学習院大学
GAKUSHUIN UNIVERSITY

量子力学100周年研究会：量子基礎・量子情報のこれまでとこれから
10:55-11:30 11 September 2025@Kyoto

量子暗号とエンタングルメント

学習院大学　　平野　琢也

謝辞：総務省委託研究「グローバル量子暗号通信網構築のための研究開発(JPJ008957)」
「量子インターネット実現に向けた要素技術の研究開発(JPMI00316)」

目次

- 量子暗号とは何か(歴史)、どこが面白いのか（個人的）
- 量子暗号の現在地
- 量子鍵配送の実験について
- まとめ

量子暗号とは：歴史

BB84プロトコル
Bennett, C. H. and Brassard, G., “Quantum cryptography: Public-key distribution and coin tossing”, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179. (https://arxiv.org/abs/2003.06557)

前史
1960年代終頃 Stephen Wiesner, “Conjugate Coding”
IEEE Transactions on Information Theoryに投稿したが、リジェクトされた
SIGACT News. 15 (1), 78–88 (1983). doi:10.1145/1008908.1008920

The uncertainty principle imposes restrictions on the

量子情報科学：量子力学の基本的な原理や効果を直接利用した情報処理、通信技術

paper will show that in compensation for this "quantum noise"

quantum mechanics allows us novel forms of coding without

analogue in communication channels adequately described by

classical physics.

量子暗号とは：歴史

1960年代終頃 Stephen Wiesner, “Conjugate Coding”

Let us suppose to be definite that the money contains twenty isolated systems, S_i, i=1, 2, ... 20. At the mint they create two random binary sequences of twenty digits each which we will call M_i and N_i, i=1,2,...20, M_i = 0 or 1, N_i = 0 or 1. Then the two-state systems are placed in one of the four states a, b, α or β in accordance with the scheme shown in Fig. 2.

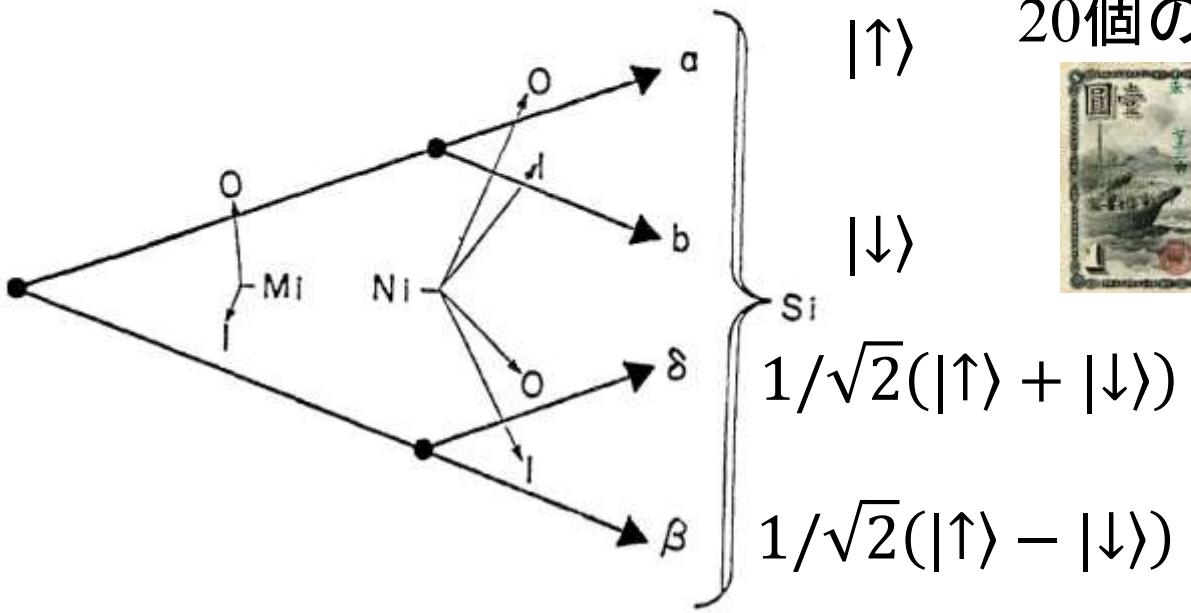


FIG. 2

偽造できない通貨

Spin 1/2 の系

20個の量子メモリ入り紙幣

https://ja.wikipedia.org/wiki/円_(通貨)#/media/ファイル:JAPAN-10-Constitutional_Monarchy-One_Yen_(1873).jpg

量子暗号とは：歴史

BB84プロトコル

前史

C.H. Bennett, G. Brassard and S. Breidbart, “Quantum Cryptography II : How to reuse a one-time pad safely even if P=NP ”, Rejected from 15th Annual ACM Symposium on Theory of Computing, Boston, May 1983.

Shortly thereafter, my good friend Vijay Bhargava was in charge of a special session on coding and information theory for yet another IEEE conference, which took place in Bangalore, India[11], in December 1984. He invited me to give a talk on any subject of my choice, and naturally I chose Quantum Cryptography considering how difficult it was to get these ideas published at the time. The resulting paper [7] gave its name to the “BB84 protocol” even though it had been described in detail as early as 1983 at the IEEE ISIT *talk* but not in the *paper* (how much can you say in a one-page abstract?). Retrospectively, it is amusing to note that the only reason the BB84 protocol was finally published is that it had not been submitted to the conference that printed it in its proceedings! Thanks Vijay!

Gilles Brassard, “Brief History of Quantum Cryptography: A Personal Perspective,” arXiv:quant-ph/0604072

量子暗号とは：歴史

BB84プロトコル
Bennett, C. H. and Brassard, G., “Quantum cryptography: Public-key distribution and coin tossing”, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179. (https://arxiv.org/abs/2003.06557)

Quantum cryptographyとは
- Quantum Key Distribution
- coin tossing
- その他の量子的な暗号プロトコル

（最近の使い方　量子暗号 = QKD + One time pad）

Coin tossing　→ AliceはEPRを使ってチートできる

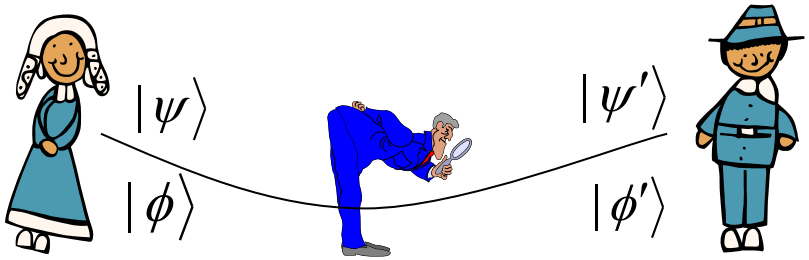
H.-K. Lo and H.F. Chau, “Is quantum bit commitment really possible?”, Physical Review Letters 78(17), pp. 3410 – 3413, 1997; D. Mayers, “Unconditionally secure quantum bit commitment is impossible”, Physical Review Letters 78(17), pp. 3414 – 3417, 1997.

Coin tossingの手順

Alice's bit string	1	0	1	0	0	1	1	1	0	1	0	1	1	0	0
Alice's random basis							Rectilinear								
Photons Alice sends	↕	↔	↕	↔	↔	↕	↕	↕	↔	↕	↔	↕	↕	↔	↔
Bob's random bases	R	D	D	D	R	R	D	R	R	D	R	R	D	D	R
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		
Bob's guess															
Alice's reply							'Rectilinear'								
							'You win'								
Alice sends her original bit string to certify	'1	0	1	0	0	1	1	1	0	1	0	1	1	0	0'
Bob's rectilinear table	1					1					0				0
Bob's diagonal table		0		1						1			0		

量子暗号どこが面白いのか（個人的）

Quantum Key Distribution



信頼し合う二人は量子力学の原理を利用して秘密を共有できる

Coin Tossing

Created by copilot: 毒舌AliceとBobとコイン投げ

互いに信頼していない二人はエンタングルメントがあるので公平なゲームを実施できない

量子暗号：量子力学の基礎の意味を社会的な関係の中で探る

量子暗号の現在地

Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).

QC could well be the first application of quantum mechanics at the single-quantum level. Experiments have demonstrated that keys can be exchanged over distances of a few tens of kilometers at rates on the order of at least a thousand bits per second. There is no doubt that the technology can be mastered and the question is not whether QC will find commercial applications, but when. At present QC is still very limited in distance and in secret bit rate. Moreover, public-key systems dominate the market and, being pure software, are tremendously easier to manage. Every so often, we hear in the news that some classical cryptosystem has been broken. This would be impossible with properly implemented QC. But this apparent strength of QC might turn out to be its weak point: security agencies would be equally unable to break quantum cryptograms!

量子暗号は、単一量子レベルの量子力学の最初の応用になると考えられる。この技術が習得可能であることに疑いの余地はなく、問題は、量子暗号が商業的な利用を見つけることができるかではなく、その時期が何時になるかである。
現代暗号は時間の経過とともに安全ではなくなるが、量子暗号は未来永劫安全
この量子暗号の強みは弱みにもなりうる：情報機関も破ることができないから

量子未来社会ビジョン　（令和4年4月22日）
内閣府 科学技術・イノベーション推進事務局

未来社会ビジョンに向けた 2030年に目指すべき状況

国内の量子技術の利用者を1,000万人に

- 先進諸国においてはインターネットの利用者率が5-10%を超えると普及が爆発的に加速。
- 量子技術の国内利用者について同様の比率を目指し、国内利用者1,000万人を想定。
- このため、多様なユーザがアクセスし、ユースケースを探索・創出するための量子コンピュータの利用環境を整備（テストベッド整備等）。

量子技術による生産額を50兆円規模に

- 2030年の人口（1億1913万人※1）に対する量子技術の利用者1,000万人の割合と、量子技術が寄与し得る産業の生産額（2030年）約615兆円※2を考慮して、生産額を50兆円規模と想定。本数字は生産額ベースであることに留意すべきである。
- なお、2030年の量子技術による国内付加価値額は約1.2兆円と予測され※3、これに海外獲得分（約0.1兆円※4）を加え、総付加価値額は約1.3兆円を想定。
- このため、産学官の関係者がより緊密に連携し、民間事業活動の後押しなど産業競争力強化に向けて本格的かつ戦略的に取り組んでいく。

未来市場を切り拓く量子ユニコーンベンチャー企業を創出

- 国内では、ユニコーン企業（評価額が10億ドル（約1,050億円）を超える未上場のスタートアップテクノロジー企業）は5社（2021年12月時点）。
- 量子主要３分野（量子コンピュータ、量子暗号通信、量子計測・センシング）でユニコーン企業（各分野数社以上）を創出し、ベンチャー企業の参入を活性化。
- このため、官民が一体となって、起業家育成、研究開発支援、投資家とのマッチング、政府系ファンド等を活用したリスクマネー供給など総合的な起業環境を整備する。

※1 日本の将来推計人口（平成29年推計）（国立社会保障・人口問題研究所）
※2 産業連関表（平成27年度）のうち、製造業、電力、商業、金融・保険、運輸、情報通信、医療、広告の生産額の合計に対して、2022年度以降CAGR 1%と仮定して算出（日本経済中期予測(2022～31年度)（大和総研、2022年01月24日）の実質GDP成長率年率＋1.0%を参考）
※3 出典：株式会社矢野経済研究所「2021 量子コンピュータ市場の現状と将来展望」（2021年9月）、「2022年版 量子技術市場の現状と展望」（2022年2月）
※4 平成27年産業連関表の全産業の国内最終需要92.3%と輸出分7.7%の比率を参考に、海外市場分を約0.1兆円と想定。

量子未来社会ビジョン　（令和4年4月22日）
内閣府 科学技術・イノベーション推進事務局

各技術分野の取組

1．量子コンピュータ

国産量子コンピュータの研究開発の抜本的な強化、産業界への総合支援

- ✓ 量子技術と従来型（古典）計算システム（半導体等も含む）の**ハイブリッドなコンピューティングシステム・サービス実現**、海外に比肩する**国産量子コンピュータの研究開発の抜本的な強化**
- ✓ 有志国を含む国内外の企業との連携による事業化等の支援のための環境整備、標準化支援等の**産業界への総合的な支援**（産総研に新センター等を設置）
- ✓ 量子コンピュータの大規模化・実用化に向けた**ブレークスルー技術の戦略的研究開発や基礎研究の推進**

国産量子コンピュータ（理研で開発中）

2．量子ソフトウェア

量子コンピュータの利用環境の整備、ソフトウェア研究開発の抜本的な強化

- ✓ 多様なユーザがアクセスし、ユースケースを探索・創出できる**量子コンピュータの利用環境整備（テストベッド整備等）**
- ✓ 量子・古典のハイブリッドなコンピューティングサービスも見据えた**創薬・医療、材料、金融等の他分野やAI等の従来型（古典）技術分野との融合によるソフトウェアの開発（産学共創）**
- ✓ **量子ソフトウェアに関する国家プロジェクトの抜本的な充実・強化**、優れた**アイデアを発掘・支援する仕組み**

量子ソフト市場（2040年・世界）40～75兆円

3．量子セキュリティ・ネットワーク

量子暗号通信の利用拡大、総合的セキュリティの実現、量子インターネット研究

- ✓ 量子暗号通信**テストベッドや利用実証の拡大・充実**、耐量子計算機暗号も含め量子技術と従来型（古典）技術が一体となった**総合的なセキュリティの実現**
- ✓ 量子暗号通信技術の導入を後押しするための**評価・認証制度などの支援**
- ✓ 量子状態を維持した通信を可能とする**量子インターネット研究開発の国家プロジェクトの立ち上げ**

4．量子計測・センシング／量子マテリアル等

量子計測・センシング技術の応用分野の拡大、事業化支援

- ✓ 量子計測・センシング技術の**応用分野・活用事例の拡大、利用環境の整備（テストベッド整備等）、利活用を支える技術基盤の充実・強化**
- ✓ 将来のビジネス戦略を睨んだ**企業（ユーザー・ベンダー）の発掘・事業化支援**
- ✓ 世界最先端の量子機能を発揮する**量子マテリアルの研究開発・供給基盤の整備**

量子センサでEVの電流・温度を100倍以上高精度計測

EVの走行距離を10%以上向上（省エネ化）

量子暗号の現在地

Yu-Ao Chen, *et al*., An integrated space-to-ground quantum communication network over 4,600 Kilometres, Nature 589, 214–219 (2021).

