Quantum key distribution and quantum error correction with continuous variables

by Aurélie Denys

under the supervision of Anthony Leverrier

05/04/2024

Quantum Information

1st and 2nd quantum revolutions

- 1st revolution: lasers, transistors
- 2nd revolution: control of individual particles

Quantum Communication

- Communication whose security is guaranteed by quantum physics
- Quantum key distribution for setting with 2 protagonists

Quantum Computing

- Perform computations by processing quantum information
- Deal with errors $\Rightarrow$ quantum error correction

Quantum Information

1st and 2nd quantum revolutions

- 1st revolution: lasers, transistors
- 2nd revolution: control of individual particles

Quantum Communication

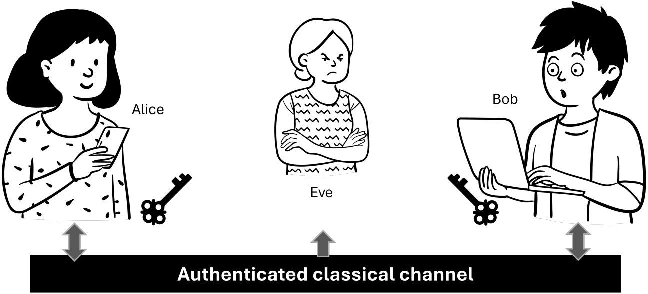
- Communication whose security is guaranteed by quantum physics
- Quantum key distribution for the setting with 2 protagonists

Quantum Computing

- Perform computations by processing quantum information
- Deal with errors $\Rightarrow$ quantum error correction

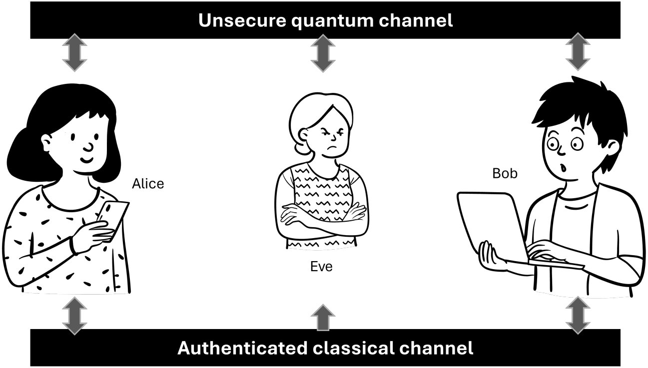
The key distribution problem

A secret shared key can be used to securely encrypt communications... but how to agree on a key?



Quantum key distribution (QKD)

Idea: Key exchange protocol with security guaranteed by quantum physics[1]



[1] Bennett & Brassard 1984, Ekert 1991

QKD Protocol

Quantum transmission phase

- Alice: random variable α_k
- She sends a quantum state $|\phi(\alpha_k)\rangle$ to Bob
- Bob's measure $\rightarrow \beta_k$

Classical post-processing

- Obtain a shared secret key from the correlated strings $(\alpha_1, \alpha_2, \alpha_3, \dots)$ and $(\beta_1, \beta_2, \beta_3, \dots)$

Security proofs

- Bound Eve's information using level of correlation of strings
- Compute length of secret key that can be distilled

QKD with discrete or continuous variables

Discrete-variable QKD[2]

- $\alpha_k,\ \beta_k \in \{0, \ldots, d\}$
- Easy proofs[3]
  States in $\mathcal{H} = Span(\{|0\rangle, |1\rangle\})$
- Requires expensive single-photon detectors

Continuous-variable (CV) QKD[4]

- $\alpha_k,\ \beta_k \in \mathbb{C}$
- Harder proofs
  $\mathcal{H} = Span(\{|n\rangle, n \in \mathbb{N}\})$
- Uses standard telecom equipment
  $\Rightarrow$ Reduced gap between theory and experiments

Our goal: Security of *realistic* CV QKD protocols

[2] Bennett & Brassard 1984, Ekert 1991
[3] Shor & Preskill 2000
[4] Grosshans & Grangier 2002

Quantum Information

1st and 2nd quantum revolutions

- 1st revolution: lasers, transistors
- 2nd revolution: control of individual particles

Quantum Communication

- Communication whose security is guaranteed by quantum physics
- Quantum key distribution for the setting with 2 protagonists

Quantum Computing

- Perform computations by processing quantum information
- Deal with errors $\Rightarrow$ quantum error correction

Quantum error correction

Why error correction?

