Post-quantum Efficient Proof for Graph 3-Coloring Problem

Ehsan Ebrahimi

FSTM & SnT, University of Luxembourg

April 14, 2022

Abstract. In this paper, we construct an efficient interactive proof system for the graph 3-coloring problem and shows that it is computationally zero-knowledge against a quantum malicious verifier. Our protocol is inline with the sketch of an efficient protocol by Brassard and Crepéau (FOCS 1986) that later has been elaborated by Kilian (STOC 1992). Their protocol is not post-quantum secure since its soundness property holds based on the intractability of the factoring problem. Putting aside the post-quantum security, we argue that Kilian's interactive protocol for the graph 3-coloring problem does not fulfill the soundness property even in the classical setting.[1]
In addition, we propose an XOR-homomorphic commitment scheme based on the Learning Parity with Noise (LPN) problem and shows that it fulfills quantum computationally hiding and perfect binding properties.

Keywords. Efficient Interactive Proof System, Post-quantum Security, Computational Zero-knowledge

1 Introduction

An interactive proof system [20] is a two-party protocol for an unbounded classical prover[2] and a classical verifier with the goal of convincing the verifier that a certain statement is true. To be more rigorous, the statement is treated as an instance of a Language $\mathcal{L}$ and the prover wants to convince the verifier that the given statement belongs to $\mathcal{L}$ (this means the statement is true). A proof system must fulfil two properties: 1) *Completeness*: if the statement is in $\mathcal{L}$, an honest prover is able to convince the verifier. 2) *Soundness*: if the statement is not in $\mathcal{L}$, no (malicious) prover is able to convince the verifier. The soundness property deals with a malicious prover, in other words, the security of the verifier is a concern in this definition.

The notion of *zero-knowledge* introduced by Goldwasser, Micali and Rackoff [20] deals with a malicious verifier. Informally, we say an interactive proof system is zero-knowledge if a malicious verifier interacting with an honest prover is not able to learn any information beyond the validity of the statement. There has

[1] This can be purely because of the lack of details in [26].

[2] A relaxation of an interactive proof system is an interactive argument system in which the prover is computationally bounded [8].

been extensive research (and success) to construct interactive proof systems with the zero-knowledge property for different computational problems [9, 5, 32, 18, 30, 19, 16].

One computational problem that accepts a zero-knowledge interactive proof system is the graph 3-coloring problem [18]. We say a graph G is 3-colorable if one can color the vertices of G with 3 colors in a way that any two adjacent vertices receive two different colors. In a nutshell, the Goldwasser-Micali-Rackoff proof system [18] works as follows. The prover on inputs of a graph G and a 3-coloring χ, commits to a permuted 3-coloring of χ using a commitment scheme, and sends the commitments to the verifier. The verifier sends a random edge to challenge the prover. The prover opens the colors of the vertices of this edge and the verifier accepts if these colors are different. The drawback of this protocol is that it is not efficient as it is explained in the coming lines. In this protocol a malicious prover (on the input of a graph G that is not 3-colorable) can convince the verifier with a probability at most $1 - 1/|E|$ where $|E|$ is the number of the edges of G. To make this probability negligible, the protocol has to be repeated many times sequentially and in each execution the prover has to send fresh commitments otherwise the opening in the last phase of the protocol reveals information about χ and it renders the protocol not-zero-knowledge.

A sketch of an efficient zero-knowledge protocol for the graph 3-coloring problem has been given by Brassard and Crepéau [9]. Later Kilian [26] presented an efficient zero-knowledge proof system for the graph 3-coloring problem. The protocol is based on the implementation of "notarized envelops" using "ideal bit commitment" and"pair-blobs". Since the formal definitions of these primitives are not given in the reference available [26] (this reference is an extended abstract), we present the informal definitions of them from the reference. A "pair-blob" is a representation of a bit b by a random XOR of two bits, that is, $b = b_0 \oplus b_1$ for random bits b_0, b_1. And the prover instead of committing to b, it commits to b_0 and b_1 using an ideal bit commitment scheme. It has been stated that a notarized envelop can be constructed using an ideal bit commitment scheme and pair-blobs [9, 26]. Notarized envelops allow a prover to commit to some set of bits and to later prove that some predicate holds on those bits without revealing any information about the bits.

Kilian's protocol [26]. In a nutshell, the prover commits to a coloring χ for a graph G using pair-blobs. When the verifier challenges the prover by sending a random vertex (v_i, v_j) from G, the prover proves that $\chi(v_i) \neq \chi(v_j)$ without revealing any information about $\chi(v_i)$ and $\chi(v_j)$.

1.1 Motivation

Here, we give some motivations to revisit the efficient zero-knowledge protocol for the graph 3-coloring problem proposed in [9, 26]. We explain why the soundness property of Kilian's protocol [26] does not hold [3]. And why the sketch of the efficient protocol by Brassard and Crepéau [9] is not post-quantum secure.

[3] Note that we do not dismiss Kilian's result regarding hash-based argument systems. We only discuss Kilian's proof system for graph 3-coloring problem in this paper.

Why is Kilian's protocol [26] not sound? Regrettably, a full version of [26] is not available and some of the details of the proof is unclear. For instance, to show the soundness property of this protocol, Kilian argues that:

> "if G is not 3-colorable, then no matter what coloring a prover $\hat{\mathcal{P}}$ commits to, the verifier $\mathcal{V}$ will choose a bad edge with probability at least $1/m$ (where m is the number of edges). In this case, no matter what strategy $\mathcal{P}$ uses, $\mathcal{V}$ will reject with some nonconstant probability."

We explain why this reasoning is not sufficient. Note that in Kilian's protocol, the prover doesn't reveal any information beyond $\chi(v_i) \neq \chi(v_j)$ and a graph G that is not 3-colorable can be colored using more colors. So a malicious prover can use pair-blobs to commit to a coloring χ' for G that uses more than 3 colors, and for any edge (v_i, v_j), $\chi'(v_i) \neq \chi'(v_j)$. Later the malicious prover can pass the verifier's challenge with the probability 1. Note that this issue will not arise in the the Goldwasser-Micali-Rackoff zero-knowledge proof system for the graph 3-coloring problem [18] because in their protocol the prover has to reveal $\pi(\chi'(v_i))$ and $\pi(\chi'(v_j))$ where π is a random permutation on three allowed colors. So with some probability the verifier can detect when a malicious prover uses an extra color. But in Kilian's protocol the prover does not reveal any information about $\chi'(v_i)$ and $\chi'(v_j)$ beside the fact that they are not equal. This issue has not been addressed in [26] and it is not clear if Kilian's protocol (see Section 3.1 in [26]) has the soundness property or not.

Why is the Brassard-Crepéau protocol [9] not post-quantum secure? Beside the issue sketched above, the efficient protocol for the graph 3-coloring problem presented in [9] is not post-quantum secure since its soundness is based on the difficulty of the factoring problem. In more details, in the protocols of [9] the verifier chooses two distinct large primes p and q, and sends their product $N = pq$ to the prover along with a randomly chosen quadratic residue modulo N, lets call it y.[4] To commit to a bit b, the prover chooses a random $w \in \mathbb{Z}_N^*$ and sends $z = w^2 y^b$ to the verifier with the opening information (b, w). The soundness property (against a malicious polynomial-time prover[5]) of the protocols relies on the binding property of this commitment. But a malicious quantum prover can send $z = w^2 y$ as a commitment to its input, factor N to p and q using the Shor's algorithm [31], compute the square root of y and later open z to both 0 or 1 by sending $w\sqrt{y}$ or w respectively.

Why do we care? Given the rapid progress on quantum computing and the existence of efficient quantum algorithms to solve some computational problems like factoring and discrete logarithm [31], it is necessary to investigate the security of cryptographic constructions against a quantum adversary. The post-quantum security of the Goldwasser-Micali-Rackoff proof system for the graph 3-coloring problem has been studied by Watrous [35]. Watrous showed that this protocol is quantum computationally zero-knowledge under the assumption of the existence of *unconditionally binding* and *quantum computationally hiding*

[4] y is a quadratic residue modulo N if there exists x such that $x^2 \equiv y \pmod N$.
[5] In other words, the protocols in [9] are argument systems.

commitment schemes. Assuming the existence of this primitive, the main challenge in the proof is the inability of using the classical `rewinding` argument to construct the simulator for a malicious quantum verifier. Watrous developed a `quantum rewinding` technique to overcome this challenge[6]. However, the post-quantum security of efficient protocols for the graph 3-coloring problem will not follow solely by the Watrous's rewinding technique since the techniques to make the proof succinct may not be post-quantum secure (as briefed for the Brassard-Crepéau protocol [9] above.)

1.2 Our Contribution

In this paper, we propose the first LPN-based XOR-homomorphic commitment scheme where its security holds in the post-quantum setting under LPN quantum-hard assumptions. This commitment scheme will definitely have applications in other research, specifically, with the current interest to transmit to the post-quantum era among the community. Following an idiom, "do not putt all your eggs in one basket", studying cryptographic primitives based on different quantum-hard assumptions seems a necessity.

In addition, we construct an efficient zero-knowledge interactive proof system for the graph 3-coloring problem and show that it is quantum computationally zero-knowledge. Our protocol is a modification of Kilian's protocol with a post-quantum implementation.

How to fix the soundness issue of Kilian's protocol. As explained above, Kilian's protocol does not fulfill the soundness property. In our protocol, we allow the prover to reveal extra information about the colors of an edge beyond their inequality. Namely, for an edge (v_i, v_j), the prover proves that $\chi(v_i)$ and $\chi(v_j)$ are valid colors in addition to $\chi(v_i) \neq \chi(v_j)$. Our proof does not reveal any further information about $\chi(v_i)$ and $\chi(v_j)$ to fulfill the zero-knowledge property. Even though our correction is straightforward in theory, its implementation is not trivial. Actually, our correction is a topic that has attracted intensive attention in the literature. In more details, let S be the set of valid colors, the prover needs to prove that an element belongs to the set S without revealing its identity. This problem can be solved by constructing a zero-knowledge protocol for set-membership problem [10, 1, 2]. We emphasize that our solution for this problem is independent from the existing solutions. In the following, we explain how this is done in our paper.

