Quantum Bit-Commitment for Small Storage Based on Quantum One-Way Permutations (Extended Abstract)

Toshiyuki Isshiki
Keisuke Tanaka
Department of Mathematical and Computing Sciences,
Tokyo Institute of Technology,
1-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
{ isshiki9, keisuke} @is.titech.ac.jp

Abstract

We propose quantum bit-commitment schemes based on quantum one-way permutations. Our schemes reduces the number of bits which Bob needs to store until the opening phase compared with the classical counterpart.

Keywords

Bit-commitment, Quantum computation, One-way permutation.

1 Introduction

A bit-commitment protocol involves two party: a sender (say Alice) and a receiver (say Bob). Alice has a classical string in mind, which she wants to communicate to Bob at a later time. In order to guarantee that she will not change her mind in the interim, Alice agrees to lock her commitment in a safe which she sends to Bob, but keeps the key of the safe. At the moment of truth, Alice unveils her commitment and opens the safe to prove her honesty. A bit-commitment protocol has two security requirements. One is binding that Alice cannot change her initial commitment without being detected. The other is concealing that Bob has no reasonable way of obtaining any information on Alice's commitment before she discloses it.

Since Bennett and Brassard [1] proposed the quantum key-exchange protocol, various quantum cryptographic protocols including bit-commitment have been investigated. However, Mayers [6] proved that any quantum bit-commitment scheme can either be defeated by Alice or Bob as long as both have unrestricted quantum computational power.

This does not exclude the study on quantum bit-commitment based on some quantum computational assumption. Generally speaking, a bit-commitment based on the computational assumption comes in two flavors: (1) statistically (perfectly) concealing and computationally binding, and (2) statistically (perfectly) binding and computationally concealing. Informally, statistically concealing means that Bob cannot obtain more than a negligible amount of information about the committed string. Statistically binding means that whatever Alice does it is impossible to open both x_1 and x_2 with non-negligible probability of success.

Recently, Dumais, Mayers, and Salvail proposed a quantum bit-commitment scheme based on any quantum one-way permutation [4]. This scheme is statistically concealing and computationally binding, and reduces the number of interaction and the total amount of communication compared with the classical counterpart proposed by Noar, Ostrovsky, Venkatesen, and Young [7].

There are several measures for the cost of communication, the number of interactions, the total number of bits communicated, and so on. In this paper, we focus on the number of bits which Bob needs to store until the opening phase. We consider this as crucial in the quantum setting, since Bob must protect the received quantum states against decoherence until the opening phase. For some practical application, the length between the committing phase and the opening phase could be years. We will propose two quantum bit-commitment schemes based on quantum one-way permutations. One has the property of statistically binding and computationally concealing. The other has the property of statistically concealing and computationally binding. Our scheme reduces the number of bits which Bob needs to store (i.e., Alice sends) compared with the classical counterpart (e.g. see the textbook by Schneier [9]). Particularly, in the first protocol of statistically binding and computationally concealing, in order to commit an n-bit classical string with security parameter n, Bob needs to store only an $O((\log n)^3)$-bit quantum string in our method, while an n-bit string in the classical method. (all logarithms in this paper are base two.)

In the second protocol of statistically concealing and computationally binding, in order to commit an n-bit classical string with security parameter n, Bob needs to store only an $O(n(\log n)^3)$-bit quantum string in our method, while an n^2-bit string in the classical method (also in the previous quantum method by Dumais, Mayers, Salvail [4]).

Our protocols are based on a standard classical bit-commitment method, a quantum bit-commitment method proposed by Dumais, Mayers, Salvail [4], and a quantum fingerprinting scheme proposed by Buhrman, Cleve, Watrous, and de Wolf [2].

2 Preliminaries

In this section, we briefly review the definition of quantum one-way functions and the quantum fingerprinting. First, we give the definition [4] of quantum one-way functions. We denote quantum circuits built out of the universal set of quantum gates $\mathcal{UG} = \{\mathbf{CNot}, \mathbf{H}, \mathbf{R}_Q\}$, where **CNot** denotes the controlled-NOT, **H** is the one qubit Hadamard gate, and $\mathbf{R}_Q$ is an arbitrary one qubit non-trivial rotation specified by a matrix containing only rational numbers.

