2nd Kyoto Workshop on Quantum Information, Computation, and Foundation
organized by Quantum Information Unit and Yukawa Institute for Theoretical Physics, Kyoto Univ.
September 15, 2021

Non-Interactive Statistically-Hiding Quantum Bit Commitment from Any Quantum One-way Function

Takeshi Koshiba (Waseda Univ.)

This talk is based on a revised version of arXiv:1102.3441.
The revision will be uploaded.

WASEDA University

Bit Commitments

- 2-party cryptographic protocol (between Alice and Bob)
    - Alice has a bit.

- 2-phase protocol (commit phase and reveal phase)
    - **commit phase**
        - Alice puts her secret bit to be sent in a box and locks it.
        - Alice sends the box to Bob via the communication.
        - After the communication, Bob finally gets the box. (Since Bob does not have the key, he cannot unlock the box yet.
    - **reveal phase**
        - Alice sends the key to Bob. Then Bob can get her secret bit from the box.

Requirements for Bit Commitments

* **Hiding**
    * Bob cannot know the contents in the box before he gets the key.
* **Binding**
    * Alice cannot replace the contents after she sends the box.

* In real applications, unconditionally hiding bit commitments are more desirable. Since the commit phase is over in a limited time, it is sufficient to guarantee the binding in a computational sense.

Applications of Bit Commitments

* Fair (Secure) Coin Flipping via Network
* Building Block for Zero-Knowledge Protocol
    * Bitwise commitment of NP-witness
    * Partial reveal so as to keep Zero-Knowledge

Efficiency of Bit Commitments

* Round complexity
  * Reducing Round Complexity of Bit Commitment
  * Reducing Round Complexity of Zero-Knowledge

One-Way Functions and SubClasses

* Evaluation is efficiently computable
* Inversion is computationally intractable
* The existence is unproven, but the most standard assumption in Cryptology

* APS (approximable-preimage-size) OWF
    * For a given image, there exists an algorithm to approximate its preimage-size.
* Regular OWF
    * Every preimage-size is constant.
* OWP (one-way permutation)
    * Length-preserving 1-to-1 function

Classical Bit Commitments

* Naor (J. Cryptol. ’91)
  * unconditional Binding
  * Interacitve, Round Complexity $O(1)$
  * computational Hiding based on PRG (i.e., OWF)
* Naor, Ostrovsky, Venkatesan & Yung (J. Cryptol. ’98)
  * unconditional Hiding
  * Interactive, Round Complexity $O(n/\log n)$
  * Matching UpperBound: Koshiba & Seri (ECCC ’06), Haitner & Reingold (CCC ’07)
  * computational Binding based on OWP

