Institute for Theoretical Physics
Quantum Information Group

Leibniz Universität Hannover

Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks

Fabian Furrer
Leibniz Universität Hannover

PRL 109, 100502

Joint work with
T. Franz, R. F. Werner (Leibniz Universität Hannover)
M. Berta, A. Leverrier, V.B. Scholz, (ETH Zurich)
M. Tomamichel (CQT Singapore)

Qcrypt 2012, Singapore, 14.09.2012

Security of a QKD Protocol

Constraints:

- Information theoretic
- Experimental

-Key length
-Certification of security

Security Analysis

?

Experimental implementation

Secure Key

Minimizing the assumption and maximizing the key length!

Security of a QKD Protocol

Constraints:

- Information theoretic
  - Asymptotic key rate vs. finite uses of QM channel (finite-key effects)
  - Notion of security: composable?
  - Limitation on attacks: collective (tensor product) or coherent (general)?
  - ...
- Experimental / Implementation
  - Model of the measurement devices
  - Model of the quantum source
  - ...

Contribution: Security analysis for continuous variable (CV) protocol based on the distribution of **two-mode squeezed states** (EPR states) measured via **homodyne detection.**

Contribution: Security analysis for continuous variable (CV) protocol based on the distribution of **two-mode squeezed states** (EPR states) measured via **homodyne detection.**

What's New: Computation of key length secure against **coherent attacks** for achievable experimental parameters.

Security proof based on **Uncertainty relation**
(c.f. Tomamichel et al., Nat. Comm. 3, 634 ,2012)

Discrete Variables vs. Continuous Variables

Implementation

Discrete Variables	Continuous Variables
-Encoding in finite-dimensional systems (e.g., polarization of photon)	-Encoding in infinite-dimensional systems (bosonic modes) [1] -Gaussian States -Quadratures of EM-field: Homodyne or Heterodyne detection **Advantage:** - Compatible with **standard telecom technology** - high repetition rates for homodyne - efficient state preparation

[1] Weedbrook et al., Reviews of Modern Physics 84, 621 (2012)

Security Analysis for CV QKD Protocols

Challenge: infinite dimensions

Finite-Key Analysis:
- Leverrier et al, Phys. Rev. A 81, 062343 (2010)
- Berta, FF, Scholz, arXiv:1107.5460 (2011)

Lifting proofs from collective to coherent (general) attacks:

- Exponential de Finetti [Renner & Cirac, PRL 102, 110504 (2009)]
  Problem: Bad bounds, feasible only in the asymptotic limit
- Post-selection technique,
  Recent: Leverrier et al., arXiv:1208.4920 (Talk on Monday)

Security Analysis for CV QKD Protocols

Challenge: infinite dimensions

Finite-Key Analysis:
- Leverrier et al, Phys. Rev. A 81, 062343 (2010)
- Berta, FF, Scholz, arXiv:1107.5460 (2011)

Lifting proofs from collective to coherent (general) attacks:
- Exponential de Finetti [Renner & Cirac, PRL 102, 110504 (2009)]
  Problem: Bad bounds, feasible only in the asymptotic limit
- Post-selection technique,
  Recent: Leverrier et al., arXiv:1208.4920 (Talk on Monday)

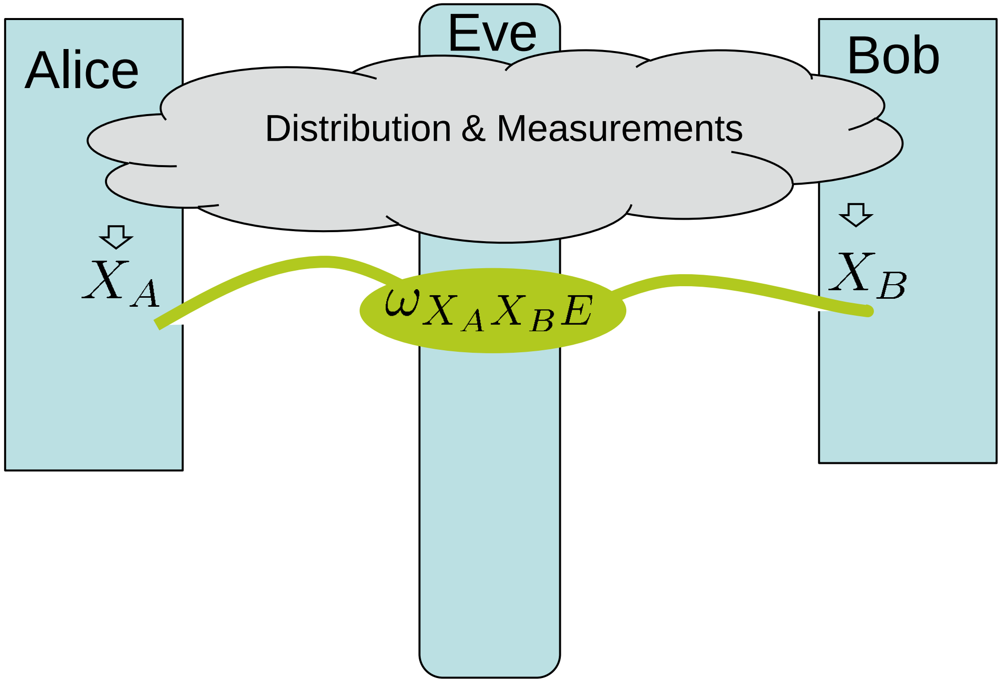
Uncertainty Relation (direct) : This Talk!

