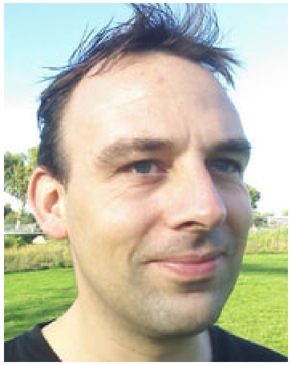
Quantum Secret Sharing with Squeezing and Almost Any Passive Interferometer

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 no single player is able to retrieve the information alone

Secret Sharing

A **dealer** shares a **secret** with several **players** in such a way that no single player is able to retrieve the information alone

$$
\begin{aligned}
a &= 11111 \\
& \quad \oplus \\
b &= 10011 \\
\text{(random)} & \quad = \\
c &= 01100
\end{aligned}
$$

Secret Sharing

A **dealer** shares a **secret** with several **players** in such a way that no single player is able to retrieve the information alone

$$a = 11111$$
$$\oplus$$
$$b = 10011$$
(random)
$$=$$
$$c = 01100$$

$\oplus \rightarrow a$

- **Access parties**: Groups that can retrieve the secret
- **Adversary structure**: Groups that should not get information
- **Quantum** Secret Sharing: secret encoded in a quantum state

Several paradigms

CC: Classical information shared using classical resources

CQ: Classical information shared using quantum resources

→ Improved security

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)

Continuous Variables

Discrete and Continuous variables

DV : information encoded in *d*-level systems (typically *d* = 2)

$$\alpha\left|0\right\rangle + \beta\left|1\right\rangle$$

$$\Pr\left(0\right) = \left|\alpha\right|^2$$

$$\left|\alpha\right|^2 + \left|\beta\right|^2 = 1$$

$$\mathcal{H} = \mathbb{C}^2$$

Discrete and Continuous variables

DV : information encoded in *d*-level systems (typically *d* = 2)

$$\alpha\,|0\rangle + \beta\,|1\rangle$$

$$\Pr(0) = |\alpha|^2$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$\mathcal{H} = \mathbb{C}^2$$

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

$$\int_{\mathbb{R}} \psi(x)\,|x\rangle_q\,\mathrm{d}x$$

$$\Pr\left(q \in [x, x + \mathrm{d}x]\right) = |\psi(x)|^2\,\mathrm{d}x$$

$$\int_{\mathbb{R}} |\psi(x)|^2\,\mathrm{d}x = 1$$

$$\mathcal{H} = \mathcal{L}^2(\mathbb{R}, \mathbb{C})$$

Discrete and Continuous variables

DV : information encoded in *d*-level systems (typically *d* = 2)

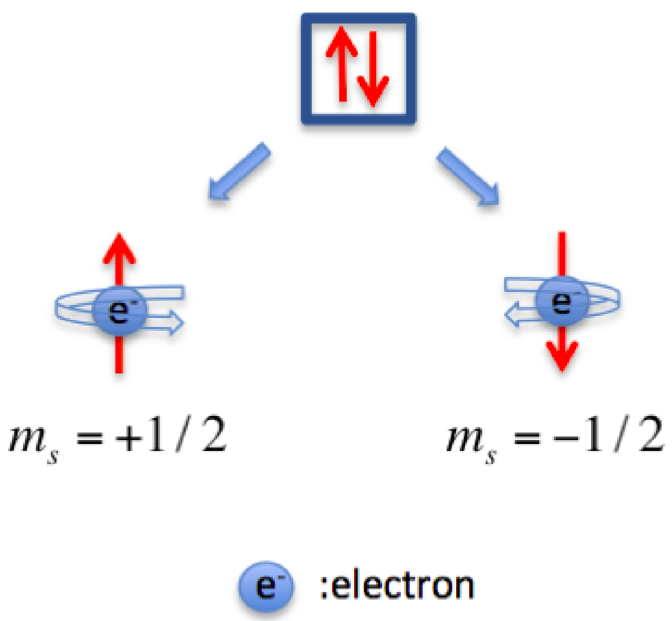
$$\alpha\,|0\rangle + \beta\,|1\rangle$$

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

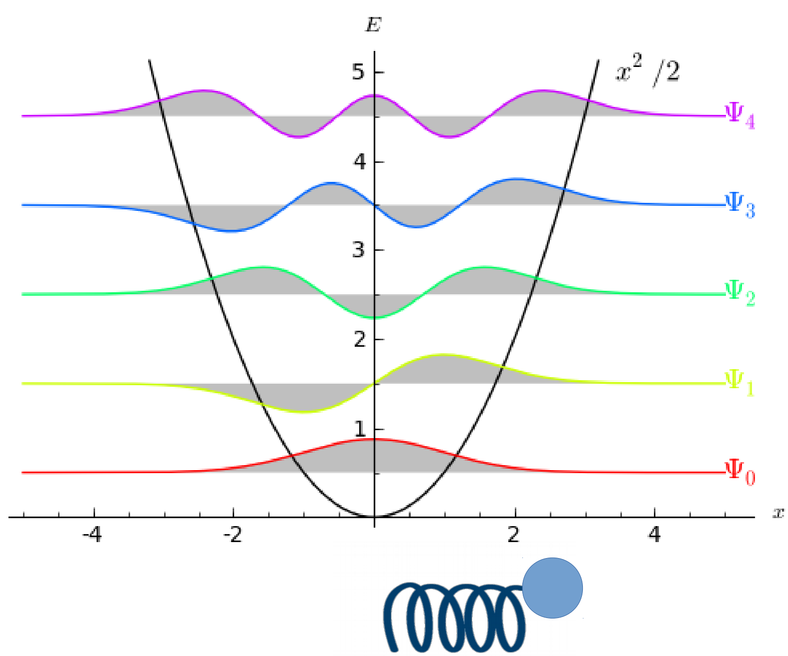
$$\int_{\mathbb{R}} \psi(x)\,|x\rangle_q\,\mathrm{d}x$$

Examples

DV : spins



CV : Harmonic oscillator



Discrete and Continuous variables

DV : information encoded in d-level systems (typically *d* = 2)

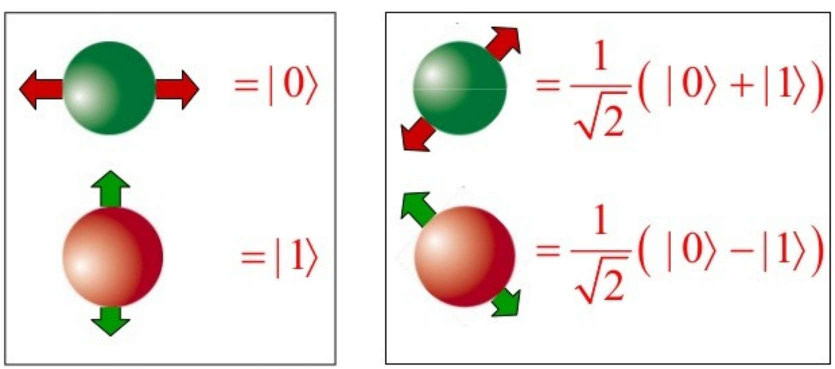
$$\alpha\,|0\rangle + \beta\,|1\rangle$$

