A Gaussian de Finetti reduction for continuous-variable QKD

Anthony Leverrier

Inria Paris

Trustworthy Quantum Information 2017

21 June 2017, Paris

Continuous-variable QKD

QKD with continuous variables

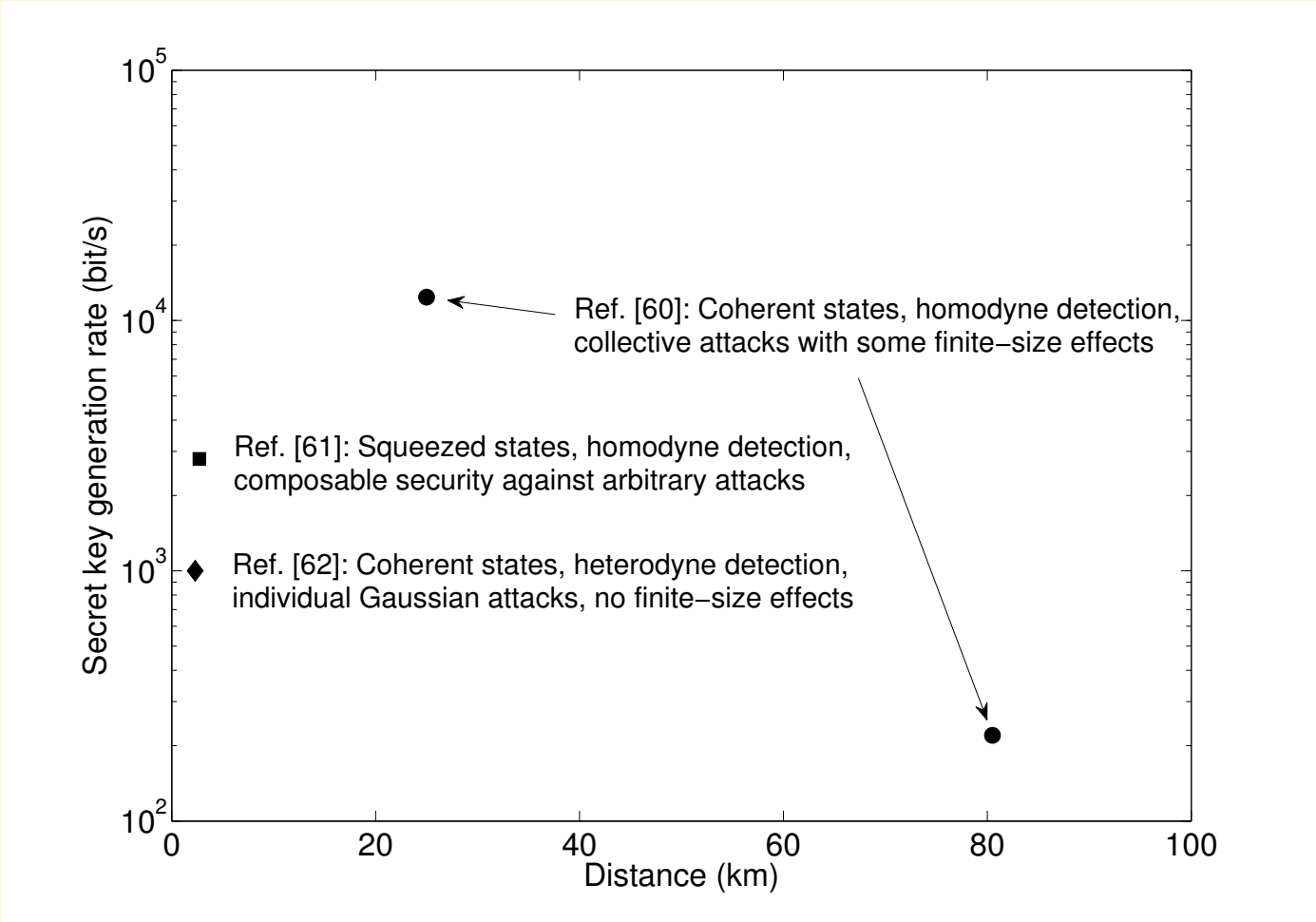
- quite recent — T.C. Ralph **PRA 61** 010303(R) (1999)
- information encoded on the quadratures (X, P) of the EM field
- measured with homodyne / heterodyne (interferometric) detection
- no need for single-photon counters
- **infinite dimension $\Rightarrow$ usual proof techniques don't apply directly (eg de Finetti)**