Advantage:
- one-sided device independent
- no tomography
- no additional measurements

Outline

1. Security Definition and Finite-key length formula
2. Experimental Set Up and Protocol
3. Finite-Key Rates
4. (Security Analysis)

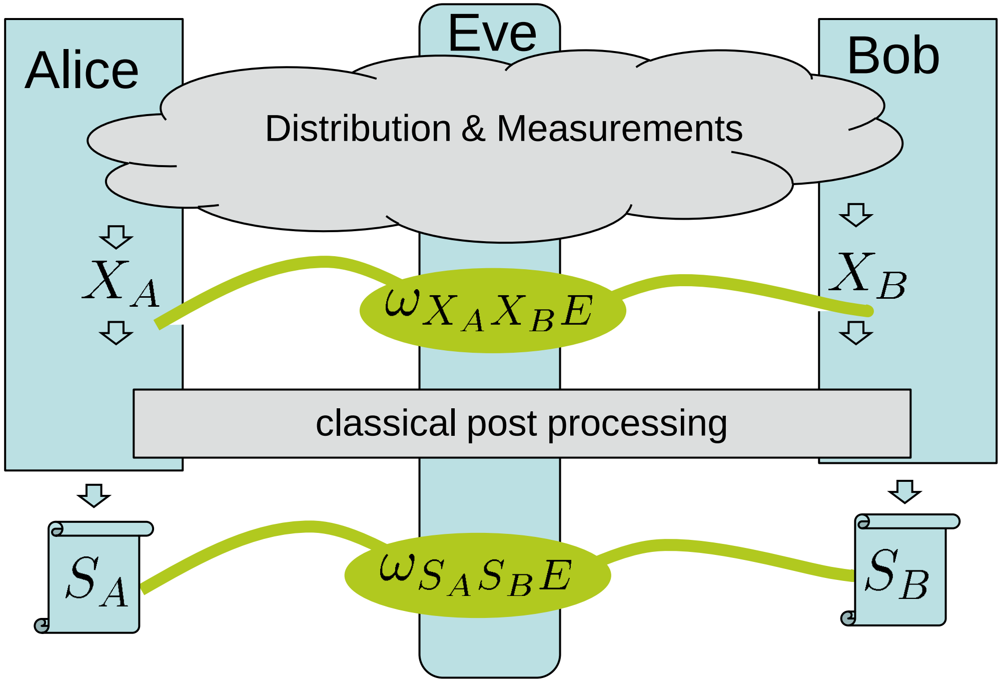
General QKD Protocol



Part I:

1) Distribution of quantum state
2) Measurements
3) Parameter estimation
4) **Output:** Raw keys X_A, X_B or abort

General QKD Protocol



Part 1:

1) Distribution of quantum state
2) Measurements
3) Parameter estimation
4) **Output:** Raw keys X_A, X_B or abort

Part 2:

1) Error correction
2) Privacy amplification

Output: Key S_A, S_B

Security Definitions (trace distance)

A protocol which outputs the state

$$\omega_{S_A S_B E}$$

is **secure** if it is:

- **correct** : $\mathrm{Prob}[S_A \neq S_B] \leq \varepsilon_c$

- **secret**: $p_{\mathrm{pass}} \cdot \|\omega_{S_A E} - \tau_{S_A} \otimes \omega_E\|_1 \leq \varepsilon_s$

  where τ_{S_A} is the uniform distribution over all keys.

Composable Secure*

* R. Renner, PhD Thesis (ETH 2005)

Classical Post Processing

1) **Error Correction:**

   Alice and Bob broadcast ℓ_{EC} bits to match their strings.

2) **Privacy amplification via two-universal hash functions:**

   ... apply random hash function from two-universal family onto ℓ bits

$$f : X_A \to S_A$$

Key length

Classical Post Processing

1) **Error Correction:**

Alice and Bob broadcast ℓ_{EC} bits to match their strings.

2) **Privacy amplification via two-universal hash functions:**

... apply random hash function from two-universal family onto ℓ bits

$$f : X_A \to S_A$$

Key length

Secure key of length:

$$\ell \approx \underbrace{H_{\min}^{\varepsilon}(X_A|E)_\omega}_{\text{Smooth min-entropy}} - \ell_{\mathrm{EC}} - O(\log \frac{1}{\varepsilon'})$$

R. Renner, PhD Thesis (2005), M. Tomamichel et al. IEEE Trans. Inf. Theory, 57 (8) (2011),
M. Berta, FF, V.B. Scholz, arXiv1107.5460 (infinite-dimensional side-information)

Classical Post Processing

1) **Error Correction:**

   Alice and Bob broadcast ℓ_{EC} bits to match their strings.

