Security proofs for continuous-variable QKD

Anthony Leverrier

Inria Paris

Recent advances in CV quantum information theory

7 April 2016, Barcelona

Executive summary

According to the introduction of a lot of papers, everything looks ok...

Executive summary

According to the introduction of a lot of papers, everything looks ok...

But in fact, the issue is far from settled:

- Gaussian attacks **are NOT known** to be optimal, **even in the asymptotic limit!** (except for one protocol)
- finite-size security available only for a single protocol (squeezed states and homodyne detection)

Executive summary

According to the introduction of a lot of papers, everything looks ok...

But in fact, the issue is far from settled:

- Gaussian attacks **are NOT known** to be optimal, **even in the asymptotic limit!** (except for one protocol)
- finite-size security available only for a single protocol (squeezed states and homodyne detection)

To be clear, except for these 2 protocols, we don't even know how to bound the Devetak-Winter bound:

$$I(A;B) - \chi(A;E)$$

Continuous-variable QKD

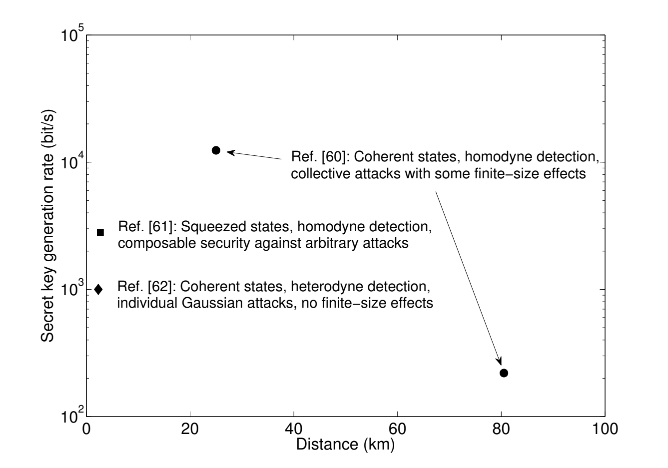
QKD with continuous variables

- quite recent — T.C. Ralph **PRA 61** 010303(R) (1999)
- information encoded on the quadratures (X, P) of the EM field
- measured with homodyne / heterodyne (interferometric) detection
- **infinite dimension $\Rightarrow$ usual proof techniques don't apply**

With coherent states

- much more practical! — Grosshans, Grangier **PRL 88**, 057902 (2002)
- Alice sends coherent states $|\alpha\rangle$, with $\alpha \sim \mathcal{N}(0, V_A)_{\mathbb{C}}$
- Bob measures with homodyne or heterodyne detection
- no need for single-photon counters
- no need for squeezing, only standard telecom components
- additional symmetries: useful for security analysis

Experimental results



[60] Jouguet *et al*, **Nat. Photon. 7** 378–381 (2013): Gaussian attacks in finite size regime
[61] Gehring *et al* **Nat.Comm. 6** 8795 (2015): composable security in finite size regime
[62] Lance *et al* **Phys. Rev. Lett. 95** 180503 (2005): Gaussian attacks in asympt. regime

Prepare-and-Measure *vs* Entanglement-based

Prepare-and-Measure (*i.e.* most implementations)

- Protocol characterized by
  - input states: coherent or squeezed
  - modulation: Gaussian, discrete...
  - Bob's measurement: homodyne or heterodyne
- For ex, Alice prepares the cq state: $\rho_{X^n B_0^n} = \bigotimes_{i=1}^n \int \mathrm{d}x_i p(x_i) |x_i\rangle\langle x_i| \otimes |\Phi_{x_i}\rangle\langle\Phi_{x_i}|$
- State after quantum channel: $\mathcal{N} : B_0^{\otimes n} \to B^{\otimes n}$:

$$\rho_{X^n B^n} = \left(\bigotimes_{i=1}^n \int \mathrm{d}x_i p(x_i) |x_i\rangle\langle x_i| \right) \otimes \mathcal{N}\left(\bigotimes_{i=1}^n |\Phi_{x_i}\rangle\langle\Phi_{x_i}| \right)$$