「京滬幹線」は2017年8月末に完成し全長2,000キロメートルを超えた世界最長の中継プランに基づく量子セキュリティ鍵配送幹線である。現在すでに金融、電力、行政事務等の業種・機関の150余のユーザーがアクセスしている。
「墨子号」は2016年8月に打ち上げを成功させ、河北興隆地上ステーションと光リンクを構築している。

https://crds.jst.go.jp/dw/20210317/2021031726240/

量子暗号の現在地

Yang Li, *et al*., Microsatellite-based real-time quantum key distribution, Nature 640, 47 (2025).

Extended Data Table 2 | Comparison with previous missions

Parameter	Micius[6]	This work
Payload weight	~250 kg	22.7 kg
Satellite weight	635 kg	95.9 kg
Transmitter aperture	300 mm	200 mm
Divergence angle	~10 μrad	9 ~10 μrad
Tracking precision (RMS)	0.6~1.5 μrad	0.55~1.6 μrad
QKD light source frequency	100 MHz	625 MHz
Communication scheme for key distillation	Microwave	Laser
Ground station weight	~13000 kg	~100 kg
Key distillation timeliness	2~3 days	Real time

Also, a secret key, enabling one-time pad encryption of images, is created between China and South Africa at locations separated by over 12,900 kilometres on Earth. The compact quantum payload can be readily assembled on existing space stations or small satellites, paving the way for a satellite-constellation-based quantum and classical network for widespread real-life applications.

量子暗号の現在地: 情報機関による否定的なコメント

米国国家安全保障局(NSA)

https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2394053/nsa-cybersecurityperspectives-on-quantum-key-distribution-and-quantum-cryptogr/

英国国家サイバーセキュリティセンター(NCSC)

https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

欧州ネットワーク・情報セキュリティ機関(ENISA)

https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantummitigation

NSAの見解

In summary, NSA views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications in National Security Systems, and does not anticipate certifying or approving any QKD or QC security products for usage by NSS customers unless these limitations are overcome.

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

量子暗号の現在地: NSAが指摘するQKDの限界

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Technical limitations

1. Quantum key distribution is only a partial solution. QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.

2. Quantum key distribution requires special purpose equipment. QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches.

3. Quantum key distribution increases infrastructure costs and insider threat risks. QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.

4. Securing and validating quantum key distribution is a significant challenge. The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than in most physical engineering scenarios making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.[2]

5. Quantum key distribution increases the risk of denial of service. The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

量子暗号の現在地: NSAが指摘するQKDの限界

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Technical limitations

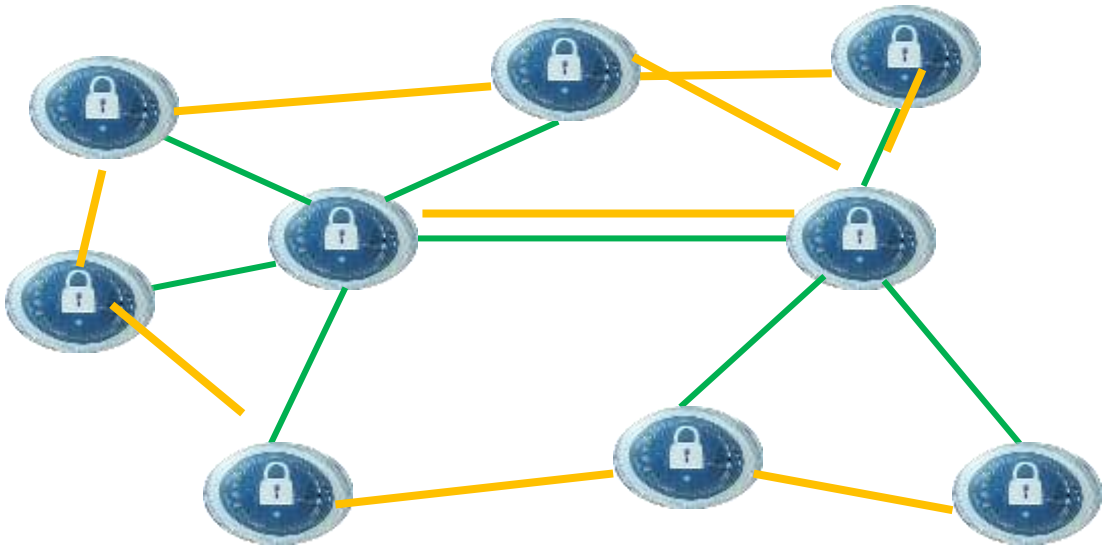
1. QKD は認証を必要としており、部分的な解決策でしかない.
2. QKD は特殊な装置を必要とする.
3. QKD は多くの場合トラステッドノードを必要とし，それはインフラのコストと内部からの脅威を増大させる.
4. QKD を安全にし，検証することは大きな挑戦.
5. QKD はサービス拒否(denial of service) のリスクを増やす

Rennerらによる反論 R. Renner and R. Wolf: AIAA Journal, 61 (2023) 1895–1910. (doi:10.2514/1.J062267).

1.初期認証は根本的な問題であり，通信相手についての情報がなければ，どのような手段でも解決できない．BobとEve を区別するための情報をAlice が持っていないのであれば，通信相手がBob なのかEve なのかをAlice は知ることができず，逆にAlice とBob がなんらかの秘密情報を共有しているのであれば，認証が可能になる．また，QKDの認証はリアルタイムに破る必要があり（事後に認証情報が漏洩しても，QKD で生成する鍵は漏洩しないので），第3者の認証局を信頼する計算量的な安全性に基づく認証を利用できる可能性もある.

2～4　技術的な課題として、解決するための研究開発が行われている。

量子鍵配送ネットワーク(QKDN)



QKD allows two parties to share a secret key whose secrecy is guaranteed by the laws of quantum physics.

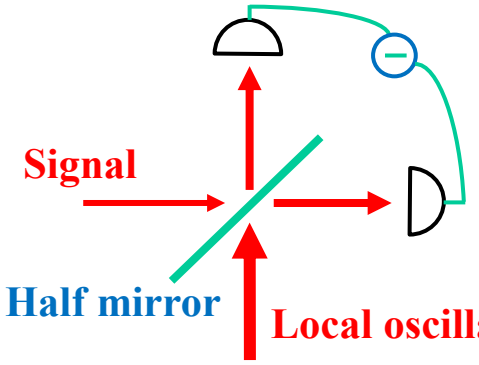
Building a QKD network by connecting a pair of nodes with QKD greatly enhances the capabilities of QKD.

The QKD network must be a part of communication system consisting of high-speed optical network and routing mechanism.

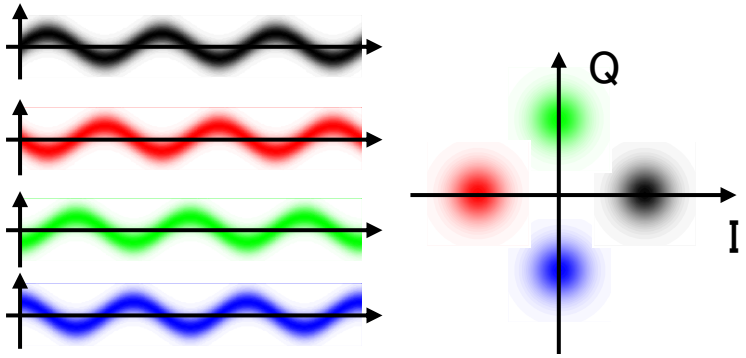
Continuous-Variable QKD : faint light is detected by homodyne detection

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

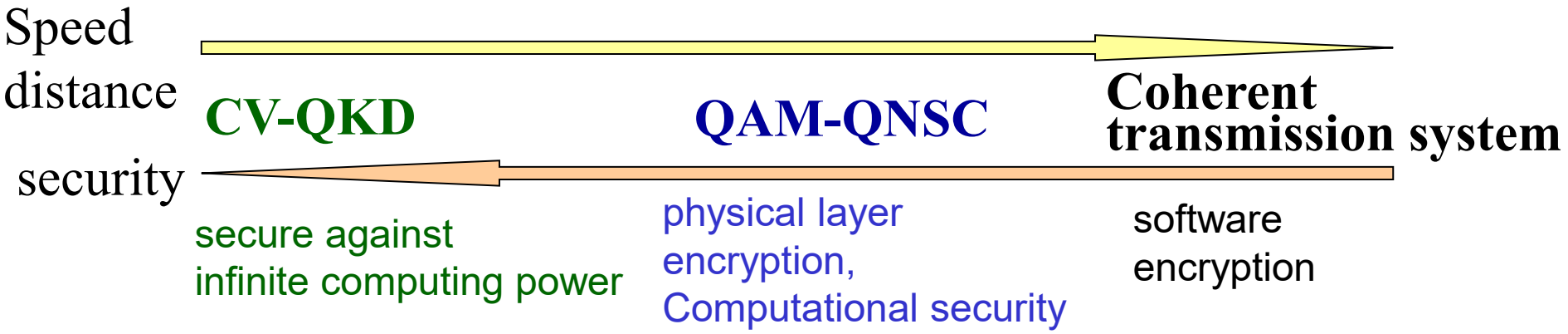
Similarities

- 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.



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 than ordinary coherent comm.

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.

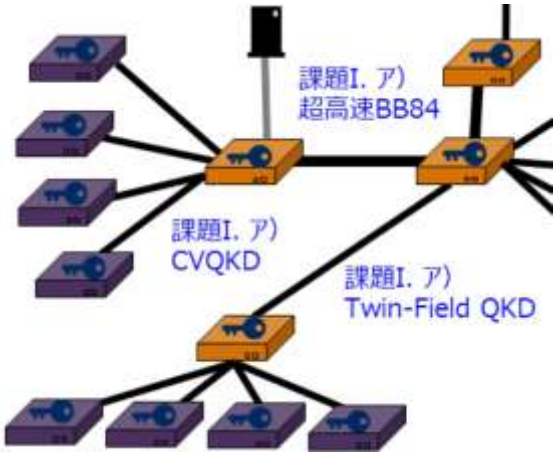
In CV-QKD, the amplitude of the electromagnetic field is measured, and the wave amplitude can be divided, then other person may receive the information.

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

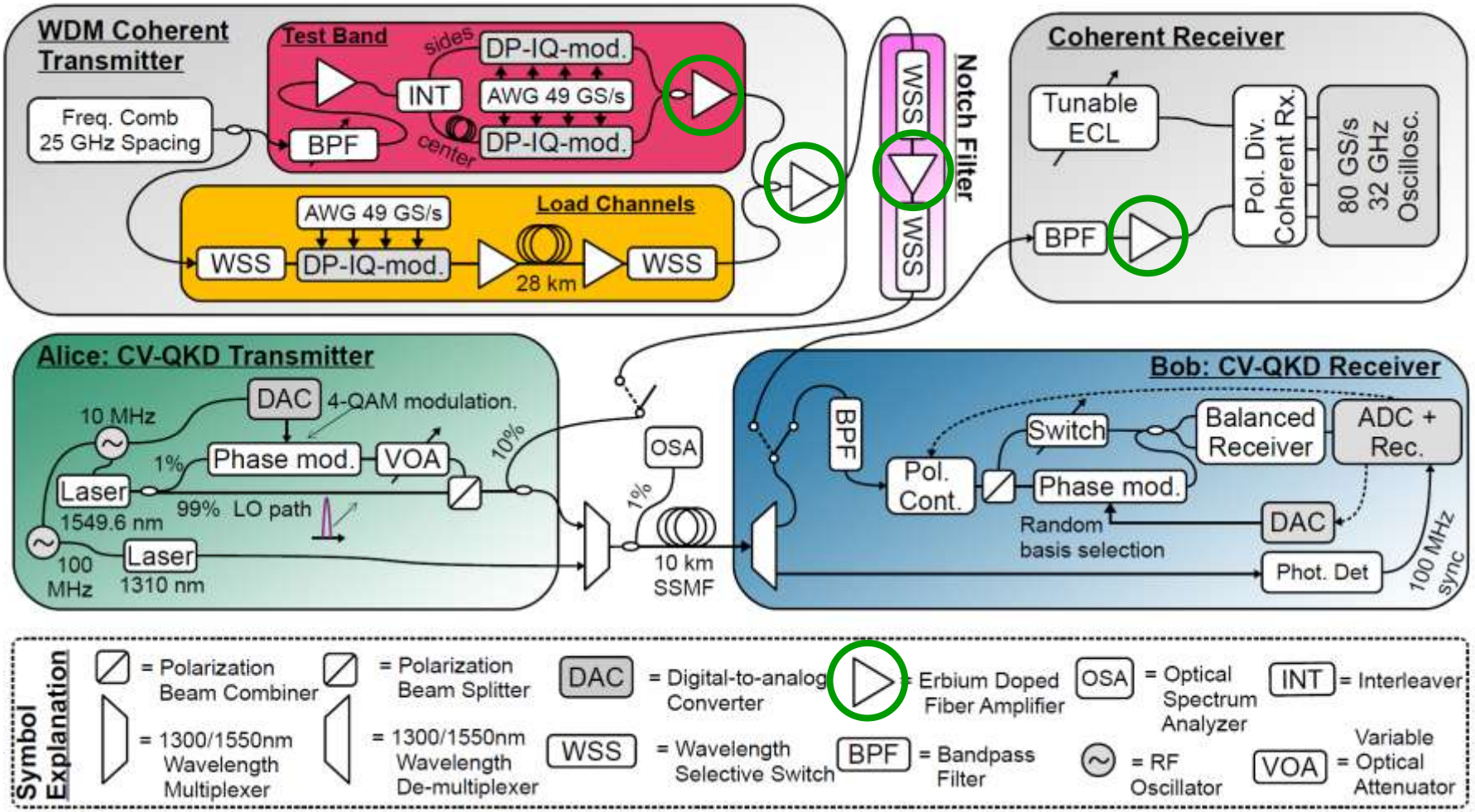
R&D on CV-QKD in Japan

Cabinet Office SIP 2nd 2018-2023.3
(Cross-Ministerial Strategic Innovation Promotion Program) "Photonics and Quantum Technology for Society 5.0“
Development of CV-QKD with NEC

MIC Project "R&D for building a global quantum cryptography communication network“ 2020-2025.3

