A Perfectly Binding Commitment Scheme Against Quantum Attacks

Zeng Bing, Chen Liang, and Tang Xueming

Abstract—It's known that perfectly binding quantum computationally hiding commitment schemes can be constructed from any quantum one-way permutation. Since no quantum one-way permutations are known, it has been unknown by far whether we can get such a concrete commitment scheme. In this paper, we give a positive answer. Specifically, we present such a lattice-based commitment scheme, which is built from the results gained by Gentry et al.

Index Terms—Commitment scheme, zero-knowledge, lattice, quantum attack.

1 Introduction

A commitment scheme is a two-phase two-party interactive protocol: in the commit phase, a sender P_1 sends a commitment to a receiver P_2, where the security property hiding should prevent P_2 from knowing the committed value; in the reveal phase, P_1 reveals the committed value, where the security property binding should prevent P_1 from revealing a value that is different from the committed value.

Commitment schemes are one of the most basic building blocks for cryptographic protocols. For example, assuming the existence of perfectly binding commitment schemes, the well-known Goldreich-Micali-Wigderson protocol for graph 3-coloring is zero-knowledge [7], which implies the existence of a computational zero-knowledge proof system for any language in $\mathcal{NP}$ under the same assumption. In 2009, Watrous furthers this result to hold in the quantum setting under a stronger assumption that there exists perfectly binding commitment schemes with security against quantum attacks [14].

We remark that using statistically binding ones with corresponding security level in the protocols of [7], [14] is appropriate too, this is justified by observing that later Goldreich in fact uses a statistically binding one to restate the protocol for graph 3-coloring and its proof in [Gol01, Section 4.4]. A concrete statistically binding scheme with security against quantum attacks can be obtained by combining the works of [2], [11] which respectively present an efficient pseudo-random generator with security against quantum attacks and a way to construct statistically binding bit-commitment from any pseudo-random generator.

However, to our best knowledge, there doesn't exist a perfectly binding commitment scheme that is known to be secure against quantum attacks. The main difficulties are, first, it's impossible to build such schemes from quantum information alone [8], [9], and so a basis of computational hardness assumptions is necessary. Second, the computational hardness assumptions of factoring integers and finding discrete logarithms don't hold in the quantum setting because of Shor's beautiful work [13]. Third, though such schemes can be built from any quantum one-way permutation [1], no the one-way permutation is known. Therefore, other approach is needed.

1.1 Our Contribution

In this paper, based on the hardness assumption of lattice problem learning with errors (LWE), we present a perfectly binding commitment scheme. Since the hardness of LWE is implied by the worst-case hardness of any one of standard lattice problems SIVP and GapSVP [12] which are generally believed to resist quantum attacks [10], our scheme is the first perfectly binding commitment known to be secure against quantum attacks. As an independent contribution, we proves that a folklore that there is

This work is supported by China Postdoctoral Science Foundation (No. 20100480900).

The authors are with the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan City, Hubei 430074 China (e-mail: zeng.bing@smail.hust.edu.cn, chenliang100@smail.hust.edu.cn, tang.xueming.txm@gmail.com).

no commitment scheme that is both information-theoretically binding and information-theoretically hiding is true.

Our scheme makes use of Regev's LWE-based public-key cryptosystem [12] or its variant presented by [3]. The main idea is that, turning to ciphertext-indistinguishability of the cryptosystems, we gain property computational hiding against quantum attacks for our schemes; turning to an efficient deterministic algorithm that can be used to verify that a given legal public key indeed corresponds to a unique private key [3], we gain property perfectly binding.

1.2 Organization

This paper is organized as follows. In Section 2, we describe the notations used in this paper, briefly introduce the notions of various types of commitments, and clarify their names. In Section 3, we prove the folklore mentioned previously is true. In Section 4, we construct a perfectly binding commitment scheme.

2 PRELIMINARIES

2.1 Basic Notations

We denote an unspecified positive polynomial by $poly(.)$; denote the set consists of all natural numbers and the set consists of all prime numbers by $\mathbb{N}$ and $\mathbb{P}$ respectively; denote security parameter used to measure security and complexity by k.

A function $\mu(.)$ is negligible in k, if there exists a positive constant integer n_0, for any $poly(.)$ and any k which is greater than n_0, it holds that $\mu(k) < 1/poly(k)$. A probability ensemble $X \stackrel{def}{=} \{X(1^k, a)\}_{k\in\mathbb{N}, a\in\{0,1\}^*}$ is an infinite sequence of random variables indexed by (k, a), where a represents various types of inputs used to sample the instances according to the distribution of the random variable $X(1^k, a)$.