- Joint classical distribution after Bob's measurement: $\mathcal{M}_B : B^{\otimes n} \to Y^{\otimes n}$

$$\begin{aligned}\rho_{X^n Y^n} &= \left(\bigotimes_{i=1}^n \int \mathrm{d}x_i p(x_i) |x_i\rangle\langle x_i| \right) \otimes \mathcal{M}_B\left(\mathcal{N}\left(\bigotimes_{i=1}^n |\Phi_{x_i}\rangle\langle\Phi_{x_i}| \right)\right) \\ &= \int \mathrm{d}\mathbf{x}\mathrm{d}\mathbf{y}\, \tilde{p}(\mathbf{x},\mathbf{y}) |x_1 \cdots x_n, y_1 \cdots y_n\rangle\langle x_1 \cdots x_n, y_1 \cdots y_n|\end{aligned}$$

- security is difficult to analyze for the Prepare-and-Measure protocol
- requires a statement that holds for any quantum channel $\mathcal{N} : B_0^{\otimes n} \to B^{\otimes n}$

Prepare-and-Measure *vs* Entanglement-based

E-B protocol: purification of Alice's system

- Note that the state $\rho_{X^n B^n}$ can result from Alice's measurement on an entangled bipartite state: $\mathcal{M}_A : A^{\otimes n} \to X^{\otimes n}$

$$\begin{aligned} \rho_{X^n B^n} &= (\mathcal{M}_A \otimes \mathrm{id}_B)(\rho_{A^n B^n}) \\ &= (\mathcal{M}_A \otimes \mathcal{E})(\rho_{A^n B_0^n}) \end{aligned}$$

  where $\mathcal{M}_A$ is controlled by Alice.
- for many protocols, $\mathcal{M}_A$ and $\rho_{A^n B_0^n}$ are rather simple:
  e.g., heterodyne measurement on two-mode squeezed vacuum states $\Leftrightarrow$ Gaussian modulation of coherent states
- to prove security, one should consider all possible states $\rho_{A^n B^n}$
- usually simpler than considering channels

Composable security in QKD

QKD protocol = CPTP map $\mathcal{E}$

$$\begin{array}{rccc} \mathcal{E}: & \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} & \to & \mathcal{S}_A \otimes \mathcal{S}_B \otimes \mathcal{C} \\ & \rho_{A^n B^n} & \mapsto & \rho_{S_A, S_B, C}. \end{array}$$

It doesn't really matter what Eve does: wlog, she holds a system E that purifies $\rho_{A^n B^n}$.

Requirements

- correctness: $\mathbb{P}[S_A \neq S_B] \leq \epsilon_{\mathrm{corr}}$
- secrecy: $\frac{1}{2} \left\| \rho_{S_A E} - \left(\frac{1}{2^k} \sum_{\vec{k}} |\vec{k}\rangle\langle\vec{k}| \right) \otimes \rho_E \right\|_1 \leq \epsilon_{\mathrm{sec}}$
- $\mathcal{E}$ is ϵ-secure if $\epsilon_{\mathrm{corr}} + \epsilon_{\mathrm{sec}} \leq \epsilon$
- robustness: $p_{\mathrm{abort}} = \epsilon_{\mathrm{rob}}$ (small!) if passive adversary

In other words, for any purification $|\Psi\rangle_{ABE}$ of $\rho_{A^n B^n}$,

$$(\mathcal{E}_{AB} \otimes \mathrm{id}_E)|\Psi\rangle_{ABE} \approx_\epsilon \left[\frac{1}{2^k} \sum_{\vec{k}} |\vec{k}, \vec{k}\rangle\langle\vec{k}, \vec{k}| \right]_{AB} \otimes \rho_E$$

where $\mathcal{H}_A, \mathcal{H}_B$ are n-mode Fock spaces.