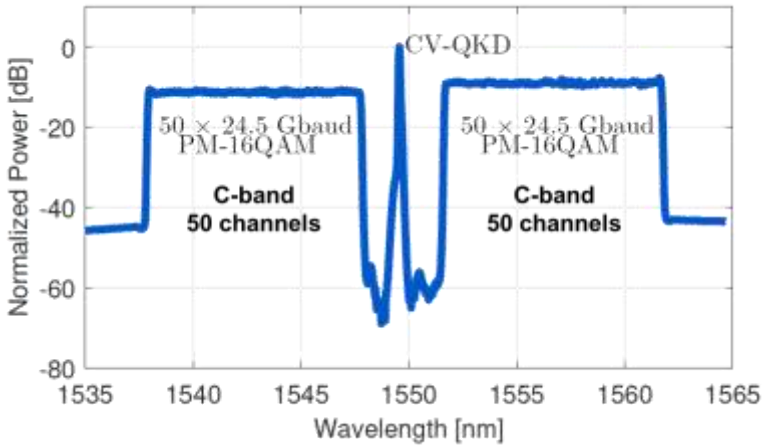


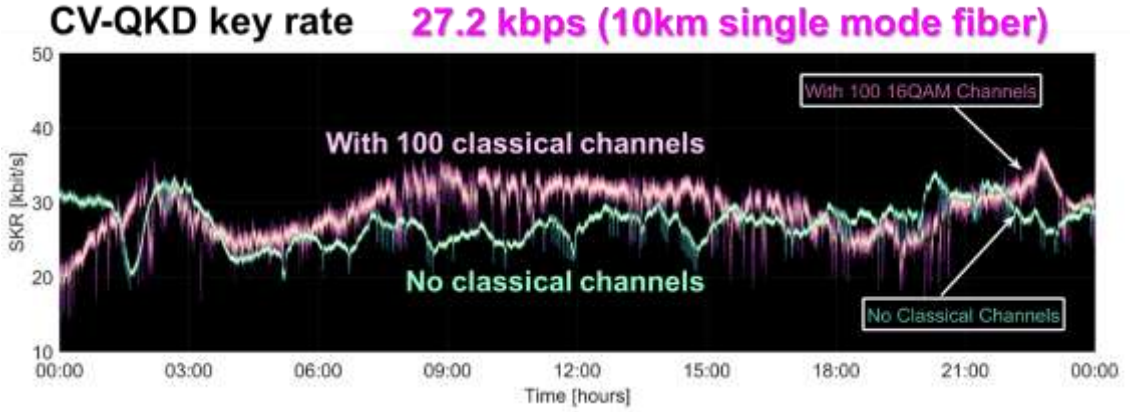
Coexistence of CV-QKD and 100 WDM coherent channels: Experimental Setup

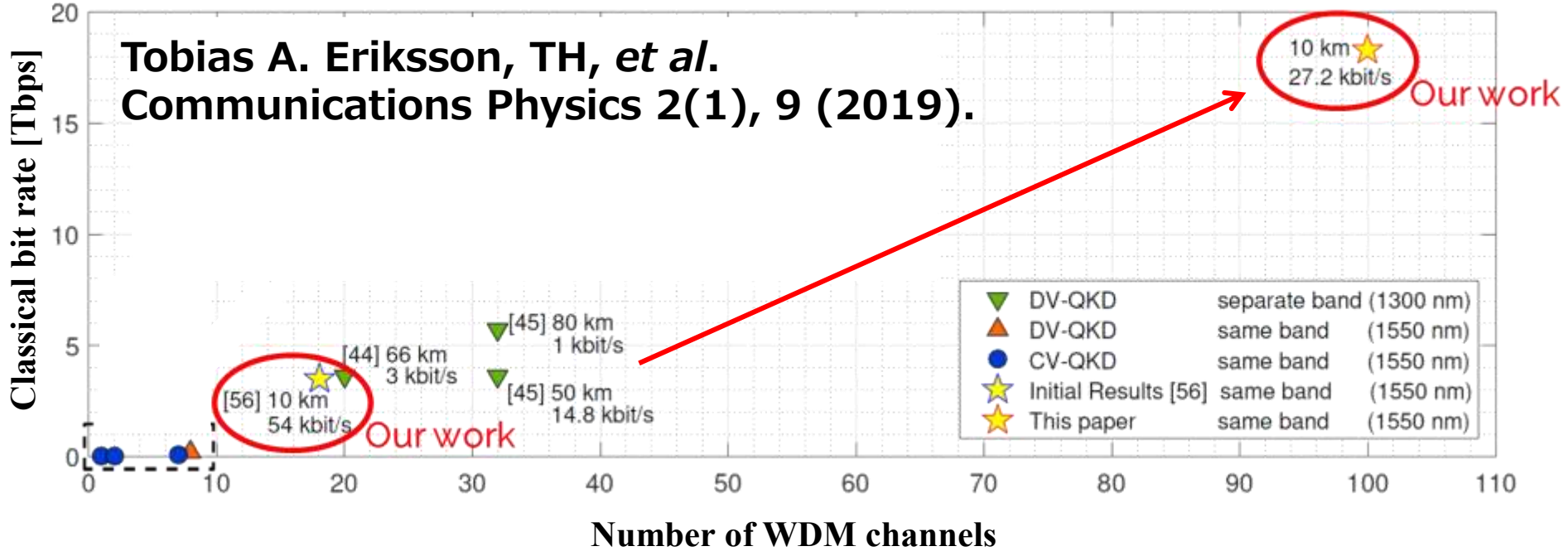


To the best of our knowledge, previous demonstrations have not used any optical amplification of the data signals. For widespread deployment, it is crucial to demonstrate that QKD channels can co-exist in the current state of the art fiber optical network.

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







学習院大学
GAKUSHUIN UNIVERSITY

CV-QKD: Discrete Modulation and Gaussian Modulation

Discrete Modulation

Proposal and first experiment: TH *et al.* (Meeting abstract of the Physical Society of Japan, 53, Issue 2, Part 2, 341 (1998)); PCT/JP99/04328, US 7305091.

Security against entangling cloner attack using trusted receiver: R. Namiki *et al.*, Phys. Rev. A **98**, 042319 (2018).

Finite-size security against general attack: T. Matsuura *et al.*, Nature Communications **12**, 252 (2021).

Gaussian Modulation

Proposal and first experiment: F. Grosshans *et al.,* Nature **421**, 238 (2003).

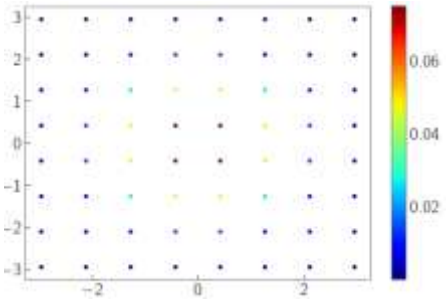
Security against general attack: A. Leverrier, Phys. Rev. Lett. **118**, 200501, (2017).

"Unfortunately, a Gaussian modulation is merely a theoretical idealization since in practice modulators have a finite range and precision, meaning that the true number of states possibly available is finite." (A. Denys *et al.,* Quantum **5**, 540 (2021).)

Discrete Gaussian modulation

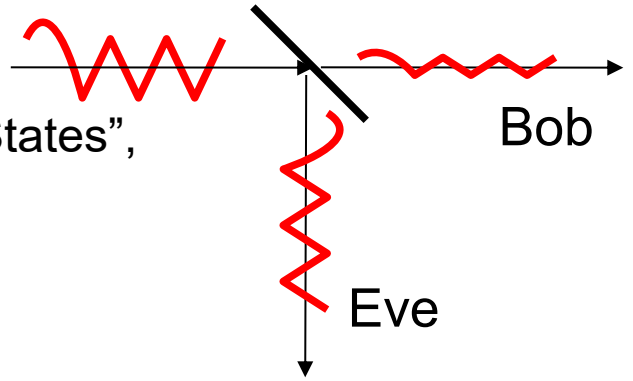
Security against general attack:

A. Denys *et al.,* Quantum **5**, 540 (2021).



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).

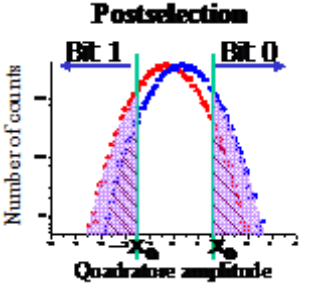
Recipe for beating 3dB-loss-limit

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.

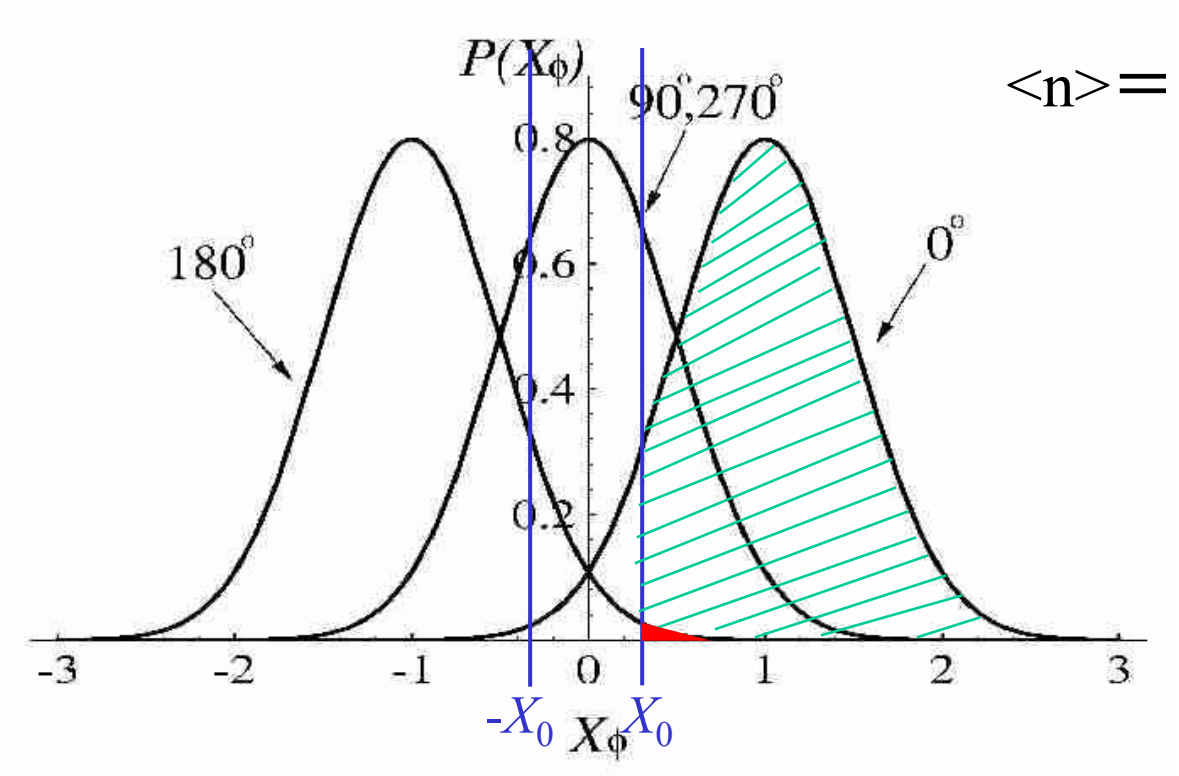
"Security of quantum cryptography using balanced homodyne detection",
R. Namiki, T. Hirano, Phys. Rev. A, vol. 67, no.2, 022308-1-7 (2003).



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).

Probability distribution of quadrature amplitude: Post selection



Bob sets up a threshold values X_0.

If the measured value $X\phi < -X_0$, Bob judges that ϕ=180°.

If $X\phi > X_0$, Bob judges that ϕ=0°.

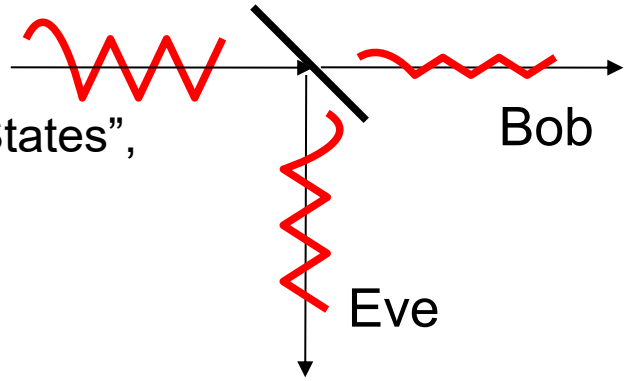
If $-X_0 < X\phi < X_0$, Bob abandons the judgement.

Increasing X_0, the error rate, $e_{B,}$ decreases to an arbitrary small value.

The "effective" detection efficiency, $P,$ also decreases.

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).

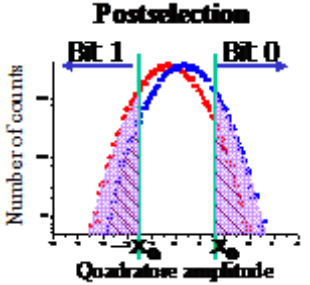
Recipe for beating 3dB-loss-limit

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).



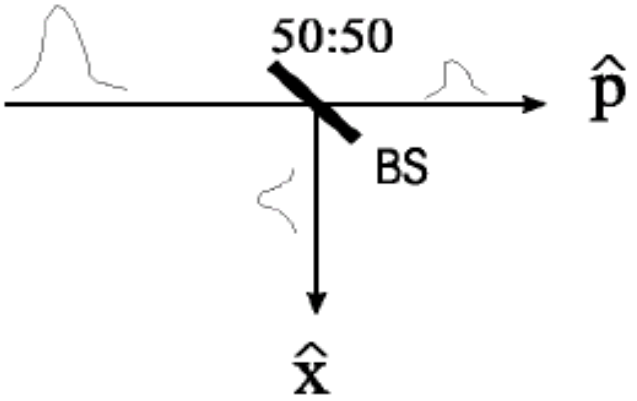
Reverse reconciliation

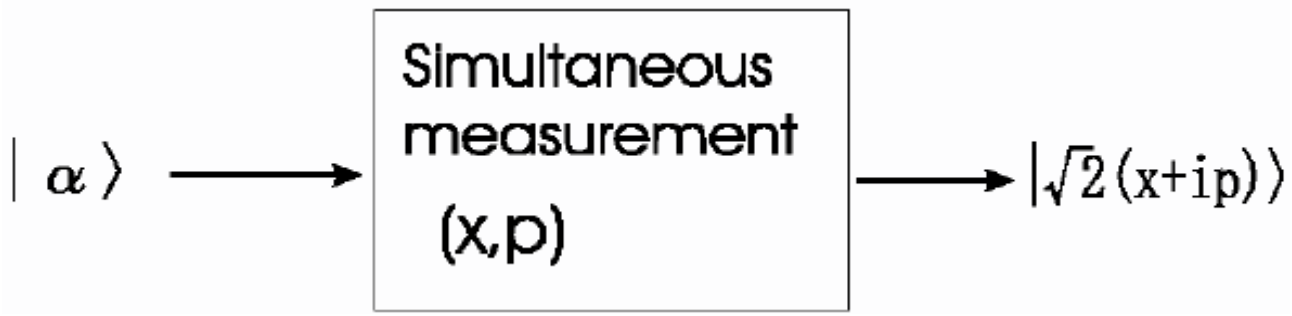
"Quantum key distribution using gaussian-modulated coherent states" , F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, Ph. Grangier, Nature **421**, 238 (2003).

