

Local Transformations of Quantum States Requiring Infinite Rounds of Classical Communication

Eric Chitambar
(CQIQC) University of Toronto

IQC Colloquium
February 28, 2011

The Problem of Investigation:

For a system of fixed dimensions and variable number of rounds n , how does the power of LOCC increase as a function of n ?

Outline

- Description of LOCC and terminology
- Discussion of previous work
- Fortescue & Lo Random Distillation Protocol
- Modify Random Distillation Protocol
 - $LOCC_{n+2} > LOCC_n$
 - $LOCC_\infty$

Local Operations and Classical Communication (LOCC)



Alice



Alice and Bob share bipartite state $|\psi\rangle_{AB}$.



Bob the

$$\{A_0, A_1\} \downarrow \left(A_1^{(A_0)} \otimes A_0^{(A_1)} \right) \text{ or } \left(A_1^{(A_0)} \otimes A_0^{(A_1)} \right) |\psi\rangle \left(B_0^{(B_1)} \dots B_1 B_0^{(B_0)} \right)$$

$$\left\{ \omega_0, \omega_1, \dots \right\} \downarrow \left\{ \omega_0^{(0)}, \omega_1^{(0)}, \dots \right\} \text{ or } \left\{ \omega_0^{(1)}, \omega_1^{(1)}, \dots \right\}$$

$$A_0 \otimes B_0^{(0)} |\psi\rangle \quad A_1 \otimes B_1^{(0)} |\psi\rangle$$

$$A_0 \otimes B_0^{(1)} |\psi\rangle \quad A_1 \otimes B_1^{(1)} |\psi\rangle$$

$\{A_0^{(0)}, B_1^{(0)}\}$, in $A_0^{(0)} L Q C C$ protocol corresponds to a product operator.

$\{A_0^{(10)}, A_1^{(10)}\}$, or $\{A_0^{(11)}, A_1^{(11)}\}$

Terminology

- A single measurement performed by one of the parties and the subsequent broadcast of that result constitutes one **round** in the LOCC operation.
- Any local unitary (LU) operation *does not* consume one round of action.
- An LOCC **protocol** is a set of instructions which:
 - (1) identifies a single party as the acting agent in each round,
 - (2) specifies the particular measurement that party is to perform given the measurement outcomes in all previous rounds,
- A **finite round** LOCC protocol is one that necessarily halts after n rounds for some $n \in \mathbb{Z}^+$ (3) describes any LU operations to be performed by the other parties given the outcome of the measurement in (2), and
- An **infinite round** protocol is one that does not halt whenever certain sequences of measurement outcomes are obtained.

Previous Results on LOCC Round Dependence

- For distillation of bipartite mixed states, multiply rounds is stronger than just one¹:

$$D_1(W_{5/8}) = 0 < D_2(W_{5/8}).$$

$$W_{5/8} = \frac{5}{8}\Psi^- + \frac{3}{8}(\Psi^+ + \Phi^+ + \Phi^-)$$

- “Breeding Protocol” uses an indefinite number of rounds to improve the fidelity of Werner states²:

$$F' = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}.$$

- Any bipartite pure state transformation can be completed in just one round of LOCC³.
- Two-way communication strengthens state distinguishability⁴. Xin and Duan construct an example of $n^2 - 2n + 3$ product states in an $n \otimes n$ system needing $2n - 2$ rounds to distinguish⁵.

Random Distillation⁶

- Alice, Bob and Charlie share one copy of the W-state:

$$|W\rangle = \sqrt{1/3} (|100\rangle + |010\rangle + |001\rangle).$$

For $\epsilon > 0$, define measurement with operators:

$$M_0 = \sqrt{1 - \epsilon} |0\rangle\langle 0| + |1\rangle\langle 1| \quad M_1 = \sqrt{\epsilon} |0\rangle\langle 0|.$$

- Alice, Bob, and Charlie each perform the measurement $\{M_0, M_1\}$.

repeat →

halt ↛ ↚

A	B	C	Final State	Probability
0	0	0	$ W\rangle$	$(1 - \epsilon)^2$
0	0	1	$ EPR\rangle_{AB}$	$\frac{2}{3}(1 - \epsilon)\epsilon$
0	1	0	$ EPR\rangle_{AC}$	$\frac{2}{3}(1 - \epsilon)\epsilon$
1	0	0	$ EPR\rangle_{BC}$	$\frac{2}{3}(1 - \epsilon)\epsilon$
0	1	1	Failure	$O(\epsilon^2)$
.

