Reverse Reconciliation Continuous Variable Quantum Key Distribution Based on the Uncertainty Principle

arXiv:1405.5965

QCRYPT 2014, Paris, 2. September 2014

FABIAN FURRER

KAKENHI grant No. 24-02793

Outline

1) Introduction

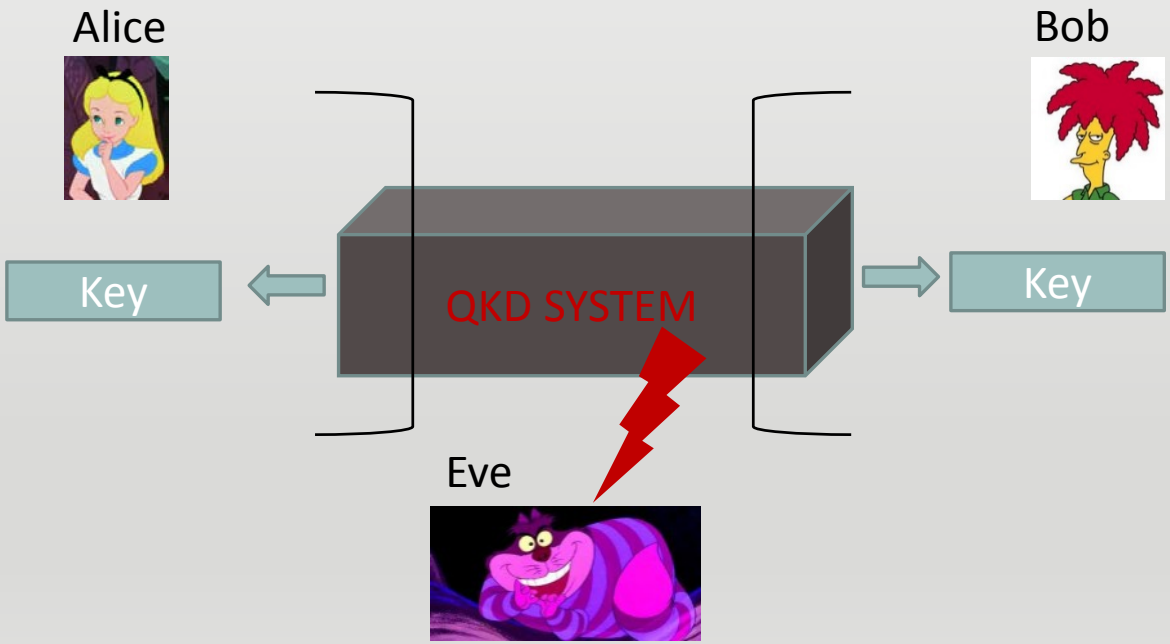
2) Description of the particular QKD protocol

3) Key Rates and Basic Proof Ideas

4) Optimality Discussion of the Key Rates

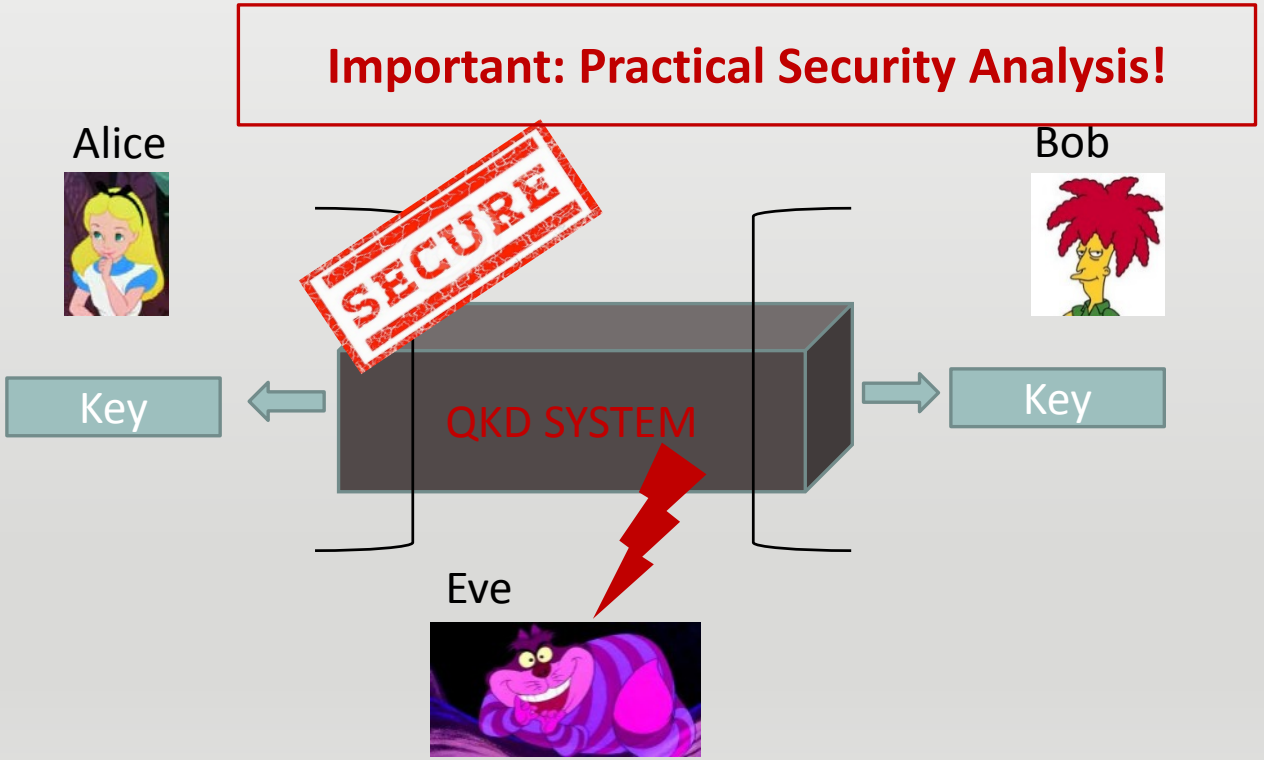
Quantum Key Distribution (QKD)

