エンタングルメントネットワークの生成と応用

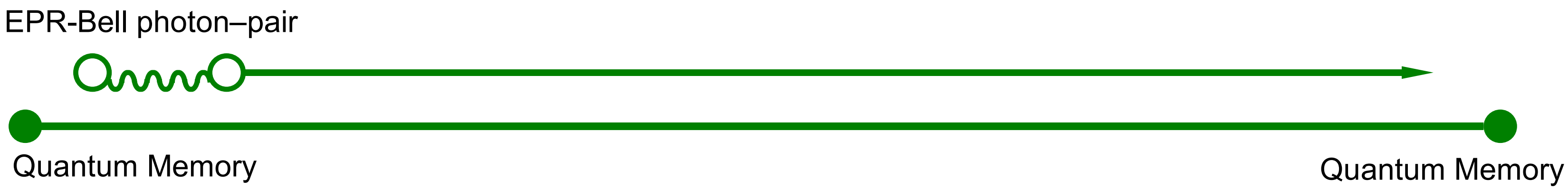
国立情報学研究所

山本喜久
松本啓史
根本香絵

エンタングルメント対の生成

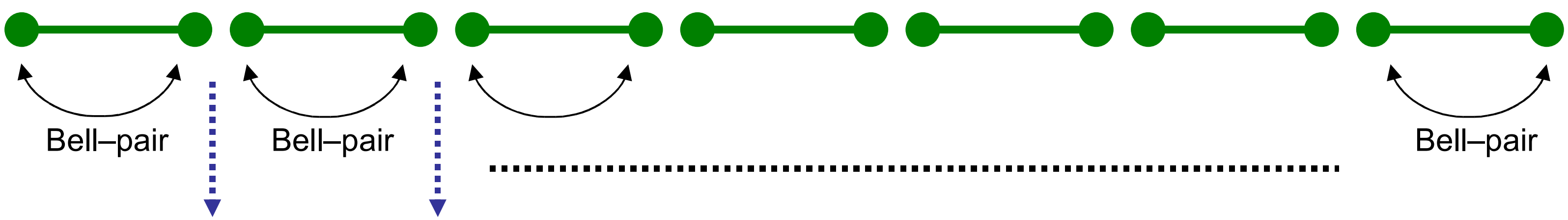
Principle of Quantum Repeater

-How to distribute entanglement between two distant nodes?-



Probability of successful transmission of a single photon: $P(L) = e^{-L/L_0}$ (L_0 : absorption length)

Average number of trials until the first success: $n(L) = \dfrac{1}{P(L)} = e^{L/L_0}$ ⇨ Exponential scaling (L=500km → 10^{13} trials)
Each trial costs 5 msec → 2000 years!!



EPR-Bell measurement → Quantum teleportation (entanglement swapping)

Average number of trials per section: e^{L/NL_0}

Total number of trials: $n'(L) = Ne^{L/NL_0} \xrightarrow[\text{if} \quad N = \frac{L}{L_0}]{} n'(L) = e\dfrac{L}{L_0}$

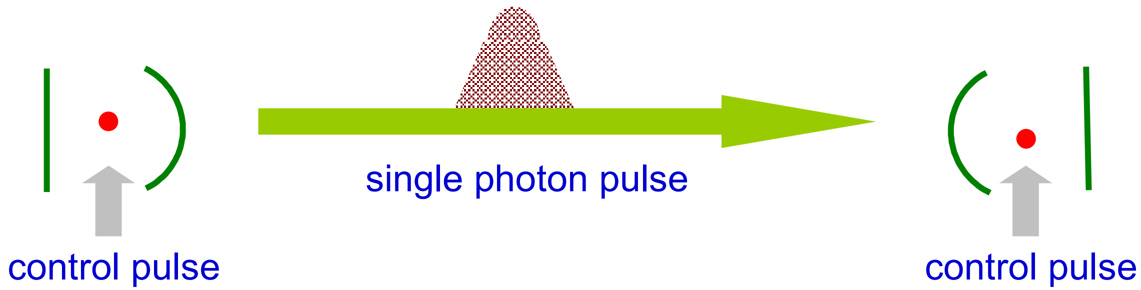
⇨ Linear scaling (L=500km → 90 trials)
10msec!! (simultaneous processing)

A quantum repeater is a long distance fiber interferometer connected by distributed quantum computers. How to construct it as a practical system based on realistic devices?

