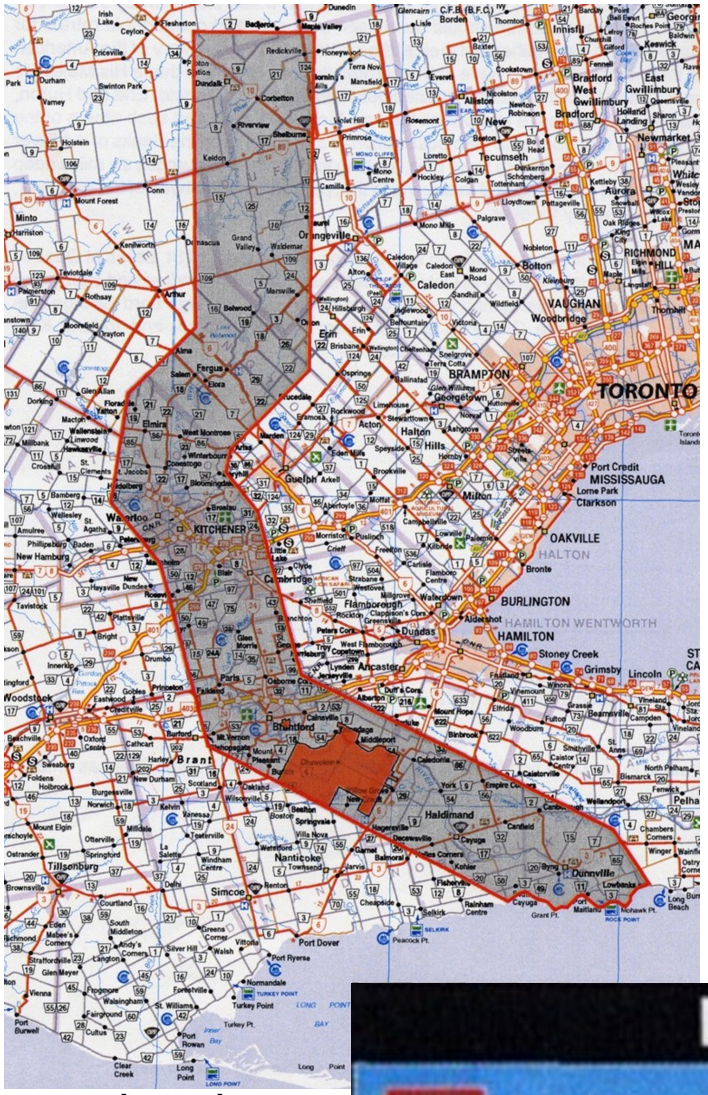
Practical Quantum Fingerprinting and Appointment Scheduling

QF with Norbert Lütkenhaus
AS with Norbert Lütkenhaus and Dave Touchette

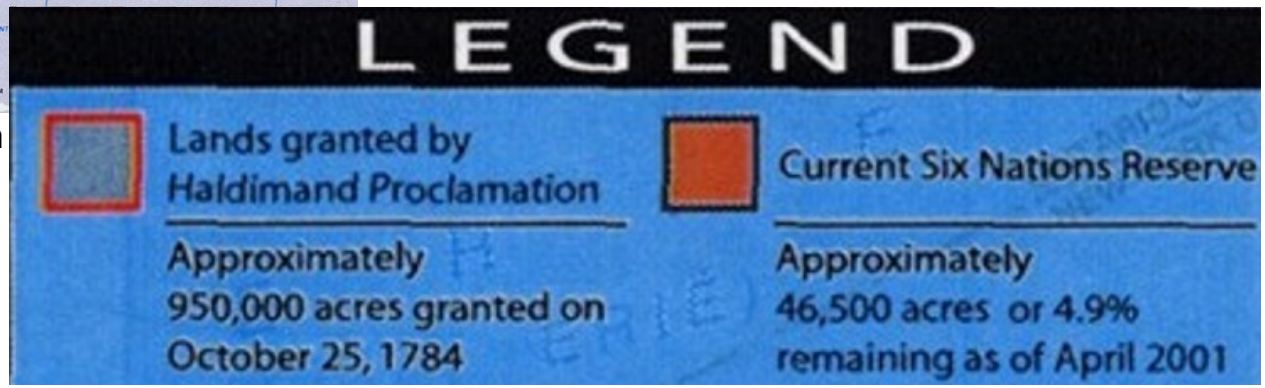
Benjamin Lovitz
Physics (Quantum Information)
MSc. Defense
Supervisor: Norbert Lütkenhaus

Institute for Quantum Computing, University of Waterloo

17 October, 2017

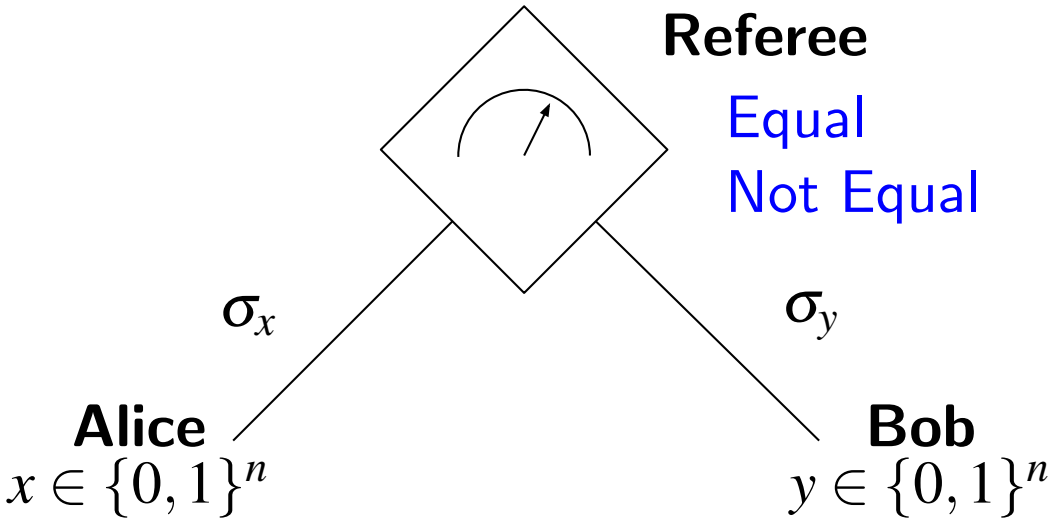


www.sixnations.ca



I acknowledge that I am a settler on the traditional territory of the Attawandaron (Neutral), Anishnawbe, and Haudenosaunee peoples.
This land was promised to the Haudenosaunee peoples in the Haldimand Treaty of 1784.

Quantum fingerprinting



Quantum fingerprinting

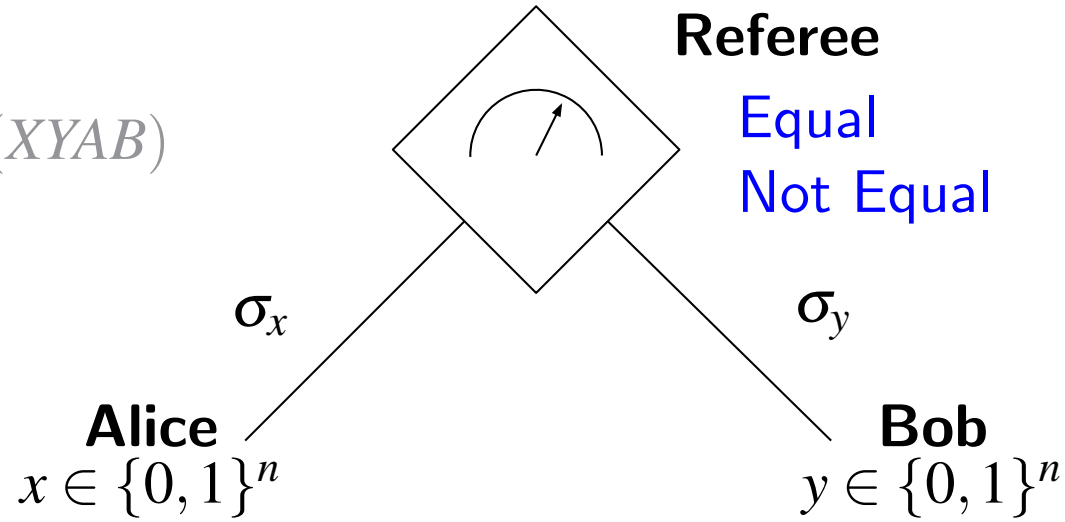
CC=Communication Cost $= \log\dim(A) + \log\dim(B)$

QIL=Information Leakage $= \sup_P \mathrm{I}(XY;AB)_{\rho_P}$

Where: $\rho_P = \sum_{x,y\in\{0,1\}^n} P(x,y)|xy\rangle\langle xy| \otimes \sigma_x^A \otimes \sigma_y^B$

$P \in \Pr(\{0,1\}^n \times \{0,1\}^n)$

$\mathrm{I}(XY;AB) = \mathrm{H}(XY) + \mathrm{H}(AB) - \mathrm{H}(XYAB)$



Quantum fingerprinting

Classical CC, QIL $\Omega(\sqrt{n})$
Quantum CC, QIL $O(\log n)$

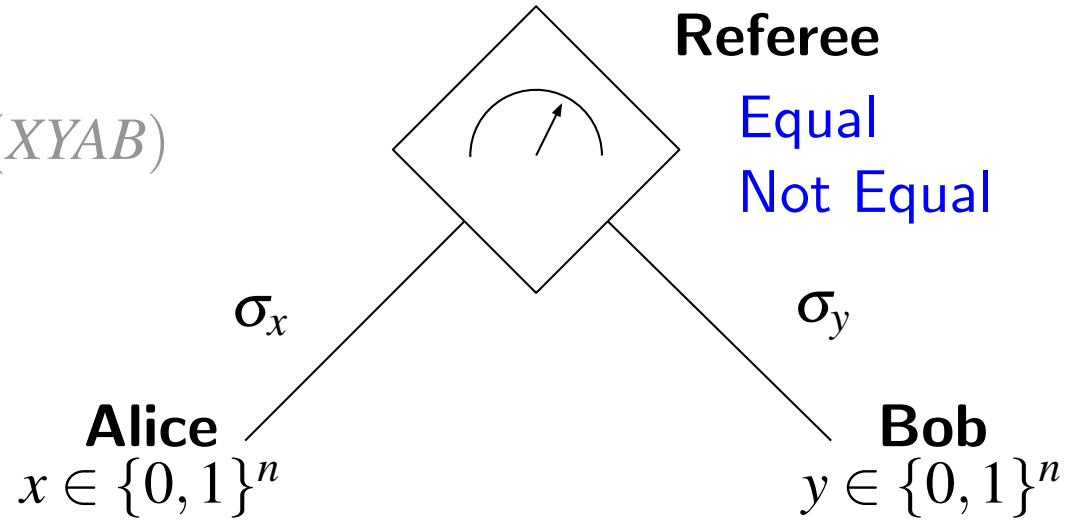
CC=Communication Cost $= \log\dim(A) + \log\dim(B)$

QIL=Information Leakage $= \sup_P \mathrm{I}(XY;AB)_{\rho_P}$

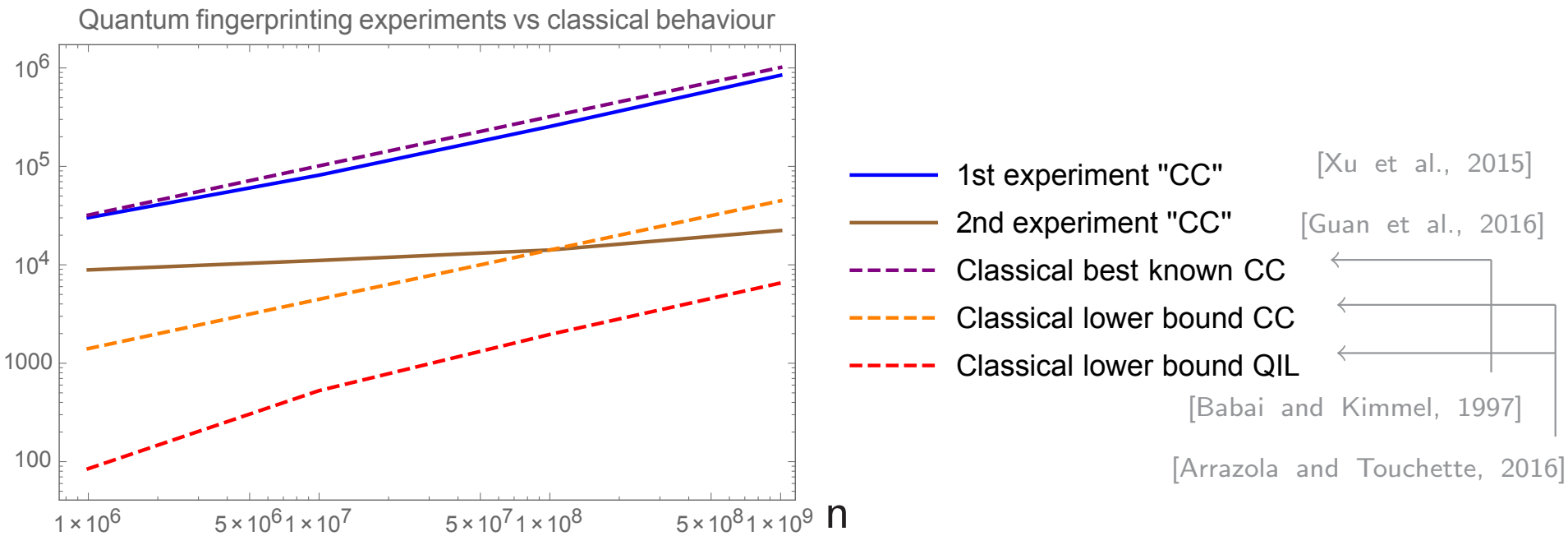
Where: $\rho_P = \sum_{x,y\in\{0,1\}^n} P(x,y)|xy\rangle\langle xy| \otimes \sigma_x^A \otimes \sigma_y^B$