Using quantum communication to generate a secret key between two remote parties Alice and Bob not known by any third party Eve.



Quantum Key Distribution (QKD)

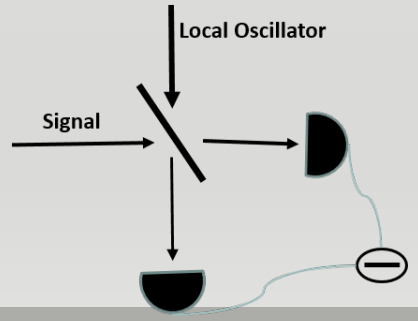
Using quantum communication to generate a secret key between two remote parties Alice and Bob not known by any third party Eve.

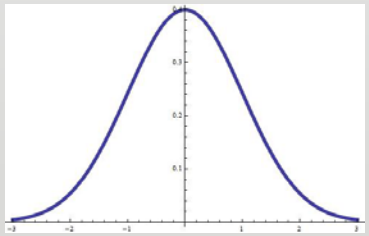


Implementations of QKD

- **Discrete Variable Protocols**: Observables with a finite number of outcomes
  - Example: BB84 with polarization degree of photon
  - Based on single photon source and detectors

- **Continuous Variable (CV) Protocols:** Observables with a continuous spectrum
  - Encoding by amplitude and phase modulations of the EM-field
  - **Continuous Gaussian Modulation**
  - Measurement: Homodyne detection
  - Source: Gaussian states





Displacement

Pros and Cons of CV Protocols

+ State generation (Gaussian states) and measurement (homodyne detection) are robust and have high efficiency (compared to single photon detectors)
+ Based on standard telecommunication technology (simple integration into current networks)

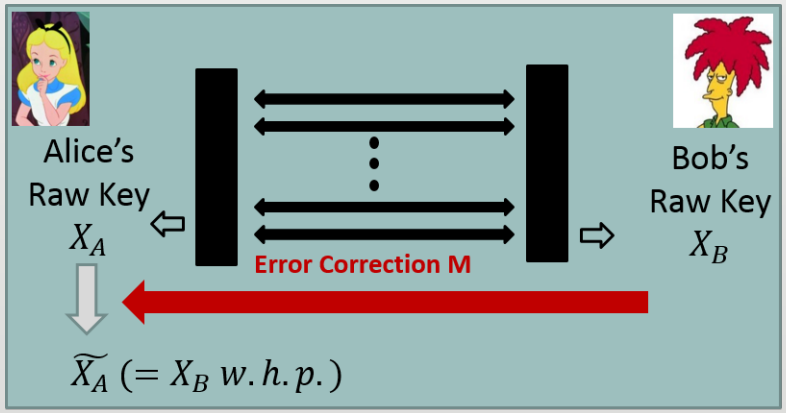
– Error correction for Gaussian distributed variables more difficult

–Security proofs more involved

  – Infinite-dimensional system and continuous measurement range
  – state estimation and finite-statistics are difficult
  – important tools developed for discrete protocols do not apply (e.g. exponential de Finetti theorems, postselection technique)

Long distance CV QKD (Gaussian modulation)

- Limited distance due to losses
- Long distances requires a **reverse reconciliation protocol** (Grosshans et al., Nature, 421, 2003):



  - Classical post-processing: Bob sends information to Alice in the reconciliation protocol
  - Measurement of Bob introduces randomness that cannot be controlled by Eve (shot noise)
  - Reverse reconciliation allows (theoretically) to tolerate arbitrary amount of losses (arbitrary distances)

Security proofs for CV QKD:

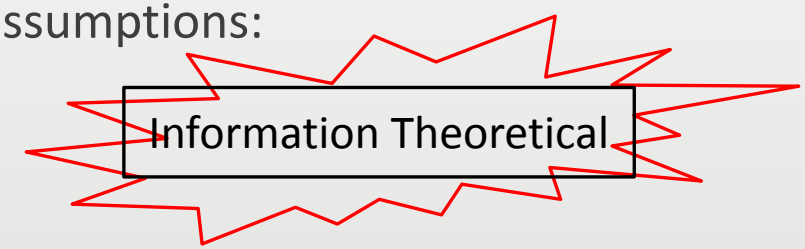
Security usually as strong as the assumptions:

Implementation	Information Theoretical

Security proofs for CV QKD:

Security usually as strong as the assumptions:

Implementation



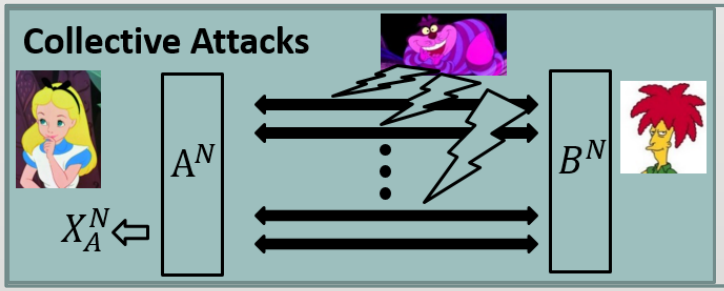
Security proofs for CV QKD:

Security usually as strong as the assumptions:

Implementation

Information Theoretical

1) Assumption on Attacks:



Each QM signal is attacked independently and identically

Eve can attack arbitrarily: no restriction!

