Classically Verifiable NIZK for QMA with Preprocessing

Tomoyuki Morimae[1] and Takashi Yamakawa[1,2]

[1] Yukawa Institute for Theoretical Physics, Kyoto University, Japan
[2] NTT Social Informatics Laboratories, Tokyo, Japan

Abstract. We propose three constructions of classically verifiable non-interactive zero-knowledge proofs and arguments (CV-NIZK) for **QMA** in various preprocessing models.

1. We construct a CV-NIZK for **QMA** in the quantum secret parameter model where a trusted setup sends a quantum proving key to the prover and a classical verification key to the verifier. It is information theoretically sound and zero-knowledge.
2. Assuming the quantum hardness of the learning with errors problem, we construct a CV-NIZK for **QMA** in a model where a trusted party generates a CRS and the verifier sends an instance-independent quantum message to the prover as preprocessing. This model is the same as one considered in the recent work by Coladangelo, Vidick, and Zhang (CRYPTO '20). Our construction has the so-called dual-mode property, which means that there are two computationally indistinguishable modes of generating CRS, and we have information theoretical soundness in one mode and information theoretical zero-knowledge property in the other. This answers an open problem left by Coladangelo et al, which is to achieve either of soundness or zero-knowledge information theoretically. To the best of our knowledge, ours is the first dual-mode NIZK for **QMA** in any kind of model.
3. We construct a CV-NIZK for **QMA** with quantum preprocessing in the quantum random oracle model. This quantum preprocessing is the one where the verifier sends a random Pauli-basis states to the prover. Our construction uses the Fiat-Shamir transformation. The quantum preprocessing can be replaced with the setup that distributes Bell pairs among the prover and the verifier, and therefore we solve the open problem by Broadbent and Grilo (FOCS '20) about the possibility of NIZK for **QMA** in the shared Bell pair model via the Fiat-Shamir transformation.

1 Introduction

1.1 Background

The zero-knowledge [GMR89], which ensures that the verifier learns nothing beyond the statement proven by the prover, is one of the most central concepts in cryptography. Recently, there have been many works that constructed non-interactive zero-knowledge (NIZK) [BFM88] proofs or arguments for **QMA**, which is the "quantum counterpart" of **NP**, in various kind of models [ACGH20,

CVZ20, BG20, Shm21, BCKM21, BM21]. We note that we require the honest prover to run in quantum polynomial-time receiving sufficiently many copies of a witness when we consider NIZK proofs or arguments for **QMA**. All known protocols except for the protocol of Broadbent and Grilo [BG20] only satisfy computational soundness. The protocol of [BG20] satisfies information theoretical soundness and zero-knowledge in the *secret parameter (SP) model* [Ps05] where a trusted party generates proving and verification keys and gives them to the corresponding party while keeping it secret to the other party as setup.[3] A drawback of their protocol is that the prover sends a quantum proof to the verifier, and thus the verifier should be quantum. Therefore it is natural to ask the following question.

Can we construct a NIZK proof for **QMA** *with classical verification assuming a trusted party that generates proving and verification keys?*

In addition, the SP model is not a very desirable model since it assumes a strong trust in the setup. In the classical literature, there are constructions of NIZK proofs for **NP** in the common reference string (CRS) model [BFM88, FLS99, PS19] where the only trust in the setup is that a classical string is chosen according to a certain distribution and then published. Compared to the SP model, we need to put much less trust in the setup in the CRS model. Indeed, several works [BG20, CVZ20, Shm21] mention it as an open problem to construct a NIZK proofs (or even arguments) for **QMA** in the CRS model. Though this is still open, there are several constructions of NIZKs for **QMA** in different models that assume less trust in the setup than in the SP model [CVZ20, Shm21, BCKM21]. However, all of them are arguments. Therefore, we ask the following question.

Can we construct a NIZK proof for **QMA** *with classical verification in a model that assumes less trust in the setup than in the SP model?*

The Fiat-Shamir transformation [FS87] is one of the most important techniques in cryptography that have many applications. In particular, NIZK can be constructed from a Σ protocol: the prover generates the verifier's challenge β by itself by applying a random oracle H on the prover's first message α, and then the prover issues the proof $\pi = (\alpha, \gamma)$, where γ is the third message generated from α and $\beta = H(\alpha)$. It is known that Fiat-Shamir transform works in the post-quantum setting where we consider classical protocols secure against quantum adversaries [LZ19, DFMS19, DFM20]. On the other hand, it is often pointed out that (for example, [Shm21, BG20]) this standard technique cannot be used in the fully quantum setting. In particular, due to the no-cloning, the application of random oracle on the first message does not work when the first message is quantum like so-called the Ξ-protocol constructed by Broadbent and Grilo [BG20]. Broadbent and Grilo left the following open problem:

Is it possible to construct NIZK for **QMA** *in the CRS model (or shared Bell pair model) via the Fiat-Shamir transformation?*

[3] The SP model is also often referred to as *preprocessing model* [DMP90].

Note that the shared Bell pair model is the setup model where the setup distributes Bell pairs among the prover and the verifier. It can be considered as a "quantum analogue" of the CRS [Kob03].

1.2 Our Results

We answer the above questions affirmatively.

1. We construct a classically verifiable NIZK (CV-NIZK) for **QMA** in the QSP model where a trusted party generates a quantum proving key and classical verification key and gives them to the corresponding parties. We do not rely on any computational assumption for this construction either, and thus both soundness and the zero-knowledge property are satisfied information theoretically. This answers our first question. Compared with [BG20], ours has an advantage that verification is classical at the cost of making the proving key quantum. The proving key is a very simple state, i.e., a tensor product of randomly chosen Pauli X, Y, or Z basis states. We note that we should not let the verifier play the role of the trusted party for this construction since that would break the zero-knowledge property.
2. Assuming the quantum hardness of the learning with errors problem (the LWE assumption) [Reg09], we construct a CV-NIZK for **QMA** in a model where a trusted party generates a CRS and the verifier sends an instance-independent quantum message to the prover as preprocessing. We note that the CRS is reusable for generating multiple proofs but the quantum message in the preprocessing is not reusable. In this model, we only assume a trusted party that just generates a CRS once, and thus this answers our second question. This model is the same as one considered in [CVZ20] recently, and we call it the CRS + $(V \to P)$ model. Compared to their work, our construction has the following advantages.
   (a) In their protocol, both soundness and the zero-knowledge property hold only against quantum polynomial-time adversaries, and they left it open to achieve either of them information theoretically. We answer the open problem. Indeed, our construction has the so-called dual-mode property [GOS12, PS19], which means that there are two computationally indistinguishable modes of generating CRS, and we have information theoretical soundness in one mode and information theoretical zero-knowledge property in the other. To the best of our knowledge, ours is the first dual-mode NIZK for **QMA** in any kind of model.
   (b) Our protocol uses underlying cryptographic primitives (which are lossy encryption and oblivious transfer with certain security) only in a black-box manner whereas their protocol heavily relies on non-black-box usage of the underlying primitives. Indeed, their protocol uses fully homomorphic encryption to homomorphically runs the proving algorithm of a NIZK for **NP**, which would make the protocol extremely inefficient. On the other hand, our construction uses the underlying primitives only in a black-box manner, which results in a much more efficient construction.

Table 1. Comparison of NIZKs for **QMA**.

Reference	Soundness	ZK	Ver.	Model	Assumption	Misc
[ACGH20]	comp.	comp.	C	SP	LWE + QRO	
[CVZ20]	comp.	comp.	Q+C	CRS + $(V \to P)$	LWE	AoQK
[BG20]	stat.	stat.	Q	SP	None	
[Shm21]	comp.	comp.	Q	MDV	LWE	reusable
[BCKM21]	comp.	comp.	Q	MDV	LWE	reusable and single-witness
[BM21]	comp.	stat.	C	CRS	iO + QRO (heuristic)	
Section 3	stat.	stat.	C	QSP	None	
Section 4	stat. comp.	comp. stat.	Q+C	CRS + $(V \to P)$	LWE	dual-mode
Section 5	comp. (query)	comp. (query)	C	$V \to P$/Bell pair	QRO	

In column "Soundness" (resp. "ZK"), stat., and comp. mean statistical, and computational soundness (resp. zero-knowledge), respectively. Also, comp.(query) means that only the number of queries should be polynomial. In column "Ver.", "Q" and "C" mean that the verification is quantum and classical, respectively, and "Q+C" means that the verifier needs to send a quantum message in preprocessing but the online phase of verification is classical. QRO means the quantum random oracle.

We note that black-box constructions have been considered desirable for both theoretical and practical reasons in the cryptography community (e.g., see introduction of [IKLP06]).

(c) The verifier's quantum operation in our preprocessing is simpler than that in theirs: in the preprocessing of our protocol, the verifier has only to do single-qubit gate operations (Hadamard, bit-flip or phase gates), while in the preprocessing of their protocol, the verifier has to do five-qubit (entangled) Clifford operations. In their paper [CVZ20], they left the following open problem: how far their preprocessing phase could be weakened? Our construction with the weaker verifier therefore partially answers the open problem.

On the other hand, Coladangelo et al. [CVZ20] proved that their protocol is also an *argument of quantum knowledge (AoQK)*. We leave it open to study if ours is also a proof/argument of knowledge.

3. We construct a CV-NIZK for **QMA** with quantum preprocessing in the quantum random oracle model. This quantum preprocessing is the one where the verifier sends a random Pauli-basis states to the prover. Our construction uses the Fiat-Shamir transformation. Importantly, the quantum preprocessing can be replaced with the setup that distributes Bell pairs among the prover and the verifier. The distribution of Bell pairs by the setup can be considered as a "quantum analogue" of the CRS. This result gives an answer to our third question (and the second question as well). (Note that both the soundness and zero-knowledge property of the construction are computational one, but it does not mean that we use some computational assumptions: just the oracle query is restricted to be polynomial time.)

Comparison among NIZKs for **QMA**. We give more comparisons among our and known constructions of NIZKs for **QMA**. Since we already discuss comparisons with ours and [BG20, CVZ20], we discuss comparisons with other works. A summary of the comparisons is given in Table 1.

Alagic et al. [ACGH20] gave a construction of a NIZK for **QMA** in the SP model. Their protocol has an advantage that both the trusted party and verifier are completely classical. On the other hand, the drawback is that only computational soundness and zero-knowledge are achieved, whereas our first two constructions achieve (at least) either statistical soundness or zero-knowledge. Their protocol also uses the Fiat-Shamir transformation with quantum random oracle like our third result, but their setup is the secret parameter model, whereas ours can be the sharing Bell pair model, which is a quantum analogue of the CRS model.

Shmueli [Shm21] gave a construction of a NIZK for **QMA** in the malicious designated-verifier (MDV) model, where a trusted party generates a CRS and the verifier sends an instance-independent classical message to the prover as preprocessing. In this model, the preprocessing is *reusable*, i.e., a single preprocessing can be reused to generate arbitrarily many proofs later. This is a crucial advantage of their construction compared to ours. On the other hand, in their protocol, proofs are quantum and thus the verifier should perform quantum computations in the online phase whereas the online phase of the verifier is classical in our constructions. Also, their protocol only satisfies computational soundness and zero-knowledge whereas we can achieve (at least) either of them statistically.

Recently, Bartusek et al. [BCKM21] gave another construction of a NIZK for **QMA** in the MDV model that has an advantage that the honest prover only uses a single copy of a witness. (Note that all other NIZKs for **QMA** including ours require the honest prover to take multiple copies of a witness if we require neglible completeness and soundness errors.) However, their construction also requires quantum verifier in the online phase and only achieves computational soundness and zero-knowledge similarly to [Shm21].

Subsequently to our work, Bartusek and Malavolta [BM21] recently constructed the first CV-NIZK argument for **QMA** in the CRS model assuming the LWE assumption and ideal obfuscation for classical circuits. An obvious drawback is the usage of ideal obfuscation, which has no provably secure instantiation.[4] They also construct a witness encryption scheme for **QMA** under the same assumptions. They use the verification protocol of Mahadev [Mah18] and therefore the LWE assumption is necessary. If our CV-NIZK in the QSP model is used, instead, a witness encryption for **QMA** (with quantum ciphertext) would be constructed without the LWE assumption, which is one interesting application of our results.

[4] In the latest version, they give a candidate instantiation based on indistinguishability obfuscation and random oracles. However, the instantiation is heuristic since they obfuscate circuits that involve the random oracle, which cannot be done in the quantum random oracle model.

1.3 Technical Overview

Classically verifiable NIZK for **QMA** *in the QSP model.* Our starting point is the NIZK for **QMA** in [BG20], which is based on the fact that a **QMA** language can be reduced to the 5-local Hamiltonian problem with *locally simulatable* history states [BG20, GSY19]. (We will explain later the meaning of "locally simulatable".) An instance $\mathtt{x}$ corresponds to an N-qubit Hamiltonian $\mathcal{H}_{\mathtt{x}}$ of the form $\mathcal{H}_{\mathtt{x}} = \sum_{i=1}^{M} p_i \frac{I+s_iP_i}{2}$, where $N = \mathsf{poly}(|\mathtt{x}|)$, $M = \mathsf{poly}(|\mathtt{x}|)$, $s_i \in \{+1, -1\}$, $p_i > 0$, $\sum_{i=1}^{M} p_i = 1$, and P_i is a tensor product of Pauli operators (I, X, Y, Z) with at most 5 nontrivial Pauli operators (X, Y, Z). There are $0 < \alpha < \beta < 1$ with $\beta - \alpha = 1/\mathsf{poly}(|\mathtt{x}|)$ such that if $\mathtt{x}$ is a yes instance, then there exists a state ρ_{hist} (called the *history state*) such that $\mathrm{Tr}(\rho_{\mathrm{hist}}\mathcal{H}_{\mathtt{x}}) \leq \alpha$, and if $\mathtt{x}$ is a no instance, then for any state ρ, we have $\mathrm{Tr}(\rho\mathcal{H}_{\mathtt{x}}) \geq \beta$.