Post-quantum security. Under the assumption of the existence of an XOR-homomorphic bit commitment scheme which its randomness is distributed uniformly at random and fulfills quantum computational hiding and perfect binding properties, we present a protocol to prove the inequality of two committed values without revealing any further information about the values. This protocol helps to prove the $\chi(v_i) \neq \chi(v_j)$ inequality in our efficient proof system for the

[6] Other quantum rewinding techniques are available for the *proof of knowledge* property of an interactive protocol [34, 12].

graph 3-coloring problem without revealing any information beyond the inequality. In addition, to prove that $\chi(v_i)$ and $\chi(v_j)$ are valid colors, we assume that $\{01, 10, 11\}$ is the set of the valid colors and the prover uses a modification of the inequality protocol to prove $\chi(v_i) \neq 00$ and $\chi(v_j) \neq 00$.

We propose a bit commitment scheme based on the LPN problem, a special case of the Learning With Errors (LWE) assumption [29], that is homomorphic under XOR operation. Our commitment scheme is perfectly binding and quantum computationally hiding (under the quantum-hardness assumption of the LPN problem). We show that our commitment scheme preserves its properties (correctness, hiding and binding) under constant number of XOR-operations. Our scheme is a modification of the commitment scheme by Jain et al. [23]. Their scheme does not preserve the correctness property under homomorphic operations (details in Appendix A). Regrettably, we are not able to use our commitment scheme in the 3-coloring protocol since it uses an error vector with low Hamming weight as a randomness when generating a commitment value (see discussion in Section 4).

1.3 Organization

The Section 2 is dedicated to notations, preliminary backgrounds and definitions needed in this paper. We construct an XOR-homomorphic commitment scheme that is perfectly binding and quantum computationally hiding in Section 3. The underlying computational assumption to show the hiding property is the LPN problem. In Section 4, we construct a post-quantum computationally zero-knowledge interactive proof system for proving the inequality of two inputs using a perfectly binding and quantum computationally hiding XOR-homomorphic commitment scheme. In Section 5, we construct an efficient proof system for the graph 3-coloring problem using the inequality protocol in Section 4. We show our protocol is computationally zero-knowledge against a quantum malicious verifier. And finally, we briefly explain how our technique can be used to construct a post-quantum efficient zero-knowledge proof system for SAT problem in Appendix B.

2 Preliminaries

Notations. The notation $x \xleftarrow{\$} X$ means that x is chosen uniformly at random from the set X. For a natural number n, $[n]$ means the set $\{1, \cdots, n\}$. The closest integer to k is shown with $\lfloor k \rceil$. The lower-case and upper-case letters like $\mathbf{a}, \mathbf{A}$ are used to denote vectors and matrices, respectively. $\mathbf{A}^\intercal$ denotes the transpose of the matrix $\mathbf{A}$. For a binary vector $\mathbf{a}$, the notation $\omega(\mathbf{a})$ indicates the number of 1s in $\mathbf{a}$ (that is the Hamming weight of $\mathbf{a}$). For two values e and e', $[e = e']$ is 1 if $e = e'$ and it is 0 otherwise. For two strings x_1, x_2, their bitwise XOR is denoted by $x_1 \oplus x_2$. $\Pr[P : G]$ is the probability that the predicate P holds true where free variables in P are assigned according to the program in G. The function $\mathtt{negl}(n)$ is any non-negative function that is smaller than the inverse of any non-negative polynomial $p(n)$ for sufficiently large n. That is, $\lim_{n\to\infty} \mathtt{negl}(n)p(n) = 0$ for any polynomial $p(n)$. Assuming n is the security parameter, by an overwhelming probability we mean $1-\mathtt{negl}(n)$ probability.

Quantum Computing. We present basics of the quantum computing in this subsection. The interested reader can refer to [28] for more information. For two vectors $|\Psi\rangle = (\psi_1, \psi_2, \cdots, \psi_n)$ and $|\Phi\rangle = (\phi_1, \phi_2, \cdots, \phi_n)$ in $\mathbb{C}^n$, the inner product is defined as $\langle \Psi, \Phi\rangle = \sum_i \psi_i^* \phi_i$ where ψ_i^* is the complex conjugate of ψ_i. Norm of $|\Phi\rangle$ is defined as $\| \, |\Phi\rangle \, \| = \sqrt{\langle \Phi, \Phi\rangle}$. The n-dimensional Hilbert space $\mathcal{H}$ is the complex vector space $\mathbb{C}^n$ with the inner product defined above. A quantum system is a Hilbert space $\mathcal{H}$ and a quantum state $|\psi\rangle$ is a vector $|\psi\rangle$ in $\mathcal{H}$ with norm 1. An unitary operation over $\mathcal{H}$ is a transformation $\mathbb{U}$ such that $\mathbb{U}\mathbb{U}^\dagger = \mathbb{U}^\dagger\mathbb{U} = \mathbb{I}$ where $\mathbb{U}^\dagger$ is the Hermitian transpose of $\mathbb{U}$ and $\mathbb{I}$ is the identity operator over $\mathcal{H}$. An orthogonal projection $\mathbb{P}$ over $\mathcal{H}$ is a linear transformation such that $\mathbb{P}^2 = \mathbb{P} = \mathbb{P}^\dagger$. A measurement on a Hilbert space is defined with a family of orthogonal projectors that are pairwise orthogonal. An example of measurement is the computational basis measurement in which any projection is defined by a basis vector. The computational basis for $\mathbb{C}^{2^n}$ consists of 2^n vectors $|x\rangle$ where x is a bit-string of length n ($x \in \{0,1\}^n$). The output of computational measurement on a state $|\Psi\rangle$ is x with probability $\|\langle x, \Psi\rangle\|^2$ and the post-measurement state is $|x\rangle$.

For two parties $\mathcal{P}$ and $\mathcal{V}$, the notation $\langle \mathcal{P}, \mathcal{V}\rangle$ denotes the output of an interaction between $\mathcal{P}$ and $\mathcal{V}$.

Definition 1 (Interactive Proof System [20]). *An interactive proof system for a language $\mathcal{L}$ with the soundness error ϵ is a two party protocol between an unbounded prover $\mathcal{P}$ and a polynomial-time verifier $\mathcal{V}$ that fulfills the following two properties:*

1. *Completeness. For any $x \in \mathcal{L}$,* $\Pr[\langle \mathcal{P}(x), \mathcal{V}(x)\rangle = 1] = 1$.
2. *Soundness. For any malicious prover $\mathcal{P}^*$ and $x \notin \mathcal{L}$,*

$$\Pr[\langle \mathcal{P}^*(x), \mathcal{V}(x)\rangle = 1] \leq \epsilon.$$

Informally, an interactive protocol is zero-knowledge if the verfier can perform the protocol without the prover. This is formalized by the existence of a simulator that knows the code of the malicious verifer and can produce a transcript indistinguishable from the transcript of a real execution of the protocol. In the definition below, we define the computational zero-knowledge property against a malicious quantum verifier. It is a modification of the Watrous's quantum computational zero-knowledge definition [35, 33]. In the Watrous's definition, a malicious quantum verifier, after receiving some classical states (the commitments) from the prover and doing some quantum computations on this classical states and some auxiliary quantum registers, (is able to) sends a quantum state to the prover as an output. The classical prover will measure this quantum state in the computational basis measurement to obtain the final output. Then, the definition is stated as "polynomially quantum indistinguishability" of "admissible super-operators" induced by such interactions. Here, we define a slightly different definition in which a malicious quantum verifier does the final measurement and only sends classical information to the prover. In other words, we assume that the transcripts of the executions of the protocol are classical as it projects the post-quantum setting. So even though $\mathcal{V}^*$ and consequently $\mathcal{S}$ are quantum, the output of the simulator as the transcript of its interaction with $\mathcal{V}^*$ is required to be classical. Then, we require that the indistinguishablity of two transcripts holds against any quantum polynomial-time distinguisher given access to the auxiliary quantum register used by the verifier. (Note that our definition below is similar to Unruh's definition, Definition 15 in [33], with a difference that the final transcript of the interaction of $\mathcal{V}^*$ and $\mathcal{P}$ is classical, that is, the ancillary register Z is measured at the end of the interaction.)