Definition 1 *A family of deterministic functions* $F = \{f_n : \{0,1\}^n \to \{0,1\}^{m(n)} | n > 0\}$ *is* $R(n)$*-secure quantum one-way if*

- *there exists an exact family of quantum circuits* $\mathbf{C} = \{\mathcal{C}_n^{-1}\}_{n>0}$ *and for* F *such that for all* $n > 0$,

$||\mathcal{C}_n|| \leq poly(n)$ *and*

- *for all family of quantum circuits* $\mathbf{C}^{-1} = \{\mathcal{C}_n^{-1}\}_{n>0}$ *and for all* n *sufficiently large, it is always the case that* $||\mathcal{C}_n^{-1}||_{\mathcal{UG}} S(n) \geq R(n)$ *where* $S(n) = \Pr(f_n(\mathcal{C}_n^{-1}(f_n(\mathbf{x}_n))) = f_n(\mathbf{x}_n))$.

Each family of quantum circuits $\boldsymbol{C}^{-1}$ *is called an inverter and the mapping* $S(n)$ *is called its probability of success.*

Note that whenever f_n is a permutation, $S(n)$ can be written as $S(n) = \Pr(f_n(\mathcal{C}_n^{-1}(\mathbf{y}_n)) = \mathbf{y}_n)$ where $\mathbf{y}_n$ is a uniformly distributed random variable in $\{0,1\}^n$

Next, we review the quantum fingerprinting proposed by Buhrman, Cleve, Watrous, and de Wolf [2], which can distinguish any two distinct classical strings with high probability by using much shorter fingerprints associating them. It should be mentioned that they do not investigate their fingerprinting method in respect of security.

Suppose that for fixed $c > 1$ and $\delta < 1$ we have an error-correcting code $e^n : \{0,1\}^n \to \{0,1\}^m$ for each n, where $m = cn$ and such that the Hamilton distance between distinct codewords $e^n(x)$ and $e^n(y)$ is at least $(1-\delta)m$. For any choice of n, we define the $(\log m + 1)$-qubit state $|h_x\rangle$ as

$$|h_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |e_i^n(x)\rangle$$

for each $x \in \{0,1\}^n$, where $e_i^n(x)$ is the i-th bit of $e^n(x)$. This $|h_x\rangle$ is called a quantum fingerprint of x. Since two distinct codewords can be equal in at most δm positions, for any $x \neq y$ we have $\langle h_x | h_y \rangle \leq \delta m / m = \delta$. Justesen codes [5] is a reasonable choice of such codes, which give $\delta < 9/10 + 1/(15c)$ for any chosen $c > 2$.

Distinguishing $|h_x\rangle$ and $|h_y\rangle$ can be done with one-sided error probability by the procedure that measures and outputs the first qubit of the state

$$(H \otimes I)(controlled - SWAP)(H \otimes I)|0\rangle|h_x\rangle|h_y\rangle,$$

where H is Hadamard transform, which maps $|b\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$, SWAP is the operation $|h_x\rangle|h_y\rangle \to |h_y\rangle|h_x\rangle$, and controlled-SWAP is SWAP controlled by the first qubit. With these operations, we have the final state before measurement:

$$\frac{1}{2}(|0\rangle(|h_x\rangle|h_y\rangle + |h_y\rangle|h_x\rangle) + |1\rangle(|h_x\rangle|h_y\rangle - |h_y\rangle|h_x\rangle)).$$

Measuring the first qubit of this state produces outcome 1 with probability $\frac{1}{2} - \frac{1}{2}|\langle h_x|h_y\rangle|^2$. This probability is 0 if $x = y$ and is at least $\frac{1}{2}(1-\delta^2) > 0$ if $x \neq y$. Thus, the test determines which case holds with one-sided error $\frac{1}{2}(1+\delta^2)$.

The error probability of this test can be reduced to any $\epsilon > 0$. This can be done by making the fingerprint $k = O(\log(1/\epsilon))$ times and from such fingerprints, one can independently perform the test k times, resulting in an error probability below ϵ. In this case, the length of each fingerprint is $O((\log n)(\log(1/\epsilon)))$.

3 First Protocol

In this section, we describe the first protocol. Let $\Sigma = \{\sigma^n : \{0,1\}^n \to \{0,1\}^n \mid n > 0\}$ be a family of quantum one-way permutations, and $E = \{e^n : \{0,1\}^n \to \{0,1\}^m \mid n > 0\}$ a family of error-correcting codes mentioned above. The commitment scheme takes, as common input, the number of bits to be committed (a security parameter) n, and the descriptions of family Σ and E. Our protocol is based on a standard classical bit-commitment method and the quantum fingerprinting scheme described above.

