On Round Optimal Statistical Zero Knowledge Arguments

Nir Bitansky[1]* and Omer Paneth[2] †

[1] Tel Aviv University
[2] MIT and Northeastern University

Abstract. We construct the first three message statistical zero knowledge arguments for all of NP, matching the known lower bound. We do so based on keyless multi-collision resistant hash functions and the Learning with Errors assumption — the same assumptions used to obtain round optimal computational zero knowledge.
The main component in our construction is a statistically witness indistinguishable argument of knowledge based on a new notion of statistically hiding commitments with subset opening.

1 Introduction

Since their introduction three decades ago [GMR89], the concept of zero knowledge protocols has played a central role in the development of modern cryptography. Different flavors of zero knowledge protocols have been studied according to the level of soundness and zero knowledge achieved. Either property can be *statistical* or *computational*, meaning that it holds against unbounded or computationally bounded adversaries, respectively. Protocols that satisfy both properties statistically, known as *statistical zero knowledge proofs*, are only possible for languages in $\mathbf{AM} \cap \mathbf{coAM}$ [For89, AH91]; however, once either property is relaxed to computational, protocols for all of **NP** can be constructed assuming one way functions [GMW91, Nao91, BCC88, NOVY98, HNO$^+$09].

In this work, we focus on *statistical zero knowledge arguments* for **NP**; namely, computationally sound protocols where the view of any efficient verifier can be efficiently simulated up to a negligible statistical difference. Such protocols are especially appealing due to their *everlasting zero knowledge guarantee* — even if the verifier stores conversations with the prover and post-processes

*Member of the Check Point Institute of Information Security. Supported by ISF grant 18/484, the Alon Young Faculty Fellowship, and by Len Blavatnik and the Blavatnik Family Foundation.

†Supported by NSF Grants CNS-1413964, CNS-1350619 and CNS-1414119, and the Defense Advanced Research Projects Agency (DARPA) and the U.S. Army Research Office under contracts W911NF-15-C-0226 and W911NF-15-C-0236.

them for as long as it wants, it does not learn anything that cannot be simulated efficiently.

A foundational question is the round complexity of such protocols. Four message protocols can be constructed based on collision resistant hash functions [BJY97]. In terms of lower bounds, at least three messages are necessary even for computational zero knowledge [GO94]. Constructing zero knowledge arguments with matching round complexity has so far appeared more difficult in the statistical setting than in the computational one. Computational zero knowledge in three messages has been long known under unfalsifiable knowledge assumptions [HT98, BP04, CD09, BCC$^+$14] and recently also under a falsifiable multi-collision resistance assumption on keyless hash functions [BKP18]. In contrast, three message statistical zero knowledge has been out of reach (even under knowledge assumptions).

The difference between the statistical and computational settings seems to run somewhat deeper, and manifests itself even in *witness indistinguishability*, a relaxation of zero knowledge. While computational witness indistinguishability has been long known in three [GMW91, FLS99], two [DN07], or even one message [BOV07, GOS12], statistical witness indistinguishability in less than four messages has only been very recently achieved [KKS18]. In fact, *witness indistinguishable arguments of knowledge*, which are essential in the constructions of three message computational zero knowledge, are still not known in less than four messages in the statistical setting.

All and all, we are faced with the question:

What is the round complexity of statistical zero knowledge arguments?

1.1 Results

We construct the first round optimal statistical zero knowledge argument under the same assumptions on which computational zero knowledge arguments are currently known.

Theorem 1.1 (Informal). *Assuming keyless multi-collision resistant hash functions and LWE, both quasi-polynomially hard, there exist three message statistical zero knowledge arguments.*[3]

Keyless multi-collision resistant hash functions, introduced in [BKP18], are functions $\mathsf{H} : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}$ guaranteeing that no efficient adversary with non-uniform description of polynomial size S can find more than $\text{poly}(S)$ elements that collide under H. Here poly is some fixed polynomial and the adversary's running time may be an arbitrarily larger polynomial, or even quasipolynomial (as required in the above theorem). While at this point non-standard, multi-collision resistance of keyless hash functions is a falsifiable and relatively simple assumption, which plausibly holds for existing keyless hash functions (see discussion in [BKP18]).

[3] Here LWE is used to realize several generic primitives, which we address in the body.

Four message protocols from weaker assumptions. When considering keyed hash functions, multi-collision resistance becomes a standard assumption that relaxes the classical notion of collision resistance. A recent line of work explores such hash functions demonstrating that their power goes beyond one-way functions to achieve some of the applications of collision resistance [BDRV18, BKP18, KNY17, KNY18, BHKY19]. Our second result is along this vein showing that four message statistical zero knowledge arguments can be based on (keyed) multi-collision resistance instead of full fledged collision resistance.

Theorem 1.2 (Informal). *Assuming (keyed) multi-collision resistant hash functions, there exist four message statistical zero knowledge arguments.*

A main building block in both of the above results is a new statistically witness indistinguishable argument of knowledge, which was so far known from collision resistance in four messages.

Theorem 1.3 (Informal). *Assuming multi-collision resistant hash functions, there exist four message statistically witness indistinguishable arguments of knowledge. If the hash functions are keyless the arguments have three messages.*

Most of the technical effort in this work is devoted toward proving this theorem.

1.2 Technical Overview

We now provide an overview of the main ideas and techniques behind our results. We start with our construction of statistically witness indistinguishable arguments of knowledge and then move on to explain how they are used to construct statistical zero knowledge arguments.

Classical witness indistinguishable protocols from bit commitments. To understand the challenge, let us recall how classical witness indistinguishable arguments of knowledge are designed. Such protocols traditionally involve three basic steps: a prover commitment, a verifier challenge, and a prover decommitment. The prover commitment consists of multiple bit commitments, a subset of which are opened in the decommitment step according to the challenge given by the verifier. For instance, in Blum's Hamiltonocity protocol [Blu86], the prover commits to the entries of the adjacency matrix of a graph and then, according to the challenge, either opens a subset of edges corresponding to a Hamiltonian cycle or the entire graph. This is repeated in parallel to decrease the soundness error to negligible. (The protocol contains additional details that we omit.)

Indeed, given statistically hiding bit commitments, such protocols can be shown to be statistically witness indistinguishable. However, focusing on round complexity, such commitments inherently require at least two messages — if the commitment was non-interactive, a cheating prover could have equivocal openings for some commitments non-uniformly hardwired into its code; such openings always exist due to statistical hiding.

Weakly binding commitments. While standard binding cannot be achieved non-interactively for statistically hiding bit commitments, keyless multi-collision resistant hash functions are known to imply non-interactive statistically hiding commitments with *weak binding* [BKP18]. Weak binding says that an attacker could only ever open a given commitment to values from some polynomial-size set. Intuitively, this means that even if it has equivocal openings of some commitment hardwired in its code, these cannot be used to sample more openings (except with negligible probability). Weak binding, however, is only meaningful in commitments for long strings and is completely meaningless for bit commitments, where the prover can open commitments to both zero and one. Accordingly, it is not clear how to use it in classical witness indistinguishable protocols that are all based on bit commitments.

An analogous problem is encountered in the work of [BKP18]. They define commitments for long strings with a subset opening property that enables to open only a given subset of bits, without having to open the entire string. While traditionally we require that every individual bit is fixed by the commitment, they suggest a relaxed definition suited for the setting of weak binding. They require that for any fixed adversary, a commitment to a long string $X \in \{0,1\}^L$ fixes a *global* set of strings $\mathbf{X} \subseteq \{0,1\}^L$ of polynomial size K, so that whenever the adversary opens some subset of bits $I \subseteq [L]$, they must all be *simultaneously consistent* with one string in the set $\mathbf{X}$ (except with negligible probability over the adversary's coins).

Our first observation is that commitments with subset opening and the above weak, but global, binding guarantee is sufficient for establishing soundness and also knowledge extraction in classical protocols. Roughly speaking, this is because for any prover that convinces the verifier of accepting with noticeable probability ε, there must be a single string $X \in \mathbf{X}$, such that with probability ε/K, the prover convinces the verifier *while answering consistently with* X. Since ε/K is still noticeable, soundness and knowledge extraction essentially reduce to those of the original protocol in the fully binding setting.

The work of [BKP18] constructs commitments with subset opening that fall short of achieving statistical hiding (indeed they focus on succinctness rather than hiding). In their construction, an opening of a given subset also reveals information regarding unopened bits, thus making them unfit for instantiating witness indistinguishable protocols. At high level, the reason they do not achieve statistical hiding is that to enforce consistency, subsets of bits are always opened in a correlated way and the correlations also pertain to unopened bits (this will become more clear below when we describe our construction).

Statistically hiding commitments with subset opening. We provide a construction that also achieves statistical hiding. Specifically, commitments to any two vectors X, X' are statistically indistinguishable, even given an opening of any subset of entries where X and X' agree. Our construction combines ideas from [BKP18] along with new ideas aimed toward statistical hiding.

The construction is based on statistically hiding weakly binding string commitments (with no subset opening) and Shamir secret sharing [Sha79]. At abstract level, Shamir secret sharing with parameters (n, d) allows to sample an encoding $\hat{b} \in \Sigma^n$ over some alphabet Σ of a secret bit $b \in \{0, 1\}$, so that two properties are guaranteed. First, any two encodings $\hat{0}$ and $\hat{1}$ of zero and one agree on at most d entries. Second, any d entries of a random encoding $\hat{b}$ perfectly hide the bit b.

The commitment scheme works as follows:

- **Commitment:** to commit to a string $X \in \{0, 1\}^L$, we sample encodings $\widehat{X}_i$ for all bits X_i of X. Then, considering the matrix $\widehat{X} = \left(\widehat{X}_{i,j}\right)$ whose rows are the encodings $\widehat{X}_i$, we compute a statistically hiding weakly-binding commitment to each row and each column of the matrix $\widehat{X}$.
- **Opening:** opening a subset of entries $I \subseteq [L]$ consists of two messages: a receiver challenge C, and a corresponding decommitment. The challenge consists of d random indices $C \subseteq [n]$. A decommitment involves opening the commitments to all rows $i \in I$ and all columns $j \in C$. The receiver verifies that the individual decommitments are valid and are consistent (on the intersection of corresponding rows and columns).

Let us explain at high level how the scheme satisfies statistical hiding and (global) weak binding. To show that any unopened entry $i \notin I$ remains statistically hidden, we rely on the fact that the commitment corresponding to its row $\widehat{X}_i$ is statistically hiding and never opened. Since only d column commitments are opened, only d entries of $\widehat{X}_i$ are revealed and thus the Shamir hiding property guarantees that the bit X_i remains statistically hidden.

Proving weak (global) binding is inspired by ideas from [BKP18]. Roughly speaking, the weak binding of individual row commitments guarantees that for every row i, the sender can only ever open the corresponding commitment to encodings $\widehat{X}_i$ from some fixed set $\mathbf{S}_i$ of polynomial size $K = \text{poly}(\lambda)$ in the security parameter λ. We then use the fact that encodings of two distinct bits are far apart to argue that with overwhelming probability the answers to the random challenge (columns) uniquely fix all the bits of the string X. We further show that due to the individual weak binding of column commitments, these answers come from a polynomial set, and accordingly the string X determined by these answers must also come from a polynomial-size set $\mathbf{X}$.

In a bit more detail, we choose the parameters (n, d) of Shamir secret sharing so that the relative agreement of encodings of distinct bits is polynomially small $d/n < \lambda^{-\Omega(1)}$. Then choosing a large enough constant τ such that

$$L \cdot K^2 \cdot (d/n)^\tau \ll 1$$

guarantees that for τ random locations $T \subseteq [n]$, for all bits $i \in [L]$, any two encodings in $\mathbf{S}_i$ that agree on T must encode the same bit.

By the weak binding of column commitments, any opened column $j \in T$ is taken from a fixed set $\mathbf{S}'_j$ of polynomial size K, which means that all opened bits must simultaneously be consistent with some X taken from a set $\mathbf{X}_T$ of polynomial size K^τ. The actual construction chooses d random challenges C for super-logarithmic d, so that with overwhelming probability they include a fixing set $T \subseteq C$, and the set $\mathbf{X}$ is the union of all corresponding sets $\mathbf{X}_T$ (the number of which is at most d^τ and thus polynomial).

