Security of continuous-variable quantum key distribution against general attacks

arXiv: 1208.4920

Anthony Leverrier (ETH Zürich)

with Raúl García-Patrón, Renato Renner and Nicolas J. Cerf

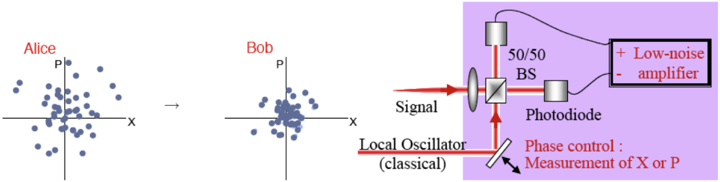
QCRYPT 2012

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Key Distribution with continuous variables

What's different?

- Alice encodes information on the quadratures (X, P) of the EM field
- Bob measures with an homodyne (interferometric) detection



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

Features

- no need for single-photon counters
- compatible with WDM — Bing Qi *et al.* *NJP* **12** 103042 (2010)
- "Gaussian Quantum Information" — C. Weedbrook *et al*, *RMP* **84** 621 (2012)

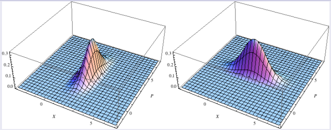
Many protocols

Four Gaussian entangled protocols

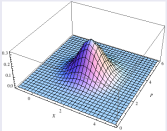
1. Alice prepares N EPR pairs $|\Psi\rangle = \sqrt{1-x^2}\sum_{n=0}^{\infty} x^n |n,n\rangle$
2. for each pair, she keeps one mode and sends the other one to Bob
3. Alice and Bob perform either homodyne or heterodyne detection
   - homodyne = measuring X OR P
   - heterodyne = measuring X AND P (with higher noise)

Prepare and measure versions

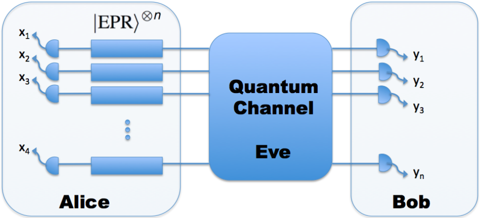
- homodyne meas. for Alice
  ⇔ preparation of a **squeezed state**



- heterodyne meas. for Alice
  ⇔ preparation of a **coherent state**



Description of the protocol



- A and B **measure** ρ_{AB}^n with homodyne/hererodyne detection
  - Alice obtains $\mathbf{x} = (x_1, x_2, \cdots x_n) \in \mathbb{R}^n$
  - Bob obains $\mathbf{y} = (y_1, y_2, \cdots, y_n) \in \mathbb{R}^n$
- **(Reverse) reconciliation**: Bob sends some information to Alice who guesses $\hat{y}$
- **Privacy amplification**: Alice and Bob apply some hash function and obtain (S_A, S_B) plus some transcript C of all classical information

QKD protocol: map $\mathcal{E}$

$$\mathcal{E} : \rho_{AB}^n \longmapsto (S_A, S_B, C)$$

Experimental implementations

- in fiber:
  Qi *el al, PRA* (2007), Lodewyck *et al, PRA* (2007), Fossier *et al, NJP* (2009), Xuan *et al, Opt Exp* (2009) · · ·
- in free space:
  S. Tokunaga *et al, CLEO* (2007), D. Elser *et al, NJP* (2010), B. Heim *et al, APL* (2010) · · ·
- with an entangled source T. Eberle *et al, arXiv preprint* (2011), L. Madsen *et al, arXiv preprint* (2011)

Reliable technology

field test during more than 6 months over around 20 km

P. Jouguet *et al. Opt Expr* **20** 14030 (2012)

Long distance

Current record: over 80 km! ⇒ **see P. Jouguet's talk on Friday!**

What about security?

Security proofs for CV QKD (before 2012)

OK $\cdots$ in the asymptotic limit

- de Finetti theorem for infinite-dimensional quantum systems
  $\Rightarrow$ collective attacks are asymptotically optimal
  R.Renner, J.I. Cirac, *PRL* (2008)
- Gaussian attacks are asymptotically optimal among collective attacks
  R.García-Patrón, N.J. Cerf *PRL* (2006)
  M. Navascués, F. Grosshans, A. Acín *PRL* (2006)

Problems

- de Finetti useless in practical settings: convergence is too slow
- parameter estimation is problematic for CVQKD (unbounded variables)

Two solutions

- Entropic uncertainty relation: $H^{\epsilon}_{\min}(X|E) + H^{\epsilon}_{\max}(P|B) \geq N \log \frac{1}{c(\delta)}$
  F. Furrer *et al, PRL* **109** 100502 (2012) $\Rightarrow$ **see Fabian's talk on Friday!**
- combining the postselection technique (M. Christandl *et al, PRL* 2009) with symmetries in phase space $\Rightarrow$ this talk