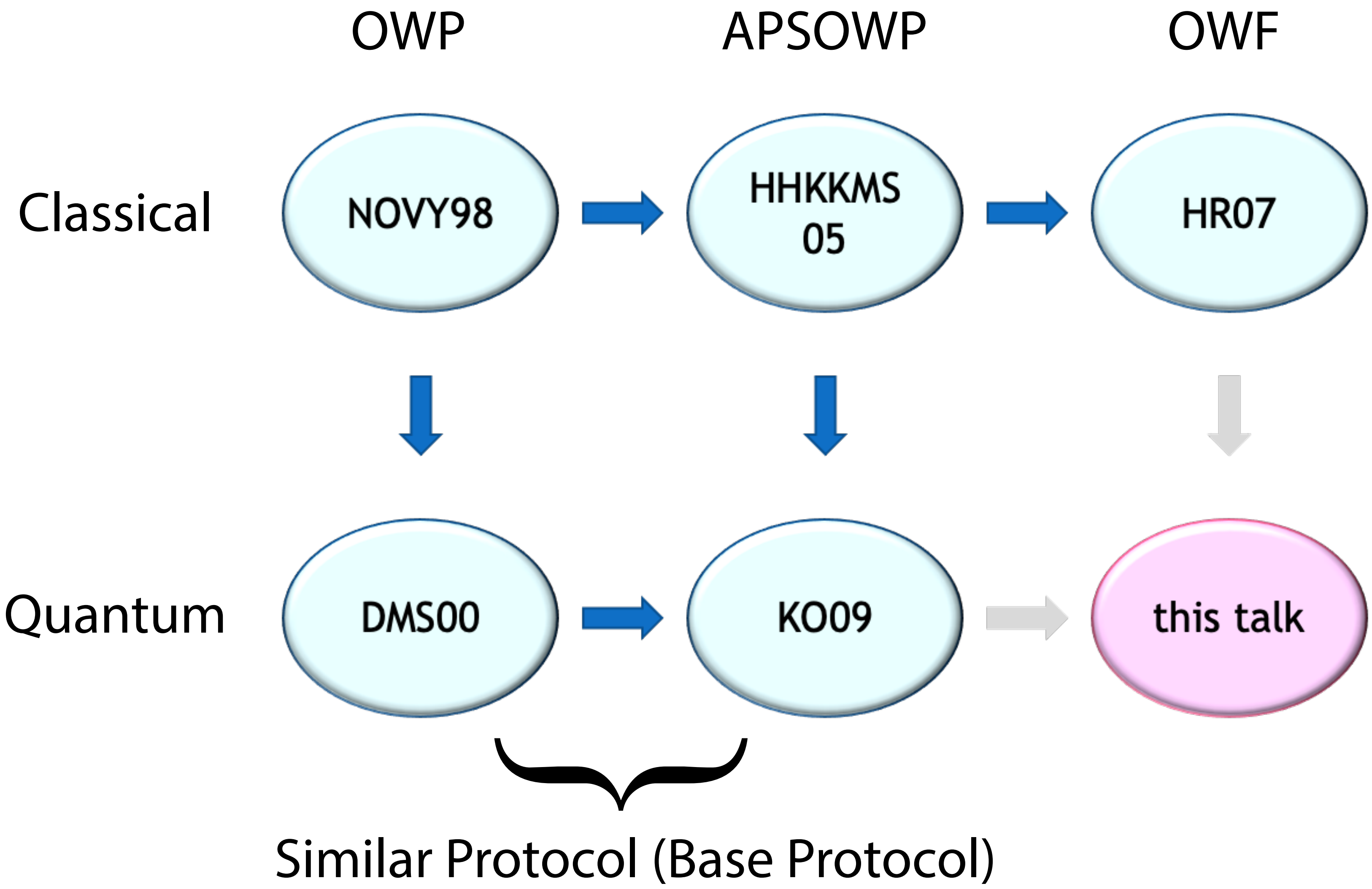
Classical Bit Commitments (cont'd)

* Haitner, Horvitz, Katz, Koo, Morselli & Shaltiel (EUROCRYPT '05, J. Cryptol. '09)
  * unconditional Hiding
  * computational binding based on APSOWF
* Haitner & Reingold (STOC '07)
  * unconditional Hiding
  * computational Binding based on OWF

Quantum Bit Commitments

- Impossibility of QBC with unconditional Hiding & Binding
  - Mayers (PRL ’97), Lo & Chau (PRL ’97)
  - Many variants have been developed.
- Computational
  - Dumais, Mayers & Salvail (EUROCRYPT ’00)
    - unconditional Hiding
    - Non-interactive (Impossible in the classical case)
    - computational Binding based on QOWP
  - Koshiba & Odaira (TQC ’09)
    - QOWP to Quantum APSOWF

Classical & Quantum Bit Commitments



Base Protocol : Outline

* Non-interactive
* Computational Binding based on QOWF
  * Inverting QOWF is reducible to violating Binding
* Unconditional Hiding depends on a special property of QOWF:
  * QOWP [DMS00]
  * APSQOWF [KO09]
  * For general QOWF, we need a new technique.