Security proofs for CV QKD:

2) Asymptotic Limit (infinite number of quantum communication)

- simplifies Security Analysis extremely (Gaussian modulation)

- Coherent attacks = collective attacks
- Optimality of Gaussian attacks
- No finite statistics required
- Mutual Information

Security analysis based on mutual information can be restricted to Gaussian collective attacks (e.g Nature, 421,2003; PRL 93,170504, 2004)

Security proofs for CV QKD:

2) Asymptotic Limit (infinite number of quantum communication)

- simplifies Security Analysis extremely (Gaussian modulation)

- Coherent attacks = collective attacks
- Optimality of Gaussian attacks
- No finite statistics required
- Mutual Information

Security analysis based on mutual information can be restricted to Gaussian collective attacks (e.g Nature, 421,2003; PRL 93,170504, 2004)

- not practical: **finite-size effects** appear in real-life implementations
- composable security: Eve's knowledge estimated by one shot entropy (e.g., smooth min-entropy)
- **Against Gaussian Collective:** Leverrier et al., PRA 81, 062343 (2010), Jouget et al, Nature Phot, 7, 2012

Security proofs for CV QKD:

2) Asymptotic Limit (infinite number of quantum communication)

- simplifies Security Analysis extremely (Gaussian modulation)

- Coherent attacks = collective attacks
- Optimality of Gaussian attacks
- No finite statistics required
- Mutual Information

Security analysis based on mutual information can be restricted to Gaussian collective attacks (e.g Nature, 421,2003; PRL 93,170504, 2004)

- not practical: **finite-size effects** appear in real-life implementations
- composable security: Eve's knowledge estimated by one shot entropy (e.g., smooth min-entropy)
- **Against Gaussian Collective:** Leverrier et al., PRA 81, 062343 (2010), Jouget et al., Nature Phot, 7, 2012
- **Against General Collective Attacks:** Leverrier arXiv:1408.5689

Security Proofs against Coherent Attacks

Only few finite-size security proofs against **general (coherent) attacks:**

1. Based on **symmetrization and the postselection technique** Leverrier et al, PRL 110, 030502, 2013
   - allows to lift collective to coherent attacks (similar to discrete variable)
   - currently only feasible for direct reconciliation protocols (symmetrization)
   - Doesn't scale well in number of rounds

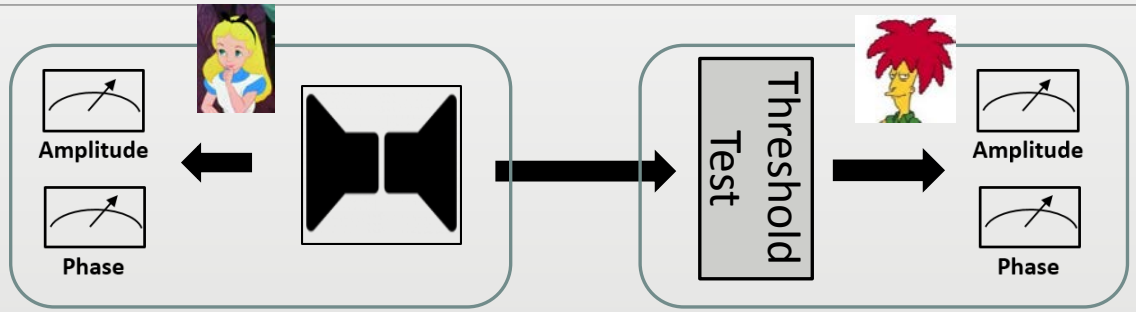
2. Based on the **entropic uncertainty principle with quantum memory** (FF et al, PRL 109, 2012)
   - entanglement based squeezed state protocols
   - complete experimental demonstration Gering et al, arXiv:1406.6174
   - so far **only for direct reconciliation protocols** (short distances)

Poster 65 & 74

Contribution here:

Extending 2. to reverse reconciliation → improved distance!

The Protocol: Quantum Phase



Similar to FF et al, PRL 109, 2012

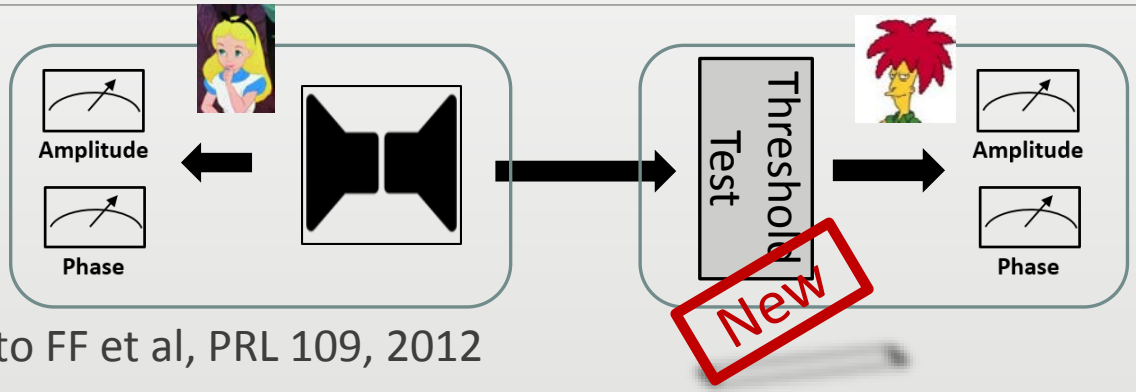
1) Alice prepares and distributes a **two mode squeezed state (EPR state)**.