2) **Privacy amplification via two-universal hash functions:**

   ... apply random hash function from two-universal family onto ℓ bits

$$f : X_A \to S_A$$

Key length

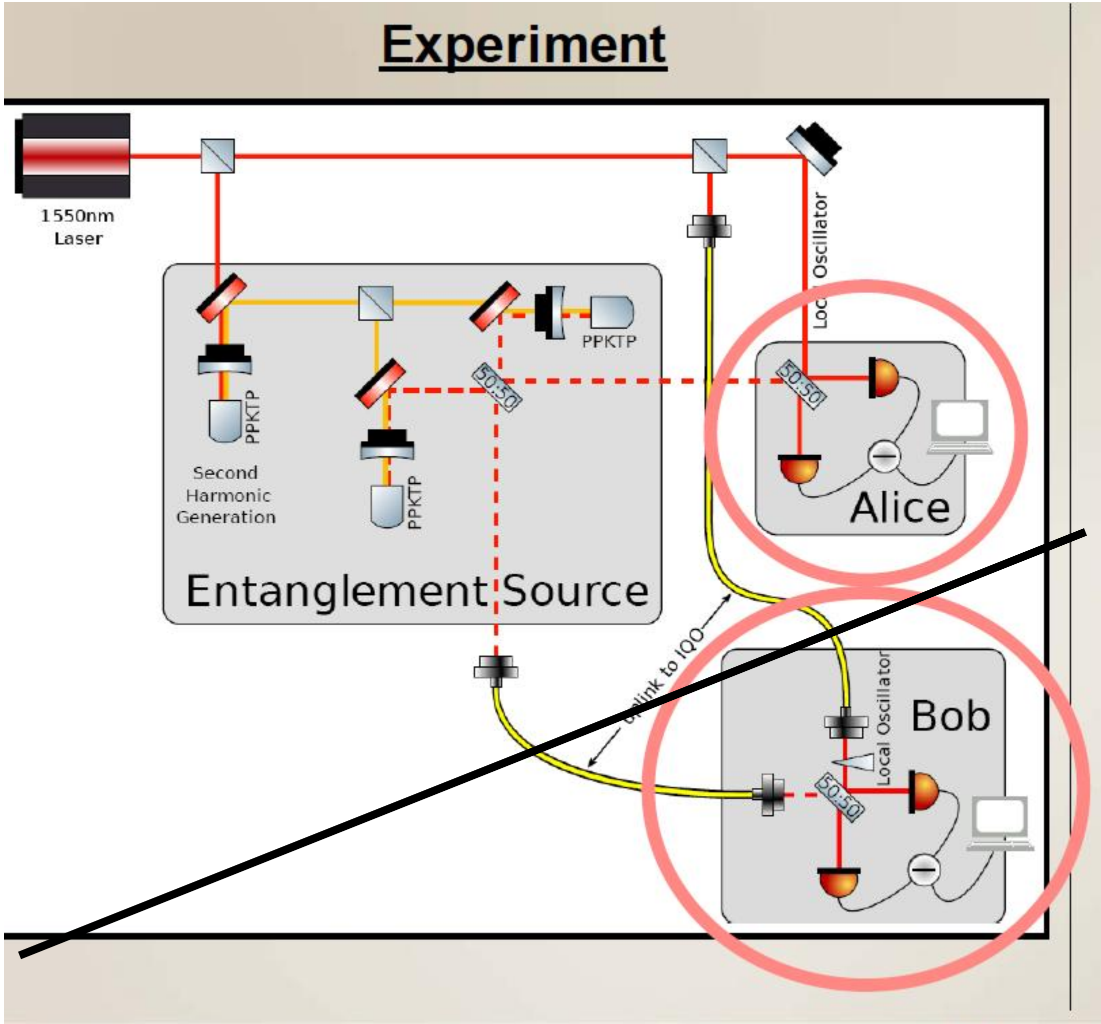
Secure key of length:

$$\ell \approx \underbrace{H_{\min}^{\varepsilon}(X_A|E)_\omega}_{\text{Smooth min-entropy}} - \ell_{\mathrm{EC}} - O(\log \frac{1}{\varepsilon'})$$

R. Renner, PhD Thesis (2005), M. Tomamichel et al. IEEE Trans. Inf. Th, 57 (8) (2011),
M. Berta, FF, V.B. Scholz, arXiv1107.5460 (infinite-dimensional side-information)

Use parameter estimation to bound min-entropy!