Tools (1)

* Quantum States
  * $|0\rangle_+, |1\rangle_+$: basis vectors in the computational basis
  * $|0\rangle_\times, |1\rangle_\times$: basis vectors in the diagonal basis
  * $|0\rangle_\times = \dfrac{|0\rangle_+ + |1\rangle_+}{\sqrt{2}}, |1\rangle_\times = \dfrac{|0\rangle_+ - |1\rangle_+}{\sqrt{2}}$

Tools (2)

* Distances
  * Variation distance between probability distributions X and Y
    * $\delta(X, Y) = \frac{1}{2} \left| \Pr[X = a] - \Pr[Y = a] \right|$
  * Trace distance between density matrices ρ and σ
    * $\delta(\rho, \sigma) = \mathrm{tr}\sqrt{(\rho - \sigma)^{\dagger}(\rho - \sigma)}$
  * If we consider density matrices to represent probability distributions, the trace distance coincides with the variation distance.

Tools (3)

* Universal Hashing
  * $\mathfrak{H}$: a uniform distribution over a class of hash functions $h : A \to B$
    * $\forall y_1, y_2 \in B \, \forall x_1, x_2 \in A$ s.t. $x_1 \neq x_2$ $\Pr_{h \leftarrow \mathfrak{H}}[h(x_1) = y_1 \wedge h(x_2) = y_2] = \dfrac{1}{|B|^2}$
* **Leftover Hash Lemma** :
  * Assume that $H_\infty(X) = \lambda$. If the image length of hash functions is $c = \lambda - 2\log(1/\varepsilon)$, then

$$\delta((\mathfrak{H}, \mathfrak{H}(X)), (\mathfrak{H}, U_c)) \leq \varepsilon/2$$

where U_c is the uniform distribution over $\{0,1\}^c$.

Base Protocol : Description

- **Commit Phase** (when Alice has a bit b)
  - Let $\mathfrak{B}(0) = +$, $\mathfrak{B}(1) = \times$.
  - Alice randomly chooses x and sends $|\psi\rangle = |f(x)\rangle_{\mathfrak{B}(b)}$ to Bob.
- **Reveal Phase**
  - Alice sends (b, x) to Bob.
  - Bob measures $|\psi\rangle$ w.r.t. $\mathfrak{B}(b)$-basis and accepts if the observed value equals to x.

Base Protocol : Unconditional Hiding

* $|U_c\rangle_+ = |U_c\rangle_\times$, where U_c is a uniform distribution.
* If $\delta(X, U_c) \leq \varepsilon$, then from the triangle inequality we have
    * $\delta(|X\rangle_+, |X\rangle_\times) \leq 2\varepsilon$.
* If f' is APSQOWF,
    * $\exists$ one-wayness-preserving conversion $f' \Rightarrow f$ s.t. $\delta(f(U_n), U_{\ell(n)}) \leq \varepsilon$.
    * Thus, $\delta(|f(U_n)\rangle_+, |f(U_n)\rangle_\times) \leq 2\varepsilon$

Base Protocol : Computational Binding

- If there exists a p-size quantum circuit $\mathscr{A}$ to violate Binding, then we can construct a p-size quantum circuit $\mathscr{B}$ to invert QOWF f.

  - [DMS00] shows the case of QOWP.

  - [KO09] observes that the permutation is not essential.