Given n, Σ, and E (with fixed c and δ), Alice and Bob determine the instances $\sigma^n : \{0,1\}^n \to \{0,1\}^n \in \Sigma$ and $e^n : \{0,1\}^n \to \{0,1\}^m \in E$. Fix also $k = (\log n)^2$.

3.1 Committing

1. Alice decides a classical string $x \in \{0,1\}^n$ to be committed.

2. Alice computes $\sigma^n(x)$, and then $e^n(\sigma^n(x))$.

3. Alice makes k copies of the quantum state $|\phi\rangle$:

$$|\phi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |e_i^n(\sigma^n(x))\rangle,$$

   (Alice independently makes $|\phi\rangle$, k times.) and sends them to Bob.

Notice that Bob must protect the received quantum state, k copies of $|\phi\rangle$, against decoherence until the opening phase.

In the committing phase, only Alice sends the information to Bob, and there is no interaction. The length of the string which Alice sends in this phase is

$$(\log m + 1) \times k = (\log cn + 1) \times (\log n)^2 = O((\log n)^3).$$

Thus, Bob needs to store only an $O((\log n)^3)$-bit quantum string until the opening phase.

The computation that Alice needs in this phase is one evaluation of the one-way function σ^n, one evaluation of the coding function e^n. Alice also needs to make k copies of the quantum state $|\phi\rangle$. Each $|\phi\rangle$ can be obtained by $\log m$ operations of the Hadamard transform, and one one-bit addition corresponding to writing $e_i^n(\sigma^n(x))$.

3.2 Opening

1. Alice sends x' to Bob. (x' is supposed to be x.)

2. Bob computes $\sigma^n(x')$, and then $e^n(\sigma^n(x'))$.

3. For each $|\phi\rangle$, Bob makes the quantum state $|\psi\rangle$:

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |e_i^n(\sigma^n(x'))\rangle,$$

   and tests $|\psi\rangle$ and $|\phi\rangle$ by the controlled-swap method described above.

4. Bob determines whether $|\phi\rangle$'s are consistent with x' or not.

In the opening phase, again, only Alice sends the information to Bob, and there is no interaction. The string which Alice sends in this phase is a classical string of length n.

The computation that Bob needs in this phase is that Alice needs in the committing phase plus the controlled-swap tests and the final decision. Each controlled-swap test require 2 operations of the Hadamard transform, one controlled-swap operation, and one observation.

3.3 Binding and Concealing

In this section, we show that our bit-commitment scheme is statistically binding and computationally concealing. First, we consider the binding condition. Thus, we regard Alice as an adversary, and define $S_0(n)$ and $S_1(n)$ as the probabilities that Alice succeeds to unveil x_1 and x_2, respectively.

As mentioned in the paper by Dumais, Mayers, and Salvail [4], when considering adversarial Alice in the classical setting, one can always fix Alice's committed string by fixing the content of her random tape, i.e., we can require that either the probability to unveil 0 or the probability to unveil 1 vanishes, for every fixed value of the random tape. This kind of definition of binding does not apply in the quantum setting, since Alice could introduce randomness in the quantum computation even if we fix the random tape. In particular, Alice can always commit to a superposition of x_0 and x_1 by preparing the quantum state:

$$\sqrt{c}|0\rangle|\Phi_0\rangle + \sqrt{1-c}|1\rangle|\Phi_1\rangle,$$

where $|\Phi_0\rangle$ and $|1\rangle|\Phi_1\rangle$ are the honest states generated for committing to x_0 and x_1 respectively, and $|0\rangle$ and $|1\rangle$ are two orthogonal states of an extra ancilla kept by Alice. In this case, Alice can unveil x_0 and x_1 with some non zero probability, i.e., $S_0(n) > 0$ and $S_1(n) > 0$.

The binding condition that $S_0(n) = 0$ or $S_1(n) = 0$ is too strong was previously noticed by Mayers [6], and Dumais, Mayers, and Salvail [4] proposed the weaker condition $S_0(n)+S_1(n) \leq 1+\epsilon(n)$, where $\epsilon(n)$ is negligible (i.e. smaller than $1/poly(n)$ for any polynomial $poly(n)$). In this paper, we also follow this condition, and call a bit-commitment scheme *statistically binding* if it satisfies this condition. This definition is also taken by the paper by Crépeau, Légaré, and Salvail [3].

