MPC in the Quantum Head (or: Superposition-Secure (Quantum) Zero-Knowledge)

Andrea Coladangelo[1], Ruta Jawale[2], Dakshita Khurana[3], Giulio Malavolta[4], and Hendrik Waldner[5]

[1]University of Washington
[2]University of Illinois, Urbana-Champaign
[3]University of Illinois, Urbana-Champaign and NTT Research
[4]Bocconi University
[5]CISPA

The MPC-in-the-head technique (Ishai et al., STOC 2007) is a celebrated method to build zero-knowledge protocols with desirable theoretical properties and high practical efficiency. This technique has generated a large body of research and has influenced the design of real-world post-quantum cryptographic signatures. In this work, we present a generalization of the MPC-in-the-head paradigm to the quantum setting, where the MPC is running a quantum computation.

As an application of our framework, we propose a new approach to build zero-knowledge protocols where security holds even against a verifier that can obtain a *superposition* of transcripts. This notion was pioneered by Damgård et al., who built a zero-knowledge protocol for NP (in the common reference string model) secure against superposition attacks, by relying on perfectly hiding and unconditionally binding dual-mode commitments. Unfortunately, no such commitments are known from standard cryptographic assumptions. In this work we revisit this problem, and present two new three-round protocols in the common reference string model: (i) A zero-knowledge argument for NP, whose security reduces to the standard learning with errors (LWE) problem. (ii) A zero-knowledge argument for QMA from the same assumption.

Contents

1 Introduction

The MPC-in-the-head paradigm [30] is a celebrated method to build zero-knowledge (ZK) proof systems. Loosely speaking, it allows one to bootstrap a *semi-honest* multi-party computation (MPC) scheme into a ZK proof system, by letting a prover run an MPC protocol *in their head* and then selectively reveal parts of the transcript to the verifier, who checks for consistency in the views that have been revealed. The original motivation for this technique was to build *constant rate* zero-knowledge protocols, but over the years this method has found more applications in the design of concretely efficient ZK proofs [5, 15, 26] and digital signature schemes [15, 33].In this work, we propose a quantum generalization of the MPC-in-the-head paradigm and show how it can be used to construct ZK protocols with security against *superposition* attacks.

Superposition security is an emerging notion in cryptography that allows the adversary to query a given oracle on a *superposition* of inputs, which may leak more information than classical queries alone. This notion has been fruitfully studied in the context of random oracles [9, 20, 22], pseudorandom functions [43], message authentication codes [7, 25], encryption and signature schemes [8, 24], and zero-knowledge protocols [19]. While superposition security is interesting from a theoretical standpoint as a natural generalization of "classical-query" security, it is also well-motivated in many practical settings. For instance, consider a computing device that runs a program on some some hidden secret information. A quantum adversary with access to such a device can cool it down and force quantum effects on it, allowing for the aforementioned superposition attacks. Though this may at first seem implausible, similar types of (classical) attacks have already been performed in the context of side channel leakage on cryptographic hardware, which was also previously considered implausible [28, 29, 42].

In the future, various (classical) primitives might natively be connected through quantum networks, either to benefit from speed-ups or because some of the parties participating in the protocol are inherently quantum. In such a setting, for example, one party may use a quantum computer to encrypt messages for another party whose prescribed implementation is classical. One might try to enforce classical communication by requiring honest parties to measure all incoming messages. However, this shifts the security of the protocol onto an additional physical assumption: that the honest party's device really performs the intended measurement, and does not preserve or process quantum coherence in a way that a quantum adversary could exploit. Proving superposition security avoids relying on such an implementation-specific assumption. Other examples in which an attacker may be able to trick a classical device into exhibiting quantum behavior arise when a classical scheme is used as a subprotocol in a larger quantum protocol [31]. A prominent example of a primitive satisfying a superposition-security notion is that of superposition-secure pseudorandom functions (qPRFs) [43]. qPRFs and related superposition-secure symmetric-key primitives have since been used as building blocks in a range of quantum-secure constructions, including quantum-secure signatures [7], QCCA1-secure secret-key encryption of quantum data [2], and authenticated encryption [6].Beyond these classical cryptographic applications, they also underlie constructions of pseudorandom quantum states [11], pseudorandom unitaries [10], and quantum obfuscation [3]. This body of work suggests that superposition security is not only a natural strengthening of classical security, but also a useful design principle for primitives that are intended to be composed within larger quantum-secure protocols. A similar setting in which one could imagine using a superposition-secure zero-knowledge protocol is in GMW-style compilers [27], where zero knowledge is used to amplify the security of semi-honest multiparty computation protocols to malicious security. In the presence of a quantum adversary, one could analogously seek such a compiler that provides security amplification even against superposition attacks. Such a compiler would naturally require the underlying zero-knowledge protocol to remain secure under superposition access. We therefore view superposition-secure zero-knowledge as a natural addition to this landscape.

ZK under Superposition Attacks. In this work, we build proof systems whose zero-knowledge property holds even when the quantum verifier is allowed to issue several different challenges to the prover in superposition, and to receive the corresponding responses in superposition. The only known proof system in this setting, proposed by Damgård et al. [19], is a three-round protocol based on a perfectly hiding and binding dual-mode commitment. Unfortunately, such commitments are not known to exist from standard cryptographic assumptions. Furthermore, their proof technique

does not appear to easily generalize to prove QMA statements, the natural quantum analogue of NP. Our work aims to address these drawbacks.

As already observed by Damgård et al. [19], any non-interactive zero-knowledge (NIZK) proof is *trivially* superposition secure, since the verifier does not make any "queries" to the prover. However, to the best of our knowledge, NIZKs for QMA are not known to exist under any standard cryptographic assumptions. The main candidate NIZK for QMA that we are aware of [3] is in an oracle model and relies on strong heuristic assumptions about classical obfuscation. Another NIZK construction [1], in the quantum random oracle model, requires designated verifiers which results in interaction between the prover and the verifier during the setup procedure. To adequately adapt the model of superposition security to this setting, we would need to prove security against an adversary that can ask superposition queries in the setup as well. We leave this as future work and focus on the setting where the setup only outputs public information.

Furthermore, even in the simpler setting of ZK for NP, our three-round protocols are essentially specialized Σ-protocols; these are significantly more lightweight than (post-quantum) NIZKs.

Our Contributions. We build ZK with superposition security for languages in QMA, based on the learning with errors (LWE) assumption. The main building block needed for this result, and the main technical contribution of this work, is the first instantiation of the MPC-in-the-head paradigm [30] for quantum functionalities.

Theorem 1.1 (Informal)**.** *Assuming the post-quantum security of LWE, there exist three-round Σ-protocols for QMA in the CRS model satisfying zero-knowledge against malicious verifiers that make superposition queries to a prover.*

As a warmup, we consider the (weaker) setting of superposition-secure ZK for languages in *NP*. Here, we obtain Σ-protocols satisfying superposition security against malicious verifiers based on *any* dual-mode commitment scheme, allowing for instantiations based on the learning with errors (LWE) assumption. This improves prior work [19] which relied on perfectly binding dual-mode commitments, that were not known to exist based on standard assumptions. This leads to the following (informal) theorem.

Theorem 1.2 (Informal)**.** *Assuming the existence of any post-quantum dual-mode commitments, there exist three-round Σ-protocols for NP in the CRS model satisfying zero-knowledge against malicious verifiers that make superposition queries to a prover.*

Note that post-quantum dual-mode commitments exist from various assumptions, including LWE [38], which implies that our results can be based on the standard post-quantum hardness of the LWE problem.

1.1 Our Techniques

In the following, we provide a somewhat informal and brief overview of our techniques, and we refer the reader to the subsequent sections for more details.

1.1.1 Superposition-Secure Zero-Knowledge for NP

Before presenting our protocol, it is useful to recap the three-round protocol of [19], based on the MPC-in-the-head paradigm. Their protocol is the following:

- Let x be the instance of the problem. To compute its first message, the prover, on input a witness w, runs, in its head, an MPC protocol that computes the NP relation $\mathcal{R}(x, m_1 \oplus \cdots \oplus m_n)$ where m_i is the input of the i-th party and $m_1 \oplus \cdots \oplus m_n = w$ (in other words, one can think of $m_1, \ldots, m_n$ as shares of an n-out-of-n secret sharing of the witness). Then, the prover generates commitments to the views of the parties of the previously executed protocol and sends them over to the verifier as the first message.
- The verifier asks the prover to open a uniformly sampled subset of these commitments.

- The prover responds with the corresponding openings. If the openings are valid, the verifier checks that the views are correct (by checking that all local operations are executed correctly and that all messages are passed consistently across parties), and that the output of the prover's MPC protocol was "accept". If so, the verifier outputs "accept".

The soundness of this protocol, in the presence of quantum adversaries, follows by appealing to the (perfect) robustness of the MPC (similarly as in the classical case)[1]. On the other hand, zero-knowledge needs to be proven against a malicious verifier that asks the prover for a superposition of openings. This is shown in two steps:

- First, since the underlying MPC protocol achieves perfect privacy, the messages of the prover can be viewed as a secret sharing of the witness, and therefore remains hidden as long as the verifier only receives openings of a small enough subset of views.
- Second, and this is the key novelty in the argument of Damgård et al. [19], one invokes the following lemma.

  Lemma 1.3 ([19], informal)**.** *A t-out-of-n perfectly secure secret sharing scheme remains perfectly secure even if the distinguisher queries the shares in superposition, as long as less than $2t$ shares are queried.*

We highlight that this approach crucially relies on the fact that the commitment scheme being used is *perfectly* hiding. Otherwise, one cannot directly argue that the opened views of the MPC, together with the unopened commitments, are a perfectly secure secret sharing scheme. For instance, if the secret sharing scheme is only computationally hiding, then an unbounded adversary can simply learn the shares that the prover did not open. Quite surprisingly though, even for a *statistically* secure secret sharing scheme it is not easy to argue that the resulting secret sharing scheme resists superposition attacks! Indeed, as far as we know, it is an interesting open question to determine whether Lemma 1.3 holds if we replace "perfect" with "statistical" security.[2]

Our Technique. In this work, we overcome the aforementioned issue via a new proof strategy. We rely on *dual-mode commitments*, where a common reference string is sampled in one of two indistinguishable modes. The commitment is statistically binding in one mode and statistically (but not perfectly) hiding in the other. In order to establish the zero knowledge property, we rely (only) on the statistically hiding mode of the commitment. In the proof, we introduce an additional hybrid where all of the commitments that the prover sends are commitments to 0 (as opposed to the honestly generated MPC views). Since these commitments are statistically hiding, and thus only computationally binding, they can still be *opened* by the prover to the same honest MPC views as before (with a small statistical security loss). Of course, the latter cannot be done efficiently, but this is fine for the purposes of the reduction in this proof, since an efficient quantum verifier that distinguishes the two hybrids still implies an (inefficient) adversary that breaks the statistical hiding property.[3] Once we have made this change, we observe that the commitments to 0 generated by the prover, together with (a small enough) subset of openings to honest MPC views, correspond to (a small enough number of) shares of a *perfectly* secure secret sharing scheme. From here on, we can conclude the security proof by applying similar arguments as in [19]. The formal description and analysis of this protocol can be found in Section 3.

[1] An MPC protocol is t-robust if any set of corrupted parties of size at most t cannot make an honest party output the incorrect output of the circuit being computed.

[2] Morally, Lemma 1.3 is proven using a similar idea as a subsequent result by Zhandry [44] showing that q quantum queries to a uniformly random oracle can be simulated using a $2q$-wise family of hash functions. There, the result is also not known to extend to approximate $2q$-wise hash functions. This is because, in the statistical case, the security loss is the sum of exponentially many (exponentially small) losses. These are all zero in the perfect case. An avid reader might think that subexponential security might help to overcome this issue but this still does leave open the question of the superposition security for statistical secure secret sharing schemes.

[3] To provide answers to quantum queries here, we apply the same operation (modeled as a unitary), controlled on the received quantum state.

1.1.2 MPC in the Quantum Head

Upgrading the above protocol to a superposition-secure zero-knowledge protocol for QMA presents the following challenge: a QMA verification circuit is quantum, and the witness is a quantum state, so we need to consider a multiparty *quantum* computation protocol (MPQC) rather than an MPC protocol. However, in adapting the MPC-in-the-head paradigm to an MPQC protocol, we run into the following fundamental obstacle: since an MPQC protocol involves quantum inputs computation and communication, the views of the parties in the protocol are no longer classical, and there is no well-defined notion of a *transcript* that the verifier can check for consistency. In a bit more detail, in each round of an MPQC protocol, each party receives quantum messages from another party and operates on them using its private quantum state. Therefore, at the end of the protocol, a party is not in possession of a full transcript of the execution but only of its final state! This makes it harder to verify the correctness of the computation. We resolve this obstacle with the following idea:

- We view the global MPQC protocol, including the exchange of messages, as a quantum circuit (where message passing is substituted by SWAP gates). We then apply Kitaev's circuit-to-Hamiltonian reduction [36] to this quantum circuit to obtain a local Hamiltonian (recall that the local terms of this Hamiltonian serve to enforce the correct execution of the computation). The ground state of this Hamiltonian, also referred to as the *history state*, has low-energy *if and only if the MPQC protocol accepts* (on a well-formed input), i.e. if and only if the QMA verification has a valid witness.

- Similarly as in [13], the prover commits to the *history state* of the Hamiltonian (this commitment is done qubit-by-qubit, so that an arbitrary subset of qubits can be opened while the others stay hidden). The verifier then asks the prover to open the qubits corresponding to one of the Hamiltonian terms. Upon receiving the opening, the verifier can measure the Hamiltonian term, and check that the energy is below a certain threshold. This check, averaged over all of the Hamiltonian terms, ensures that the history state corresponds to a correctly executed MPQC protocol (with an accepting output), and thus ensures soundness.

- The ZK property follows from the following crucial observation: opening only the qubits corresponding to any one of the local checks of the Hamiltonian does not reveal any more information about the witness than what could be learnt by controlling a small subset of parties in the MPQC protocol. Since the MPQC protocol (similarly to the classical MPC-in-the-head setting) is running the QMA verification circuit on a *secret-sharing* of the witness, this ensures that no information about the witness is revealed.

We call this approach *MPC in the quantum head*. This can be seen as a generalization and abstraction of the approach taken by Broadbent and Grilo in [12]. In more detail, the locally simulatable proofs they introduce, relying on the circuit-to-Hamiltonian reduction and the local Hamiltonian problem in the same way as we do, realizes similar properties to the properties we rely on in this work, i.e., allowing for verification while only revealing parts of the witness. In order to instantiate our approach, we identify a suitable notion of MPQC, and show that the MPQC protocol of Crepeau et al. [17], with an adapted security analysis (described in Section 2.6), suffices for our purpose.

This generalization of the approach of Broadbent and Grilo [12] using MPQC [17] is the main conceptual contribution of this work. We believe that this technique can be extended to other commit-and-open [14, 18, 21] and cut-and-choose protocols [16, 32, 40, 41], as well as to other protocols requiring partial verification of quantum computations. Besides the applications to security against superposition attacks, we envision that such a technique could be used to show QMA-hardness of problems beyond CLDM [12]. We leave this exploration as a fascinating open research direction.

We provide a bit more detail about our MPC-in-the-quantum-head approach. In our MPQC protocol (which is meant to be executed "in the head"), the QMA witness is secret-shared across the parties in the following way: the witness $|w\rangle$ is encrypted using a quantum one-time pad $|v\rangle = X^a Z^b |w\rangle$ and shares (a_i, b_i) of the key are distributed among the first $n-1$ parties. The n^{th} party (which we shall think of as a dummy party) does not receive a key share but the quantum one-time pad encryption $|v\rangle$ instead. The MPQC executes the circuit that

(i) Recombines all the key shares (a_i, b_i) of the first $n-1$ parties to obtain the key (a, b), and uses it to decrypt the ciphertext $|v\rangle$, which is provided by the n^{th} party, to obtain the witness $|w\rangle$.

(ii) Runs the QMA verification circuit on the recovered witness $|w\rangle$.

As outlined above, the prover in our ZK protocol commits to a *history state* of the Hamiltonian corresponding to the "global" MPQC circuit. This commitment is also done using a quantum one-time pad: to commit to the history state $|\psi_{hist}\rangle$, apply a uniformly random one-time pad to obtain $|\phi\rangle = X^a Z^b |\psi\rangle$, and then use the dual-mode commitment to commit to the (classical) keys a, b. This results in a commitment scheme that is *dual-mode*: in one mode it is statistically hiding and computationally binding, and in the other it is perfectly binding and computationally hiding. Furthermore, the two modes are computationally indistinguishable.

The proof of the ZK property of this protocol uses a similar technique as the one we described in Section 1.1.1 to obtain a superposition-secure ZK protocol for NP. The key difference is that now, instead of introducing a hybrid where the prover commits to 0's, like we did earlier, we introduce a hybrid where all of the commitments are replaced with commitments to half of an EPR pair. This allows an unbounded prover to open each commitment to an arbitrary quantum state $|\psi\rangle$ as follows: teleport $|\psi\rangle$ into the committed register, and then inefficiently open the (computationally binding) commitments of the one-time pad keys to the teleportation errors.

An interesting difference compared to the classical setting is that our MPQC-in-the-head framework does *not* require the underlying MPC to be perfectly correct, nor robust, as was the case for [30]. This is due to the fact that we can "force" parties in the MPQC to sample their random coins honestly (for instance, by measuring a $|+\rangle$ state), whereas no such procedure exists classically.

2 Preliminaries

In this section, we introduce all the necessary preliminaries for our protocols. We start with the local Hamiltonian problem.

