T. Eberle[1], V. Händchen[1], F. Furrer[2], T. Franz[3], J. Duhme[3], R.F. Werner[3], R. Schnabel[1]

Realization of Finite-Size Continuous-Variable Quantum Key Distribution based on Einstein-Podolsky-Rosen Entangled Light

(1) Institute for Gravitational Physics, Leibniz University Hannover
and Max Planck Institute for Gravitational Physics (Albert Einstein Institute),
Callinstr. 38, 30167 Hannover, Germany
(2) Department of Physics, Graduate School of Science, University of Tokyo,
7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan, 113-0033
(3) Institute for Theoretical Physics, Leibniz University Hannover,
Appelstraße 2, 30167 Hannover, Germany

QCrypt 2013
August, 5th 2013

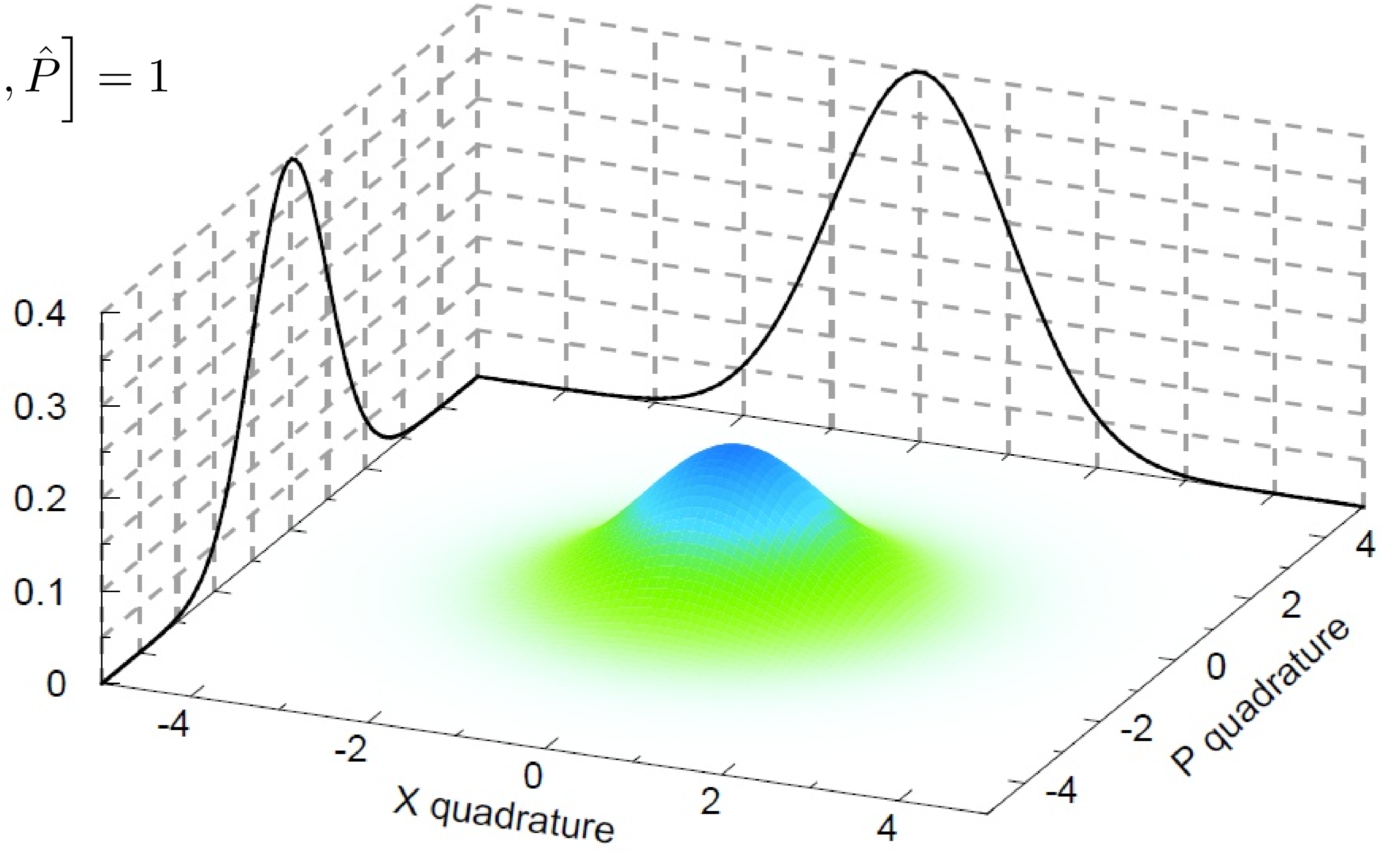
Continuous Variables

- **QKD protocol requires two non-commuting observables**
- **Observables:** Amplitude and Phase Quadrature of Light Fields

$\hat{X}$ $\hat{P}$

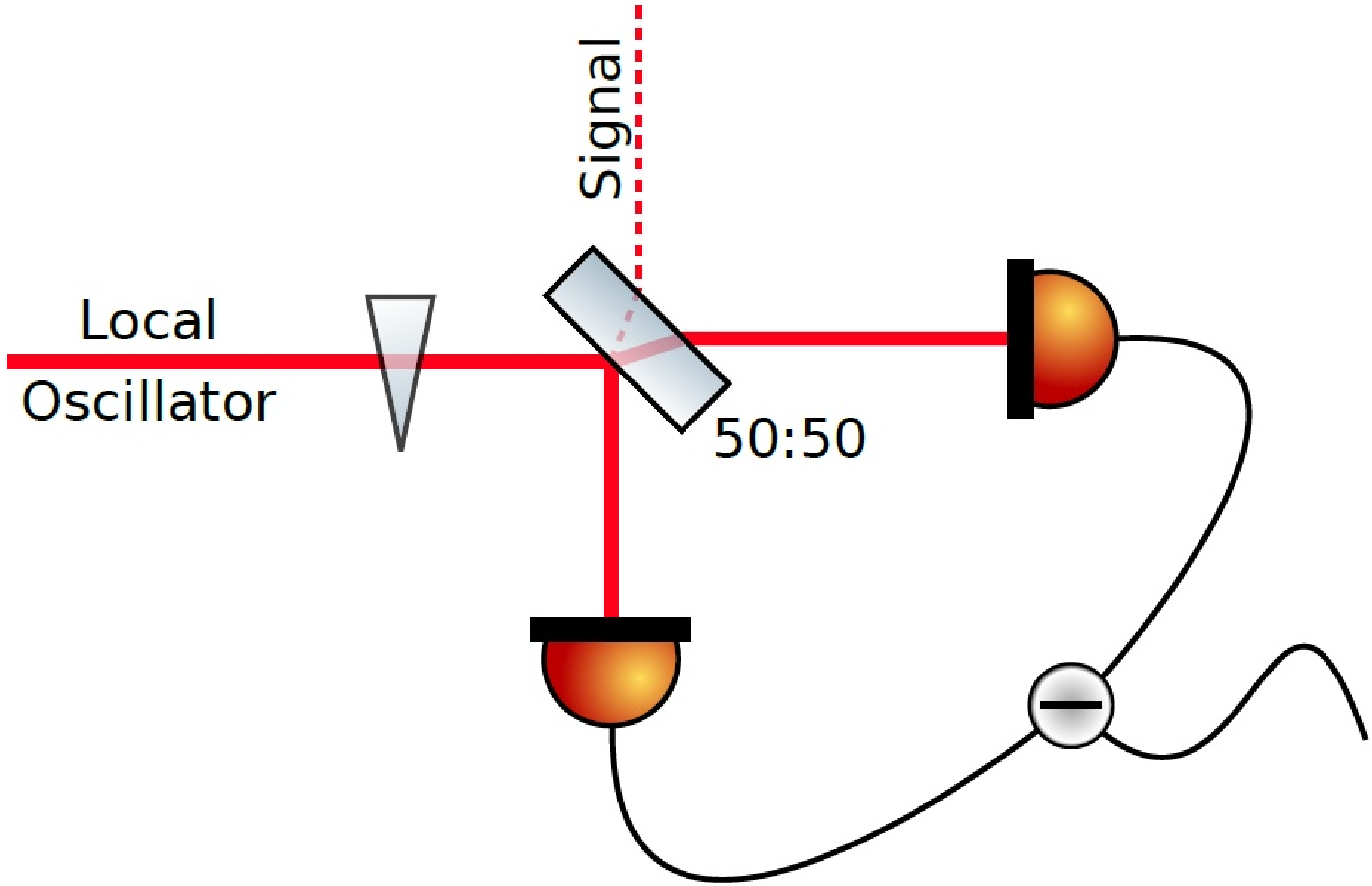
- Commutator: $\left[\hat{X}, \hat{P}\right] = 1$

