Spacetime Replication of Quantum Information

Barry C. Sanders

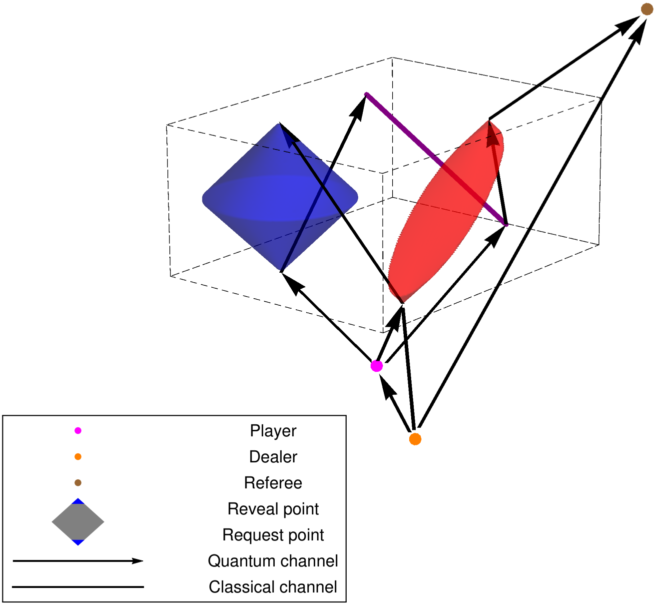
Patrick Hayden, Sepehr Nezami, Grant Salton, Yadong Wu,
Abdullah Khalid and Masoud Habibi

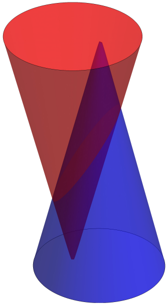
17 November 2016

Motivation

- Generalize no-cloning to a relativistic setting.
- Establish quantum secret sharing as the underlying cryptographic protocol for state replication.
- Interpret spacetime replication as an adversarial game.
- Cast continuous-variable quantum secret sharing as a ramp quantum secret sharing scheme.

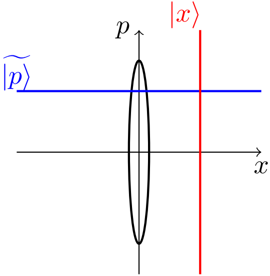
Spacetime replication of quantum information



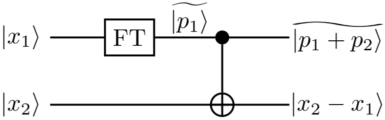


Continuous-variable Clifford group

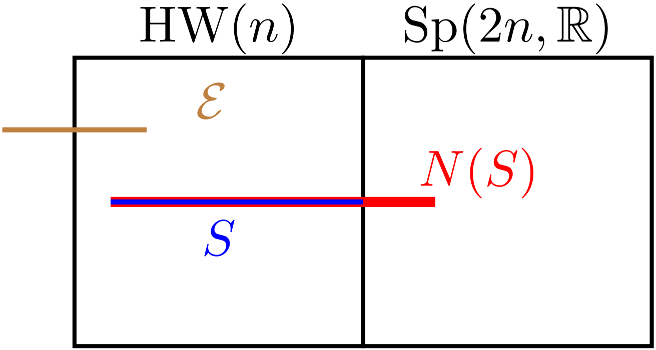
$\mathrm{HW(n)} \rtimes \mathrm{Sp(2n}, \mathbb{R})$	
$X(\boldsymbol{s}) := \exp\left(\mathrm{i}\boldsymbol{s} \cdot \hat{\boldsymbol{x}}\right)$	$S_k(r) := \exp\left(\mathrm{i}r(\hat{x}_k\hat{p}_k + \hat{p}_k\hat{x}_k)\right)$
$P(\boldsymbol{t}) := \exp\left(\mathrm{i}\boldsymbol{t} \cdot \hat{\boldsymbol{p}}\right)$	$\mathrm{QND}_{jk}(g) := \exp\left(\mathrm{i}g\hat{x}_j\hat{p}_k\right)$
	$\mathrm{FT}_k := \exp(\mathrm{i}\frac{\pi}{4}(\hat{x}_k^2 + \hat{p}_k^2))$



