

Security proofs for continuous-variable quantum key distribution

Anthony Leverrier

▶ **To cite this version:**

Anthony Leverrier. Security proofs for continuous-variable quantum key distribution. QCrypt 2020 - 10th International Conference on Quantum Cryptography, Aug 2020, Amsterdam / Virtual, Netherlands. hal-03135753

HAL Id: hal-03135753
https://inria.hal.science/hal-03135753

Submitted on 9 Feb 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Security proofs for continuous-variable quantum key distribution

Anthony Leverrier

Inria Paris

QCrypt 2020 - virtual

10 August 2020

Disclaimer

- there won't be any COVID joke, sorry!
- I won't really talk about experimental stuff
- I won't talk about the zillion CVQKD protocols out there, only about a couple that are
  - simple to describe
    AND
  - simple to implement
- the talk might contain controversial[1] statements such as:

"sure, BB84 is a fine protocol, but it's high time we move to CV protocols!"

[1] but nothing too provocative! e.g. I won't talk about the quantum Internet

Outline

Discrete versus continuous variables

- BB84 vs CVQKD

State-of-the-art for security proofs

- Gaussian vs discrete modulation of coherent states

Next steps, open questions

- finite size setting, general attacks

Discrete versus continuous variables

Two natural/simple qkd protocols

BB84

- so natural that it would have been discovered eventually (much later?), even without B&B
- distribute copies of $|00\rangle + |11\rangle$
- measure with $\mathbb{1} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|)$

CVQKD = THE ∞-dim generalization

- distribute copies of $|00\rangle + \lambda|11\rangle + \lambda^2|22\rangle + \cdots + \lambda^k|kk\rangle + \cdots \quad = e^{\lambda \hat{a}^\dagger \hat{b}^\dagger}|\text{vacuum}\rangle$
- measure with $\mathbb{1} = \frac{1}{\pi}\int_{\mathbb{C}} |\alpha\rangle\langle\alpha| d\alpha$, with coherent state $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{k=0}^{\infty}\frac{\alpha^k}{\sqrt{k!}}|k\rangle \quad = e^{\alpha \hat{a}^\dagger}|\text{vacuum}\rangle$

  a.k.a. *coherent detection*, *heterodyne* measurement, or *double-homodyne* measurement

alternative for CVQKD

- measure the quadratures (homodyne detection) $\implies$ the setup of the EPR paper from 1935![2]

[2] formalized much later: Ralph (99), Reid (00), Cerf & al. (01), Grosshans-Grangier (02), Weedbrook & al. (03)...

Two natural/simple qkd protocols

BB84

- so natural that it would have been discovered eventually (much later?), even without B&B
- distribute copies of $|00\rangle + |11\rangle$
- measure with $\mathbb{1} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|)$

CVQKD = THE ∞-dim generalization

- distribute copies of $|00\rangle + \lambda|11\rangle + \lambda^2|22\rangle + \cdots + \lambda^k|kk\rangle + \cdots \quad = e^{\lambda \hat{a}^\dagger \hat{b}^\dagger}|\text{vacuum}\rangle$
- measure with $\mathbb{1} = \frac{1}{\pi}\int_{\mathbb{C}} |\alpha\rangle\langle\alpha| d\alpha$, with coherent state $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}}|k\rangle \quad = e^{\alpha \hat{a}^\dagger}|\text{vacuum}\rangle$

  a.k.a. *coherent detection*, *heterodyne* measurement, or *double-homodyne* measurement

alternative for CVQKD

- measure the quadratures (homodyne detection) $\implies$ the setup of the EPR paper from 1935![2]

[2] formalized much later: Ralph (99), Reid (00), Cerf & al. (01), Grosshans-Grangier (02), Weedbrook & al. (03)...