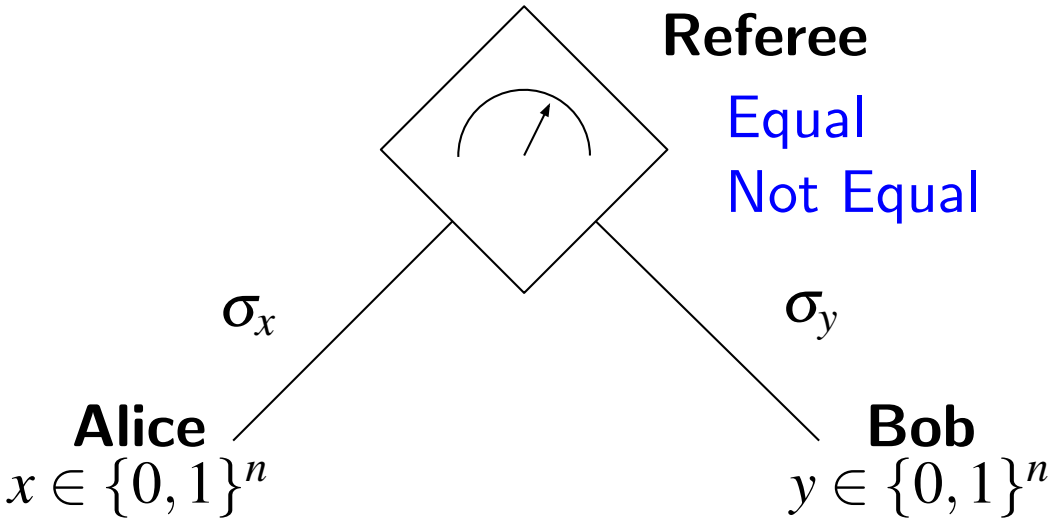
$P \in \Pr(\{0,1\}^n \times \{0,1\}^n)$

$\mathrm{I}(XY;AB) = \mathrm{H}(XY) + \mathrm{H}(AB) - \mathrm{H}(XYAB)$



Optical quantum fingerprinting experiments





Practical quantum fingerprinting

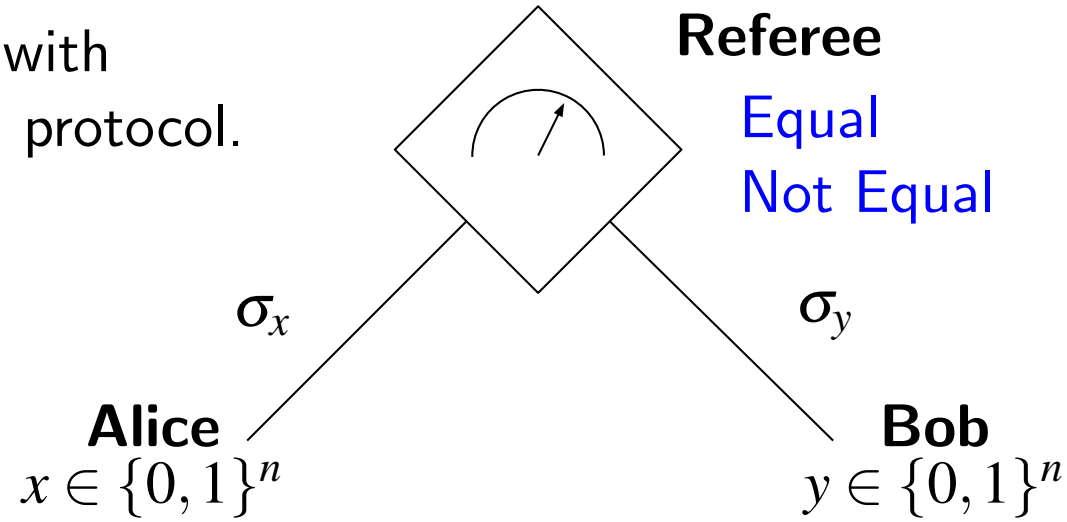
Existing protocols:

- Original protocol: a few high-dimensional signals [Buhrman et al., 2001]
- Optical protocol: many low-dimensional signals. [Arrazola and Lütkenhaus, 2014]

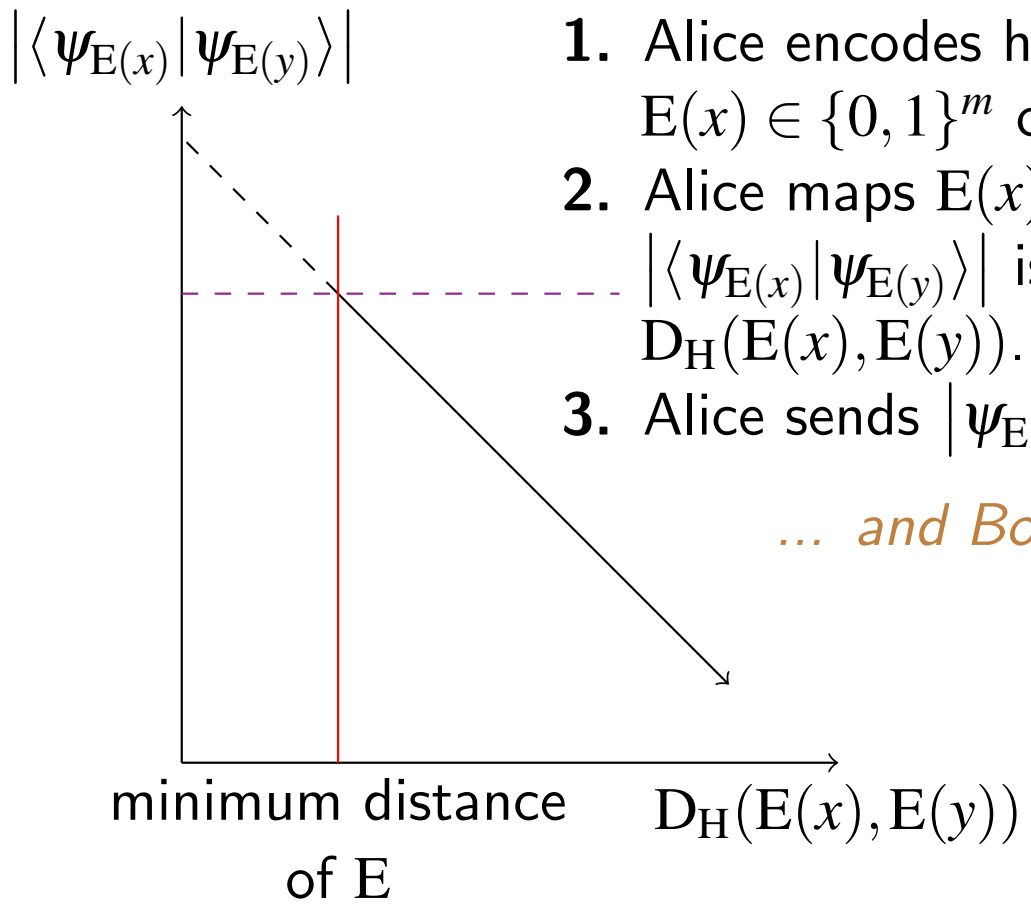
Our results:

- Family of protocols which interpolate between original and optical protocols, demonstrates trade-off between number of signals and dimension of each signal.
- Coherent state protocols with fewer signals than optical protocol.

signals=tensor factors of product states σ_x^A and σ_y^B



Quantum fingerprinting

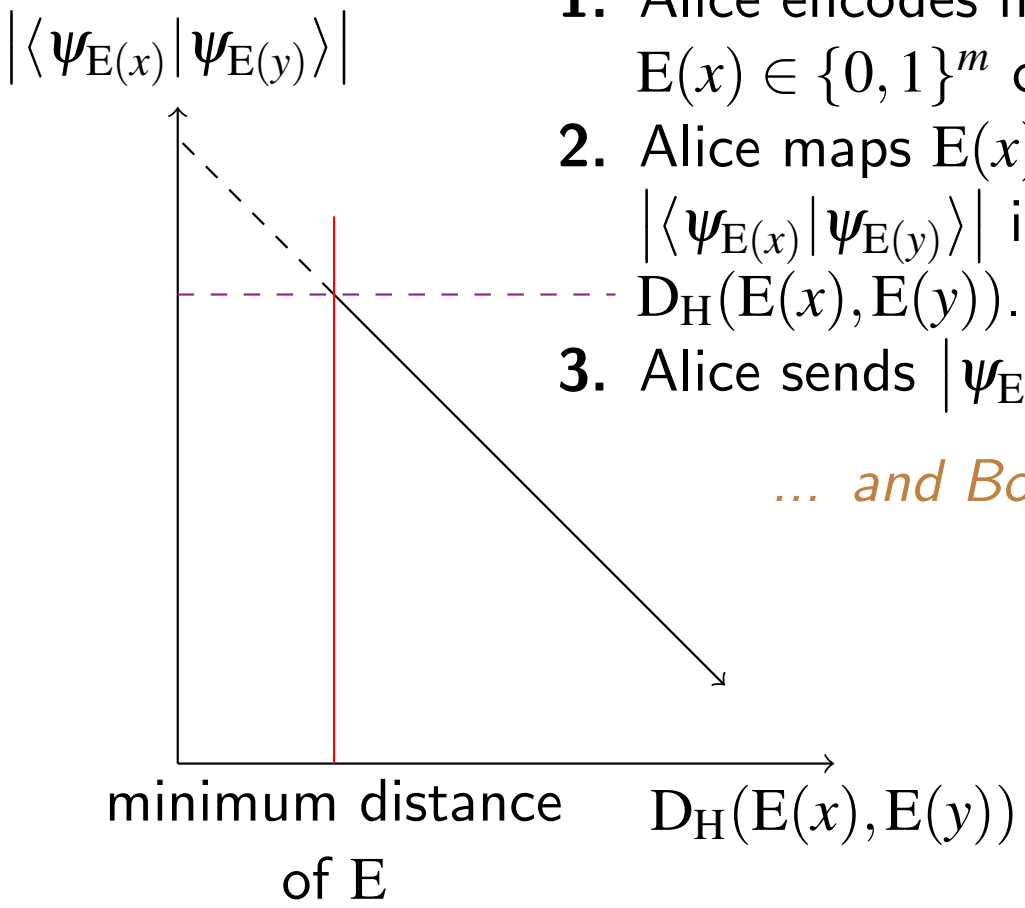


General protocol:

1. Alice encodes her input $x \in \{0,1\}^n$ into a codeword $\mathrm{E}(x) \in \{0,1\}^m$ of an error-correcting code E.
2. Alice maps $\mathrm{E}(x)$ to a state $\left|\psi_{\mathrm{E}(x)}\right\rangle$ for which $\left|\langle\psi_{\mathrm{E}(x)}|\psi_{\mathrm{E}(y)}\rangle\right|$ is a decreasing function of $\mathrm{D_H}(\mathrm{E}(x),\mathrm{E}(y))$.
3. Alice sends $\left|\psi_{\mathrm{E}(x)}\right\rangle$ to the referee.