Wigner function
of a vacuum state



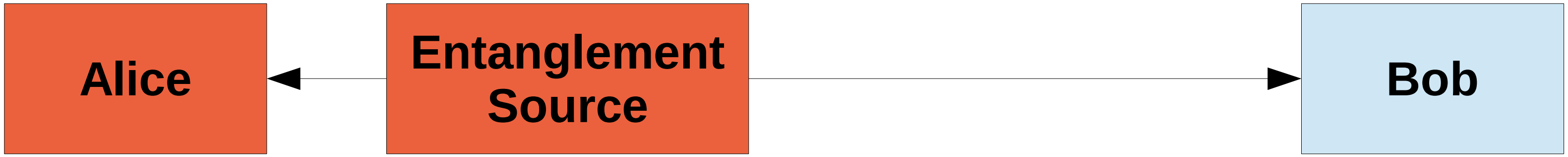
Measurement of Field Quadratures

Homodyne detection

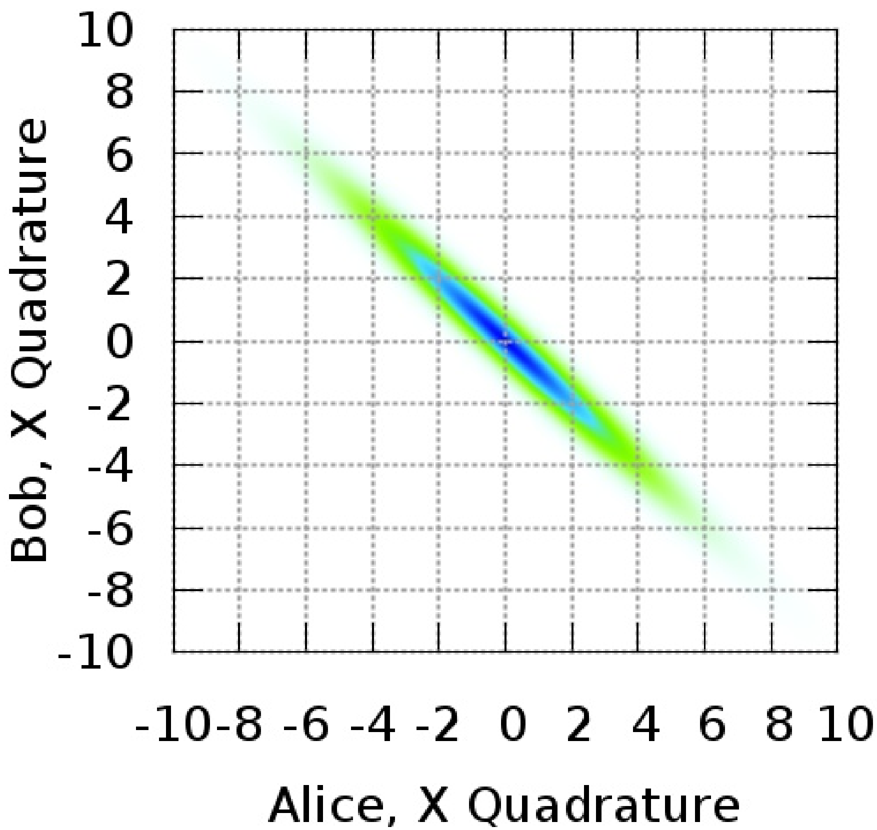


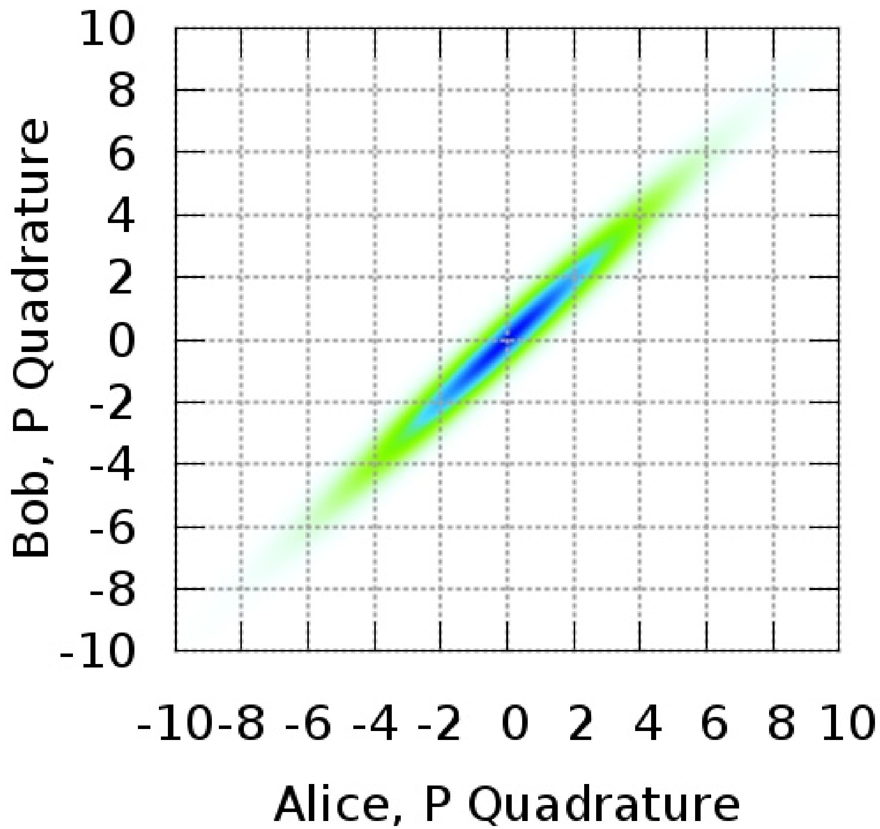
Phase of local oscillator with respect to signal determines measured quadrature

Entanglement based QKD



Simultaneous homodyne measurements at Alice and Bob





Why entanglement based CV QKD?

Gaussian Modulation

- Only standard telecommunication components
  Amplitude, phase modulators,
  PIN photo diodes
- Security analysis for **collective attacks** includes finite-size effects

  A. Leverrier et al., Phys.l Rev. A **81**, 062343 (2010).
- 80 km distance reached

  P. Jouguet et al., Nature Photonics **7**, 378–381 (2013).
- Compatibility with intense DWDM classical channels demonstrated

Security analysis for **arbitrary attacks** including finite-size effects given in

F. Furrer et al., Phys. Rev. Lett. **109**, 100502 (2012).

requires **quadrature entanglement**

Outline

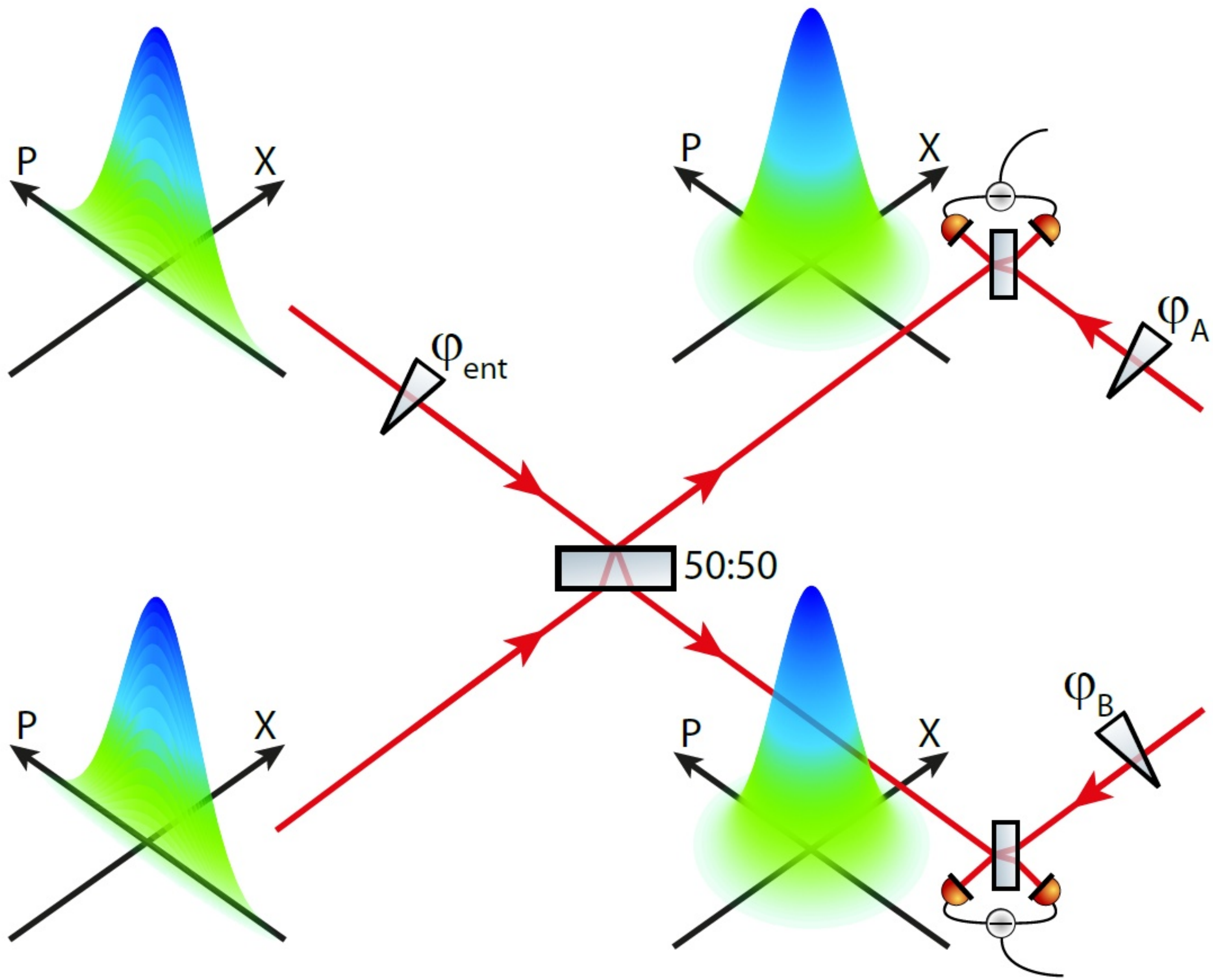
Realization of
Finite-Size Continuous-Variable
Quantum Key Distribution
based on
Einstein-Podolsky-Rosen Entangled Light