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

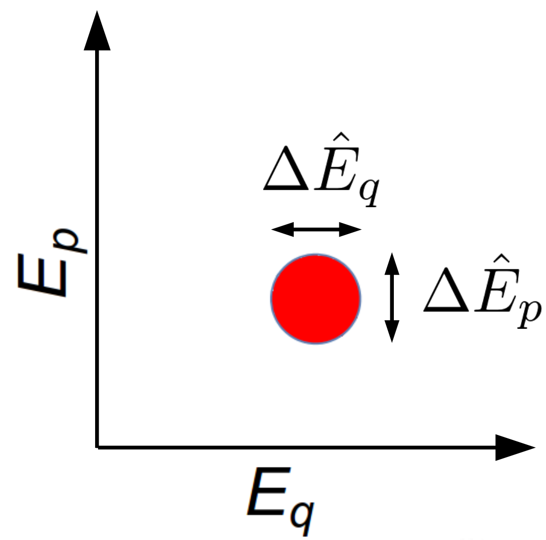
$$\int_{\mathbb{R}} \psi(x)\,|x\rangle_q\,\mathrm{d}x$$

In quantum optics

DV : polarization of single photon



CV : quadratures of the field



$$\hat{E}_q \propto \hat{a} + \hat{a}^\dagger$$
$$\hat{E}_p \propto \hat{a} - \hat{a}^\dagger$$
$$\left[\hat{E}_q, \hat{E}_p\right] = [\hat{q}, \hat{p}]$$

Often simply $\hat{q}$, $\hat{p}$ in the following

Wigner function, Gaussian states & Transformations

CV states can be visualized with a phase-space representation

(Also a useful mathematical tool!)

Wigner function, Gaussian states & Transformations

CV states can be visualized with a phase-space representation

(Also a useful mathematical tool!)

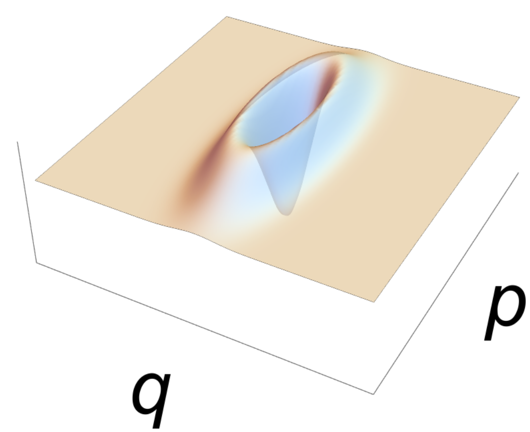
Wigner function ~ Distribution in phase space

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

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

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

May be negative!



Wigner function, Gaussian states & Transformations

CV states can be visualized with a phase-space representation

(Also a useful mathematical tool!)

Wigner function ~ Distribution in phase space

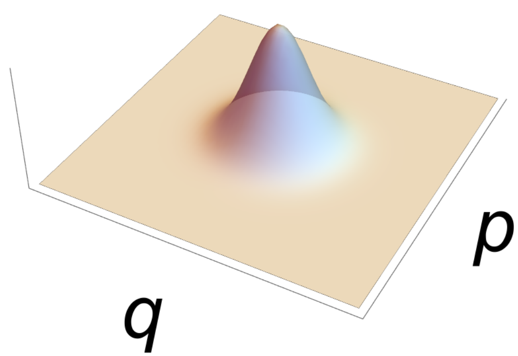
$$|\psi\rangle \longrightarrow W_\psi(q,p)$$

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

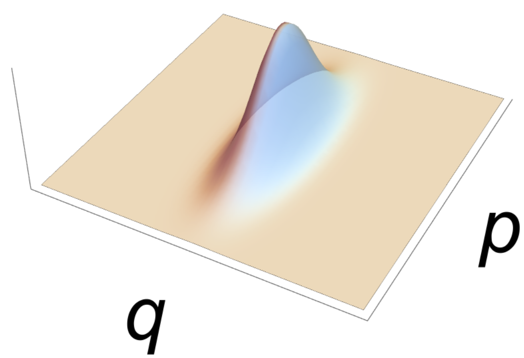
$$\int \mathrm{d}q\, W(q,p) = |\langle p|\psi\rangle|^2$$

Gaussian states:

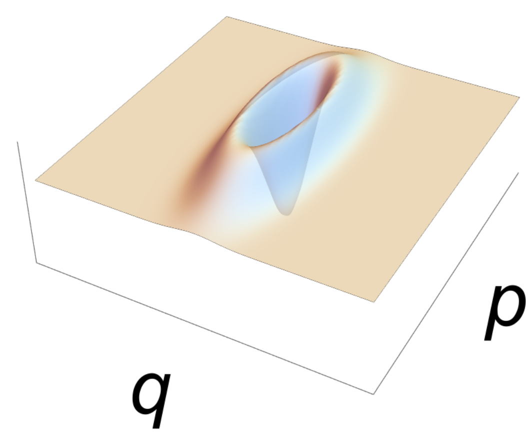
May be negative!



Vacuum → Same marginals



Squeezing



Wigner function, Gaussian states & Transformations

CV states can be visualized with a phase-space representation

(Also a useful mathematical tool!)

Wigner function ~ Distribution in phase space

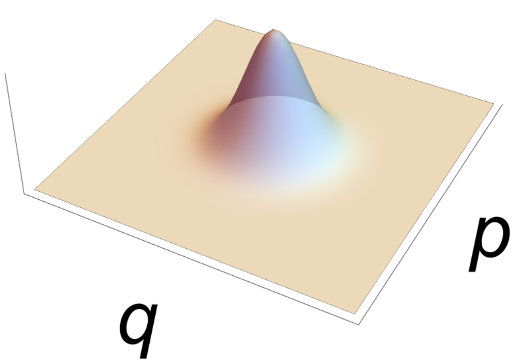
$$|\psi\rangle \longrightarrow W_\psi(q,p)$$

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

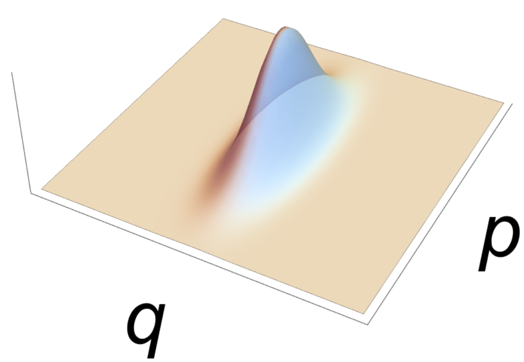
$$\int \mathrm{d}q\, W(q,p) = |\langle p|\psi\rangle|^2$$

Gaussian states:

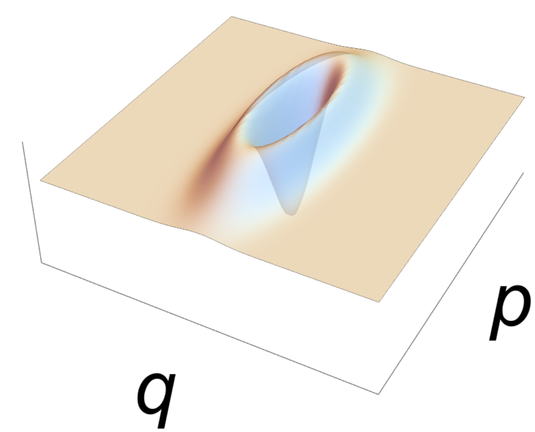
May be negative!