2.1 Local Hamiltonian Problem is QMA-complete

Definition 2.1 (QMA [35])**.** *Let $\mathcal{B}$ be the Hilbert space of a qubit. Fix $\epsilon(\cdot)$ such that $2^{-\Omega(\cdot)} \leq \epsilon(\cdot) \leq \frac{1}{3}$. Then, a promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no}) \in$ QMA if there exists a quantum polynomial-size family of circuits $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and a polynomial $p(\cdot)$ such that:*

- *For all $x \in \mathcal{L}_{yes}$, there exists $|\xi\rangle \in \mathcal{B}^{\otimes p(|x|)}$ such that $\Pr\left[\mathcal{M}_{|x|}(|x\rangle, |\xi\rangle) = 1\right] \geq 1 - \epsilon(|x|)$.*
- *For all $x \in \mathcal{L}_{no}$, and for all $|\xi\rangle \in \mathcal{B}^{\otimes p(|x|)}$ it holds that $\Pr\left[\mathcal{M}_{|x|}(|x\rangle, |\xi\rangle) = 1\right] \leq \epsilon(|x|)$.*

Definition 2.2 (2-local Hamiltonian problem)**.** *The 2-local Hamiltonian problem with functions a, b where $b(n) > a(n)$ for all $n \in \mathbb{N}$ is the promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ defined as follows. An instance is a Hermitian operator on some number n of qubits, taking the following form:*

$$H = \sum_S d_S S$$

where each d_S is a real number and S is a "2-local" operator, i.e., it acts non-trivially only on 2 out of the n qubits.

- *$H \in \mathcal{L}_{yes}$ if the smallest eigenvalue of H is at most $a(n)$.*
- *$H \in \mathcal{L}_{no}$ if the smallest eigenvalue of H is at least $b(n)$.*

Theorem 2.3 (2-local Hamiltonian is QMA-complete [34])**.** *The 2-local Hamiltonian problem with functions a, b is QMA-complete if $b(n) - a(n) > 1/\mathsf{poly}(n)$.*

2.2 Circuit-to-Hamiltonian Reduction

We recall the notion of a Circuit-to-Hamiltonian reduction, and of a history state.

Lemma 2.4 (Lemma 3 of [34])**.** *There exists an efficiently computable map from quantum circuits $\mathcal{C}$ to 2-local Hamiltonians $H_{\mathcal{C}}$, which we refer to as a "Circuit-to-Hamiltonian reduction", that satisfies the following. Let $\epsilon > 0$.*

(i) If there exists a state $|\nu\rangle$ such that $\mathcal{C}$ outputs 1 on input $|\nu, 0\rangle$ with probability at least $1-\epsilon$, then $H_{\mathcal{C}}$ has an eigenvalue smaller than ϵ. Moreover, suppose that $\mathcal{C} = U_T \dots U_1$ for some 2-qubit unitaries $U_1, \dots, U_T$. Then, the state

$$|\phi_{hist}\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=1}^{T} U_t \dots U_1 |\nu, 0\rangle \otimes |t\rangle$$

is the ground state of $H_{\mathcal{C}}$ (i.e. the eigenvector with the lowest eigenvalue). We refer to this state as the "history state".

(ii) if, for all $|\nu\rangle$, $\mathcal{C}$ outputs 1 on input $|\nu, 0\rangle$ with proability at most ϵ, then all eigenvalues of $H_{\mathcal{C}}$ are larger than $\frac{1}{2} - \epsilon$.

By Definition 2.2, the Hamiltonian H can be written as $H = \sum_S d_S S$ where $d_S \in \mathbb{R}$ and S is a tensor product of Pauli operators where only two operators are Z or X, and others are $\mathbb{I}$.

In order to perform a verification, we need to convert H to a measurement and discuss the new thresholds. We can rescale H as

$$H' = \sum_S p_S \left(\frac{\mathbb{I} + \text{sign}(d_S) S}{2} \right)$$

where $p_S = \frac{|d_S|}{\sum_S |d_S|} \in [0, 1]$.

We now outline a verification scheme for a purported history state ρ. The verification that ρ is a ground state of H' involves repeating the following check:

- Sample a term S with probability p_S.
- Apply the measurement $\{M_1 = \frac{\mathbb{I}+S}{2}, M_{-1} = \frac{\mathbb{I}-S}{2}\}$ to get outcome $e \in \{1, -1\}$. Note that this measurement involves only the two qubits that S acts non-trivially on.
- Output accept iff $e = -\text{sign}(d_S)$.

On input a state ρ, the probability that the protocol accepts is $1 - \mathsf{Tr}[H'\rho] = \frac{1}{2} - \frac{\mathsf{Tr}[H\rho]}{2\sum_S |d_S|}$.

2.3 Commitment Schemes and Quantum One-Time Pad

Definition 2.5 (Commitment Scheme)**.** *$\mathcal{C} = (\mathsf{Gen}, \mathsf{Com})$ is a commitment scheme if it has the following syntax:*

- $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$*: The classical polynomial-time key generation algorithm on input security parameter 1^λ outputs public commitment key ck.*
- $c \leftarrow \mathsf{Com}(\mathsf{ck}, m; r)$*: The classical polynomial-time commitment algorithm on input commitment key ck, message m and randomness r outputs commitment c.*

$\mathcal{C}$ has the following properties:

- ***Perfect Binding**: For all messages m, m' such that $m \neq m'$, all randomness r, r', and all $\lambda \in \mathbb{N}$,*

$$\Pr_{\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)} [\mathsf{Com}(\mathsf{ck}, m; r) = \mathsf{Com}(\mathsf{ck}, m'; r')] = 0.$$

- ***Computational Hiding***: *For all quantum polynomial-size circuits* $\mathcal{D} = \{\mathcal{D}_\lambda\}_{\lambda\in\mathbb{N}}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for all messages* m *and* m'*, and all* $\lambda \in \mathbb{N}$*,*

$$\left| \Pr_{\substack{\mathsf{ck}\leftarrow\mathsf{Gen}(1^\lambda)\\ c\leftarrow\mathsf{Com}(\mathsf{ck},m)}} [\mathcal{D}_\lambda(\mathsf{ck},c)=1] - \Pr_{\substack{\mathsf{ck}\leftarrow\mathsf{Gen}(1^\lambda)\\ c'\leftarrow\mathsf{Com}(\mathsf{ck},m')}} [\mathcal{D}_\lambda(\mathsf{ck},c')=1] \right| \leq \mathsf{negl}(\lambda).$$

As an instantiation for the described commitments, we can rely on the work of [37], in which the authors present non-interactive commitments based on the LWE assumption.

Definition 2.6 (Dual-mode Commitment)**.** $\mathcal{C} = (\mathsf{Gen}_B, \mathsf{Gen}_H, \mathsf{Com})$ *is a dual-mode commitment scheme if it has the following syntax:*

- $\mathsf{ck}_B \leftarrow \mathsf{Gen}_B(1^\lambda)$*: In the binding mode, the classical polynomial-time key generation algorithm on input security parameter* 1^λ *outputs public commitment key* ck_B*.*
- $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$*: In the hiding mode, the classical polynomial-time key generation algorithm on input security parameter* 1^λ *outputs public commitment key* ck_H*.*
- $c \leftarrow \mathsf{Com}(\mathsf{ck}, m; r)$*: The classical polynomial-time commitment algorithm on input commitment key* ck *(generated either in binding or hiding mode), message* m *and randomness* r *outputs commitment* c*.*

$\mathcal{C}$ *has the following properties:*

- ***Indistinguishability of Modes:*** *For all quantum polynomial-size circuits* $\mathcal{D} = \{\mathcal{D}_\lambda\}_{\lambda\in\mathbb{N}}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for all* $\lambda \in \mathbb{N}$*,*

$$\left| \Pr_{\mathsf{ck}_H\leftarrow\mathsf{Gen}_H(1^\lambda)} [\mathcal{D}_\lambda(\mathsf{ck}_H)=1] - \Pr_{\mathsf{ck}_B\leftarrow\mathsf{Gen}_B(1^\lambda)} [\mathcal{D}_\lambda(\mathsf{ck}_B)=1] \right| \leq \mathsf{negl}(\lambda).$$

- ***Perfect Binding***: *For all messages* m*,* m' *such that* $m \neq m'$*, all randomness* r*,* r'*, and all* $\lambda \in \mathbb{N}$*,*

$$\Pr_{\mathsf{ck}_B\leftarrow\mathsf{Gen}_B(1^\lambda)} [\mathsf{Com}(\mathsf{ck}_B, m; r) = \mathsf{Com}(\mathsf{ck}_B, m'; r')] = 0.$$

- ***Statistical Hiding***: *For all quantum unbounded-size circuits* $\mathcal{D} = \{\mathcal{D}_\lambda\}_{\lambda\in\mathbb{N}}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for all messages* m *and* m'*, and all* $\lambda \in \mathbb{N}$*,*

$$\left| \Pr_{\substack{\mathsf{ck}_H\leftarrow\mathsf{Gen}_H(1^\lambda)\\ c\leftarrow\mathsf{Com}(\mathsf{ck}_H,m)}} [\mathcal{D}_\lambda(\mathsf{ck}_H,c)=1] - \Pr_{\substack{\mathsf{ck}_H\leftarrow\mathsf{Gen}_H(1^\lambda)\\ c'\leftarrow\mathsf{Com}(\mathsf{ck}_H,m')}} [\mathcal{D}_\lambda(\mathsf{ck}_H,c')=1] \right| \leq \mathsf{negl}(\lambda).$$

To instantiate the above described dual-mode commitment scheme, we rely on the work of Peikert, Vaikuntanathan and Waters [38] where the authors construct a LWE-based dual-mode cryptosystem, which can be cast as a commitment scheme.

Definition 2.7 (Quantum One-time Pad (Quantum OTP))**.** *Let* $m \in \mathbb{N}$ *and* $|\varphi\rangle$ *an* m*-qubit state be given. Let* a *and* b *be sampled uniformly at random from* $\{0,1\}^m$*. Let* $|\psi\rangle = X^a Z^b |\varphi\rangle$*. We say that* $|\varphi\rangle$ *is the Quantum OTP of* $|\psi\rangle$ *with keys* (a, b)*.*

Lemma 2.8. *Let* $m \in \mathbb{N}$ *and* $|\varphi\rangle$ *an* m*-qubit state be given. We have that*

$$\frac{1}{2^{2m}} \sum_{a,b\in\{0,1\}^m} X^a Z^b |\varphi\rangle\langle\varphi| Z^b X^a = \frac{1}{2^m}\mathbb{I}_m.$$

2.4 Zero-Knowledge

In this section, we define classical zero-knowledge notions as well as their quantum analogues in parenthesis.

Definition 2.9 (Zero-Knowledge Argument (for Promise Problem))**.** *Let* NP *relation* $\mathcal{R}$ *with corresponding language* $\mathcal{L}$ *be given such that they can be indexed by a security parameter* $\lambda \in \mathbb{N}$*. (Let* QMA *promise problem* $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ *be given with a corresponding deciding quantum polynomial-size circuit* $\mathcal{M}$*.)*

$\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *is a post-quantum (quantum) zero-knowledge argument for* NP *(for* QMA*) in the CRS model if it has the following syntax and properties.*

Syntax. *The input* 1^λ *is left out when it is clear from context.*

- Setup *is a probabilistic polynomial-size circuit that on input* 1^λ *outputs a common reference string* CRS*.*
- P *is an interactive probabilistic (quantum) polynomial-size circuit that takes as input a common reference string* CRS *and a pair* $(x, w) \in \mathcal{R}_\lambda$ *(where* $x \in \mathcal{L}_{yes}$ *with* $|x| = \lambda$*, and* $|w\rangle$ *is a valid witness).*
- V *is an interactive probabilistic (quantum) polynomial-size circuit* V *that takes as input a common reference string* CRS*, an instance* x*, and outputs* 0 *or* 1*.*

In the following, we use the notation $\langle \mathsf{P}(w), \mathsf{V}\rangle(\mathsf{CRS}, x)$ *to denote* V*'s output given an interaction with* P *where* (CRS, x) *are shared inputs and* w *is a private input to* P*.*

Properties.

- **Completeness:** *There exists a negligible function* $\mathsf{negl}(\cdot)$ *such that every* $\lambda \in \mathbb{N}$ *and every* $(x, w) \in \mathcal{R}_\lambda$ *(every* $x \in \mathcal{L}_{yes}$ *with a valid witness* $|w\rangle$ *and where* $|x| = \lambda$*),*

$$\Pr_{\mathsf{CRS} \leftarrow \mathsf{Setup}(1^\lambda)}[\langle \mathsf{P}(w), \mathsf{V}\rangle(\mathsf{CRS}, x) = 1] = 1$$
$$\left(\Pr_{\mathsf{CRS} \leftarrow \mathsf{Setup}(1^\lambda)}[\langle \mathsf{P}(|w\rangle), \mathsf{V}\rangle(\mathsf{CRS}, x) = 1] \geq 1 - \mathsf{negl}(\lambda)\right).$$

- **Computational Soundness:** *For every polynomial-size family of quantum circuits* $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for every* $\lambda \in \mathbb{N}$*, and every* $x \notin \mathcal{L}_\lambda$ *(every* $x \in \mathcal{L}_{no}$ *where* $|x| = \lambda$*),*

$$\Pr_{\mathsf{CRS} \leftarrow \mathsf{Setup}(1^\lambda)}[\langle \mathcal{A}_\lambda, \mathsf{V}\rangle(x, \mathsf{CRS}) = 1] \leq \mathsf{negl}(\lambda).$$

- **Computational Zero-Knowledge:** *There exists a probabilistic (quantum) polynomial-size circuit* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *such that for all polynomial-size quantum circuit* $\mathcal{A}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *for all* $\lambda \in \mathbb{N}$*, and all* $(x, w) \in \mathcal{R}_\lambda$ *(all* $x \in \mathcal{L}_{yes}$ *with a valid witness* $|w\rangle$ *and where* $|x| = \lambda$*),*

$$\left|\Pr_{\mathsf{CRS} \leftarrow \mathsf{Setup}(1^\lambda)}[\langle \mathsf{P}(w), \mathcal{A}\rangle(\mathsf{CRS}, x) = 1] - \Pr_{(\mathsf{CRS}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)}[\langle \mathsf{Sim}_1(\mathsf{td}), \mathcal{A}\rangle(\mathsf{CRS}, x) = 1]\right| \leq \mathsf{negl}(\lambda)$$
$$\left(\left|\Pr_{\mathsf{CRS} \leftarrow \mathsf{Setup}(1^\lambda)}[\langle \mathsf{P}(|w\rangle), \mathcal{A}\rangle(\mathsf{CRS}, x) = 1] - \Pr_{(\mathsf{CRS}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)}[\langle \mathsf{Sim}_1(\mathsf{td}), \mathcal{A}\rangle(\mathsf{CRS}, x) = 1]\right| \leq \mathsf{negl}(\lambda)\right).$$

Next, we define the notion of superposition security for zero-knowledge arguments. For notational convenience, we only define it for the special case of three-round protocols, although a more general definition can be derived by extending the syntax accordingly.

Definition 2.10 (Superposition-Secure Zero-Knowledge Argument)**.** *A protocol* $\Pi = (\mathsf{P}, \mathsf{V})$ *is a post-quantum (quantum) superposition-secure zero-knowledge argument if it is a post-quantum (quantum) zero-knowledge argument (Definition 2.9) where the zero-knowledge adversary is additionally given superposition-query access, and the simulator is a quantum polynomial-size circuit. Specifically, let* $\mathsf{Sim}_2^*(c) \to r_c$ *be next-message function of the simulator that, on input a challenge* $c \in \mathcal{C}$*, returns a response* r_c*, and let*

$$U_{\mathsf{Sim}_2} |c\rangle |y\rangle \to |c\rangle |y \oplus r_c\rangle$$

be its unitary implementation. Then we require that zero-knowledge holds even if the distinguisher can query U_{Sim_2} *once.*

2.5 Secret Sharing Scheme

Definition 2.11 (t-out-of-n Secret Sharing Scheme)**.** $S = (\mathsf{Share}, \mathsf{Reconstruct})$ *is a* t*-out-of-*n *secret sharing scheme over the set of all possible secrets* $\mathbb{S}$ *and randomness* $\mathcal{R}$ *if it has the following syntax and properties.*

Syntax.

- $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m; r)$*: The classical polynomial-time share algorithm that on any input secret* $s \in \mathbb{S}$ *and randomness* $r \in \mathcal{R}$ *outputs* n *shares* $(s_1, \ldots, s_n)$*.*
- $s \leftarrow \mathsf{Reconstruct}(s_1, \ldots, s_n)$*: The classical polynomial-time reconstruct algorithm that on any input of* n *shares* $(s_1, \ldots, s_n)$ *will output a secret* $s \in \mathbb{S}$*.*

Properties.