Gate fidelity of 99.9% $\Rightarrow \sim 1000$ gates possible $\neq 10^{12}$ gates needed[5]

- Key idea: introduce redundancy
- Encode information into higher-dimensional space
  $\Rightarrow$ Quantum error correcting codes[6]
- Corrected memory not enough, also want gates
  $\Rightarrow$ Fault-tolerant quantum computing[7]

[5] Beverland et al. 2022
[6] Shor 1995
[7] Aharonov & Ben-Or 1996

Discrete and continuous classical error correction (EC)

Discrete EC

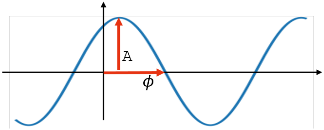
- Encode logical bit into physical bits
- Example: repetition code

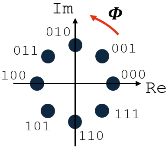
$$0_L = 000, \quad 1_L = 111$$

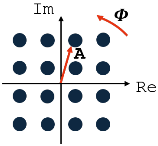
- Information recovered by majority vote $\rightarrow$ corrects a single bit flip

Continuous EC

Encode strings of bits into continuous variables, e.g. phase and amplitude of electric signal





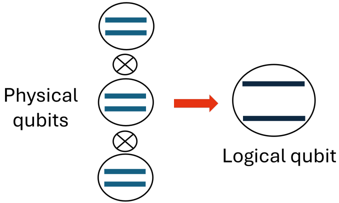


Discrete and continuous quantum error correction (QEC)

Discrete QEC

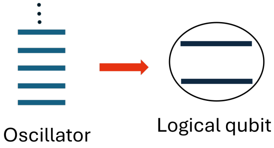
Logical qubit encoded into physical qubits[8], e.g.,

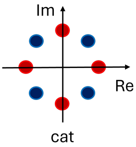
$$|0\rangle_L = |0\rangle\,|0\rangle\,|0\rangle \qquad |1\rangle_L = |1\rangle\,|1\rangle\,|1\rangle$$

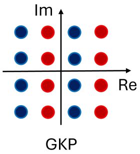


Continuous QEC

Logical qubit encoded into bosonic mode(s) $=$ oscillator(s)[9]



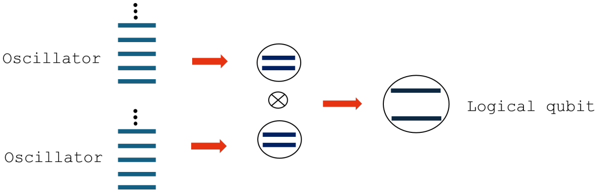




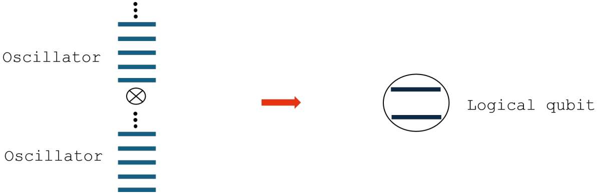
[8] Shor 1995, Steane 1996, Calderbank & Shor 1996
[9] Cochrane et al. 1999, Gottesman & Kitaev & Preskill 2001

Multi-mode encodings

- Concatenation of discrete and continuous encodings



- Better performances expected from multi-mode codes



Our goal: Initiate study of two-mode codes

Outline

1. Continuous-variable quantum key distribution
   - Explicit analytical bound on Eve's information, in CV QKD protocols, using arbitrary state modulation[10]
2. Multimode bosonic codes
   - Construction of a new two-mode bosonic code: the $2T$-qutrit[11]
   - Construction of two-mode bosonic codes with easily implementable gates[12]