Different notions of security

Denote $\rho_{S_A S_B E} = \mathcal{E}_{AB} \otimes \mathrm{id}_E(\rho_{A^n B^n E})$ and $\tau_{SS} = \frac{1}{2^k} \sum_{\mathbf{k}} |\mathbf{k}, \mathbf{k}\rangle\langle \mathbf{k}, \mathbf{k}|$

From strongest to weakest:

1. **Composable security against arbitrary attacks**:

   if explicit bound on $\frac{1}{2} \left\| \rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E \right\|_1 \leq \varepsilon$ for any $\rho_{A^n B^n E}$
2. **Composable security against collective attacks**:

   same, but restricted to $\rho_{A^n B^n} = (\rho_{AB})^{\otimes n}$

- (2) $\implies$ (1) thanks to de Finetti [Renner,Cirac PRL 2009] but with **huge loss** in ε

Different notions of security

Denote $\rho_{S_A S_B E} = \mathcal{E}_{AB} \otimes \mathrm{id}_E(\rho_{A^n B^n E})$ and $\tau_{SS} = \frac{1}{2^k} \sum_{\mathbf{k}} |\mathbf{k}, \mathbf{k}\rangle\langle \mathbf{k}, \mathbf{k}|$

From strongest to weakest:

1. **Composable security against arbitrary attacks**:

   if explicit bound on $\frac{1}{2} \left\| \rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E \right\|_1 \leq \varepsilon$ for any $\rho_{A^n B^n E}$
2. **Composable security against collective attacks**:

   same, but restricted to $\rho_{A^n B^n} = (\rho_{AB})^{\otimes n}$
3. **Asymptotic security against collective attacks** assuming the covariance matrix of ρ_{XY} is known $\Rightarrow$ **not composable!**

   if known upper bound on $\chi(X; E)$ (Devetak-Winter formula)

- (2) $\Longrightarrow$ (1) thanks to de Finetti [Renner,Cirac PRL 2009] but with **huge loss** in ε
- (3) uses Gaussian optimality: [Wolf et al PRL 2005], [Garcia-Patron, Cerf PRL 2006], [Navascues, Grosshans Acin PRL 2006]
  (3) + de Finetti $\not\Longrightarrow$ (1)
- Important **unproven** conjecture: Gaussian attacks are optimal

Main message of this talk

- de Finetti and "extremality of Gaussian states" are **not sufficient** to establish security against general attacks
- Gaussian attacks are well understood [Pirandola *et al.*, *PRL* 2008]
  but we don't know whether they are optimal, even in the asymptotic limit

- The issue lies in the estimation of the classical covariance matrix $\Gamma(\rho_{XY})$ which is unbounded a priori.
  $\Longrightarrow$ discrete-variable tomography techniques don't apply!

- For almost all protocols (except coh. states + heterodyne), no explicit procedure to estimate $\Gamma(\rho_{XY})$

Parameter Estimation: the issue

One needs to define a protocol $\mathcal{PE}(n, \varepsilon)$:

For any state $\rho^{\otimes n} \in \mathcal{H}^{\otimes n}$:

1. fix $k \leq n$, the number of samples
2. observe k subsystems (e.g. k copies of ρ)
3. output a confidence region $\mathcal{R}_{\varepsilon,n}$ for the CM of the $n-k$ remaining subsystems such that
$$\Pr[\Gamma(\rho^{\otimes(n-k)}) \in \mathcal{R}_{\varepsilon,n}] \geq 1-\varepsilon$$

Asymptotic limit

Take $n \to \infty$ and hope that $\mathrm{size}(\mathcal{R}_{\varepsilon,n}) \to 0 \quad$ and $\quad \varepsilon \to 0$

Problem

For any $\mathcal{PE}(n, \varepsilon)$ as above, there exists ρ that makes the protocol fail:

e.g. $\rho = (1-\delta)|0\rangle\langle 0| + \delta |N\rangle\langle N|, \quad \Gamma = \begin{bmatrix} 1+N\delta/2 & 0 \\ 0 & 1+N\delta/2 \end{bmatrix}$

But tomographic procedure that only examines $k \ll 1/\delta$ modes will conclude $\Gamma \approx \mathbb{1}$, which is clearly incorrect if $N\delta \gg 1$.