Entanglement Distribution with Single Photons

Stimulated Raman Adiabatic Passage (STIRAP)

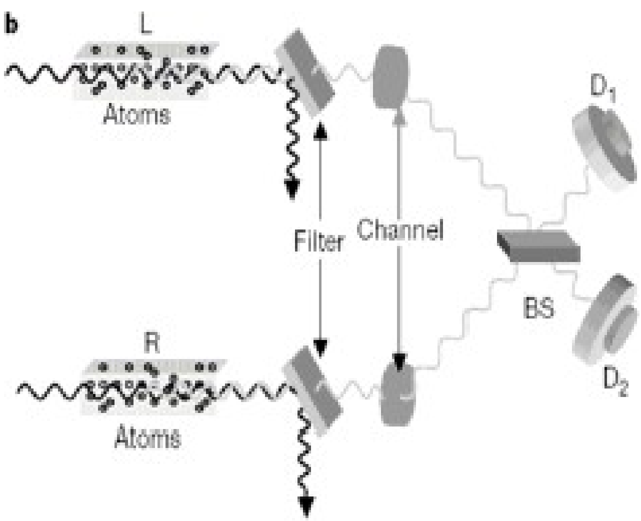
J.I. Cirac, P. Zoller, H.J. Kimble and H. Mabuchi, Phys. Rev. Lett. 78, 3221 (1997)



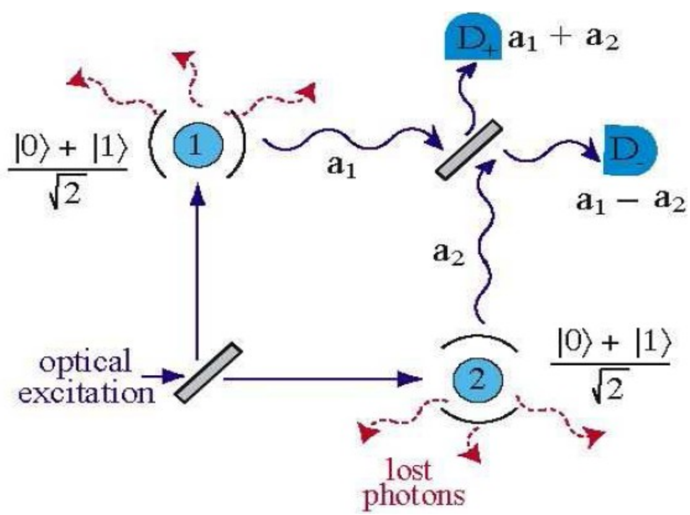
- two strictly identical nodes
- photon bandwith much smaller than atom-cavity coupling constant (adiabaticity)
  - ☐ solved by W. Yao et al., Phys. Rev. Lett. 92, 30504 (2005)
- strong coupling regime
- large detuning
- solution unknown for arbitrary (distorted) pulse shape

solved by D. Fattal et al., Quant-ph/0606204 (2006)

Detection of single photons (post-selection)



L.-M. Duan, M.D. Lukin, J. I. Cirac, P. Zoller, *Nature* **414**, 413 (2001)