2) Both apply randomly either **amplitude or phase measurements**

3) Bob applies a **threshold test** before his measurement and aborts the protocol if the test fails.

5) They repeat the procedure N times

The Protocol: Quantum Phase



Similar to FF et al, PRL 109, 2012

1) Alice prepares and distributes a **two mode squeezed state (EPR state)**.

2) Both apply randomly either **amplitude or phase measurements**

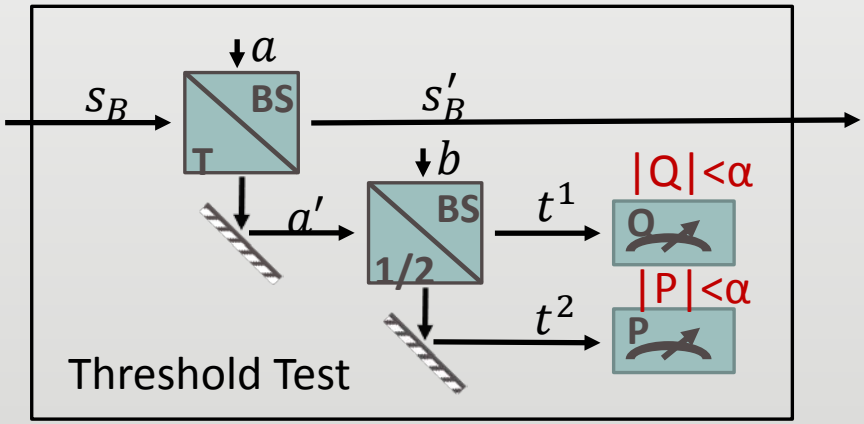
3) Bob applies a **threshold test** before his measurement and aborts the protocol if the test fails.

5) They repeat the procedure N times

Threshold Test

Goal: Control probability for large measurement outcomes (>M)

→ cut-off for unbounded measurement range



1) Incoming signal is mixed with vacuum by a beam splitter (BS) with almost perfect transmittance T ≈ 0.99

2) Heterodyne detection of the reflected beam

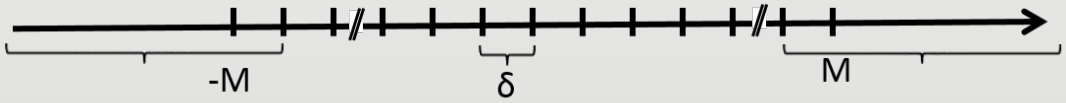
3) Test passed if outcomes of the heterodyne detection are smaller than a value **α**.

The Protocol: Classical Phase

1) Alice and Bob publicly announce measurement choices

2) Discretization of Measurement Outcomes:

- threshold parameter M (smaller than detector range)
- constant binning δ (compatible with the detector resolution)



3) Parameter Estimation with phase measurements:

- Average distance $d_{PE} = \frac{1}{N_P}\sum_{i=1}^{N_P} |X_A^i - X_B^i|$
- Variance of d and variance of all individual measurements

4) Key generation from amplitude measurements X_A , X_B:

- reverse reconciliation protocol
- applying two-universal hash functions

Finite-Key Length

- composable
- finite-size

Main Result: secure key length against **coherent attacks**

$$n\left[log\frac{1}{c(\delta)} - log\gamma(d_{PE}+\mu)\right] - \ell_{EC} - \mathcal{O}(log\frac{1}{\epsilon})$$

- Number of amplitude measurements
- Overlap of Bob's phase and amplitude measurements
- Correlation betw Alice and Bob (μ = statistical uncertainty)
- Bits exchanged in reverse recondiliation

Finite-Key Length

- composable
- finite-size

Main Result: secure key length against **coherent attacks**

$$n\left[\log\frac{1}{c(\delta)} - \log\gamma(d_{PE}+\mu)\right] - \ell_{EC} - \mathcal{O}(\log\frac{1}{\epsilon})$$