Definition 2 (Post-quantum Computational Zero-knowledge). *Let η be the security parameter and* $\texttt{Pol}$ *is a polynomial function. Let Z, E be auxiliary quantum registers of at most $\texttt{Pol}(\eta)$ size. An interactive proof system is quantum computationally zero-knowledge if there exists a quantum polynomial-time simulator $\mathcal{S}$ such that for any polynomial-time quantum verifier $\mathcal{V}^*$, for any $x \in \mathcal{L}$ with $|x| \leq \texttt{Pol}(\eta)$, any quantum state $|\psi\rangle$ stores in Z, E, the transcript of the interaction $\langle \mathcal{P}(x), \mathcal{V}^*(x, Z)\rangle$ is computationally indistinguishable from the transcript of the interaction $\langle \mathcal{S}(x, Z), \mathcal{V}^*(x, Z)\rangle$. That is for any $x \in \mathcal{L}$, any quantum state $|\psi\rangle$ stores in Z, E, any quantum polynomial-time distinguisher $\mathcal{D}$,*

$$\begin{aligned}|\Pr[\mathcal{D}(\mathbf{H}_0, E) = 1 : \mathbf{H}_0 \leftarrow \langle \mathcal{P}(x), \mathcal{V}^*(x, Z)\rangle]\\ - \Pr[\mathcal{D}(\mathbf{H}_1, E) = 1 : \mathbf{H}_1 \leftarrow \langle \mathcal{S}(x, Z), \mathcal{V}^*(x, Z)\rangle| \leq \texttt{neg}(\eta).\end{aligned}$$

Usually, a simulator $\mathcal{S}$ in the classical zero-knowledge proofs saves the initial state of $\mathcal{V}^*$ and it executes $\mathcal{V}^*$ on this state several times until $\mathcal{V}^*$ returns a "good" output. When the verifier is quantum, this procedure does not work since $\mathcal{S}$ can not save the initial state of $\mathcal{V}^*$ (that is a quantum state) due to the no-cloning theorem. Fortunately, Watrous showed that if the output of $\mathcal{V}^*$ in a single execution (after the final measurement) is a "good" state with a probability close to a constant probability (possibly negligible) independent of the initial state of $\mathcal{V}^*$, there exits a polynomial-size quantum circuit $\mathbb{R}$ whose output is a "good" state with an overwhelming probability for any initial state. (The formal presentation is given in the following lemma.)

We say a quantum state of size $n + k$ qubits is a good (bad) state if the computational basis measurement on its first qubit returns 0 (1) with the probability 1. For an unitary $\mathbb{Q}$ acting on quantum registers of size $n + k$ qubits, we can write $\mathbb{Q}|\psi\rangle|0^k\rangle = \sqrt{p_\psi}|\psi_{good}\rangle + \sqrt{1 - p_\psi}|\psi_{bad}\rangle$ for some unique orthogonal vectors $|\psi_{good}\rangle$ and $|\psi_{bad}\rangle$. Note that p_ψ, $|\psi_{good}\rangle$ and $|\psi_{bad}\rangle$ may depend on the initial state $|\psi\rangle$.

Lemma 1 (Quantum rewinding with small perturbations [35]). *Let $p_0, q \in (0, 1)$ and $\epsilon \in (0, 1/2)$ be real numbers. Let $\mathbb{Q}$ be an (n, k)-quantum circuit such that for all n-qubit states $|\psi\rangle$:*

$$|p_\psi - q| < \epsilon,\ \ p_\psi \geq p_0,\ \ \text{and } p_0(1 - p_0) \leq q(1 - q).$$

Then there exists a general quantum circuit $\mathbb{R}$ *with*

$$size(\mathbb{R}) = O\big(\frac{\log(1/\epsilon)size(\mathbb{U})}{p_0(1-p_0)}\big)$$

such that, for every n-qubit state $|\psi\rangle$*, the output* Φ_ψ *of* $\mathbb{R}$ *satisfies*

$$\langle\psi_{good}|\Phi_\psi|\psi_{good}\rangle \geq 1 - 16\epsilon\frac{\log^2(1/\epsilon)}{p_0^2(1-p_0)^2}.$$

We define a commitment scheme and its security properties in the following.

Definition 3. *A commitment scheme consists of three polynomial (possibly randomized) algorithms* Gen*,* Com *and* Ver *described below with the correctness property.*

- *The key generating algorithm* Gen *takes as input the security parameter* 1^n *and returns a public parameter* pk*.*
- *The commitment algorithm* Com *takes as input* pk *and a message* m*, it chooses a randomness* r *and returns* $(c,d) := \mathrm{Com}(pk,m;r)$ *where* c *is the commitment and* d *is an opening information. (We may omit the randomness and write* $(c,d) \leftarrow \mathrm{Com}(pk,m)$*. Or we may use* Com_{pk} *when* pk *has been determined.)*
- *The verification algorithm* Ver *on inputs* pk*,* (c,d)*, and* m*, returns a bit* b *that indicates the accept (when* $b=1$*) or the reject (when* $b=0$*).*

The scheme fulfills the correctness property, that is, the verification algorithm returns 1 *with the probability* 1 *if* (c,d) *is the output of* Com*:*

$$\Pr[b=1 : pk \leftarrow \mathrm{Gen}(1^n), (c,d) \leftarrow \mathrm{Com}(pk,m), b \leftarrow \mathrm{Ver}(pk,c,d,m)] = 1.$$

A commitment scheme needs to fulfill the hiding and the binding security properties that come in different flavors. In this paper, we define quantum computationally hiding and perfect binding commitment schemes.

Definition 4 (Quantum Computationally Hiding). *We say a commitment scheme* $(\mathrm{Gen}(1^n), \mathrm{Com}, \mathrm{Ver})$ *is quantum computationally hiding if for any* $pk \leftarrow \mathrm{Gen}(1^n)$*, for any two messages* m_1, m_2 *and for any quantum polynomial-time distinguisher* $\mathcal{D}$

$$|\Pr[\mathcal{D}(pk,c_1) = 1 : (c_1,d_1) \leftarrow \mathrm{Com}_{pk}(m_1)] - \Pr[\mathcal{D}(pk,c_2) = 1 : (c_2,d_2) \leftarrow \mathrm{Com}_{pk}(m_2)]| \leq \mathtt{neg}(n).$$

Definition 5 (Perfect Binding). *A commitment scheme* $(\mathrm{Gen}(1^n), \mathrm{Com}, \mathrm{Ver})$ *is perfectly binding if for any commitment* c*, any two messages* m_1, m_2 *and any two openings* d_1, d_2

$$|\Pr[\mathrm{Ver}(pk,c,m_1,d_1) = 1 \wedge \mathrm{Ver}(pk,c,m_2,d_2) = 1 \wedge m_1 \neq m_2 : pk \leftarrow \mathrm{Gen}(1^n)]| \leq \mathtt{neg}(n).$$

3 Commitment From LPN Problem

Let ξ_τ be an error distribution over binary vectors of length k where each element of a vector is chosen independently from the Bernoulli distribution with the parameter τ, that is, $\mathbf{v} = (v_1, \cdots, v_\ell)^\intercal \leftarrow \xi_\tau$ means $\Pr[v_i = 1] = \tau$ for each $i \in [\ell]$. Let $S_{\ell\times k}$ denotes the set of all binary matrix with ℓ rows and k columns.

Definition 6 (Search (τ, ℓ, k)-LPN Problem). *On input* $(\mathbf{A}, \mathbf{A}\mathbf{s} \oplus \mathbf{e})$ *where* $\mathbf{A} \xleftarrow{\$} S_{\ell\times k}$, $\mathbf{s} \xleftarrow{\$} S_{k\times 1}$ *and* $\mathbf{e} \leftarrow \xi_\tau$*, find* $\mathbf{s}$.

Note that an LPN problem is parameterized by (τ, ℓ, k) and we use the (τ, ℓ, k)-LPN problem to make them explicit. The search LPN problem (Definition 6) is conjectured to be quantum-hard with the proper choice of parameters (page 25 of [14])[7] after receiving many attempts to be solved [22, 36, 6, 4].

Definition 7 (Decisional (τ, ℓ, k)-LPN Problem). *The task is to distinguish between* $(\mathbf{A}, \mathbf{A}\mathbf{s} \oplus \mathbf{e})$ *and* $(\mathbf{A}, \mathbf{r})$ *where* $\mathbf{A} \xleftarrow{\$} S_{\ell\times k}$, $\mathbf{s} \xleftarrow{\$} S_{k\times 1}$, $\mathbf{e} \leftarrow \xi_\tau$ *and* $\mathbf{r} \xleftarrow{\$} S_{\ell\times 1}$.

It has been shown that if the search LPN problem is hard, then the decisional LPN problem is hard too [25, 29, 3].

Lemma 2 (Lemma 1 in [25]). *If there exists an algorithm that solves the decisional (τ, ℓ, k)-LPN problem (Definition 7) in time t with the advantage δ, then there exists an algorithm that can solve the search $(\tau, O(\ell\cdot\delta^{-2} \log k), k)$-LPN problem in time $t' = O(t \cdot k\delta^{-2} \log k)$.*

We define our bit commitment scheme in the following based on the LPN problem. We show that it is quantum computationally hiding and perfect binding in Section 3.1. In addition, we show that our scheme preserves its properties with a constant number of XOR-operations.

Scheme 1 (Bit commitment scheme from LPN)**.** *We define a bit commitment scheme based on the LPN problem.*

- *Here* Gen(τ, ℓ, k) *returns a random binary matrix* $\mathbf{A}_{\ell\times(k+1)}$ *and distribution* ξ_τ*. Let set* $\mathbf{A} = \mathbf{A}'_{\ell\times 1}||\mathbf{A}''_{\ell\times k}$.
- *The commitment algorithm* Com *on input* $\mathbf{A}$ *and* $b \in \{0, 1\}$ *chooses an uniformly at random binary vector* $\mathbf{s}$ *of size* k*, draws an error vector* $\mathbf{e}$ *from* ξ_τ *such that* $\omega(\mathbf{e}) < 2\tau\ell$*, and computes* $\mathbf{c} = \mathbf{A}'b \oplus \mathbf{A}''\mathbf{s} \oplus \mathbf{e}$*. The corresponding opening information for* $\mathbf{c}$ *is* $\mathbf{d} = (b, \mathbf{s}, \mathbf{e})$.
- *The verification algorithm* Ver *on inputs* $\mathbf{A}, \tau, \mathbf{c}$ *and* $\mathbf{d} = (b, \mathbf{s}, \mathbf{e})$ *returns* 1 *if* $\mathbf{c} = \mathbf{A}'b \oplus \mathbf{A}''\mathbf{s} \oplus \mathbf{e}$ *and* $\omega(\mathbf{e}) < 2\tau\ell$ *and it returns* 0 *otherwise.*

Obviously, this scheme fulfills the correctness property.