Parameter Estimation: the issue

Solutions

1. Assume finite higher moments $\Rightarrow$ no composable security...
2. Assume a Gaussian distribution $\Rightarrow$ no composable security...
3. Symmetrize the state! ok for protocol with coherent states and heterodyne detection [AL, *PRL* 2015]

OPEN PROBLEM

robust estimation of CM with homodyne detection

Recall that a QKD protocol is essentially a tomographic procedure that checks that A and B are sufficiently "correlated" to decide whether they can distill a secret key.
$\Longrightarrow$ Parameter estimation is the central part of any security proof, not a simple technicality

Current security status of the main CVQKD protocols

Protocol	(PM) State preparation	(PM) Modul.	Bob's measurement	Best available security proofs
Cerf-Levy -van Assche 2001	squeezed	Gaussian	homo	composable [Furrer et al *PRL* 2012] $K^{\varepsilon}(N) > 0$ for practical N $\lim_{N\to\infty} K^{\varepsilon}(N) < K_{\text{coll}}^{\text{asympt}}$
Weedbrook *et al* 2004 (also MDI CVQKD)	coherent	Gaussian	hetero	composable [AL *PRL* 2015] $K_{\text{coll}}^{\varepsilon}(N) \approx K_{\text{coll}}^{\text{asympt}}$ for pract. N $K^{\varepsilon}(N) = 0$ for practical N [AL *et al PRL* 2013]
Grosshans -Grangier 2002	coherent	Gaussian	homo	asympt. collective assum. CM [GC *PRL* 2006], [NGA *PRL* 2006]
Usenko - Grosshans 2015	coherent	Gaussian 1D	homo	asympt. collective assum. CM [Usenko-Grosshans *PRA* 2015]
Garcia-Patron -Cerf 2009	squeezed	Gaussian	hetero	asympt. collective assum. CM [Garcia-Patron-Cerf *PRL* 2009]
Filip 2008	thermal	Gaussian	homo/hetero	asympt. collective assum. CM [Usenko-Filip *PRA* 2010] [Weedbrook *et al PRL* 2010]
Madsen *et al* 2013	squeezed	Gaussian + add. Gauss.	homo	asympt. collective assum. CM [Madsen *et al Nat. Comm.* 2013]
Fiurásek-Cerf 2012 Walk *et al* 2013	coherent	Gaussian	homo/hetero Gauss. postsel	asympt. collective assum. CM [Fiurásek -Cerf *PRA* 2012] [Walk *et al PRA* 2013]
Pirandola *et al* 2008	Two-way QKD		homo/hetero	asympt. collective assum. CM [Ottaviani *et al PRA* 2015]

For other protocols, security is only established against Gaussian attacks: *e.g.*, protocols with non Gaussian modulation, or with postselection.

Security proofs: state-of-the-art

Two main approaches:

1. **Entropic uncertainty principle**
2. [reduction: coll. $\Rightarrow$ general] + [Security against coll. attacks]

Entropic Uncertainty Principle

- tightest key rate for BB84 — M. Tomamichel *et al.* *Nat. Comm.* **3** 634 (2012)
- successfully ported to CV — F. Furrer *et al.* *PRL* **109** 100502 (2012)
- compatible with reverse reconciliation — F. Furrer *PRA* **90**, 042325 (2015)
- experiment! — T. Gehring *et al.* *Nat.Comm.* **6** 8795 (2015)

but . . .

- requires squeezing
- discrepancy with asymptotic secret key rate for Gaussian attacks

$\Rightarrow$ not very tolerant to losses

Security proofs: state-of-the-art

Two main approaches:

1. Entropic uncertainty principle
2. [**reduction: coll. $\Rightarrow$ general**] + [**Security against coll. attacks**]

Collective attacks are optimal (in the limit $n \to \infty$)

- de Finetti theorem — R. Renner, J.I. Cirac, *PRL* **102** 110504 (2009)
- "Postselection technique" (de Finetti reduction)

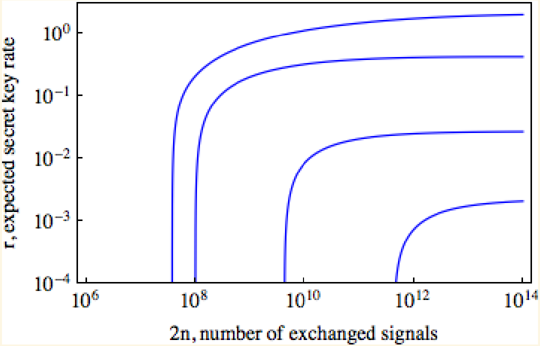
  AL, R. García-Patrón, R. Renner, N.J. Cerf, *PRL* **110** 030502 (2013)