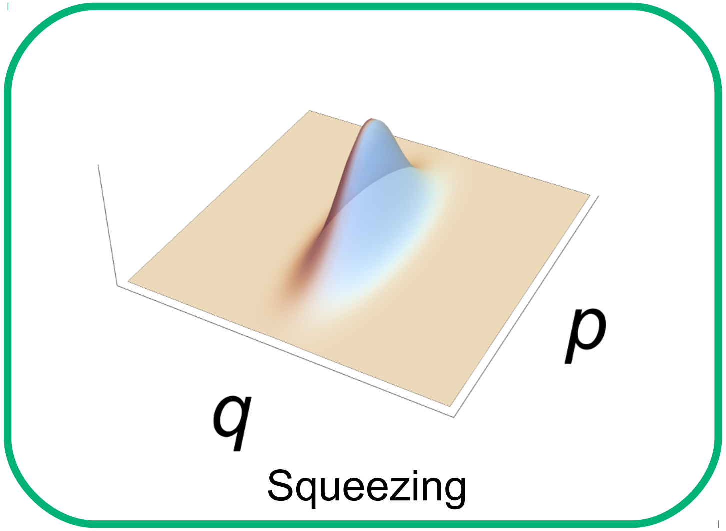
Vacuum → Same marginals



Squeezing



Squeezed states

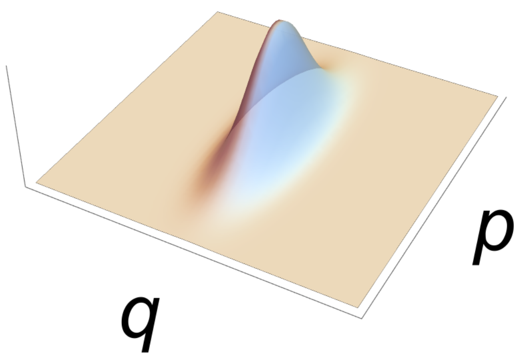


Reduced fluctuations in q or p

$\Downarrow$

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

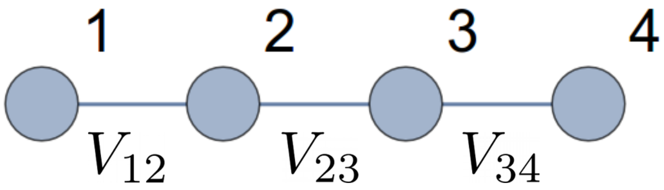
Workhorse of CV Quantum information:

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

Cluster states

$$\exp\left(i\sum_{i>j} V_{ij}\hat{q}_i \otimes \hat{q}_j\right)|0\rangle_p^{\otimes N}$$

- Can be represented as graphs
- Characterized by **nullifier operators**
- Approximated by Gaussian states

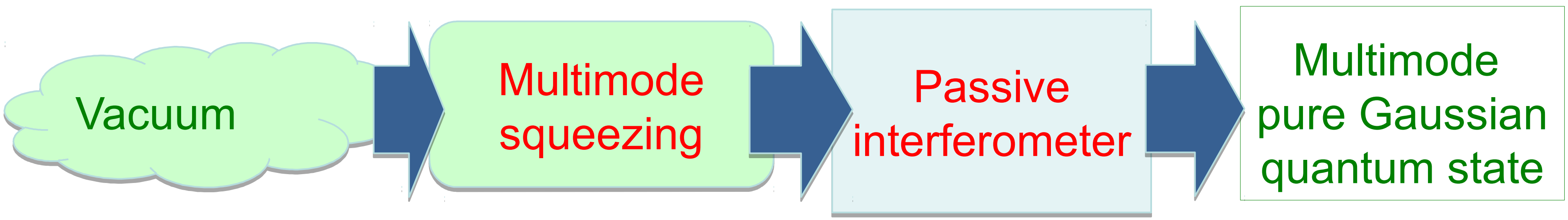


$$\begin{aligned}
\hat{\delta}_1 &= \hat{p}_1 - \hat{q}_2 \\
\hat{\delta}_2 &= \hat{p}_2 - \hat{q}_1 - \hat{q}_3 \\
\hat{\delta}_3 &= \hat{p}_3 - \hat{q}_2 - \hat{q}_4 \\
\hat{\delta}_4 &= \hat{p}_4 - \hat{q}_3
\end{aligned}$$

Producing Gaussian cluster states

For pure Gaussian states (Quantum Optics):

S. Braunstein,
PRA 71, 055801 (2005)



These operations are **deterministic**!

(No post-selection)

Finite Sqz → Non-zero Q fluctuations → Logical errors

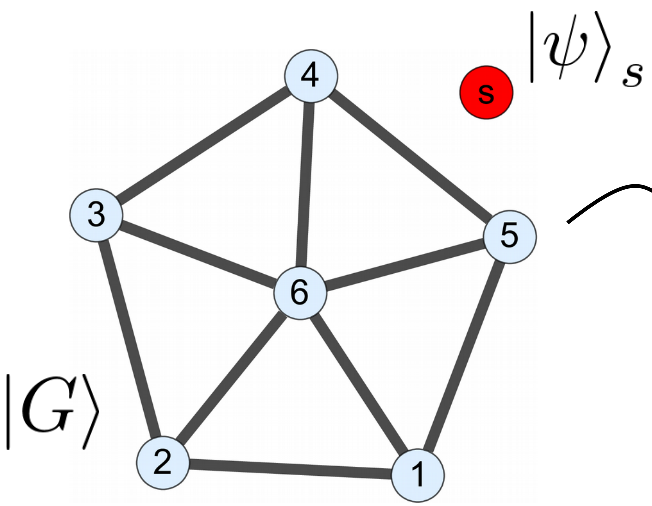
(CV) Quantum secret sharing

FA, G. Ferrini, F. Grosshans, D. Markham, arXiv:1808.06870

A quantum *(3,5)* scheme with Cluster States

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

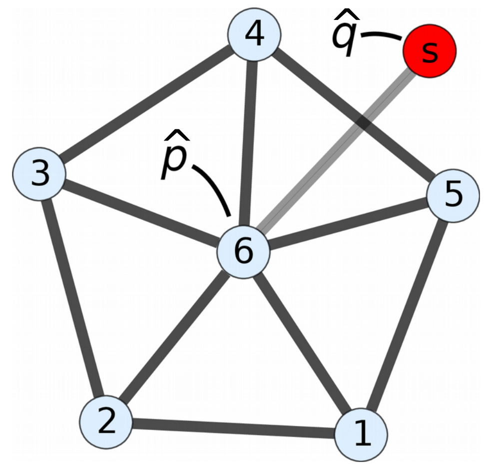
Start



$$\hat{\delta}_j \, |G\rangle = 0 \;\forall j$$

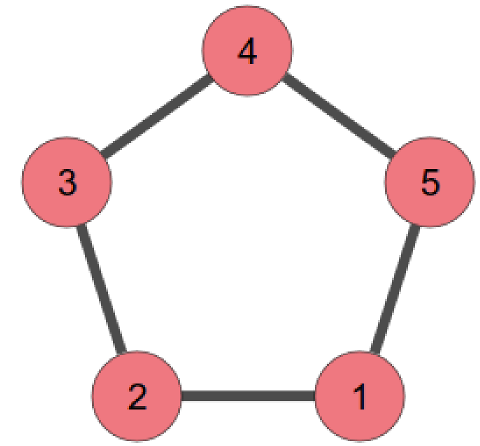
$$|\psi\rangle_s = \int \mathrm{d}y \;\psi(y)\,|y\rangle_{q_s}$$

