Optical Fiber Communication Conference 2022
Tu3I Quantum Communications

Introduction to Continuous Variable Quantum Key Distribution

Takuya Hirano
Gakushuin University

In this talk, we will review the present status of continuous-variable quantum key distribution, including optical configuration and security analysis, and would like to discuss future prospects for integration with coherent optical communications.

Supported by CSTI SIP "Photonics and Quantum Technology for Society 5.0" (Funding agency: QST), JSPS KAKENHI under Grant Number 18H05237, and MIC Project "R&D for building a global quantum cryptography communication network"

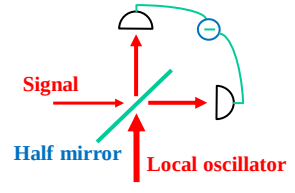
1

Optical Fiber Communication Conference 2022

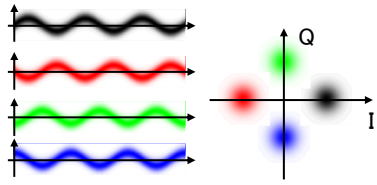
Continuous-Variable QKD : faint light is detected by homodyne detection

Photon counting	particle nature	custom-build for QKD	Require cooling	expensive	sensitive to stray light
Homodyne detection	wave nature	commercially available	room-temperature	low cost and small	insensitive to stray light

Schematic of homodyne detection



homodyne detection itself works as an efficient filter



Quantum noise due to *uncertainty relation*

⇩

Limitation on signal discrimination

Advantageous in
practical implementation,
multiplexing with optical communication

CV-QKD and QAM optical transmission

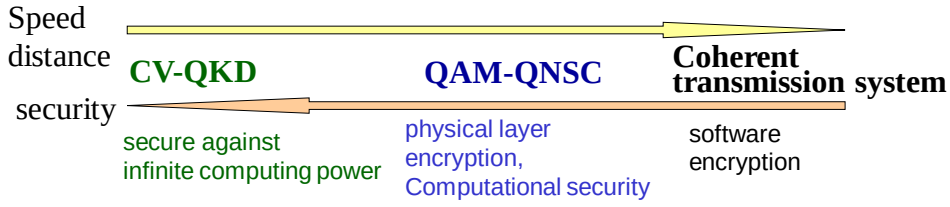
Similarities

- Coherent states modulated in phase-space are sent
- Homodyne detection is utilized to readout quadrature-phase amplitudes

➡ A coherent optical communication system operating in quantum noise limit is ready for CV QKD.

Development of QKD and optical secure transmission technology that can be seamlessly integrated with coherent optical communications

→ will offer diverse functions ranging from unconditionally secure communications to high-speed and high-secure data transmission in a unified way.



学習院大学 GAKUSHUIN UNIVERSITY Optical Fiber Communication Conference 2022

CV-QKD and QAM optical transmission

Differences

- Transmitted signal light of CV-QKD should be very weak.
- Quantum noise limited detection is necessary for CV-QKD to be secure.

➡ CV-QKD is technically more difficult.

Security aspects: DV-QKD vs. CV-QKD

Simple picture

In DV-QKD, a single photon is sent by Alice, and a single photon cannot be divided, then if Bob receives a photon, no other person should receive the photon and it is expected that only Bob knows the information.

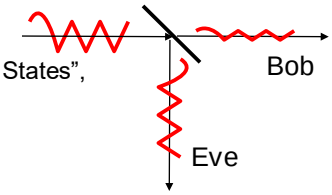
In CV-QKD, the amplitude of the electromagnetic field is measured, and the wave amplitude can be divided, then other person may receive the information.

➡ CV-QKD is more difficult to understand its security.

CV-QKD and 3-dB loss limit

3dB loss limit

"Continuous Variable Quantum Cryptography Using Coherent States", F. Grosshans and P. Grangier, PRL **88** ,057902 (2002).



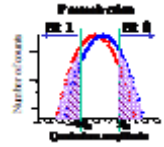
Recipe for beating 3dB-loss-limit

Post-selection

"Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit", Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. 89, 167901 (2002).

"Quantum cryptography using balanced homodyne detection," T. Hirano, T. Konishi, R. Namiki, quant-ph/0008037; Extened abstract for EQIS 2001.

"Security of quantum cryptography using balanced homodyne detection", R. Namiki, T. Hirano, Phys. Rev. A, vol. 67, no.2, 022308-1-7 (2003).



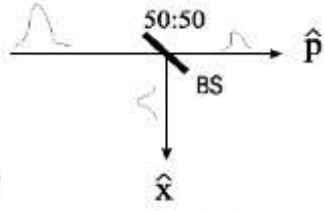
Reverse reconciliation

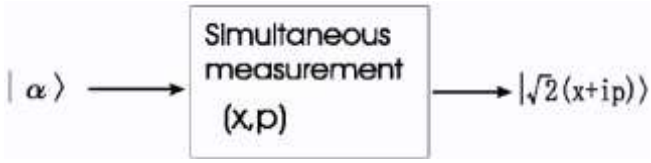
"Quantum key distribution using gaussian-modulated coherent states" , F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, Ph. Grangier, Nature **421**, 238 (2003).