Analysis of Protocol

- For $3n$ rounds, the total probability of EPR yield is:

$$P_{tot} := p_{AB} + p_{AC} + p_{BC} = 2(1 - \epsilon)\epsilon \sum_{i=0}^{n-1} (1 - \epsilon)^{2n}.$$

- When $\epsilon = 1/4$ and $n = 3$, $P_{tot} \approx .7$.
- Outperforms distillation to a specified party:

$$P_{max}\left(|W\rangle \rightarrow |EPR\rangle_{AB}\right) = \frac{2}{3}.$$

- In infinite rounds,

$$P_{tot} = 2(1 - \epsilon)\epsilon \sum_{i=0}^{\infty} (1 - \epsilon)^{2n} = \frac{2 - 2\epsilon}{2 - \epsilon} < 1.$$

$$P_{tot} < 1$$

- Does there exist any finite round protocol that achieves $P_{tot} = 1$?

No.

If finite rounds, in the last rounds there must be some tripartite state $|\phi\rangle_{ABC}$ such that:

$$|\phi\rangle_{ABC} \rightarrow |EPR\rangle \quad \text{with probability one.}$$

only possible with a GHZ-type state

- Does there exist an infinite round protocol that achieves $P_{tot} = 1$?

No.

The proof requires the construction of a new entanglement monotone⁷.

Reduce the Distilled Entanglement

- Concurrence measure of entanglement for two qubit $|\psi\rangle_{AB}$:

$$C(\psi) = 2[\det \rho_A]^{1/2}.$$

$C(|\psi\rangle) = 1$ iff $|\psi\rangle$ is an EPR state.

- Generalize the transformation:

$$|W\rangle \rightarrow \begin{cases} |EPR\rangle_{AB} & \text{with probability } p_{AB}, \\ |EPR\rangle_{AC} & \text{with probability } p_{AC}, \\ |\psi\rangle_{BC} & \text{with probability } p_{BC} \end{cases}$$

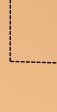
$$p_{AB} + p_{AC} + p_{BC} = 1$$

where $0 < C(\psi) < 1$.

Nice Properties of Concurrence⁸⁻⁹

- For an $n \otimes 2 \otimes 2$ state $|\phi\rangle$, define the “Concurrence of Assistance” (COA):

$$C_a^{(A)}(\phi) = \max \sum_i p_i C(\psi_i).$$


 $\sum_i p_i |\psi_i\rangle\langle\psi_i| = \text{tr}_A(|\phi\rangle\langle\phi|)$

- $C_a^{(A)}(\phi) = F(\rho_{BC}, \tilde{\rho}_{BC}) = \sum_{i=1}^4 \sqrt{\lambda_i}$ ← eigenvalues of $\rho \tilde{\rho}$
- For a W-class state $|W'\rangle = \sqrt{x_A}|100\rangle + \sqrt{x_B}|010\rangle + \sqrt{x_C}|001\rangle$,
 $\rho_{BC} = \sigma_y \otimes \sigma_y (\rho^*) \sigma_y \otimes \sigma_y$
- COA is an entanglement monotone.
 - General W-class state: $\sqrt{x_0}|000\rangle + \sqrt{x_1}|100\rangle + \sqrt{x_2}|010\rangle + \sqrt{x_3}|001\rangle$
- Deterministic LOCC transformation $|\phi\rangle_{ABC} \rightarrow |\psi\rangle_{BC}$ is possible iff
 - Any W-class state has COA < 1.

$$C_a^{(A)}(\phi) \geq C(\psi).$$

Consequences

$$|W\rangle \rightarrow \begin{cases} |EPR\rangle_{AB} & \text{with probability } p_{AB}, \\ |EPR\rangle_{AC} & \text{with probability } p_{AC}, \\ |\psi'\rangle_{BC} & \text{with probability } p_{BC} \end{cases}$$

$p_{AB} + p_{AC} + p_{BC} = 1$

- Since $|\psi'\rangle_{BC} \rightarrow |\psi\rangle_{BC}$ with probability \sqrt{s} , Alice must be the acting party in the last round.