1. Einstein-Podolsky Rosen (EPR) Entanglement

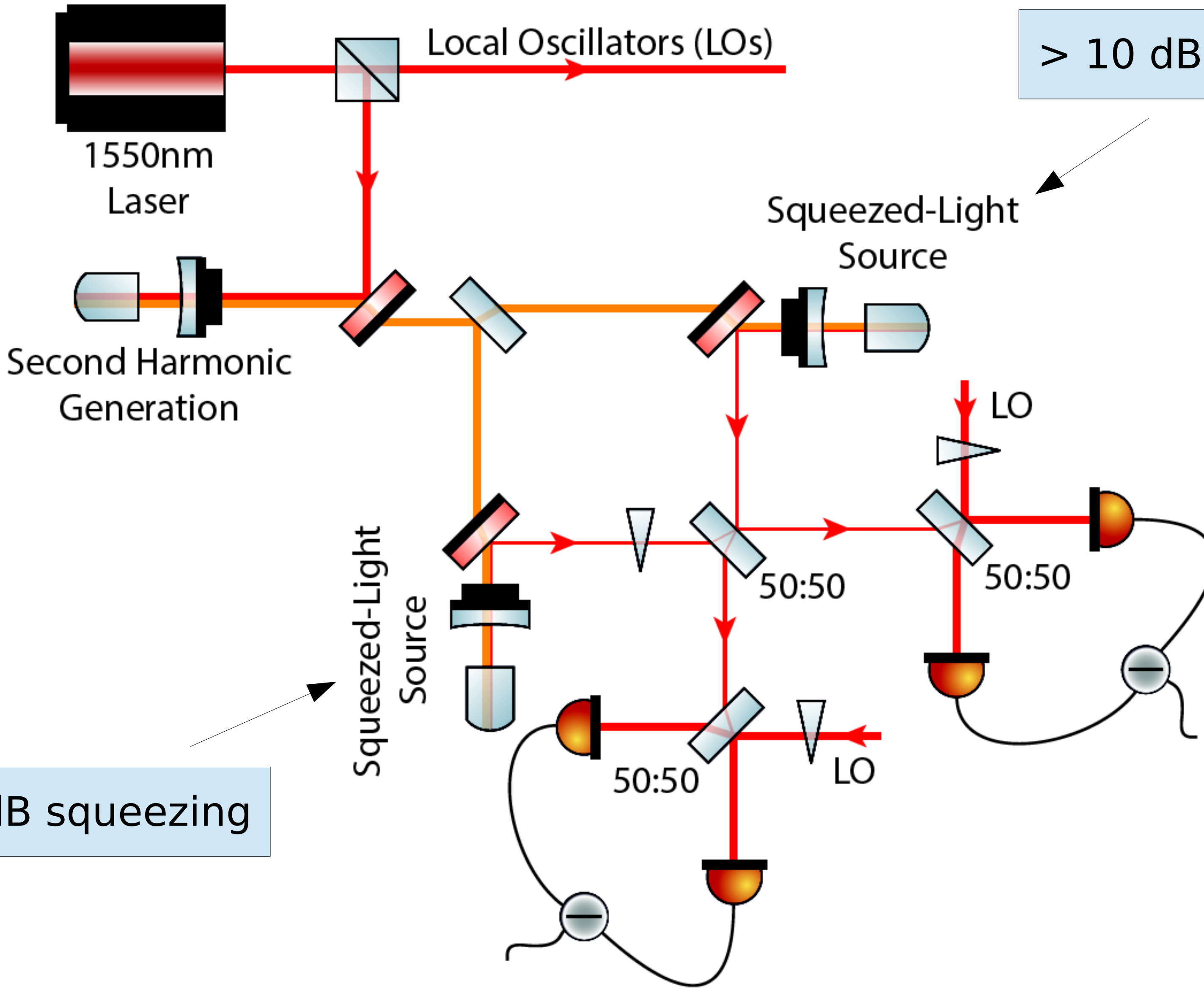
2. Continuous-Variable Quantum Key Distribution

    - Generate a secure key under collective attacks
    - Demonstrate the feasibility to have security under arbitrary attacks