Let $X \stackrel{def}{=} \{X(1^k, a)\}_{k\in\mathbb{N}, a\in\{0,1\}^*}$ and $Y \stackrel{def}{=} \{Y(1^k, a)\}_{k\in\mathbb{N}, a\in\{0,1\}^*}$ be two probability ensembles. They are said to be computationally indistinguishable, denoted $X \stackrel{c}{=} Y$, if for any non-uniform probabilistic polynomial-time (PPT) algorithm D with an infinite auxiliary information sequence $z = (z_k)_{k\in\mathbb{N}}$ (where each $z_k \in \{0,1\}^*$), there exists a negligible function $\mu(.)$ such that for any sufficiently large k, any a, it holds that

$$|Pr(D(1^k, X(1^k, a), a, z_k) = 1) - Pr(D(1^k, Y(1^k, a), a, z_k) = 1)| \leqslant \mu(k)$$

They are said to be equal, denoted $X \equiv Y$, if for any sufficiently large k, any a, the distributions of $X(1^k, a)$ and $Y(1^k, a)$ are identical. Obviously, if $X \equiv Y$ then $X \stackrel{c}{=} Y$.

2.2 Commitment Scheme

For historical reasons, there are no standard names for various types of commitment schemes. Even the same author would give the same name to two different type commitment schemes in different literature, let alone different authors refer to the same type commitment scheme using different names. For example, Goldreich names both the commitment scheme with perfectly hiding property in [4, Page 279] and the commitment scheme with statistically hiding property in [6, Page 175] perfectly hiding commitment.

To eliminate those confusions, it's necessary to clarify names for various types of commitment schemes. We start by defining the perfectly binding commitment scheme. To our end, a non-strict version suffices. For the strict definition and the details, please see [4], [6], [14].

Definition 1 (perfectly binding commitment scheme, non-strict description)**.** *A commitment scheme is a two-party protocol involving two phases.*

- *Initial Inputs. At the beginning, all parties know the public security parameter k. The unbounded sender P_1 holds a randomness $r_1 \in \{0,1\}^*$, a value $m \in \{0,1\}^{poly(k)}$ to be committed to, where the polynomial $poly(.)$ is public. The PPT receiver P_2 holds a randomness $r_2 \in \{0,1\}^*$.*
- *Commit Phase. P_1 computes a commitment, denoted α, based on his knowledge, i.e., $\alpha \leftarrow P_1(1^k, m, r_1)$, then P_1 send α to P_2.*
  - *The security for P_1 is implied by the property computationally hiding, which prevents P_2 from the knowledge of the value committed by P_1. That is, for any PPT P_2, any $m_1, m_2 \in \{0,1\}^{poly(k)}$, it holds that*

$$\{ViewC_{P_2}(< P_1(m_1), P_2 > (1^k))\}_{k\in\mathbb{N}} \stackrel{c}{=} \{ViewC_{P_2}(< P_1(m_2), P_2 > (1^k))\}_{k\in\mathbb{N}}, \quad (1)$$

  where $ViewC_{P_2}(.)$ denotes P_2's view in the commit phase.
- *Reveal Phase. P_1 computes and sends a de-commitment, which typically consists of m, r_1, to P_2 to let P_2 know m. Receiving de-commitment, P_2 checks its validity. Typically P_2 checks that*

$\alpha = P_1(1^k, m, r_1)$ *holds. If de-commitment pass the check,* P_2 *knows and accepts* m.

- *The security for* P_2 *is implied by the property perfectly binding, which guarantees that for any unbounded* P_1*, any* $m_1, m_2 \in \{0,1\}^{poly(k)}$ *such that* $m_1 \neq m_2$*, the probability that* P_2 *accepts* m_2 *while* P_1 *commits to* m_1 *is* 0*, where the probability is taken only over the randomness used by* P_2.

If the probability regarding the binding in Definition 1 is relaxed to be negligibly small, the resulting scheme is said to be statistically binding. In the setting that P_1 is PPT and P_2 is unbounded, if the distributions of P_2's views in the commit phase of distinct executions are statistically indistinguishable (see [4] for the meaning of statistical indistinguishability), the scheme is said to be statistically hiding; if the distributions of P_2's views in the commit phase of distinct executions are identical, the scheme is said to be perfectly hiding.