Security of CV QKD: loss limit caused by excess noise (1)

R. Namiki and TH, Phys. Rev. Lett., vol. 92, 117901 (2004).

1. Eve performs a simultaneous measurement on both quadrature amplitudes (x,p) using a beam splitter.
2. Eve resends a coherent state $|\sqrt{2}(x+ip)\rangle$ to Bob.



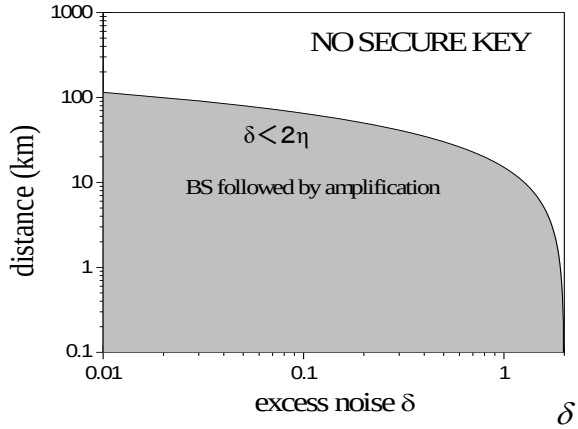


No secret key because Eve knows the state that Bob measures.
(entanglement breaking)

Applicable to any protocol using coherent states and homodyne detection

Security of CV QKD: loss limit caused by excess noise (2)

R. Namiki and TH, Phys. Rev. Lett., vol. 92, 117901 (2004).



Define excess noise δ:

$$\delta = \frac{(\Delta x_{\text{obs}})^2}{(\Delta x)^2} - 1$$

Intercept & resend attack increases excess noise:

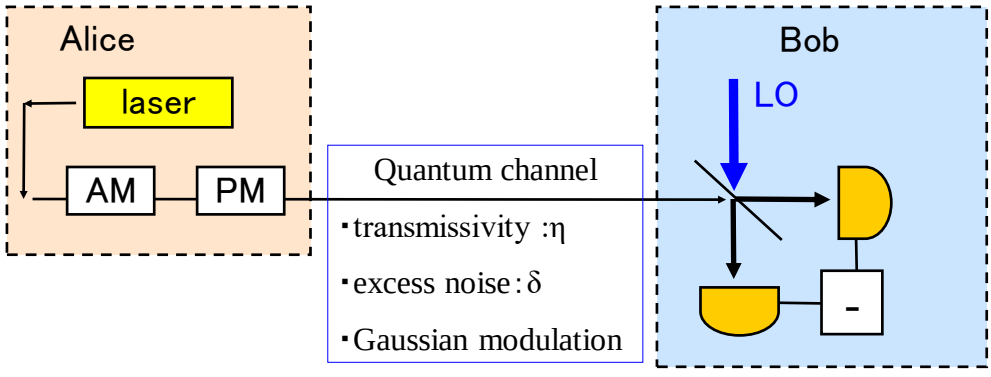
$\delta = 2.$

Excess noise decreases by loss:

$\delta = 2\eta$, η:transmissivity.

$\delta < 2\eta$ is a necessary condition.

Entangling cloner attack (1)

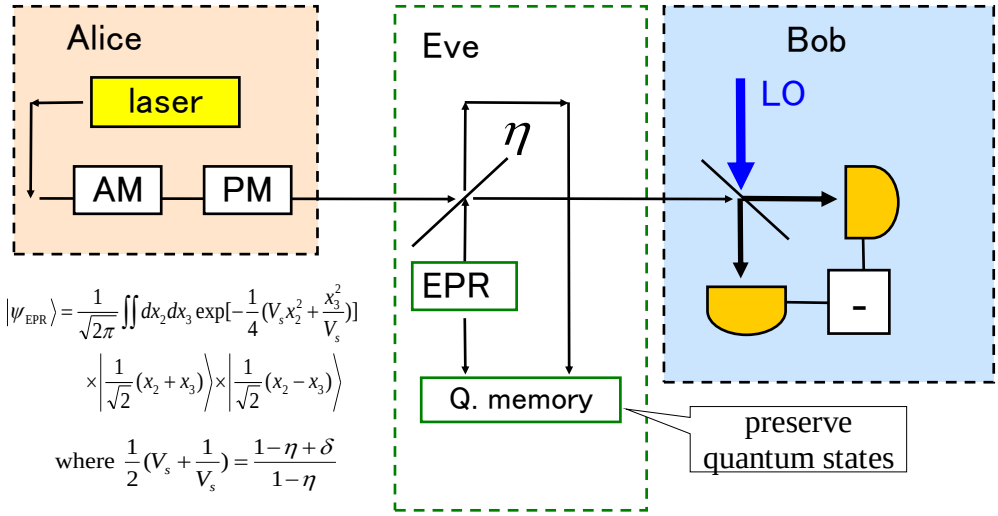


Entangling cloner attack is optimum collective attack

M. Heid and N. Lütkenhaus, PRA **76**, 022313 (2007)

9

Entangling cloner attack (2)