Two natural/simple qkd protocols

BB84

- so natural that it would have been discovered eventually (much later?), even without B&B
- distribute copies of $|00\rangle + |11\rangle$
- measure with $\mathbb{1} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|)$

CVQKD = THE ∞-dim generalization

- distribute copies of $|00\rangle + \lambda|11\rangle + \lambda^2|22\rangle + \cdots + \lambda^k|kk\rangle + \cdots \quad = e^{\lambda \hat{a}^\dagger \hat{b}^\dagger}|\text{vacuum}\rangle$
- measure with $\mathbb{1} = \frac{1}{\pi}\int_{\mathbb{C}} |\alpha\rangle\langle\alpha| d\alpha$, with coherent state $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}}|k\rangle \quad = e^{\alpha \hat{a}^\dagger}|\text{vacuum}\rangle$

  a.k.a. *coherent detection*, *heterodyne* measurement, or *double-homodyne* measurement

alternative for CVQKD

- measure the quadratures (homodyne detection) $\implies$ the setup of the EPR paper from 1935![2]

[2] formalized much later: Ralph (99), Reid (00), Cerf & al. (01), Grosshans-Grangier (02), Weedbrook & al. (03)...

Theory vs practice

BB84 in practice: NOT SO SIMPLE!

- single photons are usually prepared via $|00\rangle + \lambda|11\rangle + \lambda^2|22\rangle + \cdots + \lambda^k|kk\rangle + \cdots$ and heralding
- experimentally-friendlier version of BB84 relies on (phase-randomized) coherent states

$\Longrightarrow$ same states as in CVQKD! requires to ~~tweak~~ completely redo the analysis (multi-photon pulses)

- photon counters hard to implement replaced by threshold detectors

$\Longrightarrow$ infinite-dimensional Fock space, same as CVQKD!

CVQKD: pretty much as advertised

- same states, same measurement as specified (modulo a finite precision issue)
- P&M version: Alice prepares $|\alpha\rangle$ with $\alpha \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$ (or α from finite set)
- implementations today closely match the original protocols

my personal (provocative) view:
BB84 was nice to launch the field of quantum crypto, but the future belongs to CV!

Theory vs practice

BB84 in practice: NOT SO SIMPLE!

- single photons are usually prepared via $|00\rangle + \lambda|11\rangle + \lambda^2|22\rangle + \cdots + \lambda^k|kk\rangle + \cdots$ and heralding
- experimentally-friendlier version of BB84 relies on (phase-randomized) coherent states

$\Longrightarrow$ same states as in CVQKD! requires to ~~tweak~~ completely redo the analysis (multi-photon pulses)

- photon counters hard to implement replaced by threshold detectors

$\Longrightarrow$ infinite-dimensional Fock space, same as CVQKD!

CVQKD: pretty much as advertised

- same states, same measurement as specified (modulo a finite precision issue)
- P&M version: Alice prepares $|\alpha\rangle$ with $\alpha \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$ (or α from finite set)
- implementations today closely match the original protocols

my personal (provocative) view:
BB84 was nice to launch the field of quantum crypto, but the future belongs to CV!

Theory vs practice

BB84 in practice: NOT SO SIMPLE!

- single photons are usually prepared via $|00\rangle + \lambda|11\rangle + \lambda^2|22\rangle + \cdots + \lambda^k|kk\rangle + \cdots$ and heralding
- experimentally-friendlier version of BB84 relies on (phase-randomized) coherent states

$\Longrightarrow$ same states as in CVQKD! requires to ~~tweak~~ completely redo the analysis (multi-photon pulses)

- photon counters hard to implement replaced by threshold detectors

$\Longrightarrow$ infinite-dimensional Fock space, same as CVQKD!

CVQKD: pretty much as advertised

- same states, same measurement as specified (modulo a finite precision issue)
- P&M version: Alice prepares $|\alpha\rangle$ with $\alpha \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$ (or α from finite set)
- implementations today closely match the original protocols

my personal (provocative) view:
BB84 was nice to launch the field of quantum crypto, but the future belongs to CV!

ok... are there any drawbacks to CVQKD?

~~*of course not!*~~

More challenging theory[3]

- ∞ dimension (same is kind of true for implementations of DVQKD)
- continuous-valued AND unbounded measurement operators
- quality of the correlations measured via *covariance matrix (unbounded)*, not QBER or CHSH score
  $\Longrightarrow$ conceptual difficulties, but rather *clean problems*

Experimental performance: seems less robust to loss than DV

- losses are filtered out for DV: discard the no-click events[4]
- all pulses are there for CV, but noisier $\Longrightarrow$ harder to estimate the channel parameters precisely
- very large blocks required for long distance

[3] modern DVQKD protocols are also very complex!

[4] modulo some assumptions on the detectors (as demonstrated by Vadim Makarov!)

ok... are there any drawbacks to CVQKD?

