Port-based teleportation and its applications

Satoshi Ishizaka

Graduate School of Integrated Arts and Sciences
Hiroshima University

Collaborator: Tohya Hiroshima (ERATO-SORST)

Outline

- **Port-based teleportation**

  [SI and T. Hiroshima, PRL **101**, 240501 (2008); PRA **79**, 042306 (2009)]

- **Its applications**

  - universal programmable processor

  - attacking position-based cryptography

    [S. Beigi and R. König, New J. Phys. **13**, 093036 (2011)]

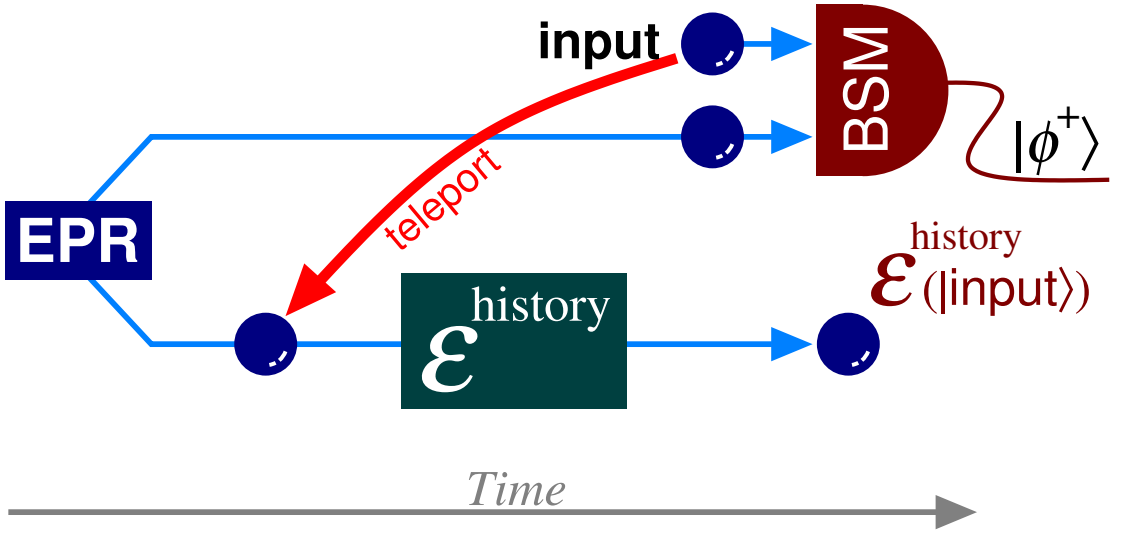
  - entanglement recycling and generalized teleportation

    [S. Strelchuk, M. Horodecki, and J. Oppenheim, PRL **110**, 010505 (2013)]

  - relation to no-signaling

    [D. Pitalúa-García, arXiv:1206.4836 (2012)]

A reliving machine



Teleportation enables to "relive" the past events

[C. H. Bennett, private comm.]

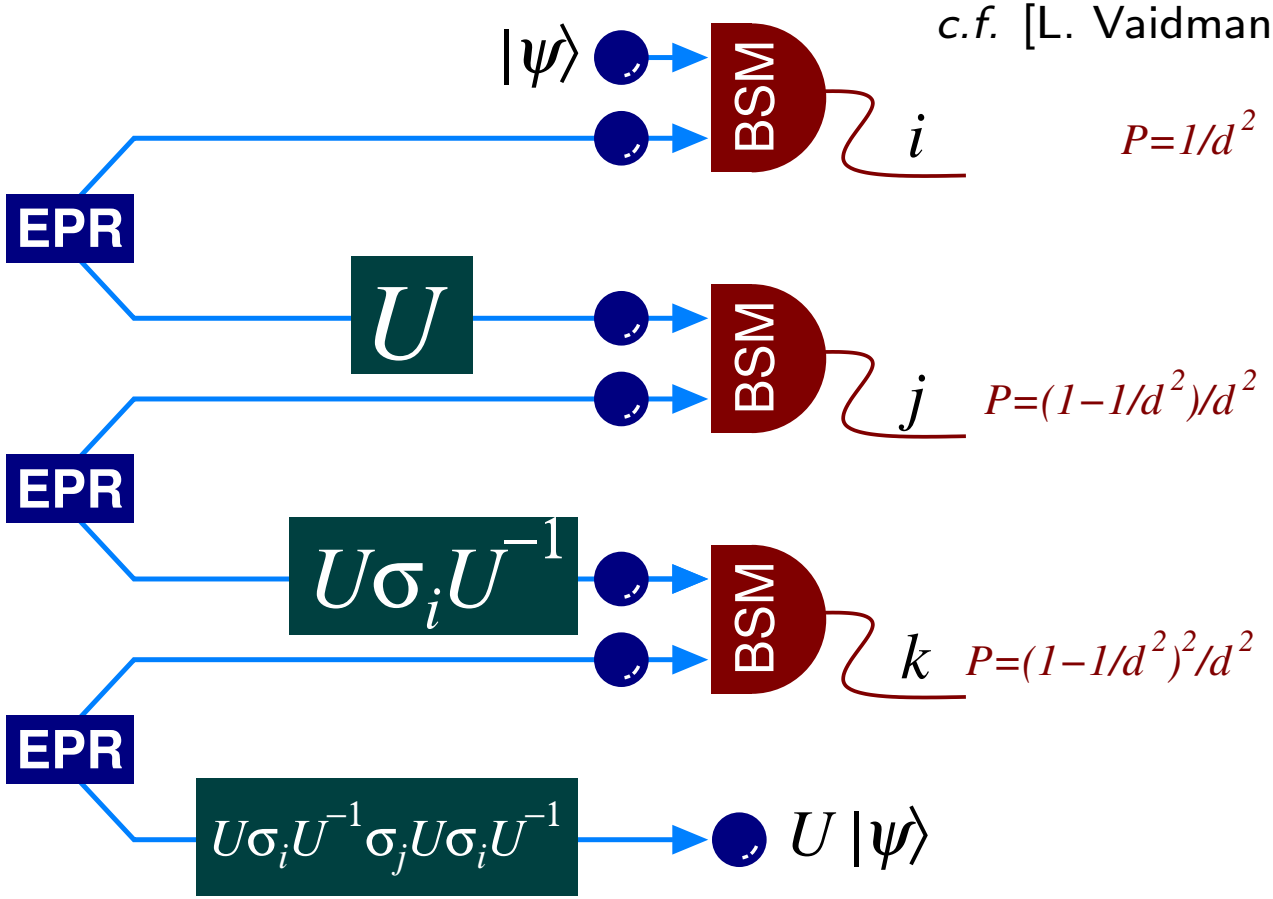
[N. Imoto, 7th QCM&C]

[Č. Brukner, *et. al.*, Phys. Rev. A (2003)]