The completeness and the soundness of the NIZK for **QMA** in [BG20] is based on the posthoc verification protocol [FHM18], which is explained as follows. To prove that $\mathtt{x}$ is a yes instance, the prover sends the history state to the verifier. The verifier first chooses P_i with probability p_i, and measures each qubit in the Pauli basis corresponding to P_i. Let $m_j \in \{0, 1\}$ be the measurement result on jth qubit. The verifier accepts if $(-1)^{\oplus_j m_j} = -s_i$ and rejects otherwise. The probability that the verifier accepts is $1 - \mathrm{Tr}(\rho\mathcal{H}_{\mathtt{x}})$ when the prover's quantum message is ρ, and therefore the verifier accepts with probability at least $1-\alpha$ if $\mathtt{x}$ is a yes instance and the prover is honest whereas it accepts with probability at most $1-\beta$ if $\mathtt{x}$ is a no instance. (See Lemma 2.3 and [FHM18].) The gap between completeness and soundness can be amplified by simple parallel repetitions.

The verifier in the posthoc protocol is, however, not classical, because it has to receive a quantum state and measure each qubit. Our first idea to make the verifier classical is to use the quantum teleportation. Suppose that the prover and verifier share sufficiently many Bell pairs at the beginning. Then the prover can send the history state to the verifier with classical communication by the quantum teleportation. Though this removes the necessity of quantum communication, the verifier still needs to be quantum since it has to keep halves of Bell pairs and perform a measurement after receiving a proof.

To solve the problem, we utilize our observation that the verifier's measurement and the prover's measurement commute with each other, which is our second idea. In other words, we can let the verifier perform the measurement at the beginning without losing completeness or soundness. In the above quantum-teleportation-based protocol, when the prover sends its measurement outcomes $\{(x_j, z_j)\}_{j\in[N]}$ to the verifier, the verifier's state collapses to $X^xZ^z\rho_{\mathrm{hist}}Z^zX^x$ where ρ_{hist} denotes the history state and X^xZ^z means $\prod_{j=1}^{N} X_j^{x_j}Z_j^{z_j}$. Then the verifier applies the Pauli correction X^xZ^z and then measures each qubit in a Pauli basis. We observe that the Pauli correction can be applied even after the verifier measures each qubit because $X_j^{x_j}Z_j^{z_j}$ before a Pauli measurement on the jth qubit has the same effect as XOR by z_j or x_j after the measurement (see Lemma 2.2). Therefore, if a trusted party generates Bell pairs and measures half of them in random Pauli basis and gives the unmeasured halves to the prover as

a proving key while the measurement outcomes to the verifier as a verification key, a completely classical verifier can verify the **QMA** promise problem.

The last remaining issue is that the distribution of bases that appear in P_i depends on the instance $\mathtt{x}$, and thus we cannot sample the distribution at the setup phase where $\mathtt{x}$ is not decided yet. To resolve this issue, we use the following idea (which was also used in [ACGH20]). The trusted party just chooses random bases, and the verifier just accepts if they are inconsistent to P_i chosen by the verifier in the online phase. Since there are only 3 possible choices of the bases and P_i non-trivially acts on at most 5 qubits, the probability that the randomly chosen bases are consistent to P_i is at least 3^{-5}.[5] Therefore we can still achieve inverse-polynomial gap between completeness and soundness.

The zero-knowledge property of the NIZK for **QMA** in [BG20] uses the local simulatability of the history state. It roughly means that a classical description of the reduced density matrix of the history state for any 5-qubit subsystem can be efficiently computable without knowing the witness. Broadbent and Grilo [BG20] used this local simulatability to achieve the zero-knowledge property as follows. A trusted party randomly chooses $(\widehat{x},\widehat{z}) \xleftarrow{\$} \{0,1\}^N \times \{0,1\}^N$, and randomly picks a random subset $S_V \subseteq [N]$ such that $1 \leq |S_V| \leq 5$. Then it gives $(\widehat{x},\widehat{z})$ to the prover as a proving key and gives $\{(\widehat{x}_j,\widehat{z}_j)\}_{j\in S_V}$ to the verifier as a verification key where $\widehat{x}_j$ and $\widehat{z}_j$ denote the j-th bits of $\widehat{x}$ and $\widehat{z}$, respectively. The prover generates the history state ρ_{hist} and sends $\rho' = X^{\widehat{x}}Z^{\widehat{z}}\rho_{\mathrm{hist}}Z^{\widehat{z}}X^{\widehat{x}}$ to the verifier as a proof. The verifier then measures each qubit as is done in the posthoc verification protocol. This needs the quantum verifier, but as we have explained, we can make the verifier classical by using the teleportation technique.

An intuitive explanation of why it is zero-knowledge is that the verifier can access at most five qubits of the history state, because other qubits are quantum one-time padded. Due to the local simulatability of the history state, the information that the verifier gets can be classically simulated without the witness. This results in our classically verifiable NIZK for **QMA** in the QSP model. In our QSP model, the trusted setup sends random Pauli basis states to the prover and their classical description to the verifier. Furthermore, the trusted setup also sends randomly chosen $(\widehat{x},\widehat{z}) \xleftarrow{\$} \{0,1\}^N \times \{0,1\}^N$ to the prover, and $\{(\widehat{x}_j,\widehat{z}_j)\}_{j\in S_V}$ to the verifier with randomly chosen subset S_V.

Classically verifiable NIZK for QMA in the CRS + $(V \to P)$ model. We want to reduce the trust in the setup, so let us first examine what happens if the verifier runs the setup as preprocessing. Unfortunately, such a construction is not zero-knowledge since the verifier can know whole bits of $(\widehat{x},\widehat{z})$ and thus it may obtain information of qubits of ρ_{hist} that are outside of S_V, in which case we cannot rely on the local simulatability. Therefore, for ensuring the zero-knowledge property, we have to make sure that the verifier only knows $\{(\widehat{x}_j,\widehat{z}_j)\}_{j\in S_V}$. Then suppose that the prover chooses $(\widehat{x},\widehat{z})$ whereas other setups are still done by the verifier. Here, the problem is how to let the verifier know $\{(\widehat{x}_j,\widehat{z}_j)\}_{j\in S_V}$. A naive

[5] There is a subtle issue that the probability depends on the number of qubits on which P_i non-trivially acts. We adjust this by an additional biased coin flipping.

solution is that the verifier sends S_V to the prover and then the prover returns $\{(\widehat{x}_j, \widehat{z}_j)\}_{j \in S_V}$. However, such a construction is not sound since it is essential that the prover "commits" to a single quantum state independently of S_V when reducing soundness to the local Hamiltonian problem. So what we need is a protocol between the prover and verifier where the verifier only gets $\{(\widehat{x}_j, \widehat{z}_j)\}_{j \in S_V}$ and the prover does not learn S_V. We observe that this is exactly the functionality of 5-*out-of-N oblivious transfer* [BCR87].

Though it may sound easy to solve the problem by just using a known two-round 5-out-of-N oblivious transfer, there is still some subtlety. For example, if we use an oblivious transfer that satisfies only indistinguishability-based notion of receiver's security (e.g., [NP01, BD18]),[6] which just says that the sender cannot know indices chosen by the receiver, we cannot prove soundness. Intuitively, this is because the indistinguishability-based receiver's security does not prevent a malicious sender from generating a malicious message such that the message derived on the receiver's side depends on the chosen indices, which does not force the prover to "commit" to a single state.

If we use a *fully-simulatable* [Lin08] oblivious transfer, the above problem does not arise and we can prove both soundness and zero-knowledge. However, the problem is that we are not aware of any efficient fully-simulatable 5-out-of-N oblivious transfer based on post-quantum assumptions (in the CRS model). The LWE-based construction of [PVW08] does not suffice for our purpose since a CRS can be reused only a bounded number of times in their construction. Recently, Quach [Qua20] resolved this issue, and proposed an efficient fully-simulatable 1-out-of-2 oblivious transfer based on the LWE assumption.[7] We can extend his construction to a fully-simulatable 1-out-of-N oblivious transfer efficiently. However, we do not know how to convert this into 5-out-of-N one efficiently without losing the full-simulatability. We note that a conversion from 1-out-of-N to 5-out-of-N oblivious transfer by a simple 5-parallel repetition loses the full-simulatability against malicious senders since a malicious sender can send different inconsistent messages in different sessions, which should be considered as an attack against the full-simulatability. One possible way to prevent such an inconsistent message attack is to let the sender prove that the messages in all sessions are consistent by using (post-quantum) CRS-NIZK for **NP** [PS19]. However, such a construction is very inefficient since it uses the underlying 1-out-of-N oblivious transfer in a non-black-box manner, which we want to avoid.

We note that the parallel repetition construction preserves indistinguishability-based receiver's security and fully-simulatable sender's security for two-round protocols. Therefore, we have an efficient (black-box) construction of 5-out-of-N oblivious transfer if we relax the receiver's security to the indistinguishability-based one. As already explained, such a security does not suffice for proving soundness. To resolve this issue, we add an additional mechanism to force the prover to "commit" to a single state. Specifically, instead of directly sending

[6] The indistinguishability-based receiver's security is also often referred to as half-simulation security [CNs07].

[7] Actually, his construction satisfies a stronger UC-security [Can20, PVW08].

(x, z) by a 5-out-of-N oblivious transfer, the prover sends a commitment of (x, z) and then sends (x, z) and the corresponding randomness used in the commitment by a 5-out-of-N oblivious transfer. When the verifier receives $\{x_j, z_j\}_{j \in S_V}$ and corresponding randomness, it checks if it is consistent to the commitment by recomputing it, and immediately rejects if not. This additional mechanism prevents a malicious prover's inconsistent behavior, which resolves the problem in the proof of soundness.

Finally, our construction satisfies the dual-mode property if we assume appropriate dual-mode properties for building blocks. A dual-mode oblivious transfer (in the CRS model) has two modes of generating a CRS and it satisfies statistical (indistinguishability-based) receiver's security in one mode and statistical (full-simulation-based) sender's security in the other mode. The construction of [Qua20] is an instantiation of a 1-out-of-2 oblivious transfer with such a dual-mode property, and this can be converted into 5-out-of-N one as explained above. We stress again that it is important to relax the receiver's security to the indistinguishability-based one to make the conversion work. A dual-mode commitment (in the CRS model) has two modes of generating a CRS and it is statistically binding in one mode and statistically hiding in the other mode. We can use lossy encryption [BHY09, Reg09] as an instantiation of such a dual-mode commitment. Both of dual-mode 5-out-of-N oblivious transfer and lossy encryption are based on the LWE assumption (with super-polynomial modulus for the former) and fairly efficient in the sense that they do not rely on non-black-box techniques. Putting everything together, we obtain a fairly efficient (black-box) construction of a dual-mode NIZK for **QMA** in the CRS + $(V \to P)$ model.

NIZK for **QMA** *via Fiat-Shamir transformation.* Finally, let us explain our construction of NIZK for **QMA** via the Fiat-Shamir transformation. It is based on so-called the Ξ-protocol for **QMA** [BG20], which is equal to the standard Σ-protocol except that the first message is quantum. Because the first message is quantum, the Fiat-Shamir technique cannot be directly applied. Our idea is again to use the teleportation technique: if we introduce a setup that sends random Pauli basis states to the prover and their classical description to the verifier, the first message can be classical. We thus obtain a (classical) Σ-protocol in the QSP model, where the trusted setup sends random Pauli basis states to the prover and their classical description to the verifier. This task can be, actually, done by the verifier, not the trusted setup, unlike our first construction. We therefore obtain a (classical) Σ-protocol with quantum preprocessing (Definition 5.2), where the verifier sends random Pauli basis states to the prover as the preprocessing.

We then apply the (classical) Fiat-Shamir transformation to the Σ-protocol with quantum preprocessing, and obtain the CV-NIZK for **QMA** in the quantum random oracle plus $V \to P$ model (Definition 5.1), where $V \to P$ means the communication from the verifier to the prover as the preprocessing. Note that we are considering a classical Σ-protocol with quantum preprocessing differently from previous works. By a close inspection, we show that an existing security proof for classical Σ-protocol in the QROM [DFM20] also works in our setting.

Importantly, in this case, unlike the previous two constructions, the quantum preprocessing can be replaced with the setup that distributes Bell pairs among the prover and the verifier. As a corollary, we therefore obtain NIZK for **QMA** in the shared Bell pair model (plus quantum random oracle). The distribution of Bell pairs by a trusted setup can be considered as a "quantum analogue" of the CRS, and therefore we can say that we obtain NIZK for **QMA** in the "quantum CRS" model via the Fiat-Sharmir transformation.

2 Preliminaries

2.1 Quantum Computation Preliminaries

Here, we briefly review basic notations and facts on quantum computations.

For any quantum state ρ over registers $\mathbf{A}$ and $\mathbf{B}$, $\mathrm{Tr}_{\mathbf{A}}(\rho)$ is the partial trace of ρ over $\mathbf{A}$. We use I to mean the identity operator. (For simplicity, we use the same I for all identity operators with different dimensions, because the dimension of an identity operator is clear from the context.) We use X, Y, and Z to mean Pauli operators i.e., $X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $Y := iXZ$. We use H to mean Hadamard operator, i.e., $H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. We also define the T operator by $T := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$. The $CNOT := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ is the controlled-NOT operator.

