Composable security proof for CVQKD with coherent states

arXiv:1408.5689

Anthony Leverrier

Inria Paris-Rocquencourt

QCrypt 2014

Continuous-variable QKD with coherent states

QKD with continuous variables

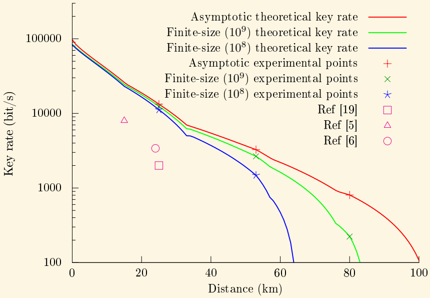
- quite recent — T.C. Ralph **PRA 61** 010303(R) (1999)
- information encoded on the quadratures (X, P) of the EM field
- measured with homodyne / heterodyne (interferometric) detection
- infinite dimension $\Rightarrow$ usual proof techniques don't apply

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

Implementations

- long distance — Jouguet *et al*, **Nat. Photon. 7** 378–381 (2013)
- stability — Jouguet *et al*, **Opt. Expr. 20** 14030 (2012)
- commercial system



Cygnus : a commercial product by SeQureNet

What about the security of continuous-variable QKD?

Composable security in QKD (cf talk by R. Renner)

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

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

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 ρ_{AB},

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

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

Security proofs: state-of-the-art

Two main approaches:

1. **Entropic uncertainty principle**
2. [reduction: collective $\Rightarrow$ 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 the CV paradigm F. Furrer et al. **PRL 109** 100502 (2012)
- compatible with reverse reconciliation F. Furrer arXiv:1405.5965 (2014)
- experiment! T. Gehring, et al. arXiv:1406.6174 (2014)

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: collective** $\Rightarrow$ **general**] + [**Security against coll. attacks**]

Collective attacks are optimal!

- de Finetti theorem — R. Renner, J.I. Cirac, **PRL 102** 110504 (2009)
- "Postselection technique" — AL, R. García-Patrón, R. Renner, N.J. Cerf, **PRL 110** 030502 (2013)

but no composable security proof against collective attacks

Current proofs against coll. attacks assume that the covariance matrix is given

M. Navascués, F. Grosshans, A. Acín **PRL 97** 190502 (2006)

R.García-Patrón, N.J. Cerf **PRL 97** 190503 (2006)

This talk: new protocol with assumption-free PE procedure

The protocol (reverse reconciliation, EB version)

Preparation

Alice prepares $2n$ two-mode squeezed vacuum states: $|\Phi\rangle_{AA'}^{\otimes 2n}$.
In the P & M version, she prepares $2n$ coherent states (Gauss. modulation).

- **Distribution:** Collective attacks: $\rho_{AB}^{\otimes 2n} = (\mathrm{id}_A \otimes \mathcal{N})(\Phi))^{\otimes 2n}$
- **Measurement:** with heterodyne detection $\Rightarrow X, Y \in \mathbb{R}^{4n}$
- **Discretization:** $Y \mapsto U \in \{0,1\}^{4dn}$
- **Error Correction:** Bob sends the syndrome of U for an ECC.
- **Parameter Estimation:** Alice computes $\|X\|^2, \|Y\|^2, \langle X, Y\rangle$
- **PE test** passes if $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$
- **Privacy Amplification:** random universal$_2$ hashing $\Rightarrow S_A, S_B$

The protocol (reverse reconciliation, EB version)

- **Preparation:** $2n$ two-mode squeezed vacuum states: $|\Phi\rangle_{AA'}^{\otimes 2n}$

Distribution

Alice sends register A' to Bob. The quantum channel $\mathcal{N}$ is i.i.d.

$$\Rightarrow \rho_{AB}^{\otimes 2n} = (\mathrm{id}_A \otimes \mathcal{N})(\Phi))^{\otimes 2n}$$

