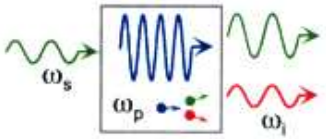


UNCONDITIONALLY SECURE QUANTUM BIT COMMITMENT

Horace P. Yuen
Center for Photonic Communication and Computing
Department of Electrical and Computer Engineering
and Department of Physics and Astronomy
Northwestern University, Evanston, IL 60208-3118
Tel: (847) 491-7335; Fax: (847) 491-4455;
E-mail: yuen@ece.northwestern.edu

quant-ph/ 0305142
0305143
0305144

BIT COMMITMENT
(2-party protocol)

	Example
• A gives evidence to B for committed bit **b**	bit written on paper locked in a box
• bit concealing to B	Can't open box
• A opens **b**	Gives box key to B
• B verifies	Checks bit on paper in box
• Binding on A	Can't change words on paper in box

QUANTUM BIT COMMITMENT (simplest scenario)

Commitment:

- A gives B state space $\mathbf{H}^{B}$ in one of M possible states $|\phi_{bi}\rangle$ for **b = 0,1**

$$|\Phi_b\rangle = \sum_i \sqrt{p_{bi}}\,|e_i\rangle|\phi_{bi}\rangle$$

Opening:

- A tells B which $|\phi_{bi}\rangle$ he gave her

Verification:

- B verifies by measuring corresponding projector $|\phi_{bi}\rangle\langle\phi_{bi}|$
  - perfect verification: probability of yes equals 1

- B's cheating:

  Try to determine **b** from evidence

  Optimal probability

$$\overline{P_c^B} = \underbrace{\frac{1}{4}}_{\text{guessing level}}(2 + \underbrace{\left\|\rho_0^B - \rho_1^B\right\|_1}_{\text{trace distance}})$$

- A's cheating: **Assume perfect** opening for **b** = 0,

  $\overline{P_c^A}$ **probability that B measures** yes on **b** = 1

  verifying measurement optimized over his action

- Perfect concealing: $\overline{P_c^B} = \frac{1}{2}$

- Perfect binding: $\overline{P_c^A} = 0$

UNCONDITIONAL SECURITY (US)

- Security parameter n

$$\lim_{n\to\infty} \overline{P_c^B}(n) = \frac{1}{2}, \qquad \lim_{n\to\infty} \overline{P_c^A}(n) = 0$$

equivalent to

- ε-concealing $\overline{P_c^B}(n) \le \frac{1}{2} + \varepsilon_n$

- ε-binding $\overline{P_c^A}(n) \le \varepsilon_n$

$$\varepsilon_n \to 0$$

Cheating probabilities computed under ideal (no imperfection of any kind) conditions, restricted only by logic and the laws of physics

---- facts of nature?!

- Thus not affected by technology advance

GENERAL IMPOSSIBILITY PROOF FOR US QBC (Mayers, Lo & Chau)

- Pure state $|\Phi_b\rangle$ shared between A & B ($H^A \otimes H^B$) at end of commitment
- Perfect concealing ($\rho_0^B = \rho_1^B$) case:

$$|\Phi_1\rangle = U^A |\Phi_0\rangle$$

U^A on H^A determined by Schmidt decomposition

$$|\Phi_b\rangle = \sum_j \sqrt{\tilde{p}_j}\,|e_{bj}\rangle|\tilde{\phi}_j\rangle$$

→ eigenvectors of ρ_b^B

So

$$\overline{P}_c^B = \frac{1}{2}, \overline{P}_c^A = 1$$

IMPOSSIBILITY PROOF CONTD.

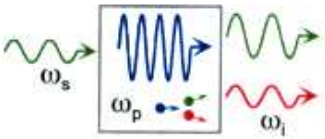
- ε -concealing ($\rho_0^B \sim \rho_1^B$) case:

  A determines U^A from $|\Phi_b\rangle$ and obtains

  $$\lim_{n\to\infty} \overline{P_c^B}(n) = \frac{1}{2} \quad \Rightarrow \quad \lim_{n\to\infty} \overline{P_c^A}(n) = 1 \quad \text{(IP)}$$

  stronger than mere no (US)

EXAMPLE: "BB84"- QBC



$$b=0: \quad \phi_{01} = \uparrow, \qquad \phi_{02} = \rightarrow$$

$$b=1: \quad \phi_{11} = \nearrow, \qquad \phi_{12} = \searrow$$

- Perfect concealing $\rho_0^B = \rho_1^B = \mathrm{I}/2$
- If A cheats by declaring, say ϕ_{11} on $\phi_{01,}$ $p_A = 1/2$

  Thus $P_c^A < \varepsilon$ in an n-sequence $P_c^A = p_A^n$.
- If A entangles ϕ_{01} and ϕ_{02}, can cheat with $P_c^A = 1$ by EPR attack.