Teleportation



CV Bell Measurement

Secret is encoded



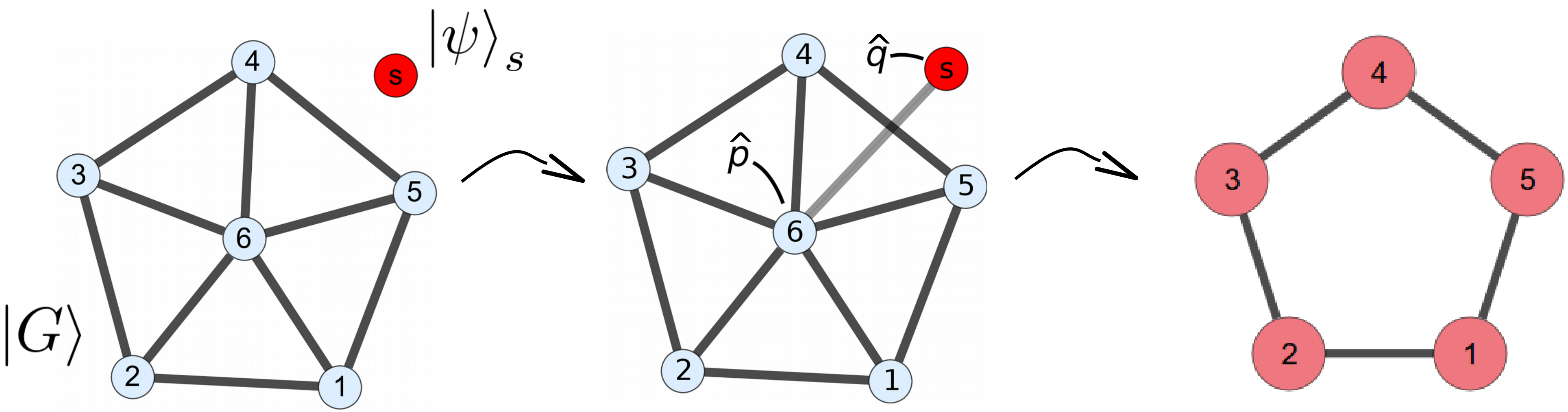
$$\int \mathrm{d}x \;\psi(x)\,|G(x)\rangle$$

$$\hat{\delta}_j \, |G(x)\rangle = x\,|G(x)\rangle \;\;\forall j$$

A quantum *(3,5)* scheme with Cluster States

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

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



$$\hat{\delta}_j\,|G\rangle = 0 \;\forall j$$

$$|\psi\rangle_s = \int \mathrm{d}y\;\psi(y)\,|y\rangle_{q_s}$$

CV Bell Measurement

$$\int \mathrm{d}x\;\psi(x)\,|G(x)\rangle$$

$$\hat{\delta}_j\,|G(x)\rangle = x\,|G(x)\rangle \;\;\forall j$$

<u>Logical operators</u>

$$\hat{q}_L = \hat{\delta}_j$$

$$\hat{p}_L = \hat{q}_1 + \hat{q}_2 + \hat{q}_3 + \hat{q}_4 + \hat{q}_5$$

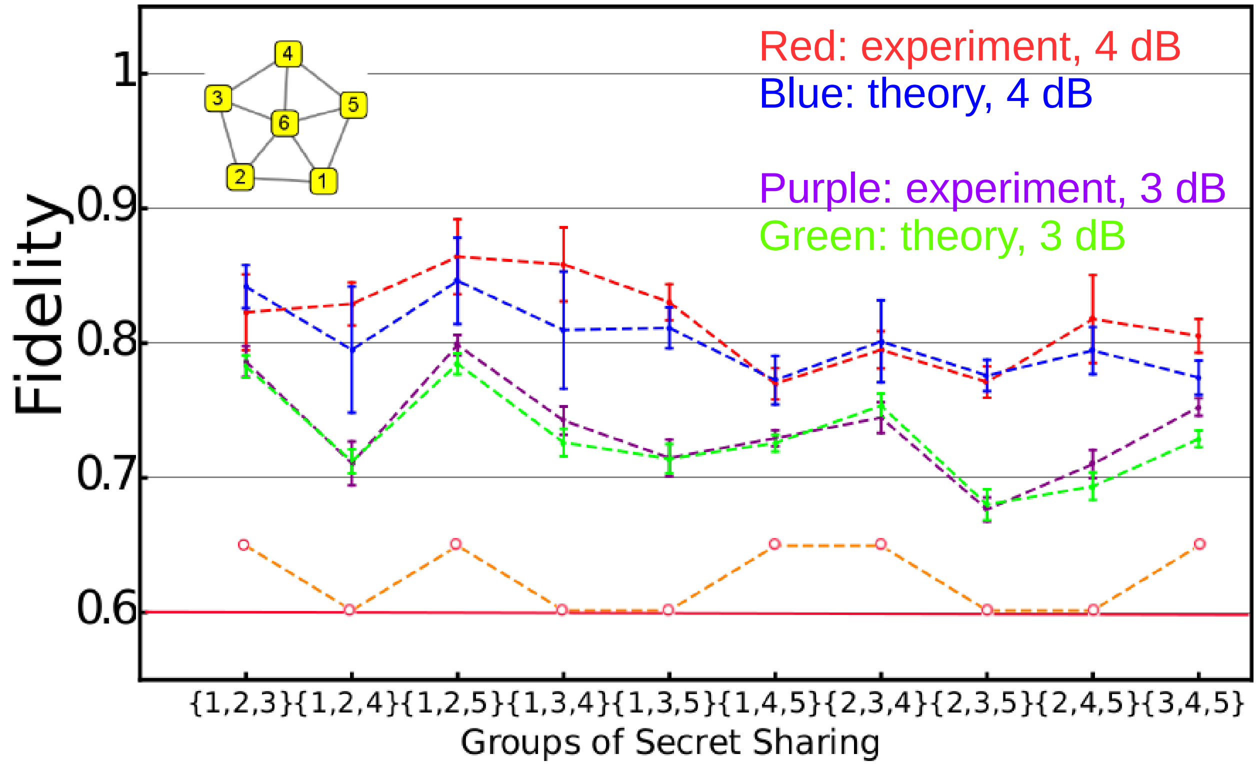
- Same statistics on encoded state as *q*, *p* on secret state
- Can be measured locally by any access party