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.



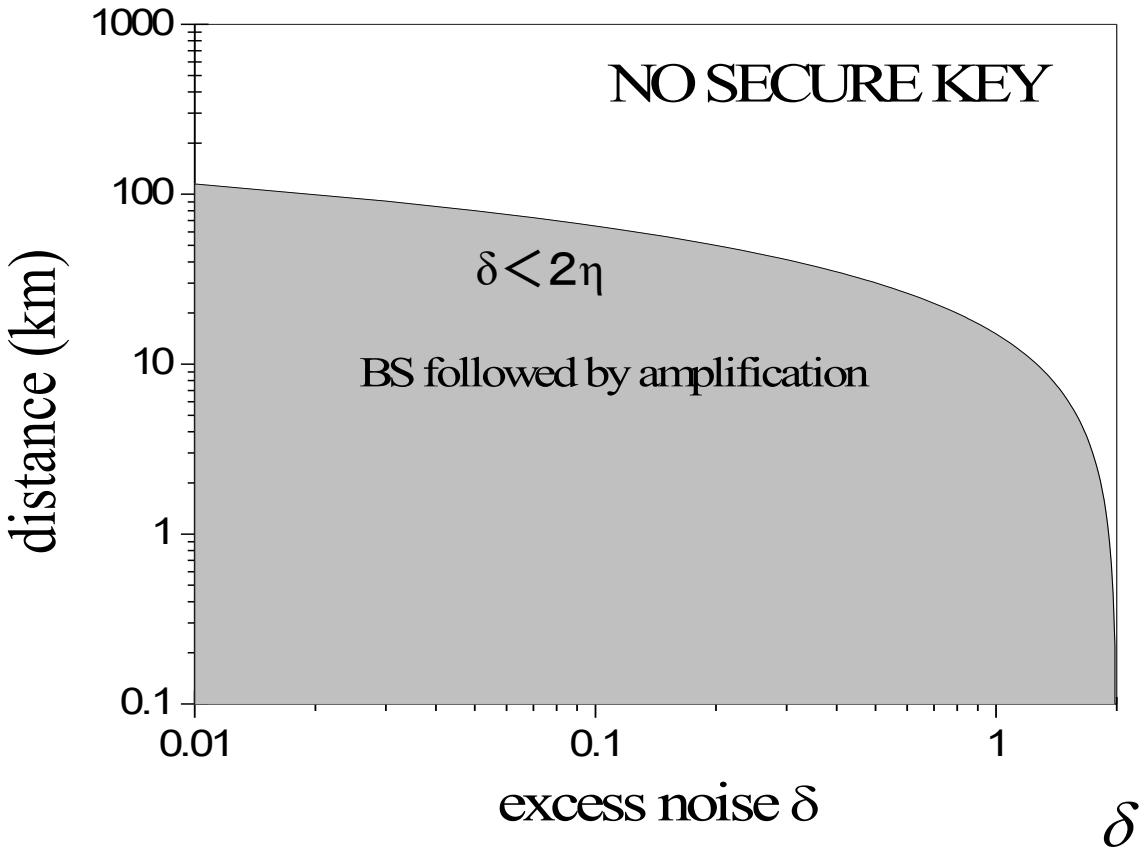


No secret key because Eve knows the state that Bob measures.
(entanglement breaking)

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:

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

Intercept & resend attack increases excess noise:

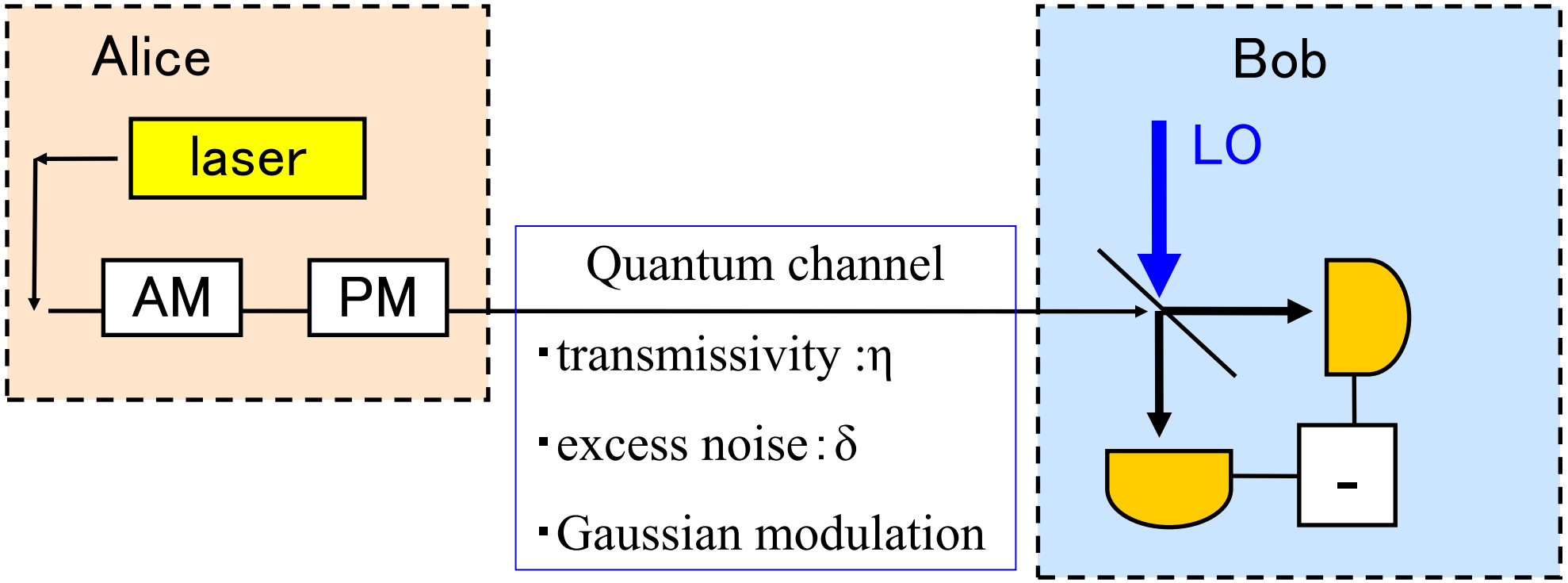
$$\delta = 2.$$

Excess noise decreases by loss:

$\delta = 2\eta$, η:transmissivity.

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

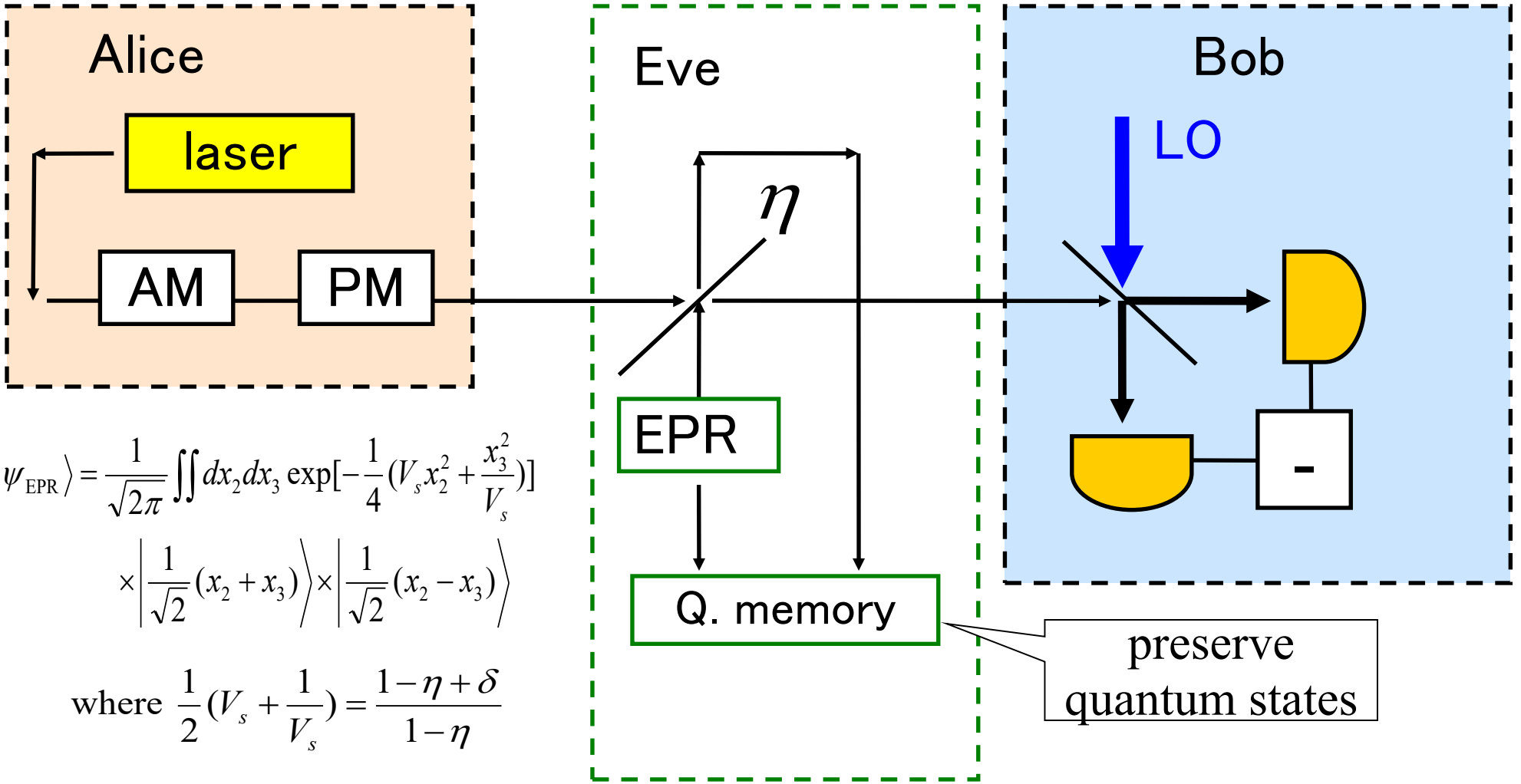
Entangling cloner attack (1)



Entangling cloner attack is optimum collective attack

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

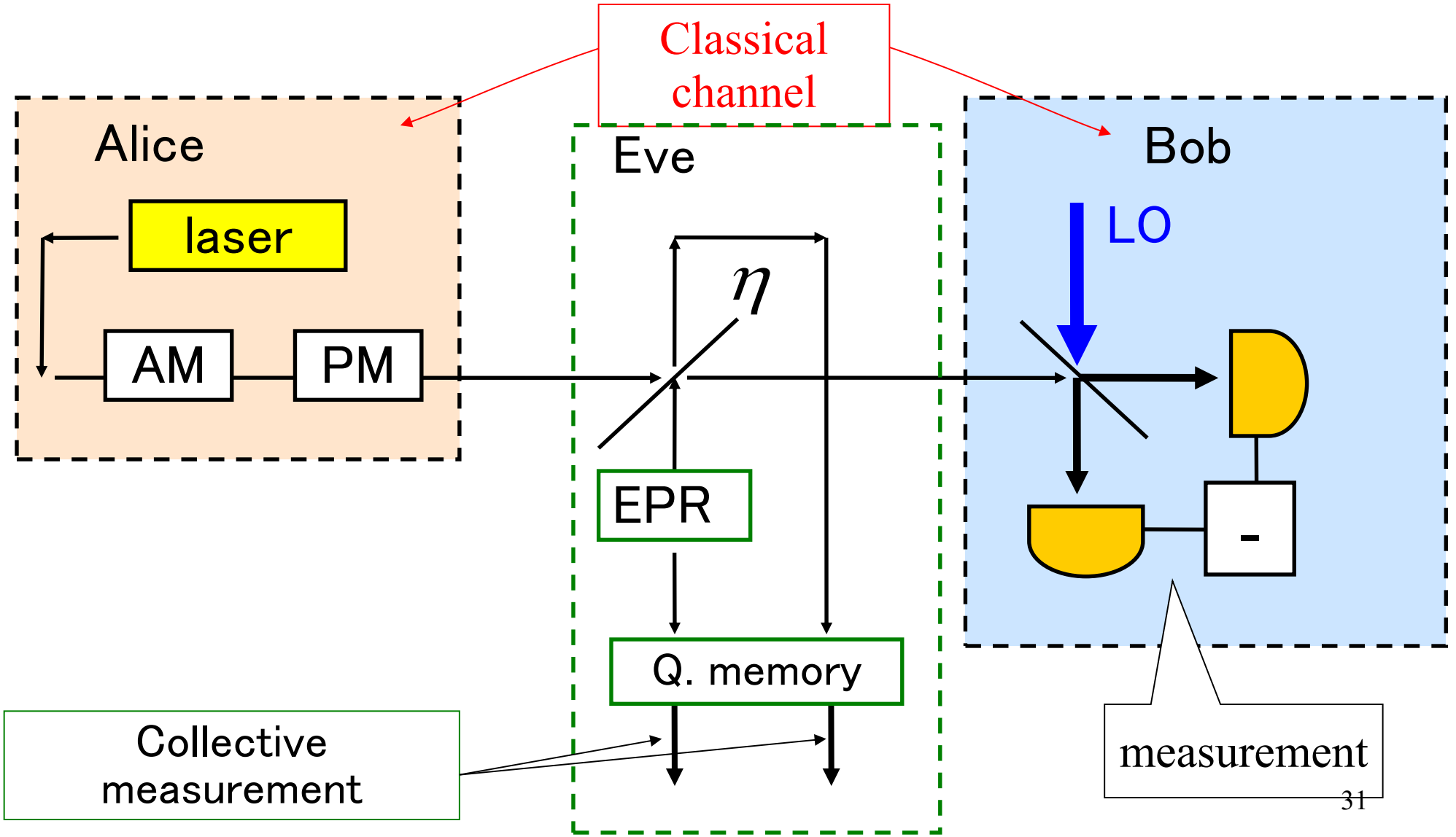
Entangling cloner attack (2)