Statistical zero knowledge. We now explain how the statistical zero knowledge protocols behind Theorems 1.1 and 1.2 is obtained. The four message protocol from (keyed) multi-collision resistance is obtained in a black-box way by replacing the statistically witness indistinguishable argument of knowledge (from collision resistance) in the protocol of [BJY97] with our witness indistinguishable argument from multi-collision resistance. We focus on explaining how three-message statistical zero knowledge is obtained from keyless multi-collision resistant hashing.

Our starting point is the three-message *computational* zero knowledge argument of [BBK$^+$16] and its subsequent extension in [BKP18] based on multi-collision resistant hash functions. At high level, their protocol follows the recipe of Barak's non-black-box simulation technique [Bar01]. To prove an **NP** statement $x \in \mathcal{L}$, the prover sends a shrinking commitment cmt to the code of some (potentially long) program Π and the verifier responds with a random string r. Then, the prover gives a succinct witness indistinguishable argument of knowledge proving that either $x \in \mathcal{L}$ or that the committed program $\Pi(\mathsf{cmt})$ outputs r. At high level, by committing to the code of the verifier itself, a non-black-box simulator is able to produce an accepting transcript without using the witness, while a cheating prover, who does not know the verifier's randomness r, can only commit to such a program with negligible probability.

In [BBK$^+$16, BKP18], the succinct witness indistinguishable argument of knowledge is constructed from a (non-succinct) witness indistinguishable argument of knowledge, a *secure function evaluation scheme*, and a *weak memory delegation scheme*, which they construct based on keyless multi-collision resistant hashing. Upgrading the protocol from computational zero knowledge to statistical zero knowledge requires two main changes. First, the prover commitment cmt is replaced with a statistically hiding commitment that is weakly binding, which as already observed in [BKP18] is sufficient. Second, the succinct witness indistinguishable argument of knowledge is replaced with a statistically witness indistinguishable one.

To obtain the succinct witness indistinguishable argument, we replace the (computationally) witness indistinguishable argument with our statistically witness indistinguishable argument. In addition, need the secure function evaluation scheme to satisfy statistical function hiding, which can be achieved assuming LWE [OPP14, BD18]. The actual construction requires that the witness indistinguishable argument possesses additional properties, such as adaptive witness indistinguishability and adaptive argument of knowledge, when the statement proven is adversarially chosen after the first two messages of the protocol. The protocol we construct is a slightly tweaked version of the protocol described in this introduction that satisfies these properties.

1.3 More Related Work

We next address additional related work in more detail.

More on statistical zero knowledge arguments. From the early constructions of zero knowledge protocols [GMW91, BCC88] it was evident that statistically hiding commitments are sufficient to obtain statistically zero knowledge arguments in a super logarithmic number of rounds. (See [HNO$^+$09] for a survey on statistically hiding commitments.) Early constant round constructions [BCY91] were based on specific number theoretic assumptions. The work of Bellare, Jakobson, and Yung constructed computational zero knowledge arguments in four messages from one-way functions; however, their construction in fact uses a four message witness indistinguishable argument of knowledge in a generic manner. Using two-message statistically hiding commitments [DPP93, HM96], such arguments can be obtained from collision resistant hashing.

The round complexity of zero knowledge proofs. This paper focuses on the notion of (statistical zero knowledge) arguments. The round complexity of zero-knowledge proofs (which are statistically sound) for **NP** has also been studied extensively. Four-message proofs are impossible to achieve via black-box simulation, except for languages in **NP**$\cap$**coAM** [Kat12]. Four message proofs with non-black-box simulation are only known assuming multi-collision-resistance keyless hash functions [BKP18]. Recent evidence [FGJ18] suggests that, differently from zero-knowledge arguments, zero-knowledge proofs may be impossible to achieve in three messages (even with non-black-box simulation).

The black box barrier. Goldreich and Krawczyk show that three message computational (let alone, statistical) zero knowledge arguments cannot be achieved with black box simulation [GK96]. The seminal work of Barak was the first to show that *non-black-box simulation* could potentially cross such black box barriers [Bar01]. Works of Bitansky et al. [BCPR14, BBK$^+$16] obtain three message (computational) zero knowledge arguments in case where either the (adversarial) verifier or prover have an a-priori bounded description (and arbitrary polynomial running time). Following, the work of [BKP18] obtains such arguments also against non-uniform verifiers and provers relying on keyless multi-collision resistance.

A stronger notion of statistical zero knowledge. The literature (e.g. [HNO$^+$09]) also considers a stronger form of statistical zero knowledge than the one presented in this introduction where the simulator is not only required to statistically simulate the view of efficient verifiers, but also of inefficient ones, given oracle access to the verifier. We note that this notion is outright impossible in three messages where black box simulation is impossible [GK96]. Our four message protocol, in fact, does achieve this stronger notion.

2 Preliminaries

We rely on the standard computational concepts and notation:

- A PPT is a probabilistic polynomial-time algorithm.
- A uniform algorithm is T-time if it runs in time polynomial in T. (T may be super-polynomial in its input size.)
- We follow the standard habit of modeling any efficient adversary strategy as a family of polynomial-size circuits. For an adversary $\mathcal{A}$ corresponding to a family of polynomial-size circuits $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, we often omit the subscript λ, when it is clear from the context.
- We say that a function $f : \mathbb{N} \to \mathbb{R}$ is negligible if for all constants $c > 0$, there exists $N \in \mathbb{N}$ such that for all $n > N$, $f(n) < n^{-c}$. We sometimes denote negligible functions by negl.
- We say that a function $f : \mathbb{N} \to \mathbb{R}$ is noticeable if there exists a constant $c > 0$ and $N \in \mathbb{N}$ such that for all $n > N$, $f(n) \geq n^{-c}$.
- We denote statistical distance by $\mathbf{SD}$.
- For two random variables X, Y and $\varepsilon \in [0, 1]$, we write $X \approx_\varepsilon Y$ to denote the fact that $\mathbf{SD}(X, Y) \leq \varepsilon$.
- For two ensembles $\mathcal{X} = \{X_\lambda\}_{\lambda\in\mathbb{N}}$ and $\mathcal{Y} = \{Y_\lambda\}_{\lambda\in\mathbb{N}}$, we say that $\mathcal{X}$ and $\mathcal{Y}$ are statistically indistinguishable if there exists a negligible $\mu(\cdot)$, such that for all λ, $X_\lambda \approx_{\mu(\lambda)} Y_\lambda$. We denote this by $\mathcal{X} \approx_s \mathcal{Y}$.
- For a string X of length n, and a subset $I \subseteq [n]$, we denote by $X|_I$ its restriction to the entries in I.

2.1 Statistical Zero-Knowledge Arguments

In what follows, we denote by $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ a protocol between two parties P and V. For input w for P, and common input x, we denote by $\langle \mathsf{P}(w) \leftrightarrows \mathsf{V} \rangle(x)$ the output of V in the protocol. For honest verifiers this output will be a single bit indicating acceptance (or rejection), whereas malicious verifiers output their entire view. Throughout, we assume that honest parties in all protocols are uniform PPT algorithms.

Definition 2.1. *A protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ for an* ***NP*** *relation $\mathcal{R}(x, w)$ is a statistical zero-knowledge argument if it satisfies:*

Completeness: *For any $\lambda \in \mathbb{N}, x \in \mathcal{L}(\mathcal{R}) \cap \{0, 1\}^\lambda$, $w \in \mathcal{R}(x)$:*

$$\Pr\left[\langle \mathsf{P}(w) \leftrightarrows \mathsf{V} \rangle(x) = 1\right] = 1 \ .$$

Computational Soundness: *For every polynomial-size circuit family of provers $\mathsf{P}^* = \{\mathsf{P}^*_\lambda\}_\lambda$, there exists a negligible function μ, such that for any $x \in \{0, 1\}^\lambda \setminus \mathcal{L}(\mathcal{R})$,*

$$\Pr\left[\langle \mathsf{P}^*_\lambda \leftrightarrows \mathsf{V} \rangle(x) = 1\right] \leq \mu(\lambda) \ .$$

Statistical Zero-Knowledge: *There exists a PPT simulator S such that for every polynomial-size circuit family $\mathsf{V}^* = \{\mathsf{V}^*_\lambda\}_\lambda$:*

$$\{\langle \mathsf{P}(w) \leftrightarrows \mathsf{V}^*_\lambda \rangle(x)\}_{\substack{(x,w)\in\mathcal{R} \\ |x|=\lambda}} \approx_s \{\mathsf{S}(x, \mathsf{V}^*_\lambda)\}_{\substack{(x,w)\in\mathcal{R} \\ |x|=\lambda}} \ .$$

2.2 Weakly Binding Commitments and Multi-Collision Resistant Hash Functions

We define weakly-binding statistically-hiding commitments [BKP18]. The definition addresses both the setting of keyed hash functions as well as keyless ones.

Syntax: A commitment scheme is associated with an input length function $\ell(\lambda)$ and polynomial-time algorithms $\mathsf{SHC} = (\mathsf{SHC.Gen}, \mathsf{SHC.Com})$ with the following syntax:

- $\mathsf{pk} \leftarrow \mathsf{SHC.Gen}(1^\lambda)$: a probabilistic algorithm that takes the security parameter 1^λ and outputs a key $\mathsf{pk} \in \{0,1\}^\lambda$. In the keyless setting, this algorithm is deterministic and outputs a fixed key $\mathsf{pk} \equiv 1^\lambda$.
- $\mathsf{cmt} \leftarrow \mathsf{SHC.Com}(X;\mathsf{pk})$: a probabilistic algorithm that takes the key pk and an input $X \in \{0,1\}^{\ell(\lambda)}$ and outputs a commitment cmt. When we want to be explicit about the randomness r used by the algorithm, we may write $\mathsf{SHC.Com}(X;\mathsf{pk},r)$.

Definition 2.2 (Weakly-Binding Statistically-Hiding Commitments). *For a polynomial $\ell(\cdot)$, a weakly-binding statistically-hiding commitment* $\mathsf{SHC} = (\mathsf{SHC.Gen},\ \mathsf{SHC.Com})$*, for messages of length ℓ, satisfies:*

Statistical Hiding: *For any key and any two plaintexts, the corresponding commitments are statistically close:*

$$\left\{\mathsf{SHC.Com}(X;\mathsf{pk})\right\}_{\substack{\lambda\in\mathbb{N},\mathsf{pk}\in\{0,1\}^\lambda,\\ X,X'\in\{0,1\}^{\ell(\lambda)}}} \approx_{2^{-\lambda}} \left\{\mathsf{SHC.Com}(X';\mathsf{pk})\right\}_{\substack{\lambda\in\mathbb{N},\mathsf{pk}\in\{0,1\}^\lambda,\\ X,X'\in\{0,1\}^{\ell(\lambda)}}} .$$

Weak Binding: *For any non-uniform polynomial-size probabilistic $\mathcal{A} = \left\{\mathcal{A}^1_\lambda, \mathcal{A}^2_\lambda\right\}_\lambda$ there exists a polynomial $K(\cdot)$ and a negligible $\mu(\cdot)$, such that for all $\lambda \in \mathbb{N}$,*

$$\Pr_{\substack{\mathsf{pk}\leftarrow\mathsf{SHC.Gen}(1^\lambda)\\ (\mathsf{cmt},\mathsf{st})\leftarrow\mathcal{A}^1_\lambda(\mathsf{pk})}} \left[\begin{array}{l} \exists\mathbf{X} \textit{ of size } K(\lambda): \\ \Pr_{(X,r)\leftarrow\mathcal{A}^2_\lambda(\mathsf{st})}\left[\begin{array}{l}\mathsf{cmt} = \mathsf{SHC.Com}(X;\mathsf{pk},r)\\ X \notin \mathbf{X}\end{array}\right] \leq \mu(\lambda)\end{array}\right] \geq 1-\mu(\lambda) .$$

Multi-collision resistance. We also define multi-collision resistant hash functions [BKP18], which are similar to weakly binding commitments, only that the hiding requirement is replaced with the requirement that they shrink their input (accordingly, they are also deterministic).