- There must be some final round with probability p_{EPR}^m (or $|EPR\rangle_{AB}$ (or $|EPR\rangle_{AC}$) is a post-measurement EPR state. with probability p_{AC} , with probability p_{BC})
- $$|W\rangle = \sqrt{x_0}|000\rangle + \sqrt{x_1}\left(\frac{\sqrt{\frac{1-s}{2}}(|100\rangle + |010\rangle) + \sqrt{s}|001\rangle}{\sqrt{p_{AB} + p_{AC} + p_{BC}}}\right) + \sqrt{x_2}|001\rangle$$
- $$p_{AB} + p_{AC} + p_{BC} = 1$$

$$C_a^{(A)}(W') \leq \sqrt{2} \sqrt{C_2(\psi')} \leq \sqrt{2} \sqrt{C_1(\psi'_1)} \geq \sqrt{\frac{1-s}{2}}$$

Transformation with $C(\psi) = \sqrt{\frac{1}{2}}$

- Protocol: notation¹⁰:

$$\sqrt{x_0}|000\rangle M_0(x)\sqrt{x_1}|100\rangle x|Q\rangle\langle Q|\theta_1\theta_2\rangle + 1\sqrt{x_3}|001\rangle M_1(x) \vec{x} \sqrt{x}|\theta_1\rangle\langle\theta_2|, x_3)$$

$$\alpha = \frac{2\sqrt{2}}{2+\sqrt{2}} \quad \beta = \frac{2+3\sqrt{2}}{4+2\sqrt{2}}$$

$$x_0 = 1 - x_1 - x_2 - x_3$$

I.

Charlie:
 $\{M_0(\alpha), M_1(\alpha)\}$

III.

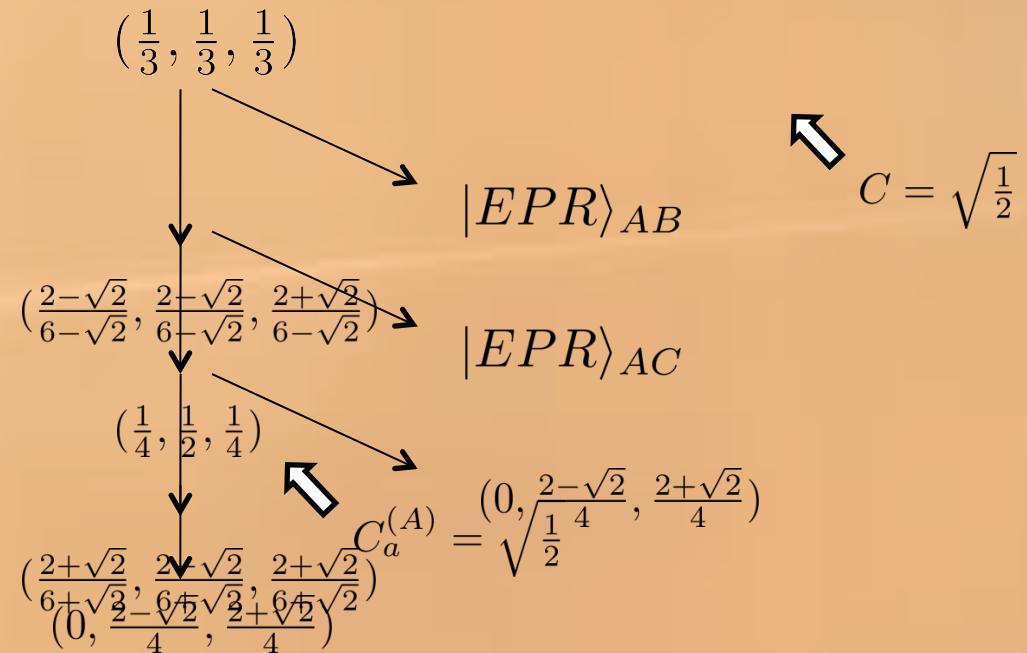
Bob:
 $\{M_0(\beta), M_1(\beta)\}$

II.

Alice:
 $\{M_0(\alpha), M_1(\alpha)\}$

IV.