Experimental Set Up



Source:
two-mode squeezed state (EPR state)

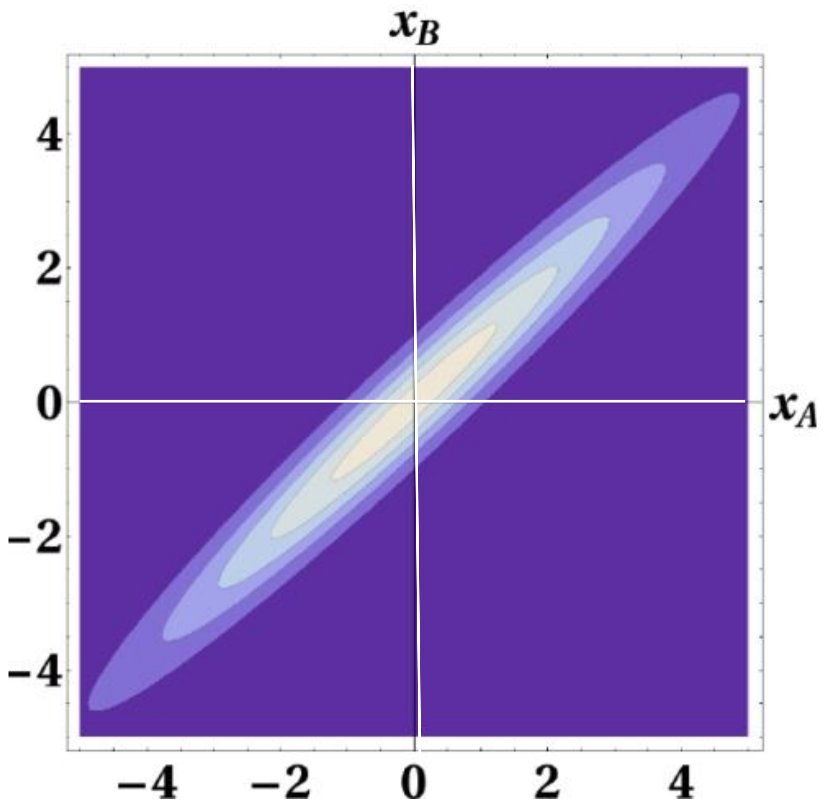
Measurements:
homodyne detection, randomly either amplitude or phase (synchronized via LO)

Entanglement based!

Cerf, N. J., M. Levy, and G. van Assche, 2001, Phys. Rev. A **63,** 052311

Measurements

Correlated outcomes if both measure amplitude or phase:



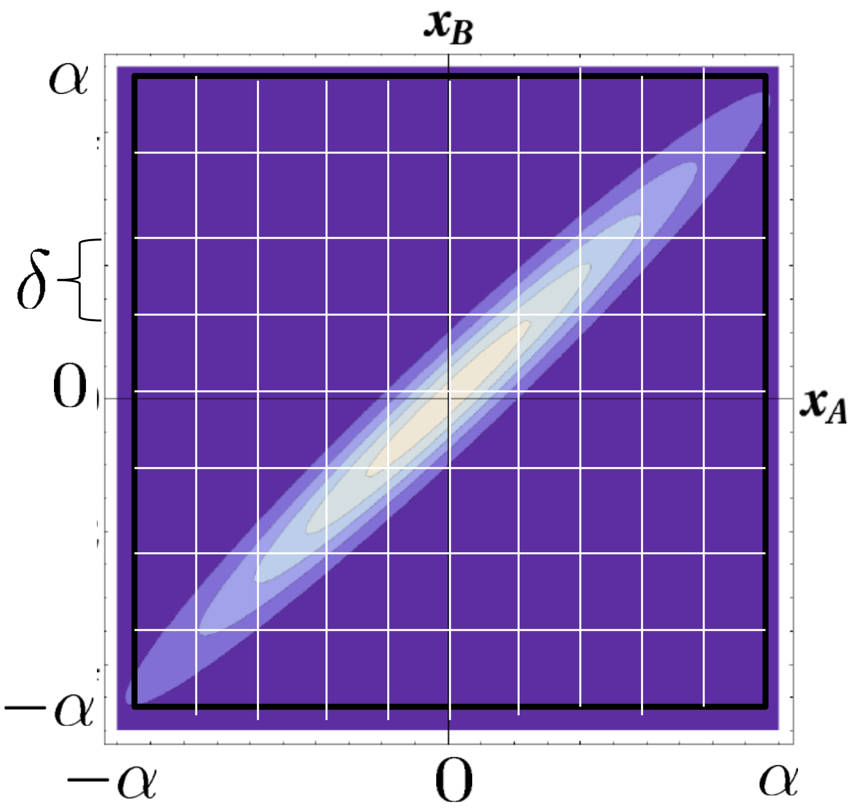
Source:
two-mode squeezed state

Measurements:
homodyne detection, randomly either amplitude or phase (synchronized via LO)

Entanglement based!