Syntax: A hashing scheme is associated with an input length function $\ell(\lambda)$ and polynomial-time algorithms $\mathsf{H} = (\mathsf{H.Gen}, \mathsf{H.Hash})$ with the following syntax:

- $\mathsf{pk} \leftarrow \mathsf{H.Gen}(1^\lambda)$: a probabilistic algorithm that takes the security parameter 1^λ and outputs a key $\mathsf{pk} \in \{0,1\}^\lambda$. In the keyless setting, this algorithm is deterministic and outputs a fixed key $\mathsf{pk} \equiv 1^\lambda$.
- $Y \leftarrow \mathsf{H.Hash}(X;\mathsf{pk})$: a deterministic algorithm that takes the key pk and an input $X \in \{0,1\}^{\ell(\lambda)}$ and outputs a hash value Y.

Definition 2.3 (Multi-Collision Resistant Hash). *For a polynomial $\ell(\cdot)$, a multi-collision resistant hash $\mathsf{H} = (\mathsf{H.Gen}, \mathsf{H.Hash})$, for messages of length ℓ, satisfies:*

Compression: *$\ell(\lambda) > \lambda$ and $|\mathsf{H.Hash}(X)| = \lambda$ for all $\lambda \in \mathbb{N}$, key $\mathsf{pk} \in \{0,1\}^{\lambda}$, and $X \in \{0,1\}^{\ell(\lambda)}$. If $\ell = \lambda \cdot (1 + \Omega(1))$ we say that H is linearly compressing and if $\ell = \lambda^{1+\Omega(1)}$ we say that H is polynomially compressing.*

Multi-Collision Resistance: *For any non-uniform polynomial-size probabilistic $\mathcal{A} = \left\{\mathcal{A}^1_\lambda, \mathcal{A}^2_\lambda\right\}_\lambda$ there exists a polynomial K and a negligible $\mu(\cdot)$, such that for all $\lambda \in \mathbb{N}$,*

$$\Pr_{\substack{\mathsf{pk} \leftarrow \mathsf{SHC.Gen}(1^\lambda) \\ (Y,\mathsf{st}) \leftarrow \mathcal{A}^1_\lambda(\mathsf{pk})}} \left[\begin{array}{l} \exists \mathbf{X} \textit{ of size } K(\lambda) : \\ \Pr_{X \leftarrow \mathcal{A}^2_\lambda(\mathsf{st})} \left[Y = \mathsf{H.Hash}(X;\mathsf{pk}) \wedge X \notin \mathbf{X} \right] \leq \mu(\lambda) \end{array} \right] \geq 1 - \mu(\lambda) \ .$$

We also consider a generalized notion of T-secure multi-collision resistant hashing that allows addressing attackers that run in super-polynomial time. The constructions in this paper all rely on the above polynomial notion. Quasipolynomial security is used in [BKP18] to construct weak memory delegation as defined in Section 2.3. We state the definition here for completeness.

T-Secure Multi-Collision Resistance: *For any non-uniform polynomial-size probabilistic $\mathcal{A} = \left\{\mathcal{A}^1_\lambda\right\}$ and any uniform T-time $\mathcal{A}_2$ there exists a polynomial K and a negligible $\mu(\cdot)$, such that for all $\lambda \in \mathbb{N}$,*

$$\Pr_{\substack{\mathsf{pk} \leftarrow \mathsf{SHC.Gen}(1^\lambda) \\ (Y,\mathsf{st}) \leftarrow \mathcal{A}^1_\lambda(\mathsf{pk})}} \left[\begin{array}{l} \exists \mathbf{X} \textit{ of size } K(\lambda) : \\ \Pr_{X \leftarrow \mathcal{A}^2(\mathsf{st})} \left[Y = \mathsf{H.Hash}(X;\mathsf{pk}) \wedge X \notin \mathbf{X} \right] \leq \mu(\lambda) \end{array} \right] \geq 1 - \mu(\lambda) \ .$$

Remark 2.1. Note that for polynomial $T(\lambda) = \mathrm{poly}(\lambda)$, T-security coincides with (plain) security. Indeed, the non-uniformity of $\mathcal{A}^2$ can always be pushed to $\mathcal{A}^1$ who passes a state to $\mathcal{A}^2$.

In [BKP18], it is shown that multi-collision resistant hashing implies weakly binding string commitments.

Theorem 2.1 ([BKP18]). *Assuming a multi-collision-resistant keyless hash that is either:*

- *polynomially compressing*
- *or, linearly compressing and* quasipoly(λ)*-secure*

there exist, for every polynomial $L(\cdot)$, a weakly-binding statistically-hiding commitment and multi-collision-resistant keyless hash, both for messages of length L.

2.3 Weak Memory Delegation

The notion of weak memory delegation was defined in [BKP18] as a relaxation of memory delegation [CKLR11, KP16]. In a two-message memory delegation scheme, an untrusted server provides the client a short commitment or *digest* dig of a large memory D. The client can then delegate any arbitrary deterministic computation M to be executed over the memory. The server responds with the computation's output y, as well as a short proof of correctness that can be verified by the client in time that is independent of that of the delegated computation and the size of the memory.

In the definition of memory delegation in [KP16], the soundness requirement says that having provided the digest dig, a cheating prover should not be able to prove that a given computation M results in more than a single outcome y. In weak memory delegation, the prover should not be able to prove consistency with *too many* outcomes y.

Syntax: A two-message memory delegation scheme is associated with polynomial-time algorithms
$(\mathsf{MD.Mem}, \mathsf{MD.Query}, \mathsf{MD.Prove}, \mathsf{MD.Ver})$ with the following syntax:

- $\mathsf{dig} \leftarrow \mathsf{MD.Mem}(1^\lambda, D)$: a deterministic polynomial-time algorithm that given the security parameter 1^λ and memory D, outputs a digest $\mathsf{dig} \in \{0,1\}^\lambda$ of the memory.
- $(\mathsf{q}, \mathsf{vst}) \leftarrow \mathsf{MD.Query}(1^\lambda)$: a randomized polynomial-time algorithm that given the security parameter 1^λ, outputs a query q and a secret state vst.
- $\pi \leftarrow \mathsf{MD.Prove}(1^\lambda, D, (M, 1^t, y), \mathsf{q})$: a deterministic algorithm that takes the security parameter 1^λ, a memory string D, a (deterministic) Turing machine M, an output string y, and time bound 1^t such that $|D| \leq t \leq 2^\lambda$ and $M(D)$ outputs y within t steps. It outputs a proof π.
- $b \leftarrow \mathsf{MD.Ver}(1^\lambda, \mathsf{dig}, (M, t, y), \mathsf{vst}, \pi)$: a deterministic polynomial time oracle algorithm that takes the security parameter 1^λ, a digest dig, a (deterministic) Turing machine M, a time bound t, an output string y, a secret state vst and a proof π. It outputs an acceptance bit b.

Definition 2.4 (Entropic Distribution Ensemble). *We say that an efficiently samplable distribution ensemble $\{Y_\lambda\}_{\lambda \in \mathbb{N}}$ is entropic if*

$$H_\infty(Y_\lambda) := -\log \max_{y \in \mathrm{supp}(Y_\lambda)} \Pr[Y_\lambda = y] = \Omega(\lambda) \ .$$

Definition 2.5 (Weak Memory Delegation). *A two-message delegation scheme*
$\mathsf{MD} = (\mathsf{MD.Mem}, \mathsf{MD.Query}, \mathsf{MD.Prove}, \mathsf{MD.Ver})$ *satisfies:*

Efficiency: *There exists a polynomial p such that for every $\lambda \in \mathbb{N}$ and D such that $|D| \leq 2^\lambda$, $\mathsf{MD.Mem}(1^\lambda, D)$ outputs a digest dig of length at most $p(\lambda)$.*

Correctness: *For every security parameter $\lambda \in \mathbb{N}$, every $(M, t, y) \in \{0,1\}^\lambda$, and every D such that $M(D)$ outputs y within t steps, and $|D| \leq t \leq 2^\lambda$:*

$$\Pr\left[\mathsf{MD.Ver}(1^\lambda, \mathsf{dig}, (M,t,y), \mathsf{vst}, \pi) = 1 \;\middle|\; \begin{array}{l} \mathsf{dig} \leftarrow \mathsf{MD.Mem}(1^\lambda, D) \\ (\mathsf{q}, \mathsf{vst}) \leftarrow \mathsf{MD.Query}(1^\lambda) \\ \pi \leftarrow \mathsf{MD.Prove}(1^\lambda, D, (M, 1^t, y), \mathsf{q}) \end{array}\right] = 1 \enspace .$$

Weak Soundness for Time-T: *For every non-uniform polynomial-size probabilistic $(\mathcal{A}_1, \mathcal{A}_2)$, there exists a negligible function μ, such that for every ensemble of samplable entropic distributions $\{Y_\lambda\}_{\lambda \in \mathbb{N}}$, $\lambda \in \mathbb{N}$ and $t \leq T(\lambda)$:*

$$\Pr\left[\mathsf{MD.Ver}(1^\lambda, \mathsf{dig}, (M,t,y), \mathsf{vst}, \pi) = 1 \;\middle|\; \begin{array}{l} (\mathsf{dig}, M, \mathsf{st}) \leftarrow \mathcal{A}_1(1^\lambda) \\ (\mathsf{q}, \mathsf{vst}) \leftarrow \mathsf{MD.Query}(1^\lambda) \\ y \leftarrow Y_\lambda \\ \pi \leftarrow \mathcal{A}_2(\mathsf{q}, y; \mathsf{st}) \end{array}\right] \leq \mu(\lambda) \enspace .$$

Theorem 2.2 ([BKP18]). *Assuming a linearly compressing* quasipoly(λ)-*secure multi-collision-resistant keyless hash and* quasipoly(λ)*-secure fully-homomorphic encryption, there exists a two-message memory-delegation scheme with weak soundness for time-*quasipoly(λ)*.*

2.4 Function Hiding Secure Function Evaluation

We define two-message secure function evaluation protocols with statistical function hiding.

Syntax: Let $\mathcal{C} = \{\mathcal{C}_\lambda\}_\lambda$ be a family of circuits. A two-message secure function evaluation protocol for $\mathcal{C}$ is associated with polynomial-time algorithms (SFE.Enc, SFE.Eval, SFE.Dec) with the following syntax:

- $(\mathsf{sk}, \mathsf{ct}) \leftarrow \mathsf{SFE.Enc}(1^\lambda, x)$: a probabilistic algorithm that takes a security parameter 1^λ and a string $x \in \{0,1\}^*$ and outputs a secret key sk and a ciphertext ct.
- $\widehat{\mathsf{ct}} \leftarrow \mathsf{SFE.Eval}(C, \mathsf{ct})$: a probabilistic algorithm that takes a circuit $C \in \mathcal{C}$ and a ciphertext ct and outputs an evaluated ciphertext $\widehat{\mathsf{ct}}$.
- $\widehat{x} \leftarrow \mathsf{SFE.Dec}(\widehat{\mathsf{ct}}; \mathsf{sk})$: a deterministic algorithm that takes a ciphertext $\widehat{\mathsf{ct}}$ and the secret key sk and outputs a string $\widehat{x}$.

Definition 2.6. *A two-message secure function evaluation protocol* (SFE.Enc, SFE.Eval, SFE.Dec) *for a family of circuits $\mathcal{C} = \{\mathcal{C}_\lambda\}_\lambda$ satisfies:*

- **Perfect Correctness:** *For any $\lambda \in \mathbb{N}$, $x \in \{0,1\}^*$ and circuit $C \in \mathcal{C}_\lambda$*

$$\Pr\left[\mathsf{SFE.Dec}(\widehat{\mathsf{ct}}; \mathsf{sk}) = C(x) \;\middle|\; \begin{array}{l} (\mathsf{sk}, \mathsf{ct}) \leftarrow \mathsf{SFE.Enc}(x; 1^\lambda) \\ \widehat{\mathsf{ct}} \leftarrow \mathsf{SFE.Eval}(C, \mathsf{ct}) \end{array}\right] = 1 \enspace .$$

- **Semantic Security:** *For any polynomial $\ell(\lambda)$ and non-uniform polynomial-size probabilistic $\mathcal{A} = \{\mathcal{A}_\lambda\}_\lambda$, there exists a negligible function ν such that every $\lambda \in \mathbb{N}$, and pair of messages $x_0, x_1 \in \{0,1\}^{\ell(\lambda)}$:*

$$\Pr\left[\mathcal{A}_\lambda(\mathsf{ct}) = b \;\middle|\; \begin{array}{l} b \leftarrow \{0,1\} \\ (\mathsf{sk}, \mathsf{ct}) \leftarrow \mathsf{SFE.Enc}(x_b; 1^\lambda) \end{array}\right] \leq \frac{1}{2} + \mu(\lambda) \enspace .$$

- **Statistical Circuit Privacy:** *There exist unbounded algorithms* $\mathsf{Sim}, \mathsf{Ext}$ *such that:*

$$\left\{\mathsf{SFE.Eval}(C, \mathsf{ct}^*)\right\}_{\substack{\lambda\in\mathbb{N}, C\in\mathcal{C}_\lambda \\ \mathsf{ct}^*\in\{0,1\}^{\mathrm{poly}(\lambda)}}} \approx_s \left\{\mathsf{Sim}(C(\mathsf{Ext}(\mathsf{ct}^*; 1^\lambda)); 1^\lambda)\right\}_{\substack{\lambda\in\mathbb{N}, C\in\mathcal{C}_\lambda \\ \mathsf{ct}^*\in\{0,1\}^{\mathrm{poly}(\lambda)}}} \enspace .$$

Such secure function evaluation schemes are known based on LWE [OPP14, BV11, BD18].