Generation of Quadrature Entanglement



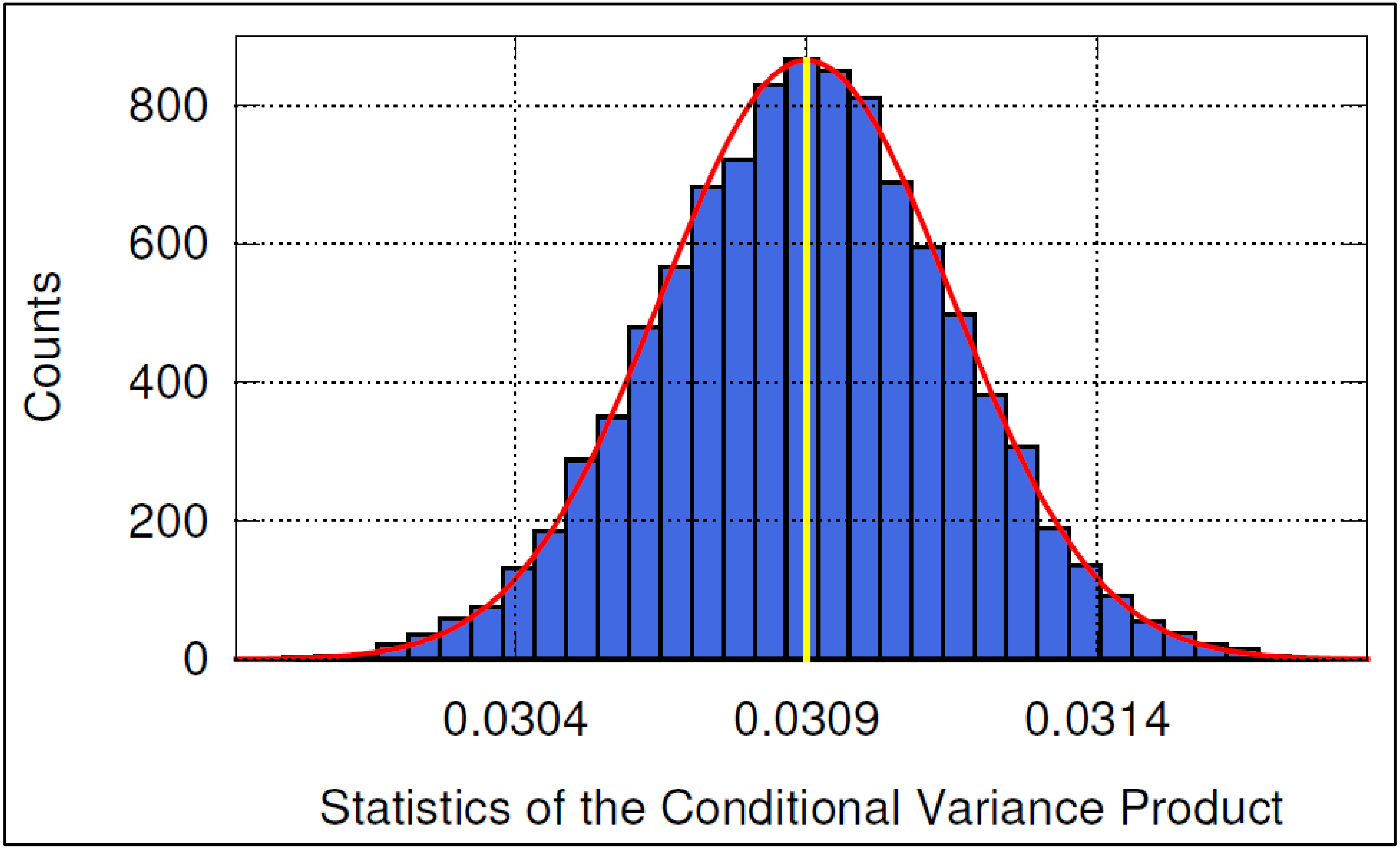
Experimental Setup



> 10 dB squeezing

> 10 dB squeezing

Results: EPR Entanglement

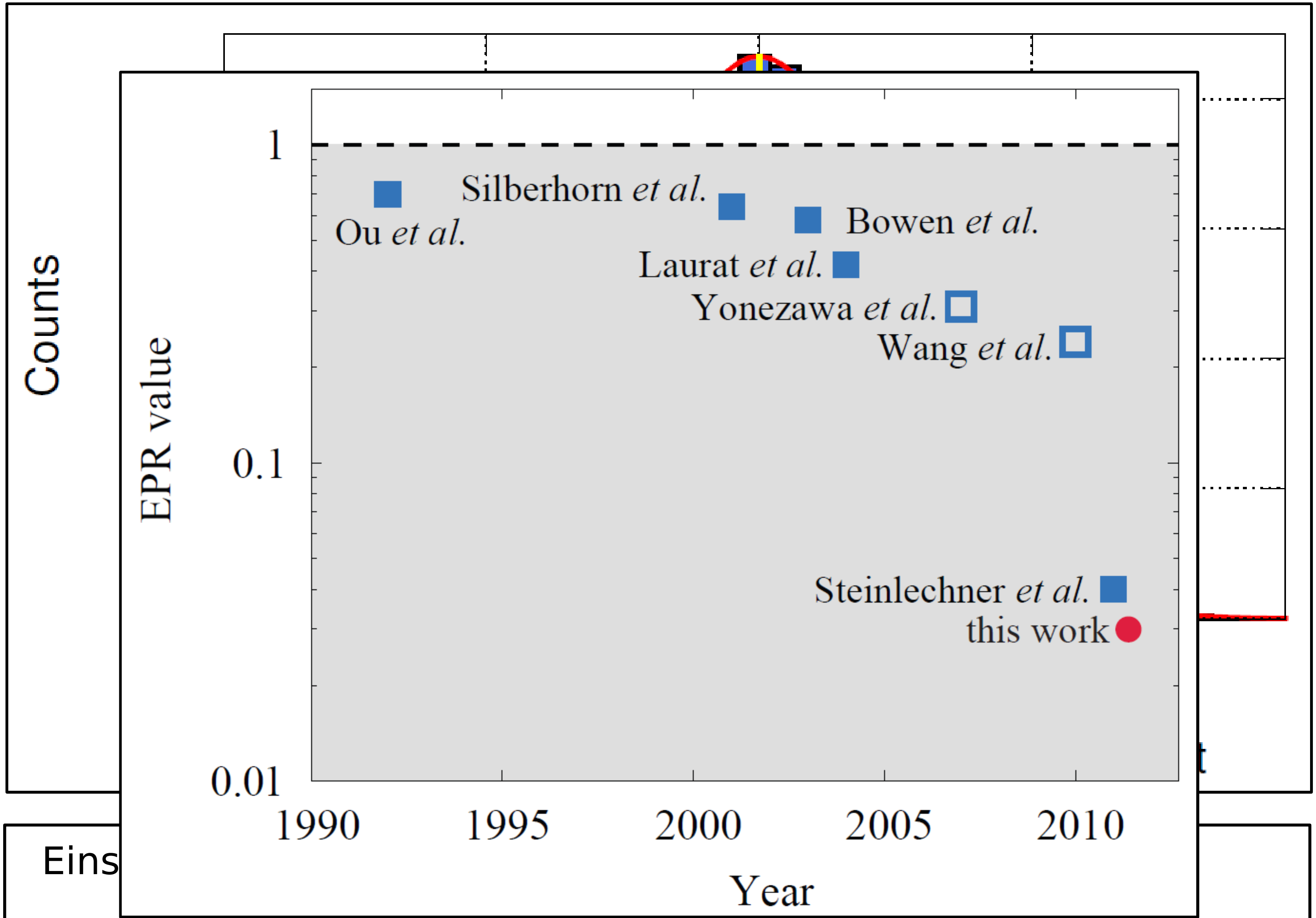


Einstein-Podolsky-Rosen Entanglement:

$$\min_g \mathrm{Var}(\hat{X}_A - g\hat{X}_B) \cdot \min_h \mathrm{Var}(\hat{P}_A - h\hat{P}_B) < 1$$

Reid, Phys. Rev. A **40**, 913 (1989)

Results: EPR Entanglement



Eins

$$\min_g \mathrm{Var}(X_A - gX_B) \; \min_h \mathrm{Var}(Y_A - hY_B) < 1$$

Reid, Phys. Rev. A **40**, 913 (1989)

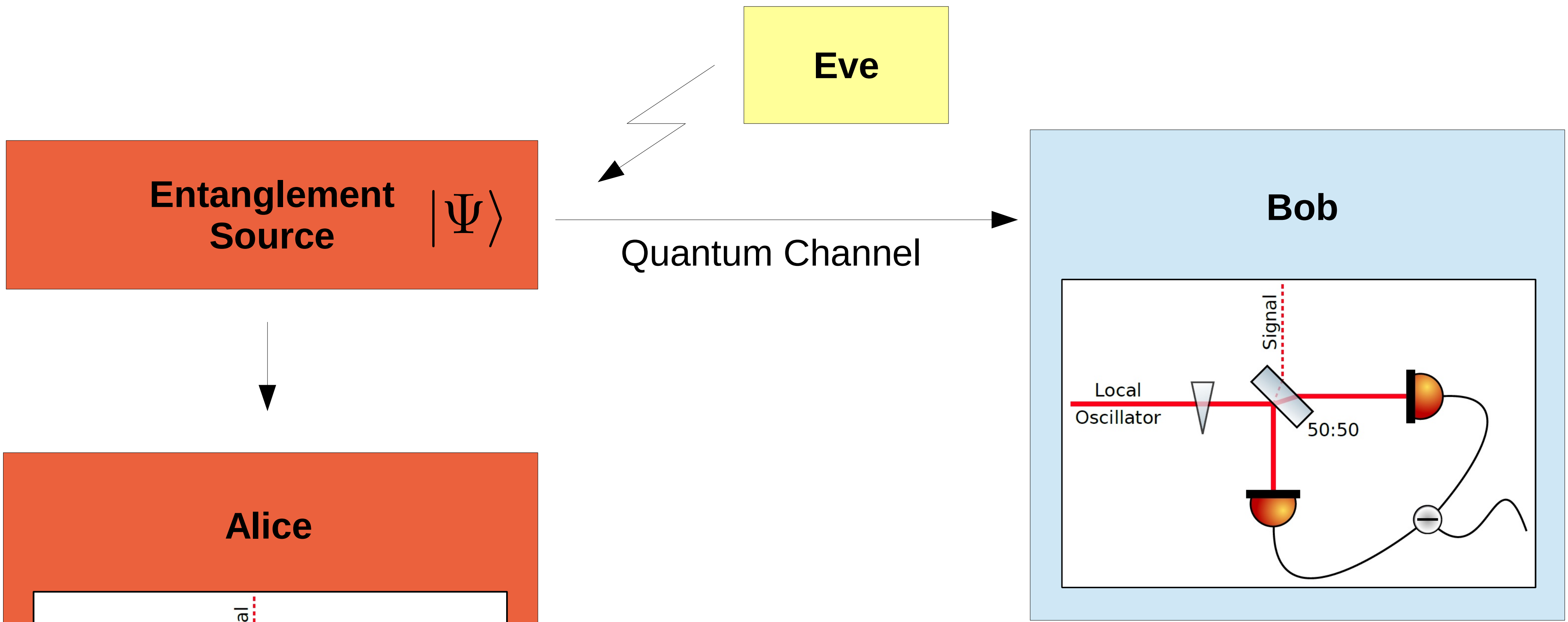
Realization of Finite-Size Continuous-Variable Quantum Key Distribution based on Einstein-Podolsky-Rosen Entangled Light