"Reliving" succeeds only with $P_{\text{success}} = \frac{1}{d^2}$

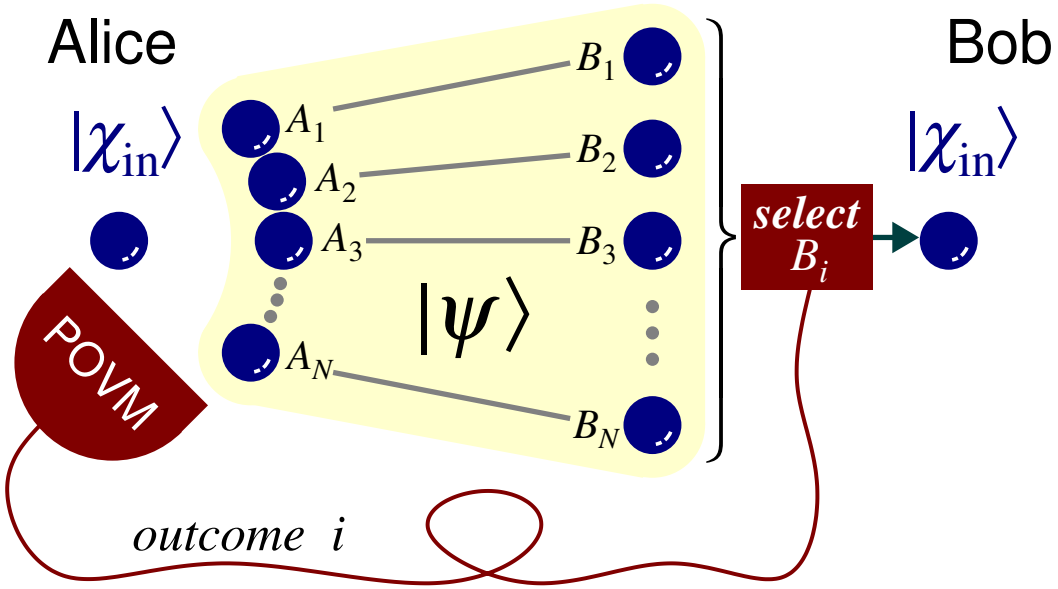
A simple way to increase P_{success}

c.f. [L. Vaidman (2003)]



- R round $\cdots$ $P = 1-(1-1/d^2)^R = 1-\epsilon$
- huge EPR resource $\cdots$ $2^{2n2^{2n}\log(1/\epsilon)}$ (double exp)
- only for reversible operations, complicated

Port-based teleportation



- **Such a teleportation scheme is truly possible?**
- **What is the optimal success probability or fidelity?**
- **What is the optimal $|\psi\rangle$ and optimal POVM?**

We answer these questions

Formulation

- Bob's operation is fixed

  teleportation = discrimination of quantum signals

- e.g. standard teleportation scheme

  Bob's operation is fixed to $\{I, \sigma_x, \sigma_y, \sigma_z\} = \{\sigma_i\}$

  $\Downarrow$

  Alice must (globally) descriminate 4 quantum signals:

  $\{(I \otimes \sigma_i)|\psi\rangle\} = \{|\phi^+\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^-\rangle\}$

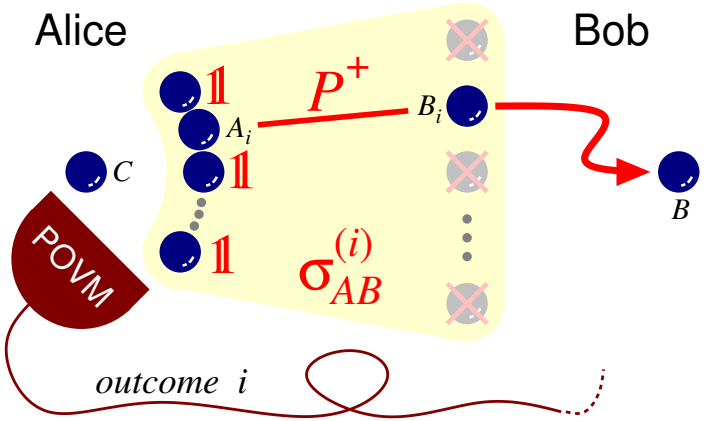
  $\Downarrow$

  $\therefore$ Bell state measurement is optimal for Alice

  (Alice measures a qubit to be teleported instead of Bob's qubit)

Formulation

$$|\psi\rangle = |\phi^+\rangle_{A_1B_1} \cdots |\phi^+\rangle_{A_NB_N}$$



- Alice's POVM: $\Pi^{(i)}{}_{AC}$

$$\sigma^{(i)}_{AB} = \frac{1}{d^{N-1}} P^+_{A_iB} \otimes \mathbb{1}_{\bar{A}_i} \quad \cdots \text{ non-commutable \& mixed}$$

- Average fidelity: $f = (Fd+1)/(d+1)$

$$F = \frac{1}{d^2} \sum_{i=1}^{N} \mathrm{tr}\Pi^{(i)}{}_{AB} \sigma^{(i)}_{AB} \quad \cdots \quad \text{Entanglement fidelity maximized}$$

- Problem of discriminating $\{\sigma^{(1)}, \sigma^{(2)}, \cdots, \sigma^{(N)}\}$

$$p_{\mathrm{err}} = 1 - d^2 F/N$$

Duality is broken

- Duality between superdense coding and teleportation

  (i) All teleportation schemes

$$\sum_{x \in X} \mathrm{tr}[(M_x \otimes \Lambda_x)(\sigma \otimes \psi)]A = \mathrm{tr}\sigma A$$

  (ii) All dense coding schemes

$$\mathrm{tr}(\Lambda_x \otimes M_y)\psi = \delta_{xy}$$

  (i) $\Longleftrightarrow$ (ii) for "tight" cases [R. F. Werner, (2000)]

- but $p_{\mathrm{err}} = 1 - \dfrac{d^2 F}{N}$ for port-based teleportation ("non-tight")

Deterministic scheme — optimal protocol ($d=2$)

- $|\psi\rangle$ is maximally entangled ($|\psi\rangle = |\phi^+\rangle^{\otimes N}$)

$$\Pi_i = \rho^{-\frac{1}{2}} \sigma^{(i)} \rho^{-\frac{1}{2}} \quad \text{with} \quad \rho = \sum_{i=1}^{N} \sigma^{(i)} \qquad \cdots \text{ SRM is optimal}$$

$$F = \frac{1}{2^{N+3}} \sum_{k=0}^{N} \left(\frac{N-2k-1}{\sqrt{k+1}} + \frac{N-2k+1}{\sqrt{N-k+1}} \right)^2 \binom{N}{k}$$

