Conference key-agreement and secret sharing through noisy GHZ states

Kai Chen and Hoi-Kwong Lo

Center for Quantum Information and Quantum Control,
Dept. of Elect. & Computer Engineering (ECE),
& Dept. of Physics
University of Toronto

July 20, 2004

Reference: quant-ph/0404133

Outline

- Background and motivation
- Tasks: Conference key-agreement and secret sharing in a noisy channel
- What’s the approach?
- Results and significance
- Summary and future scope

Background and motivation (I)

Theoretical

- Entanglement distillation (for bipartite case much is known)
- Distill multipartite entanglement directly (proved to be more efficient than two-party distillation separately)
- Better understand and quantify multipartite entanglement

Practical

- New application of quantum cryptography in multipartite setting

Bridge the gap

- Develop a class of protocols with feasible experimental technology
  - Conference key-agreement
  - Quantum sharing of classical secrets

Motivation (II): Why use multipartite entanglement?

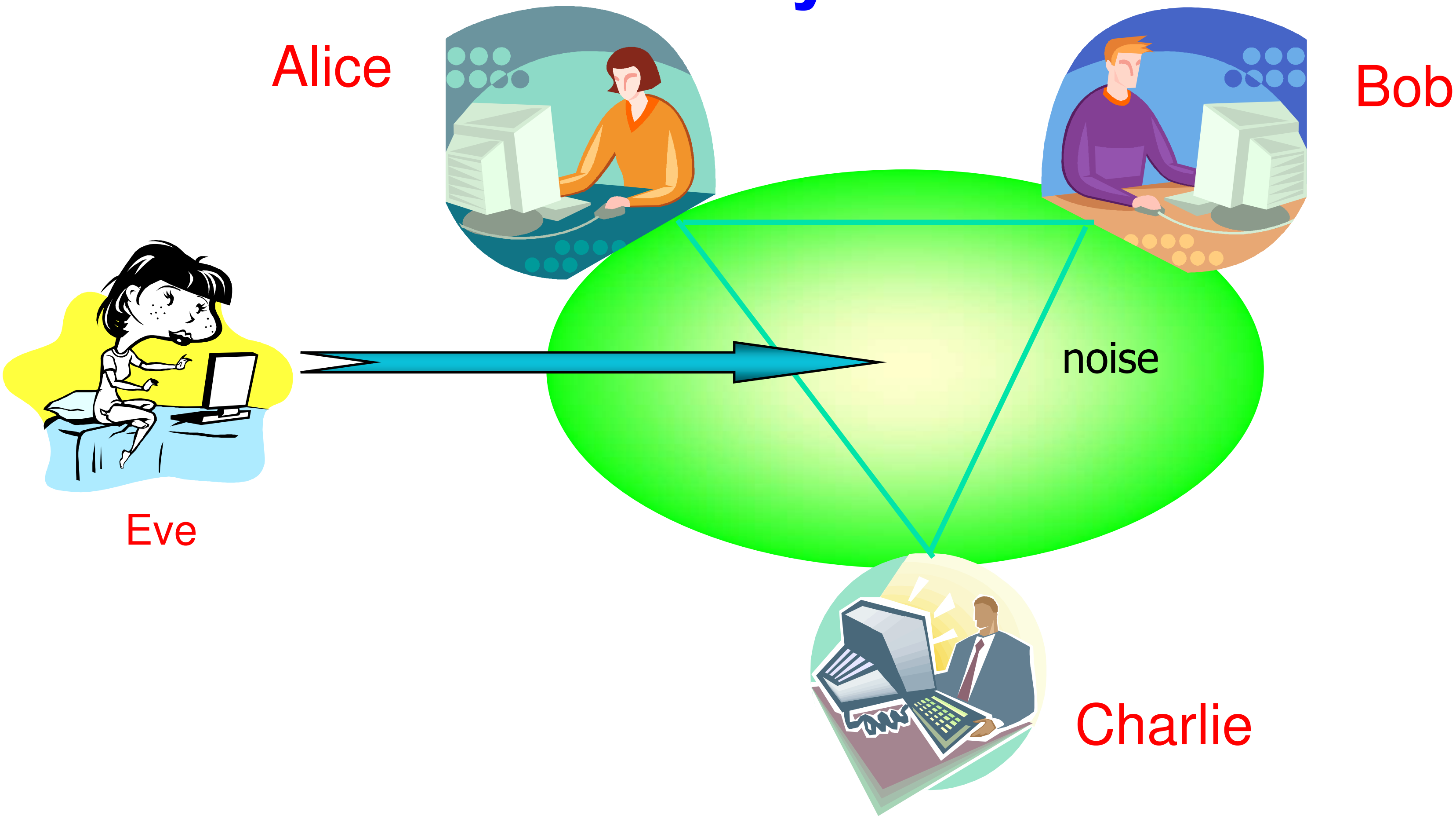
For conference key-agreement protocols:

- Alternative solution
- Relatively less sources
- Nice physical insight
- Advantage: more efficient, more robust

For secrets sharing, comparing with QKD+classical secret sharing scheme

- Finish information splitting and eavesdropper protection simultaneously

Task 1: Conference key-agreement scheme in a noisy channel



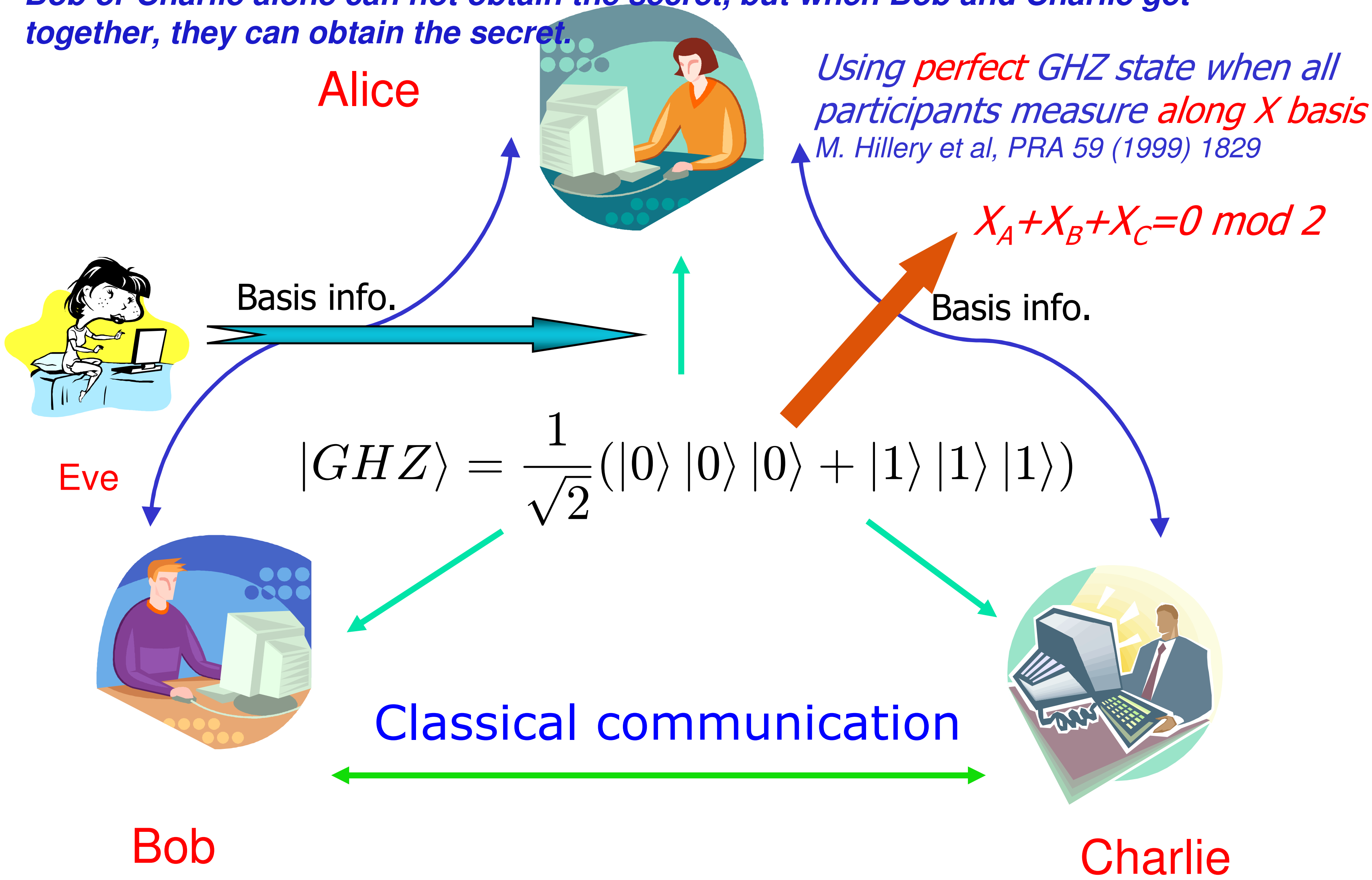
Task: Alice, Bob and Charlie generate the same secure key string k.

