Lattice-Based Timed Cryptography

Russell W. F. Lai¹ and Giulio Malavolta^{2,3}

¹Aalto University ²Bocconi University ³Max Planck Institute for Security and Privacy

April 7, 2024

Abstract

Timed cryptography studies primitives that retain their security only for a predetermined amount of time, such as proofs of sequential work and time-lock puzzles. This feature has proven to be useful in a large number of practical applications, e.g. randomness generation, sealed-bid auctions, and fair multi-party computation. However, the current state of affairs in timed cryptography is unsatisfactory: Virtually all efficient constructions rely on a single sequentiality assumption, namely that repeated squaring in unknown order groups cannot be parallelised. This is a single point of failure in the classical setting and is even false against quantum adversaries.

In this work we put forward a new sequentiality assumption, which essentially says that a repeated application of the standard lattice-based hash function cannot be parallelised. We provide concrete evidence of the validity of this assumption and perform some initial cryptanalysis. We also propose a new template to construct proofs of sequential work, based on lattice techniques.

1 Introduction

Timed cryptography studies a family of cryptographic primitives with diverse functionalities designed to meet their security goals only for a short (polynomial) amount of time. This includes, for example, time-lock puzzles [RSW96], timed-commitments [BN00], proofs of sequential work [MMV13], verifiable delay functions [BBBF18], and delay encryption [BD21]. This branch of cryptography has important theoretical implications in the context of non-malleable commitments [LPS17] and in the average-case hardness of the class PPAD [BCH⁺22], which characterises the complexity of computing a Nash equilibrium. Furthermore, timed cryptography has attracted significant interest in the industry (e.g. [vdf19]), in part due to their large number of practical applications (see [BBBF18, MT19] for a survey of applications).

The Repeated Squaring Assumption. The current state of affairs in timed cryptography is largely unsatisfactory: Virtually all efficient schemes are based on the hardness of a *single* problem (or variants thereof), namely the sequential squaring assumption. Loosely speaking, such an assumption postulates that the repeated application of the function

$$f_N(x) = x^2 \bmod N$$

where N = pq is an RSA modulus, is the fastest algorithm to compute $x^{2^T} \mod N$ given x. In other words, there is no better algorithm than *T*-sequential iterations of f_N , provided that the order of the group is unknown by the evaluator. Unfortunately, this assumption is clearly false if we allow the attacker to run in *quantum* polynomial time. At present, there is no valid alternative sequential function with conjectured post-quantum security. Besides post-quantum security, the lack of other candidates places the entirety of efficient timed cryptography on thin foundations, and only one cryptanalytic breakthrough away from being wiped out. The goal of our work is to make progress on this front, and to establish broader foundations for timed cryptographic primitives.

1.1 Our Contributions

The contributions of this work can be summarised as follows. A more detailed technical overview is in Section 3.1.

A New Lattice-Based Sequential Function. We put forward a new candidate family of sequential functions, whose design is closely connected with lattice-based cryptography. Concretely, we define our new sequential function to be the *T*-fold repeated application of the binary decomposition operation followed by the SIS-based collision-resistant hash function [Ajt96, GGH96], with parameters set in such a way to make the domain and the range of the function coincide. In other words, our base function $f_{\mathbf{A}} : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ is defined as

$$f_{\mathbf{A}}(\mathbf{x}) := -\mathbf{A}\mathbf{G}^{-1}(\mathbf{x}) \mod q$$

where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, for $m \approx n \log q$, and $\mathbf{G}^{-1} : \mathbb{Z}_q^n \to \mathbb{Z}_2^m$ is the binary decomposition operator. Then we define $f_{\mathbf{A}}^T$ to be the *T*-fold repeated application of $f_{\mathbf{A}}$. Based on the observation that computing $\mathbf{y} = f_{\mathbf{A}}^T(\mathbf{x})$ is equivalent to establishing the satisfiability of a linear relation defined by $(\mathbf{A}, \mathbf{x}, \mathbf{y})$ by a binary vector \mathbf{u} , we conjecture that finding such (\mathbf{y}, \mathbf{u}) for random (\mathbf{A}, \mathbf{x}) is hard for (potentially quantum) circuits of depth less than *T* by some super-constant function in *T*.

Evidence of Sequentiality. The design of our new sequential function is motivated by concrete properties that one can prove about the base function, balanced with enough algebraic structure to enable advanced cryptographic applications. More specifically, the choice of our sequential function is based on the following guiding principles:

- Recursive composition: In order to have a succinct description, the sequential function is defined as the recursive application of a *base function* with cryptographic properties. There is evidence that this is a robust design principle: If the base function is modelled as a random oracle, then one can show that sequentiality holds unconditionally [CP18].
- Collision resistance: The base function must be collision-resistant (and one way). This is a property that is trivially satisfied by a random oracle and something that we can prove using standard computational assumptions.
- Uniformity preserving: Similar to a random oracle, the base function must map uniform distributions to uniform distributions over the specified domains and co-domains. Once again, we are able to prove that this property holds assuming the intractability of standard problems over lattices.

- Post-quantum security: Contrary to the sequential squaring problem, we want to conjecture that the sequentiality of our function holds also against *quantum* algorithms.
- Algebraic structure: Unlike a random oracle, we want our base function to have enough algebraic structure to produce relations that are amenable to efficient proofs.

In particular, we justify our assumption by showing that $f_{\mathbf{A}}$ is collision-resistant and uniformity preserving (for some choice of parameters) based on the standard lattice assumptions, suggesting other heuristic evidence, and discussing (failed) attack strategies.

Application: Proof of Sequential Work. As an additional contribution, we construct a simple and efficient proof of sequential work (PoSW), where a prover aims to convince a verifier that it has performed a T-steps sequential computation. Crucially, the verifier runtime is only logarithmic in T. Our PoSW is based on a variant of the sequential function family introduced above, with an important modification:

• (Relaxed Norm Constraints) Instead of checking that each step of the computation is a *binary string*, our PoSW will only ensure that is norm is *small*. This is done for efficiency reasons, since it is much easier to prove the latter property using lattice techniques.

However, subsequent to the publication of this work, attacks against the assumption were discovered, which render the security proof vacuous and even cast doubts on the heuristic security of our PoSW. We discuss in more details the attacks and the current state of affairs of lattice-based sequential functions in Section 2 and Appendix A.

On the Necessity of New Assumptions. We stress that we can only offer heuristic evidence for the sequentiality of our function family, and we are not able to reduce it to any "standard" computational problem. In fact, arguably the *only* "standard" computational assumption in timed cryptography is the repeated squaring assumption! Clearly, if we want to obtain a plausibly post-quantum candidate, new assumptions are necessary.

On the other hand, traditional computational assumptions in cryptography (such as LWE or DDH) do not make fine-grained distinctions on the parallelism of the attacker: The problem is assumed to be hard for all polynomial-size circuits, regardless of their depth/parallel runtime. In other words, such assumptions imply that $NP \neq P$ but do *not* imply that $NC \neq P$, which is a necessary condition for sequential functions to exist. Overall, this suggests that new assumptions may be necessary for timed cryptography, and we view our work as a promising first step towards a better understanding of this area.