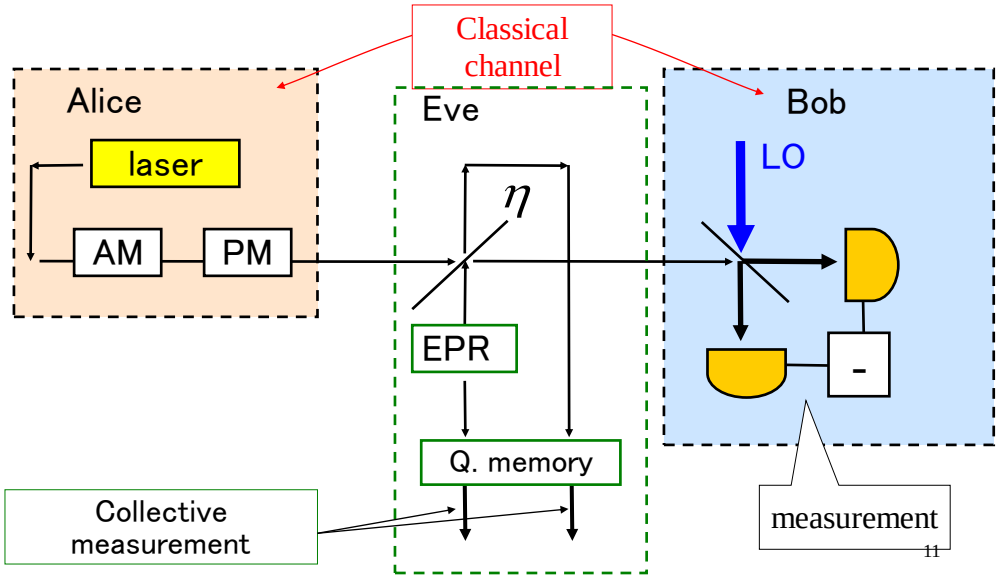


$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2\pi}} \iint dx_2 dx_3 \exp[-\frac{1}{4}(V_s x_2^2 + \frac{x_3^2}{V_s})] \times \left|\frac{1}{\sqrt{2}}(x_2 + x_3)\right\rangle \times \left|\frac{1}{\sqrt{2}}(x_2 - x_3)\right\rangle$$

where $\frac{1}{2}(V_s + \frac{1}{V_s}) = \frac{1-\eta+\delta}{1-\eta}$

10

Entangling cloner attack (3)



11

Secret key rate when the detection process is inaccessible to eavesdroppers

R. Namiki, A. Kitagawa, and TH, Phys. Rev. A 98, 042319 (2018).

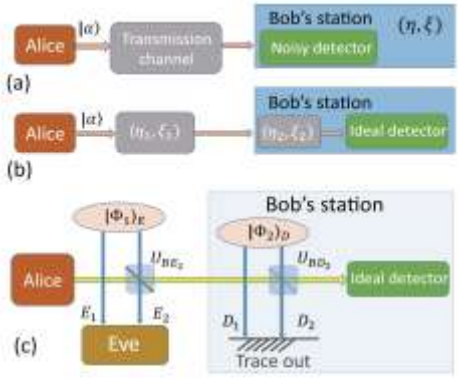
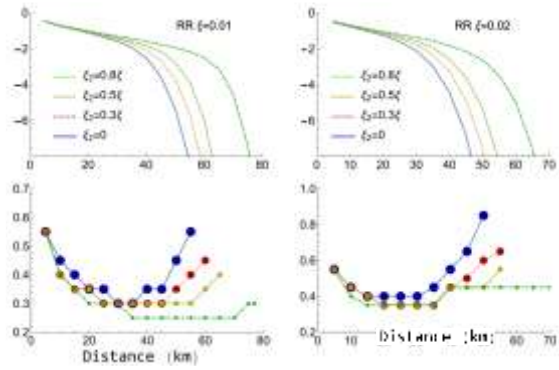


FIG. 1. (a) Alice sends a coherent state $|\alpha\rangle$ through a lossy and noisy channel. Bob observes quadrature with the total transmission η and the total excess noise ξ. (b) The transmission channel is modeled by a lossy and noisy Gaussian channel with the transmission η_1 and the excess noise ξ_1. Bob's detector is modeled by another lossy and noisy Gaussian channel with the transmission η_2 and the excess noise ξ_2 followed by an ideal homodyne detector. (c) The action of Gaussian channels (η_i, ξ_i) with $i = 1, 2$ can be described by beam-splitter unitaries U_{BE_i} and U_{BD_i} coupling to two-mode squeezed states $|\Phi_1\rangle_{E}$ and $|\Phi_2\rangle_{D}$.