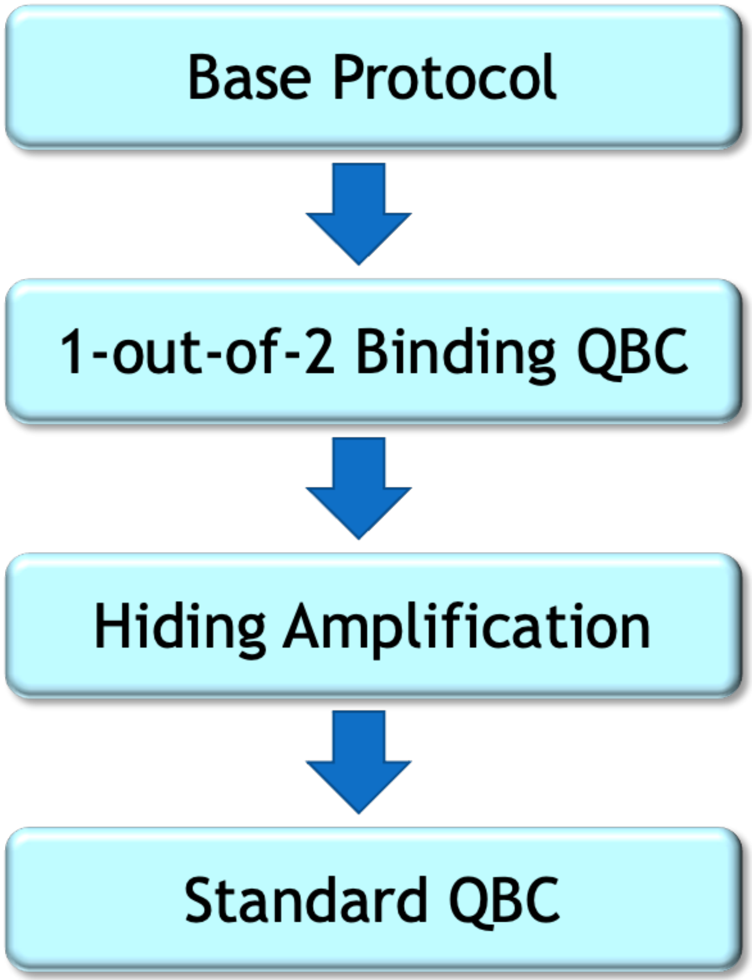
  - For general QOWF, we develop a new technique "Non-interactive Quantum Hashing Theorem" .

    - In some sense, this is a quantum variant of "New Interactive Hashing Theorem" by Haitner & Reingold [CCC '07].

Adversary Model for Computational Binding

- Adversary's Space
  - Private space for cheating
  - Spaces for Commit Phase and Reveal Phase
- Assume that a b-commitment state is stored in Commit Space.
- Adversary is a pair of p-size quantum circuits $(\mathscr{C}_0, \mathscr{C}_1)$.
  - $\mathscr{C}_i$ produces a quantum state for Reveal Phase which makes Bob accept the commitment $b \oplus i$ with probability p_i
  - If $p_0 + p_1 - 1 \geq 1/\mathrm{poly}(n)$ then the adversary wins.

Construction from QOWF



1st Obstacle

- We do not know $H_\infty(f(U_n))$ for any regular QOWF with unknown preimage size.
- Let $y = f(x)$ and $f : \{0,1\}^n \to \{0,1\}^n$.
- For any a, consider the following hashing functions:
  - $h_1 : \{0,1\}^n \to \{0,1\}^a$
  - $h_2 : \{0,1\}^n \to \{0,1\}^{n-a}$
- Then,
  - either $(h_1, h_1(y))$ or $(h_2, h_2(x))\|y$ is almost uniform, and
  - for $a = H_\infty(f(U_n))$, both are almost uniform.

1-out-of-2 Binding Commitment

- Alice has two bits b_1, b_2
- **Commit Phase**
  - Alice sends $|h_1, h_1(f(x))\rangle_{\mathfrak{B}(b_1)}$ and $|h_2, h_2(x)\rangle_{\mathfrak{B}(b_2)}$ to Bob.
- **Reveal Phase**
  - Alice sends (b_1, h_1, y) and (b_2, h_2, x) to Bob.
  - Bob measures the 1st quantum state w.r.t. $\mathfrak{B}(b_1)$-basis and the 2nd quantum state w.r.t. $\mathfrak{B}(b_2)$-basis and accepts if $y = f(x)$ and the observed values are equal to $(h_1, h_1(y))$ and $(h_2, h_2(x))$.
- The protocol looks like two parallel executions of Base Protocol.