~~*of course not!*~~

More challenging theory[3]

- ∞ dimension (same is kind of true for implementations of DVQKD)
- continuous-valued AND unbounded measurement operators
- quality of the correlations measured via *covariance matrix (unbounded)*, not QBER or CHSH score
  $\implies$ conceptual difficulties, but rather *clean problems*

Experimental performance: seems less robust to loss than DV

- losses are filtered out for DV: discard the no-click events[4]
- all pulses are there for CV, but noisier $\implies$ harder to estimate the channel parameters precisely
- very large blocks required for long distance

[3] modern DVQKD protocols are also very complex!

[4] modulo some assumptions on the detectors (as demonstrated by Vadim Makarov!)

P&M version of CVQKD

- Alice sends $|\alpha_1\rangle, \cdots |\alpha_n\rangle$
  - α_k either Gaussian variable or element from a finite set (e.g. $\{\pm\alpha, \pm i\alpha\}$)

- Bob measures with heterodyne detection: gets $\beta_1, \cdots, \beta_n \in \mathbb{C}$.
  - typical model: $\beta = t\alpha + \gamma$ with fixed *attenuation* t and Gaussian noise $\gamma \sim \mathcal{N}_{\mathbb{C}}(0, 1 + t^2\xi)$
  - $t \sim 0.1$ at 100km
  - ξ is the *excess noise*: $10^{-3} - 10^{-2}$ in implementations $\implies$ hard to mesure precisely

- classical postprocessing (essentially identical to DV)
  - key map: from Bob's data (reverse reconcilation[5])

$$\beta_1, \cdots \beta_n \to x_1, \cdots x_N \in \{0, 1\}$$

  - parameter estimation: covariance matrix of α, β
    (informally, want to estimate t, ξ) $\implies$ *the most challenging part*
  - privacy amplification

[5] actually same for BB84 due to discarding no-click events

P&M version of CVQKD

- Alice sends $|\alpha_1\rangle, \cdots |\alpha_n\rangle$
  - α_k either Gaussian variable or element from a finite set (e.g. $\{\pm\alpha, \pm i\alpha\}$)
- Bob measures with heterodyne detection: gets $\beta_1, \cdots, \beta_n \in \mathbb{C}$.
  - typical model: $\beta = t\alpha + \gamma$ with fixed *attenuation* t and Gaussian noise $\gamma \sim \mathcal{N}_{\mathbb{C}}(0, 1 + t^2\xi)$
  - $t \sim 0.1$ at 100km
  - ξ is the *excess noise*: $10^{-3} - 10^{-2}$ in implementations $\implies$ hard to mesure precisely
- classical postprocessing (essentially identical to DV)
  - key map: from Bob's data (reverse reconcilation[5])

$$\beta_1, \cdots \beta_n \to x_1, \cdots x_N \in \{0, 1\}$$

  - parameter estimation: covariance matrix of α, β
    (informally, want to estimate t, ξ) $\implies$ *the most challenging part*
  - privacy amplification

[5] actually same for BB84 due to discarding no-click events

P&M version of CVQKD

- Alice sends $|\alpha_1\rangle, \cdots |\alpha_n\rangle$
  - α_k either Gaussian variable or element from a finite set (e.g. $\{\pm\alpha, \pm i\alpha\}$)
- Bob measures with heterodyne detection: gets $\beta_1, \cdots, \beta_n \in \mathbb{C}$.
  - typical model: $\beta = t\alpha + \gamma$ with fixed *attenuation* t and Gaussian noise $\gamma \sim \mathcal{N}_{\mathbb{C}}(0, 1 + t^2\xi)$
  - $t \sim 0.1$ at 100km
  - ξ is the *excess noise*: $10^{-3} - 10^{-2}$ in implementations $\implies$ hard to mesure precisely
- classical postprocessing (essentially identical to DV)
  - key map: from Bob's data (reverse reconcilation[5])

$$\beta_1, \cdots \beta_n \to x_1, \cdots x_N \in \{0, 1\}$$

  - parameter estimation: covariance matrix of α, β
    (informally, want to estimate t, ξ) $\implies$ *the most challenging part*
  - privacy amplification

[5] actually same for BB84 due to discarding no-click events

CV or DV?