“Theory inspired” experiment

Y. Cai et al, Nat. Comm. 8, 15645 (2017)

Squeezed states: supermodes

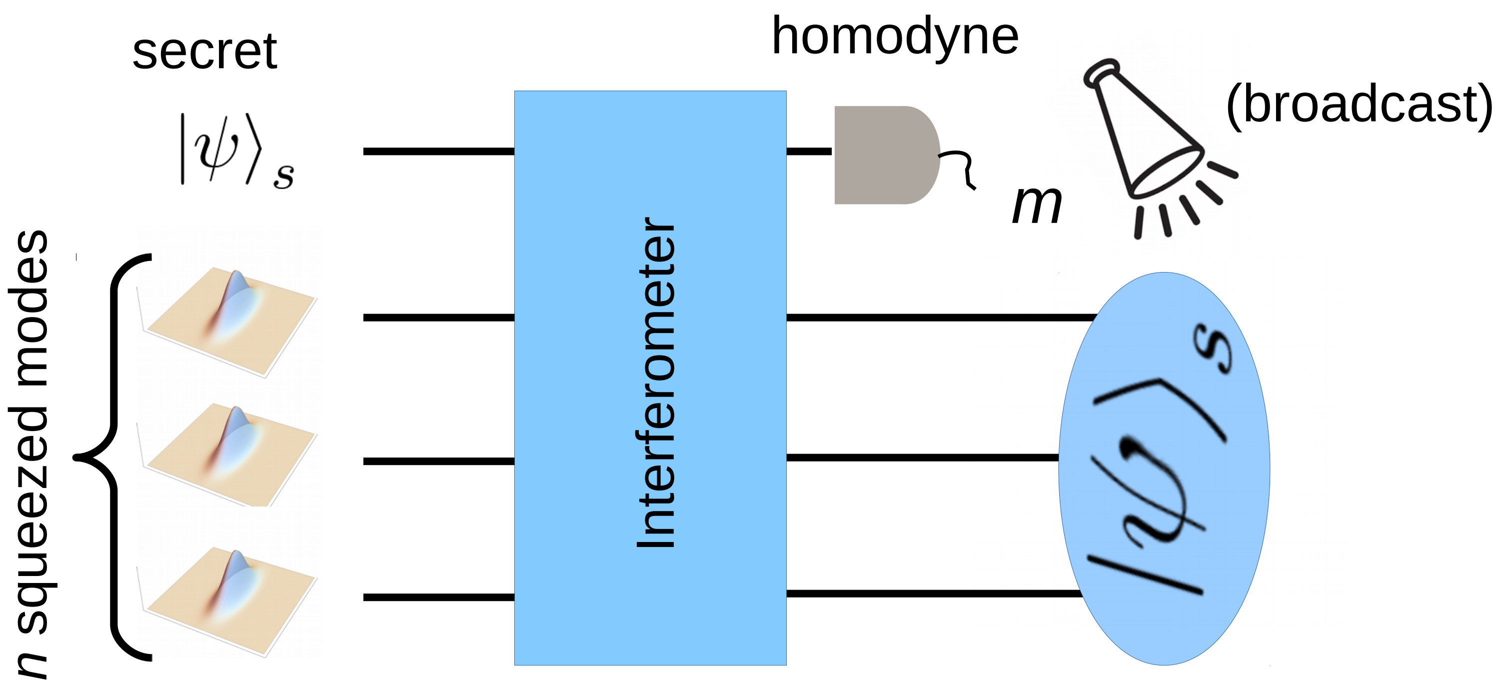
Linear optics → Change of mode basis
(Linear combinations of supermodes)



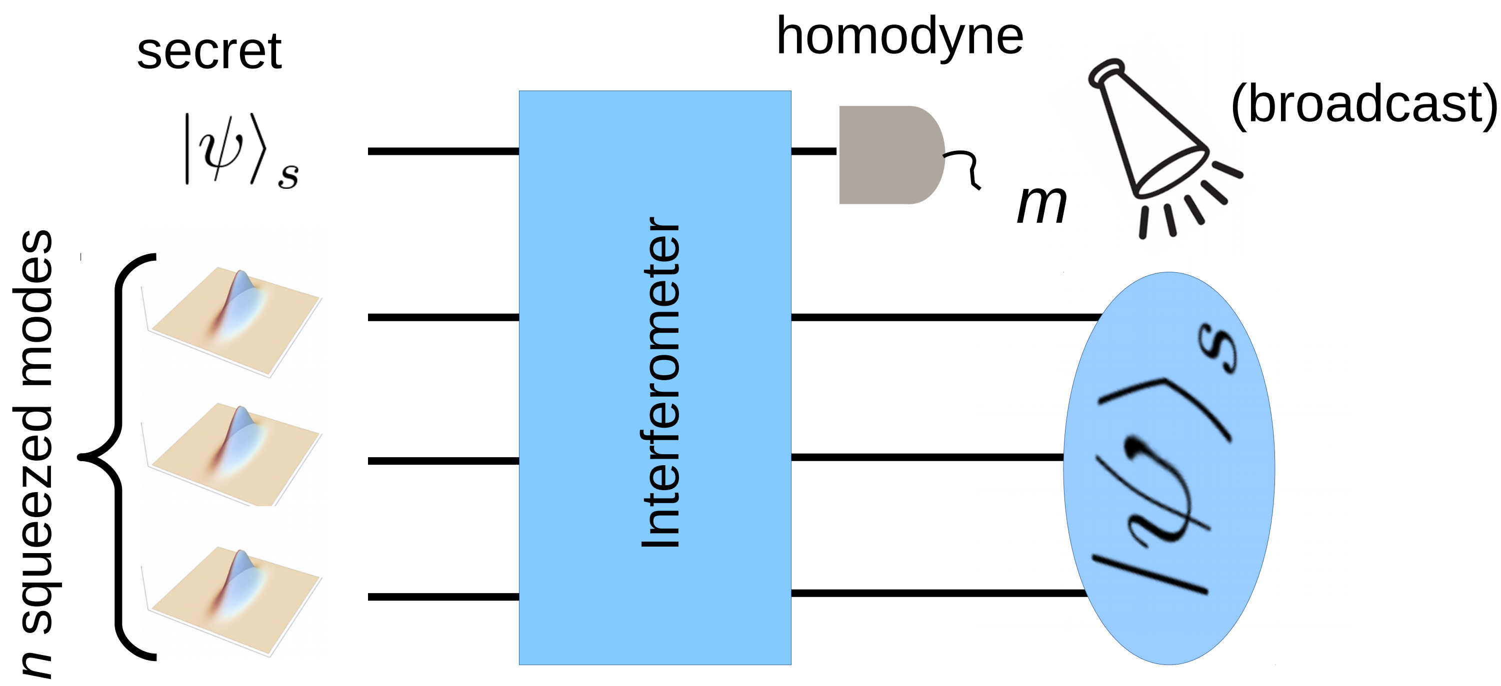
Fidelity above classical bound

The protocol was *simulated*:
modes are not really separated, only gives an estimate of the excess noise

