Continuous-Variable Quantum Cryptography with Entanglement in the Middle

Christian Weedbrook,
University of Toronto

Phys. Rev. A 87, 022308 (2013)

INVESTMENTS IN EDUCATION DEVELOPMENT

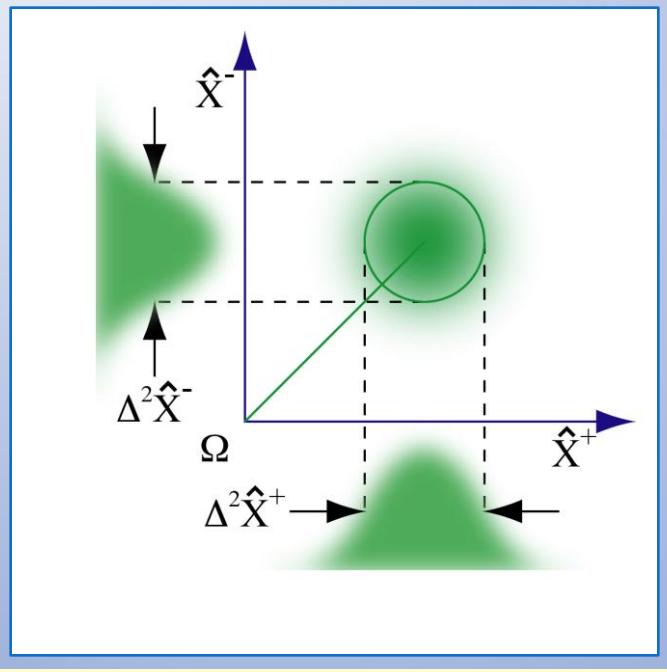
Outline of Talk

1. Quantum Information using Continuous Variables
2. Quantum Cryptography
3. Continuous-Variable QKD
4. Error Correction Protocols
5. QKD with Entanglement in the Middle
6. Results
7. Conclusion

Quantum Information using Continuous Variables

Quantum Harmonic Oscillator

$$\hat{H} = \frac{1}{2}(\hat{x}^2 + \hat{p}^2) \qquad [\hat{x}, \hat{p}] = i\hbar$$



CONTINUOUS VARIABLES:

- Many photons: laser beam
- Annihilation and creation operators used

$$\hat{a} = \frac{1}{\sqrt{2\hbar}}(\hat{x} + i\hat{p}) \qquad [\hat{a}, \hat{a}^\dagger] = 1$$

- Quadratures (x,p) are used:

$$\hat{x} = \sqrt{\frac{\hbar}{2}}(\hat{a} + \hat{a}^\dagger) \qquad \hat{p} = \sqrt{\frac{\hbar}{2}}i(\hat{a}^\dagger - \hat{a})$$

- Phase space is commonly used.

Applications:
- Teleportation
- Dense coding
- Quantum Cryptography
- Quantum Computation
- Cloning

Van Loock and Braunstein, Reviews of Modern Physics **77**, 513 (2005).

Quantum Information using Continuous Variables

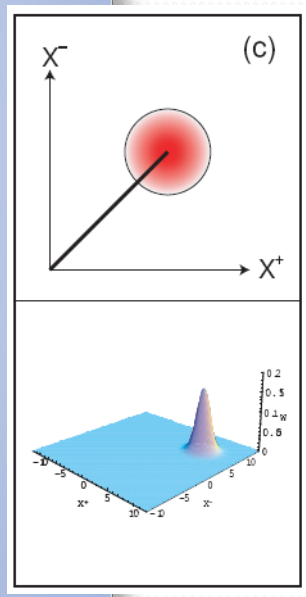
Coherent State

$$|\alpha\rangle = \hat{D}\,|0\rangle$$

$$\hat{D} = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$$

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$$

$$|\alpha\rangle = \exp(-\frac{1}{2}|\alpha|^2)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle$$