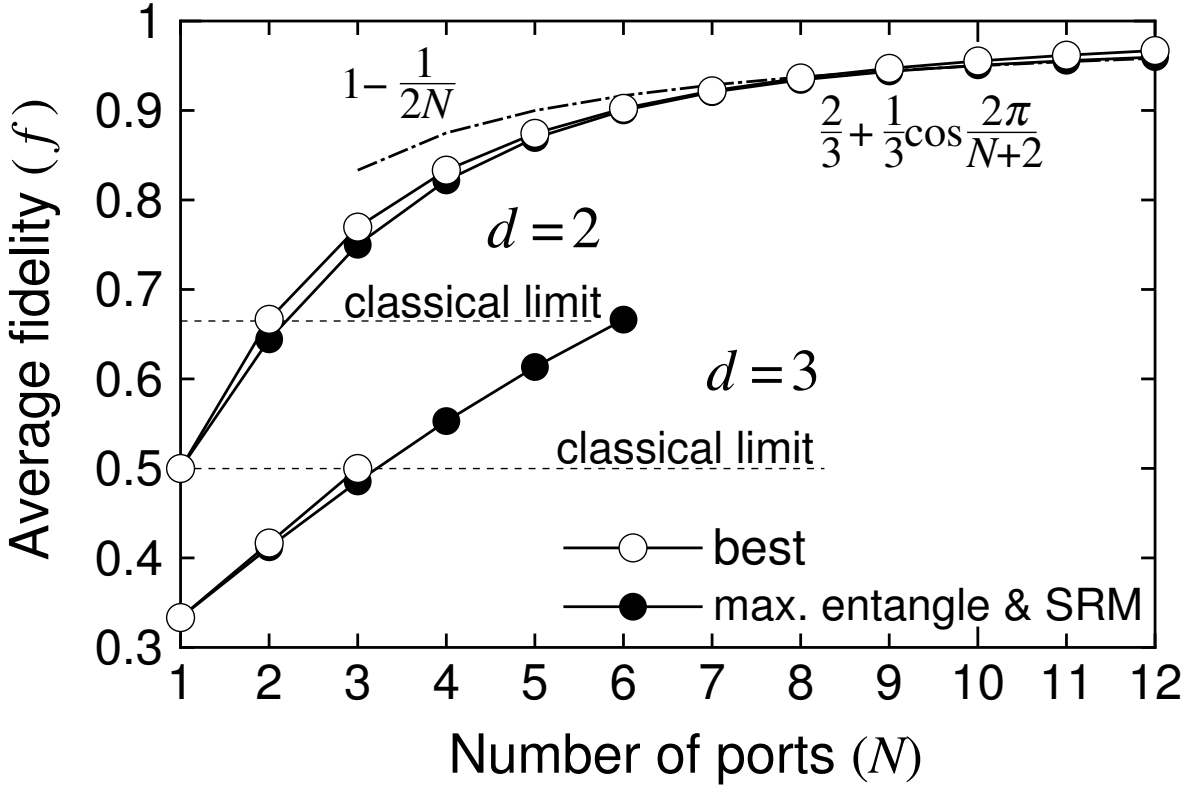
- $|\psi\rangle$ is also optimized

$$O^\dagger \Pi_i O = \sum_s z(s) \rho_s^{-\frac{1}{y(s)}} \sigma_s^{(i)} \rho_s^{-\frac{1}{y(s)}} \qquad \cdots \text{ generalized SRM}$$

$$O^\dagger O = \sum_j \gamma(j) \mathbb{1}(j)_A^{[N]}, \qquad \left(\frac{N-2s+1}{N+2s+3} \right)^{\frac{1}{y(s)}} = \frac{s}{s+1} \frac{\sin \frac{2\pi(s+1)}{N+2}}{\sin \frac{2\pi s}{N+2}}$$

$$F = \cos^2 \left(\frac{\pi}{N+2} \right)$$

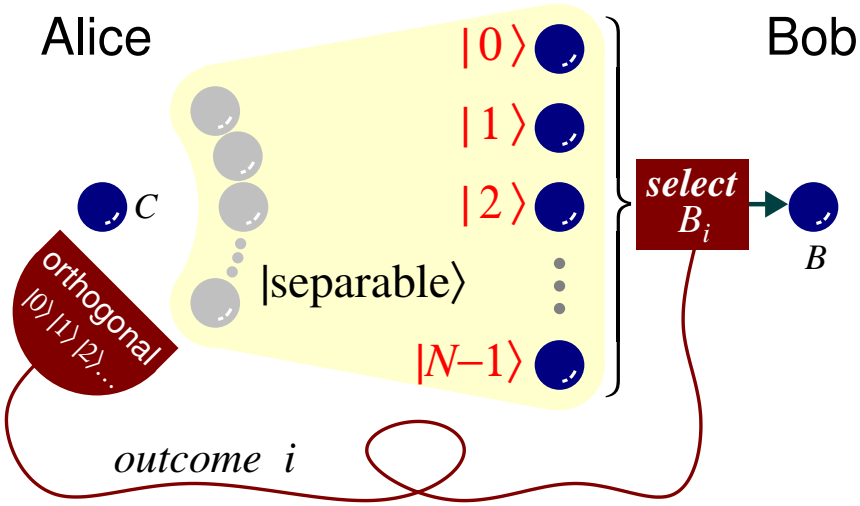
Deterministic scheme — optimal fidelity



- f exceeds $f_{\rm cl}=2/3$ for $N>2$ and approaches to 1 for $N\to\infty$
  - ▷ This scheme certainly works as quantum teleportation
  - ▷ Three EPR-pairs are enough to demonstrate this scheme
  - ▷ $|\phi^+\rangle^{\otimes N}$+SRM nearly achieves the best f around small N

When the number of ports is small...

- Alice performs an orthogonal measurement $\{|0\rangle, |1\rangle, |2\rangle, \cdots\}$



- This M&P protocol is optimal for $N \leq d$
- This is not quantum teleportation $\cdots f \leq f_{\rm cl} = \dfrac{2}{d+1}$
- $N > d$ is necessary to exceed $f_{\rm cl}$

Can fidelity exceed the classical limit by using entanglement?

Formulation

- $|\psi\rangle = (O_A \otimes \mathbb{1})|\phi^+\rangle_{A_1B_1}\cdots|\phi^+\rangle_{A_NB_N}$ with $\mathrm{tr}OO^\dagger = d^N$
- POVM: $\{\Pi_0, \Pi_i\}$ $\cdots$ teleportation fails for Π_0
- Faithful teleportation for $\Pi_1 \cdots \Pi_N$

$$O\Pi_i O^\dagger = P^+_{BA_i} \otimes \Theta_{\bar{A}_i}$$

- $\Lambda(\sigma^{\mathrm{in}}) = \sum_{i=1}^{N} \mathrm{tr}_{AC}\Pi_i \left[(O\otimes\mathbb{1})\sigma^{(i)}_{AB}(O^\dagger\otimes\mathbb{1})\right]\otimes\sigma^{\mathrm{in}}_C$
- Success probability of entanglement swapping

$$p = \mathrm{tr}(\Lambda\otimes\mathbb{1})P^+_{CD} = \frac{1}{d^{N+1}}\sum_{i=1}^{N}\mathrm{tr}O^\dagger\Pi_i O \quad \cdots \text{ maximized}$$

Probabilistic scheme — optimal protocol ($d=2$)

- $|\psi\rangle$ is maximally entangled ($|\psi\rangle = |\phi^+\rangle^{\otimes N}$)

$$\Pi_i = P^+_{BA_i} \otimes \sum_s \frac{4}{N+3+2s} \mathbb{1}(s)^{[N-1]}_{\bar{A}_i} \qquad \Pi_0 = \mathbb{1} - \sum_{i=1}^{N} \Pi_i$$