L. Childress, J.M. Taylor, A.S. Sörensen, M.D. Lukin, *Phys. Rev. A 72, 52330* (2005)

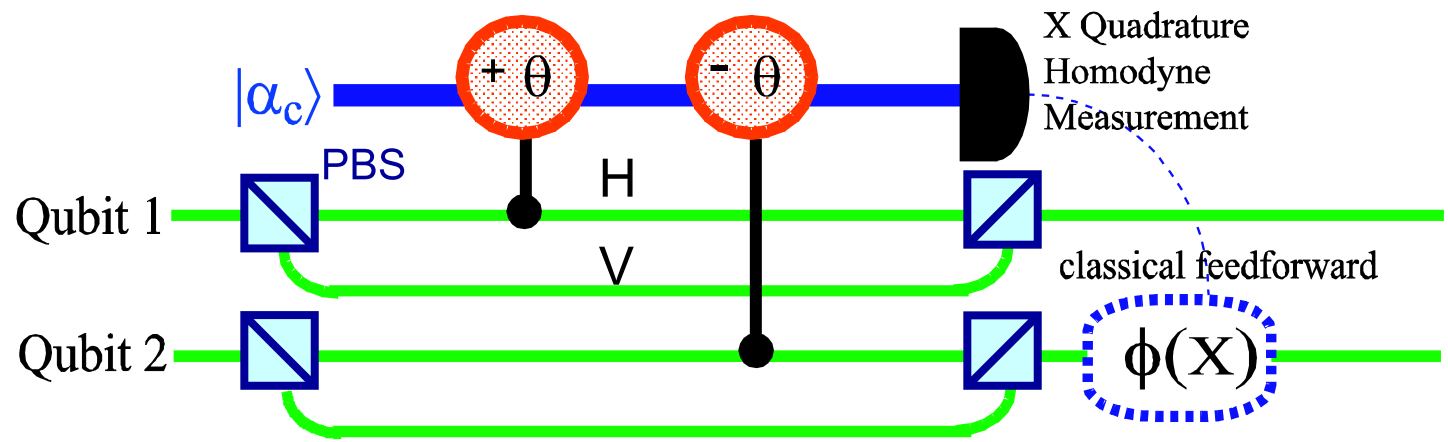
Entanglement shareing using coherent state

- QND measurement can be used to do parity measurement.

Input states:

$$|\Psi_{in}\rangle_1 = c_0|H\rangle + c_1|V\rangle$$

$$|\Psi_{in}\rangle_2 = d_0|H\rangle + d_1|V\rangle$$

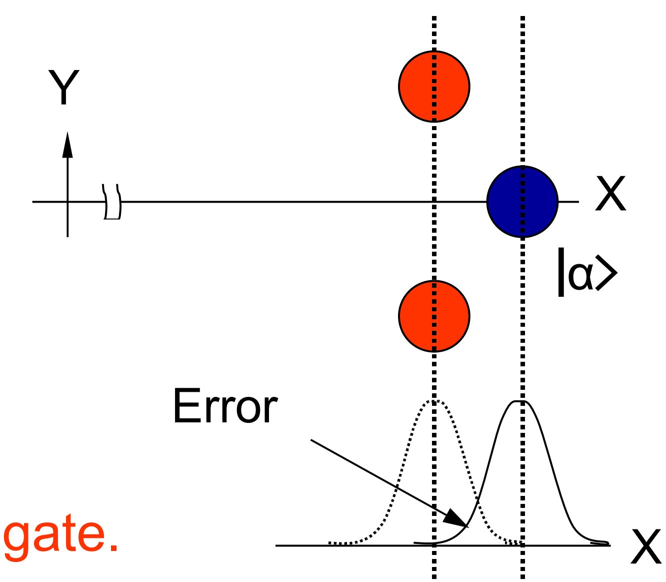


Kae Nemoto, *et. al.*, PRL 93, 260502 (2004)

Output state before the measurement:

$$|\Psi_T\rangle = c_0 d_0|HH\rangle|\alpha\rangle + c_1 d_1|VV\rangle|\alpha\rangle + c_0 d_1|HV\rangle|\alpha e^{i\theta}\rangle + c_1 d_0|VH\rangle|\alpha e^{-i\theta}\rangle$$

Dependent on the measurement outcome, we can distinguish these two states.



- This parity measurement works as a entangling gate.