If a property is secure against unbounded adversaries, the property is said to be information-theoretically/unconditionally secure. It's easy to see that perfect or statistical properties are information-theoretically secure. We will show in Section 3 that there is no commitment scheme that is both information-theoretically binding and information-theoretically hiding. Thus, there is no need to explicitly refer to computationally secure properties in their names for schemes holding a information-theoretically secure property. We remark that computationally hiding and computationally binding commitment schemes also exist.

3 An Impossibility Result On Commitment Scheme

There is a folklore that there is no commitment scheme that is both information-theoretically binding and information-theoretically hiding. However, we are not aware of any related full proof having appeared before and so prove here that this folklore indeed holds.

Theorem 2. *There is no commitment scheme that is both information-theoretically binding and information-theoretically hiding.*

Proof: We begin by proving that there is no commitment scheme that is both perfectly binding and perfectly hiding. Assume $\mathcal{H}$ is a perfectly hiding commitment scheme, then for any two distinct values m_1 and m_2 of the same length l, we have

$$\{ViewC_{P_2}(< P_1(m_1), P_2 > (1^k))\}_{k\in\mathbb{N}} \equiv \{ViewC_{P_2}(< P_1(m_2), P_2 > (1^k))\}_{k\in\mathbb{N}}.$$

Because there exists 2^l values of length l, for any transcript viewed by P_2 in the commit phase, there exists 2^l legal interpretations. Thus, perfectly binding is impossible.

Regarding the case of statistically binding and statistically hiding, the case of statistically binding and perfectly hiding, and the case of perfectly binding and statistically hiding, the proof is similar and so we omit it. □

4 Constructing A Perfectly Binding Commitment Scheme

In this section, we construct a lattice-based perfectly binding commitment scheme, which is built from the results of [3], [12]. Since lattice-based cryptography is generally believed to resist quantum attacks [10], our scheme meets Watrous's need in [14].

4.1 Background

In lattice, the modulo operation is defined as $x \bmod y \stackrel{def}{=} x - \llcorner x/y \lrcorner y$. Let α be an arbitrary positive real number. Let Ψ_α be a probability density function whose distribution is over $[0,1)$ and obtained by sampling from a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$ and reducing the result modulo 1, more specifically

$$\Psi_\alpha : [0,1) \to R^+,$$
$$\Psi_\alpha(r) \stackrel{def}{=} \sum_{k=-\infty}^{\infty} \frac{1}{\alpha} \exp(-\pi(\frac{r-k}{\alpha})^2).$$

Given an arbitrary integer $q \geq 2$, an arbitrary probability destiny function $\phi : [0,1) \to R^+$, the discretization of ϕ over Z_q is defined as

$$\bar{\phi} : Z_q \to R^+,$$
$$\bar{\phi}(i) \stackrel{def}{=} \int_{(i-1/2)/q}^{(i+1/2)/q} \phi(x)dx.$$

The problem learning with errors can be formulated as follows.

Definition 3 (learning with errors)**.** *Let* $q \in \mathbb{P}$*,* $\alpha = \alpha(k) \in (0,1)$ *such that* $\alpha q > 2\sqrt{k}$*. Learning with errors* ($LWE_{q,\bar{\Psi}_\alpha}$) *is a problem that given* $(q, m, \bar{\Psi}_\alpha, (\vec{a}_i, b_i)_{i\in[m]})$*, finds* $\vec{s}$ *with non-negligible*

probability, where the input and the output is specified in the following way.

- $m \leftarrow poly(1^k)$, $\vec{s} \in_U (Z_q)^k$. *For each* $i \in \{1, 2, \ldots, m\}$, $\vec{a}_i \in_U (Z_q)^k$, $e_i \in_{\bar{\Psi}_\alpha} Z_q$, $b_i \leftarrow \vec{s}^T \cdot \vec{a}_i + e_i \mod q$.

$LWE_{q,\bar{\Psi}_\alpha}$ is an average-case problem, however, [12] shows that its hardness is implied by the worst-case hardness of any one of standard lattice problems SIVP and GapSVP for quantum algorithms. In other words, any algorithm breaking $LWE_{q,\bar{\Psi}_\alpha}$ also is a algorithm breaking both SIVP and GapSVP which are hard at present even for quantum algorithms.