- **Measurement:** with heterodyne detection $\Rightarrow X, Y \in \mathbb{R}^{4n}$
- **Discretization:** $Y \mapsto U \in \{0,1\}^{4dn}$
- **Error Correction:** Bob sends the syndrome of U for an ECC.
- **Parameter Estimation:** Alice computes $\|X\|^2, \|Y\|^2, \langle X, Y\rangle$
- **PE test** passes if $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$
- **Privacy Amplification:** random universal$_2$ hashing $\Rightarrow S_A, S_B$

The protocol (reverse reconciliation, EB version)

- **Preparation:** $2n$ two-mode squeezed vacuum states: $|\Phi\rangle_{AA'}^{\otimes 2n}$
- **Distribution:** Collective attacks: $\rho_{AB}^{\otimes 2n} = (\mathrm{id}_A \otimes \mathcal{N})(\Phi))^{\otimes 2n}$

Measurement

Alice and Bob perform heterodyne detection on their respective $2n$ modes

$$\Rightarrow X, Y \in \mathbb{R}^{4n}$$

- **Discretization:** $Y \mapsto U \in \{0,1\}^{4dn}$
- **Error Correction:** Bob sends the syndrome of U for an ECC.
- **Parameter Estimation:** Alice computes $\|X\|^2, \|Y\|^2, \langle X, Y \rangle$
- **PE test** passes if $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$
- **Privacy Amplification:** random universal$_2$ hashing $\Rightarrow S_A, S_B$

The protocol (reverse reconciliation, EB version)

- **Preparation:** $2n$ two-mode squeezed vacuum states: $|\Phi\rangle_{AA'}^{\otimes 2n}$
- **Distribution:** Collective attacks: $\rho_{AB}^{\otimes 2n} = (\mathrm{id}_A \otimes \mathcal{N})(\Phi))^{\otimes 2n}$
- **Measurement:** with heterodyne detection $\Rightarrow X, Y \in \mathbb{R}^{4n}$

Discretization

Bob discretizes his data with d bits per symbol:

$$Y \mapsto U \in \{0,1\}^{4dn}$$

- **Error Correction:** Bob sends the syndrome of U for an ECC.
- **Parameter Estimation:** Alice computes $\|X\|^2, \|Y\|^2, \langle X, Y\rangle$
- **PE test** passes if $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$
- **Privacy Amplification:** random universal$_2$ hashing $\Rightarrow S_A, S_B$

The protocol (reverse reconciliation, EB version)

- **Preparation:** $2n$ two-mode squeezed vacuum states: $|\Phi\rangle_{AA'}^{\otimes 2n}$
- **Distribution:** Collective attacks: $\rho_{AB}^{\otimes 2n} = (\mathrm{id}_A \otimes \mathcal{N})(\Phi))^{\otimes 2n}$
- **Measurement:** with heterodyne detection $\Rightarrow X, Y \in \mathbb{R}^{4n}$
- **Discretization:** $Y \mapsto U \in \{0,1\}^{4dn}$

Error Correction (before Parameter Estimation!)

- Bob sends the syndrome of U for an ECC.
- Alice outputs a guess $\hat{U}$.
- Alice and Bob compute a small hash of U and $\hat{U}$ and abort if they differ.

- **Parameter Estimation:** Alice computes $\|X\|^2, \|Y\|^2, \langle X, Y\rangle$
- **PE test** passes if $[\gamma_a \le \Sigma_a^{\max}] \wedge [\gamma_b \le \Sigma_b^{\max}] \wedge [\gamma_c \ge \Sigma_c^{\min}]$
- **Privacy Amplification:** random universal$_2$ hashing $\Rightarrow S_A, S_B$

The protocol (reverse reconciliation, EB version)

- **Preparation:** $2n$ two-mode squeezed vacuum states: $|\Phi\rangle_{AA'}^{\otimes 2n}$
- **Distribution:** Collective attacks: $\rho_{AB}^{\otimes 2n} = (\mathrm{id}_A \otimes \mathcal{N})(\Phi))^{\otimes 2n}$
- **Measurement:** with heterodyne detection $\Rightarrow X, Y \in \mathbb{R}^{4n}$
- **Discretization:** $Y \mapsto U \in \{0,1\}^{4dn}$
- **Error Correction:** Bob sends the syndrome of U for an ECC.