Security definition

A protocol $\mathcal{E}$ is secure if it is *undistinguishable from an ideal protocol* $\mathcal{F} : \rho_{AB}^n \longmapsto (S, S, C)$:

- $\mathcal{F}$ outputs the same key S for Alice and Bob
- S is uniformly distributed over the set of keys and uncorrelated with Eve's quantum state:

$$\rho_{SE} = \frac{1}{2^k} \sum |s_1, \cdots, s_k\rangle\langle s_1, \cdots, s_k| \otimes \rho_E.$$

For instance, $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$ where $\mathcal{S}$ replaces (S_A, S_B) by a perfect key (S, S).

ϵ-security: $||\mathcal{E} - \mathcal{F}||_\diamond \leq \epsilon$

$\Rightarrow$ the advantage in distinguishing $\mathcal{E}$ from $\mathcal{F}$ is less than ϵ.

$$||\mathcal{E} - \mathcal{F}||_\diamond := \sup_{\rho_{ABE}} \|(\mathcal{E} - \mathcal{F}) \otimes \mathrm{id}_\mathcal{K}(\rho_{ABE})\|_1$$

How to compute the diamond norm?

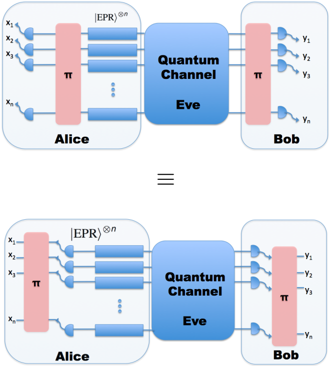
If the maps are permutation invariant: **postselection technique**

M. Christandl, R. König, R. Renner, *PRL* 2009

$\cdots$ **but only for finite dimension**

The postselection technique

For protocol invariant under permutations:



Theorem [Christandl *et al.*]

$$||\mathcal{E}-\mathcal{F}||_\diamond \leq (n+1)^{d^2-1} ||(\mathcal{E}-\mathcal{F})\otimes \mathrm{id}(\tau_{\mathcal{HR}})||_1$$

where

- $d = \dim(\mathcal{H}_A \otimes \mathcal{H}_B)$
- $\tau_{\mathcal{HR}}$ is a purification of $\tau_{\mathcal{H}} = \int \sigma_{\mathcal{H}}^{\otimes n} \mu(\sigma_{\mathcal{H}})$

$||(\mathcal{E}-\mathcal{F})\otimes \mathrm{id}(\tau_{\mathcal{HR}})||_1$ is exponentially small for protocols secure against collective attacks

Security against collective attacks implies security against general attacks if

- the protocol is permutation invariant
- the dimension of $\mathcal{H}_A \otimes \mathcal{H}_B$ is finite

Dealing with infinite dimension

Two ideas

1. We prepend *a test $\mathcal{T}$* to the protocol:
   - if the test succeeds, Alice and Bob continue with the usual protocol
   - otherwise they abort

   The goal of the test is to make sure that the state ρ_{AB}^n contains not too many photons, i.e. is close to a finite dimensional state.
2. The permutation symmetry is not sufficient for the test:
   $\Rightarrow$ we exploit *symmetries in phase space* specific to CV QKD.

Sketch of the proof

Some notations

- $\mathcal{E}_0 : \rho_{AB}^n \mapsto (S_A, S_B, C)$: the usual protocol, secure against collective attacks; and $\mathcal{F}_0 := \mathcal{S} \circ \mathcal{E}_0$ the ideal version
- a test $\mathcal{T} : \rho_{AB}^N \mapsto \rho_{AB}^n \otimes \{\text{pass}/\text{fail}\}$ with $N > n$
- a projection $\mathcal{P} : (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n} \to (\overline{\mathcal{H}}_A \otimes \overline{\mathcal{H}}_B)^{\otimes n}$ with

$$\overline{\mathcal{H}}_A := \mathrm{Span}(|0\rangle, \cdots, |d_A - 1\rangle); \dim(\overline{\mathcal{H}}_A) = d_A < \infty$$

$$\overline{\mathcal{H}}_B := \mathrm{Span}(|0\rangle, \cdots, |d_B - 1\rangle); \dim(\overline{\mathcal{H}}_B) = d_B < \infty$$

