Theoretical challenges in continuous-variable quantum cryptography

Anthony Leverrier

Inria Paris

QCrypt 2017 - Cambridge

18 September 2017

Outline

- why continuous variables?
- difficulties / specificities
  - the formalism!
  - from CV to bits: discretization & truncation
  - infinite dimension, unbounded distributions
- some important open questions

Outline

- why continuous variables?
- difficulties / specificities
  - the formalism!
  - from CV to bits: discretization & truncation
  - infinite dimension, unbounded distributions
- some important open questions

Why continuous variables?

Practical considerations: nice alternative to qubit-based crypto

- states: **coherent states** (same as most implementations of BB84), but with a natural encoding of information (phase space)
- homodyne detection: **"off-the-shelf"**, compared to single-photon detectors (developed on purpose)

Performances

- **high rate** for metropolitan range (better than DV)
- but less suited for very long distances (on-off detectors of DV act as a very good filter)

Why haven't CV taken over quantum crypto yet?

probably (in part) because of a number of theoretical difficulties

Outline

- why continuous variables?
- difficulties / specificities
  - the formalism!
  - from CV to bits: discretization & truncation
  - infinite dimension, unbounded distributions
- some important open questions

Main theoretical difficulties in CV quantum cryptography

A specific formalism

- qubits are replaced by optical modes (∞ – dim Hilbert spaces)
- states described in phase space ($\mathbb{R}^2$) instead of Bloch sphere
- two types of measurements: homodyne and heterodyne, with outcomes in $\mathbb{R}$ or $\mathbb{R}^2$ $\Longrightarrow$ the defining difference

From CV to bits

Need to go from $\vec{x} \in \mathbb{R}^n$ to $k \in \mathbb{F}_2^n$

- truncation (to get rid of unbounded variables)
- discretization (to get bits)

Infinite dimension

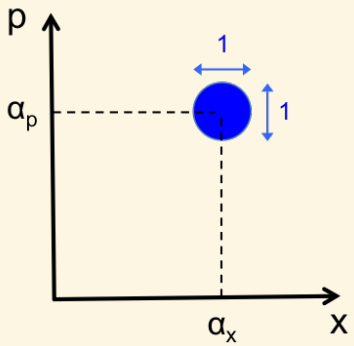
- usual de Finetti fails $\Longrightarrow$ problem for general attacks
- parameter estimation of unbounded quantities $\Longrightarrow$ pb even for collective attacks

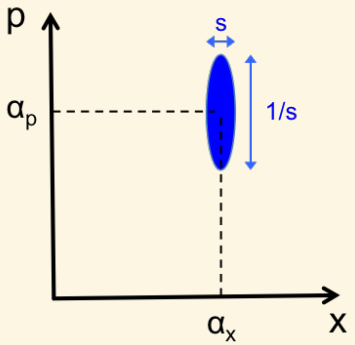
Outline

- why continuous variables?
- difficulties / specificities
  - the formalism!
  - from CV to bits: discretization & truncation
  - infinite dimension, unbounded distributions
- some important open questions

Difficulty 1: a specific formalism (states)

- qubits are replaced by optical modes ($\infty-$dim Hilbert space) spanned the Fock basis of photon-number states: $\{|0\rangle, |1\rangle, \ldots, |n\rangle, \ldots\}$
- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ replaced by $\sqrt{1-|\lambda|^2}(|00\rangle + \lambda|11\rangle + \lambda^2|22\rangle + \cdots + \lambda^n|nn\rangle + \cdots)$
  $\Longrightarrow$ two-mode squeezed vacuum states, defined for any $|\lambda| < 1$
- the single-mode states are described in phase space by their Wigner function $W(x,p)$ (= quasi-probability distribution over $\mathbb{R}^2$), x and p are called the quadratures
- the states of interest are Gaussian (i.e. W is Gaussian)
  - coherent states: $|\alpha\rangle$: $\quad W(x,p) = \mathcal{N}\left(\left[\begin{smallmatrix}\alpha_x\\ \alpha_p\end{smallmatrix}\right], \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]\right)$
  - squeezed states $|\alpha, s\rangle$: $\quad W(x,p) = \mathcal{N}\left(\left[\begin{smallmatrix}\alpha_x\\ \alpha_p\end{smallmatrix}\right], \left[\begin{smallmatrix}s & 0\\ 0 & 1/s\end{smallmatrix}\right]\right)$





