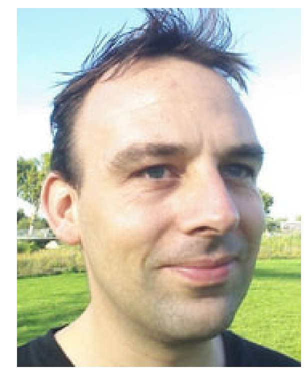
Random coding for sharing bosonic quantum secrets

F. Arzani, G. Ferrini, F. Grosshans, D. Markham

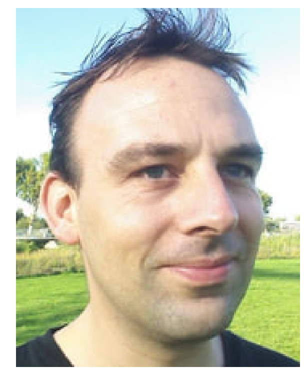
VanQuTe

Random coding for sharing bosonic quantum secrets

(continuous-variable)

F. Arzani, G. Ferrini, F. Grosshans, D. Markham





VanQuTe

Secret Sharing

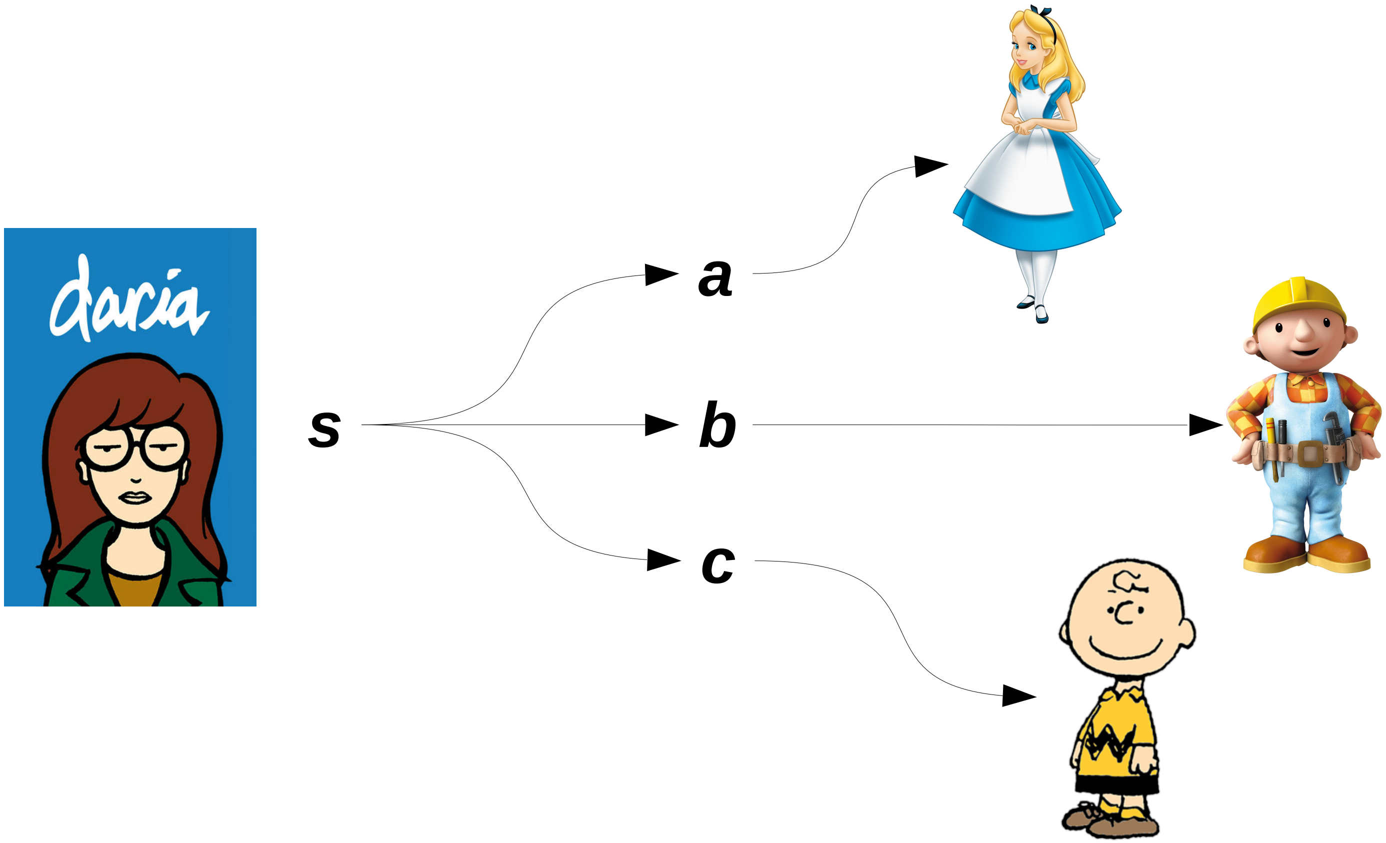
Secret Sharing

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

s

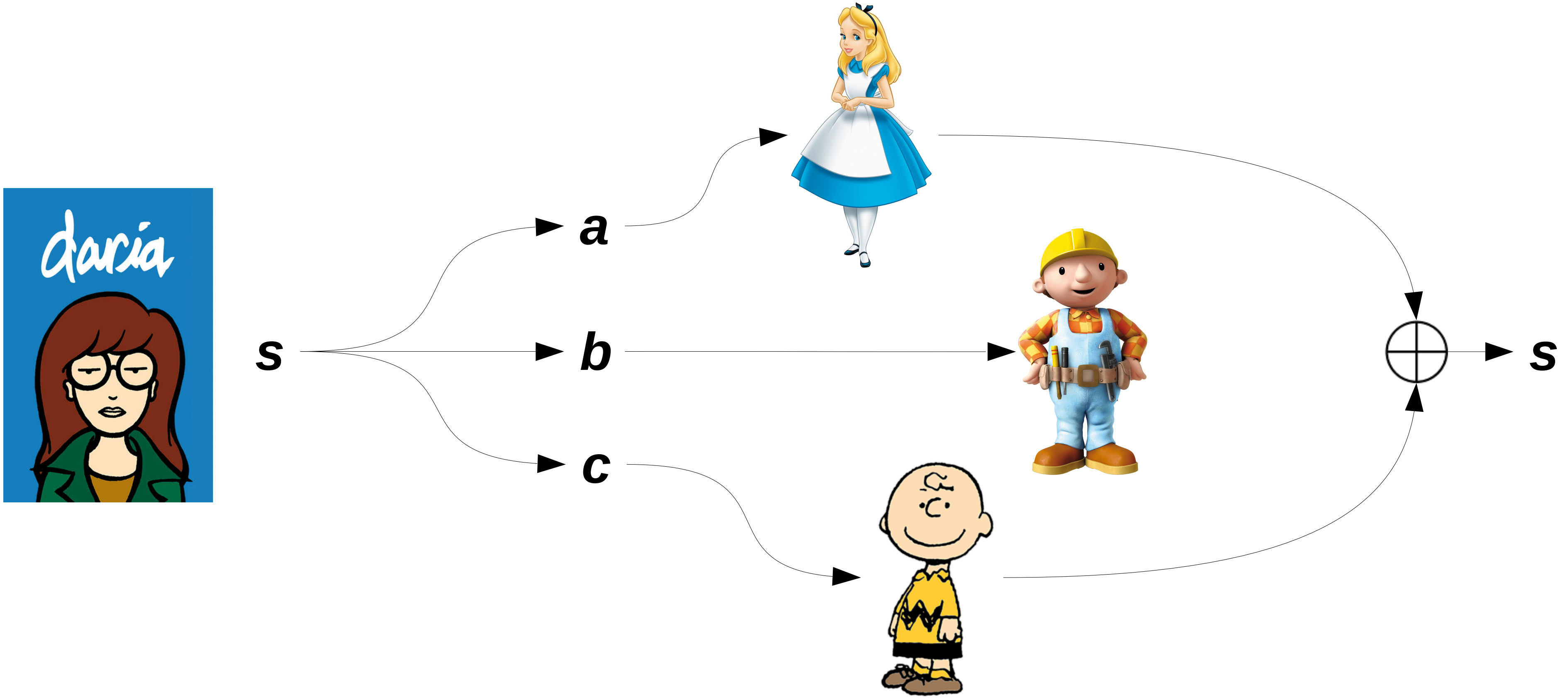
Secret Sharing

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



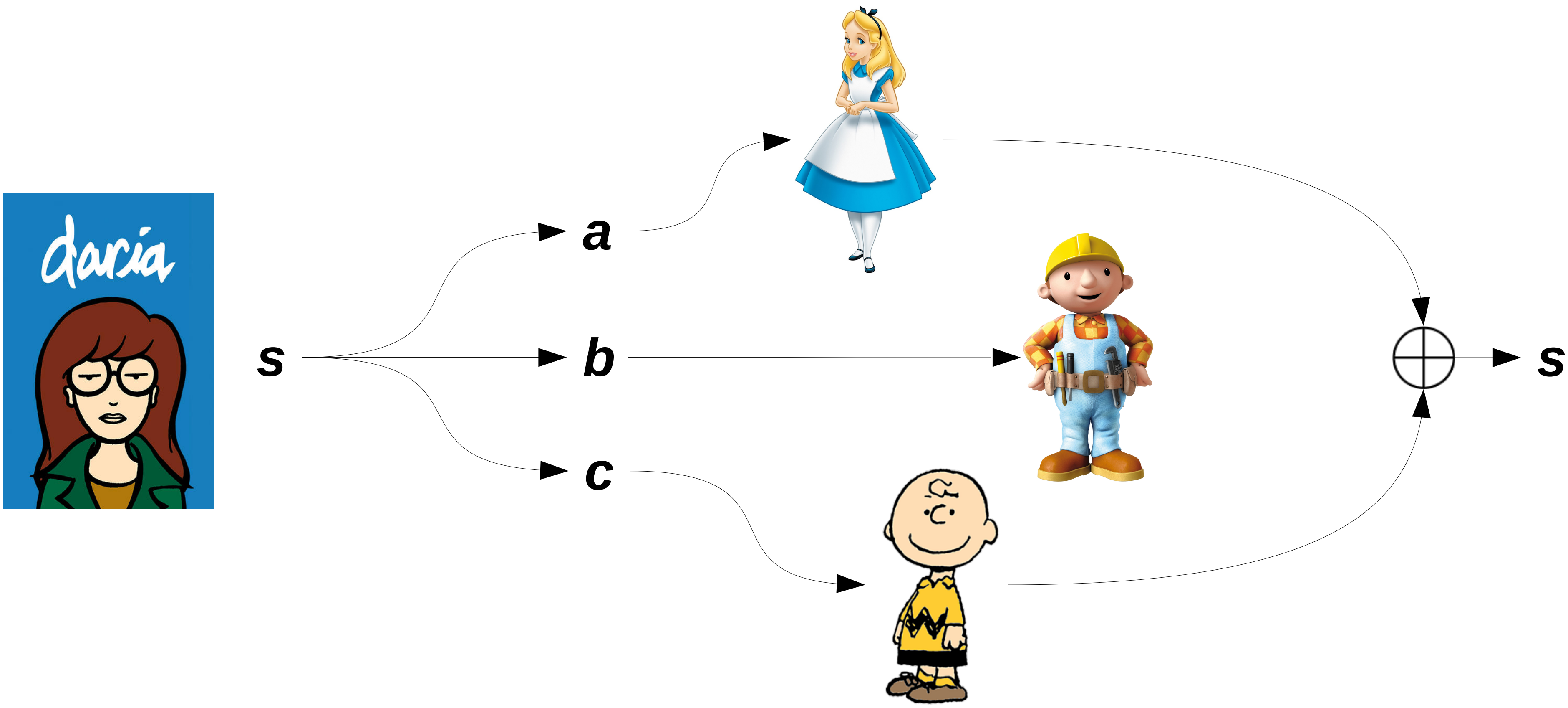
Secret Sharing

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



Secret Sharing

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



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

Several configurations

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

Some previous work

- First classical protocol *A. Shamir, Comms of the ACM 22 (11) (1979)*
- First proposal in DV (qubits) *M. Hillery, V. Bužek & A. Berthiaume, PRA 59 (1999)*
  R. Cleve, D. Gottesman & H.-K. Lo, PRL 83 (1999)
- Cluster-state based protocols in DV *D. Markham & B.C. Sanders, PRA 78 (2008)*
- Several proposals in CV... *T. Tyc & B.C. Sanders, PRA 65 (2002)*
  T. Tyc & B.C. Sanders, JoP A 36 (2003)
- ...and experiments *A.M. Lance et al, PRL 92 (2004)*
- CV cluster state - based protocols

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