- the new protocol of interest: $\mathcal{E} := \mathcal{E}_0 \circ \mathcal{T} : \rho_{AB}^N \mapsto (S_A, S_B, C)$

$$\begin{aligned}
||\mathcal{E} - \mathcal{F}||_\diamond &\leq ||\mathcal{E}_0\mathcal{P}\mathcal{T} - \mathcal{F}_0\mathcal{P}\mathcal{T}||_\diamond + ||\mathcal{E} - \mathcal{E}_0\mathcal{P}\mathcal{T}||_\diamond + ||\mathcal{F} - \mathcal{F}_0\mathcal{P}\mathcal{T}||_\diamond \\
&= ||\mathcal{E}_0\mathcal{P}\mathcal{T} - \mathcal{F}_0\mathcal{P}\mathcal{T}||_\diamond + ||\mathcal{E}_0 \circ (\mathrm{id} - \mathcal{P}) \circ \mathcal{T}||_\diamond + ||\mathcal{F}_0 \circ (\mathrm{id} - \mathcal{P}) \circ \mathcal{T}||_\diamond \\
&\leq \underbrace{||\mathcal{E}_0\mathcal{P}\mathcal{T} - \mathcal{F}_0\mathcal{P}\mathcal{T}||_\diamond}_{\text{Postselection technique}} + \underbrace{2||(\mathrm{id} - \mathcal{P}) \circ \mathcal{T}||_\diamond}_{\text{small for a "good" test}}
\end{aligned}$$

How to choose the test $\mathcal{T}$?

Note: because Eve does not interact with Alice's state, it is sufficient to apply the test on Bob's state ρ_B^N.
Goal: find $\mathcal{T}$ such that $||(\mathrm{id} - \mathcal{P}) \circ \mathcal{T}||_\diamond \leq \epsilon$, i.e.

$$\mathrm{Prob}\left([\text{passing the test}] \quad \text{AND} \quad \left[\max_k m_k \geq d_B\right]\right) \leq \epsilon$$

where m_k is the result of a photon counting measurement of mode k of ρ_B^n.

Idea: photon counting ≈ energy measurement ≈ heterodyne detection

$\mathcal{T}$ should be easy to implement: one measures $m := N - n$ modes with heterodyne detection:

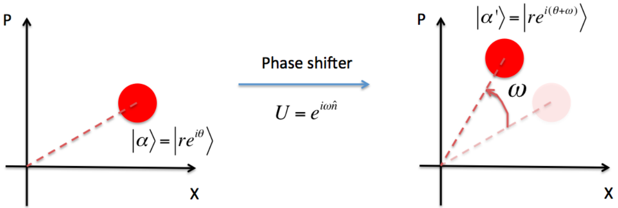
- results: $\mathbf{z} = (z_1, z_2, \cdots, z_{2m})$
- given $\mathbf{z}$, pass or fail

Permutation symmetry is not sufficient

In fact, even independence is not sufficient.
Ex: $\rho^N = \sigma^{\otimes N}$ with $\sigma = (1-\delta)|0\rangle\langle 0| + \delta |N\rangle\langle N|$. The probability of passing the test is large, but the projection will fail if $\delta = O(1/N)$.

Transformations in phase space

$\mathcal{U} \cong U(n)$: group generated by phase shifts and beamsplitters
$\Rightarrow$ act like orthogonal transformations in phase space.



Action of phase shits and beamsplitters on *n* modes

There exists $U \in U(n)$: $V = \mathrm{Re}(U)$ and $W = -\mathrm{Im}(U)$

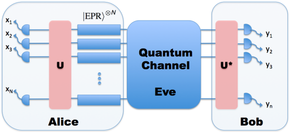
$$\mathbf{a} \to U\mathbf{a}; \qquad \mathbf{a}^\dagger \to U^*\mathbf{a}^\dagger$$

$$\begin{pmatrix} \mathbf{X} \\ \mathbf{P} \end{pmatrix} \to \begin{pmatrix} V & W \\ -W & V \end{pmatrix} \begin{pmatrix} \mathbf{X} \\ \mathbf{P} \end{pmatrix}$$

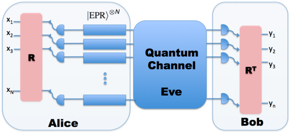
$\Rightarrow$ *U* commutes with a heterodyne detection

Symmetry in phase space

For any linear passive transformation in phase space U (corresponding to a ***network of beamsplitters and phase shifts***), there exists an orthogonal transformation in $\mathbb{R}^{2N}$ such that:



$\equiv$



One can assume that

- ρ_{AB}^N is invariant under $U_A \otimes U_B^*$
- $U \rho_B^N U^\dagger = \rho_B^N \quad \forall U$.