We define $V(Z) := I$, $V(X) := H$, and $V(Y) := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$ so that for each $W \in \{X, Y, Z\}$, $V(W)|0\rangle$ and $V(W)|1\rangle$ are the eigenvectors of W with eigenvalues $+1$ and -1, respectively. For each $W \in \{X, Y, Z\}$, we call $\{V(W)|0\rangle, V(W)|1\rangle\}$ the W-basis.

When we consider an N-qubit system, for a Pauli operator $Q \in \{X, Y, Z\}$, Q_j denotes the operator that acts on j-th qubit as Q and trivially acts on all the other qubits. Similarly, $V_j(W)$ denotes the operator that acts on j-th qubit as $V(W)$ and trivially acts on all the other qubits. For any $x \in \{0,1\}^N$ and $z \in \{0,1\}^N$, $X^x Z^z$ means $\prod_{j=1}^N X_j^{x_j} Z_j^{z_j}$.

We call the state $\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$ the Bell pair. We call the set $\{|\phi_{x,z}\rangle\}_{(x,z)\in\{0,1\}^2}$ the Bell basis where $|\phi_{x,z}\rangle := (X^x Z^z \otimes I)\frac{|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle}{\sqrt{2}}$. Let us define $U(X) := V(X)$, $U(Y) := V(Y)X$, and $U(Z) := V(Z)$.

Lemma 2.1 (State Collapsing). *If we project one qubit of a Bell pair onto $V(W)|m\rangle$ with $W \in \{X, Y, Z\}$ and $m \in \{0, 1\}$, the other qubit collapses to $U(W)|m\rangle$.*

Lemma 2.2 (Effect of $X^x Z^z$ before measurement). *For any N-qubit state ρ, $(W_1, ..., W_N) \in \{X, Y, Z\}^N$, and $(x, z) \in \{0,1\}^N \times \{0,1\}^N$, the distributions of $(m'_1, ...m'_n)$ sampled in the following two ways are identical.*

1. *For $j \in [N]$, measure j-th qubit of ρ in W_j basis, let $m_j \in \{0,1\}$ be the outcome, and set*

$$m'_j := \begin{cases} m_j \oplus x_j & (W_j = Z), \\ m_j \oplus z_j & (W_j = X), \\ m_j \oplus x_j \oplus z_j & (W_j = Y). \end{cases}$$

2. *For $j \in [N]$, measure j-th qubit of $X^x Z^z \rho Z^z X^x$ in W_j basis and let $m'_j \in \{0,1\}$ be the outcome.*

The proofs of the above lemmas are straightforward. The following lemma is implicit in previous works, e.g., [MNS18, FHM18].

Lemma 2.3. *Let $\mathcal{H} := \frac{1}{2}\left[I + s(\prod_{j\in S_X} X_j)(\prod_{j\in S_Y} Y_j)(\prod_{j\in S_Z} Z_j)\right]$ be an N-qubit projection operator, where $s \in \{+1,-1\}$, and S_X, S_Y, and S_Z are disjoint subsets of $[N]$. For any N-qubit quantum state ρ, suppose that for all $j \in S_W$, where $W \in \{X,Y,Z\}$, we measure j-th qubit of ρ in the W-basis, and let $m_j \in \{0,1\}$ be the outcome. Then we have $\Pr\left[(-1)^{\bigoplus_{j\in S_X\cup S_Y\cup S_Z} m_j} = -s\right] = 1 - \mathrm{Tr}(\rho\mathcal{H})$.*

2.2 QMA and Local Hamiltonian Problem

For any **QMA** promise problem $L = (L_{\mathsf{yes}}, L_{\mathsf{no}})$ and $\mathtt{x} \in L_{\mathsf{yes}}$, we denote by $R_L(\mathtt{x})$ to mean the (possibly infinite) set of all quantum states $\mathtt{w}$ such that $\Pr[V(\mathtt{x},\mathtt{w}) = 1] \geq 2/3$.

Recently, Broadbent and Grilo [BG20] showed that any **QMA** problem can be reduced to a 5-local Hamiltonian problem with *local simulatability*. (See also [GSY19].) Moreover, it is easy to see that we can make the Hamiltonian $\mathcal{H}_{\mathtt{x}}$ be of the form $\mathcal{H}_{\mathtt{x}} = \sum_{i=1}^M p_i \frac{I+s_iP_i}{2}$ where $s_i \in \{+1,-1\}$, $p_i \geq 0$, $\sum_{i=1}^M p_i = 1$, and P_i is a tensor product of Pauli operators (I,X,Z,Y) with at most 5 nontrivial Pauli operators (X,Y,Z). Then we have the following lemma.

Lemma 2.4 (QMA-completeness of 5-local Hamiltonian problem with local simulatability [BG20]). *For any* **QMA** *promise problem $L = (L_{\mathsf{yes}}, L_{\mathsf{no}})$, there is a classical polynomial-time computable deterministic function that maps $\mathtt{x} \in \{0,1\}^*$ to an N-qubit Hamiltonian $\mathcal{H}_{\mathtt{x}}$ of the form $\mathcal{H}_{\mathtt{x}} = \sum_{i=1}^M p_i \frac{I+s_iP_i}{2}$, where $N = \mathsf{poly}(|\mathtt{x}|)$, $M = \mathsf{poly}(|\mathtt{x}|)$, $s_i \in \{+1,-1\}$, $p_i > 0$, $\sum_{i=1}^M p_i = 1$, and P_i is a tensor product of Pauli operators (I,X,Y,Z) with at most 5 nontrivial Pauli operators (X,Y,Z), and satisfies the following: There are $0 < \alpha < \beta < 1$ such that $\beta - \alpha = 1/\mathsf{poly}(|\mathtt{x}|)$ and*

- *if $\mathtt{x} \in L_{\mathsf{yes}}$, then there exists an N-qubit state ρ such that $\mathrm{Tr}(\rho\mathcal{H}_{\mathtt{x}}) \leq \alpha$, and*
- *if $\mathtt{x} \in L_{\mathsf{no}}$, then for any N-qubit state ρ, we have $\mathrm{Tr}(\rho\mathcal{H}_{\mathtt{x}}) \geq \beta$.*

Moreover, for any $\mathtt{x} \in L_{\mathsf{yes}}$, we can convert any witness $\mathtt{w} \in R_L(\mathtt{x})$ into a state ρ_{hist}, called the history state, such that $\mathrm{Tr}(\rho_{\mathrm{hist}}\mathcal{H}_{\mathtt{x}}) \leq \alpha$ in quantum polynomial time. Moreover, there exists a classical deterministic polynomial time algorithm $\mathsf{Sim}_{\mathrm{hist}}$ such that for any $\mathtt{x} \in L_{\mathsf{yes}}$ and any subset $S \subseteq [N]$ with $|S| \leq 5$,

$\mathsf{Sim}_{\mathrm{hist}}(\mathtt{x}, S)$ *outputs a classical description of an* $|S|$*-qubit density matrix* ρ_S *such that* $\|\rho_S - \mathrm{Tr}_{[N]\setminus S}\rho_{\mathrm{hist}}\|_{tr} = \mathsf{negl}(\lambda)$ *where* $\mathrm{Tr}_{[N]\setminus S}\rho_{\mathrm{hist}}$ *is the state of* ρ_{hist} *in registers corresponding to* S *tracing out all other registers.*

2.3 Classically-Verifiable Non-Interactive Zero-knowledge Proofs

Definition 2.1 (CV-NIZK in the QSP model). *A classically-verifiable non-interactive zero-knowledge proof (CV-NIZK) for a* **QMA** *promise problem* $L = (L_{\mathsf{yes}}, L_{\mathsf{no}})$ *in the quantum secret parameter (QSP) model consists of algorithms* $\Pi = (\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$ *with the following syntax:*

$\mathsf{Setup}(1^\lambda)$**:** *This is a QPT algorithm that takes the security parameter* 1^λ *as input and outputs a quantum proving key* k_P *and a classical verification key* k_V*.*

$\mathsf{Prove}(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$**:** *This is a QPT algorithm that takes the proving key* k_P*, a statement* $\mathtt{x}$*, and* $k = \mathsf{poly}(\lambda)$ *copies* $\mathtt{w}^{\otimes k}$ *of a witness* $\mathtt{w} \in R_L(\mathtt{x})$ *as input and outputs a classical proof* π*.*

$\mathsf{Verify}(k_V, \mathtt{x}, \pi)$**:** *This is a PPT algorithm that takes the verification key* k_V*, a statement* $\mathtt{x}$*, and a proof* π *as input and outputs* $\top$ *indicating acceptance or* $\bot$ *indicating rejection.*

We require Π *to satisfy the following properties for some* $0 < s < c < 1$ *such that* $c - s > 1/\mathsf{poly}(\lambda)$*. Especially, when we do not specify* c *and* s*, they are set as* $c = 1 - \mathsf{negl}(\lambda)$ *and* $s = \mathsf{negl}(\lambda)$*.*

***c*-Completeness.** *For all* $\mathtt{x} \in L_{\mathsf{yes}} \cap \{0,1\}^\lambda$*, and* $\mathtt{w} \in R_L(\mathtt{x})$*, we have*

$$\Pr\left[\mathsf{Verify}(k_V, \mathtt{x}, \pi) = \top : (k_P, k_V) \xleftarrow{\$} \mathsf{Setup}(1^\lambda), \pi \xleftarrow{\$} \mathsf{Prove}(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})\right] \geq c.$$

***(Adaptive Statistical) s*-Soundness.** *For all unbounded-time adversary* $\mathcal{A}$*, we have*

$$\Pr\left[\mathtt{x} \in L_{\mathsf{no}} \wedge \mathsf{Verify}(k_V, \mathtt{x}, \pi) = \top : (k_P, k_V) \xleftarrow{\$} \mathsf{Setup}(1^\lambda), (\mathtt{x}, \pi) \xleftarrow{\$} \mathcal{A}(k_P)\right] \leq s.$$

(Adaptive Statistical Single-Theorem) Zero-Knowledge. *There exists a PPT simulator* Sim *such that for any unbounded-time distinguisher* $\mathcal{D}$*, we have*

$$\left|\Pr\left[\mathcal{D}^{\mathcal{O}_P(k_P,\cdot,\cdot)}(k_V) = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{O}_S(k_V,\cdot,\cdot)}(k_V) = 1\right]\right| = \mathsf{negl}(\lambda)$$

where $(k_P, k_V) \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$*,* $\mathcal{D}$ *can make at most one query, which should be of the form* $(\mathtt{x}, \mathtt{w}^{\otimes k})$ *where* $\mathtt{w} \in R_L(\mathtt{x})$ *and* $\mathtt{w}^{\otimes k}$ *is unentangled with* $\mathcal{D}$*'s internal registers,*[8] $\mathcal{O}_P(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$ *returns* $\mathsf{Prove}(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$*, and* $\mathcal{O}_S(k_V, \mathtt{x}, \mathtt{w}^{\otimes k})$ *returns* $\mathsf{Sim}(k_V, \mathtt{x})$*.*

[8] Though our protocols are likely to remain secure even if they can be entangled, we assume that they are unentangled for simplicity. To the best of our knowledge, none of existing works on interactive or non-interactive zero-knowledge for **QMA** [BJSW20, CVZ20, BS20, BG20, Shm21, BCKM21] considered entanglement between a witness and distinguisher's internal register.

It is easy to see that we can amplify the gap between completeness and soundness thresholds by a simple parallel repetition. Moreover, we can see that this does not lose the zero-knowledge property. Therefore, we have the following lemma.

Lemma 2.5 (Gap Amplification for CV-NIZK). *If there exists a CV-NIZK for L in the QSP model that satisfies c-completeness and s-soundness, for some $0 < s < c < 1$ such that $c - s > 1/\mathsf{poly}(\lambda)$, then there exists a CV-NIZK for L in the QSP model (with $(1 - \mathsf{negl}(\lambda))$-completeness and $\mathsf{negl}(\lambda)$-soundness).*

3 CV-NIZK in the QSP model

In this section, we construct a CV-NIZK in the QSP model (Definition 2.1). Specifically, we prove the following theorem.

Theorem 3.1. *There exists a CV-NIZK for* **QMA** *in the QSP model (without any computational assumption).*

Our construction of a CV-NIZK for a **QMA** promise problem L is given in Figure 1 where $\mathcal{H}_{\mathbf{x}}$, N, M, p_i, s_i, P_i, α, β, and ρ_{hist} are as in Lemma 2.4 for L and $V_j(W_j)$ is as defined in Section 2.1.

To show Theorem 3.1, we prove the following lemmas.

Lemma 3.1 (Completeness and Soundness). *Π_{NIZK} satisfies $\left(1 - \frac{\alpha}{N'}\right)$-completeness and $\left(1 - \frac{\beta}{N'}\right)$-soundness where $N' := 3^5 \sum_{i=1}^{5} \binom{N}{i}$.*

Lemma 3.2 (Zero-Knowledge). *Π_{NIZK} satisfies the zero-knowledge property.*

Since $\left(1 - \frac{\alpha}{N'}\right) - \left(1 - \frac{\beta}{N'}\right) = \frac{\beta - \alpha}{N'} \geq 1/\mathsf{poly}(\lambda)$, by combining Lemmas 2.5, 3.1 and 3.2, Theorem 3.1 follows.

In the following, we give proofs of Lemmas 3.1 and 3.2.