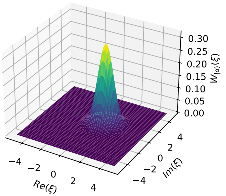
[10] **Aurélie Denys**, Peter Brown, Anthony Leverrier, *Quantum* 5, 540 (2021)
[11] **Aurélie Denys**, Anthony Leverrier, *Quantum* 7, 1032 (2023)
[12] **Aurélie Denys**, Anthony Leverrier, arXiv:2306.11621 (2023)

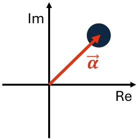
Continuous-variable quantum key distribution

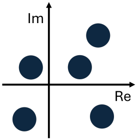
Continuous-variable QKD Protocol

States sent by Alice

- Idealisation of laser light
- Coherent state $|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n\in\mathbb{N}} \frac{\alpha^n}{\sqrt{n!}}|n\rangle$, $\alpha \in \mathbb{C}$
- Set of coherent states $\rightarrow$ constellation of points in the complex plane





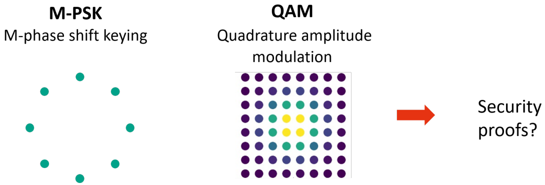


Measurement performed by Bob

- Double-homodyne measurement, $P(\beta|\alpha) = \frac{1}{\pi} e^{-|\alpha-\beta|^2}$

Discretely-modulated CV QKD

- Optimal case: Gaussian modulation[13] $\alpha \sim \mathcal{N}(0, V_A)$
- Well-understood security[14]
- But unrealistic $\Rightarrow$ Look at discrete constellations
  - analytical bounds for 2-3 states[15], numerical bounds for 4 states[16]
  - bigger discrete constellations?



[13] Grosshans & Grangier 2002
[14] García-Patrón & Cerf 2006, Navascues et. al. 2006, Leverrier 2017
[15] Zhao et al. 2009, Brádler & Weedbrock 2018
[16] Ghorai et al. 2019, Lin et. al. 2019, Upadhyaya et. al. 2021

Bounding Eve's information

- Goal: Bound Eve's information on key, from observed correlations

- Equivalent entanglement-based protocol $\rightarrow$ shared state $\rho_{AB}^{\otimes n}$
- Restriction to collective attacks, asymptotic regime

- García-Patrón & Cerf 2006, Navascues et al. 2006: Eve's information bounded by

$$f\left(\underbrace{\operatorname{tr}\left(\rho_{AB}\hat{a}^\dagger\hat{a}\right)}_{\text{depends on modulation}}, \underbrace{\operatorname{tr}\left(\rho_{AB}\hat{b}^\dagger\hat{b}\right)}_{\text{measured by Bob}}, \underbrace{\operatorname{tr}\left(\rho_{AB}(\hat{a}^\dagger\hat{b}^\dagger+\hat{a}\hat{b})\right)}_{\text{no access in experiment}}\right)$$

where $\hat{a}$ and $\hat{b}$ are Alice's and Bob's annihilation operators

$\Rightarrow$ Bound $Z = \operatorname{tr}(\rho_{AB}C)$, where $C = \hat{a}^\dagger\hat{b}^\dagger + \hat{a}\hat{b}$

SKR semi-definite program

- Ghorai et al. 2019: semi-definite program (SDP) whose solution is a lower bound on $Tr(\rho_{AB} C)$

$$
\min_{\rho} tr(\rho C)
$$

$$
\text{s.t.}
\begin{cases}
tr_B(\rho) = \bar{\tau} \\
tr(\rho C_1) = 2c_1 \\
tr(\rho C_2) = 2c_2 \\
tr\left(\rho(\Pi \otimes b^\dagger b)\right) = n_b \\
\rho \succcurlyeq 0
\end{cases}
$$

$\tau = \sum_k p_k |\alpha_k\rangle\langle\alpha_k|$

from observed statistics

ρ density matrix

- Numerical method explodes when number of states in constellation grows $\Rightarrow$ analytical bound?