2.5 Shamir Secret Sharing

We define Shamir secret sharing schemes.

Syntax: A Shamir secret sharing scheme is associated with functions $\delta(\lambda), n(\lambda)$, a field $\mathbb{F}_\lambda$ and a probabilistic polynomial-time encoding algorithm $\widehat{S} \leftarrow \mathsf{SSS.Enc}(S; 1^\lambda)$ that takes a secret $S \in \mathbb{F}$ and a parameter 1^λ and outputs an encoding $\widehat{S} \in \mathbb{F}^n$.

Definition 2.7 (Shamir Secret Sharing). *For polynomials $\delta(\cdot), n(\cdot)$ A Shamir secret sharing encoding* $\mathsf{SSS.Enc}$ *satisfies:*

Perfect Hiding: *Any δ coordinates in the encoding are perfectly hiding:*

$$\left\{\mathsf{SSS.Enc}(S_0; 1^\lambda)|_I\right\}_{\substack{\lambda\in\mathbb{N}, \\ S_0, S_1\in\mathbb{F}, \\ I\in\binom{[n]}{\delta}}} \equiv \left\{\mathsf{SSS.Enc}(S_1; 1^\lambda)|_I\right\}_{\substack{\lambda\in\mathbb{N}, \\ S_0, S_1\in\mathbb{F}, \\ I\in\binom{[n]}{\delta}}} \enspace ,$$

where $\binom{[n]}{\delta}$ denotes the collection of subsets $I \subseteq [n]$ of size δ.

Distance: *For any $\lambda \in \mathbb{N}$ and distinct secrets $S_0, S_1 \in \mathbb{F}$,*

$$\varDelta(\mathsf{SSS.Enc}(S_0; 1^\lambda), \mathsf{SSS.Enc}(S_1; 1^\lambda)) \geq 1 - \delta/n \enspace ,$$

where $\varDelta$ denotes the relative hamming distance over $\mathbb{F}^n$.

Shamir secret sharing schemes are known to exist unconditionally [Sha79].

3 Weakly-Binding Commitments with Subset Opening

In this section, we define and construct weakly-binding statistically hiding commitments with subset opening.

3.1 Definition

The definition addresses both the setting of keyed hash functions as well as keyless ones.

Syntax: A commitment with subset opening is associated with a length function $L(\lambda)$ and polynomial-time algorithms $\mathsf{SHC} = (\mathsf{CSO.Gen}, \mathsf{CSO.Com}, \mathsf{CSO.Chal}, \mathsf{CSO.Open}, \mathsf{CSO.Ver})$ with the following syntax:

- $\mathsf{pk} \leftarrow \mathsf{CSO.Gen}(1^\lambda)$: a probabilistic algorithm that takes the security parameter 1^λ and outputs a key $\mathsf{pk} \in \{0,1\}^\lambda$. In the keyless setting, this algorithm is deterministic and outputs a fixed key $\mathsf{pk} \equiv 1^\lambda$.
- $(\mathsf{cmt}, \mathsf{st}) \leftarrow \mathsf{CSO.Com}(X; \mathsf{pk})$: a probabilistic algorithm that takes the key pk and a string $X \in \{0,1\}^{L(\lambda)}$ and outputs a commitment cmt and private state st.
- $C \leftarrow \mathsf{CSO.Chal}(\mathsf{pk})$: a probabilistic algorithm that takes the key pk and outputs a challenge C.
- $d \leftarrow \mathsf{CSO.Open}(I, C, \mathsf{st})$: a deterministic algorithm that takes an index set I, a challenge C and private state st and outputs a decommitment d.
- $b \leftarrow \mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d)$: a deterministic algorithm that takes a commitment cmt, an index set I, an assignment $\alpha : I \to \{0,1\}$, and decommitment d and outputs an acceptance bit b.

Definition 3.1 (Weakly-Binding Statistically-Hiding Commitments with Subset Opening). *For a polynomial $L(\cdot)$, a weakly-binding statistically-hiding commitment with subset opening* $\mathsf{CSO} = (\mathsf{CSO.Gen}, \mathsf{CSO.Com}, \mathsf{CSO.Chal}, \mathsf{CSO.Open}, \mathsf{CSO.Ver})$*, for strings of length L, satisfies:*

Subset Statistical Hiding: *There exists a negligible $\mu(\cdot)$ such that for all $\lambda \in \mathbb{N}$, no unbounded adversary $\mathcal{A}$ wins the following game with probability greater than $1/2 + \mu(\lambda)$:*

1. *$\mathcal{A}$ submits to a challenger $\mathsf{pk} \in \{0,1\}^\lambda$, $X_0, X_1 \in \{0,1\}^{L(\lambda)}$.*
2. *The challenger samples a random $b \leftarrow \{0,1\}$ and $(\mathsf{cmt}_b, \mathsf{st}_b) \leftarrow \mathsf{CSO.Com}(X_b; \mathsf{pk})$, and gives cmt_b to $\mathcal{A}$.*
3. *$\mathcal{A}$ submits a commitment challenge C.*
4. *The challenger computes $d = \mathsf{CSO.Open}(I, C, \mathsf{st})$ where $I = \{i \in [L] : X_0[i] = X_1[i]\}$ is the set of indices on which the strings X_0, X_1 agree.*
5. *$\mathcal{A}$ wins if it correctly guesses the bit b.*

Weak Binding: *For any non-uniform polynomial-size probabilistic $\mathcal{A} = \left\{\mathcal{A}^1_\lambda, \mathcal{A}^2_\lambda\right\}_\lambda$ there exists a polynomial $K(\cdot)$ and a negligible $\mu(\cdot)$, such that for all $\lambda \in \mathbb{N}$,*

$$\Pr_{\substack{\mathsf{pk} \leftarrow \mathsf{CSO.Gen}(1^\lambda) \\ (\mathsf{cmt},\mathsf{st}) \leftarrow \mathcal{A}^1_\lambda(\mathsf{pk})}} \left[\begin{array}{l} \exists \mathbf{X} \textit{ of size } K(\lambda) : \\ \Pr_{\substack{C \leftarrow \mathsf{CSO.Chal}(1^\lambda) \\ (\alpha, I, d) \leftarrow \mathcal{A}^2_\lambda(C; \mathsf{st})}} \left[\begin{array}{l} \mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d) = 1 \\ \alpha \notin \mathbf{X}_I \end{array} \right] \leq \mu(\lambda) \end{array} \right]$$
$$\geq 1 - \mu(\lambda) \ ,$$

where $\mathbf{X}_I$ *denotes the set of assignments* $X|_I : I \to \{0,1\}$ *to indices in* I *induced by every* $X \in \mathbf{X}$.

Succinct Commitment: $|\mathsf{cmt}| = \lambda$ *for any* $\mathsf{pk} \in \{0,1\}^\lambda$ *and any* cmt *in the support of* $\mathsf{CSO.Com}(\cdot;\mathsf{pk})$.

In the remainder of this section we construct weakly-binding statistically hiding commitments with subset opening.

Theorem 3.1. *Assuming a polynomially compressing multi-collision-resistant keyless hash there exists a weakly-binding statistically-hiding commitment with subset opening for strings of length* L *for any polynomial* L.

3.2 Construction

We provide a construction of weakly-binding statistically-hiding commitments with subset opening from (plain) weakly-binding statistically-hiding commitments and multi-collision resistant hash functions.

Ingredients:

- $\mathsf{SSS.Enc}$ a Shamir secret sharing encoding with parameters $\delta(\lambda) = \sqrt{\lambda}$, $n(\lambda) = \lambda$, and field $\mathbb{F} = \{\mathbb{F}_\lambda\}_\lambda$.
- SHC a weakly binding statistically hiding commitment for strings of length $\ell = |\mathbb{F}_\lambda| \cdot \max(L, n)$. We denote the size of commitment in this scheme by $t(\lambda)$.
- H a multi-collision resistant hash for strings of length $\ell' = (L+n)\cdot t$.

The scheme CSO**:**

- $\mathsf{CSO.Gen}(1^\lambda)$: Runs the key generator for the underlying commitment $\mathsf{pk}_1 \leftarrow \mathsf{CSO.Gen}(1^\lambda)$ and hash $\mathsf{pk}_2 \leftarrow \mathsf{H.Gen}(1^\lambda)$, and outputs $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$.
- $\mathsf{CSO.Com}(X;\mathsf{pk})$:
  - For $i \in [L]$, compute an encoding $\widehat{X}_i \leftarrow \mathsf{SSS.Enc}(X_i; 1^\lambda)$.
  - Consider the matrix $\widehat{X} = \left(\widehat{X}_{i,j}\right)_{i\in[L],j\in[n]}$.
  - Compute commitments to the rows $\mathsf{rowcmt}_i \leftarrow \mathsf{SHC.Com}(\widehat{X}_{i,1},\ldots,\widehat{X}_{i,n};\mathsf{pk}_1)$.
  - Compute commitments to the columns $\mathsf{colcmt}_j \leftarrow \mathsf{SHC.Com}(\widehat{X}_{1,j},\ldots,\widehat{X}_{L,j};\mathsf{pk}_1)$.
  - Compute a hash of all of the above commitments $Y \leftarrow \mathsf{H.Hash}((\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j;\mathsf{pk}_2)$ and output $\mathsf{cmt} = Y$ as the commitment.
  - Output as the state st all the commitments $(\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j$, all the randomness $(\hat{\mathsf{r}}_i)_i, (\mathsf{rr}_i)_i, (\mathsf{rc}_j)_j$ used to generate the encodings $\widehat{X}_i$ and commitments $\mathsf{rowcmt}_i, \mathsf{colcmt}_j$, respectively, and the encoding $\widehat{X}_i$ themselves.
- $\mathsf{CSO.Chal}(\mathsf{pk}_1)$: sample δ random column indices $j_1,\ldots,j_\delta \leftarrow [n]$ and output $C = (j_i)_{i\in[\delta]}$.

- $\mathsf{CSO.Open}(I, C, \mathsf{st})$: output as the decommitment information d all the commitments $(\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j$, the randomness $(\hat{\mathsf{r}}_i, \mathsf{rr}_i)_{i \in I}$ used to compute the encodings and commitments corresponding to all rows $i \in I$, the randomness $(\mathsf{rc}_j)_{j \in C}$ and the columns $\left(\widehat{X}_{1,j}, \dots, \widehat{X}_{L,j}\right)_{j \in C}$ themselves, corresponding to all challenge columns $j \in C$.
- $\mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d)$:
  - Parse d as $(\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j$, $(\mathsf{rr}_i, \hat{\mathsf{r}}_i)_{i \in I}$, $(\mathsf{rc}_j, \widehat{X}_{1,j}, \dots, \widehat{X}_{L,j})_{j \in C}$.
  - Verify that $\mathsf{cmt} = \mathsf{H.Hash}(((\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j); \mathsf{pk}_2)$.
  - For every $i \in I$, compute $\hat{\alpha}_i := \mathsf{SSS.Enc}(\alpha(i); \hat{\mathsf{r}}_i)$ and verify that $\mathsf{rowcmt}_i = \mathsf{SHC.Com}(\hat{\alpha}_i; \mathsf{pk}_1, \mathsf{rr}_i)$.
  - For every $j \in C$, verify that $\mathsf{colcmt}_j = \mathsf{SHC.Com}(\widehat{X}_{1,j}, \dots, \widehat{X}_{L,j}; \mathsf{pk}_1, \mathsf{rc}_j)$ and that for every $i \in I$, $\alpha_{i,j} = \widehat{X}_{i,j}$.