[7] For instance to achieve the quantum security level of 128 bit, $k = 1150$ and $\tau = 1/8$ has been suggested [14].

3.1 Quantum Computationally Hiding & Perfect Binding

We show that the Scheme 1 is quantum computationally hiding using the hardness of the decisional LPN problem (Lemma 2). First, we show that for an error vector $\mathbf{e} \leftarrow \xi_\tau$, with a high probability $\omega(\mathbf{e}) < 2\tau\ell$. Then, the quantum computationally hiding property is following directly by the Lemma 2.

For the binding property, we use this assumption that when ℓ is big enough and τ is small enough, for any vector $\mathbf{x}_{(k+1)\times 1} \neq 0$,

$$\Pr[\omega(\mathbf{Ax}) \leq 4\ell\tau : \mathbf{A} \xleftarrow{\$} S_{\ell\times(k+1)}] \leq \mathtt{negl}(\eta).$$

We show how this assumption holds. Note that $\mathbf{Ax}$ is a random binary vector of the size ℓ when $\mathbf{A}$ is chosen uniformly at random and $\mathbf{x} \neq 0$. Suppose $X_1, \cdots, X_\ell$ are independent Bernoulli random variables each with the parameter $1/2$. Let $X = \sum_{i=1}^{\ell} X_i$. It is easy to see that the expected value of X is $\ell/2$. Then, for any $0 < \delta < 1$

$$\Pr[X \leq (1-\delta)\ell/2] \leq e^{-\frac{\delta^2\ell}{4}},$$

that is the Chernoff bound on the deviation below the mean (Theorem 4.5 in [27]). This means that

$$\Pr[\omega(\mathbf{Ax}) \leq (1-\delta)\ell/2 : \mathbf{A} \xleftarrow{\$} S_{\ell\times(k+1)},\ \mathbf{x} \neq 0] \leq e^{-\frac{\delta^2\ell}{4}}.$$

And for $\delta = 1/2$,

$$\Pr[\omega(\mathbf{Ax}) \leq \ell/4 : \mathbf{A} \xleftarrow{\$} S_{\ell\times(k+1)},\ \mathbf{x} \neq 0] \leq e^{-\frac{\ell}{16}}.$$

Now for any $\tau \leq 1/16$,

$$\Pr[\omega(\mathbf{Ax}) \leq 4\ell\tau : \mathbf{A} \xleftarrow{\$} S_{\ell\times(k+1)},\ \mathbf{x} \neq 0] \leq e^{-\frac{\ell}{16}}.$$

Theorem 1. *Let η be the security parameter. The Scheme 1 is a quantum computationally hiding and perfectly binding commitment scheme under the hardness of decisional (τ, ℓ, k)-LPN, where $\ell = poly(\eta)$, $\lim_{\ell\to\infty} \tau\ell = \infty$, and ℓ is big enough and τ is small enough such that for any vector $\mathbf{x}_{(k+1)\times 1} \neq 0$,*

$$\Pr[\omega(\mathbf{Ax}) \leq 4\ell\tau : \mathbf{A} \xleftarrow{\$} S_{\ell\times(k+1)}] \leq \mathtt{negl}(\eta).$$

Proof. First we show that this scheme is quantum computationally hiding under the hardness of the LPN problem. By the Lemma 2, $\mathbf{A}''\mathbf{s} \oplus \mathbf{e}$ is indistinguishable from an uniformly random binary vector $\mathbf{r}$ when $\mathbf{e} \leftarrow \xi_\tau$. That is $\mathbf{A}'b \oplus \mathbf{A}''\mathbf{s} \oplus \mathbf{e}$ is indistinguishable from $\mathbf{A}'b \oplus \mathbf{r}$ and therefore it is indistinguishable from $\mathbf{A}'(1 \oplus b) \oplus \mathbf{A}''\mathbf{s}' \oplus \mathbf{e}'$ when $\mathbf{s}, \mathbf{s}' \xleftarrow{\$} S_{k\times 1}$ and $\mathbf{e}, \mathbf{e}' \leftarrow \xi_\tau$. The only difference in the Scheme 1 is that the inequality $\omega(\mathbf{e}) < 2\tau\ell$ should hold, additionally. We show that for an $\mathbf{e} \leftarrow \xi_\tau$, with a negligible probability $\omega(\mathbf{e}) \geq 2\tau\ell$ and therefore $\mathbf{As} \oplus \mathbf{e}$

is indistinguishable from an uniformly random binary vector in the Scheme 1 as well. Suppose $X_1, \cdots, X_\ell$ are independent Bernoulli random variables each with the parameter τ. Let $X = \sum_{i=1}^{\ell} X_i$. It is easy to see that the expected value of X is $\tau\ell$. Then, for any $0 < \delta \leq 1$

$$\Pr[X \geq (1+\delta)\tau\ell] \leq e^{-\frac{\delta^2 \tau\ell}{3}},$$

that is the Chernoff bound on the deviation above the mean (Theorem 4.4 in [27]). This means that

$$\Pr[\omega(\mathbf{e}) \geq (1+\delta)\tau\ell : \mathbf{e} \leftarrow \xi_\tau] \leq e^{-\frac{\delta^2 \tau\ell}{3}}.$$

And for $\delta = 1$, $\Pr[\omega(\mathbf{e}) \geq 2\tau\ell : \mathbf{e} \leftarrow \xi_\tau] \leq e^{-\frac{\tau\ell}{3}}$ that is negligible on ℓ.

To show the binding property, let assume that the adversary can successfully open a commitment $\mathbf{c}$ to $(b, \mathbf{s}_1, \mathbf{e}_1)$ and $(b \oplus 1, \mathbf{s}_2, \mathbf{e}_2)$. This means that $\mathbf{e}_1 \oplus \mathbf{e}_2 = \mathbf{A}' \oplus \mathbf{A}''(\mathbf{s}_1 \oplus \mathbf{s}_2)$ and $\omega(\mathbf{e}_1), \omega(\mathbf{e}_2) < 2\tau\ell$. Then we can write

$$\omega(\mathbf{A}' \oplus \mathbf{A}''(\mathbf{s}_1 \oplus \mathbf{s}_2)) \leq \omega(\mathbf{e}_1) + \omega(\mathbf{e}_2) \leq 4\tau\ell.$$

And this holds only with a negligible probability by the assumption. $\square$

We define an XOR-homomorphic bit commitment scheme below.

Definition 8 (XOR-homomorphic Bit Commitment Scheme). *We say a bit commitment scheme* (Gen, Com, Ver) *accepts β XOR operations if for any $pk \leftarrow \mathrm{Gen}(1^n)$, any $1 \leq i \leq \beta$ and $(c_1, d_1), \cdots, (c_i, d_i)$ generated by Com_{pk} on inputs $b_1, \cdots, b_i$ respectively, the following properties holds:*

1. *Correctness:* $\Pr[\mathrm{Ver}_{pk}(i, \sum_{j=1}^{i} c_j, (\sum_{j=1}^{i} b_j, \sum_{j=1}^{i} d_j)) = 1] = 1$.
2. *Quantum computationally hiding: For any quantum polynomial-time adversary, $\sum_{j=1}^{i} c_j$ and c' are indistinguishable where $i \leq \beta$ and $c_1, \cdots, c_i$ and c' are generated by Com_{pk} on the input $b_1, \cdots, b_i$ and $1 \oplus \sum_{j=1}^{i} b_j$, respectively.*
3. *Perfect binding: For any commitment c (either obtained directly by Com_{pk} or by XOR operations), any bit b and two openings (i, d) and (i', d') with the condition that $i, i' \leq \beta$,*

$$\Pr\left[\Big(\mathrm{Ver}_{pk}(i, c, (b, d)) = 1\Big) \wedge \Big(\mathrm{Ver}_{pk}(i', c, (1 \oplus b, d')) = 1\Big)\right] \leq \mathtt{neg}(n),$$

where the probability is over random selection of pk.

We modify the verification algorithm of the Scheme 1 to fulfill the Definition 8. The new verification algorithm Ver' on inputs $\mathbf{A}, i, \mathbf{c}, \tau, \mathbf{d} = (\mathbf{s}, \mathbf{e})$ checks if $\mathbf{c} = \mathbf{A}\mathbf{s} \oplus \mathbf{e}$ and $\omega(\mathbf{e}) < 2i\tau\ell$. Note that the main reason that we modify the verification algorithm in the Scheme 1 to Ver' (that gets i as input) is to preserve the correctness property under β XOR operations. In other words, if a commitment c is obtained by XORing i commitments $c_1 \leftarrow \mathrm{Com}_{pk}, \cdots, c_i \leftarrow \mathrm{Com}_{pk}$, then the error vector of c may have a Hamming weight bigger than $2\tau\ell$ and the verification algorithm in Scheme 1 returns 0. In this case, the sender sends i along with the opening information and Ver$'$ checks if the Hamming weight of the error vector is less than $2i\tau\ell$ or not. In the following theorem, we show that this modification does not have any effect on the quantum computationally hiding and the perfect binding property with the proper choice of parameters.

