Institute for
Quantum Information Science
at the University of Calgary

"Continuous Variable" Quantum Information: Sharing Quantum Secrets

Barry C. Sanders
Institute for Quantum Information Science
http://www.iqis.org/

Congress of the Canadian Association of Physicists
Winnipeg, Manitoba — 14 June 2004

Members of Calgary's Institute for QIS

Faculty

- R. Cleve (Comp Sci)
- D. Feder (Th. Physics)
- P. Høyer (Comp Sci)
- K.-P. Marzlin (Th. Physics)
- A. Lvovsky (Exp. Physics)
- B. C. Sanders (Th. Physics)
- J. Watrous (Comp Sci)
- Affiliates: D. Hobill (Gen. Rel.), R. Thompson (Ion Trap), R. Scheidler & H. Williams (Crypto)

Postdocs

S. Ghose, H. Klauck, H. Roehrig, A. Scott, J. Walgate

Students

I. Abu-Ajamieh, M. Adcock, S. Fast, D. Gavinsky, G. Gutoski, T. Harmon, Y. Kim, S. van der Lee, K. Luttmer, A. Morris, X. S. Qi, Z. B. Wang

Research Assistants

L. Hanlen, R. Horn, G. Howard

Q. Information Science (QIS)

- Multidisciplinary research area that combines chemistry, physics, mathematics, computer science, electrical engineering, philosophy, ….
- Goal: communication & computation that exploit quantum laws of nature – beyond “bits” and Boolean (AND, XOR, NOT, …) operations.
- New technologies, materials, devices now allow quantum effects to extend to the nano- and meso-scale enabling QIS experiments and applications.

Superposition/Entanglement

- Classically: 0 and 1, and NOT flips values.
- Superposition: 0 and 1 coexist as two waves.
- “Rotate” between 0 wave and 1 wave.
- Refer to 0 state as $|0\rangle$ and 1 state as $|1\rangle$.
- Consider two systems in states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, or superpositions thereof.
- In binary, 00=0, 01=1, 10=2, 11=3, and all four of these states can coexist and be simultaneously processed.

Collaborators on CV QIS

Australian National University (Exp)

- Warwick Bowen
- Andrew Lance
- Ping Koy Lam
- Thomas Symul

Masaryk University

- Tomás Tyc

University of Toronto

- David Rowe

Funding

- iCORE
- Australian Research Council
- Macquarie University, Sydney
- NSERC

Outline

I. On continuous variable quantum information

II. Logical states and operations

III. Quantum teleportation – CV QI task

IV. Sharing secrets – background

V. Shared quantum secrets: theory & experiment

VI. Conclusions

I. On continuous variable quantum information

Analogue QIS

- Digital vs analogue communication and computing: discrete vs continuous
- Qubits vs coding via amplitude modulation
- Quantum optics: low decoherence, excellent squeezing, and homodyne detection
- Challenge for analogue information: error correction
- What is quantum? (i) Exceed vacuum noise limit. (ii) outperform analogue info processing

II. Logic states and operations

Analogue Quantum Information

- Digital vs analogue information has a quantum counterpart: qubit vs ‘continuous variable (CV) quantum information’.
- Advantage: CVQI is amenable to quantum optics experiments using squeezed light and has low decoherence.
- Drawback to CVQI: lack error correction (but qudits can be encoded into CV).

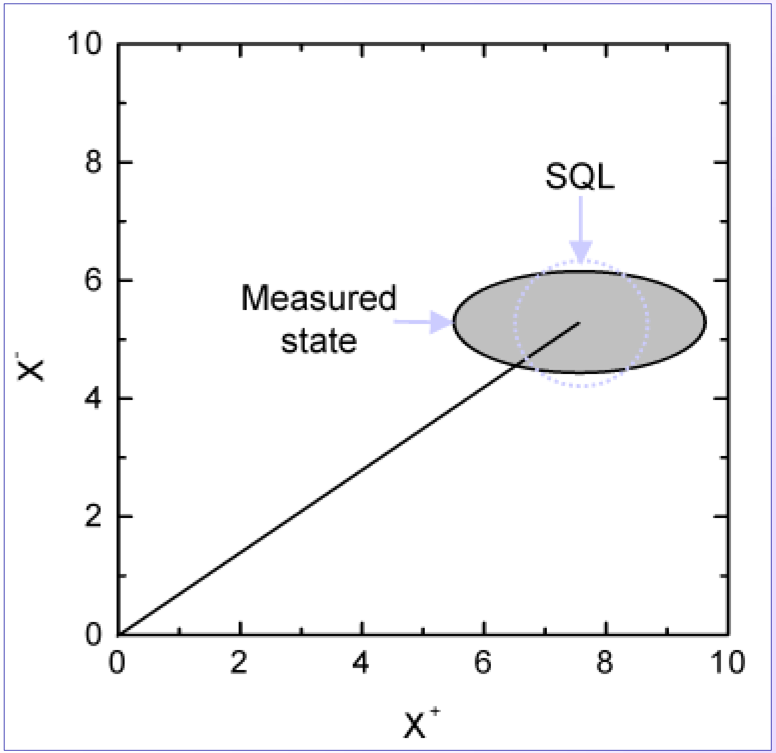
Logic states

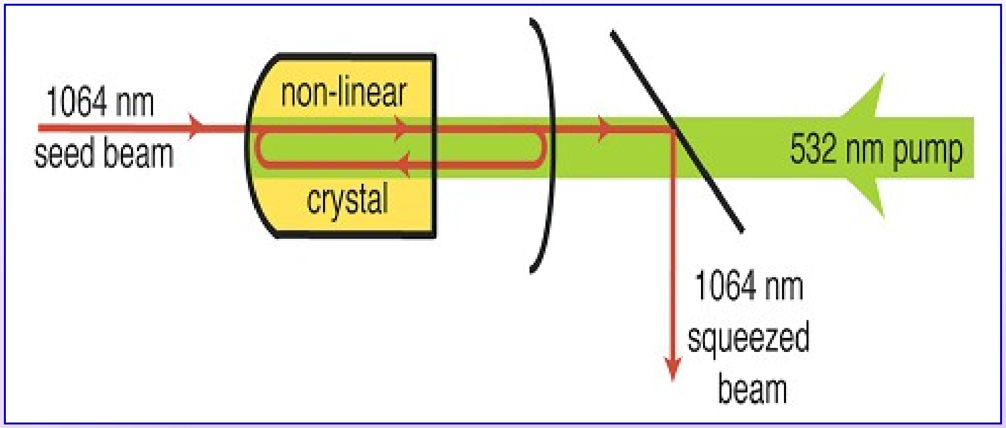
- For qubit, logical basis: $|0\rangle$ and $|1\rangle$.
- For CVQI, logical states are $|x\rangle$, for x real, but these states are not attainable physically.
- Gaussian (squeezed) states approximate these logical states (but lose orthogonality).