The perfectly binding commitment scheme, which we will present soon, needs to use a $LWE_{q,\bar{\Psi}_\alpha}$-based public key cryptosystem presented by [3], which is a slight variant of [12]'s cryptosystem. This cryptosystem is described as follows.

- Message space: $\{0, 1\}$.
- $Setup(1^k)$: $q \leftarrow q(1^k) \wedge q \in \mathbb{P} \wedge q \in [k^2, 2k^2]$, $m \leftarrow (1+\varepsilon)(k+1)\log q$ (where $\varepsilon > 0$ is an arbitrary constant), $\bar{\Psi}_\alpha \leftarrow \bar{\Psi}_{\alpha(k)} \wedge \alpha(k) = o(1/(\sqrt{k}\log k))$ (e.g., $\alpha(k) = \frac{1}{\sqrt{k}(\log k)^2}$). $para \leftarrow (q, m, \bar{\Psi}_\alpha)$, finally outputs $para$.
- $KeyGen(1^k, para)$: $A \in_U (Z_q)^{m\times k}$, $\vec{s} \in_U (Z_q)^k$, $\vec{e} \in_{\bar{\Psi}_\alpha} (Z_q)^m$ (which means each entry of $\vec{e}$ is independently drawn from Z_q according to $\bar{\Psi}_\alpha$), $\vec{b} \leftarrow A\vec{s} + \vec{e} \mod q$, $pk \leftarrow (A, \vec{b})$, $sk \leftarrow \vec{s}$, finally outputs a public-private key pair (pk, sk).
- $Enc(.)$, $Dec(.)$: Since $Enc(.)$, $Dec(.)$ are immaterial to understand this paper, we omit their detailed procedure here.

[3, Section 8] shows that the cryptosystem holds the following properties.

Lemma 4 ([3]). *If $LWE_{q,\bar{\Psi}_\alpha}$ is hard, choosing appropriate parameters, the public-key cryptosystem provides semantical security against chosen plaintext attacks.*

Lemma 5 (summary of Proposition 8.8 and Lemma 8.9 in [3]). *For the $LWE_{q,\bar{\Psi}_\alpha}$-based cryptosystem mentioned early, there exists an efficient* deterministic *algorithm such that, for all but at most negligible fraction of public key generated by $KeyGen$, given a trapdoor for the matrix A and a public key $(A, A^T\vec{s}+\vec{e})$, it can efficiently extract the unique private key $\vec{s}$. For the implementation of the algorithm, please see [3].*

4.2 A Perfectly Binding Commitment Scheme

The commitment scheme is described as follows.

Construction 6 (a perfectly binding commitment)**.**

- *Common inputs: All entities know the public security parameter k, the length of values $l = poly(k)$, and the public-key cryptosystem mentioned previously.*
- *Private inputs: The unbounded sender P_1 holds a randomness $r_1 \in \{0,1\}^*$, a value $m \in \{0,1\}^l$ to be committed to. The PPT receiver P_2 holds a randomness $r_2 \in \{0,1\}^*$.*
- *The protocol proceeds as follows.*
  1) *Commit phase.*
     a) *P_1: $para \leftarrow Setup(1^k)$; chooses a public-private key pair $((A, \vec{b}), \vec{s}) \leftarrow KeyGen(1^k, para)$ along with a trapdoor T of the matrix A; checks that $\vec{s}$ is extractable by using the extraction algorithm guaranteed by Lemma 5. If not, P_1 repeats choosing until a extractable public-private key pair is gained. Then, P_1 takes this public-private pair.*
     Note that following Lemma 5, the fraction of legal key pairs that are not extractable is negligible, so P_1 can efficiently find a extractable key pair.
     b) *Let m^i denote the i-th bit of m. Let $E_{A,\vec{b}}(m)$ denote*

$$(E_{A,\vec{b}}(m^1), E_{A,\vec{b}}(m^2), \ldots, E_{A,\vec{b}}(m^l)).$$

     P_1 sends the commitment $(para, (A, \vec{b}), E_{A,\vec{b}}(m))$ to P_2.
  2) *Reveal phase.*
     a) *P_1 sends the committed value m, the randomness r_1 used in commit phase, and the trapdoor T of the matrix A to P_2.*
     b) *P_2 checks that the commitment $(para, (A, \vec{b}), E_{A,\vec{b}}(m))$ is legally generated by using r_1, that the private key is extractable, and that the extracted private key $\widetilde{\vec{s}}$ is equivalent to the private key $\vec{s}$ generated by using r_1. P_2 accepts value m if and only if all checks pass.*

Theorem 7. *Assuming $LWE_{q,\bar{\Psi}_\alpha}$ is hard, the commitment scheme described in Construction 6 is computationally hiding and perfectly binding.*

Proof: First, we claim that the commitment scheme is computationally hiding in the case that P_1 is honest and P_2 is malicious.