Proof of Lemma 3.1. We prove this lemma by considering virtual protocols that do not change completeness and soundness. First, we consider the virtual protocol 1 described in Figure 2. There are two differences from the original protocol. The first is that k_V includes the whole $(\widehat{x}, \widehat{z})$ instead of $\{\widehat{x}_j, \widehat{z}_j\}_{j \in S_V}$. This difference does not change the (possibly malicious) prover's view since k_V is not given to the prover. The second is that the setup algorithm generates N Bell pairs and gives each halves to the prover and verifier, and the verifier obtains $(m_1, ..., m_N)$ by measuring his halves in Pauli basis. Because the verifier's measurement and the prover's measurement commute with each other, in the virtual protocol 1, the verifier's acceptance probability does not change even if the verifier chooses $(W_1, ..., W_N)$ and measures ρ_V in the corresponding basis to obtain outcomes $(m_1, ..., m_N)$ before ρ_P is given to the prover. Moreover, conditioned on the above measurement outcomes, the state in $\mathbf{P}$ collapses to $\bigotimes_{j=1}^{N}(U(W_j)|m_j\rangle)$ (See Lemma 2.1). Therefore, the virtual protocol 1 is exactly the same as the original protocol from the prover's view, and the verifier's acceptance probability

$\mathsf{Setup}(1^\lambda)$: The setup algorithm chooses $(W_1, ..., W_N) \xleftarrow{\$} \{X, Y, Z\}^N$, $(m_1, ..., m_N) \xleftarrow{\$} \{0,1\}^N$, $(\widehat{x}, \widehat{z}) \xleftarrow{\$} \{0,1\}^N \times \{0,1\}^N$, and a uniformly random subset $S_V \subseteq [N]$ such that $1 \leq |S_V| \leq 5$, and outputs a proving key $k_P := \left(\rho_P := \bigotimes_{j=1}^N (U(W_j)|m_j\rangle), \widehat{x}, \widehat{z}\right)$ and a verification key $k_V := (W_1, ..., W_N, m_1, ..., m_N, S_V, \{\widehat{x}_j, \widehat{z}_j\}_{j \in S_V})$.

$\mathsf{Prove}(k_P, \mathtt{x}, \mathtt{w})$: The proving algorithm parses $(\rho_P, \widehat{x}, \widehat{z}) \leftarrow k_P$, generates the history state ρ_{hist} for $\mathcal{H}_{\mathtt{x}}$ from $\mathtt{w}$, and computes $\rho'_{\mathrm{hist}} := X^{\widehat{x}} Z^{\widehat{z}} \rho_{\mathrm{hist}} Z^{\widehat{z}} X^{\widehat{x}}$. It measures j-th qubits of ρ'_{hist} and ρ_P in the Bell basis for $j \in [N]$. Let $x := x_1 \| x_2 \| ... \| x_N$, and $z := z_1 \| z_2 \| ... \| z_N$ where $(x_j, z_j) \in \{0,1\}^2$ denotes the outcome of j-th measurement. It outputs a proof $\pi := (x, z)$.

$\mathsf{Verify}(k_V, \mathtt{x}, \pi)$: The verification algorithm parses $(W_1, ..., W_N, m_1, ..., m_N, S_V, \{\widehat{x}_j, \widehat{z}_j\}_{j \in S_V}) \leftarrow k_V$ and $(x, z) \leftarrow \pi$, chooses $i \in [M]$ according to the probability distribution defined by $\{p_i\}_{i \in [M]}$ (i.e., chooses i with probability p_i). Let

$$S_i := \{j \in [N] \mid j\text{th Pauli operator of } P_i \text{ is not } I\}.$$

We note that we have $1 \leq |S_i| \leq 5$ by the 5-locality of $\mathcal{H}_{\mathtt{x}}$. We say that P_i is consistent to $(S_V, \{W_j\}_{j \in S_V})$ if and only if $S_i = S_V$ and the jth Pauli operator of P_i is W_j for all $j \in S_i$. If P_i is not consistent to $(S_V, \{W_j\}_{j \in S_V})$, it outputs $\top$. If P_i is consistent to $(S_V, \{W_j\}_{j \in S_V})$, it flips a biased coin that heads with probability $1 - 3^{|S_i|-5}$. If heads, it outputs $\top$. If tails, it defines

$$m'_j := \begin{cases} m_j \oplus x_j \oplus \hat{x}_j & (W_j = Z), \\ m_j \oplus z_j \oplus \hat{z}_j & (W_j = X), \\ m_j \oplus x_j \oplus \hat{x}_j \oplus z_j \oplus \hat{z}_j & (W_j = Y) \end{cases}$$

for $j \in S_i$, and outputs $\top$ if $(-1)^{\bigoplus_{j \in S_i} m'_j} = -s_i$ and $\bot$ otherwise.

Fig. 1. CV-NIZK Π_{NIZK} in the QSP model.

of the virtual protocol 1 is the same as that of the original protocol Π_{NIZK} for any possibly malicious prover.

Next, we further modify the protocol to define the virtual protocol 2 described in Figure 3. The difference from the virtual protocol 1 is that instead of setting m'_j, the verification algorithm applies a corresponding Pauli $X^{x \oplus \widehat{x}} Z^{z \oplus \widehat{z}}$ on ρ_V, and then measures it to obtain m'_j. By Lemma 2.2, this does not change the distribution of $(m'_1, ..., m'_N)$. Therefore, the verifier's acceptance probability of the virtual protocol 2 is the same as that of the virtual protocol 1 for any possibly malicious prover.

Therefore, it suffices to prove $(1 - \frac{\alpha}{N'})$-completeness and $(1 - \frac{\beta}{N'})$-soundness for the virtual protocol 2. When $\mathtt{x} \in L_{\mathsf{yes}}$ and π is honestly generated, then ρ'_V is the history state ρ_{hist}, which satisfies $\mathrm{Tr}(\rho_{\mathrm{hist}} \mathcal{H}_{\mathtt{x}}) \leq \alpha$, by the correctness of quantum teleportation. For any fixed P_i, the probability that P_i is consis-

$\mathsf{Setup}_{\mathsf{vir\text{-}1}}(1^\lambda)$: The setup algorithm generates N Bell-pairs between registers $\mathbf{P}$ and $\mathbf{V}$ and lets ρ_P and ρ_V be quantum states in registers $\mathbf{P}$ and $\mathbf{V}$, respectively. It chooses $(\widehat{x},\widehat{z}) \xleftarrow{\$} \{0,1\}^N \times \{0,1\}^N$. It chooses a uniformly random subset $S_V \subseteq [N]$ such that $1 \leq |S_V| \leq 5$, and outputs a proving key $k_P := (\rho_P, \widehat{x}, \widehat{z})$ and a verification key $k_V := (\rho_V, S_V, \widehat{x}, \widehat{z})$.

$\mathsf{Prove}_{\mathsf{vir\text{-}1}}(k_P, \mathtt{x}, \mathtt{w})$: This is the same as $\mathsf{Prove}(k_P, \mathtt{x}, \mathtt{w})$ in Figure 1.

$\mathsf{Verify}_{\mathsf{vir\text{-}1}}(k_V, \mathtt{x}, \pi)$: The verification algorithm chooses $(W_1, ..., W_N) \xleftarrow{\$} \{X, Y, Z\}^N$, and measures j-th qubit of ρ_V in the W_j basis for all $j \in [N]$, and lets $(m_1, ..., m_N)$ be the measurement outcomes. The rest of this algorithm is the same as $\mathsf{Verify}(k_V, \mathtt{x}, \pi)$ given in Figure 1.

Fig. 2. The virtual protocol 1 for Π_{NIZK}

$\mathsf{Setup}_{\mathsf{vir\text{-}2}}(1^\lambda)$: This is the same as $\mathsf{Setup}_{\mathsf{vir\text{-}1}}(1^\lambda)$ in Figure 2.

$\mathsf{Prove}_{\mathsf{vir\text{-}2}}(k_P, \mathtt{x}, \mathtt{w})$: This is the same as $\mathsf{Prove}(k_P, \mathtt{x}, \mathtt{w})$ in Figure 1.

$\mathsf{Verify}_{\mathsf{vir\text{-}2}}(k_V, \mathtt{x}, \pi)$: The verification algorithm parses $(\rho_V, S_V, \widehat{x}, \widehat{z}) \leftarrow k_V$ and $(x, z) \leftarrow \pi$, computes $\rho'_V := X^{x\oplus\widehat{x}} Z^{z\oplus\widehat{z}} \rho_V Z^{z\oplus\widehat{z}} X^{x\oplus\widehat{x}}$, chooses $(W_1, ..., W_N) \xleftarrow{\$} \{X, Y, Z\}^N$, measures j-th qubit of ρ'_V in the W_j basis for all $j \in [N]$, and lets $(m'_1, ..., m'_N)$ be the measurement outcomes.
It chooses $i \in [M]$ and defines $S_i \subseteq [N]$ similarly to $\mathsf{Verify}(k_V, \mathtt{x}, \pi)$ in Figure 1. If P_i is not consistent to $(S_V, \{W_j\}_{j\in S_V})$, it outputs $\top$. If P_i is consistent to $(S_V, \{W_j\}_{j\in S_V})$, it flips a biased coin that heads with probability $1 - 3^{|S_i|-5}$. If heads, it outputs $\top$. If tails, it outputs $\top$ if $(-1)^{\bigoplus_{j\in S_i} m'_j} = -s_i$ and $\bot$ otherwise.

Fig. 3. The virtual protocol 2 for Π_{NIZK}

tent to $(S_V, \{W_j\}_{j\in S_V})$ and the coin tails is $\frac{1}{N'}$. Therefore, by Lemma 2.3 and Lemma 2.4, the verifier's acceptance probability is $1 - \frac{1}{N'}\mathrm{Tr}(\rho_{\mathrm{hist}}\mathcal{H}_{\mathtt{x}}) \geq 1 - \frac{\alpha}{N'}$.

Let $\mathcal{A}$ be an adaptive adversary against soundness of virtual protocol 2. That is, $\mathcal{A}$ is given k_P and outputs $(\mathtt{x}, \pi)$. We say that $\mathcal{A}$ wins if $\mathtt{x} \in L_{\mathsf{no}}$ and $\mathsf{Verify}(k_V, \mathtt{x}, \pi) = \top$. For any $\mathtt{x}$, let $\mathsf{E}_{\mathtt{x}}$ be the event that the statement output by $\mathcal{A}$ is $\mathtt{x}$, and $\rho'_{V,\mathtt{x}}$ be the state in $\mathbf{V}$ right before the measurement by Verify conditioned on $\mathsf{E}_{\mathtt{x}}$. Similarly to the analysis for the completeness, by Lemma 2.3 and Lemma 2.4, we have

$$\Pr[\mathcal{A}\text{ wins}] = \sum_{\mathtt{x}\in L_{\mathsf{no}}} \Pr[\mathsf{E}_{\mathtt{x}}] \left(1 - \frac{1}{N'}\mathrm{Tr}(\rho'_{V,\mathtt{x}}\mathcal{H}_{\mathtt{x}})\right) \leq \sum_{\mathtt{x}\in L_{\mathsf{no}}} \Pr[\mathsf{E}_{\mathtt{x}}] \left(1 - \frac{\beta}{N'}\right) \leq 1 - \frac{\beta}{N'}.$$

Proof of Lemma 3.2. We describe the simulator Sim below.

$\mathsf{Sim}(k_V, \mathtt{x})$: The simulator parses $(W_1, ..., W_N, m_1, ..., m_N, S_V, \{\widehat{x}_j, \widehat{z}_j\}_{j\in S_V}) \leftarrow k_V$ and does the following.

1. Generate the classical description of the density matrix $\rho_{S_V} := \mathsf{Sim}_{\mathrm{hist}}(\mathtt{x}, S_V)$ where $\mathsf{Sim}_{\mathrm{hist}}$ is as in Lemma 2.4.
2. Sample $\{x_j, z_j\}_{j\in S_V}$ according to the probability distribution of outcomes of the Bell-basis measurements of the corresponding pairs of qubits of $\left(\prod_{j\in S_V} X_j^{\widehat{x}_j} Z_j^{\widehat{z}_j}\right) \rho_{S_V} \left(\prod_{j\in S_V} Z_j^{\widehat{z}_j} X_j^{\widehat{x}_j}\right)$ and $\bigotimes_{j\in S_V}(U(W_j)\,|m_j\rangle)$. We emphasize that this measurement can be simulated in a classical probabilistic polynomial time since $|S_V| \leq 5$.
3. Choose $(x_j, z_j) \xleftarrow{\$} \{0,1\}^2$ for all $j \in [N] \setminus S_V$.
4. Output $\pi := (x, z)$ where $x := x_1\|x_2\|...\|x_N$ and $z := z_1\|z_2\|...\|z_N$.

We prove that the output of this simulator is indistinguishable from the real proof. For proving this, we consider the following sequences of modified simulators. We note that these simulators may perform quantum computations unlike the real simulator.

$\mathsf{Sim}_1(k_V, \mathtt{x})$**:** The simulator parses $(W_1, ..., W_N, m_1, ..., m_N, S_V, \{\widehat{x}_j, \widehat{z}_j\}_{j\in S_V}) \leftarrow k_V$ and does the following.

1. Generate the classical description of the density matrix $\rho_{S_V} := \mathsf{Sim}_{\mathrm{hist}}(\mathtt{x}, S_V)$ where $\mathsf{Sim}_{\mathrm{hist}}$ is as in Lemma 2.4. (This step is the same as the step 1 of $\mathsf{Sim}(k_V, \mathtt{x})$.)
2. Generate $\widetilde{\rho'}_{\mathrm{hist}} := \left(\prod_{j\in S_V} X_j^{\widehat{x}_j} Z_j^{\widehat{z}_j}\right) \rho_{S_V} \left(\prod_{j\in S_V} Z_j^{\widehat{z}_j} X_j^{\widehat{x}_j}\right) \otimes \frac{I_{[N]\setminus S_V}}{2^{|[N]\setminus S_V|}}$.
3. Measure j-th qubits of $\widetilde{\rho'}_{\mathrm{hist}}$ and $\rho_P := \bigotimes_{j=1}^N (U(W_j)|m_j\rangle)$ in the Bell basis for $j \in [N]$, and let (x_j, z_j) be the j-th measurement result.
4. Output $\pi := (x, z)$ where $x := x_1\|x_2\|...\|x_N$ and $z := z_1\|z_2\|...\|z_N$.