2 History of This Work

The idea of using

$$f_{\mathbf{A}}(\mathbf{x}) := -\mathbf{A}\mathbf{G}^{-1}(\mathbf{x}) \bmod q$$

or similar as a candidate sequential function was, to the best of our knowledge, first conceived independently by Bogdanov and Rosen [BR23] but not published. We [LM23] later independently engineered the same idea, made the first attempt of formalising the sequentiality assumption and applying it to build a proof of sequential work (PoSW) protocol. We based the security of the PoSW protocol on a bounded-norm variant of the SIS-sequentiality assumption, which postulates that no parallel algorithm can find a *short* solution (as opposed to a *binary* solution required by the exact variant) to the system of equations induced by the *T*-folded repetition of the function $f_{\mathbf{A}}(\mathbf{x}) = -\mathbf{A}\mathbf{G}^{-1}(\mathbf{x}) \mod q$ in time $o(T) \cdot \mathsf{poly}(\lambda)$.

Subsequently to the publication of this work, Attema and Ducas [AD23] and Peikert and Tang [PT23] independently discovered attacks against the bounded-norm variant (but not the exact variant) of this assumption, as well as the PoSW protocol. Below and in Appendix A, we discuss these attacks in more detail.

The Attema-Ducas Attack. Attema and Ducas [AD23] discovered an attack against the SISsequentiality assumption, which runs in depth $\sqrt{T} \log T \cdot \text{poly}(\lambda)$ and can find solutions of norm at most m. Their attack exploits the sparsity of the image vector of the sequential-SIS relation.

The Peikert-Tang Attack. Independently and more generally, Peikert and Tang [PT23] discovered a family of attacks against the SIS-sequentiality assumption, which offers a trade-offs between the parallel time of the solver and the norm of the solution found. Specifically, their attack has depth $k \log_k T \cdot \operatorname{poly}(\lambda)$, and can find solutions of norm at most $m^{(\log_k T)/2}$, for any $1 \le k \le T$. For $k = \sqrt{T}$, the Peikert-Tang attack is as performant as that of Attema-Ducas, and has no restriction on the image vector.

Implications on our PoSW Protocol. Underlying our PoSW protocol is a succinct interactive argument system which allows the prover to recursively prove knowledge of a short solution to a sequential-SIS relation. However, for the parameter choices and security proof techniques considered, the norm bound checked by the verifier is around $m^{\log T}$ times larger than the norm of the sequential-SIS solution (known as the "completeness gap"), and the witness extracted by the knowledge extractor in the security proof is yet another $m^{\log T}$ times longer (known as the "soundness gap"). Due to the large soundness gap, the security proof of the PoSW protocol becomes vacuous, because it relies on an instantiation of the SIS-sequentiality assumption which is false (for desirable parameters) due to the above attacks.

In addition to their attack against the SIS-sequentiality assumption, Peikert and Tang [PT23] also discovered attacks against a variant of our PoSW protocol (but not on the protocol presented in this work), with similar norm-time trade-offs as their attacks against the SIS-sequentiality assumption. This casts doubts on the heuristic security of our PoSW protocol, although at present we are not aware of any attack against the protocol.

The (Almost) Exact Sequentiality Assumption. We remark that both attacks discussed above allow to find solutions which are short but non-binary. We are currently unaware of any attack against the exact version of the SIS-sequentiality assumption, where the adversary is required to find a binary (or in general *p*-ary) solution, or even against the bounded-norm variant with a very strict norm bound of $m^{1/2(1-\epsilon)}$ where $\epsilon > 0$. This means that the verifiable delay functions proposed in [CLM23] based on the *exact* version of the assumption is unaffected by the above attacks.

3 Related Work

Besides works based on the repeated squaring assumption, there are various other approaches for constructing timed cryptographic primitives from different computational assumptions. In the following, we discuss the trade-offs when compared with our work. **Hash-Based Schemes.** As alluded at earlier, random oracles are good candidates for constructing sequential functions, since the sequentiality of their repeated applications can be proven unconditionally. This approach has appealing properties: It offers a clean model to prove concrete statements, schemes are typically very efficient as they only involve symmetric-key operations, and one can conjecture (or even prove) post-quantum security. In fact, random oracles have been used to construct PoSW [MMV13, CP18, DLM19] with high concrete efficiency. However, the construction paradigm adopted by these hash-based PoSWs restricts them to only offer a weak sequentiality guarantee: For any constant $0 \le \alpha < 1$, the soundness of the scheme (parametrised by α) is only guaranteed against cheating provers who run in parallel time $(1 - \alpha) \cdot T$, where the verifier runtime is $\frac{1}{\log(1-\alpha)} \cdot O(\lambda)$. On the other hand, constructions based on unknown order groups (e.g. [Pie19]), which we aim to emulate with lattice-based techniques, seem to resist any adversary running in time at most $(1 - \omega(1)) \cdot T$, i.e. no adversary can speed up the computation by any additive factor super-constant in T, while still having the verifier run in a fixed polynomial time.

Isogeny-Based Schemes. Recent works have explored constructions of timed cryptography from isogenies over elliptic curves [DMPS19, BD21]. This approach allows one to construct verifiable delay functions (VDF) [BBBF18] and even delay encryption [BD21]. However, such constructions are not post-quantum secure [DMPS19], or they rely on generic composition with succinct non-interactive arguments [CSRT22], making them impractical. Furthermore, the underlying assumptions have received substantially less scrutiny than sequential squaring.

Generic Approaches. Finally, we mention that one can use general-purpose cryptographic primitives to build timed cryptographic schemes. Assuming only the existence (but not knowledge) of an (iterative) sequential function, it is possible to provably construct an (iterative) sequential function from fully homomorphic encryption [JMRR21]. Incremental verifiable computation [Val08] can be immediately used to construct PoSWs and VDFs given a sequential function [BBBF18, DGMV20], and indistinguishability obfuscation can be used to construct time-lock puzzles [BGJ⁺16]. While theoretically elegant, such generic constructions use heavy cryptographic machinery and result in schemes that are (concretely) prohibitively inefficient.

3.1 Technical Overview

In the following, we elaborate more on the results summarised in Section 1.1. For simplicity, the exposition in this technical overview is done over the set of rational integers, i.e. \mathbb{Z} . In the technical sections, we will be working over a ring of integers \mathcal{R} of some cyclotomic field, which captures \mathbb{Z} as a special case.

Lattice-based Sequential Function/Relation. We propose a new candidate sequential function defined as the *T*-fold repeated application of the binary decomposition operation followed by the SIS-based collision-resistant hash function [Ajt96, GGH96], with parameters set in such a way to make the domain and the codomain of the function coincide. Concretely, (a special case of) our base function $f_{\mathbf{A}} : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ is defined as

$$f_{\mathbf{A}}(\mathbf{x}) := -\mathbf{A}\mathbf{G}^{-1}(\mathbf{x}) \bmod q$$

where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, for $m \approx n \log q$, and $\mathbf{G}^{-1} : \mathbb{Z}_q^n \to \mathbb{Z}_2^m$ is the binary decomposition operator. Below, we assume for simplicity that $m = n \log q$. At first glance, it may seem that the function $f_{\mathbf{A}}$ is not proof-friendly, since \mathbf{G}^{-1} is a highly non-linear operation. However, a few simple but crucial observations allow us to express the relations induced by $f_{\mathbf{A}}$ in a proof-friendly form. Specifically, we observe that a pair (\mathbf{x}, \mathbf{y}) satisfies $\mathbf{y} = f_{\mathbf{A}}(\mathbf{x})$ if and only if there exists a binary vector $\mathbf{u} \in \mathbb{Z}_2^m$ such that

$$\begin{pmatrix} \mathbf{G} \\ \mathbf{A} \end{pmatrix} \cdot \mathbf{u} = \begin{pmatrix} -\mathbf{x} \\ \mathbf{y} \end{pmatrix} \bmod q$$

where \mathbf{G} is the binary reconstruction gadget matrix, which in particular is a linear operator.

