Random coding for sharing bosonic quantum secrets

F. Arzani[1,2]*, G. Ferrini[3], *F. Grosshans[2]*, *D. Markham[2]*

[1]*Université de Lorraine, CNRS, Inria, LORIA, F 54000 Nancy, France*

[2]*Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6, F-75005 Paris, France*

[3]*Department of Microtechnology and Nanoscience (MC2),Chalmers University of Technology, SE-412 96 Gothenburg, Sweden*

VanQuTe

Introduction

What ? A vast class of random schemes to share continuous-variable states.

How ? Bosonic modes in **arbitrary secret** states are mixed with ancillary **squeezed modes** through a **passive interferometer**. We prove that **almost any interferometer can be used**.

Where ? The protocol was devised having **optical systems** in mind but can be adapted to **any bosonic system**.

Why ?
- Ease experimental requirements
- Potentially applicable to share interesting/useful states across networks
- Connections with relativity & black holes (via error correction)

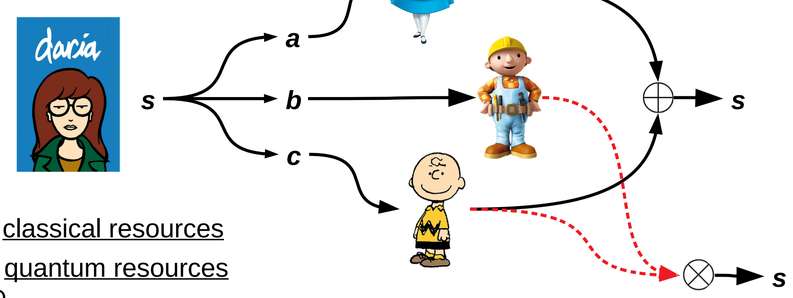
When ? Hopefully experiments will be implemented soon ;-)

Bonus : **Decoding** computed and implemented efficiently with a **Gaussian** unitary, # of squeezers ≤ 2 x # of secret modes

Secret sharing 101

A. Shamir, Comms of the ACM 22 (11) (1979)

A **dealer** shares a **secret** with several **players** in such a way that **authorized subsets** of players have to **collaborate** to retrieve it



CC: Classical information shared using classical resources

CQ: Classical information shared using quantum resources
→ Improved security ~ multipartite QKD

QQ: The secret is a quantum state

M. Hillery, V. Bužek & A. Berthiaume, PRA 59 (1999)
R. Cleve, D. Gottesman & H.-K. Lo, PRL 83 (1999)

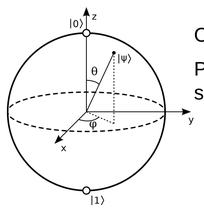
T. Tyc & B.C. Sanders, PRA 65 (2002)

Access parties: Authorized subsets of players
Adversary structure: Groups that should not get information
Threshold schemes: any *k* or more players are authorized

Continuous-variable systems

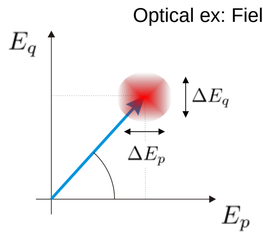
DV : information encoded in qubits

CV : observables with continuous spectrum e.g. : $\hat{q}$, $\hat{p}$



Optical ex:
Polarization of single photon

Optical ex: Field quadratures



$$\hat{E}_Q \propto \hat{a} + \hat{a}^\dagger$$

$$\hat{E}_P \propto i(\hat{a}^\dagger - \hat{a})$$

Wigner function ~ quantum optical phase space

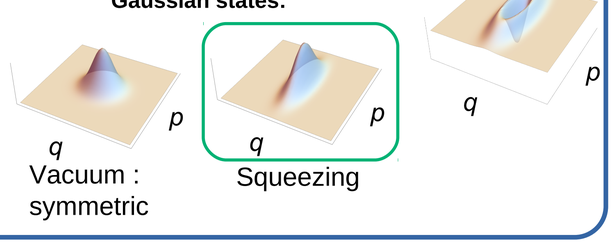
May be negative!

$$|\psi\rangle \longrightarrow W_\psi(q,p)$$

$$\int \mathrm{d}p\, W(q,p) = |\langle q\,|\psi\rangle|^2$$

$$\int \mathrm{d}q\, W(q,p) = |\langle p\,|\psi\rangle|^2$$

Gaussian states:

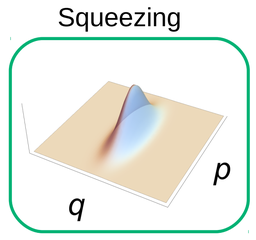


Vacuum : symmetric

Squeezing

Squeezed states

Squeezing



Reduced fluctuations in *q* or *p*

⇩

In the limit, eigen-states of *q* or *p*

Workhorse of CV Quantum information:

- **Easy** to produce in the lab (non-linear optics)
- Deterministic entanglement with passive linear optics
- Used for quantum teleportation
- Experimental production of **CV graph states**

Gaussian unitaries

Vector notation for quadratures reveals symplectic structure:

$$\boldsymbol{\xi} = \begin{pmatrix} \boldsymbol{q} \\ \boldsymbol{p} \end{pmatrix} \qquad [\xi_j, \xi_k] = iJ_{jk}$$

$$J = \begin{pmatrix} 0 & \mathbb{I} \\ -\mathbb{I} & 0 \end{pmatrix}$$

Standard symplectic form

Symplectic Group

$$S^T J S = J$$

$$\mathrm{Sp}(2n, \mathbb{R})$$

Unitary Gaussian transformations

$$U_G^\dagger \boldsymbol{\xi} U_G = S\boldsymbol{\xi} + \boldsymbol{x} = \boldsymbol{\xi}'$$

Symplectic — Phase-space translation

Any ***S*** composing:

$$S = R_1 K R_2$$

Squeezing:

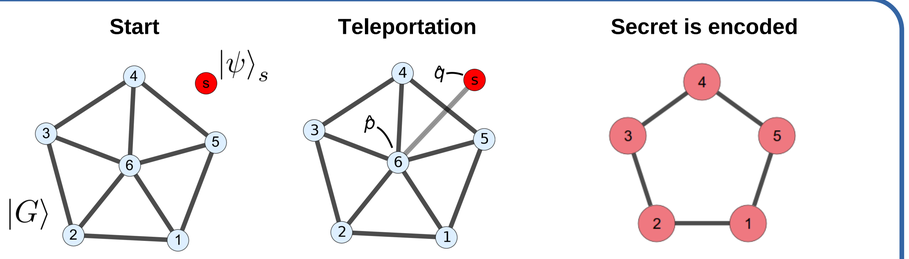
$$K = \mathrm{diag}\left(e^{r_1}, \ldots, e^{r_n}, e^{-r_1}, \ldots, e^{-r_n}\right)$$

Linear optics (passive **interferometers**)

$$R = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix}, \quad X + iY \in U(n)$$

Graphs states example

Start **Teleportation** **Secret is encoded**



(CV) Bell Measurement

Any 3 modes can retrieve the secret (decoding from stabilizer formalism)

P. Van Loock & D. Markham, AIP Conf. Proc. 1363, 256, (2011)

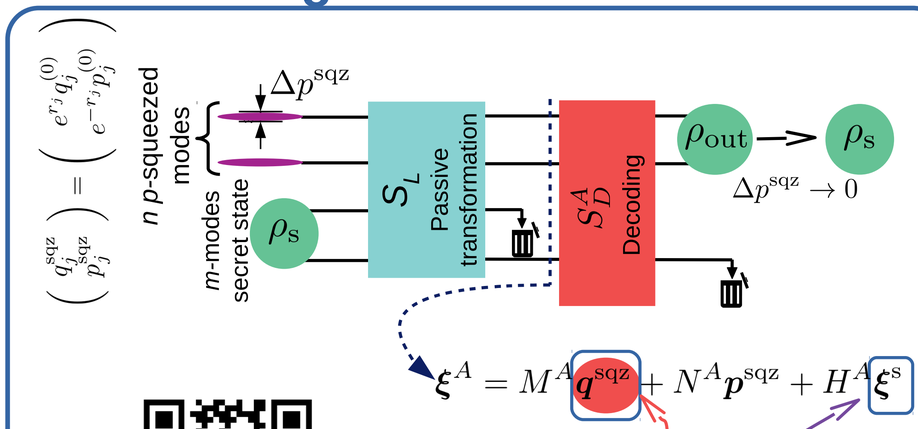
Ideal cluster states : momentum eigenstates + C_Zs (entangling gates)
Realistic cluster states : squeezed states + C_Zs (entangling gates)

Experiments : squeezed states + linear optics

What's the most general interferometer that does the trick ?