Stabilizer $P(t)$, $X(s)$



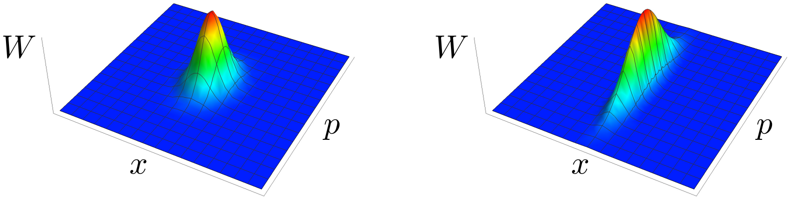
Bartlett Sanders Braunstein Nemoto *Phys. Rev. Lett.* **88** (2002) 10/b7sftd



$S \cup \mathcal{E}$: errors corrected by $S \leq \mathrm{HW}(n)$

The replication game
Interactive protocol

Verifier (dealer+referee) ⟷ Prover (player+agents)



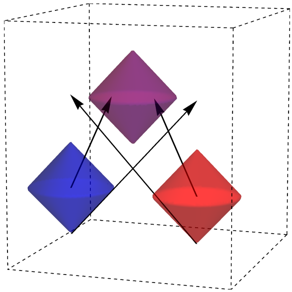
$|\psi\rangle$ — Succeed — Decision = Accept(%) (Complete)

$|\psi\rangle$ — Fail — Decision = Reject(%) (Sound)

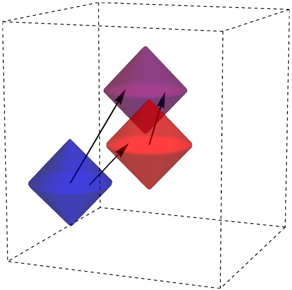
Conditions for spacetime replication

Hayden May *J. Phys. A* 49 (2016) 10/bsfk

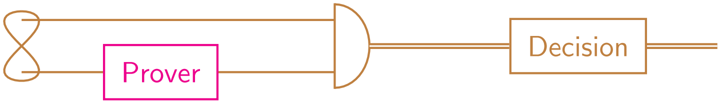
Spacetime replication is possible iff each pair of causal diamonds is causally connected.



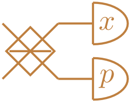
✓

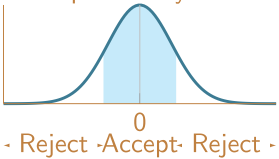


✗

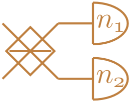


$$\left| x := \frac{x_1+x_2}{\sqrt{2}}, p := \frac{p_1-p_2}{\sqrt{2}} \right\rangle$$





$$|-\alpha, \alpha\rangle - |\alpha, -\alpha\rangle$$



Accept when
$n_1 = 0, n_2 = \mathrm{odd}$

Jeong Kim Lee *Phys. Rev. A* **64** (2001) 10/bpgqr2

Honest-prover strategies

- DV codeword-stabilized codes[1]
- CV codeword-stabilized codes[2]
- (2,3) quantum secret sharing and teleportation codes

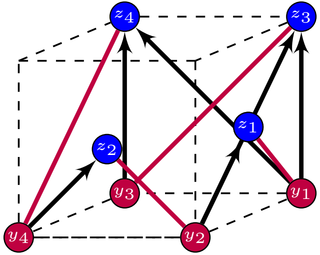
Cheating-prover strategies

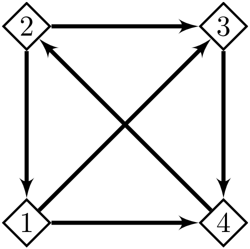
- Return random state
- Return partial clone
- Return state prepared using knowledge from tomography