Generalising, suppose $\mathbf{x}_T = f_{\mathbf{A}}^T(\mathbf{x}_0)$ is the *T*-fold repeated application of $f_{\mathbf{A}}$ on \mathbf{x}_0 . Writing $\mathbf{x}_i = f_{\mathbf{A}}(\mathbf{x}_{i-1})$ and $\mathbf{u}_i = -\mathbf{G}^{-1}(\mathbf{x}_i)$, we observe the following equivalent relation:

We conjecture and give evidence that, if the short integer solution problem SIS_{n,m,q,\mathbb{Z}_2} is hard, then for any $T \in \mathbb{N}$ and uniformly random $(\mathbf{A}, \mathbf{x}_0)$, it is infeasible for an adversary to find $(\mathbf{u}_0, \ldots, \mathbf{u}_{T-1}, \mathbf{x}_T)$ satisfying the above relation in parallel time $(1 - \omega(1)) \cdot T$.

Sequential Relation and Proof of Sequential Work. In the sequential relation (Eq. (1)) proposed above, enforcing $\mathbf{u} \in \mathbb{Z}_2^{mT}$ ensures that for each instance \mathbf{x}_0 there exists a unique witness $(\mathbf{u}_0, \ldots, \mathbf{u}_{T-1}, \mathbf{x}_T)$. To construct a verifiable delay function (VDF), it suffices to prove the satisfiability of Eq. (1) with binary $(\mathbf{u}_0, \ldots, \mathbf{u}_{T-1})$ using a (preprocessing) succinct non-interactive argument (SNARG) with a (quasi-)linear-time prover and a sublinear-time verifier (after preprocessing). Instantiating with a post-quantum-secure SNARG, which exists unconditionally in the quantum random oracle model [CMS19], we can obtain a candidate post-quantum VDF. For concrete efficiency, however, it may be beneficial to use a SNARG which natively supports proving lattice relations, e.g. that of [CLM23].

Although we believe that the above generic approach yields a somewhat efficient VDF, especially when instantiated with a SNARG optimised for proving the sequential relation, in this work we focus on constructing a tailor-made proof of sequential work (PoSW) which explicitly takes advantage of the block-bidiagonal structure of \mathbf{A}_T in Eq. (1). Towards this, we propose a variant of the sequential relation introduced above with a major change:

• (Bounded-Norm Variant) The binary constraint, i.e. $\mathbf{u} \in \mathbb{Z}_2^{mT}$, is relaxed to a bounded-norm constraint, i.e. $\mathbf{u} \in \mathbb{Z}_{\beta}^{mT}$ for some $2 \leq \beta \ll q$.

The relation in Eq. (1) is therefore replaced by

$$\underbrace{\begin{pmatrix} \mathbf{G} & & \\ \mathbf{A} & \mathbf{G} & & \\ & \mathbf{A} & \ddots & & \\ & & \mathbf{A} & \ddots & \ddots & \\ & & & \ddots & \ddots & \mathbf{G} \\ & & & \mathbf{A} & \end{pmatrix}}_{\mathbf{A}_{T}:=} \cdot \underbrace{\begin{pmatrix} \mathbf{u}_{0} \\ \mathbf{u}_{1} \\ \vdots \\ \vdots \\ \mathbf{u}_{T-1} \end{pmatrix}}_{\mathbf{u}:=} = \begin{pmatrix} -\mathbf{x} \\ \mathbf{0} \\ \vdots \\ \vdots \\ \mathbf{0} \\ \mathbf{y} \end{pmatrix} \mod q \quad \text{and} \quad \mathbf{u} \in \mathbb{Z}_{\beta}^{mT}.$$
(2)

The main observation which underlies our PoSW construction is the following. When T = 2t + 1, the matrix \mathbf{A}_T can be partitioned into

$$\mathbf{A}_T = egin{pmatrix} \mathbf{A}_t & & & & & \ & & \mathbf{G} & & & \ & & & \mathbf{A} & & \ & & & \mathbf{A}_t & & \ & & & \mathbf{A}_t & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \mathbf{A}_t & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \ & & \mathbf{A}_t & & \mathbf{A}$$

This structure allows us to construct a PoSW with a $O(\log T)$ -time verifier in the random oracle model following the strategy in the (VDF) construction in [Pie19].

In more detail, we sketch an interactive variant of the PoSW construction. Since the verifier is public-coin, the non-interactive variant follows from the Fiat-Shamir transform [FS87, AFK22] in the random oracle model. An instance of our PoSW is set up by sampling a random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, which defines \mathbf{A}_T for any T, and a random vector $\mathbf{x}_0 \leftarrow \mathbb{Z}_q^n$. To convince the verifier that Eq. (1) holds for some $T \in \mathbb{N}$, the prover and the verifier engage in the following interactive protocol: We focus on the more interesting where T = 2t + 1 is odd¹. The prover sends \mathbf{u}_t to the verifier, reducing the linear relation in Eq. (1) to

$$\mathbf{A}_t \cdot \begin{pmatrix} \mathbf{u}_0 & \mathbf{u}_{t+1} \\ \vdots & \vdots \\ \mathbf{u}_{t-1} & \mathbf{u}_{T-1} \end{pmatrix} = \begin{pmatrix} -\mathbf{x} & -\mathbf{A} \cdot \mathbf{u}_t \\ \mathbf{0} & \mathbf{0} \\ \vdots & \vdots \\ \mathbf{0} & \mathbf{0} \\ -\mathbf{G} \cdot \mathbf{u}_t & \mathbf{y} \end{pmatrix} \mod q.$$

The verifier checks that $\mathbf{u}_t \in \mathbb{Z}_{\beta}^m$. If the check passes, the verifier sends a random challenge $r \in S \subseteq \mathbb{Z}$ chosen from challenge set S to the prover. The prover and verifier then engage in the same protocol but with parameter t for proving

$$\mathbf{A}_t \begin{pmatrix} \mathbf{u}_0 + \mathbf{u}_{t+1}r \\ \vdots \\ \mathbf{u}_{t-1} + \mathbf{u}_{T-1}r \end{pmatrix} = \begin{pmatrix} -(\mathbf{x} + \mathbf{A}\mathbf{u}_t r) \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{y}r - \mathbf{G}\mathbf{u}_t \end{pmatrix} \mod q, \ \begin{pmatrix} \mathbf{u}_0 + \mathbf{u}_{t+1}r \\ \vdots \\ \mathbf{u}_{t-1} + \mathbf{u}_{T-1}r \end{pmatrix} \in \mathbb{Z}_{\beta'}^{mt}$$

for an appropriately chosen $\beta' > \beta$. After recursing for $O(\log T)$ times, the prover and the verifier arrives at a statement of size independent of T for which the prover can simply send the witness to the verifier.