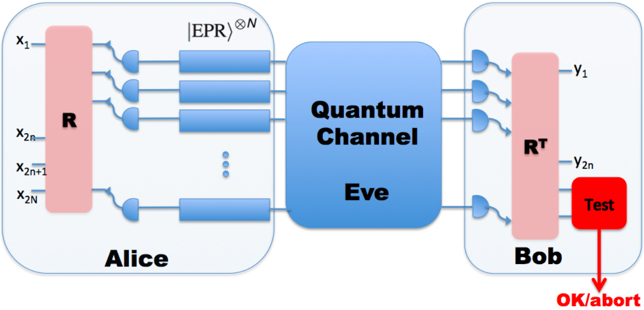
$\Rightarrow \rho_B^N = \sum_{k=0} \lambda_k \sigma_k^n$

$$\sigma_k^n = \frac{1}{\binom{n+k-1}{k}} \sum_{k_1+\cdots+k_N=k} |k_1 \cdots k_N\rangle\langle k_1 \cdots k_N|$$

ρ_B^N is a mixture of generalized N-mode Fock states
$\Rightarrow$ very unlikely to pass the test and fail the projection $\mathcal{P}$

The vector $(\mathbf{X}, \mathbf{P}) \in \mathbb{R}^{2n}$ is uniformly distributed on the sphere of radius $\sqrt{||\mathbf{X}||^2 + ||\mathbf{P}||^2} \Rightarrow$ concentration of measure on the sphere.

The test



Bob computes:

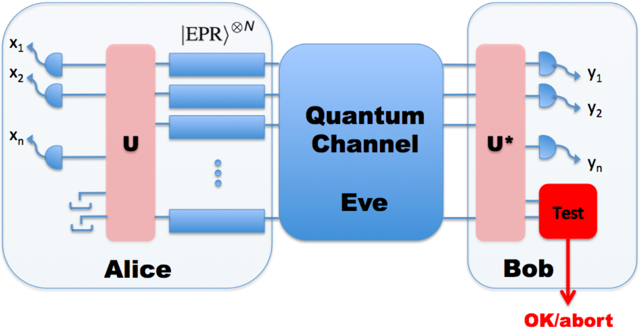
$$Z := y_{2n+1}^2 + y_{2n+2}^2 + \cdots + y_{2N}^2$$

- If $Z \leq (N-n)Z_{\text{test}}$, Alice and Bob continue
- otherwise, they abort

Concentration of measure:

$$\text{Prob}\left([\text{test succeeds}] \quad \text{AND} \quad \left[y_1^2 + \cdots + y_{2n}^2 \geq n\left(Z_{\text{test}} + \delta\right)\right]\right) \leq \epsilon$$

The test



Bob computes:

$$Z := y_{2n+1}^2 + y_{2n+2}^2 + \cdots + y_{2N}^2$$

- If $Z \leq (N-n)Z_{\text{test}}$, Alice and Bob continue
- otherwise, they abort

Concentration of measure:

$$\text{Prob}\left([\text{test succeeds}] \quad \text{AND} \quad \left[y_1^2 + \cdots + y_{2n}^2 \geq n\left(Z_{\text{test}} + \delta\right)\right]\right) \leq \epsilon$$

Sketch of the proof

- $\mathrm{Prob}\left([\text{pass test}] \quad \text{AND} \quad \sum_{i=1}^n X_i^2 + P_i^2 \geq C_1 n\right) \leq \epsilon_{\mathrm{test}}$
- $\mathrm{Prob}\left([\text{pass test}] \quad \text{AND} \quad \sum_{i=1}^n \hat{n}_i \geq C_2 n\right) \leq \epsilon_{\mathrm{test}}$
- $\mathrm{Prob}\left([\text{pass test}] \quad \text{AND} \quad \max \hat{n}_i \geq C_3 \log \frac{n}{\epsilon_{\mathrm{test}}}\right) \leq \epsilon_{\mathrm{test}}$

for some explicit constants C_1, C_2, C_3

Putting all together

- choose $d_A, d_B = O\left(\log \frac{n}{\epsilon_{\mathrm{test}}}\right)$
- postselection technique: if $\mathcal{E}_0$ is ϵ_0-secure against collective attacks, then $\mathcal{E}$ is ϵ-secure against general attacks with

$$\epsilon = \epsilon_0 2^{O\left(\log^4 (n/\epsilon_{\mathrm{test}})\right)} + 2\epsilon_{\mathrm{test}}.$$

ok because one can take $\epsilon_0 = 2^{-cn}$.

Conclusion

Summary

We show that *collective attacks are optimal* for Gaussian protocols thanks to two ideas

- prepending an test to the usual protocol *to truncate* the Hilbert space
- permutation symmetry is not sufficient to prove security: one needs rotation invariance in phase space

Open questions

Our proof is somewhat suboptimal: first, we truncate, then we use the finite-dimensional postselection technique

- Can we generalize the technique for maps which are symmetric in phase space?
- Same question for de Finetti theorem (only partial results are known)