[1] Hayden May *J. Phys. A* **49** (2016) 10/bsfk

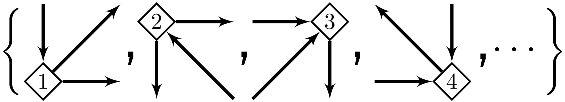
[2] Hayden Nezami Salton Sanders *New J. Phys.* **18** (2016) 10/bsfm

Continuous-variable stabilizer codes

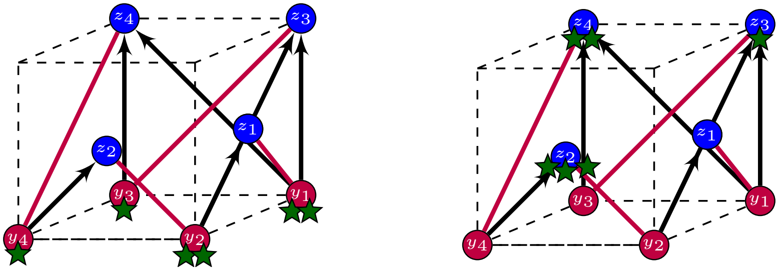




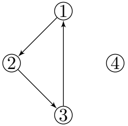
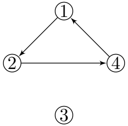
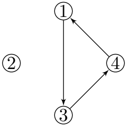
Access Structure :=



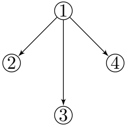
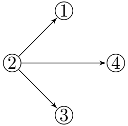
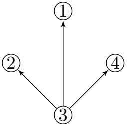
Hayden Nezami Salton Sanders *New J. Phys.* **18** (2016)


z_4
z_3
z_2
z_1
y_3
y_1
y_4
y_2
z_4
z_3
z_1
z_2
y_3
y_1
y_4
y_2

Continuous-variable stabilizer codes

$\mathcal{C}_v :=$ span $\{$  ,  ,  $\}$

$\boldsymbol{s}_{23} = (1, -1, 0, 1, 0, 0)$ $\quad \boldsymbol{s}_{24} = (1, 0, -1, 0, 1, 0)$ $\quad \boldsymbol{s}_{34} = (0, 1, -1, 0, 0, 1)$

$\mathcal{C}_A :=$ span $\{$  ,  ,  $\}$

$\boldsymbol{A}_1 = (1, 1, 1, 0, 0, 0)$ $\quad \boldsymbol{A}_2 = (-1, 0, 0, 1, 1, 0)$ $\quad \boldsymbol{A}_3 = (0, -1, 0, -1, 0, 1)$

$$\underset{\displaystyle (\mathcal{C}_v \oplus \mathcal{C}_A)}{\overset{\boldsymbol{s}}{\downarrow}} \oplus \underset{\displaystyle (\mathcal{C}_v \oplus \mathcal{C}_A)}{\overset{\boldsymbol{t}}{\downarrow}} \cong \mathbb{R}^{12} \cong \mathrm{HW}(6)$$

$$\mathcal{C}_v \perp \mathcal{C}_A \Rightarrow \boldsymbol{s} \cdot \boldsymbol{t} = 0 \Rightarrow [X(\boldsymbol{s}), P(\boldsymbol{t})] = 0$$

Continuous-variable stabilizer codes

$$S = \langle X(\boldsymbol{s}_{23}), X(\boldsymbol{s}_{24}), X(\boldsymbol{s}_{34}), P(\boldsymbol{t}_2), P(\boldsymbol{t}_3) \rangle$$

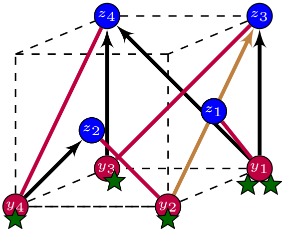
$$\begin{array}{c} \boldsymbol{s}_{23} \\ \boldsymbol{s}_{24} \\ \boldsymbol{s}_{34} \end{array} \begin{pmatrix} 1 & -1 & 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{pmatrix}$$