Using standard techniques for arguing about security of (lattice-based) Σ -protocols (e.g. [BLNS20, AL21, ACK21]), one could argue that (a parallel repetition [AF22] of) the above protocol allows to convince the verifier that the prover has knowledge of a witness satisfying Eq. (2) with certain norm bound $\beta^* > \beta$. However, for typical choices of parameters, such β^* is some $\lambda^{\omega(1)}$ factor larger than β such that the sequentiality assumption becomes vacuous due to the attacks by Attema and

¹If T is even, the prover can reveal the last step of the computation. It then suffices for the prover to prove Eq. (1) for T - 1, which is odd.

Ducas [AD23] and by Peikert and Tang [PT23]. We are therefore unable to prove the security of the PoSW protocol from any simpler assumption.

Note that even if we start with $\beta = 2$, the above protocol can only convince the verifier about the satisfiability of Eq. (1) with some $\beta^* > \beta$, where witnesses are not unique. This is the why our construction of PoSW does not yield a VDF, even though our construction is morally similar to the VDF construction of [Pie19].

4 Preliminaries

We denote by $\lambda \in \mathbb{N}$ the security parameter. A function $\operatorname{negl}(\cdot)$ is negligible if it vanishes faster than any polynomial. The cryptographic definitions in the paper follow the convention of modeling security against non-uniform adversaries. An efficient adversary \mathcal{A} is modeled as a sequence of circuits $\mathcal{A} = \{\mathcal{A}_{\lambda}\}_{\lambda \in \mathbb{N}}$, such that the circuit \mathcal{A}_{λ} is of polynomial size in λ . We define the *parallel* runtime of a given algorithm as the depth of the corresponding circuit, whereas the *total* runtime is determined by the size of the circuit.

For $n \in \mathbb{N}$, denote $[n] := \{1, 2, ..., n\}$. For a finite set S, we write U(S) for the uniform distribution over S. We will use $p, q, s \in \mathbb{N}$ to denote moduli.

We use bold capital letters, e.g. **A**, to denote matrices, and bold lower-case letters, e.g. **x**, to denote column vectors. An *m*-dimensional column vector is denoted by $\mathbf{x} = (x_1, \ldots, x_m)$.

Lattice Background. Let $\mathcal{R} = \mathbb{Z}[\zeta]$ be the ring of integers of a cyclotomic field $\mathbb{Q}(\zeta)$, where $\zeta \in \mathbb{C}$ is a fixed f-th primitive root of unity for some $\mathfrak{f} = \mathsf{poly}(\lambda)$. The degree of \mathcal{R} is $\varphi = \varphi(\mathfrak{f})$. An element $x \in \mathcal{R}$ is represented by its coefficients encoding $x = \sum_{i=0}^{\varphi-1} x_i \zeta^i$, and its (infinity) norm is $||x|| \coloneqq \max_{i=0}^{\varphi-1} |x_i|$, where $x_i \in \mathbb{Z}$. The norm extends naturally to vectors $\mathbf{u} = (u_1, \ldots, u_m) \in \mathcal{R}^m$, where $||\mathbf{u}|| = \max_{i \in [m]} ||u_i||$. The expansion factor of \mathcal{R} is defined as $\gamma_{\mathcal{R}} \coloneqq \max_{a,b \in \mathcal{R}} \frac{||a \cdot b||}{||\mathbf{u}|| \cdot ||\mathbf{b}||}$. We will always assume that \mathfrak{f} is a prime-power, and in that case it is known that $\gamma_{\mathcal{R}} \leq 2\varphi$ [AL21]. For $q \in \mathbb{N}$, define $\mathcal{R}_q \coloneqq \mathcal{R}/q\mathcal{R}$. By a slight abuse of notation, we identify \mathcal{R}_q by

$$\left\{\sum_{i=0}^{\varphi-1} x_i \zeta^i : x_i \in \{-\lceil q/2 \rceil + 1, \dots, \lfloor q/2 \rfloor\}\right\}$$

and thus $||x|| \leq q/2$ for any $x \in \mathcal{R}_q$. The sets of units in \mathcal{R} and \mathcal{R}_q are denoted by \mathcal{R}^{\times} and \mathcal{R}_q^{\times} respectively. A set $S \subseteq \mathcal{R}$ is said to be subtractive if $(a - b) \in \mathcal{R}^{\times}$ for any distinct $a, b \in S$.

We recall the following useful fact.

Lemma 4.1 (Adapted from [BJRW20, Lemma 7]). Let $n = \text{poly}(\lambda)$, $p, q \in \mathbb{N}$, q prime, and $m \ge n \log_p q + \omega(\log \lambda)$. The following distributions are statistically close in λ :

$$\left\{ \begin{aligned} \mathbf{A} &\leftarrow \$ \, \mathcal{R}_q^{n \times m} \\ (\mathbf{A}, \mathbf{v}) &: \mathbf{u} \leftarrow \$ \, \mathcal{R}_p^m \\ \mathbf{v} &:= \mathbf{A} \cdot \mathbf{u} \bmod q \end{aligned} \right\} \qquad \text{and} \qquad \left\{ (\mathbf{A}, \mathbf{v}) : \frac{\mathbf{A} \leftarrow \$ \, \mathcal{R}_q^{n \times m}}{\mathbf{v} \leftarrow \$ \, \mathcal{R}_q^n} \right\}.$$

Gadget Matrices. For any $n, p, q \in \mathbb{N}$, let $\ell = \lceil \log_p q \rceil$ and $m = n\ell$. If $q < p^{\ell}$, write $q = \sum_{i=0}^{\ell-1} q_i \cdot p^i$ in *p*-ary expansion. If $q = p^{\ell}$, let $q_0 = \ldots = q_{\ell-2} = 0$ and $q_{\ell-1} = p$. Define the generalised "gadget

vector" $\mathbf{g}_{p,q}$, generalised "gadget matrix" $\mathbf{G}_{p,q}$, and "parity-check matrix" $\mathbf{H}_{p,q}$ by

$$\mathbf{g}_{p,q}^{\mathsf{T}} \coloneqq \begin{pmatrix} 1 & p & \dots & p^{\ell-1} \end{pmatrix}, \quad \mathbf{G}_{p,q} \coloneqq \mathbf{I}_n \otimes \mathbf{g}_{p,q}^{\mathsf{T}}, \quad \mathbf{H}_{p,q} \coloneqq \mathbf{I}_n \otimes \begin{pmatrix} p & & q_0 \\ -1 & p & & q_1 \\ & -1 & \ddots & & \vdots \\ & & \ddots & \ddots & p & \vdots \\ & & & -1 & q_{\ell-1} \end{pmatrix}$$

respectively. Define the operator $\mathbf{G}_{p,q}^{-1}: \mathcal{R}_q^n \to \mathcal{R}_p^m$ which maps $\mathbf{v} = (v_i)_{i=0}^{n-1} \in \mathcal{R}_q^n$ to the concatenation of its *p*-ary representation $\left((v_{0,j})_{j=0}^{\ell-1}, \ldots, (v_{n-1,j})_{j=0}^{\ell-1}\right) \in \mathcal{R}_p^m$, i.e. $v_i = \sum_{j=0}^{\ell-1} v_{i,j} \cdot p^j$. The operator $\mathbf{G}_{p,q}^{-1}$ is naturally extended to act on any matrix \mathbf{V} over \mathcal{R}_q with *n* rows, with $\mathbf{G}_{p,q} \cdot \mathbf{G}_{p,q}^{-1}(\mathbf{V}) = \mathbf{V}$. Note that $\mathbf{G}_{p,q} \cdot \mathbf{H}_{p,q} = \mathbf{0} \mod q$. Indeed, $\mathbf{H}_{p,q}$ is a basis of the right-kernel of $\mathbf{G}_{p,q}$ over \mathcal{K} . When the choices of n, p, q are clear from the context, we omit the subscripts and write $\mathbf{G} \coloneqq \mathbf{G}_{p,q}$.