Motivated by actual experimental setup : *Y. Cai, et al, Nat. Comm. 8, 15645 (2017)*

A general scheme



Scan for details

Goal: 1) Get rid of these

2) solve for these

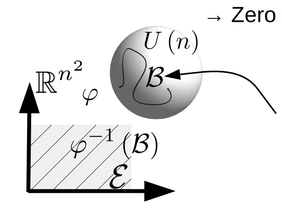
Sketch of the proof

For each *A*, find *R* s.t

$$RM^A = \mathbf{0} \Leftarrow k \geq m + \lceil \frac{n}{2} \rceil$$

$$\det\left(RH^A\right) \neq 0$$

$\det\left(RH^A\right) = 0$ →«bad» matrices = lower dimensional set of *U(n)*
→ Zero Haar (constant) measure



«bad» matrices

If $S_L \notin \mathcal{B}$: ***A*** can **sample**

$$q_s + \sum_{l=1}^{n-1} B_{1l} p_l^{\mathrm{sqz}} = \sum_{j=1}^{j=k} \alpha_j \left(\cos\theta_j Q_j^A + \sin\theta_j P_j^A\right)$$

Or construct a **unitary Gaussian** decoding

Finite squeezing effects

Output fidelity for coherent state secret:

$$\mathcal{F}^A(r) = 1/\sqrt{1 + \sigma^2(r)\,\eta + \sigma^4(r)\,\zeta}$$

Depend on S_L

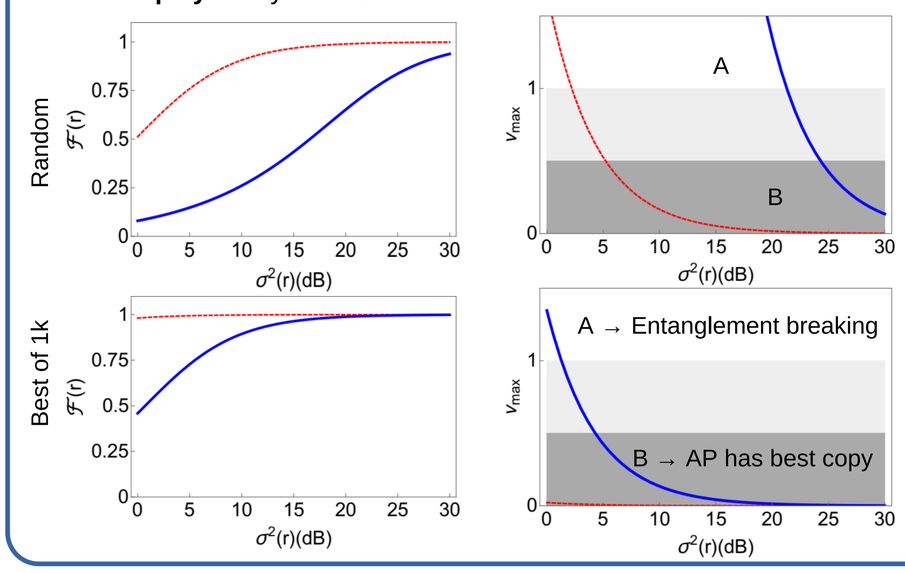
Any state:

$$W_{\mathrm{out}}(\boldsymbol{\xi}) = \int \left(\prod_{j=1}^{n} \mathrm{d}y_j \frac{e^{-\frac{y_j^2}{2\sigma_j^2}}}{\sigma_j \sqrt{2\pi}} \right) W_{\mathrm{in}}(\boldsymbol{\xi} - B\boldsymbol{y})$$

→ eigenvalues of $\mathcal{N} = B\Delta^2 B^T$

$$\Delta^2 = \mathrm{diag}\left(\sigma_1^2, \ldots, \sigma_n^2\right)$$

2 out of 3 players try to reconstruct **1** secret **mode**:



Adversaries

Finite squeezing:
some information always leaked to adversaries

Mutual information can be bounded *Habibidavijani & Sanders arXiv:1904.09506 (2019)*

High enough squeezing:
bound information leak (optimal cloning)

For infinite squeezing: **ramp scheme**:

$k \geq m + \lceil \frac{n}{2} \rceil$ → reconstruct

$k < \lceil \frac{n}{2} \rceil$ → no information

else → *some* secret quadratures w/o anti-sqz

Summary

Protocol for sharing any bosonic state using
1)Squeezed states
2)Random passive transformations (linear optics)

Still works for realistic squeezing values

Decoding is also Gaussian

Generalizes random erasure correcting codes to CV

TODO: Losses?
Optimize interferometer?
Experiments?

Further reading:
- *FA, G. Ferrini, F. Grosshans, D. Markham, PRA 100, 022303 (2019) [details on this work]*
- *Y. Cai, et al, Nat. Comm. 8, 15645 (2017) [a precursor, experimental]*
- *T. Tyc et al,"Quantum State Sharing with CV", in QI with CV of atoms and light (2007) [tutorial on CV state sharing]*
- *P. Hayden and A. May, Quantum 3, 196 (2019) [CV error correction in space-time]*

**fra.arzani@gmail.com*