teleportation fails

$$p = \frac{1}{2^N} \sum_s \frac{(2s+1)^2}{(N+1)} \binom{N+1}{\frac{N+3}{2}+s}$$

- $|\psi\rangle$ is optimized

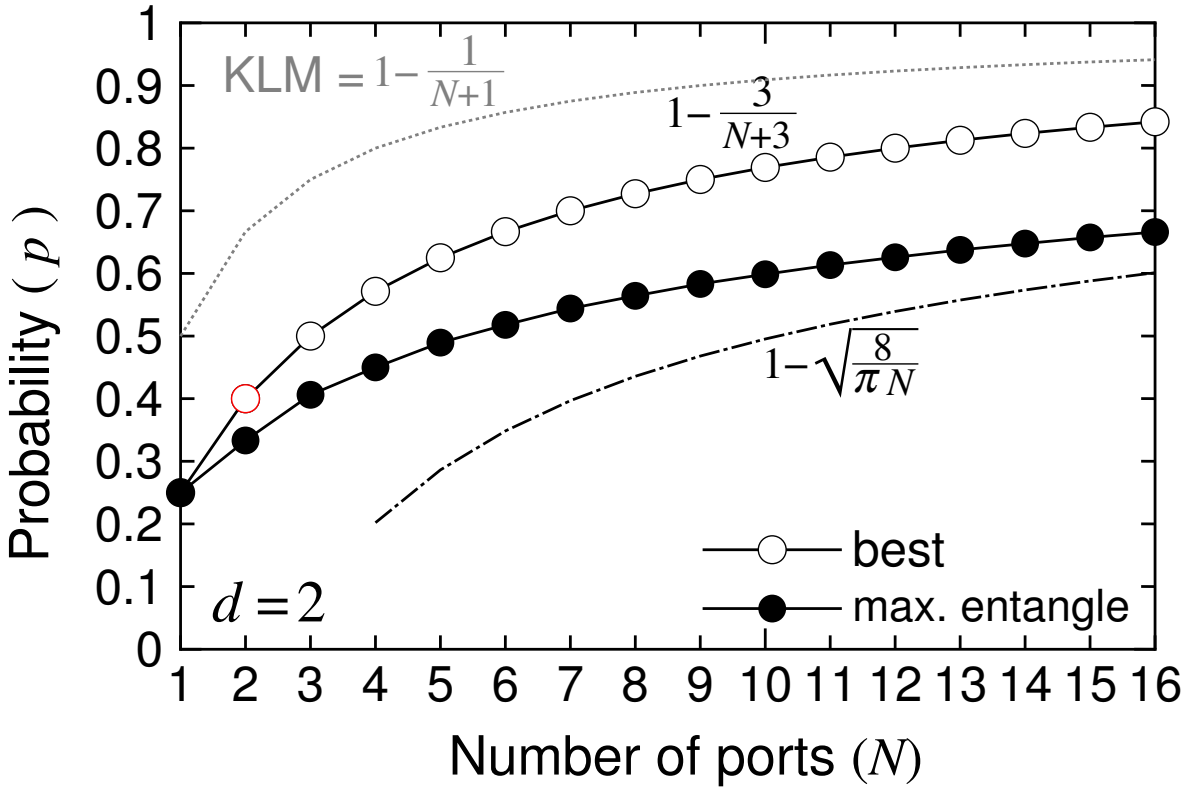
$$O^\dagger \Pi_i O = P^+_{BA_i} \otimes \sum_s \beta(s) \mathbb{1}(s)^{[N-1]}_{\bar{A}_i} \qquad \Pi_0 = \mathbb{1} - \sum_{i=1}^{N} \Pi_i$$

teleportation fails

$$O^\dagger O = \sum_j \gamma(j) \mathbb{1}(j)_A$$

$$p = \frac{N}{N+3} = 1 - \frac{3}{N+3}$$

Optimal success probability



- Optimizing $|\psi\rangle$ considerably enhances p

  ▷ Non-maximally entangled $|\psi\rangle$ provides considerably larger p

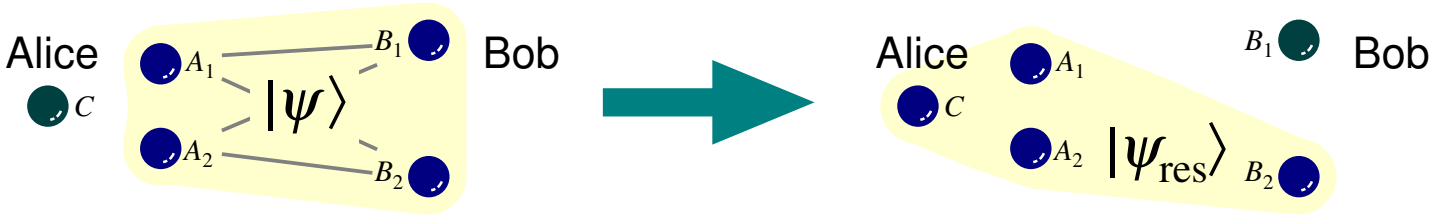
- N must be just 3 times larger than KLM to achive the same p

  $=$ the cost for removing Bob's unitary transformation

Example ($N=2$, $p=2/5$)

- $|\psi\rangle = \sqrt{\frac{3}{10}}\Big[\ \underbrace{|00\rangle_A|00\rangle_B + |11\rangle_A|11\rangle_B + |\psi^+\rangle_A|\psi^+\rangle_B}_{\text{spin-triplet}}\ \Big]$

$$+\sqrt{\frac{1}{10}}\ \underbrace{|\psi^-\rangle_A|\psi^-\rangle_B}_{\text{spin-singlet}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ E=1.895 \text{ ebits}$$



- $\sqrt{\Pi_1}|\psi\rangle \otimes \underline{(\alpha|0\rangle+\beta|1\rangle)_C} = \sqrt{\frac{1}{5}}\ |\psi_{\rm res}\rangle \otimes \underline{(\alpha|0\rangle+\beta|1\rangle)_{B_1}}$

- $|\psi_{\rm res}\rangle = \sqrt{\frac{1}{6}}\Big[|00\rangle|00\rangle + |11\rangle|11\rangle + |\psi^+\rangle|\psi^+\rangle\Big]_{A_1A_2CB_2}$

$$+\sqrt{\frac{1}{2}}|\psi^-\rangle_{A_1A_2}|\psi^-\rangle_{CB_2} \quad \ldots\ldots\ldots\ldots\ldots\ E=1 \text{ ebits}$$

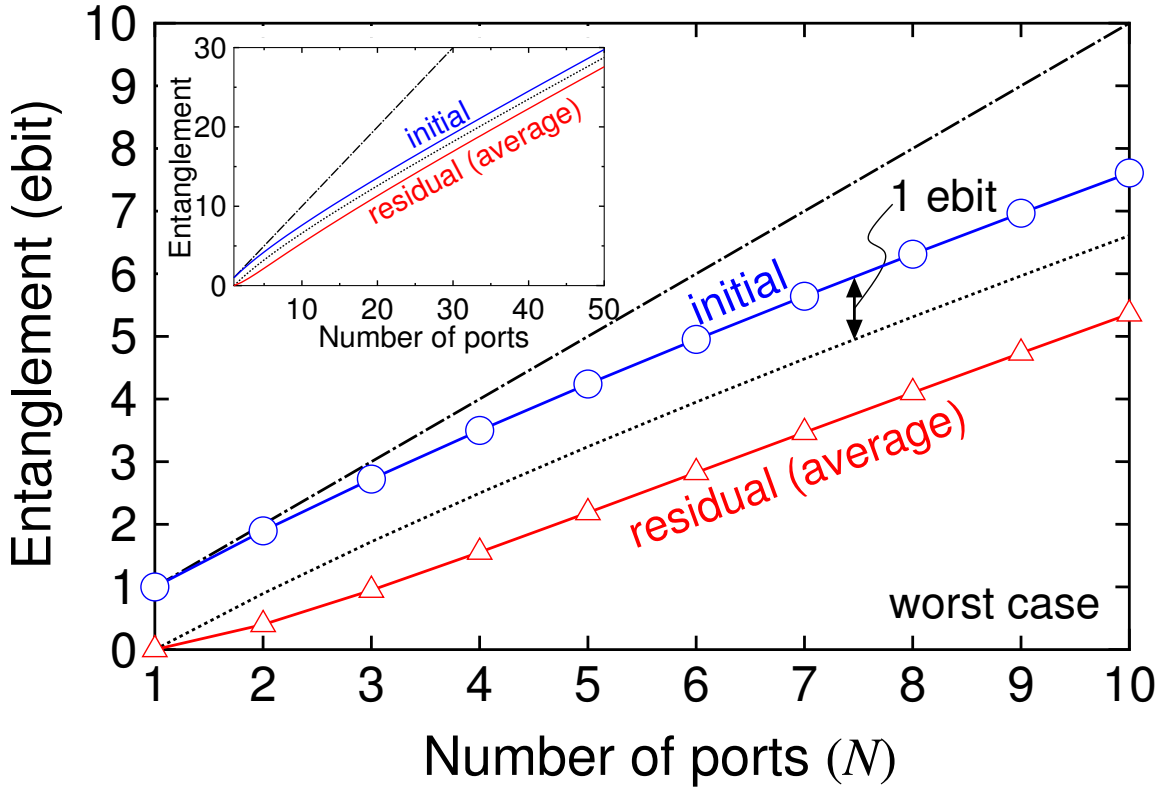
Entanglement consumption $\Delta E = 0.895$ ebits < 1 ebit