... and Bob does the same with his input y

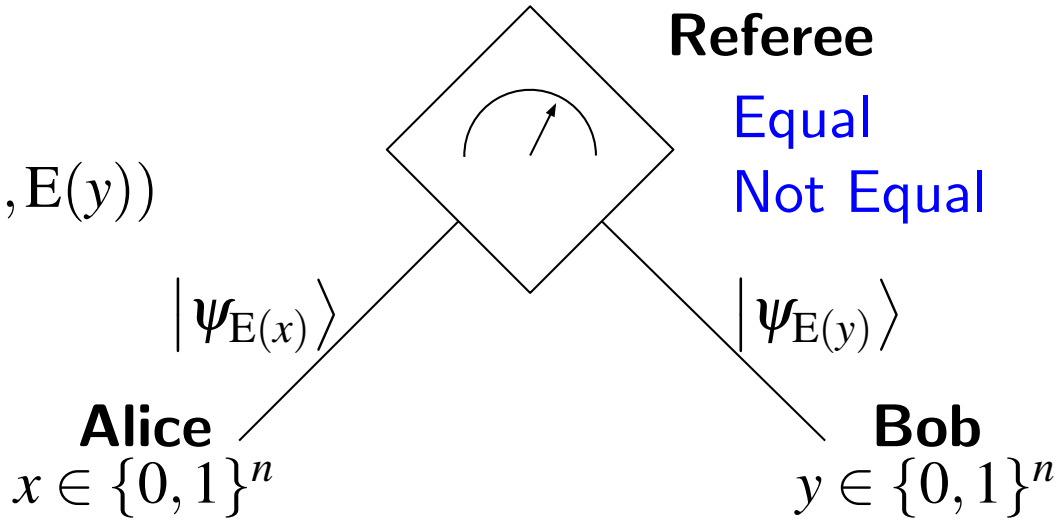
Quantum fingerprinting



General protocol:

1. Alice encodes her input $x \in \{0,1\}^n$ into a codeword $\mathrm{E}(x) \in \{0,1\}^m$ of an error-correcting code E.
2. Alice maps $\mathrm{E}(x)$ to a state $\left|\psi_{\mathrm{E}(x)}\right\rangle$ for which $\left|\langle\psi_{\mathrm{E}(x)}|\psi_{\mathrm{E}(y)}\rangle\right|$ is a decreasing function of $\mathrm{D_H}(\mathrm{E}(x),\mathrm{E}(y))$.
3. Alice sends $\left|\psi_{\mathrm{E}(x)}\right\rangle$ to the referee.

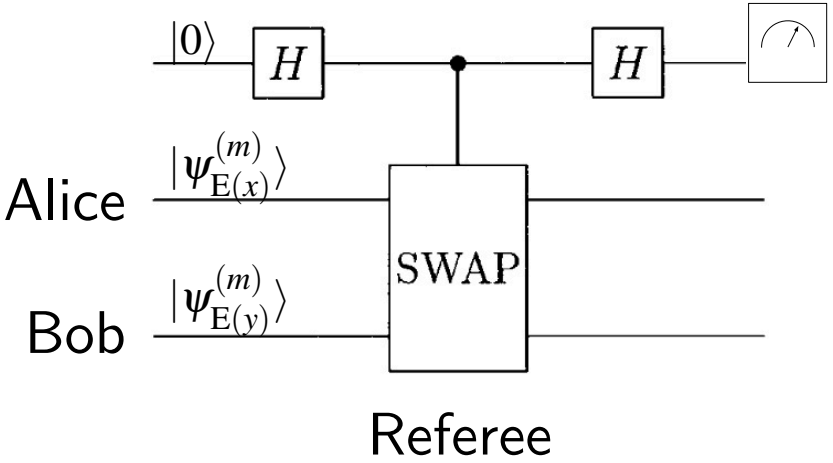
... and Bob does the same with his input y



Remember $\mathrm{E}(x) \in \{0,1\}^m$ and $m = O(n)$.

Original protocol

$$\left|\psi^{(m)}_{\mathrm{E}(x)}\right\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle\,|\mathrm{E}(x)_i\rangle$$



[Buhrman et al., 2001]

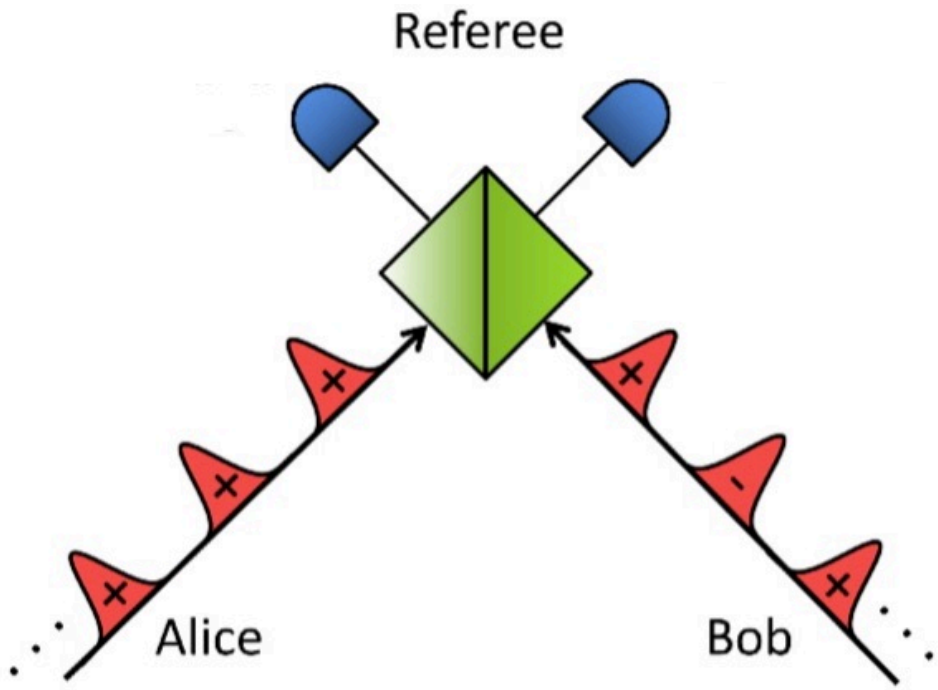
# signals	Signal dimension	Information leakage
$O(1)$	$O(n)$	$O(\log n)$

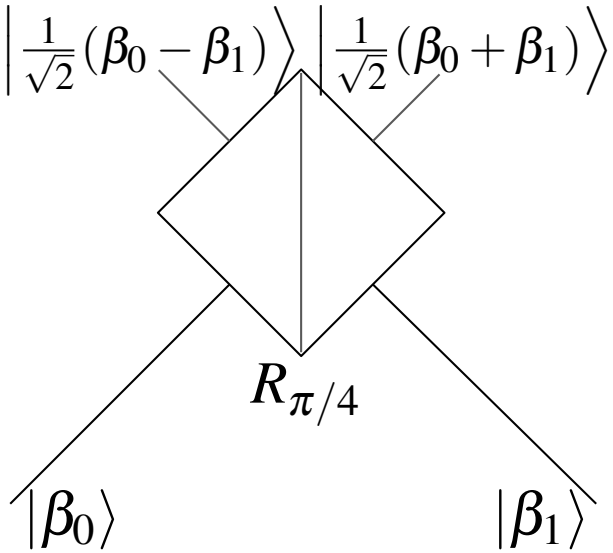
Remember $\mathrm{E}(x) \in \{0,1\}^m$ and $m = O(n)$.

Optical protocol

$$|\beta\rangle := e^{\frac{-|\beta|^2}{2}} \sum_{N=0}^{\infty} \frac{\beta^N}{\sqrt{N!}} |N\rangle$$

$$\left|\psi^{(1)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{i=1}^{m} \left|(-1)^{\mathrm{E}(x)_i} \frac{\alpha}{\sqrt{m}}\right\rangle_i$$





# signals	Signal dimension	Information leakage
$O(1)$	$O(n)$	$O(\log n)$
$O(n)$	2	$O(\log n)$

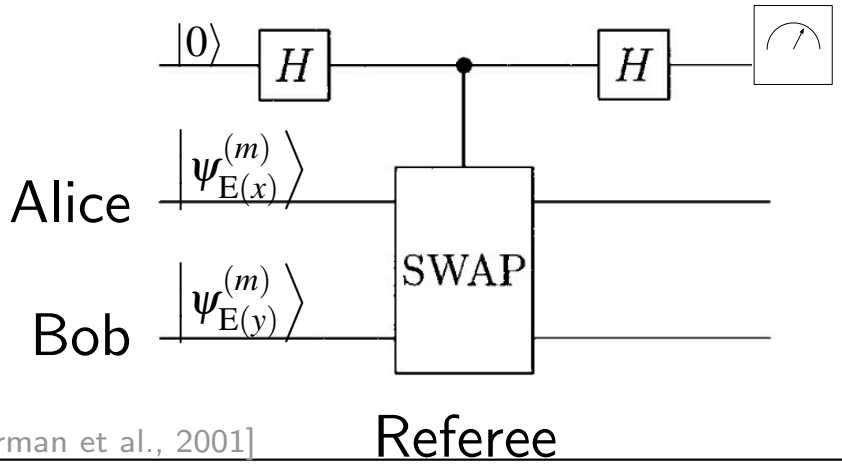
[Arrazola and Lütkenhaus, 2014]

Remember $\mathrm{E}(x) \in \{0,1\}^m$ and $m = O(n)$.

Original protocol

$$\left|\psi^{(m)}_{\mathrm{E}(x)}\right\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle\,|\mathrm{E}(x)_i\rangle$$

$$= \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle\left|q^{(m)}_{\mathrm{E}(x)_i}\right\rangle$$

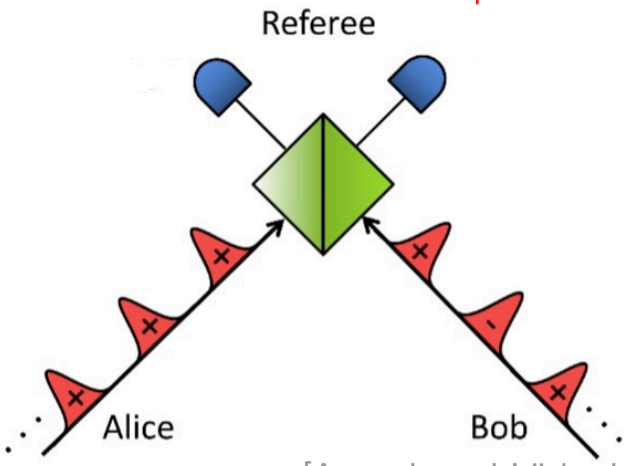


[Buhrman et al., 2001]

Optical protocol

$$\left|\psi^{(1)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{i=1}^{m}\left|(-1)^{\mathrm{E}(x)_i}\frac{\alpha}{\sqrt{m}}\right\rangle_i$$

$$\cong \bigotimes_{i=1}^{m}|i\rangle\left|q^{(1)}_{\mathrm{E}(x)_i}\right\rangle$$



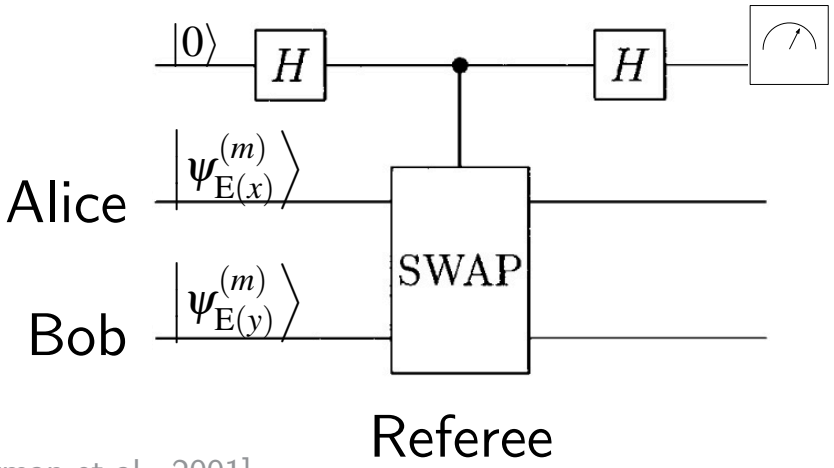
[Arrazola and Lütkenhaus, 2014]

# signals	Signal dimension	Information leakage
$O(1)$	$O(n)$	$O(\log n)$
"$O(n/k)$"	"$O(k)$"	"$O(\log n)$"
$O(n)$	2	$O(\log n)$

Remember $\mathrm{E}(x) \in \{0,1\}^m$ and $m = O(n)$.