- ***Perfect*** t***-Correctness:*** *For all* $s \in \mathbb{S}$*, for all* $I \subseteq [n]$ *where* $|I| = t$*,*

$$\Pr_{(s_1,\ldots,s_n)\leftarrow\mathsf{Share}(s)}[\mathsf{Reconstruct}((s_i)_{i\in I}) = s] = 1.$$

- ***Perfect*** $(t-1)$***-Security:*** *For all* $s, s' \in \mathbb{S}$*, for all* $I \subseteq [n]$ *where* $|I| \leq t-1$*,*

$$\{(s_i)_{i\in I}\}_{(s_1,\ldots,s_n)\leftarrow\mathsf{Share}(s)} = \{(s'_i)_{i\in I}\}_{(s'_1,\ldots,s'_n)\leftarrow\mathsf{Share}(s')}.$$

2.6 Multiparty (Quantum) Computation

Definition 2.12 (Local consistency [30])**.** *We say that a pair of views* V_i*,* V_j *are consistent (with respect to the protocol* Π *and some public input* x*) if the outgoing messages implicit in* V_i *are identical to the incoming messages reported in* V_j *and vice versa.*

Lemma 2.13 (Local vs. global consistency [30])**.** *Let* Π *be an* n*-party protocol as above and* x *be a public input. Let* $V_1, \ldots, V_n$ *be an* n*-tuple of (possibly incorrect) views. Then all pairs of views* V_i*,* V_j *are consistent with respect to* Π *and* x *if and only if there exists an honest execution of* Π *with public input* x *(and some choice of private inputs* w_i *and random inputs* r_i*) in which* V_i *is the view of* P_i *for every* $1 \leq i \leq n$*.*

Definition 2.14 (Secure Multiparty Computation (MPC) [30])**.** Π *is MPC protocol with if it has the following syntax and properties.*

Syntax:

- *There are* n *parties* $P_1, \ldots, P_n$ *which all share a public input* x*. Each party, for* $i \in [n]$*,* P_i *holds a private input* w_i *and randomness* r_i*.*
- *It securely realizes an* n*-party functionality* f*, where* f *maps the inputs* $(x, w_1, \ldots, w_n)$ *to an* n*-tuple of outputs.*

- *It is specified via its next message function. That is,* $\Pi(1^\lambda, i, x, w_i, r_i, (m_1, \ldots, m_j))$ *returns the set of* n *messages (and, possibly, a broadcast message) sent by* P_i *in Round* $j+1$ *given security parameter* λ*, the public input* x*, its local input* w_i*, its random input* r_i*, and the messages* $m_1, \ldots, m_j$ *it received in the first* j *rounds.*
- *The output of* Π *may also indicate that the protocol should terminate, in which case* Π *returns the local output of* P_i *for its input* $i \in [n]$*.*
- *The view of* P_i*, for* $i \in [n]$*, denoted by* V_i*, includes* (w_i, r_i) *and the messages received by* P_i *during the execution of* Π*.*

Properties:

- ***Perfect Correctness****: For all inputs* $x, w_1, \ldots, w_n$*, the probability that the output of some player is different from the output of* f *is* 0*, where the probability is over the independent choices of the random inputs* $r_1, \ldots, r_n$*.*
- ***Perfect*** t***-Robustness:*** *We say that* Π *realizes* f *with perfect* t*-robustness if it is perfectly correct in the presence of a semi-honest adversary, and furthermore for any computationally unbounded malicious adversary corrupting a set* T *of at most* t *players, and for any inputs* $(x, w_1, \ldots, w_n)$*, the following robustness property holds. If there is no* $(w'_1, \ldots, w'_n)$ *such that* $f(x, w'_1, \ldots, w'_n) = 1$*, then the probability that some uncorrupted player outputs* 1 *in an execution of* Π *in which the inputs of the honest players are consistent with* $(x, w_1, \ldots, w_n)$ *is* 0*.*
- ***Perfect*** t***-Privacy:*** *Let* $1 \leq t \leq n$*. We say that* Π *realizes* f *with perfect* t*-privacy if there is a probabilistic polynomial-size circuit simulator SIM such that for any inputs* $x, w_1, \ldots, w_n$ *and every set of corrupted players* $T \subseteq [n]$*, where* $|T| \leq t$*, the joint view* $\mathsf{View}_T(x, w_1, \ldots, w_n)$ *of players in* T *is distributed identically to* $\mathsf{SIM}(T, x, (w_i)_{i \in T}, f_T(x, w_1, \ldots, w_n))$*.*

Theorem 2.15 (MPC [4])**.** *Let* $n \in \mathbb{N}, t < n/3$ *and* $t' < n/2$*, then there exists an* n*-party,* t*-robust, and perfectly* t'*-private MPC protocol (as in Definition 2.14).*

Proof (Sketch). To prove this theorem, we rely on the protocol of Ben-Or, Goldwasser and Wigderson [4]. We start by analysing the robustness of the protocol. In [4, Theorem 3], the authors show that for $t < n/3$ their protocol is t-resilient. Since the notion of resilience directly corresponds to the notion of robustness, the first half of the theorem follows.

To argue the privacy case, we rely on [4, Theorem 1], where the authors show that their protocol achieves t'-privacy for $t' < n/2$ against semi-honest adversaries. Since their protocol does not require any computational assumptions, perfect privacy directly follows. □

We now introduce a definition for a multi-party computation in the quantum setting. This definition, unlike our classical definition, is written in the real and ideal world paradigm.

Definition 2.16 (MPQC Syntax)**.** *For each round of a MPQC protocol, each party computes a local unitary on its input and exchange message registers with all other parties. We formalize this for an* n*-party,* K*-round MPQC protocol as follows:*

- ***Registers****: The* i*th party computes on one input register* Input_i*,* Kn *message registers for each party and each round of the protocol* $\{\mathsf{Message}_{i,j,k}\}_{j \in [n] \setminus \{i\}, k \in [K]}$*, and one output register* Output_i*.*
- ***Rounds****: During the* k*th round, a unitary* $U_{i,k}$ *is applied to the* i*th parties' registers for all* $i \in [n]$*, and a swap operation between* $\mathsf{Message}_{i,j,k}$ *and* $\mathsf{Message}_{j,i,k}$ *for all pairs of parties* $i, j \in [n]$ *with* $i \neq j$*.*
- ***Views****: Let* ρ *be the input to the* n *parties. The view of parties in* $T \subseteq [n]$ *in round* k*,* $\mathsf{View}_{T,k}(\rho)$*, is the reduced density on all registers for parties in* T *at the end of the* k*th round.*

Definition 2.17 (Secure Multiparty Quantum Computation (MPQC) [17, 39])**.** Π *is an* n*-party,* t*-robust, and* t*-private MPQC protocol which computes a quantum circuit* $\mathcal{C}$ *(with* n *inputs and* n *outputs) if we can define a "real" and "ideal" model with the following properties.*

Syntax. *The MPQC protocol can be written as in Definition 2.16.*

Real Model. *Given an adversary $\mathcal{A}$ which can corrupt at most t parties (but not abort), and an input configuration ρ:*

- *Every pair of parties are connected by perfect quantum and classical channels. There is a classical authenticated broadcast channel.*
- *When $t < n/3$, the parties can perform classical multi-party computations.*
- *Initial configuration is joint state ρ of $n+2$ systems: input system $\mathcal{I}_i$ containing the parties' inputs for $i \in [n]$, $\mathcal{A}$'s auxiliary input system $\mathcal{I}_{aux}$, and an outside reference system $\mathcal{I}_{ref}$; input can be an arbitrary quantum state, possibly entangling all these systems.*
- *Protocol interaction: all parties receive their input system $\mathcal{I}_i$ and $\mathcal{A}$ receives the state $\mathcal{I}_{aux}$; $\mathcal{A}$ chooses subset C of size at most t of parties to corrupt; $\mathcal{A}$ has access to the state of the players in C and controls what they send over the channels; $\mathcal{A}$ may cause the cheaters' systems to interact arbitrarily; $\mathcal{A}$ has no access to the state of the honest players and cannot intercept their communication; the reference system $\mathcal{I}_{ref}$ is untouched during this process.*
- *Output: all parties produce output (honest parties output according to the protocol); system output by party i is denoted $\mathcal{O}_i$; adversary outputs an additional system $\mathcal{O}_{aux}$.*
- *Output configuration: joint state of $\mathcal{O}_1, \ldots, \mathcal{O}_n$; $\mathcal{A}$'s state $\mathcal{O}_{aux}$; and the reference system $\mathcal{I}_{ref}$. This state depends on $\mathcal{A}$ and the initial configuration ρ, and is denoted $Real(\mathcal{A}, \rho)$. (This configuration does not include any ancillary states or workspace used by honest parties, only the output specified by the protocol, all other parts of the honest parties' systems are "traced out".)*

Ideal Model. *Given an adversary $\mathcal{A}$ which can corrupt at most t parties (but not abort), and an input configuration ρ:*

- *There is a trusted (uncorruptable) third party $\mathcal{TTP}$ which receives no input.*
- *The communications model is the same as in the real model, except that every party is connected to $\mathcal{TTP}$ via a perfect (i.e. authentic, secret) quantum channel.*
- *Initial configuration: n systems $\mathcal{I}_i$ containing the parties' inputs, system $\mathcal{I}_{aux}$, and system $\mathcal{I}_{ref}$.*
- *The protocol proceeds as in the real model, except that the players may interact with $\mathcal{TTP}$.*
- *Output: same as in real model (final state of $\mathcal{TTP}$ is not included); the output configuration for adversary $\mathcal{A}$ and initial configuration ρ is denoted $Ideal(\mathcal{A}, \rho)$.*

Given a quantum circuit $\mathcal{C} = U_T \ldots U_1$ with n inputs and n outputs:

- *Input: Each party gets an input system I_i.*
- *Input Sharing: For each party i, party i sends I_i to TTP. If TTP does not receive anything, then they broadcast "Party i is cheating" to all parties. Otherwise, TTP broadcasts "Party i is OK."*
- *Computation: TTP evaluates the circuit $\mathcal{C}$ on the inputs I_i. For all i who cheated, TTP creates I_i in a known state (say $|0\rangle$).*
- *Output: TTP sends i^{th} output to party i. Party i outputs the system they receive from TTP.*

Properties.

- ***Statistical Security:*** *There exists a quantum polynomial-time simulator* Sim *such that for all quantum unbounded-size circuits* $\mathcal{A}$ *that corrupt at most* t *parties and all sequences of input configurations* $\{\rho_\lambda\}$ *(possibly mixed or entangled), we have that for large enough* $\lambda \in \mathbb{N}$*:*

$$\|Real(1^\lambda, \mathcal{A}, \rho_\lambda) - Ideal(1^\lambda, \mathsf{Sim}^{\mathcal{A}}, \rho_\lambda)\|_1 \leq \frac{1}{2^{\lambda/2-1}}.$$

- ***Statistical Correctness:*** *For all initial configurations* $\{\rho_\lambda\}_{\lambda\in\mathbb{N}}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for all security parameters* $\lambda \in \mathbb{N}$ *it holds that*

$$\|\mathsf{Output}(1^\lambda, \rho_\lambda) - \mathcal{C}(\rho_\lambda))\|_1 \leq \mathsf{negl}(\lambda)$$

- ***Perfect*** t***-Privacy:*** *Let* $1 \leq t \leq n$ *and* K *be the number of rounds of the MPQC protocol. We say that* Π *realizes* $\mathcal{C}$ *with perfect* t*-privacy if there is a polynomial-size quantum circuit* Sim *such that for all input configurations* $\{\rho_\lambda\}_{\lambda\in\mathbb{N}}$*, all security parameters* $\lambda \in \mathbb{N}$*, all set of players* $T \subseteq [n]$ *where* $|T| \leq t$*, and all rounds* $k \in [K]$*, it holds that*

$$\mathsf{View}_{T,k}(1^\lambda, \rho_\lambda) \equiv \mathsf{Sim}(1^\lambda, T, \rho_\lambda|_T, \mathcal{C}_T(\rho_\lambda), k)$$

where $\mathsf{View}_{T,k}(1^\lambda, \rho_\lambda)$ *is defined in Definition 2.16.*

We highlight that there are two notions concerning the privacy of the parties' inputs in the definition above, statistical security and perfect privacy. The key difference between these two notions lies in the adversarial model: in statistical security, simulation needs to be achieved against a malicious adversary, arbitrarily choosing the messages output in the protocol, while, in the privacy notion, the confidentiality of the inputs only needs to be protected against an adversary that generates all of its messages accordingly to the protocol description.

In the theorem below, we show that there exists a statistically secure protocol that also achieves perfect privacy; trading weaker security for stronger indistinguishability while increasing the threshold by a factor of 2. Looking ahead, in the proof of our main protocol, we crucially rely on the perfect privacy of the MPQC.

Theorem 2.18 (MPQC [17, 39])**.** *Let* $n \in \mathbb{N}$ *and* $t < n/6$*. There exists an* n*-party, statistically secure against* t *corrupted parties, and perfectly* $2t$*-private MPQC protocol (as in Definition 2.17).*

Proof (Sketch). Since the work does not contain an explicit statement about t-privacy, we provide a sketch of the proof here. Before delving into the argument, it is useful to recall a high-level description of the main steps of the protocol. The protocol proceeds as follows:

- All parties share their input via a verifiable quantum secret sharing scheme.
- All computations are transversally over the shares, except for the measurement used in the degree reduction step. The result of this measurement is broadcast to all parties.
- To reconstruct the output, each party sends the share of their i-th output wire to the i-th party.

It is shown in [39, Lemma 2.23] that the measurement done in the degree-reduction step is independent of the inputs, and therefore broadcasting this value reveals no information about the inputs. The above described broadcasted value is the value that will be generated by the simulator $\mathsf{Sim}(1^\lambda, \ldots, k)$ for the corresponding round k. Thus, what is left to be shown is that the secret sharing protocol is perfectly simulatable for $2t$ shares. Crucially, as mentioned above, the notion of $2t$-privacy only requires simulatability in the presence of honest parties (i.e., the analysis does not need to take into account corrupted parties), which is the reason why one can prove perfect, as opposed to statistical, privacy. It is shown in [39, Section 2.2.6] (considering only the case where the dealer D is honest) that the secret sharing is perfectly private, as long as at most $n - (n - 2t) = 2t$ shares are revealed to the distinguisher. Informally, this is shown by arguing that the following procedures are equivalent:

- Share the input state using the honest algorithm.
- Share the $|0\rangle$ state, then run the ideal interpolation on an arbitrary set of $n - 2t$ honest parties. Swap the input state sent by the trusted third party, and run the ideal interpolation circuit backwards.

This equivalence follows by arguing that the verification of the verifiable secret sharing acts as the identity if the dealer D is honest. □

2.7 MPQC to Circuit-to-Hamiltonian

In the Section 4.2, we will apply the Circuit-to-Hamiltonian reduction to the circuit simulating the MPQC interaction. Given an MPQC protocol $\Pi_{\mathcal{C}}$, we derive the corresponding quantum circuit as follows: The inputs for the parties are given as inputs to the circuits, along with sufficiently many ancillas $|0\rangle$. The gates of the circuit correspond to the unitaries $U_{i,k}$ (computing the "next-message" function for each party) acting on each party's workspace, along with SWAP gates that correspond to sending the message to another party.

To argue the indistinguishability of the resulting history state, if different MPQC inputs are used that lead to the same circuit evaluation, i.e., $\mathcal{C}(x_\lambda^0) = \mathcal{C}(x_\lambda^1)$, we introduce and prove the following helping lemma.

Lemma 2.19. *Let $\mathcal{C}$ be a circuit computed by a perfectly t-private MPQC protocol $\Pi_{\mathcal{C}}$. Then, for all $\lambda \in \mathbb{N}$, the following holds. Let x_λ^0 and x_λ^1 be two (pure state) inputs such that $\mathcal{C}(x_\lambda^0) = \mathcal{C}(x_\lambda^1)$ and $x_\lambda^0|_T = x_\lambda^1|_T = x_\lambda|_T$, where T is a set of corrupted parties with $|T| \leq t$. Define $\phi_{hist,T}^0$ and $\phi_{hist,T}^1$ to be the reduced densities on the registers corresponding to the parties in T and the clock register, of the history states generated by executing $\Pi_{\mathcal{C}}(x_\lambda^0)$ and $\Pi_{\mathcal{C}}(x_\lambda^1)$, respectively. Then*

$$\phi_{hist,T}^0 \equiv \phi_{hist,T}^1.$$

Proof. First observe that, by the t-privacy of the MPQC protocol $\Pi_{\mathcal{C}}$, we have that

$$\mathsf{View}_{T,k}(1^\lambda, x_\lambda^0) \equiv \mathsf{Sim}(1^\lambda, T, x_\lambda|_T, \mathcal{C}_T(x_\lambda), k) \equiv \mathsf{View}_{T,k}(1^\lambda, x_\lambda^1)$$

for any step k of the computation, where the view $\mathsf{View}_{T,k}(1^\lambda, x_\lambda^b)$ is defined as in Definition 2.16. Recall that the Circuit-to Hamiltonian reduction results in a state that contains a superposition of all steps of the computation. Note that

$$\left|\phi_{hist}^b\right\rangle = \frac{1}{\sqrt{K+1}} \sum_{\kappa=1}^{K} U'_\kappa \dots U'_1 \left|x_\lambda^b, 0\right\rangle \otimes |\kappa\rangle = \frac{1}{\sqrt{K+1}} \sum_{\kappa=1}^{K} \mathsf{View}_\kappa(1^\lambda, x_\lambda^b) \otimes |\kappa\rangle$$

where U'_i denotes the unitary applied at the i-th step of the circuit. Let us consider each state $\mathsf{View}_\kappa(1^\lambda, x_\lambda^b) \otimes |\kappa\rangle$, for all κ. When tracing out all registers not in T, the argument above establishes that the two reduced densities (for $b = 0$ and $b = 1$) are identical. Thus, by Uhlmann theorem, there exists a unitary V_κ acting on the traced out system such that

$$(V_\kappa \otimes \mathsf{Id}_T)\mathsf{View}_\kappa(1^\lambda, x_\lambda^0) \otimes |\kappa\rangle = \mathsf{View}_\kappa(1^\lambda, x_\lambda^1) \otimes |\kappa\rangle\,.$$

We can assume without loss of generality that all honest parties of the MPQC keep track of the step number in one of its internal registers and we refer to one such register (that is not part of T) as R. Furthermore, we can assume that $V_\kappa = V'_\kappa \otimes \mathsf{Id}_R$, since the register R is in the state $|\kappa\rangle$ for both $\mathsf{View}_\kappa(1^\lambda, x_\lambda^0)$ and $\mathsf{View}_\kappa(1^\lambda, x_\lambda^1)$. This allows us to define $V = \sum_\kappa V'_\kappa \otimes |\kappa\rangle\langle\kappa|_R$, as the controlled application of V_κ on R. Then we have that

$$(V \otimes \mathsf{Id}_T)\left|\phi_{hist}^0\right\rangle = \left|\phi_{hist}^1\right\rangle$$

Observe that V does not act on any of the T registers, which implies that $\phi_{hist,T}^0 \equiv \phi_{hist,T}^1$. □

3 Superposition-Attack Secure, Zero-Knowledge Argument for NP

3.1 Secret Sharing Scheme Secure Against Superposition Attacks [19]

Definition 3.1 (Party views)**.** *Let $P_1, \ldots, P_n$ be parties in a secret sharing scheme S where $s \in \mathbb{S}$ is the secret shared using randomness $r \in \mathcal{R}$. Each party, P_i, receives a share $v_i(s;r) \in \{0,1\}^k$, also called its private view. For $A \subset [n]$, let $v_A(s;r) = \{v_i(s;r)\}_{i \in A}$ be the string containing the concatenation of views for parties P_i with $i \in A$.*

Definition 3.2 (Perfect security)**.** *Let G be a family of subsets of $2^{[n]}$. A secret sharing scheme S is perfectly secure against classical G-attacks if for any $A \in G$, the distribution of shares $v_A(s;r) \in \{0,1\}^t$ does not depend on s.*

Definition 3.3 (Adversary structure)**.** *The adversary structure of a secret sharing scheme is the maximal $G \subset 2^{[n]}$ for which the scheme is perfectly secure against classical G-attacks (Definition 3.2).*

Definition 3.4 (Perfect security against superposition attacks)**.** *A secret sharing scheme S is perfectly secure against superposition F-attacks if, and only if, for all unitary matrices,*

$$U_{query}^{adv,F} \; : \; \mathcal{H}_{env} \otimes \mathcal{H}_{query} \to \mathcal{H}_{env} \otimes \mathcal{H}_{query}$$

and all possible pairs of inputs, $s, s' \in \mathbb{S}$ it holds that $\rho_s^{adv,F} = \rho_{s'}^{adv,F}$, where for $s^* \in \{s, s'\}$

$$\begin{aligned} \rho_{s^*}^{adv,F} &= \sum_{r \in \mathcal{R}} p_r \left|\psi_{adv,F,s^*}\right\rangle \left\langle\psi_{adv,F,s^*}\right|, \text{ and} \\ \left|\psi_{adv,F,s^*}\right\rangle &= U_{query}^{adv,F} \left(\sum_x \alpha_x \left|x\right\rangle_e \otimes \left|0,0\right\rangle_q \right) \\ &= \sum_{x, A \in F, a \in \{0,1\}^t} \alpha_{x,A,a} \left|x\right\rangle_e \otimes \left|A, a \oplus v_A(s^*, r)\right\rangle_q . \end{aligned}$$

Here, $\mathcal{H}_{env}$ is the environment in which the adversary can store auxiliary information. The dimension of this register is arbitrary, but finite. In the $\mathcal{H}_{query}$ register, the adversary submits its queries and receives the corresponding responses from the oracle.