Theorem 1 *Our bit-commitment protocol is statistically binding, i.e., it satisfies* $S_0(n) + S_1(n) \leq 1 + \epsilon(n)$*, where* $\epsilon(n)$ *is negligible.*

Proof. Without loss of generality, consider Alice wants to open both x_1 and x_2 ($x_2 \neq x_1$). In the opening phase of our protocol, after Bob receives a classical string x' from Alice, he makes the quantum state $|\psi\rangle$ by himself. This quantum state must corresponds to some codeword. In particular, when Bob receives x_1 (x_2) in the opening phase, he makes the quantum state $|\psi_1\rangle$ ($|\psi_2\rangle$) corresponding to a codeword $e^n(\sigma^n(x_1))$ ($e^n(\sigma^n(x_2))$).

Because of this, Alice has to send a quantum state $|\phi\rangle$ close to both two codewords $e^n(\sigma^n(x_1))$ and $e^n(\sigma^n(x_2))$ in the committing phase. In particular, Alice has to send $|\phi\rangle$ such that the probabilities $\frac{1}{2} - \frac{1}{2}|\langle\phi|\psi_1\rangle|^2$ and $\frac{1}{2} - \frac{1}{2}|\langle\phi|\psi_2\rangle|^2$ are both negligible. This implies $|\langle\phi|\psi_1\rangle| = 1 - \epsilon(n)$ and $|\langle\phi|\psi_2\rangle| = 1 - \epsilon(n)$, while $|\langle\psi_1|\psi_2\rangle| \leq \delta$. Since $\delta < 1$ is a fixed constant, this a contradiction.

One might be concerned with the situation that $|\phi\rangle$'s are entangled. As mentioned in the paper by Watrous [10], a simple analysis reveals that entanglement among $|\phi\rangle$'s sent by Alice can yield no increase in the probability of success on the attack as compared to the situation in which these strings are not entangled, and that the probability of error is bounded by the tail of a binomial series as expected. ∎

Next, we consider the concealing condition. Thus, we regard Bob as an adversary.

Theorem 2 *Our bit-commitment protocol is computationally concealing.*

Proof. In the committing phase, Bob has the quantum state $|\phi\rangle$ sent by Alice with a committed string x. Observe that, from $|\phi\rangle$, Bob can extract the information no more than the configuration of $|\phi\rangle$, as the formula:

$$|\phi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |y_i\rangle,$$

where $y_i \in \{0,1\}$. Notice that the coding function employed in our method is not quantum one-way. Thus, Bob can compute $\sigma^n(x)$ by decoding the codeword
$y_1 y_2 \cdots y_m$. Thus, attacking $\sigma^n(x)$ to get x with non-negligible probability of success implies the ability to compute x from $\sigma^n(x)$ with non-negligible probability. ∎

4 Second Protocol

In this section, we describe the second protocol.

In order to do this, we briefly explain the quantum encoding. We denote the m-dimensional Hilbert space by $\mathcal{H}_m$. The basis $\{|0\rangle, |1\rangle\}$ denotes the computational or rectilinear or "+" basis for $\mathcal{H}_2$. We also write $\{|0\rangle_+, |1\rangle_+\}$ to denote them. The diagonal basis, denoted "×", is defined as The basis $\{|0\rangle_\times, |1\rangle_\times\}$

where $|0\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The states $|0\rangle$, $|1\rangle$, $|0\rangle_\times$, and $|1\rangle_\times$ are the BB84 states.

We also define θ as $\theta(0) = +$ and $\theta(1) = \times$. For any $x = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ and $y \in \{0,1\}$, the state $|x\rangle_{\theta(y)}$ is defined as $\otimes_{i=1}^{n} |x_i\rangle_{\theta(y)}$.

4.1 Committing

1. Alice decides a classical string $x \in \{0,1\}^n$ to be committed.
2. Alice randomly picks m classical strings
   $y^1, \ldots, y^m \in \{0,1\}^n$, and a classical bit $z \in \{0,1\}$.
3. Alice computes $\sigma^n(y^1), \ldots, \sigma^n(y^m)$, and $e^n(x)$.
4. Alice makes k copies of the quantum state $|\phi\rangle$:

   $$|\phi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |\sigma^n(y^i)\rangle_{\theta(e_i^n(x))},$$

   (Alice independently makes $|\phi\rangle$, k times.) and sends them to Bob.

Notice that Bob must protect the received quantum state, k copies of $|\phi\rangle$, against decoherence until the opening phase.