Original protocol

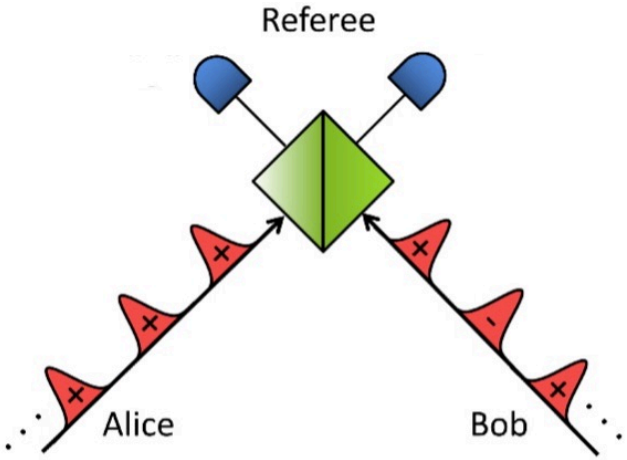
$$\left|\psi^{(m)}_{\mathrm{E}(x)}\right\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle\,|\mathrm{E}(x)_i\rangle$$
$$= \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle\left|q^{(m)}_{\mathrm{E}(x)_i}\right\rangle$$



[Buhrman et al., 2001]

Optical protocol

$$\left|\psi^{(1)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{i=1}^{m}\left|(-1)^{\mathrm{E}(x)_i}\frac{\alpha}{\sqrt{m}}\right\rangle_i$$
$$\cong \bigotimes_{i=1}^{m}|i\rangle\left|q^{(1)}_{\mathrm{E}(x)_i}\right\rangle$$



[Arrazola and Lütkenhaus, 2014]

Interpolation protocol with block-size k

$$\left|\psi^{(k)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{j=1}^{m/k}\left[\frac{1}{\sqrt{k}}\sum_{i\in\mathrm{I}[j,k]}|i\rangle\left|q^{(k)}_{\mathrm{E}(x)_i}\right\rangle\right]$$

$\mathrm{I}[j,k]$ indexes the j-th block of k bits of $\{0,1\}^m$

Measurement is combination of controlled-SWAP and beamsplitter measurements

Formally, $\mathrm{I}[j,k]$ is the set of integers in the range $[(j-1)k+1, jk]$

Original protocol

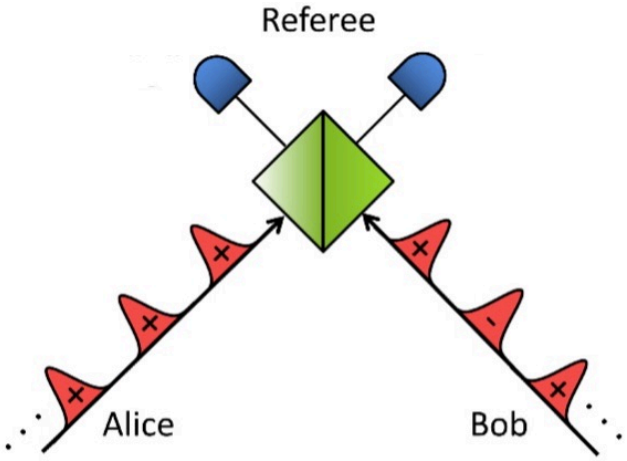
$$\left|\psi^{(m)}_{\mathrm{E}(x)}\right\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle\,|\mathrm{E}(x)_i\rangle$$
$$= \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle\left|q^{(m)}_{\mathrm{E}(x)_i}\right\rangle$$

# signals	Signal dimension	Information leakage
$O(1)$	$O(n)$	$O(\log n)$
"$O(n/k)$"	"$O(k)$"	"$O(\log n)$"
$O(n)$	2	$O(\log n)$

Remember $\mathrm{E}(x) \in \{0,1\}^m$ and $m = O(n)$.

Optical protocol

$$\left|\psi^{(1)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{i=1}^{m}\left|(-1)^{\mathrm{E}(x)_i}\frac{\alpha}{\sqrt{m}}\right\rangle_i$$
$$\cong \bigotimes_{i=1}^{m}|i\rangle\left|q^{(1)}_{\mathrm{E}(x)_i}\right\rangle$$



[Arrazola and Lütkenhaus, 2014]

Interpolation protocol with block-size k

$$\left|\psi^{(k)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{j=1}^{m/k}\left[\frac{1}{\sqrt{k}}\sum_{i\in\mathrm{I}[j,k]}|i\rangle\left|q^{(k)}_{\mathrm{E}(x)_i}\right\rangle\right]$$

$\mathrm{I}[j,k]$ indexes the j-th block of k bits of $\{0,1\}^m$

Measurement is combination of controlled-SWAP and beamsplitter measurements

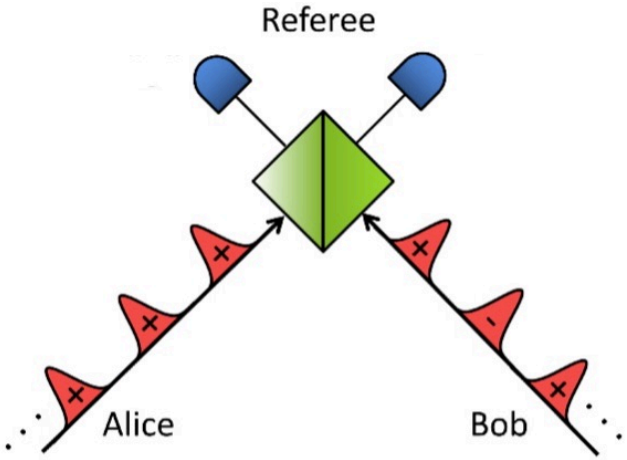
Formally, $\mathrm{I}[j,k]$ is the set of integers in the range $[(j-1)k+1, jk]$

Coherent state protocols

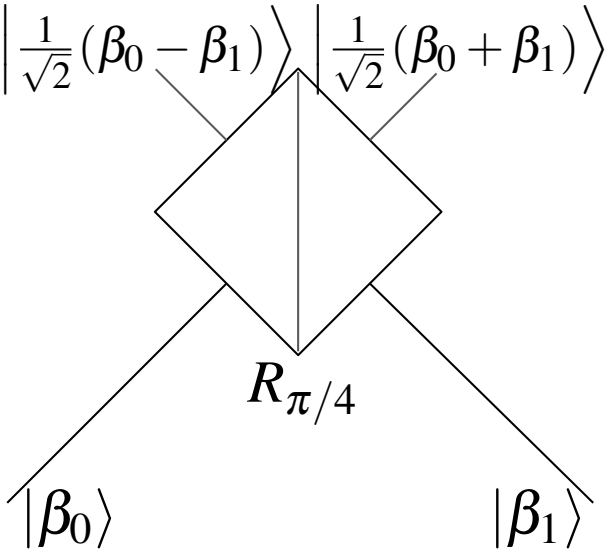
$$|\beta\rangle := e^{\frac{-|\beta|^2}{2}} \sum_{N=0}^{\infty} \frac{\beta^N}{\sqrt{N!}} |N\rangle$$

Optical protocol

$$\left|\psi^{(1)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{i=1}^{m} \left|(-1)^{\mathrm{E}(x)_i} \frac{\alpha}{\sqrt{m}}\right\rangle_i$$

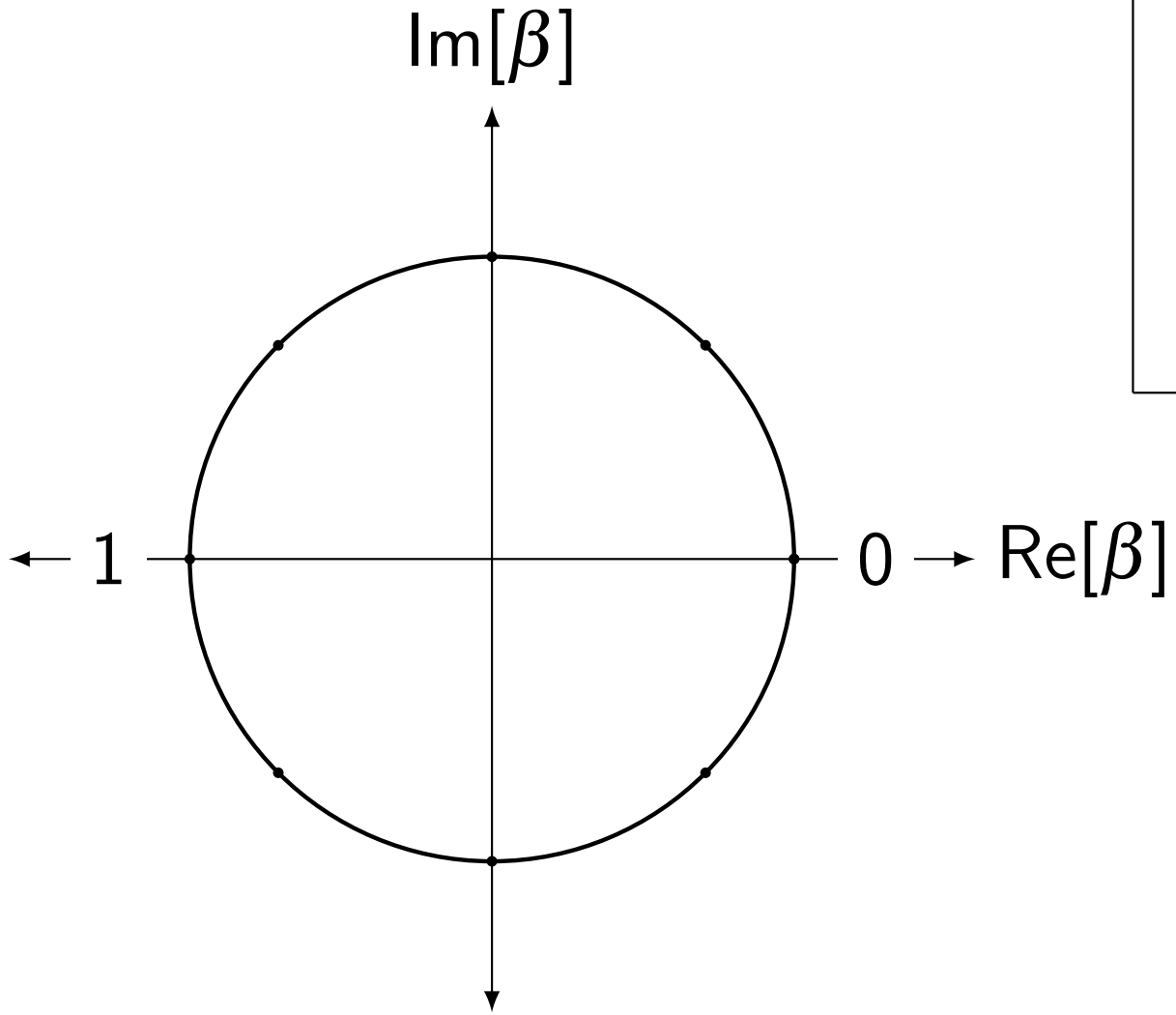


[Arrazola and Lütkenhaus, 2014]



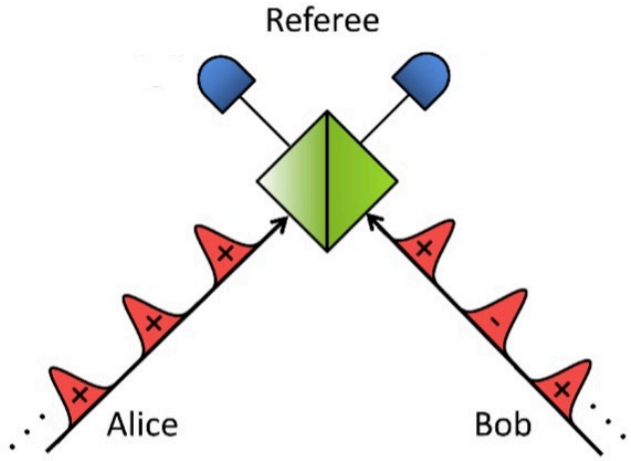
Coherent state protocols

$$|\beta\rangle := e^{\frac{-|\beta|^2}{2}} \sum_{N=0}^{\infty} \frac{\beta^N}{\sqrt{N!}} |N\rangle$$

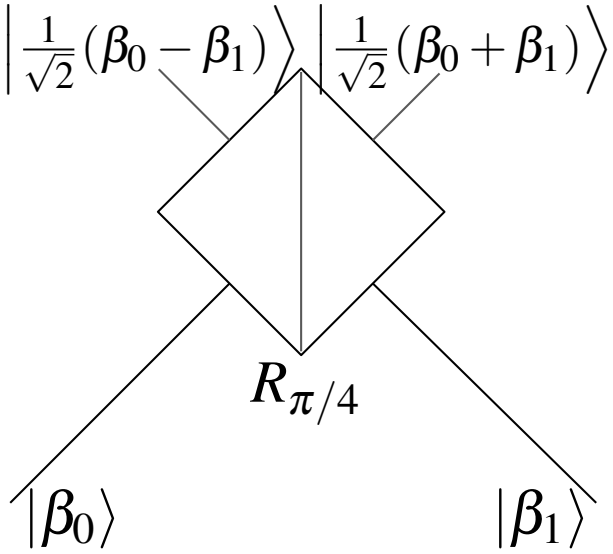


Optical protocol

$$\left|\psi^{(1)}_{\mathrm{E}(x)}\right\rangle = \bigotimes_{i=1}^{m} \left|(-1)^{\mathrm{E}(x)_i} \frac{\alpha}{\sqrt{m}}\right\rangle_i$$