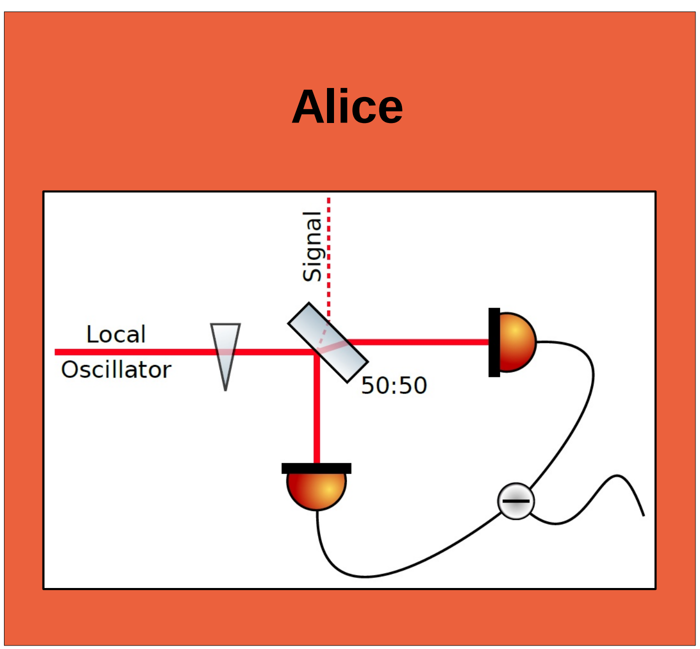
1. Einstein-Podolsky Rosen (EPR) Entanglement

2. Continuous-Variable Quantum Key Distribution

    - Generate a secure key under collective attacks
    - Demonstrate the feasibility to have security under arbitrary attacks

Quantum Key Distribution Scheme





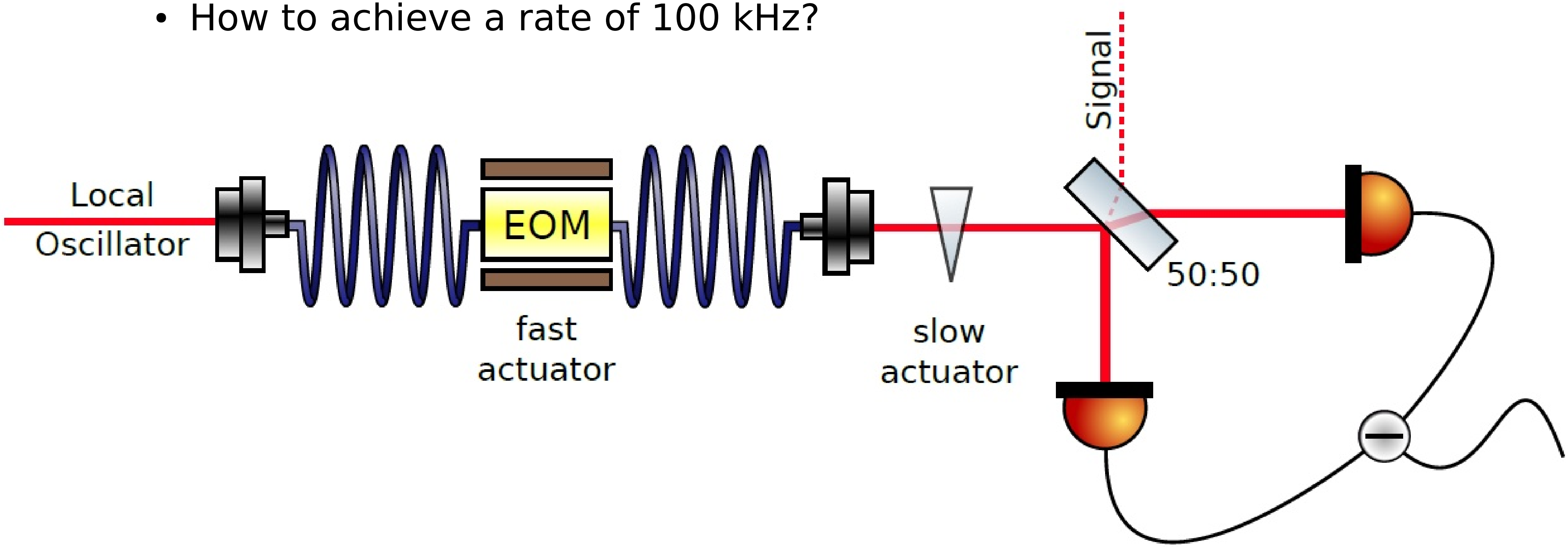
Random choice of quadrature for each measurement

Alice	X	X	P	X	P	P	P	X	...
Bob	P	P	P	X	X	P	P	X	...

Random Quadrature Choice: Implementation

Quantum part of QKD protocol: Measurement of 10^8-10^9 samples necessary

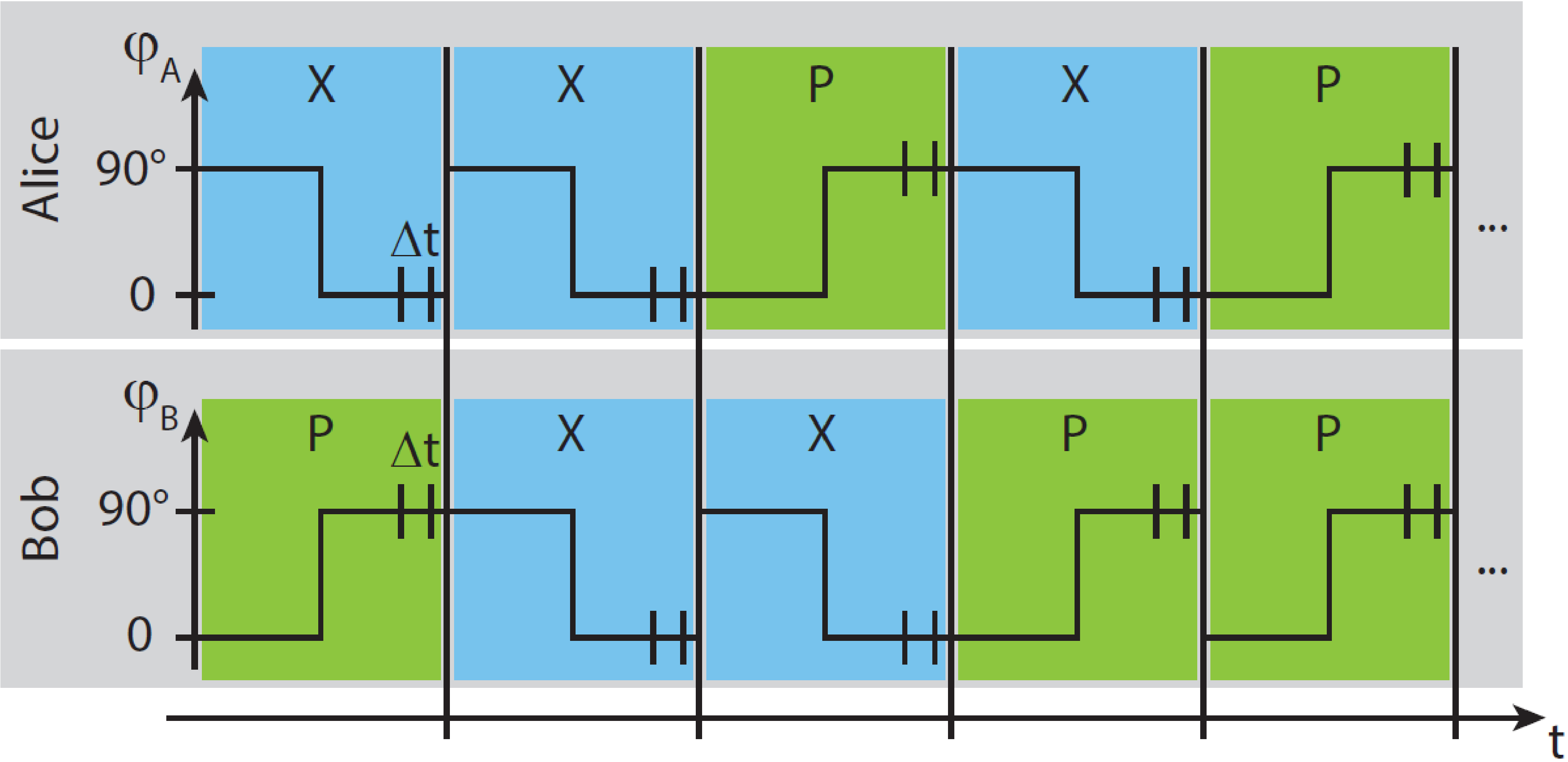
- Usual phase locks have unity gain frequencies < 1kHz
- How to achieve a rate of 100 kHz?