Remark 3.1. If $S = (\mathsf{Share}, \mathsf{Reconstruct})$ is t-secure (as defined in Definition 2.11), then S is secure against classical G-attacks where G is the family of all subsets of size t (Definition 3.2).

Theorem 3.5 ([19, Theorem 1])**.** *Let S be a secret sharing scheme with adversary structure G. If $F^2 \subseteq G$ where $F^2 \triangleq \{A \mid \exists B, C \in F \; : \; A = B \cup C\}$, then S is perfectly secure against superposition F-attacks (Definition 3.4).*

For completeness, we refer the reader to Appendix A for a full proof.

3.2 Our Protocol

We describe our protocol in Fig. 1. Our protocol draws upon the prior works of [30] and [19].

3.3 Analysis

Theorem 3.6. *Let $n \in \mathbb{N}$ and $t < n/3$. Let a dual-mode commitment $(\mathsf{Gen}_H, \mathsf{Gen}_B, \mathsf{DualCom})$ (Definition 2.6), a perfectly binding commitment $(\mathsf{Gen}, \mathsf{Com})$ (Definition 2.5), and a n-party, perfectly correct, perfectly t-private, perfectly t-robust MPC protocol Π (Definition 2.14) be given. Then, the protocol in Fig. 1 is a statistically sound, computationally zero-knowledge against superposition-attacks proof for NP in the common reference string model.*

Proof.

Completeness. This follows from the perfect binding of the commitment scheme and the MPC protocol.

Superposition-Attack Secure Zero-Knowledge Proof for NP from MPC

Let $(\mathsf{Gen}_H, \mathsf{Gen}_B, \mathsf{DualCom})$ be a dual-mode commitment scheme. Let $(\mathsf{Gen}, \mathsf{Com})$ be a perfectly binding, computationally hiding commitment scheme. Let Π be an n-party, perfectly correct, perfectly t-private, perfectly t-robust MPC protocol. Let $\mathcal{R}$ be an NP relation.

$\underline{\textsc{Setup}(1^\lambda)}$: Let $\mathsf{CRS} = (\mathsf{ck}_B, \mathsf{ck}, c)$ where two commitment keys and a commitment are sampled as follows: $\mathsf{ck}_B \leftarrow \mathsf{Gen}_B(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, and $c \leftarrow \mathsf{Com}(\mathsf{ck}, 0)$. Outputs CRS.

Let $\mathcal{R}' = \{((x, c, \mathsf{ck}), (w, r)) : (x, w) \in \mathcal{R} \vee c \equiv \mathsf{Com}(\mathsf{ck}, 1; r)\}$. Let $\mathcal{C}'_{\mathcal{R}}$ be a circuit that on input $(x', (w_1, r_1), \ldots, (w_n, r_n))$ computes $\mathcal{R}'(x', \oplus_{i\in[n]}(w_i, r_i))$. Let $(x, w) \in \mathcal{R}$.

$\underline{\mathsf{P}_1(\mathsf{CRS}, x, w)}$:

- Samples $r \leftarrow \{0,1\}^\lambda$ uniformly at random. Let m be the size of witnesses to $\mathcal{R}$. Sample witness shares $w'_1, \ldots, w'_n \in \{0,1\}^m \times \{0,1\}^\lambda$ such that $\oplus_{i\in[n]} w'_i = (w, r)$.
- Emulates an execution of Π for $\mathcal{C}_{\mathcal{R}'}$ on input $(x', w'_1, \ldots, w'_n)$. Defines $V_1, \ldots, V_n$ to be the views of the n players.
- Computes commitments $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_B, V_i; r_i)$ with uniformly random r_i for $i \in [n]$. Defines openings $\zeta_i = (V_i, r_i)$ for $i \in [n]$.
- Outputs $(\alpha = (\alpha_1, \ldots, \alpha_n), \zeta = (\zeta_1, \ldots, \zeta_n))$.

$\underline{\mathsf{V}_1(\mathsf{CRS}, x, \alpha)}$: Outputs a set of $t/2$ parties: $\beta = (\beta_1, \ldots, \beta_{t/2})$ where $\beta_i \in [n]$ for $i \in [t/2]$.

$\underline{\mathsf{P}_2(\mathsf{CRS}, x, w, \alpha, \beta, \zeta)}$: Outputs $\gamma = \{\zeta_{\beta_i}\}_{i\in[t/2]}$ with $\beta = (\beta_1, \ldots, \beta_{t/2})$ and $\zeta = (\zeta_1, \ldots, \zeta_n)$.

$\underline{\mathsf{V}_2(\mathsf{CRS}, x, \alpha, \beta, \gamma)}$: Outputs 1 if and only if the following checks pass:

- The openings are valid, i.e. $\alpha_{\beta_i} \equiv \mathsf{DualCom}(\mathsf{ck}_B, V_{\beta_i}; r_{\beta_i})$ for $i \in [t/2]$.
- For $i \in [t/2]$, view V_{β_i} has the β_ith party output 1.
- The views V_{β_i} and V_{β_j} are consistent with respect to Π and x for $i, j \in [t/2]$.

Else, outputs 0.

Figure 1: Superposition-Secure MPC in the Head for NP

Statistical Soundness. Our proof closely follows the proof from [30, Theorem 4.1]. Let a language $\mathcal{L} \in \mathsf{NP}$, a polynomial $p(\cdot)$, an unbounded-size quantum circuit $\mathcal{A}$, and an instance $x \notin \mathcal{L}$ be given such that

$$\Pr_{\mathsf{CRS}\leftarrow\mathsf{Setup}(1^\lambda)}[\langle \mathcal{A}_\lambda, \mathsf{V}\rangle(x, \mathsf{CRS}) = 1] \geq \frac{1}{p(\lambda)}. \tag{1}$$

$\mathcal{A}$ is unable to break the perfect binding property with respect to the $(\mathsf{Gen}, \mathsf{Com})$ commitment. As such, we know that there is no private input for each party which would cause an honest execution of $\mathcal{C}_{\mathcal{R}'}$ to output 1. We also have that $\mathcal{A}$ is unable to break the perfect binding property with respect to the dual-mode commitment. This leads us to having only two cases in this scenario: the prover corrupts either less than (or equal to) t or greater than t parties in the MPC protocol. We show contradictions in both of these two scenarios.

- Say we have that $\mathcal{A}$ corrupts less than (or equal to) t parties in the MPC protocol and manages to succeed in the event from Eq. (1) with advantage $\frac{1}{2p(\lambda)}$. When the instance $x \notin \mathcal{L}$, then, by the t-robustness of the MPC protocol, no uncorrupted party will output 1. As such, for the verifier to accept, it must necessarily be the case that the verifier chooses to open only

corrupted parties. This happens with probability at most $(\frac{t}{n})^{t/2}$, which we calculate with replacement, which gives a negligible upperbound on the soundness error in this case.

- Say instead that $\mathcal{A}$ corrupts greater than t parties in the MPC protocol and manages to succeed in the event from Eq. (1) with advantage $\frac{1}{2p(\lambda)}$. For the verifier to accept, the verifier cannot pick any pair of parties with "inconsistent" views. All pairs of inconsistent parties have at least one party in the set of at least t corrupted parties. So, there must be strictly greater than $t/2$ independent [4] pairs of inconsistent parties. For simplicity of computing the soundness error, we convert the notion of picking inconsistent pairs to picking a set of parties without inconsistencies.

  We count the number of ways that the verifier could avoid picking even one of these pairs of parties. For our count, we will assume the worst case, where there are only $t/2$ independent pairs. We will enumerate over the number of parties, $k \in [t/2]$, that are picked from the set of those within an independent pair. There are $\binom{t/2}{k}$ such ways to choose a pair and 2 options of party to pick for each choice, leading to a count of $\binom{t/2}{k}2^k$. Now, we must choose the remaining $t/2-k$ from the $n-t$ parties which do not have a pair, leading to a count of $\binom{n-t}{t/2-k}$. As such, we get a union bound on probability that the verifier does not pick even one of these pairs of parties,

$$\sum_{k\in[t/2]} \binom{n-t}{t/2-k}\binom{t/2}{k}2^k \Bigg/ \binom{n}{t/2},$$

  which yields a negligible upperbound on the soundness error in this setting.

Since we have negligible error in either scenario, we have an overall negligible soundness error.

Superposition-secure Computational Zero-Knowledge. To model superposition access of the adversary, we consider a classical algorithm P'_2 that has values $(\mathsf{CRS}, x, w, \alpha, \zeta)$ hardcoded inside and takes as an input only β and then, internally, runs $\mathsf{P}_2(\mathsf{CRS}, x, w, \alpha, \beta, \zeta)$. Given the classical algorithm for P'_2, there also exists a unitary $U_{\mathsf{P}'_2}$ implementing P'_2 quantumly. When the verifier now submits a superposition query $\sum_\iota |\beta_\iota\rangle$, it is possible to compute the reply, an opening over all the challenges contained in this superposition, by applying the unitary $U_{\mathsf{P}'_2}$ controlled on the challenge $\sum_\iota |\beta_\iota\rangle$. More precisely, we apply $U_{\mathsf{P}'_2} \sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}} = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$ and then return the register M as a reply to the verifier.

We define a two-part simulator $\mathsf{Sim} = (\mathsf{Sim}_1, \mathsf{Sim}_2)$. The first algorithm Sim_1 takes as input an instance x:

- Computes $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$ by sampling two commitment keys $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, and computing the commitment $c = \mathsf{Com}(\mathsf{ck}, 1; r)$ with uniform randomness r.
- Samples $w \leftarrow \{0,1\}^m$ uniformly at random. Samples witness shares $w'_1, \ldots, w'_n \in \{0,1\}^m \times \{0,1\}^\lambda$ such that $\oplus_{i\in[n]} w'_i = (w, r)$. Sets $x' = (x, c, \mathsf{ck})$.
- Emulates an execution of Π for $\mathcal{C}_{\mathcal{R}'}$ on input $(x', w'_1, \ldots, w'_n)$. Defines $V_1, \ldots, V_n$ to be the views of the n players.
- Computes commitments $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, V_i; r_i)$ with uniformly random r_i for $i \in [n]$. Defines openings $\zeta_i = (V_i, r_i)$ for $i \in [n]$.
- Outputs $(\mathsf{CRS}, \alpha = (\alpha_1, \ldots, \alpha_n), \zeta = (\zeta_1, \ldots, \zeta_n))$.

The second algorithm Sim_2 takes $(\mathsf{CRS}, x, w, \alpha, \sum_\iota |\beta_\iota\rangle, \zeta)$ as input, where $\sum_\iota |\beta_\iota\rangle$ may be a superposition query, hardcodes $(\mathsf{CRS}, x, w, \alpha, \zeta)$ into $U_{\mathsf{P}'_2}$, and outputs $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle)$.

Some of the hybrids for the proof of our construction are inefficient. For example the third hybrid in which the commitment schemes are opened an inefficient way. We highlight that this

[4] Here by "independent" we mean that the two parties in the pair are inconsistent with each other irrespective of their relationship with other parties.

inefficiency is only required to prove the indistinguishability between some of the hybrids and that the final simulator described above is efficient.

Let a relation $\mathcal{R}$ and a quantum polynomial-size quantum circuit $\mathcal{A}$ that can send superposition queries be given. We define the following series of hybrids, for any $\lambda \in \mathbb{N}$ and instance-witness pair $(x, w) \in \mathcal{R}$ where $|x| = \lambda$, which we will argue are all indistinguishable:

- $\mathcal{H}_0$: Same as the real world.

  $\mathsf{CRS} \leftarrow \mathsf{Setup}(1^\lambda)$, $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, hardcode $U_{\mathsf{P}_2'}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$, compute $U_{\mathsf{P}_2'}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$, and where register M is output.

- $\mathcal{H}_1$: Same as $\mathcal{H}_0$ except the commitment in the CRS is a commitment to 1.

  $\mathsf{ck}_B \leftarrow \mathsf{Gen}_B(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_B, \mathsf{ck}, c)$, $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$, $(\beta, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, hardcode $U_{\mathsf{P}_2'}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$, compute $U_{\mathsf{P}_2'}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$, and where register M is output.

  The indistinguishability between this and the previous hybrid follows from the hiding of the commitment scheme Com. We prove the indistinguishability of $\mathcal{H}_0$ and $\mathcal{H}_1$ in Claim 3.7.

- $\mathcal{H}_2$: Same as $\mathcal{H}_1$ except the dual mode commitment is in hiding mode.

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, hardcode $U_{\mathsf{P}_2'}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$, compute $U_{\mathsf{P}_2'}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$, and where register M is output.

  The indistinguishability between this and the previous hybrid follows from the indistinguishability of modes from the dual-mode commitment scheme. We prove the indistinguishability of $\mathcal{H}_1$ and $\mathcal{H}_2$ in Claim 3.8.

- $\mathcal{H}_3$: It works the same as $\mathcal{H}_2$ except the prover's first message is replaced with commitments to 0, and the binding of the commitments are broken to open them to the prover's third message. This hybrid runs in exponential time.

  For this hybrid, and the following, we define the following polynomial-size classical circuit $\mathcal{B}$ which is hardcoded with $\{(V_i, r_i)\}_{i\in[n]}$: output $\{(V_{\beta_i}, r_{\beta_i})\}_{i\in[t/2]}$. This classical circuit can be implemented as a unitary $U_{\mathcal{B}}$.

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, $(\cdot, \{(V_i, \cdot)\}_{i\in[n]}) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$, $\alpha = (\alpha_1, \ldots, \alpha_n)$ where $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, 0)$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, computes valid openings $(r_1, \ldots, r_n)$ to $(V_1, \ldots, V_n)$ (by running in unbounded-time), hardcodes $U_{\mathcal{B}}$ with $\{(V_i, r_i)\}_{i\in[n]}$, and computes $U_{\mathcal{B}}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$ where M is output.

  The indistinguishability between this and the previous hybrid follows from the statistical hiding property of the dual-mode commitment scheme. We prove the indistinguishability of $\mathcal{H}_2$ and $\mathcal{H}_3$ in Claim 3.9.

- $\mathcal{H}_4$: Same as $\mathcal{H}_3$ except the binding of the commitments are broken to open them to the simulator's third message. This hybrid also runs in exponential time.

  See the definition of $U_{\mathcal{B}}$ in the previous hybrid.

  $(\mathsf{CRS}, \cdot, \{(V_i, \cdot)\}_{i\in[n]}) \leftarrow \mathsf{Sim}_1(x)$, $\alpha = (\alpha_1, \ldots, \alpha_n)$ where $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, 0)$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, computes valid openings $(r_1, \ldots, r_n)$ to $(V_1, \ldots, V_n)$ (by running in unbounded-time), hardcodes $U_{\mathcal{B}}$ with $\{(V_i, r_i)\}_{i\in[n]}$, compute $U_{\mathcal{B}}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$ where register M is output.

  The indistinguishability between this and the previous hybrid follows from the t-privacy of the underlying MPC protocol. We prove the indistinguishability of $\mathcal{H}_3$ and $\mathcal{H}_4$ in Claim 3.11 using the results of Claim 3.10.

- $\mathcal{H}_5$: This hybrid corresponds to the ideal world. It is the same as $\mathcal{H}_4$ except that the dual-mode commitments are generated using the views of the different parties.