3.3 Analysis

We now analyze the construction. We first prove subset statistical hiding and then prove weak binding.

Proposition 3.1. *The construction is subset statistically hiding.*

Proof. We first claim that statistical hiding holds for any fixed challenge set C.

Claim 3.2. *Fix any* pk *and* $C \in [n]^\delta$*, and set of indices* $I \subseteq [n]$*. There exists a simulator* S *such that for any* $X \in \{0,1\}^L$*,*

$$\mathsf{cmt}, d \approx_{2^{-\Omega(\lambda)}} S(X|_I) \;\;,$$

where $(\mathsf{cmt}, \mathsf{st}) \leftarrow \mathsf{CSO.Com}(X; \mathsf{pk})$ *and* $d \leftarrow \mathsf{CSO.Open}(I, C, \mathsf{st})$.

Proof. We describe how the simulator samples the commitments $\mathsf{rowcmt}_i, \mathsf{colcmt}_j$:

- For every $i \in I$, compute an encoding $\widehat{X}_i$ of X_i, and sample a commitment rowcmt_i to this encoding.
- For every $i \notin I$, sample a commitment rowcmt_i to the all-zero string. Also sample an encoding $\widehat{Y}_i$ of for an arbitrary bit Y, and store $\widehat{Y}_i$.
- For every $j \in C$, sample a commitment colcmt_j to the j-th column of the matrix whose rows are given by the encodings $\widehat{X}_i$ for $i \in I$ and by the encodings $\widehat{Y}_i$ for $i \notin I$.
- For every $j \notin C$ sample a commitment colcmt_j to the all-zero string.

We now argue that the commitments $\mathsf{rowcmt}_i, \mathsf{colcmt}_j$ produced above along with an opening with respect to I, C are $2^{-\Omega(\lambda)}$-close to their distribution in a commitment to X.

Consider a hybrid distribution cmt^*, d^* where we change the distribution of commitments to X as follows. For all unopened rows $i \notin I$, we change the commitment rowcmt_i from a commitment to $\widehat{X}_i$ to a commitment to an all-zero string, and for all unopened columns $j \notin C$, we change the commitment colcmt_j from a commitment to the j-column of the matrix $(\widehat{X}_{i,j})_{i,j}$ to a commitment to the all zero string.

Then by the statistical hiding of the underlying commitment SHC,

$$\mathsf{cmt}, d \quad \approx_{2^{-\lambda}\cdot(L+n)} \quad \mathsf{cmt}^*, d^* \ ,$$

where $2^{-\lambda}(L+n) \leq 2^{-\Omega(\lambda)}$.

Next, note that the only difference between the hybrid distribution cmt^*, d^* and the simulated distribution $S(X|_I)$ is in the commitments to the columns $j \in C$. In the first, the plaintexts are the columns of the matrix $\left(\widehat{X}_{ij}\right)_{i\in[L],j\in C}$, whereas in the second its the concatenation of $\left(\widehat{X}_{ij}\right)_{i\in I,j\in C}$ and $\left(\widehat{Y}_{ij}\right)_{i\in[L]\setminus I,j\in C}$. However, since $|C| \leq \delta$, the perfect hiding of the Shamir secret sharing implies that these two matrices are identically distributed.

Now fix any key pk and any two $X, X' \in \{0,1\}^L$, and let $I \subseteq [L]$ be the set of indices on they agree. Then by Claim 3.2, for any fixed challenge C, the distributions cmt, d and cmt', d' corresponding to X and X', respectively, are $2^{-\Omega(\lambda)}$-close.

To complete the proof, we now show that they remain close also when C is chosen adaptively.

Claim 3.3. *For any (unbounded) adversary $\mathcal{A}$,*

$$\mathsf{cmt}, C, d \quad \approx_{2^{\Omega(\lambda)}} \mathsf{cmt}', C', d' \ ,$$

where $(\mathsf{cmt}, \mathsf{st}) \leftarrow \mathsf{CSO.Com}(X; \mathsf{pk})$*,* $C \leftarrow \mathcal{A}(\mathsf{cmt})$ *and* $d \leftarrow \mathsf{CSO.Open}(I, C, \mathsf{st})$*, and* cmt', C', d' *is sampled similarly with respect to* X'*.*

Proof.

$$\begin{aligned}\mathbf{SD}((\mathsf{cmt}, C, d),(\mathsf{cmt}', C', d')) = \\ &\sum_{\alpha,\beta,\gamma} |\Pr[(\mathsf{cmt}, C, d) = (\alpha,\beta,\gamma)] - \Pr[(\mathsf{cmt}', C', d') = (\alpha,\beta,\gamma)]| \leq \\ &\sum_{\beta\in[n]^\delta} 2^{-\Omega(\lambda)} = \lambda^{\sqrt{\lambda}} \cdot 2^{-\Omega(\lambda)} \leq 2^{-\Omega(\lambda)} \ ,\end{aligned}$$

where the first inequality follows from Claim 3.2.

This completes the proof of Proposition 3.1

Proposition 3.2. *The construction is weakly binding.*

Proof. Fix a polynomial-size adversary $\mathcal{A} = \left\{\mathcal{A}^1_\lambda, \mathcal{A}^2_\lambda\right\}_\lambda$ against the commitment. The proof is divided to two main claims. We first prove a (computational) claim attesting that with overwhelming probability $\mathcal{A}$'s commitment fixes a polynomial-size set of strings $\mathbf{S}$, such that any valid opening of the underlying weakly-binding commitment is to a string from $\mathbf{S}$. This claim relies on the weak binding of the underlying commitment and the multi-collision resistance of the hash function. Then we prove an information-theoretic claim that shows that provided the restriction to the set $\mathbf{S}$ there also exists a polynomial-size global set of strings $\mathbf{X}$, such that any opening of some subset must be consistent with one of the strings in $\mathbf{X}$.

The following claim asserts that a commitment from the adversary $\mathcal{A}$, fixes a polynomial-size set of strings $\mathbf{S} \subseteq \{0,1\}^\ell$, such that the adversary can only open any commitments $\mathsf{rowcmt}_i, \mathsf{colcmt}_j$ to a string from $\mathbf{S}$.

Claim 3.4. *There exist a polynomial $K(\cdot)$ and a negligible function $\mu(\cdot)$ such that for all $\lambda \in \mathbb{N}$, except with probability $\mu(\lambda)$ over $\mathsf{pk} \leftarrow \mathsf{CSO.Gen}(1^\lambda)$ and $(\mathsf{cmt}, \mathsf{st}) \leftarrow \mathcal{A}^1_\lambda(\mathsf{pk})$ there exists a set $\mathbf{S} \subseteq \{0,1\}^\ell$ of size $K(\lambda)$ such that*

$$\Pr_{\substack{C \leftarrow \mathsf{CSO.Chal}(1^\lambda) \\ (\alpha, I, d) \leftarrow \mathcal{A}^2_\lambda(C; \mathsf{st})}} \left[\mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d) = 1 \wedge \widehat{X}(\alpha, I, d) \not\subseteq \mathbf{S} \right] \leq \mu(\lambda) \ ,$$

where $\widehat{X}(\alpha, I, d) \subseteq \{0,1\}^\ell$ is the set of rows and columns of the matrix $(\widehat{X})_{ij}$, which $\mathcal{A}$ opens in its decommitment.

Proof. Assume toward contradiction that for any polynomial K, there exists a noticeable function ε, such that for infinitely many $\lambda \in \mathbb{N}$, with probability $\varepsilon(\lambda)$ over $\mathsf{pk} \leftarrow \mathsf{CSO.Gen}(1^\lambda)$ and $(\mathsf{cmt}, \mathsf{st}) \leftarrow \mathcal{A}^1_\lambda(\mathsf{pk})$ for any set $\mathbf{S} \subseteq \{0,1\}^\ell$ of size $K(\lambda)$

$$\Pr_{\substack{C \leftarrow \mathsf{CSO.Chal}(1^\lambda) \\ (\alpha, I, d) \leftarrow \mathcal{A}^2_\lambda(C; \mathsf{st})}} \left[\mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d) = 1 \wedge \widehat{X}(\alpha, I, d) \not\subseteq \mathbf{S} \right] \geq \varepsilon(\lambda) \ .$$

We consider two complementary cases:

1. For infinitely many λ, except with probability $\varepsilon/2$ over $\mathsf{pk}, \mathsf{cmt}, \mathsf{st}$ there exists a set $\mathbf{S}' \subseteq \{0,1\}^{\ell'}$ of size $\sqrt{K}$ such that except with probability $\varepsilon/2$, $\mathcal{A}$ never opens the hash value cmt to $S = \left((\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j\right) \notin \mathbf{S}'$.
2. For infinitely many λ, with probability at least $\varepsilon/2$ over $\mathsf{pk}, \mathsf{cmt}, \mathsf{st}$ for any set $\mathbf{S}' \subseteq \{0,1\}^{\ell'}$ of size $\sqrt{K}$, with probability $\varepsilon/2$, $\mathcal{A}$ opens the hash value cmt to $S = \left((\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j\right) \notin \mathbf{S}'$.

First, note that the second case implies that $\mathcal{A}$ breaks the multi-collision resistance of the underlying hash H. Thus, we can assume that the first case holds. It follows that

Claim 3.5. *For infinitely many λ, with probability at least $\varepsilon/2$ over $\mathsf{pk}, \mathsf{cmt}, \mathsf{st}$, there exists a set $\mathbf{S}' \subseteq \{0,1\}^{\ell'}$ of size $\sqrt{K}$ as required by the first condition, but for any set $\mathbf{S}$ of size K and with probability $\varepsilon/2$ over the decommitment phase $\widehat{X}(\alpha, I, d) \not\subseteq \mathbf{S}$ whereas the opened $S = \left((\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j\right) \in \mathbf{S}'$.*

Proof. This follows directly from our assumption toward contradiction and the fact that the first case above holds.

From hereon fix $\mathsf{pk}, \mathsf{cmt}, \mathsf{st}$ such that Claim 3.5 holds. We next argue that

Claim 3.6. *There exists* $S' = \left((\mathsf{rowcmt}_i)_i, (\mathsf{colcmt}_j)_j\right) \in \mathbf{S}'$ *and* $\mathsf{cmt}' \in S'$ *such that for any set* $\mathbf{X} \subseteq \{0,1\}^\ell$ *of size* $\sqrt{K}/(L+n)$*, with probability* $\varepsilon/2(L+n)\sqrt{K}$ *over the decommitment phase* cmt *is opened to* S'*, but* cmt' *is opened to* $X \notin \mathbf{X}$*.*

Proof. Otherwise, for each $S' \in \mathbf{S}'$ and $\mathsf{cmt}' \in S'$, we can choose $\mathbf{X}(S', \mathsf{cmt}')$ such that the above does not hold, and obtain

$$\mathbf{S} = \bigcup_{S' \in \mathbf{S}, \mathsf{cmt}' \in S'} \mathbf{X}(S', \mathsf{cmt}')$$

of size K, which violates Claim 3.5.

We now obtain an adversary $\mathcal{B} = \left\{\mathcal{B}^1_\lambda, \mathcal{B}^2_\lambda\right\}_\lambda$ that breaks the weak binding of the commitment SHC. $\mathcal{B}^1_\lambda(\mathsf{pk}_1)$ first samples $\mathsf{pk}_2 \leftarrow \mathsf{H.Gen}(1^\lambda)$, sets $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$, runs $\mathcal{A}^1_\lambda(\mathsf{pk})$ and obtains a state st, it then simulates a random challenge $C \leftarrow C(1^\lambda)$ and runs $\mathcal{A}^2_\lambda(C; \mathsf{st}$. It then takes the set of commitments $S' = (\mathsf{rowcmt}_i)_{i \in L}, (\mathsf{colcmt}_j)_{j \in [n]}$ and outputs a random commitment $\mathsf{cmt}' \in S'$ along with the state st. $\mathcal{B}^2_\lambda(\mathsf{st})$ samples a new random challenge C' and runs $\mathcal{A}^2_\lambda(C'; \mathsf{st})$, and outputs whatever opening $\mathcal{A}^2_\lambda$ outputs for cmt', or $\perp$ if there is no such opening.