Composable security proof against collective attacks

Most proofs assume that the covariance matrix is given NGA, GC, *PRL* (2006)
$\Rightarrow$ not sufficient
Only exception: coherent states + heterodyne detection
$\Rightarrow$ symmetries of the protocol allow for an assumption-free estimation of the covariance matrix — AL, *PRL* **114** 070501 (2015)

Numerical results for $\epsilon = 10^{-20}$ (for collective attacks)

AL, *PRL* **114** 070501 (2015)



Reasonable experimental parameters:

- distance = 1 km, 10 km, 50 km, 100 km
- excess noise: 1% of shot noise
- reconciliation efficiency $\beta = 90\%$
- $\epsilon_{\mathrm{rob}} \approx 1\%$ (prob. that the protocol aborts for a passive channel)

Limitations of current proof techniques

Entropic uncertainty relation:

- does not seem able to match the bound corresponding to Gaussian attacks
- fails for coherent state protocols

de Finetti-type reductions:

- exponential de Finetti of Renner-Cirac: no hope in the finite-size regime (already the "worst" technique for discrete variables)
- "Postselection technique":
  - ε-secure against collective attacks $\implies$ ε'-secure against general attacks with
    $$\varepsilon' = \varepsilon n^{d^4}$$
  - much better than de Finetti for DV [Christandl, Koenig, Renner *PRL* 2009]
  - continuous variable version obtained by truncating the Hilbert space for each mode [AL, Garcia-Patron, Cerf, Renner *PRL* 2013]
    $\implies$ local dimension $= O(\log n)$

New results in preparation (with Matthias Christandl)

better de Finetti reductions tailored for CV

based on a quite old idea:
"Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space"

AL, Karpov, Grangier, Cerf *NJP* 2009

Idea behind de Finetti reductions

1. Most protocols are permutation-invariant
   $\Longrightarrow$ it is typically enough to prove security for $\rho_{A^nB^n}$ such that

$$\pi \rho_{A^nB^n} \pi^\dagger = \rho_{A^nB^n} \quad \forall \pi \in S_n$$

   $\Longrightarrow$ There exists a purification of ρ in the symmetric subspace.
2. The symmetric subspace is **much smaller** than the full space: for n qudits:
   - Full space: $(\mathbb{C}^d)^{\otimes n} \Longrightarrow$ exponential dimension d^n
   - Symmteric subspace

$$\vee^n \mathbb{C}^d = \left\{ |\psi\rangle \in \mathbb{C}^d)^{\otimes n} \, : \, \pi|\psi\rangle = |\psi\rangle \quad \forall \pi \in S_n \right\}$$

$$\dim\left(\vee^n \, \mathbb{C}^d \right) = \binom{n+d-1}{n} \leq (n+d-1)^d$$

   $\Longrightarrow$ polynomial dimension!

Main tool: an operator equality

Theorem 1

$$\vee^n \mathbb{C}^d = \mathrm{Span}\{|\phi\rangle^{\otimes n} \,:\, |\phi\rangle \in \mathbb{C}^d\}$$

The symmetric space is spanned by i.i.d. states.

Theorem 2

$$\Pi_{\vee^n \mathbb{C}^d} = \binom{n+d-1}{n} \int (|\phi\rangle\langle\phi|)^{\otimes n} \,\mathrm{d}\phi$$

where $\mathrm{d}\phi$ is the Haar measure over $U(d)$

Consequence for QKD [Christandl-Koenig-Renner *PRL* 2009]

ε-security against collective attacks $\Longrightarrow$ ε'-security against general attacks with

$$\varepsilon' = \binom{n+d-1}{n}\varepsilon = O(\varepsilon n^{d_A^2 d_B^2})$$

and $d = d_A^2 d_B^2$ (ex: $d = 16$ for BB84)

Moving to continuous variables

$$\Pi_{\vee^n \mathbb{C}^d} = \binom{n+d-1}{n} \int (|\phi\rangle\langle\phi|)^{\otimes n} \, \mathrm{d}\phi$$

only makes sense in finite dimension.
$\Longrightarrow$ truncate the Hilbert space.