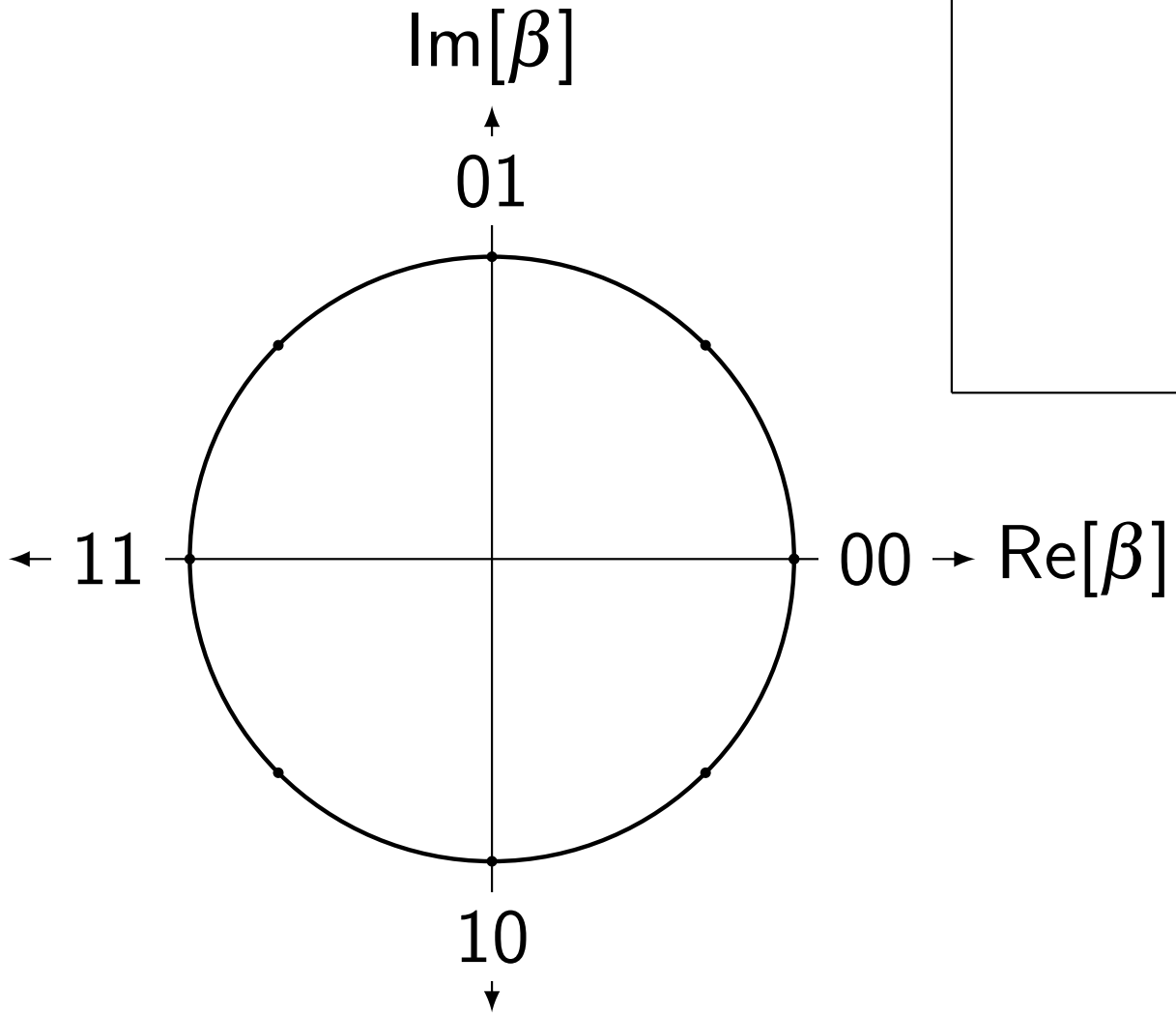


[Arrazola and Lütkenhaus, 2014]



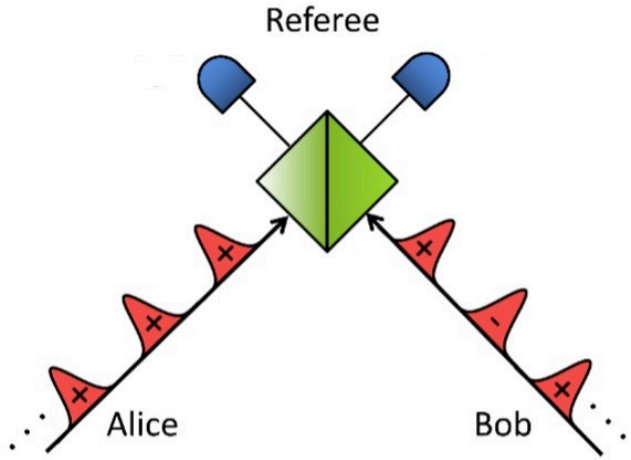
Coherent state protocols

$$|\beta\rangle := e^{\frac{-|\beta|^2}{2}} \sum_{N=0}^{\infty} \frac{\beta^N}{\sqrt{N!}} |N\rangle$$

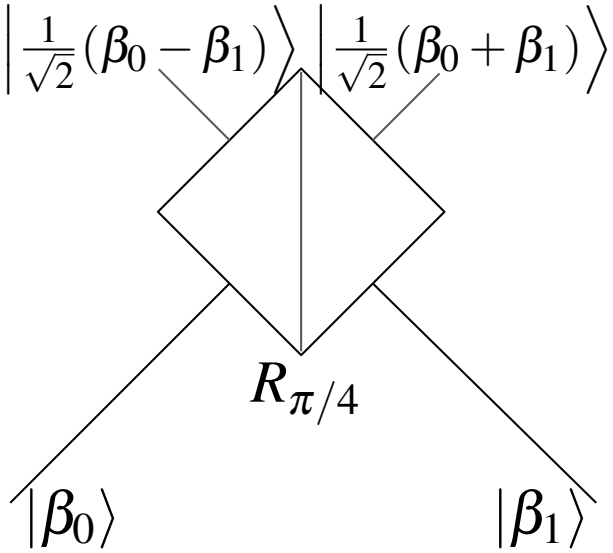


Optical protocol

$$\bigotimes_{\substack{j=1 \\ \text{odd}}}^{m} \left| (-1)^{\mathrm{E}(x)_j} \times (i)^{\mathrm{E}(x)_j \oplus \mathrm{E}(x)_{j+1}} \frac{\alpha}{\sqrt{m/2}} \right\rangle_j$$



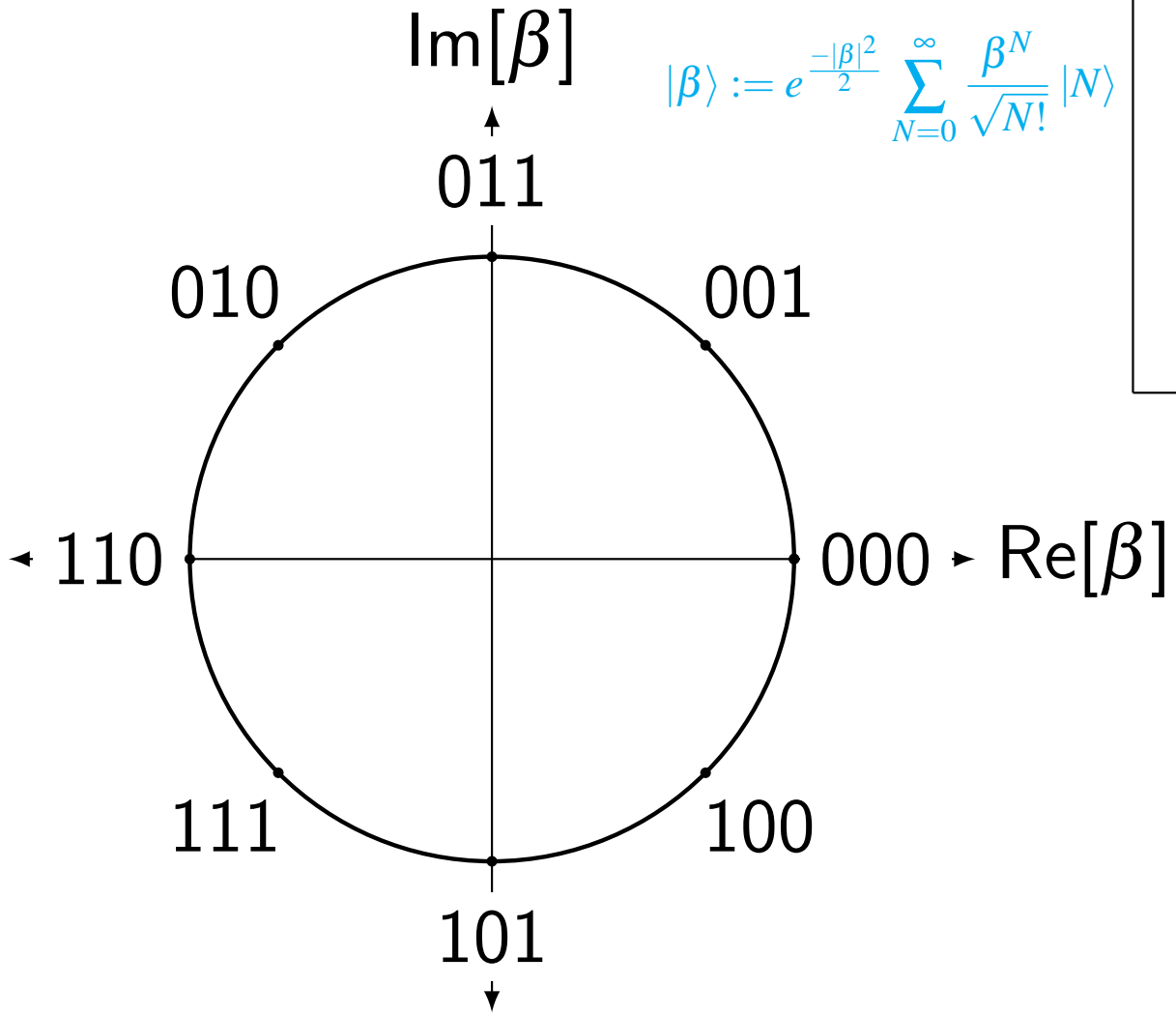
[Arrazola and Lütkenhaus, 2014]



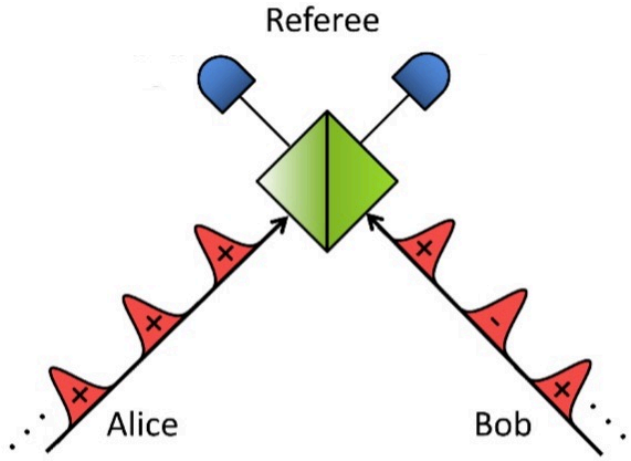
Coherent state protocols

Ring Gray coding of $k-$bit blocks for $k = 1$ (blue), $k = 2$ (blue and red), and $k = 3$ (blue, red and green):

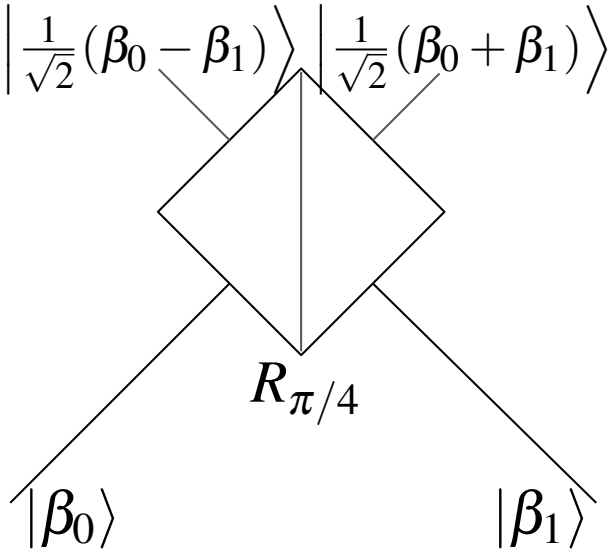
$$|\beta\rangle := e^{\frac{-|\beta|^2}{2}} \sum_{N=0}^{\infty} \frac{\beta^N}{\sqrt{N!}} |N\rangle$$



Optical protocol



[Arrazola and Lütkenhaus, 2014]



