Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation

Paul Dumais[1] ⋆, Dominic Mayers[2] ⋆⋆, and Louis Salvail[3] ⋆⋆⋆

[1] Université de Montréal, Dept. of Computer Science
dumais@iro.umontreal.ca
[2] NEC Research Institute, Princeton, N-J, USA
mayers@research.nj.nec.com
[3] BRICS†, Dept. of Computer Science
University of Århus, Århus, Denmark
salvail@brics.dk

Abstract. We show that although unconditionally secure quantum bit commitment is impossible, it can be based upon any family of quantum one-way permutations. The resulting scheme is unconditionally concealing and computationally binding. Unlike the classical reduction of Naor, Ostrovski, Ventkatesen and Young, our protocol is non-interactive and has communication complexity $O(n)$ qubits for n a security parameter.

1 Introduction

The non-classical behaviour of quantum information provides the ability to expand an initially short and secret random secret-key shared between a pair of trusted parties into a much longer one without compromising its security. The BB84 scheme was the first proposed quantum secret-key expansion protocol[3] and was shown secure by Mayers [12,14]. Secret-key expansion being incompatible with classical information theory indicates that quantum cryptography is more powerful than its classical counterpart. However, quantum information has also fundamental limits when cryptography between two potentially collaborative but untrusted parties is considered. Mayers [13] has proven that any quantum bit commitment scheme can either be defeated by the committer or the receiver as long as both sides have unrestricted quantum computational power. Mayers' general result was built upon previous works of Mayers [11] and Lo and Chau [9].

However, the no-go theorem does not imply that quantum cryptography in the two-party case is equivalent to complexity-based classical cryptography. For example, quantum bit commitment schemes can be built from physical assumptions that are independent of the existence of one-way functions [16]. Moreover,

⋆ Supported by a NSERC grant, part of this work was done while visiting BRICS and McGill SOCS.

⋆⋆ Part of this work was done while visiting BRICS and NEC Tsukuba Laboratory, Japan.

⋆⋆⋆ Supported by the Thomas B. Thriges Center for KvanteInformatik (CKI).

† Basic Research in Computer Science of the Danish National Research Foundation.

B. Preneel (Ed.): EUROCRYPT 2000, LNCS 1807, pp. 300–315, 2000.

bit commitment is sufficient for quantum oblivious transfer [4,19] which would be true in the classical world only if one-way functions imply trapdoor one-way functions [8]. The physical assumption addressed in [16] restricts the size of the entanglement the adversary's quantum computer can deal with. Implementing any successful attack was shown, for a particular protocol with security parameter n, to require a $\Omega(n)$-qubits quantum computer. However, such a physical assumption says nothing about the complexity of the attack. In this paper, we construct an unconditionally concealing quantum bit commitment scheme which can be attacked successfully only if the adversary can break a general quantum computational assumption.

We show that similarly to the classical case [15], unconditionally concealing quantum bit commitment scheme can be based upon any family of quantum one-way permutations. This result is not the direct consequence of the classical construction proposed by Noar, Ostrovsky, Ventkatesen and Young (NOVY) [15]. One reason is that NOVY's analysis uses classical derandomization techniques (rewinding) in order to reduce the existence of an inverter to a successful adversary against the binding condition. In [18], it is shown that such a proof fails completely in a quantum setting: if rewinding was possible then no quantum one-way permutation would exist. Therefore, in order to show that NOVY's protocol is conditionally binding against the quantum computer, one has to provide a different proof.

We present a different construction using quantum communication in order to enforce the binding property. In addition, whereas one NOVY's commitment requires $\Omega(n)$ rounds (in fact $n-1$ rounds) of communication for some security parameter n, our scheme is non-interactive. Whether or not this is possible to achieve classically is still an open question. In addition, the total amount of communication of our scheme is $O(n)$ qubits which also improves the $\Omega(n^2)$ bits needed in NOVY's protocol, as far as qubits and bits may be compared. Since unconditionally concealing bit commitment is necessary and sufficient for Zero-Knowledge arguments [5], using our scheme gives implementations requiring few rounds of interaction with provable security based upon general computational assumptions. Perfectly concealing commitment schemes are required for the security of several applications (as in [5]). Using them typically forces the adversary to break the computational assumption before the end of the opening phase, whereas if the scheme was computationally concealing the dishonest receiver could carry out the attack as long as the secret bit remains relevant. Any secure application using NOVY as a sub-protocol can be replaced by one using our scheme instead thus improving communication complexity while preserving the security.

This work provides motivations for the study of one-way functions in a quantum setting. Quantum one-way functions and classical one-way functions are not easily comparable [6]. On the one hand, Shor's algorithm [17] for factoring and extracting discrete logs rules out any attempt to base quantum one-wayness upon those computational assumptions. This means that several flexible yet useful classical one-way functions cannot be used for computationally based quantum cryptography.

On the other hand, because the quantum computer evaluates some functions more efficiently than the classical one, some quantum one-way functions might not be classical one-way since classical computers could even not be able to compute them in the forward direction. This suggests that quantum cryptography can provide new foundations for computationally based security in cryptography.

Organization. First, we give some preliminaries and definitions in Sect.2. Therein, we define the model of computation, quantum one-way functions, and the security criteria for the binding condition. In Sect. 3, we describe our perfectly concealing but computationally binding bit commitment scheme. In Sect. 4, we show that our scheme is indeed unconditionally concealing. Then we model the attacks against the binding condition in Sec. 5. Section 6 reduces the existence of a perfect inverter for a family of one-way permutations to any perfect adversary against the binding condition of our scheme. In Sect. 7, we extend the reduction by showing that any efficient adversary to the binding condition implies an inverter for the family of one-way permutations working efficiently and having good probability of success.

2 Preliminaries

After having introduced the basic quantum ingredients, we define quantum one-way functions and the attacks against the binding condition of computationally binding quantum commitment schemes. We assume the reader familiar with the basics of quantum cryptography and computation.

2.1 Quantum Encoding

In the following, 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 $\mathcal{H}_2$. When the context requires, we write $|b\rangle_+$ to denote the bit b in the rectilinear basis. The diagonal basis, denoted "$\times$", is defined as $\{|0\rangle_\times, |1\rangle_\times\}$ 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 four BB84 states. For any $x \in \{0,1\}^n$ and $\theta \in \{+,\times\}^n$, the state $|x\rangle_\theta$ is defined as $\otimes_{i=1}^n |x_i\rangle_{\theta_i}$. An orthogonal (or Von Neumann) measurement of a quantum state in $\mathcal{H}_m$ is described by a set of m orthogonal projections $\mathbb{M} = \{\mathbb{P}_i\}_{i=1}^m$ acting in $\mathcal{H}_m$ thus satisfying $\sum_i \mathbb{P}_i = \mathbb{1}_m$ for $\mathbb{1}_m$ denoting the identity operator in $\mathcal{H}_m$. Each projection or equivalently each index $i \in \{1,\ldots,m\}$ is a possible classical outcome for $\mathbb{M}$. In the following, we write $\mathbb{P}_+^0 = |0\rangle\langle 0|$, $\mathbb{P}_+^1 = |1\rangle\langle 1|$, $\mathbb{P}_\times^0 = |0\rangle_\times\langle 0|$ and $\mathbb{P}_\times^1 = |1\rangle_\times\langle 1|$ for the projections along the four BB84 states. We also define for any $y \in \{0,1\}^n$ the projection operators $\mathbb{P}_{+^n}^y = \otimes_{i=1}^n \mathbb{P}_+^{y_i}$ and $\mathbb{P}_{\times^n}^y = \otimes_{i=1}^n \mathbb{P}_\times^{y_i}$. Since the basis $+^n$ in $\mathcal{H}_{2^n}$ is the computational basis, we also write $\mathbb{P}^y = \mathbb{P}_{+^n}^y$. In order to simplify the notation, in the following we write $\theta(0) = +$ and $\theta(1) = \times$. For any $w \in \{0,1\}$, we denote by $\mathbb{M}_{\theta(w)^n}$ the Von Neumann measurement $\{\mathbb{P}^y_{\theta(w)^n}\}_{y\in\{0,1\}^n}$. We denote by $\mathbb{M}_n$ for $n \in \mathbb{N}$, the Von Neumann measurement in the computational basis applied on an n-qubit register.