Uncertainty relation: $\Delta x \Delta p \geq 1$ (constraint on covariance matrix)

Difficulty 1: a specific formalism (measurements)

each single-mode state is described by its Wigner function $\rho \leftrightarrow W(x,p)$

$\int W(x,p)\mathrm{d}p$ and $\int W(x,p)\mathrm{d}x$ are genuine probability density functions (normalized, ≥ 0)

Homodyne detection

- homodyne measurement of x quadrature: sample according to $\int W(x,p)\mathrm{d}p$
- homodyne measurement of p quadrature: sample according to $\int W(x,p)\mathrm{d}x$

They play a role similar to measurements in the computational or Hadamard basis for qubit states.

Heterodyne detection (more symmetric)

- mix the optical mode with vacuum on a balanced beamsplitter, measure a different quadrature for each output mode $\implies (x,p) \in \mathbb{R}^2$
- alternate description as projection on coherent states since $\frac{1}{2\pi}\int |\alpha\rangle\langle\alpha|\mathrm{d}\alpha = \mathbb{1}_{\mathcal{H}}$ $\implies \alpha \in \mathbb{C}$

Difficulty 1: a specific formalism (EB CV protocols)

Gaussian protocols

Alice prepares two-mode squeezed states $|\lambda\rangle$, keeps one mode, sends the other one to Bob

protocols vary as function of measurements

- homodyne/homodyne: similar to BBM92, requires sifting
- heterodyne/homodyne
- heterodyne/heterodyne: the most symmetric version

EB *vs* PM: Homodyning a mode of 2-mode squeezed vacuum state prepares a squeezed state for the 2nd mode; heterodying prepares a coherent state.

Reverse reconciliation (Grosshans, Grangier 2002)

- Bob's measured data forms the raw key
- seems strange to people used to BB84, necessary to tolerate $\geq 50\%$ losses
- but same thing for BB84 if Alice and Bob postselect on Bob's detectors clicking!!

Difficulty 1: a specific formalism (PM CV protocols)

Protocol	(PM) State preparation	(PM) Modul.	Bob's measurement
Cerf-Levy -van Assche 2001	squeezed	Gaussian	homo
Weedbrook *et al* 2004 (also MDI CVQKD Pirandola *et al* Nat Phot 2015)	coherent	Gaussian	hetero
Grosshans -Grangier 2002	coherent	Gaussian	homo
Usenko - Grosshans 2015	coherent	Gaussian 1D	homo
Garcia-Patron -Cerf 2009	squeezed	Gaussian	hetero
Filip 2008	thermal	Gaussian	homo/hetero
Madsen *et al* 2013	squeezed	Gaussian + add. Gauss.	homo/hetero
Fiurásek-Cerf 2012 Walk *et al* 2013	coherent	Gaussian	homo/hetero Gauss. postsel

and many other with non-Gaussian modulations (e.g. discrete) ...

Difficulty 1: a specific formalism (PM CV protocols)

Protocol	(PM) State preparation	(PM) Modul.	Bob's measurement
Cerf-Levy -van Assche 2001	squeezed	Gaussian	homo
Weedbrook *et al* 2004 (also MDI CVQKD Pirandola *et al* Nat Phot 2015)	coherent	Gaussian	hetero
Grosshans -Grangier 2002	coherent	Gaussian	homo
Usenko - Grosshans 2015	coherent	Gaussian 1D	homo
Garcia-Patron -Cerf 2009	squeezed	Gaussian	hetero
Filip 2008	thermal	Gaussian	homo/hetero
Madsen *et al* 2013	squeezed	Gaussian + add. Gauss.	homo/hetero
Fiurášek-Cerf 2012 Walk *et al* 2013	coherent	Gaussian	homo/hetero Gauss. postsel

for all Gaussian protocols, we have a conjecture for the asymptotic key rate (= rate against Gaussian collective attacks)

Outline

- why continuous variables?
- difficulties / specificities
  - the formalism!
  - from CV to bits: discretization & truncation
  - infinite dimension, unbounded distributions
- some important open questions

Difficulty 2: from CV to bits

(Naturally done by any physical detector: always outputs a number on 12 or 24 bits!)