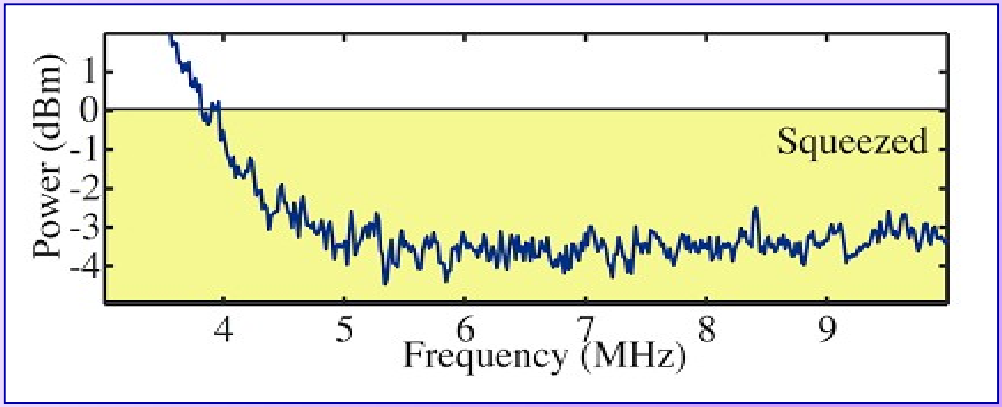
$$\boxed{\varphi_a(x) = \langle x | \varphi_a \rangle = \frac{e^{-x^2/2a^2}}{\sqrt[4]{\pi a^2}}}$$

- Coherent state (laser output) corresponds to a=1
- General state is $\boxed{|\psi\rangle \in \mathcal{H} \sim \mathcal{L}^2(\mathcal{R})}$

Squeezed light







Measurement

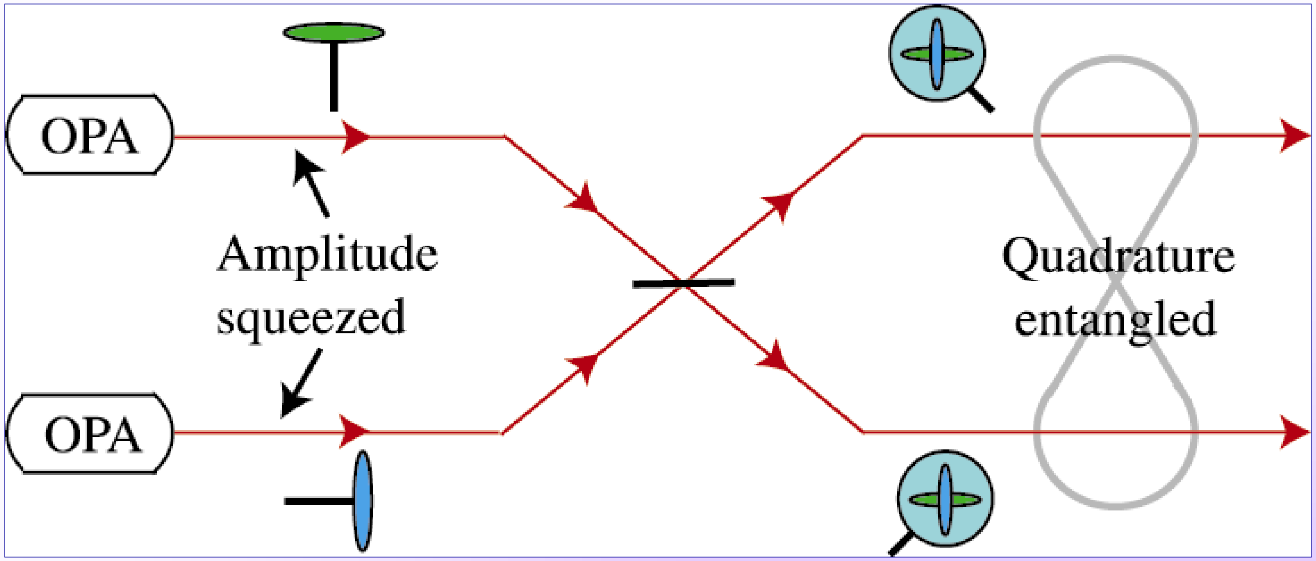
- The field quadratures
$$x_\varphi = p_{\varphi-\pi/2} = x\cos\varphi + p\sin\varphi.$$
are measured via homodyne measurement; reference phase set by local oscillator.
- The x distribution for density
$$\rho \text{ is } P(x) = \langle x|\rho|x\rangle.$$

Resource: two-mode entangled state

- Mixing a squeezed state $\varphi_a(x)$ and its antisqueezed counterpart $\varphi_{1/a}(x)$ at a beam splitter yields a two-mode squeezed (or Einstein-Podolsky-Rosen) state

$$|\eta\rangle \text{ such that } \langle xx'|\eta\rangle = \left(1-\eta^2\right)^{1/2} \sum \eta^n u_n(x) u_n(x'), \; u_n(x) = \langle x|n\rangle.$$

$$\text{NB}: \left(1-\eta^2\right)^{-1/2} |\eta\rangle \xrightarrow{\eta\to 1} |\Theta\rangle.$$



$$X_x^{+} = \frac{1}{\sqrt{2}}\left(X^{+}_{\mathrm{sqz},1} + X^{+}_{\mathrm{anti},2}\right) \qquad X_x^{-} = \frac{1}{\sqrt{2}}\left(X^{-}_{\mathrm{anti},1} + X^{-}_{\mathrm{sqz},2}\right)$$

$$X_y^{+} = \frac{1}{\sqrt{2}}\left(X^{+}_{\mathrm{sqz},1} - X^{+}_{\mathrm{anti},2}\right) \qquad X_y^{-} = \frac{1}{\sqrt{2}}\left(X^{-}_{\mathrm{anti},1} - X^{-}_{\mathrm{sqz},2}\right)$$

Transformations

- Squeezing: $|x\rangle \mapsto |x\mathrm{e}^{-r}\rangle$
- BS: $|x\rangle|y\rangle \text{ a } |y\sin\theta + x\cos\theta\rangle|y\cos\theta - x\sin\theta\rangle.$
- Two-mode squeezing

  $$|x\rangle|y\rangle \text{ a } |y\sinh\theta + x\cosh\theta\rangle|y\cosh\theta + x\sinh\theta\rangle.$$
- QND interaction: $|x\rangle|y\rangle \text{ a } |x\rangle|x + y\rangle.$
- General linear transformation for *k* modes in coordinate representation yields unitary transformation in Sp*(2k*,R*)*; add displacement to obtain [HW*(k)*]Sp*(2k*,R*)*
- Universal gates requires transformation outside this set; otherwise efficiently simulatable.

III. Quantum teleportation – a CV QI task

Quantum Teleportation

Example of a quantum information task

- How to send a quantum state down a channel that is too fragile for sending quantum states?
  - Alice and Bob share entanglement in advance and share a classical information channel.
  - Alice is provided a q. state to send to Bob
  - Alice mixes q. state with her share of entangled state, measures, then transmits the measurement outcome as classical information to Bob, who uses this information to reconstruct q. state from his share of entangled state.

Schematic of optical experiment for teleporting a qubit encoded in the polarization state of a photon

Quantum Teleportation

Applications of Q. Teleportation

- A network of quantum nodes (to distribute quantum keys for cryptography or a distributed quantum computer) may need to send qubits down classical channels because quantum channels are too fragile.
- Q. teleportation allows sending of qubits if entanglement is shared in advance.
- CV q. teleportation: Alice and Bob share two-mode squeezed state and Alice transmits homodyne detection results.

IV. Sharing secrets – background

Classical Secret Sharing

- Cryptographic protocol for sharing information with players who are unreliable or not trustworthy.
- Trust in numbers: players must collaborate.
- Only authorized subsets (access structure) can extract secret; unauthorized subsets (adversary structure) learn nothing about secret.
- *(k,n)*-threshold secret sharing: in a set of *n* players, any subset of *k* or more players can extract secret.

Background

- Liu's combinatoric problem: document locked in safe with many locks, and keys distributed to players who must collaborate to open safe.
- Shamir (polynomial interpolation) and Blakley's (projective spaces) threshold secret sharing, which replaces locks and keys by mathematical problem that can only be solved by collaborating.
- Quantum version of threshold secret sharing.

Motivation for sharing quantum secrets

- Quantum cryptography: Alice and Bob share a quantum key, then distribute to other players.
- Quantum computation: partially calculated quantum computer output shared in distributed quantum computation system.
- Entanglement sharing schemes.
- Quantum error correction.
- Robust storage of states in a network.