With coherent states

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

This talk: for some CV QKD protocols, security against Gaussian attacks implies security against general attacks, in the finite-size setting

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

E-B protocol: purification of Alice's system

- Alice and Bob receive a bipartite state (think two-mode squeezed state) and apply measurements:
  e.g., homodyne or heterodyne measurement
- 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: $\mathbb{P}[S_A \neq S_B] \leq \epsilon_{\text{corr}}$
- secrecy: $\frac{1}{2} \left\| \rho_{S_A E} - \left(\frac{1}{2^k} \sum_{\vec{k}} |\vec{k}\rangle\langle\vec{k}| \right) \otimes \rho_E \right\|_1 \leq \epsilon_{\text{sec}}$
- $\mathcal{E}$ is ϵ-secure if $\epsilon_{\text{corr}} + \epsilon_{\text{sec}} \leq \epsilon$
- robustness: $p_{\text{abort}} = \epsilon_{\text{rob}}$ (small!) if passive adversary

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

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

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 general 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. **Composable security against Gaussian collective attacks**:

   same, but restricted to $\rho_{A^n B^n} = (\rho_{AB}^G)^{\otimes n}$, with ρ^G a Gaussian state

Remark: many papers use Gaussian optimality to argue security: [Wolf et al PRL 2005], [García-Patrón, Cerf PRL 2006], [Navascués, Grosshans Acín PRL 2006]

- For a fixed covariance matrix, the Gaussian state maximizes $\chi(X; E)$
  $\Longrightarrow$ not composable in general
- Important **unproven** conjecture: Gaussian attacks are optimal

For most protocols, we don't have composable security

- against Gaussian collective attacks: easy since restricted to Gaussian states
- reduction: collective $\Longrightarrow$ general: ok via de Finetti [Renner, Cirac PRL 2009]

- but no known reduction to Gaussian attacks : Gaussian $\not\Longrightarrow$ collective

Collective attacks are hard to analyze ($\neq$ discrete variables!)

- 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 $\Gamma(\rho_{XY})$

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	general [Furrer et al *PRL* 2012] $K^{\varepsilon}(N) > 0$ for practical N $\lim_{N\to\infty} K^{\varepsilon}(N) < K_{\mathrm{Gauss}}$
Weedbrook *et al* 2004 (also MDI CVQKD)	coherent	Gaussian	hetero	general [AL *PRL* 2015] $K^{\varepsilon}_{\mathrm{coll}}(N) \approx K_{\mathrm{Gauss}}$ 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]
Fiurášek-Cerf 2012 Walk *et al* 2013	coherent	Gaussian	homo/hetero Gauss. postsel	asympt. collective assum. CM [Fiurášek -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.

This talk

Protocol	(PM) State preparation	(PM) Modul.	Bob's measurement	Best available security proofs
Cerf-Levy -van Assche 2001	squeezed	Gaussian	homo	general [Furrer et al *PRL* 2012] $K^\varepsilon(N) > 0$ for practical N $\lim_{N\to\infty} K^\varepsilon(N) < K_{\mathrm{Gauss}}$
Weedbrook *et al* 2004 (also MDI CVQKD)	coherent	Gaussian	hetero	general [AL *PRL* 2015] $K^\varepsilon(N) = K_{\mathrm{Gauss}}$ for practical N [AL *PRL* 2017]
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.

Main result: a Gaussian de Finetti reduction

- For the protocol where
  - Alice sends coherent states with a Gaussian modulation
  - Bob performs heterodyne measurement
- if Alice and Bob randomize their classical data (with a random rotation in $\mathbb{R}^n$),

then sufficient to consider Gaussian collective attacks

Theorem (AL, *PRL* 118 2017)

If the protocol is ε-secure against Gaussian attacks, then it is ε'-secure against general attacks with

$$\varepsilon' = Cn^4(d_A + d_B)\varepsilon.$$

d_A, d_B: average energy in Alice's or Bob's modes

Main idea

symmetry $\Leftrightarrow$ independence

de Finetti [Caves, Fuchs, Schack, Christandl, König, Mitchison, Renner . . .]

invariance under permutations (S_n) $\Longrightarrow$ i.i.d.