Main result

- Sum-of-squares technique: exhibit K s.t. $KK^\dagger = C - E$ and $\mathrm{Tr}(\rho E)$ is easily bounded

$$KK^\dagger \succeq 0 \Rightarrow \mathrm{tr}(\rho C) \geq \mathrm{tr}(\rho E)$$

- Difficult technical part: find K leading to tight bound

$$K = z(A - xP^\dagger) + \frac{1}{z}B^\dagger \quad \text{with } x, z \in \mathbb{C} \text{ and operator } P \text{ optimised}$$

- Explicit analytical bound

$$\boxed{tr(\rho C) \geq 2c_1 - 2\left(\left(n_B - \frac{c_2^2}{\langle n \rangle}\right) w\right)^{\frac{1}{2}}}$$

Depends on the modulation

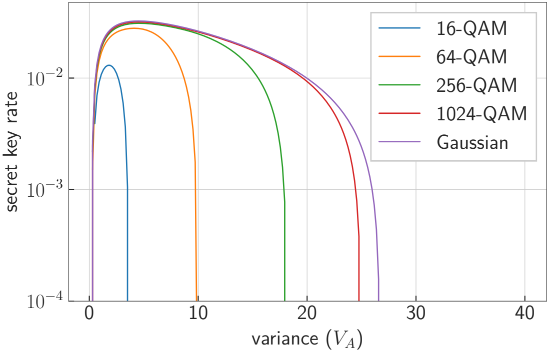
Estimated experimentally

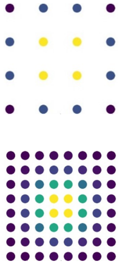
Average photon number

- Recover known values for 4-PSK and Gaussian modulation
- Can study big discrete constellations

Quadrature amplitude modulations

64-QAM already gives performances close to that of Gaussian modulation





Parameters: distance = 50 km, excess noise $\xi = 0.02$, binomial distribution

Conclusion

Main result

- Analytical bound on the secret key rate for CV QKD protocols with an arbitrary constellation of states
  $\Rightarrow$ 64 coherent states enough to get good performances

Follow-up works

- Experimental realisations[17]
- Optimisation of constellations[18]

Open question

Composable security against general attacks, in finite-size regime

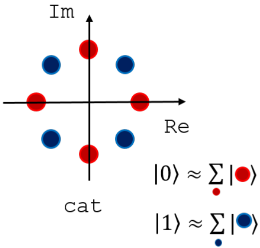
[17] Roumestan et al. 2022, Pan et al. 2022, Tian et al. 2023
[18] Almeida et al. 2021

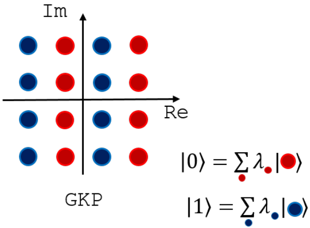
Multimode bosonic codes

Bosonic quantum error correction

Single-mode codes

Examples: cat[19] and GKP[20] codes





Multimode codes

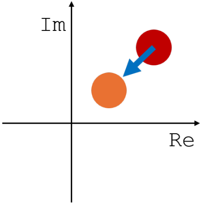
Example: multi-mode GKP

[19] Cohrane et al. 1999, Leghtas et al. 2013, Ofek et al. 2016
[20] Gottesman & Kitaev & Preskill 2021, Sivak et al. 2022

Noise in bosonic systems

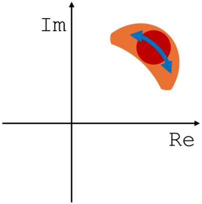
$$\mathcal{N} : \rho \mapsto \sum_k C_k \rho C_k^\dagger \quad \text{with} \quad \sum_k C_k^\dagger C_k = I$$