V. Shared quantum secrets: theory & experiment

(k=2,2k-1=3) Threshold QSS with Qutrits

Encode a secret qutrit into three qutrits (Cleve et al., PRL 1999):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \text{ a } |\Phi\rangle = \alpha\sum_{k=1}^{3}|kkk\rangle + \beta\left(|012\rangle + |120\rangle + |201\rangle\right)$$
$$+\gamma\left(|021\rangle + |102\rangle + |210\rangle\right)$$

Single share yields no information: $\mathrm{Tr}_{jk}|\Phi\rangle\langle\Phi| = \hat{I}$.

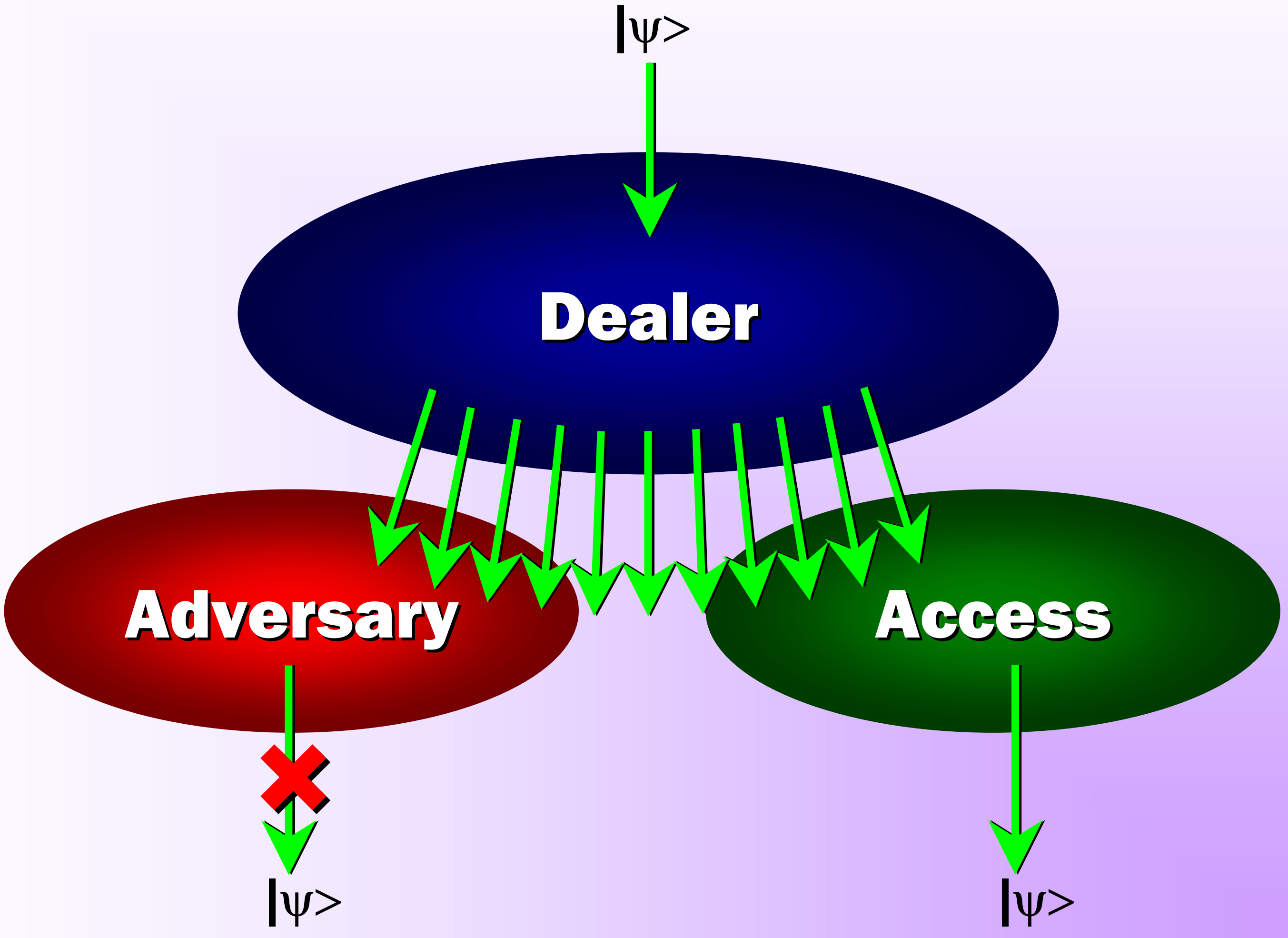
Unitarily combine first two shares by (i) adding value of first share to second, then (ii) adding resultant value of second share to first:

$$|\Phi\rangle \text{ a } |\Phi'\rangle = \left(\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle\right) \otimes \left(|00\rangle + |12\rangle + |21\rangle\right).$$

Shareholders 1 and 2 have collaborated to reproduce the secret in shar

Shareholder 3 has no information about the secret: $\mathrm{Tr}_{12}|\Phi'\rangle\langle\Phi'| = \hat{I}$.

Sharing a quantum state



Characterization of QSS

- Due to finite squeezing and other effects, access structure obtains degraded secret and adversary structure obtains part of secret.
- Characterize QSS by fidelity (squared) for access and adversary structures.

$$\mathrm{F} = \left\langle \psi_{\mathrm{in}} \middle| \rho_{\mathrm{out}} \middle| \psi_{\mathrm{in}} \right\rangle$$

- Exceeding vacuum limit: ***F > 0.5***

(2,3) CV q. secret sharing

The dealer combines the secret state $|\psi\rangle = \int_{-\infty}^{\infty} dx\,\psi(x)|x\rangle$ with the EPR state to obtain the product state $|\psi\rangle_1|\Theta\rangle_{23}$, which is encoded into the 3-mode state $|\Phi\rangle = \int_{-\infty}^{\infty} dx_1 \int_{-\infty}^{\infty} dx_2 \psi(x_1)\left|\frac{x_2+x_1}{\sqrt{2}}\right\rangle_1\left|\frac{x_2-x_1}{\sqrt{2}}\right\rangle_2 |x_2\rangle_3$. Players 1 and 2 employ U_{12} such that $U_{12}|X\rangle_1|Y\rangle_2 = \left|\frac{X-Y}{\sqrt{2}}\right\rangle_1\left|\frac{X+Y}{\sqrt{2}}\right\rangle_2$ so $U_{12}|\Phi\rangle = |\psi\rangle_1|\Theta\rangle_{23}$.

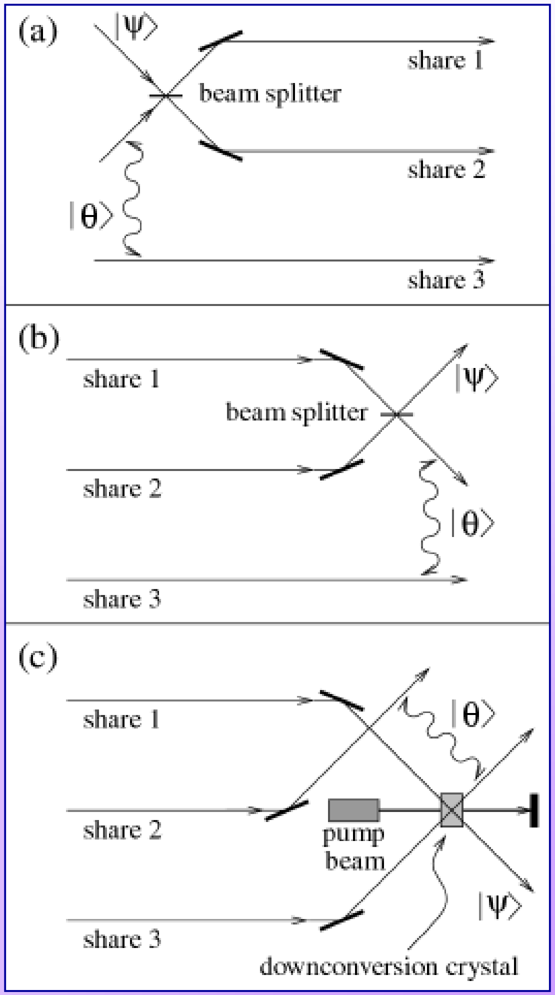
Players 1 and 3 use U_{13} such that $U_{13}|X\rangle_1|Y\rangle_3 = |\sqrt{2}X - Y\rangle_1|\sqrt{2}Y - X\rangle_3$ so $U_{13}|\Phi\rangle = |\psi\rangle_1|\Theta\rangle_{23}$. In both cases the adversary acquires zero information.