Alice:



Result:

$$|W\rangle \rightarrow \begin{cases} |EPR\rangle_{AB} & \text{with probability } p_{AB}, \\ |EPR\rangle_{AC} & \text{with probability } p_{AC}, \\ |\psi\rangle_{BC} & \text{with probability } p_{BC} \end{cases}$$

$$p_{AB} + p_{AC} + p_{BC} = 1$$

$$\text{if and only if } C(\psi) \leq \sqrt{\frac{1}{2}}.$$

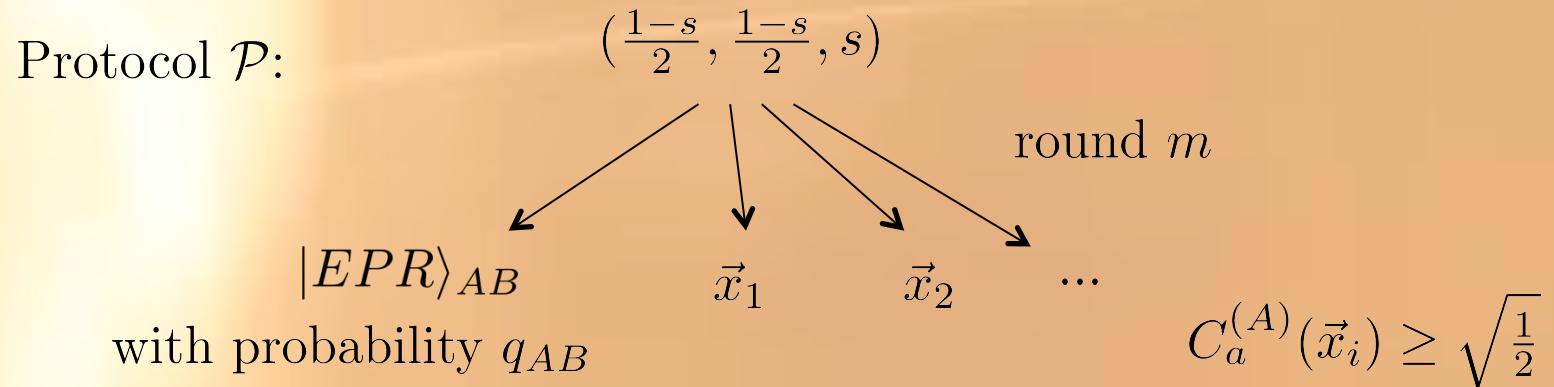
- Achievable in four rounds
- What if we want to maximize $p_{AB} + p_{AC}$?
- Possible to optimize in four rounds?

$$LOCC_{n+2} > LOCC_n$$

$$|W\rangle \rightarrow \begin{cases} |EPR\rangle_{AB} & \text{with probability } p_{AB}, \\ |EPR\rangle_{AC} & \text{with probability } p_{AC}, \\ (0, \frac{2-\sqrt{2}}{4}, \frac{2+\sqrt{2}}{4}) & \text{with probability } p_{BC} \end{cases}$$

$$p_{AB} + p_{AC} + p_{BC} = 1.$$

- Consider any n round transformation \mathcal{P} :
- There must be some final round $m < n$ in which $|EPR\rangle_{AB}$ is a post-measurement state.



$$LOCC_{n+2} > LOCC_n$$

- Modified protocol \mathcal{P}' : $(\frac{1-s}{2}, \frac{1-s}{2}, s)$

Charlie:
 $\{M_0(\frac{q_{AB}}{1-s}), M_1(\frac{q_{AB}}{1-s})\}$

$$C_a^{(A)} = \sqrt{\frac{1}{2}}$$

round m
 $(\frac{1-s'}{2}, \frac{1-s'}{2}, s')$
 $|EPR\rangle_{AB}$
 with probability q_{AB}