A general CV threshold scheme



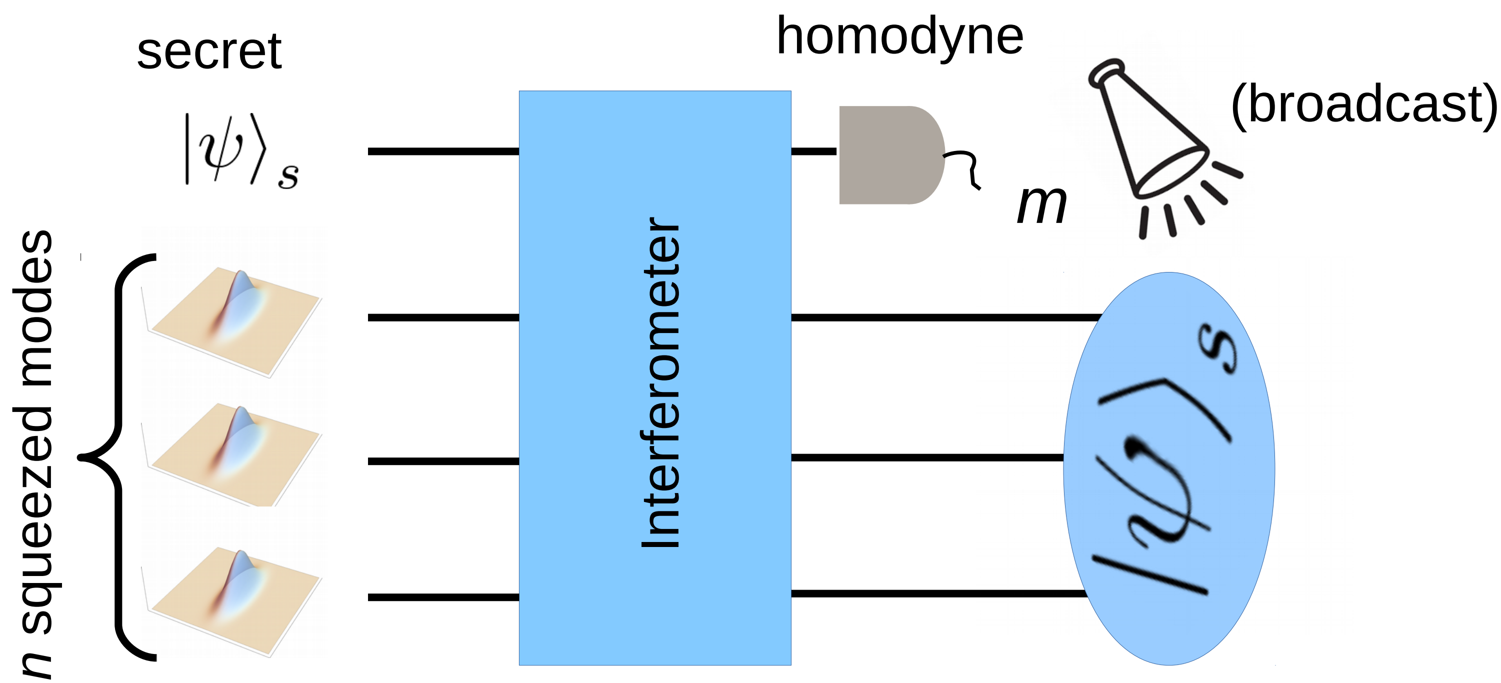
A general scheme



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

- Measure secret quadratures
- Physically reconstruct the secret

A general scheme



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

- Measure secret quadratures
- Physically reconstruct the secret

Almost all passive interferometers can be used for Quantum Secret Sharing with squeezed states

(In the sense of Haar measure)

Derivation

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

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

Phase-space deformation

Phase-space translation

Symplectic Group

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

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

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

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

Phase-space deformation

Phase-space translation

Symplectic Group

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

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

Squeezing:

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

Linear optics (passive **interferometers**):

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

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

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

Phase-space deformation

Phase-space translation

Symplectic Group

$$[\xi_j', \xi_k'] = iJ_{jk} \iff S^T J S = J$$

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

Bloch-Messiah:

$$S = R_1 K R_2$$

Squeezing:

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

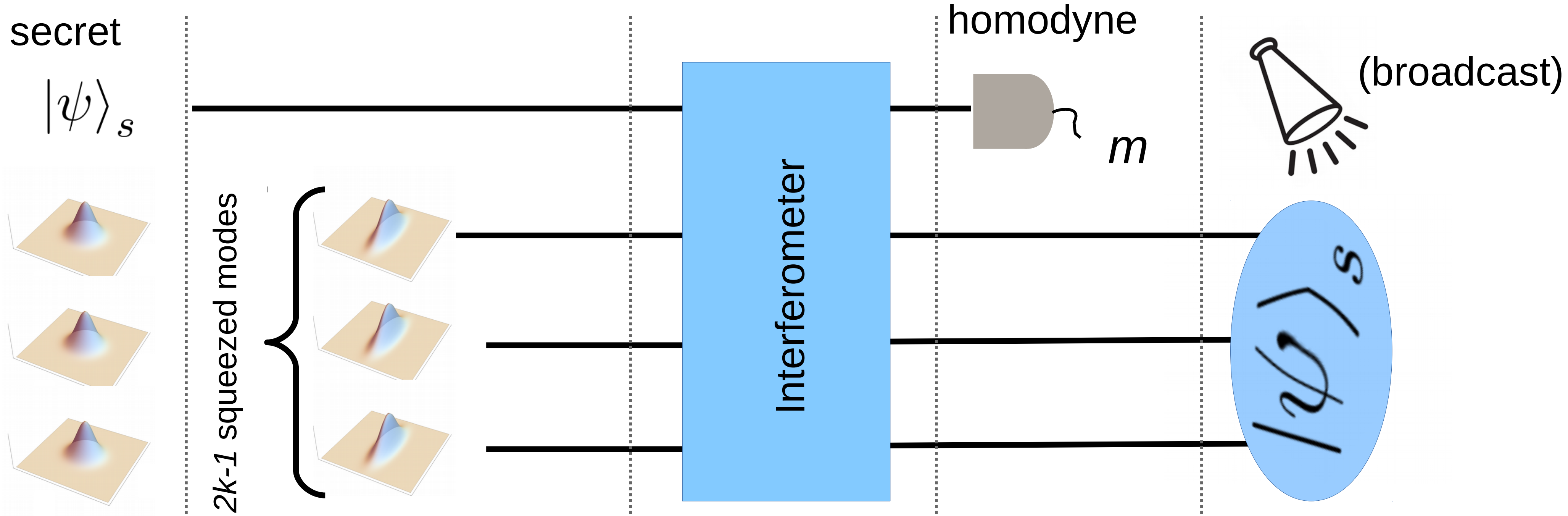
Linear optics (passive **interferometers**):

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

Gaussian **CPTP**:
(Stinespring)

Gaussian unitary with
Gaussian ancillae
+
Partial trace

The scheme revisited



$$\begin{pmatrix} q^s \\ \boldsymbol{q}^{(0)} \\ p^s \\ \boldsymbol{p}^{(0)} \end{pmatrix} \qquad \boldsymbol{\xi}^{\mathrm{sqz}} = \begin{pmatrix} q^s \\ \boldsymbol{q}^{\mathrm{sqz}} \\ p^s \\ \boldsymbol{p}^{\mathrm{sqz}} \end{pmatrix} \qquad \begin{pmatrix} q^d \\ \boldsymbol{q}^{\mathrm{net}} \\ p^d \\ \boldsymbol{p}^{\mathrm{net}} \end{pmatrix} = R\boldsymbol{\xi}^{\mathrm{sqz}} \qquad p^d \mapsto m$$

$$\begin{pmatrix} q_j^{\mathrm{sqz}} \\ p_j^{\mathrm{sqz}} \end{pmatrix} = \begin{pmatrix} e^{r_j} q_j^{(0)} \\ e^{-r_j} p_j^{(0)} \end{pmatrix} \qquad R = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix}$$

Encoding procedure

Each player has 2: $$\xi_j^{\text{net}} = \sum_l M_{jl} q_l^{\text{sqz}} + \sum_l N_{jl} p_l^{\text{sqz}} + \alpha_j p^s + \beta_j q^s$$

Encoding procedure

Each player has 2: $$\xi_j^{\text{net}} = \overset{\text{noise}}{\boxed{\sum_l M_{jl} q_l^{\text{sqz}} + \sum_l N_{jl} p_l^{\text{sqz}}}} + \alpha_j p^s + \beta_j q^s$$

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

Encoding procedure

noise

Each player has 2: $\xi_j^{\text{net}} = \boxed{\sum_l M_{jl} q_l^{\text{sqz}} + \sum_l N_{jl} p_l^{\text{sqz}}} + \alpha_j p^s + \beta_j q^s$

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

Goal: Get rid of these!