Claim 3.7. *$\mathcal{B}$ breaks weak binding.*

Proof. By construction and Claims 3.5,3.6, with probability at least $\frac{\varepsilon}{2} \cdot \frac{\varepsilon}{2(L+n)\sqrt{K}}$ over the commitment phase of $\mathcal{B}^1_\lambda$, for any set $\mathbf{X} \subseteq \{0,1\}^\ell$ of size $\sqrt{K}/(L+n)$, $\mathcal{B}^2_\lambda$ opens that commitment to a value $X \notin \mathbf{X}$ with probability at least $\varepsilon/2(L+n)\sqrt{K}$.

This complete the proof of Claim 3.4.

We now proceed to prove the binding property of the scheme. The following claim asserts that whenever all strings $\widehat{X}$ are consistent with some set $\mathbf{S}$, there exists a polynomial-size set of strings $\mathbf{X} \subseteq \{0,1\}^L$ such that all openings are consistent with $\mathbf{X}$, which will conclude the proof.

Claim 3.8. *Let K be the polynomial given by Claim 3.4 and let τ be a constant such that $\tau > 2\log_\lambda(2K^2)$. Fix λ, pk, cmt, st such that Claim 3.4 holds with respect to a set $\mathbf{S}$. Then there exists $\mathbf{X} \subseteq \{0,1\}^L$ of size $K' = (nK)^\tau$ such that*

$$\Pr_{\substack{C \leftarrow \mathsf{CSO.Chal}(1^\lambda) \\ (\alpha, I, d) \leftarrow \mathcal{A}^2_\lambda(C; \mathsf{st})}} \left[\mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d) = 1 \wedge \alpha \notin \mathbf{X}|_I\right] \leq \mu(\lambda) \ .$$

Proof. We first argue that random τ locations fix at most a single encoding in $\mathbf{S}$.

Claim 3.9. *Let $T \subseteq [n]$ be a set of τ indices chosen independently at random, then*

$$\Pr_T\left[\exists \widehat{S}_0, \widehat{S}_1 \in \mathbf{S} \textit{ such that } \widehat{S}_0|_T = \widehat{S}_1|_T \;\middle|\; \begin{array}{c} \widehat{S}_b \in \mathsf{SSS.Enc}(S_b) \\ S_0 \neq S_1 \end{array}\right] \leq 1/2 \enspace .$$

We call any set T as above fixing.

Proof. The proof follows directly from the distance of Shamir encodings, the bound K on the size of $\mathbf{S}$, and the definition of τ. Specifically the above can be bounded by

$$|\mathbf{S}|^2 \left(\frac{\delta}{n}\right)^\tau \leq K^2 \left(\frac{\sqrt{\lambda}}{\lambda}\right)^{2\log_\lambda(2K^2)} = \frac{1}{2} \enspace .$$

Now, let T be any fixing set and consider any set of τ columns

$$Q = \{(Q_{1,j}, \dots, Q_{L,j}) : j \in [T]\} \enspace .$$

Then, T, Q fix a unique string $X(T,Q) \in \{0,1,\perp\}^L$ defined as follows:

- If T is not fixing, set $X(T,Q) = \perp$. Otherwise, proceed to the following.
- For any $i \in [L]$, if for some $b \in \{0,1\}$, there exists a Shamir ecnoding $\widehat{X}_i \in \mathsf{SSS.Enc}(b; 1^\lambda)$ such that $\widehat{X}_i \in \mathbf{S}$ and $\widehat{X}_{i,j} = Q_{i,j}$ for all $j \in T$, set $X_i(T,Q) = b$. Otherwise, set $X_i(T,Q) = \perp$.
  (Since T is fixing, there exists at most a single $b \in \{0,1\}$ that satisfies the condition.)

We now define the set $\mathbf{X}$ as follows:

$$\mathbf{X} := \{X(T,Q) \mid T \in [n]^\tau, Q \in \mathbf{S}^\tau\} \enspace .$$

First, note that $\mathbf{X}$ is of size at most $(n \cdot |\mathbf{S}|)^\tau = (nK)^\tau$, which is polynomial in λ. We now argue that

$$\Pr_{\substack{C \leftarrow \mathsf{CSO.Chal}(1^\lambda) \\ (\alpha, I, d) \leftarrow \mathcal{A}^2_\lambda(C;\mathsf{st})}}[\mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d) = 1 \wedge \alpha \notin \mathbf{X}|_I] \leq \mu(\lambda) \enspace .$$

Recall that $C \subseteq [n]$ consists of λ indices chosen independently at random. In particular, by Claim 3.9, C contains a fixing set T except with probability $(1/2)^{\delta/\tau} = 2^{-\widetilde{\Omega}(\sqrt{\lambda})}$. Recall that except with negligible probability all row and column commitments opened by $\mathcal{A}$ are consistent with some string in $\mathbf{S}$. From hereon we assume that the latter occurs and that C contains a fixing T.

Then when $\mathsf{CSO.Ver}(\mathsf{cmt}, \alpha, I, C, d) = 1$, $\mathcal{A}$ opens the columns in T to some $Q = (Q_{1,j}, \dots, Q_{L,j})_{j \in [T]} \in \mathbf{S}^\tau$. Also the assignment $\alpha : I \to \{0,1\}$ is such that for every $i \in I$, there exists an encoding $\hat{\alpha}_i \in \mathsf{SSS.Enc}(\alpha_i; 1^\lambda) \in \mathbf{S}$ and $\hat{\alpha}$ is consistent with Q. By definition, it follows that for every $i \in I$, $\alpha_i = X_i(T,Q)$; namely, $\alpha \in \mathbf{X}|_I$ as required.

This completes the proof of Claim 3.8.

This completes the proof of Proposition 3.2

4 Offline-Online Statistically WI Arguments of Knowledge

In this section, we define and construct offline-online statistically witness indistinguishable arguments of knowledge.

4.1 Definition

In offline-online statistically WI arguments of knowledge, the protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ can be divided to:

- an offline protocol $\langle \mathsf{OffP} \leftrightarrows \mathsf{OffV} \rangle(1^\lambda, 1^\ell)$, where the parties take as common input the security parameter 1^λ and an input size 1^ℓ and output each a state $\mathsf{st}_\mathsf{P}, \mathsf{st}_\mathsf{V}$.
- an online protocol $\langle \mathsf{OnP}(\mathsf{st}_\mathsf{P}, w) \leftrightarrows \mathsf{OnV}(\mathsf{st}_\mathsf{V}) \rangle(x)$, where the parties, in addition to their previous state, take as common input an instance $x \in \mathcal{L} \cap \{0,1\}^\ell$ and the prover obtains also obtain as input a witness $w \in \mathcal{R}_\mathcal{L}(x)$.

We now formally define the properties that such systems are required to satisfy.

Definition 4.1 (Offline-Online SWIAOK). $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ *is an offline-online statistically witness indistinguishable argument of knowledge for* $\mathcal{L}$ *if it satisfies:*

Completeness: *For any* $\ell, \lambda \in \mathbb{N}$*,* $x \in \mathcal{L} \cap \{0,1\}^\ell$*, and* $w \in \mathcal{R}_\mathcal{L}(x)$*:*

$$\Pr\left[\begin{array}{l} \langle \mathsf{OffP} \leftrightarrows \mathsf{OffV} \rangle(1^\lambda, 1^\ell) = (\mathsf{st}_\mathsf{P}, \mathsf{st}_\mathsf{V}) \\ \langle \mathsf{OnP}(\mathsf{st}_\mathsf{P}, w) \leftrightarrows \mathsf{OnV}(\mathsf{st}_\mathsf{V}) \rangle(x) = 1 \end{array}\right] = 1 \ .$$

Adaptive statistical witness indistinguishability: *For any polynomial* $\ell(\cdot)$ *and unbounded verifier* V^**, there exists a negligible function* $\mu(\cdot)$ *such that for all* $\lambda \in \mathbb{N}$*:*

$$\begin{array}{l} \Pr\big[\langle \mathsf{OnP}(\mathsf{st}_\mathsf{P}, w_b) \leftrightarrows \mathsf{OnV}^*(\mathsf{st}_\mathsf{V}) \rangle(x) = b \mid \\ \qquad \left.\begin{array}{l} \langle \mathsf{OffP} \leftrightarrows \mathsf{OffV}^* \rangle(1^\lambda, 1^{\ell(\lambda)}) = (\mathsf{st}_\mathsf{P}, (\mathsf{st}_\mathsf{V}, x, w_0, w_1)) \\ b \leftarrow \{0,1\} \end{array}\right] \le \dfrac{1}{2} + \mu(\lambda) \ , \end{array}$$

where $x \in \mathcal{L} \cap \{0,1\}^{\ell(\lambda)}$ *and* $w_0, w_1 \in \mathcal{R}_\mathcal{L}(x)$*.*

Adaptive proof of knowledge: *there is a uniform PPT extractor* $\mathcal{E}$ *such that for any polynomial* $\ell(\cdot)$ *and any non-uniform polynomial-size prover* $\mathsf{P}^* = \{\mathsf{P}^*_\lambda\}_{\lambda \in \mathbb{N}}$ *there is a polynomial* $K(\cdot)$ *and a negligible* $\mu(\cdot)$ *such that for all* $\lambda \in \mathbb{N}$*:*

$$
\begin{array}{ll}
\textit{if} & \Pr\left[\langle \mathsf{OnP}^*_\lambda(\mathsf{st_P}) \leftrightarrows \mathsf{OnV}(\mathsf{st_V})\rangle(x) = 1 \mid \right. \\
& \qquad \left. \langle \mathsf{OffP}^* \leftrightarrows \mathsf{OffV}\rangle(1^\lambda, 1^{\ell(\lambda)}) = ((\mathsf{st_P}, x), \mathsf{st_V})\right] = \varepsilon \enspace , \\
\textit{then} & \Pr\left[\begin{array}{l} \langle \mathsf{OnP}^*_\lambda(\mathsf{st_P}) \leftrightarrows \mathsf{OnV}(\mathsf{st_V})\rangle(x) = 1 \\ w \leftarrow \mathcal{E}^{\mathsf{P}^*_\lambda}(x, \mathsf{st_P}, \mathsf{st_V}) \\ w \in \mathcal{R}_{\mathcal{L}}(x) \end{array} \right| \\
& \qquad \left. \langle \mathsf{OffP}^* \leftrightarrows \mathsf{OffV}\rangle(1^\lambda, 1^{\ell(\lambda)}) = ((\mathsf{st_P}, x), \mathsf{st_V})\right] \\
& \qquad \geq \mathrm{poly}\left(\frac{\varepsilon}{K(\lambda)}\right) - \mu(\lambda) \enspace ,
\end{array}
$$

where $x \in \{0,1\}^{\ell(\lambda)}$.

Offline succinctness: *All messages sent by* OffP *in the offline stage are of length* λ *(independently of* ℓ*).*

In the remainder of this section we construct offline-online statistically witness indistinguishable arguments of knowledge.

Theorem 4.1. *Assuming a polynomially-compressing multi-collision-resistant keyless hash there exists an offline-online statistically witness indistinguishable argument of knowledge for* ***NP*** *with two messages in the offline part and one message in the online part.*

4.2 A Protocol for Hamiltonicity

We now give an offline-online protocol for the NP complete problem of Hamiltonicity. The protocol is essentially the Lapidot-Shamir protocol [LS90a] whereas instead of using standard (binding) commitments, we rely on the notion of weakly-binding commitments with subset opening from the previous section.

Ingredients and notation:

- Let $n(\cdot)$ be a polynomial and let $(\mathsf{CSO.Gen}, \mathsf{CSO.Com}, \mathsf{CSO.Chal}, \mathsf{CSO.Open})$ be a weakly binding statistically hiding commitment with subset opening for strings of length $n^2 \cdot \lambda$.
- A graph G with n nodes will be represented by its $n \times n$ adjacency matrix. Sometimes we may think of G as a string in the natural way.
- Let G, H be two graphs on the same set of nodes $[n]$ and let $\varphi : [n] \to [n]$ be a permutation. We write $H \subseteq G$ to denote the fact that H's set of edges is contained in G's set of edges. We write $\varphi(G) = H$ to denote the fact that $H_{\varphi(i),\varphi(j)} = G_{i,j}$ for every $i, j \in [n]$.
- A Hamiltonian cycle graph H is a graph that consists of a Hamiltonian cycle (and no additional edges).