Loss



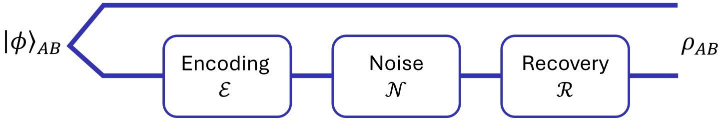
$$L_k = \frac{1}{\sqrt{k!}} \left(\frac{\gamma}{1-\gamma} \right)^{\frac{k}{2}} \hat{a}^k \, (1-\gamma)^{\hat{n}/2}$$

Dephasing



$$D_k = \sqrt{\frac{\gamma_\phi^k}{k!}} e^{-\frac{\gamma_\phi}{2}\hat{n}^2} \hat{n}^k$$

Figure of merit: the entanglement fidelity



$$f(\mathcal{R}\circ\mathcal{N}\circ\mathcal{E}) = \langle\phi|\underbrace{(I_A\otimes(\mathcal{R}\circ\mathcal{N}\circ\mathcal{E}))(|\phi\rangle\langle\phi|)}_{\rho_{AB}}|\phi\rangle$$

with $|\phi\rangle$ maximally entangled state

- Quantifies how close a state is from the original state after performing a recovery operation
- Find good code = find $\mathcal{E}$ such that fidelity is large (for optimal $\mathcal{R}$)

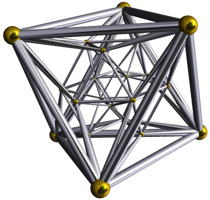
Defining a code

Two steps

- Choice of constellation of 2-mode coherent states
- Choice of subspace of small dimension within constellation span

Constellation

- GKP codes $\rightarrow$ additive group
  Cat codes $\rightarrow$ multiplicative group
- Look at subgroups of units of quaternions
- Our choice: 24 coherent states $|\alpha_\ell\rangle\,|\beta_\ell\rangle$ s.t. $\alpha_\ell + j\beta_\ell \in 2T$
- Corresponds to vertices of the 24-cell



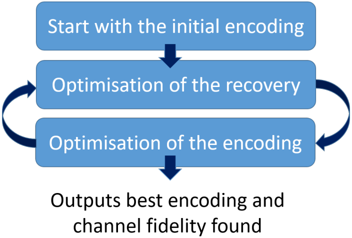
Projection of 24-cell[21]

[21] Robert Webb's Stella software, CC-BY-SA-3.0

Finding a good subspace (1/2)

First idea: maximise entanglement fidelity for loss to find qubit within 24-dimensional space

- Iterative optimisation method[22] (via SDPs)

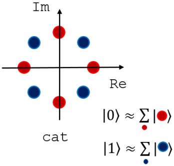


- Work in the basis given by the 24 coherent states $\Rightarrow$ avoid need for truncations
- Did not work well to find an explicit code in practice

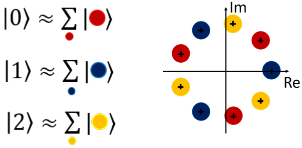
[22] Reimpell & Werner, 2005

Finding a good subspace (2/2)

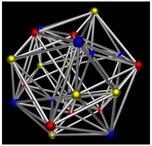
Second idea: Look at the symmetries of the constellation



8-legged cat qubit



9-legged cat qutrit



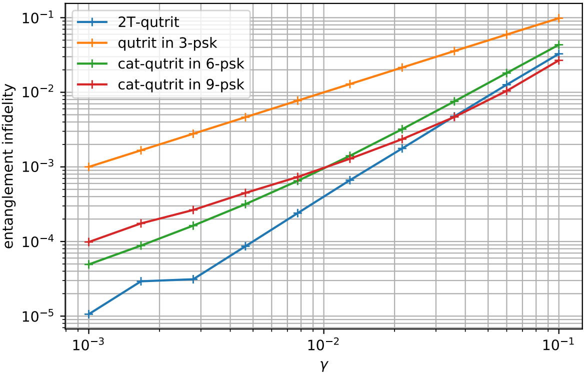
2T-qutrit[23]