Encoding procedure

noise

Each player has 2: $$\xi_j^{\mathrm{net}} = \boxed{\sum_l M_{jl} q_l^{\mathrm{sqz}} + \sum_l N_{jl} p_l^{\mathrm{sqz}}} + \alpha_j p^s + \beta_j q^s$$

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

Goal: Get rid of <u>these</u>!

After measurement:

$$p^{\mathrm{d}} \mapsto m = \sum_{l=1}^{2k-1} Y_{2k,l} q_l^{\mathrm{sqz}} + \sum_{l=1}^{2k-1} X_{2k,l} p_l^{\mathrm{sqz}} + Y_{2k,2k} q_{\mathrm{s}} + X_{2k,2k} p_{\mathrm{s}}$$

Each player eliminates one

Encoding procedure

noise

Each player has 2: $\xi_j^{\text{net}} = \boxed{\sum_l M_{jl} q_l^{\text{sqz}} + \sum_l N_{jl} p_l^{\text{sqz}}} + \alpha_j p^s + \beta_j q^s$

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

Goal: Get rid of these!

After measurement:

$$p^{\text{d}} \mapsto m = \sum_{l=1}^{2k-1} Y_{2k,l} q_l^{\text{sqz}} + \sum_{l=1}^{2k-1} X_{2k,l} p_l^{\text{sqz}} + Y_{2k,2k} q_{\text{s}} + X_{2k,2k} p_{\text{s}}$$

Each player eliminates one

Set of *k* players ***A*** (access party)

$$2k \Big[\ \boldsymbol{\xi}^A = M^A \bar{\boldsymbol{q}}^{\text{sqz}} + N^A \boldsymbol{p}^{\text{sqz}} + \boldsymbol{h}_q^A q^s + \boldsymbol{h}_p^A p^s + \boldsymbol{h}_{\text{d}}^A m$$

Encoding procedure

Each player has 2:

$$\xi_j^{\text{net}} = \overbrace{\sum_l M_{jl} q_l^{\text{sqz}} + \sum_l N_{jl} p_l^{\text{sqz}}}^{\text{noise}} + \alpha_j p^s + \beta_j q^s$$

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

Goal: Get rid of <u>these</u>!

After measurement:

$$p^{\text{d}} \mapsto m = \sum_{l=1}^{2k-1} Y_{2k,l} q_l^{\text{sqz}} + \sum_{l=1}^{2k-1} X_{2k,l} p_l^{\text{sqz}} + Y_{2k,2k} q_{\text{s}} + X_{2k,2k} p_{\text{s}}$$

Each player eliminates one

Set of *k* players ***A*** (access party)

2k

$$\boldsymbol{\xi}^A = M^A \bar{\boldsymbol{q}}^{\text{sqz}} + N^A \boldsymbol{p}^{\text{sqz}} + \boldsymbol{h}_q^A q^s + \boldsymbol{h}_p^A p^s + \cancel{\boldsymbol{h}_{\text{d}}^A m}$$

Correct

Encoding procedure

Each player has 2: $$\xi_j^{\text{net}} = \overbrace{\sum_l M_{jl} q_l^{\text{sqz}} + \sum_l N_{jl} p_l^{\text{sqz}}}^{\text{noise}} + \alpha_j p^s + \beta_j q^s$$

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

Goal: Get rid of <u>these</u>!

After measurement:

$$p^{\text{d}} \mapsto m = \sum_{l=1}^{2k-1} Y_{2k,l} q_l^{\text{sqz}} + \sum_{l=1}^{2k-1} X_{2k,l} p_l^{\text{sqz}} + Y_{2k,2k} q_{\text{s}} + X_{2k,2k} p_{\text{s}}$$

Each player eliminates one

Set of *k* players ***A*** (access party)

$$\underbrace{\boldsymbol{\xi}^A}_{2k} = \underbrace{M^A}_{2k-2} \bar{\boldsymbol{q}}^{\text{sqz}} + N^A \boldsymbol{p}^{\text{sqz}} + \boldsymbol{h}_q^A q^s + \boldsymbol{h}_p^A p^s + \cancel{\boldsymbol{h}_{\text{d}}^A m}$$

Correct

$$\exists R | R M^A = 0 \longrightarrow R\boldsymbol{\xi}^A = R N^A \boldsymbol{p}^{\text{sqz}} + T^A \begin{pmatrix} q^s \\ p^s \end{pmatrix}$$

Encoding procedure

Each player has 2: $$\xi_j^{\mathrm{net}} = \overbrace{\sum_l M_{jl} q_l^{\mathrm{sqz}} + \sum_l N_{jl} p_l^{\mathrm{sqz}}}^{\text{noise}} + \alpha_j p^s + \beta_j q^s$$

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

Goal: Get rid of <u>these</u>!

After measurement:

$$p^{\mathrm{d}} \mapsto m = \sum_{l=1}^{2k-1} Y_{2k,l} q_l^{\mathrm{sqz}} + \sum_{l=1}^{2k-1} X_{2k,l} p_l^{\mathrm{sqz}} + Y_{2k,2k} q_{\mathrm{s}} + X_{2k,2k} p_{\mathrm{s}}$$

Each player eliminates one

Set of *k* players ***A*** (access party)

$$2k\ \Big[\ \boldsymbol{\xi}^A = \underbrace{M^A}_{2k-2} \bar{\boldsymbol{q}}^{\mathrm{sqz}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + \boldsymbol{h}_q^A q^s + \boldsymbol{h}_p^A p^s + \cancel{\boldsymbol{h}_{\mathrm{d}}^A m}$$

Correct

$$\exists R | R M^A = 0 \longrightarrow R\boldsymbol{\xi}^A = R N^A \boldsymbol{p}^{\mathrm{sqz}} + T^A \begin{pmatrix} q^s \\ p^s \end{pmatrix}$$