TWO DISTINCT ISSUES

Whether there is, for US QBC:

1) An impossibility theorem
2) A protocol provably unconditionally secure

A priori
No Impossibility Theorem
without QBC Definition

Similar to:

No Church-Turing theorem (onlyThesis)
without definition of "algorithm"

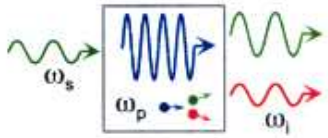
Different Forms of algorithms:

Turing, Post, Markov, etc.

Different Types of QBC protocols:

1,2,3,4,… from cheating detection,
quantum games,
evidence questioning etc.

EXAMPLE: SPLIT ENTANGLED PAIR



- $\left|\mathrm{A}\right\rangle\!\rangle \equiv \sum_{n,m} \mathrm{A}_{\mathrm{n,m}} \left|n\right\rangle \left|m\right\rangle$

$$\left\langle\!\left\langle \mathrm{B} \middle| \mathrm{A} \right\rangle\!\right\rangle = tr\mathrm{B}^{\dagger}\mathrm{A}$$

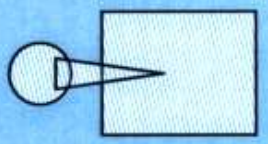
- $A \otimes B \ \left|\mathrm{C}\right\rangle\!\rangle = \left|\mathrm{ACB}^{\mathrm{T}}\right\rangle\!\rangle$

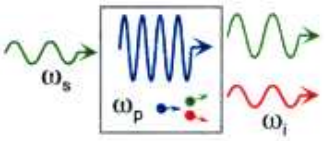
- $\left|\mathrm{A_b}\right\rangle\!\rangle$ for bit b=0,

  second qubit committed

  first qubit to open

safe/key





EXAMPLE: continues

- Perfect concealing $\rho_0^B = \rho_1^B$

$$A_0^\dagger A_0 = A_1^\dagger A_1 \qquad (*)$$

- Perfect cheating by Adam

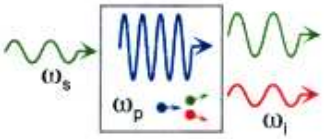
$$A_1 = U^A A_0 \qquad from\ (*)$$

so he can apply $U^A \otimes I$

◆ This is an impossibility proof different from IP

$\Longrightarrow$ IP at best incomplete.

QBC4p & QBC4



i. B sends A

$$\Psi_k = (U_k \otimes I)\Psi_{12}^- \in \mathcal{H}_1 \otimes \mathcal{H}_2,$$

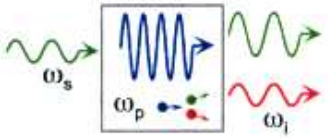
$\{U_k\} = \{I, R_z\}$, R_z the rotation by $\pi/2$ around qubit z-axis

ii. A applied $U_0 = I$ or $U_1 = \sigma_x$ on $\mathcal{H}_2$, and commits it as evidence.

iii. A opens by sending in $\mathcal{H}_1$; B verifies by measurement.

- QBC4 extends QBC4p to a sequence of Ψ_{km}, each U_{km} independently and randomly drawn from $\{I, R_z\}$

QBC4 CONCELING PROOF



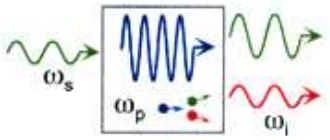
- $\rho_0^B = \rho_1^B$ condition for QBC4p and arbitrary $\{U_k\}$

$$(*) \quad \langle 0 | U_{K'}^{\dagger} U_K | 1 \rangle = \langle 1 | U_{k'}^{\dagger} U_k | 0 \rangle \quad \forall k \neq k'$$

So $(*)$ satisfied for $\{U_k\} = \{I, R_z\}$

- Extension to product for a sequence

QBC4 BINDING PROOF



- assume open perfectly for b=0
- $\{U_k\}$ used with prob $\{\lambda_k\}$ in QBC4p

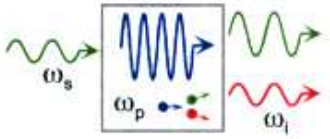
$$P_c^A = \sum_k \lambda_k \left| \langle\langle U_k \, \sigma_x \left| U^A \, U_k \right\rangle\rangle \right|^2 \qquad (*)$$

- $P_c^A < \varepsilon$ bounded away from 1 even though protocol perfectly concealing