Lemma 3. *Let η be the security parameter. The Scheme 1 with the verification algorithm* Ver$'$ *accepts β XOR operations under the hardness of decisional (τ, ℓ, k)-LPN, where $\ell = poly(\eta)$, $\lim_{\ell\to\infty} \tau\ell = \infty$, and ℓ is big enough and τ is small enough such that for any vector $\mathbf{x}_{(k+1)\times 1} \neq 0$,*

$$\Pr[\omega(\mathbf{A}\mathbf{x}) \leq 4\beta\ell\tau : \mathbf{A} \xleftarrow{\$} S_{\ell\times(k+1)}] \leq \texttt{negl}(\eta).$$

Proof. The correctness property in the Definition 8 holds clearly. The computational hiding property holds similarly to the proof of Theorem 1. Namely, we have that

$$\Pr[\omega(\mathbf{e}) \geq (1+\delta)\tau\ell : \mathbf{e} \leftarrow \xi_\tau] \leq e^{-\frac{\delta^2\tau\ell}{3}}.$$

Now for $\delta = 2\beta$, the probability that $\omega(\mathbf{e}) \geq (1+2\beta)\tau\ell$ is negligible when $\mathbf{e}$ is sampled from ξ_τ. Since $\omega(\sum_{j=1}^{i} \mathbf{e}_j) \leq 2i\tau\ell \leq 2\beta\tau\ell$, we can conclude that

$$\sum_{j=1}^{i} c_j = \mathbf{A}(\sum_{j=1}^{i} b_j, \sum_{j=1}^{i} \mathbf{s}_j) \oplus \sum_{j=1}^{i} \mathbf{e}_j$$

is indistinguishable from an uniformly random binary vector by Lemma 2.

Let assume the perfect binding property in the Definition 8 does not hold and $\mathbf{c}$ can be opened to both b and $1 \oplus b$ with the opening $(i, \mathbf{s}, \mathbf{e})$ and $(i', \mathbf{s}', \mathbf{e}')$ respectively. Thus $\omega(\mathbf{e}) < 2i\tau\ell$, $\omega(\mathbf{e}') < 2i'\tau\ell$ and we can write

$$\mathbf{A}'b \oplus \mathbf{A}''\mathbf{s} \oplus \mathbf{e} = \mathbf{A}'(1 \oplus b) \oplus \mathbf{A}''\mathbf{s}' \oplus \mathbf{e}'.$$

So

$$\omega\big(\mathbf{A}' \oplus \mathbf{A}''(\mathbf{s} \oplus \mathbf{s}')\big) \leq \omega(\mathbf{e}) + \omega(\mathbf{e}') < 2i\tau\ell + 2i'\tau\ell \leq 4\beta\tau\ell,$$

that happens only with a negligible probability. □

4 Equality and Non-equality Problems

In this section, we show how an XOR-homomorphic bit commitment scheme can be used to prove that two inputs are not equal without revealing any information beyond the non-equality assurance. Here, we assume that a randomness r_i used to generate a commitment $\mathbf{c}_i = \mathrm{Com}_{pk}(b_i; r_i)$ is chosen uniformly at random. Consequently, for a target commitment $\mathbf{c} = \mathrm{Com}_{pk}(b; r)$ the opening information of $\mathbf{c}_i \oplus \mathbf{c}$ is $(b_i \oplus b, r_i \oplus r)$ and therefore $r_i \oplus r$ is hiding r information theoretically. This is crucial to prove the zero-knowledge property of protocols below. With this formulation, the idea can be modified to additive homomorphic commitment schemes easily. Regrettably, the Scheme 1 does not fulfill this requirement since the error vector $\mathbf{e}$ is not distributed uniformly at random (see below for more details).

Equality Problem. A prover $\mathcal{P}$ has two inputs m_1 and m_2 and wants to prove that $m_1 = m_2$ without revealing any extra information about its inputs.

Protocol 1. *The prover $\mathcal{P}$ on inputs m_0, m_1 and the security parameter 1^n runs $\mathrm{Gen}(1^n)$ to get pk. Then it chooses two randomness r_0, r_1 and computes $\mathrm{Com}_{pk}(m_0; r_0) = (c_0, d_0)$ and $\mathrm{Com}_{pk}(m_1; r_1) = (c_1, d_1)$. Finally, it sends pk, c_0, c_1 and $d := d_0 \oplus d_1$ to $\mathcal{V}$. The verifier $\mathcal{V}$ accepts if $\mathrm{Ver}(pk, c_0 \oplus c_1, (0, d)) = 1$ and it rejects otherwise.*

Non-equality Problem. A prover $\mathcal{P}$ has two inputs m_0 and m_1 and wants to prove that $m_0 \neq m_1$ without revealing any extra information about its inputs.

If the inputs of $\mathcal{P}$ are bits, the non-equality problem can be solved by a slight modification to the Protocol 1. Namely, the verifier $\mathcal{V}$ accepts if $\mathrm{Ver}(pk, c_0 \oplus c_1, (1, d)) = 1$ and it rejects otherwise. But when the inputs are bit-strings, the approach of the Protocol 1 will leak a position in which m_0 and m_1 have different bits and this is beyond $m_0 \neq m_1$ assurance. In the following, we present a protocol that proves $m_0 \neq m_1$ without revealing a position in which m_0 and m_1 differ.

Protocol 2. *Let η is the security parameter and $|k| \leq \mathtt{Pol}(\eta)$. Let $\mathrm{ComiT} = (\mathrm{Com}, \mathrm{Gen}, \mathrm{Ver})$ be an XOR-homomorphic commitment scheme. This is a protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. Both has $pk \leftarrow \mathrm{Gen}(1^\eta)$ as input.*

1. *The prover $\mathcal{P}$ on inputs pk, bit-strings $m_0 = (m_0^1, \cdots, m_0^k)$ and $m_1 = (m_1^1, \cdots, m_1^k)$, computes $(c_0^i, d_0^i) = \mathrm{Com}_{pk}(m_0^i; r_0^i)$ and $(c_1^i, d_1^i) = \mathrm{Com}_{pk}(m_1^i; r_1^i)$ for $i \in [k]$. It sends all c_0^i, c_1^i to $\mathcal{V}$.*
2. *The prover chooses η random permutations π_j of $[k]$ and computes $(c_{i,j}, d_{i,j}) = \mathrm{Com}_{pk}(0; r_{i,j}) \oplus c_0^{\pi_j(i)} \oplus c_1^{\pi_j(i)}$ for any $i \in [k]$ and $j \in [\eta]$. Finally, it sends all $c_{i,j}$ to $\mathcal{V}$.*
3. *The verifier $\mathcal{V}$ chooses a random subset S of $[\eta]$ and sends it to $\mathcal{P}$.*
4. *For each $j \in S$, the prover $\mathcal{P}$ sends an i_j and $d_{i_j,j}$ for which $m_0^{\pi_j(i_j)} \neq m_1^{\pi_j(i_j)}$. For each $j \notin S$, the prover sends the permutation π_j and the set $\{d_{i,j} \oplus d_0^{\pi_j(i)} \oplus d_1^{\pi_j(i)}\}_{i \in [k]}$.*
5. *The verifier $\mathcal{V}$ accepts if the following verifications pass:*
   - *for each $j \in S$, $\mathrm{Ver}(3, pk, c_{i_j,j}, (1, d_{i_j,j})) = 1$,*
   - *for each $j \notin S$ and $i \in [k]$,*

   $$\mathrm{Ver}(1, pk, c_{i,j} \oplus c_0^{\pi_j(i)} \oplus c_1^{\pi_j(i)}, (0, d_{i,j} \oplus d_0^{\pi_j(i)} \oplus d_1^{\pi_j(i)})) = 1.$$

   Otherwise, it rejects.

We show that the Protocol 2 is a post-quantum computational zero-knowedge proof system with the soundness error $O(1/2^\eta)$ when the underlying commitment scheme ComiT is quantum computationally hiding and perfect binding. The zero-knwledge property holds without using the rewinding technique. We start with a simulator S_0 that possesses $\mathcal{P}$'s inputs m_0, m_1 and runs the protocol exactly the same as $\mathcal{P}$ does. Then, we define k hybrids in which the simulator ignores the k-th component of m_0, m_1 and replaces them by two bits b and $b \oplus 1$ where b is chosen randomly, and runs the protocol with these modified inputs. The transcripts of the executions of two consecutive hybrids will be indistinguishable for any quantum polynomial-time distinguisher since the commitment scheme is quantum computationally hiding and accepts XOR-homomorphic operations. Since in the last hybrid the simulator ignores all the components of m_0, m_1, $\mathcal{V}^*$ can not learn any information about m_0, m_1 in this hybrid.

Theorem 2. *The Protocol 2 is a post-quantum computational zero-knowledge proof system with the soundness error $O(1/2^\eta)$ if the underlying commitment scheme* ComiT *is quantum computationally hiding and perfect binding.*

Proof. For the completeness property, we show that the verifier accepts with the probability 1 in the honest execution of the protocol. First we show that for any $j \in S$ there exists an i_j such that $\mathrm{Ver}'(3, pk, c_{i_j,j}, (1, d_{i_j,j})) = 1$ with the probability 1. Note that when $m_0 \neq m_1$, there exists an $\alpha \in [k]$ such that $m_0^\alpha \neq m_1^\alpha$. Now the honest prover can set $i_j := \pi_j^{-1}(\alpha)$. The verification pass because $c_{\pi_j^{-1}(\alpha),j} = \mathrm{Com}_{pk}(0; r_{\pi_j^{-1}(\alpha),j}) \oplus c_0^\alpha \oplus c_1^\alpha$ that is the commitment of 1 with the opening string $d_{\pi_j^{-1}(\alpha),j}$. For any $j \notin S$ and $i \in [k]$, it is obvious that $c_{i,j} \oplus c_0^{\pi_j(i)} \oplus c_1^{\pi_j(i)}$ is the commitment of 0 with the opening string $d_{i,j} \oplus d_0^{\pi_j(i)} \oplus d_1^{\pi_j(i)}$. So the verification pass with the probability 1.