Protocol 1

Offline:

Common Input: $(1^\lambda, 1^n)$.

1. OffV samples a key $\mathsf{pk} \leftarrow \mathsf{CSO.Gen}(1^\lambda)$ for a weakly-binding commitment with length parameter $L = n^2 \cdot \lambda$, and sends pk. (In a keyless scheme, $\mathsf{pk} \equiv 1^\lambda$, and this message is skipped).
2. OffP computes
   - λ random Hamiltonian cycle graphs $\mathbf{H} = (H_1, \dots, H_\lambda) \in \{0,1\}^{n^2 \times \lambda}$.
   - a commitment with subset opening $(\mathsf{cmt}, \mathsf{st}) \leftarrow \mathsf{CSO.Com}(\mathbf{H}; \mathsf{pk})$.

   It sends cmt.
3. OffV computes
   - a commitment challenge $C \leftarrow \mathsf{CSO.Chal}(\mathsf{pk})$,
   - λ random challenges $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_\lambda) \leftarrow \{\text{cycle}, \text{antiedges}\}^\lambda$.

   It sends $(C, \boldsymbol{\sigma})$.
4. OffP and OffV output $\mathsf{st}_\mathsf{P} = (\mathsf{pk}, \mathbf{H}, \mathsf{st}, C, \boldsymbol{\sigma})$ and $\mathsf{st}_\mathsf{V} = (\mathsf{pk}, \mathsf{cmt}, C, \boldsymbol{\sigma})$.

Online:

Common Input: A graph $G \in \{0,1\}^{n \times n}$.
Prover Input: A Hamiltonian cycle graph $H \subseteq G$ and the state st_P.
Verifier Input: state st_V.

5. OnP computes
   - for every $j \in [\lambda]$,
     - If $\sigma_j = \text{cycle}$, let $I_j = (j-1)n^2 + [n^2]$ be the set of all indices corresponding to H_j.
     - If $\sigma_j = \text{antiedges}$, sample a random permutation φ_j such that $\varphi(H) = H_j$. Let $I_j \subset (j-1)n^2 + [n^2]$ be the set of indices corresponding to anti-edges in $\varphi_j(G)$.
   - $\mathbf{I} = \bigcup_{j \in [\lambda]} I_j$, $\boldsymbol{\varphi} = (\varphi_j)_j$.
   - $d \leftarrow \mathsf{CSO.Open}(\mathbf{I}, C, \mathsf{st})$.

   and sends $(\mathbf{I}, \mathbf{H}|_\mathbf{I}, \boldsymbol{\varphi}, d)$.
6. OnV verifies that:
   - $\mathsf{CSO.Ver}(\mathsf{cmt}, \mathbf{H}|_\mathbf{I}, \mathbf{I}, C, d) = 1$,
   - the sets $I_j \in \mathbf{I}$ are defined consistently with σ_j and φ_j.
   - $\mathbf{H}_{I_j}$ represents a Hamiltonian cycle graph, if $\sigma_j = \text{cycle}$,
   - $\mathbf{H}_{I_j} \equiv 0$ if $\sigma_j = \text{antiedges}$.

Fig. 1: A 3-message SWI argument of knowledge for Hamiltonicity.

4.3 Analysis

The offline succinctness property follows directly from the succinct commitment property of the underlying commitment with subset opening. We focus on proving the argument of knowledge and the statistical witness indistinguishability properties.

Proposition 4.1. *Protocol 1 is an adaptive argument of knowledge.*

Proof. Fix a non-uniform polynomial-size prover $\mathsf{P}^* = \{\mathsf{P}^*_\lambda\}_{\lambda\in\mathbb{N}}$ such that

$$\Pr\left[\langle \mathsf{OnP}^*_\lambda(\mathsf{st}_\mathsf{P}) \leftrightarrows \mathsf{OnV}(\mathsf{st}_\mathsf{V})\rangle(x) = 1 \;\middle|\; \langle \mathsf{OffP}^* \leftrightarrows \mathsf{OffV}\rangle(1^\lambda, 1^\ell) = ((\mathsf{st}_\mathsf{P}, x), \mathsf{st}_\mathsf{V})\right] = \varepsilon \ .$$

We now describe how the witness extractor $\mathcal{E}(\mathsf{P}^*_\lambda, x, \mathsf{st}_\mathsf{P}, \mathsf{st}_\mathsf{V})$ operates. $\mathcal{E}$ first emulates the last prover message corresponding to the state of the offline phase it is given. It obtains $(\mathbf{I}, \mathbf{H}|_\mathbf{I}, \boldsymbol{\varphi})$. $\mathcal{E}$ then rewinds the prover P^*_λ back to the offline phase, and sends it a fresh random challenge $\boldsymbol{\sigma}', C'$. It then obtains in the online phase corresponding $(\mathbf{I}', \mathbf{H}'|_{\mathbf{I}'}, \boldsymbol{\varphi}')$. $\mathcal{E}$ now looks for an $i \in [\lambda]$ such that $\sigma_i = \text{antiedges}$ and $\sigma'_i = \text{cycle}$, and returns the cycle $\varphi_i^{-1}(H'_i)$. If any of the above fail, it aborts.

Claim 4.2. *There exists a polynomial $K(\cdot)$ and a negligible $\mu(\cdot)$ such that*

$$\Pr\left[\begin{array}{l} \langle \mathsf{OnP}^*_\lambda(\mathsf{st}_\mathsf{P}) \leftrightarrows \mathsf{OnV}(\mathsf{st}_\mathsf{V})\rangle(x) = 1 \\ w \leftarrow \mathcal{E}(\mathsf{P}^*_\lambda, x, \mathsf{st}_\mathsf{P}, \mathsf{st}_\mathsf{V}) \\ w \in \mathcal{R}_\mathcal{L}(x) \end{array} \;\middle|\; \langle \mathsf{OffP}^* \leftrightarrows \mathsf{OffV}\rangle(1^\lambda, 1^{\ell(\lambda)}) = ((\mathsf{st}_\mathsf{P}, x), \mathsf{st}_\mathsf{V})\right] \geq \frac{\varepsilon^3}{8K^2(\lambda)} - \mu(\lambda) \ .$$

Proof. First, by an averaging argument with probability at least $\varepsilon/2$ over the choice of the first two messages in the protocol, namely the key pk and commitment cmt, it holds that with probability at least $\varepsilon/2$ over the rest of the protocol the prover convinces the verifier of accepting. In addition, by the weak binding property of the underlying commitment with subset opening, there exists a polynomial K, such that except with negligible probability $\nu(\lambda)$ over the first two messages, there exists a set $\mathbf{X}$ of size at most K, consisting of strings $\mathbf{H} \in \{0,1\}^{n^2\times\lambda}$, such that except with negligible probability $\nu(\lambda)$, any valid opening of the commitment by the prover is consistent with some $\mathbf{H} \in \mathbf{X}$. Also, note that for two random challenges $\boldsymbol{\sigma}, \boldsymbol{\sigma}'$ there exists some i such that $\sigma_i = \text{antiedges}$ and $\sigma'_i = \text{cycle}$ except with probability $(3/4)^\lambda$.

It follows that with probability at least $\varepsilon/2 - \nu$ over the choice of the first two messages, there exists a single string $\mathbf{H}^* \in \mathbf{X}$, such that with probability at least $(\varepsilon/2K)^2 - (3/4)^\lambda$, in both executions performed by $\mathcal{E}$:

1. The prover convinces the verifier.
2. Both openings $\mathbf{H}|_\mathbf{I}$ and $\mathbf{H}'|_{\mathbf{I}'}$ obtained by $\mathcal{E}$ are consistent with $\mathbf{H}$.
3. For some i, $\sigma_i = \text{antiedges}$ and $\sigma'_i = \text{cycle}$.

Since the verifier accepts in the second execution, H_i is a Hamiltonian cycle graph. Since the verifier accepts in the first execution, and H_i is a Hamiltonian cycle, $\varphi_i^{-1}(H_i)$ is a Hamiltonian cycle in G, since all anti-edges in G are mapped to anti-edges in H_i.

Overall, the extractor succeeds with probability at least $\varepsilon^3/8K^2 - \lambda^{-\omega(1)}$.

Proposition 4.2. *Protocol 1 satisfies adaptive statistical witness indistinguishability.*

The proof of witness indistinguishability is similar to that of the original Lapidot-Shamir protocol [LS90b]. The main difference is that there it is convenient to first prove WI for a single instance (with a single challenge σ) and then rely on a generic hybrid argument, whereas in our protocol the commitment with subset opening correlates the λ instances. The proof accordingly proceeds via a slightly less generic hybrid argument. The proof the the proposition can be found in the full version of this work.

5 A Three Message Statistical Zero Knowledge Argument

In this section, we construct a three message statistical zero knowledge argument.

Theorem 5.1. *Assuming a linearly compressing* quasipoly(λ)*-secure multi-collision-resistant keyless hash, a* quasipoly(λ)*-secure fully-homomorphic encryption, and a two-message secure function evaluation protocol with statistical function hiding, there exists a statistical zero knowledge argument for* ***NP*** *with three messages.*

Ingredients and notation:

- A two-message weak memory delegation scheme ($\mathsf{MD.Mem}$, $\mathsf{MD.Query}$, $\mathsf{MD.Prove}$, $\mathsf{MD.Ver}$) with weak soundness for time-T for $T = \text{quasipoly}(\lambda)$, as in Definition 2.5.
- A two-message secure function evaluation protocol ($\mathsf{SFE.Enc}, \mathsf{SFE.Eval}, \mathsf{SFE.Dec}$) with statistical function hiding as in Definition 2.6.
- An offline-online statistically witness indistinguishable argument of knowledge $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ where the offline part of the protocol $\langle \mathsf{OffP} \leftrightarrows \mathsf{OffV} \rangle$ consists of two messages and the online part of the protocol $\langle \mathsf{OnP} \leftrightarrows \mathsf{OnV} \rangle$ consists of one message. Such a protocol is defined and constructed in Section 4.
- A weakly-binding statistically-hiding keyless commitment $\mathsf{SHC.Com}$ as in Definition 2.2.
- For a string x, denote by $\mathcal{M}_x$ a Turing machine that given memory $D = \mathsf{V}^*$, emulates the Turing machine encoded by V^* on the input x, parses the result as $(u, \mathsf{wi}_2, \mathsf{q}, \widehat{\mathsf{ct}}_\tau)$, and outputs u.
- Denote by $\mathcal{V}_{\mathsf{param}}$ a circuit that has the string param hardcoded and operates as follows. Given as input a secret state vst for the delegation scheme:

- parse $\mathsf{param} = (x, \mathsf{q}, u, \mathsf{dig}, t, \pi)$,
- return 1 ("accept") if either of the following occurs:
  - $*$ the delegation verifier accepts: $\mathsf{MD.Ver}(1^\lambda, \mathsf{dig}, (\mathcal{M}_x, t, u), \mathsf{vst}, \pi) = 1$,
  - $*$ the query and secret state are inconsistent: $(\mathsf{q}, \mathsf{vst}) \notin \mathsf{MD.Query}(1^\lambda)$. (We can assume without loss of generality that the state vst contains the random coins of $\mathsf{MD.Query}$ and, therefore, consistency can be tested efficiently.)

In words, $\mathcal{V}_{\mathsf{param}}$, given the secret state vst, first verifies the proof π that "$\mathcal{M}_x(D) = (u, \cdots)$" where D is the database corresponding to the digest dig. In addition, it verifies that q is truly consistent with the coins vst.

– Denote by $\mathbf{1}$ a circuit of the same size as $\mathcal{V}_{\mathsf{param}}$ that always returns 1.

We describe our three-message zero-knowledge protocol in Figure 2.

Proposition 5.1. *Protocol 2 is a statistical zero-knowledge argument.*

Proof (Sketch). As explained in the introduction, the protocol is based on the zero-knowledge protocols in [BBK$^+$16, BKP18]. In particular, Bitansky et al. [BBK$^+$16] show a three-message computational zero knowledge protocol in the *global hash model*, where parties have access to a collision-resistant hash function sampled during a setup phase. The main differences between our protocol and theirs is:

– Their two-message memory delegation scheme has full soundness instead of weak soundness.

– Their secure function evaluation has computational function-hiding instead of statistical.

– Their offline-online argument of knowledge is computationally witness indistinguishable instead of statistically.