Finally, in order to indicate that $|\phi\rangle \in \mathcal{H}_{2^r}$ is the state of a quantum register $H_R \simeq \mathcal{H}_{2^r}$ we write $|\phi\rangle^R$. If $H_R \simeq \mathcal{H}_{2^r}$ and $H_S \simeq \mathcal{H}_{2^s}$ are two quantum registers and $|\phi\rangle = \sum_{x\in\{0,1\}^r}\sum_{y\in\{0,1\}^s}\gamma^{x,y}|x\rangle\otimes|y\rangle \in \mathcal{H}_{2^r}\otimes\mathcal{H}_{2^s}$ then we write $|\phi\rangle^{RS} = \sum_{x\in\{0,1\}^r}\sum_{y\in\{0,1\}^s}\gamma^{x,y}|x\rangle^R\otimes|y\rangle^S$ to denote the state of both registers H_R and H_S. Given any transformation U_R that acts on a register H_R and any state $|\phi\rangle \in H_R \otimes H_{Others}$, where H_{Others} corresponds to other registers, we define $U_R\,|\phi\rangle \stackrel{def}{=} (U_R \otimes \mathbb{1}_{Others})\,|\phi\rangle$. We use the same notation when U_R denotes a projection operator.

2.2 Model of Computation and Quantum One-Wayness

Quantum one-way functions are defined as the natural generalization of classical one-way functions. Informally, a quantum one-way function is a *classical* function that can be evaluated *efficiently* by a quantum algorithm but cannot be inverted *efficiently* and with *good* probability of success by any quantum algorithm. An algorithm for inverting a one-way function is called an inverter. In this paper, we model inverters (and adversaries against the binding condition) by quantum circuits built out of the universal set of quantum gates $\mathcal{UG} = \{\mathtt{CNot}, \mathtt{H}, \mathtt{R}_{\mathbb{Q}}\}$, where $\mathtt{CNot}$ denotes the controlled-NOT, $\mathtt{H}$ the one qubit Hadamard gate, and $\mathtt{R}_{\mathbb{Q}}$ is an arbitrary one qubit non-trivial rotation specified by a matrix containing only rational numbers [1]. A circuit $\mathcal{C}$ executed in the reverse direction is denoted $\mathcal{C}^\dagger$. The composition of two circuits $\mathcal{C}_1, \mathcal{C}_2$ is denoted $\mathcal{C}_1\cdot\mathcal{C}_2$. If the initial state before the execution of a circuit $\mathcal{C}$ is $|\Phi\rangle$, the final state after the execution is $\mathcal{C}|\Phi\rangle$. To compute a deterministic function $f : \{0,1\}^n \rightarrow \{0,1\}^{m(n)}$, we need a circuit $\mathcal{C}_n$ on $l(n)$ qubits and we must specify $n \leq l(n)$ input qubits and $m(n) \leq l(n)$ output qubits. The classical input x is encoded in the state $|x\rangle$ of the n input qubits. The other qubits, i.e. the non input qubits, are always initialized in the fixed state $|\mathbf{0}\rangle$. The random classical output of the circuit $\mathcal{C}_n$ on input $x \in \{0,1\}^n$ is defined as the classical outcome of $\mathbb{M}_{m(n)}$ on the $m(n)$ output qubits at the end of the circuit. A family $\mathbf{C} = \{\mathcal{C}_n\}_{n=1}^\infty$ is an *exact family of quantum circuits for the family of deterministic functions* $F = \{f_n : \{0,1\}^n \rightarrow \{0,1\}^{m(n)}\}_{n=1}^\infty$ if the the classical output of the circuit $\mathcal{C}_n$ on input $|x\rangle\otimes|\mathbf{0}\rangle \in \mathcal{H}_{2^{l(n)}}$ produces with certainty $f_n(x)$ as output. This definition can be generalized the obvious way in order to cover the non exact case and families of random functions.

The complexity of the circuit $\mathcal{C}_n$ is simply the number $\|\mathcal{C}_n\|_{\mathcal{UG}}$ of elementary gates in $\mathcal{UG}$ contained in $\mathcal{C}_n$. Finally, the family $\mathbf{C}$ is *uniform* if, given 1^n as input, there exists a (quantum) Turing machine that produces $\mathcal{C}_n \in \mathbf{C}$ in (quantum) polynomial time in n. The family $\mathbf{C}$ is *non-uniform* otherwise. Our results hold for both the uniform and the non-uniform cases. The following definition is largely inspired by Luby's definitions for classical one-way functions [10]. Let $\mathbf{x}_n$ be a uniformly distributed random variable over $\{0,1\}^n$.

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

- *there exists an exact family of quantum circuits* $\mathbf{C} = \{\mathcal{C}_n\}_{n>0}$ *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* $S(n) = \Pr\left(f_n(\mathcal{C}_n^{-1}(f_n(\mathbf{x}_n))) = f_n(\mathbf{x}_n)\right)$.

Each family of quantum circuits $\mathbf{C}^{-1}$ *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 $S(n) = \Pr\left(f_n(\mathcal{C}_n^{-1}(\mathbf{y}_n)) = \mathbf{y}_n\right)$ where $\mathbf{y}_n$ is a uniformly distributed random variable in $\{0,1\}^n$.

2.3 The Binding Condition

In a non interactive bit commitment scheme, an honest committer A for bit w starts with a system $H_{All} = H_{Keep} \otimes H_{Open} \otimes H_{Commit}$ in the initial state $|\mathbf{0}\rangle$, executes a quantum circuit $\mathcal{C}_{n,w}$ on $|\mathbf{0}\rangle$ returning the final state $|\Psi_w\rangle \in H_{All}$ and finally sends the subsystem H_{Commit} to B in the reduced state $\rho_B(w) = \mathrm{Tr}_A(|\Psi_w\rangle\langle\Psi_w|)$, where A's Hilbert space is $H_A = H_{Keep} \otimes H_{Open}$. Once the system H_{Commit} is sent away to B, A has only access to $\rho_A(w) = \mathrm{Tr}_B(|\Psi_w\rangle\langle\Psi_w|)$, where B's Hilbert space is $H_B = H_{Commit}$. To open the commitment, A needs only to send the system H_{Open} together with w. The receiver B then tests the value of w by measuring the system $H_{Open} \otimes H_{Commit}$ with some measurement that is fixed by the protocol in view of w. He obtains the outcome $w = 0$, $w = 1$, or $w = \perp$ when the value of w is rejected.