Average entanglement consumption

- If teleportation fails ... $\Delta E = 0.31$ ebits for $N = 2$

  Best case: e-swapping $\cdots$ $\log(N+1)$ ebits remains

  Worst case: give up $\cdots$ $\langle \Delta E \rangle = E_{\rm ini} \cdot \frac{3}{N+3} < 3$ ebits



Only a few ebits are consumed on average even for large N

Outline

- **Port-based teleportation**

  [SI and T. Hiroshima, PRL **101**, 240501 (2008); PRA **79**, 042306 (2009)]

- **Its applications**

  - universal programmable processor

  - attacking position-based cryptography

    [S. Beigi and R. König, New J. Phys. **13**, 093036 (2011)]

  - generalized teleportation and entanglement recycling

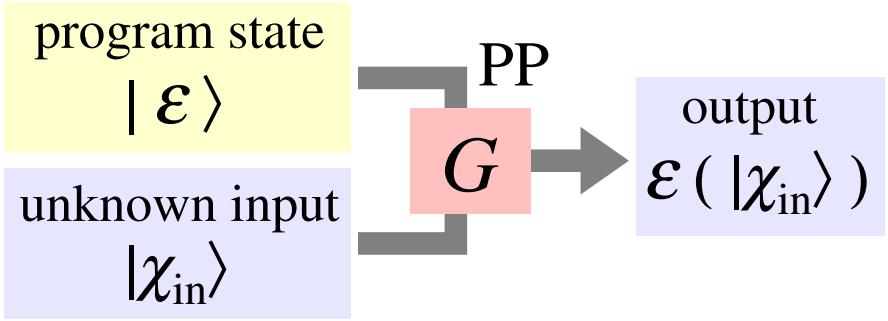
    [S. Strelchuk, M. Horodecki, and J. Oppenheim, PRL **110**, 010505 (2013)]

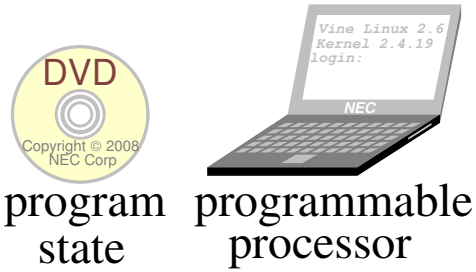
  - relation to no-signaling

    [D. Pitalúa-García, arXiv:1206.4836 (2012)]

Application: universal programmable processor

- Device to manipulate a state via program states ($|\varepsilon\rangle$)





$G \cdots$ fixed operation (indep of $|\varepsilon\rangle$ and $|\chi_{\rm in}\rangle$)

- Universal PP can deal with arbitrary ε

  Unitary, measurements, trace-nonpreserving, etc ...

- No-go theorem: [M. A. Nielsen and I. L. Chuang (1997)]

  Faithful & deterministic UPP cannot be realized

Port-based teleportation evades the no-go theorem

No-go theorem of UPP

[M. A. Nielsen and I. L. Chuang, PRL **79**, 321 (1997)]

$G|\chi_{\rm in}\rangle|U\rangle = (U|\chi_{\rm in}\rangle)|U'\rangle$ for all $|\chi_{\rm in}\rangle$ $\cdots$ deterministic

$$\begin{cases} G|\chi_1\rangle|U\rangle = (U|\chi_1\rangle)|U'\rangle \\ G|\chi_2\rangle|U\rangle = (U|\chi_2\rangle)|U''\rangle \end{cases} \rightarrow \langle\chi_1|\chi_2\rangle = \langle\chi_1|\chi_2\rangle\langle U'|U''\rangle$$

$\therefore |U'\rangle$ is input indep

$$\begin{cases} G|\chi\rangle|U\rangle = (U|\chi\rangle)|U'\rangle \\ G|\chi\rangle|V\rangle = (V|\chi\rangle)|V'\rangle \end{cases} \rightarrow \langle U|V\rangle = \langle\chi|U^\dagger V|\chi\rangle\langle U'|V'\rangle$$

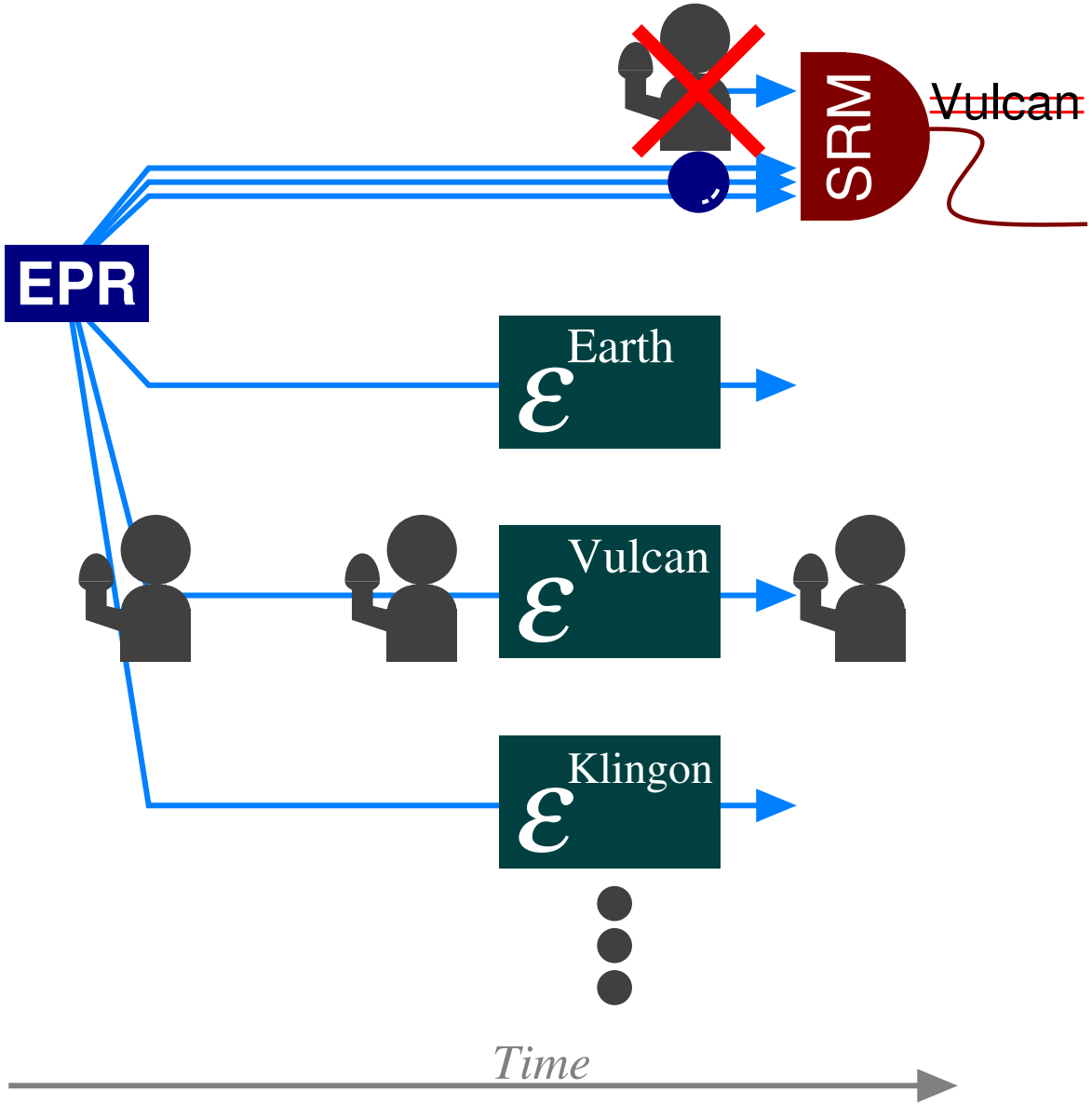
$\therefore \langle\chi|U^\dagger V|\chi\rangle$ is input indep

