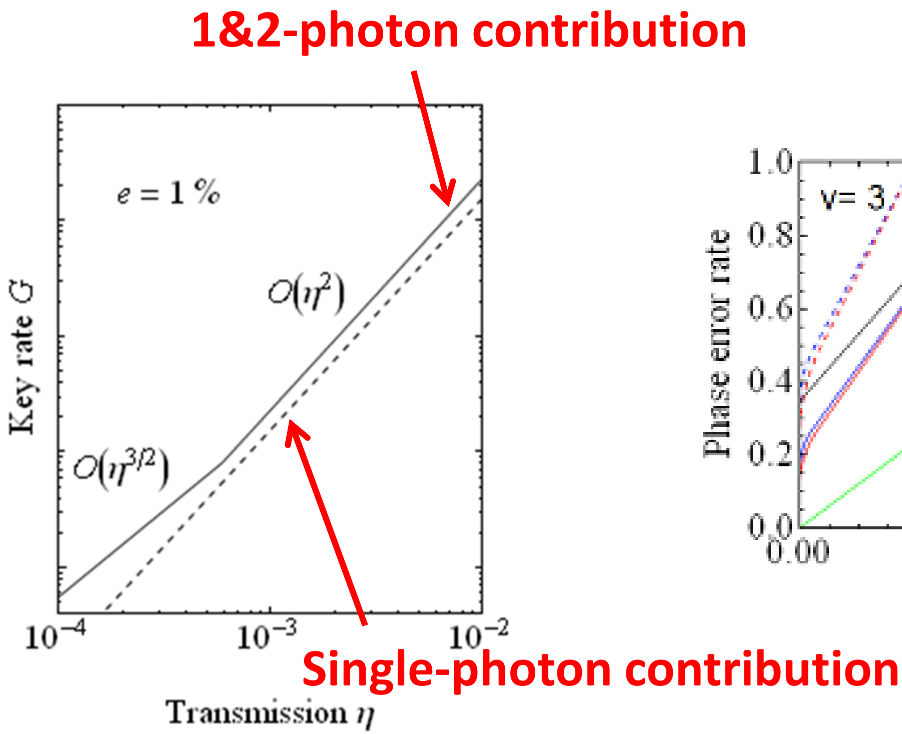
Solid line: n=9

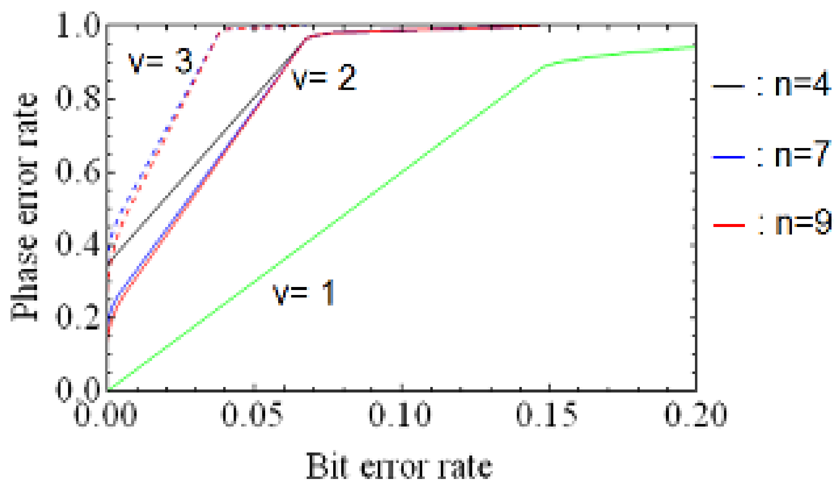
Dashed line: n=4

Optimal mean photon number～ 10^{-3}-10^{-2}

KT, M. Koashi, and G. Kato, arXiv:1208.1995

Robustness against PNS attacks for low-bit error rate regime





Low QBER & low η ⇒ key generation solely from 2-photon part is possible

✓ DPS is robust against PNS attacks at least such a regime

KT, M. Koashi, and G. Kato, arXiv:1208.1995

Outline of the talk

BB84:

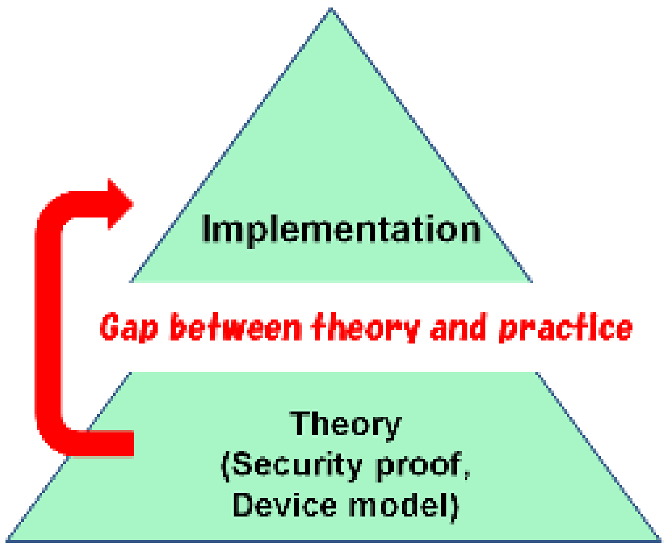
- ✓ Maintenance-free long term demonstration of NEC's QKD system
- ✓ Issues of imperfections of the devices

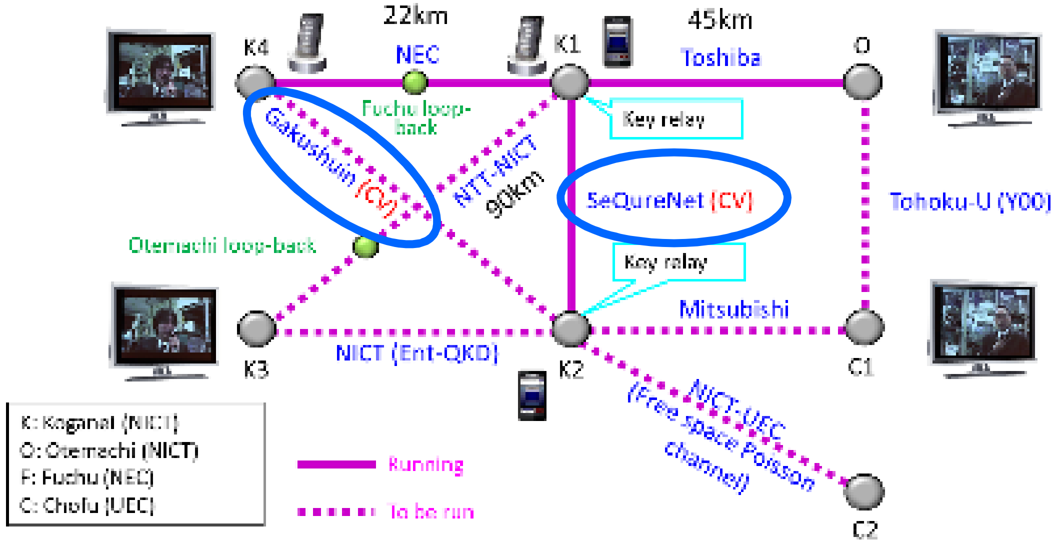
Differential phase shift QKD (DPS QKD):

- ✓ Field demonstration of NTT-NICT QKD system
- ✓ Unconditional security proof of DPS-QKD

Continuous variable QKD (CV QKD):

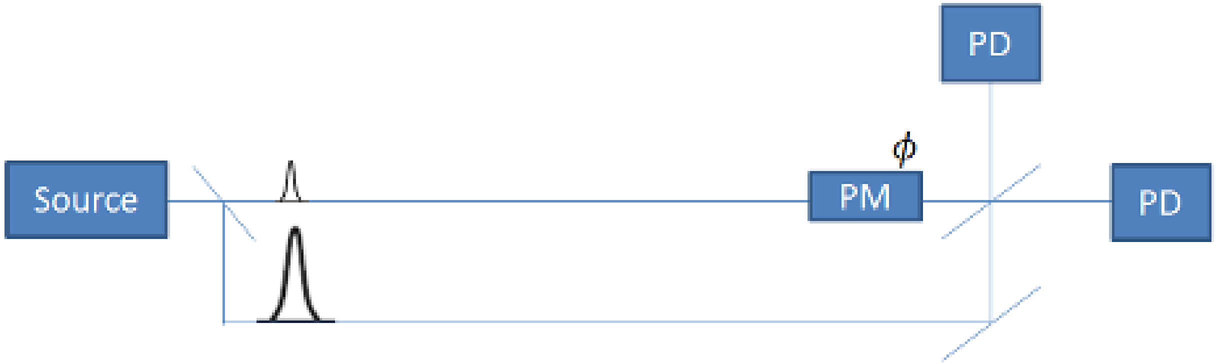
- ✓ Security proof against calibration attack on the local oscillator