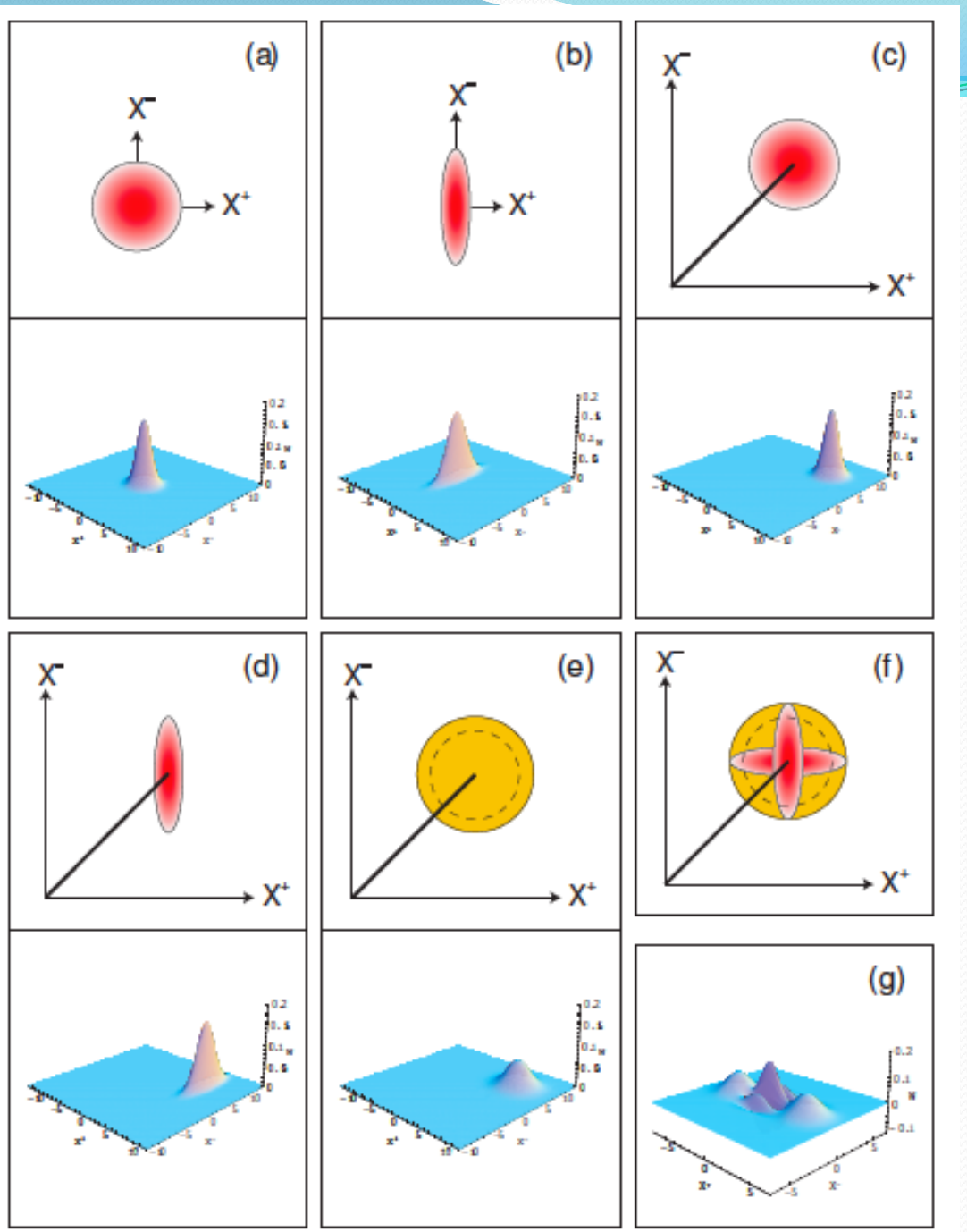


GAUSSIAN STATES:

- Examples of CV states: coherent states, squeezed states, Cat states, EPR states and thermal states.
- Simpler laser: coherent state.
- Offers advantages in e.g. detection efficiency and preparation of the states (QKD).

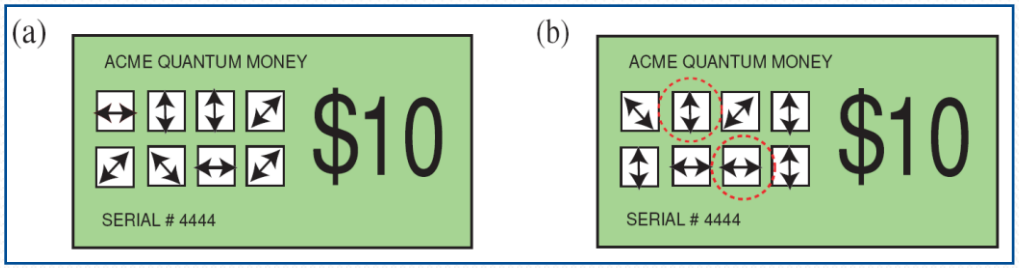
E.g., of non-Gaussian :
• Universal Quantum Computation
• Entanglement distillation

Weedbrook, Pirandola, et al., Reviews of Modern Physics 84, 621 (2012).


(a)
X⁻
X⁺
(b)
X⁻
X⁺
(c)
X⁻
X⁺
(d)
X⁻
X⁺
(e)
X⁻
X⁺
(f)
X⁻
X⁺
(g)

Quantum Cryptography

- Better way to describe it: Quantum key distribution (QKD).
- Security is due to the no-cloning theorem.
- Eavesdropper's presence is known: disturbs the system.
- First protocol was developed in 1984 by Charles Bennett and Gilles Brassard.
- From an initial idea by Stephen Wiesner: quantum money!



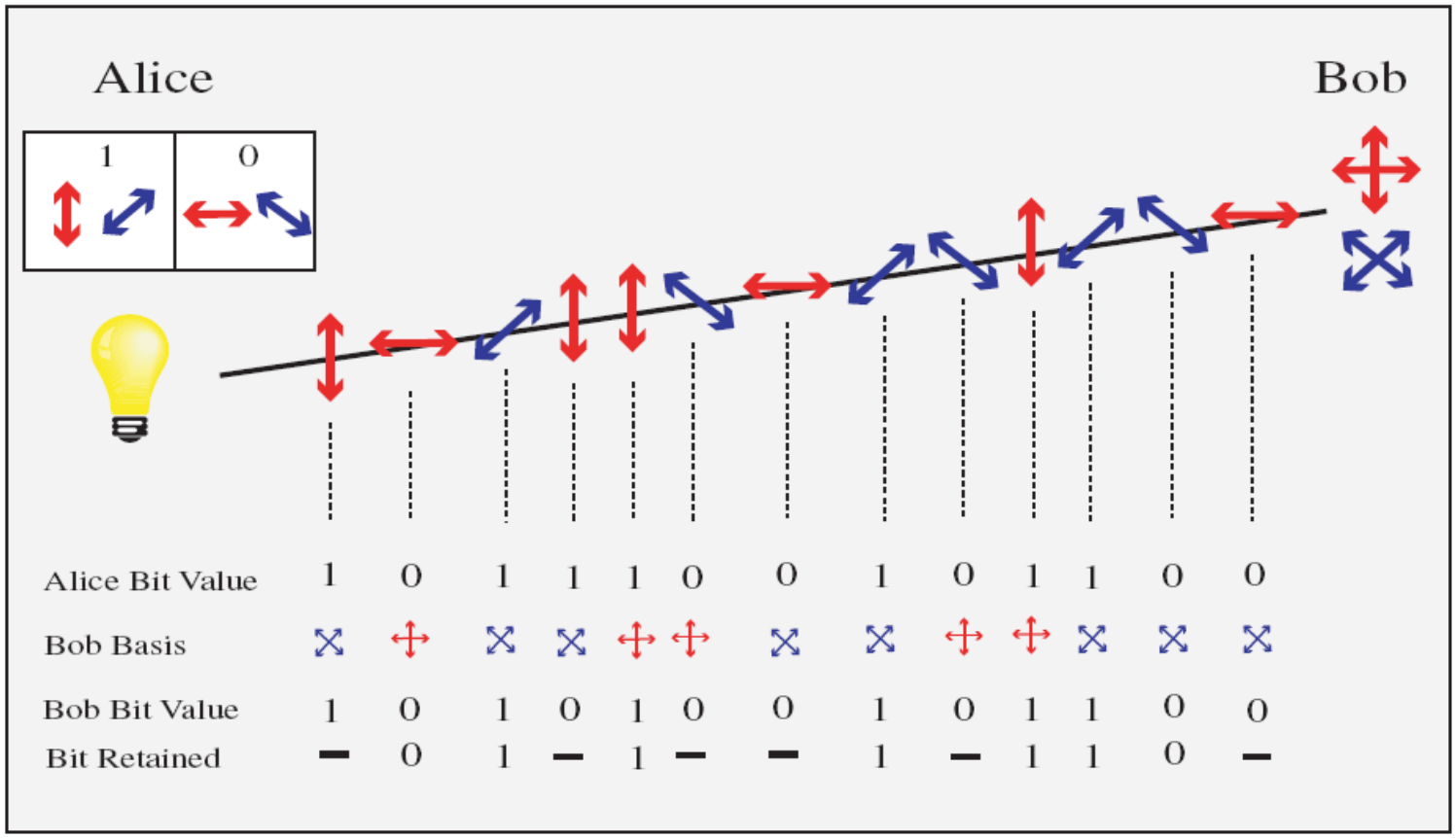
Quantum Cryptography

II. A BEAUTIFUL IDEA

The idea of quantum cryptography was first proposed in the 1970s by Stephen Wiesner[2] (1983) and by Charles H. Bennett of IBM and Gilles Brassard of The University of Montréal (1984, 1985).[3] However, this idea is so simple that any first-year student since the infancy of quantum mechanics could actually have discovered it!