Measurements

Binning of the Outcome Range:



- **Spacing parameter:** δ
- **Cutoff parameter**: α

$$I_1 = (-\infty, -\alpha + \delta]$$
$$I_k = (-\alpha + (k-1)\delta, -\alpha + (k-2)\delta]$$
$$I_{2\alpha/\delta} = (\alpha - \delta, \infty)$$

Outcome Range:

$$\mathcal{X} = \{1, 2, ..., 2\alpha/\delta\}$$

Protocol

1. Performing 2N measurements
2. **Sifting**: approx. **N** data points left $X_A^{tot},\ X_B^{tot} \in \mathcal{X}^N$
3. **Parameter estimation:**

   pick random sample of k data points $Y_A, Y_B \in \mathcal{X}^k$ and check correlation:
   Hamming distance:

$$d(Y_A, Y_B) = \frac{1}{k}\sum_{i=1}^{k} |Y_A^i - Y_B^i|$$

4. **Classical post-processing** on remaining strings $X_A, X_B \in \mathcal{X}^n$:

Protocol

1. Performing 2N measurements
2. **Sifting**: approx. **N** data points left $X_A^{tot},\ X_B^{tot} \in \mathcal{X}^N$
3. **Parameter estimation:**
   pick random sample of k data points $Y_A, Y_B \in \mathcal{X}^k$ and check correlation:
   Hamming distance:
   $$d(Y_A, Y_B) = \frac{1}{k}\sum_{i=1}^{k} |Y_A^i - Y_B^i|$$
4. **Classical post-processing** on remaining strings $X_A, X_B \in \mathcal{X}^n$:

A secret key of length

$$\ell = n[\log \frac{1}{c(\delta)} - \log \gamma\big(d(Y_A, Y_B) + \mu\big)] - O(\log \frac{1}{\epsilon}) - \ell_{\mathrm{EC}}$$

can be extracted

Protocol

1. Performing 2N measurements
2. **Sifting**: approx. **N** data points left $X_A^{tot},\ X_B^{tot} \in \mathcal{X}^N$
3. **Parameter estimation:**
   pick random sample of k data points $Y_A, Y_B \in \mathcal{X}^k$ and check correlation:
   Hamming distance:
   $$d(Y_A, Y_B) = \frac{1}{k}\sum_{i=1}^{k} |Y_A^i - Y_B^i|$$
4. **Classical post-processing** on remaining strings $X_A, X_B \in \mathcal{X}^n$:

A secret key of length

$$\ell = n[\log \frac{1}{c(\delta)} - \log \gamma\big(d(Y_A, Y_B) + \mu\big)] - O(\log \frac{1}{\epsilon}) - \ell_{\mathrm{EC}}$$

can be extracted

Statistical correction

Monotonic function

Complementarity of amplitude and phase measurement: depending on spacing parameter

Finite-Key Length

The key is …

- **composable** secure
- provides security against **coherent attacks**

Experimental constraints:

- Alice's measurements are modeled by projections onto spectrum of quadrature operator for amplitude and phase (parameter: δ, α)
  - subsequent measurements commute
- trusted source in Alice's lab of Gaussian states (can be relaxed)
- No assumptions about Bob's measurements: **one-sided device independent**