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

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

Entangling cloner attack (3)



Four-state CV-QKD protocal

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

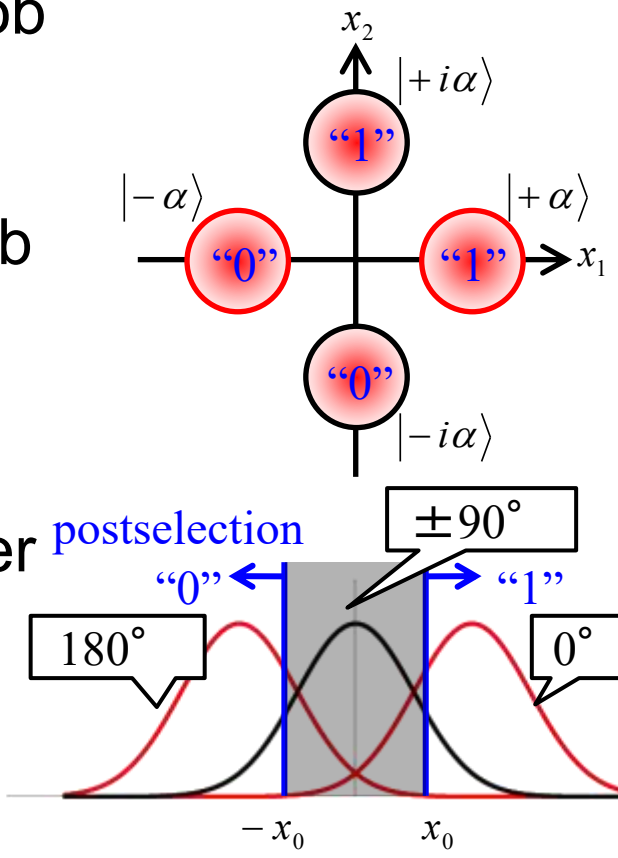
Protocol: 4 states + post-selection

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

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

学習院大学 GAKUSHUIN UNIVERSITY

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

The secret fraction r is given by the average of the information difference:

$$r = \int dm\, P(m|\alpha)\Delta I.$$

where $P(m|S)$ is the probability density that Bob obtains the quadrature value m when Alice sends $|S\rangle = |\pm\alpha\rangle$. The information difference is given by

$$\Delta I = I_{AB} - \chi,$$

where $I_{AB} = 1 - fh(\epsilon)$ is the mutual information between Alice and Bob taking into account the error correction efficiency f, $h(\epsilon)$ is the binary entropy, and χ is the Holevo quantity which gives the information accessible to Eve when she performs the entangling cloner attack.

The secure key generation rate N_{secure} is expressed using r:

$$N_{\text{secure}} = f_{\text{pulse}}\eta_{\text{sys}}\eta_{\text{est}}\eta_{\text{pr}}r,$$

where f_{pulse} is a repetition rate of the light pulse, η_{sys} is the operating efficiency of the QKD machine, 1 - η_{est} is the fraction used for parameter estimation, η_{pr} is the efficiency of the QKD protocol

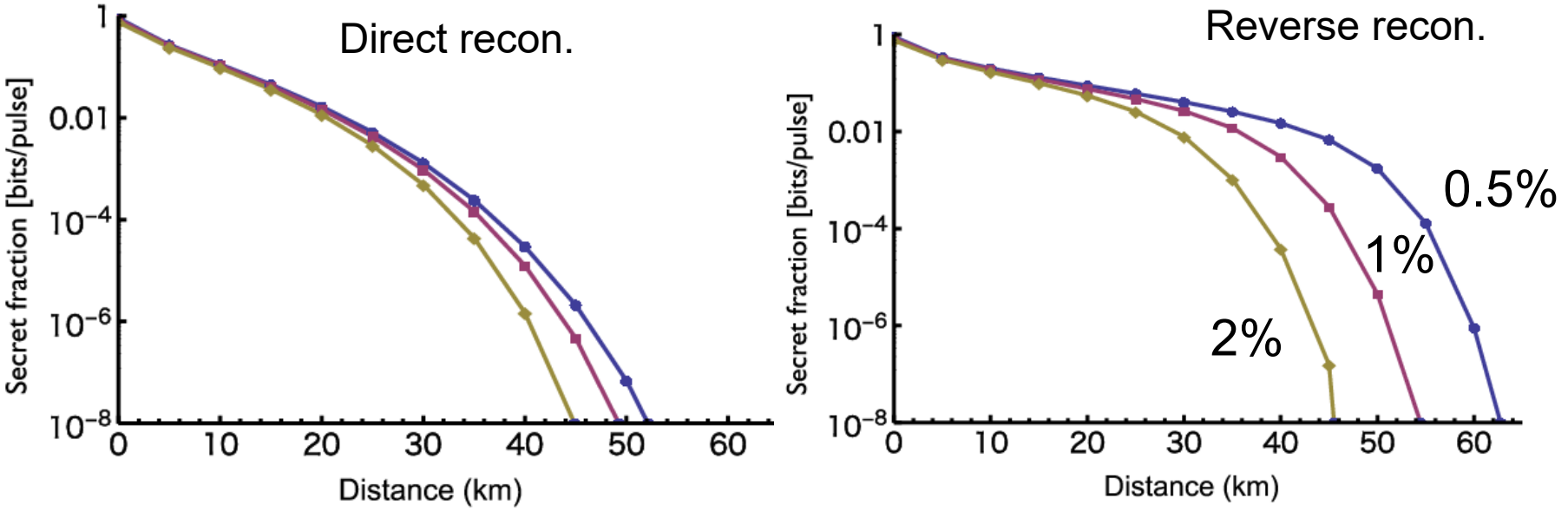
Secret fraction of four-states postselection protocol against entangling cloner attack

学習院大学 GAKUSHUIN UNIVERSITY

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

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.

Secret key rate when the detection process is inaccessible to eavesdroppers

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

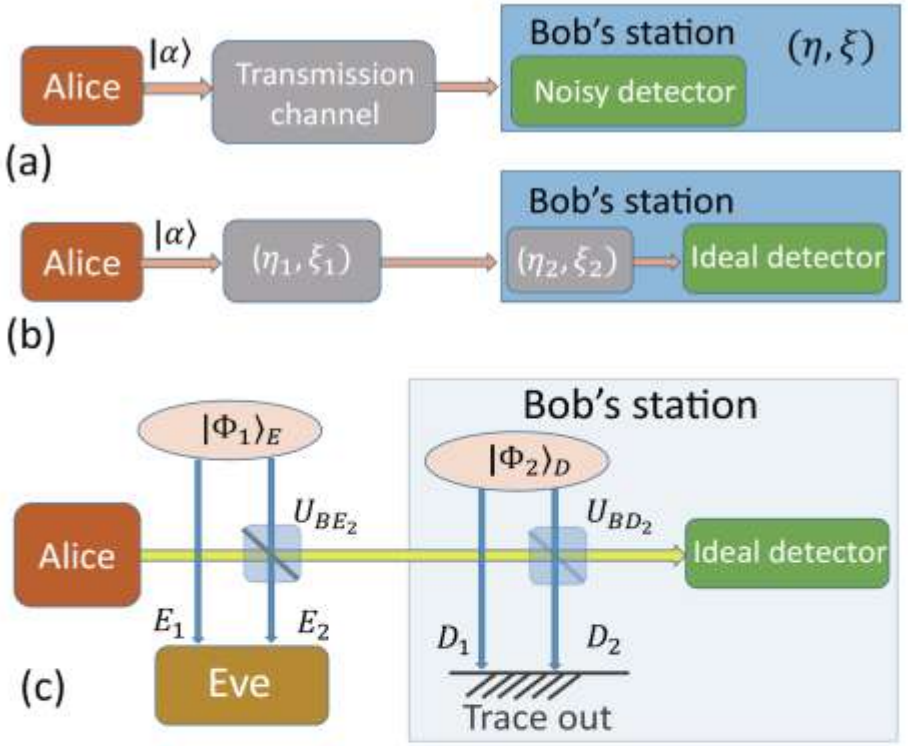
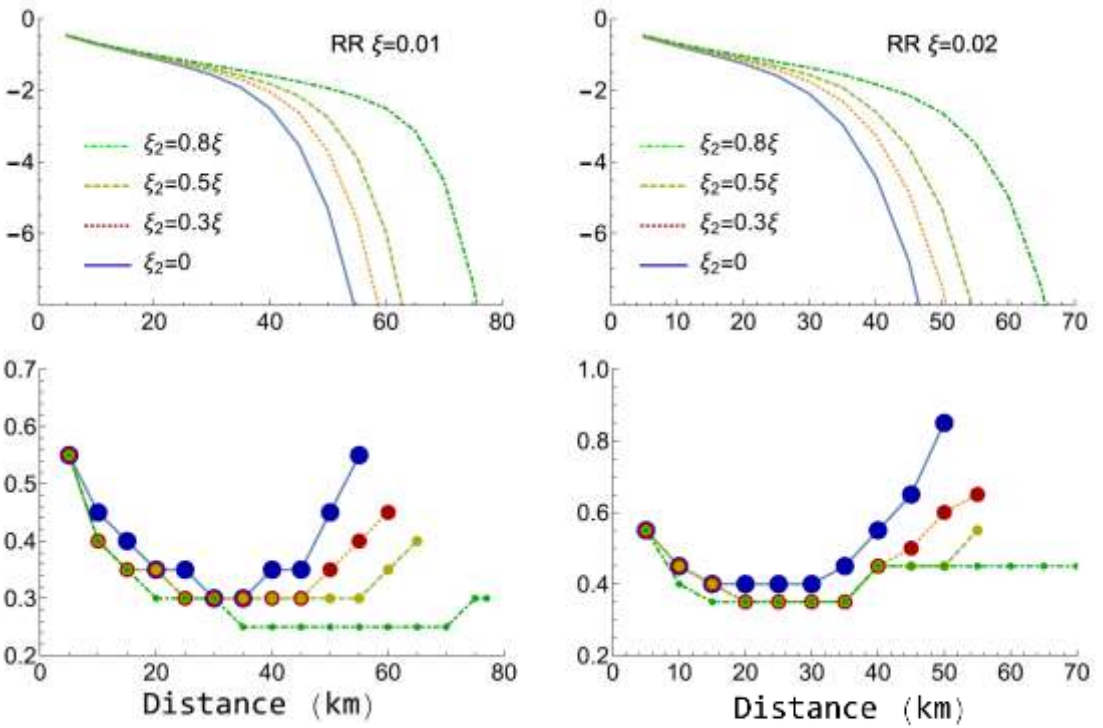


FIG. 1. (a) Alice sends a coherent state $|\alpha\rangle$ through a lossy and noisy channel. Bob observes quadrature with the total transmission η and the total excess noise ξ. (b) The transmission channel is modeled by a lossy and noisy Gaussian channel with the transmission η_1 and the excess noise 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_2} and U_{BD_2} 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.

nature COMMUNICATIONS

ARTICLE

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

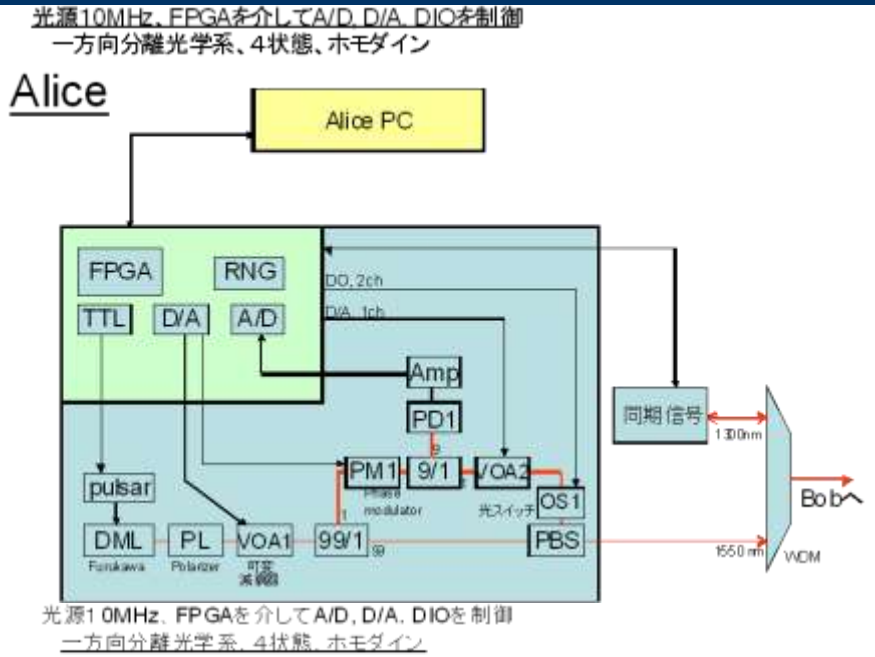
Finite-size security of continuous-variable quantum key distribution with digital signal processing

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

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.