For the soundness property, we show that if a malicious prover on inputs $m_0 = m_1$ does not guess the set S correctly, at least one of the verifications in the step 4 output reject with an overwhelming probability. Note that for any $j \in S$, a malicious prover needs to return an i_j for which $c_{i_j,j}$ opens to 1. If the prover generates $c_{i_j,j}$ honestly, the first verification returns reject since the commitment scheme is binding with respect to 3 XOR operations and the prover can open $c_{i_j,j}$ to 1 only with a negligible probability. So a malicious prover should generate $c_{i_j,j}$ dishonestly (for instance by XORing Com(1) to $c_0^{\pi_j(i_j)} \oplus c_1^{\pi_j(i_j)}$) in order to open it to 1. And this requires that the malicious prover guesses S correctly in the step 1 of the protocol and for each $j \in S$ it generates at least one of $c_{i,j}$ dishonestly.

In more details, let assume that S' is the $\mathcal{P}$'s guess for S that is incorrect ($S' \neq S$). Note that $S' \neq S$ implies two cases: 1) there exists a value $j \in [\eta]$ such that $j \in S$ but $j \notin S'$. 2) there exists a value $j \in [\eta]$ such that $j \notin S$ but $j \in S'$. When $j \in S$ and $j \notin S'$, by the binding property of Com, there is no i_j for which $c_{i_j,j}$ opens to 1 and the first verification outputs reject with on overwhelming probability. When $j \notin S$ and $j \in S'$, there is an i_j for which the adversary has generated $c_{i_j,j}$ dishonestly to be bale to open it to 1. But now the adversary can not open $c_{i_j,j} \oplus c_0^{\pi_j(i_j)} \oplus c_1^{\pi_j(i_j)}$ to 0 by the binding property of the commitment scheme. So at least one of the verification output reject with an overwhelming probability is the prover does not guess the challenge set S correctly.

We show that the protocol is post-quantum computationally zero-knowledge. Let $\mathsf{Hybrid\ 0}$ be the execution of the Protocol 2 by the honest prover $\mathcal{P}$ and a malicious quantum verifier $\mathcal{V}^*$ and $\mathbf{H}_0$ be the transcript of this execution.

In $\mathsf{Hybrid\ 1}$, we assume that a simulator $\mathcal{S}_0$ has pk and the inputs of $\mathcal{P}$, m_0 and m_1. The simulator $\mathcal{S}_0$ runs $\mathcal{V}^*$ with the inputs m_0, m_1 the same as $\mathcal{P}$. It is clear that the distributions of $\mathbf{H}_0$ and $\mathbf{H}_1$ are equal.

In $\mathsf{Hybrid\ 2}$, we change $\mathcal{S}_0$ to a simulator $\mathcal{S}_1$ that ignores the first bit of m_0 and m_1 and sets $(c_0^1, d_0^1) := \mathrm{Com}_{pk}(b; r_0^1)$ and $(c_1^1, d_1^1) := \mathrm{Com}_{pk}(1 \oplus b; r_1^1)$ for a randomly chosen bit b in the step 1 of the protocol. The rest of the commitments are computed the same as the step 1 of $\mathsf{Hybrid\ 1}$. The commitments in the step 2 are computed similar to $\mathsf{Hybrid\ 1}$ but using these modified (c_0^1, d_0^1) and (c_1^1, d_1^1) commitments. The rest of the protocol will be executed considering these changes. Since the commitment scheme is quantum computationally hiding that accepts XOR operations, $\mathcal{V}^*$ can distinguish the steps 1 and 2 in $\mathsf{Hybrid\ 1}$ and $\mathsf{Hybrid\ 2}$ only with a negligible probability. The distributions of the transcripts of steps 3-5 in $\mathsf{Hybrid\ 1}$ and $\mathsf{Hybrid\ 2}$ are indistinguishable in both hybrids because this modification in stpes 1-2 does not effect these steps of the protocol. In more details, assuming $m_0^i \neq m_1^i$, the modified inputs in $\mathsf{Hybrid\ 2}$ have different bits in the i-th position as well. So $\mathcal{S}_1$ can execute the step 4 similar to $\mathcal{S}_0$.

We keep modifying the hybrids to reach $\mathsf{Hybrid\ (k+1)}$ in which a simulator $\mathcal{S}_k$ ignores the $\mathcal{P}$'s inputs and chooses a random bit string $(b_1, \cdots, b_k)$ and runs $\mathcal{V}^*$ with the inputs $(b_1, \cdots, b_k)$ and $(1 \oplus b_1, \cdots, 1 \oplus b_k)$. Similar to above, we can show each two consecutive hybrids produce quantum computationally indistinguishable transcripts.

Since $|k| \leq \mathtt{Pol}(\eta)$ and each two consecutive hybrids produce quantum computationally indistinguishable transcripts, $\mathsf{Hybrid\ 0}$ and $\mathsf{Hybrid\ (k+1)}$ produce quantum computationally indistinguishable transcripts. This finishes the proof since $\mathcal{S}_k$ does not use m_0, m_1 at all and therefore $\mathcal{V}^*$ can not learn anything about m_0, m_1 beyond their inequality in $\mathsf{Hybrid\ (k+1)}$. □

Comment on the implementation using Scheme 1. Note that in the step 5 of Protocol 2, for any $j \in S$ the prover has to reveal the opening information for a commitment $c_{i_j,j} = \mathrm{Com}(0; r_{i,j}) \oplus c_0^{\pi_j(i_j)} \oplus c_1^{\pi_j(i_j)}$. If we use Scheme 1, $r_{i,j} = (\mathbf{s}_{i,j}, \mathbf{e}_{i,j})$ and the randomnesses to generates $c_0^{\pi_j(i_j)}$ and $c_1^{\pi_j(i_j)}$ are $(\mathbf{s}_0^{i_j}, \mathbf{e}_0^{i_j})$ and $(\mathbf{s}_1^{i_j}, \mathbf{e}_1^{i_j})$, respectively. So the opening information for $c_{i_j,j}$ has the vector $\mathbf{e}_{i,j} \oplus \mathbf{e}_0^{i_j} \oplus \mathbf{e}_1^{i_j}$. Since these vectors have low Hamming weight, the adversary can learn information about them after observing many of them (S can be a large set and k can be a small number.) In other words, since $\mathbf{e}_{i,j}$ is not distributed uniformly at random, it can not hide $\mathbf{e}_0^{i_j} \oplus \mathbf{e}_1^{i_j}$ information theoretically.

If a prover wants to show that its input m is not equal to 0 bit-string without revealing any further information about m, a simplification of the Protocol 2 can be used.

Protocol 3. *Let η is the security parameter and $|k| \leq \texttt{Pol}(\eta)$. Let* $\mathrm{ComiT} = (\mathrm{Gen}, \mathrm{Com}, \mathrm{Ver})$ *be an XOR-homomorphic commitment scheme. This is a protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. Both has $pk \leftarrow \mathrm{Gen}(1^\eta)$ as input.*

1. *The prover $\mathcal{P}$ on inputs pk, the bit-string $m = (m^1, \cdots, m^k)$, computes $(c^i, d^i) = \mathrm{Com}_{pk}(m^i; r^i)$ for each $i \in [k]$. It sends all c^i to $\mathcal{V}$.*
2. *It chooses η random permutations π_j of $[k]$ and for any $i \in [k]$ and $j \in [\eta]$ computes $(c_{i,j}, d_{i,j}) = \mathrm{Com}_{pk}(0; r_{i,j}) \oplus c^{\pi_j(i)}$. Finally, it sends all $c_{i,j}$ to $\mathcal{V}$.*
3. *The verifier $\mathcal{V}$ chooses a random subset S of $[\eta]$ and sends it to $\mathcal{P}$.*
4. *For each $j \in S$, the prover $\mathcal{P}$ sends an i_j and $d_{i_j,j}$ for which $m^{\pi_j(i_j)} \neq 0$. For each $j \notin S$, the prover sends the permutation π_j and the set $\{d_{i,j} \oplus d^{\pi_j(i)}\}_{i \in [k]}$.*
5. *The verifier $\mathcal{V}$ accepts if the following verifications pass:*
   - *for each $j \in S, \mathrm{Ver}'(2, pk, c_{i_j,j}, d_{i_j,j}, 1) = 1$,*
   - *for each $j \notin S$ and $i \in [k]$,*
   $$\mathrm{Ver}'(1, pk, c_{i,j} \oplus c^{\pi_j(i)}, d_{i,j} \oplus d^{\pi_j(i)}, 0) = 1.$$

   Otherwise, it rejects.

Similar to the proof of the Theorem 2, we can show that the Protocol 3 is post-quantum computationally zero-knowledge proof system with the soundness error $O(1/2^\eta)$ if the underlying commitment scheme ComiT is quantum computationally hiding and perfect binding.

5 Graph 3-coloring Problem

We say a graph $G(V, E)$ is 3-colorable if there exists a map $\chi : V \to \{01, 10, 11\}$ such that for any edge $(v_1, v_2) \in E$, $\chi(v_1) \neq \chi(v_2)$, that is, any two adjacent vertices are mapped to two different colors. Given a graph $G(V, E)$, determining if G is 3-colorable or not is an NP-complete problem [15]. This problem has a computationally zero-knowledge proof system assuming the existence of an unconditionally binding and computationally hiding commitment scheme [18]. The post-quantum security of this proof system has been shown in [35] under the assumption of the existence of an unconditionally binding and quantum computationally hiding commitment scheme. To prove this proof system is zero-knowledge against a quantum verifier, Watrous [35] presented a quantum rewinding technique to construct the simulator.