- photons live in ∞-dimensional Fock space: why encode information on some qubit space?
- the simplest states to prepare are coherent (= Gaussian) states! (already used in telecom industry)
- coherent (heterodyne) detection is needed for the whole telecom industry: huge incentives!
- more natural/efficient to encode information in phase-space: continuous variables!
- what about DI / MDI /TF QKD? those don't really work with CV... Well, they're only needed because we don't quite know how to implement vanilla BB84 :-)

$\Longrightarrow$ *qubits are good for computing, less for communicating* *classical information*

Outline

Discrete versus continuous variables

- BB84 vs CVQKD

State-of-the-art for security proofs

- Gaussian vs discrete modulation of coherent states

Next steps, open questions

- finite size setting, general attacks

State-of-the-art for security proofs

QKD as a tomography problem

Goal

get sufficient correlations between A and B to upper bound on Eve's information about $\vec{x}$:

- composable security: $H^{\varepsilon}_{\min}(X_1, \cdots, X_N|E)_{\rho^{(n)}_{AXE}}$
- asymptotic bound[6]: $H(X_1|E)_{\rho_{AXE}}$ (single channel use)

major difficulty already for collective attacks in the asymptotic limit: ρ_{AXE} is a pure

- 4-qubit state for BB84: 16 parameters
- 4-mode state in $\mathsf{Span}(|i, j, k, \ell\rangle : i, j, k, \ell \in \mathbb{N})$ for CVQKD; even truncating the Fock space to 10 photons/mode gives more than 10^4 parameters

One (only?) useful tool: von Neumann entropy maximized by Gaussian states $S(\rho) \leq S(\rho_G)$

QKD version: $\chi(\beta, E)_\rho \leq \chi(\beta, E)_{\rho_G}$ (ρ_G the Gaussian state with same covariance matrix as ρ)

$\Longrightarrow$ asymptotic security against collective attacks for protocols with Gaussian modulation

[Wolf, Giedke, Cirac PRL 2005] [Garcia-Patron, Cerf PRL 2006] [Navascues, Grosshans, Acin PRL 2006]

[6] for "nice" protocols

QKD as a tomography problem

Goal

get sufficient correlations between A and B to upper bound on Eve's information about $\vec{x}$:

- composable security: $H^{\varepsilon}_{\min}(X_1, \cdots, X_N|E)_{\rho^{(n)}_{AXE}}$
- asymptotic bound[6]: $H(X_1|E)_{\rho_{AXE}}$ (single channel use)

major difficulty already for collective attacks in the asymptotic limit: ρ_{AXE} is a pure

- 4-qubit state for BB84: 16 parameters
- 4-mode state in $\mathsf{Span}(|i, j, k, \ell\rangle : i, j, k, \ell \in \mathbb{N})$ for CVQKD; even truncating the Fock space to 10 photons/mode gives more than 10^4 parameters

One (only?) useful tool: von Neumann entropy maximized by Gaussian states $S(\rho) \leq S(\rho_G)$

QKD version: $\chi(\beta, E)_\rho \leq \chi(\beta, E)_{\rho_G}$ (ρ_G the Gaussian state with same covariance matrix as ρ)

$\Longrightarrow$ asymptotic security against collective attacks for protocols with Gaussian modulation

[Wolf, Giedke, Cirac PRL 2005] [Garcia-Patron, Cerf PRL 2006] [Navascues, Grosshans, Acin PRL 2006]

[6] for "nice" protocols

Last few years

- Gaussian modulation: essentially solved!
- discrete modulation: still very open, and somewhat pressing issue!

Gaussian modulation: $\alpha \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$

2 approaches to prove security against general attacks:

Entropic uncertainty relation [Furrer & al. PRL 2012]

- discretize $\implies$ $\mathrm{X}_\delta, \mathrm{P}_\delta$
- $\mathrm{H}^\varepsilon_{\mathsf{min}}(\mathrm{X}_\delta|\mathrm{E})_{\rho^{\mathrm{n}}} + \mathrm{H}^\varepsilon_{\mathsf{max}}(\mathrm{P}_\delta|\mathrm{B})_{\rho^{\mathrm{n}}} \geq -\log \frac{\delta^2}{2\pi} \mathrm{S}_0^{(1)}\big(1, \frac{\delta^2}{4}\big)^2$

but protocol requires squeezed states, bound not believed to be tight

*Gaussian de Finetti [**AL** PRL 2017]*

crucial fact: protocol is symmetric wrt $\mathrm{U}(\mathrm{n})$ (instead of S_{n} for BB84) $\implies$ stronger de Finetti