Gaussian de Finetti

invariance under unitaries (U_n) $\Longrightarrow$ Gaussian i.i.d.

de Finetti reduction: Christandl, König, Renner (PRL 2009)

Diamond norm $\|\mathcal{E}-\mathcal{F}\|_\diamond$ between CPTP maps $\mathcal{E},\mathcal{F}:\mathcal{H}^{\otimes n}\to\mathcal{H}'$

- natural notion of distance between 2 CPTP maps, with an operational meaning:
  - quantifies the maximal probability of distinguishing $\mathcal{E}$ and $\mathcal{F}$
  - ex: $\mathcal{E}=$ actual qkd protocol and $\mathcal{F}=$ ideal protocol
  - $\|\mathcal{E}-\mathcal{F}\|_\diamond\leq\varepsilon \quad\Longrightarrow\quad \mathcal{E}$ is ε-secure
- not easy to compute

$$\|\mathcal{E}-\mathcal{F}\|_\diamond := \sup_{\|\rho\|_1\leq 1} \|((\mathcal{E}-\mathcal{F})_{\mathcal{H}^{\otimes n}}\otimes \mathbb{1}_{\mathcal{K}})\rho_{\mathcal{H}^{\otimes n}\mathcal{K}}\|_1 \qquad (\text{with}\,\mathcal{K}\cong\mathcal{H}^{\otimes n})$$

de Finetti reduction

If $\Delta=\mathcal{E}-\mathcal{F}$ is permutation-invariant, then

$$\|\Delta\|_\diamond \leq n^{\mathrm{poly}(d)}\|(\Delta\otimes\mathbb{1})\tau_{\mathcal{H}^n\mathcal{R}}\|_1 \quad \text{with} \quad \tau_{\mathcal{H}^n}=\int \sigma_{\mathcal{H}}^{\otimes n}\mu(\sigma_{\mathcal{H}})$$

- only needs to consider a specific i.i.d. state (= collective attack)
- loss in security parameter : $\dim \mathrm{Sym}^n(\mathbb{C}^d)=n^{\mathrm{poly}(d)}$

ε-secure against collective $\Longrightarrow$ $n^{\mathrm{poly}(d)}\varepsilon$-secure against general attacks

Moving to continuous variables

Main idea of the DV proof: resolution of the identity

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

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

Truncation

- It should be possible to replace $\mathcal{H} = \mathrm{Span}\{|0\rangle, |1\rangle, \ldots\}$ by

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

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

$$d_{\mathrm{max}} = O(\text{average energy} \times \log n) \quad\Longrightarrow\quad \varepsilon' = O(\varepsilon n^{\log^4 n})$$

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

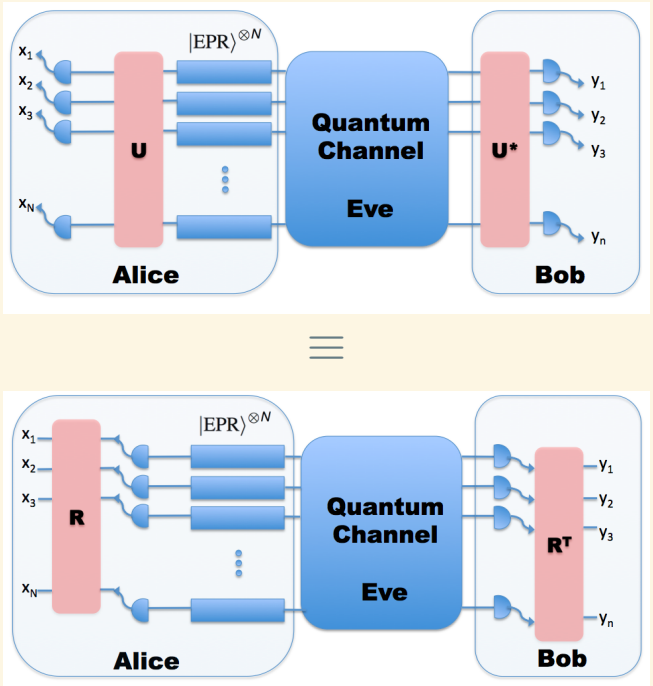
- invariance under permutations in S_n will not suffice
- but some CV protocols are invariant under a larger symmetry group $\cong U(n)$