In the committing phase, only Alice sends the information to Bob, and there is no interaction. The length of the string which Alice sends in this phase is

$$(\log m + n) \times k = (\log cn + n) \times (\log n)^2 = O(n(\log n)^2).$$

Thus, Bob needs to store only an $O(n(\log n)^2)$-bit quantum string until the opening phase.

The computation that Alice needs in this phase is m evaluation of the one-way function σ^n, and one evaluation of the coding function e^n. Alice also needs to make k copies of the quantum state $|\phi\rangle$. Each $|\phi\rangle$ can be obtained by at most $nm \log m$ operations of the one-bit Hadamard transform.

4.2 Opening

1. Alice sends $x, y^1, \ldots, y^m$ to Bob.
2. Bob computes $\sigma^n(y^1), \ldots, \sigma^n(y^m)$, and $e^n(x)$.
3. For each $|\phi\rangle$, Bob makes the quantum state $|\psi\rangle$:

   $$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle|\sigma^n(y^i)\rangle_{\theta(e_i^n(x))},$$

   and tests $|\psi\rangle$ and $|\phi\rangle$ by the controlled-swap method described above.
4. Bob determines whether $|\phi\rangle$'s are consistent with $x, y^1, \ldots, y^m$ or not.

In the opening phase, again, only Alice sends the information to Bob, and there is no interaction. The string which Alice sends in this phase is a classical string of length $n(m+1)$.

The computation that Bob needs in this phase is that Alice needs in the committing phase plus the controlled-swap tests and the final decision. Each controlled-swap test require 2 operations of the Hadamard transform, one controlled-swap operation, and one observation.

4.3 Binding and Concealing

In this section, we show that our scheme is statistically concealing and computationally binding. First, we consider the concealing condition. Thus, we regard Bob as an adversary.

Theorem 3 *Our bit-commitment protocol is statistically concealing.*

Proof. Let us fix i in $|\phi\rangle$, and let $|\phi_i\rangle$ be

$$|\phi_i\rangle = |\sigma^n(y^i)\rangle_{\theta(e_i^n(x))}.$$

Let ρ_w for $w \in \{0,1\}$ be the density matrix to the mixture corresponding to $|\phi_i\rangle$ when $w = e_i^n(x)$. Since y^i is independent of x (so is w) and σ^n is a permutation in the set $\{0,1\}^n$, we get

$$\rho_0 = \sum_{z \in \{0,1\}^n} 2^{-n}|z\rangle_+\langle z| = 2^{-n}I = \sum_{z \in \{0,1\}^n} 2^{-n}|z\rangle_\times\langle z| = \rho_1$$

where I is the identity operator in $\mathcal{H}_{2^n}$.

Let ρ_x for $x \in \{0,1\}^n$ be the density matrix to the mixture corresponding to $|\phi\rangle$ when classical string x is committed. Since

$$|\phi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle|\phi_i\rangle$$

and $y^1, \ldots, y^m$ are mutually independent, all of the quantum states ρ_x are the same. The theorem follows that no quantum measurement can distinguish among the commitments of x. ∎

Next, we consider the binding condition. Thus, we regard Alice as an adversary.

Theorem 4 *Our bit-commitment protocol is computationally binding, i.e., if we have the adversary with $S_0(n) + S_1(n) \geq 1 + \epsilon(n)$ where $\epsilon(n) > 0$, then there is an inverter for the one-way permutation σ^n where the success probability is non-negligible.*

Proof. Before we describe the proof, we briefly summarize the attack considered in the paper by Dumais, Mayers, and Salvail [4], where they consider the commitment protocol for a single-bit.

We regard Alice as an adversary. An attack of Alice must start with the state $|0\rangle$ of some system $H_{All} = H_{Extra} \otimes H_A \otimes H_{Commit}$. A quantum circuit C^n that acts on H_{All} is executed to obtain a state $|\Psi\rangle$ and the subsystem H_{Commit} is sent to Bob. Later, any quantum circuit O^n which acts on $H_{Extra} \otimes H_{Keep} \otimes H_{Open}$ can be executed before sending the subsystem H_{Open} to Bob. The quantum circuits O^n_w, $w = 0, 1$ which respectively maximize the probability that the bit $w = 0, 1$ is unveiled with success. Then, Alice can be modeled by a triplet $\{(C^n, O^n_0, O^n_1)\}_{n>0}$ of quantum circuits.