  $(\mathsf{CRS}, \alpha, \zeta) \leftarrow \mathsf{Sim}_1(x)$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, and $\mathsf{Sim}_2(\mathsf{CRS}, x, w, \alpha, \sum_\iota |\beta_\iota\rangle, \zeta)$ outputs register M.

The indistinguishability between this and the previous hybrid follows by, again, relying on the statistical hiding property of the dual-mode commitment scheme. The proof of this transition proceeds similarly to the proof of Claim 3.9.

To prove our next claim, we construct a reduction that breaks the following property which is implied by the computational hiding property in Definition 2.5: instead of quantifying over all messages m and m', the distinguisher gets to choose m and m' before it receives the commitment key. To see why this implication holds, imagine a distinguisher $\mathcal{D}$ broke the property we wrote above. We can define a reduction that receives m and m' from $\mathcal{D}$ as the first message in its interaction. The reduction then sets the parameters to the game that it will play with the challenger from Definition 2.5 to be with respect to m and m'. Now the reduction's success probability will be the same as the success probability of $\mathcal{D}$. This shows the implication.

Claim 3.7. *Let* $(\mathsf{Gen}, \mathsf{Com})$ *be a computationally hiding commitment scheme, then the hybrids* $\mathcal{H}_0$ *and* $\mathcal{H}_1$ *are computationally indistinguishable.*

Proof. We have that $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable by the computational hiding of the plain commitment scheme. Say, for contradiction that there existed a quantum polynomial-size quantum circuit $\mathcal{D}$ that given input $(\mathsf{CRS}, x, \alpha, \sum_\iota |\beta_\iota, \gamma_\iota\rangle, \zeta)$ could distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$.

We define an efficient reduction, hardwired with the instance-witness pair (x, w), that receives $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$ from the challenger. The reduction sends 0 and 1 to the challenger. The challenger sends back c^*. The reduction then samples the remainder of the common reference string $\mathsf{CRS} = (\mathsf{ck}_B, \mathsf{ck}, c^*)$ as follows: samples $\mathsf{ck}_B \leftarrow \mathsf{Gen}_B(1^\lambda)$. The reduction computes $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$. The reduction then sends (CRS, α) to $\mathcal{A}$. The reduction receives $\sum_\iota |\beta_\iota\rangle$ from $\mathcal{A}$ and then, to compute the reply, the reduction hardcodes $U_{\mathsf{P}'_2}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$ and computes $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle |0\rangle) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle$. Lastly, the reduction outputs the result of $\mathcal{D}(\mathsf{CRS}, x, \alpha, \sum_\iota |\beta_\iota, \gamma_\iota\rangle, \zeta)$.

Our reduction will preserve the distinguishing advantage of $\mathcal{D}$. However, this contradicts the property we defined above this claim. Since this property is implied by the computational hiding property in Definition 2.5, we contradict the computational hiding of the commitment. As such, we must have that $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable except with negligible probability. □

Claim 3.8. *Let* $(\mathsf{Gen}_H, \mathsf{Gen}_B, \mathsf{DualCom})$ *be a dual-mode commitment scheme, then the hybrids* $\mathcal{H}_1$ *and* $\mathcal{H}_2$ *are computationally indistinguishable.*

Proof. $\mathcal{H}_1$ and $\mathcal{H}_2$ are indistinguishable by the computational indistinguishability of hiding and binding modes for the dual-mode commitment. Say, for contradiction that there existed a quantum polynomial-size quantum circuit $\mathcal{D}$ that given input $(\mathsf{CRS}, x, \alpha, \sum_\iota |\beta_\iota, \gamma_\iota\rangle, \xi)$ could distinguish between $\mathcal{H}_1$ and $\mathcal{H}_2$.

We define an efficient reduction, hardwired with the instance-witness pair (x, w), that receives ck^* from the challenger either sampled according to Gen_H or Gen_B. The reduction then samples the remainder of the common reference string $\mathsf{CRS} = (\mathsf{ck}^*, \mathsf{ck}, c)$ as follows: samples $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$ and $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$. The reduction computes $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$. The reduction then sends (CRS, α) to $\mathcal{A}$. The reduction receives $(\sum_\iota |\beta_\iota\rangle, \xi)$ from $\mathcal{A}$ and then, to compute the reply, the reduction hardcodes $U_{\mathsf{P}'_2}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$ and computes $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle |0\rangle) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle$. Lastly, the reduction outputs the result of $\mathcal{D}(\mathsf{CRS}, x, \alpha, \sum_\iota |\beta_\iota, \gamma_\iota\rangle, \xi)$.

Our reduction will preserve the distinguishing advantage of $\mathcal{D}$. However, this contradicts the computational indistinguishability of keys for the dual-mode commitment scheme. As such, we must have that $\mathcal{H}_1$ and $\mathcal{H}_2$ are indistinguishable except with negligible probability. □

Claim 3.9. *Let* $(\mathsf{Gen}_H, \mathsf{Gen}_B, \mathsf{DualCom})$ *be a dual-mode commitment scheme, then the hybrids* $\mathcal{H}_2$ *and* $\mathcal{H}_3$ *are statistically indistinguishable.*

Proof. $\mathcal{H}_2$ and $\mathcal{H}_3$ are indistinguishable by the statistical hiding property of the dual-mode commitment. We argue this by switching each commitment one at a time and using a union bound to get an overall negligible distinguishing probability. Say we switch the first commitment, then the second, and so on until the n'th commitment. Let $i \in [n]$ be chosen arbitrarily. Say, for contradiction that there existed an unbounded-time distinguisher $\mathcal{D}$ that given input $(\mathsf{CRS}, x, \alpha, \beta, \gamma, \xi)$ could distinguish whether the i'th commitment was a commitment to a view or 0.

We define a computationally unbounded reduction, hardwired with the instance-witness pair (x, w) and index i, that receives $\mathsf{ck}_B \leftarrow \mathsf{Gen}_B(1^\lambda)$ from the challenger. The reduction then samples the remainder of the common reference string $\mathsf{CRS} = (\mathsf{ck}_B, \mathsf{ck}, c)$ as follows: samples $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$ and $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$. The reduction computes $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$. The reduction then sends two messages V_i (taken from α_i) and 0 to the challenger. The challenger sends back c^*. The reduction then sends (CRS, α') to $\mathcal{A}$ where $\alpha' = (\mathsf{DualCom}(\mathsf{ck}_B, 0), \ldots, \mathsf{DualCom}(\mathsf{ck}_B, 0), c^*, \alpha_{i+1}, \ldots, \alpha_n)$. The reduction receives $(\sum_\iota |\beta_\iota\rangle, \xi)$ from $\mathcal{A}$. In the next step, the reduction runs in unbounded time to find openings $(r'_1, \ldots, r'_n)$ such that all the commitments $(\alpha_1, \ldots, \alpha_n)$ open to $(V_1, \ldots, V_n)$. Afterwards, to compute the reply, the reduction hardcodes $U_{\mathcal{B}}$ with $\{(V_i, r'_i)\}_{i\in[n]}$ and computes $U_{\mathcal{B}}(\sum_\iota |\beta_\iota\rangle |0\rangle) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle$. Lastly, the reduction outputs the result of $\mathcal{D}(\mathsf{CRS}, x, \alpha, \sum_\iota |\beta_\iota, \gamma_\iota\rangle, \xi)$.

Our reduction will preserve the distinguishing advantage of $\mathcal{D}$. However, this contradicts the statistical hiding of the commitment. As such, we must have that $\mathcal{H}_2$ and $\mathcal{H}_3$ are indistinguishable except with negligible probability. We have a similar argument for the indistinguishability of $\mathcal{H}_4$ and $\mathcal{H}_5$. The main difference is that we sample the common reference string and views of the parties according to Sim_1. □

Before proceeding with the proof of Claim 3.11, we cast the first two steps of the prove procedure $\mathsf{P}_1(\mathsf{CRS}, x, w)$, together with some parts of the CRS, as the sharing procedure of a secret sharing scheme for a secret $w \in \{0,1\}^m$. More precisely:

$\mathsf{Setup}(1^\kappa)$: Generate a commitment key $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$ for a perfectly binding, computationally hiding commitment scheme and a commitment $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$. Output $\mathsf{CRS} = (\mathsf{ck}, c)$.

$\mathsf{Share}(w)$: Sample $r \leftarrow \{0,1\}^\lambda$ as well as $w_1, \ldots, w_{n-1} \leftarrow \{0,1\}^m$ and $r_1, \ldots, r_{n-1} \leftarrow \{0,1\}^\lambda$ uniformly at random and set $(w_n, r_n) \coloneqq (w_1, r_1) \oplus \ldots \oplus (w_{n-1}, r_{n-1}) \oplus (w, r)$. Emulate an execution Π for $\mathcal{C}_{\mathcal{R}'}$ on input $(x', w'_1, \ldots, w'_n)$ where $w'_i \coloneqq (w_i, r_i)$ and let $s_1, \ldots, s_n$ to be the views of the players $P_1, \ldots, P_n$. Output $\{s_i\}_{i\in[n]}$ as the set of shares.

$\mathsf{Reconstruct}(\mathsf{CRS}, \{s_i\}_{i\in[n]})$: Parse the shares $\{s_i\}_{i\in[n]}$ as the views of the parties P_i for all $i \in [n]$. Then, potentially using CRS, reconstruct w'_i from the view of P_i for all $i \in [n]$. Compute $(w, r) = \oplus_{i\in[n]} w'_i$ and output w as the secret.

In the next step, we prove that the presented secret sharing scheme achieves perfect t-out-of-n security.

Claim 3.10. *Let Π be a perfectly t-private MPC protocol, then the above secret sharing scheme is perfectly secure against classical G attacks where G contains all subsets of $[n]$ of size t.*

Proof. To prove this lemma, it suffices to prove that the above described secret sharing scheme is a t-out-of-n secret sharing scheme, following Remark 3.1. We prove this using the following hybrids:

Hybrid $\mathcal{H}_0$: This hybrid corresponds to the case where the secret sharing scheme is executed using the secret w.

Hybrid $\mathcal{H}_1$: This hybrid corresponds to the setting where the messages of the MPC protocol Π are generated using the shares of the opening of the commitment c as an input instead of honestly generated using the shares of the witness w. The perfect indistinguishability between this and the previous hybrid follows from the perfect t-privacy of the MPC protocol Π.

Hybrid $\mathcal{H}_2$: In this hybrid, the shares $w_1, \ldots, w_n$ are sampled as a secret sharing of 0 instead of the secret w. This hybrid is perfectly indistinguishable from the previous hybrid due to the security of the secret sharing scheme $w_1, \ldots, w_n$. This hybrid corresponds to an execution of the sharing algorithm that does not rely on the witness w and, therefore, concludes the proof.

Indistinguishability of hybrids $\mathcal{H}_0$ and $\mathcal{H}_1$: We prove the indistinguishability of the hybrids $\mathcal{H}_0$ and $\mathcal{H}_1$ using the perfect t-privacy of the MPC protocol. We do this by describing an adversary $\mathcal{B}$ that interacts with the adversary $\mathcal{A}$ of the secret sharing scheme. In the first step, the adversary $\mathcal{B}$ generates the CRS as described in the setup procedure and sends it to $\mathcal{A}$, afterwards, it receives the secret w as well as a set of indices T from the adversary $\mathcal{A}$. In the next step, the adversary $\mathcal{B}$ samples $r_1, \ldots, r_n$ such that $r \coloneqq \oplus_{i\in[n]} r_i$ where r is the opening of the commitment of the

CRS. Furthermore, the adversary samples $w_1, \ldots, w_{n-1} \leftarrow \{0,1\}^m$ uniformly at random and sets $w_n := w_1 \oplus \ldots \oplus w_{n-1} \oplus w$. It now follows from the security of the MPC that the views of the parties $\{P_i\}_{i \in T}$ generated using the inputs $(w_i, r'_i)_{i \in [n]}$ for random r'_i are indistinguishable from the views $\{P_i\}_{i \in T}$ generated using the inputs $(w'_i, r_i)_{i \in [n]}$ for random w'_i. This implies the indistinguishability of $\mathcal{H}_0$ and $\mathcal{H}_1$ and concludes the transition.

Indistinguishability of hybrids $\mathcal{H}_1$ and $\mathcal{H}_2$: The indistinguishability of the hybrids $\mathcal{H}_1$ and $\mathcal{H}_2$ follows directly from the fact that

$$\{(w_i | i \in T) | (w_1, \ldots, w_n) \leftarrow \mathsf{Share}(w)\} = \{(w_i | i \in T) | (w_1, \ldots, w_n) \leftarrow \mathsf{Share}'(0)\}$$

where $\mathsf{Share}'(w)$ samples $w_1, \ldots, w_{n-1}$ randomly and sets $w_n := \bigoplus_{i \in [n-1]} w_i$. More precisely, for a challenge w, T submitted by an adversary, the above equality implies that it is (perfectly) indistinguishable if the values $w_1, \ldots, w_n$ used as the input to the MPC protocol Π are generated using $\mathsf{Share}'(w)$ or using $\mathsf{Share}'(0)$. This implies that the hybrids $\mathcal{H}_1$ and $\mathcal{H}_2$ are perfectly indistinguishable.

Combining both of the above analyses yields the lemma. □

Taking into account Theorem 3.5, we observe that the above defined secret sharing scheme is secure against superposition attacks as long as only $t/2$ shares are revealed.

Claim 3.11. *Let Π be a perfectly t-private MPC protocol, then the hybrids $\mathcal{H}_3$ and $\mathcal{H}_4$ are perfectly indistinguishable.*

Proof. This claim directly follows with the observation made in Claim 3.10 that the above described scheme is a t-out-of-n secret sharing scheme. Therefore, we can rely on the results of Damgård et al. [19, Theorem 1] which state that a perfectly secure t-out-of-n secret sharing scheme is secure against superposition attacks as long as only $t/2$ of the shares are revealed. This directly implies the perfect indistinguishability of the hybrids $\mathcal{H}_3$ and $\mathcal{H}_3$ since the interaction between the prover and the verifier in the third round corresponds to revealing $t/2$ shares that have either been generated for the witness w of the relation (in the case of $\mathcal{H}_3$) or the opening of the commitment c (in the case of $\mathcal{H}_4$). This concludes the proof of the claim. □

□

4 Superposition-attack secure, Zero-Knowledge Argument for QMA

4.1 Quantum Secret Sharing Schemes [19, Section 4] & MPQC

In this section, we introduce some preliminaries on the superposition security of quantum secret sharing schemes and multiparty quantum computation.

4.1.1 Quantum Secret Sharing Secure against Superposition Attacks

Our protocol relies on a quantum secret sharing scheme that is secure against superposition attacks.

Definition 4.1 (Quantum Secret Sharing)**.** *Let $|sec\rangle = \sum_{s \in \mathbb{S}} \alpha_s |s\rangle$ be the secret quantum state. A quantum secret sharing scheme is defined as a unitary transformation that maps each basis state $|s\rangle$ plus an ancilla of appropriate size to a state $|\phi_s\rangle = \sum_{v_1,\ldots,v_n \in \{0,1\}^k} \alpha_{v_1,\ldots,v_n} |v_1\rangle \ldots |v_n\rangle$. The content of the i'th register is the share of the i'th party.*

A quantum secret sharing scheme is secure against adversary structure F, if any subset of shares corresponding to a subset $A \in F$ contains no information about the secret state, but any subset of shares B where $B \notin F$ allows reconstruction of the secret. It follows from the no-cloning theorem that security can only hold if F has the property that for any $B \notin F$, the complement $\overline{B}$ is in F.

Definition 4.2 (F-Share Capture Attacks)**.** *Let $\vec{v} = v_1, \ldots, v_n$ and $|\vec{v}_A\rangle$ be the basis state where $|\vec{v}_A\rangle = |w_1\rangle \ldots |w_n\rangle$, with $w_i = v_i$ if $i \in A$ and $w_i = \perp$ otherwise. Furthermore, we specify a unitary U by the following action on basis states for shares and player subsets: $U(|v_1\rangle \ldots |v_n\rangle |A\rangle |\perp\rangle^{\otimes n}) = |\vec{v}_{\overline{A}}\rangle |A\rangle |\vec{v}_A\rangle$.*

In an F-share capture attack, the adversary gets to specify a "query" state $\sum_{A\in F}\alpha_A|A\rangle|\perp\rangle^{\otimes n}$. The unitary U is then applied to the secret shared state as well as the query state, i.e. $U(|\phi_s\rangle\sum_{A\in F}\alpha_A|A\rangle|\perp\rangle^{\otimes n})$. In return, the adversary receives the last two registers (which contain the corrupted sets and the captured shares).

We say that the scheme is secure against F-share capture attacks if it always holds that the state the adversary gets is independent of $|s\rangle$. By linearity, security trivially extends to superpositions over different $|s\rangle$'s.

Theorem 4.3 (Superposition Security of Quantum Secret Sharing (Proposition 1 [19]))**.** *Any quantum secret sharing scheme that is secure for adversary structure F (Definition 3.3) is also secure against F-share capture attacks.*

In the proof of Theorem 4.4, more specifically the hybrid transition of Claim 4.7, we rely on the superposition security of a quantum secret sharing scheme. In this hybrid transition, we consider the circuit-to-Hamiltonian reduction over the MPQC circuit as the quantum secret sharing scheme. Note that, strictly speaking, this procedure does not satisfy all the properties of a standard quantum secret sharing scheme, since there is no well-defined reconstruction procedure for *all* subsets of parties (although there is one for a particular choice of a subset). We can nevertheless rely on Theorem 4.3 since the proof of this theorem only relies on the secrecy of the quantum secret sharing scheme, which is given by the above construction, and not its reconstruction property.