New idea: Symmetry in phase space

- annihilation operators of $\mathcal{H}_A$ and $\mathcal{H}_B$: $\vec{a} = (a_1, \cdots, a_n)$ and $\vec{b} = (b_1, \cdots, b_n)$
- $U(n)$: group of transformations generated by linear optical networks on n modes

$$\vec{a} \to u\vec{a}, \quad \vec{b} \to \overline{u}\vec{b}$$

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



- commutes with heterodyne detection
- protocol with heterodyne detection is covariant with respect to the action of $U(n)$

Action of the unitary group on the Fock space $F_{2,2,n}$

- Want to study $2n$-modes bipartite mixed states ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$
- Consider purifications in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$

A $4n$-mode quantum state can be described as a function of $4n$ variables $|\psi\rangle = f(\vec{a}, \vec{b}, \vec{c}, \vec{d})|0\rangle$

$$\underbrace{(a_1^\dagger \dots a_n^\dagger)}_{\vec{a}}, \underbrace{(b_1^\dagger \dots b_n^\dagger)}_{\vec{b}}; \underbrace{(c_1^\dagger \dots c_n^\dagger)}_{\vec{c}}, \underbrace{(d_1^\dagger \dots d_n^\dagger)}_{\vec{d}}$$

The unitary group $U(n)$ acts in a natural way on this Fock space

$$\vec{a} \mapsto u\vec{a}, \quad \vec{b} \mapsto \overline{u}\vec{b} \quad \text{(change of variables)}$$

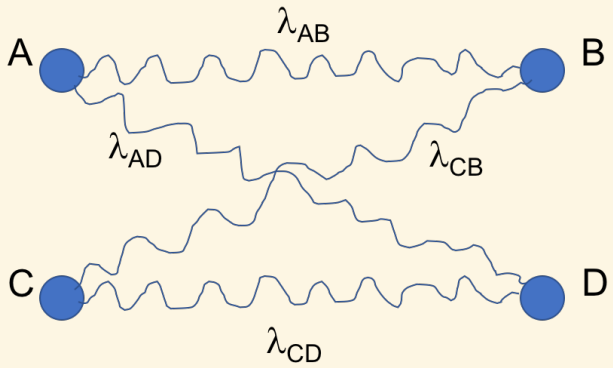
$\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$ carries a representation of $U(n)$:

$$\forall u \in U(n) \qquad V_u : \psi(\vec{a}, \vec{b}, \vec{c}, \vec{d}) \mapsto \psi(u\vec{a}, \overline{u}\vec{b}, u\vec{c}, \overline{u}\vec{d})$$

Goal: define a new symmetric subspace spanned by states invariant under $U(n)$

A new symmetric subspace (for $U(n)$ instead of S_n)

$$\mathrm{Sym} = \{|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D \ : \ V_u|\psi\rangle = |\psi\rangle, \forall u \in U(n)\}$$



Characterization of symmetric subspace [arXiv:1612.05080]

- The symmetric subspace is spanned by i.i.d. Gaussian states $|\Lambda\rangle^{\otimes n}$

$$|\Lambda\rangle := \det(1 - \Lambda\Lambda^\dagger)^{1/2} \exp(\lambda_{AB} a^\dagger b^\dagger + \lambda_{AD} a^\dagger d^\dagger + \lambda_{CB} c^\dagger b^\dagger + \lambda_{CD} c^\dagger d^\dagger)|0\rangle$$

  associated with $\Lambda = \begin{bmatrix} \lambda_{AB} & \lambda_{AD} \\ \lambda_{CB} & \lambda_{CD} \end{bmatrix}$ such that $\Lambda\Lambda^\dagger < \mathbb{1}_2$