N.Gisin et al., Reviews of Modern Physics, 74, 145 (2002).

The BB84 Protocol



Bennett and Brassard, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984).

Who is Working on CV-QKD Globally?

- UQ/ANU (Australia)
- MIT (USA)
- Olomouc (Czech Repubic)
- Beijing/Hefei (China)
- IQC/ University of Waterloo (Canada)
- Max-Planck-Institute (Germany)
- QuIC (Belgium)
- Laboratoire Charles Fabry (France)
- Telecom ParisTech (France)
- University of York (UK)
- Gakushuin University (Tokyo)

PRL 102, 180504 (2009) PHYSICAL REVIEW LETTERS

Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key with Discrete Modulation

Anthony Leverrier

Institut Telecom/Telecom ParisTech, CNRS LTCI, 46, rue Barrault, 75634 Paris Cedex 13, Franc

Philippe Grangier

Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechniqu RD 128, 91127 Palaiseau Cedex, France

(Received 22 December 2008; published 6 May 2009)

VOLUME 93, NUMBER 17 PHYSICAL REVIEW LETTERS

Quantum Cryptography Without Switchi

Christian Weedbrook,[1] Andrew M. Lance,[1] Warwick P. Bowen,[1] Timothy C. Ralph,[2] and Ping Koy Lam[1]

[1]*Quantum Optics Group, Department of Physics, Faculty of Science, Australian Nationa*

[2]*Department of Physics, University of Queensland, St. Lucia, Queenslan*

(Received 18 May 2004; published 22 October 2004)

We propose a new coherent state quantum key distribution protocol that randomly switch between measurement bases. This protocol provides signifi rates with increased bandwidths than previous schemes that only make single q It also offers the further advantage of simplicity compared to all previous proto

PRL 98, 030503 (2007) PHYSICAL REVIEW LETTERS

Experimental Implementation of Non-Gaussian on a Continuous-Variable Quantum-Key-Distribut

Jérôme Lodewyck,[1,2] Thierry Debuisschert,[1] Raúl García-Patrón,[3] R Nicolas J. Cerf,[3] and Philippe Grangier[2]

[1]*Thales Research and Technologies, RD 128, 91767 Palaiseau C*

[2]*Laboratoire Charles Fabry de l'Institut d'Optique, CNRS UMR 8501, C Bâtiment 503, 91403 Orsay Cedex, France*

[3]*QuIC, École Polytechnique, CP 165, Université Libre de Bruxelles, 105*

(Received 2 June 2006; published 19 January 2007)

An intercept-resend attack on a continuous-variable quantum-key-distributio experimentally. By varying the interception fraction, one can implement a fa eavesdropper totally controls the channel parameters. In general, such attacks channel, and may also result in non-Gaussian output distributions. We implen measurements needed to detect these attacks, and evaluate experimentally the i to the legitimate users and the eavesdropper. The results are consistent with t attacks resulting from the security proofs.

PRL 95, 070501 (2005) PHYSICAL REVIEW LE

Non-Gaussian Cloning of Quantum Coher

N. J. Cerf,[1] O. Krüger,[2] P. Navez,[1] R. F. Werne

[1]*QUIC, Ecole Polytechnique, CP 165, Université Libre de B*

[2]*Institut für Mathematische Physik, Technische Universität Braunschweig, Me*

[3]*Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str*

(Received 7 October 2004; revised manuscript received 14 Decem

We consider the optimal cloning of quantum coherent states v figures of merit. While the latter is maximized by a Gaussian cloner clone fidelity for a symmetric 1-to-2 cloner is 0.6826, compared to can be realized with an optical parametric amplifier and certain nor show that the single-clone fidelity of the optimal 1-to-∞ cloner is 1/ and cannot be surpassed even with supplemental bound entangled

letters to nature

Quantum key distribution using gaussian-modulated coherent

R. Renner

Institute for Theoretical Physics, ETH Zurich, CH-8093 Zurich, Switzerland

J. I. Cirac

Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany

(Received 20 October 2008; published 19 March 2009)

We show that the quantum de Finetti theorem holds for states on infinite-dimensional systems, provided they satisfy certain experimentally verifiable conditions. This result can be applied to prove the security of

ARTICLES

tinuous-variable quantum cryptography
g two-way quantum communication

PIRANDOLA[1]*, STEFANO MANCINI[2], SETH LLOYD[1,3] AND SAMUEL L. BRAUNSTEIN[4]

ratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
i Fisica & CNISM, Università di Camerino, Camerino 62032, Italy
Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
Science, University of York, York YO10 5DD, UK

UMBER 11 PHYSICAL REVIEW LETTERS week ending 19 MARCH 2004

mitation for Continuous-Variable Quantum Cryptography using Coherent States

Ryo Namiki* and Takuya Hirano

rch Team for Photonic Quantum Information, Department of Physics, Gakushuin University, Mejiro 1-5-1, Toshima-ku, Tokyo 171-8588, Japan

Received 20 May 2003; revised manuscript received 8 January 2004; published 16 March 2004)

2005) PHYSICAL REVIEW LETTERS week ending 28 OCTOBER 2005

ing Quantum Key Distribution Using Broadband Modulated Coherent Light

[1] Thomas Symul,[1] Vikram Sharma,[1] Christian Weedbrook,[1,2] Timothy C. Ralph,[2] and Ping Koy Lam[1]

cs Group, Department of Physics, Faculty of Science, Australian National University, ACT 0200, Australia

[2]*Department of Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

(Received 31 March 2005; published 28 October 2005)

realize an end-to-end no-switching quantum key distribution protocol using continuous-wave ent light. We encode weak broadband Gaussian modulations onto the amplitude and phase atures of light beams. Our no-switching protocol achieves high secret key rate via a post-selection col that utilizes both quadrature information simultaneously. We establish a secret key rate of bits/s for a lossless channel and 1 kbit/s for 90% channel loss, per 17 MHz of detected bandwidth, ing individual Gaussian eavesdropping attacks. Since our scheme is truly broadband, it can ially deliver orders of magnitude higher key rates by extending the encoding bandwidth with -end telecommunication technology.