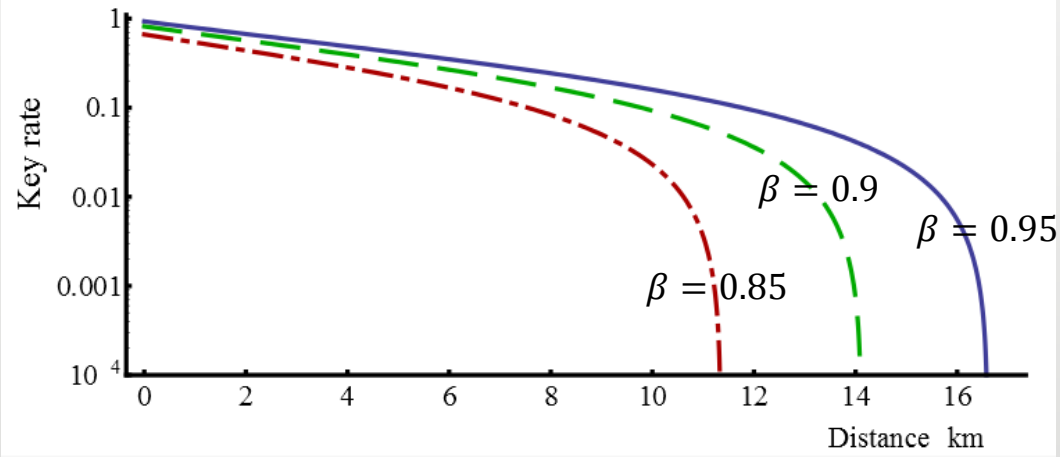
- Number of amplitude measurements
- Overlap of Bob's phase and amplitude measurements
- Correlation betw Alice and Bob (μ = statistical uncertainty)
- Bits exchanged in reverse recondiliation

Assumptions:

Bob's discretized measurements: ideal phase and amplitude measurements with phase difference $\pi/2 \rightarrow c(\delta)$.

- sequential measurements are independent
- the **local oscillator** has to be trusted (or monitored)

Key rate against Distance



Loss= 0.2dB/km + coupling losses

$N = 10^9$

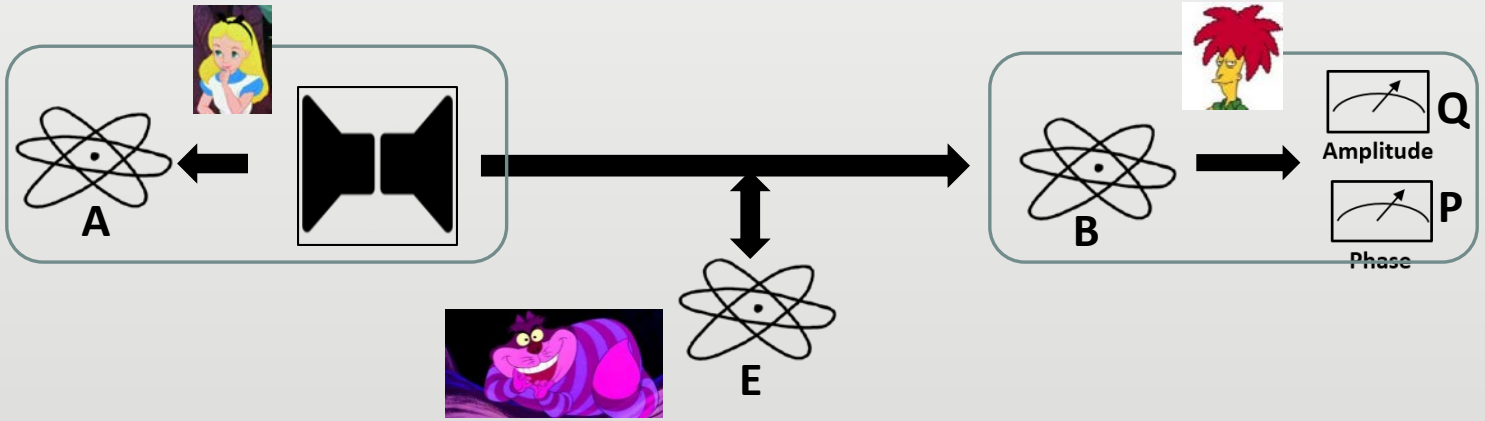
$\epsilon_s = 10^{-9}$

- **Key rate** = key length per communicated quantum signal $N = 10^9$
- **Source:** squeezing/antisqueezing of 11/16dB (Eberle et al, PRA 83, 052329, 2011)
- **Reconciliation efficiency β*:** $\ell_{EC} = H(X_B) - \beta\, I(X_A : X_B)$
- **Energy test:** transmittance T=0.99 and threshold α=28 ($\hbar = 2$) (robust!)
- **Discretization:** $\delta \approx 0.1$, $M \approx 1000$ (14 bits → can be reduced for post-processing)

* Gehring et al, arxiv1406.6174, Jouguet et al, arXiv:1406.1050

Security Proof: Part 1

Main Ingredient: Uncertainty principle with quantum side information
(similar as in FF et al, PRL 109, 2013)



"Uncertainty of Q given E" + "Uncertainty of P given B" $\geq$ "Overlap of P and Q"