Computational Assumptions. In the following we define the ring variant of the well-known short integer solution (SIS) problem [Ajt96].

Assumption 4.2 (Short Integer Solution). Let \mathcal{R}, n, m, q, s be parametrised by λ . The $SIS_{\mathcal{R},n,m,q,s}$ assumption states that for any $\mathbf{v} \in \mathcal{R}_q^n$ and any PPT adversary \mathcal{A} it holds that

$$\Pr\left[\mathbf{A} \cdot \mathbf{u} = \mathbf{v} \mod q \land \mathbf{u} \in \mathcal{R}^m_\beta \middle| \begin{array}{c} \mathbf{A} \leftarrow \$ \mathcal{R}^{n \times m}_q \\ \mathbf{u} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{v}) \end{array} \right] \le \mathsf{negl}(\lambda).$$

We also recall the learning with errors (LWE) problem [Reg05], and in particular the version over rings [LPR10].

Assumption 4.3 (Learning with Errors). Let $\mathcal{R}, n, m, q, \chi$ be parametrised by λ . The (normal form of the) LWE_{\mathcal{R},n,m,q,χ} assumption states that for any PPT adversary \mathcal{A} it holds that

$$\left| \Pr \begin{bmatrix} \mathcal{A}(\mathbf{A}, \mathbf{b}) = 1 & \begin{vmatrix} \mathbf{A} \leftarrow \$ \, \mathcal{R}_q^{n \times m} \\ \mathbf{s} \leftarrow \$ \, \chi^n \\ \mathbf{e} \leftarrow \$ \, \chi^m \\ \mathbf{b}^{\mathsf{T}} \coloneqq \mathbf{s}^{\mathsf{T}} \cdot \mathbf{A} + \mathbf{e}^{\mathsf{T}} \mod q \end{bmatrix} - \Pr \begin{bmatrix} \mathcal{A}(\mathbf{A}, \mathbf{b}) = 1 & \begin{vmatrix} \mathbf{A} \leftarrow \$ \, \mathcal{R}_q^{n \times m} \\ \mathbf{b} \leftarrow \$ \, \mathcal{R}_q^m \end{bmatrix} \right| \le \mathsf{negl}(\lambda).$$

For convenience, we state here a decisional variant of the SIS problem, which is known to be as hard as LWE. For completeness, we recall also a proof of this fact.

Assumption 4.4 (Decisional Short Integer Solution). Let $\mathcal{R}, n, m, q, \chi$ be parametrised by λ . The $\mathsf{dSIS}_{\mathcal{R},n,m,q,\chi}$ assumption states that for any PPT adversary \mathcal{A} it holds that

$$\left| \Pr \left[\mathcal{A}(\mathbf{A}, \mathbf{v}) = 1 \middle| \begin{array}{c} \mathbf{A} \leftarrow \$ \, \mathcal{R}_q^{n \times m} \\ \mathbf{u} \leftarrow \$ \, \chi^m \\ \mathbf{v} \coloneqq \mathbf{A} \cdot \mathbf{u} \bmod q \end{array} \right] - \Pr \left[\mathcal{A}(\mathbf{A}, \mathbf{v}) = 1 \middle| \begin{array}{c} \mathbf{A} \leftarrow \$ \, \mathcal{R}_q^{n \times m} \\ \mathbf{v} \leftarrow \$ \, \mathcal{R}_q^n \end{array} \right] \right| \le \mathsf{negl}(\lambda).$$

Lemma 4.5. If $m = n + \Omega(\lambda)$ and the LWE_{\mathcal{R},n,m,q,χ} assumption holds, then the dSIS_{\mathcal{R},n,m,q,χ} assumption holds.

Proof. Suppose there exists a PPT algorithm \mathcal{A} which solves the $\mathsf{dSIS}_{\mathcal{R},n,m,q,\chi}$ problem. We construct a PPT algorithm \mathcal{B} which solves the $\mathsf{LWE}_{\mathcal{R},n,m,q,\chi}$ problem. On input $(\bar{\mathbf{A}}, \bar{\mathbf{b}}) \in \mathcal{R}_q^{n \times m} \times \mathcal{R}_q^m$, \mathcal{B} samples $\mathbf{A} \leftarrow \Re \mathcal{R}_q^{n \times m}$ uniformly conditioned on $\bar{\mathbf{A}} \cdot \mathbf{A}^{\mathsf{T}} = \mathbf{0} \mod q$. It then computes $\mathbf{v} \coloneqq \mathbf{A} \cdot \bar{\mathbf{b}} \mod q$ and outputs $b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{v})$.

We next analyse the distribution of (\mathbf{A}, \mathbf{v}) . First, since $\bar{\mathbf{A}}$ is uniformly random over $\mathcal{R}_q^{n \times m}$, so does \mathbf{A} . Furthermore, since $m = n + \Omega(\lambda)$, with overwhelming probability in λ we have that the columns of \mathbf{A} spans \mathcal{R}_q^n . Conditioning on this, we show that \mathcal{B} is given an LWE sample if and only if \mathcal{B} gives a SIS sample to \mathcal{A} . Observe that if $(\bar{\mathbf{A}}, \bar{\mathbf{b}})$ is an LWE sample, then $\bar{\mathbf{b}}$ is of the form $\bar{\mathbf{b}}^{\mathsf{T}} = \mathbf{s}^{\mathsf{T}} \cdot \bar{\mathbf{A}} + \mathbf{e}^{\mathsf{T}}$ for some $\mathbf{e} \leftarrow \$ \chi^m$. It follows that \mathbf{v} is of the form $\mathbf{v} = \mathbf{A} \cdot \mathbf{e} \mod q$. If $(\bar{\mathbf{A}}, \bar{\mathbf{b}})$ is a random sample, then $\mathbf{v} = \mathbf{A} \cdot \bar{\mathbf{b}} \mod q$ is uniformly random.

5 A Lattice-Based Sequential Function/Relation

In what follows we formally define our family of sequential functions and state our conjecture regarding the sequentiality of the T-fold repetition of such functions. We consider two variants of the assumptions, that we describe below.