Key rate for the reverse-reconciliation (RR) scheme as functions of distance with the total excess noise $\xi = \{0.01, 0.02\}$.
The photon number α^2 is chosen to maximize the key rate with 0.05 steps. The amount of the detector's excess noise ξ_2 is set to 0, 30%, 50%, and 80% of the total excess noise ξ.

12

ARTICLE

https://doi.org/10.1038/s41467-020-19916-1 OPEN

Check for updates

Finite-size security of continuous-variable quantum key distribution with digital signal processing

Takaya Matsuura[1], Kento Maeda[1], Toshihiko Sasaki[1,2] & Masato Koashi[1,2]✉

In comparison to conventional discrete-variable (DV) quantum key distribution (QKD), continuous-variable (CV) QKD with homodyne/heterodyne measurements has distinct advantages of lower-cost implementation and affinity to wavelength division multiplexing. On the other hand, its continuous nature makes it harder to accommodate to practical signal processing, which is always discretized, leading to lack of complete security proofs so far. Here we propose a tight and robust method of estimating fidelity of an optical pulse to a coherent state via heterodyne measurements. We then construct a binary phase modulated CV-QKD protocol and prove its security in the finite-key-size regime against general coherent attacks, based on proof techniques of DV QKD. Such a complete security proof is indispensable for exploiting the benefits of CV QKD.

13

https://doi.org/10.1038/s41467-020-19916-1 OPEN

Finite-size security of continuous-variable quantum key distribution with digital signal processing

Takaya Matsuura[1], Kento Maeda[1], Toshihiko Sasaki[1,2] & Masato Koashi[1,2]

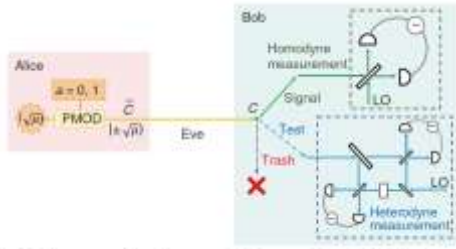
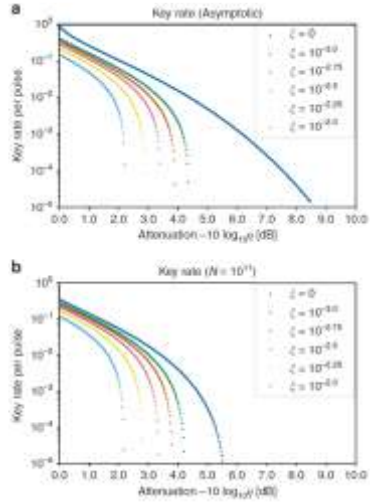


Fig. 2 The proposed continuous-variable quantum key distribution protocol. Alice generates a random bit $a \in \{0, 1\}$ and sends a coherent state with amplitude $(-1)^a\sqrt{\mu}$. Bob chooses one of the three measurements based on the predetermined probability. In the signal round, Bob performs a homodyne measurement on the received optical pulse and obtains an outcome $\hat{x}$. In the test round, Bob performs a heterodyne measurement on the received optical pulse and obtains an outcome $\hat{\alpha}$. In the trash round, he produces no outcome.



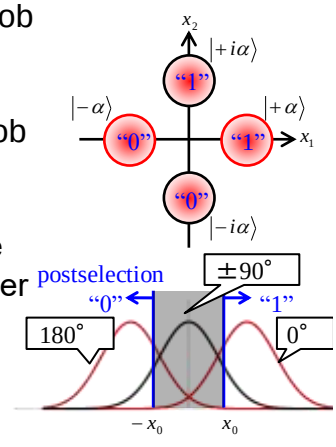
14

CV-QKD system of Gakushuin Univ.

TH *et al*. Phy. Rev. A 68, 042331 (2003).

Protocol: 4 states + post-selection

1. Alice randomly sends one of the 4 states to Bob
2. Bob randomly performs I- or Q-measurement
3. Alice announces which state she sent, and Bob announces which measurement he performed
5. Alice reconciles her bits with Bob's bits on the basis of Bob's ones (Reverse reconciliation). After that, they make a privacy amplification



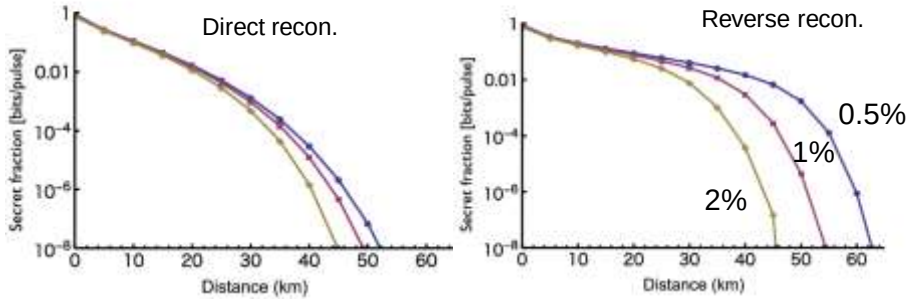
Advantage: simpler implementation and post-processing