H.-K. Lo & C. Weedbrook, PRA 88 (2013)

So what's new?

- **random encoding**! (...*almost any* passive interferometer)
- Multi-mode secrets

So what’s new?

- **random encoding**! (...*almost any* passive interferometer)
- Multi-mode secrets

Why would I care?

So what’s new?

- **random encoding**! (...*almost any* passive interferometer)
- Multi-mode secrets

Why would I care?

- Useful to design experiments

So what's new?

- **random encoding**! (...*almost any* passive interferometer)

- Multi-mode secrets

Why would I care?

- Useful to design experiments
- Potentially applicable to share interesting/useful states

So what's new?

- **random encoding**! (...*almost any* passive interferometer)

- Multi-mode secrets

Why would I care?

- Useful to design experiments
- Potentially applicable to share interesting/useful states
- Connections with relativity & black holes (via error correction)

Hayden & May arXiv:1806.04154 (2018)

Wu, Khalid & Sanders NJP 20 (2018)

Hayden & Preskill JHEP (2007)

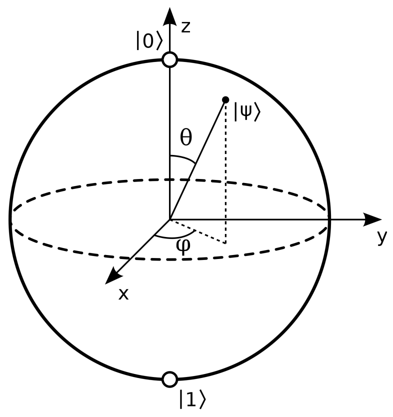
Outline

- Continuous-variable systems
- (Prologue &) Main result
- Sketch of the proof
- Quality of the scheme(s)
- Conclusions

Continuous variables

DV and CV, Gaussian states

DV : information encoded in qu-bits



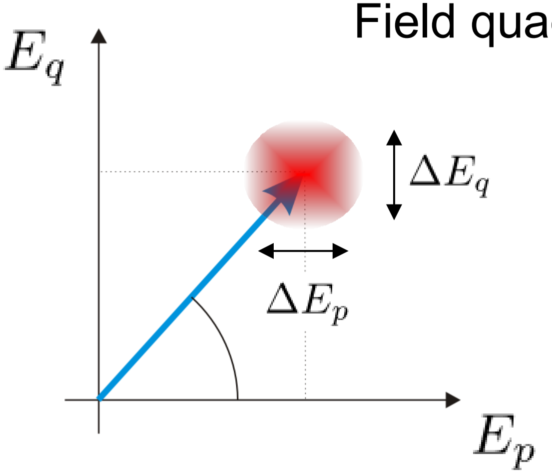
Optical ex:

Polarization of single photon

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

Optical ex:

Field quadratures

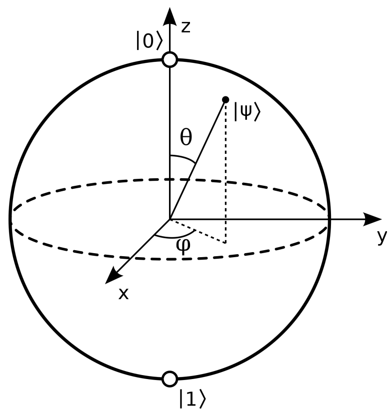


$$\hat{E}_Q \propto \hat{a} + \hat{a}^\dagger$$

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

DV and CV, Gaussian states

DV : information encoded in qu-bits



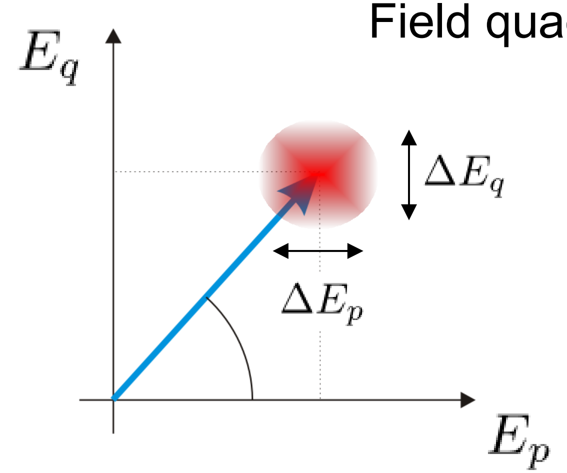
Optical ex:

Polarization of single photon

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

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

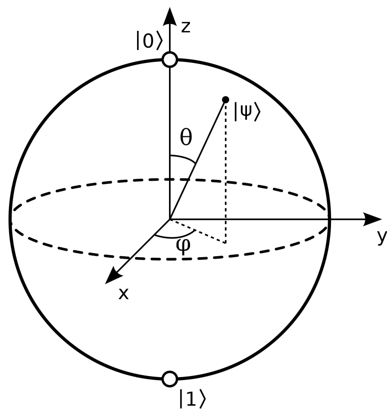
$$|\psi\rangle \longrightarrow W_\psi(q,p)$$

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

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

DV and CV, Gaussian states

DV : information encoded in qu-bits



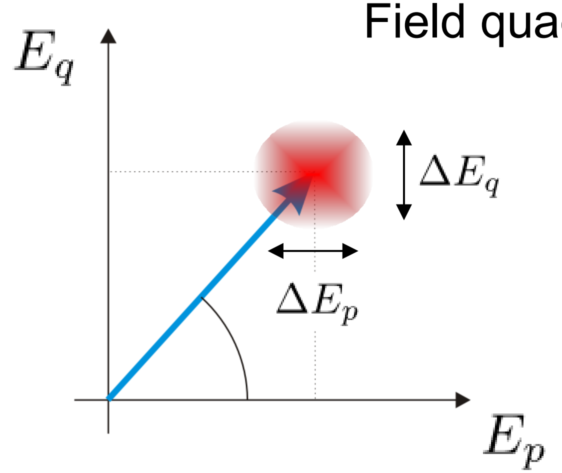
Optical ex:

Polarization of single photon

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

Optical ex:

Field quadratures



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

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

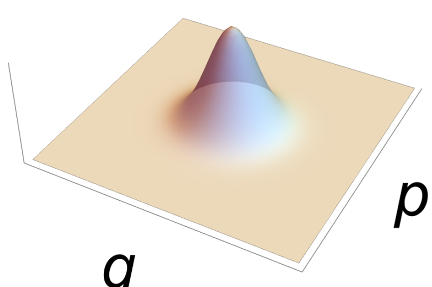
Wigner function ~ quantum optical phase space

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

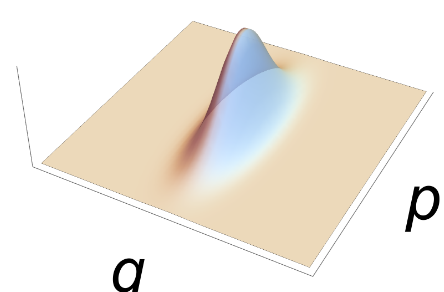
$$\int \mathrm{d}p \; W(q,p) = |\langle q \,|\psi\rangle|^2$$

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

Gaussian states:

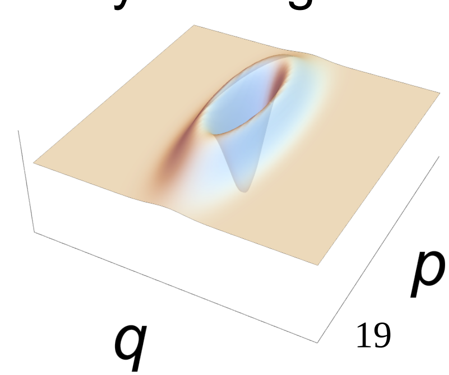


Vacuum → symmetric



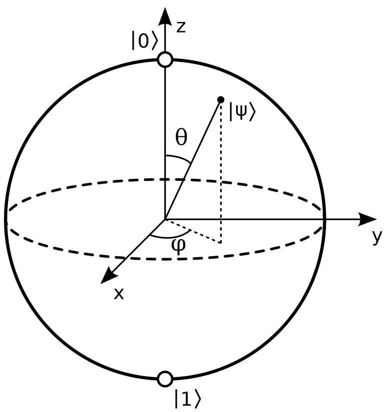
Squeezing

May be negative!



DV and CV, Gaussian states

DV : information encoded in qu-bits



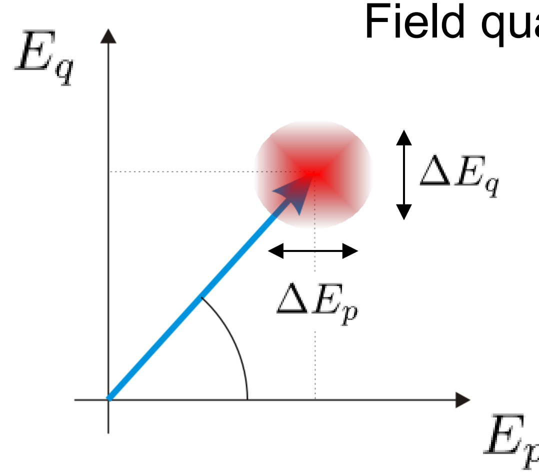
Optical ex:

Polarization of single photon

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

Optical ex:

Field quadratures



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

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

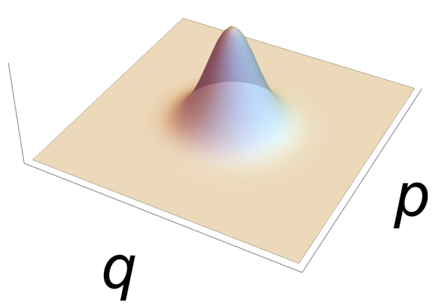
Wigner function ~ quantum optical phase space

Gaussian states:

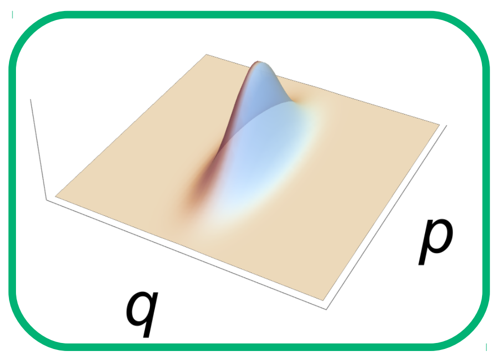
$$|\psi\rangle \longrightarrow W_\psi(q,p)$$

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

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

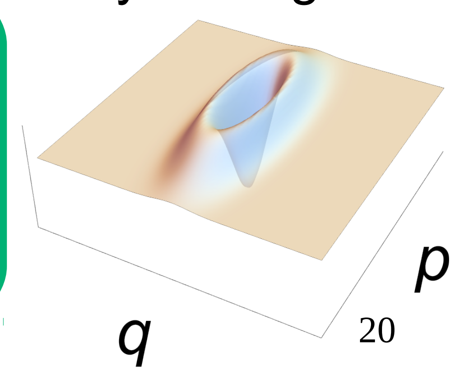


Vacuum → symmetric

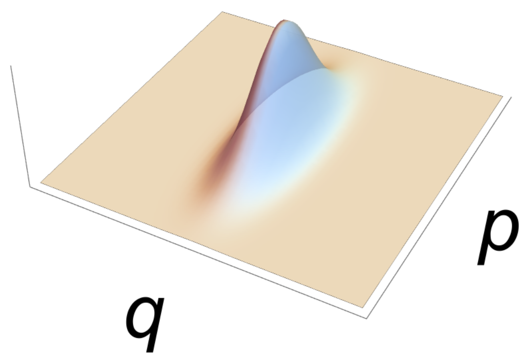


Squeezing

May be negative!