- If $U \neq V$, then $\langle U|V\rangle = 0$ $\cdots$ orthogonal
- $|\varepsilon\rangle$ can only store limited number of operations

  $\Rightarrow$ deterministic & approximate,

  probabilistic & faithful, or infinite resource

Port-based teleportation as a reliving machine



Outline

- **Port-based teleportation**

  [SI and T. Hiroshima, PRL **101**, 240501 (2008); PRA **79**, 042306 (2009)]

- **Its applications**

  - universal programmable processor

  - attacking position-based cryptography

    [S. Beigi and R. König, New J. Phys. **13**, 093036 (2011)]

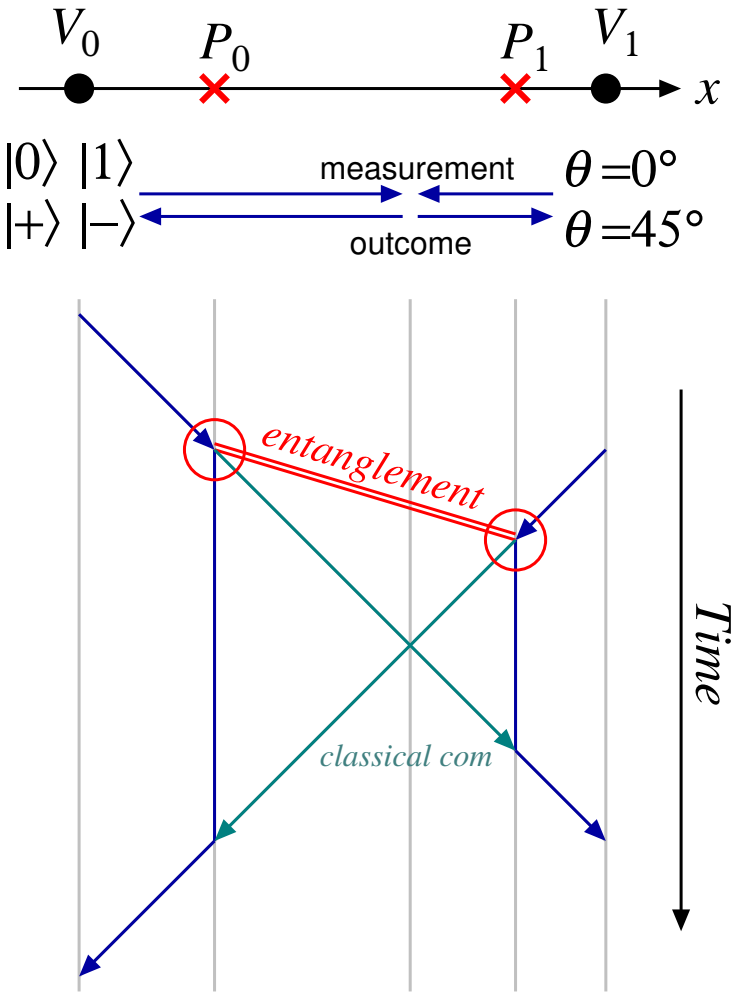
  - generalized teleportation and entanglement recycling

    [S. Strelchuk, M. Horodecki, and J. Oppenheim, PRL **110**, 010505 (2013)]

  - relation to no-signaling

    [D. Pitalúa-García, arXiv:1206.4836 (2012)]

Position-verification in position-based cryptography



Quantum tagging & entangle attack

[A. Kent, *et. al.* (2011)]

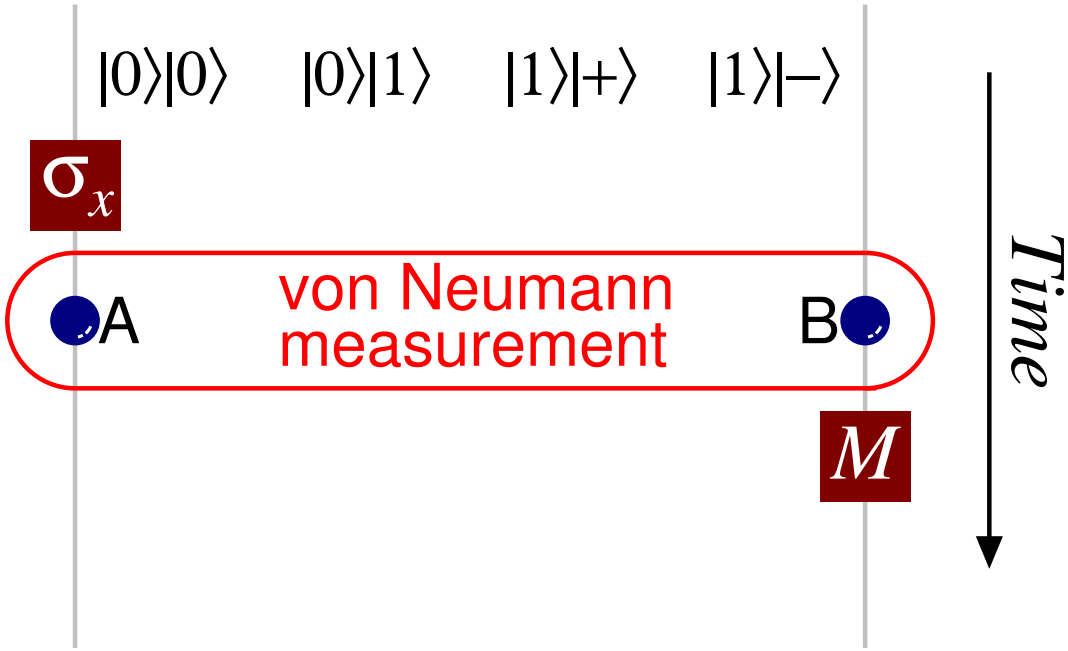
Generic entanglement attack

[H. Buhrman, *et. al.* (2011)]

using instantaneous measurement

[L. Vaidman (2003)]

Measurement & causality



Standard von Neumann measurement contradicts causality

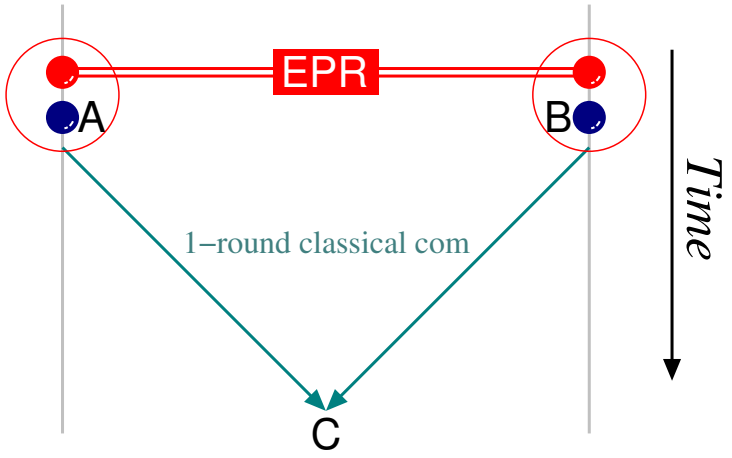
[Landau, Peierls, (1931)]

How to measure nonlocal variables using entangled probes

[Aharonov, Albert, (1980)]

Instantaneous measurerability of all (non-local) variables?