Compact and low cost CV-QKD system

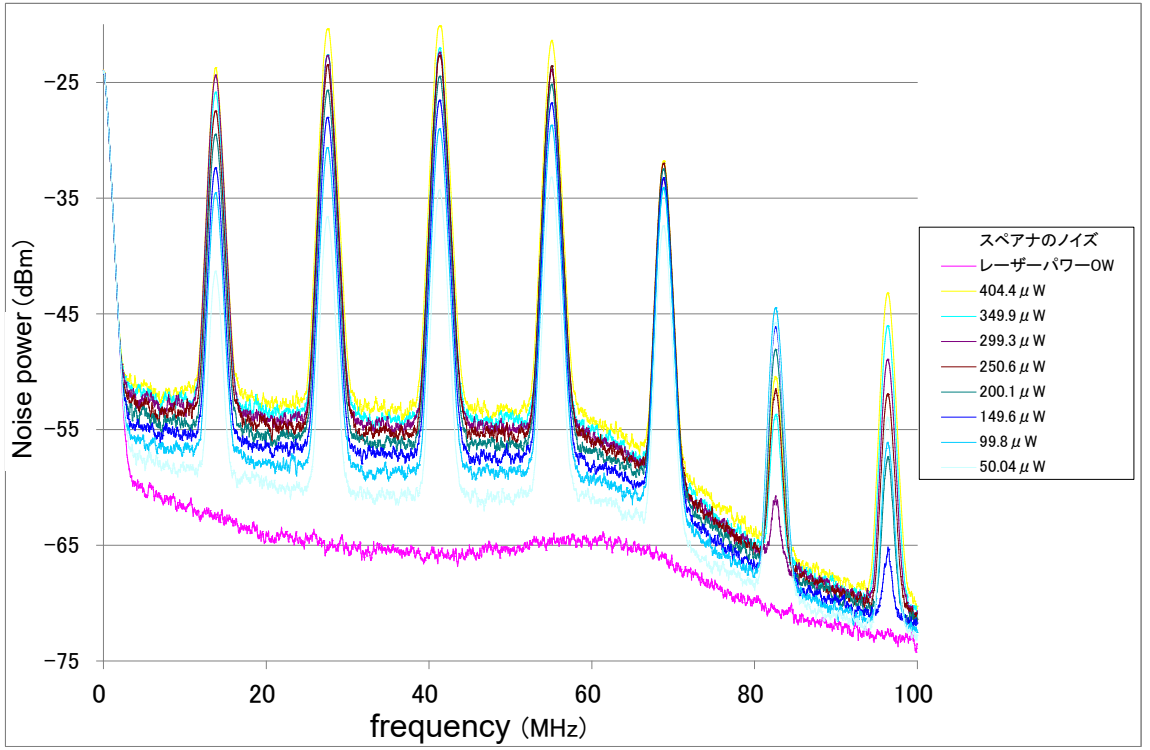
学習院大学 GAKUSHUIN UNIVERSITY

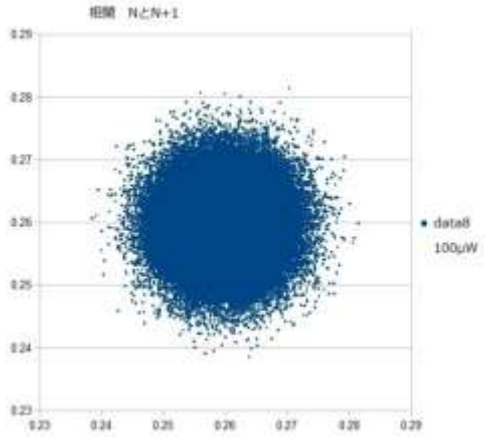


- 10MHz operation
- Capable of auto calibration and adjustment: the system includes variable optical attenuators (VOAs), optical switches (OSs) and optical receivers.

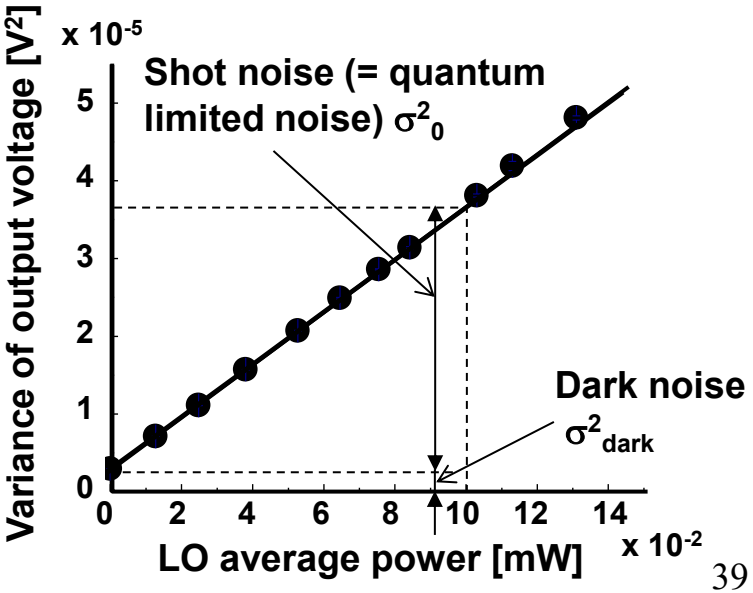
TH *et al*. Quantum Science and Technology, 2, 024010 (2017).

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





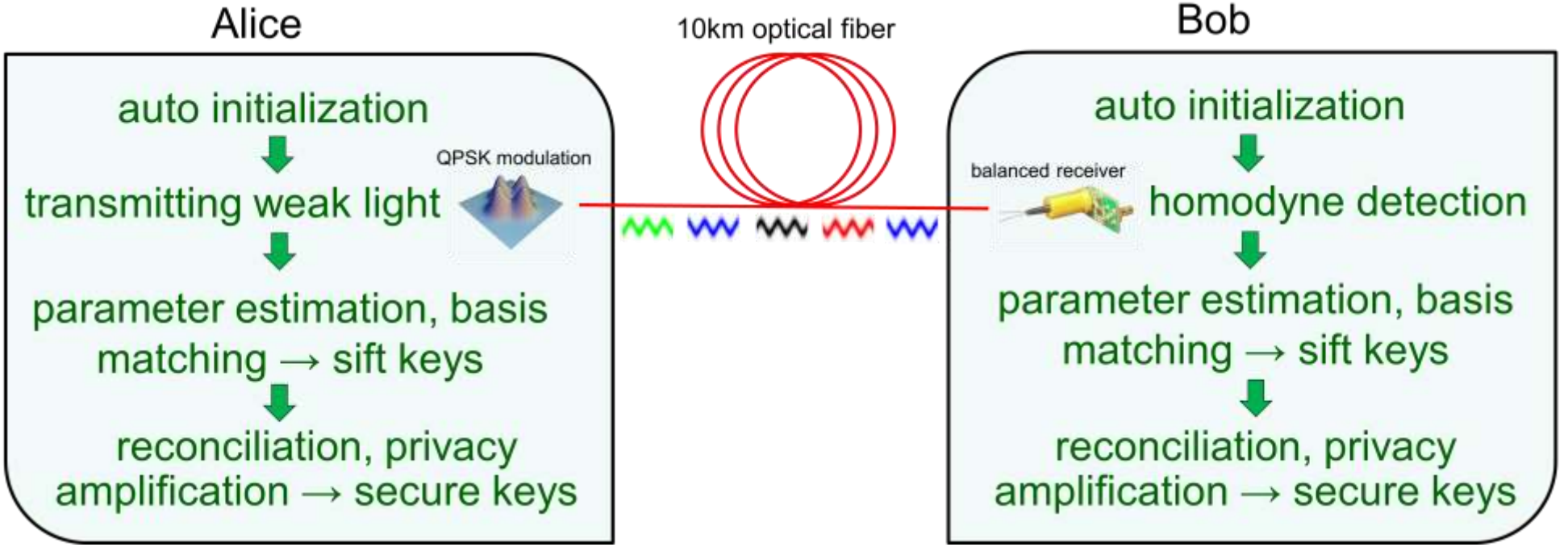
Excess noise due to detector ($\sigma^2_{dark}/\sigma^2_0$)
$\sigma^2_{dark}/\sigma^2_0$ ~ 0.1 for P_{LO}=0.1 mW



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

Compact and low cost CV-QKD system

学習院大学 GAKUSHUIN UNIVERSITY



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

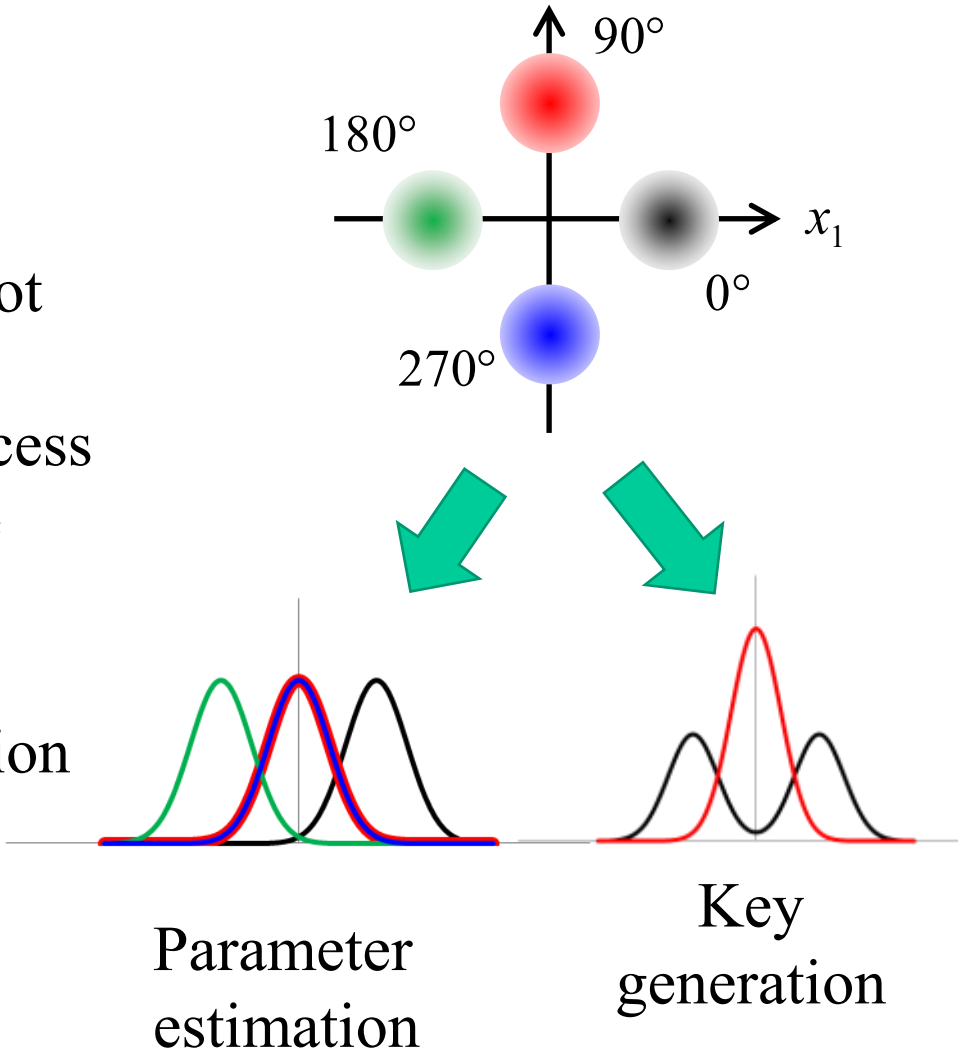
$$\begin{bmatrix} t_0 & t_1 & \cdots & t_{n-1} \\ t_{-1} & t_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & t_1 \\ t_{-(n-1)} & \cdots & t_{-1} & t_0 \end{bmatrix}$$

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

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.