An attack of the committer $\tilde{A}$ must start with the state $|\mathbf{0}\rangle$ of some system $H_{All} = H_{Extra} \otimes H_A \otimes H_{Commit}$. A quantum circuit $\mathbf{C}^n$ that acts on H_{All} is executed to obtain a state $|\tilde{\Psi}\rangle$ and the subsystem H_{Commit} is sent to the receiver. Later, any quantum circuit $\mathbf{O}^n$ which acts on $H_{Extra} \otimes H_{Keep} \otimes H_{Open}$ can be executed before sending the subsystem H_{Open} to the verifier. The important quantum circuits which act on $H_{Extra} \otimes H_{Keep} \otimes H_{Open}$ are the quantum circuits $\mathbf{O}_w^n$, $w = 0,1$, which respectively maximize the probability that the bit $w = 0$ and $w = 1$ is unveiled with success. Therefore, any attack can be modeled by triplets of quantum circuits $\{(\mathbf{C}^n, \mathbf{O}_0^n, \mathbf{O}_1^n)\}_{n>0}$.

The efficiency of an adversary is determined by 1) the total number of elementary gates $T(n) = \|\mathbf{C}^n\|_{\mathcal{UG}} + \|\mathbf{O}_0^n\|_{\mathcal{UG}} + \|\mathbf{O}_1^n\|_{\mathcal{UG}}$ in the three circuits $\mathbf{C}^n$, $\mathbf{O}_0^n$ and $\mathbf{O}_1^n$ and 2) the probabilities $S_w(n)$, $w = 0,1$, that he succeeds to unveil w using the associated optimal circuit $\mathbf{O}_w^n$. The definition of $S_w(n)$ explicitly requires that the value of w, which the adversary tries to open, is chosen not only before the execution of the measurement on $H_{Open} \otimes H_{Commit}$ by the receiver but also before the execution of the circuit $\mathbf{O}_w^n$ by the adversary.

In the classical world, one can always fix the adversary's committed bit by fixing the content of his random tape, that is, 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 way of defining the security of a bit commitment scheme does not apply in the quantum world because, even if we fix the random tape, the adversary could still introduce randomness in the quantum computation. In particular, a quantum committer can always commit to a superposition of $w = 0$ and $w = 1$ by preparing the following state

$$|\Psi(c_0)\rangle = \sqrt{c_0}\,|0_A\rangle \otimes |\Psi_0\rangle + \sqrt{1-c_0}\,|1_A\rangle \otimes |\Psi_1\rangle, \tag{1}$$

where $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are the honest states generated for committing to 0 and 1 respectively and $|0_A\rangle$ and $|1_A\rangle$ are two orthogonal states of H_{Extra}, an extra ancilla kept by A. In this case, for both value of $w \in \{0,1\}$, the opening circuit $\mathbf{O}^n_w$ can put H_{Open} into a mixture that will unveil w successfully with some non zero probability. So we have $S_0(n), S_1(n) > 0$. The fact that the binding condition $S_0(n) = 0 \vee S_1(n) = 0$ is too strong was previously noticed in [13]. We propose the weaker condition $S_0(n) + S_1(n) - 1 \leq \epsilon(n)$ where $\epsilon(n)$ is negligible (i.e. smaller than $1/poly(n)$ for any polynomial $p(n)$). For classical applications, this binding condition (with $\epsilon(n) = 0$) is as good as if the commiter was forced to honestly commit a random bit (with the bias of his choice) and only had the power to abort in view of the bit. The power of this binding condition for quantum applications is unclear, but we think it is a useful condition even in that context.

We now extend this binding condition to a computational setting. It is convenient to restrict ourselves to the cases where $\mathbf{O}^n_0$ is the identity circuit. We can adopt this restriction without lost of generality because any triplet $(\mathbf{C}^n, \mathbf{O}^n_0, \mathbf{O}^n_1)$ can easily be replaced by the three quantum circuits $(\mathbf{C}^n_0, \mathbb{1}, \mathbf{U}^n_{0,1})$, where $\mathbf{C}^n_0 = (\mathbf{O}^n_0 \otimes \mathbb{1}_{Commit}) \cdot \mathbf{C}^n$ and $\mathbf{U}^n_{0,1} = \mathbf{O}^n_1 \cdot (\mathbf{O}^n_0)^\dagger$, without changing the adversaries strategy. The difference in complexity between applying $(\mathbf{C}^n, \mathbf{O}^n_0, \mathbf{O}^n_1)$ and $(\mathbf{C}^n_0, \mathbb{1}, \mathbf{U}^n_{0,1})$ is only $\Delta T(n) = \|\mathbf{O}^n_0\|_{\mathcal{UG}}$. Therefore, the adversary is completely determined by the pair $(\mathbf{C}^n_0, \mathbf{U}^n_{0,1})$ where $\mathbf{C}^n_0$ acts on all registers in H_{All}, and $\mathbf{U}^n_{0,1}$ is restricted to act only in $H_{Extra} \otimes H_{Keep} \otimes H_{Open}$.

Definition 2 *An adversary $\tilde{A} = \{(\mathbf{C}^n_0, \mathbf{U}^n_{0,1})\}_n$ for the binding condition of a quantum bit commitment scheme is $(S(n), T(n))$–*successful *if for all $n \in \mathbb{N}$, $\|\mathbf{U}^n_{0,1}\|_{\mathcal{UG}} + \|\mathbf{C}^n_0\|_{\mathcal{UG}} \leq T(n)$ and $S_0(n) + S_1(n) - 1 = S(n)$. An adversary with $S(n) = 1$ is called a* perfect adversary.

Any $(0, T(n))$-successful adversary does not achieve more than what an honest committer is able to do. In order to cheat, an adversary must be $(S(n), T(n))$-successful for some non-negligible $S(n) > 0$. The security of a quantum bit commitment scheme is defined as follow:

Definition 3 *A quantum bit commitment scheme is $R(n)$–*binding *if there exists no $(S(n), T(n)$–successful quantum adversary against the binding condition that satisfies $T(n)/S(n) \leq R(n)$. A quantum bit commitment scheme is* perfectly concealing (statistically concealing) *if the systems received for the commitments of 0 and 1 are identical (resp. statistically indistinguishable).*

It is easy to verify that if a $R(n)$-binding classical bit commitment scheme (satisfying the classical definition) allows to implement a cryptographic task securely, then using a $R(n)$-binding quantum bit commitment scheme instead would also provide a secure implementation.

The scheme we describe next will be shown to be perfectly concealing and $\Omega(R(n))$-binding whenever used with a $R(n)^2$-secure family of one-way permutations.