Instantaneous measurement & port-based teleportation

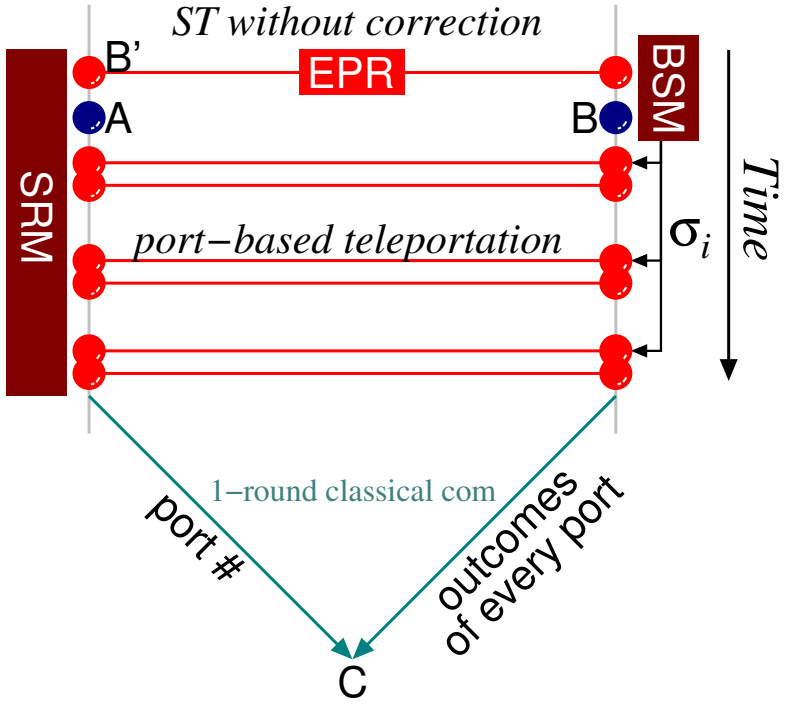


Vaidman's scheme

[L. Vaidman, PRL **90**, 010402 (2003)]

Success probability: $P = 1 - \epsilon$

EPR resource: $\mathcal{O}(2^{4n2^{4n}\log(1/\epsilon)})$



Using port-based teleportation

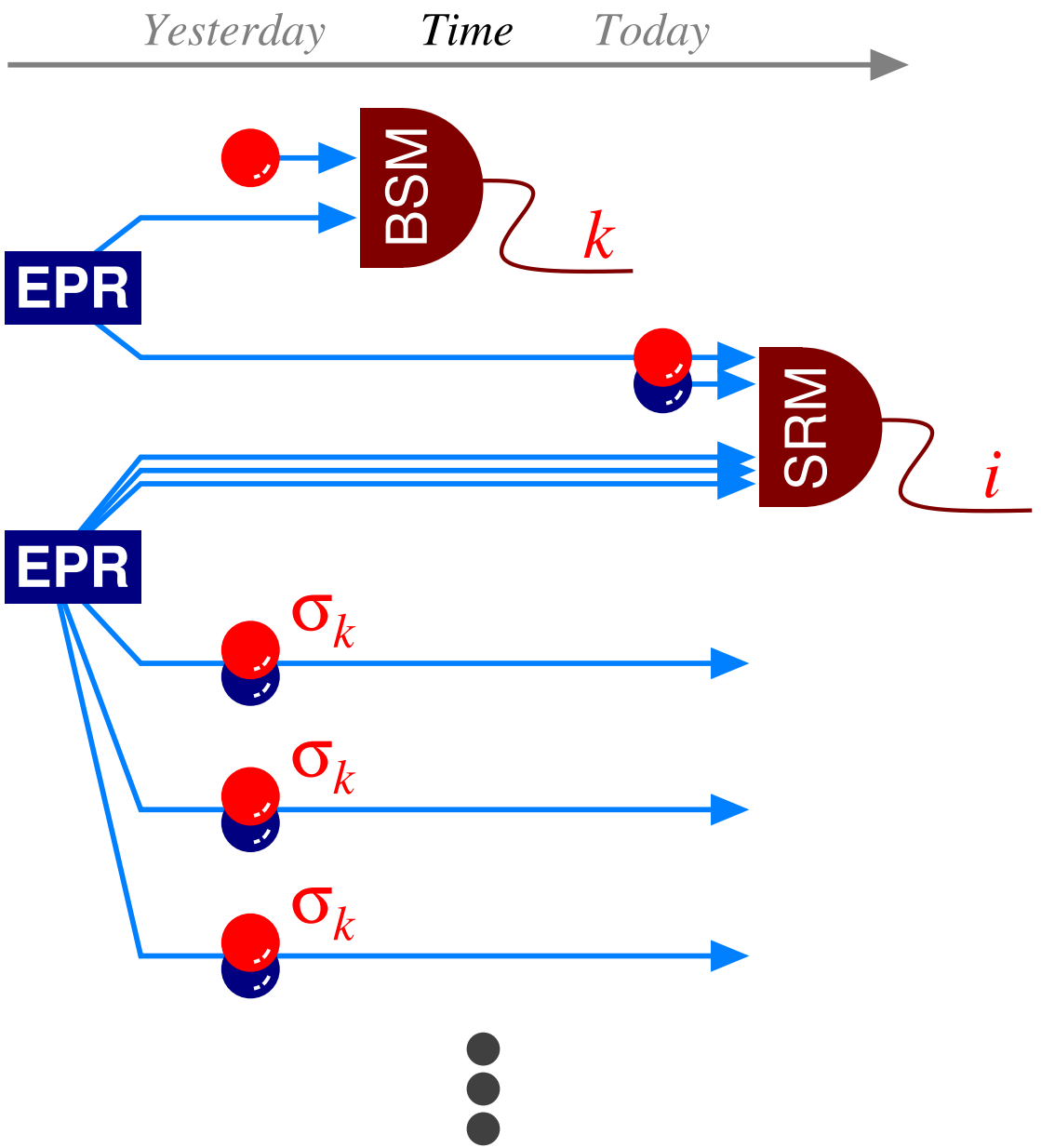
[S. Beigi, R. König, NJP **13**, 093036 (2011)]

Success probability: $P = 1 - \epsilon$

EPR resource: $\mathcal{O}(2^{4n}\log(1/\epsilon))$

exponentially efficient!

Applying CNOT to yesterday's qubit



Outline

- **Port-based teleportation**

  [SI and T. Hiroshima, PRL **101**, 240501 (2008); PRA **79**, 042306 (2009)]

- **Its applications**

  - universal programmable processor

  - attacking position-based cryptography

    [S. Beigi and R. König, New J. Phys. **13**, 093036 (2011)]

  - generalized teleportation and entanglement recycling

    [S. Strelchuk, M. Horodecki, and J. Oppenheim, PRL **110**, 010505 (2013)]

  - relation to no-signaling

    [D. Pitalúa-García, arXiv:1206.4836 (2012)]

Generalized teleportation

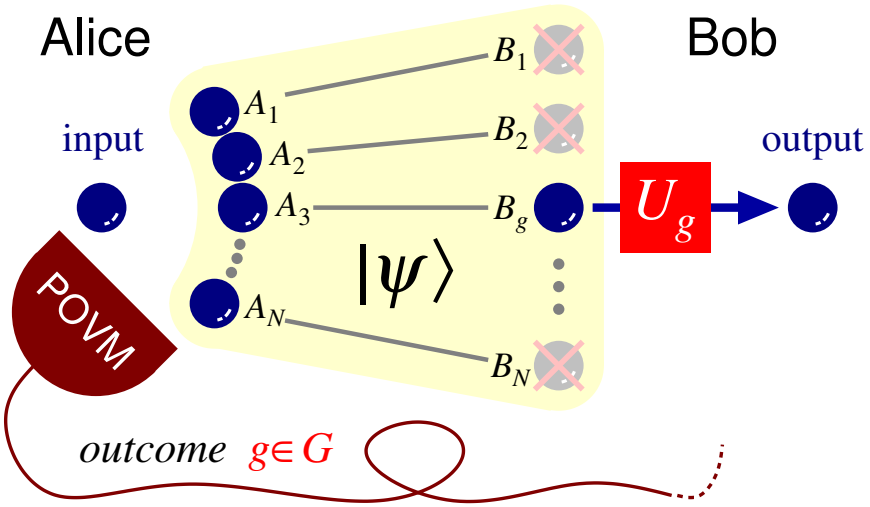
[S. Strelchuk, M. Horodecki, J. Oppenheim, PRL **110**, 010505 (2013)]