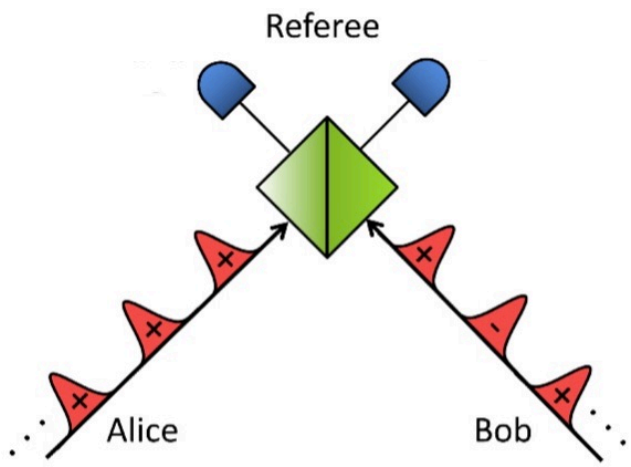
Coherent state protocols

Error $\varepsilon = 0.01$

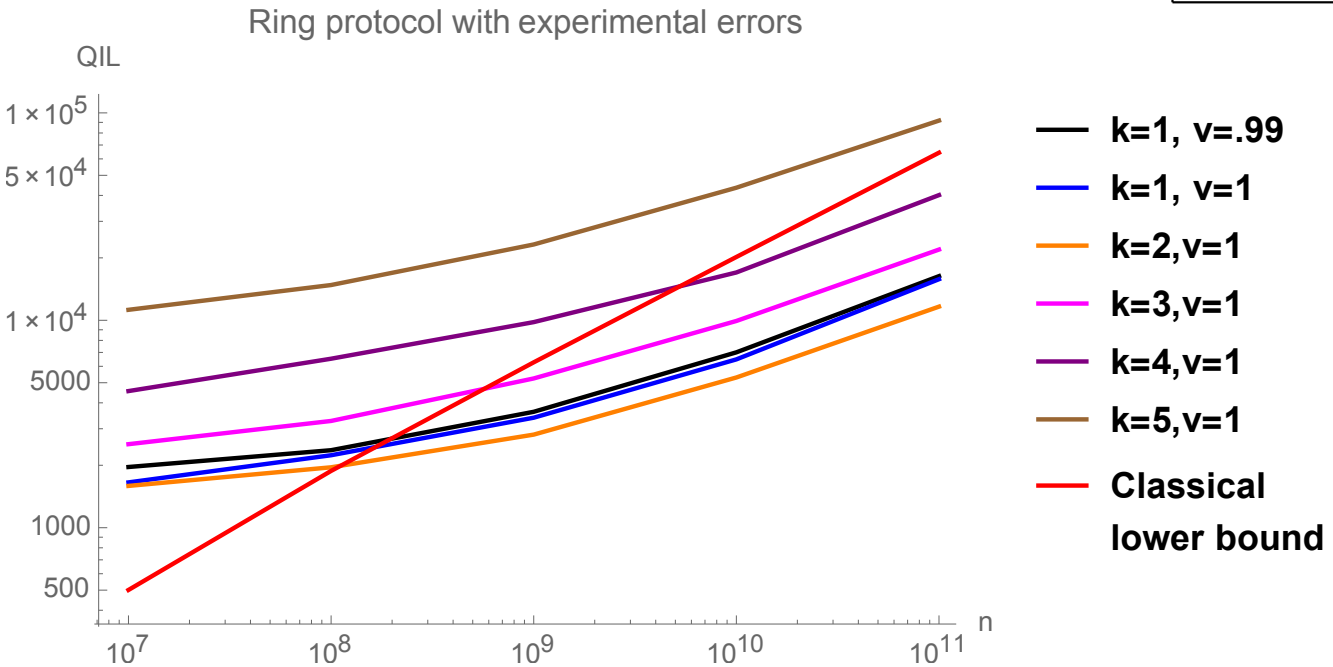
Transmittivity $\eta = 0.3$

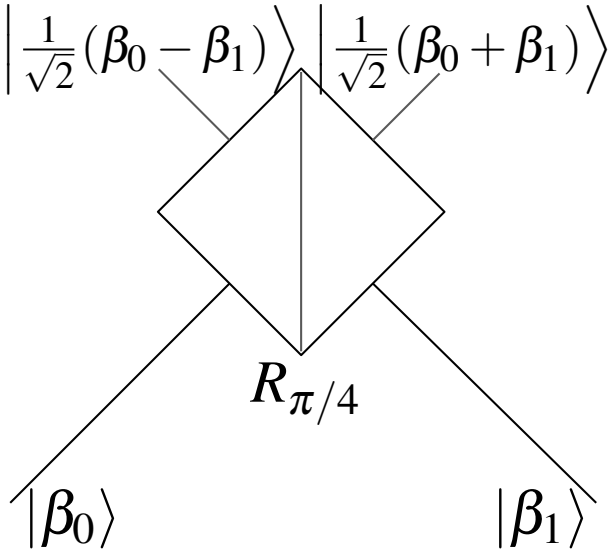
Dark count probability $p_{\mathrm{d}} = 7.3 \times 10^{-11}$

Optical protocol



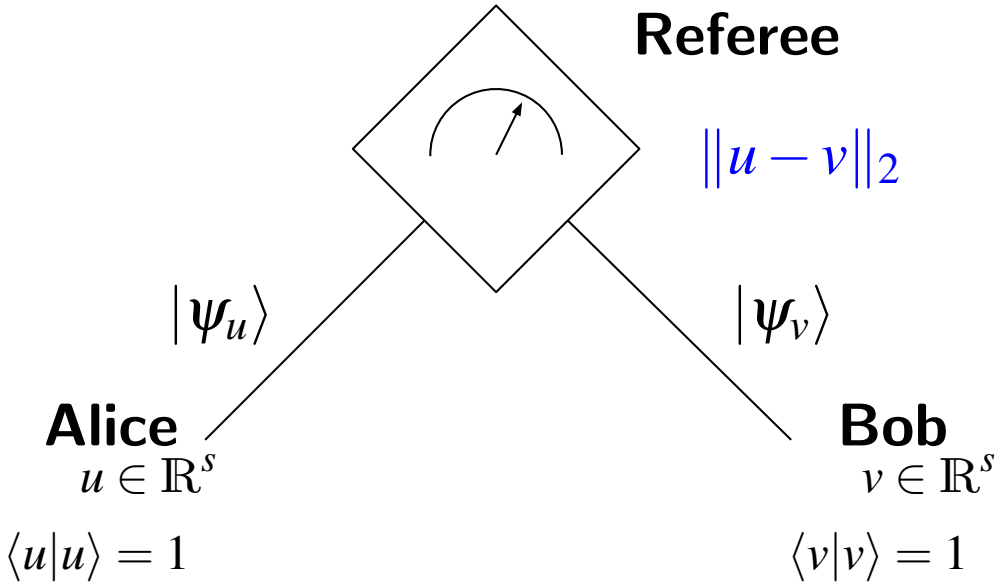
[Arrazola and Lütkenhaus, 2014]





Euclidean distance

Classical CC $\Omega(\sqrt{n})$
Quantum CC, QIL $O(\log n)$

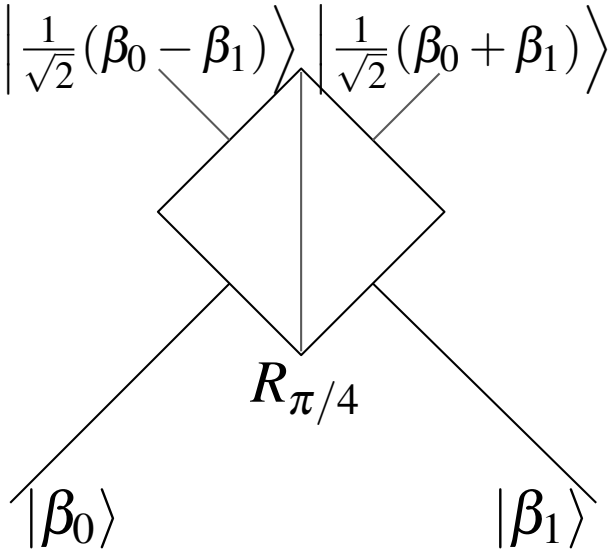


Existing optical protocol
[Kumar et al., 2017]

$$|\psi_u\rangle_1 = \bigotimes_{j=1}^{s} |u_j\alpha\rangle_j.$$

Our protocol

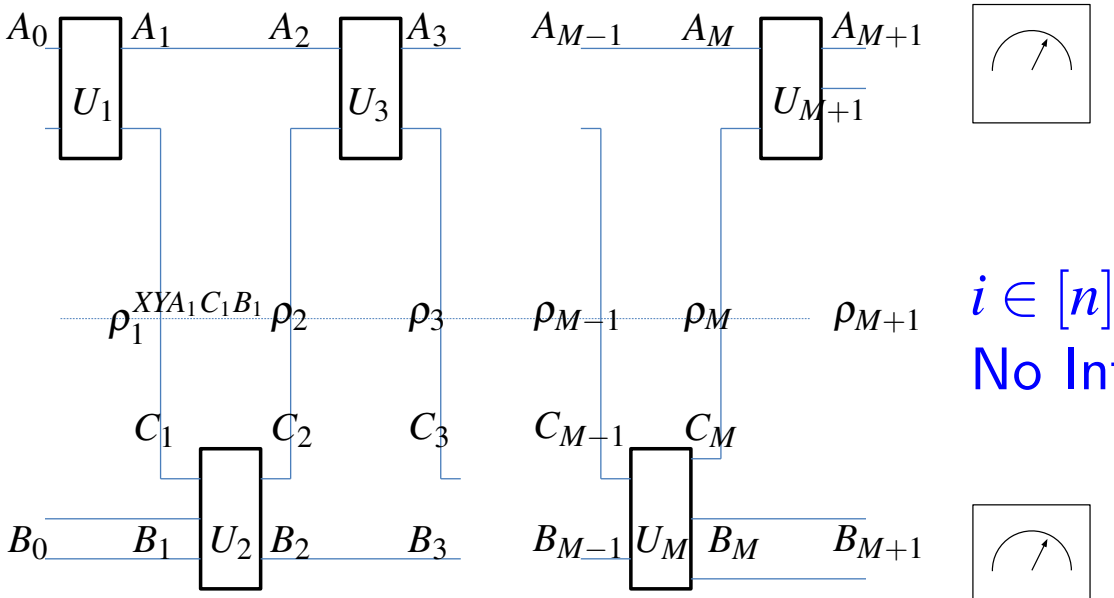
$$|\psi_u\rangle_2 = \bigotimes_{\substack{j=1\\ \text{odd}}}^{s} |(u_j + iu_{j+1})\alpha\rangle_j$$



$\|u-v\|_2$ is a function of α and the expected difference in the number of clicks in the dark port and light port detectors.

Appointment scheduling

Alice
$x \in \{0,1\}^n$

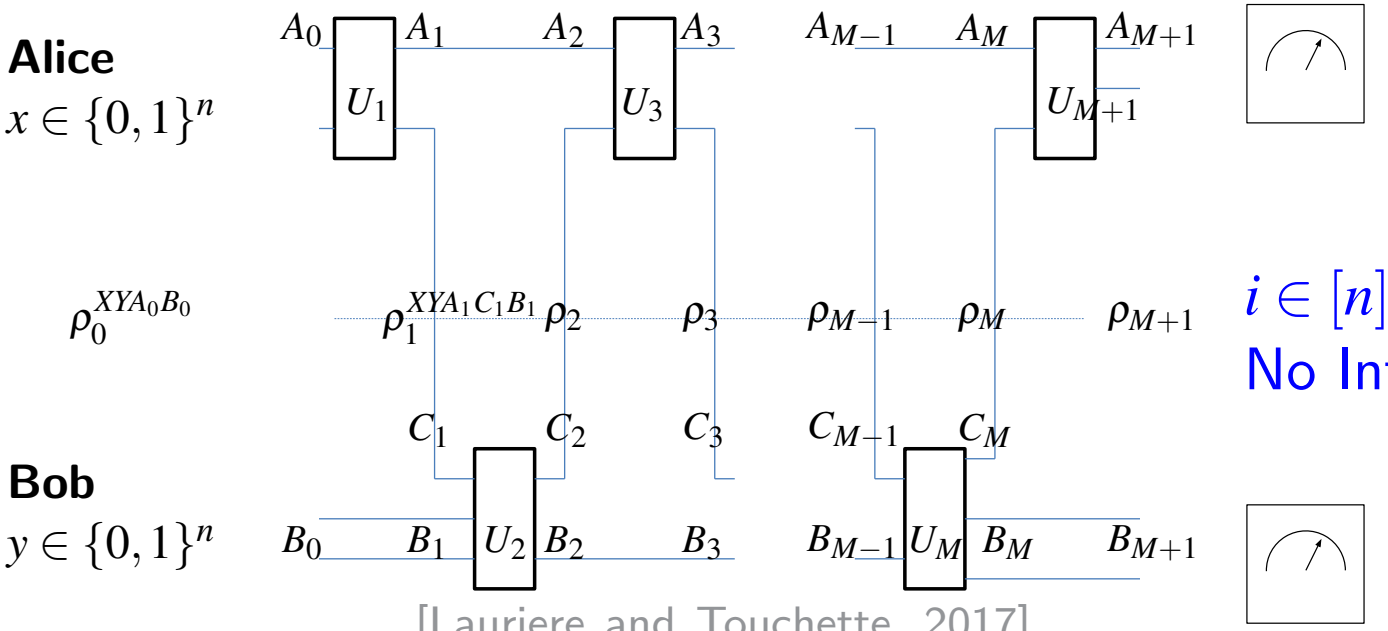


Bob
$y \in \{0,1\}^n$

[Lauriere and Touchette, 2017]

$i \in [n]$ such that $x_i = y_i = 1$
No Intersection

Appointment scheduling



[Lauriere and Touchette, 2017]