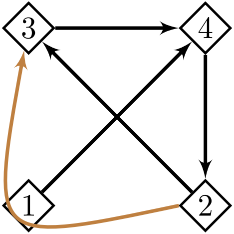
$$\begin{array}{c} \boldsymbol{t}_2 := A_1 + A_2 \\ \boldsymbol{t}_3 := A_1 + A_3 \end{array} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & -1 & 0 & 1 \end{pmatrix}$$

$$|x\rangle_{\mathsf{enc}} = \int \mathrm{d}y\mathrm{d}z \, |x+z, x+y, x+y+z, y-z, y, z\rangle$$

$$\boldsymbol{s}_{23} \cdot \hat{\boldsymbol{x}} \, |x\rangle_{\mathsf{enc}} = (\hat{x}_1 - \hat{x}_2 + \hat{x}_4) \, |x\rangle_{\mathsf{enc}} = 0$$

A five-mode ad hoc code





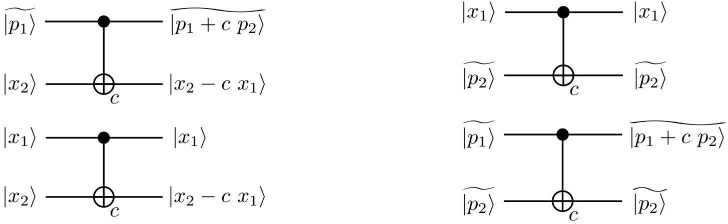
$$S = \langle X(\boldsymbol{s}_1), X(\boldsymbol{s}_2), P(\boldsymbol{t}_1), P(\boldsymbol{t}_2)\rangle$$

$$\begin{array}{c} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \end{array} \begin{pmatrix} -1 & -1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 & -2 \end{pmatrix} \quad \begin{array}{c} \boldsymbol{t}_1 \\ \boldsymbol{t}_2 \end{array} \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 & 1 \end{pmatrix}$$

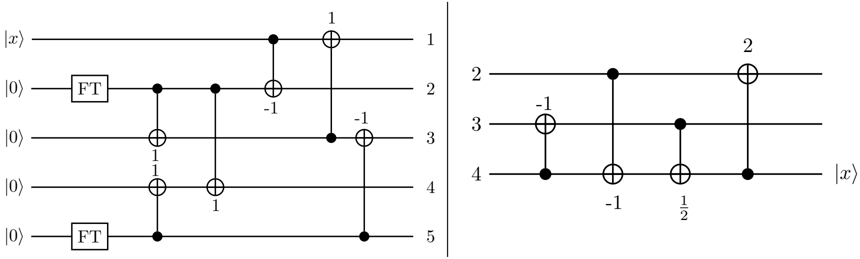
$$|x\rangle_{\mathsf{enc}} := \int \mathrm{d}y\mathrm{d}z \, |x+y, y-x, y-z, z+y, z\rangle$$

$$\boldsymbol{s}_1 \cdot \hat{\boldsymbol{x}} \, |x\rangle_{\mathsf{enc}} = (-\hat{x}_1 - \hat{x}_2 + \hat{x}_3 + \hat{x}_4) \, |x\rangle_{\mathsf{enc}} = 0$$