Parameter Estimation:

- Alice computes $\|X\|^2, \|Y\|^2, \langle X, Y\rangle$
- **PE test** passes if $[\gamma_a \le \Sigma_a^{\max}] \wedge [\gamma_b \le \Sigma_b^{\max}] \wedge [\gamma_c \ge \Sigma_c^{\min}]$

$$\gamma_a := \frac{1}{2n}\left[1 + 5\sqrt{\frac{\log(24/\epsilon_{\mathrm{PE}})}{n}}\right]\|X\|^2 - 1 \qquad \gamma_b := \frac{1}{2n}\left[1 + 5\sqrt{\frac{\log(24/\epsilon_{\mathrm{PE}})}{n}}\right]\|Y\|^2 - 1$$

$$\gamma_c := \frac{1}{2n}\langle X, Y\rangle - 4\sqrt{\frac{\log(96/\epsilon_{\mathrm{PE}})}{n^3}}\left[\|X\|^2 + \|Y\|^2\right]$$

- **Privacy Amplification:** random universal$_2$ hashing $\Rightarrow S_A, S_B$

The protocol (reverse reconciliation, EB version)

- **Preparation:** $2n$ two-mode squeezed vacuum states: $|\Phi\rangle_{AA'}^{\otimes 2n}$
- **Distribution:** Collective attacks: $\rho_{AB}^{\otimes 2n} = (\mathrm{id}_A \otimes \mathcal{N})(\Phi))^{\otimes 2n}$
- **Measurement:** with heterodyne detection $\Rightarrow X, Y \in \mathbb{R}^{4n}$
- **Discretization:** $Y \mapsto U \in \{0,1\}^{4dn}$
- **Error Correction:** Bob sends the syndrome of U for an ECC.
- **Parameter Estimation:** Alice computes $\|X\|^2, \|Y\|^2, \langle X, Y\rangle$
- **PE test** passes if $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$

Privacy Amplification:

- Alice and Bob apply a random universal$_2$ hash function to their respective strings.
- They obtain two strings S_A and S_B of size l.

Main result

Theorem

$\mathcal{E}$ is ϵ-secure against collective attacks if $\epsilon = 2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm ent}$ and

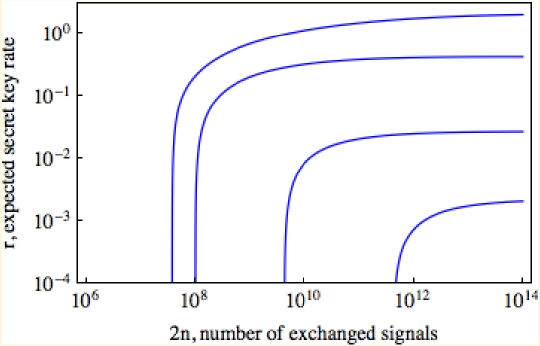
$$l \leq 2n\left[2\hat{H}_{\rm MLE}(U) - f(\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min})\right] - \mathrm{leak}_{\rm EC} - \Delta_{\rm AEP} - \Delta_{\rm ent} - 2\log\frac{1}{2\bar{\epsilon}},$$

where

- $\hat{H}_{\rm MLE}(U) =$ empirical entropy of U (computed from the empirical probabilities)
- $\Delta_{\rm AEP} := 4\log(2^{d/2}+2)\sqrt{4n\log_2 2/\epsilon_{\rm sm}^2}$,
- $\Delta_{\rm ent} := \sqrt{8n\log^2(4n)\log(2/\epsilon_{\rm ent})}$
- $f = \chi(Y,E)$ for a Gaussian state with CM $\begin{bmatrix} \Sigma_a^{\max}\mathbb{1}_2 & \Sigma_c^{\min}\sigma_z \\ \Sigma_c^{\min}\sigma_z & \Sigma_b^{\max}\mathbb{1}_2 \end{bmatrix}$

- asymptotic value: Gaussian attacks
- NEW TOOL: robust estimation of the CM without any assumption

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



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)

Parameter Estimation: the issue

To obtain a bound on $H_{\min}^{\epsilon}(U|E)$, we need to compute a confidence region for the **Covariance Matrix** of ρ_{AB}^{2n}.