$i \in [n]$ such that $x_i = y_i = 1$
No Intersection

CC=Communication Cost= $\sum_{i=1}^{M} \log \dim(C_i)$

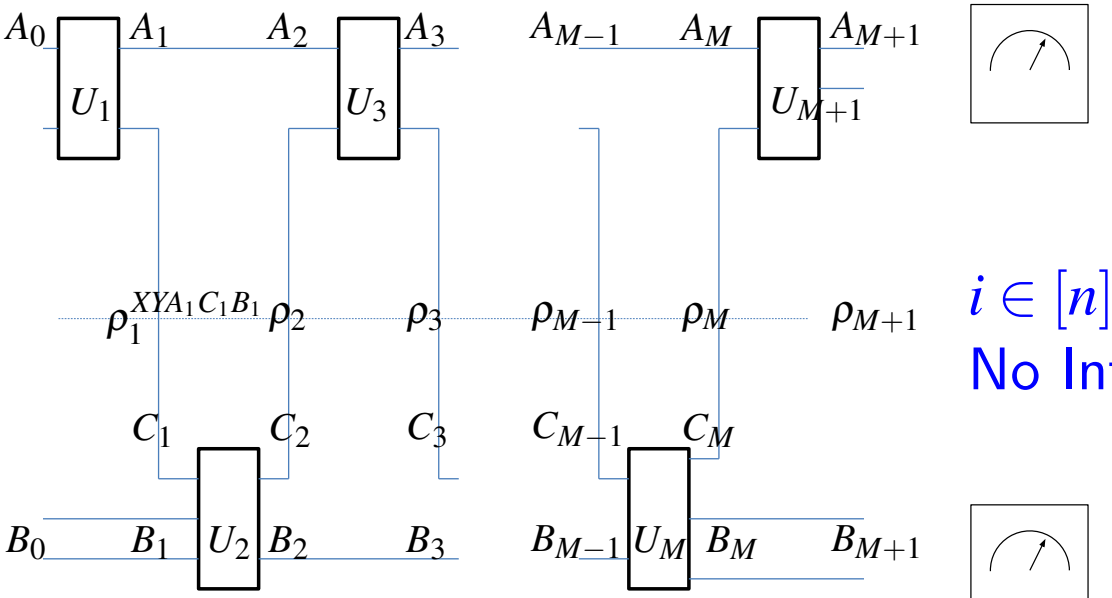
QIC=Information Cost= $\sup_P \sum_{i=1}^{M} \mathrm{I}(C_i; X|YB_i)_{\rho_i} + \mathrm{I}(C_i; Y|XA_i)_{\rho_i}$

Where: x, y distributed $\sim P \in \Pr(\{0,1\}^n \times \{0,1\}^n)$

Appointment scheduling

Classical CC, QIC $\Omega(n)$
Quantum CC, QIC $O(\sqrt{n}\log n)$

Alice
$x \in \{0,1\}^n$



Bob
$y \in \{0,1\}^n$

[Lauriere and Touchette, 2017]

$i \in [n]$ such that $x_i = y_i = 1$
No Intersection

CC=Communication Cost= $\sum_{i=1}^{M} \log \dim(C_i)$

QIC=Information Cost= $\sup_P \sum_{i=1}^{M} \mathrm{I}(C_i; X|YB_i)_{\rho_i} + \mathrm{I}(C_i; Y|XA_i)_{\rho_i}$

Where: x, y distributed $\sim P \in \Pr(\{0,1\}^n \times \{0,1\}^n)$

Practical appointment scheduling

Original protocol: [Buhrman et al., 1998]
Distributed version of Grover's search protocol with CC, QIC $O(\sqrt{n}\log n)$.

- Requires impractical states and two global unitaries: oracle calls and inversion about mean.

Our results:

1. Coherent state version of distributed Grover's search with QIC $O(\sqrt{n}\log n)$. Practical states and oracle calls, but requires global linear optics transformation for inversion about mean.
2. New protocol[†] using coherent state AND protocol on each pair of bits $x_i, y_i \in \{0, 1\}$ which is more feasible for implementation.

   Unfortunately, still requires very low loss and beamsplitters with very high transmittivity

[†] Based on a protocol in [Braverman et al., 2015].

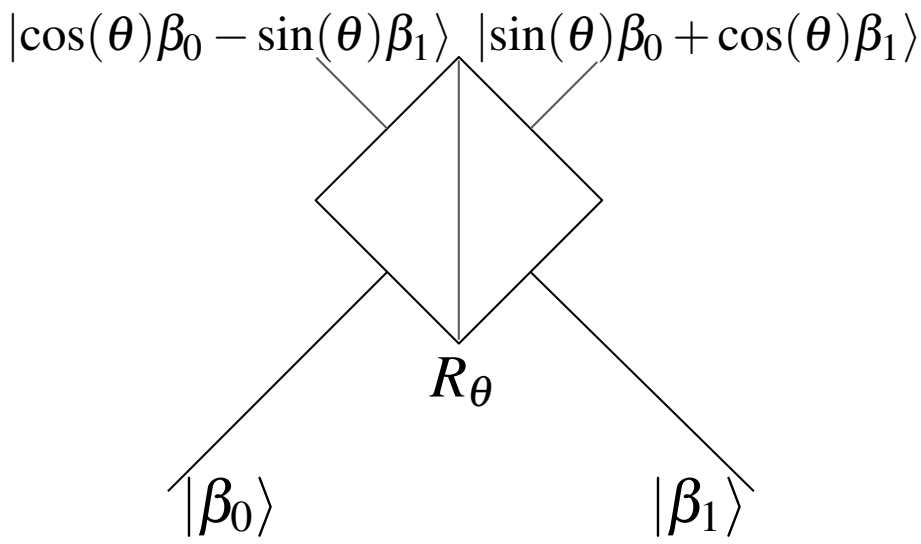
Coherent state AND protocol for appointment scheduling

Alice prepares $|\alpha\rangle|0\rangle$.
On each of the r rounds, Alice and Bob do the following:

1. On $x_i = 0$ ($x_i = 1$), Alice applies $\mathbb{1}$ ($R_{\frac{\pi}{2r}}$) and sends the transformed state to Bob.
2. On $y_i = 0$, Bob destroys the state received and sends $|\alpha\rangle|0\rangle$ to Alice. On $y_i = 1$, Bob applies $\mathbb{1}$ and returns the state to Alice.

After r rounds, Alice measures both modes with single photon threshold detectors and communicates the result to Bob.

$|0\rangle|\alpha\rangle$ **On (0,0) and (0,1)**



$\longrightarrow |\alpha\rangle|0\rangle$

Coherent state AND protocol for appointment scheduling

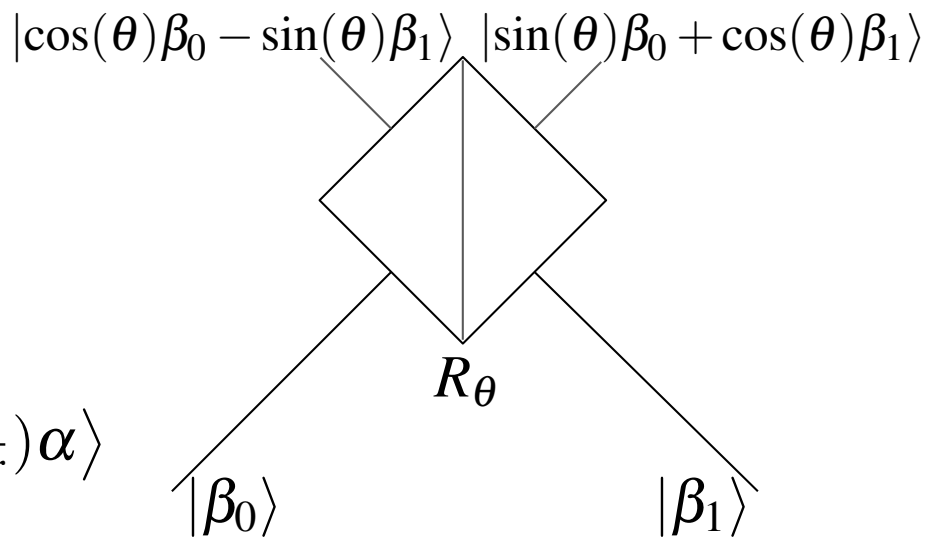
Alice prepares $|\alpha\rangle|0\rangle$.
On each of the r rounds, Alice and Bob do the following:

1. On $x_i = 0$ ($x_i = 1$), Alice applies $\mathbb{1}$ ($R_{\frac{\pi}{2r}}$) and sends the transformed state to Bob.
2. On $y_i = 0$, Bob destroys the state received and sends $|\alpha\rangle|0\rangle$ to Alice. On $y_i = 1$, Bob applies $\mathbb{1}$ and returns the state to Alice.

After r rounds, Alice measures both modes with single photon threshold detectors and communicates the result to Bob.

$|0\rangle|\alpha\rangle$

On (1,0)



$|\cos(\frac{\pi}{2r})\alpha\rangle|\sin(\frac{\pi}{2r})\alpha\rangle$

$|\alpha\rangle|0\rangle$

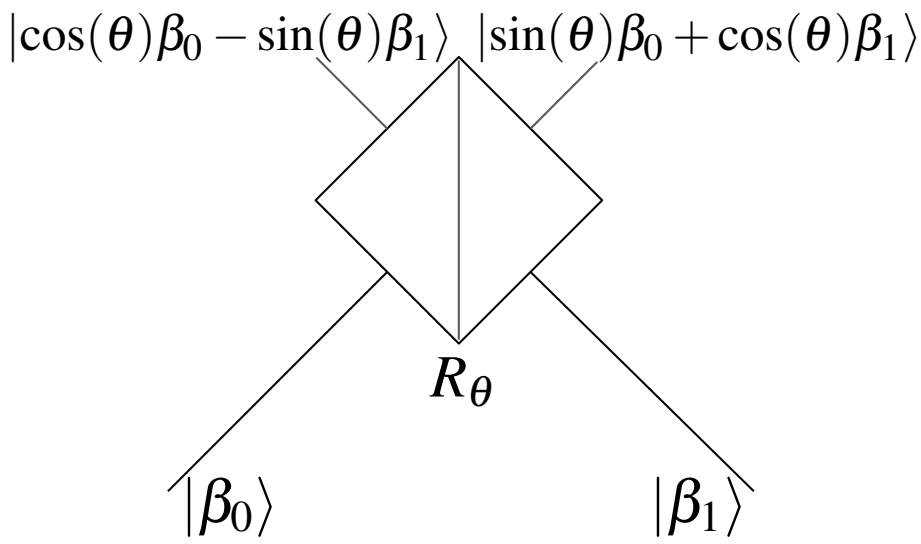
Coherent state AND protocol for appointment scheduling

Alice prepares $|\alpha\rangle|0\rangle$.
On each of the r rounds, Alice and Bob do the following:

1. On $x_i = 0$ ($x_i = 1$), Alice applies $\mathbb{1}$ ($R_{\frac{\pi}{2r}}$) and sends the transformed state to Bob.
2. On $y_i = 0$, Bob destroys the state received and sends $|\alpha\rangle|0\rangle$ to Alice. On $y_i = 1$, Bob applies $\mathbb{1}$ and returns the state to Alice.

After r rounds, Alice measures both modes with single photon threshold detectors and communicates the result to Bob.

$|0\rangle|\alpha\rangle$ **On (1,0)**



$\longrightarrow |\alpha\rangle|0\rangle$

Coherent state AND protocol for appointment scheduling

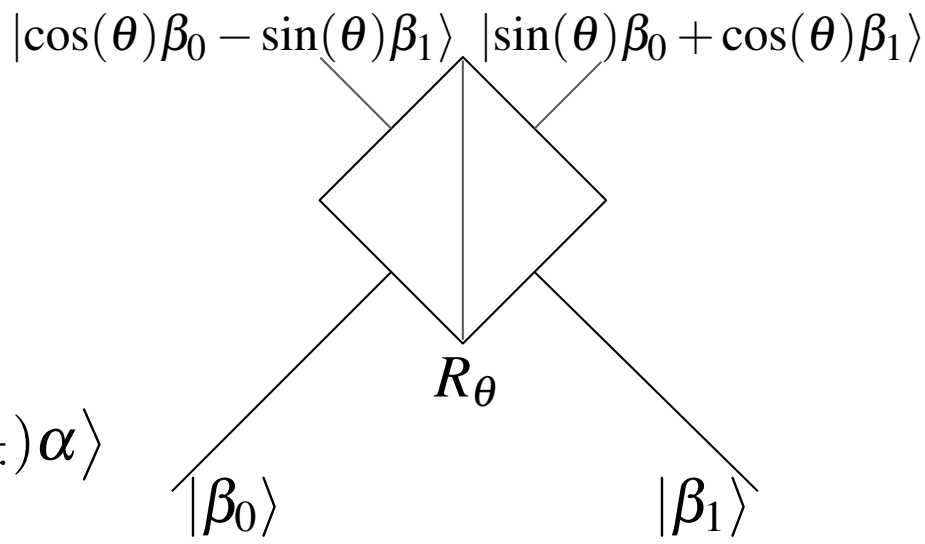
Alice prepares $|\alpha\rangle|0\rangle$.
On each of the r rounds, Alice and Bob do the following:

1. On $x_i = 0$ ($x_i = 1$), Alice applies $\mathbb{1}$ ($R_{\frac{\pi}{2r}}$) and sends the transformed state to Bob.
2. On $y_i = 0$, Bob destroys the state received and sends $|\alpha\rangle|0\rangle$ to Alice. On $y_i = 1$, Bob applies $\mathbb{1}$ and returns the state to Alice.

After r rounds, Alice measures both modes with single photon threshold detectors and communicates the result to Bob.