PHYSICAL REVIEW LETTERS 14 OCTOBER 2002

Variable Quantum Cryptography: Beating the 3 dB Loss Limit

Ch. Silberhorn,[1] T. C. Ralph,[2] N. Lütkenhaus,[1] and G. Leuchs[1]

für Moderne Optik, Universität Erlangen–Nürnberg, 91058 Erlangen, Germany

Quantum Computer Technology, University of Queensland, QLD 4072, Australia

(Received 11 April 2002; published 25 September 2002)

ate that secure quantum key distribution systems based on continuous variable can operate beyond the apparent 3 dB loss limit that is implied by the beam splitting limit was established for standard minimum uncertainty states such as coherent states.

PRL 101, 200504 (2008) PHYSICAL REVIEW LETTERS week ending 14 NOVEMBER 2008

Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography

Stefano Pirandola,[1] Samuel L. Braunstein,[2] and Seth Lloyd[1,3]

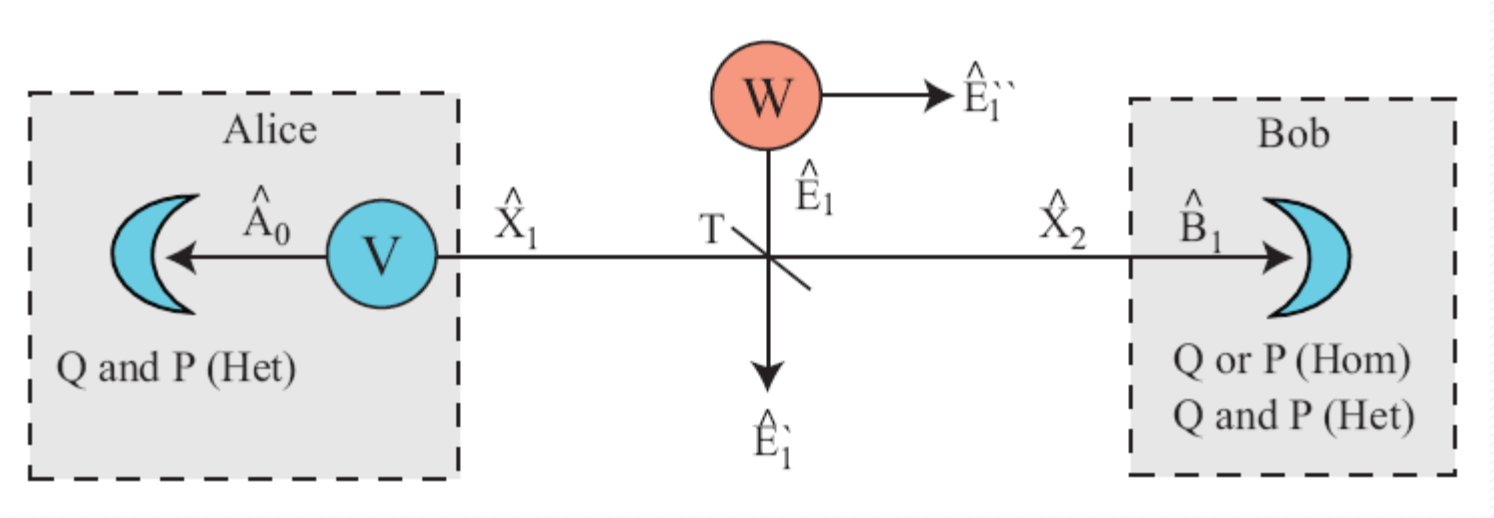
[1]*Research Laboratory of Electronics, MIT, Cambridge, Massachusetts 02139, USA*

[2]*Computer Science, University of York, York YO10 5DD, United Kingdom*

[3]*Department of Mechanical Engineering, MIT, Cambridge, Massachusetts 02139, USA*

(Received 5 June 2008; published 14 November 2008)

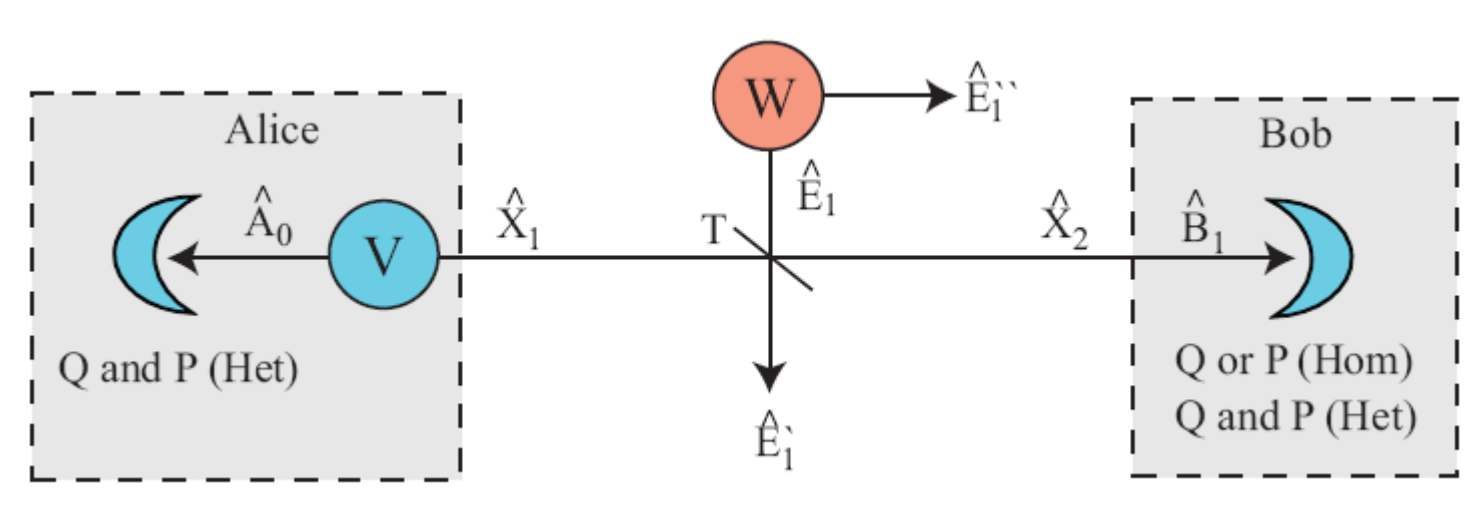
How a Typical CV-QKD Protocol Works



Alice:

- Alice controls the source!
- Modulates a pure vacuum state or squeezed state
- Chosen from a Gaussian distribution (x,p) with variance V centred at zero
- Sends a whole ensemble to Bob