Our Exact Sequential Function. For any $\mathbf{A} \in \mathcal{R}_q^{n \times m}$, define the function $f_{\mathbf{A}} : \mathcal{R}_q^m \to \mathcal{R}_q^m$ as

$$f_{\mathbf{A}}(\mathbf{x}) := -\mathbf{A}\mathbf{G}^{-1}(\mathbf{x}) \bmod q.$$

For $T \in \mathbb{N}$, the T-fold recursive evaluation of $f_{\mathbf{A}}$ is defined as:

$$f_{\mathbf{A},\mathbf{z}}^{T}(\mathbf{x}) := \underbrace{f_{\mathbf{A}}(\dots f_{\mathbf{A}}(f_{\mathbf{A}}))\dots}_{T \text{ times}}(\mathbf{x})\dots$$

We conjecture that for uniformly distributed (\mathbf{A}, \mathbf{x}) , the evaluation of $f_{\mathbf{A}}^{T}(\mathbf{x})$ take sequential time at least $\Omega(T)$.²

Our Sequential Relation. We also consider a relaxed variant of the assumption as stated above, that will be useful in the context of our PoSW. Compared to the above function, we introduce one modification: We only require that the transcript is of small norm. To formally state our conjecture, it is convenient to define



²Note that this exact version of the conjecture is unaffected by known attacks [AD23, PT23].

Let $\mathbf{x}_0 := \mathbf{x}$. Observe that if the evaluation of each step of $f_{\mathbf{A},\mathbf{z}}^T(\mathbf{x})$ is split into two sub-steps as $\mathbf{u}_{i-1} = -\mathbf{G}^{-1}(\mathbf{x}_{i-1}) \in \mathcal{R}_p^m$ and $\mathbf{x}_i = \mathbf{A}\mathbf{u}_{i-1} \mod q$ for all $i \in [T]$, then

$$\mathbf{A}_{T}\begin{pmatrix}\mathbf{u}_{0}\\\mathbf{u}_{1}\\\vdots\\\vdots\\\mathbf{u}_{T-1}\end{pmatrix} = \begin{pmatrix}\mathbf{G}\\\mathbf{A}\\\mathbf{G}\\\mathbf{A}\\\mathbf{G}\\\mathbf{A}\\\mathbf{A}\end{pmatrix}\begin{pmatrix}\mathbf{u}_{0}\\\mathbf{u}_{1}\\\vdots\\\vdots\\\mathbf{u}_{T-1}\end{pmatrix} = \begin{pmatrix}-\mathbf{x}_{0}\\\mathbf{0}\\\vdots\\\vdots\\\mathbf{0}\\\mathbf{x}_{T}\end{pmatrix} \mod q \quad \text{and} \quad \begin{pmatrix}\mathbf{u}_{0}\\\mathbf{u}_{1}\\\vdots\\\vdots\\\mathbf{u}_{T-1}\end{pmatrix} \in \mathcal{R}_{p}^{mT}.$$

Furthermore, if $q = p^{\ell}$, we observe that the preimage $\mathbf{u} := (\mathbf{u}_0^{\mathsf{T}} \quad \mathbf{u}_1^{\mathsf{T}} \quad \dots \quad \mathbf{u}_{T-1}^{\mathsf{T}})^{\mathsf{T}}$, and hence the evaluation result \mathbf{x}_T , are unique. Moreover, for any $\beta \ge p$, we see that $\mathbf{u} \in \mathcal{R}_p^{mT}$ implies the relaxed condition $\mathbf{u} \in \mathcal{R}_{\beta}^{mT}$.

Formally, we state a family of conjectures parametrised by $\mathcal{R}, n, m, p, q, \beta, \sigma$ as follows.

Assumption 5.1 (SIS-Sequentiality). Let $\mathcal{R}, n, p, q, \beta, \sigma$ be parametrised by λ , where $\beta : \mathbb{N} \to \mathbb{R}^+$ and $\sigma : \mathbb{N} \to \mathbb{N}$ are functions, and let $m = n \lceil \log_p q \rceil$. For any $T \in \mathbb{N}$, if the $\mathsf{SIS}_{\mathcal{R},n,m,q,\beta,\sigma}$ assumption holds for $\beta = \beta(T)$, then for all polynomial-size adversary \mathcal{A} it holds that

$$\Pr\begin{bmatrix} \mathbf{A}_T \cdot \mathbf{u} = \begin{pmatrix} -\mathbf{x}^T & \mathbf{0}^T & \dots & \mathbf{0}^T & \mathbf{y}^T \end{pmatrix}^T \mod q & \mathbf{A} \leftarrow \$ \mathcal{R}_q^{n \times m} \\ \wedge \mathbf{u} \in \mathcal{R}_{\beta(T)}^{mT} & & \mathbf{x} \leftarrow \$ \mathcal{R}_q^n \\ \wedge \mathsf{Depth}(\mathcal{A}) < \sigma(T) & & & \begin{pmatrix} \mathbf{u} \in \mathcal{R}_q^{n, \times m} \\ \mathbf{x} \leftarrow \$ \mathcal{R}_q^n \\ (\mathbf{y}, \mathbf{u}) = \mathcal{A}(\mathbf{A}, \mathbf{x}) \end{bmatrix} \leq \mathsf{negl}(\lambda).$$

The security proof of the PoSW of the published version of this work [LM23] relies on the assumption for $\beta = (2\gamma_R)^{2\log T} \cdot p$. However, the attack by Attema and Ducas [AD23] shows that the assumption is false for $\beta = \gamma_R mp/2$ and $\sigma = O(\sqrt{T}\log T) \cdot \operatorname{poly}(\lambda)$. More generally, the attack by Peikert and Tang [PT23] falsifies the assumption in the case where $\beta > (\gamma_R m)^{(\log_k T)/2}$ and $\sigma(T) > (k \log_k T) \cdot \operatorname{poly}(\lambda)$ for some arity parameter $1 \leq k \leq T$. In particular, the Peikert-Tang attack has the same performance as that of Attema-Ducas when $k = \sqrt{T}$ and p = 2.

To avoid both attacks, one should set β and σ to fall outside the regime of

$$\beta > (\gamma_{\mathcal{R}} m)^{(\log_k T)/2}$$
 and $\sigma(T) > (k \log_k T) \cdot \mathsf{poly}(\lambda).$

For example, setting $\beta \leq (\gamma_{\mathcal{R}} m)^{\frac{1}{2(1-\epsilon)}}$ for some $0 \leq \epsilon = \epsilon(\lambda, T) < 1$ forces the Peikert-Tang attack to run in depth at least $\frac{T^{1-\epsilon}}{1-\epsilon} \cdot \operatorname{poly}(\lambda)$. We refer to Appendix A for more details on the attacks.

By the above discussion, $\{f_{\mathbf{A},\mathbf{z}}^T\}_{\mathbf{A},\mathbf{z}}$ induces a family of sequential relations. Although such a relation has potentially many solutions $(\mathbf{y}, \mathbf{u}) \in \mathcal{R}_q^n \times \mathcal{R}_\beta^{mT}$ to an input \mathbf{x} , each takes $\sigma(T)$ sequential steps to find under the SIS-sequentiality assumption.

5.1 Evidence of Sequentiality

To substantiate the plausibility of our exact sequentiality assumption, we shall offer some concrete evidence on the cryptographic properties satisfied by the function $f_{\mathbf{A}}$. First we show that the function $f_{\mathbf{A}}$ is collision resistant.