Without loss of generality, for any two values m_1, m_2, for the corresponding executions $<$

$P_1(m_1), P_2 > (1^k)$ and $< P_1(m_2), P_2 > (1^k)$, let

$$ViewC_{P_2}(< P_1(m_i), P_2 > (1^k)) = (para_i, (A_i, \vec{b}_i), E_{A_i,\vec{b}_i}(m_i)),$$

where $i = 1, 2$. It's easy to see that the distribution of $(para_1, (A_1, \vec{b}_1))$ and that of $(para_2, (A_2, \vec{b}_2))$ are identical. It's known that if a public-key cryptosystem is semantically secure under chosen plaintext attack, then it is ciphertext-indistinguishable for multiple messages under chosen plaintext attack (see [5, Section 5.4.3]). Thus following Lemma 4, the distribution of $E_{A_1,\vec{b}_1}(m_1)$ and that of $E_{A_2,\vec{b}_2}(m_2)$ are computationally indistinguishable. Getting all together, our first claim holds, i.e., the commitment scheme satisfies Equation (1).

Second, we claim that the commitment scheme is perfectly binding in the case that P_1 is malicious and P_2 is honest.

Note that the extraction algorithm guaranteed by Lemma 5 is deterministic. This implies that for a given legal public key, whether the algorithm can extract its private key only depends the public key itself. Construction 6 uses the extraction algorithm as a filter to screen out the public keys whose private keys aren't extractable. For any resulting legitimate public key, the corresponding private key is extractable and unique. Thus, the value committed by an encryption relative to such legitimate public keys is perfectly binding. Further, our second claim holds. □

4.3 Extension

For simplicity in presentation in Construction 6, we takes [3]'s cryptosystem, however, the cryptosystem of original version, i.e., [12]'s cryptosystem, is also appropriate. The only difference between two cryptosystems is their encryption algorithm. Observe that the original cryptosystem is ciphertext-indistinguishable. For a public-key cryptosystem, this also implies that it is ciphertext-indistinguishable for multiple messages (see [5, Section 5.2.2]), which suffices to hold property computationally hiding as a commitment scheme in our construction. What's more, Lemma 4 also applies to the original cryptosystem, as it depends only on the distribution of public keys, and not on the distribution of the randomness used in encryption. Thus taking the original cryptosystem doesn't influence the binding of the constructions.

ACKNOWLEDGMENT

We would like to thank Anderson C A Nascimento for pointing out errors in a previous version.

REFERENCES

[1] Mark Adcock and Richard Cleve. *A Quantum Goldreich-Levin Theorem with Cryptographic Applications*, volume 2285 of *Lecture Notes in Computer Science*, pages 729–729. Springer Berlin / Heidelberg, 2002.

[2] J.B. Fischer and J. Stern. An efficient pseudo-random generator provably as secure as syndrome decoding. In *Advances in CryptologyłEUROCRYPT96*, pages 245–255. Springer, 1996.

[3] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Stoc'08: Proceedings of the 2008 Acm International Symposium on Theory of Computing*, pages 197–206 798, 2008. the full paper is available on http://eprint.iacr.org/2007/432.

[4] O. Goldreich. *Foundations of cryptography, volume 1*. Cambridge university press, 2001.

[5] O. Goldreich. *Foundations of cryptography, volume 2*. Cambridge university press, 2004.

[6] O. Goldreich and A. Kahan. How to construct constant-round zero-knowledge proof systems for NP. *Journal of Cryptology*, 9(3):167–189, 1996.

[7] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *Journal of the ACM (JACM)*, 38(3):690–728, 1991.

[8] H.K. Lo and H.F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997.

[9] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414–3417, 1997.

[10] Daniele Micciancio and Oded Regev. *Lattice-based Cryptography*, pages 147–191. Springer Berlin Heidelberg, 2009.

[11] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991.

[12] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

[13] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[14] J. Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.