3 The Scheme

Let $\Sigma = \{\sigma_n : \{0,1\}^n \rightarrow \{0,1\}^n | n > 0\}$ be a family of one-way permutations. The commitment scheme takes, as common input, a security parameter $n \in \mathbb{N}$ and the description of family Σ. The quantum part of the protocol below is similar to the protocol for quantum coin tossing described in [3]. Given Σ and n, the players determine the instance $\sigma_n : \{0,1\}^n \rightarrow \{0,1\}^n \in \Sigma$. A sends through the quantum channel $\sigma_n(x)$ for $x \in_R \{0,1\}^n$ polarized in basis $\theta(w)^n$ where $w \in \{0,1\}$ is the committed bit. B then stores the received quantum state until the opening phase. It is implicit here that B must protect the received system

---

$\texttt{commit}_{\Sigma,n}(w)$

1. A picks $x \in_R \{0,1\}^n$, computes $y = \sigma_n(x)$ for $\sigma_n \in \Sigma$,
2. A sends the quantum state $|\sigma_n(x)\rangle_{\theta(w)^n} \in \mathcal{H}_{Commit}$ to B.

$H_{Commit} \simeq \mathcal{H}_{2^n}$ against decoherence until the opening phase. The opening phase consists only for A to unveil all her previous random choices allowing B to verify the consistency of the announcement by measuring the received state. So, $H_{Open} \simeq \mathcal{H}_{2^n}$ is only used to store classical information.

$\texttt{open}_{\Sigma,n}(w,x)$

1. A announces w and x to B,
2. B measures ρ_B with measurement $\mathbb{M}_{\theta(w)^n}$ thus providing the classical outcome $\tilde{y} \in \{0,1\}^n$,
3. B accepts if and only if $\tilde{y} = \sigma_n(x)$.

---

4 The Concealing Condition

In this section, we show that every execution of $\mathtt{commit}_{\Sigma,n}$ conceals w perfectly.

Let ρ_w for $w \in \{0,1\}$ be the density matrix corresponding to the mixture sent by A when classical bit w is committed. Since σ_n is a permutation of the elements in the set $\{0,1\}^n$, we get

$$\rho_0 = \sum_{x\in\{0,1\}^n} 2^{-n}|x\rangle_{+^n}\langle x| = 2^{-n}\mathbb{1}_{2^n} = \sum_{x\in\{0,1\}^n} 2^{-n}|x\rangle_{\times^n}\langle x| = \rho_1 \qquad (2)$$

where $\mathbb{1}_{2^n}$ is the identity operator in $\mathcal{H}_{2^n}$. The following lemma follows directly from (2).

Lemma 1. *Protocol* $\mathtt{commit}_{\Sigma,n}(w)$ *is perfectly concealing.*

Proof: The quantum states ρ_0 and ρ_1 are the same. It follows that no quantum measurement can distinguish between the commitments of 0 and 1. □

5 The Most General Attack

Here we describe the most general adversary $\tilde{A} = \{(\mathbf{C}_0^n, \mathbf{U}_{0,1}^n)\}_{n\geq n_0}$ against the binding condition of our scheme. We shall prove that any such attack can be used to invert the one-way permutation in subsequent sections.

The adversary doesn't necessarily know which value will take y on the receiver's side after the measurement $\mathbb{M}_{\theta(w)^n}$ on H_{Commit} associated with the opening of w. He computes $x \in \{0,1\}^n$ using $\mathbf{O}_w^n$, announces (x, w) and hopes that $\sigma_n(x) = y$. So we have that $H_{Open} \simeq \mathcal{H}_{2^n}$ is used to encode $x \in \{0,1\}^n$. We separate the entire system in three parts: the system H_{Commit} that encodes y, the system H_{Open} that encodes x, and the remainder of the system that we conveniently denote all together by H_{Keep} (thus including for simplicity register H_{Extra}). We easily obtain that the states $|\tilde{\Psi}_w^n\rangle = \mathbf{C}_w^n|\mathbf{0}\rangle$, $w = 0,1$, can be written in the form

$$|\tilde{\Psi}_0^n\rangle = \sum_{x,y\in\{0,1\}^n} |\gamma_0^{x,y}\rangle^{Keep} \otimes |x\rangle^{Open} \otimes |y\rangle_{+^n}^{Commit} = \mathbf{C}_0^n|\mathbf{0}\rangle \qquad (3)$$

with $\sum_{x,y} \||\gamma_0^{x,y}\rangle\|^2 = 1$, and

$$|\tilde{\Psi}_1^n\rangle = \sum_{x,y\in\{0,1\}^n} |\gamma_1^{x,y}\rangle^{Keep} \otimes |x\rangle^{Open} \otimes |y\rangle_{\times^n}^{Commit} = \mathbf{U}_{0,1}^n|\tilde{\Psi}_0^n\rangle \qquad (4)$$

with $\sum_{x,y} \||\gamma_1^{x,y}\rangle\|^2 = 1$. In the following, we shall refer to states $|\tilde{\Psi}_0^n\rangle$ and $|\tilde{\Psi}_1^n\rangle$ as the 0-state and the 1-state of the attack respectively. The transformation $\mathbf{U}_{0,1}^n$ is applied on the system $H_{Keep} \otimes H_{Open}$.

Next section restricts the analysis to the case where an adversary A can open both $w = 0$ and $w = 1$ with probability of success $p_w = 1$. Such an adversary is called a *perfect adversary*. We show that any perfect adversary can invert efficiently $\sigma_n(x)$ for any $x \in \{0,1\}^n$. In Sect. 7 we generalize the result to all imperfect but otherwise good adversaries. We show that any polynomial time adversary for which $p_0 + p_1 \geq 1 + \frac{1}{poly(n)}$ can invert $\sigma_n(x)$ for $x \in_R \{0,1\}^n$ efficiently and with non-negligible probability of success.

6 Perfect Attacks

In this section, we prove that any efficient perfect adversary $A = \{(\mathbf{C}_0^n, \mathbf{U}_{0,1}^n)\}_n$ against the binding condition can be used to invert efficiently the one-way permutation with probability of success 1. In the next section, we shall use a similar technique for the case where the attack is not perfect.

By definition, a perfect adversary A is $(1, T(n))$-successful, that is: $S_0(n) = S_1(n) = 1$. We obtain that $\| |\gamma_w^{x,y}\rangle \| = 0$ if $\sigma_n(x) \neq y$:

$$|\Psi_0^n\rangle = \sum_{x \in \{0,1\}^n} |\gamma_0^x\rangle^{Keep} \otimes |x\rangle^{Open} \otimes |\sigma_n(x)\rangle_{+^n}^{Commit} = \mathbf{C}_0^n |\mathbf{0}\rangle \tag{5}$$

where $|\gamma_0^x\rangle$ corresponds to $|\gamma_0^{x,\sigma_n(x)}\rangle$ and $\sum_x \| |\gamma_0^x\rangle \|^2 = 1$, and

$$|\Psi_1^n\rangle = \sum_{x \in \{0,1\}^n} |\gamma_1^x\rangle^{Keep} \otimes |x\rangle^{Open} \otimes |\sigma_n(x)\rangle_{\times^n}^{Commit} = \mathbf{U}_{0,1}^n |\Psi_0^n\rangle \tag{6}$$

where $|\gamma_1^x\rangle$ corresponds to $|\gamma_1^{x,\sigma_n(x)}\rangle$ and $\sum_x \| |\gamma_1^x\rangle \|^2 = 1$. Any pair of 0-state and 1-state satisfying (5) and (6) is called a *perfect pair*. Any perfect adversary $A = \{(\mathbf{C}_0^n, \mathbf{U}_{0,1}^n)\}_n$ generates a perfect pair for all $n > 0$.