Squeezed states



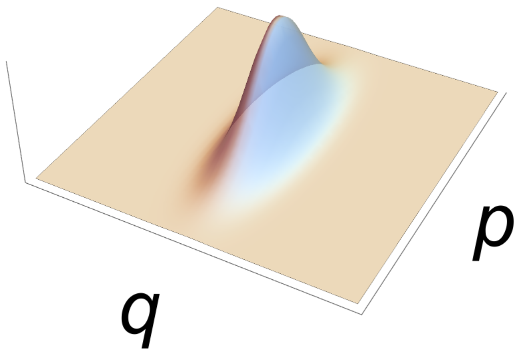
Squeezing

Reduced fluctuations in *q* or *p*

⇩

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

Squeezed states



Squeezing

Reduced fluctuations in q or p

$\Downarrow$

In the limit, eigen-states of q or p

Workhorse of CV Quantum information:

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

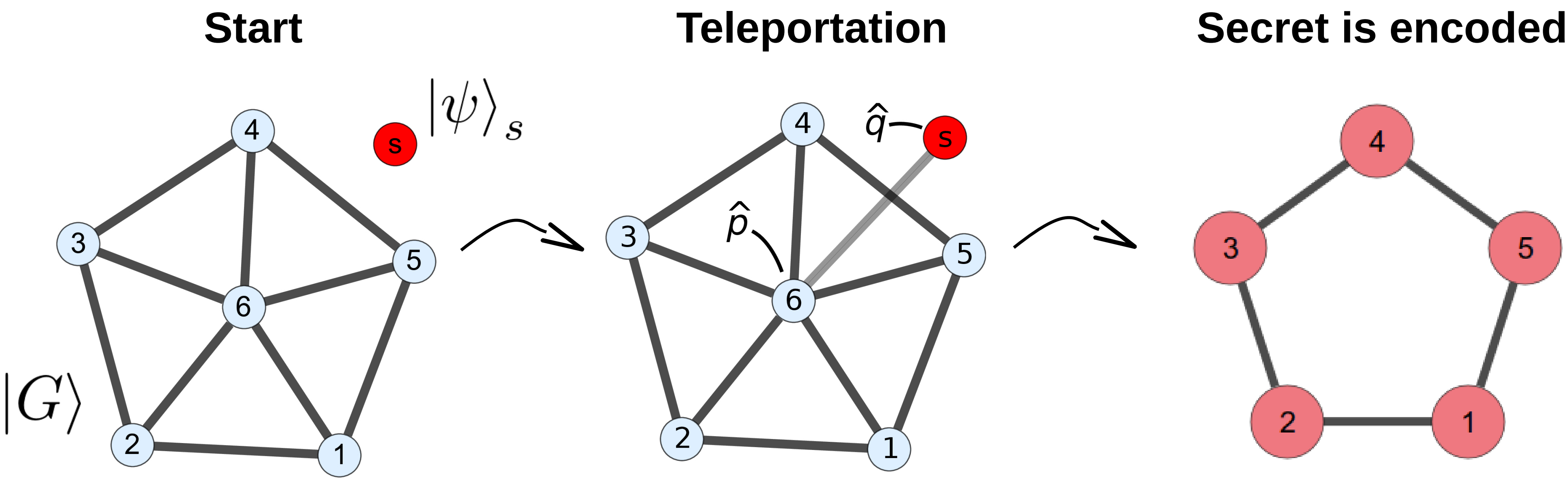
Main result

FA, G. Ferrini, F. Grosshans, D. Markham, PRA 100, 022303 (2019)

(arxiv)

A quantum *(3,5)* scheme with graph states

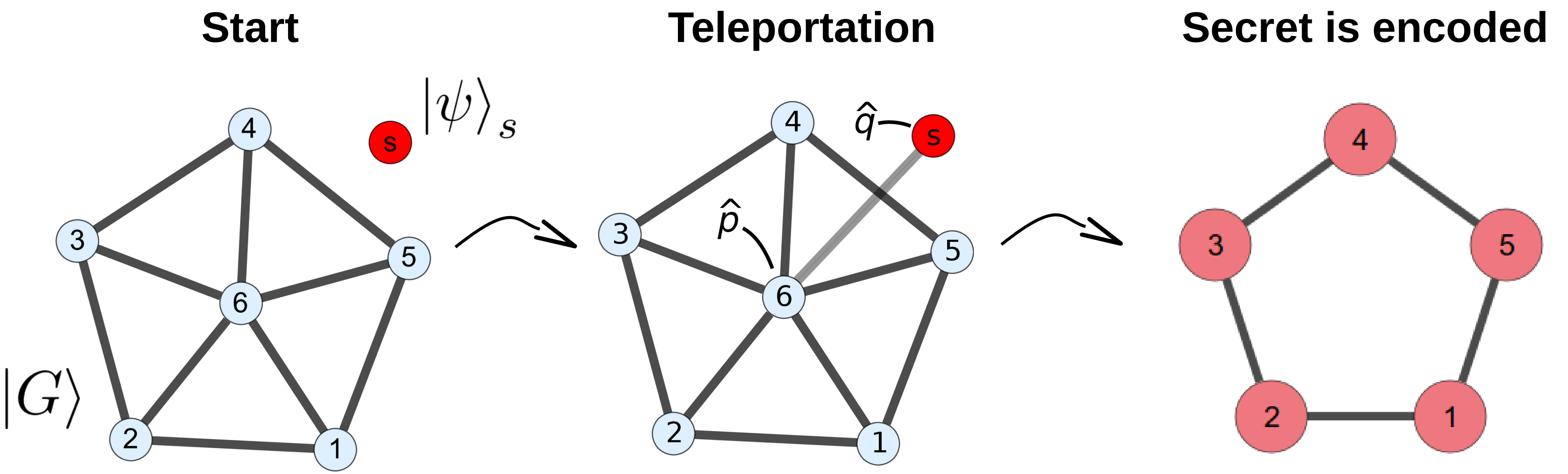
P. Van Loock & D. Markham, AIP Conf. Proc. 1363, 256, (2011)