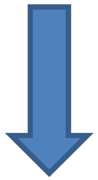


Protocol	Organization in charge of system	Status of the Theory
DPS QKD	NTT-NICT	・We need theory (Unconditionally security was ***not*** proven yet)
CV QKD	Gakushuin Univ SeQureNet	・We need theory (Imperfect local oscillator)
BB84	NEC, Toshiba, Mitsubishi	・Unconditionally secure ・The gap exists

Problem of CV-QKD (Imperfect LO)

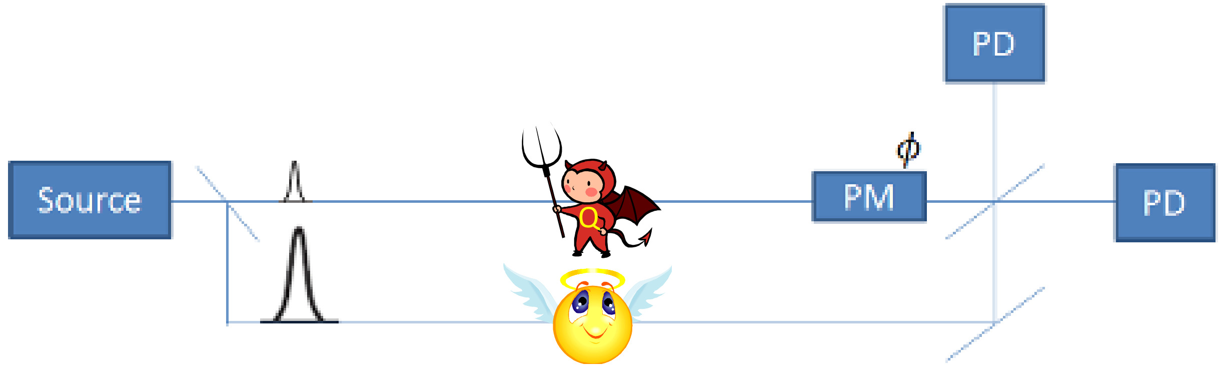


Almost all the proofs* for CV QKD assume: Perfect Homodyne or Heterodyne measurement



*Exception: Fabian Furrer, Torsten Franz, et.al., arXiv:1112.2179 (Entanglement based CV-QKD)

Problem of CV-QKD (Imperfect LO)

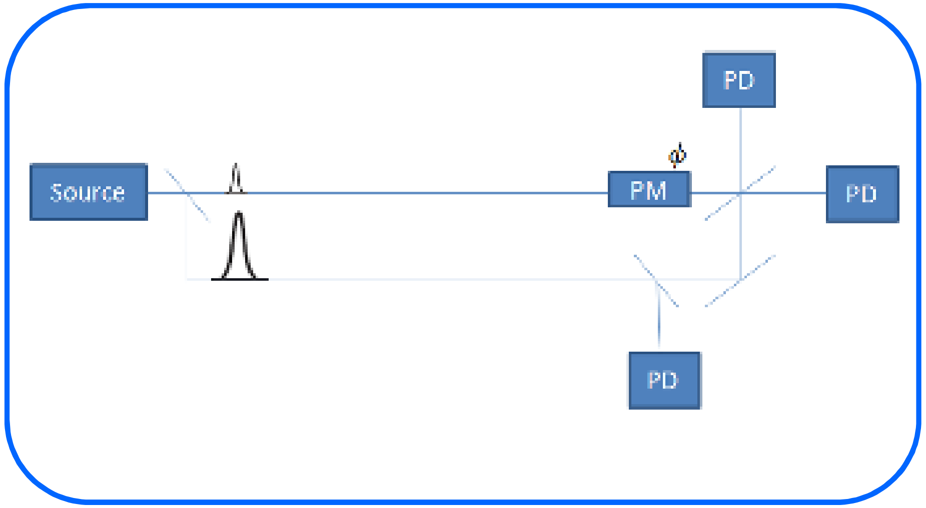


Almost all the proofs* for CV QKD assume: Perfect Homodyne or Heterodyne measurement