S Barrett, *et. al.*, PRA 71, 060302R (2005)

PHYSICAL REVIEW B **71**, 014401 (2005)

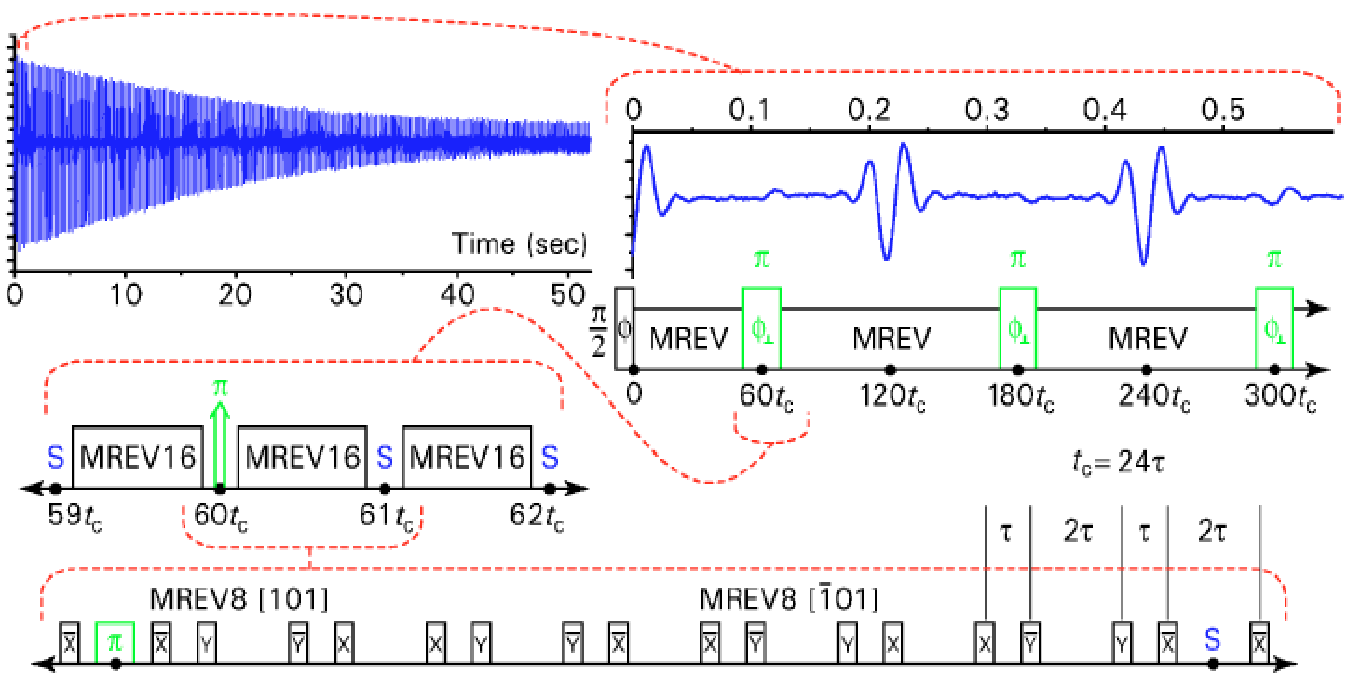
Coherence time of decoupled nuclear spins in silicon

T. D. Ladd,* D. Maryenko,† and Y. Yamamoto‡
Quantum Entanglement Project, SORST, JST, Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085, USA

E. Abe and K. M. Itoh
Department of Applied Physics and Physico-Informatics, CREST, JST, Keio University, Yokohama, 223-8522, Japan
(Received 18 August 2004; published 4 January 2005)

Nuclear spin decoherence t
are very long
(T_{2N} ℑ 25 s at 300K)