– The non-interactive commitment is perfectly binding and computationally hiding instead of weakly binding and statistically hiding.

Next we outline the analysis of [BBK$^+$16] and explain how to modify it for our protocol.

Soundness. Assuming that $x \notin \mathcal{L}$, in order to pass the witness indistinguishable argument of knowledge with respect to an evaluated cipher $\widehat{\mathsf{ct}}$ that decrypts to 1, the prover must know a proof $\pi \in \{0,1\}^\lambda$ and an opening of cmt to a digest $\mathsf{dig} \in \{0,1\}^\lambda$ and a time bound $t \leq T(\lambda)$ such that $\mathcal{V}_{\mathsf{param}}(\mathsf{vst}) = 1$. This, by definition, means that (dig, π, t) are such that the delegation verifier $\mathsf{MD.Ver}$ is convinced that the digest dig corresponds to a machine V^* such that $\mathsf{V}^*(\mathsf{wi}_1, \mathsf{cmt}) = (u, \ldots)$.

By the weak binding of cmt, the prover can only open the commitment to a polynomial number of different digests. Therefore, there must exist one digest dig for for which the prover can convince delegation verifier $\mathsf{MD.Ver}$ with high probability for an output u with high entropy, contradicting the weak soundness of the delegation scheme. In order to break the underlying delegation scheme we also rely on the semantic security of the encryption scheme to hide the secret verification state vst from the prover.

Protocol 2

Common Input: an instance $x \in \mathcal{L} \cap \{0,1\}^{\lambda}$, for security parameter λ.
P**:** a witness $w \in \mathcal{R}_{\mathcal{L}}(x)$.

1. P computes
   - wi_1, the first message of the offline prover $\mathsf{OffP}(1^{\lambda}, 1^{\ell_{\Psi}(\lambda)})$ where ℓ_{Ψ} is the length of the statement Ψ defined in Step 3 below,
   - $\mathsf{cmt} \leftarrow \mathsf{SHC.Com}(0^{2\lambda}; 1^{\lambda})$, a commitment to the all zero string,

   and sends $(\mathsf{wi}_1, \mathsf{cmt})$.
2. V computes
   - st_{V} and wi_2, the state and the second message of the offline verifier $\mathsf{OffV}(1^{\lambda}, 1^{\ell_{\Psi}(\lambda)})$ after receiving the message wi_1.
   - $(\mathsf{q}, \mathsf{vst}) \leftarrow \mathsf{MD.Query}(1^{\lambda})$, a query and secret state for the delegation scheme,
   - $(\mathsf{ct}_{\mathsf{vst}}, \mathsf{sk}) \leftarrow \mathsf{SFE.Enc}(1^{\lambda}, \mathsf{vst})$, an encryption of the secret state,
   - $u \leftarrow \{0,1\}^{\lambda}$, a uniformly random string,

   and sends $(u, \mathsf{wi}_2, \mathsf{q}, \mathsf{ct}_{\mathsf{vst}})$.
3. P computes
   - $\widehat{\mathsf{ct}} \leftarrow \mathsf{SFE.Eval}(\mathbf{1}, \mathsf{ct}_{\mathsf{vst}})$, an evaluation of the constant one function,
   - st_{P}, the state of the offline prover $\mathsf{OffP}(1^{\lambda}, 1^{\ell_{\Psi}(\lambda)})$ after receiving the message wi_2.
   - wi_3, the message for online prover OnP given the state st_{P}, the statement $\Psi = \Psi_1(x) \vee \Psi_2(\mathsf{wi}_1, \mathsf{cmt}, \mathsf{q}, u, \mathsf{ct}_{\mathsf{vst}}, \widehat{\mathsf{ct}})$ of length $\ell_{\Psi}(\lambda)$ given by:

     $$\left\{ \exists w \;\middle|\; (x,w) \in \mathcal{R}_{\mathcal{L}} \right\} \bigvee$$

     $$\left\{ \exists \begin{array}{l} \mathsf{dig}, \pi, r_{\mathsf{cmt}}, r_{\widehat{\mathsf{ct}}} \in \{0,1\}^{\mathrm{poly}(\lambda)} \\ t \le T(\lambda) \end{array} \;\middle|\; \begin{array}{l} \mathsf{cmt} = \mathsf{Com}(\mathsf{dig}, t; r_{\mathsf{cmt}}) \\ \mathsf{param} = ((\mathsf{wi}_1, \mathsf{cmt}), \mathsf{q}, u, \mathsf{dig}, t, \pi) \\ \widehat{\mathsf{ct}} = \mathsf{SFE.Eval}(\mathcal{V}_{\mathsf{param}}, \mathsf{ct}_{\mathsf{vst}}, r_{\widehat{\mathsf{ct}}}) \end{array} \right\} ,$$

     and the witness $w \in \mathcal{R}_{\mathcal{L}}(x)$ for Ψ_1,

   and sends $(\widehat{\mathsf{ct}}, \mathsf{wi}_3)$.
4. V verifies that $\mathsf{SFE.Dec}(\widehat{\mathsf{ct}}; \mathsf{sk}) = 1$ and that the online verifier OnP with state st_{V} and the statement Ψ accepts after receiving the message wi_3.

Fig. 2: A three-message statistical ZK argument of knowledge for **NP**.

Statistical zero knowledge. To show statistical zero knowledge , we construct a non-black-box simulator following the simulator of Barak [Bar01]. At high-level, the simulator uses the code of the (malicious) verifier V^* as the memory for the delegation scheme, and completes the witness indistinguishable argument of knowledge using a witness for the trapdoor statement Ψ_2. The witness consists of (dig, π, t) where dig is the digest corresponding to V^*, $t \approx |\mathsf{V}^*|$ and π is the corresponding delegation proof that $\mathsf{V}^*(\mathsf{wi}_1, \mathsf{cmt}) = (u, \dots)$, which is now true by definition.

By the perfect completeness of the delegation scheme, we know that for any encrypted secret state vst, given a query q that is consistent with vst, the delegation verifier $\mathsf{MD.Ver}$ will accept the corresponding proof. Thus, the perfect function hiding of the secure function evaluation (which holds also if the verifier produces a malformed ciphertext) guarantees that the evaluated ciphertext $\widehat{\mathsf{ct}}$ in the simulated proof is statistically close to that computed in the real proof where the prover actually evaluates the constant $\mathbf{1}$ circuit.

Relying also on the statistical witness indistinguishability of the argument of knowledge and the statistical hiding of cmt we deduce that V^*'s view in the real proof and the simulated view are statistically close.

References

[AH91] William Aiello and Johan Håstad. Statistical zero-knowledge languages can be recognized in two rounds. *J. Comput. Syst. Sci.*, 42(3):327–345, 1991.

[Bar01] Boaz Barak. How to go beyond the black-box simulation barrier. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 106–115, 2001.

[BBK+16] Nir Bitansky, Zvika Brakerski, Yael Tauman Kalai, Omer Paneth, and Vinod Vaikuntanathan. 3-message zero knowledge against human ignorance. In *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part I*, pages 57–83, 2016.

[BCC88] Gilles Brassard, David Chaum, and Claude Crépeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, 1988.

[BCC+14] Nir Bitansky, Ran Canetti, Alessandro Chiesa, Shafi Goldwasser, Huijia Lin, Aviad Rubinstein, and Eran Tromer. The hunting of the SNARK. *IACR Cryptology ePrint Archive*, 2014:580, 2014.

[BCPR14] Nir Bitansky, Ran Canetti, Omer Paneth, and Alon Rosen. On the existence of extractable one-way functions. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 505–514, 2014.

[BCY91] Gilles Brassard, Claude Crépeau, and Moti Yung. Constant-round perfect zero-knowledge computationally convincing protocols. *Theor. Comput. Sci.*, 84(1):23–52, 1991.

[BD18] Zvika Brakerski and Nico Döttling. Two-message statistically sender-private OT from LWE. In *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, pages 370–390, 2018.

[BDRV18] Itay Berman, Akshay Degwekar, Ron D. Rothblum, and Prashant Nalini Vasudevan. Multi-collision resistant hash functions and their applications. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, pages 133–161, 2018.

[BHKY19] Nir Bitansky, Iftach Hainer, Ilan Komargodski, and Eylon Yogev. Distributional collision resistance beyond one-way functions. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2019.

[BJY97] Mihir Bellare, Markus Jakobsson, and Moti Yung. Round-optimal zero-knowledge arguments based on any one-way function. In *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, pages 280–305, 1997.

[BKP18] Nir Bitansky, Yael Tauman Kalai, and Omer Paneth. Multi-collision resistance: a paradigm for keyless hash functions. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 671–684, 2018.

[Blu86] Manuel Blum. How to prove a theorem so no one else can claim it. 1986.

[BOV07] Boaz Barak, Shien Jin Ong, and Salil P. Vadhan. Derandomization in cryptography. *SIAM J. Comput.*, 37(2):380–400, 2007.

[BP04] Mihir Bellare and Adriana Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In *Proceedings of the 24th Annual International Cryptology Conference*, pages 273–289, 2004.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 97–106, 2011.

[CD09] Ran Canetti and Ronny Ramzi Dakdouk. Towards a theory of extractable functions. In *TCC*, pages 595–613, 2009.

[CKLR11] Kai-Min Chung, Yael Tauman Kalai, Feng-Hao Liu, and Ran Raz. Memory delegation. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 151–168, 2011.

[DN07] Cynthia Dwork and Moni Naor. Zaps and their applications. *SIAM J. Comput.*, 36(6):1513–1543, 2007.

[DPP93] Ivan Damgård, Torben P. Pedersen, and Birgit Pfitzmann. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. In *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, pages 250–265, 1993.

[FGJ18] Nils Fleischhacker, Vipul Goyal, and Abhishek Jain. On the existence of three round zero-knowledge proofs. *IACR Cryptology ePrint Archive*, 2018:167, 2018.

[FLS99] Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. *SIAM J. Comput.*, 29(1):1–28, 1999.

[For89] Lance Fortnow. The complexity of perfect zero-knowledge. *Advances in Computing Research*, 5:327–343, 1989.

[GK96] Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledge proof systems for NP. *J. Cryptology*, 9(3):167–190, 1996.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.

[GO94] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, December 1994.

[GOS12] Jens Groth, Rafail Ostrovsky, and Amit Sahai. New techniques for noninteractive zero-knowledge. *J. ACM*, 59(3):11, 2012.

[HM96] Shai Halevi and Silvio Micali. Practical and provably-secure commitment schemes from collision-free hashing. In *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, pages 201–215, 1996.

[HNO$^+$09] Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, and Salil P. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM J. Comput.*, 39(3):1153–1218, 2009.

[HT98] Satoshi Hada and Toshiaki Tanaka. On the existence of 3-round zero-knowledge protocols. In *Proceedings of the 18th Annual International Cryptology Conference*, pages 408–423, 1998.

[Kat12] Jonathan Katz. Which languages have 4-round zero-knowledge proofs? *J. Cryptology*, 25(1):41–56, 2012.

[KKS18] Yael Tauman Kalai, Dakshita Khurana, and Amit Sahai. Statistical witness indistinguishability (and more) in two messages. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, pages 34–65, 2018.

[KNY17] Ilan Komargodski, Moni Naor, and Eylon Yogev. White-box vs. black-box complexity of search problems: Ramsey and graph property testing. In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 622–632, 2017.

[KNY18] Ilan Komargodski, Moni Naor, and Eylon Yogev. Collision resistant hashing for paranoids: Dealing with multiple collisions. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, pages 162–194, 2018.

[KP16] Yael Tauman Kalai and Omer Paneth. Delegating RAM computations. In *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, pages 91–118, 2016.

[LS90a] Dror Lapidot and Adi Shamir. Publicly verifiable non-interactive zero-knowledge proofs. In *CRYPTO*, pages 353–365, 1990.

[LS90b] Dror Lapidot and Adi Shamir. Publicly verifiable non-interactive zero-knowledge proofs. In *Advances in Cryptology - CRYPTO '90, 10th Annual*

International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings, pages 353–365, 1990.

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *J. Cryptology*, 4(2):151–158, 1991.

[NOVY98] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for *NP* using any one-way permutation. *J. Cryptology*, 11(2):87–108, 1998.

[OPP14] Rafail Ostrovsky, Anat Paskin-Cherniavsky, and Beni Paskin-Cherniavsky. Maliciously circuit-private FHE. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, pages 536–553, 2014.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.