$|0\rangle|\alpha\rangle$

On (1,1)



$|\cos(\frac{\pi}{2r})\alpha\rangle|\sin(\frac{\pi}{2r})\alpha\rangle$

$|\alpha\rangle|0\rangle$

Coherent state AND protocol for appointment scheduling

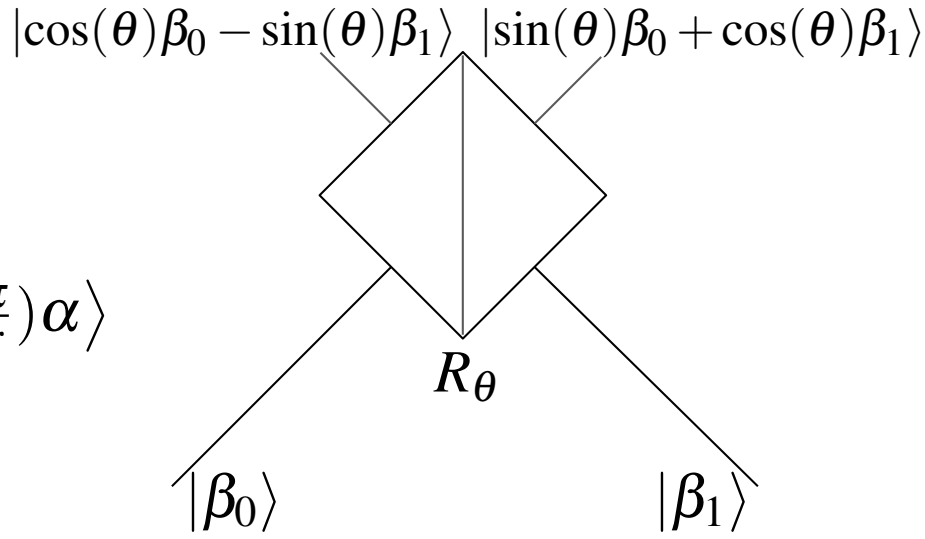
Alice prepares $|\alpha\rangle|0\rangle$.
On each of the r rounds, Alice and Bob do the following:

1. On $x_i = 0$ ($x_i = 1$), Alice applies $\mathbb{1}$ ($R_{\frac{\pi}{2r}}$) and sends the transformed state to Bob.
2. On $y_i = 0$, Bob destroys the state received and sends $|\alpha\rangle|0\rangle$ to Alice. On $y_i = 1$, Bob applies $\mathbb{1}$ and returns the state to Alice.

After r rounds, Alice measures both modes with single photon threshold detectors and communicates the result to Bob.

$|0\rangle|\alpha\rangle$

On (1,1)



$\left|\cos(\frac{2\pi}{2r})\alpha\right\rangle\left|\sin(\frac{2\pi}{2r})\alpha\right\rangle$

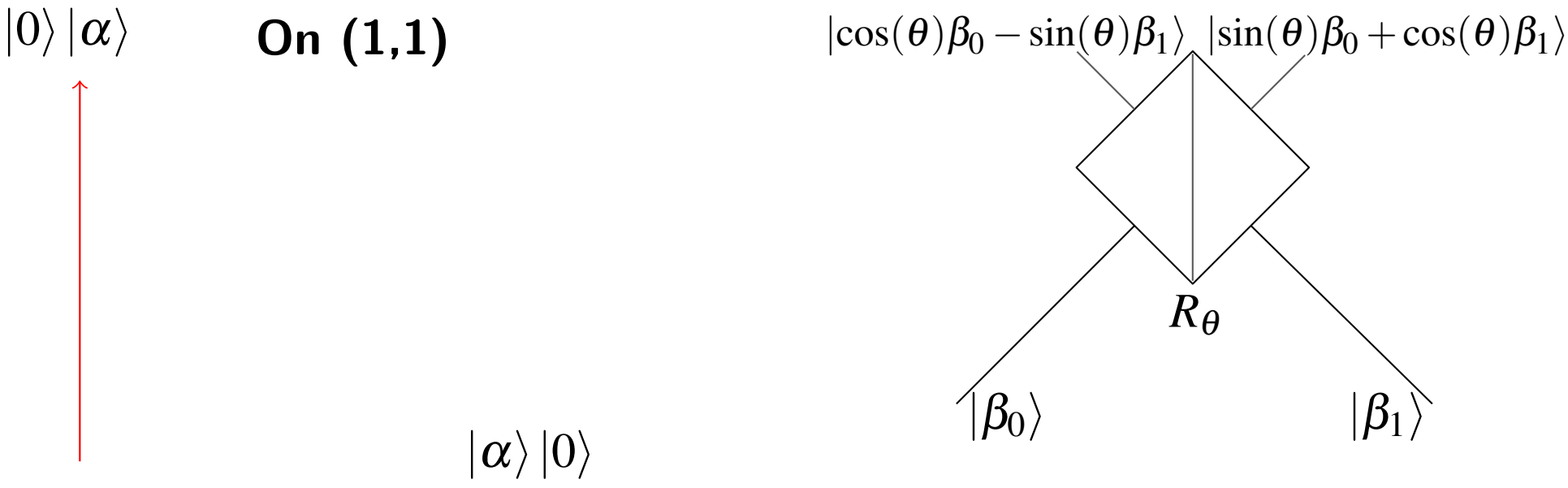
$|\alpha\rangle|0\rangle$

Coherent state AND protocol for appointment scheduling

Alice prepares $|\alpha\rangle|0\rangle$.
On each of the r rounds, Alice and Bob do the following:

1. On $x_i = 0$ ($x_i = 1$), Alice applies $\mathbb{1}$ ($R_{\frac{\pi}{2r}}$) and sends the transformed state to Bob.
2. On $y_i = 0$, Bob destroys the state received and sends $|\alpha\rangle|0\rangle$ to Alice. On $y_i = 1$, Bob applies $\mathbb{1}$ and returns the state to Alice.

After r rounds, Alice measures both modes with single photon threshold detectors and communicates the result to Bob.



Intuition for why our AND protocol exchanges low information

1. For any AND protocol, if a party (say, Bob) has $y_i = 1$, then they will learn the other party's bit.
2. But if a party (say, Bob) has $y_i = 0$, our protocol ensures they obtain very little information about x_i if the states $|\alpha\rangle|0\rangle$ and $\left|\cos(\frac{\pi}{2r})\alpha\right\rangle\left|\sin(\frac{\pi}{2r})\alpha\right\rangle$ are highly non-orthogonal.
3. To make these states highly non-orthogonal, the number of rounds r must be high, so low loss is required.

$$\left|\cos(\tfrac{\pi}{2r})\alpha\right\rangle\left|\sin(\tfrac{\pi}{2r})\alpha\right\rangle$$

$$|\alpha\rangle|0\rangle$$

QIC of coherent state bitwise AND appointment scheduling protocol

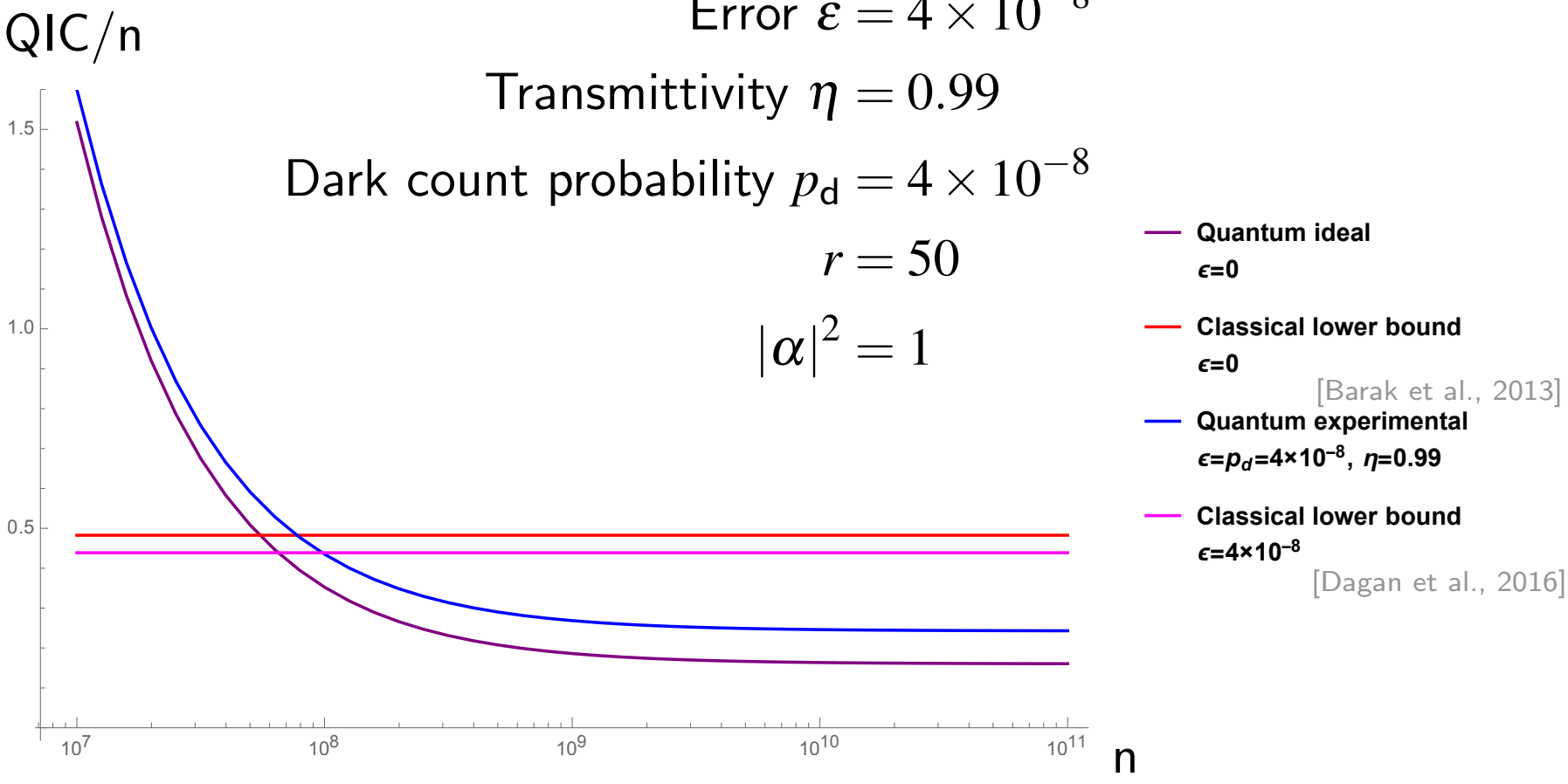
Error $\varepsilon = 4 \times 10^{-8}$

Transmittivity $\eta = 0.99$

Dark count probability $p_{\mathrm{d}} = 4 \times 10^{-8}$

$r = 50$

$|\alpha|^2 = 1$



Arrazola, J. M. and Lütkenhaus, N. (2014).

Quantum fingerprinting with coherent states and a constant mean number of photons.
Phys. Rev. A, 89:062305.

Arrazola, J. M. and Touchette, D. (2016).

Quantum advantage on information leakage for equality.
arXiv:quant-ph/1607.07516.

Babai, L. and Kimmel, P. G. (1997).

Randomized simultaneous messages: Solution of a problem of Yao in communication complexity.
In *Proceedings of the 12th Annual IEEE Conference on Computational Complexity*, CCC '97, Washington, DC, USA. IEEE Computer Society.

Barak, B., Braverman, M., Chen, X., and Rao, A. (2013).

How to compress interactive communication.
SIAM Journal on Computing, 42(3):1327–1363.

Braverman, M., Garg, A., Ko, Y. K., Mao, J., and Touchette, D. (2015).

Near-optimal bounds on bounded-round quantum communication complexity of disjointness.
In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, pages 773–791. IEEE.

Buhrman, H., Cleve, R., Watrous, J., and de Wolf, R. (2001).

Quantum fingerprinting.
Phys. Rev. Lett., 87:167902.

Buhrman, H., Cleve, R., and Wigderson, A. (1998).

Quantum vs. classical communication and computation.
In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 63–68, New York, NY, USA. ACM.

Dagan, Y., Filmus, Y., Hatami, H., and Li, Y. (2016).

Trading information complexity for error.
arXiv:quant-ph/1611.06650.

Guan, J.-Y., Xu, F., Yin, H.-L., Li, Y., Zhang, W.-J., Chen, S.-J., Yang, X.-Y., Li, L., You, L.-X., Chen, T.-Y., Wang, Z., Zhang, Q., and Pan, J.-W. (2016).

Observation of quantum fingerprinting beating the classical limit.
Phys. Rev. Lett., 116:240502.

Kumar, N., Diamanti, E., and Kerenidis, I. (2017).

Efficient quantum communications with coherent state fingerprints over multiple channels.
Phys. Rev. A, 95:032337.

Lauriere, M. and Touchette, D. (2017).

The flow of information in interactive quantum protocols: the cost of forgetting.
arXiv:quant-ph/1701.02062.

Xu, F., Arrazola, J. M., Wei, K., Wang, W., Palacios-Avila, P., Feng, C., Sajeed, S., Lütkenhaus, N., and Lo, H.-K. (2015).

Experimental quantum fingerprinting with weak coherent pulses.
Nature communications, 6.