Dumais, Mayers, and Salvail [4] showed that the adversary which can open both $w = 0$ and $w = 1$ with high probability of success, can invert efficiently the one-way permutation with high probability of success.

We can modify the attack by Dumais, Mayers, and Salvail [4] to obtain our attack. This can be done, by making triplets $\{(C^n, O^n_0, O^n_1)\}_{n>0}$ of quantum circuits to be index sensitive. For example, we make $O^{n,i}_0$ from O^n_0 such that $O^{n,i}_0$ is specialized to the index i:

$$O^{n,i}_0 \sum_j |j\rangle|\phi_j\rangle = \sum_j |j\rangle|\psi_j\rangle,$$

where $|\psi_j\rangle = |\phi_j\rangle$ (unchanged) for each $j \neq i$, $|\psi_i\rangle = |\phi'_i\rangle$ (changed). Once we have triplets $\{(C^{n,i}, O^{n,i}_0, O^{n,i}_1)\}_{n>0}$ of quantum circuits with the index sensitive property, we can construct the attack specialized to each index, since

$$|\phi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle|\phi_i\rangle$$

and $y^1, \ldots, y^m$ are mutually independent.

So, we prove that any efficient perfect adversary against the binding condition can be used to invert efficiently the one-way permutation with probability of success 1. We can generalize the result to all imperfect but otherwise good adversaries.

It is convenient to restrict ourselves to the cases where O_0^n is the identity circuit. We can adopt this restriction without lost of generality because any triplet $(C^n, O_0^{n,i}, O_1^{n,i})$ can easily be replaced by the three quantum circuits $(C_0^{n,i}, I, U_{0,1}^{n,i})$, where $C_0^n = (O_0^n \otimes I_{Commit}) \cdot C^n$ and $U_{0,1}^n = O_1^n \cdot (O_0^n)^\dagger$, without changing the adversaries strategy. The difference in complexity between applying $(C^n, O_0^{n,i}, O_1^{n,i})$ and $(C_0^{n,i}, I, U_{0,1}^{n,i})$ is only $\Delta T(n) = ||O_0^{n,i}||_{\mathcal{UG}}$. Therefore, the adversary is completely determined by the pair $(C_0^{n,i}, U_{0,1}^{n,i})$ where $C_0^{n,i}$ acts on all registers in H_{All}, and $U_{0,1}^{n,i}$ is restricted to act only in $H_{Extra} \otimes H_{Open}$.

We obtain that $|||\gamma_w^{y^i,v}\rangle|| = 0$ if $\sigma^n(y^i) \neq s$,

$$|\Psi_0^{n,i}\rangle = \sum_{y^i \in \{0,1\}^n} |\gamma_0^{y^i}\rangle^{Extra} \otimes |y^i\rangle^{Open} \otimes |\sigma^n(y^i)\rangle_{+^n}^{Commit} = C_0^{n,i}|0\rangle \tag{1}$$

where $|\gamma_0^{y^i}\rangle$ corresponds to $|\gamma_0^{y^i,\sigma^n(y^i)}\rangle$ and $\sum_{y^i} |||\gamma_0^{y^i}\rangle||^2 = 1$, and

$$|\Psi_1^{n,i}\rangle = \sum_{y^i \in \{0,1\}^n} |\gamma_1^{y^i}\rangle^{Extra} \otimes |y^i\rangle^{Open} \otimes |\sigma^n(y^i)\rangle_{\times^n}^{Commit} = U_{0,1}^{n,i}|\Psi_0^{n,i}\rangle \tag{2}$$

where $|\gamma_1^{y^i}\rangle$ corresponds to $|\gamma_1^{y^i,\sigma^n(y^i)}\rangle$ and $\sum_{y^i} |||\gamma_1^{y^i}\rangle||^2 = 1$. Any pair of 0-state and 1-state satisfying (1) and (2) is called *perfect pair*. Any perfect adversary $A = \{(C_0^{n,i}, U_{0,1}^{n,i})\}_n$ generates a perfect pair for all $n > 0$.