- **Fast phase actuator**: Shifts phase by 0 or 90° with a rate of 100 kHz
- **Slow phase actuator**: Compensates for drifts

Random Quadrature Choice: Implementation

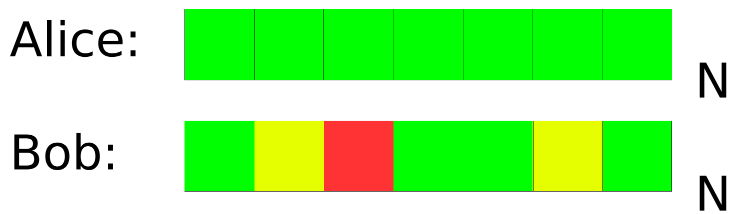
- Low frequency lock averages over phase
- **Problem:** long sequences of X or P measurements
- **Solution:**



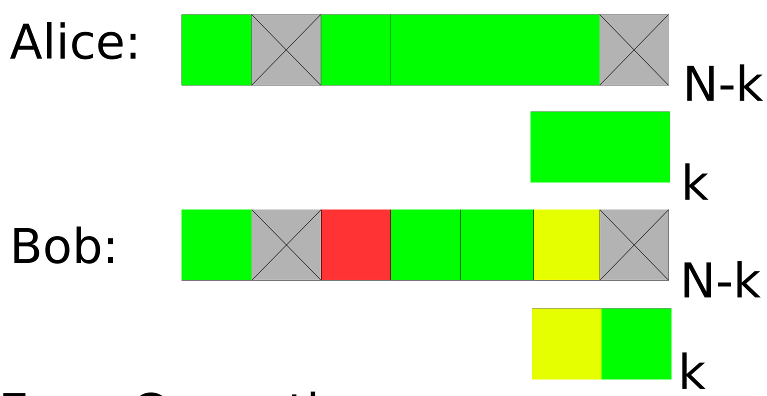
QKD Protocol

2) Sifting: Discard measurements in different quadratures

3) Binning

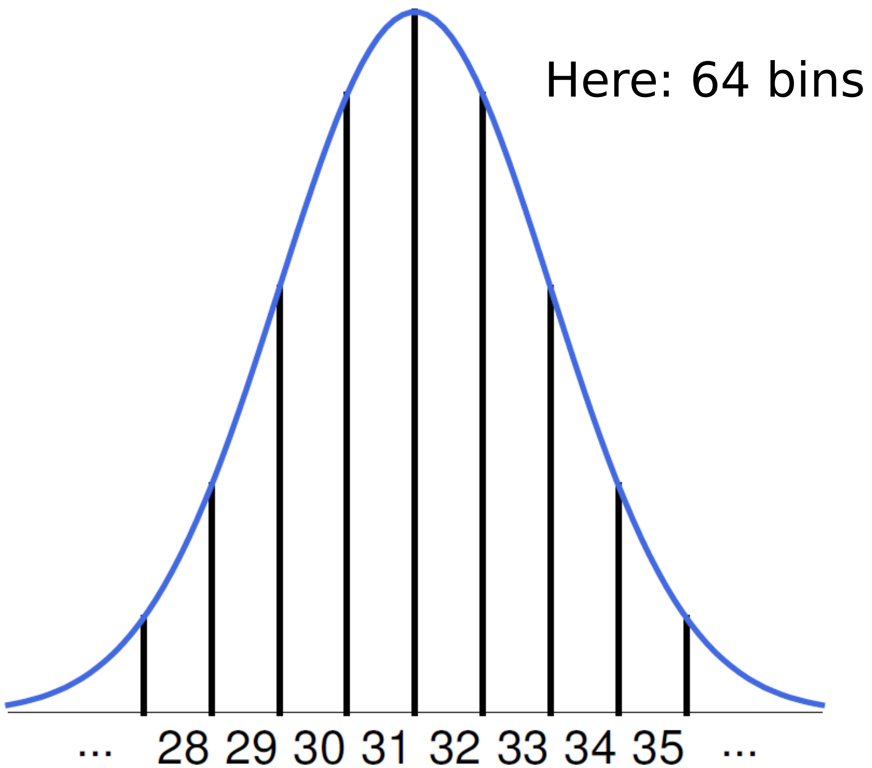


4) Channel Characterization



5) Error Correction

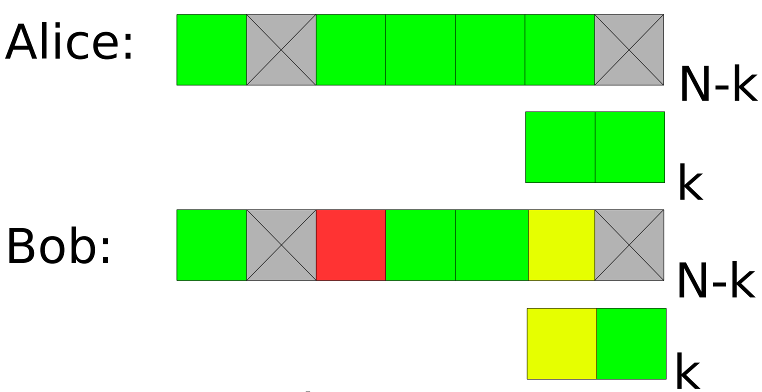
ℓ_{EC} bits disclosed to Eve



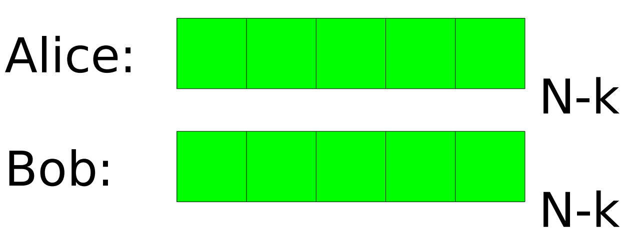
2) Sifting: Discard measurements in different quadratures