Theorem 5.2 (Collision Resistance). If the $SIS_{\mathcal{R},n,m,q,p}$ problem is hard for $m = n \cdot \lceil \log_p q \rceil$, then $f_{\mathbf{A}}$ is collision resistant.

Proof. The proof is a trivial reduction from the $SIS_{\mathcal{R},n,m,q,2p-1}$ problem. Let \mathbf{A} be an instance of $SIS_{\mathcal{R},n,m,q,2p-1}$. If $\mathbf{x}, \mathbf{x}' \in \mathcal{R}_q^n$ are distinct vectors such that $f_{\mathbf{A}}(\mathbf{x}) = f_{\mathbf{A}}(\mathbf{x}')$, write $\mathbf{u} = -\mathbf{G}^{-1}(\mathbf{x})$ and $\mathbf{u}' = -\mathbf{G}^{-1}(\mathbf{x}')$, we have $\mathbf{A} \cdot \mathbf{u} = \mathbf{A} \cdot \mathbf{u}' \mod q$. In other words, we have $\mathbf{A} \cdot (\mathbf{u} - \mathbf{u}') = \mathbf{0} \mod q$ and $\mathbf{u} - \mathbf{u}' \in \mathcal{R}_{2p-1}^m$.

Note that the same proof shows that $f_{\mathbf{A}}$ is one-way. Next, we show that the function $f_{\mathbf{A}}$ provably maps uniform distributions to distributions statistically or computationally close to uniform for certain parameter settings. It then follows from a standard hybrid argument that $f_{\mathbf{A}}^T$ also maps uniform distributions to near-uniform distributions for any polynomial T. First, we show that if qis super-polynomial and is smaller than a sufficiently large power of p by an additive polynomial factor, then the above claim holds statistically.

Theorem 5.3 (Uniformity Preserving for Large $q \leq p^k$). Let q be a prime of the form $q = p^k - r$ where $k > \log_p q + 2\lambda/n$, $r = \text{poly}(\lambda)$, $0 < r < p^k - p^{k-1}$, and $1/q = \text{negl}(\lambda)$. The following distributions are statistically close in λ :

$$\left\{\mathbf{y}:\mathbf{y} \leftarrow \$ \, \mathcal{R}_q^n\right\} \approx \left\{f_{\mathbf{A}}(\mathbf{x}): \mathbf{A} \leftarrow \$ \, \mathcal{R}_q^{n \times m}, \mathbf{x} \leftarrow \$ \, \mathcal{R}_q^n\right\}.$$

Proof. We first show that the distributions

$$\left\{\mathbf{u} \leftarrow \mathbf{R}_p^m\right\} \approx \left\{\mathbf{G}^{-1}(\mathbf{x}) : \mathbf{x} \leftarrow \mathbf{R}_q^n\right\}$$

are statistically close in λ . Let $d = \text{poly}(\lambda)$ be the degree of the ring \mathcal{R} . The statistical distance of the two distributions is given by

$$\begin{split} \Delta &\coloneqq \frac{1}{2} \cdot \left(q^{dn} \cdot \left| \frac{1}{p^{dm}} - \frac{1}{q^{dn}} \right| + (p^{dm} - q^{dn}) \cdot \frac{1}{p^{dm}} \right) \\ &= \frac{1}{2} \cdot \left(1 - \frac{q^{dn}}{p^{dm}} + 1 - \frac{q^{dn}}{p^{dm}} \right) \\ &= 1 - \left(\frac{q^n}{p^m} \right)^d. \end{split}$$

Note that $m = n \cdot \lceil \log_p q \rceil = nk$. Since $p^k > q$ and $(1+x)^n \ge 1 + nx$ for all $n \in \mathbb{N}$ and $x \ge -1$, we have

$$\left(\frac{q^n}{p^m}\right)^d = \left(\frac{q^n}{q^{nk}}\right)^d = \left(\frac{q}{p^k}\right)^{dn} = \left(\frac{p^k - r}{p^k}\right)^{dn} = \left(1 - \frac{r}{p^k}\right)^{dn} > \left(1 - \frac{r}{q}\right)^{dn} \\ \ge 1 - \frac{rdn}{q} \ge 1 - \operatorname{negl}(\lambda).$$

In other words, we have $\Delta \leq \operatorname{negl}(\lambda)$. Since $k > \log_p q + 2\lambda/n$, we have $m = nk > n \log_p q + 2\lambda$. The result then follows from the leftover hash lemma (Lemma 4.1).

Next, we show that if q is a power of p and an LWE assumption with uniform noise holds, then the claim holds computationally.

Theorem 5.4 (Uniformity Preserving for $q = p^k$). Let $q = p^k$ for some $k \in \mathbb{N}$. If the LWE_{*R*,*n*,*m*,*q*,*U*(*R*_{*p*}) assumption holds for m = nk, then the following distributions are computationally indistinguishable:}

$$\left\{\mathbf{y}:\mathbf{y}\leftarrow \mathbb{R}\mathcal{R}_q^n
ight\}pprox\left\{f_{\mathbf{A}}(\mathbf{x}):\mathbf{A}\leftarrow \mathbb{R}\mathcal{R}_q^{n imes m},\mathbf{x}\leftarrow \mathbb{R}\mathcal{R}_q^n
ight\}.$$

Proof. Since $q = p^k$ is a power of p, \mathbf{G}^{-1} is a bijection and thus the following distributions are identical:

$$\left\{\mathbf{u} \leftarrow \mathfrak{R}_p^m\right\} \equiv \left\{\mathbf{G}^{-1}(\mathbf{x}) : \mathbf{x} \leftarrow \mathfrak{R}_q^n\right\}$$

The result then follows from the $LWE_{\mathcal{R},n,m,q,U(\mathcal{R}_p)}$ assumption.

We remark that the above proof would still go through for other choices of q, by making an LWE assumption with skewed uniform noise, i.e. $U((\mathbf{g}^{\mathsf{T}})^{-1}(\mathcal{R}_q))$.

More Heuristic Evidence. We offer more heuristic evidence that the function is indeed sequential. First, it was shown in [JMRR21] that a fully homomorphic encryption scheme (FHE) can be used to show the existence of a *universal* sequential function, i.e. a function that is sequential if and only if sequential functions exist at all. The evaluation algorithm of this construction consists of running an empty circuit homomorphically. Looking at a specific instantiation of an FHE scheme [GSW13], the homomorphic evaluation algorithm consists exclusively of linear operations (over some ring), interleaved with binary decomposition. This bears strong resemblance with our candidate function, which also interleaves linear operations with p-ary decomposition, albeit with a fixed matrix **A**. In this sense, our candidate can be seen as the *minimal* non-trivial operation that is performed in the FHE evaluation, which we conjecture to be already secure.

Another evidence for the cryptographic usefulness of binary decomposition is the recent work of Chen et al. [CLMQ21] which shows that the binary decomposition operator can in some cases be used as a sound alternative to the Fiat-Shamir transformation, which is normally instantiated using a random oracle.³ Here the heuristic argument that we propose is that binary decomposition bears similarities with random oracles (in the sense that they can be both used for Fiat-Shamir) and random oracles are known to be sequential. Thus, we can conjecture that binary decomposition also bears sequentiality properties.