15

Secret fraction of four-states postselection protocol against entangling cloner attack

ξ=0.5%, 1%, 2%

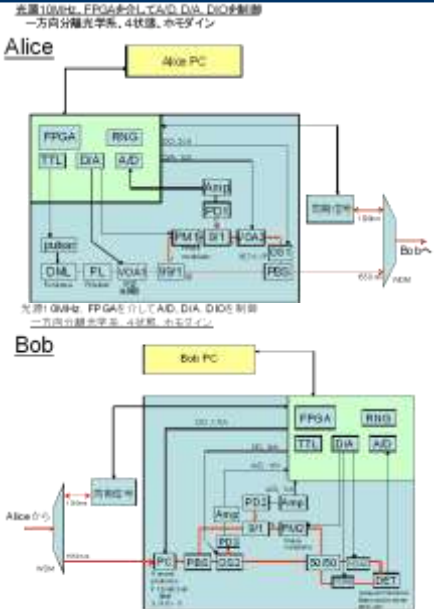
Channel loss：0.2dB/km, α value is optimized.



- Reverse reconciliation gives higher key rate.
- Excess noise should be smaller for a longer distance.

16

Compact and low cost CV-QKD system

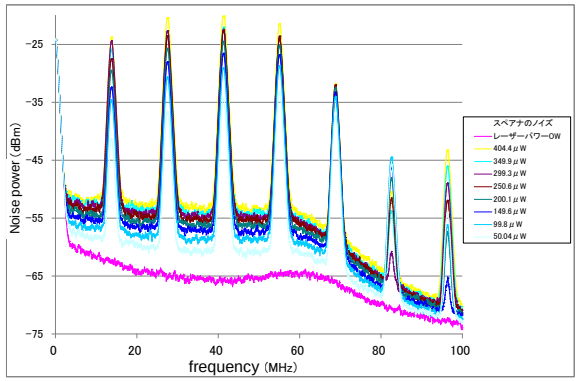


・10MHz operation
・Capable of auto calibration and adjustment: the system includes variable optical attenuators (VOAs), optical switches (OSs) and optical receivers.

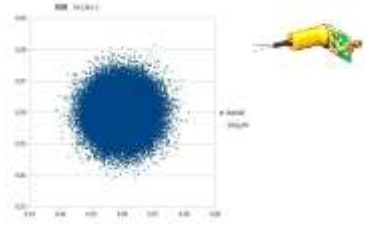
TH *et al*. Quantum Science and Technology, 2, 024010 (2017).

17

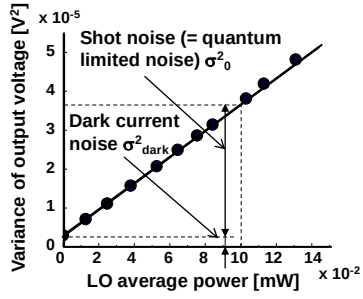
Shot-noise limited homodyne detection with commercial balanced receiver : General photonics BPD-001-50



・Quantum noise level is sufficiently larger than amplifier noise level.
・Pulse-resolved measurement at 10MHz repetition rate: adjacent correlation <0.01.

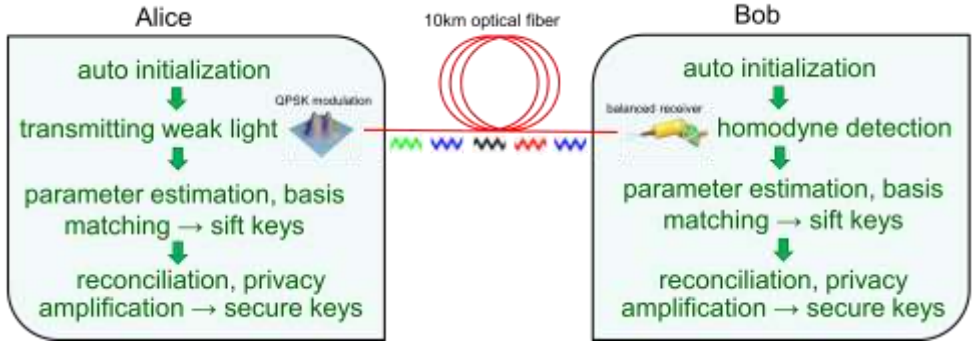


Exceeding noise of detector ($\sigma^2_{dark}/\sigma^2_0$)
$\sigma^2_{dark}/\sigma^2_0 \sim 0.1$ for P_{LO}=0.1 mW