Quantum memory



エンタングルメント対の利用

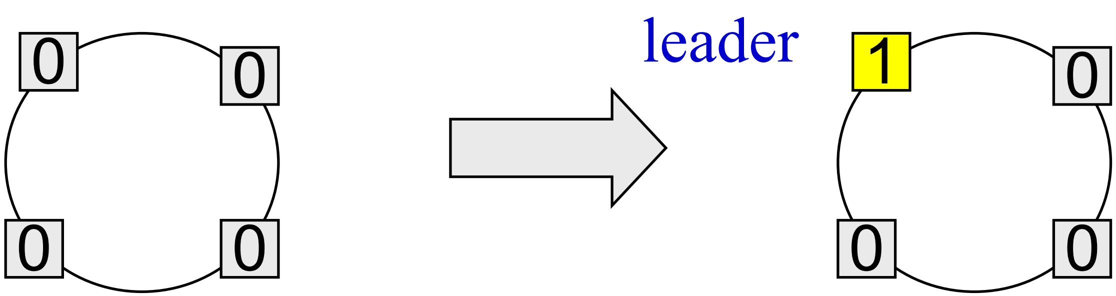
Anonymous Leader Election Problem (LE)

Given n parties connected by communication links, elect a unique leader from among n parties.

Under the anonymity Condition:

- Initially, all parties are in the same state.

  ⇒Every party needs to perform the same algorithm.



No classical algorithm can solve LE with zero-error, even with infinite computation time

We invented a quantum algorithm with $O(n^2)$ rounds and $O(n^4)$ communication complexity, which solve LE with any network topology. (Use amplitude amplification)

LOCC state Estimation

- Given n-copies of unknown bipartite pure state, shared by A and B with n≒20 or more.
  $\{|\varphi_\theta\rangle\}$: a parameterized family of pure states

- Error measure: mean distance

$$E(D(|\varphi_\theta\rangle, |\varphi_{\theta est}\rangle)^2) = a/n + b/n^{3/2} + c/n^2 + \ldots$$

want to minimize a, b, c, …. except for exponentially small order.

Question: Can we do as good as global measurement?

YES for entangled state,
No for separable state (some exceptions)

Self-teleportation [M 07]

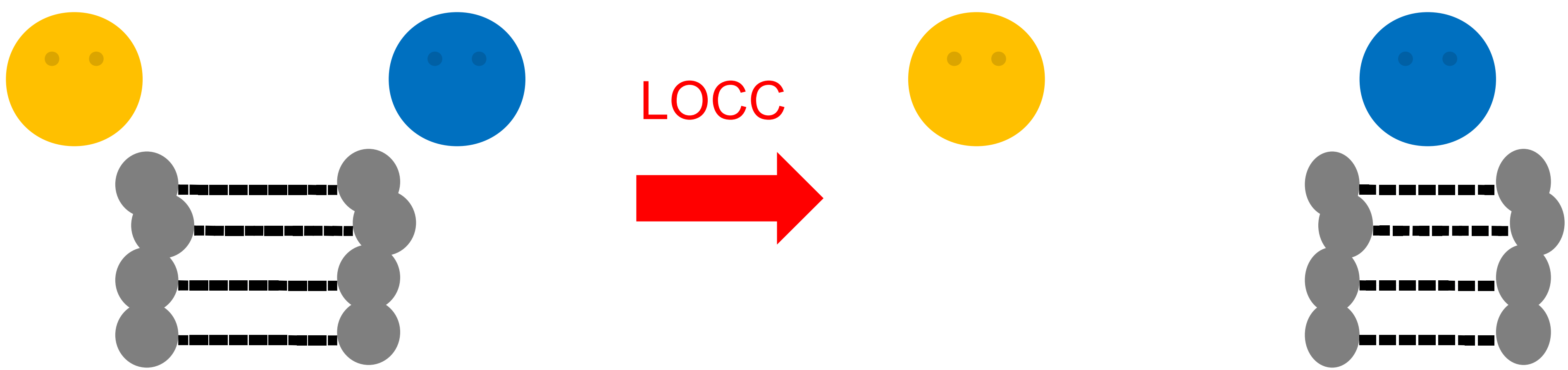
1. A and B share given ***n*** copies of an unknown pure entangled state.