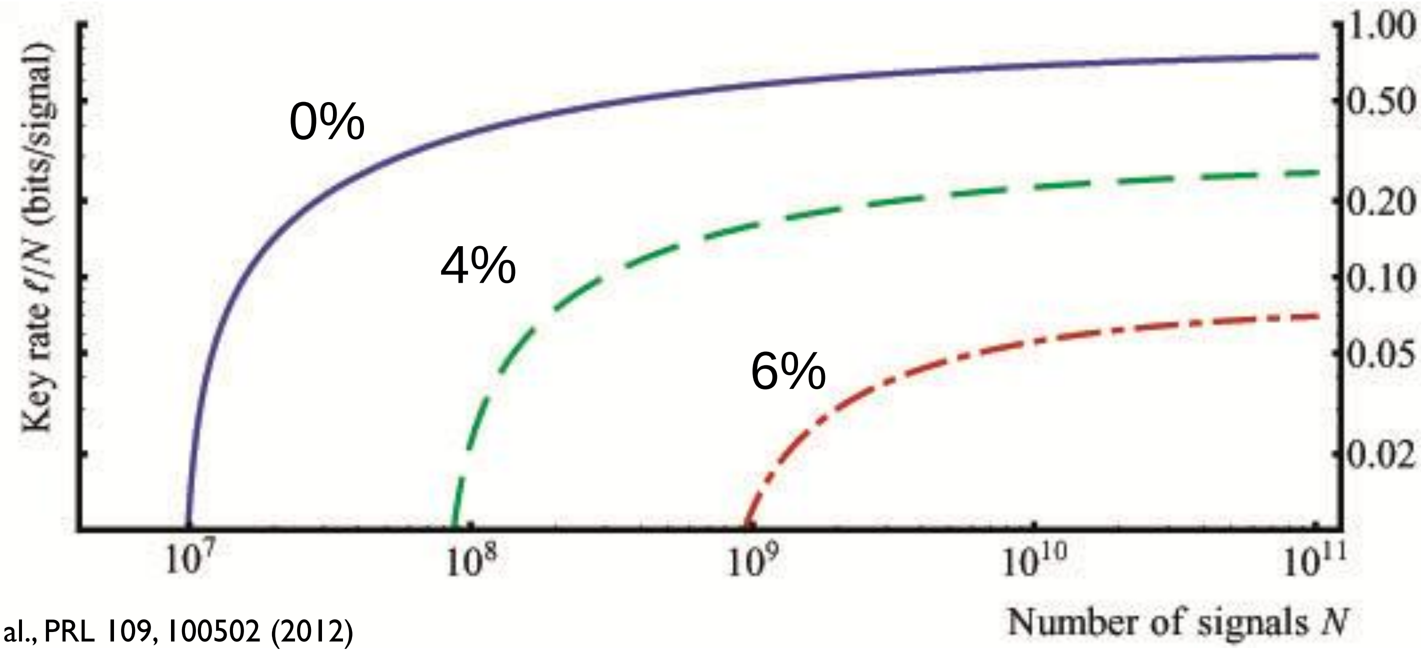
Finite-Key Rates

Key Rate ℓ/N depending on symmetric losses for two-mode squeezed state

- input squeezing/antisqueezing 11dB/16dB *
- error correction efficiency of 95%
- excess noise of 1% *
- additional symmetric losses of ...

* T. Eberle et al., arXiv:1110.3977

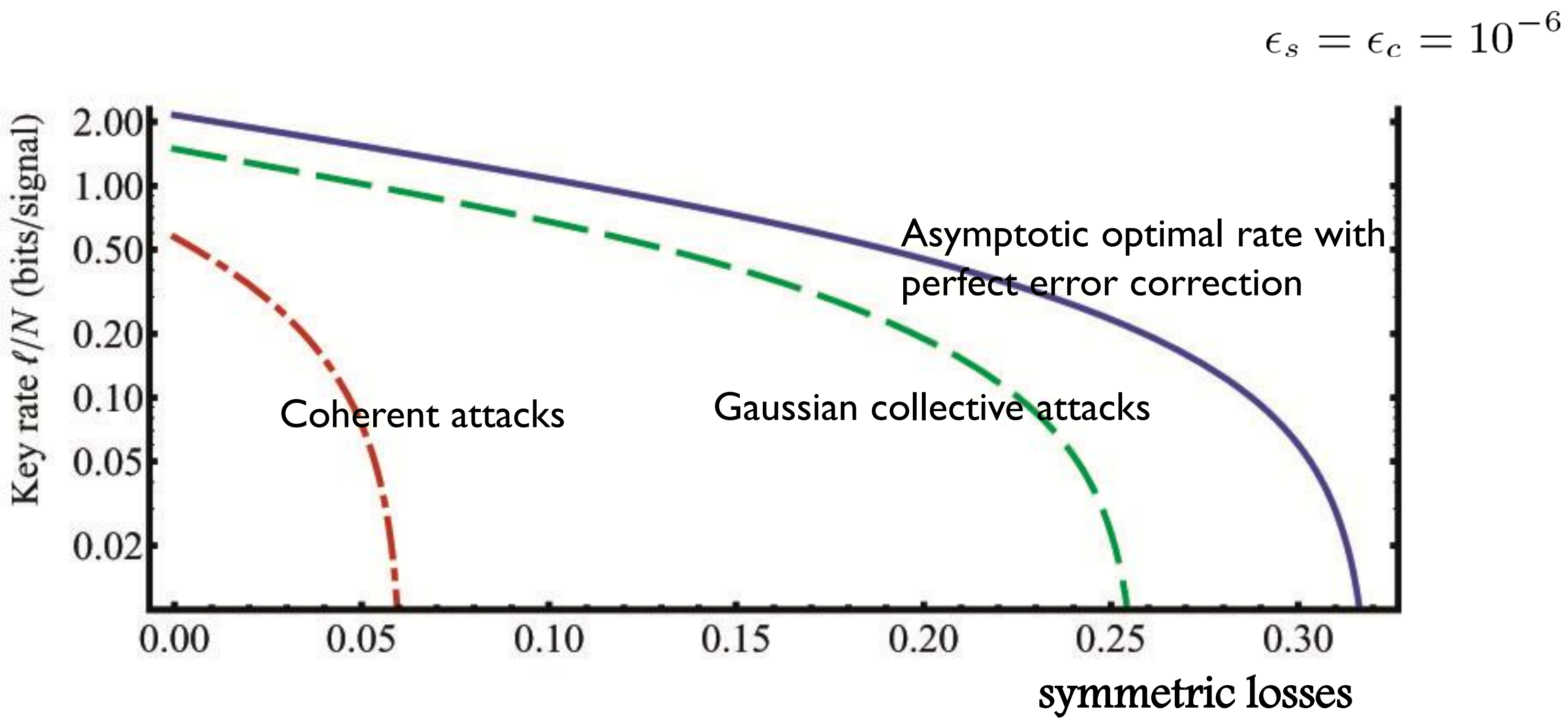
$\epsilon_s = \epsilon_c = 10^{-6}$



Plot: FF et al., PRL 109, 100502 (2012)