18

Compact and low cost CV-QKD system



Error correction

Non-Binary LDPC code
TITECH Prof. Kasai

"FFT-Based Parallel Decoder of Non-Binary LDPC Codes on GPU: KFO_NBLDPC_GPU"

https://search.star.titech.ac.jp/titech-ss/pursuer.act?event=outside&key_rid=6000012452&lang=en

PC CPU:Xeon E3-1275 V2
GPU:GeForce GTX 780 Ti
OS:CentOS 6.5

Privacy amplification using Toeplitz matrix
Mitsubishi electric

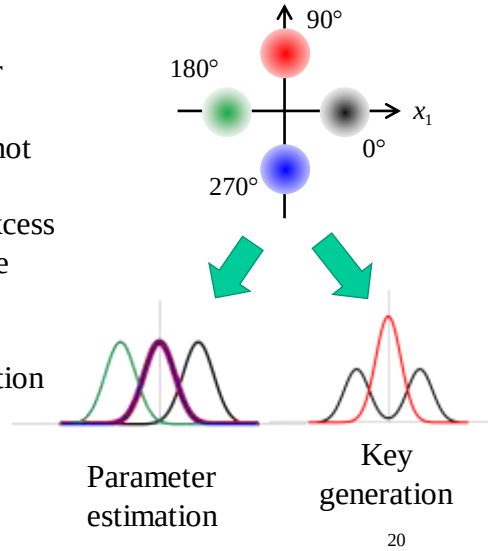
Using FFT reduce computational complexity to O($n$log$n$)

19

Post-selection and parameter estimation

After sending 10^6 optical pulses, Alice randomly choose a half of the pulses for parameter estimation.
For these pulses, Alice informs Bob of not only her basis but also her bits.
Bob calculates the transmissivity and excess noise using these data and his homodyne measurement results.

The rest of data are used for key generation after basis check.

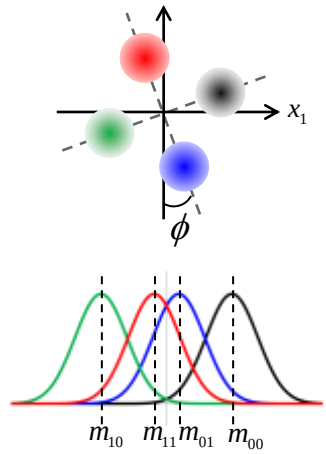


20

Post-selection and parameter estimation

phase offset between Alice's and Bob's delay

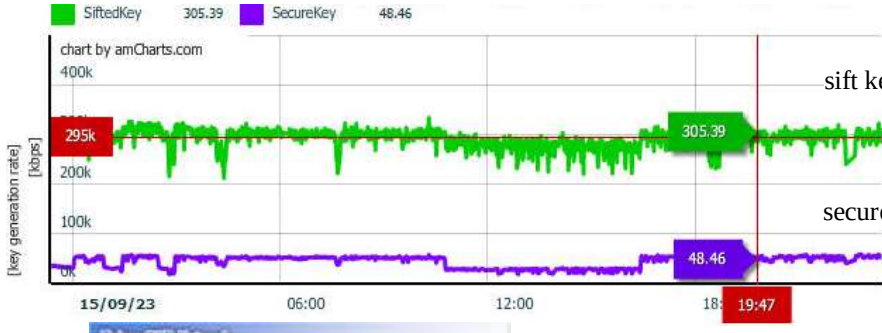
$$\phi_{ij} = \arccos(m_{ij} / A)$$
$$A = \sqrt{\sum_{i,j} m_{ij}^2} / 2 \qquad (i, j = 0,1)$$



21

Continuous operation over 10 km fibre

TH *et al*. Quantum Science and Technology, 2, 024010 (2017).



sift key rate

secure key rate

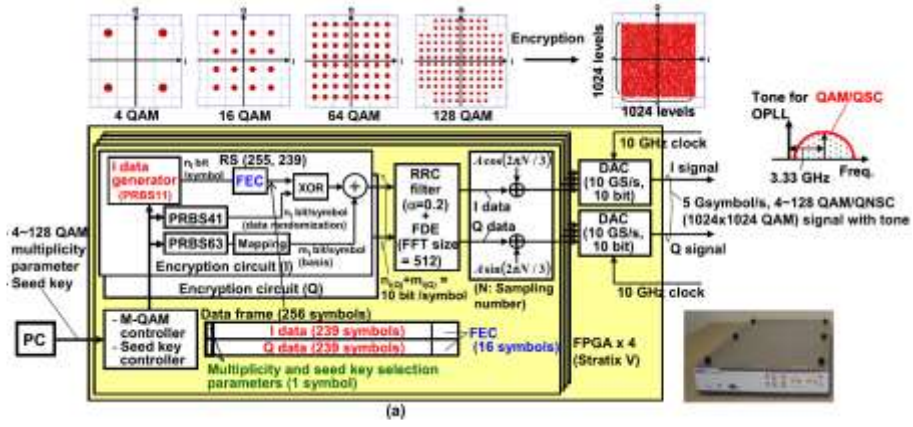
Sift key rate
~300 kbps
Secure key rate
~50 kbps