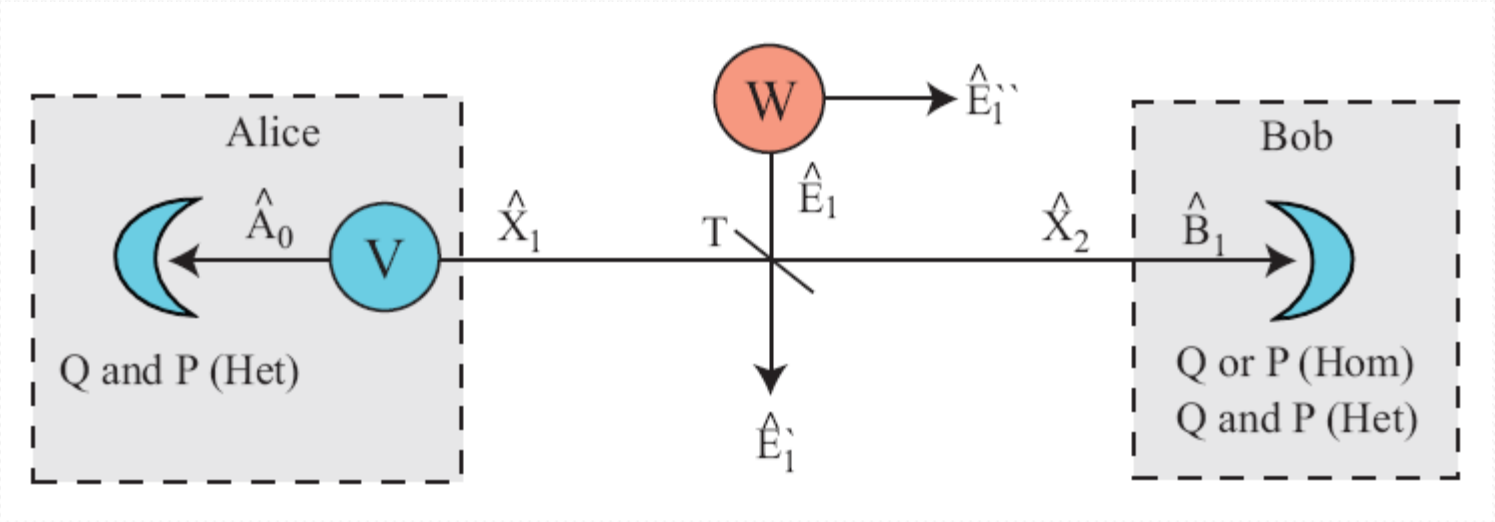
How a CV-QKD Protocol Works



Eve:

- Three possible types of attacks: individual, collective, coherent
- Replaces the quantum channel with her own channel.
- Uses a beam splitter to simulate attack.
- Gaussian attacks are optimal.
- Assume Eve is only constrained by laws of physics.

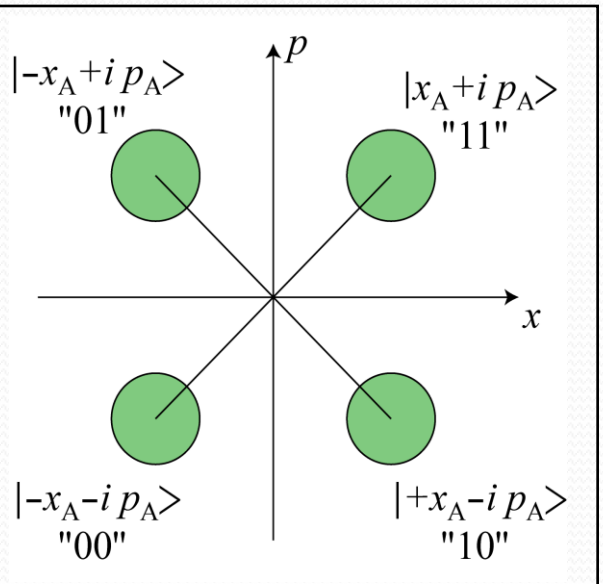
How a CV-QKD Protocol Works



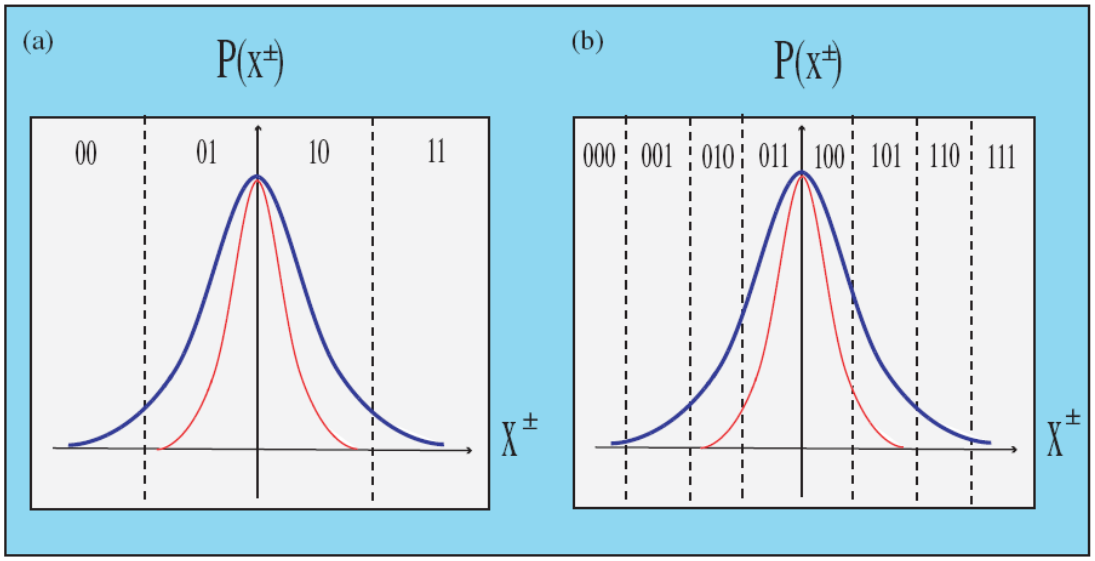
Bob:

- Measures all incoming states sent by Alice.
- Uses either homodyne (switching) or heterodyne detection (no-switching).