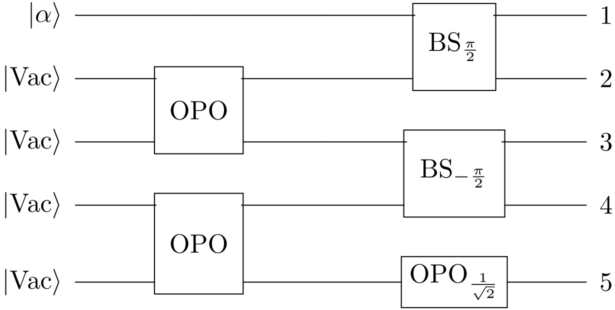
Encoding and decoding

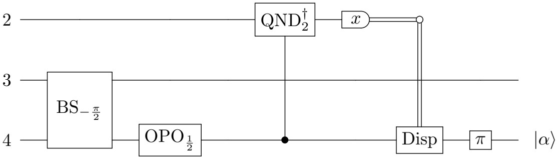


$$|x\rangle_{\mathsf{enc}} := \int \mathrm{d}y\mathrm{d}z\, |x+y, y-x, y-z, z+y, z\rangle$$



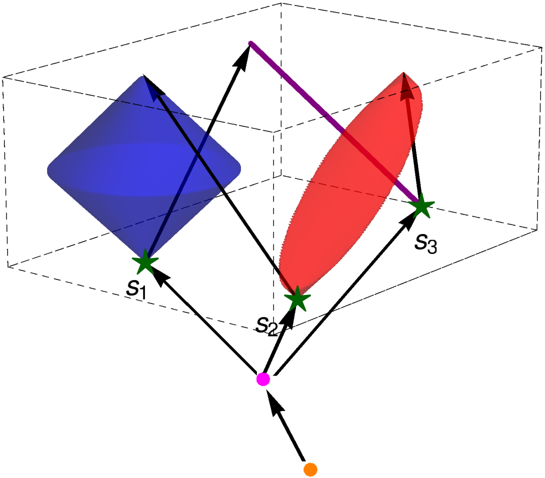
Optical implementation

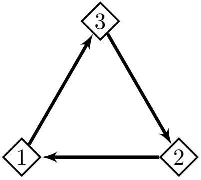




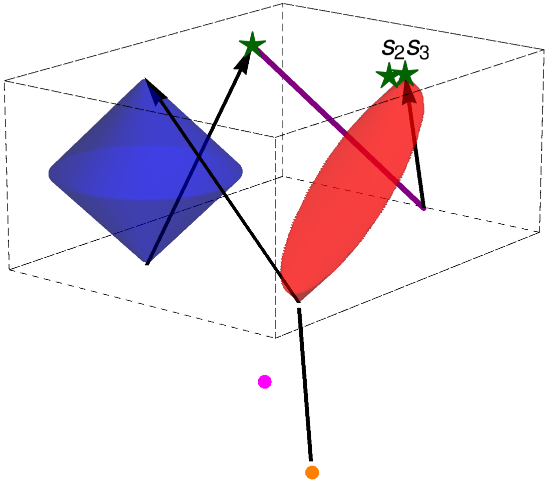
Quantum secret sharing + teleportation codes

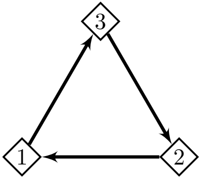
- Design algorithm to convert a complete directed graph to optical circuits for implementation.
- Establish upper bounds on resources required to simulate spacetime replication.
- Three primitive:
  - $(2, 3)$ quantum secret sharing
  - Teleportation
  - Graph decomposition algorithm