Clearly, the distributions of $\{x_j, z_j\}_{j\in S_V}$ output by $\mathsf{Sim}(k_V, \mathtt{x})$ and $\mathsf{Sim}_1(k_V, \mathtt{x})$ are the same. Moreover, the distributions of $\{x_j, z_j\}_{j\in[N]\setminus S_V}$ output by $\mathsf{Sim}(k_V, \mathtt{x})$ and $\mathsf{Sim}_1(k_V, \mathtt{x})$ are both uniformly and independently random. Therefore, output distributions of $\mathsf{Sim}(k_V, \mathtt{x})$ and $\mathsf{Sim}_1(k_V, \mathtt{x})$ are exactly the same.

Next, we consider the following modified simulator that takes a witness $\mathtt{w} \in R_L(\mathtt{x})$ as input.

$\mathsf{Sim}_2(k_V, \mathtt{x}, \mathtt{w})$**:** The simulator parses $(W_1, ..., W_N, m_1, ..., m_N, S_V, \{\widehat{x}_j, \widehat{z}_j\}_{j\in S_V}) \leftarrow k_V$ and does the following.

1. Generate the history state ρ_{hist} for $\mathcal{H}_{\mathtt{x}}$ from $\mathtt{w}$.
2. Generate $(\widehat{x}_j, \widehat{z}_j) \xleftarrow{\$} \{0,1\}^2$ for $j \in [N] \setminus S_V$ and let $\widehat{x} := \widehat{x}_1\|...\|\widehat{x}_N$ and $\widehat{z} := \widehat{z}_1\|...\|\widehat{z}_N$.
3. Compute $\rho'_{\mathrm{hist}} := X^{\widehat{x}} Z^{\widehat{z}} \rho_{\mathrm{hist}} Z^{\widehat{z}} X^{\widehat{x}}$.
4. Measure j-th qubits of ρ'_{hist} and $\rho_P := \bigotimes_{j=1}^N (U(W_j)|m_j\rangle)$ in the Bell basis for $j \in [N]$, and let (x_j, z_j) be the j-th measurement result.
5. Output $\pi := (x, z)$ where $x := x_1\|x_2\|...\|x_N$ and $z := z_1\|z_2\|...\|z_N$.

We have $\rho'_{\mathrm{hist}} = \left(\prod_{j\in S_V} X_j^{\widehat{x}_j} Z_j^{\widehat{z}_j}\right) \mathrm{Tr}_{N\setminus S_V}[\rho_{\mathrm{hist}}] \left(\prod_{j\in S_V} Z_j^{\widehat{z}_j} X_j^{\widehat{x}_j}\right) \otimes \frac{I_{[N]\setminus S_V}}{2^{|[N]\setminus S_V|}}$ from the view of a distinguisher that has no information on $\{\widehat{x}_j, \widehat{z}_j\}_{j\in[N]\setminus S_V}$. By Lemma 2.4, we have $\|\rho_{S_V} - \mathrm{Tr}_{[N]\setminus S_V}\rho_{\mathrm{hist}}\|_{tr} = \mathsf{negl}(\lambda)$. Therefore, we have $\|\widetilde{\rho'}_{\mathrm{hist}} - \rho'_{\mathrm{hist}}\|_{tr} = \mathsf{negl}(\lambda)$. This means that $\mathsf{Sim}_1(k_V, \mathtt{x})$ and $\mathsf{Sim}_2(k_V, \mathtt{x}, \mathtt{w})$

are statistically indistinguishable from the view of a distinguisher that makes at most one query.
Finally, noting that the output distribution of $\mathsf{Sim}_2(k_V, \mathtt{x}, \mathtt{w})$ is exactly the same as that of $\mathsf{Prove}(k_P, \mathtt{x}, \mathtt{w})$, the proof of Lemma 3.2 is completed.

4 Dual-Mode CV-NIZK with Preprocessing

In this section, we extend the CV-NIZK given in Section 3 to reduce the amount of trust in the setup at the cost of introducing a quantum preprocessing and relying on a computational assumption. In the construction in Section 3, we assume that the trusted setup algorithm honestly generates proving and verification keys, which are correlated with each other, and sends them to the prover and verifier, respectively, without revealing them to the other party. Here, we give a construction of CV-NIZK with preprocessing that consists of the generation of common reference string by a trusted party and a single instance-independent quantum message from the verifier to the prover. We call such a model the CRS $+$ $(V \to P)$ model. We note this is the same model as is considered in [CVZ20]. Moreover, our construction has a nice feature called the dual-mode property, which has been considered for NIZKs for **NP** [GS12, GOS12, PS19].

4.1 Definition

We give a formal definition of a dual-mode CV-NIZK in the CRS $+$ $(V \to P)$ model.

Definition 4.1 (Dual-Mode CV-NIZK in the CRS $+$ $(V \to P)$ Model). *A dual-mode CV-NIZK for a* **QMA** *promise problem $L = (L_{\mathsf{yes}}, L_{\mathsf{no}})$ in the CRS $+$ $(V \to P)$ model consists of algorithms $\Pi = (\mathsf{CRSGen}, \mathsf{Preprocess}, \mathsf{Prove}, \mathsf{Verify})$ with the following syntax:*

$\mathsf{CRSGen}(1^\lambda, \mathsf{mode})$**:** *This is a PPT algorithm that takes the security parameter 1^λ and a mode $\mathsf{mode} \in \{\mathsf{binding}, \mathsf{hiding}\}$ as input and outputs a classical common reference string crs. We note that crs can be reused and thus this algorithm is only needed to run once by a trusted third party.*

$\mathsf{Preprocess}(\mathsf{crs})$**:** *This is a QPT algorithm that takes the common reference string crs as input and outputs a quantum proving key k_P and a classical verification key k_V. We note that this algorithm is supposed to be run by the verifier as preprocessing, and k_P is supposed to be sent to the prover while k_V is supposed to be kept on verifier's side in secret. We also note that they can be used only once and cannot be reused unlike crs.*

$\mathsf{Prove}(\mathsf{crs}, k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$**:** *This is a QPT algorithm that takes the common reference string crs, the proving key k_P, a statement $\mathtt{x}$, and $k = \mathsf{poly}(\lambda)$ copies $\mathtt{w}^{\otimes k}$ of a witness $\mathtt{w} \in R_L(\mathtt{x})$ as input and outputs a classical proof π.*

$\mathsf{Verify}(\mathsf{crs}, k_V, \mathtt{x}, \pi)$**:** *This is a PPT algorithm that takes the common reference string crs, the verification key k_V, a statement $\mathtt{x}$, and a proof π as input and outputs $\top$ indicating acceptance or $\bot$ indicating rejection.*

We require Π to satisfy the following properties for some $0 < s < c < 1$ such that $c - s > 1/\mathsf{poly}(\lambda)$. Especially, when we do not specify c and s, they are set as $c = 1 - \mathsf{negl}(\lambda)$ and $s = \mathsf{negl}(\lambda)$.

c-Completeness. *For all $\mathsf{mode} \in \{\mathsf{binding}, \mathsf{hiding}\}$, $\mathtt{x} \in L_{\mathsf{yes}} \cap \{0,1\}^\lambda$, and $\mathtt{w} \in R_L(\mathtt{x})$, we have*

$$\Pr\left[\mathsf{Verify}(\mathsf{crs}, k_V, \mathtt{x}, \pi) = \top : \begin{array}{r}\mathsf{crs} \xleftarrow{\$} \mathsf{CRSGen}(1^\lambda, \mathsf{mode}) \\ (k_P, k_V) \xleftarrow{\$} \mathsf{Preprocess}(\mathsf{crs}) \\ \pi \xleftarrow{\$} \mathsf{Prove}(\mathsf{crs}, k_P, \mathtt{x}, \mathtt{w}^{\otimes k})\end{array}\right] \geq c.$$

(Adaptive) Statistical s-Soundness in the Binding Mode *For all unbounded-time adversary $\mathcal{A}$, we have*

$$\Pr\left[\mathtt{x} \in L_{\mathsf{no}} \wedge \mathsf{Verify}(\mathsf{crs}, k_V, \mathtt{x}, \pi) = \top : \begin{array}{r}\mathsf{crs} \xleftarrow{\$} \mathsf{CRSGen}(1^\lambda, \mathsf{binding}) \\ (k_P, k_V) \xleftarrow{\$} \mathsf{Preprocess}(\mathsf{crs}) \\ (\mathtt{x}, \pi) \xleftarrow{\$} \mathcal{A}(\mathsf{crs}, k_P)\end{array}\right] \leq s.$$

(Adaptive Multi-Theorem) Statistical Zero-Knowledge in the Hiding Mode. *There exists a PPT simulator Sim_0 and a QPT simulator Sim_1 such that for any unbounded-time distinguisher $\mathcal{D}$, we have*

$$\left|\Pr\left[\mathcal{D}^{\mathcal{O}_P(\mathsf{crs},\cdot,\cdot,\cdot)}(\mathsf{crs}) = 1 : \mathsf{crs} \xleftarrow{\$} \mathsf{CRSGen}(1^\lambda, \mathsf{hiding})\right]\right.$$
$$\left. - \Pr\left[\mathcal{D}^{\mathcal{O}_S(\mathsf{td},\cdot,\cdot,\cdot)}(\mathsf{crs}) = 1 : (\mathsf{crs}, \mathsf{td}) \xleftarrow{\$} \mathsf{Sim}_0(1^\lambda)\right]\right| \leq \mathsf{negl}(\lambda)$$

where $\mathcal{D}$ can make $\mathsf{poly}(\lambda)$ queries, which should be of the form $(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$ where $\mathtt{w} \in R_L(\mathtt{x})$ and $\mathtt{w}^{\otimes k}$ is unentangled with $\mathcal{D}$'s internal registers,[9] *$\mathcal{O}_P(\mathsf{crs}, k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$ returns $\mathsf{Prove}(\mathsf{crs}, k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$, and $\mathcal{O}_S(\mathsf{td}, k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$ returns $\mathsf{Sim}_1(\mathsf{td}, k_P, \mathtt{x})$.*

Computational Mode Indistinguishability. *For any non-uniform QPT distinguisher $\mathcal{D}$, we have*

$$|\Pr[\mathcal{D}(\mathsf{crs}_{\mathsf{binding}}) = 1] - \Pr[\mathcal{D}(\mathsf{crs}_{\mathsf{hiding}}) = 1]| \leq \mathsf{negl}(\lambda)$$

where $\mathsf{crs}_{\mathsf{binding}} \xleftarrow{\$} \mathsf{CRSGen}(1^\lambda, \mathsf{binding})$ and $\mathsf{crs}_{\mathsf{hiding}} \xleftarrow{\$} \mathsf{CRSGen}(1^\lambda, \mathsf{hiding})$.

Though Definition 4.1 does not explicitly require anything on soundness in the hiding mode or the zero-knowledge property in the binding mode, we can easily prove that they are satisfied in a computational sense.

Finally, we note that we can amplify the gap between the thresholds for completeness and soundness by parallel repetitions similarly to CV-NIZK in the QSP model as discussed in Section 2.3. As a result, we obtain the following lemma.

[9] We remark that k_P is allowed to be entangled with $\mathcal{D}$'s internal registers unlike $\mathtt{w}^{\otimes k}$. See also footnote 8.

Lemma 4.1 (Gap amplification for dual-mode CV-NIZK in the CRS + $(V \to P)$ model). *If there exists a dual-mode CV-NIZK for L in the CRS + $(V \to P)$ model that satisfies c-completeness and s-soundness, for some $0 < s < c < 1$ such that $c - s > 1/\mathsf{poly}(\lambda)$, then there exists a dual-mode CV-NIZK for L in the CRS + $(V \to P)$ model (with $(1 - \mathsf{negl}(\lambda))$-completeness and $\mathsf{negl}(\lambda)$-soundness).*

Since this can be proven similarly to Lemma 2.5, we omit a proof.

4.2 Building Blocks

We introduce two cryptographic bulding blocks for our dual-mode CV-NIZK in the CRS + $(V \to P)$ model.

Lossy Encryption Intuitively, a lossy encryption scheme is a public key encryption scheme with a special property that we can generate a *lossy key* that is computationally indistinguishable from an honestly generated public key, for which there is no corresponding decryption key.

Dual-Mode Oblivious Transfer The second building block is a k-out-of-n *dual-mode oblivious transfer*. Though this is a newly introduced definition in this paper, 1-out-of-2 case is already implicit in existing works on universally composable (UC-secure) [Can20] oblivious transfers [PVW08, Qua20]. Due to the space limitation, we only give its syntax and intuitive explanations for the security requirements.