If $s' < \frac{1}{2}$

$$(\frac{1-s'}{2}, \frac{1-s'}{2}, s')$$

Charlie:

$$(\frac{1-s''}{2}, \frac{1-s''}{2}, s'')$$

round $m + 1$

$$\uparrow C_a^{(A)} = \sqrt{\frac{1}{2}}$$

Alice: round $m + 2$

If $s' \geq \frac{1}{2}$ $(\frac{1-s'}{2}, \frac{1-s'}{2}, s')$

Alice:

$$(s'', 1 - 2s'', s'')$$

round $m + 1$

$$(0, \frac{2-\sqrt{2}}{4}, \frac{2+\sqrt{2}}{4})$$

Bob:

$$(s''', 1 - 2s''', s''')$$

round $m + 2$

$$\uparrow C_a^{(A)} = \sqrt{\frac{1}{2}}$$

Alice: round $m + 3$

$|EPR\rangle_{AC}$

Result:

$$p'_{AB} + p'_{AC} > p_{AB} + p_{AC}$$

$$LOCC_{n+2} > LOCC_n$$

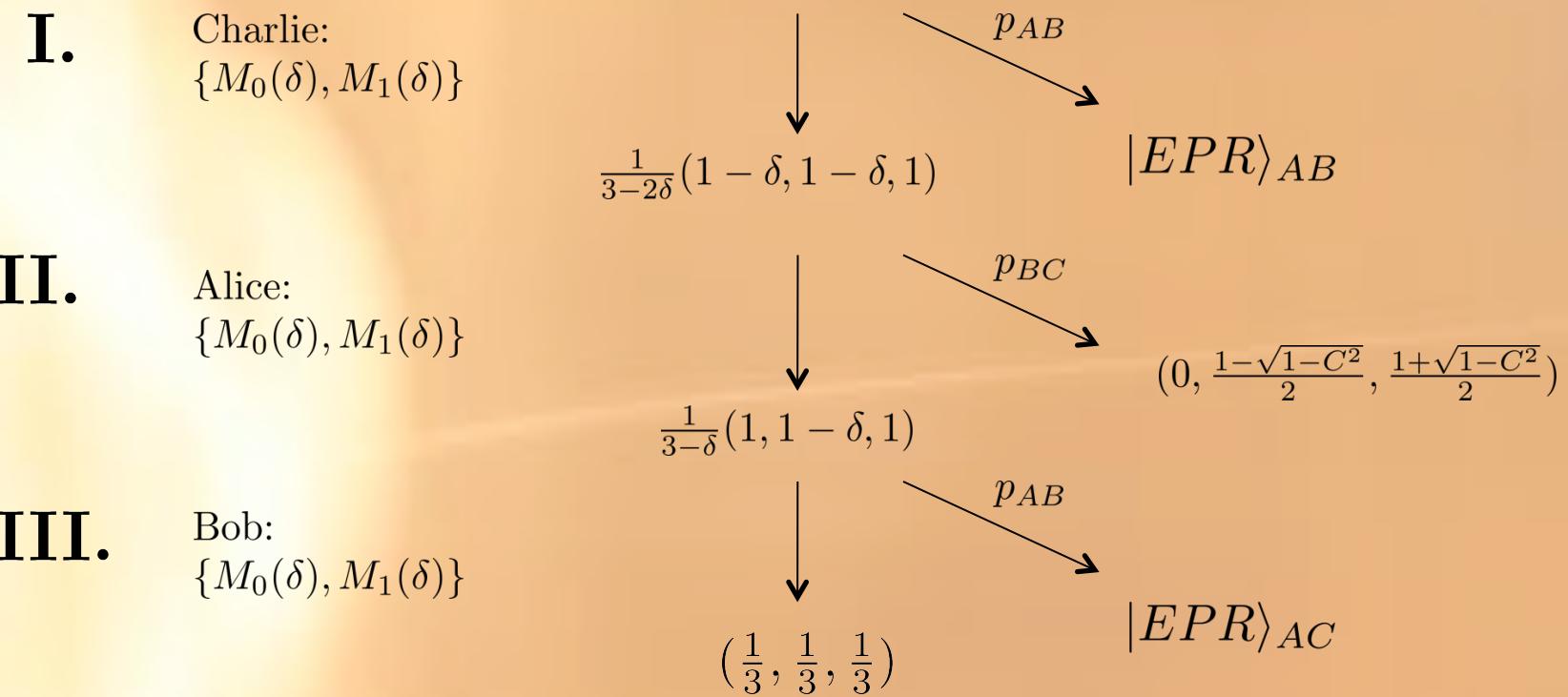
$LOCC_\infty$

$$|W\rangle \rightarrow \begin{cases} |EPR\rangle_{AB} & \text{with probability } p_{AB}, \\ |EPR\rangle_{AC} & \text{with probability } p_{AC}, \\ |\psi\rangle_{BC} & \text{with probability } p_{BC} \end{cases}$$
$$p_{AB} + p_{AC} + p_{BC} = 1$$
$$\text{with } C(\psi) < 1.$$