s_1
s_2
s_3

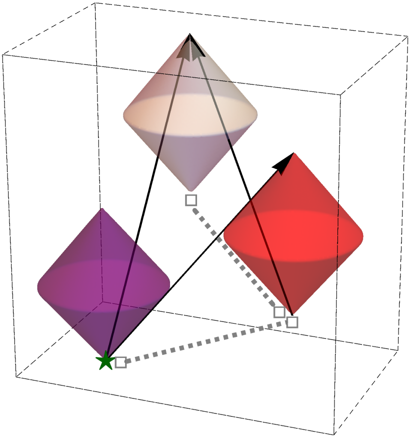

3
1
2

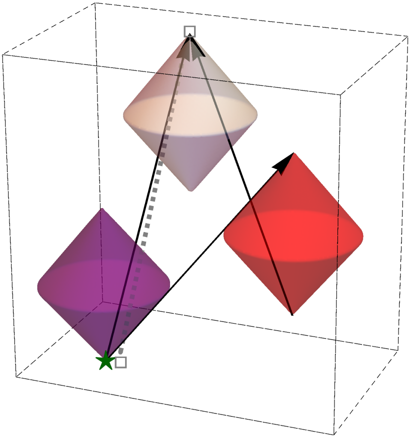
The $(2,3)$ QSS primitive: reveal

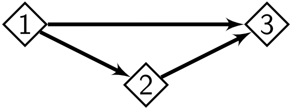




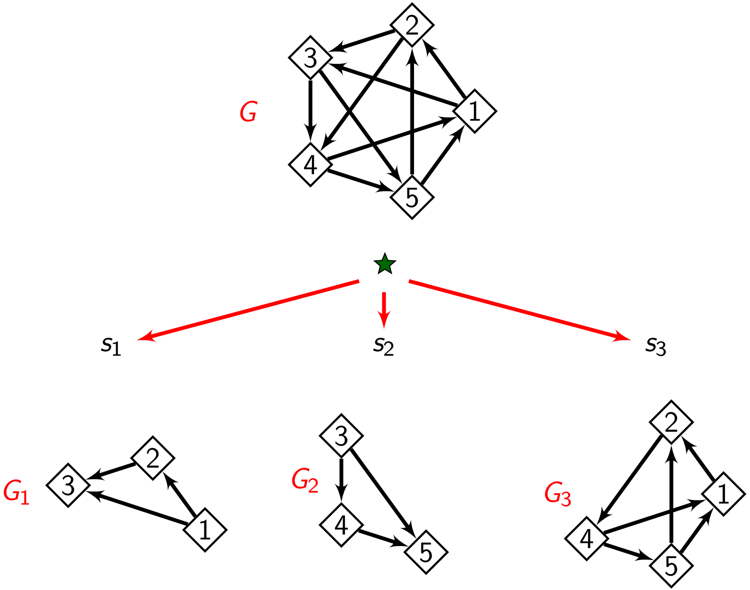
The teleportation primitive

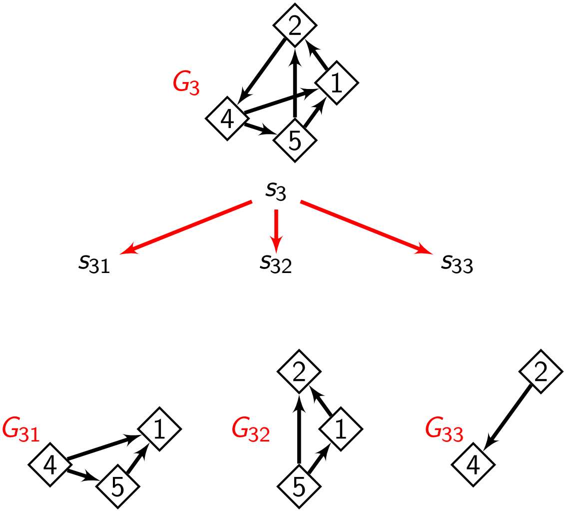




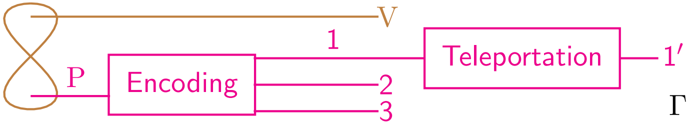


Graph decomposition primitive

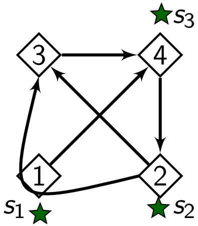


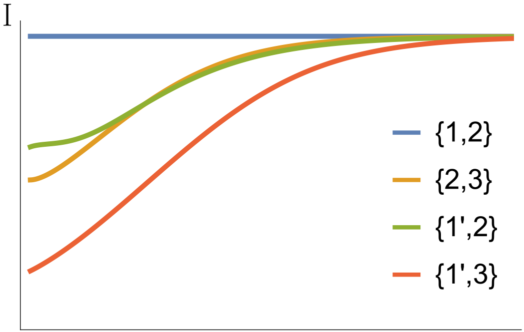

G_3
2
1
4
5
s_3
s_{31}
s_{32}
s_{33}
G_{31}
G_{32}
G_{33}

(2,3) continuous-variable quantum ramp secret sharing



$\Gamma \subseteq \{1, 1', 2, 3\}$



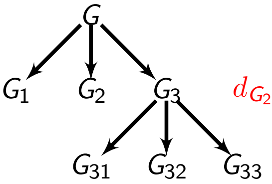


$$\mathrm{I}\left(\rho^{\mathrm{V}\Gamma}\right) = \mathrm{S}\left(\rho^{\mathrm{V}}\right) + \mathrm{S}\left(\rho^{\Gamma}\right) - \mathrm{S}\left(\rho^{\mathrm{V}\Gamma}\right)$$

$$\mathscr{G} = \{ 1, 2, 3, 4, 5 \}$$

$$\mathscr{N} = \{G, G_1, G_2, G_3, G_{31}, G_{32}, G_{33}\}$$

$$\mathscr{L} = \{G_1, G_2, G_{31}, G_{32}, G_{33}\}$$



$d_{G_2} = 1$

$d_{G_{33}} = 2$

$k_{G_{31}} = |V(G_{31})|$

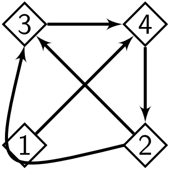
Player $\rightarrow$ Request agents	$\sum_{\ell \in \mathscr{L}} \left[(2k_\ell - 3) \lceil d_\ell \log_2 3 \rceil + 2k_\ell - 4 \right]$ bits