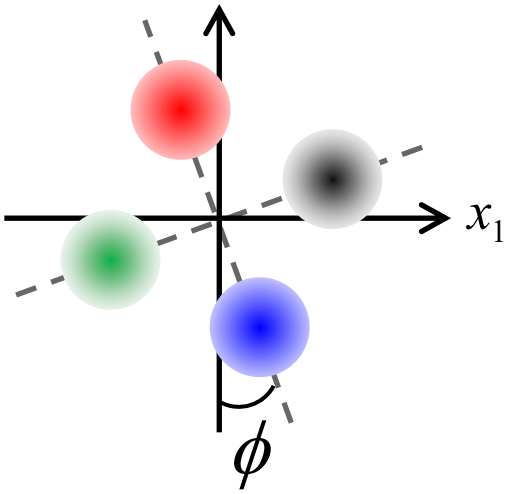
Post-selection and parameter estimation

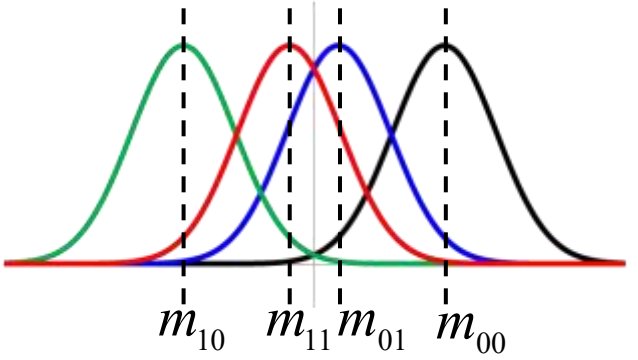
学習院大学 GAKUSHUIN UNIVERSITY

phase offset between Alice's and Bob's delay

$$\phi_{ij} = \arccos(m_{ij} / A)$$

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



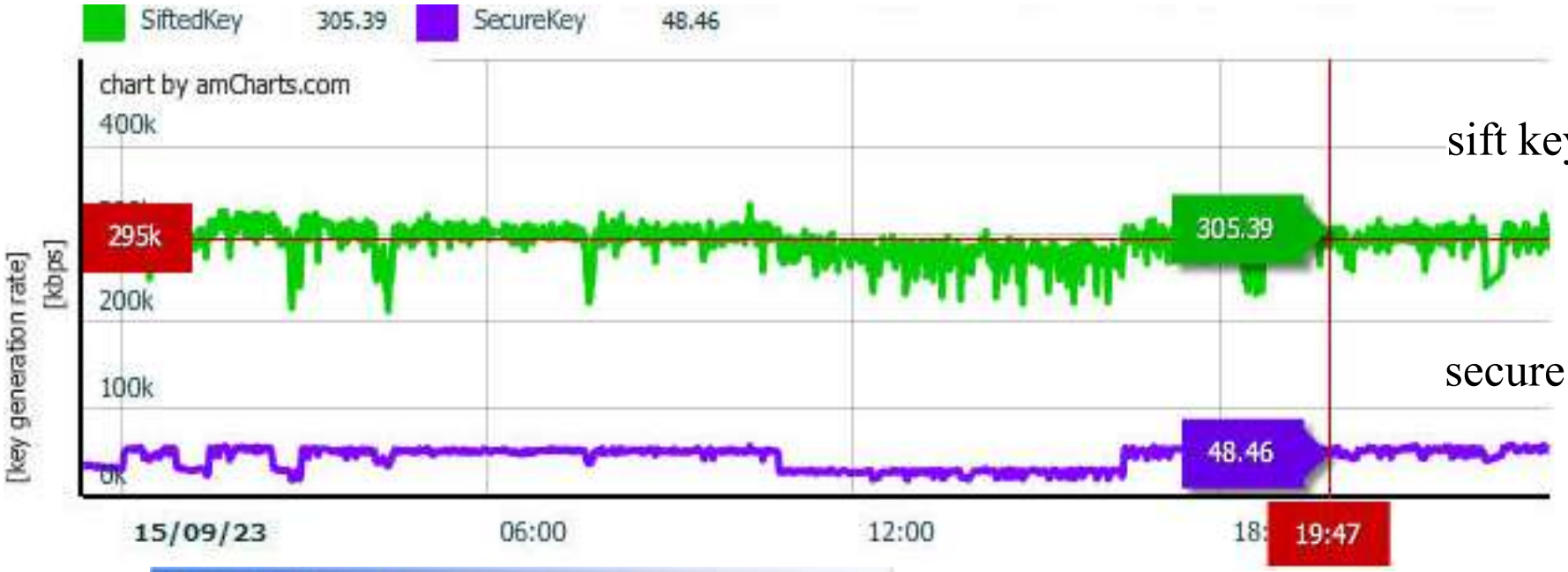



```
bob_phase_adjust: m_[00,01,10,11] = [+0.038107931987991, +0.021432066138954, +0.003387569686
bob_phase_adjust: m_bar    = +0.020777559294819          (a) m_bar=(m_[00]+m_[01]+m_[10]+m_[11]
bob_phase_adjust: (b) m'_[ij]=m_[ij]-m_bar
bob_phase_adjust: m'_[00,01,10,11] = [+0.017330372693171, +0.000654506844134, -0.017389983608
bob_phase_adjust: m_A      = +0.017371468410912          (c) m_A=(m'_[00]^2+m'_[01]^2+m'_[10]^2
bob_phase_adjust: c'_[00,01,10,11] = [+0.068798769709509, -0.037886036676260, +0.000000000000
bob_phase_adjust: c'_bar             = -0.035184183305470
bob_phase_adjust: w(file read)    = +4950.000000000000000    (d) w  = /opt/nec/mql000_manager/
bob_phase_adjust: xZ(file read)   = +1064.108325899193233    (d) xZ = /opt/nec/mql000_manager/
bob_phase_adjust: offset   = -55.437393247996930           (d) offset = c'_bar / Pi * w
bob_phase_adjust: xZ   = +1008.670932651196267             (d) xZ = xZ + c'_bar / Pi * w
bob_phase_adjust: xZ(file write) = +1008.670932651196267(OK)
bob_phase_adjust: xH(file write) = +3483.670932651196381(OK)
s_var_debug_print: c_1      = 0.040000000000000
s_var_debug_print: n_[00]   = 125356
s_var_debug_print: n_[01]   = 124780
s_var_debug_print: n_[10]   = 125660
s_var_debug_print: n_[11]   = 125507
s_var_debug_print: N        = 501303
s_var_debug_print: m_[00]   = +0.038107931987991
s_var_debug_print: m_[01]   = +0.021432066138954
s_var_debug_print: m_[10]   = +0.003387569686372
s_var_debug_print: m_[11]   = +0.020182669365961
s_var_debug_print: v_[00]   = +0.000179509951050
s_var_debug_print: v_[01]   = +0.000187263160210
s_var_debug_print: v_[10]   = +0.000177024618644
s_var_debug_print: v_[11]   = +0.000188359917337
```

Continuous operation over 10 km fibre

学習院大学 GAKUSHUIN UNIVERSITY

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



sift key rate

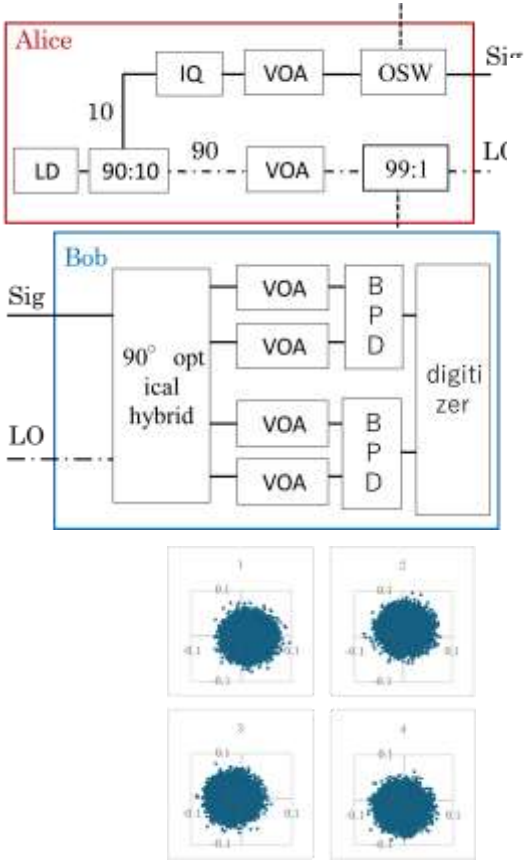
secure key rate

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

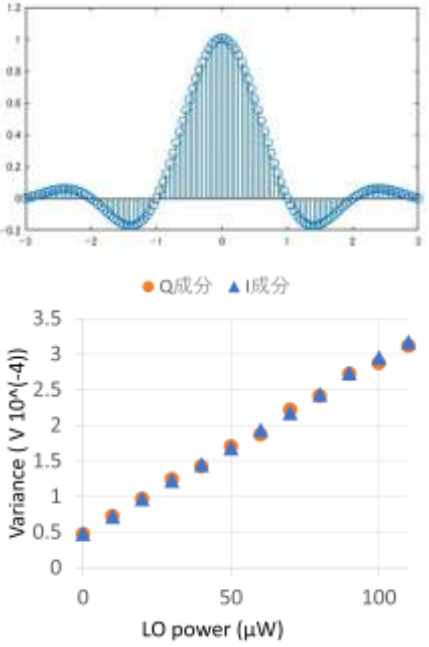
Our R&D on CV-QKD

MIC Project "R&D for building a global quantum cryptography communication network"
Joint research with NEC and NICT

Type C
IQ modulation using a root-raised-cosine filter and signal-processing using the same filter.

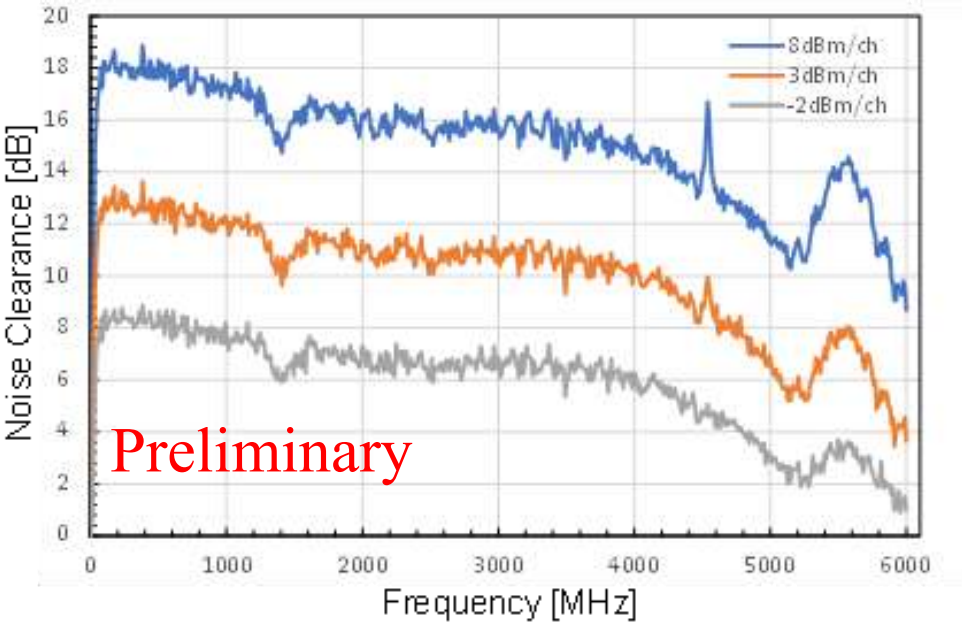


Root-raised-cosine filter



Low noise and high efficiency CV-QKD is possible.

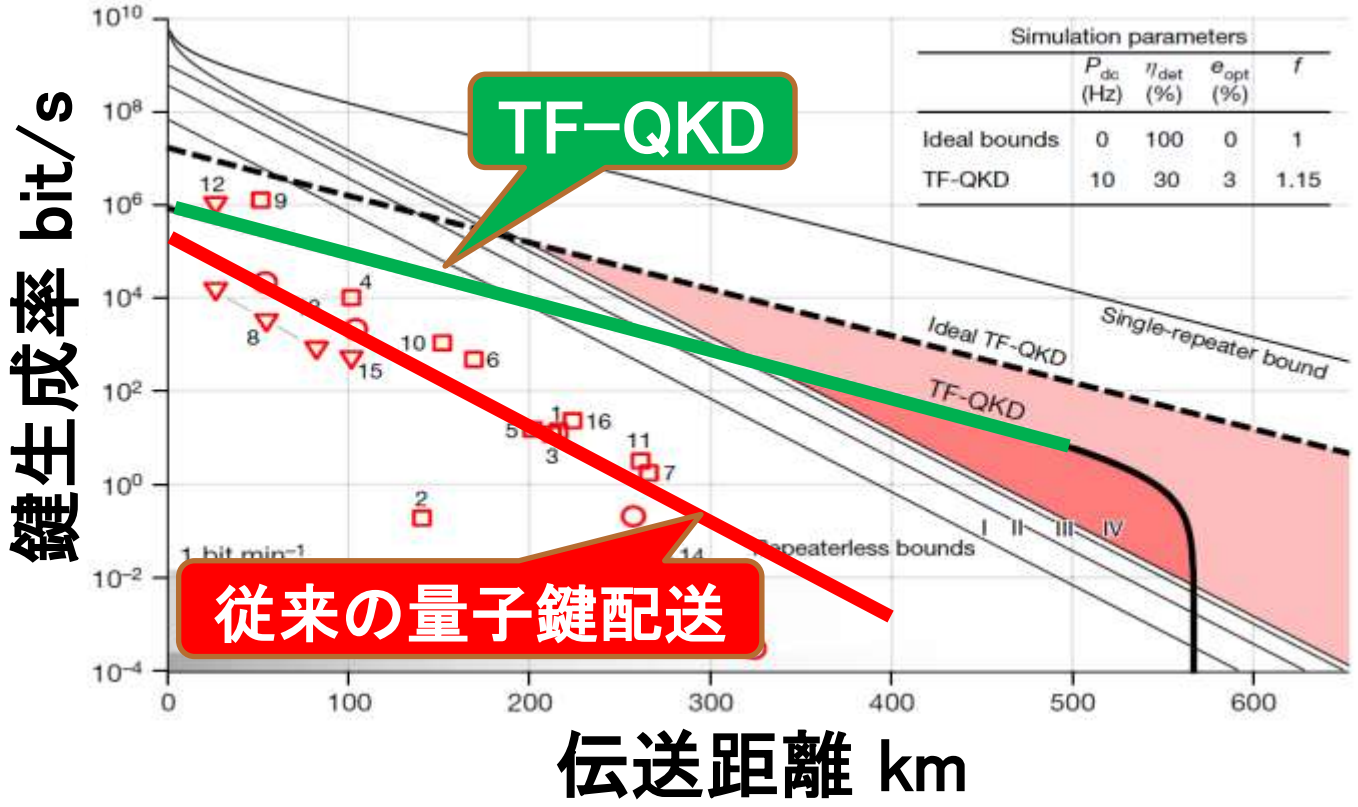
Development of high-speed low-noise homodyne receiver



Trimatiz Limited
https://www.trimatiz.com/en/

Twin-Field Quantum Key Distribution (TF-QKD)

M. Lucamarini, *et al.* Nature 557, 400–403 (2018).



従来のQKD
鍵生成率∝透過率

TF-QKD
鍵生成率∝(透過率)$^{1/2}$

Twin-Field Quantum Key Distribution (TF-QKD)

TF-QKDの歴史

東芝ケンブリッジによるTF-QKDの提案

M. Lucamarini, Z. L. Yuan, J. F. Dynes & A. J. Shields, Nature 557, 400 (2018).

一般的な安全性の証明

Tamaki, et al., https://arxiv.org/abs/1805.05511 (2018).

Ma, X., et al., Phys. Rev. X 8, 031043 (2018).

プロトコルの改良

Phase-matching protocol: Lin, J. et al., Phys. Rev. A 98, 042332 (2018).

Sending-or-not-sending protocol: Yu, Z.-W., et al., Sci. Rep. 9, 3080 (2019).

実験

中国による509km: Chen, J.-P. et al., Phys. Rev. Lett. 124, 070501 (2020).

東芝による600km: M. Pittaluga, et al., Nat. Photonics 15, 530 (2021).