Solution: Using GHZ state (Greenberger-Horne-Zeilinger states):

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)$$

Task 2: Quantum Sharing of classical Secrets in a noisy channel

Task: Alice wants to share a secret with Bob and Charlie, in such a way that either Bob or Charlie alone can not obtain the secret, but when Bob and Charlie get together, they can obtain the secret.



Our approach

- Push Shor-Preskill and Gottesman-Lo's ideas to multipartite case.
- Reduce security of cryptographic protocols to a class of distillation problems of the GHZ states
- Prepare and measure type protocols impose some restrictions on possible local operations of participants for the GHZ state distillation.

PHASE ERROR DETECTION STRICTLY FORBIDDEN!
(Phase error syndrome NOT available without quantum computers.)

Correspondence between CSS codes and BB84 (Shor-Preskill's proof)

CSS codes		BB84
bit flip error correction	⟺	error correction
phase error correction	⟺	privacy amplification (to remove Eve's info.)

PRL 85 (2000) 441

N.B.: CSS stands for Calderbank-Shor-Steane codes.

Correspondence between EDP and BB84

(Gottesman-Lo's proof)

EDP: Entanglement Distillation Protocol

2-way classical communications

CSS codes		BB84/six-state
bit-flip error detection	⟺	"advantage distillation"
bit flip error correction	⟺	error correction
phase error correction	⟺	privacy amplification

IEEE Trans. Inf. Theor. 49 (2003) 457

Notations

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle)$$

- stabilizer formulation of GHZ state

$$\begin{aligned} S_0 &= X \otimes X \otimes X, \\ S_1 &= Z \otimes Z \otimes I, \\ S_2 &= Z \otimes I \otimes Z. \end{aligned}$$

- GHZ basis

$$|\Psi_{b_0,b_1,b_2}\rangle_{ABC} = \frac{1}{\sqrt{2}}(|0\rangle|b_1\rangle|b_2\rangle + (-1)^{b_0}|1\rangle|\overline{b_1}\rangle|\overline{b_2}\rangle$$

(b_0, b_1, b_2) correspond to the eigenvalues of the 3 stabilizer generators S_0, S_1, S_2 by correspondence relation:

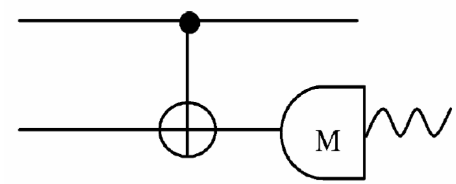
$$\begin{aligned} \text{eigenvalue } \quad 1 &\longrightarrow \text{label } 0, \\ \text{eigenvalue } -1 &\longrightarrow \text{label } 1. \end{aligned}$$