Key Rate versus Losses

Key rate versus losses for N=10^9 sifted signal:



Plot: FF et al., PRL 109, 100502 (2012)

Security Analysis Based on Uncertainty Relation

Extractable key length:

$$\ell = H_{\min}^{\varepsilon}(X_A|E)_\omega - \ell_{\mathrm{EC}} - O(\log \frac{1}{\epsilon})$$

Goal: bound for $H_{\min}^{\varepsilon}(X_A|E)_\omega$

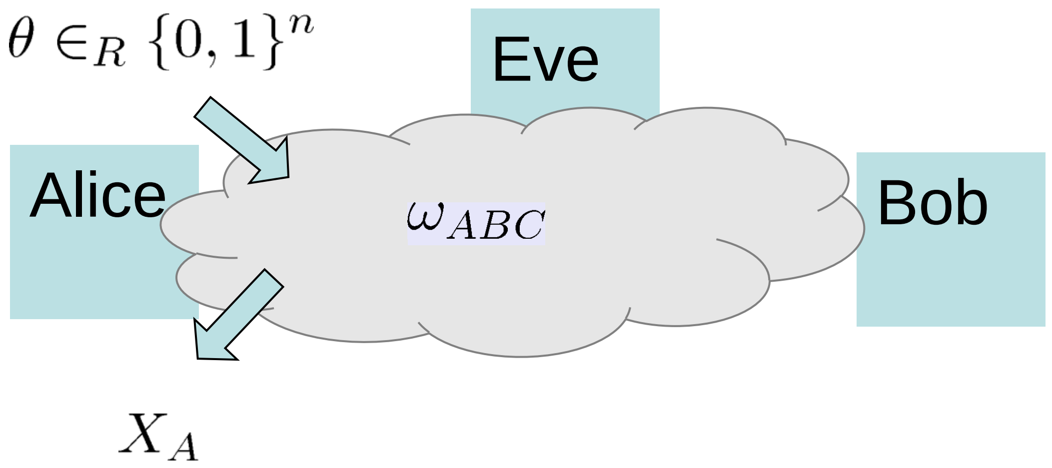
Key ingredient: **Uncertainty relation with side-information***

* Tomamichel & Renner, Phys. Rev. Lett. 106, 110506 (2011)

Entropic Uncertainty Relation with Side Information

$\theta_i = 0$: Amplitude

$\theta_i = 1$: Phase

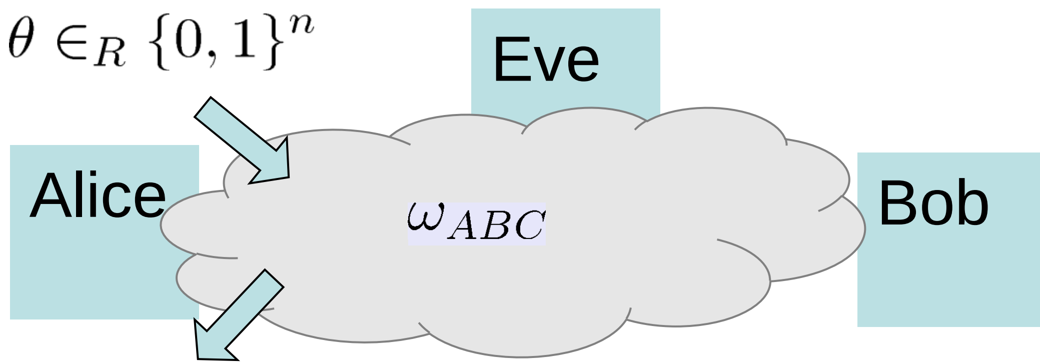


Entropic Uncertainty Relation with Side Information

$\theta_i = 0$: Amplitude

$\theta_i = 1$: Phase

$\theta \in_R \{0,1\}^n$



X_A

$$H^{\varepsilon}_{\min}(X_A|E\Theta)_\omega \geq \log \frac{1}{c(\delta)} - H^{\varepsilon}_{\max}(X_A|\Theta B)_\omega$$