1. symmetrize in phase-space $\implies$ restrict to $\rho^{\mathrm{n}} = \rho_{\mathrm{G}}^{\otimes \mathrm{n}}$
2. equipartition property: $\mathrm{H}^\varepsilon_{\mathsf{min}}(\mathrm{X}_\delta|\mathrm{E})_{\rho_{\mathrm{G}}^{\otimes \mathrm{n}}} \approx \mathrm{n}\mathrm{H}(\mathrm{X}_\delta|\mathrm{E})_{\rho_{\mathrm{G}}}$
3. $\mathrm{H}(\mathrm{X}_\delta|\mathrm{E})_{\rho_{\mathrm{Gauss}}} = \mathrm{H}(\mathrm{X}_\delta) - \chi(\mathrm{X}_\delta; \mathrm{E})_{\rho_{\mathrm{G}}}$
4. estimation of CM $\implies$ upper bound on $\chi(\mathrm{X}_\delta; \mathrm{E})_{\rho_{\mathrm{G}}}$

missing element: finite precision of measurements

Discrete modulation

Lorenz & al. (2004), Namiki, Hirano (2006), Zhao & al. (2009), AL, Grangier (2009), Sych, Leuchs (2010), Bradler, Weedbrook (2017)...

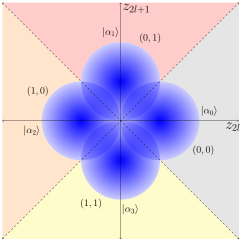
- easier to implement: same as coherent telecom industry
- better for error correction

$\Longrightarrow$ huge interest from industry, H2020 CiViQ

theory is more complicated

- EUR don't help (coherent states)
- U(n)-symmetry is broken $\Longrightarrow$ no Gaussian de Finetti, unclear how to perform PE
- non-Gaussian E-B protocol: pb for bounding vN entropy

$\Longrightarrow$ even asymptotic collective attacks are nontrivial!



Very recent finite-size analysis of a 2-state protocol *[Matsuura & al.* arXiv : 2006.04661*]*

- mapping to a qubit protocol, but 2 states aren't sufficient to get very good performance
- unclear how to extend to 4 states or more

Two recent results on the 4-state protocol

asymptotic security for collective attacks, assuming channel parameters are known

main idea: convex optimization to bound Holevo information / conditional vN entropy

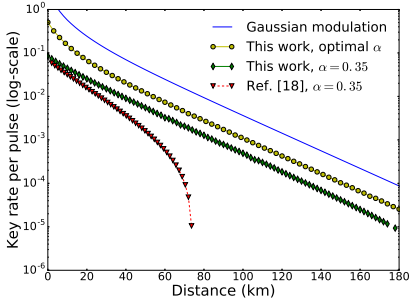
*Ghorai, Grangier, Diamanti, **AL** PRX 19*

- SDP to bound $\mathrm{f}(\rho) = \mathrm{tr}((\hat{\mathrm{q}}_\mathrm{A}\hat{\mathrm{q}}_\mathrm{B} - \hat{\mathrm{p}}_\mathrm{A}\hat{\mathrm{p}}_\mathrm{B})\rho)$
  $+$ Gaussian optimality
- pro: simple optimization, can be extended to larger constellations
- con: bounds are not tight

Lin, Upadhyaya, Lütkenhaus PRX 19: better (for now)

- SDP to bound H(X|E) directly: $\mathrm{f}(\rho) = \mathrm{D}\big(\mathcal{G}(\rho)||\mathcal{Z}[\mathcal{G}(\rho)]\big)$
- pro: much tighter key rate
- con: nonlinear objective function, optimization more involved (follows techniques from Coles & al. Nat. Comm. 16)

$$\begin{aligned} \text{minimize} \quad & \mathrm{f}(\rho) \\ \text{subject to} \quad & \rho \succeq 0 \\ & \mathrm{tr}(\rho\, \hat{\mathrm{O}}_\mathrm{PM}) = \mathrm{o}_\mathrm{PM} \\ & \mathrm{tr}(\rho) = 1 \end{aligned}$$



(from Lin & al. 2019)