... From a group-theoretic perspective all currently known teleportation protocols can be classified into two kinds: those that exploit the Pauli group [BBCJPW93] and those, which use the symmetric permutation group [IH08]. Such a simple change of the underlying group structure lead to two protocols with striking differences in the properties: ..... The former teleportation scheme was used in the celebrated result of Gottesman and Chuang [GC99] to perform universal Clifford-based computation using teleportation over the Pauli group. The generalized teleportation protocol introduced in this Letter embraces both known protocols, and paves the way for protocols which lead to programmable processors capable of executing new kinds of computation beyond Clifford-type operations.

Generalized teleportation

[S. Strelchuk, M. Horodecki, J. Oppenheim, PRL **110**, 010505 (2013)]

Generalized teleportation scheme



$$p_{\text{err}} = 1 - d^2 F/N$$

A sufficient condition for reliable teleportation

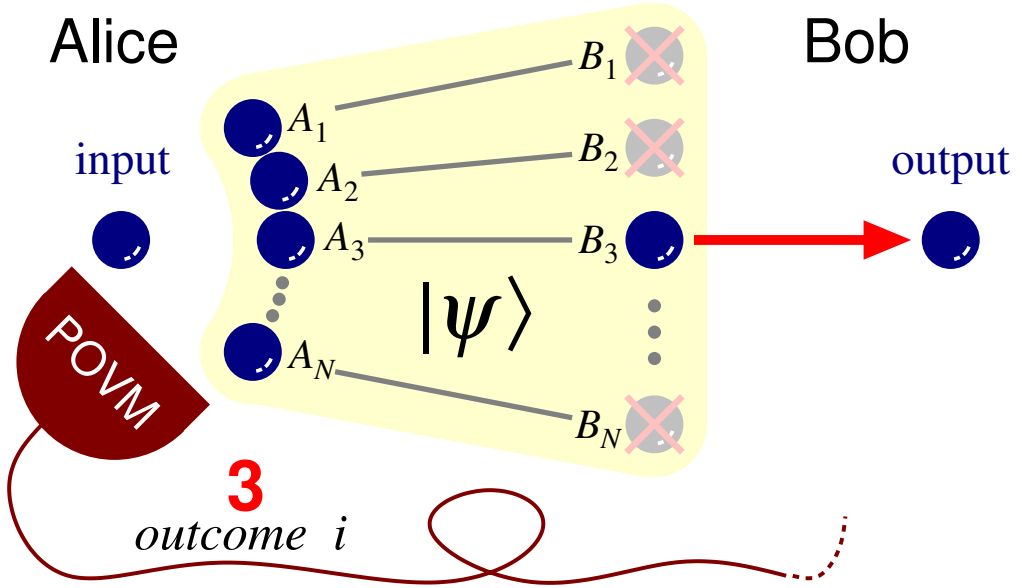
$$\text{tr}\bar{\eta}^2_{\text{signal}} \leq \frac{1}{(1-\epsilon)d^{N+1}}$$

- Standard teleportation $\cdots$ $\text{tr}\bar{\eta}^2_{\text{signal}} = \frac{1}{d^2}$
- Port-based teleportation $\cdots$ $\text{tr}\bar{\eta}^2_{\text{signal}} = \frac{1}{d^{N+1}}(1 + \frac{d^2-1}{N})$

"What novel forms of computation might lead from here?"

Entanglement recycling

[S. Strelchuk, M. Horodecki, J. Oppenheim, PRL **110**, 010505 (2013)]



Discarded $N-1$ ports still work for port-based teleportation!

After teleporting k qubits, $F \geq 1 - \frac{11k}{2N}$

Performance $\approx$ simultaneous transmission ($\frac{N!}{(N-k)!}$ outcomes)

Outline

- **Port-based teleportation**

  [SI and T. Hiroshima, PRL **101**, 240501 (2008); PRA **79**, 042306 (2009)]

- **Its applications**

  - universal programmable processor

  - attacking position-based cryptography

    [S. Beigi and R. König, New J. Phys. **13**, 093036 (2011)]

  - generalized teleportation and entanglement recycling

    [S. Strelchuk, M. Horodecki, and J. Oppenheim, PRL **110**, 010505 (2013)]

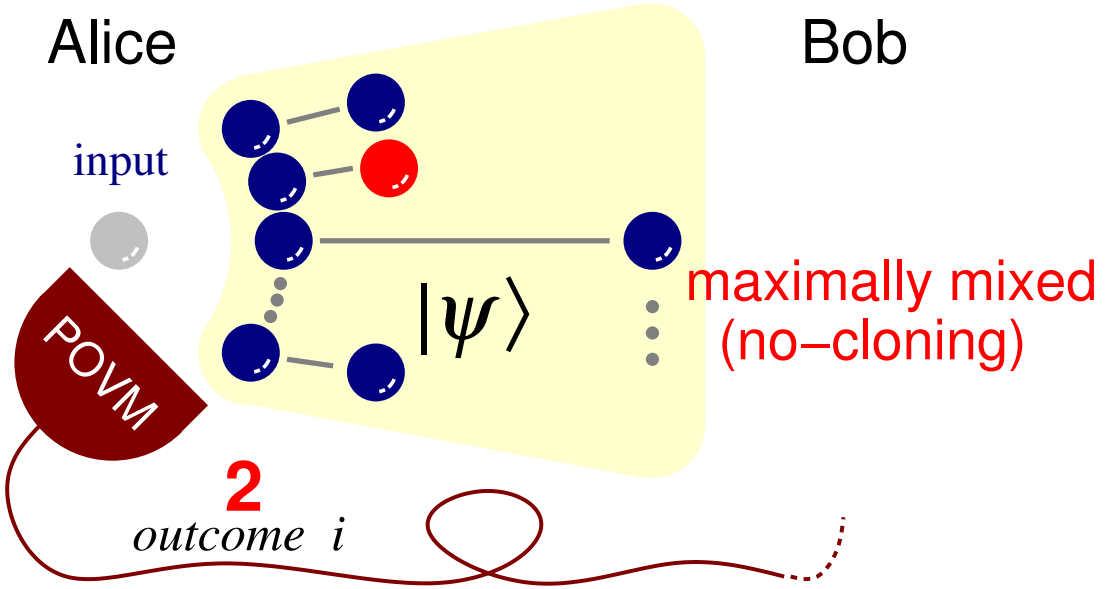
  - relation to no-signaling

    [D. Pitalúa-García, arXiv:1206.4836 (2012)]

No-signaling & port-based teleportation

[D. Pitalúa-García, arXiv:1206.4836 (2012)]

$$P_{\text{success}} \leq \frac{N}{4^n + N - 1}$$ from no-cloning and no-signaling



Standard teleportation is still possible with $\frac{1}{4^n}(P_{\text{sucsess}} - q_j)$

$$q_j + \frac{1}{4^n}(P_{\text{sucsess}} - q_j) \leq \frac{1}{4^n}$$ (no-signaling)