(CV) Bell Measurement

A quantum *(3,5)* scheme with graph states

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

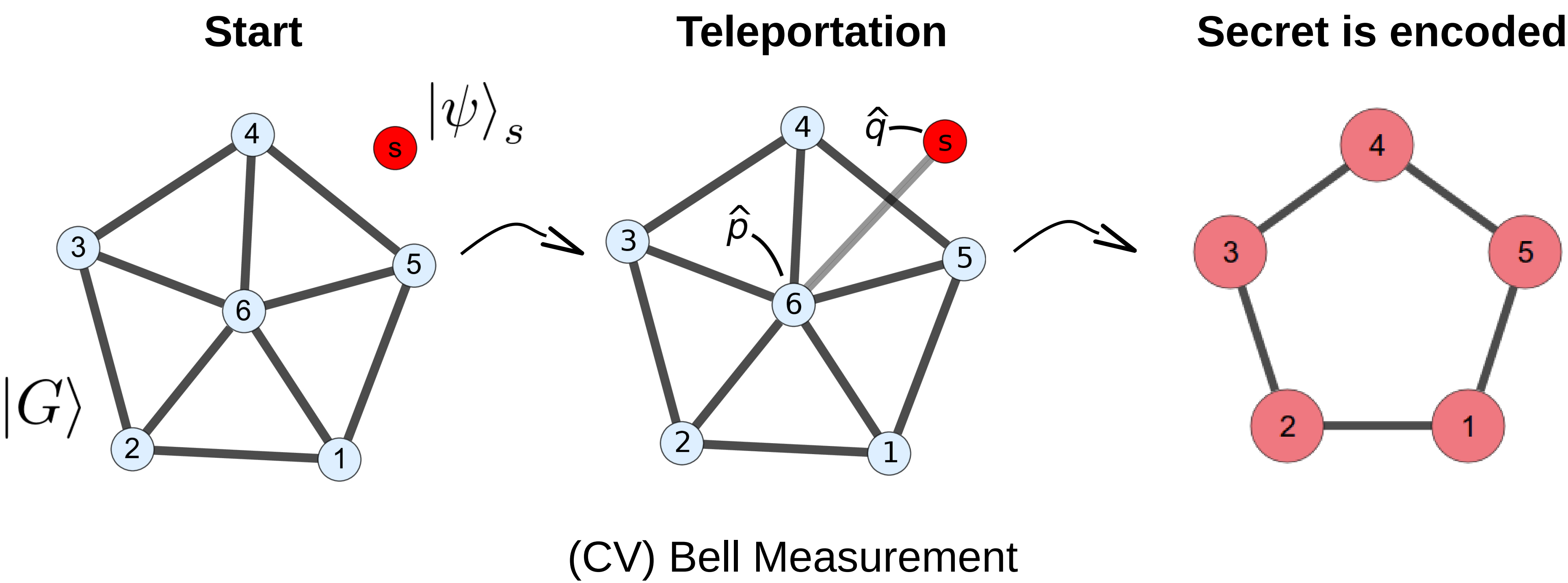


(CV) Bell Measurement

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

A quantum *(3,5)* scheme with graph states

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



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

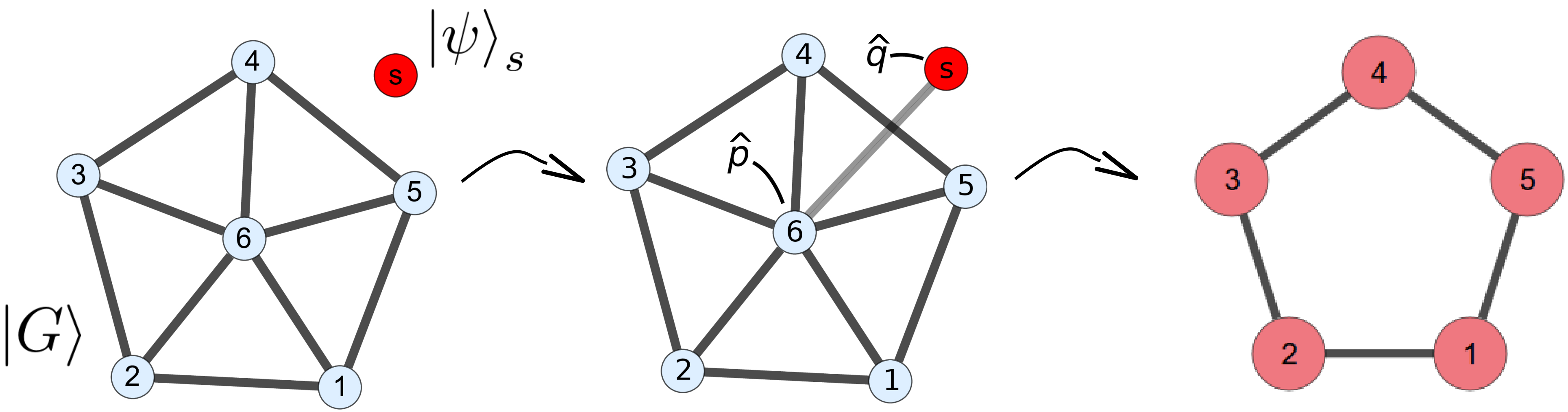
Realistic cluster states : $\underbrace{\text{squeezed states + } C_Z\text{s}}$ (entangling gates)

Experiments : squeezed states + <u>linear optics</u>

A quantum *(3,5)* scheme with graph states

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

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



(CV) Bell Measurement

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

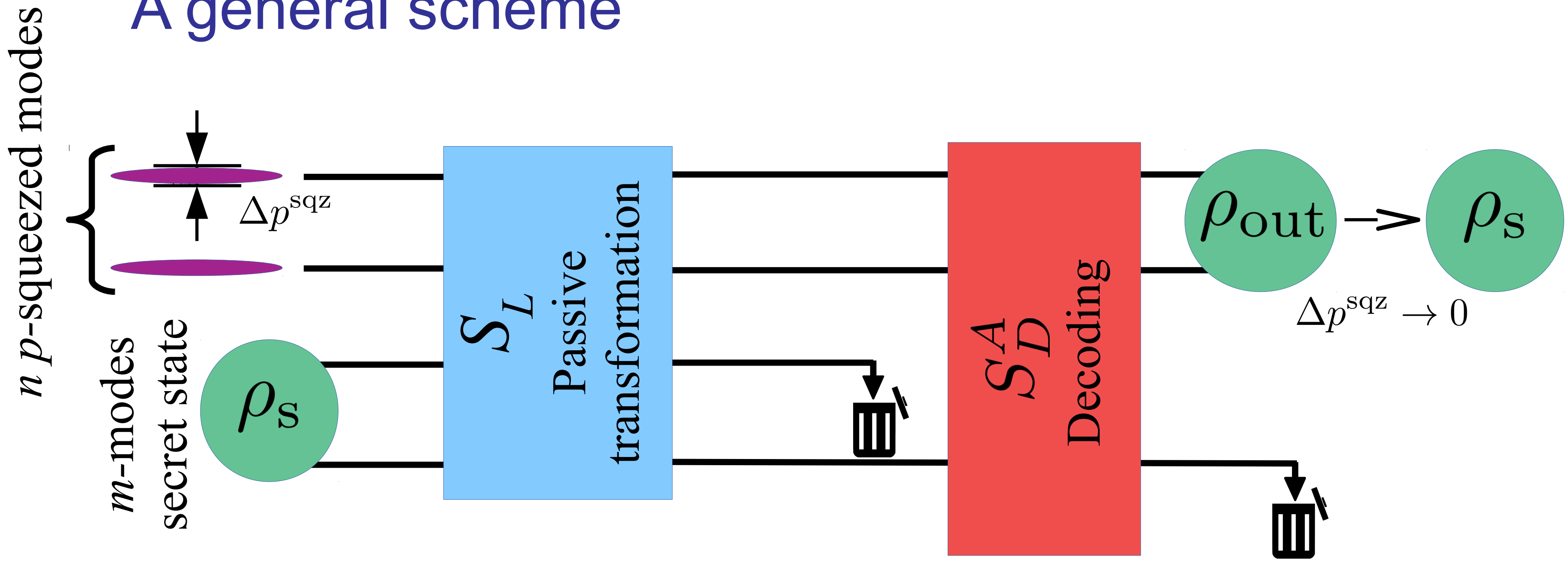
Realistic cluster states : squeezed states + C_Zs (entangling gates)