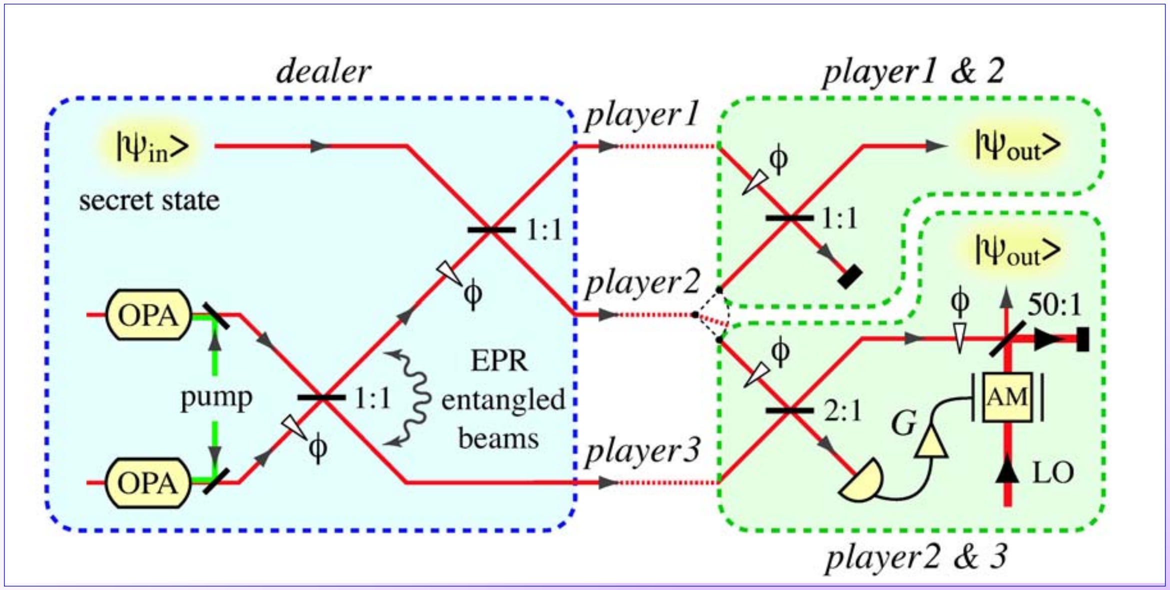
Encoding/Reconstruction

(a) Dealer creates $|\psi\rangle_1|\Theta\rangle_{23}$ and combines modes 1 and 2 at a 50/50 BS to produce $|\Phi\rangle$.

(b) Players 1 and 2 combine shares at a 50/50 BS to obtain $|\psi\rangle_1$.

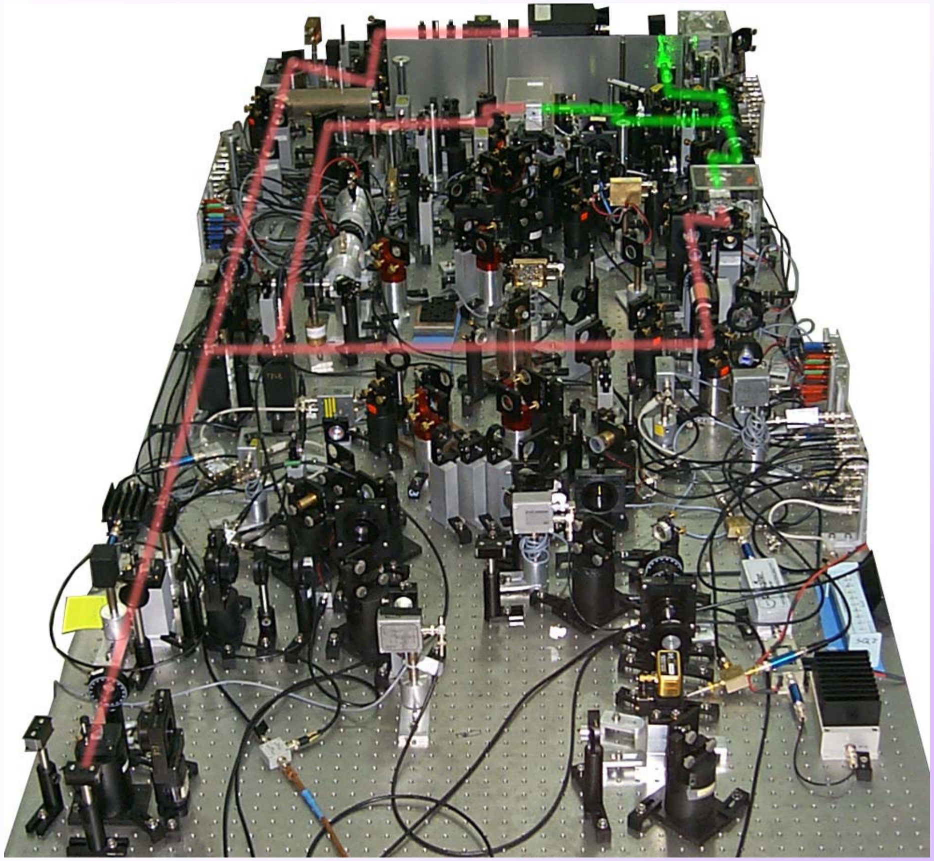
(c) Players 1 and 3 combine shares at a squeezing device to recover $|\psi\rangle_1$.