3) Binning

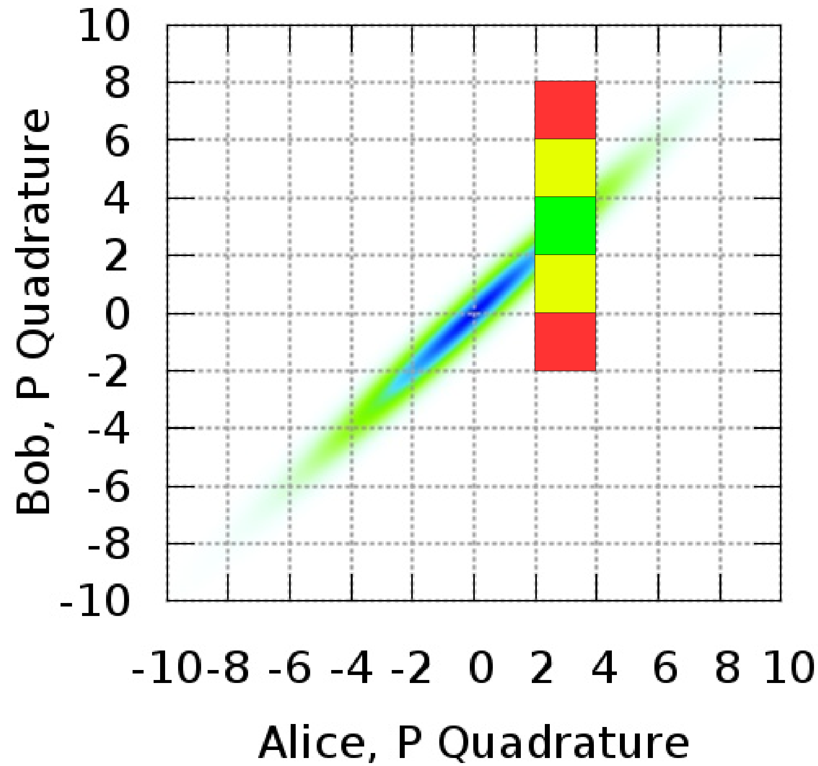
4) Channel Characterization



5) Error Correction



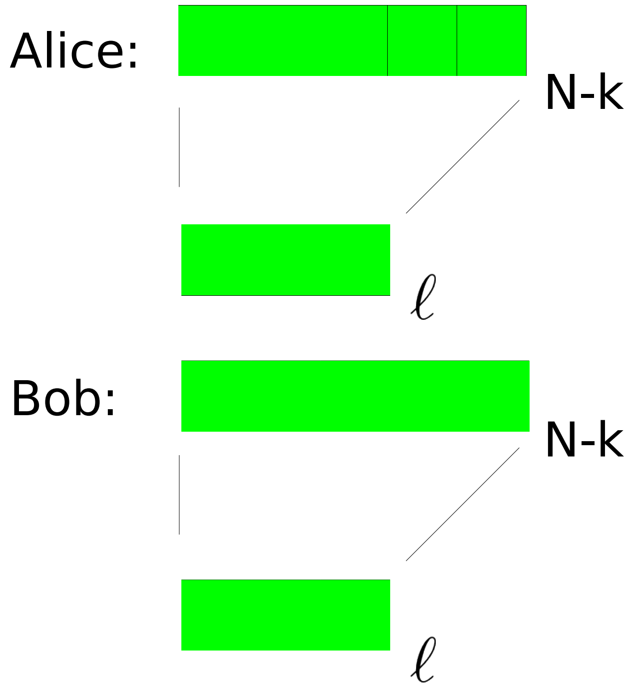
ℓ_{EC} bits disclosed to Eve

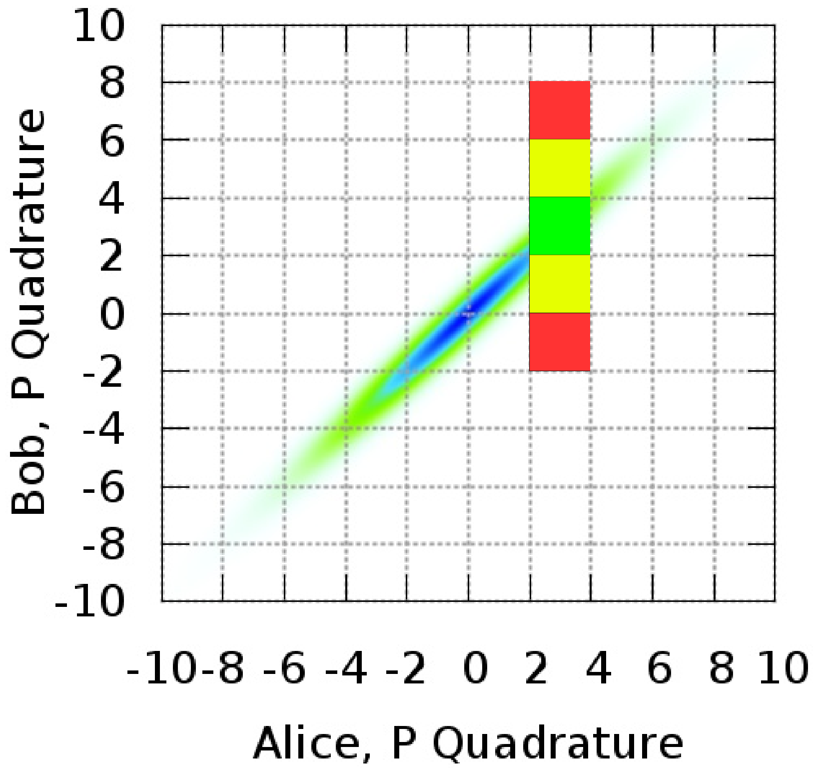


6) Calculate secure key length ℓ

- Use results from channel characterization
- Take ℓ_{EC} into account

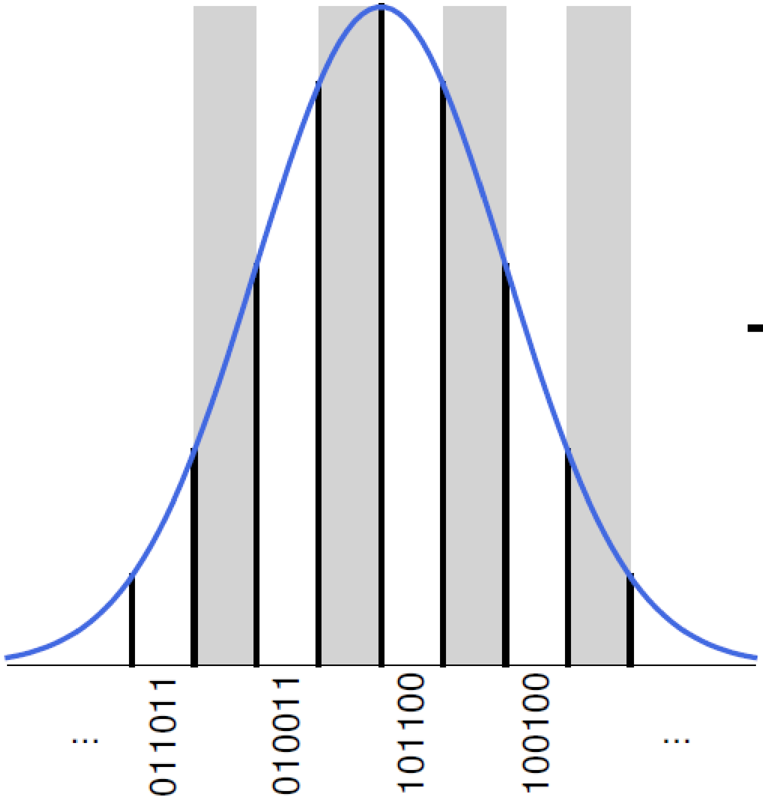
7) Privacy Amplification

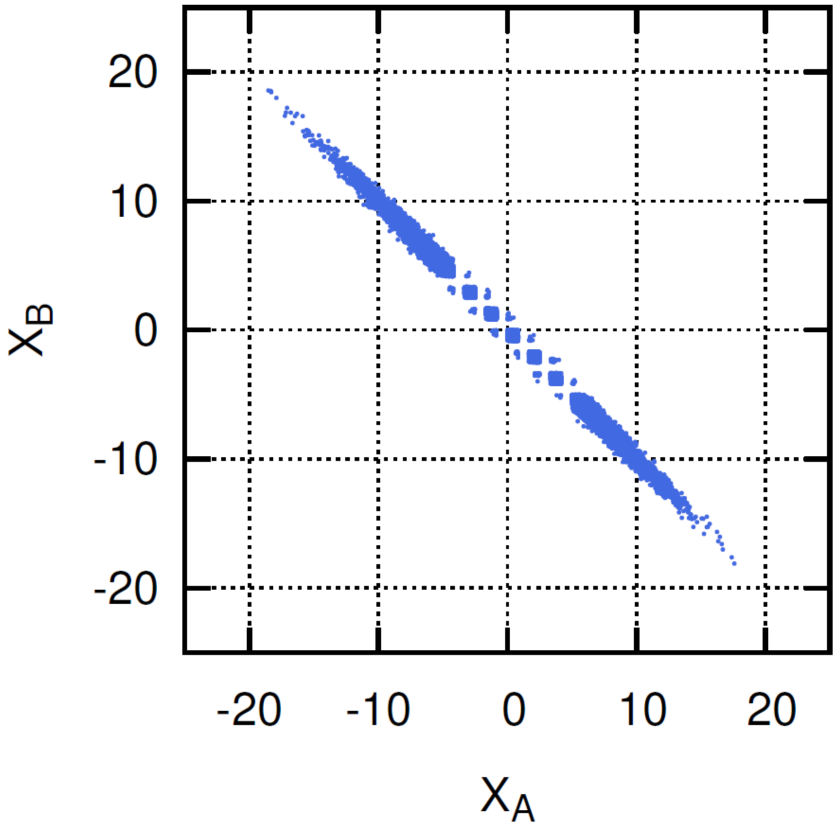




Protocol Execution under Collective Attacks

- Measurement of 10^8 samples
- Bin measurement outcomes into 2^6=64 intervals
- To use binary error correction a simple post selection technique was applied