1-out-of-2 Binding Commitment (cont'd)

* The notion appeared in [Nguyen, Ong & Vadhan (FOCS '06)].
* Either Base Protocol is computationally binding.
  * From the adversary's point of view, the other half can be regarded as a part of his private space
* Weakly Hiding
  * With probability $1/n$, both Base protocols are Hiding.
    * This happens if the guess for a coincides with $H_\infty(f(U_n))$.

2nd Obstacle

* The preimage size is not constant for general QOWF f.

* Fortunately, the same protocol works.

* Analyze the expected behavior by the technique in [Haitner, Nguyen, Ong, Reingold & Vadhan (SICOMP '09)] about a relation between Hiding and the collision probability.

Hiding Amplification

- Parallel repetition (with some adjustment) works.
- m repetitions of 1-out-of-2 Binding commitment.
  - Each subprotocol runs on public input x_i and randomly chosen private bits w_{i1}, w_{i2}.

Hiding Amplification (cont'd)

- For the 1st half,
  - Alice sends $|h_{1i}, h_{1i}(f(x_i))\rangle_{\mathfrak{B}(w_{1i})}$ for each i and $|h_1, h_1(f(x_1), \ldots, f(x_m))\rangle_{\mathfrak{B}(b_1)}$ in Commit Phase.
  - Alice sends $(w_{1i}, h_{1i}, f(x_i))$ for each i and (h_1, b_1) in Reveal Phase.
- For the 2nd half,
  - Alice sends $|h_{2i}, h_{2i}(x_i)\rangle_{\mathfrak{B}(w_{2i})}$ for each i and $|h_2, h_2(x_1, \ldots, x_m)\rangle_{\mathfrak{B}(b_2)}$ in Commit Phase.
  - Alice sends (w_{2i}, h_{2i}, x_i) for each i and (h_2, b_2) in Reveal Phase.

3rd Obstacle

* How many repetitions are necessary?

* A common technique :

  * Chernoff Bounds to bound the tail probability of the derivation from the expectation.

* But, a direct application does not work !

Hiding Amplification (cont'd)

* Preserving 1-out-of-2 Binding
* 2-step Hiding Amplification
  * 1st step : $(1/n)$-Hiding $\Rightarrow O(1)$-Hiding
    * by $O(\log n)$ repetitions
  * 2nd step : $O(1)$-Hiding $\Rightarrow (1 - 2^{-\Omega(n)})$-Hiding
    * by $O(n)$ repetitions

to Standard Bit Commitment

* Alice sets $b_1 = b_2 = b$ and runs 1-out-of-2 Binding Commitment with b_1, b_2

* Bob receives b_1, b_2 in Reveal Phase and additionally checks if $b_1 = b_2$. Bob accepts if all the tests are passed.

Non-Interactive Quantum Hashing Theorem

* Let f be an $s(n)$-secure QOWF.
* Let $W_n \subseteq \{0,1\}^n$ and $R_n = \{(f(x), x) \mid x \in W_n\}$.
* If a p-size circuit against Base Protocol can output distinct $(y, x), (y', x') \in R_n$ s.t. another p-size circuit
    * on input (y, x), produces a quantum state which makes Bob accept the commitment 0 with probability p_0,
    * on input (y', x'), produces a quantum state which makes Bob accept the commitment 1 with probability p_1,
    * $p_0 + p_1 - 1 \geq \sqrt{s(n)}$
* Then there exists yet another p-size circuit, on input y'' proportionally selected from $f(W_n)$, outputs x'' s.t. $(y'', x'') \in R_n$ with probability $\Omega(s(n))$.

Concluding Remarks

- Non-Interactive QBC from any QOWF.
  - QOWF is one of the weakest assumption in Cryptology.
- Non-Interactive QBC could be an important ingredient.
  - Simple construction for a larger system.
  - Security analysis would be simple.
- Another Proof for "Secure Computation from QOWF" [Bartusek, Coladangelo, Khurana & Ma, CRYPTO '21] ?