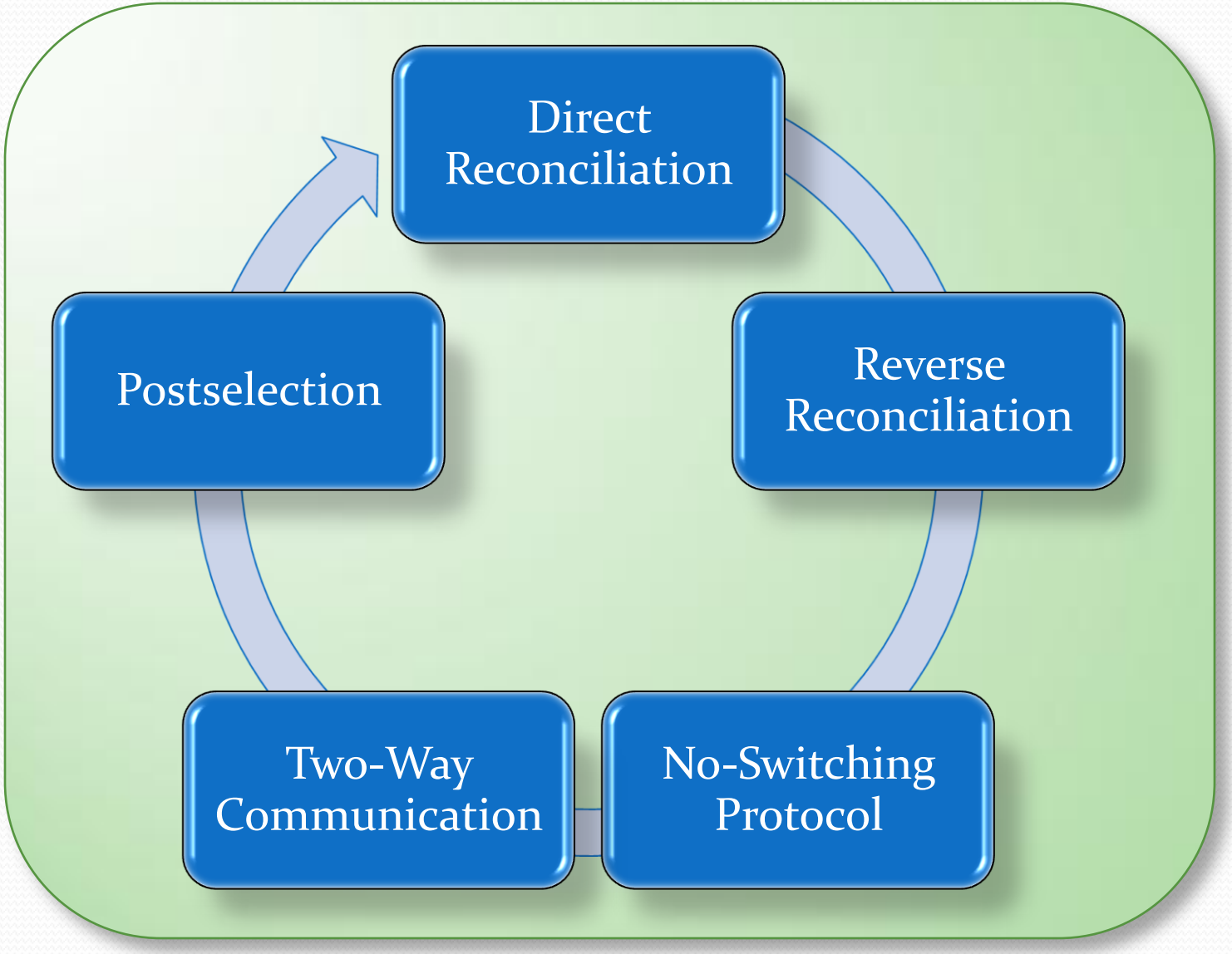
Encoding/Decoding Scheme



Binary Encoding of states



Some CV-QKD Protocols



Direct Reconciliation

Information Rates

$$R^{\blacktriangleright} := I(X_A : X_B) - I(X_A : E)$$

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A)$$

$$I(X_A : E) := S(E) - S(E|X_A)$$

BENEFITS:

- First CV-QKD protocol using coherent states with Gaussian distribution.
- No need for squeezed light.
- Bob and Eve guessing Alice encoding.

UMBER 5 PHYSICAL REVIEW LETTERS 4 FEB

Continuous Variable Quantum Cryptography Using Coherent States

Frédéric Grosshans and Philippe Grangier
Laboratoire Charles Fabry de l'Institut dOptique (CNRS UMR 8501), F-91403 Orsay, France
(Received 24 September 2001; published 16 January 2002)

Disadvantage
- 3 dB loss limit
- Alice and Bob need more information than Eve

Grosshans and Grangier, PRL, 88, 057902 (2002)

Direct Reconciliation

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A)$$

$$H(X_B) = \tfrac{1}{2}\log_2 V(X_B)$$

$$H(X_B|X_A) = \tfrac{1}{2}\log_2 V(X_B|X_A)$$

$$V_{X|Y} = \mathrm{Var}(X|Y) = \min_g \langle (Y - gX)^2 \rangle$$

$$I(X_A : E) := S(E) - S(E|X_A)$$

$$S(\rho) = \sum_{k=1}^{n} g(\nu_k)$$

where $g(\nu) := [(\nu + 1)/2]\log_2[(\nu + 1)/2] - [(\nu - 1)/2]\log_2[(\nu - 1)/2]$.

$$\nu = |i\mathbf{\Omega}\mathbf{V}|$$

$$\mathbf{\Omega} := \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}$$

Reverse Reconciliation

Information Rates

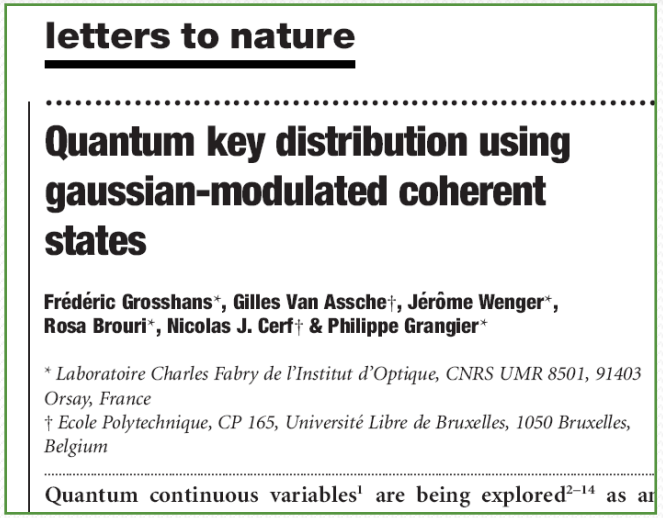
$$R^{\blacktriangleleft} := I(X_A : X_B) - I(X_B : E)$$

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A)$$

$$I(X_B : E) := S(E) - S(E|X_B)$$

BENEFITS:

- Still only using coherent states with Gaussian distribution.
- Beats the 3 dB loss limit.
- Secure for any value of line transmission – loss only.
- Alice and Eve guessing Bob's measurement results.



letters to nature

Quantum key distribution using gaussian-modulated coherent states

Frédéric Grosshans*, Gilles Van Assche†, Jérôme Wenger*, Rosa Brouri*, Nicolas J. Cerf† & Philippe Grangier*

** Laboratoire Charles Fabry de l'Institut d'Optique, CNRS UMR 8501, 91403 Orsay, France*
† Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium

Quantum continuous variables[1] are being explored[2–14] as ar

Grosshans et al., *Nature* **421**, 238 (2003).