- Generation of 1.5MB key using an error correction algorithm from AIT

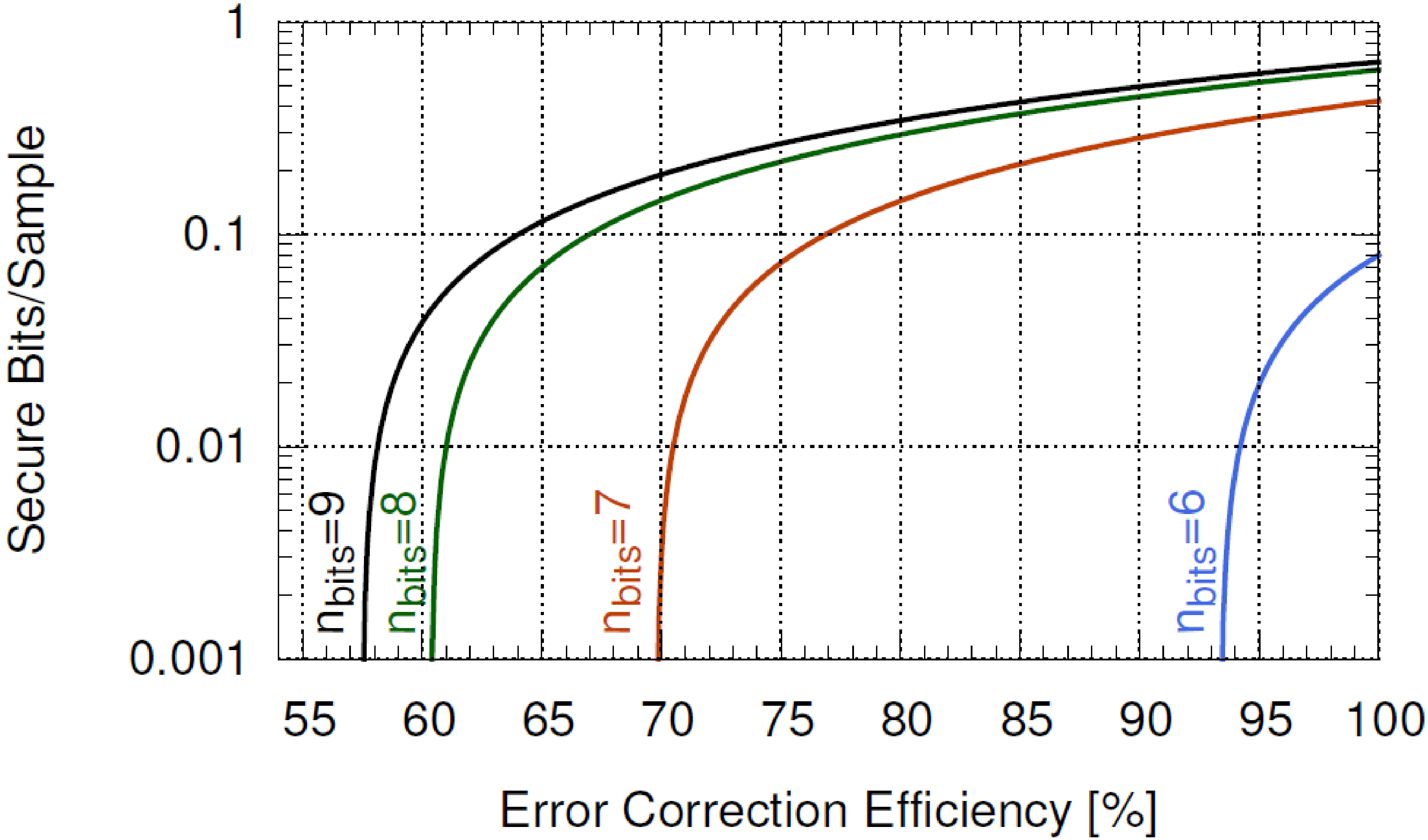
Protocol Execution under Arbitrary Attacks

- Post selection not possible since it is not covered by the security proof

  → Estimation of the necessary non-binary error correction efficiency

$$\ell_{\mathrm{EC}} = H(X_A) - \boxed{\beta} \cdot I(X_A : X_B)$$

$$\beta < 1$$



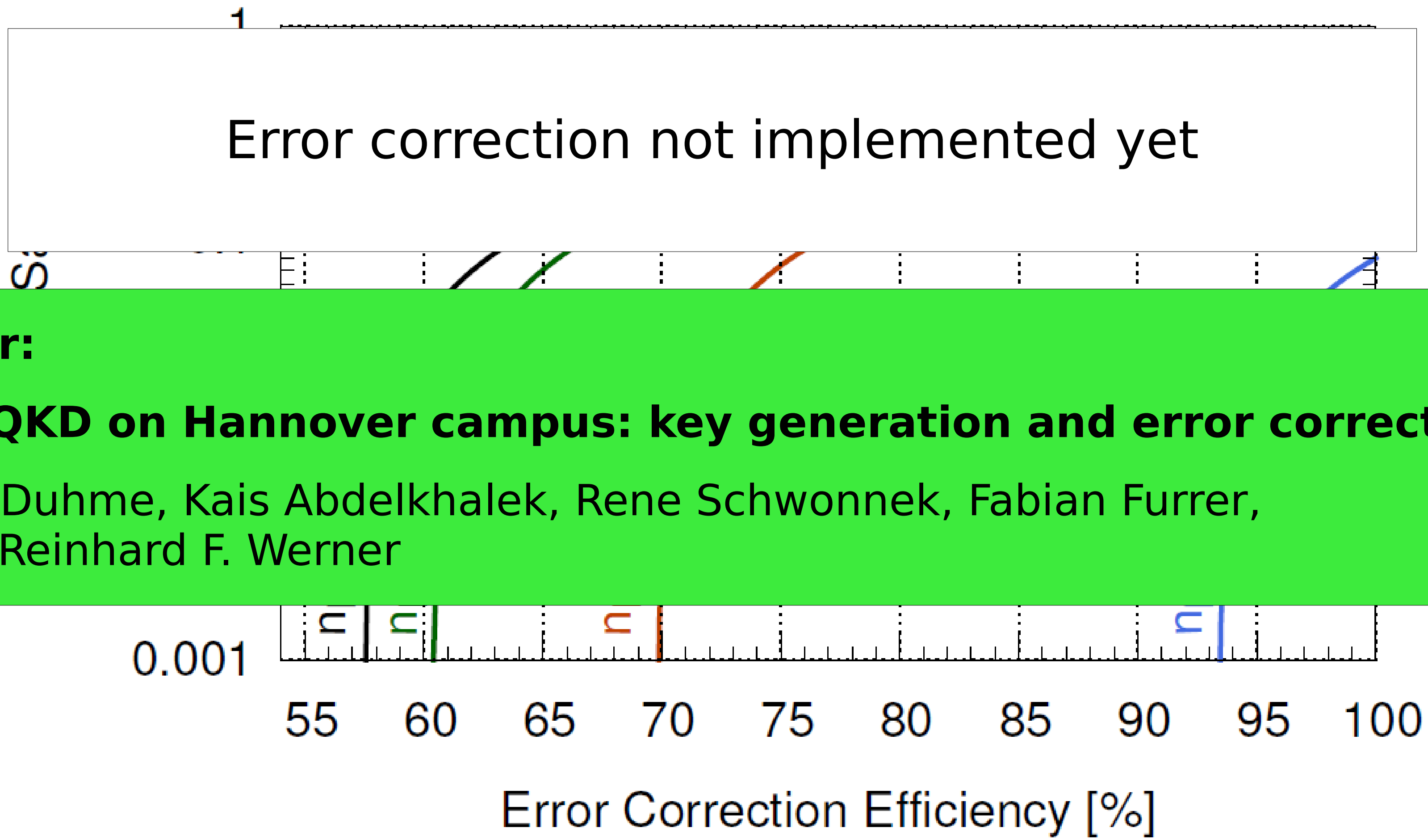
Protocol Execution under Arbitrary Attacks

- Post selection not possible since it is not covered by the security proof

→ Estimation of the necessary non-binary error correction efficiency

$$\ell_{\mathrm{EC}} = H(X_A) - \boxed{\beta} \cdot I(X_A : X_B)$$

$$\beta < 1$$



Error correction not implemented yet

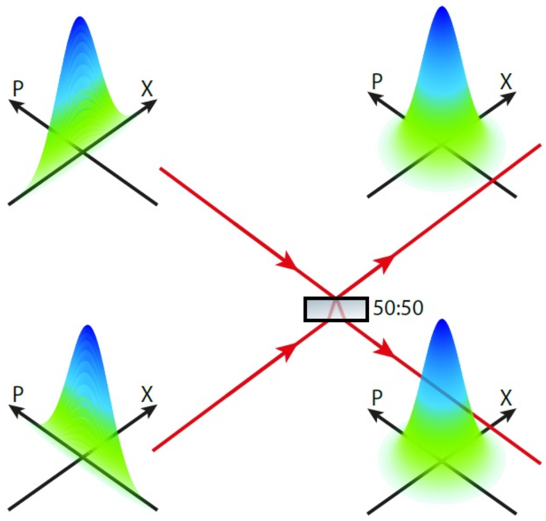
Poster:

CV-QKD on Hannover campus: key generation and error correction

Jörg Duhme, Kais Abdelkhalek, Rene Schwonnek, Fabian Furrer, and Reinhard F. Werner

Summary

Einstein-Podolsky-Rosen Entanglement



- Generation of strong quadrature entanglement

Quantum Key Distribution

- Generation of 1.5MB secret key under collective attacks
- Demonstrated feasibility of QKD under arbitrary attacks