Thus one can label a GHZ-basis diagonal state as

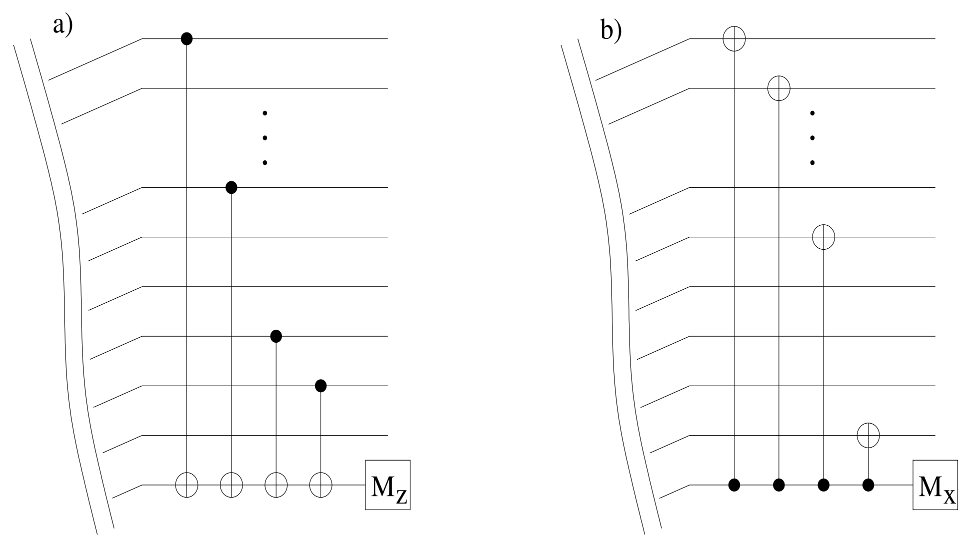
$$\rho_{ABC} = \{p_{000}, p_{001}, p_{010}, p_{011}, p_{100}, p_{101}, p_{110}, p_{111}\}$$

Conference key-agreement scheme in a noisy channel

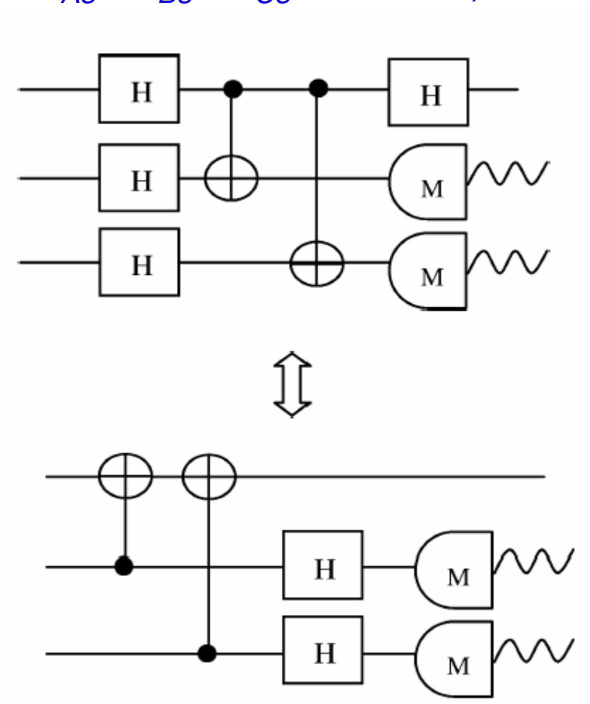
B step: bit-flip error detection
(keeps the first trio iff $M_{A2}=M_{B2}=M_{C2}$)



Multi-partite one-way hashing protocol *(from Maneva and Smolin, quant-ph/0003099)*



P step: phase-flip error correction
(3 qubits majority code)
(apply correction to the first trio (say a Z operation on Alice) iff $M_{A2}+M_{B2}+M_{C2}=M_{A3}+M_{B3}+M_{C3}=1 \bmod 2$)



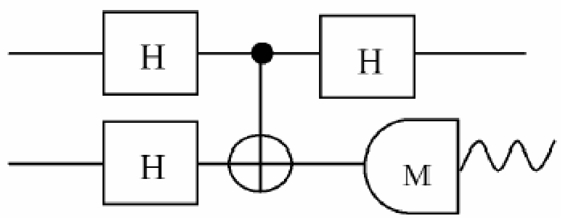
Yield: $D_h = 1 - \max_{j>0}[\{H(b_j)\}] - H(b_0)$