Definition 4.2 (Dual-mode oblivious transfer (sketch)). *A (2-round) k-out-of-n dual-mode oblivious transfer with a message space $\mathcal{M}$ consists of PPT algorithms $\Pi_{\mathsf{OT}} = (\mathsf{CRSGen}, \mathsf{Receiver}, \mathsf{Sender}, \mathsf{Derive})$.*

$\mathsf{CRSGen}(1^\lambda, \mathsf{mode})$**:** *This is an algorithm supposed to be run by a trusted third party that takes the security parameter 1^λ and a mode $\mathsf{mode} \in \{\mathsf{binding}, \mathsf{hiding}\}$ as input and outputs a common reference string crs.*

$\mathsf{Receiver}(\mathsf{crs}, J)$**:** *This is an algorithm supposed to be run by a receiver that takes the common reference string crs and an ordered set of k indices $J \in [n]^k$ as input and outputs a first message ot_1 and a receiver's state st.*

$\mathsf{Sender}(\mathsf{crs}, \mathsf{ot}_1, \boldsymbol{\mu})$**:** *This is an algorithm supposed to be run by a sender that takes the common reference string crs, a first message ot_1 sent from a receiver and a tuple of messages $\boldsymbol{\mu} \in \mathcal{M}^n$ as input and outputs a second message ot_2.*

$\mathsf{Derive}(\mathsf{crs}, \mathsf{st}, \mathsf{ot}_2)$**:** *This is an algorithm supposed to be run by a receiver that takes a receiver's state st and a second message ot_2 as input and outputs a tuple of messages $\boldsymbol{\mu}' \in \mathcal{M}^k$.*

We require the following properties.

Correctness *For all* $\mathsf{mode} \in \{\mathsf{binding}, \mathsf{hiding}\}$, $J = (j_1, ..., j_k) \in [n]^k$, *and* $\boldsymbol{\mu} = (\mu_1, ..., \mu_n) \in \mathcal{M}^n$, *we have*

$$\Pr\left[\mathsf{Derive}(\mathsf{crs}, \mathsf{st}, \mathsf{ot}_2) = (\mu_{j_1}, ..., \mu_{j_k}) : \begin{array}{l} \mathsf{crs} \xleftarrow{\$} \mathsf{CRSGen}(1^\lambda, \mathsf{mode}) \\ (\mathsf{ot}_1, \mathsf{st}) \xleftarrow{\$} \mathsf{Receiver}(\mathsf{crs}, J) \\ \mathsf{ot}_2 \xleftarrow{\$} \mathsf{Sender}(\mathsf{crs}, \mathsf{ot}_1, \boldsymbol{\mu}) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda).$$

Statistical Receiver's Security in the Binding Mode *Intuitively, this security requires that the indices chosen by a receiver are information theoretically hidden from a sender in the binding mode.*

Statistical Sender's Security in the Hiding Mode *Intuitively, this security requires that we can extract the indices of messages which a (possibly malicious) receiver tries to learn by using a trapdoor in the hiding mode.*

Computational Mode Indistinguishability. *This requires that common reference strings generated in binding and hiding modes are computationally indistinguishable.*

Lemma 4.2. *If the LWE assumption holds, then there exists k-out-of-n dual-mode oblivious transfer for arbitrary $0 < k < n$ that are polynomial in λ.*

Proof (sketch). First, we can see that the LWE-based UC-secure OT by Quach [Qua20] can be seen as a 1-out-of-2 dual-mode oblivious transfer. This construction can be converted into 1-out-of-n dual-mode oblivious transfer by using the generic conversion for an ordinary oblivious transfer given in [BCR86] observing that the conversion preserves the dual-mode property.[10] By k-parallel repetition of the 1-out-of-n dual-mode oblivious transfer, we obtain k-out-of-n dual-mode oblivious transfer.

4.3 Construction

In this section, we construct a dual-mode CV-NIZK in the CRS + $(V \to P)$ model. As a result, we obtain the following theorem.

Theorem 4.1. *If the LWE assumption holds, then there exists a dual-mode CV-NIZK in the CRS + $(V \to P)$ model.*

Let L be a **QMA** promise problem, and $\mathcal{H}_{\mathtt{x}}$, N, M, p_i, s_i, P_i, α, β, and ρ_{hist} be as in Lemma 2.4 for the language L. We let $N' := 3^5 \sum_{i=1}^{5} \binom{N}{i}$ similarly to Lemma 3.1. Let $\Pi_{\mathsf{LE}} = (\mathsf{InjGen}_{\mathsf{LE}}, \mathsf{LossyGen}_{\mathsf{LE}}, \mathsf{Enc}_{\mathsf{LE}}, \mathsf{Dec}_{\mathsf{LE}})$ be a lossy encryption scheme over the message space $\mathcal{M}_{\mathsf{LE}} = \{0,1\}^2$ and the randomness space $\mathcal{R}_{\mathsf{LE}}$. Let $\Pi_{\mathsf{OT}} = (\mathsf{CRSGen}_{\mathsf{OT}}, \mathsf{Receiver}_{\mathsf{OT}}, \mathsf{Sender}_{\mathsf{OT}}, \mathsf{Derive}_{\mathsf{OT}})$ be a 5-out-of-N dual-mode oblivious transfer over the message space $\mathcal{M}_{\mathsf{OT}} = \mathcal{M}_{\mathsf{LE}} \times \mathcal{R}_{\mathsf{LE}}$. Then our dual-mode CV-NIZK $\Pi_{\mathsf{DM}} = (\mathsf{CRSGen}_{\mathsf{DM}}, \mathsf{Preprocess}_{\mathsf{DM}}, \mathsf{Prove}_{\mathsf{DM}}, \mathsf{Verify}_{\mathsf{DM}})$ for L is described in Figure 4.

Then we prove the following lemmas.

[10] Alternatively, it may be possible to directly construct 1-out-of-n dual-mode oblivious transfer by appropriately modifying the construction by Quach [Qua20].

$\mathsf{CRSGen}_{\mathsf{DM}}(1^\lambda, \mathsf{mode})$**:** The CRS generation algorithm generates $\mathsf{crs}_{\mathsf{OT}} \xleftarrow{\$} \mathsf{CRSGen}_{\mathsf{OT}}(1^\lambda, \mathsf{mode})$.

- If $\mathsf{mode} = \mathsf{binding}$, then it generates $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{InjGen}_{\mathsf{LE}}(1^\lambda)$.
- If $\mathsf{mode} = \mathsf{hiding}$, then it generates $\mathsf{pk} \xleftarrow{\$} \mathsf{LossyGen}_{\mathsf{LE}}(1^\lambda)$.

Then it outputs $\mathsf{crs}_{\mathsf{DM}} := (\mathsf{crs}_{\mathsf{OT}}, \mathsf{pk})$.

$\mathsf{Preprocess}_{\mathsf{DM}}(\mathsf{crs}_{\mathsf{DM}})$**:** The preprocessing algorithm parses $(\mathsf{crs}_{\mathsf{OT}}, \mathsf{pk}) \leftarrow \mathsf{crs}_{\mathsf{DM}}$ and chooses $(W_1, ..., W_N) \xleftarrow{\$} \{X, Y, Z\}^N$, $(m_1, ..., m_N) \xleftarrow{\$} \{0,1\}^N$, and a uniformly random subset $S_V \subseteq [N]$ such that $1 \leq |S_V| \leq 5$. Let $J = (j_1, ..., j_5) \in [N]^5$ be the elements of S_V in the ascending order where we append arbitrary indices when $|S_V| < 5$. It generates $(\mathsf{ot}_1, \mathsf{st}) \xleftarrow{\$} \mathsf{Receiver}_{\mathsf{OT}}(\mathsf{crs}_{\mathsf{OT}}, J)$ and outputs a proving key $k_P := \left(\rho_P := \bigotimes_{j=1}^N (U(W_j)|m_j\rangle), \mathsf{ot}_1\right)$ and a verification key $k_V := (W_1, ..., W_N, m_1, ..., m_N, S_V, \mathsf{st})$.

$\mathsf{Prove}_{\mathsf{DM}}(\mathsf{crs}_{\mathsf{DM}}, k_P, \mathtt{x}, \mathtt{w})$**:** The proving algorithm parses $(\mathsf{crs}_{\mathsf{OT}}, \mathsf{pk}) \leftarrow \mathsf{crs}_{\mathsf{DM}}$ and $(\rho_P, \mathsf{ot}_1) \leftarrow k_P$, generates $(\widehat{x}, \widehat{z}) \xleftarrow{\$} \{0,1\}^N \times \{0,1\}^N$, generates the history state ρ_{hist} for $\mathcal{H}_{\mathtt{x}}$ from $\mathtt{w}$, and computes $\rho'_{\mathrm{hist}} := X^{\widehat{x}} Z^{\widehat{z}} \rho_{\mathrm{hist}} Z^{\widehat{z}} X^{\widehat{x}}$. It measures j-th qubits of ρ'_{hist} and ρ_P in the Bell basis for $j \in [N]$. Let $x := x_1 \| x_2 \| ... \| x_N$, and $z := z_1 \| z_2 \| ... \| z_N$ where (x_j, z_j) denotes the outcome of j-th measurement. For $j \in [N]$, it generates $\mathsf{ct}_j := \mathsf{Enc}_{\mathsf{LE}}(\mathsf{pk}, (\widehat{x}_j, \widehat{z}_j); R_j)$ where $R_j \xleftarrow{\$} \mathcal{R}_{\mathsf{LE}}$ and $\widehat{x}_j$ and $\widehat{z}_j$ denote the j-th bits of $\widehat{x}$ and $\widehat{z}$, respectively. It sets $\mu_j := ((\widehat{x}_j, \widehat{z}_j), R_j)$ for $j \in [N]$ and generates $\mathsf{ot}_2 \xleftarrow{\$} \mathsf{Sender}_{\mathsf{OT}}(\mathsf{crs}_{\mathsf{OT}}, \mathsf{ot}_1, (\mu_1, ..., \mu_N))$. It outputs a proof $\pi := (x, z, \{\mathsf{ct}_j\}_{j \in [N]}, \mathsf{ot}_2)$.

$\mathsf{Verify}_{\mathsf{DM}}(\mathsf{crs}_{\mathsf{DM}}, k_V, \mathtt{x}, \pi)$**:** The verification algorithm parses $(\mathsf{crs}_{\mathsf{OT}}, \mathsf{pk}) \leftarrow \mathsf{crs}_{\mathsf{DM}}$, $(W_1, ..., W_N, m_1, ..., m_N, S_V, \mathsf{st}) \leftarrow k_V$, and $(x, z, \{\mathsf{ct}_j\}_{j \in [N]}, \mathsf{ot}_2) \leftarrow \pi$. It runs $\boldsymbol{\mu}' \xleftarrow{\$} \mathsf{Derive}_{\mathsf{OT}}(\mathsf{crs}_{\mathsf{OT}}, \mathsf{st}, \mathsf{ot}_2)$ and parses $(((\widehat{x}'_1, \widehat{z}'_1), R'_1), ..., ((\widehat{x}'_5, \widehat{z}'_5), R'_5)) \leftarrow \boldsymbol{\mu}'$. If $\mathsf{Enc}_{\mathsf{LE}}(\mathsf{pk}, (\widehat{x}'_i, \widehat{z}'_i); R'_i) \neq \mathsf{ct}_{j_i}$ for some $i \in [5]$, it outputs $\bot$. Otherwise, it recovers $\{\widehat{x}_j, \widehat{z}_j\}_{j \in S_V}$ by setting $(\widehat{x}_{j_i}, \widehat{z}_{j_i}) := (\widehat{x}'_i, \widehat{z}'_i)$ for $i \in [|S_V|]$. It chooses $i \in [M]$ according to the probability distribution defined by $\{p_i\}_{i \in [M]}$ (i.e., chooses i with probability p_i). Let

$$S_i := \{j \in [N] \mid j\text{th Pauli operator of } P_i \text{ is not } I\}.$$

We note that we have $1 \leq |S_i| \leq 5$ by the 5-locality of $\mathcal{H}_{\mathtt{x}}$. We say that P_i is consistent to $(S_V, \{W_j\}_{j \in S_V})$ if and only if $S_i = S_V$ and the jth Pauli operator of P_i is W_j for all $j \in S_i$. If P_i is not consistent to $(S_V, \{W_j\}_{j \in S_V})$, it outputs $\top$. If P_i is consistent to $(S_V, \{W_j\}_{j \in S_V})$, it flips a biased coin that heads with probability $1 - 3^{|S_i|-5}$. If heads, it outputs $\top$. If tails, it defines

$$m'_j := \begin{cases} m_j \oplus x_j \oplus \hat{x}_j & (W_j = Z), \\ m_j \oplus z_j \oplus \hat{z}_j & (W_j = X), \\ m_j \oplus x_j \oplus \hat{x}_j \oplus z_j \oplus \hat{z}_j & (W_j = Y) \end{cases}$$

for $j \in S_i$, and outputs $\top$ if $(-1)^{\bigoplus_{j \in S_i} m'_j} = -s_i$ and $\bot$ otherwise.

Fig. 4. Dual-Mode CV-NIZK Π_{DM}.

Lemma 4.3. *Π_{DM} satisfies $\left(1 - \frac{\alpha}{N'} - \mathsf{negl}(\lambda)\right)$-completeness.*

Proof. By the correctness of Π_{OT}, it is easy to see that the probability that an honestly generated proof passes the verification differs from that in Π_{NIZK} in Figure 1 only by $\mathsf{negl}(\lambda)$. Since Π_{NIZK} satisfies $\left(1 - \frac{\alpha}{N'}\right)$-completeness as shown in Lemma 3.1, Π_{DM} satisfies $\left(1 - \frac{\alpha}{N'} - \mathsf{negl}(\lambda)\right)$-completeness.

Lemma 4.4. *Π_{DM} satisfies the computational mode indistinguishability.*

Proof. This can be reduced to the computational mode indistinguishability of Π_{OT} and Π_{LE} in a straightforward manner.