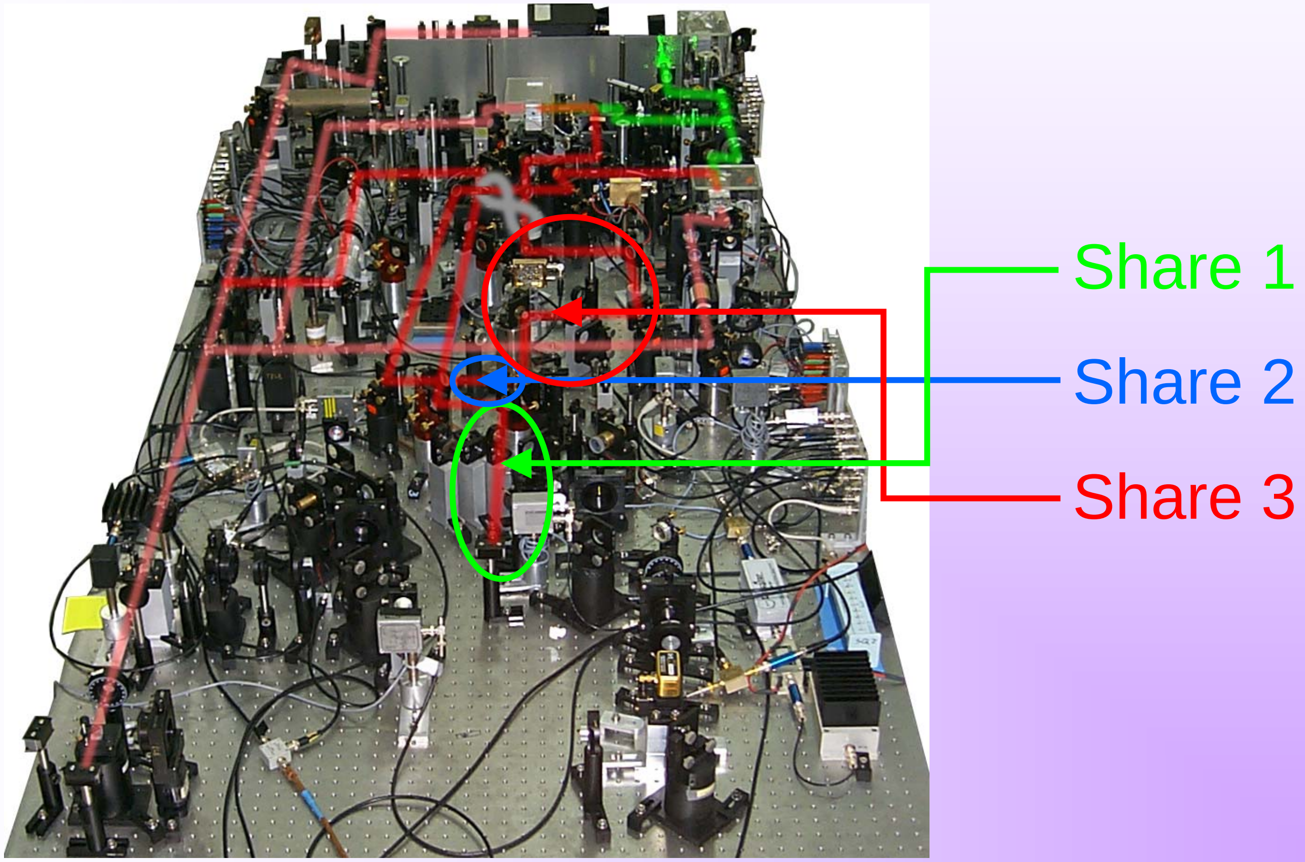


For players {2,3}, *p* quadrature of secret state reproduced at 2:1 BS for appropriate phase choice, and *x* noise correlated with other BS output. Resultant photocurrent used to displace *x* quadrature (AM = amplitude modulator) by gain *G*, ideally so that product of *x* and *p* gains is unity.