A game

- $p(x)$ is an unknown probability distribution defined on $\mathbb{R}$ with $\mathbb{E}[x] = 0, Var(x) = V$ unknown
- You observe n i.i.d. realisations: $x_1, x_2, \cdots, x_n$
- Can you upper-bound V? i.e. find $\hat{V}$ s.t. $\text{Prob}(V \geq \hat{V}) \leq \epsilon$?

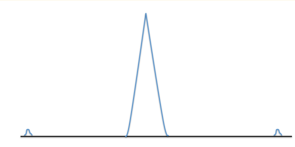
Parameter Estimation: the issue

To obtain a bound on $H^{\epsilon}_{\min}(U|E)$, we need to compute a confidence region for the **Covariance Matrix** of ρ^{2n}_{AB}.

A game

- $p(x)$ is an unknown probability distribution defined on $\mathbb{R}$ with $\mathbb{E}[x] = 0, Var(x) = V$ unknown
- You observe n i.i.d. realisations: $x_1, x_2, \cdots, x_n$
- Can you upper-bound V? i.e. find $\hat{V}$ s.t. $\text{Prob}(V \geq \hat{V}) \leq \epsilon$?

No!
because x is a priori unbounded



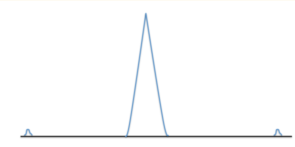
Parameter Estimation: the issue

To obtain a bound on $H_{\min}^{\epsilon}(U|E)$, we need to compute a confidence region for the **Covariance Matrix** of ρ_{AB}^{2n}.

A game

- $p(x)$ is an unknown probability distribution defined on $\mathbb{R}$ with $\mathbb{E}[x] = 0, Var(x) = V$ unknown
- You observe n i.i.d. realisations: $x_1, x_2, \cdots, x_n$
- Can you upper-bound V? i.e. find $\hat{V}$ s.t. $\text{Prob}(V \geq \hat{V}) \leq \epsilon$?

No!
because x is a priori unbounded

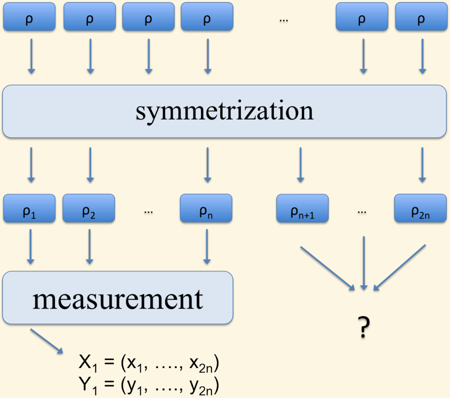


Solutions

1. Assume a Gaussian distribution $\Rightarrow$ no composable security...
2. Symmetrize the state!

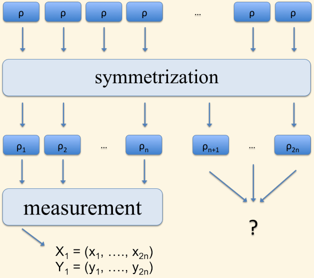
Parameter Estimation as quantum tomography

Framework introduced by Christandl and Renner *PRL* **109** 120403 (2012)



- for discrete-variable QKD, symmetrization = random permutation
- variance of classical variable: to estimate $\|X\|^2$, use random rotation
- for CVQKD, symmetrization = conjugate random networks of beamsplitters and phase shifts to Alice's and Bob's $2n$ modes

PE: an ideal (virtual) procedure

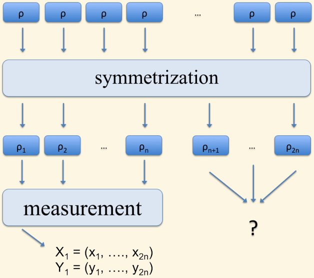


State symmetrization

Alice and Bob apply conjugate random networks of beamsplitters and phase-shifts to their modes
$\Rightarrow$ new state $\tilde{\rho}^{2n}$ with the same average covariance matrix