Lemma 4.5. *Π_{DM} satisfies statistical $\left(1 - \frac{\beta}{N'} + \mathsf{negl}(\lambda)\right)$-soundness in the binding mode.*

Lemma 4.6. *Π_{DM} satisfies the statistical zero-knowledge property in the hiding mode.*

By combining Lemmas 4.1 to 4.6 and

$$\left(1 - \frac{\alpha}{N'} - \mathsf{negl}(\lambda)\right) - \left(1 - \frac{\beta}{N'} + \mathsf{negl}(\lambda)\right) = \frac{\beta - \alpha}{N'} - \mathsf{negl}(\lambda) = \frac{1}{\mathsf{poly}(\lambda)},$$

we obtain Theorem 4.1.

In the following, we give proof sketches of Lemmas 4.5 and 4.6.

Soundness in the binding mode. For a cheating prover, we consider a modified soundness game where the challenger extracts $\{\widehat{x}_j, \widehat{z}_j\}_{j \in S_V}$ from $\{\mathsf{ct}_j\}_{j \in S_V}$ by just decrypting them instead of deriving $\{(\widehat{x}_j, \widehat{z}_j), R_j\}_{j \in S_V}$ from ot_2 and then checking the consistency to $\{\mathsf{ct}_j\}_{j \in S_V}$ as in the actual verification algorithm. This does not decrease adversary's winning probability since $\{\widehat{x}_j, \widehat{z}_j\}_{j \in S_V}$ derived from ot_2 should be equal to decryption of $\{\mathsf{ct}_j\}_{j \in S_V}$ or otherwise the verification algorithm immediately rejects. In this game, the challenger does not use st of Π_{OT}. Therefore, by the receiver's security of Π_{OT}, adversary's winning probability changes negligibly even if we generate ot_1 by the simulator $\mathsf{Sim}_{\mathsf{rec}}$. At this point, the challenger obtain no information about S_V. Then soundness in this game can be reduced to the soundness of Π_{NIZK} in Figure 1 against augmented cheating provers with an additional capability to choose $\{\widehat{x}_j, \widehat{z}_j\}_{j \in [N]}$. By carefully examining the proof of the soundness of Π_{NIZK}, one can see that the proof works against such augmented cheating provers as well. (Note that what is essential for the soundness of Π_{NIZK} is that S_V is hidden from the cheating prover.)

Zero-knowledge in the hiding mode. In the hiding mode, pk of Π_{LE} is in the lossy mode, and thus $\{\mathsf{ct}_j\}_{j \in [N]}$ can be simulated only from pk by encrypting all 0 message. Moreover, by sender's security in the hiding mode of Π_{OT}, ot_2 can be simulated from $\{\widehat{x}_j, \widehat{z}_j\}_{j \in S_V}$ where S_V is a subset such that $|S_V| = 5$ extracted from ot_1. Therefore, the zero-knowledge property of Π_{DM} can be reduced to the

zero-knowledge property of Π_{NIZK} in Figure 1 against augmented malicious verifiers with an additional capability to choose S_V and ρ_P. By carefully examining the proof of the zero-knowledge property of Π_{NIZK}, one can see that the proof works against such augmented malicious verifiers as well. (Note that what is essential for the zero-knowledge property of Π_{NIZK} is that $\{\widehat{x}_j, \widehat{z}_j\}_{j \notin S_V}$ is hidden from the malicious verifier.)

5 CV-NIZK via Fiat-Shamir Transformation

In this section, we construct CV-NIZK in the quantum random oracle model via the Fiat-Shamir transformation.

5.1 Definition

We give a formal definition of CV-NIZK in the QRO + $(V \to P)$ model.

Definition 5.1 (CV-NIZK in the QRO + $(V \to P)$ Model). *A CV-NIZK for a* **QMA** *promise problem $L = (L_{\mathsf{yes}}, L_{\mathsf{no}})$ in the QRO + $(V \to P)$ model w.r.t. a random oracle distribution* ROdist *consists of algorithms $\Pi = (\mathsf{Preprocess}, \mathsf{Prove}, \mathsf{Verify})$ with the following syntax:*

$\mathsf{Preprocess}(1^\lambda)$**:** *This is a QPT algorithm that takes the security parameter 1^λ as input, and outputs a quantum proving key k_P and a classical verification key k_V. We note that this algorithm is supposed to be run by the verifier as preprocessing, and k_P is supposed to be sent to the prover while k_V is supposed to be kept on verifier's side in secret. We also note that they can be used only once and cannot be reused.*

$\mathsf{Prove}^H(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$**:** *This is a QPT algorithm that is given quantum oracle access to the random oracle H. It takes the proving key k_P, a statement $\mathtt{x}$, and $k = \mathsf{poly}(\lambda)$ copies $\mathtt{w}^{\otimes k}$ of a witness $\mathtt{w} \in R_L(\mathtt{x})$ as input, and outputs a classical proof π.*

$\mathsf{Verify}^H(k_V, \mathtt{x}, \pi)$**:** *This is a PPT algorithm that is given classical oracle access to the random oracle H. It takes the verification key k_V, a statement $\mathtt{x}$, and a proof π as input, and outputs $\top$ indicating acceptance or $\bot$ indicating rejection.*

We require Π to satisfy the following properties.

Completeness. *For all $\mathtt{x} \in L_{\mathsf{yes}} \cap \{0,1\}^\lambda$, and $\mathtt{w} \in R_L(\mathtt{x})$, we have*

$$\Pr\left[\mathsf{Verify}^H(k_V, \mathtt{x}, \pi) = \top : \begin{array}{c} H \xleftarrow{\$} \mathsf{ROdist} \\ (k_P, k_V) \xleftarrow{\$} \mathsf{Preprocess}(1^\lambda) \\ \pi \xleftarrow{\$} \mathsf{Prove}^H(k_P, \mathtt{x}, \mathtt{w}^{\otimes k}) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda).$$

Adaptive Statistical Soundness. *For all adversaries $\mathcal{A}$ that make at most* $\mathsf{poly}(\lambda)$ *quantum random oracle queries, we have*

$$\Pr\left[\mathtt{x} \in L_{\mathsf{no}} \wedge \mathsf{Verify}^H(k_V, \mathtt{x}, \pi) = \top : \begin{array}{c} H \xleftarrow{\$} \mathsf{ROdist} \\ (k_P, k_V) \xleftarrow{\$} \mathsf{Preprocess}(1^\lambda) \\ (\mathtt{x}, \pi) \xleftarrow{\$} \mathcal{A}^H(k_P) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

Adaptive Multi-Theorem Zero-Knowledge. *For defining the zero-knowledge property in the QROM, we define the syntax of a simulator in the QROM following [Unr15]. A simulator is given quantum access to the random oracle H and classical access to reprogramming oracle* $\mathsf{Reprogram}$*. When the simulator queries (x, y) to* $\mathsf{Reprogram}$*, the random oracle H is reprogrammed so that $H(x) := y$ while keeping the values on other inputs unchanged. Then the adaptive multi-theorem zero-knowledge property is defined as follows:*

There exists a QPT simulator Sim *with the above syntax such that for any QPT distinguisher $\mathcal{D}$, we have*

$$\left|\Pr\left[\mathcal{D}^{H,\mathcal{O}_P^H(\cdot,\cdot,\cdot)}(1^\lambda) = 1 : H \xleftarrow{\$} \mathsf{ROdist}\right] - \Pr\left[\mathcal{D}^{H,\mathcal{O}_S^{H,\mathsf{Reprogram}}(\cdot,\cdot,\cdot)}(1^\lambda) = 1 : H \xleftarrow{\$} \mathsf{ROdist}\right]\right| \leq \mathsf{negl}(\lambda)$$

where $\mathcal{D}$'s queries to the second oracle should be of the form $(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$ where $\mathtt{w} \in R_L(\mathtt{x})$ and $\mathtt{w}^{\otimes k}$ is unentangled with $\mathcal{D}$'s internal registers, [11] *$\mathcal{O}_P^H(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$ returns $\mathsf{Prove}^H(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$, and $\mathcal{O}_S^{H,\mathsf{Reprogram}}(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$ returns $\mathsf{Sim}^{H,\mathsf{Reprogram}}(k_P, \mathtt{x})$.*

Remark 5.1. Remark that the "multi-theorem" zero-knowledge does not mean that a preprocessing can be reused many times. It rather means that a single random oracle can be reused as long as a fresh preprocessing is run every time. This is consistent to the definition in the CRS + $(V \to P)$ model (Definition 4.1) if we think of the random oracle as replacement of CRS.

5.2 Building Blocks

We use the two cryptographic primitives, a non-interactive commitment scheme and a Σ-protocol with quantum preprocessing, for our construction.

Definition 5.2 (Σ-protocol with Quantum Preprocessing). *A Σ-protocol with quantum preprocessing for a* **QMA** *promise problem $L = (L_{\mathsf{yes}}, L_{\mathsf{no}})$ consists of algorithms $\Pi = (\mathsf{Preprocess}, \mathsf{Prove}_1, \mathsf{Verify}_1, \mathsf{Prove}_2, \mathsf{Verify}_2)$ with the following syntax:*

$\mathsf{Preprocess}(1^\lambda)$**:** *This is a QPT algorithm that takes the security parameter 1^λ as input, and outputs a quantum proving key k_P and a classical verification*

[11] We remark that k_P is allowed to be entangled with $\mathcal{D}$'s internal registers unlike $\mathtt{w}^{\otimes k}$. See also footnote 8.

key k_V. We note that this algorithm is supposed to be run by the verifier as preprocessing, and k_P is supposed to be sent to the prover while k_V is supposed to be kept on verifier's side in secret. We also note that they can be used only once and cannot be reused.

$\mathsf{Prove}_1(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$**:** *This is a QPT algorithm that takes the proving key k_P, a statement $\mathtt{x}$, and $k = \mathsf{poly}(\lambda)$ copies $\mathtt{w}^{\otimes k}$ of a witness $\mathtt{w} \in R_L(\mathtt{x})$ as input, and outputs a classical message msg_1 and a state st.*

$\mathsf{Verify}_1(1^\lambda)$**:** *This is a PPT algorithm that takes the security parameter 1^λ, and outputs a classical message msg_2, which is uniformly sampled from a certain set.*

$\mathsf{Prove}_2(\mathsf{st}, \mathsf{msg}_2)$**:** *This is a QPT algorithm that takes the state st and the message msg_2 as input, and outputs a classical message msg_3.*

$\mathsf{Verify}_2(k_V, \mathtt{x}, \mathsf{msg}_1, \mathsf{msg}_2, \mathsf{msg}_3)$**:** *This is a PPT algorithm that takes the verification key k_V, the statement $\mathtt{x}$, and classical messages $\mathsf{msg}_1, \mathsf{msg}_2, \mathsf{msg}_3$ as input, and outputs $\top$ indicating acceptance or $\bot$ indicating rejection.*

We require Π to satisfy the following properties.

c-Completeness. *For all $\mathtt{x} \in L_{\mathsf{yes}} \cap \{0,1\}^\lambda$, and $\mathtt{w} \in R_L(\mathtt{x})$, we have*

$$\Pr\left[\mathsf{Verify}_2(k_V, \mathtt{x}, \mathsf{msg}_1, \mathsf{msg}_2, \mathsf{msg}_3) = \top : \begin{array}{c}(k_P, k_V) \xleftarrow{\$} \mathsf{Preprocess}(1^\lambda) \\ (\mathsf{msg}_1, \mathsf{st}) \xleftarrow{\$} \mathsf{Prove}_1(k_P, \mathtt{x}, \mathtt{w}^{\otimes k}) \\ \mathsf{msg}_2 \xleftarrow{\$} \mathsf{Verify}_1(1^\lambda) \\ \mathsf{msg}_3 \xleftarrow{\$} \mathsf{Prove}_2(\mathsf{st}, \mathsf{msg}_2)\end{array}\right] \geq c.$$

(Adaptive Statistical) s-soundness. *For all adversary $(\mathcal{A}_1, \mathcal{A}_2)$, we have*

$$\Pr\left[\mathtt{x} \in L_{\mathsf{no}} \wedge \Sigma.\mathsf{Verify}_2(k_V, \mathtt{x}, \mathsf{msg}_1, \mathsf{msg}_2, \mathsf{msg}_3) = \top : \begin{array}{c}(k_P, k_V) \xleftarrow{\$} \mathsf{Preprocess}(1^\lambda) \\ (\mathtt{x}, \mathsf{st}, \mathsf{msg}_1) \xleftarrow{\$} \mathcal{A}_1(k_P) \\ \mathsf{msg}_2 \xleftarrow{\$} \mathsf{Verify}_1(1^\lambda) \\ \mathsf{msg}_3 \xleftarrow{\$} \mathcal{A}_2(\mathsf{st}, \mathsf{msg}_2)\end{array}\right] \leq s.$$

Special Zero-Knowledge. *There exists a QPT algorithm Sim such that for any $\mathtt{x} \in L_{\mathsf{yes}}$, $\mathtt{w} \in R_L(\mathtt{x})$, msg_2, and QPT adversary $(\mathcal{A}_1, \mathcal{A}_2)$, we have*

$$\left|\begin{array}{l}\Pr\left[\mathcal{A}_2(\mathsf{st}_{\mathcal{A}}, \mathtt{x}, \mathsf{msg}_1, \mathsf{msg}_2, \mathsf{msg}_3) = 1 : \begin{array}{c}(k_P, \mathsf{st}_{\mathcal{A}}) \xleftarrow{\$} \mathcal{A}_1(1^\lambda) \\ (\mathsf{msg}_1, \mathsf{st}) \xleftarrow{\$} \mathsf{Prove}_1(k_P, \mathtt{x}, \mathtt{w}^{\otimes k}) \\ \mathsf{msg}_3 \xleftarrow{\$} \mathsf{Prove}_2(\mathsf{st}, \mathsf{msg}_2)\end{array}\right] \\ - \Pr\left[\mathcal{A}_2(\mathsf{st}_{\mathcal{A}}, \mathtt{x}, \mathsf{msg}_1, \mathsf{msg}_2, \mathsf{msg}_3) = 1 : \begin{array}{c}(k_P, \mathsf{st}_{\mathcal{A}}) \xleftarrow{\$} \mathcal{A}_1(1^\lambda) \\ (\mathsf{msg}_1, \mathsf{msg}_3) \xleftarrow{\$} \mathsf{Sim}(k_P, \mathtt{x}, \mathsf{msg}_2)\end{array}\right]\end{array}\right| \leq \mathsf{negl}(\lambda).$$

High Min-Entropy. Prove_1 *can be divided into the "quantum part" and "classical part" as follows:*

$\mathsf{Prove}_1^Q(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$**:** *This is a QPT algorithm that outputs a classical string st'.*

$\mathsf{Prove}_1^C(\mathsf{st}')$: *This is a PPT algorithm that outputs* msg_1 *and* st.