$$|\varphi\rangle = \sum_{i=1}^{d} \sqrt{p_i}\, |i\rangle_A |i\rangle_B \qquad p_1 \geq p_2 \geq \cdots \geq p_d$$

2. By LOCC, A sends her quantum info to B.

   No quantum channel, No extra entangled states

   Without sacrificing any of pairs

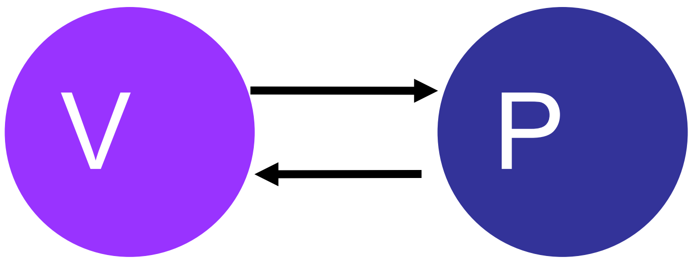


$|\varphi\rangle_{AB}^{\otimes n}$

Error: p_1^n

$|\varphi\rangle_{BB}^{\otimes n} + \varepsilon$

(Quantum) Interactive Proof System



- **Want to solve {Yes No} question**
- **Prover**

  always asserts **Yes**, even if **No** is true

  can do **any unitary**
- **Verifier**

  checks **P**'s assertion with high probability.

  can do (quantum) **polynomial time** computation

An important building block of protocols.

Also plays essential role in the theory of approximation algorithm

Multi-prover proof systems

- **Provers**

  all provers insists on **a common proposition**

  can do **any** unitary

  May share the entanglement and/or randomness
- **Verifier**

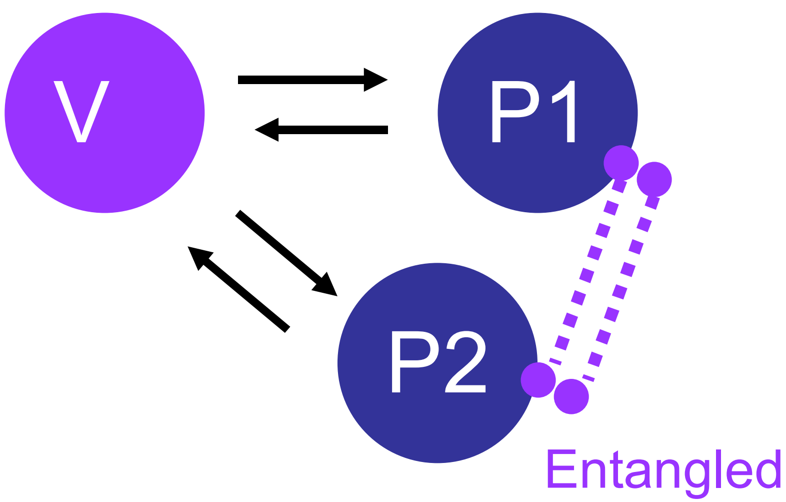
  checks his assertion via interaction with high probability.