- Define codewords from cosets of a subgroup of the constellation group
- Dimension of code = number of cosets of the subgroup

[23] figure of the 24-cell by UtilisateurTheon, CC-BY-SA-4.0, Commons

Performances of the 2T-qutrit against loss

For small loss strengths γ, $2T$-qutrit performs better than cat qutrits

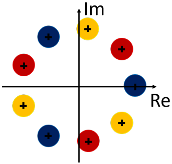


Entanglement infidelity $(1-f)$ *vs* loss parameter γ

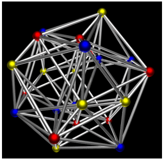
Interesting features

Logical operators

- X and $X_{12} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ gates implemented with Gaussian unitaries



9-legged cat qutrit



2T-qutrit[24]

Follow-up work

- Quantum spherical codes[25]

[24] figure of the 24-cell by UtilisateurTheon, CC-BY-SA-4.0, Commons
[25] Jain & Barg & Albert, 2023

Easily implementable gates

Question

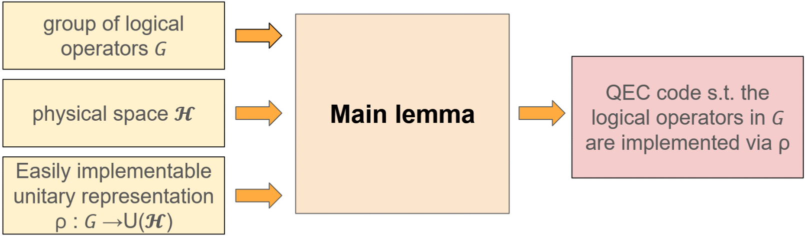
Can we find codes with specific gates implemented as passive Gaussian unitaries?

Usual approach: First find good QEC code, then look at gates that can be easily implemented

Our approach: Choose easily-implementable gates first[26]

[26] Gross, 2021

Main contribution



Two-mode bosonic qubits:

- $\mathcal{H}$: 2 oscillators
- $\rho(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) : |\alpha_1, \alpha_2\rangle \mapsto |\beta_1, \beta_2\rangle$ with $\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$
- $G \subseteq U(2)$, e.g. single Pauli group, single Clifford group
- $|\psi\rangle_L = \sum_{g \in G} \lambda_g \rho(g) |\alpha_1, \beta_1\rangle = \sum_{g \in G} \lambda_g |\alpha_g, \beta_g\rangle$

The Clifford qubit

- $H = \frac{1}{\sqrt{2}} \begin{pmatrix} \eta & \eta \\ -\eta^{-1} & \eta^{-1} \end{pmatrix}, \quad S = \begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}, \quad \eta = e^{i\frac{\pi}{4}}$
- $G = \langle H, S \rangle$, subgroup of $SU(2)$ of 48 elements

Gates

- Single-qubit Clifford operators implemented with Gaussian unitaries
- C-Z gate : $e^{\frac{i\pi}{4}(\hat{n}_1 - \hat{n}_2 - 1)(\hat{n}_3 - \hat{n}_4 - 1)} \to$ multi-qubit Clifford group
- T gate : $e^{\frac{i\pi}{16}(\hat{n}_1 - \hat{n}_2 - 1)^2} \to$ universal gate set

$\Rightarrow$ Properties similar to GKP, but with much smaller constellation

Conclusion

Summary

- Method to design QEC codes that admit a specific group of easily-implementable logical gates
- Universal gate set for Clifford code, with Gaussian unitaries and CROTs

Open questions

- State preparation?
- Error-correcting performance?
- Explicit recovery procedure?
- Experimentally-relevant examples?

Summary of contributions and open questions

CV QKD

- Explicit analytical bound on the asymptotic secret key rate of CVQKD protocols

$\Rightarrow$ Finite-size regime for general attacks?

QEC

- Definition of a new two-mode code: the 2T-qutrit
- Method to design QEC codes that admit a specific group of easily-implementable logical gates

$\Rightarrow$ Error-correcting properties of the general family of codes introduced?