$LOCC_\infty$

$$M_0(x) = \sqrt{1-x}|0\rangle\langle 0| + |1\rangle\langle 1| \quad M_1(x) = \sqrt{x}|0\rangle\langle 0|$$

$$\delta = \frac{2\sqrt{1-C^2}}{1+\sqrt{1-C^2}} \quad \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3} \right)$$



Protocol Analysis

$$p_{AB} = \frac{2}{3}\delta$$

$$p_{BC} = \frac{2}{3}\delta - \frac{1}{3}\delta^2$$

$$p_{AC} = \frac{2}{3}\delta(1 - \delta)$$

$$P_W = (1 - \delta)^2$$

$$p_{AB}(total) = \frac{2}{3}\alpha + (1 - \alpha)^2 \left(\frac{2}{3}\alpha + (1 - \alpha)^2 \left(\frac{2}{3}\alpha + \dots \right) \right)$$

$$= \frac{2}{3}\alpha \sum_{k=0}^{\infty} (1 - \alpha)^{2k} = \boxed{\frac{2}{3} \left(\frac{1}{2 - \alpha} \right)}$$

$$p_{AC}(total) = \boxed{\frac{1}{3}}$$

$$p_{BC}(total) + p_{AC}(total) + p_{AB}(total) = 1$$

$$p_{AB}(total) = \boxed{\frac{2}{3} \left(\frac{1 - \alpha}{2 - \alpha} \right)}$$

Summary of Results

$$|W\rangle \rightarrow \begin{cases} |EPR\rangle_{AB} & \text{with probability } p_{AB}, \\ |EPR\rangle_{AC} & \text{with probability } p_{AC}, \\ |\psi\rangle_{BC} & \text{with probability } p_{BC} \end{cases}$$
$$p_{AB} + p_{AC} + p_{BC} = 1,$$

- A) There exists a four round LOCC protocol that achieves the above transformation iff $C(\psi) \leq \sqrt{\frac{1}{2}}$,
- B) There exists an infinite round LOCC protocol that achieves the above transformation iff $C(\psi) < 1$,
- C) For any n round protocol \mathcal{P} with rates $p_{AB} + p_{AC}$, there exists an $n + 2$ round protocol achieving rates

$$p'_{AB} + p'_{AC} > p_{AB} + p_{AC}.$$

Additional Questions

- Lower bounds on the number of rounds for bipartite tasks
- Perhaps mixed state transformations
- Determine class of tripartite pure state transformations feasible with one-way communication
- Perform an information-theoretic analysis of infinite round transformations along the lines of Ref. [4]

References

- ¹ Bennett et al. *Phys. Rev. A* **54**, 3824 (1996).
- ² Bennett et al. *Phys. Rev. Lett.* **76**, 722 (1996).
- ³ Lo & Popescu *Phys. Rev. A* **63**, 022301 (2001).
- ⁴ Bennett et al. *Phys. Rev. A* **59**, 1070 (1999).
- ⁵ Xin & Duan *Phys. Rev. A* **77**, 012315 (2008).
- ⁶ Fortescue & Lo *Phys. Rev. Lett.* **98**, 260501 (2007).
- ⁷ Cui, Chitambar & Lo – *Manuscript in Preparation.*
- ⁸ Gour et al. *Phys. Rev. A* **72**, 042329 (2005).
- ⁹ Laustsen et al. *Quantum Inf. Comput.* **3**, 64 (2003).
- ¹⁰ Kintas & Turgut *J. Math. Phys.* **51**, 092202 (2010).

Many Thanks

- Andreas Winter
- Hoi-Kwong Lo[†]
- Wei Cui
- Debbie Leung



[†] Funding Agencies: CIFAR, CRC, NSERC, and Quantum-Works.