uncertainty Eve has about outcome of Alice

uncertainty of Bob about outcome of Alice

$$c(\delta) = ||Q([0,\delta])P([0,\delta])||^2 \approx \frac{\delta^2}{2\pi}$$

complementary of the measurements

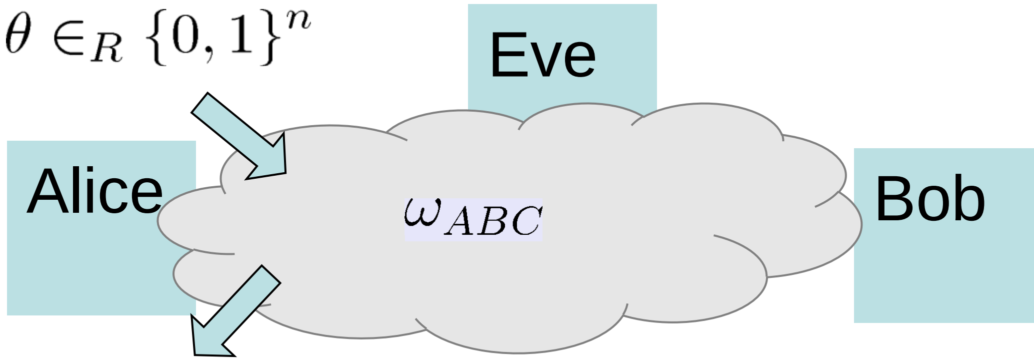
M. Tomamichel , PhD Thesis,
M. Berta, FF, V.B. Scholz, arXiv1107.5460 (2011)

Entropic Uncertainty Relation with Side Information

$\theta_i = 0$: Amplitude

$\theta_i = 1$: Phase

$\theta \in_R \{0,1\}^n$



X_A

$$H_{\min}^{\varepsilon}(X_A|E\Theta)_\omega \geq \log\frac{1}{c(\delta)} - H_{\max}^{\varepsilon}(X_A|\Theta B)_\omega$$

$$\geq \frac{1}{c(\delta)} - H_{\max}^{\varepsilon}(X_A|X_B)_\omega$$

Data processing inequality

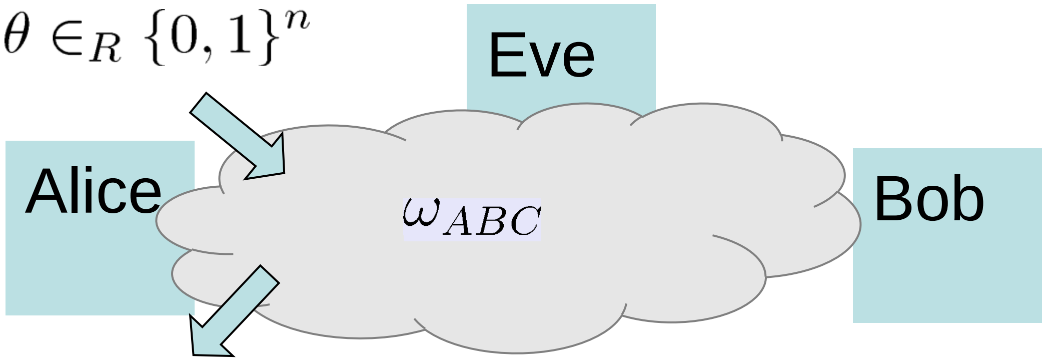
M. Tomamichel et al., Phys. Rev. Lett. 106,110506 (2011),
M. Tomamichel , PhD Thesis (2012); M. Berta, FF, V.B. Scholz, arXiv1107.5460 (2011)

Entropic Uncertainty Relation with Side Information

$\theta_i = 0$: Amplitude

$\theta_i = 1$: Phase

$$\theta \in_R \{0,1\}^n$$



$$X_A$$

$$H^{\varepsilon}_{\min}(X_A|E\Theta)_\omega \geq \log \frac{1}{c(\delta)} - H^{\varepsilon}_{\max}(X_A|\Theta B)_\omega$$

$$\geq \frac{1}{c(\delta)} - H^{\varepsilon}_{\max}(X_A|X_B)_\omega$$

Data processing inequality

Correlation betw. Alice & Bob

M. Tomamichel et al., Phys. Rev. Lett. 106,110506 (2011),
M. Tomamichel , PhD Thesis (2012); M. Berta, FF, V.B. Scholz, arXiv1107.5460 (2011)

Correlation between Alice & Bob

Correlation between Alice and Bob can be bounded in terms of the Hamming distance of a random sample

$$d(Y_A, Y_B) = \frac{1}{k}\sum_{i=1}^{k} |Y_A^i - Y_B^i| \leq d_0$$

via

$$H_{\max}^{\varepsilon}(X_A|X_B)_\omega \leq n \log \gamma(d(Y_A, Y_B) + \mu)$$

Combining with Uncertainty Relation:

$$\ell = n[\log \frac{1}{c(\delta)} - \log \gamma(d_0 + \mu)] - O(\log \frac{1}{\epsilon}) - \ell_{\mathrm{EC}}$$

Conclusion

Advantage:

- one-sided device independent (e.g. local oscillator included)
- direct approach (no additional measurements compared to post-selection approach)
- no state tomography
- robust under small deviations of experimental parameters

Problems:

- very sensitive to noise
- asymptotically not optimal: Uncertainty relation not tight for the Gaussian states used in the protocol

Implementation in Leibniz University in Hannover:

Crypto on Campus: T. Eberle, V. Händchen, J. Duhme, T. Franz, R. F. Werner, and R. Schnabel

Thank you for your attention!