We are done if $\det\left(T^A\right) \neq 0$

Decoding conditions and the Haar measure

$$\begin{cases} Y_{2k,l} \neq 0 \\ \det\left(T^A\right) \neq 0 \end{cases}$$

To eliminate the first anti-squeezed *q*

For (all) ***A*** to retrieve the secret

Decoding conditions and the Haar measure

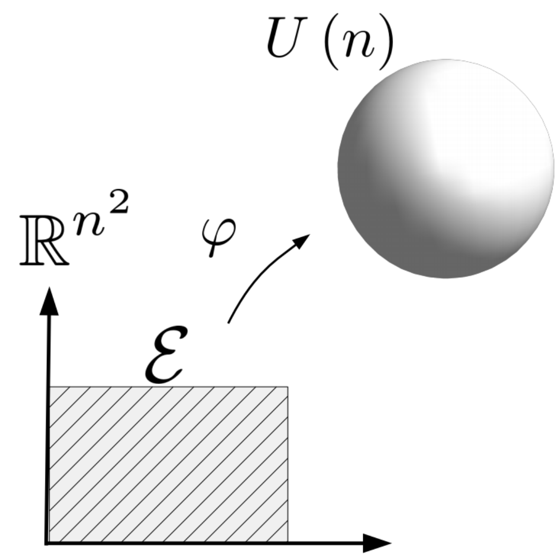
$$\begin{cases} Y_{2k,l} \neq 0 \\ \det\left(T^A\right) \neq 0 \end{cases}$$

To eliminate the first anti-squeezed *q*

For (all) ***A*** to retrieve the secret

Haar measure = uniform probability measure on *U(n)*

Coefficient of unitary matrices = real analytic functions of “angles”



Decoding conditions and the Haar measure

$$\begin{cases} Y_{2k,l} \neq 0 & \text{To eliminate the first anti-squeezed } q \\ \det\left(T^A\right) \neq 0 & \text{For (all) } \boldsymbol{A} \text{ to retrieve the secret} \end{cases}$$

Haar measure = uniform probability measure on *U(n)*

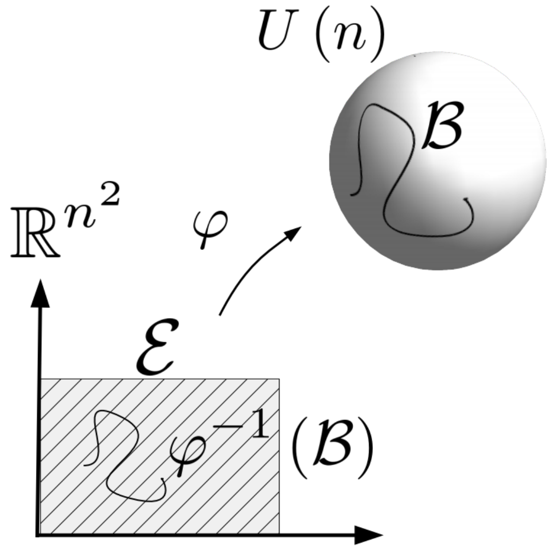
Coefficient of unitary matrices = real analytic functions of “angles”

“**= 0**” in  corresponds to null set of

real analytic functions → zero measure

B. Mityagin, arXiv:1512.07276 (2015)

→ corresponding matrices have zero Haar measure



Decoding conditions and the Haar measure

$$\begin{cases} Y_{2k,l} \neq 0 \\ \det\left(T^{A}\right) \neq 0 \end{cases}$$

To eliminate the first anti-squeezed *q*

For (all) ***A*** to retrieve the secret

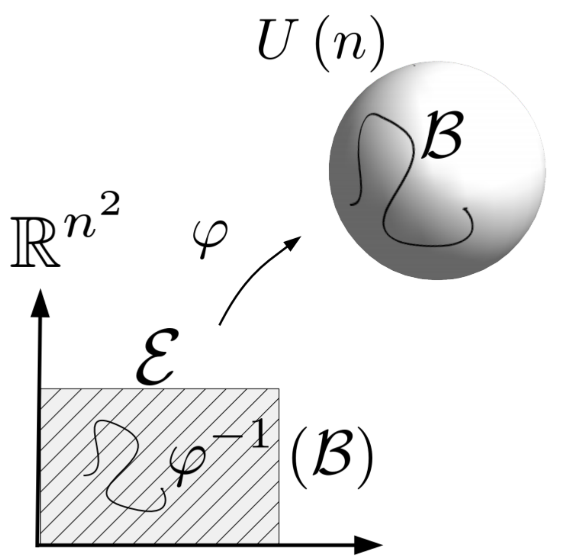
Haar measure = uniform probability measure on *U(n)*

Coefficient of unitary matrices = real analytic functions of “angles”

“**= 0**” in corresponds to null set of real analytic functions → zero measure

→ corresponding matrices have zero Haar measure

B. Mityagin, arXiv:1512.07276 (2015)



If : ***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

Conclusions & Outlook

- A general scheme with Gaussian resources
  → Works for almost any interferometer
- Decoding only requires unitary Gaussian transformations
- Decoding can be computed efficiently for any ***A***
  (May still be hard to compute *for all* ***A***)
- Decoding: only two squeezers / one sqz + HDD / Local HDD
- Easy to show that fidelity → 1 for infinite squeezing
- Easy to generalize to multi-mode secrets

TODO:

- Capacity? (Classical, quantum, private)
- Robust to losses?
- Optimize interferometer?
- Experiments?

Thank you!

Thank you!

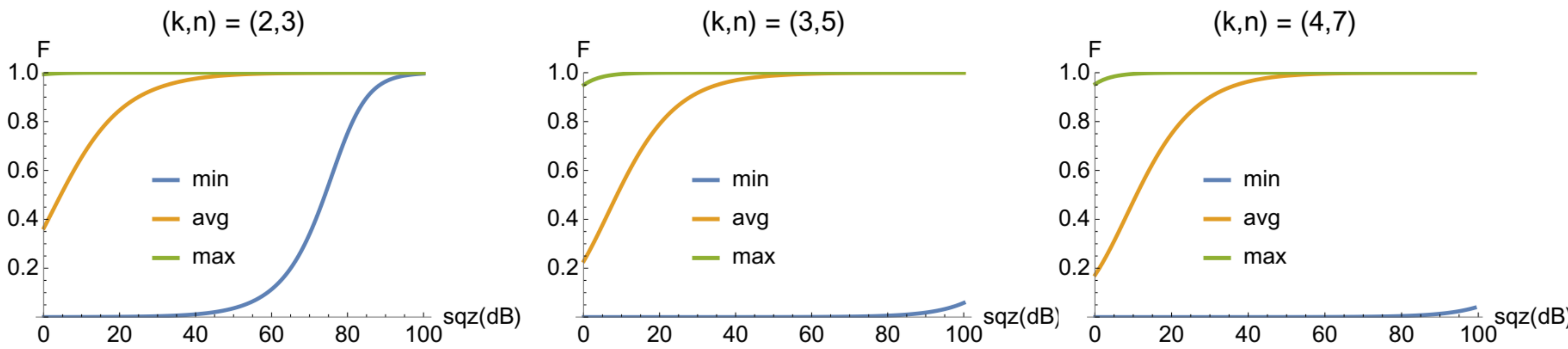
Appendix

Fidelity vs Squeezing (secret = coherent state)

$$\mathcal{F}^{A}\left(r\right) = \left[1 + \sigma^{2}\left(r\right)\eta + \sigma^{4}\left(r\right)\zeta\right]^{-\frac{1}{2}}$$

$$\Delta^{2} p_{j}^{\mathrm{sqz}} = e^{-2r}/2 \equiv \sigma^{2}\left(r\right)$$

For 1000 randomly generated interferometers



~1 sec ~5 sec ~22 sec

3 APs 10 APs 35 APs

APs = $\binom{n}{k}$