Limitations of these 2 works

- only numerical results
- the true SDP cannot be solved directly because of ∞ dim $\implies$ heuristic truncation of Hilbert space
  - seems ok, but no proof
  - see recent work by Upadhyaya & al. (poster # 92)
- only deal with ideal detection
  - rather easy to patch with approach from Ghorai & al. (still won't be tight)
  - harder for Lin & al. (see poster # 28)
- parameter estimation is ignored!
- what about larger constellations? the results from Ghorai & al. should get much tighter

Outline

Discrete versus continuous variables

- BB84 vs CVQKD

State-of-the-art for security proofs

- Gaussian vs discrete modulation of coherent states

Next steps, open questions

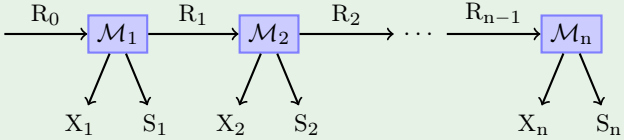
- finite size setting, general attacks

Next steps, open questions

Going further: security against general attacks, finite-size setting?

a potential approach: the entropy accumulation theorem [Dupuis, Fawzi, Renner 2016]

- gives tight bounds for DV QKD
- successfully applied to device-independent QKD [Arnon-Friedman & al. 2018]



- $\mathrm{H}^{\varepsilon}_{\mathsf{min}}(\mathrm{X}_1 \cdots \mathrm{X}_n|\mathrm{ES}^n)_{\rho^n} \geq n \min_\sigma \mathrm{H}(\mathrm{X}_1|\mathrm{ES}_1)_\sigma - \mathrm{O}(\sqrt{n})$

difficulties to adapt EAT to CV:

- requires some test. Seems much harder to define than for DV: should be related to covariance matrix, but not clear how
- test depends on some unbounded continuous outcome

The real difficulty: unbounded variables

Given $x_1, \dots, x_n \in \mathbb{R}$ *i.i.d. from unknown distribution with* $\langle x \rangle = 0$*, estimate* $\langle x^2 \rangle$

random sampling doesn't work, e.g.,

$$x_i = \begin{cases} 0 & \text{with prob } 1-\varepsilon \\ \pm C & \text{with prob } \varepsilon/2 \end{cases}$$

$\implies \langle x^2 \rangle = C^2\varepsilon$ but requires to sample a fraction $\geq 1-\varepsilon$

Solution: rotational symmetry

- apply random $R \in O(n)$ to $\vec{x}$: $\quad \vec{x} \to R\vec{x}$,
- sample first k coordinates
- concentration of measure gives tight bounds

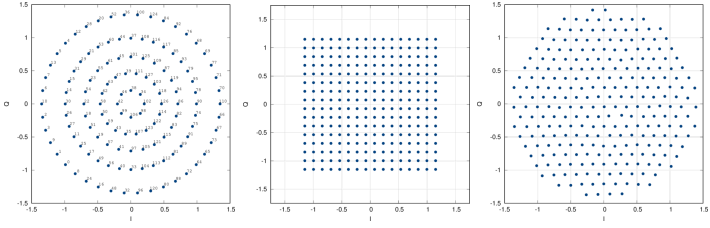
$\implies$ bound on CM for protocols with Gaussian modulation $\implies$ security against collective attacks [AL PRL 2015]

Unclear how to perform PE for discrete modulation at the moment...

unless restricted attack setting (e.g. Papanastasiou, Pirandola arXiv:1912.11418)

Optimal constellation?

- infinitely precise Gaussian modulation isn't physical $\implies$ finite constellations
- 2 or 3 states aren't enough to get good performance
- 4 states are ok, but larger constellations should allow for larger variance
  - improved asymptotics: key rate $\times 10$?
  - better for PE, for finite-size
  - "easy" for telecom industry



- previous results should extend there but unclear how tractable will be the numerics
- very large constellations might allow for continuity-type arguments (Kaur, Guha, Wilde arXiv:1901.10099)

Conclusion and perspectives

Conclusion and perspectives

- CV are well-suited to large-scale deployment of QKD:

  compatible with telecom industry standards

- security is quite involved (infinite dimension, unbounded variables, discretization, truncation...) but *not more than for modern DVQKD protocols*, and with *cleaner problems*?

challenges for theorists

- is it possible to apply entropy accumulation?
- how to perform parameter estimation without rotation symmetry? (for discrete modulation)
- what is better: 4 states or large constellations?

Thanks!

CiViQ