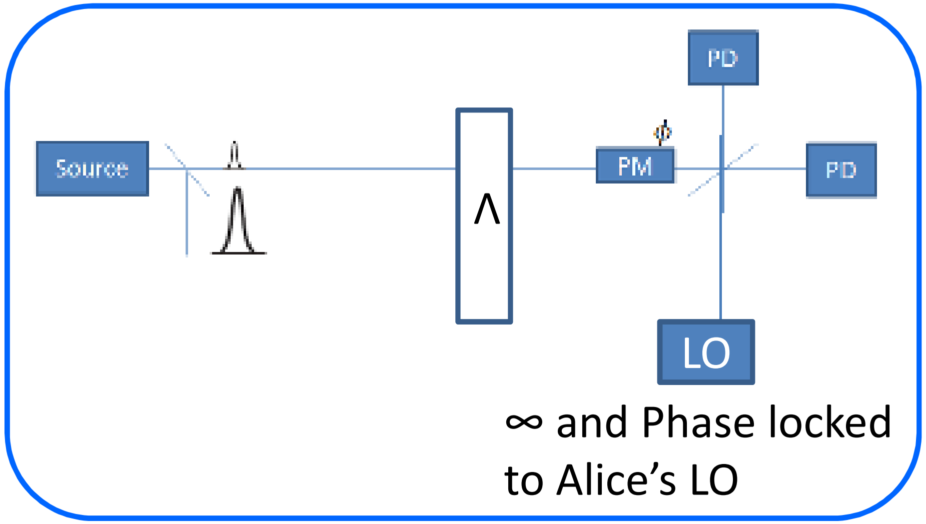
- Eve manipulates only the signal light
  ⇒ *The proofs are not unconditional*
- The intensity of the local oscillator has to be INFINITE
  ⇒ *Impossible to accomplish*

*Exception: Fabian Furrer, Torsten Franz, et.al., arXiv:1112.2179 (Entanglement based CV-QKD)

Our result



Actual protocol



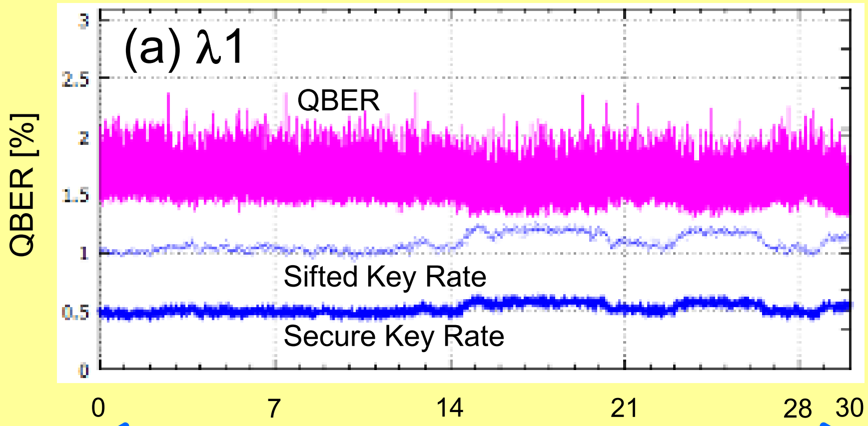
Virtual protocol

We have accommodated arbitrary attacks to LO and imperfections of LO into the security proofs of CV QKD with direct reconciliation & without post-selection by Bob

Visit our poster: "Security of CV-QKD with transmitted local oscillator"
Go Kato, KT, Koji Azuma, and Masaki Owari

BB84

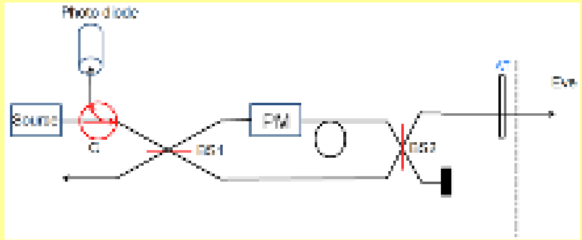
NEC's WDM QKD system (Maintenance-free field test)



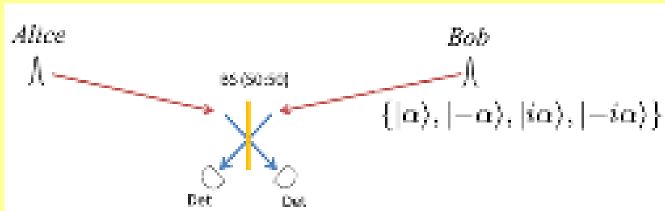
30 days

- Flexible optical system and hardware
- 22 (km) 13dB loss
- Overhead ratio: 95%
- QBER～ 1.8%
- Secure key rate～100 kbps/(wave length)