Let $\mathbf{P}_{Commit}^{u,+}$ and $\mathbf{P}_{Commit}^{u,\times}$ be the projection operators $\mathbf{P}_{+^n}^u$ and $\mathbf{P}_{\times^n}^u$ respectively, acting upon register H_{Commit}. We assume that we have an input register $H_S \simeq \mathcal{H}_{2^n}$ initialized in the basis state $|s\rangle$ on input s. The states $|\Phi_0^{n,i}(u)\rangle = \mathbf{P}_{Commit}^{u,\times}|\Psi_0^{n,i}\rangle, u \in \{0,1\}^n$, play an essential role in the mechanisms used by the inverter. These states have three key properties for every $u \in \{0,1\}^n$:

1. $|||\Phi_0^{n,i}(u)\rangle|| = 2^{-\frac{n}{2}}$,
2. there exists a simple circuit $\mathbf{W}_n$ on $H_S \otimes H_{Open} \otimes H_{Commit}$ which, if u is encoded in register H_S, unitarily maps $|\Psi_0^{n,i}\rangle$ into $2^{\frac{n}{2}}|\Phi_0^{n,i}(u)\rangle$, and
3. $U_{0,1}^{n,i}|\Phi_0^{n,i}(u)\rangle = |\gamma^{\sigma^{-1}(u)}\rangle^{Extra} \otimes |(\sigma^n)^{-1}(u)\rangle^{Open} \otimes |u\rangle_{\times^n}^{Commit}$.

On input $s \in \{0,1\}^n$, the inverter creates the state $|\Psi_0^{n,i}\rangle$, then applies the circuit $\mathbf{W}_n$, then the circuit $U_{0,1}^{n,i}$, and finally measures the register H_{Open} to obtain $(\sigma^n)^{-1}(s)$. We now prove these three properties.

First we write the state $|\Psi_0^{n,i}\rangle$ using the basis $\times^n$ for the register $H_{Commit} \simeq \mathcal{H}_{2^n}$. We get

$$|\Psi_0^{n,i}\rangle = 2^{-\frac{n}{2}} \sum_{u,v \in \{0,1\}^n} (-1)^{u \odot v} |\gamma^{(\sigma^n)^{-1}(v)}\rangle^{Extra} \otimes |(\sigma^n)^{-1}(v)\rangle^{Open} \otimes |u\rangle_{\times^n}^{Commit}$$

from which we easily obtain, after the change of variable $(\sigma^n)^{-1}(v) \to y^i$,

$$|\Phi_0^{n,i}(u)\rangle = 2^{-\frac{n}{2}} \sum_{y^i \in \{0,1\}^n} (-1)^{u \odot \sigma^n(y^i)} |\gamma_0^{y^i}\rangle^{Extra} \otimes |y^i\rangle^{Open} \otimes |u\rangle_{\times^n}^{Commit}.$$

Property 1 follows from (3). Note that the states $|\Phi_0^{n,i}(u)\rangle$ can be mapped one into the other by a unitary mapping, a conditional phase shift which depends on u and y^i. Because (2) can be rewritten as

$$|\Psi_1^{n,i}\rangle = \sum_{u\in\{0,1\}^n} |\gamma_1^{(\sigma^n)^{-1}(u)}\rangle^{Extra} \otimes |(\sigma^n)^{-1}(u)\rangle^{Open} \otimes |u\rangle_{\times^n}^{Commit},$$

it follows that, for all $u \in \{0,1\}^n$, we have

$$\begin{aligned} U_{0,1}^{n,i}|\Phi_0^{n,i}(u)\rangle &= U_{0,1}^{n,i}\mathbf{P}_{Commit}^{u,\times}|\Psi_0^{n,i}\rangle \\ &= \mathbf{P}_{Commit}^{u,\times}U_{0,1}^{n,i}|\Psi_0^{n,i}\rangle \\ &= \mathbf{P}_{Commit}^{u,\times}|\Psi_1^{n,i}\rangle \\ &= |\gamma^{\sigma^{-1}(u)}\rangle^{Extra}|(\sigma^n)^{-1}(u)\rangle^{Open}|u\rangle_{\times^n}^{Commit}. \end{aligned}$$

which concludes the proof of property 3.