$\Delta : \mathbb{R} \to \{0,1\}^d$, d bits

- pb 1: some intervals are ∞: is it ok? postselect or bound probability?
- pb 2: discretization breaks the symmetry of the protocol: bad

ex: EUR for discretized quadratures [Furrer *et al.*, JMP 2014]

X_δ, P_δ: discretized quadratures for A system with bin size δ. For ρ_{ABE},

$$H(X_\delta|B)_\rho + H(P_\delta|E)_\rho \geq -\log \frac{\delta^2}{2\pi} S_0^{(1)}\left(1, \frac{\delta^2}{4}\right)^2$$

$$H(X_\delta|B)_\rho + H(P_\delta|E)_\rho \geq -\log \frac{\delta^2}{2\pi} \quad (\delta \to 0)$$

generalization to smooth entropies $\implies$ security of homodyne/homodyne protocol against general attacks [Furrer *et al.*, PRL 2013] [Furrer PRA 2015]
experimental demonstration: [Gehring *et al.*, Nature Comm 2015]

But asymptotic rate below that corresponding to Gaussian attacks
Also used for "Beyond QKD" protocols, *e.g.* OT in noisy storage [Furrer *et al.*, arXiv:1708.00048]

Outline

- why continuous variables?
- difficulties / specificities
  - the formalism!
  - from CV to bits: discretization & truncation
  - infinite dimension, unbounded distributions
- some important open questions

Difficulty 3: infinite dimension (unbounded variables)

Assume collective attacks, $\rho^{\otimes n}$, is it possible to estimate the CM?

A simpler problem

Given $x_1, \ldots, x_n \in \mathbb{R}$ i.i.d. with unknown distribution, estimate $\langle x^2 \rangle$

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

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

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

Solution: rotational symmetry

Apply random $R \in O(n)$ to $\vec{x}$: $\vec{x} \to R\vec{x}$; sample first k coordinates
$\implies$ concentration of measure gives tight bounds

This technique can be applied to CVQKD for protocols with sufficient symmetry (hetero/hetero): $\implies$ bound on CM and security against collective attacks [AL PRL 2015]

Difficulty 3: infinite dimension (general attacks)

- de Finetti: security against coll. attacks $\Longrightarrow$ general attacks
- 2 versions: "exponential dF" [Renner, Nat Phys 2007]; "dF reduction" [Christandl, Koenig, Renner PRL 2009]
- requires finite dimension

idea: perform energy test to bound the dimension of the remaining state with high probability

results

- energy test + perm. invariance $\Longrightarrow$ most modes are close to finite-dim states $\Longrightarrow$ CV version of exponential de Finetti [Renner-Cirac PRL 2009]
- energy test + rot. inv. $\Longrightarrow$ all the modes are close to $(\log n)$-dim states $\Longrightarrow$ CV version of dF reduction [AL, Garcia-Patron, Renner, Cerf, PRL 2013]
- energy test + rot. inv. + Gaussian de Finetti reduction [AL PRL 2017] $\Longrightarrow$ sufficient to consider **Gaussian collective attacks**, compatible with finite-size analysis

Summary so far

2 protocols are secure

- homodyne/homodyne with EUR, but loose bound on the key rate
- hetero/hetero, **tight key rate** but requires active symmetrization

Two ways to get a bound on $H_{\min}^{\varepsilon}(X|E)_{\rho^n}$

- With EUR:

  discretize $\implies$ X_δ, P_δ

  $H_{\min}^{\varepsilon}(X_\delta|E)_{\rho^n} + H_{\max}^{\varepsilon}(P_\delta|B)_{\rho^n} \geq -\log \frac{\delta^2}{2\pi} S_0^{(1)}\left(1, \frac{\delta^2}{4}\right)^2$