  $\Longrightarrow$ IP does not apply here

- $P_c^A < \varepsilon$ in a sequence

FOUR CATEGORIES OF IP GAPS



A. Freedom of Operation

(A1) Honesty and Cheating Generality

--- Libertarian Principle

--- Intent Principle

(A2) Secret nonrandom versus random parameter

(A3) Imperfect Operations

B. Generality of EPR Attacks

--- # of Adam's possible operations M=1

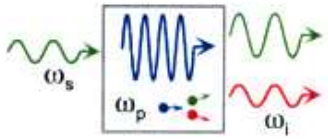
C. Opening Possibilities

(C1) Further Quantum Communications

(C2) Committing only Classical Information

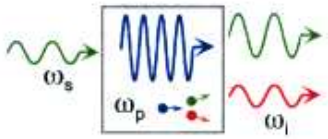
D. Non-uniqueness

SIX NEW TYPES OF QBC PROTOCOLS



- Type 1 – residue classical randomness
  ex. QBC 1 US
- Type 2 – shifting of evidence state space
  ex. QBC 2 US
- Type 3 – anonymous states
  ex. QBC 3 ?
- Type 4 – further quantum communication at opening
  ex. QBC 4 US
- Type 5 – committing only classical information
  ex. QBC 5 US
- Type 6 – necessary condition on concealing or hiding
  ex. ?
  - Note: all US protocols involve split quantum communications at rounds or opening

QUANTUM TELEPORTATION PROTOCOL



- *B* sends *A* $(U_k \otimes I)\Psi_{12}^- \in \mathcal{H}_1 \otimes \mathcal{H}_2$ $\{U_k\}$
- *A* teleports $|b\rangle \in \mathcal{H}_3$ to $\mathcal{H}_1$

  committing only Bell-basis measurement result

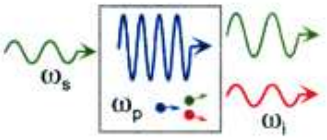
  $i \in \{1,2,3,4\}$ to B
- A opens by submitting $\mathcal{H}_1$

  B verifies $U_k \sigma_i |b\rangle$

- Perfectly concealing if *B* does not entangle $\{U_k\}$

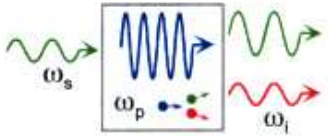
  Need QBC5p if she does entangle

PROTOCOL QBC1



- Babe sends Adam n modified singlet pairs $\Psi_{k\ell} \equiv (U_{k\ell} \otimes I)\Psi_{\ell 12}, \Psi_{\ell 12} \in \mathcal{H}_{\ell 1} \otimes \mathcal{H}_{\ell 2}, k_\ell \in \{1,2,3,4\}, \ell \in \{1,...,n\}$ with each $U_{k\ell}$ independently and randomly drawn from $\{I, R_x, R_y, R_z\}$, the R's being $\pi/2$ rotations about the qubit axes.
- Adam teleports the states $|\mathrm{b}\rangle$ for the bit b he wants to commit to each of the qubit $\mathcal{H}_{\ell 1}$, with Bell-measurement results $i_\ell \in \{1,2,3,4\}$, committing to Babe the partial results $\{i_\ell'\}, i_\ell' = \{1,4\}$ or $\{2,3\}$.
- Adam opens by announcing b and $\{i_\ell\}$ and sending $\{\mathcal{H}_{\ell 1}\}$ to Babe, who verifies by corresponding measurements on $\{U_{k\ell}\sigma_{i\ell}|\mathrm{b}\rangle\}$.

QBCp2



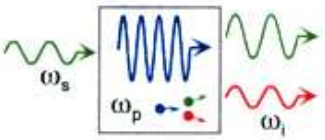
- $\mathcal{H}^{B_1} = \mathcal{H}^{B_{11}} \otimes \mathcal{H}^{B_{12}} \otimes \mathcal{H}^{B_{13}} \otimes \mathcal{H}^{B_{14}}$ 4 qubits

$\{|\psi_k\rangle\} = \{|1\rangle|2\rangle|3\rangle|4\rangle, |4\rangle|1\rangle|2\rangle|3\rangle, |3\rangle|4\rangle|1\rangle|2\rangle, |2\rangle|3\rangle|4\rangle|1\rangle\}$ BB84 states

- A can entangle the permutations among four qubits
- $U_0 = I, U_1 = \pi/2$ rotation on great circle of one qubit $\mathcal{H}^{B_{1i}}$ sent as commitment
- $\rho_0^B = \rho_1^B$ on $\mathcal{H}^{B_{1i}} \otimes \mathcal{H}^{B_2}$
- B checks other three qubits not disturbed also

$\Rightarrow P_c^A < 1$

PROTOCOL QBC1



- Adam sends Babe n qubits, each drawn at random from the set S of four BB84 states and named by its temporal position.
- Babe randomly selects $n - n_0 + 1$ of them and sends them in a random order back to Adam, who asks Babe to reveal the names for $n - n_0$ of them. After verifying them, he modulates the remaining qubit for $U_0 = I, U_1 = R_\pi$.
- Adam opens by declaring b and the states of all n_0 remaining qubits; Babe checks by corresponding projective measurements.