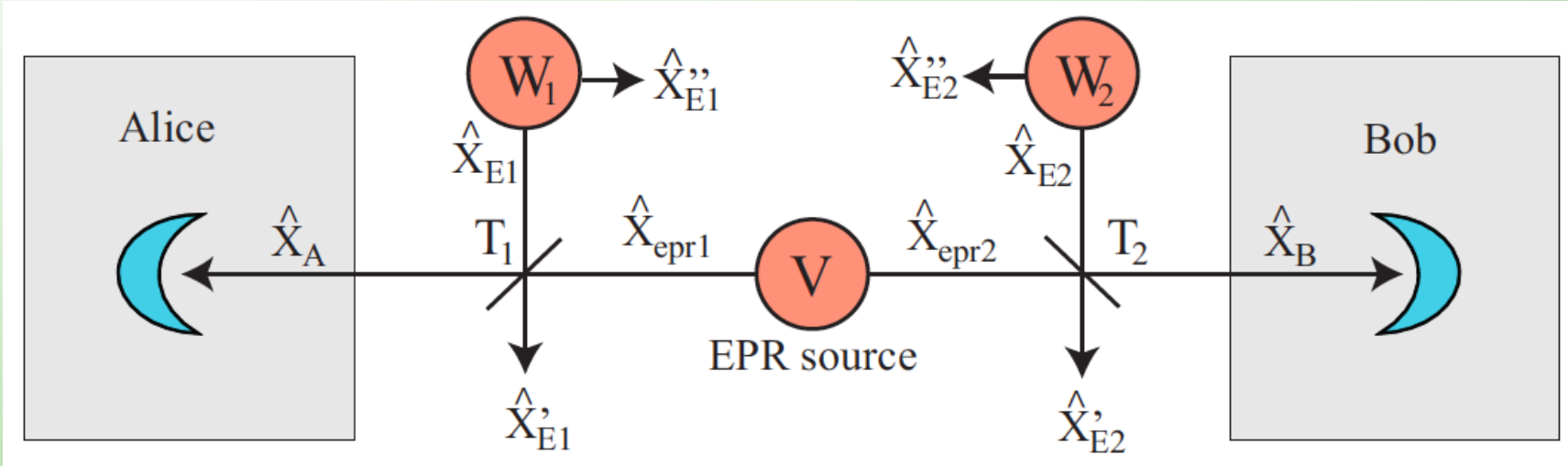
Entanglement-Based Picture of CV

- Two-mode squeezed state, shared by Alice and Bob.
- Alice does homodyne detection, Bob's collapses to a squeezed state.
- Alice does heterodyne detection, Bob's collapses to a coherent state.

$$\hat{X}_{epr1} = (\hat{X}_{s1} + \hat{X}_{s2})/\sqrt{2},$$
$$\hat{X}_{epr2} = (\hat{X}_{s1} - \hat{X}_{s2})/\sqrt{2}.$$

Quantum Cryptography with Entanglement in the Middle

- Typically in CVQKD Alice controls the source.
- Here Eve creates and distributes the resource for QKD to Alice and Bob from the middle.



Previous Works: Discrete Variables

Original EB-QKD:

- A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).

Security Proofs:

- H. -K. Lo and H. F. Chau, Science 283, 2050 (1999).
- D.Mayers and A. C. -C. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98), (IEEE Computer Society, Washington, DC, 1998), p. 503.
- A. Ac´ın, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).
- H. -K. Lo, M. Curty, B. Qi, arXiv:1109.1473 (2011).

Previous Works: Discrete Variables

Practical QKD Entangled Sources:

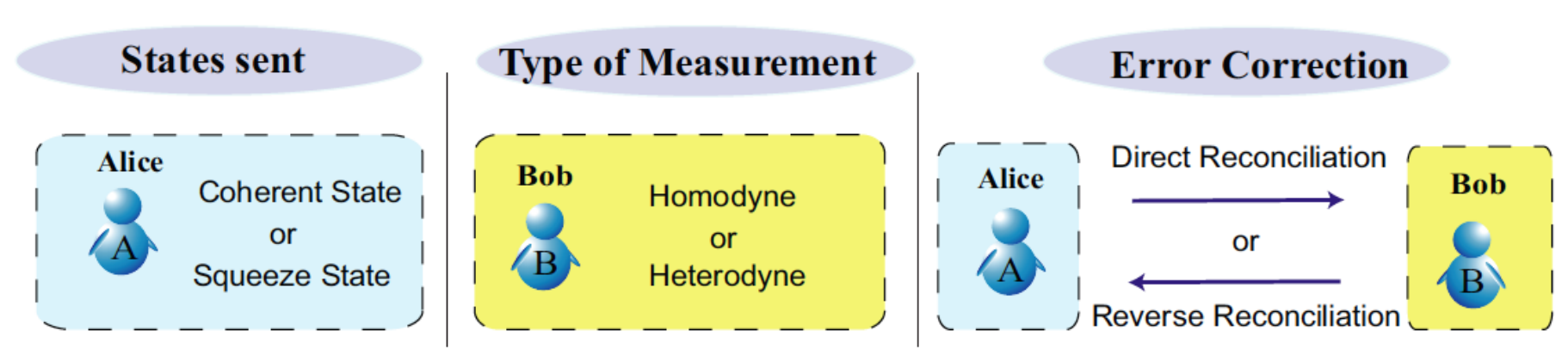
- E.Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A 65, 052310 (2002).
- X. Ma, C. -H. F. Fung, and H. -K. Lo, Phys. Rev. A 76, 012307 (2007).
- C. Erven, C. Couteau, R. Laflamme, and G. Weihs, arXiv:0807.2289 (2008).

BENEFITS:

- Tolerates higher amounts of loss.
- Can go longer distances.