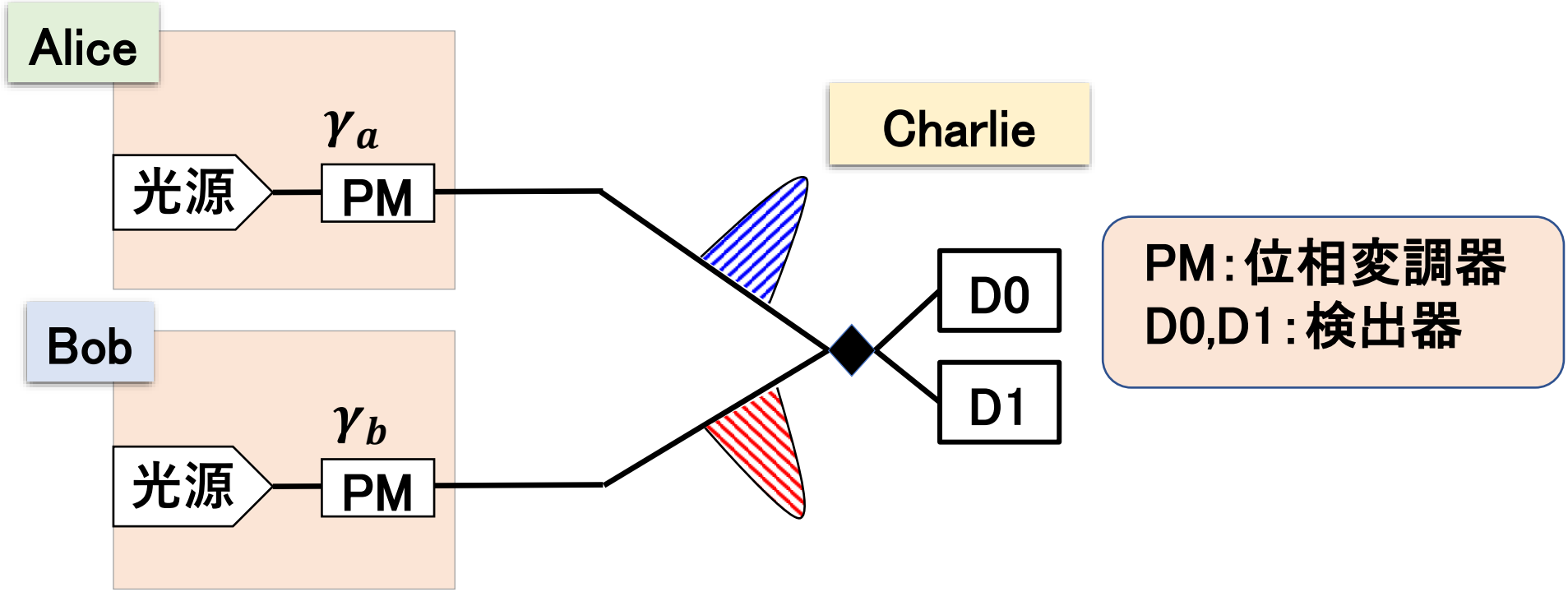
中国による敷設511km: J.-P. Chen, et al., Nat. Photonics 15, 570 (2021).

中国による830km: Shuang Wang, et al., Nat. Photonics 16, 154 (2022).

中国による1000km: Yang Liu, et al., Phys. Rev. Lett. 130, 210801 (2023).

TF-QKDプロトコルの概要

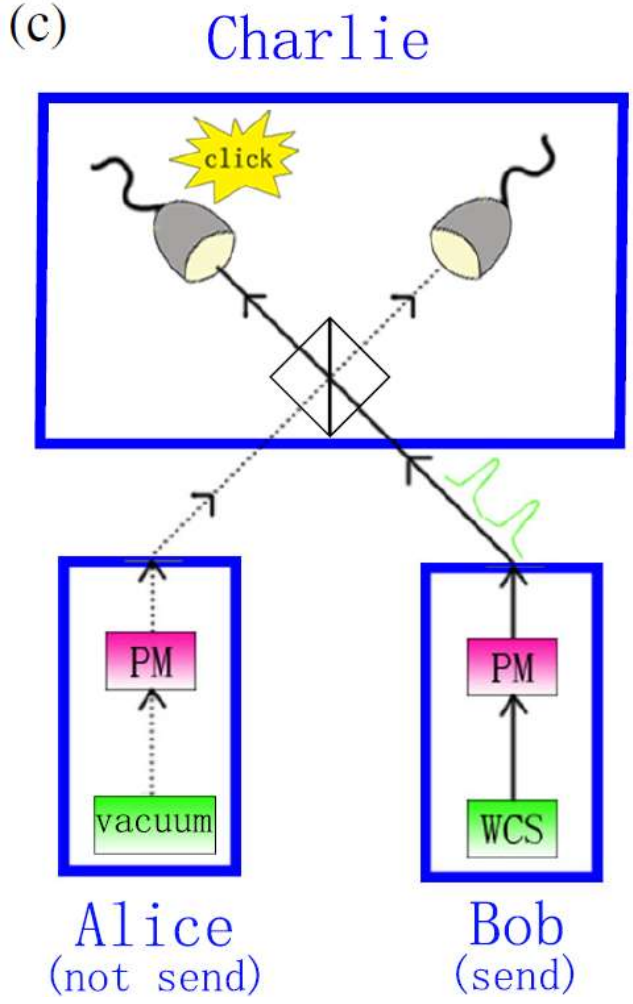
- AliceとBobは光源を持つ
- 第三者のCharlieが2つの光子検出器を持つ



- AliceとBobはレーザー光を単一光子レベルに減衰させる。
- 光源から出たパルスに、位相変調γ_a, γ_bを与えてCharlieに送信する。

Sending-or-not-sending protocol

Wang, Yu, Hu, PRA 98, 062323 (2018).



シグナル送受信（鍵をつくる）

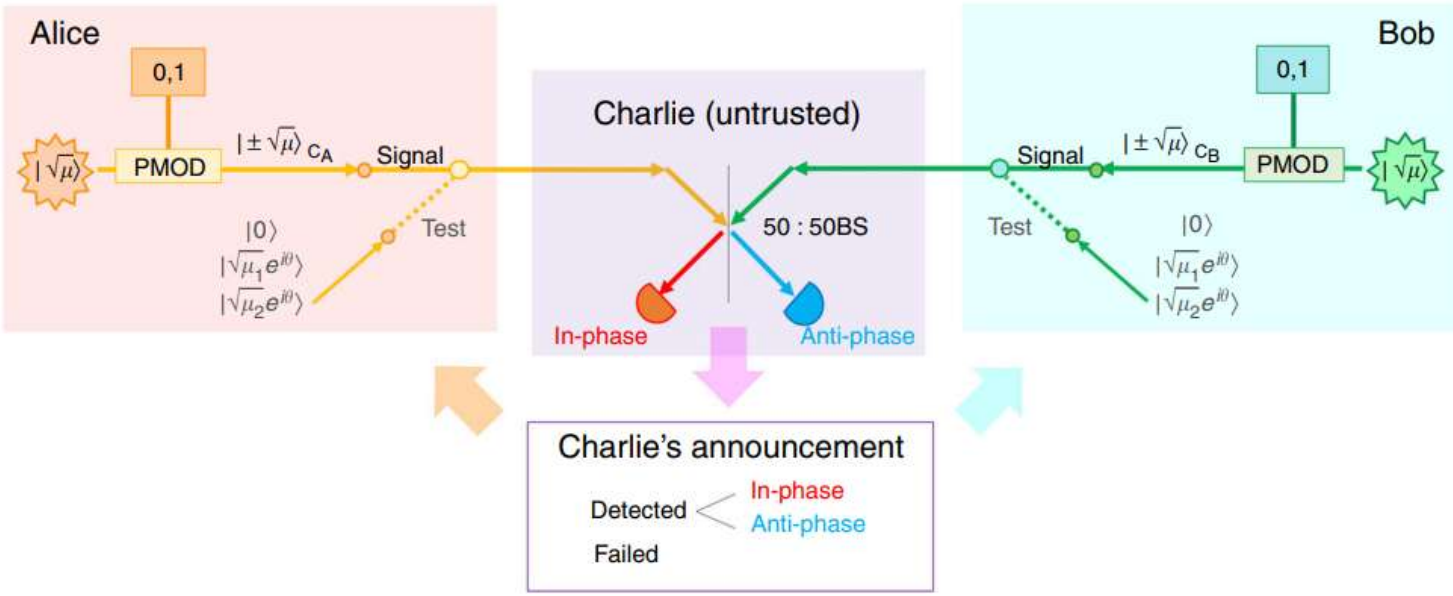
	Bit 0	Bit 1
Alice	微弱レーザー (位相ランダム、確率 ε)	光無 （確率 1-ε)
Bob	光無 （確率 1-ε)	微弱レーザー (位相ランダム、確率 ε)

テスト送受信（盗聴を見積もる）

- 3種類の強度のランダム位相の微弱レーザーを切り替えて送信
- $|\cos(\theta_A - \theta_B)| \sim 0$ のθ_A、θ_Bを事後選択する

Phase-matching protocol

Ma, Zheng, Zhou, PRX 8, 031043 (2018).



シグナル送受信（鍵をつくる）

位相ロックした微弱レーザー光を送信する

	Bit 0	Bit 1
Alice	$\|\sqrt{\mu}\rangle$	$\|-\sqrt{\mu}\rangle$
Bob	$\|\sqrt{\mu}\rangle$	$\|-\sqrt{\mu}\rangle$

テスト送受信（盗聴を見積もる）：同じ

Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Jiu-Peng Chen, *et al*., Nature Photonics **15**, 570–575 (2021).

Fig. 1 | Field deployment of SNS-TF-QKD. a, Satellite image indicating the SNS-TF-QKD experiment with field-deployed fibre between Qingdao (Alice, 36° 6' 13" N, 120° 24' 32" E) and Jinan (Bob, 36° 36' 50" N, 117° 6' 22" E). Independent lasers are used as a light source for encoding; superconducting nanowire single-photon detectors (SNSPDs) are used for detection in Mazhan (Charlie, 36° 0' 19" N, 118° 42' 35" E) in the middle of the link. Map data: Google, CNES/Astrium, DigitalGlobe. b,c, Experimental setup of Bob (b) and Alice (c). In Bob's/Alice's station, a commercial kilohertz continuous-wave fibre laser is locked to an ultra-low-expansion glass cavity as the light source. Then the frequency-locked stable laser is applied to accomplish encoding by two phase modulators and three intensity modulators. Finally the encoded light pulses are attenuated to the single-photon level using a passive attenuator and sent to the measurement station. AOM, acoustic-optic modulator; BS, beam splitter; PM, phase modulator; IM, intensity modulator; ATT, passive attenuator; HWP, half-wave plate; PBS, polarization beam splitter; QWP, quarter-wave plate; PD, photoelectric detector; PC, polarization controller. d, Experimental setup of Charlie. In Charlie's station, two electric polarization controllers (EPCs) are used to feed back the polarization of the pulses from Alice and Bob in real time, dense wavelength division multiplexers (DWDMs) are used to filter the leakage of classical communication in other fibres and the non-linear scattering from strong reference pulses, and circulators (CIRs) are used to block the reflection of the SNSPDs. e, Sectional view of a bundle of optical fibres in the field-deployed optical cable. Three of the bundle of 12 fibres are used in this experiment: one for single-photon-level signal transmission (the QKD link), one for clock synchronization and the 'start' signal (synchronization), and one for wavelength calibration to lock the optical frequency between Alice's and Bob's independent lasers (wavelength calibration). In addition to our experiment, classical communications are running in the other eight (classical communication) and one of the fibres is idle (idle link).

Long-distance coherent quantum communications in deployed telecom networks, Mirko Pittaluga, *et al*., Nature 640, 911-917 (2025).

Fig. 1 Deployed coherent quantum communications system. The TF-QKD system consists of three nodes: two transmitter nodes, Alice and Bob, and one receiver node, Charlie (called A, B and C, respectively). Bottom: equipment for nodes A, B and C was installed in three colocation data centres located in Frankfurt, Kehl and Kirchfeld alongside other running telecommunication equipment. All equipment was mounted in 19-inch telecom racks, and the 3 nodes were interconnected pairwise through 2 fibre duplexes. The A–C fibre duplex spans 156.7 km, with the 2 bundled fibres, F_Q^{AC} and F_C^{AC}, characterized by losses of 32.4 dB and 33.5 dB, respectively. The B–C duplex spans 97.2 km, with FQ BC and FC BC characterized by losses of 21.7 dB and 22.2 dB, respectively. Top: functional schematic of the subsystems installed in the three colocation centres, with equipment grouped into three layers spanning the three nodes based on their implemented functionality. COMMS, communications.

year	authors	Country	distance	fiber	protcol	note	Ref.
2018	M. Lucamarini, *et al.*	UK	550 km	spool	original	最初の提案	1
2020	J.-P. Chen, *et al.*	China	509 km	spool	SNS	有限長も考慮したSNSプロトコル	2
2021	M. Pittaluga, *et al.*	UK他	605 km	spool	CAL, SNS	2波長による位相安定化	3
2021	J.-P. Chen, *et al.*	China	511 km	deployed	SNS	済南-青島を結ぶ敷設ファイバ	4
2022	S. Wang, *et al.*	China	833.8 km	spool	NPP	NPPプロトコルによる830km	5
2022	J.-P. Chen, *et al.*	China	658 km	spool	SNS	センシングも実装	6
2022	C. Clivati, *et al.*	Italy他	206 km	deployed	not implemented	イタリア北部の敷設ファイバ	7
2023	L. Zhou, *et al.*	China	615.6 km	spool	SNS	中間点にレーザを置かない実装	8
2023	Y. Liu, *et al.*	China	1002 km	spool	SNS	1000kmを超える距離	9
2024	J.-P. Chen, *et al.*	China	502 km	spool	SNS	中間点にレーザを置かない実装	10
2025	M. Pittaluga, *et al.*	UK他	254 km	deployed	SNS	ドイツの商用回線、APD	11
2024	Hao Dong, *et al.*	China	603 km	deployed	SNS	[10]+敷設ファイバ[4]	12

[1] Nature 557, 400–403 (2018). [2] Phys. Rev. Lett. 124, 070501 (2020). [3] Nature Photonics 15, 530–535 (2021). [4] Nature Photonics 15, 570–575 (2021). [5] Nature Photonics 16, 154–161 (2022). [6] Phys. Rev. Lett. 128, 180502 (2022). [7] Nature Commun. 13, 157 (2022). [8] Nature Commun. 14, 928 (2023). [9] Phys. Rev. Lett. 130, 210801(2023). [10] Phys. Rev. Lett. 132, 260802 (2024). [11] Nature 640, 911–917 (2025). [12] Phys. Rev. Applied 22, 064057 (2024).

まとめ

- 量子暗号とは何か(歴史)、どこが面白いのか（個人的）
  - 1970年頃　Wiesner 量子力学の基本的な原理を使うアイデア
  - 信頼し合ったり、しなかったりする複数の登場人物ができること
- 量子暗号の現在地
  - 量子暗号は最も早く実利用されると期待されてきた量子技術
  - 実験・理論ともに急速に研究が進展 地上2000km、衛星12,900km
  - NSA等によるネガティブなコメント
- 量子鍵配送の実験について
  - 連続量QKD：将来はコヒーレント光通信と融合、コストの優位性
  - TF-QKD：長距離の鍵配送が可能、測定装置を信頼しなくてもよい

エンタングルメントが隠れた主役