22

IEEE JOURNAL OF QUANTUM ELECTRONICS, VOL. 53, NO. 4, AUGUST 2017 8000316

QAM Quantum Noise Stream Cipher Transmission Over 100 km With Continuous Variable Quantum Key Distribution

Masataka Nakazawa, *Fellow, IEEE*, Masato Yoshida, *Member, IEEE*, Toshihiko Hirooka, *Member, IEEE*, Keisuke Kasai, *Member, IEEE*, Takuya Hirano, Tsubasa Ichikawa, and Ryo Namiki



QAM Quantum Noise Stream Cipher Transmission Over 100 km With Continuous Variable Quantum Key Distribution

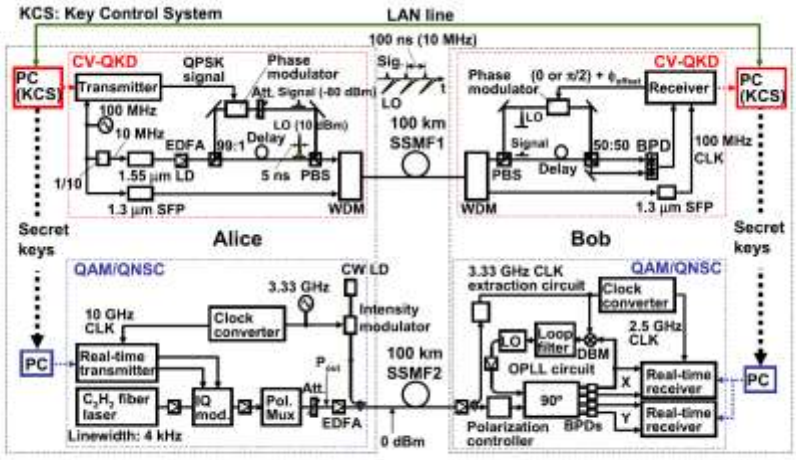
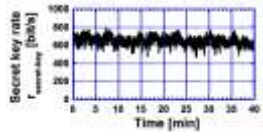


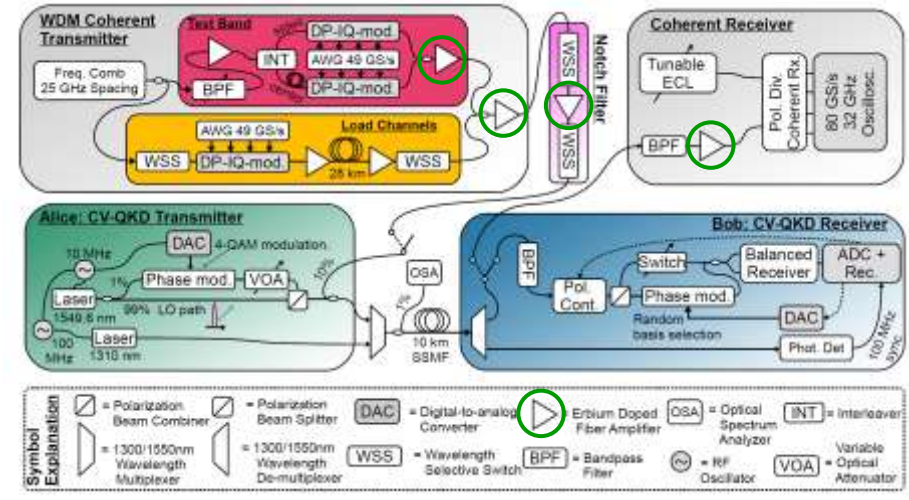
Fig. 5. Experimental setup for real-time 4~128 QAM/QNSC transmission over 100 km with secret keys delivered by CV-QKD. The upper part describes CV-QKD and the lower part shows QAM/QNSC, where two standard single-mode fibers (SSMF) are used for key delivery and QAM/QNSC transmission.



QKD keys are secure against an individual attack.

学習院大学 GAKUSHUIN UNIVERSITY NICT

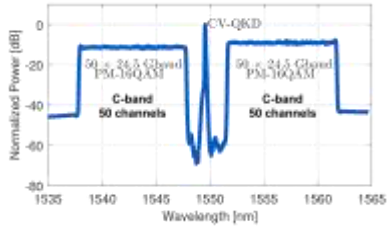
Coexistence of CV-QKD and 100 WDM coherent channels: Experimental Setup