Moreover, for any st' *generated by* Prove_1^Q*, we have*

$$\max_{\mathsf{msg}_1^*} \Pr[\mathsf{Prove}_1^C(\mathsf{st}') = \mathsf{msg}_1^*] = \mathsf{negl}(\lambda).$$

Lemma 5.1 (Gap Amplification for Σ-protocol with quantum preprocessing). *If there exists a Σ-protocol with quantum preprocessing for a promise problem L that satisfies c-completeness, s-soundness, special zero-knowledge, and high min-entropy for some $0 < s < c < 1$ such that $c - s > 1/\mathsf{poly}(\lambda)$, then there exists a Σ-protocol with quantum preprocessing for L with $(1 - \mathsf{negl}(\lambda))$-completeness, $\mathsf{negl}(\lambda)$-soundness, special zero-knowledge, and high min-entropy.*

Proof. It is clear that the parallel repetition can amplify the completeness-soundness gap, and that the high min-entropy is preserved under the parallel repetition. We can also show that parallel repetition preserves the special zero-knowledge property by a standard hybrid argument.

By applying a similar trick as in Section 3 to the quantum Σ-protocol of [BG20], we obtain the following theorem.

Theorem 5.1. *If a non-interactive commitment scheme exists, then there exists a Σ-protocol with quantum preprocessing for* **QMA**.

As mentioned in Section 5.1, a non-interactive commitment scheme unconditionally exists in the QROM. Therefore, the above theorem implies the following corollary.

Corollary 5.1. *There exists a Σ-protocol with quantum preprocessing for* **QMA** *in the QROM.*

5.3 Construction

In this section, we construct a CV-NIZK in the QRO + $(V \to P)$ model. As a result, we obtain the following theorem.

Theorem 5.2. *There exists a CV-NIZK for* **QMA** *in the QRO + $(V \to P)$ model.*

Let $L = (L_{\mathsf{yes}}, L_{\mathsf{no}})$ be a **QMA** promise problem, H be a random oracle, and $\Pi_\Sigma = (\Sigma.\mathsf{Preprocess}, \Sigma.\mathsf{Prove}_1, \Sigma.\mathsf{Verify}_1, \Sigma.\mathsf{Prove}_2, \Sigma.\mathsf{Verify}_2)$ be a Σ-protocol with quantum preprocessing (with $(1-\mathsf{negl}(\lambda))$-completeness and $\mathsf{negl}(\lambda)$-soundness). Then our CV-NIZK in the QRO + $(V \to P)$ model $\Pi_{\mathsf{QRO}} = (\mathsf{Preprocess}_{\mathsf{QRO}}, \mathsf{Prove}_{\mathsf{QRO}}, \mathsf{Verify}_{\mathsf{QRO}})$ for L is described in Figure 5.

Lemma 5.2. *Π_{QRO} satisfies $(1 - \mathsf{negl}(\lambda))$-completeness and adaptive $\mathsf{negl}(\lambda)$-soundness.*

Correctness is clear. Soundness is shown by using the measure-and-reprogram lemma shown in [DFM20].

Lemma 5.3. *Π_{QRO} satisfies adaptive multi-theorem zero-knowledge property.*

This is proven by using adaptive reprogramming lemma shown in [GHHM20].

$\mathsf{Preprocess}_{\mathsf{QRO}}(1^\lambda)$**:** It runs $\Sigma.\mathsf{Preprocess}(1^\lambda) \to (\Sigma.k_V, \Sigma.k_P)$, and outputs $k_V := \Sigma.k_V$ and $k_P := \Sigma.k_P$.

$\mathsf{Prove}^H_{\mathsf{QRO}}(k_P, \mathtt{x}, \mathtt{w}^{\otimes k})$**:** It parses $\Sigma.k_P \leftarrow k_P$, and runs $\Sigma.\mathsf{Prove}_1(k_P, \mathtt{x}, \mathtt{w}^{\otimes k}) \to (\mathsf{msg}_1, \mathsf{st})$. It computes $\mathsf{msg}_2 := H(\mathtt{x}, \mathsf{msg}_1)$. It runs $\Sigma.\mathsf{Prove}_2(\mathsf{st}, \mathsf{msg}_2) \to \mathsf{msg}_3$. It outputs $\pi := (\mathsf{msg}_1, \mathsf{msg}_3)$.

$\mathsf{Verify}^H_{\mathsf{QRO}}(k_V, \mathtt{x}, \pi)$**:** It parses $\Sigma.k_V \leftarrow k_V$ and $(\mathsf{msg}_1, \mathsf{msg}_3) \leftarrow \pi$. It computes $\Sigma.\mathsf{Verify}_2(k_V, \mathtt{x}, \mathsf{msg}_1, H(\mathtt{x}, \mathsf{msg}_1), \mathsf{msg}_3)$. If the output is $\bot$, it outputs $\bot$. If the output is $\top$, it outputs $\top$.

Fig. 5. CV-NIZK in the QRO + $(V \to P)$ model Π_{QRO}.

Shared Bell-pair model. Remark that the verifier of Π_{QRO} just sends a state $\rho_P := \bigotimes_{j=1}^N (U(W_j)|m_j\rangle)$ for $(W_1, ..., W_N) \xleftarrow{\$} \{X, Y, Z\}^N$ and $(m_1, ..., m_N) \xleftarrow{\$} \{0,1\}^N$ while keeping $(W_1, ..., W_N, m_1, ..., m_N)$ as a verification key. This step can be done in a non-interactive way if N Bell-pairs are a priori shared between the prover and verifier. That is, the verifier can measure his halves of Bell pairs in a randomly chosen bases $(W_1, ..., W_N)$ to get measurement outcomes $(m_1, ..., m_N)$. Apparently, this does not harm either of soundness or zero-knowledge since the protocol is the same as Π_{QRO} from the view of the prover and the malicious verifier's power is just weaker than that in Π_{QRO} in the sense that it cannot control the quantum state to be sent to the prover. Thus, we obtain the following theorem.

Theorem 5.3. *There exists a CV-NIZK for* **QMA** *in the QRO + shared Bell pair model.*

References

ACGH20. G. Alagic, A. M. Childs, A. B. Grilo, and S.-H. Hung. Non-interactive Classical Verification of Quantum Computation. In *TCC 2020, Part III*, pages 153–180. 2020.

BCKM21. J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma. On the Round Complexity of Secure Quantum Computation. In *CRYPTO 2021, Part I*, pages 406–435, Virtual Event, 2021.

BCR86. G. Brassard, C. Crépeau, and J.-M. Robert. Information Theoretic Reductions among Disclosure Problems. In *27th FOCS*, pages 168–173. 1986.

BCR87. G. Brassard, C. Crépeau, and J.-M. Robert. All-or-Nothing Disclosure of Secrets. In *CRYPTO'86*, pages 234–238. 1987.

BD18. Z. Brakerski and N. Döttling. Two-Message Statistically Sender-Private OT from LWE. In *TCC 2018, Part II*, pages 370–390. 2018.

BFM88. M. Blum, P. Feldman, and S. Micali. Non-Interactive Zero-Knowledge and Its Applications (Extended Abstract). In *20th ACM STOC*, pages 103–112. 1988.

BG20. A. Broadbent and A. B. Grilo. QMA-hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge. In *61st FOCS*, pages 196–205. 2020.

BHY09. M. Bellare, D. Hofheinz, and S. Yilek. Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening. In *EUROCRYPT 2009*, pages 1–35. 2009.

BJSW20. A. Broadbent, Z. Ji, F. Song, and J. Watrous. Zero-Knowledge Proof Systems for QMA. *SIAM J. Comput.*, 49(2):245–283, 2020.

BM21. J. Bartusek and G. Malavolta. Candidate Obfuscation of Null Quantum Circuits and Witness Encryption for QMA. *IACR Cryptology ePrint Archive*, 2021:421, 2021.

BS20. N. Bitansky and O. Shmueli. Post-quantum zero knowledge in constant rounds. In *52nd ACM STOC*, pages 269–279. 2020.

Can20. R. Canetti. Universally Composable Security. *J. ACM*, 67(5):28:1–28:94, 2020.

CNs07. J. Camenisch, G. Neven, and a. shelat. Simulatable Adaptive Oblivious Transfer. In *EUROCRYPT 2007*, pages 573–590. 2007.

CVZ20. A. Coladangelo, T. Vidick, and T. Zhang. Non-interactive Zero-Knowledge Arguments for QMA, with Preprocessing. In *CRYPTO 2020, Part III*, pages 799–828. 2020.

DFM20. J. Don, S. Fehr, and C. Majenz. The Measure-and-Reprogram Technique 2.0: Multi-round Fiat-Shamir and More. In *CRYPTO 2020, Part III*, pages 602–631. 2020.

DFMS19. J. Don, S. Fehr, C. Majenz, and C. Schaffner. Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model. In *CRYPTO 2019, Part II*, pages 356–383. 2019.

DMP90. A. De Santis, S. Micali, and G. Persiano. Non-Interactive Zero-Knowledge with Preprocessing. In *CRYPTO'88*, pages 269–282. 1990.

FHM18. J. F. Fitzsimons, M. Hajdušek, and T. Morimae. Post hoc verification with a single prover. *Phys. Rev. Lett.*, 120:040501, 2018.

FLS99. U. Feige, D. Lapidot, and A. Shamir. Multiple NonInteractive Zero Knowledge Proofs Under General Assumptions. *SIAM J. Comput.*, 29(1):1–28, 1999.

FS87. A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *CRYPTO'86*, pages 186–194. 1987.

GHHM20. A. B. Grilo, K. Hövelmanns, A. Hülsing, and C. Majenz. Tight adaptive reprogramming in the QROM, arXiv:2010.15103, 2020.

GMR89. S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

GOS12. J. Groth, R. Ostrovsky, and A. Sahai. New Techniques for Noninteractive Zero-Knowledge. *J. ACM*, 59(3):11:1–11:35, 2012.

GS12. J. Groth and A. Sahai. Efficient Noninteractive Proof Systems for Bilinear Groups. *SIAM J. Comput.*, 41(5):1193–1232, 2012.

GSY19. A. B. Grilo, W. Slofstra, and H. Yuen. Perfect Zero Knowledge for Quantum Multiprover Interactive Proofs. In *60th FOCS*, pages 611–635. 2019.

IKLP06. Y. Ishai, E. Kushilevitz, Y. Lindell, and E. Petrank. Black-box constructions for secure computation. In *38th ACM STOC*, pages 99–108. 2006.

Kob03. H. Kobayashi. Non-interactive Quantum Perfect and Statistical Zero-Knowledge. In *Algorithms and Computation, 14th International Sympo-*

sium, ISAAC 2003, Kyoto, Japan, December 15-17, 2003, Proceedings, pages 178–188. 2003.

Lin08. A. Y. Lindell. Efficient Fully-Simulatable Oblivious Transfer. In *CT-RSA 2008*, pages 52–70. 2008.

LZ19. Q. Liu and M. Zhandry. Revisiting Post-quantum Fiat-Shamir. In *CRYPTO 2019, Part II*, pages 326–355. 2019.

Mah18. U. Mahadev. Classical Homomorphic Encryption for Quantum Circuits. In *59th FOCS*, pages 332–338. 2018.

MNS18. T. Morimae, D. Nagaj, and N. Schuch. Quantum proofs can be verified using only single-qubit measurements. *Phys. Rev. A*, 93:022326, 2018.

NP01. M. Naor and B. Pinkas. Efficient oblivious transfer protocols. In *Proceedings of the Twelfth Annual Symposium on Discrete Algorithms, January 7-9, 2001, Washington, DC, USA*, pages 448–457. 2001.

Ps05. R. Pass and A. shelat. Unconditional Characterizations of Non-interactive Zero-Knowledge. In *CRYPTO 2005*, pages 118–134. 2005.

PS19. C. Peikert and S. Shiehian. Noninteractive Zero Knowledge for NP from (Plain) Learning with Errors. In *CRYPTO 2019, Part I*, pages 89–114. 2019.

PVW08. C. Peikert, V. Vaikuntanathan, and B. Waters. A Framework for Efficient and Composable Oblivious Transfer. In *CRYPTO 2008*, pages 554–571. 2008.

Qua20. W. Quach. UC-Secure OT from LWE, Revisited. In *SCN 20*, pages 192–211. 2020.

Reg09. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

Shm21. O. Shmueli. Multi-theorem Designated-Verifier NIZK for QMA. In *CRYPTO 2021, Part I*, pages 375–405, Virtual Event, 2021.

Unr15. D. Unruh. Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model. In *EUROCRYPT 2015, Part II*, pages 755–784. 2015.