Let $\mathbb{P}_{Commit}^{u,+}$ and $\mathbb{P}_{Commit}^{u,\times}$ be the projection operators $\mathbb{P}_{+^n}^u$ and $\mathbb{P}_{\times^n}^u$ respectively, acting upon register H_{Commit}. We assume that we have an input register $H_Y \simeq \mathcal{H}_{2^n}$ initialized in the basis state $|y\rangle$ on input y. The states $|\Phi_0^n(u)\rangle = \mathbb{P}_{Commit}^{u,\times} |\Psi_0^n\rangle$, $u \in \{0,1\}^n$, 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. $\| |\Phi_0^n(u)\rangle \| = 2^{-n/2}$,
2. there exists a simple circuit $\mathbf{W}_n$ on $H_Y \otimes H_{Open} \otimes H_{Commit}$ which, if u is encoded in register H_Y, unitarily maps $|\Psi_0^n\rangle$ into $2^{n/2} |\Phi_0^n(u)\rangle$, and
3. $\mathbf{U}_{0,1}^n |\Phi_0^n(u)\rangle = |\gamma^{\sigma^{-1}(u)}\rangle^{Keep} \otimes |\sigma_n^{-1}(u)\rangle^{Open} \otimes |u\rangle_{\times^n}^{Commit}$.

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

6.1 Proof of Properties 1 and 3

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

$$|\Psi_0^n\rangle = 2^{-n/2} \sum_{u,v \in \{0,1\}^n} (-1)^{u \odot v} |\gamma_0^{\sigma_n^{-1}(v)}\rangle^{Keep} \otimes |\sigma_n^{-1}(v)\rangle^{Open} \otimes |u\rangle_{\times^n}^{Commit}$$

from which we easily obtain, after the change of variable $\sigma_n^{-1}(v) \rightarrow x$,

$$|\Phi_0^n(u)\rangle = 2^{-n/2} \sum_{x\in\{0,1\}^n} (-1)^{u\odot\sigma_n(x)} |\gamma_0^x\rangle^{Keep} \otimes |x\rangle^{Open} \otimes |u\rangle_{\times^n}^{Commit}. \qquad (7)$$

Property 1 follows from (7). Note that the states $|\Phi_0^n(u)\rangle$ can be mapped one into the other by a unitary mapping, a conditional phase shift which depends on u and x. Because (6) can be rewritten as

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

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

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

which concludes the proof of property 3.

6.2 Proof of Property 2

A simple comparison of (5) and (7) suggests what needs to be done to obtain $2^{n/2}|\Phi_0^n(y)\rangle$ efficiently starting from $|\Psi_0^n\rangle$. Assume the input register $H_Y = H_Y^1 \otimes \ldots \otimes H_Y^n \simeq \mathcal{H}_{2^n}$ is in the basis state $|y\rangle$. The first step is to add the phase $(-1)^{y\odot\sigma_n(x)}$ in front of each term in the sum of (5). Note that, for every $y \in \{0,1\}^n$, this is a unitary mapping on $H_{Keep} \otimes H_{Open} \otimes H_{Commit}$. It is sufficient to execute a circuit $\hat{\oplus}_1$ which, for each $i \in \{1,\ldots,n\}$, acts on the corresponding pair of qubits in $H_Y^i \otimes H_{Commit}^i$. The circuit $\hat{\oplus}_1$ maps each state $|y_i\rangle \otimes |\sigma_n(x)_i\rangle$, $i = 1,\ldots,n$, into $(-1)^{(y_i \odot \sigma_n(x)_i)}(|y_i\rangle \otimes |\sigma_n(x)_i\rangle)$. It can easily be implemented as $\hat{\oplus}_1 = (\mathtt{H}\otimes \mathbb{1}_{Commit})\cdot\mathtt{CNot}\cdot(\mathtt{H}\otimes\mathbb{1}_{Commit})$ where each $\mathtt{H}$ is applied to register H_Y^i and where register H_{Commit}^i encodes the control bit of the $\mathtt{CNot}$ gate. We denote by $\hat{\oplus}_n$ the complete quantum circuit acting in $H_Y \otimes H_{Commit}$ and applying $\hat{\oplus}_1$ to each pair $i \in \{1,\ldots,n\}$ of qubits $|y_i\rangle \otimes |\sigma_n(x)_i\rangle \in H_Y^i \otimes H_{Commit}^i$.

The second step is to set the register H_{Commit} which contains the state $|\sigma_n(x)\rangle_{+^n}$ into the new state $|y\rangle_{\times^n}$. For this we use the composition of three circuits. The first circuit $\mathbf{U}_{\sigma_n} : |x\rangle^{Open}\otimes|u\rangle^{Commit} \mapsto |x\rangle^{Open}\otimes|u\oplus\sigma_n(x)\rangle^{Commit}$ sets the quantum register H_{Commit} into the new state $|\mathbf{0}\rangle_{+^n}$. Note that $\mathbf{U}_{\sigma_n}$ is the quantum circuit that is guaranteed to compute $\sigma_n(x)$ efficiently. The second circuit is $\oplus_n : |y\rangle^Y \otimes |u\rangle^{Commit} \mapsto |y\rangle^Y \otimes |y \oplus u\rangle^{Commit}$ which sets H_{Commit} into the state $|y\rangle_{+^n}$ by simply applying a $\mathtt{CNot}$ between registers $H_{Commit}^i, H_Y^i \simeq \mathcal{H}_2$ for $i \in \{1,\ldots,n\}$. Finally the third circuit executes the Hadamard transform $\mathtt{H}_n$ on H_{Commit} which maps the $+^n$ basis into the $\times^n$ basis (it is simply n Hadamard gates $\mathtt{H} \in \mathcal{UG}$) . The composition of $\hat{\oplus}_n$ with these three circuits is the circuit $\mathbf{W}_n$ shown in Fig. 1. This circuit allows to generate any $2^{n/2}|\Phi_0^n(y)\rangle$ for $y \in \{0,1\}^n$. Moreover, it is easy to verify that $\|\mathbf{W}_n\|_{\mathcal{UG}} = \|\mathbf{U}_{\sigma_n}\|_{\mathcal{UG}} + 5n$. The following is a straightforward consequence of these three properties, the definition of $\mathbf{W}_n$ and the above discussion:

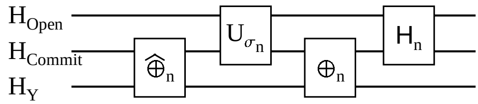

Fig. 1. Transformation $\mathbf{W}_n$.