  can do quantum polynomial time computation

Our results

1. How to prevent P's to use entanglement to crack classically secure protocols

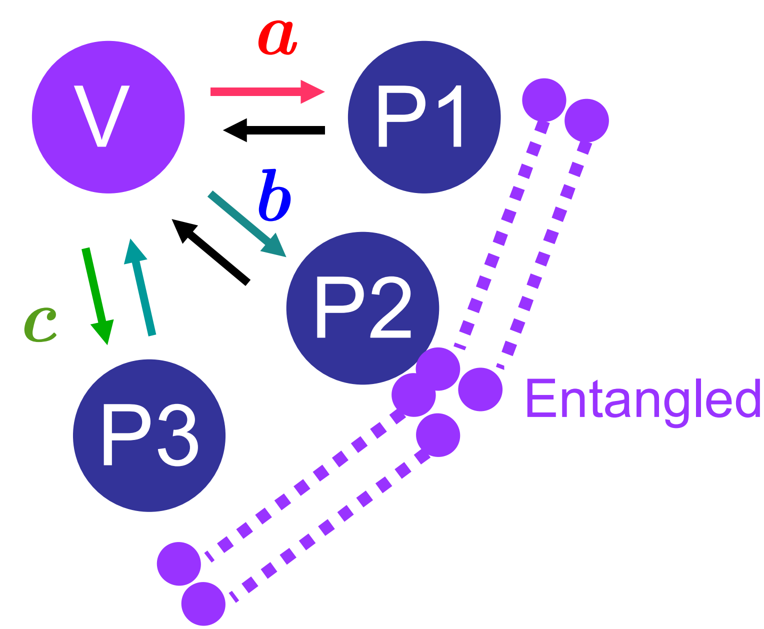
2. m-prover r-message systems =2-prover 3-message systems



.

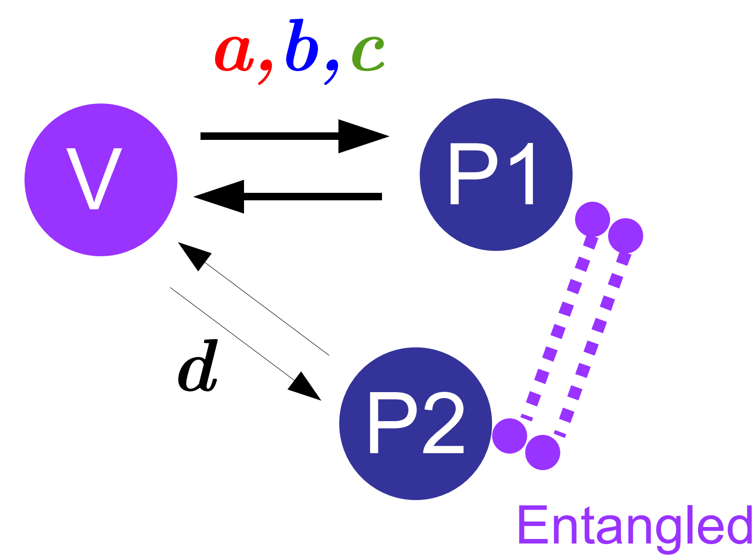
How to prevent provers to use entanglement to crack classical protocols

$c = a$ or b (chosen randomly)
V checks consistency
the answers



modify

$c = a$ or $b$or c (chosen randomly)
V checks consistency
the answers



Conclusions

DPS quantum repeater based on weak coupling cavity QED nodes and coherent state pulses

15–20Km spacing, 1 ebit/s over 1000Km

DPS quantum repeater based on strong coupling cavity QED nodes and single photon pulses

100Km spacing, 0.01ebit/s over 1000km

- **Applications**

1. Zero-error & efficient quantum algorithm for LE (classically, impossible)

2. Self-teleportation and its application to LOCC state estimation

3. Interactive proof systems

3.1 Multi-prover systems

Preventing cheating use of entanglment

Amplification of success probability (Amplitude amplification)

Reducing the number of rounds and provers

3.2 Zero-knowledge proof

Composition of the proof system robust against quantum attack,

Feasible even for computational and perfect zero-knowledge,

and for one-sided error

Conclusions

- **DPS quantum repeater based on weak coupling cavity QED nodes and coherent state pulses**

  ⇒ 15–20Km spacing, 1 ebit/s over 1000Km

  DPS quantum repeater based on strong coupling cavity QED nodes and single photon pulses

  ⇒ 100Km spacing, 0.01ebit/s over 1000km

- **100GHz clock frequency quantum computing system**

  one bit gate by single off-resonant Raman pulses

  ⇒ 100fsec for U(1) operation
  10psec for SU(2) operation

  two bit gate based on coherent state qubus

  ⇒ non-local, deterministic, measurement-free two qubit operation

- **Semiconductor donor impurity as a building block (^{31}P:Si, ^{19}F:ZnSe)**

  Experiments in progress