4.1.2 Multiparty Quantum Computation

Let $\mathcal{R}$ be a quantum circuit which has n sets of input and output registers. Let Π be an n-party MPQC protocol computing the quantum circuit $\mathcal{R}$. Π is executed on the following set of registers: for each party $i\in[n]$, an input register I_i, a work register W_i, a message register M_i (consisting of one sub-register for each party $j\neq i$ and round), and an output register O_i. We refer to the set of registers of each party as that party's *view*. Registers W_i, M_i, and O_i are initialized to $|0\rangle$. The input registers I_i contain the input to $\mathcal{R}$. We represent our MPQC protocol as a quantum circuit $\mathcal{C}=U_T\dots U_1$ where the U_i are two-qubit unitaries.

Remark 4.1. Without loss of generality, we assume that parties in the MPQC protocol do not receive randomness as input. This is because they can obtain such randomness by creating an auxiliary $|+\rangle$ state, and measuring it (and the latter measurement can of course be deferred to the very end).

4.2 Our Protocol

At a high-level, our construction involves secret sharing a quantum witness amongst n parties, constructing an n-party MPQC circuit which computes a QMA verifier, applying the quantum circuit to local Hamiltonian reduction to the MPQC circuit, and performing a commit-and-open style quantum protocol analogous to the classical MPC-in-the-head paradigm.

We describe our protocol in Fig. 2 and Fig. 3. In our protocol, we draw upon the classical MPC-in-the-head technique of [30] as well as the use of dual-mode commitments to achieve superposition-security from [19].

4.3 Analysis

Theorem 4.4. *Let $n\in\mathbb{N}$ and $t<n/3$. Let a dual-mode commitment $(\mathsf{Gen}_H,\mathsf{Gen}_B,\mathsf{DualCom})$ (Definition 2.6), a perfectly binding commitment $(\mathsf{Gen},\mathsf{Com})$ (Definition 2.5), and a n-party, statistically correct and perfectly $2t$-private MPQC protocol Π be given (Definition 2.17).*

The protocol in Figs. 2 and 3 is a statistically sound, computationally zero-knowledge against superposition-attacks for QMA in the common reference string model.

Proof. As we will see, in order to prove Theorem 4.4, it suffices to provide a proof with respect to a single repetition of the protocol in Figs. 2 and 3.

Superposition-Attack Secure Zero-Knowledge Argument for QMA from MPQC

Let $(\mathsf{Gen}_H, \mathsf{Gen}_B, \mathsf{DualCom})$ be a dual-mode commitment scheme. Let $(\mathsf{Gen}, \mathsf{Com})$ be a perfectly binding, computationally hiding commitment scheme with randomness of length λ. Let Π be an n-party statistically correct and perfectly $2t$-private MPQC protocol. Let $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no})$ be a QMA promise problem and $\mathcal{M}$ be a quantum polynomial-time family of circuits $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ for $\mathcal{L}$ that accepts yes instances with probability $1 - \mathsf{negl}(n)$. Let $x \in \mathcal{L}_{yes}$ with witness $|w\rangle$ of length m.

$\textsc{Setup}(1^\lambda)$: Let $\mathsf{CRS} = (\mathsf{ck}_B, \mathsf{ck}, c)$ where two commitment keys and a commitment are sampled as follows: $\mathsf{ck}_B \leftarrow \mathsf{Gen}_B(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, and $c \leftarrow \mathsf{Com}(\mathsf{ck}, 0)$. Outputs CRS.

Let $\mathcal{R}$ be a quantum circuit (with (x, c, ck) hardcoded) that on input $|a_1, b_1, r_1\rangle \otimes \ldots \otimes |a_{n-1}, b_{n-1}, r_{n-1}\rangle \otimes |\psi, r_n\rangle$, where $a_i, b_i \in \{0,1\}^m$ and $r_i \in \{0,1\}^\lambda$, does the following:

- Defines $(a, b) = \oplus_{i\in[n-1]}(a_i, b_i)$ and $r = \oplus_{i\in[n]} r_i$.
- Computes $|w'\rangle = Z^b X^a |\psi\rangle$.
- If $\mathcal{M}(x, |w'\rangle) = 1$ or $c \equiv \mathsf{Com}(\mathsf{ck}, 1; r)$, outputs 1. Otherwise, outputs 0.

Let $\mathcal{C}$ be a quantum circuit for the MPQC protocol Π computing the quantum circuit $\mathcal{R}$. Apply the compiler described in Section 2.2, with details from Section 2.7, to $\mathcal{C}$. This defines a Hamiltonian H. Let ℓ be the number of qubits in the work, message, and output registers.

Repeat Fig. 3 $\mathsf{poly}(\lambda)$ times in parallel, each on a separate copy of the witness. The output of the verifier is defined as the majority vote over all the instances.

Figure 2: MPQC in the Head (Part I)

We will first show that it suffices to analyze completeness and soundness for one parallel repetition. In what follows will prove that a single repetition has a noticeable completeness-soundness gap, in other words:

$$p_{yes}^{acc} - p_{no}^{acc} \geq \frac{1}{q(n)}$$

for a polynomial $q(n)$ with $n \in \mathbb{N}$. One can reduce the completeness and the soundness error using a standard technique: Composing the protocol in parallel with multiple copies of the witness and taking the majority vote. Hence, while our protocol necessarily uses multiple repetitions to achieve Theorem 4.4, it suffices to analyze completeness and soundness for one parallel repetition.

We now argue that it also suffices to analyze zero-knowledge for one parallel repetition. Our protocol, without considering the trapdoor in the CRS, is a witness-indistinguishable proof, and witness indistinguishability composes in parallel. The simulation for the parallel-repeated version of the protocol can be then argued using the technique introduced in [23], where the real witness is gradually substituted by the trapdoor in the CRS, one repetition at a time.

Statistical Completeness. Let $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no}) \in \mathsf{QMA}$ be an input promise problem, $\mathcal{A}$ be an arbitrary, unbounded-size quantum circuit, and x be an arbitrary instance $x \in \mathcal{L}_{yes}$ with corresponding witness $|w\rangle$. Let $|w'\rangle = |a_1, b_1, r_1\rangle \otimes \ldots \otimes |a_{n-1}, b_{n-1}, r_{n-1}\rangle \otimes |\psi, r_n\rangle$ be the honest prover's input.

We proceed by looking at the honest verifier's checks when interacting with an honest prover. Since the dual-mode commitment is deterministic when its randomness is provided, the honest verifier's first check that the openings are valid will pass with probability 1. By the perfect correctness of the quantum OTP, the reduced density of $|\psi'_{hist}\rangle$ on registers β_1 and β_2 is identical to that of $|\phi_{hist}\rangle$ (on the same registers). Furthermore, by the statistical correctness of the MPQC Π, the protocol Π will accept with probability $1 - \mathsf{negl}(\lambda)$. Overall, this implies that the Hamiltonian

$\underline{\text{PROVER}_1(\mathsf{CRS}, x, |w\rangle)}$:

- Sample (a, b) uniformly at random from $\{0,1\}^m \times \{0,1\}^m$. Sample $n-1$ shares $(a_1, b_1), \ldots, (a_{n-1}, b_{n-1}) \in \{0,1\}^m \times \{0,1\}^m$ such that $\oplus_{i\in[n-1]}(a_i, b_i) = (a, b)$. Compute a quantum OTP on the witness, $|\psi\rangle = X^a Z^b |w\rangle$. Sample r_i uniformly at random from $\{0,1\}^\lambda$ for $i \in [n]$.
- Let $|\phi_{hist}\rangle$ be the history state corresponding to the circuit $\mathcal{C}$ defined in Fig. 2 on input $|a_1, b_1, r_1\rangle \otimes \ldots \otimes |a_{n-1}, b_{n-1}, r_{n-1}\rangle \otimes |\psi, r_n\rangle$.
- Let m' be the number of qubits in $|\phi_{hist}\rangle$. Sample (a', b') uniformly at random from $\{0,1\}^{m'} \times \{0,1\}^{m'}$. Compute a quantum OTP on the history state, $|\psi_{hist}\rangle = X^{a'} Z^{b'} |\phi_{hist}\rangle$.
- Compute commitments $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_B, (a'_i, b'_i); r'_i)$ where a'_i and b'_i are the keys corresponding to the ith party's registers and r'_i is sampled uniformly at random for $i \in [n]$. Define openings $\zeta_i = ((a'_i, b'_i), r'_i)$ for $i \in [n]$.
- Output $(\alpha = (|\psi_{hist}\rangle, \alpha_1, \ldots, \alpha_n), \zeta = (\zeta_1, \ldots, \zeta_n))$.

$\underline{\text{VERIFIER}_1(\mathsf{CRS}, x, \alpha)}$: Sample S according to p_S as outlined in Section 2.2. Let $\beta = (\beta_1, \beta_2)$ specify a set of 2 parties which are sampled uniformly at random conditioned on opening the two qubits which are measured by S. Output $(\beta, \xi = S)$.

$\underline{\text{PROVER}_2(\mathsf{CRS}, x, \alpha, \beta, \zeta)}$: Output $\gamma = \{\zeta_{\beta_1}, \zeta_{\beta_2}\}$.

$\underline{\text{VERIFIER}_2(\mathsf{CRS}, x, \alpha, \beta, \gamma, \xi)}$: Output 1 if and only if the following checks pass:

- The openings are valid $\alpha_{\beta_i} \equiv \mathsf{DualCom}(\mathsf{ck}_B, (a'_{\beta_i}, b'_{\beta_i}); r'_{\beta_i})$ for $i \in [2]$.
- Apply $Z^{b'_{\beta_i}} X^{a'_{\beta_i}}$ to the β_i^{th} qubit in $|\psi_{hist}\rangle$ for all $i \in [2]$ to get a resulting state $|\psi'_{hist}\rangle$. The check in Section 2.2 with respect to the previously chosen measurement S passes for $|\psi'_{hist}\rangle$ at indices $\{\beta_i\}_{i\in[2]}$.

Else, output 0.

Figure 3: MPQC in the Head (Part II)

H has a ground state with a negligible eigenvalue, and furthermore the ground state is exactly $|\phi_{hist}\rangle$. Thus, verification will succeed probability negligibly close to 1/2.

Statistical Soundness. Since $x \in \mathcal{L}_{no}$, then for all quantum states , the probability that $\mathcal{M}$ accepts a given state is bounded away from 1, by at least some inverse polynomial term $1/p(n)$. Furthermore, since the commitment c is perfectly binding, the same bound must hold for the circuit $\mathcal{R}$. By the statistical correctness of Π, we can also conclude that an honest execution of $\mathcal{C}$ would reject any input state with probability at least $1/p(n)$. Consequently, the smallest eigenvalue of the Hamiltonian H is at least $1/q(n)$, for some polynomial $q(n)$.

Let us now consider the commitment message α as computed by $\mathcal{A}$. This commitment is a quantum OTP implemented with a perfectly binding dual-mode commitment. Since it is perfectly binding, there is a well-defined unique state ρ contained in α. It follows that the state must be independent of the random choices of the verifier, and consequently, the verifier of the overall protocol accept with probability at most $1/2 - 1/\mathsf{poly}(n)$.

Superposition-Secure Computational Zero-Knowledge. As in the analysis for the NP case, to model superposition access of the adversary, we consider a classical algorithm P_2' that has values $(\mathsf{CRS}, x, \alpha, \zeta)$ hardcoded and takes as an input only β and then, internally, runs $\mathsf{P}_2(\mathsf{CRS}, x, \alpha, \beta, \zeta)$.

Given the classical algorithm for P'_2, there also exists a unitary $U_{\mathsf{P}'_2}$ implementing P'_2 quantumly. When the verifier now submits a superposition query $\sum_\iota |\beta_\iota\rangle$, it is possible to compute the reply, an opening over all the challenges contained in this superposition, by applying the unitary $U_{\mathsf{P}'_2}$ controlled on the challenge $\sum_\iota |\beta_\iota\rangle$. More precisely, we apply

$$U_{\mathsf{P}'_2} \sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}} = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$$

and then return the register M as a reply to the verifier.

We define a two-part simulator $\mathsf{Sim} = (\mathsf{Sim}_1, \mathsf{Sim}_2)$. The first algorithm Sim_1 takes as input an instance x:

- Computes $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$ by sampling two commitment keys $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, and computing the commitment $c = \mathsf{Com}(\mathsf{ck}, 1; r)$ with uniform randomness r.
- Samples a, b uniformly at random from $\{0,1\}^m$ and compute a quantum OTP encryption of the $|0\rangle$ state, $|\psi\rangle = X^a Z^b |0\rangle$.
- Samples r_i uniformly at random from $\{0,1\}^\lambda$ for $i \in [n-1]$ and set $r_n = r \oplus_{i\in[n-1]} r_i$. Sets $x' = (x, c, \mathsf{ck})$.
- Defines the history state $|\phi_{hist}\rangle$ as described in Section 2.2 to the MPQC protocol Π computing the quantum circuit $\mathcal{R}$ given input $|a_1, b_1, r_1\rangle \otimes \ldots \otimes |a_{n-1}, b_{n-1}, r_{n-1}\rangle \otimes |\psi, r_n\rangle$ with a_i, b_i randomly sampled for all $i \in [n-1]$. [5].
- Let m' be the number of qubits in $|\psi_{hist}\rangle$. Sample a', b' uniformly at random from $\{0,1\}^{m'}$. Compute a quantum OTP on the history state, $|\psi_{hist}\rangle = X^{a'} Z^{b'} |\phi_{hist}\rangle$.
- Compute commitments $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_B, (a'_i, b'_i); r'_i)$ where a'_i is the ith bit of a' (similarly for b'_i) with uniformly random r'_i for $i \in [m']$. Define openings $\zeta_i = ((a'_i, b'_i), r'_i)$ for $i \in [n]$.
- Outputs $(\mathsf{CRS}, \alpha = (\alpha_1, \ldots, \alpha_n), \zeta = (\zeta_1, \ldots, \zeta_n))$.

The second algorithm Sim_2 takes input $(\mathsf{CRS}, x, w, \alpha, \sum_\iota |\beta_\iota\rangle, \zeta)$ as input where $\sum_\iota |\beta_\iota\rangle$ may be a superposition query, hardcodes $(\mathsf{CRS}, x, w, \alpha, \zeta)$ into $U_{\mathsf{P}'_2}$, and outputs $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle)$.

Let a relation $\mathcal{R}$ and a quantum polynomial-size quantum circuit $\mathcal{A}$ that can send superposition queries. We define the following series of hybrids, for any $\lambda \in \mathbb{N}$ and instance-witness pair $(x, w) \in \mathcal{R}$ where $|x| = \lambda$, which we will argue are all indistinguishable:

- $\mathcal{H}_0$: Same as the real world.

  $\mathsf{CRS} \leftarrow \mathsf{Setup}(1^\lambda)$, $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, hardcode $U_{\mathsf{P}'_2}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$, compute $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$, and where register M is output.

- $\mathcal{H}_1$: Same as $\mathcal{H}_0$ except the commitment in the CRS is a commitment to 1.

  $\mathsf{ck}_B \leftarrow \mathsf{Gen}_B(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_B, \mathsf{ck}, c)$, $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$, $(\beta, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, hardcode $U_{\mathsf{P}'_2}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$, compute $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$, and where register M is output.

  The indistinguishability between this and the previous hybrid follows as in the NP case, i.e., from the hiding of the commitment scheme Com. Therefore, we refer to the proof of Claim 3.7 to argue the indistinguishability between $\mathcal{H}_0$ and $\mathcal{H}_1$.

- $\mathcal{H}_2$: Same as $\mathcal{H}_1$ except the dual mode commitment is in hiding mode.

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, $(\alpha, \zeta) \leftarrow \mathsf{P}_1(\mathsf{CRS}, x, w)$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, hardcode $U_{\mathsf{P}'_2}$ with $(\mathsf{CRS}, x, w, \alpha, \zeta)$, compute $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$, and where register M is output.

  The indistinguishability between this and the previous hybrid follows as in the NP case, i.e., from the indistinguishability of modes from the dual-mode commitment scheme. Therefore, we refer to the proof of Claim 3.7 to argue the indistinguishability between $\mathcal{H}_1$ and $\mathcal{H}_2$.

[5] Here, the circuit $\mathcal{R}$ will decrypt the state $|\psi\rangle$ by xoring the random values a_i, b_i to obtain a and b which will lead to a wrong witness and therefore the xor of the opening shares $r_1, \ldots, r_n$ are used as the witness.

- $\mathcal{H}_3$: It works the same as $\mathcal{H}_2$ except that the dual commitments in the prover's first message are replaced with commitments to 0, and the binding of the commitments are broken to open them to the prover's third message. This hybrid runs in exponential time.

  For this hybrid, and the following, we define the following polynomial-size classical circuit $\mathcal{B}$ which is hardcoded with $\{((a'_i, b'_i), r'_i)\}_{i\in[n]}$: output $\{((a'_{\beta_i}, b'_{\beta_i}), r'_{\beta_i})\}_{i\in[t]}$. This classical circuit can be implemented as a unitary $U_{\mathcal{B}}$.

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, $\alpha = (|\psi_{hist}\rangle, \alpha_1, \ldots, \alpha_n)$ where $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, (0,0))$ and $|\psi_{hist}\rangle$ is generated as described in P_1, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, computes valid openings $(r'_1, \ldots, r'_n)$ to $((a'_1, b'_1), \ldots, (a'_n, b'_n))$ (by running in unbounded-time), hardcodes $U_{\mathcal{B}}$ with $\{((a'_i, b'_i), r'_i)\}_{i\in[n]}$, and computes $U_{\mathcal{B}}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$ where M is output to the adversary.

  The indistinguishability between this and the previous hybrid follows from the statistical hiding property of the dual-mode commitment scheme. We prove the indistinguishability of $\mathcal{H}_2$ and $\mathcal{H}_3$ in Claim 3.9.

- $\mathcal{H}_4$: Same as $\mathcal{H}_3$ except that the messages of the MPQC protocol are teleported into the one-time pad encryptions and the binding of the commitments are broken to open them to the corresponding teleportation keys. This hybrid also runs in exponential time.