- **Distribution to additional players:** $\tilde{\rho}_i^n$ given to A_i and B_i
- **Parameter Estimation:** A_1 and B_1 compute a confidence region for $\tilde{\rho}_2^n$

PE: an ideal (virtual) procedure



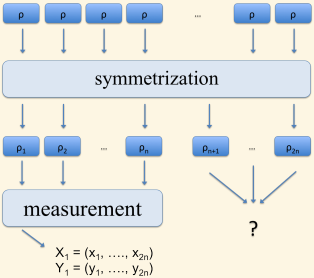
- **State symmetrization:** with random optical networks

Distribution to additional players

Alice and Bob distribute $\tilde{\rho}_1^n$ corresponding to the first n modes of $\tilde{\rho}^{2n}$ to A_1 and B_1. Similarly, they give $\tilde{\rho}_2^n$ to A_2 and B_2.

- **Parameter Estimation:** A_1 and B_1 compute a confidence region for $\tilde{\rho}_2^n$

PE: an ideal (virtual) procedure



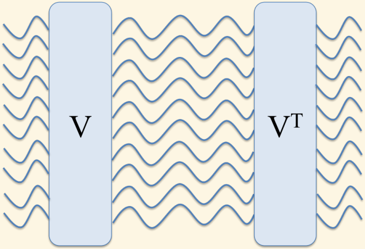
- **State symmetrization:** with random optical networks
- **Distribution to additional players:** $\tilde{\rho}_i^n$ given to A_i and B_i

Parameter Estimation

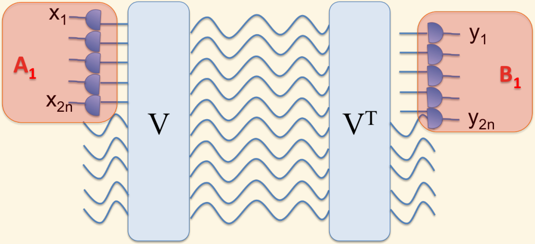
A_1 and B_1 try to estimate the covariance matrix of $\tilde{\rho}_2^n$. Similarly, A_2 and B_2 compute a confidence region for that of $\tilde{\rho}_1^n$.

Parameter Estimation: additional parties

Parameter Estimation: additional parties

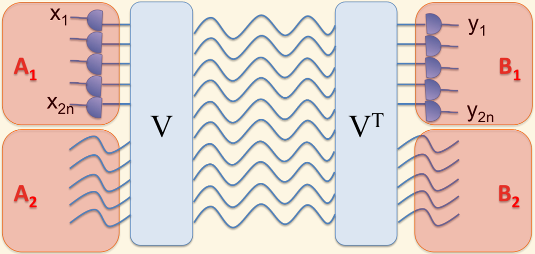


Parameter Estimation: additional parties



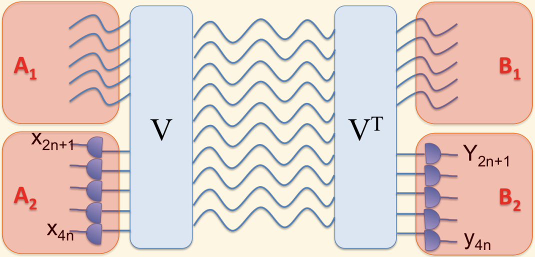
- A_1 and B_1 try to estimate the covariance matrix of $\rho_{A_2 B_2}$

Parameter Estimation: additional parties



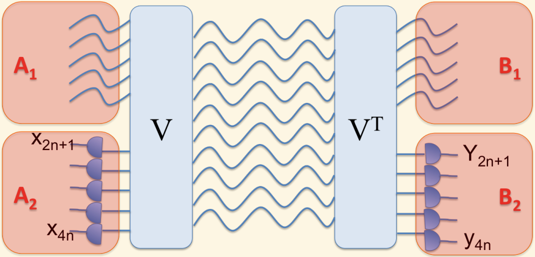
- A_1 and B_1 try to estimate the covariance matrix of $\rho_{A_2 B_2}$