Experiments : squeezed states + <u>linear optics</u>

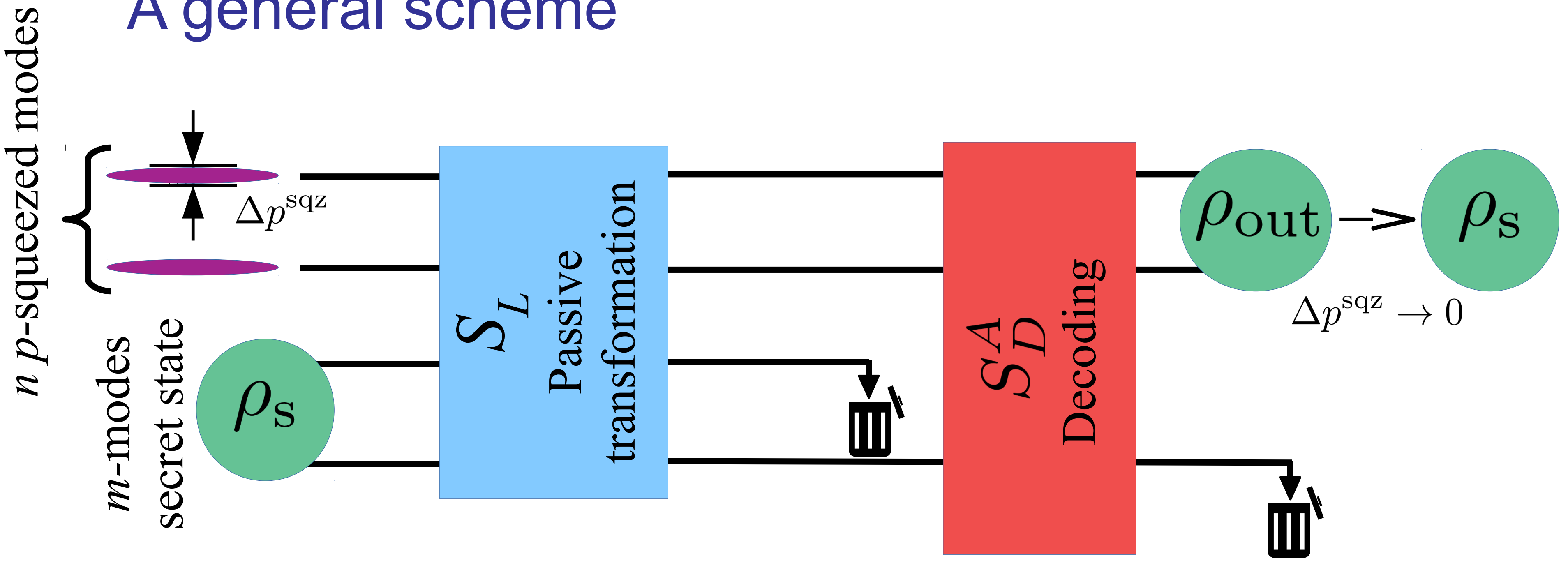
What's the most general interferometer that does the trick ?

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

A general scheme



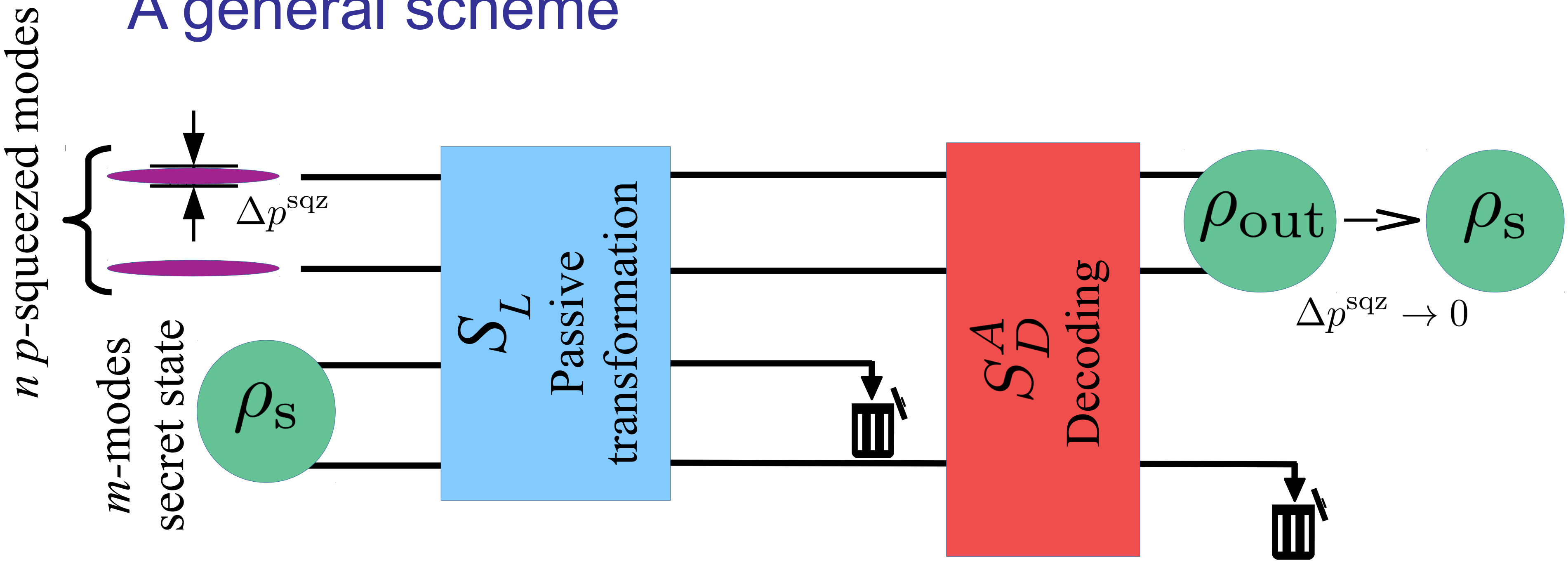
A general scheme



Derive conditions on the interferometer such that each access party can either:

- Measure secret quadratures
- Physically reconstruct the secret

A general scheme



Derive conditions on the interferometer such that each access party can either:

- Measure secret quadratures
- Physically reconstruct the secret

Almost any passive interferometer can do

(In the sense of Haar measure)

Sketch of the proof

Gaussian transformations and Symplectic matrices

$$\boldsymbol{\xi} = \begin{pmatrix} \boldsymbol{q} \\ \boldsymbol{p} \end{pmatrix} \qquad [\xi_j, \xi_k] = iJ_{jk} \qquad J = \begin{pmatrix} 0 & \mathbb{I} \\ -\mathbb{I} & 0 \end{pmatrix}$$

Standard symplectic form

Gaussian transformations and Symplectic matrices

$$\boldsymbol{\xi} = \begin{pmatrix} \boldsymbol{q} \\ \boldsymbol{p} \end{pmatrix} \qquad [\xi_j, \xi_k] = iJ_{jk} \qquad J = \begin{pmatrix} 0 & \mathbb{I} \\ -\mathbb{I} & 0 \end{pmatrix}$$

Standard symplectic form

Unitary Gaussian transformations

$$U_G^\dagger \boldsymbol{\xi} U_G = \underbrace{S}_{\text{Symplectic}}\boldsymbol{\xi} + \underbrace{\boldsymbol{x}}_{\text{Phase-space translation}} = \boldsymbol{\xi}'$$

Symplectic Group

$$[\xi'_j, \xi'_k] = iJ_{jk} \iff S^T J S = J$$

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

Gaussian transformations and Symplectic matrices

$$\boldsymbol{\xi} = \begin{pmatrix} \boldsymbol{q} \\ \boldsymbol{p} \end{pmatrix} \qquad [\xi_j, \xi_k] = iJ_{jk} \qquad J = \begin{pmatrix} 0 & \mathbb{I} \\ -\mathbb{I} & 0 \end{pmatrix}$$

Standard symplectic form

Unitary Gaussian transformations

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

Symplectic

Phase-space translation

Symplectic Group

$$[\xi'_j, \xi'_k] = iJ_{jk} \iff S^T JS = J$$

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

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**):

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

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boldsymbol{q}^{\mathrm{sqz}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boldsymbol{\xi}^{\mathrm{s}}$$