A simple comparison of (1) and (3) suggests what needs to be done to obtain $2^{\frac{n}{2}}|\Phi_0^{n,i}(s)\rangle$ efficiently starting from $|\Psi_0^{n,i}\rangle$. Assume the input register $H_S = H_S^1 \otimes \cdots \otimes H_S^n \simeq \mathcal{H}_{2^n}$ is in the basis state $|s\rangle$. The first step is to add the phase $(-1)^{y\odot\sigma^n(y^i)}$ in front of each term in the sum of (1). Note that, for every $s \in \{0,1\}^n$, this is a unitary mapping on $H_{Extra} \otimes H_{Open} \otimes H_{Commit}$. It is sufficient to execute a circuit $\hat{\oplus}_1$ which, for each $j \in \{1,\ldots,n\}$, acts on the corresponding pair of qubits in $H_S^j \otimes H_{Commit}^j$. The circuit $\hat{\oplus}_1$ maps each state $|s_j\rangle \otimes |\sigma^n(y^i)_j\rangle$, $j = 1,\ldots,n$, into $(-1)^{(s_j\odot\sigma^n(y^i)_j)}(|s_j\rangle \otimes |\sigma^n(y^i)_j\rangle)$. It can easily be implemented as $\hat{\oplus}_1 = (\mathbf{H} \otimes I_{Commit}) \cdot \mathbf{CNot} \cdot (\mathbf{H} \otimes I_{Commit})$ where each $\mathbf{H}$ is applied to register H_S^j by $\hat{\oplus}_n$ the complete quantum circuit acting in $H_S \otimes H_{Commit}$ and applying $\hat{\oplus}_1$ to each pair $j \in \{1,\ldots,n\}$ of qubits $|s_j\rangle \otimes |\sigma^n(y^i)_j\rangle \in H_S^j \otimes H_{Commit}^j$.

The second step is to set the register H_{Commit} which contains the state $|\sigma^n(y^i)\rangle_{+^n}$ into the new state $|s\rangle_{\times^n}$. For this we use the composition of three circuits. The first circuit $U_{\sigma^n} : |y^i\rangle^{Open} \otimes |u\rangle^{Commit} \mapsto |y^i\rangle^{Open} \otimes |u \oplus \sigma^n(y^i)\rangle^{Commit}$ sets the quantum register H_{Commit} into the new state $|0\rangle_{+^n}$. Note that U_{σ^n} is the quantum circuit that is guaranteed to compute $\sigma^n(y^i)$ efficiently. The second circuit is $\oplus_n : |y\rangle^S \otimes |u\rangle^{Commit} \mapsto |s\rangle^S \otimes |s \oplus u\rangle^{Commit}$ which sets H_{Commit} into the state $|s\rangle_{+^n}$ by simply applying a **CNot** between registers H_{Commit}^j, $H_S^j \simeq \mathcal{H}_2$ for $j \in \{1,\ldots,n\}$. Finally the third circuit executes the Hadamard transform $\mathbf{H}_n$ on H_{Commit} which maps the $+^n$ basis into the $\times^n$ basis. The composition of $\hat{\oplus}_n$ with these three circuits is the circuit $\mathbf{W}_n$. ∎

5 Concluding Remarks

In this paper, we propose quantum bit-commitment schemes based on quantum one-way permutations. Our future work is replacing assumption to quantum one-way functions from quantum one-way permutations.

References

[1] Bennett, C. H., and Brassard, G. An update on quantum cryptography. In *Advances in Cryptology: Proceedings of CRYPTO 84* (19–22 Aug. 1984), G. R. Blakley and D. Chaum, Eds., vol. 196 of *Lecture Notes in Computer Science*, Springer-Verlag, 1985, pp. 475–480.

[2] Buhrman, H., Cleve, R., Watrous, J., and de Wolf, R. Quantum fingerprinting. *Physical Review Letters 87*, 16 (2001).

[3] Crépeau, C., Légaré, F., and Salvail, L. How to convert the flavor of a quantum bit commitment. In *Advances in Cryptology—EUROCRYPT2001* (2001), pp. 60–77.

[4] Dumais, P., Mayers, D., and Salvail, L. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *Advances in Cryptology—EUROCRYPT2000* (2000), pp. 300–315.

[5] Justesen, J. A class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory 18* (1972), 652–656.

[6] Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters 78*, 17 (1997), 3414–3417.

[7] Naor, M., Ostrovsky, R., Ventkatesan, R., and Young, M. Perfect zero-knowledge arguments for np using any one-way permutation. *Journal of Cryptology 11*, 2 (1998), 78–108.

[8] Okamoto, T., Tanaka, K., and Uchiyama, S. Quantum public-key cryptosystems. In *Advances in Cryptology—CRYPTO2000* (2000), pp. 147–165.

[9] Schneier, B. *Applied Cryptography—Second Edition.* Wiley, 1996.

[10] Watrous, J. Succinct quantum proofs for properties of finite n groups. In *41st Annual Symposium on Foundations of Computer Science: proceedings: 12–14 November, 2000, Redondo Beach, California* (2000), pp. 537–546.