Lemma 2. *If there exists a $(1, T(n))$-successful adversary against* $\texttt{commit}_{\Sigma,n}$ *then there exists an adversary against Σ with time-success ratio*

$$R(n) \leq T(n) + \|\mathbf{U}_{\sigma_n}\|_{\mathcal{UG}} + 5n.$$

It follows that the adversary against Σ has about the same complexity than the one against the binding condition of $\texttt{commit}_{\Sigma,n}$. In the next section, we show that the same technique can be applied to the case where the adversary does not implement a perfect attack against $\texttt{commit}_{\Sigma,n}$.

7 The General Case

In this section, we are considering any attack that yields a non-negligible success probability to a cheating committer. In terms of Definition 2, such an adversary $\tilde{A} = \{(\mathbf{C}_0^n, \mathbf{U}_{0,1}^n)\}_n$ must be $(\epsilon(n), T(n))$-successful for some $\epsilon(n) \geq 1/poly(n) \geq 0$. In order for the attack to be efficient, $T(n)$ must also be upper bounded by some polynomial.

In general, the 0-state $|\tilde{\Psi}_0^n\rangle$ and 1-state $|\tilde{\Psi}_1^n\rangle$ of adversary $\tilde{A}$ can always be written as in (3) and (4) respectively. In this general case, the probability of success of unveiling the bit w, i.e. the probability of not being caught cheating, is the probability of the event $\tilde{A}$ *announces a value x and the outcome of B's measurement happens to be $\sigma_n(x)$*. One can see easily that this probability is given by :

$$S_w^{\tilde{A}} = S_w^{\tilde{A}}(n) = \sum_v \| |\gamma_w^{v,\sigma_n(v)}\rangle \|^2. \tag{8}$$

If the adversary $\tilde{A}$ is $(\epsilon(n), T(n))$-successful then

$$S_0^{\tilde{A}} + S_1^{\tilde{A}} \geq 1 + \epsilon(n). \tag{9}$$

In that setting, our goal is to show that from such an adversary $\tilde{A}$, $\sigma_n^{-1}(y)$ can be computed similarly to the perfect case and with probability of success at least $1/poly(n)$ whenever $y \in_R \{0,1\}^n$ and $\epsilon(n)^{-1}$ is smaller than some positive polynomial.

7.1 The Inverter

Compared to the perfect case, the inverter for the general case will involve an extra step devised to produce a *perfect* $|\Psi_0^n\rangle$ from the initial and *imperfect* 0-state

$|\tilde{\Psi}_0^n\rangle$. Although this preprocessing will succeed only with some probability, any $(\frac{1}{p(n)}, T(n))$-successful adversary can *distill* $|\Psi_0^n\rangle$ from $|\tilde{\Psi}_0^n\rangle$ efficiently and with good probability of success. From $|\Psi_0^n\rangle$, the inverter then proceeds the same way as in the perfect case.

The distillation process involves a transformation $\mathbf{T}_n$ acting in $H_{Open} \otimes H_{Commit} \otimes H_T$ where $H_T \simeq \mathcal{H}_{2^n}$ is an extra register. We define $\mathbf{T}_n$ as:

$$\mathbf{T}_n : |x\rangle^{Open}|y\rangle^{Commit}|a\rangle^T \mapsto |x\rangle^{Open}|y\rangle^{Commit}|\sigma_n(x) \oplus y \oplus a\rangle^T. \tag{10}$$

Clearly, one can always write

$$\begin{aligned}\mathbf{T}_n(|\tilde{\Psi}_0^n\rangle^{All} \otimes |\mathbf{0}\rangle^T) = &\sum_{\sigma_n(x)\neq z} |\gamma_0^{x,z}\rangle^{Keep}|x\rangle^{Open}|z\rangle^{Commit}|\sigma_n(x) \oplus z\rangle^T \\ &+ \sum_x |\gamma_0^{x,\sigma_n(x)}\rangle^{Keep}|x\rangle^{Open}|\sigma_n(x)\rangle^{Commit}|\mathbf{0}\rangle^T. \end{aligned} \tag{11}$$

Upon standard measurement of register H_T in state $|\mathbf{0}\rangle$, the adversary obtains the quantum residue (by tracing out the ancilla):

$$|\Psi_0^n\rangle = \sum_x |\gamma_0^x\rangle^{Keep} \otimes |x\rangle^{Open} \otimes |\sigma_n(x)\rangle^{Commit} \tag{12}$$

where $|\gamma_0^x\rangle^{Keep} = \frac{1}{\sqrt{S_0^{\tilde{A}}}}|\gamma^{x,\sigma_n(x)}\rangle^{Keep}$, with probability

$$S_0^{\tilde{A}} = \sum_v \| |\gamma_0^{v,\sigma_n(v)}\rangle\|^2 = |\langle\Psi_0^n|\tilde{\Psi}_0^n\rangle|^2.$$

It is easy to verify that $\mathbf{T}_n$ can be implemented by a quantum circuit of $O(\|\mathbf{U}_{\sigma_n}\|_{\mathcal{UG}})$ elementary gates. On input $y \in_R \{0,1\}^n$, the inverter then works exactly as in the perfect case. In Fig. 2, the quantum circuit for the general inverter $\mathbf{I}_n^{\tilde{A}}(y)$ is shown. The input quantum register is H_Y and the output register is H_{Open}. The output is the outcome of the standard measurement $\mathbb{M}_n$ applied to the output register H_{Open} which hopefully contains $x = \sigma_n^{-1}(y)$. The

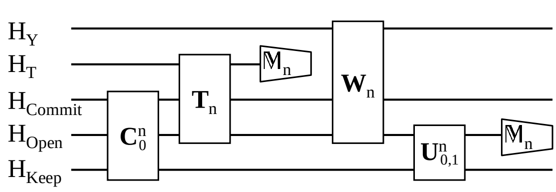

Fig. 2. The inverter $\mathbf{I}_n^{\tilde{A}}(y), y \in \{0,1\}^n$ obtained from adversary $\tilde{A} = (\mathbf{C}_0^n, \mathbf{U}_{0,1}^n)$.

following lemma is straightforward and establishes the efficiency of the inverter in terms of the efficiency of $\tilde{A}$'s against $\texttt{commit}_{\Sigma,n}$:

Lemma 3. *If $\tilde{A}$ is $(\cdot, T(n))$-successful then*

$$\|\mathbf{I}_n^{\tilde{A}}(y)\|_{\mathcal{UG}} \in O(T(n) + \|\mathbf{U}_{\sigma_n}\|_{\mathcal{UG}}).$$

It should be noted that gates $\oplus_n$ and $\mathtt{H}_n$ appearing in circuit $\mathbf{W}_n$ are not taken into account in the statement of Lemma 3. The reason is that none of them influence the final outcome since they commute with the final measurement in H_{Open}. They have been included in $\mathbf{W}_n$ to help the reader with the analysis of the success probability described in the next section.