Experimental setup



Experimental setup

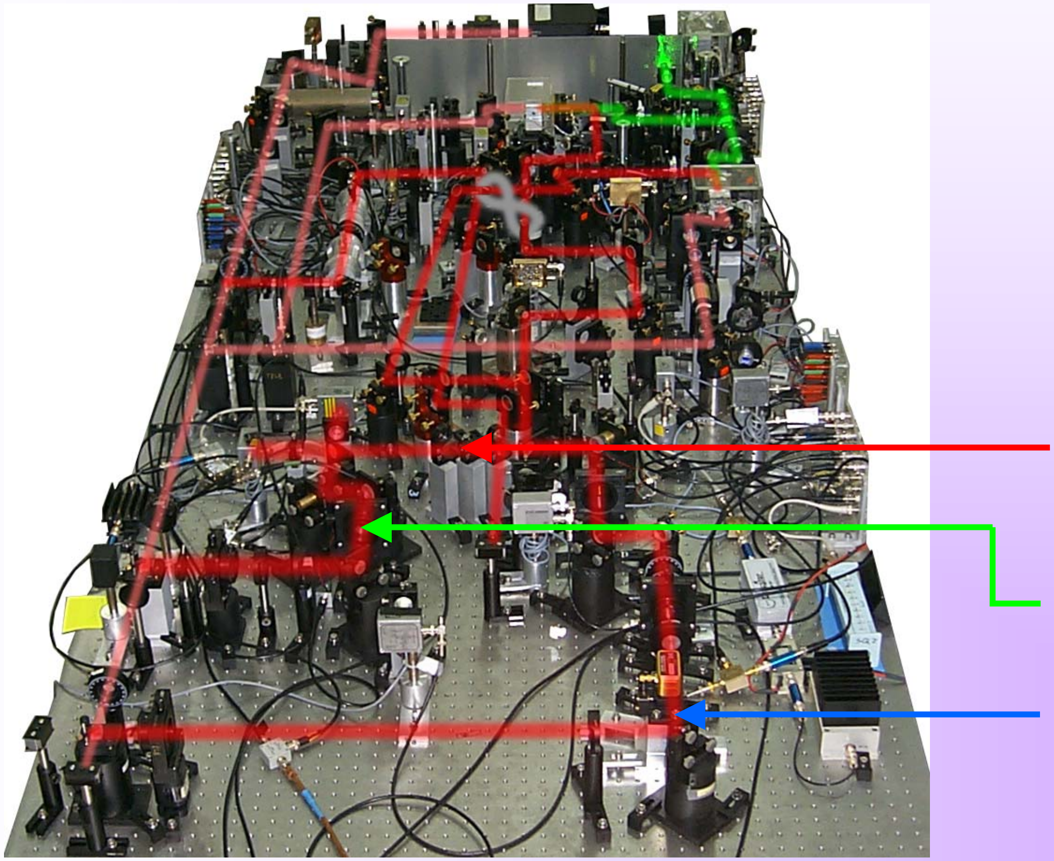


Share 1

Share 2

Share 3

Experimental setup

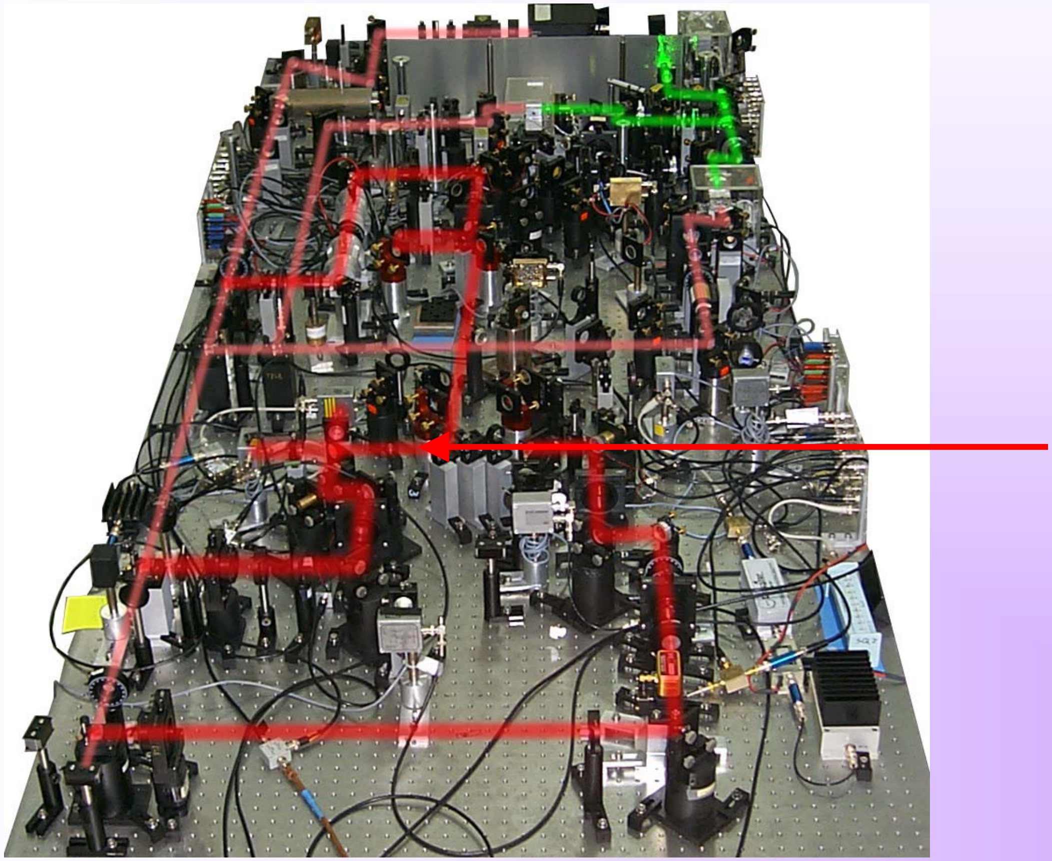


Reconstructed secret

Local Oscillator

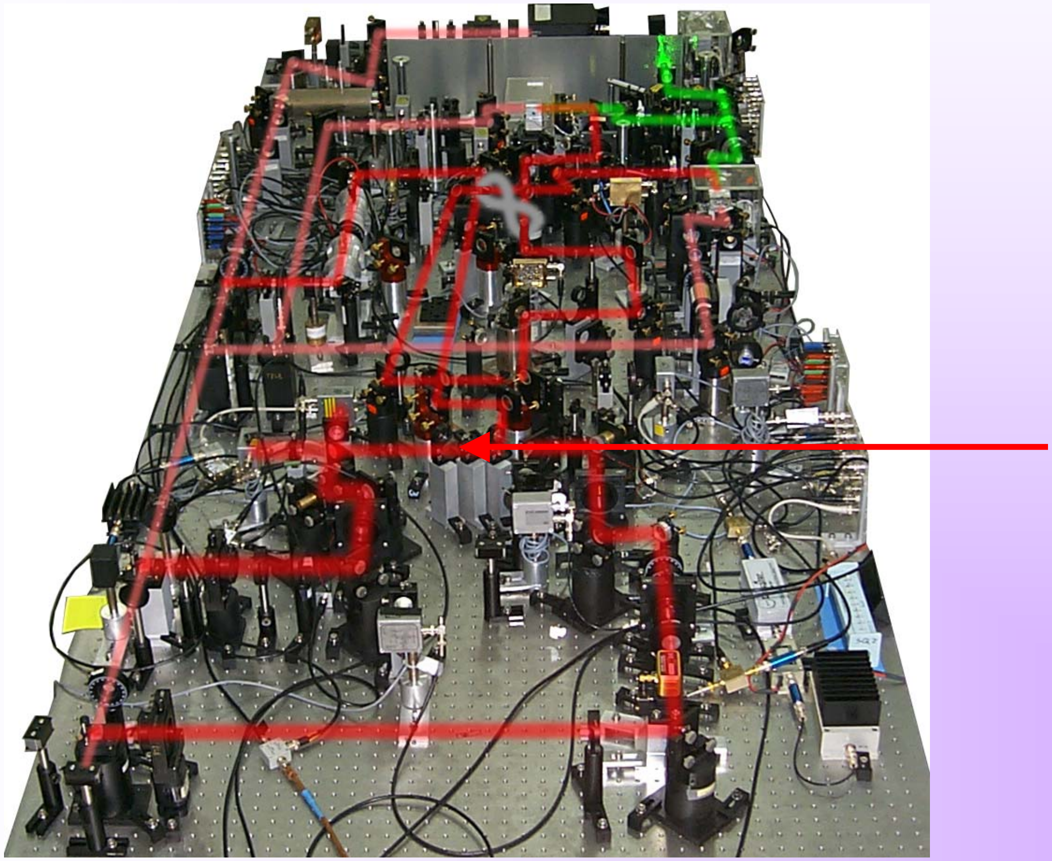
Fat Beam

Experimental setup



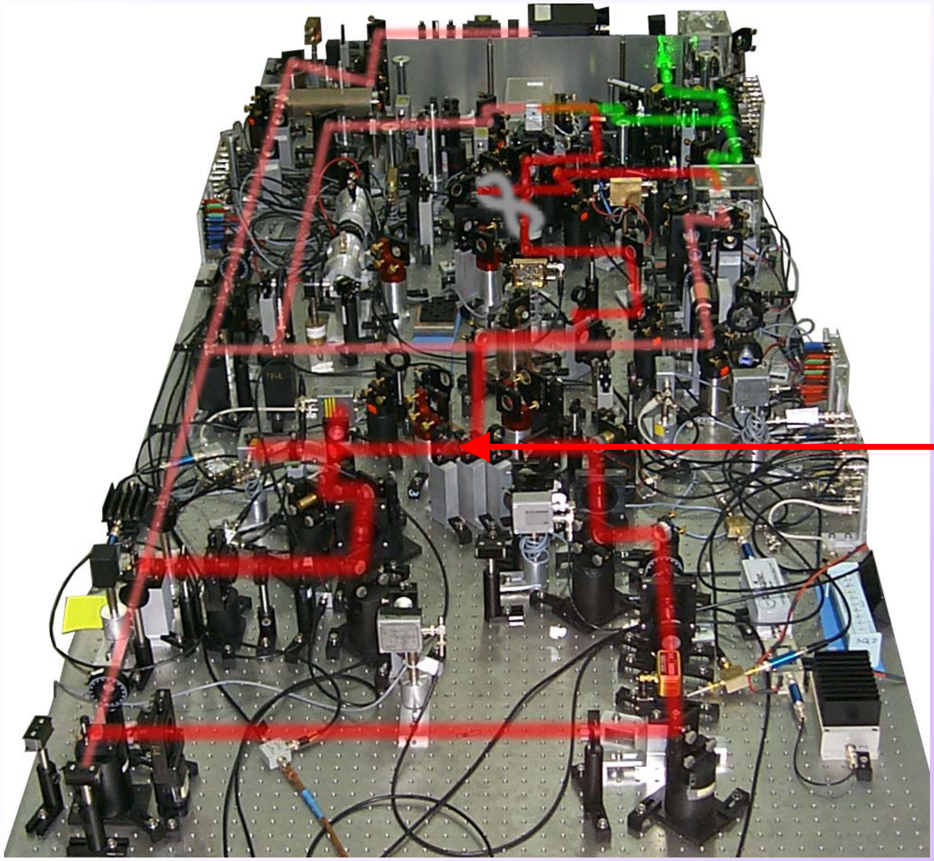
Input state

Experimental setup



Adversary

Experimental setup



EPR 2

or

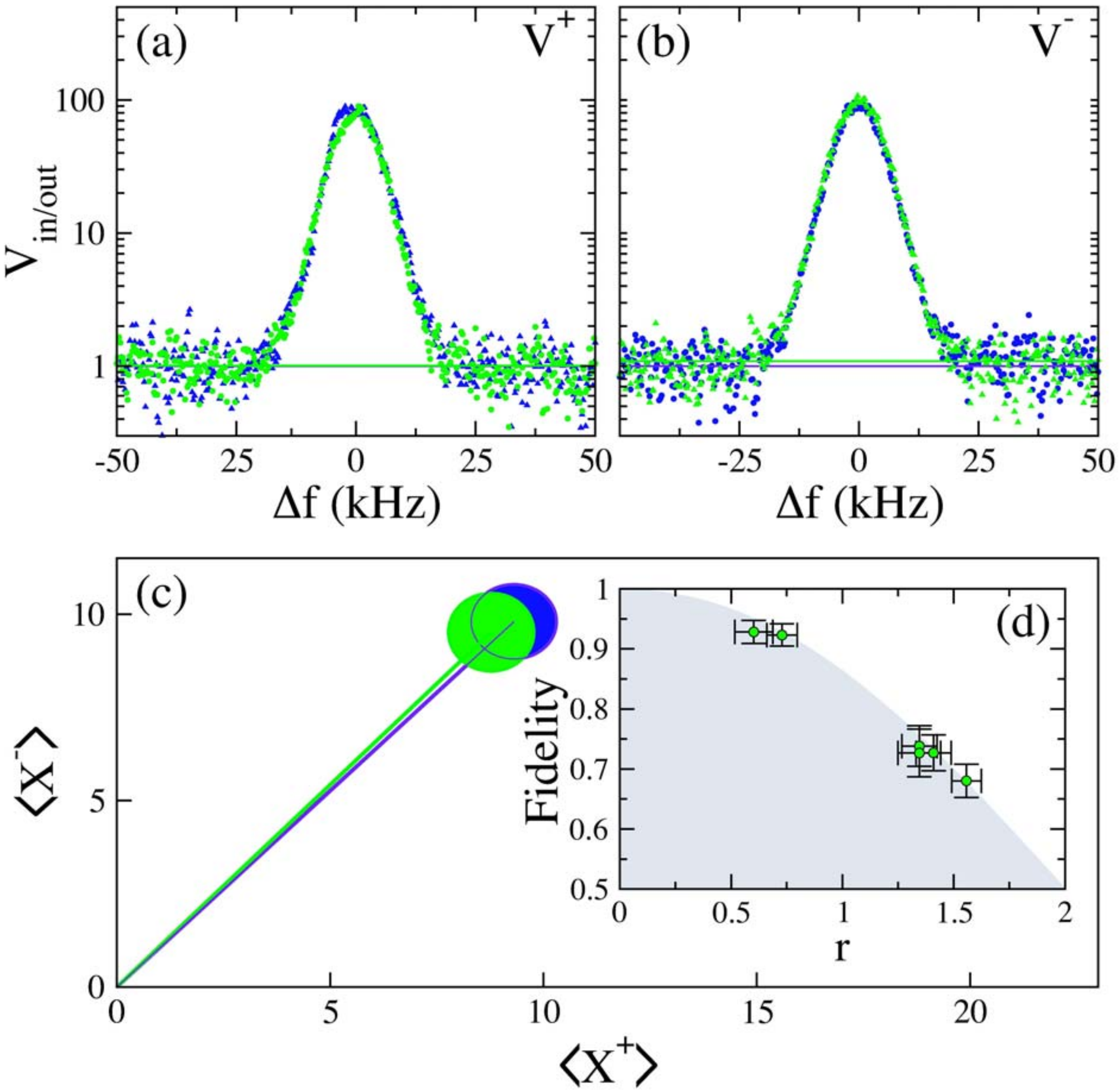
½ SQZ 1

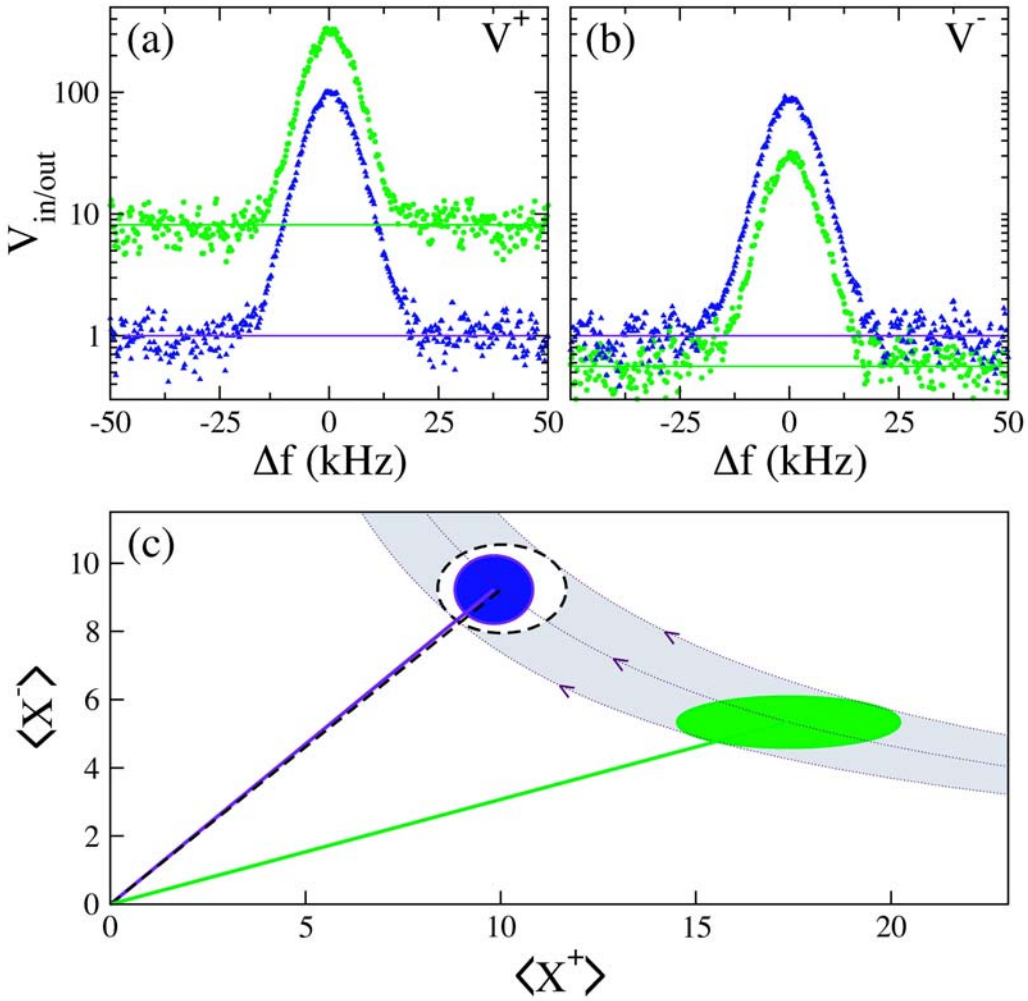
or

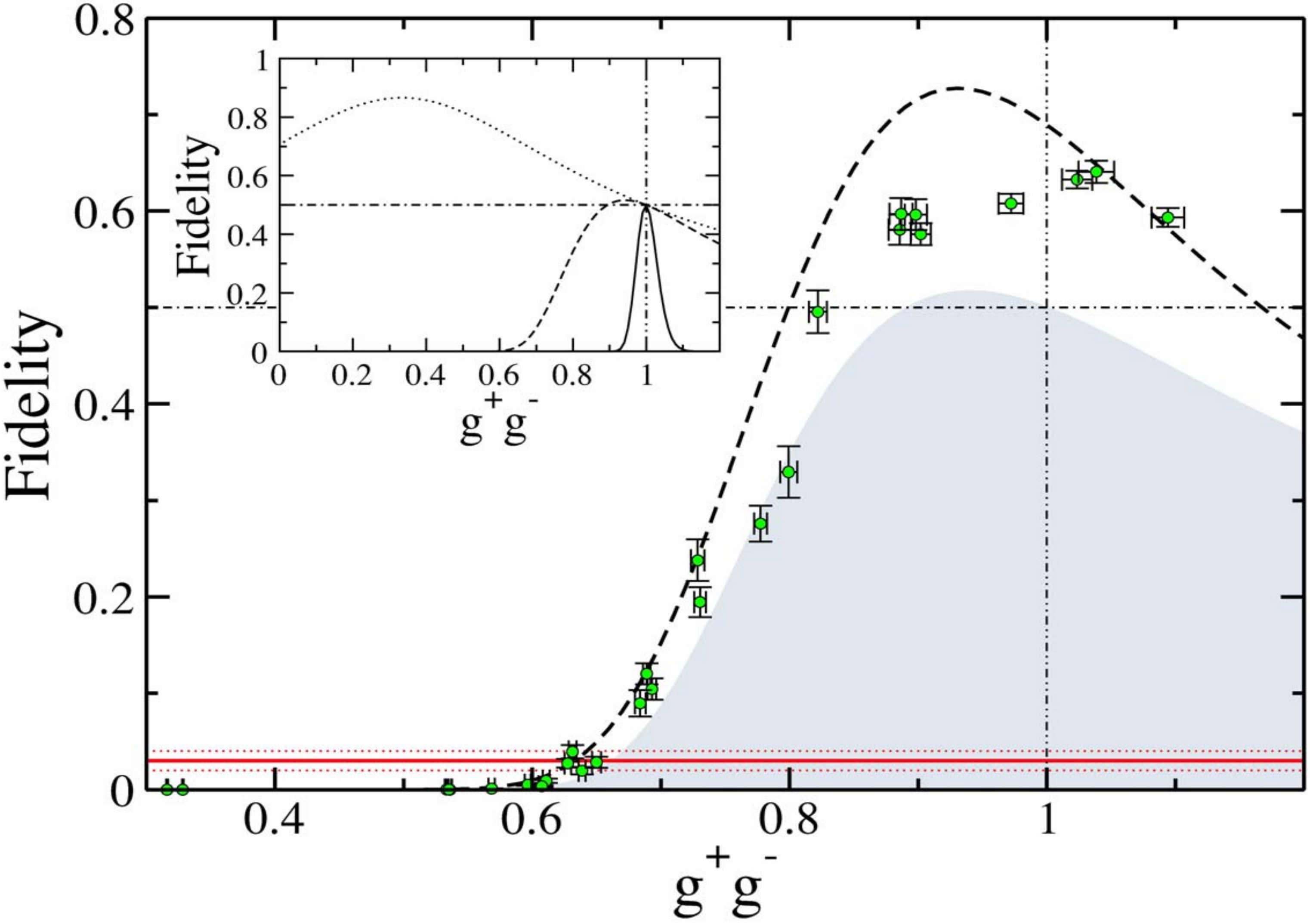
½ SQZ 2

Experimental properties

- Laser source: Nd:YAG at 1064 nm
- OPA pumped at 532 nm
- Secret state by AM and PM at 6.12 MHz
- Squeezing 4.5 dB
- Homodyne detection efficiency 0.89
- Visibility of 1:1 beam splitter is 99.2%
- Resolution bandwidth: 1 kHz

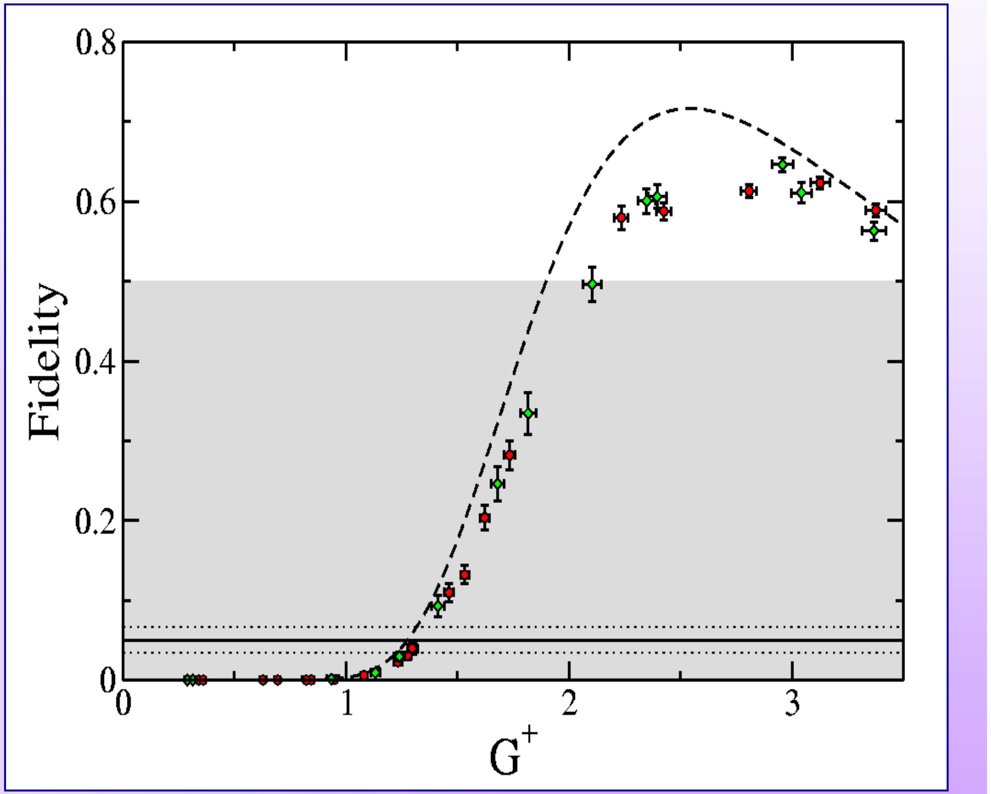

(a)
V$^+$
(b)
V$^-$
V$_{in/out}$
100
10
1
-50
25
0
25
50
Δf (kHz)
-25
0
25
50
Δf (kHz)
(c)
⟨X$^-$⟩
10
5
0
0
5
10
15
20
⟨X$^+$⟩
(d)
Fidelity
1
0.9
0.8
0.7
0.6
0.5
0
0.5
1
1.5
2
r


(a)
V$^+$
(b)
V$^-$
$V_{in/out}$
100
10
1
-50
-25
0
25
50
Δf (kHz)
(c)
⟨X$^-$⟩
⟨X$^+$⟩
0
2
4
6
8
10
5
15
20


Fidelity
0.8
0.6
0.4
0.2
0
0.4
0.6
0.8
1
g^+g^-
Fidelity
1
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8
1
g^+g^-

Experimental Fidelity results