Truncation

- Intuitively, each mode contains a thermal state
- It should be possible to replace $\mathcal{H} = \mathrm{Span}\{|0\rangle, |1\rangle, \ldots\}$ by

  $$\hat{\mathcal{H}} = \mathrm{Span}\{|0\rangle, |1\rangle, \ldots, |d_{\max}\rangle\}$$

  with $d_{\max} = O(\text{average energy})$.
- unfortunately, if we want that $\mathrm{tr}(\rho^{\otimes n} \Pi_{\hat{\mathcal{H}}^{\otimes n}}) \geq 1 - \varepsilon$, then we need:

  $$d_{\max} = O(\text{average energy} \times \log n)$$

  $$\Longrightarrow \varepsilon' = O(\varepsilon n^{\log^4 n})$$

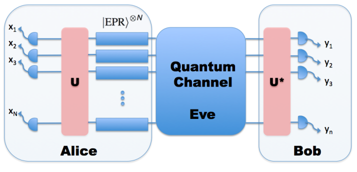
[AL, Garcia-Patron, Cerf, Renner *PRL* 2013]

Symmetry in phase space

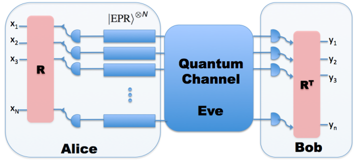
Consider the group of transformations generated by linear optical networks on n modes: isomorphic to $U(n)$:

$$\vec{a} \to u\vec{a}, \quad \vec{a}^\dagger \to u^\dagger \vec{a}^\dagger$$

For any linear passive transform. $u \in U(n)$ in phase space, there exists $R \in O(2n)$ such that:



$$\equiv$$



$\Longrightarrow$ u commutes with heterodyne detection

The protocol where Alice prepares two-mode squeezed vacuum states, and where both parties perform heterodyne measurements is in fact invariant under $u_A \otimes u_B^*$ for any $u \in U(n)$

Towards a CV version of de Finetti

CV protocols are more symmetric than BB84

One can assume that $\rho_{A^nB^n}$ is invariant under the action of the unitary group $U(n)$:

$$(u_A \otimes u_B^*)\rho_{A^nB^n}(u_A \otimes u_B^*)^\dagger = \rho_{A^nB^n} \quad \forall u \in U(n)$$

Note that $S_n \subset U(n)$

Define a new symmetric subspace

$$\mathrm{Sym} = \{|\phi\rangle \in \mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} \,:\, u_A \otimes u_B^*|\phi\rangle \quad \forall u \in U(n)\}$$

$u^* =$ complex conjugate

It's a subspace of the usual symmetric subspace since $S_n \subset U(n)$.
$\dim(\mathrm{Sym}) = \infty$
Note that two-mode squeezed vacuum states belong to that space.

The "continuous-variable" / unitary symmetric subspace

Theorem 1

$$\mathrm{Sym} = \mathrm{Span}\{|\lambda\rangle^{\otimes n} \; : \; |\lambda| < 1\}$$

where $|\lambda\rangle$ is the two-mode squeezed state with squeezing parameter λ:

$$|\lambda\rangle \propto \exp(\lambda a^\dagger b^\dagger)|\mathrm{vacuum}\rangle$$

Theorem 2

For $n \geq 2$,

$$\Pi_{\mathrm{Sym}} = \frac{n-1}{\pi} \int_{|\lambda|<1} \frac{1}{(1-|\lambda|^2)^2} \left(|\lambda\rangle\langle\lambda|\right)^{\otimes n} \mathrm{d}\lambda$$

with $\mathrm{d}\lambda =$ uniform measure on open unit disk.

Similarity with:

$$\Pi_{\vee^n \mathbb{C}^d} = \binom{n+d-1}{n} \int \left(|\phi\rangle\langle\phi|\right)^{\otimes n} \mathrm{d}\phi$$

Conclusion and perspectives

- security of CV QKD is not settled
- Main open conjecture: Gaussian attacks are asymptotically optimal

- new approach: a more useful symmetric subspace for CV protocols based on the invariance under the unitary group in $\mathbb{C}^n$
- gives a good reduction from collective to general attacks in the finite-size setting!