Protocol 4 (Graph 3-coloring proof system [18])**.** *This is a protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. Both have pk and $G(V, E)$ as input. In addition, the prover knows a 3-coloring χ for G. Let* $\mathrm{ComiT} = (\mathrm{Gen}, \mathrm{Com}, \mathrm{Ver})$ *be an commitment scheme, $|V| = n$ and $|E| = m$.*

1. *The prover chooses a random permutation π over $\{01, 10, 11\}$ and computes $(c_i, d_i) = \mathrm{Com}(pk, \pi(\chi(v_i)))$ for all $i \in [n]$.*

2. *The verifier $\mathcal{V}$ chooses a random edge (v_k, v_j) from E and sends it to $\mathcal{P}$.*
3. *The prover sends $\pi(\chi(v_k)), d_k$ and $\pi(\chi(v_j)), d_j$ to $\mathcal{V}$.*
4. *$\mathcal{V}$ accepts if $\pi(\chi(v_k)) \neq \pi(\chi(v_j))$ and $\mathrm{Ver}(pk, c_k, d_k, \pi(\chi(v_k))) = 1$ and $\mathrm{Ver}(pk, c_j, d_j, \pi(\chi(v_j))) = 1$.*

The soundness error of the Protocol 4 is $1/m$. So the protocol needs to be executed $O(m\gamma)$ times sequentially to obtain a soundness error of $1/2^\gamma$. Consequently, in total the prover needs to send $O(nm\gamma)$ commitments to the verifier. We use the Protocol 2 and the Protocol 3 to propose a more efficient proof system for the graph 3-coloring problem. In the protocol below we use the Protocol 2 and the Protocol 3 with the soundness error $1/2$, that is, these protocols with $\eta = 1$.

Protocol 5. *This is a protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. Both have $pk \leftarrow \mathrm{Gen}(1^n)$ and $G(V, E)$ as input. Let $\mathrm{ComiT} = (\mathrm{Gen}, \mathrm{Com}, \mathrm{Ver})$ be an XOR-homomorphic commitment scheme. Let $|V| = n$ and $|E| = m$. In addition, the prover knows a 3-coloring χ for G. Let $\chi_0(v_i)$ and $\chi_1(v_i)$ denote the first bit and the second bit of $\chi(v_i)$, respectively.*

1. *For all $i \in [n]$, the prover computes $(c_0^i, d_0^i) = \mathrm{Com}_{pk}(\chi_0(v_i); r_0^i)$ and $(c_1^i, d_1^i) = \mathrm{Com}_{pk}(\chi_1(v_i); r_0^i)$.*
2. *The verifier $\mathcal{V}$ chooses a random edge (v_k, v_j) from E and sends it to $\mathcal{P}$.*
3. *The prover uses the Protocol 3 and the Protocol 2 (steps 2-5) with the parameter $\eta = 1$ to prove that $\chi(v_k) \neq 00$, $\chi(v_j) \neq 00$ and $\chi(v_k) \neq \chi(v_j)$.*
4. *$\mathcal{V}$ accepts if all verifications in the Protocol 3 and the Protocol 2 pass.*

In the following, we show that the Protocol 5 is computationally zero-knowledge proof system against a quantum malicious verifier. The proof for the zero-knowledge property is similar to the Watrous's proof for the Protocol 4 [35], so we only present a high-level proof for it in this paper.

Theorem 3. *The Protocol 5 is a post-quantum computationally zero-knowledge interactive proof system with the soundness error $1 - \frac{1}{2m} + \mathtt{neg}(n)/2m$ if ComiT is a quantum computationally hiding and perfect biding XOR-homomorphic commitment scheme.*

Proof. The completeness property follows trivially by the completeness property of the Protocol 3 and the Protocol 2. For the soundness error, we show that if a malicious prover commits to an invalid 3-coloring χ' for G, $\mathcal{V}$ outputs reject with the probability at least $\frac{1}{2m}$. Without loss of generality, we can assume that a map χ' is an invalid 3-coloring for G if there exists an edge (v_k, v_j) such that $\chi'(v_k) = \chi'(v_j)$ or at least one of v_k or v_j maps to 00 by χ'. (In other words, if a vertex v_k with degree 0 maps to 00 by χ', we can replace 00 with one of the valid colors and this will not have any effect on the (in)validity of χ' on other vertices. So without loss of generality we consider the vertices with degree 0 never receive the color 00.) With the probability $1/m$, $\mathcal{V}$ challenges this edge (v_k, v_j). And by the soundness property of the Protocol 2 and the Protocol 3, one of the verifications output reject with a probability negligibly close to 1/2. Overall, $\mathcal{V}$ rejects with a probability negligibly close to $1/2m$.

It has been left to show that the protocol is quantum computationally zero-knowledge. The idea of the proof is the same as the Watrous's proof [35]. First we sketch the classical simulator.

1. The simulator chooses a random edge $e := (v_k, v_j)$, it sets $\chi(v_k)$ and $\chi(v_j)$ to be two distinct valid colors $01, 10$, and for the rest of vertices v it sets $\chi(v) = 11$. It commits to this χ.
2. The malicious quantum verifier sends a random edge e'.
3. If $e = e'$, the simulator continues the rest of the protocol, otherwise, it rewinds the verifier to the step 1.

Rewinding in the step 3 of this simulator may not work against a malicious quantum verifier $\mathcal{V}^*$. Here, we use the Watrous's quantum rewinding lemma [35] (Lemma 1) to construct a quantum simulator $\mathcal{S}$. Let $\mathbb{U}_1$ be the unitary that shows the action of $\mathcal{V}^*$ (note that if $\mathcal{V}^*$ performs some measurement, we consider its purification here) after getting the classical commitments in the step 1. Let assume the response of $\mathcal{V}^*$ for the challenge edge (lets call it e') is stored in a register R_e under $\mathbb{U}_1$. The quantum simulator $\mathcal{S}$ chooses a random edge e, prepares an ancillary register R_A, sets it to $|0\rangle$ and applies an unitary $\mathbb{U}_2$ to the registers R_e and R_A that stores the bit $[e = e']$ in R_A.

We show that the Lemma 1 can be used for the unitary $\mathbb{Q} = \mathbb{U}_2\mathbb{U}_1$. Note that the exact value of the parameters n, k does not play any role in the Lemma 1. It is only needed that the size of $\mathbb{Q}$ be polynomial. Let p_ψ be the probability that the computational basis measurement on R_A returns 0 after a single application of $\mathbb{Q}$ on some initial state $|\psi\rangle|0\rangle$. It is clear that $|p_\psi - 1/m| \leq \texttt{neg}(n)$ because the commitment scheme is quantum computationally hiding. There will be a negligible function ϵ such that $|p_\psi - 1/m| < \epsilon$ for all $|\psi\rangle$. Now if we set $q = p_0 = 1/m$, all the conditions in the Lemma 1 hold. Therefore, there exists a quantum circuit $\mathbb{R}$ of a polynomial size such that its output will be close to $|\psi_{good}\rangle$ (any state with 0 in the R_A register).

The quantum simulator $\mathcal{S}$ applies $\mathbb{R}$ and then it measures the R_A register. By the Lemma 1, with an overwhelming probability this measurement returns 0. This means that with an overwhelming probability the R_e register collapses to e. So with an overwhelming probability $e = e'$ in the step 3.

It is clear that when $e = e'$, the distribution of the transcript of this simulation is indistinguishable from the real execution against a quantum polynomial-time distinguisher $\mathcal{D}$, since the commitment scheme is quantum computationally hiding and it accepts XOR operations.

So overall, for any ψ the distribution of the transcripts of $\langle \mathcal{P}(x), \mathcal{V}^*(x, |\psi\rangle)\rangle$ and $\langle \mathcal{S}(x, |\psi\rangle), \mathcal{V}^*(x, |\psi\rangle)\rangle$ are quantum computationally indistinguishable. $\square$

Efficiency. In the Protocol 5, the steps 2-4 need to be repeated $O(\gamma m)$ times to obtain a soundness error $O(1/2^\gamma)$. The step 1 of the Protocol 5 consists of $2n$ commitments and each execution of the steps 2-4 needs $O(1)$ commitments. So with the Protocol 5 we can achieve the soundness error $1/2^\gamma$ with $O(n + m\gamma)$

commitments that is a significant improvement compare to the Protocol 4 that requires $O(nm\gamma)$ commitments to achieve the soundness error $1/2^{\gamma}$.

References

1. Stephanie Bayer and Jens Groth. Zero-knowledge argument for polynomial evaluation with application to blacklists. In *EUROCRYPT 2013*, volume 7881, pages 646–663. Springer, 2013.
2. Daniel Benarroch, Matteo Campanelli, Dario Fiore, Kobi Gurkan, and Dimitris Kolonelos. Zero-knowledge proofs for set membership: Efficient, succinct, modular. In *FC 2021*, volume 12674 of *Lecture Notes in Computer Science*, pages 393–414. Springer, 2021.
3. Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In *CRYPTO 1993*, volume 773 of *Lecture Notes in Computer Science*, pages 278–291. Springer, 1993.
4. Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *J. ACM*, 50(4):506–519, 2003.
5. Manuel Blum. How to prove a theorem so no one else can claim it. In *In: Proceedings of the International Congress of Mathematicians*, pages 1444–1451, 1987.
6. Sonia Bogos and Serge Vaudenay. Optimization of lpn solving algorithms. In *ASIACRYPT 2016*, volume 10031 of *Lecture Notes in Computer Science*, pages 703–728, 2016.
7. Joan Boyar, S. A. Kurtz, and Mark W. Krentel. A discrete logarithm implementation of perfect zero-knowledge blobs. *J. Cryptol.*, 2(2):63–76, 1990.
8. Gilles Brassard, David Chaum, and Claude Crépeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, 1988.
9. Gilles Brassard and Claude Crépeau. Non-transitive transfer of confidence: A perfect zero-knowledge interactive protocol for SAT and beyond. In *FOCS 1986*, pages 188–195. IEEE Computer Society, 1986.
10. Jan Camenisch, Rafik Chaabouni, and Abhi Shelat. Efficient protocols for set membership and range proofs. In *ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 234–252. Springer, 2008.
11. Nai-Hui Chia, Kai-Min Chung, Qipeng Liu, and Takashi Yamakawa. On the impossibility of post-quantum black-box zero-knowledge in constant rounds. *IACR Cryptol. ePrint Arch.*, page 376, 2021.
12. Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. Post-quantum succinct arguments. *Electron. Colloquium Comput. Complex.*, 28:38, 2021.
13. Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, page 151–158, New York, NY, USA, 1971. Association for Computing Machinery.
14. Andre Esser, Robert Kübler, and Alexander May. LPN decoded. In *CRYPTO 2017*, volume 10402 of *Lecture Notes in Computer Science*, pages 486–514. Springer, 2017.
15. M. R. Garey, David S. Johnson, and Larry J. Stockmeyer. Some simplified np-complete graph problems. *Theor. Comput. Sci.*, 1(3):237–267, 1976.
16. Oded Goldreich and Shafi Goldwasser. On the limits of nonapproximability of lattice problems. *J. Comput. Syst. Sci.*, 60(3):540–563, 2000.
17. Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledge proof systems for NP. *J. Cryptol.*, 9(3):167–190, 1996.

18. Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.
19. Oded Goldreich and Salil P. Vadhan. Comparing entropies in statistical zero-knowledge with applications to the structure of SZK. *Electron. Colloquium Comput. Complex.*, 5(63), 1998.
20. Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.
21. Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.*, 17(2):281–308, 1988.
22. Qian Guo, Thomas Johansson, and Carl Löndahl. Solving LPN using covering codes. *J. Cryptol.*, 33(1):1–33, 2020.
23. Abhishek Jain, Stephan Krenn, Krzysztof Pietrzak, and Aris Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In *ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 663–680. Springer, 2012.
24. Jonathan Katz. Which languages have 4-round zero-knowledge proofs? In *TCC*, volume 4948 of *Lecture Notes in Computer Science*, pages 73–88. Springer, 2008.
25. Jonathan Katz, Ji Sun Shin, and Adam D. Smith. Parallel and concurrent security of the HB and hb^+ protocols. *J. Cryptol.*, 23(3):402–421, 2010.
26. Joe Kilian. A note on efficient zero-knowledge proofs and arguments (extended abstract). In *STOC 1992*, pages 723–732. ACM, 1992.
27. Michael Mitzenmacher and Eli Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis.* Cambridge University Press, 2005.
28. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition).* Cambridge University Press, 2016.
29. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.
30. Amit Sahai and Salil P. Vadhan. A complete promise problem for statistical zero-knowledge. In *FOCS 1997*, pages 448–457. IEEE Computer Society, 1997.
31. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
32. Martin Tompa and Heather Woll. Random self-reducibility and zero knowledge interactive proofs of possession of information. In *FOCS 1987*, pages 472–482. IEEE Computer Society, 1987.
33. Dominique Unruh. Quantum proofs of knowledge. *IACR Cryptol. ePrint Arch.*, 2010:212, 2010.
34. Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 135–152. Springer, 2012.
35. John Watrous. Zero-knowledge against quantum attacks. In *STOC 2006*, pages 296–305. ACM, 2006.
36. Bin Zhang, Lin Jiao, and Mingsheng Wang. Faster algorithms for solving LPN. In *EUROCRYPT 2016*, volume 9665 of *Lecture Notes in Computer Science*, pages 168–195. Springer, 2016.

A Related Work

Our commitment scheme (Scheme 1) is a modification of the commitment scheme by Jain et al. [23]. Their scheme does not accept XOR-homomorphic operations. Here we briefly present the LPN based commitment scheme in [23].

Let S_ℓ^λ denotes the set of all binary vectors of length ℓ that have the Hamming weight λ. In [23], authors define the exact-(τ, ℓ, k)-LPN problem, a new version of (τ, ℓ, k)-LPN problem, in which the error vector $\mathbf{e}$ is chosen uniformly at random from $S_\ell^{\lfloor \tau k \rceil}$. In other words, the error vector has the exact Hamming weight $\lfloor \tau k \rceil$. Both the search and decisional versions of LPN are defined with this modification. They leave investigating the exact hardness of these new problems as open questions. Then, they suggest a commitment scheme that its hiding property holds based on the hardness assumption of the decisional exact-LPN problem.

We briefly describe their scheme. The public key is an uniformly random binary matrix $\mathbf{A} = \mathbf{A}'||\mathbf{A}''$ of size $\ell \times (j + k)$. To commit to a message $\mathbf{m} \in \{0,1\}^j$, the committer chooses an uniformly at random vector $\mathbf{s}$ of size $k \times 1$ and $\mathbf{e} \xleftarrow{\$} S_\ell^{\lfloor \tau k \rceil}$ and computes $\mathbf{c} = \mathbf{A}'\mathbf{m} \oplus \mathbf{A}''\mathbf{s} \oplus \mathbf{e}$ with the opening $(\mathbf{m}, \mathbf{s})$. Given a commitment $\mathbf{c}$, and opening $(\mathbf{m}', \mathbf{s}')$, a verifier accepts if and only if $\mathbf{e} = \mathbf{c} \oplus \mathbf{A}'\mathbf{m}' \oplus \mathbf{A}''\mathbf{s}'$ has the Hamming weight $\lfloor \tau k \rceil$.

Obviously, this scheme is not XOR-homomorphic because the verification algorithm checks if the error vector has the exact Hamming weight $\lfloor \tau k \rceil$ and XORing two commitments $\mathbf{c}_1 = \mathbf{A}'\mathbf{m}_1 \oplus \mathbf{A}''\mathbf{s}_1 \oplus \mathbf{e}_1$ and $\mathbf{c}_2 = \mathbf{A}'\mathbf{m}_2 \oplus \mathbf{A}''\mathbf{s}_2 \oplus \mathbf{e}_2$ might not open to $\mathbf{m}_1 \oplus \mathbf{m}_2$ using the opening $\mathbf{s}_1 \oplus \mathbf{s}_2$. In other words, this scheme does not preserve the correctness property under XOR-homomorphic operations.

B Other Protocols

We can use our XOR-homomorphic bit commitment scheme (Scheme 1) to construct post-quantum proof systems for other problems. For instance, similar to [9], we can use the equality protocol (Protocol 1) to construct a quantum computationally zero-knowledge interactive proof system for the Boolean satisfiability problem (or SAT) that is proven to be NP-complete [13]. We sketch the protocol without the proof.

Given a satisfiable Boolean function $f : \{0,1\}^k \to \{0,1\}$, $\mathcal{P}$ wants to prove that he knows an assignment $a_1, \cdots, a_k$ such that $f(a_1, \cdots, a_n) = 1$. First, we show how $\mathcal{P}$ on inputs a_1, a_2 proves that $\text{NAND}(a_1, a_2) = 1$ without revealing any information about a_1, a_2. Since NAND gate can reproduce the functions of all the other logic gates (that is, NAND is an universal gate), $\mathcal{P}$ can show that $f(a_1, \cdots, a_n) = 1$ step by step using this protocol.

A truth table for NAND gate is the evaluation of NAND gate on all inputs. It is a bitstring of length 12 that consists of four blocks of length 3. The i-th block is $(b_1, b_2, \text{NAND}(b_1, b_2))$ where $b_1 b_2$ is the bit representation of $i - 1$. A permuted truth table is obtained if one permutes these four blocks randomly.

Protocol 6 (Zero-knowledge computation of NAND)**.** *This is a protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. Both have pk as input. The prover has two input bits a_1, a_2 such that $NAND(a_1, a_2) = 1$.*

1. *$\mathcal{P}$ commits to bits $a_1, a_2, NAND(a_1, a_2)$ using the Scheme 1. That is, it computes* $\text{Com}_{pk}(a_i; r_i) = (c_i, d_i)$ *for $i = 1, 2$ and* $\text{Com}_{pk}(NAND(a_1, a_2); r_3) =$

(c_3, d_3). Let $c = (c_1, c_2, c_3)$. $\mathcal{P}$ chooses η permuted truth table for NAND. It uses the Scheme 1 to commit to all these truth tables. It sends all the commitments to $\mathcal{V}$.

2. *$\mathcal{V}$ chooses a random subset S of $[\eta]$ and sends it to $\mathcal{P}$.*
3. *For any $j \in S$, $\mathcal{P}$ opens all the commitments in the corresponding j-th truth table. For any $j \notin S$, $\mathcal{P}$ points out a block number in the j-th truth table and uses the Protocol 1 to show that this block is equal to c.*
4. *$\mathcal{V}$ accepts if all the verifications of openings for any $j \in S$ and all the verfications of the Protocol 1 for any $j \notin S$ pass.*

Another efficiency measure for a zero-knowledge proof system is the round complexity. For the graph 3-coloring problem, Goldreich and Kahan constructed a 5-round computational zero-knowledge proof system [17], assuming the existence of a collection of claw-free functions. It has been shown that 5-round complexity for a computational zero-knowledge proof system w.r.t. black-box simulation is optimal for any NP-complete language if the polynomial hierarchy does not collapse [24]. Assuming that the polynomial hierarchy does not collapse, any further improvement in the round complexity of the Goldreich-Kahan construction is not possible. However, one can improve the Goldreich-Kahan construction with respect to the communication complexity between $\mathcal{P}$ and $\mathcal{V}$ using our technique. In addition, Goldreich and Kahan [17] stated that the claw-free functions exist if factoring Blum Integers is hard ([21]), or alternatively if the Discrete Logarithm Problem is intractable ([7]). Obviously, these assumptions are not quantum-hard and the post-quantum security of the Goldreich-Kahan construction is an open question.[8] We leave investigating this for a future work.[9]

[8] There are some evidence that there is no constant-round post-quantum zero-knowledge proof (or argument) for NP w.r.t. black-box simulation unless NP is contained in BQP [11].

[9] Investigating the existence of a constant-round post-quantum zero-knowledge proof system with respect to non-black-box simulations.