7.2 Analysis of the Success Probability

Let $\tilde{A} = \{(\mathbf{C}_0^n, \mathbf{U}_{0,1}^n)\}_{n>0}$ be any $(\epsilon(n), \cdot)$-successful adversary for some $\epsilon(n) > 0$ thus satisfying $S_0^{\tilde{A}} + S_1^{\tilde{A}} \geq 1 + \epsilon(n)$. Let $\mathbb{P}_{Open}^x$ be the projection operator $\mathbb{P}^x$ applied to register H_{Open}. We recall that $\mathbb{P}_{Commit}^{y,+}$ and $\mathbb{P}_{Commit}^{y,\times}$ are the projection operators $\mathbb{P}_{+^n}^y$ and $\mathbb{P}_{\times^n}^y$ respectively, acting upon register H_{Commit}. We now define the two projection operators:

$$\boldsymbol{P}_0 = \sum_{x \in \{0,1\}^n} \mathbb{P}_{Open}^x \otimes \mathbb{P}_{Commit}^{\sigma_n(x),+} \text{ and } \boldsymbol{P}_1 = \sum_{x \in \{0,1\}^n} \mathbb{P}_{Open}^x \otimes \mathbb{P}_{Commit}^{\sigma_n(x),\times} \tag{13}$$

which have the property, using (8), that $S_0^{\tilde{A}} = \|\boldsymbol{P}_0|\tilde{\Psi}_0^n\rangle\|^2$ and $S_1^{\tilde{A}} = \|\boldsymbol{P}_1|\tilde{\Psi}_1^n\rangle\|^2$. Next lemma relates the success probability to projections $\boldsymbol{P}_0$ and $\boldsymbol{P}_1$.

Lemma 4. *The probability of success p_s of inverter $\mathbf{I}_n^{\tilde{A}}(y)$ satisfies*

$$p_s = \|\boldsymbol{P}_1 \mathbf{U}_{0,1}^n \boldsymbol{P}_0 |\tilde{\Psi}_0^n\rangle\|^2.$$

Proof: We recall that the probability of success is defined in terms of a uniformly distributed input y. We will first compute the probability $p_s(y)$ that the inverter succeeds on input $y \in \{0,1\}^n$. Assume that right after gate $\mathbf{T}_n$, the register H_T is observed in state $|\mathbf{0}\rangle$. The registers $H_{All} \otimes H_Y$ have now collapsed to the state $|y\rangle^Y \otimes |\Psi_0^n\rangle$ where $|\Psi_0^n\rangle$ is the state $\boldsymbol{P}_0|\tilde{\Psi}_0^n\rangle$ after renormalization. Note that $|\Psi_0^n\rangle$ is a perfect 0-state. This event has probability $\|\boldsymbol{P}_0|\tilde{\Psi}_0\rangle\|^2 = S_0^{\tilde{A}}$ to happen according to (12). Next the circuit $\mathbf{W}_n$, with y encoded in H_Y, unitarily maps the state $|\Psi_0^n\rangle$ into the state $2^{n/2}|\Phi_0^n(y)\rangle = 2^{n/2}\,\mathbb{P}_{Commit}^{y,\times}\,|\Psi_0^n\rangle$ (see Sect. 6). Then the circuit $\mathbf{U}_{0,1}^n$ returns the state $2^{n/2}\,\mathbb{P}_{Commit}^{y,\times}\,\mathbf{U}_{0,1}^n\,|\Psi_0^n\rangle$. Finally, the register H_{Open} is measured and the probability of success given the initial state $|\Psi_0^n\rangle$ is $\|2^{n/2}\,\mathbb{P}_{Open}^{\sigma_n^{-1}(y)}\,\mathbb{P}_{Commit}^{y,\times}\,\mathbf{U}_{0,1}^n\,|\Psi_0^n\rangle\|^2$. Using (12), we get that $p_s(y) = S_0^{\tilde{A}} 2^n\,\|\mathbb{P}_{Open}^{\sigma_n^{-1}(y)}\,\mathbb{P}_{Commit}^{y,\times}\,\mathbf{U}_{0,1}^n\,|\Psi_0^n\rangle\|^2 = 2^n\,\|\mathbb{P}_{Open}^{\sigma_n^{-1}(y)}\,\mathbb{P}_{Commit}^{y,\times}\,\mathbf{U}_{0,1}^n\,\boldsymbol{P}_0\,|\tilde{\Psi}_0^n\rangle\|^2$. Averaging over all values of the uniformly distributed variable y we obtain:

$$\begin{aligned} p_s &= \sum_{y \in \{0,1\}^n} 2^{-n} p_s(y) = \sum_{y \in \{0,1\}^n} \|\left(\mathbb{P}_{Open}^{\sigma_n^{-1}(y)} \otimes \mathbb{P}_{Commit}^{y,\times}\right) \mathbf{U}_{0,1}^n \boldsymbol{P}_0 |\tilde{\Psi}_0^n\rangle\|^2 \\ &= \|\left(\sum_{y \in \{0,1\}^n} \mathbb{P}_{Open}^{\sigma_n^{-1}(y)} \otimes \mathbb{P}_{Commit}^{y,\times}\right) \mathbf{U}_{0,1}^n \boldsymbol{P}_0 |\tilde{\Psi}_0^n\rangle\|^2 = \|\boldsymbol{P}_1 \mathbf{U}_{0,1}^n \boldsymbol{P}_0\,|\tilde{\Psi}_0^n\rangle\|^2 \end{aligned} \tag{14}$$

where (14) is obtained from the fact that $\{\mathbb{P}^x_{Open} \otimes \mathbb{P}^{\sigma_n(x),\times}_{Commit}\}_{x\in\{0,1\}^n}$ is a set of orthogonal projections and from Pythagoras theorem. □

We are now ready to relate the probability of success for the inverter given a *good* adversary against the binding condition of $\mathtt{commit}_{\Sigma,n}$.

Lemma 5. *Let $\boldsymbol{I}^{\tilde{A}}_n$ be the inverter obtained from a $(S^{\tilde{A}}_0 + S^{\tilde{A}}_1 - 1, \cdot)$-successful adversary $\tilde{A}$ with $S^{\tilde{A}}_0 + S^{\tilde{A}}_1 \geq 1+\epsilon(n)$ for $\epsilon(n) > 0$ for all $n > 0$. Then the success probability p_s to invert with success a random image element satisfies*

$$p_s \geq (\sqrt{S^{\tilde{A}}_1} - \sqrt{1 - S^{\tilde{A}}_0}\,)^2.$$

Proof: Using lemma 4, we can write

$$\begin{aligned} p_s &= \|\boldsymbol{P}_1 \mathbf{U}^n_{0,1} \boldsymbol{P}_0 |\tilde{\Psi}^n_0\rangle\|^2 = \|\boldsymbol{P}_1 \mathbf{U}^n_{0,1} (\mathbb{1}_{\tilde{A}} - \boldsymbol{P}^{\perp}_0)|\tilde{\Psi}^n_0\rangle\|^2 \\ &= \|\boldsymbol{P}_1 \mathbf{U}^n_{0,1} |\tilde{\Psi}^n_0\rangle - \boldsymbol{P}_1 \mathbf{U}^n_{0,1} \boldsymbol{P}^{\perp}_0 |\tilde{\Psi}^n_0\rangle\|^2 = \|\boldsymbol{P}_1 |\tilde{\Psi}^n_1\rangle - \boldsymbol{P}_1 \mathbf{U}^n_{0,1} \boldsymbol{P}^{\perp}_0 |\tilde{\Psi}^n_0\rangle\|^2. \end{aligned}$$