- with Gaussian de Finetti:
  1. symmetrize in phase-space $\implies$ restrict to $\rho^n = \rho_{\text{Gauss}}^{\otimes n}$
  2. equipartition property: $H_{\min}^{\varepsilon}(X_\delta|E)_{\rho_{\text{Gauss}}^{\otimes n}} \approx nH(X_\delta|_E)_{\rho_{\text{Gauss}}}$
  3. $H(X_\delta|_E)_{\rho_{\text{Gauss}}} = H(X_\delta) - \chi(X_\delta;_E)_{\rho_{\text{Gauss}}}$
  4. estimation of CM $\implies$ upper bound on $\chi(X_\delta;_E)_{\rho_{\text{Gauss}}}$

(Some) open questions in CV QKD

- better EUR?
- symmetrization procedure: necessary?
- other Gaussian protocols: can we prove that Gaussian attacks are optimal?
- imperfect modulation: how to deal with it?
- discrete modulation: 2-state has been done, going beyond linear channels?

Better EUR?

Would also be useful for other CV quantum crypto protocols: bit commitment, OT

$\Longrightarrow$ avoid to discretize too early in the protocol (less symmetries $\Longrightarrow$ loose bounds)

Idea 1: use mutual info

$H_{\min}(X|E)$ is ill-defined if X is real, but $\chi(X;E)$ is well-defined and bounded.

- For given CM, $\chi(X;E)$ is maximized for Gaussian state [Wolf, Giedke, Cirac PRL 2005] [Garcia-Patron, Cerf PRL 2006] [Navascues, Grosshans, Acin PRL 2006]
- Can we get a useful UR with mutual information? exists for classical info [Hall PRL 1995]

Idea 2: see G. De Palma's preprint today arXiv: 1709.04921

"Uncertainty relations with quantum memory for the Wehrl entropy"

- Wehrl entropy = differential Shannon entropy of the outcome of a heterodyne measurement

  $$S(Z|B) + S(Z|C) \geq n \ln 4$$

  with $S(Z|B)$ conditional Shannon entropy
- can we exploit such quantities for a security proof?

Symmetrization procedure

The issue

To apply de Finetti, the state must be rotation invariant (protocol covariant wrt $U(n)$).

- this can be enforced if A and B should $U \sim U(n)$ and perform $\vec{x} \to U\vec{x}; \vec{y} \to \bar{U}\vec{y}$
- very costly to choose a random U: complexity $= O(n^3)$ (random Gaussian + Gram-Schmidt)
- but same issue for BB84 with random permutation and cost $O(n \log n)$
- for BB84, we know that symmetrization isn't necessary (from EUR)
- same for CV?

Solution?

- the whole protocol doesn't have to be covariant wrt $U(n)$
- we only need to bound $H_{\min}^{\varepsilon}(X|E)_{\rho^n}$
- Idea: use Portman's technique to decompose the QKD protocols in 2 steps [arXiv: 1705.10595]
  1. state distribution + measurement $\implies$ "quantum min-entropy resource"
  2. + classical postprocessing (ec, pa) $\implies$ secret key

Other Gaussian protocols (1/2)

Protocol	(PM) State preparation	(PM) Modul.	Bob's measurement
Cerf-Levy -van Assche 2001	squeezed	Gaussian	homo
Weedbrook *et al* 2004 (also MDI CVQKD Pirandola *et al* Nat Phot 2015)	coherent	Gaussian	hetero
Grosshans -Grangier 2002	coherent	Gaussian	homo
Usenko - Grosshans 2015	coherent	Gaussian 1D	homo
Garcia-Patron -Cerf 2009	squeezed	Gaussian	hetero
Filip 2008	thermal	Gaussian	homo/hetero
Madsen *et al* 2013	squeezed	Gaussian + add. Gauss.	homo/hetero
Fiurásek-Cerf 2012 Walk *et al* 2013	coherent	Gaussian	homo/hetero Gauss. postsel

Other Gaussian protocols (2/2)

- current EUR only works if Alice performs homodyne detection (protocol with squeezed states)
- alternative: Gaussian optimality + de Finetti: requires bound on the CM

Estimation of the CM

- note that there are 2 CM: one for ρ, and one for measurement outcomes (x, y) (not equivalent for PM protocols)
- "manageable" if protocol sufficiently symmetric [AL, PRL 2015]
- seems harder but doable for GG02
- but unclear whether the Gaussian de Finetti can be adapted $\implies$ problem for finite size setting