  In this, and the following hybrids, we consider a modified (quantum) circuit $U_{\mathcal{B}'}$. $U_{\mathcal{B}'}$ also works controlled on the challenge of the adversary but, before outputting the reply to the query, it executes the teleportation procedure for all the indices contained in the challenge query of the adversary and then uses the output bits of the teleportation procedure to brute force the opening as in the procedure $\mathcal{B}$. More formally, $U_{\mathcal{B}'}$ takes as an input the state $\sum_\iota |\beta_\iota\rangle |\phi_{hist}\rangle |\mathsf{EPR}\rangle_A |0\rangle_{\mathsf{T}} |0\rangle_{\mathsf{M}}$ then applies the teleportation unitary U_T controlled with $\sum_\iota |\beta_\iota\rangle$ on the corresponding registers of $|\mathsf{EPR}\rangle_A |0\rangle_{\mathsf{T}}$. For the classical teleportation bits, contained in the register T, are then used as the values for which the openings for the dual-mode commitments are (coherently) brute forced[6]. The output of this brute force operation are then contained in the register M, which is then output to the adversary.

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, sample n EPR pairs $|\mathsf{EPR}\rangle_{A,B} := |\mathsf{EPR}\rangle_{A,B,1}, \ldots, |\mathsf{EPR}\rangle_{A,B,n}$, $\alpha = (|\mathsf{EPR}\rangle_B, \alpha_1, \ldots, \alpha_n)$ where $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, (0,0))$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, apply the unitary $U_{\mathcal{B}'}(\sum_\iota |\beta_\iota\rangle |\phi_{hist}\rangle |\mathsf{EPR}\rangle_A |0\rangle_{\mathsf{T}} |0\rangle_{\mathsf{M}})$ (by running in unbounded-time) with $|\phi_{hist}\rangle$ being generated as described in P_1, and output M to the adversary.

  The indistinguishability between this and the previous hybrid follows from the (perfect) security of the quantum one-time pad. We prove the indistinguishability of $\mathcal{H}_3$ and $\mathcal{H}_4$ in Claim 4.5.

- $\mathcal{H}_5$: Same as $\mathcal{H}_4$ except that the first message computed by the prover is completely independent of the witness $|w\rangle$ and computed for the value $|0\rangle$ instead. This also implies that the history state $|\phi_{hist}\rangle$, is generated using the shares $r_1, \ldots, r_n$ of the opening r from the commitment c instead of the decryption keys (a, b) for the quantum one-time pad ciphertext. This hybrid also runs in exponential time.

  See the definition of $U_{\mathcal{B}'}$ in the previous hybrid.

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, generate $|\psi\rangle$ by encrypting the $|0\rangle$ state, i.e., $|\psi\rangle = X^a Z^b |0\rangle$ for random a, b, generate $|\phi_{hist}\rangle$ using the secret shares $r_1, \ldots, r_n$ of the opening r of the commitment c and using random a_i, b_i for all $i \in [n]$ as well as $|\psi\rangle$, sample n EPR pairs $|\mathsf{EPR}\rangle_{A,B} := |\mathsf{EPR}\rangle_{A,B,1}, \ldots, |\mathsf{EPR}\rangle_{A,B,n}$, $\alpha = (|\mathsf{EPR}\rangle_B, \alpha_1, \ldots, \alpha_n)$ where $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, (0,0))$, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, apply the unitary $U_{\mathcal{B}'}(\sum_\iota |\beta_\iota\rangle |\phi_{hist}\rangle |\mathsf{EPR}\rangle_A |0\rangle_{\mathsf{T}} |0\rangle_{\mathsf{M}})$ (by running in unbounded-time), and output M to the adversary.

  The indistinguishability between this and the previous hybrid follows from the (perfect) security of the one-time pads and the (perfect) $2t$-privacy of the underlying MPC protocol.

[6] Here, we assume that the classical dual-mode commitments are hardcoded inside the unitary

We prove the indistinguishability of $\mathcal{H}_4$ and $\mathcal{H}_5$ in Claim 4.7 using the results of Claim 4.6 where we abstract the computation of the first message of the prover as a quantum secret sharing scheme.

- $\mathcal{H}_6$: Same as $\mathcal{H}_6$ except that the EPR pairs are, again, replaced with quantum one-time pad encryptions of the history state $|\phi_{hist}\rangle$. In this hybrid, it is also possible to, again, rely on the unitary $U_{\mathcal{B}}$ to program the opening of the dual-mode commitments. In more detail:

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, generate $|\psi\rangle$ by encrypting the $|0\rangle$ state, i.e., $|\psi\rangle = X^a Z^b |0\rangle$ for random a, b, generate $|\phi_{hist}\rangle$ using the secret shares $r_1, \ldots, r_n$ of the opening r of the commitment c and using random a_i, b_i for all $i \in [n]$ as well as $|\psi\rangle$, $\alpha = (|\psi_{hist}\rangle, \alpha_1, \ldots, \alpha_n)$ where $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, (0,0))$ and $|\psi_{hist}\rangle$ is generated as described in $\textsc{Prover}_1$ using $|\phi_{hist}\rangle$ as generated above, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, computes valid openings $(r'_1, \ldots, r'_n)$ to $((a'_1, b'_1), \ldots, (a'_n, b'_n))$ (by running in unbounded-time), hardcodes $U_{\mathcal{B}}$ with $\{((a'_i, b'_i), r'_i)\}_{i\in[n]}$, and computes $U_{\mathcal{B}}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$ where M is output to the adversary.

  The indistinguishability between this and the previous hybrid follows from the (perfect) security of the quantum one-time pad. We prove the indistinguishability of $\mathcal{H}_3$ and $\mathcal{H}_4$ in Claim 4.5.

- $\mathcal{H}_7$: Same as $\mathcal{H}_6$ except that the dual-mode commitments are, again, generated using the actual one-time pad keys (a', b'), which are used to encrypt the history state $|\phi_{hist}\rangle$.

  $\mathsf{ck}_H \leftarrow \mathsf{Gen}_H(1^\lambda)$, $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$, $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$, $\mathsf{CRS} = (\mathsf{ck}_H, \mathsf{ck}, c)$, generate $|\psi\rangle$ by encrypting the $|0\rangle$ state, i.e., $|\psi\rangle = X^a Z^b |0\rangle$ for random a, b, generate $|\phi_{hist}\rangle$ using the secret shares $r_1, \ldots, r_n$ of the opening r of the commitment c and using random a_i, b_i for all $i \in [n]$ as well as $|\psi\rangle$, $\alpha = (|\psi_{hist}\rangle, \alpha_1, \ldots, \alpha_n)$ where $\alpha_i = \mathsf{DualCom}(\mathsf{ck}_H, (a'_i, b'_i); r'_i)$, $\zeta = \{\zeta_i = ((a'_i, b'_i), r'_i)\}_{i\in[n]}$ and $|\psi_{hist}\rangle$ is generated as described in $\textsc{Prover}_1$ using $|\phi_{hist}\rangle$ as generated above, $(\sum_\iota |\beta_\iota\rangle, \xi) \leftarrow \mathcal{A}(\mathsf{CRS}, x, \alpha)$, hardcodes $U_{\mathsf{P}'_2}$ with $(\mathsf{CRS}, x, \alpha, \zeta)$, compute $U_{\mathsf{P}'_2}(\sum_\iota |\beta_\iota\rangle |0\rangle_{\mathsf{M}}) = \sum_\iota |\beta_\iota\rangle |\gamma_\iota\rangle_{\mathsf{M}}$, and output register M to the adversary.

  The statistical indistinguishability between this and the previous hybrid follows from the statistical security of the dual-mode commitments. The proof proceeds analogously to the proof of the indistinguishability between $\mathcal{H}_6$ and $\mathcal{H}_7$ (Claim 3.9).

Claim 4.5. *The hybrids $\mathcal{H}_3$ and $\mathcal{H}_4$ are perfectly indistinguishable.*

Proof. This claim follows directly using the observation that one half of an EPR pair is perfectly indistinguishable from a quantum one-time pad encryption. Therefore, sampling $|\psi_{hist}\rangle$ as half of an EPR pair is indistinguishable to providing an actual encryption of the history state $|\phi_{hist}\rangle$ as the state $|\psi_{hist}\rangle$.

Now, when the adversary asks its challenge, it follows that, after the teleportation protocol has been executed, that the classical bits a, b obtained from the teleportation procedure allow to reconstruct the state state $|\phi_{hist}\rangle$ from the state $|\psi_{hist}\rangle$. This happens using the same operations as in the case that the state $|\psi_{hist}\rangle$ corresponds to a one-time pad encryption. In the next step, the reduction runs in unbounded time to compute the openings for the challenged dual-mode commitments that corresponds to the bits a, b obtained from the quantum teleportation protocol. This concludes the proof of the claim. □

Before proceeding with the proof of Claim 4.7, we cast the first three steps of the prove procedure $\textsc{Prover}_1(\mathsf{CRS}, x, |w\rangle)$, together with some parts of the CRS, as the sharing procedure of a secret sharing scheme for a secret $|w\rangle$ of length m. More precisely:

$\mathsf{Setup}(1^\kappa)$**:** Generate a commitment key $\mathsf{ck} \leftarrow \mathsf{Gen}(1^\lambda)$ for a perfectly binding, computationally hiding commitment scheme and a commitment $c \leftarrow \mathsf{Com}(\mathsf{ck}, 1)$. Output $\mathsf{CRS} = (\mathsf{ck}, c)$.

$\mathsf{Share}(\mathsf{CRS}, |w\rangle, n)$**:** Sample $(a_1, b_1), \ldots, (a_{n-1}, b_{n-1})$ uniformly at random from $\{0,1\}^m \times \{0,1\}^m$. Set $(a, b) \coloneqq \bigoplus_{i\in[n-1]}(a_i, b_i)$. Compute a quantum OTP of the witness, $|\psi\rangle = X^a Z^b |w\rangle$ and sample r_i uniformly at random from $\{0,1\}^\lambda$ for $i \in [n]$. Compute the history state $|\phi_{hist}\rangle$ corresponding to the circuit $\mathcal{C}$ defined in Fig. 2 on input $|a_1, b_1, r_1\rangle \otimes \ldots \otimes |a_{n-1}, b_{n-1}, r_{n-1}\rangle \otimes$

$|\psi, r_n\rangle$ and using CRS. Let m' be the number of qubits in $|\phi_{hist}\rangle$. Sample (a', b') uniformly at random from $\{0,1\}^{m'} \times \{0,1\}^{m'}$. Compute a quantum OTP of the history state, $|\psi_{hist}\rangle = X^{a'} Z^{b'} |\phi_{hist}\rangle$. Output $((a'_i, b'_i)_{i\in[n]}, |\psi_{hist}\rangle)$ with a'_i and b'_i being the keys corresponding to the ith party's registers. (a'_i, b'_i) is the share of the ith party and $|\psi_{hist}\rangle$ is made public.

Reconstruct$(\mathsf{CRS}, |\psi_{hist}\rangle, (a'_i, b'_i)_{i\in[n]})$**:** Compute $|\phi_{hist}\rangle = Z^{b'} X^{a'} |\psi_{hist}\rangle$. In the next step, undo all of the controlled $U_t, \ldots, U_1$ of the history state $|\phi_{hist}\rangle$ using CRS to obtain the inputs $|a_1, b_1, r_1\rangle \otimes \ldots \otimes |a_{n-1}, b_{n-1}, r_{n-1}\rangle \otimes |\psi, r_n\rangle$ of the circuit $\mathcal{C}$. Next, compute and output $|w\rangle = Z^b X^a |\psi\rangle$.

In the next step, we prove that the presented secret sharing scheme achieves perfect t'-out-of-n security.

Claim 4.6. *Let* Π *be a perfectly* t'*-private MPQC protocol, then the above secret sharing scheme is perfectly secure against classical* G *attacks where* G *contains all subsets of* $[n]$ *of size* t'*.*

Proof. To prove this lemma, it suffices to prove that the above described quantum secret sharing scheme is a t'-out-of-n secret sharing scheme, following Remark 3.1. We prove this using the following hybrids:

Hybrid $\mathcal{H}_0$: This hybrid corresponds to the case where (above) the secret sharing scheme is executed using the secret $|w\rangle$.

Hybrid $\mathcal{H}_1$: In this hybrid, the positions of the history state that the adversary does not request as shares are replaced with encryptions of $|0\rangle$. In more detail, if the adversary requests the set of shares T then the state that it will receive is the state $|\psi_{hist}\rangle = X^{a'_1} Z^{b'_1} |\phi_{hist,1}\rangle \otimes \ldots \otimes X^{a'_1} Z^{b'_1} |\phi_{hist,n'}\rangle$ where $|\phi_{hist,i}\rangle = |0\rangle$ for all $i \in T$. The perfect indistinguishability between this and the previous hybrid follows from the security of the quantum one-time pad.

Hybrid $\mathcal{H}_2$: This hybrid corresponds to the setting where the messages of the MPQC protocol Π are generated using the opening of the commitment c as an input instead of the inputs $|a_1, b_1, r_1\rangle \otimes \ldots \otimes |a_{n-1}, b_{n-1}, r_{n-1}\rangle \otimes |\psi, r_n\rangle$ where $(a_1, b_1), r_1, \ldots, (a_{n-1}, b_{n-1}), r_{n-1}, r_n$ are randomly sampled $(a, b) := \bigoplus_{i\in[n-1]} (a_i, b_i)$ and $|\psi\rangle = X^a Z^b |w\rangle$. The perfect indistinguishability between this and the previous hybrid follows from the perfect t'-privacy of the MPQC protocol Π.

Hybrid $\mathcal{H}_3$: In this hybrid, the state $|\psi\rangle$ is generated as an encryption of $|0\rangle$ instead of an encryption of $|w\rangle$. This hybrid is perfectly indistinguishable from the previous hybrid due to the secruity of the quantum one-time pad.

Since this hybrid does not make any use of the $|w\rangle$, this hybrid concludes the security analysis.

Indistinguishability of hybrids $\mathcal{H}_0$ and $\mathcal{H}_1$: The (perfect) indistinguishability of the hybrids $\mathcal{H}_0$ and $\mathcal{H}_1$ follows from the (perfect) security of the quantum one-time pad. We construct a reduction that interacts with the challenger of the quantum one-time pad and simulates the hybrid $\mathcal{H}_0$ or $\mathcal{H}_1$ to the adversary. Here, the underlying challenger runs T different quantum OTP instances, all using the same challenge bit. Such a challenger directly follows from the standard quantum OTP challenger. In the first step, the reduction sets up the CRS and, afterwards, receives the values $(T, |w\rangle)$ from the adversary. Then, the reduction proceeds with the execution of the sharing procedure until it comes to the encryption of the history state $|\phi_{hist}\rangle$. Here, the reduction submits $(|\phi_{hist,i}\rangle, |0\rangle)_{i\in[T]}$ to the underlying challenger and obtains as a reply the ciphertexts $\{|\psi_{hist,i}\rangle\}_{i\in T}$. The remaining encryptions, i.e., $|\psi_{hist,i}\rangle = X^{a'_i} Z^{b'_i} |\phi_{hist,i}\rangle$ with random (a'_i, b'_i) for all $i \in [n'] \setminus T$, are generated as described in the sharing procedure. The reduction then sets $|\psi_{hist}\rangle := |\psi_{hist,1}\rangle \otimes \ldots \otimes |\psi_{hist,n'}\rangle$ and sends this state to the adversary. Our reduction will preserve the distinguishing advantage of $\mathcal{D}$ and we observe that if the underlying challenger encrypts the actual history state the reduction simulates hybrid $\mathcal{H}_0$ and if it encrypts $|0\rangle$ it simulates $\mathcal{H}_1$. This results in the perfect indistinguishability of $\mathcal{H}_0$ and $\mathcal{H}_1$.

Indistinguishability of hybrids $\mathcal{H}_1$ and $\mathcal{H}_2$: We prove the indistinguishability of the hybrids $\mathcal{H}_1$ and $\mathcal{H}_2$ by constructing an adversary $\mathcal{B}$ that breaks the perfect t'-privacy of the MPQC protocol. In the first step, the adversary $\mathcal{B}$ generates the setup for the secret sharing scheme and sends CRS to $\mathcal{A}$. Afterwards, it receives the secret $|w\rangle$ as well as a set of indices T from the adversary $\mathcal{A}$. In the next step, the adversary $\mathcal{B}$ samples $n-1$ shares $(a_1, b_1), \ldots, (a_{n-1}, b_{n-1}) \in \{0,1\}^m$, sets $(a, b) \coloneqq \oplus_{i\in[n-1]}(a_i, b_i)$ and computes a quantum OTP encryption of the witness, $|\psi\rangle = X^a Z^b |w\rangle$. It also computes an additive secret sharing $r_1, \ldots, r_n$ for the opening of the commitment c. Now, by applying Lemma 2.19, we can argue that a history state generated using the inputs that contain the key of the quantum OTP $|a_1, b_1, r'_1\rangle \otimes \ldots \otimes \left|a_{n-1}, b_{n-1}, r'_{n-1}\right\rangle \otimes |\psi, r'_n\rangle$, for the circuit induced by $\Pi_{\mathcal{C}}$ using random r'_i, is indistinguishable from a history state generated using the inputs that contain the trapdoor $|a'_1, b'_1, r_1\rangle \otimes \ldots \otimes \left|a'_{n-1}, b'_{n-1}, r_{n-1}\right\rangle \otimes |\psi, r_n\rangle$, for the circuit induced by $\Pi_{\mathcal{C}}$ using random a'_i, b'_i. This is true since both of these inputs lead to 1 as an output of the MPQC evaluation. Since Lemma 2.19 relies on the perfect t-privacy of the MPQC, it follows that the hybrids $\mathcal{H}_1$ and $\mathcal{H}_2$ are perfectly indistinguishable based on the t-privacy of the MPQC.