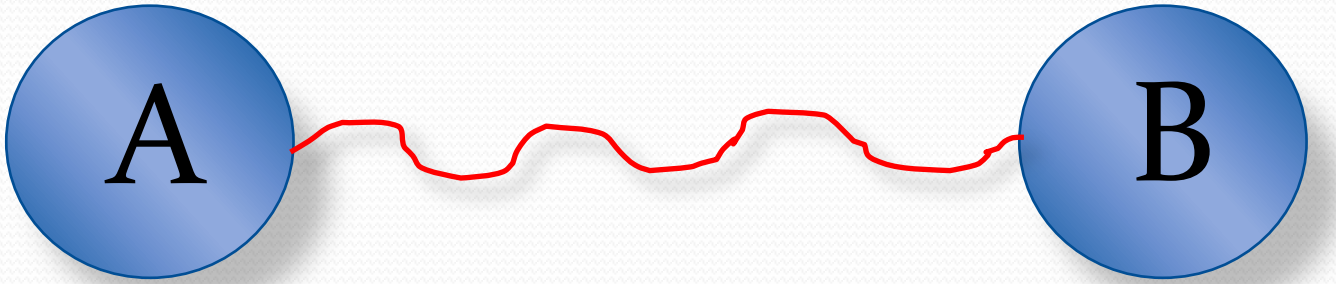
Does Continuous Variables Offer the Same Benefits?

Equivalences Between Error Correction Protocols…



A family of 8 protocols.

Equivalences Between Error Correction Protocols…



HOM: Squeezed
HET: Coherent

HOM: Squeezed
HET: Coherent

Direct and reverse are equivalent!

Equivalences Between Error Correction Protocols

- Coherent states and homodyne with direct (reverse) is the same as squeezed states and heterodyne with reverse (direct).
- Direct and reverse reconciliation are equivalent for squeezed states and homodyne and also for coherent states and heterodyne.

We can reduce the number of protocols we need to analyze!

Our Analysis!

Reverse Reconciliation

$$R^{\blacktriangleleft} := I(X_A : X_B) - I(X_B : E)$$

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A)$$

$$I(X_B : E) := S(E) - S(E|X_B)$$

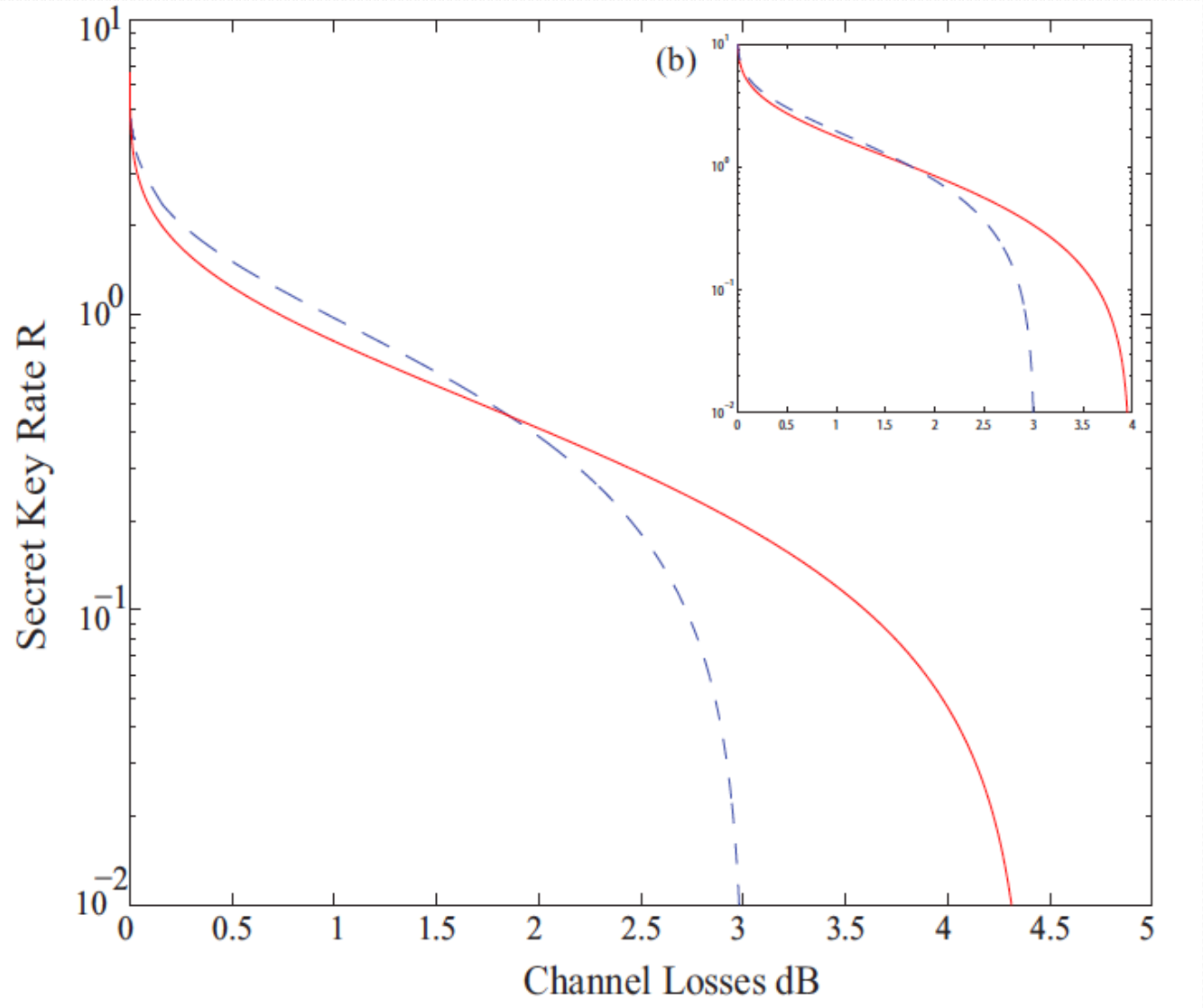
Direct Reconciliation

$$R^{\blacktriangleright} := I(X_A : X_B) - I(X_A : E)$$

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A)$$

$$I(X_A : E) := S(E) - S(E|X_A)$$

Weedbrook, Phys. Rev. A 87, 022308 (2013) .



Weedbrook, Phys. Rev. A 87, 022308 (2013).

Results

- By having the entanglement in the middle we can beat the 3dB loss limit for direct reconciliation.
- Using both coherent states and squeezed states.
- However, due to the equivalences we showed previously, this can alternatively be thought of as reverse reconciliation performing with excess channel noise.
- CVQKD: a secure key can still be generated even when the eavesdropper has control over the source.

Future Work

- Explore other CVQKD protocols such as postselection and two-way quantum communication to see how having entanglement in the middle affects their performance.
- Device independent CV-QKD?
- Measurement device independent CV-QKD?

Conclusion

- We considered what impact on the performance of CVQKD having an entangled state originating from Eve.
- We showed equivalences between the various protocols when entanglement is in the middle.
- Can beat 3dB loss limit for direct reconciliation, thereby tolerating higher loss.
- However in our equivalences this can be thought of as a poorly performing reverse reconciliation.
- CVQKD is still secure if Eve controls the source!

Thank you!