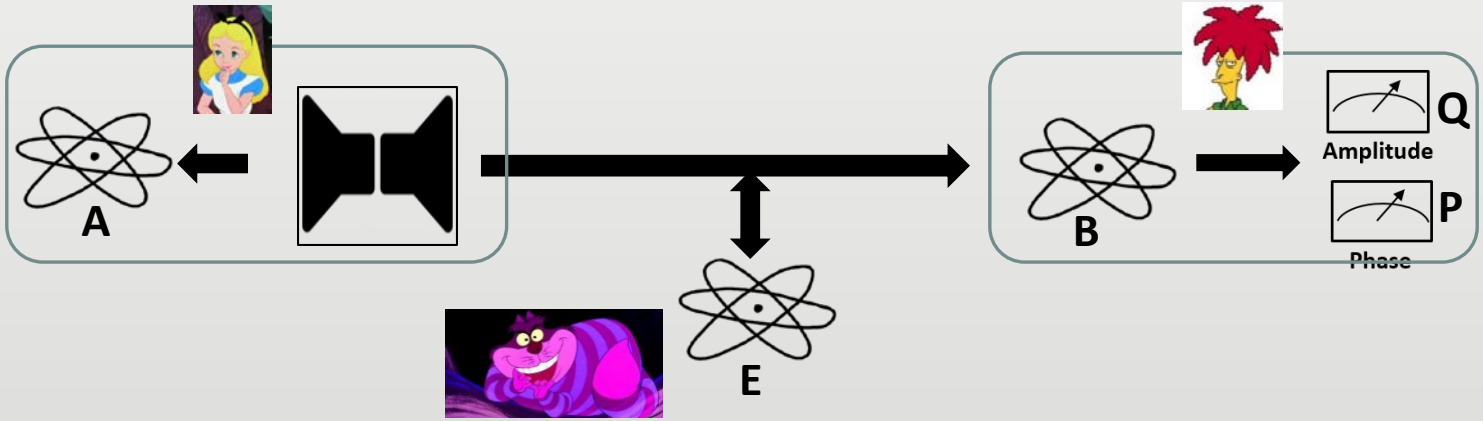
$$H_{\min}^{\epsilon}(Q|E) + H_{max}^{\epsilon}(P|A) \geq -\log c(\delta)$$

right entropy measure for QKD

Berta et al, arXiv:1308.4527

Security Proof: Part 1

Main Ingredient: Uncertainty principle with quantum side information
(similar as in FF et al, PRL 109, 2013)



"Uncertainty of Q given E" + "Uncertainty of P given B" ≥ "Overlap of P and Q"

$$H_{\min}^{\epsilon}(Q|E) + H_{max}^{\epsilon}(P|A) \geq -\log c(\delta)$$

right entropy measure for QKD

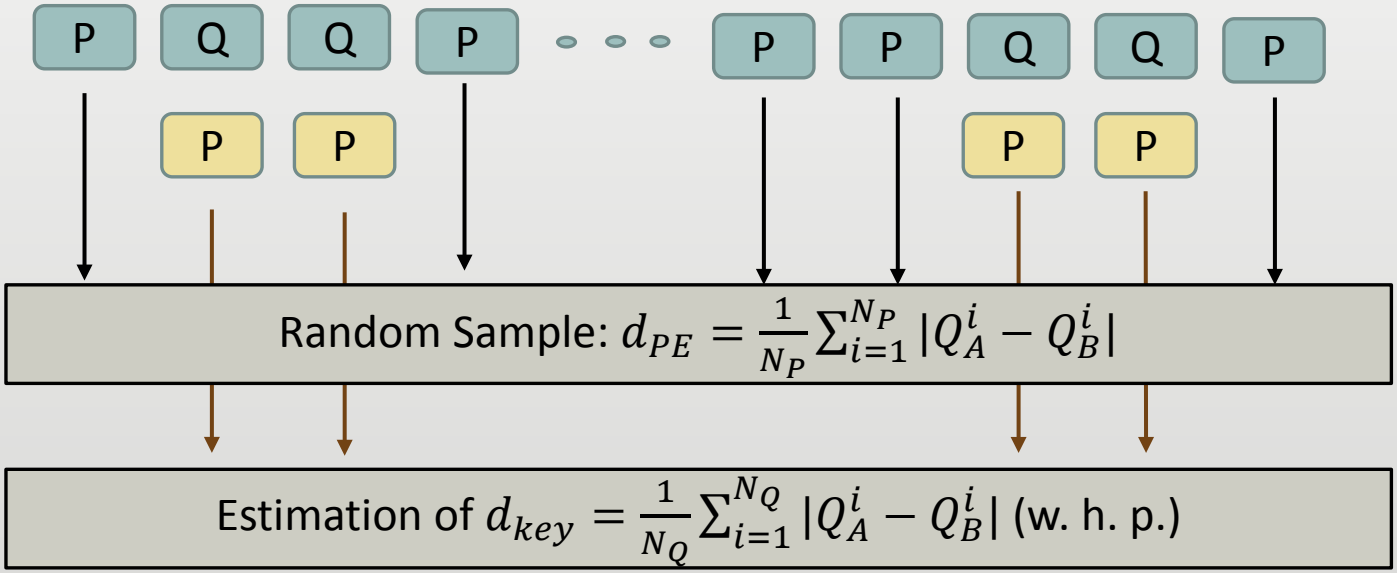
Berta et al, arXiv:1308.4527

Important: Measurement Q and P have to go over the entire range (real line)!

→ threshold test to reduce to bounded range!