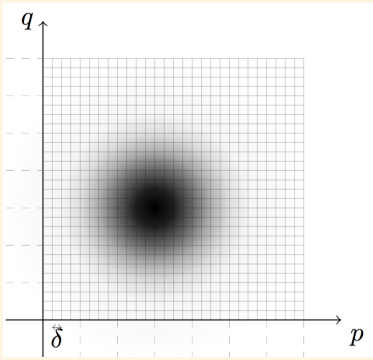
Remark: for protocols with Gaussian modulation, one can easily compute the CM of the quantum state in the EB version from the CM of the classical data in the PM version

Imperfect modulation

For all the PM protocols, one assumes that Alice prepares the states with a Gaussian modulation

$\Longrightarrow$ never the case in practice!

$\Longrightarrow$ No really satisfying answer at the moment!



Only analysis: Jouguet *et al*, Phys. Rev. A 86, 032309 (2012)

idea: bound trace distance between ideal state sent by Alice and true state

- ideal state: Gaussian distribution $\rho = \sum_{n=0}^{\infty} \frac{\bar{x}^n}{(\bar{x}+1)^{n+1}} |n\rangle\langle n|$ (thermal state)
- Cartesian modulation: $\sigma_{\mathrm{cart}} = \sum_{k=-N}^{N} \sum_{\ell=-N}^{N} p_k p_\ell |x_k + i p_\ell\rangle\langle x_k + i p_\ell|$
- polar modulation: $\sigma_{\mathrm{pol}} = \sum_{k=0}^{N} \sum_{\ell=0}^{M} r_k q_\ell |r_k e^{i\theta_\ell}\rangle\langle r_k e^{i\theta_\ell}|$

results: $\|\rho - \sigma\|_{\mathrm{tr}} \approx 10^{-10}$ for "reasonable" parameters: $2^8 \times 2^8$ bins for Cartesian modulation; 2000×2000 for polar modulation

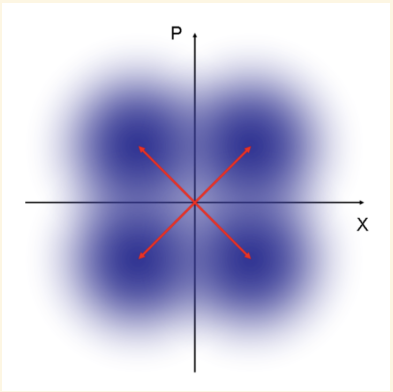
Open questions: 1) make the analysis composable; 2) intuitively approximate modulation should be sufficient

Discrete modulation

A solution is to switch to discrete modulation! [Lorenz, Korolkova, Leuchs (2004), Namiki, Hirano (2006), Zhao, Heid, Rigas, Lütkenhaus (2009), AL, Grangier (2009), Sych, Leuchs (2010), Bradler, Weedbrook (2017)...]

$\Longrightarrow$ easier to implement

$\Longrightarrow$ better for error correction



- unclear how to use EUR; what about collective attacks (+ de Finetti)?

2 covariance matrices

- A and B implement the PM protocol: they have data $\vec{x} \in \{0,1\}^n, \vec{y} \in \mathbb{R}^n$ (ignoring many issues) they can estimate the CM of $(\vec{x}, \vec{y})$
- pb: the bound on $\chi(Y;E)$ depends on the CM of ρ in the EB protocol!
- unknown how to relate $CM(\rho)$ and $CM(\vec{x}, \vec{y})$, except for nice quantum channels, or 2-state protocol ($\neq$ Gaussian protocols)

Note that Zhao *et al* (PRA 2009) manage to study the 2-state protocol in asymptotic limit (assuming CM is known)

Idea: extend approach of Coles/Winick/Lütkenhaus (reliable numerical key rates) to CV?

Conclusion and perspectives

- CV protocols are attractive for implementation reasons
- but their security is quite involved (infinite dimension, unbounded variables, discretization, truncation...)

challenges for theorists

- find better/tighter entropic uncertainty relations
- show that active symmetrization isn't necessary
- prove the security of all Gaussian protocols, eg GG02
- security of 4-state protocol (rate $\gg$ 2-state protocol)

Thanks!