Parameter Estimation: additional parties



- A_1 and B_1 try to estimate the covariance matrix of $\rho_{A_2 B_2}$
- A_2 and B_2 try to estimate the covariance matrix of $\rho_{A_1 B_1}$

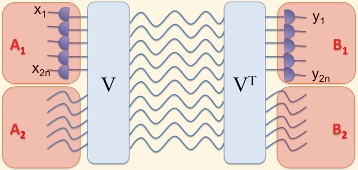
Parameter Estimation: additional parties



- A_1 and B_1 try to estimate the covariance matrix of $\rho_{A_2B_2}$
- A_2 and B_2 try to estimate the covariance matrix of $\rho_{A_1B_1}$

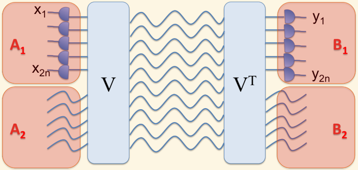
- By combining both estimates, one can compute a lower bound for the key size.
- Crucially, Alice can efficiently simulate both the symmetrization and the distribution to additional parties.

Parameter Estimation: simulation is enough



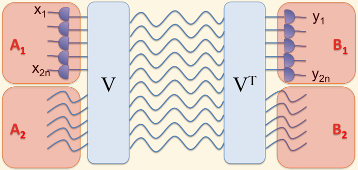
- A_1 and B_1 want to estimate the CM of $\rho_{A_2B_2}$:
  - they have access to heterodyne measurement results: $\vec{X}_1 = (x_1, \ldots, x_{2n})$, $\vec{Y}_1 = (y_1, \ldots, y_{2n})$
  - Lemma 1: it is sufficient to know $\|\vec{X}_1\|^2, \|\vec{Y}_1\|^2, \langle \vec{X}_1, \vec{Y}_1 \rangle$

Parameter Estimation: simulation is enough



- A_1 and B_1 want to estimate the CM of $\rho_{A_2 B_2}$:
  - they have access to heterodyne measurement results: $\vec{X}_1 = (x_1, \ldots, x_{2n})$, $\vec{Y}_1 = (y_1, \ldots, y_{2n})$
  - Lemma 1: it is sufficient to know $\|\vec{X}_1\|^2, \|\vec{Y}_1\|^2, \langle \vec{X}_1, \vec{Y}_1 \rangle$
- Alice knows $\|\vec{X}\|^2, \|\vec{Y}\|^2, \langle \vec{X}, \vec{Y} \rangle$
  - Lemma 2: she can infer a confidence region for $\|\vec{X}_1\|^2, \|\vec{Y}_1\|^2, \langle \vec{X}_1, \vec{Y}_1 \rangle$

Parameter Estimation: simulation is enough



- A_1 and B_1 want to estimate the CM of $\rho_{A_2B_2}$:
  - they have access to heterodyne measurement results: $\vec{X}_1 = (x_1, \ldots, x_{2n}), \vec{Y}_1 = (y_1, \ldots, y_{2n})$
  - Lemma 1: it is sufficient to know $\|\vec{X}_1\|^2, \|\vec{Y}_1\|^2, \langle \vec{X}_1, \vec{Y}_1 \rangle$
- Alice knows $\|\vec{X}\|^2, \|\vec{Y}\|^2, \langle \vec{X}, \vec{Y} \rangle$
  - Lemma 2: she can infer a confidence region for $\|\vec{X}_1\|^2, \|\vec{Y}_1\|^2, \langle \vec{X}_1, \vec{Y}_1 \rangle$

Theorem

- Alice can simulate A_1 and B_1 efficiently. (as well as A_2 and B_2)
- she gets a lower bound for $H^{\epsilon}_{\min}(U|E)$

Conclusion

Composable security of CVQKD with coherent states

- main new tool: PE procedure for covariance matrices
- almost all the raw key is used to distill the secret key
- fairly tight security bound against collective attacks

Open questions

- improve (a lot!) the reduction from general to collective attacks
- when is the symmetrization required? when can it be simulated?

Other applications for the parameter estimation procedure

- quantify bipartite CV entanglement without any assumptions