Security Proof: Part 2

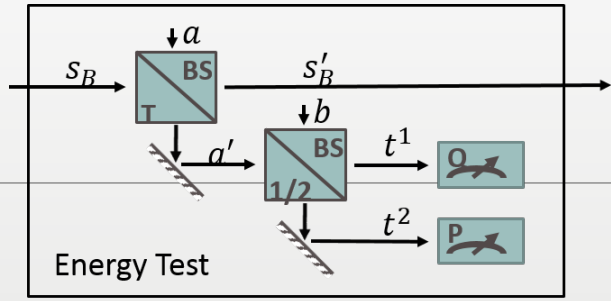
Statistical Estimation:



Problem with CV systems:

- Unbounded measurement range
- Usual statistical bounds like, e.g., Hoeffding or Bernstein's bound on the sum of random variables require finite range

Security Proof: Part 2



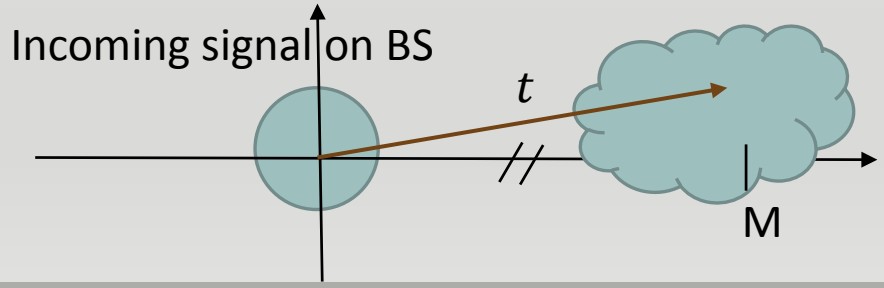
1) Threshold Test:

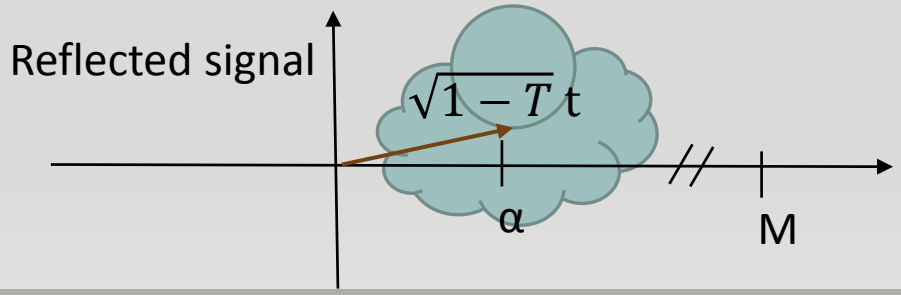
Theorem:
Probability that the probability to measure a phase/amplitude larger than M conditioned on test pass for α decays exponentially:

$$\Pr\left[|q_s| > M \; and \; |q_{t_1}| \leq \alpha\right] \leq C \exp\left[-\left(\sqrt{\frac{1-T}{2T}}M - \alpha\right)^2\right]$$

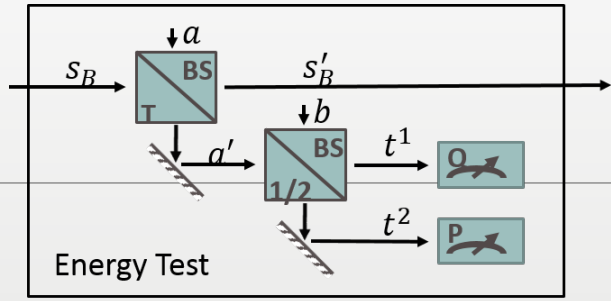
- Independent on input state

Idea of proof (phase space picture):





Security Proof: Part 2



1) Threshold Test:

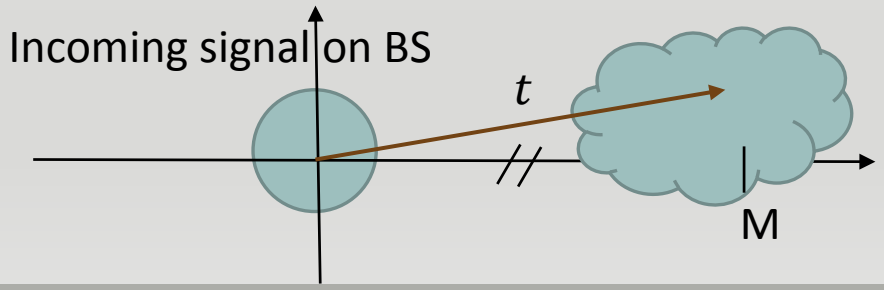
Theorem:
Probability that the probability to measure a phase/amplitude larger than M conditioned on test pass for α decays exponentially:

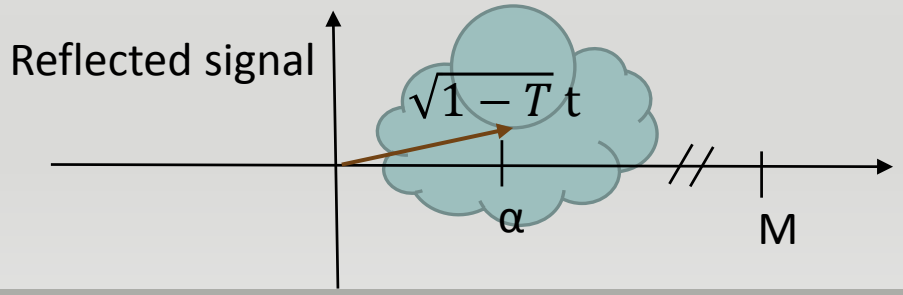
$$\Pr\left[|q_s| > M \; and \; |q_{t_1}| \leq \alpha\right] \leq C \exp\left[-\left(\sqrt{\frac{1-T}{2T}}M - \alpha\right)^2\right]$$

Need a large M

- Independent on input state

Idea of proof (phase space picture):





Security Proof: Part 2

2) Two step estimation that can tolerate large M (prop. alphabet size):