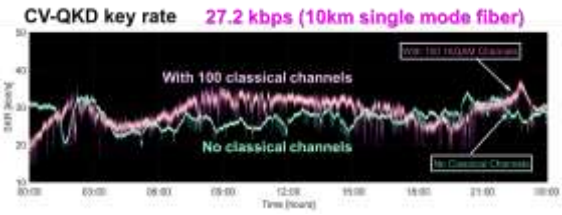


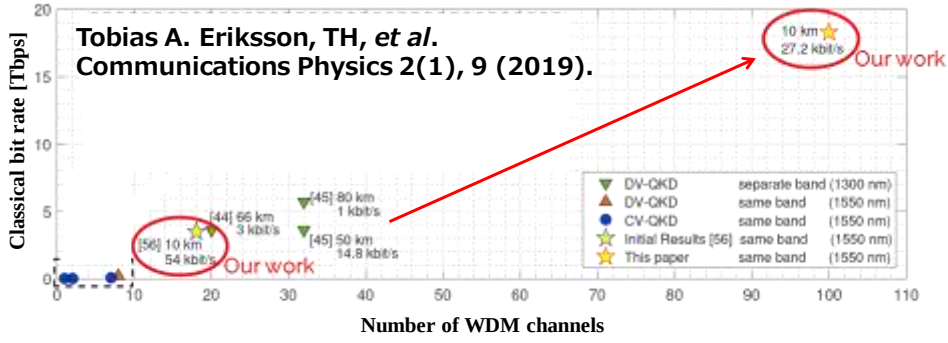
To the best of our knowledge, previous demonstrations have not used any optical amplification of the data signals. For widespread deployment, it is crucial to demonstrate that QKD channels can co-exist in the current state of the art fiber optical network.

学習院大学 GAKUSHUIN UNIVERSITY NICT

Coexistence of CV-QKD and 100 WDM coherent channels (18.3 Tbit/s): Results







Various implementation of CV-QKD

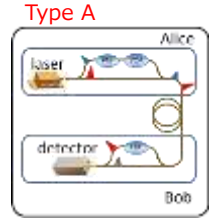
LO	A. Self, B. PLL, C. Digital coherent
modulation	a. Discrete mod., b. Gaussian mod.
detection	i. Homodyne det., ii. Heterodyne det.

A. Self-homodyne:
Both signal and LO are sent from Alice
pros: cost (low coherence light source can be employed)
cons: long-distance operation is difficult due to the decrease of LO

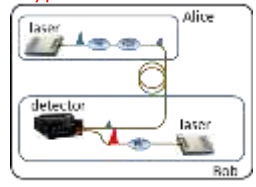
B. Phase-lock loop:
Optical PLL or injection locking to generate phase-lock LO
pros: free from disadvantage of Type A
pros: narrow band lasers are needed for both Alice and Bob

C. Digital coherent
Digital signal processing is utilized for phase compensation
pros: complex phase-lock loop is unnecessary.
pros: real-time digital signal processing is demanding.

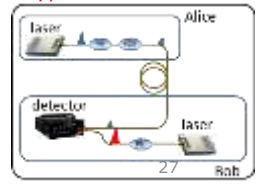
Type A



Type B



Type C



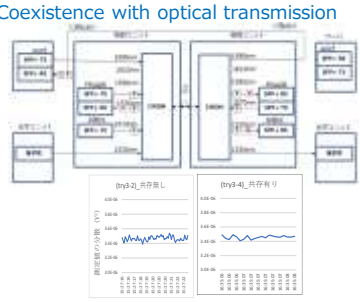
Our R&D on CV-QKD

CSTI(Council for Science, Technology and Innovation) SIP(Cross-Ministerial Strategic Innovation Promotion Program) "Photonics and Quantum Technology for Society 5.0" (Funding agency: QST)

Joint research with NEC

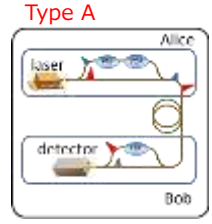
Type A
higher speed (10MHz → 40 MHz), low cost and stable
Type B
proof of principle, higher speed

Coexistence with optical transmission

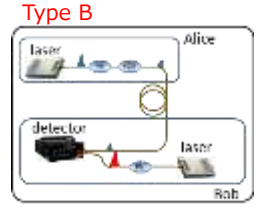


Control unit

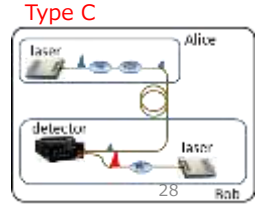
Type A



Type B



Type C

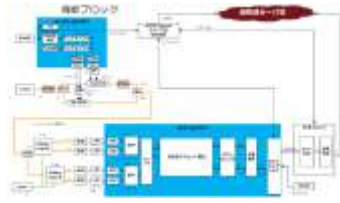


MIC Project "R&D for building a global quantum cryptography communication network"

Joint research with NEC and NICT

Type C
basic R&D on algorithm and setups
proof of concept

Development of high-speed low-noise homodyne receiver



28

Summary

- We have discussed similarities and differences between CV-QKD and QAM optical communication, and CV-QKD and DV-QKD.
- Similarities between the QAM optical communication and the CV-QKD show us a future vision of integration of both technologies.
- We also have discussed the security of CV-QKD, and various implementations.

Thank you very much for watching !!

29