Using the triangle inequality and $S^{\tilde{A}}_1 > 1 - S^{\tilde{A}}_0$, we are led to

$$\begin{aligned} p_s &\geq \left(\|\boldsymbol{P}_1 |\tilde{\Psi}^n_1\rangle\| - \|\boldsymbol{P}_1 \mathbf{U}^n_{0,1} \boldsymbol{P}^{\perp}_0 |\tilde{\Psi}^n_0\rangle\|\right)^2 \\ &\geq \left(\|\boldsymbol{P}_1 |\tilde{\Psi}^n_1\rangle\| - \|\boldsymbol{P}^{\perp}_0 |\tilde{\Psi}^n_0\rangle\|\right)^2 = \left(\sqrt{S^{\tilde{A}}_1} - \sqrt{1 - S^{\tilde{A}}_0}\right)^2. \end{aligned}$$

□

From Lemma 5 and a few manipulations, we conclude that $S^{\tilde{A}}_0 + S^{\tilde{A}}_1 > 1 + \epsilon(n)$ implies that $p_s > \epsilon(n)^2/4$. In addition, if $\epsilon(n) \in \Omega(\frac{1}{poly(n)})$ and $T(n) \in O(poly(n))$ then the inverter works in polynomial time with probability of success in $\Omega(1/poly(n)^2)$.

8 Conclusion

The concealing condition is established unconditionally by Lemma 1. Lemmas 3 and 5 imply that any $(S(n), T(n))$-successful adversary against $\mathtt{commit}_{\Sigma,n}$ can invert the family of one-way permutations Σ with time-success ratio roughly $T(n)/S(n)^2$. We finally obtain:

Theorem 1. *Let Σ be a $R(n)$-secure family of one-way permutations. Protocol $\mathtt{commit}_{\Sigma,n}$ is unconditionally concealing and $R'(n)$–binding where $R'(n) \in \Omega(\sqrt{R(n)})$.*

Our reduction produces only a quadratic blow-up in the worst case between the time-success ratio of the inverter and the time-success ratio of the attack. Compared to NOVY's construction, the reduction is tighter by several degrees of magnitude. If Σ is $T(n)/S(n)$–secure with $\frac{1}{S(n)} \in O(\sqrt{T(n)})$ then the reduction is optimal.

In order for the scheme to be practical, the receiver should not be required to store the received qubits until the opening phase. It is an open question whether or not our scheme is still secure if the receiver measures each qubit π_i upon reception in a random basis $\theta_i \in_R \{+, \times\}$. The opening of $w \in \{0,1\}$ being accepted if each time $\theta_i = \theta(w)$, the announced $x \in \{0,1\}^n$ is such that $[\sigma_n(x)]_i = \tilde{y}_i$. That way, the protocol would require similar technology than the one needed for implementing the BB84 quantum-key distribution protocol [2].

It is also not clear how to modify the scheme in order to deal with noisy quantum transmissions. Another problem linked to practical implementation is the lack of tolerance to multi-photon pulses. If for $x, w \in \{0,1\}$, the quantum state $|\phi_x\rangle_{\theta(w)} \otimes |\phi_x\rangle_{\theta(w)}$ is sent instead of $|\phi_x\rangle_{\theta(w)}$ then $\texttt{commit}_{\Sigma,n}$ is no more concealing. Moreover, it is impossible in practice to make sure that only one qubit per pulse is sent.

Our main open problem is the finding of candidates for families of quantum one-way permutations or functions. If a candidate family of quantum one-way functions was also computable efficiently on a classical computer then classical cryptography could provide computational security even against quantum adversaries. It would also be interesting to find candidates one-way functions that are not classical one-way. Quantum cryptography could then provide a different basis for computational security in cryptography.

Acknowledgements. Thanks to Ivan Damgård for several enlightening discussions and to Peter Høyer for helping with the circuitry. Thanks also to Alain Tapp for helpful comments on earlier drafts.

References

1. Barenco, A., C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, "Elementary Gates for Quantum Computation", *Physical Review A*, vol. 52, no 5, November 1995, pp. 3457 – 3467.
2. Bennett, C.H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental Quantum Cryptography", *Journal of Cryptology*, vol. 5, no. 1, 1992, pp. 3 – 28.
3. Bennett, C. H. and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, December 1984, pp. 175 – 179.
4. Bennett, C. H., G. Brassard, C. Crépeau and M.-H. Skubiszewska, "Practical Quantum Oblivious Transfer", *Advances in Cryptology : CRYPTO '91 : Proceedings*, Lecture Notes in Computer Science, no 576, Springer–Verlag, August 1992, pp. 362 – 371.
5. Brassard, G., D. Chaum and C. Crépeau, "Minimum Disclosure Proofs of Knowledge", *Journal of Computer and System Sciences*, vol. 37 , 1988, pp. 156 – 189.
6. Damgård, I., personal communication, December 1998.
7. DiVincenzo, D.P., "Two-Bit Gates Are Universal For Quantum Computation", *Physical Review A*, vol. 51, no 2, February 1995, pp. 1015 – 1022.
8. Impagliazzo, R. and S. Rudich, "Limits on Provable Consequences of One-Way Permutations", *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*, May 1989, pp. 44 – 61.

9. Lo, H.–K. and H. F. Chau, “Is quantum Bit Commitment Really Possible?”, *Physical Review Letters*, vol. 78, no 17, April 1997, pp. 3410 – 3413.
10. Luby, M., *Pseudorandomness and Cryptographic Applications*, Princeton University Press, 1996.
11. Mayers, D., “The Trouble With Quantum Bit Commitment”, `http://xxx.lanl.gov/abs/quant-ph/9603015`, March 1996.
12. Mayers, D., “Quantum Key Distribution and String Oblivious Transfer in Noisy Channels”, *Advances in Cryptology : CRYPTO ’96 : Proceedings*, Lecture Notes in Computer Science, no 1109, Springer–Verlag, August 1996, pp. 343 – 357.
13. Mayers, D., “Unconditionally Secure Quantum Bit Commitment is Impossible”, *Physical Review Letters*, vol. 78, no 17, April 1997, pp. 3414 – 3417.
14. Mayers, D., “Unconditional Security in Quantum Cryptography”, `http://xxx.lanl.gov/abs/quant-ph/9802025`, February 1998.
15. Naor, M., R. Ostrovsky, R. Ventkatesan and M. Young, “Perfect Zero-Knowledge Arguments For NP Using Any One-Way Permutation”, *Journal of Cryptology*, vol. 11, no 2, 1998, pp. 87 – 108.
16. Salvail, L., “Quantum Bit Commitment From a Physical Assumption”, *Advances in Cryptology : CRYPTO ’98 : Proceedings*, Lecture Notes in Computer Science, no 1462, Springer–Verlag, August 1998, pp. 338 – 353.
17. Shor, P., “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp. 124 – 134.
18. van de Graaf, J., *Torwards a Formal Definition of Security for Quantum Protocols*, Ph.D. thesis, Département d’informatique et de recherche opérationelle, Université de Montréal, 1997.
19. Yao, A. C.–C., “Security of Quantum Protocols Against Coherent Measurements”, *Proceedings of the Twenty-seventh Annual ACM Symposium on Theory of Computing*, May 1995, pp. 67 – 75.