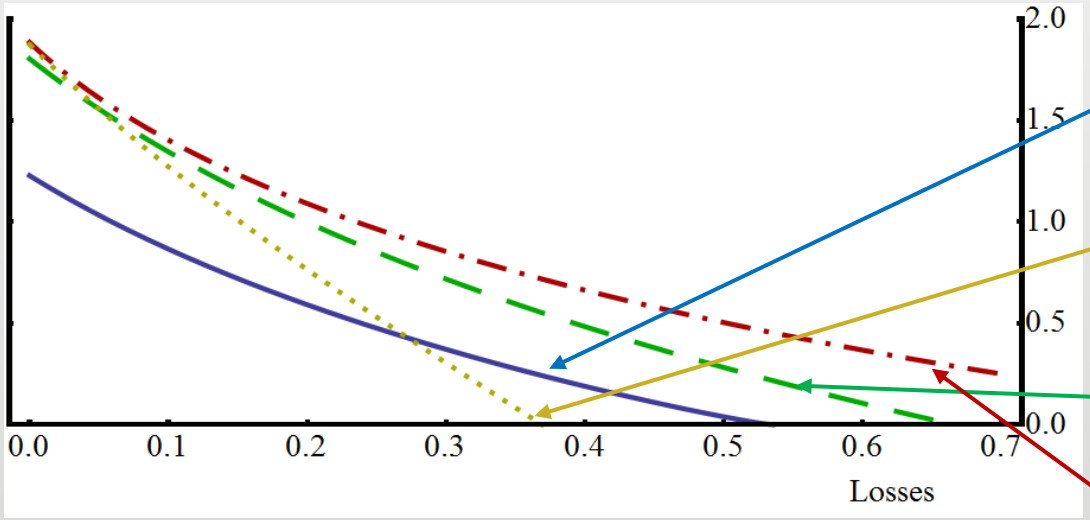
1. Estimate the variance of the phase → Estimate of the variance of d

2. Estimate d_{key} based on the estimated variance of d by using Bernstein's inequality with statistical uncertainty μ

3. Bound on Eve's information via entropic uncertainty relation:

$$H_{\min}^{\epsilon}(Q|E) \geq -\log c(\delta) - \underbrace{H_{max}^{\epsilon}(P|A)}_{\leq log\gamma(d_{PE}+\mu)}$$

Optimality of Key Rate Estimation based on Uncertainty Relation



Finite-Key rate for reverse reconciliation (RR)

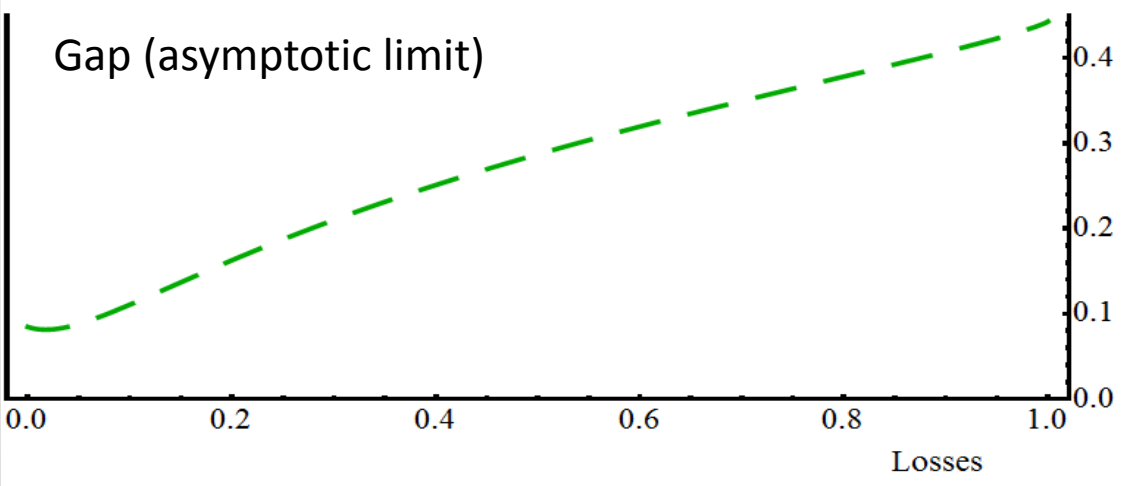
Finite-Key rate for direct reconciliation

Asymptotic key rate for RR

Optimal key rate in the asymptotic limit

- Gap between asymptotic key rate for RR to the optimal asymptotic key rate because of non-tightness of uncertainty relation

Fundamental Limit on Loss Tolerance due to Application of Uncertainty Relation



- Uncertainty relation with quantum memory is not tight for the setup
- Same state as for key rate plots

Limitation due to entropic uncertainty relation

Conclusion and Outlook

- Security of CV QKD against coherent attacks for practical urban distances
  - Experimentally feasible:recent implementation of complete protocol for direct reconciliation (Gering et al, arXiv:1406.6174)
  - Error correction currently tested for important loss regime
- Threshold test and theorem
  - allows to overcome estimation problems due to unbounded measurement range
  - applies to detector threshold problem (usual assumption on implementation)
- Fundamental limitation due to entropic uncertainty relation

→ need different approach for longer distances

Poster 65 & 74

東京大学
THE UNIVERSITY OF TOKYO

Thank you for your attention.

arXiv:1405.5965