Request agents $\rightarrow$ Reveal agents	$\sum_{\ell \in \mathscr{L}} (k_\ell - 2)(k_\ell + 1)$ reals and $1 + \sum_{\ell \in \mathscr{L}} \left[\frac{(k_\ell - 2)(k_\ell + 1)}{2} \lceil d_\ell \log_2 3 \rceil + \lceil d_\ell \log_2 3 \rceil \right]$ bits

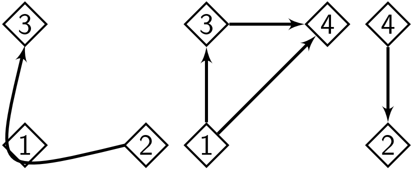
Player $\to$ Request agents	$\lvert\mathscr{L}\rvert + \sum_{\ell\in\mathscr{L}} 2(k_\ell - 2)$ fields
Request agents $\to$ Reveal agents	$\sum_{\ell\in\mathscr{L}} \min[k_\ell - 1, 2]$ fields

Single-mode squeezing	$3(\lvert\mathscr{N}\rvert - \lvert\mathscr{L}\rvert) + 2\sum_{\ell\in\mathscr{L}}(k_\ell - 2)$
Homodyne measurements	$\lvert\mathscr{N}\rvert - \lvert\mathscr{L}\rvert + 2\sum_{\ell\in\mathscr{L}}(k_\ell - 2)$

Lance Symul Bowen Tyc Sanders Lam *New J. Phys.* **5** (2003) 10/c5zggd

Comparison between ad hoc code and QSS&T code





	Ad hoc code	QSS&T scheme
Single-mode squeezing	9	5
Homodyne measurements	4	3

		Ad hoc code	QSS&T scheme
Quantum	Alice → Request	5 fields	5 fields
	Request → Reveal	5 fields	4 fields
Classical	Alice → Request	3 bits	12 bits
	Request → Reveal	5 bits	4 reals and 12 bits