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

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

$$RM^A = \mathbf{0}$$

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

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

For each A, find R s.t

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

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

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

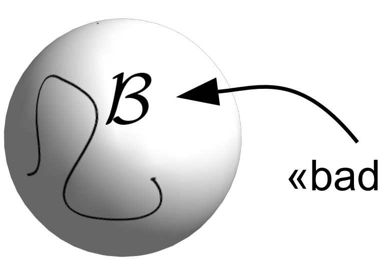
For each *A*, find *R* s.t

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

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

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

$$U(n) \simeq \mathrm{Sp}(2n, \mathbb{R}) \cap O(2n)$$



«bad» matrices

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

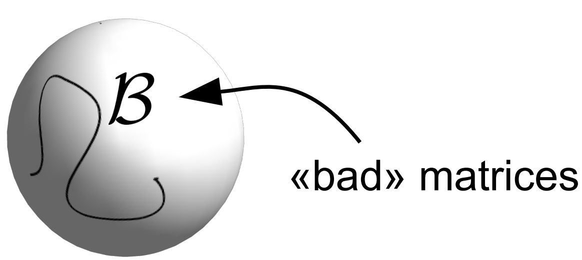
For each *A*, find *R* s.t

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

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

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

$$U(n) \simeq \mathrm{Sp}(2n, \mathbb{R}) \cap O(2n)$$



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

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

Or construct a **unitary Gaussian** decoding

Reconstruction by authorized sets

Coherent state secret:

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

Depend on S_L

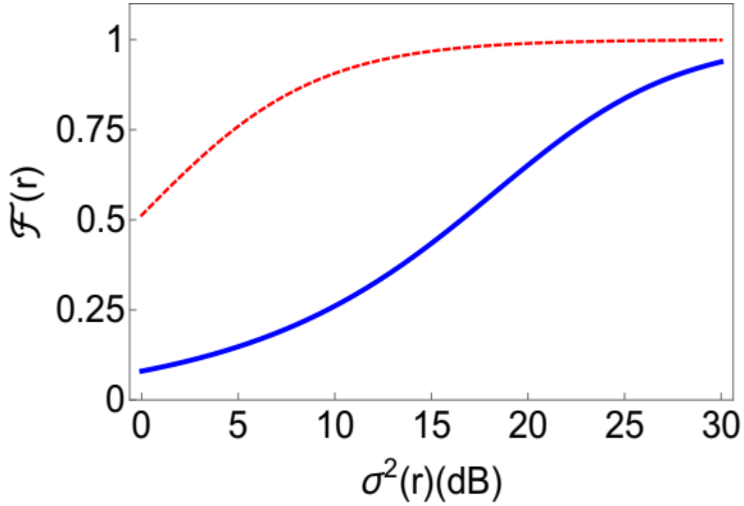
Reconstruction by authorized sets

Coherent state secret:

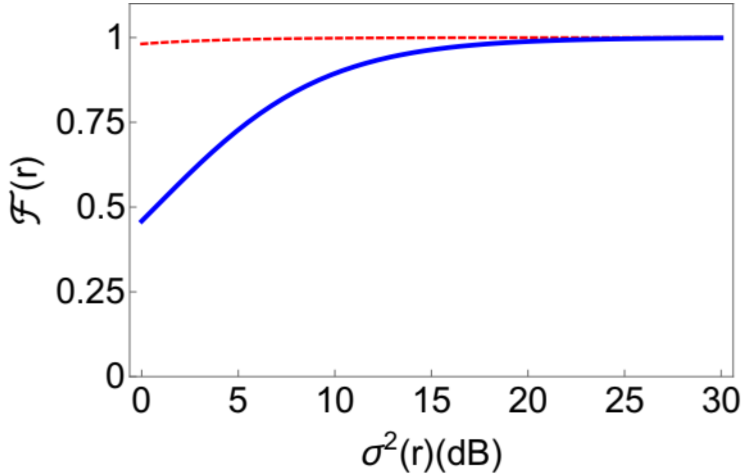
$$\mathcal{F}^{A}(r) = 1/\sqrt{1 + \sigma^2(r)\eta + \sigma^4(r)\zeta}$$

Depend on S_L

Random



Best of 1k



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

Reconstruction by authorized sets

Coherent state secret:

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

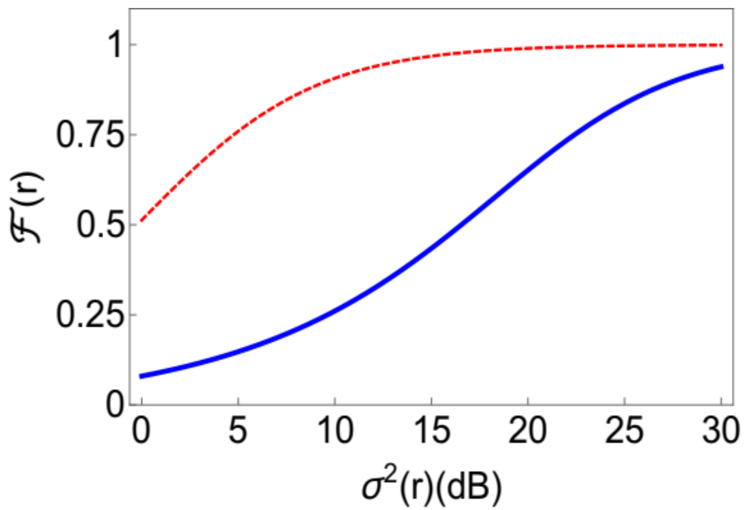
Depend on S_L

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

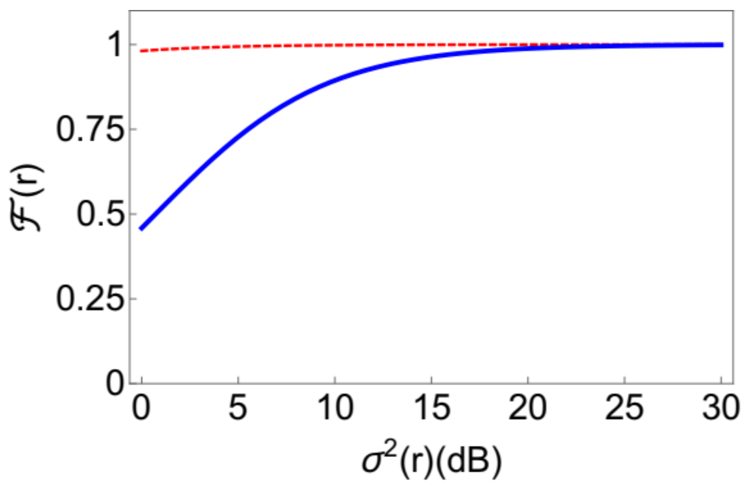
→ eigenvalues of $\mathcal{N} = B\Delta^2 B^T$

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

Random



Best of 1k



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

Reconstruction by authorized sets

Coherent state secret:

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

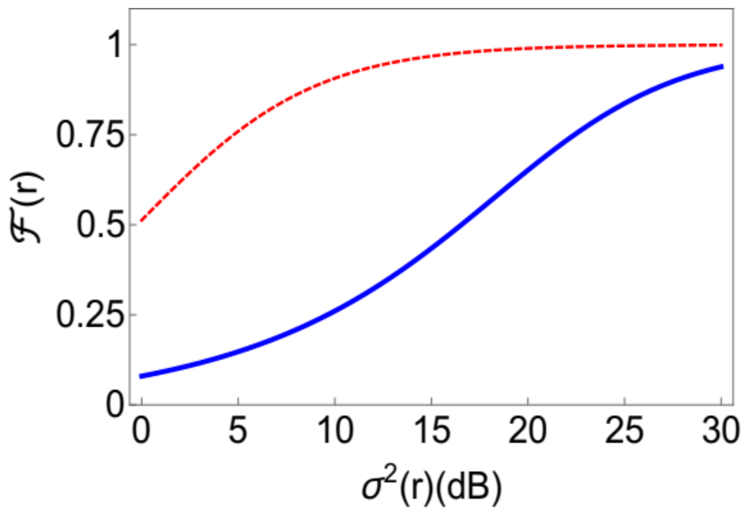
Depend on S_L

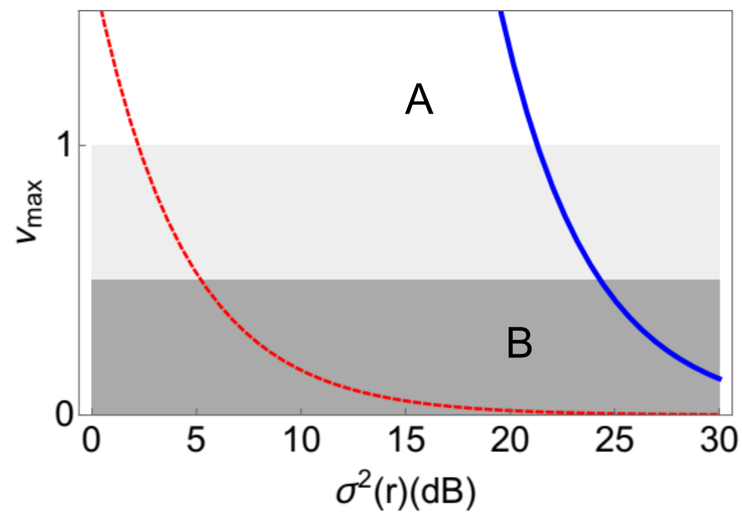
Any state: $W_{\text{out}}(\boldsymbol{\xi}) = \int \left(\prod_{j=1}^{n} \mathrm{d}y_j \frac{e^{-\frac{y_j^2}{2\sigma_j^2}}}{\sigma_j\sqrt{2\pi}} \right) W_{\text{in}}(\boldsymbol{\xi} - B\boldsymbol{y})$

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

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

Random

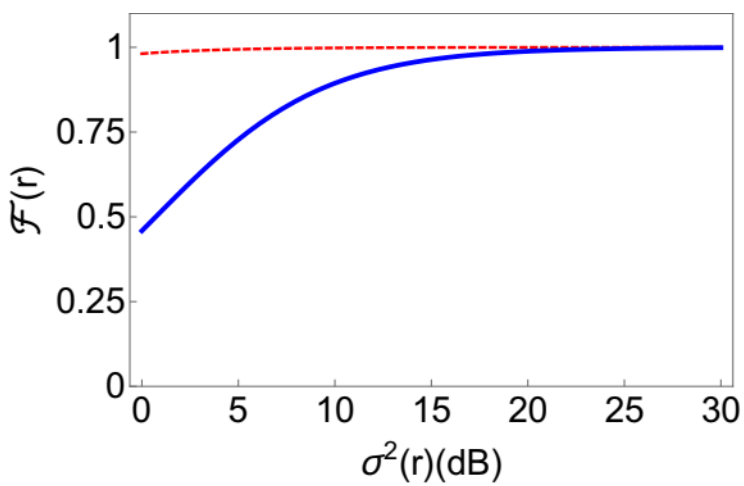


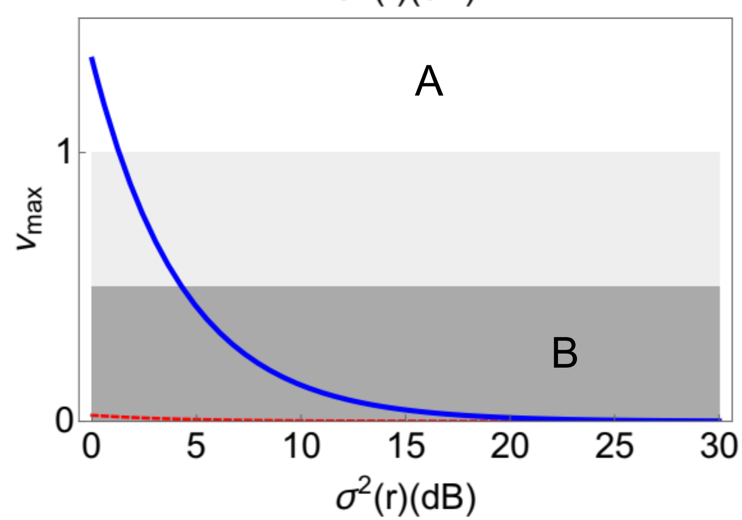


A) Entanglement breaking

B) Best copy

Best of 1k





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

Unauthorized subsets

- Finite squeezing:
  some information always leaked to adversaries

Unauthorized subsets

- Finite squeezing:
  some information always leaked to adversaries
- **Mutual information** can be bounded *Habibidavijani & Sanders arXiv:1904.09506 (2019)*

Unauthorized subsets

- 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)

Unauthorized subsets

- 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

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?

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?

Thank you!

Decoding conditions

$$\begin{pmatrix} q_j^{\text{sqz}} \\ p_j^{\text{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\text{sqz}}} + N^A \boldsymbol{p}^{\text{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\text{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

For each A, find R s.t

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

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

$$\det\left(RH^A\right) = 0$$ $\rightarrow$ polynomial equations for coefficients of S_L

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

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

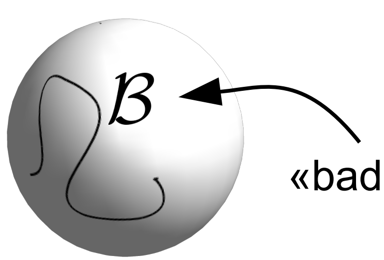
$$RM^A = \mathbf{0} \Leftarrow k \geq m + \lceil \frac{n}{2} \rceil$$

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

$\det\left(RH^A\right) = 0$ → polynomial equations for coefficients of S_L

→ zeros («bad» matrices) are lower dimensional sets of *U(n)*

$$U(n) \simeq \mathrm{Sp}(2n, \mathbb{R}) \cap O(2n)$$



«bad» matrices

Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

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

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

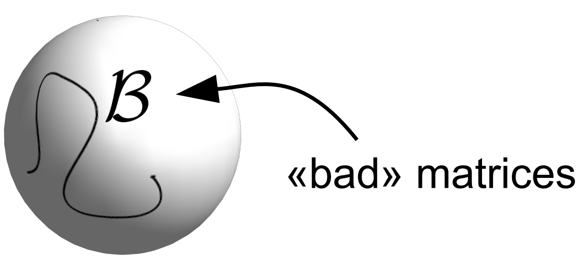
$$\det\left(RH^A\right) \neq 0$$

$\det\left(RH^A\right) = 0$ → polynomial equations for coefficients of S_L

→ zeros («bad» matrices) are lower dimensional sets of *U(n)*

→ Zero Haar (constant) measure

$$U(n) \simeq \mathrm{Sp}(2n, \mathbb{R}) \cap O(2n)$$



Decoding conditions

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix}$$

$$\boldsymbol{\xi}^A = M^A \boxed{\boldsymbol{q}^{\mathrm{sqz}}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boxed{\boldsymbol{\xi}^{\mathrm{s}}}$$

Goal: 1) Get rid of <u>these</u>

2) solve for <u>these</u>

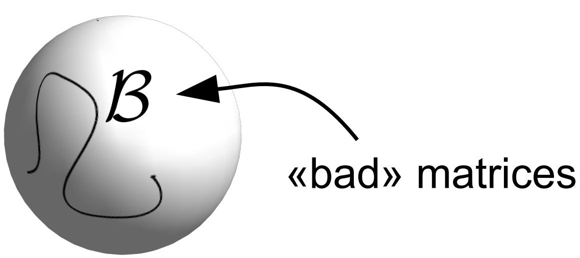
For each *A*, find *R* s.t

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

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

$\det\left(RH^A\right) = 0$ → polynomial equations for coefficients of S_L
→ zeros («bad» matrices) are lower dimensional sets of *U(n)*
→ Zero Haar (constant) measure

$$U(n) \simeq \mathrm{Sp}\left(2n, \mathbb{R}\right) \cap O\left(2n\right)$$



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

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

Or construct a **unitary Gaussian** decoding