Countermeasure of side-channels



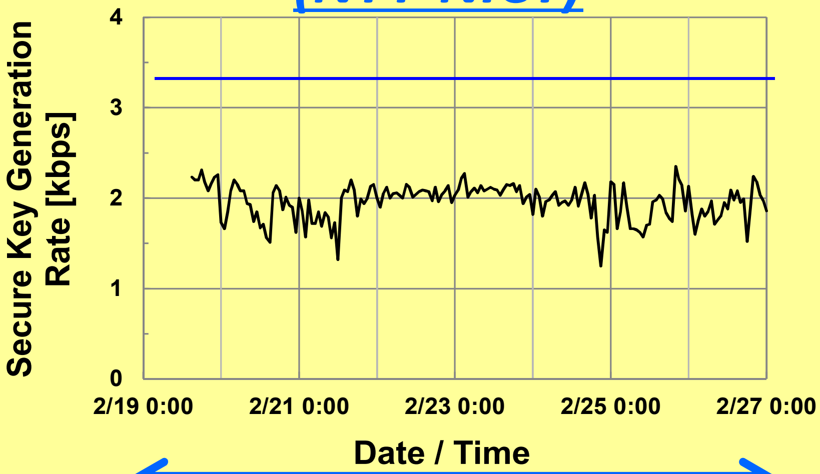
- PM with real time monitoring & interferometer-independent accuracy



- Phase encoding MDIQKD essentially multi mode MDIQKD

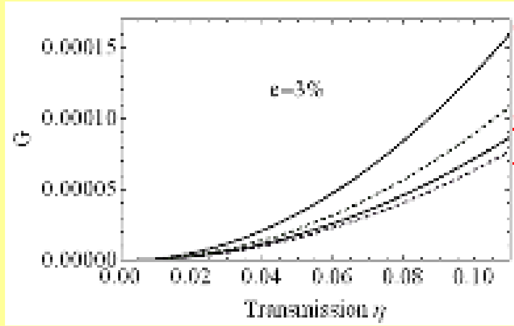
DPS QKD

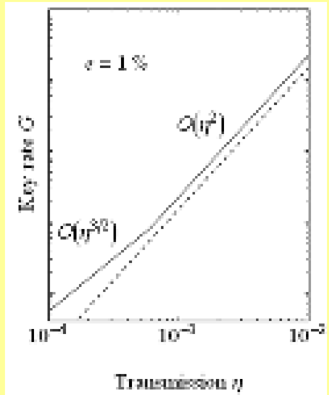
Field demonstration (NTT-NICT)



- 90 (km) 26.5dB loss
- Overhead ratio: 50%
- QBER～ 2%
- Secure key rate～2 kbps

Security proof

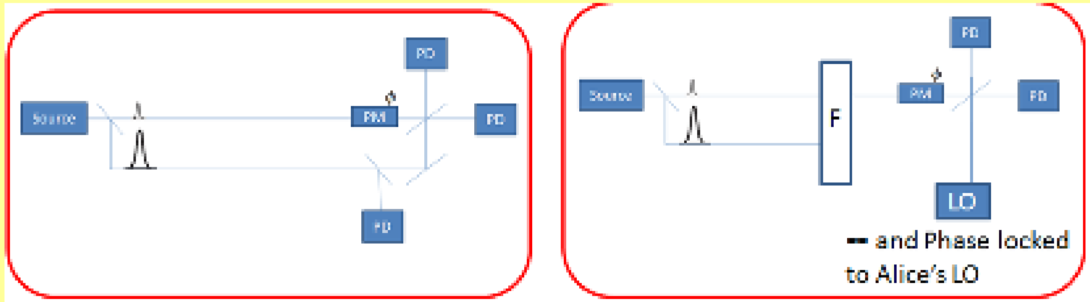




- Unconditional security of block-wise phase randomized DPS QKD
- Robustness of DPS against PNS attack

Gaussian modulated CV QKD

Security proof



Actual protocol *Virtual protocol*

We have accommodated the calibration attack to LO into the security proofs of Gaussian CV-QKD

Visit our poster: "Security of CV-QKD with transmitted local oscillator"
Go Kato, KT, Koji Azuma, and Masaki Owari

Organizations and people of QKD theory team

Hokkaido univ

Akihisa Tomita

Mitsubishi electric

Toyohiro Tsurumaru
Wataru Matsumoto
Takeshi Asai

Nagoya univ

Masahito Hayashi (NUS)

Tokyo inst. tech

Ryutaroh Matsumoto
Kenta Kasai

NTT

Koji Azuma
Go Kato
KT

Collaborators:
Hoi-Kwong Lo (UofT)
Masato Koashi (Tokyo Univ)
Nobuyuki Imoto (Osaka Univ)

Towards implementation of secure and reliable QKD system!

We thank the support from NICT