Our Improved yield:

$$D_h' = 1 - \max\{H(b_1), H(b_2|b_1)\} - H(b_0) + I(b_0; b_1, b_2)$$

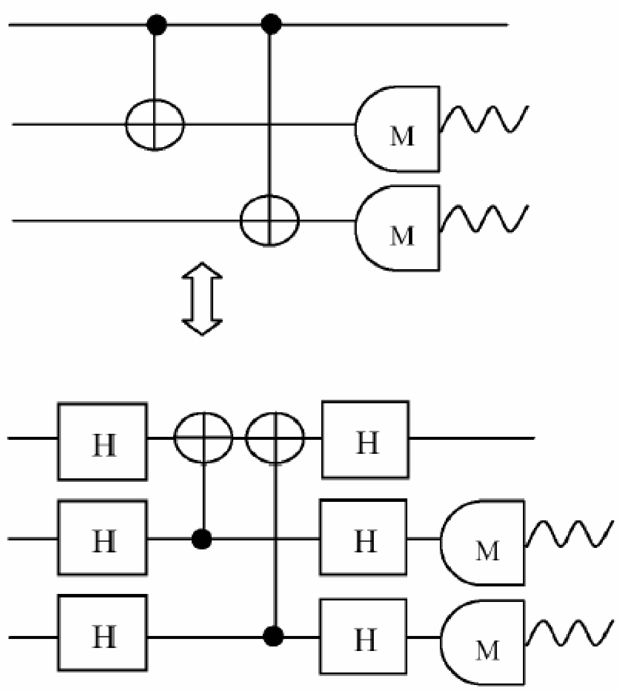
Quantum Sharing of classical Secrets in a noisy channel

B′ step: bit-flip error detection



(keeps the first trio iff $M_{A2}+M_{B2}+M_{C2}=0 \ mod \ 2$)

P′ step: phase-flip error correction (3 qubits majority code)



(apply correction to the first trio iff

$M_{A2}+M_{B2}=M_{A3}+M_{B3}=1$: an X operation on Bob

$M_{A2}+M_{C2}=M_{A3}+M_{C3}=1$: an X operation on Charlie

+ Multi-partite one-way hashing protocol

Reduction to prepare and measure type protocols

- Depolarization to the GHZ-basis diagonal states (applying stabilizer generators with probability 1/2)
- Error rate estimation and derivation of density matrix (GHZ-basis diagonal) by measuring stabilizer group elements
- Adaptively apply B and P steps plus random hashing method, which can be done by local individual quantum measurements and local classical computations and classical communications *(CCCCs)*

Remark:

1. All the participants do not need to perform phase error correction. (The point is that, it would have been successful, if they had performed it).
2. They simply to take the parity $Z_1+Z_2+Z_3$ *mod 2* for conference key-agreement and the parity $X_1+X_2+X_3$ *mod 2* for secret sharing in the phase error correction procedure. No classical communication is needed.

Our results

For Werner-like states: $\rho_W = \alpha \left|GHZ\right\rangle \left\langle GHZ\right| + \frac{1-\alpha}{2^N} I, \quad 0 \le \alpha \le 1,$

where the fidelity F is defined as $F = \left\langle GHZ\right| \rho_W \left|GHZ\right\rangle = \alpha + \frac{1-\alpha}{2^N}$

- Secure conference key-agreement is attainable whenever *F>0.3976* while for secret sharing whenever *F>0.5372*

Significance

- *Better than protocols with only one-way classical communications which will fail whenever F≤9/16=0.5625*
- *Better than the requirement of violation of the standard Bell inequality F>9/16*
- *Reduction to protocols with only bi-partite entanglement: feasible with current technology*

In a prepare-and-measure protocol, Alice has the option to *pre-measure* her subsystem (the same as the Shor-Preskill and Gottesman-Lo's arguments).

Summary and further scope

- Start with protocols for GHZ distillation and reduce it to *prepare-and-measure* type protocols for quantum cryptography.
- Our protocols can be implemented with only *bi-partite* entangled states which are feasible with current technology.
- This is only a first step of theoretical demonstration for multipartite entanglement to quantum cryptography.

More work should be done:

1. Exploring more parties and more complicated structure of quantum cryptographic tasks. e.g. secret sharing for a general access structure.
2. Develop better protocols which works for more noisier states and higher yield.
3. Experimental realization (we are actively discussing with experimentalists on implementation).

Reference: quant-ph/0404133

Thank you!