- The best experimental fidelity for the collaborating player is F=0.646±0.009 for a gain of G+=2.96 ±0.05
- The fidelity of the access structure is F=0.050±0.016



Generalization to (k,n)

- CV sharing of q. secrets can be generalized to the arbitrary (*k*,*n*) case.
- Dealer begins with $\Psi(\vec{x}) = \psi(x)\prod_{i=1}^{k-1}\varphi_a(y_i)\prod_{j=1}^{k-1}\varphi_{1/a}(z_i)$ where

$$\vec{x} = (x, y_1, \ldots, y_{k-1}, z_1, \ldots, z_{k-1}) \in \Re^{n=2k-1}$$

- Dealer encodes via GL transformation on coordinates so that any *k* players can undo transformation

$$\left|\Psi_g\right\rangle = \left|\mathrm{det} g\right|^{1/2} \int \mathrm{d}^n\vec{x}\,\Psi(\vec{x})\left|g_1(\vec{x})\right\rangle \otimes \cdots \otimes \left|g_n(\vec{x})\right\rangle$$

Extraction of the q. secret

- The players all know the linear canonical point transformation to reconstruct secret q. state.
- *k* players use a symplectic interferometer to perform

$$g_i \rightarrow \xi_i = \sum_j \xi_{ij} f_j$$

- Of course $g_i = \xi_i \forall i > k$
- Provided that the vectors $\{g_i\}$ are chosen such that any *k* vectors from the set $\{f_1 \equiv x_1, \zeta_1, \ldots, \zeta_n\}$ are linearly independent, and *a* is large, any *k* players can extract the secret q. state.

V. Conclusions

Conclusions

- CV QI yields imperfect but deterministic QI tasks.
- Recent experimental demonstration of (2,3) threshold sharing of secret quantum states with fidelity F>0.5 corresponding to quantum domain.
- General theory of CV (k,n) threshold sharing of secret states, with state extraction by players requiring at most two squeezers.
- Mathematical methods for interferometers with squeezers that are applicable to general, complex quantum optical systems.
- Threshold state sharing allows robust sharing of quantum states within a network.

Our papers on the subject

- Theory of sharing CV q. secrets: T. Tyc and B. C. Sanders, Continuous-variable quantum secret sharing by optical interferometry, Physical Review A 65(4), 042310 (2002).
- Efficient sharing plus rigorous treatment: T. Tyc, D. J. Rowe and B. C. Sanders Efficient sharing of a continuous-variable quantum secret, Journal of Physics A: Mathematical and General 36(27), 7625-7637 (2003).
- How to share CV q. secrets experimentally: A M Lance, T Symul, W P Bowen, T Tyc, B C Sanders and P K Lam Continuous variables (2,3) threshold quantum secret sharing schemes , New Journal of Physics 5, 4 (2003).
- Experiment: A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Sharing a secret quantum state, Physical Review Letters ?(?), ? (2004).