- 4-mode squeezed Gaussian state
- $|\Lambda\rangle^{\otimes n}$ is a generalized $SU(2,2)$ coherent state (Perelomov 1972)

Gaussian de Finetti

de Finetti Theorem (arXiv:1612.05080)

Let $n, k \geq 4$, $\rho = |\psi\rangle\langle\psi|$ symmetric (pure) state in $F_{2,2,n+k}^{U(n+k)}$. Then tracing out over $4k$ modes gives an approximate mixture of $SU(2,2)$ coherent states:

$$\mathrm{tr}_{4k}(\rho) \approx_\varepsilon \int \nu(\Lambda)(|\Lambda\rangle\langle\Lambda|)^{\otimes n} \mathrm{d}\mu(\Lambda) \quad \text{with} \quad \varepsilon = O\left(\frac{n}{n+k}\right)$$

Gaussian de Finetti reduction [AL, *PRL* 118, 200501 2017]

Let $\Delta : \mathrm{End}(F_{1,1,n}^{\leq K}) \to \mathrm{End}(\mathcal{H}')$ such that $\Delta \circ V_u = \Delta$ for all $u \in U(n)$, then

$$\|\Delta\|_\diamond \leq \frac{K^4}{50} \|(\Delta \otimes \mathrm{id})\tau_{\mathcal{HN}}^\eta\|_1,$$

with $\tau_{\mathcal{H}}^\eta$ a mixture of $|\Lambda\rangle^{\otimes n}$.

$\Longrightarrow$ K = total number of photons, linear in n

$\Longrightarrow$ prefactor improved from $2^{\mathrm{polylog(n)}}$ to $O(n^4)$ compared to previous results

$\Longrightarrow$ sufficient to consider security for Gaussian i.i.d. input states

Gaussian de Finetti: proof technique

rather straightforward once we have defined the coherent states

Resolution of the identity on $F_{2,2,n}^{U(n)}$ (arXiv:1612.05080)

For $n \geq 5$,

$$\int_{\mathcal{D}} (|\Lambda\rangle\langle\Lambda|)^{\otimes n} \mathrm{d}\mu_n(\Lambda) = \mathbb{1}_{F_{2,2,n}^{U(n)}},$$

with the invariant measure on $\mathcal{D}$: $\mathrm{d}\mu_n(\Lambda) = C_n[\det(\mathbb{1}_2 - \Lambda\Lambda^\dagger)]^{-4} \prod_{i,j}^2 \mathrm{d}\Lambda_{i,j}$

Approximate version for bounded energy, (AL, *PRL* 118, 2017)

For $n \geq 5$ and $\eta \in [0,1[$, if $K \leq \frac{\eta N}{1-\eta}$ for $N = n-5$, then

$$\int_{\mathcal{D}_\eta} (|\Lambda\rangle\langle\Lambda|)^{\otimes n} \mathrm{d}\mu_n(\Lambda) \geq (1-\varepsilon)\Pi_{\leq K}$$

with $\varepsilon = 2N^4(1+K/N)^7 \exp(-ND(\frac{K}{K+N}\|\eta))$ and $\Pi_{\leq K}$ projector onto the finite subspace with less than K excitations in $F_{2,2,n}^{U(n)}$

Conclusion and perspectives

Summary

- new security reduction for CV QKD protocols based on the invariance under the unitary group in $\mathbb{C}^n$

  security against Gaussian attacks $\Longrightarrow$ security against general attacks

- efficient reduction even with finite size

Open questions

- problem: requires (for now) to symmetrize classical data $\Longrightarrow$ quite unpractical
  - can we remove this??
- Main open conjecture: Gaussian attacks are asymptotically optimal for protocols with homodyne detection?

Conclusion and perspectives

Summary

- new security reduction for CV QKD protocols based on the invariance under the unitary group in $\mathbb{C}^n$

  security against Gaussian attacks $\Longrightarrow$ security against general attacks

- efficient reduction even with finite size

Open questions

- problem: requires (for now) to symmetrize classical data $\Longrightarrow$ quite unpractical
  - can we remove this??
- Main open conjecture: Gaussian attacks are asymptotically optimal for protocols with homodyne detection?

Thanks!