Indistinguishability of hybrids $\mathcal{H}_2$ and $\mathcal{H}_3$: The (perfect) indistinguishability of the hybrids $\mathcal{H}_2$ and $\mathcal{H}_3$ follows from the (perfect) security of the quantum one-time pad. We construct a reduction that interacts with the challenger of the quantum one-time pad and simulates the hybrid $\mathcal{H}_2$ or $\mathcal{H}_3$ to the adversary. In the first step, the reduction sets up the CRS, receives the values $(T, |w\rangle)$ from the adversary, submits the two states $(|0\rangle, |w\rangle)$ to the underlying challenger and obtains as a reply the ciphertext $|\psi\rangle$. Afterwards, the reduction proceeds as described in the definition of $\mathcal{H}_2/\mathcal{H}_3$. We observe that none of these steps requires the decryption of $|\psi\rangle$. This is due to the fact that the history state $|\phi_{hist}\rangle$ is generated using the secret shares $r_1, \ldots, r_n$ of the opening r of the commitment c and using random a_i, b_i for all $i \in [n]$ as well as $|\psi\rangle$. Here, the secret shares $r_1, \ldots, r_n$ of the opening r of the commitment c will be used as a witness in the circuit $\mathcal{R}$. Therefore, it is not required to provide valid decryption keys for $|\psi\rangle$ to a state $|w\rangle$ that leads to $\mathcal{M}(x, |w\rangle) = 1$. Our reduction will preserve the distinguishing advantage of $\mathcal{D}$. However, this contradicts the perfect indistinguishability of the quantum one-time pad. As such, we must have that $\mathcal{H}_2$ and $\mathcal{H}_3$ are perfectly indistinguishable.

Combining the above analyses yields the lemma. □

Taking into account Theorem 4.3, we observe that the above defined secret sharing scheme is secure against superposition attacks as long as only $t/2$ shares are revealed for $t' = 2t$.

Claim 4.7. *Let Π be a perfectly $2t$-private MPQC protocol, then the hybrids $\mathcal{H}_4$ and $\mathcal{H}_5$ are perfectly indistinguishable.*

Proof. This claim directly follows with the observation made in Claim 4.6 that the above described scheme is a $2t$-out-of-n secret sharing scheme and that the security of it remains after applying the Circuit-to-Hamiltonian reduction.[7] Therefore, we can rely on the results of Damgård et al. [19, Proposition 1] which state that a perfectly secure $2t$-out-of-n quantum secret sharing scheme is secure against superposition attacks/F-share capture attacks as long as only $t/2$ of the shares are revealed. This directly implies the perfect indistinguishability of the hybrids $\mathcal{H}_4$ and $\mathcal{H}_5$ since in the interaction between the prover and the verifier in the third round only $t/2$ shares are revealed. □

□

Acknowledgments

RJ and DK were supported in part by AFOSR, NSF CAREER CNS-2238718, NSF 2112890, NSF CNS-2247727 and a Google Research Scholar award. This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-23-1-0543. GM is supported by the European Research Council through an ERC Starting Grant (Grant agreement No. 101077455, ObfusQation) and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972.

[7] Otherwise an adversary could simply apply the reduction itself and break the security of the secret sharing scheme.

References

[1] Gorjan Alagic et al. “Non-interactive Classical Verification of Quantum Computation”. In: *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*. Ed. by Rafael Pass and Krzysztof Pietrzak. Vol. 12552. Lecture Notes in Computer Science. Springer, 2020, pp. 153–180. DOI: 10.1007/978-3-030-64381-2˙6.

[2] Gorjan Alagic et al. “On Quantum Chosen-Ciphertext Attacks and Learning with Errors”. In: *Cryptogr.* 4.1 (2020), p. 10. DOI: 10.3390/CRYPTOGRAPHY4010010.

[3] James Bartusek and Giulio Malavolta. “Indistinguishability Obfuscation of Null Quantum Circuits and Applications”. In: *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*. Ed. by Mark Braverman. Vol. 215. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 15:1–15:13. DOI: 10.4230/LIPIcs.ITCS.2022.15.

[4] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. “Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract)”. In: *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*. Ed. by Janos Simon. ACM, 1988, pp. 1–10. DOI: 10.1145/62212.62213.

[5] Rishabh Bhadauria et al. “Ligero++: A New Optimized Sublinear IOP”. In: *CCS ’20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*. Ed. by Jay Ligatti et al. ACM, 2020, pp. 2025–2038. DOI: 10.1145/3372297.3417893.

[6] Ritam Bhaumik et al. “QCB: Efficient Quantum-Secure Authenticated Encryption”. In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Lecture Notes in Computer Science. Springer, 2021, pp. 668–698. DOI: 10.1007/978-3-030-92062-3˙23.

[7] Dan Boneh and Mark Zhandry. “Quantum-Secure Message Authentication Codes”. In: *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 592–608. DOI: 10.1007/978-3-642-38348-9˙35.

[8] Dan Boneh and Mark Zhandry. “Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World”. In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. Lecture Notes in Computer Science. Springer, 2013, pp. 361–379. DOI: 10.1007/978-3-642-40084-1˙21.

[9] Dan Boneh et al. “Random Oracles in a Quantum World”. In: *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. Lecture Notes in Computer Science. Springer, 2011, pp. 41–69. DOI: 10.1007/978-3-642-25385-0˙3.

[10] Zvika Brakerski and Nir Magrafta. “Real-Valued Somewhat-Pseudorandom Unitaries”. In: *Theory of Cryptography - 22nd International Conference, TCC 2024, Milan, Italy, December 2-6, 2024, Proceedings, Part II*. Ed. by Elette Boyle and Mohammad Mahmoody. Lecture Notes in Computer Science. Springer, 2024, pp. 36–59. DOI: 10.1007/978-3-031-78017-2˙2.

[11] Zvika Brakerski and Omri Shmueli. “Scalable Pseudorandom Quantum States”. In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Lecture Notes in Computer Science. Springer, 2020, pp. 417–440. DOI: 10.1007/978-3-030-56880-1˙15.

[12] Anne Broadbent and Alex Bredariol Grilo. “QMA-Hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge”. In: *SIAM J. Comput.* 51.4 (2022), pp. 1400–1450. DOI: 10.1137/21M140729X.

[13] Anne Broadbent et al. “Zero-Knowledge Proof Systems for QMA”. In: *SIAM J. Comput.* 49.2 (2020), pp. 245–283. DOI: 10.1137/18M1193530.

[14] André Chailloux. “Tight quantum security of the Fiat-Shamir transform for commit-and-open identification schemes with applications to post-quantum signature schemes”. In: *CoRR* abs/1906.05415 (2019). DOI: 10.48550/arXiv.1906.05415.

[15] Melissa Chase et al. “Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. Ed. by Bhavani Thuraisingham et al. ACM, 2017, pp. 1825–1842. DOI: 10.1145/3133956.3133997.

[16] Kai-Min Chung et al. “Constant-Round Blind Classical Verification of Quantum Sampling”. In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Lecture Notes in Computer Science. Springer, 2022, pp. 707–736. DOI: 10.1007/978-3-031-07082-2˙25.

[17] Claude Crepeau, Daniel Gottesman, and Adam Smith. *Secure Multi-party Quantum Computing*. 2002. DOI: 10.48550/ARXIV.QUANT-PH/0206138.

[18] Ivan Damgård et al. “Improving the Security of Quantum Protocols via Commit-and-Open”. In: *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Ed. by Shai Halevi. Lecture Notes in Computer Science. Springer, 2009, pp. 408–427. DOI: 10.1007/978-3-642-03356-8˙24.

[19] Ivan Damgård et al. “Superposition Attacks on Cryptographic Protocols”. In: *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013, Proceedings*. Ed. by Carles Padró. Vol. 8317. Lecture Notes in Computer Science. Springer, 2013, pp. 142–161. DOI: 10.1007/978-3-319-04268-8˙9.

[20] Jelle Don et al. “Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model”. In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11693. Lecture Notes in Computer Science. Springer, 2019, pp. 356–383. DOI: 10.1007/978-3-030-26951-7˙13.

[21] Jelle Don et al. “Efficient NIZKs and Signatures from Commit-and-Open Protocols in the QROM”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Lecture Notes in Computer Science. Springer, 2022, pp. 729–757. DOI: 10.1007/978-3-031-15979-4˙25.

[22] Jelle Don et al. “Online-Extractability in the Quantum Random-Oracle Model”. In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 677–706. DOI: 10.1007/978-3-031-07082-2˙24.

[23] Uriel Feige, Dror Lapidot, and Adi Shamir. “Multiple Non-Interactive Zero Knowledge Proofs Based on a Single Random String (Extended Abstract)”. In: *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume I*. IEEE Computer Society, 1990, pp. 308–317. DOI: 10.1109/FSCS.1990.89549.

[24] Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. “Semantic Security and Indistinguishability in the Quantum World”. In: *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9816. Lecture Notes in Computer Science. Springer, 2016, pp. 60–89. DOI: 10.1007/978-3-662-53015-3˙3.

[25] Sumegha Garg, Henry Yuen, and Mark Zhandry. "New Security Notions and Feasibility Results for Authentication of Quantum Data". In: *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10402. Lecture Notes in Computer Science. Springer, 2017, pp. 342–371. DOI: 10.1007/978-3-319-63715-0˙12.

[26] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. "ZKBoo: Faster Zero-Knowledge for Boolean Circuits". In: *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, 2016, pp. 1069–1083.

[27] Oded Goldreich, Silvio Micali, and Avi Wigderson. "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority". In: *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*. Ed. by Alfred V. Aho. ACM, 1987, pp. 218–229. DOI: 10.1145/28395.28420.

[28] J. Alex Halderman et al. "Lest We Remember: Cold Boot Attacks on Encryption Keys". In: *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*. Ed. by Paul C. van Oorschot. USENIX Association, 2008, pp. 45–60. DOI: 10.1145/1506409.1506429.

[29] Michael Hutter and Jörn-Marc Schmidt. "The Temperature Side Channel and Heating Fault Attacks". In: *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*. Ed. by Aurélien Francillon and Pankaj Rohatgi. Vol. 8419. Lecture Notes in Computer Science. Springer, 2013, pp. 219–235. DOI: 10.1007/978-3-319-08302-5˙15.

[30] Yuval Ishai et al. "Zero-Knowledge Proofs from Secure Multiparty Computation". In: *SIAM J. Comput.* 39.3 (2009), pp. 1121–1152. DOI: 10.1137/080725398.

[31] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom Quantum States". In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 126–152. DOI: 10.1007/978-3-319-96878-0˙5.

[32] Elham Kashefi, Luka Music, and Petros Wallden. "The Quantum Cut-and-Choose Technique and Quantum Two-Party Computation". In: *CoRR* abs/1703.03754 (2017). DOI: 10.48550/ARXIV.1703.03754.

[33] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*. Ed. by David Lie et al. ACM, 2018, pp. 525–537. DOI: 10.1145/3243734.3243805.

[34] Julia Kempe, Alexei Y. Kitaev, and Oded Regev. "The Complexity of the Local Hamiltonian Problem". In: *SIAM J. Comput.* 35.5 (2006), pp. 1070–1097. DOI: 10.1137/S0097539704445226.

[35] Julia Kempe and Oded Regev. "3-local Hamiltonian is QMA-complete". In: *Quantum Inf. Comput.* 3.3 (2003), pp. 258–264. DOI: 10.26421/QIC3.3-7.

[36] Alexei Y. Kitaev, A. H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*. Vol. 47. Graduate studies in mathematics. American Mathematical Society, 2002. ISBN: 978-0-8218-3229-5.

[37] Alex Lombardi and Luke Schaeffer. "A Note on Key Agreement and Non-Interactive Commitments". In: *IACR Cryptol. ePrint Arch.* 2019 (2019), p. 279.

[38] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. "A Framework for Efficient and Composable Oblivious Transfer". In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*. Ed. by David A. Wagner. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 554–571. DOI: 10.1007/978-3-540-85174-5˙31.

[39] Adam Smith. “Multi-party Quantum Computation”. In: *CoRR* abs/0111030 (2026). DOI: 10.48550/ARXIV.QUANT-PH/0111030.

[40] Fabian Wiesner and Anna Pappa. “Verified delegated quantum computation requires techniques beyond cut-and-choose”. In: *CoRR* abs/2603.09368 (2026). DOI: 10.48550/ARXIV.2603.09368.

[41] Fabian Wiesner et al. “Why cut-and-choose quantum state verification cannot be both efficient and secure”. In: *IACR Communications in Cryptology* 2.4 (Jan. 8, 2026). ISSN: 3006-5496. DOI: 10.62056/ay11c3c2h.

[42] Salessawi Ferede Yitbarek et al. “Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors”. In: *2017 IEEE International Symposium on High Performance Computer Architecture, HPCA 2017, Austin, TX, USA, February 4-8, 2017*. IEEE Computer Society, 2017, pp. 313–324. DOI: 10.1109/HPCA.2017.10.

[43] Mark Zhandry. “How to Construct Quantum Random Functions”. In: *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*. IEEE Computer Society, 2012, pp. 679–687. DOI: 10.1109/FOCS.2012.37.

[44] Mark Zhandry. “Secure Identity-Based Encryption in the Quantum Random Oracle Model”. In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*. Ed. by Reihaneh Safavi-Naini and Ran Canetti. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 758–775. DOI: 10.1007/978-3-642-32009-5˙44.

A Proof of Security Against Superposition Attacks [19]

Theorem A.1 (Theorem 3.5)**.** *Let S be a secret sharing scheme with adversary structure G. If $F^2 \subseteq G$ where $F^2 \triangleq \{A \mid \exists B, C \in F \ : \ A = B \cup C\}$, then S will be perfectly secure against superposition F-attacks (Definition 3.4).*

Proof of Theorem 3.5. We consider the adversary's final state for any $s \in \mathbb{S}$,

$$\begin{aligned}\rho_s^{adv,F} &= \sum_{r\in\mathcal{R}} p_r \sum_{\substack{x,x'\in\mathcal{X}\\ a,a'\in\{0,1\}^t\\ A,A'\in F}} \alpha^*_{x',A',a'}\,\alpha_{x,A,a}\ |x'\rangle_e\langle x|_e \otimes |A', a'\oplus v_{A'}(s;r)\rangle_q\langle A, a\oplus v_A(s;r)|_q \\ &= \sum_{\substack{x,x'\in\mathcal{X}\\ a,a'\in\{0,1\}^t\\ A,A'\in F}} \alpha^*_{x',A',a'}\,\alpha_{x,A,a}\ |x'\rangle_e\langle x|_e \otimes \sum_{r\in\mathcal{R}} p_r\,|A', a'\oplus v_{A'}(s;r)\rangle_q\langle A, a\oplus v_A(s;r)|_q\,.\end{aligned}$$

We rewrite our state in the following form

$$\rho_s^{adv,F} = \sum_{\substack{a,a'\in\{0,1\}^t\\ A,A'\in F}} \rho_s^{adv,F}|_{a,a',A,A'} \tag{2}$$

where we define

$$\rho_s^{adv,F}|_{a,a',A,A'} = \sum_{x,x'\in\mathcal{X}} \alpha^*_{x',A',a'}\,\alpha_{x,A,a}\ |x'\rangle_e\langle x|_e \otimes \sum_{r\in\mathcal{R}} p_r\,|A', a'\oplus v_{A'}(s;r)\rangle_q\langle A, a\oplus v_A(s;r)|_q\,. \tag{3}$$

Let us fix any arbitrary $a, a' \in \{0,1\}^t$, and $A, A' \in F$. Temporarily consider the state in Equation 3 for some secret $s \in \mathbb{S}$. We notice that only the second term depends on the secret s, so we focus on this term. This term contains information about the views of parties in $B = A' \cup A \in F^2 \subseteq G$. Since our secret sharing scheme S has adversary structure G, S is perfectly secure against classical G-attacks which ensures that the distribution of $v_B(s;r)$ does not depend on s. This, in turn, translates to the statement that for all $s, s' \in \mathbb{S}$, we will have

$$\sum_{r\in\mathcal{R}} p_r\,|A', a'\oplus v_{A'}(s;r)\rangle_q\langle A, a\oplus v_A(s;r)|_q = \sum_{r\in\mathcal{R}} p_r\,|A', a'\oplus v_{A'}(s';r)\rangle_q\langle A, a\oplus v_A(s';r)|_q$$

which would then imply that

$$\rho_s^{adv,F}|_{a,a',A,A'} = \sum_{x,x'\in\mathcal{X}} \alpha^*_{x',A',a'}\,\alpha_{x,A,a}\;|x'\rangle_e\langle x|_e \otimes \sum_{r\in\mathcal{R}} p_r\,|A',a'\oplus v_{A'}(s;r)\rangle_q\langle A,a\oplus v_A(s;r)|_q$$

$$= \sum_{x,x'\in\mathcal{X}} \alpha^*_{x',A',a'}\,\alpha_{x,A,a}\;|x'\rangle_e\langle x|_e \otimes \sum_{r\in\mathcal{R}} p_r\,|A',a'\oplus v_{A'}(s';r)\rangle_q\langle A,a\oplus v_A(s';r)|_q = \rho_{s'}^{adv,F}|_{a,a',A,A'}.$$

Observe that since we fixed arbitrary values for terms $s\in\mathbb{S}$, $a,a'\in\{0,1\}^t$, and $A,A'\in F$, the above argument will follow for any value.

Furthermore, by our definition in Equation 2, we have for all $s,s'\in\mathbb{S}$

$$\rho_s^{adv,F} = \sum_{\substack{a,a'\in\{0,1\}^t\\A,A'\in F}} \rho_s^{adv,F}|_{a,a',A,A'} = \sum_{\substack{a,a'\in\{0,1\}^t\\A,A'\in F}} \rho_{s'}^{adv,F}|_{a,a',A,A'} = \rho_{s'}^{adv,F}.$$

Thus proving that S will be secure against superposition F-attacks. □