5.2 Cryptanalysis

We discuss some attack strategies and why they do not apply to our candidate sequential function. In Appendix A, we summarise attacks discovered by other authors.

Finding Associative Structure. One simple approach to attack the sequentiality of our scheme would be to find some associative structure in the computation. For example, say we omitted the decomposition operator \mathbf{G}^{-1} from the definition of $f_{\mathbf{A}}$ (adjusting the parameters suitably), then one could use the associativity of matrix multiplication to parallelise the computation, since the function

$$g_{\mathbf{A}}^{T}(\mathbf{x}) = \underbrace{\mathbf{A} \cdot \mathbf{A} \cdots \mathbf{A}}_{T\text{-times}} \cdot \mathbf{x} \mod q$$

can be computed in parallel time $O(\log(T))$ by computing the matrix products in a tree fashion. However, the same attack does not appear to be viable once we interleave each multiplication with the operator \mathbf{G}^{-1} , since the composition of these two operations is not associative.

³Although the signature scheme presented in [CLMQ21] actually relies on random oracles, it is only used to upgrade random-message unforgeability to existential unforgeability, while the use of random oracles for the Fiat-Shamir transformation is eliminated.

Gluing Parallel Threads. Another (related) attack strategy is to glue together two parallel computation transcripts. For example, suppose T = 2t + 1, the adversary may sample a random $\mathbf{x}^* \leftarrow \$ \mathcal{R}_q^n$ declare it to be output of the function at time t + 1. Then it would spawn two parallel threads computing $\mathbf{x}_t \leftarrow f_{\mathbf{A}}^t(\mathbf{x})$ and $\mathbf{y} \leftarrow f_{\mathbf{A}}^t(\mathbf{x}^*)$. To obtain a consistent transcript, the adversary must now find a vector $\mathbf{u}_t \in \mathcal{R}^m$ such that:

$$\begin{pmatrix} \mathbf{G} \\ \mathbf{A} \end{pmatrix} \cdot \mathbf{u}_t = \begin{pmatrix} -\mathbf{x}_t \\ \mathbf{x}^* \end{pmatrix} \mod q \qquad \text{and} \qquad \mathbf{u}_t \in \mathcal{R}^m_\beta$$

which is not easier than solving $SIS_{\mathcal{R},n,m,q,\beta}$. Note that this attack is only plausible when the solution to the sequential relation is not unique, e.g. when $\beta > p/2$.

5.3 Verifiable Delay Functions

We shall remark that our sequential function can be combined with a succinct non-interactive argument with a (quasi-)linear-time prover to obtain a verifiable delay function. While this is a known implication [DGMV20], we explicitly mention this here since the statement to be proven has a particularly simple form. Specifically, for an input instance \mathbf{x} and an output \mathbf{y} the prover only needs to show the existence of a vector \mathbf{u} such that:

$$\begin{pmatrix} \mathbf{G} & & \\ \mathbf{A} & \mathbf{G} & \\ & \mathbf{A} & \ddots & \\ & & \ddots & \mathbf{G} \\ & & & \mathbf{A} \end{pmatrix} \cdot \mathbf{u} = \begin{pmatrix} -\mathbf{x} \\ \mathbf{0} \\ \vdots \\ \vdots \\ \mathbf{0} \\ \mathbf{y} \end{pmatrix} \mod q \qquad \text{and} \qquad \mathbf{u} \in \mathcal{R}_p^{mT}.$$

In other words, the statement to be proven consists of a highly structured linear relation and a bounded-norm or set-membership constraint. For small p, e.g. p = 2, and ring \mathcal{R} of low degree, e.g. $\mathcal{R} = \mathbb{Z}$, the latter can be viewed as a simple low-degree relation $(\prod_{a \in \mathcal{R}_p} (u_i - a) = 0)_{i=1}^{mT}$ which reduces to $(u_i \cdot (u_i - 1) = 0)_{i=1}^{mT}$ for $(p, \mathcal{R}) = (2, \mathbb{Z})$. We expect that recent constructions of efficient succinct arguments for structured relations, e.g. [BSCG⁺19, CLM23], can efficiently prove statements of this form without too much overhead needed to manipulate the statement. We leave exploring the concrete efficiency of this approach as future work.

6 Proof of Sequential Work

We recall the definition of proofs of sequential work (PoSW) and present a construction based on the new lattice-based sequential relation. Due to the attacks by Attema and Ducas [AD23] and by Peikert and Tang [PT23] against the SIS-sequentiality assumption, the construction is not known to be provably secure against any simpler assumption. Moreover, we warn that due to another attack of Peikert and Tang [PT23] against a close variant of the PoSW, whatever security the construction below has might be fragile.

6.1 Definitions

We recall the definition of a proof of sequential work (PoSW).

Gen(pp)	$\langle Eval(x,1^T),Verify(x,T)\rangle$
$\overline{\mathbf{A} \! \leftarrow \! \$ \mathcal{R}_q^{n imes m}}$	Eval :
$\mathbf{x} \leftarrow \$ \mathcal{R}_q^n$	$\mathbf{x}_0 := \mathbf{x}$
$x \coloneqq (\mathbf{A}, \mathbf{x})$	for $i \in \{0, \dots, T-1\}$ do
return ×	$\mathbf{u}_i := -\mathbf{G}^{-1}(\mathbf{x}_i)$
	$\mathbf{x}_{i+1} := \mathbf{A} \cdot \mathbf{u}_i \bmod q$
	$wit \coloneqq (\mathbf{u}_i)_{i=0}^{T-1} \mathbf{send} \ \mathbf{y} := \mathbf{x}_T$
	$\langle Eval, Verify \rangle$:
	$params\coloneqq\mathbf{A}$
	$stmt := (\mathbf{x}, \mathbf{y}, p, T)$
	for $j \in [\lambda/\log \lambda]$ do
	$b_j \leftarrow \langle \mathcal{P}(params,stmt,wit), \mathcal{V}(params,stmt) angle$
	$Verify:\mathbf{return}(b_1\wedge\ldots\wedge b_{\lambda/\log\lambda})$

Figure 1: Construction of proof of sequential work.

Definition 6.1 ((Interactive) Proof of Sequential Work (PoSW)). An (interactive) proof of sequential work (PoSW) is a tuple of PPT algorithms/protocols (Gen, (Eval, Verify)) with the following syntax:

- $x \leftarrow \text{Gen}(1^{\lambda})$: The instance generation algorithm inputs the security parameter $\lambda \in \mathbb{N}$ and generates a problem instance x.
- $b \leftarrow \langle \mathsf{Eval}(\mathsf{x}, 1^T), \mathsf{Verify}(\mathsf{x}, T) \rangle$: The evaluation-verification protocol is run between the the interactive evaluation and verification algorithms. Both algorithms input an instance x . The evaluation algorithm further inputs a time parameter 1^T in unary while the verification algorithm inputs T in binary. The protocol terminates when the verification algorithm returns a bit $b \in \{0, 1\}$.

A PoSW is required to satisfy the following properties:

Efficiency. For any $x \in \text{Gen}(1^{\lambda})$, the circuit-depth of Eval (as a function of (λ, T)) satisfies

$$\mathsf{Depth}(\mathsf{Eval}(\cdot, 1^T)) = T \cdot \mathsf{poly}(\lambda).$$

Completeness. For any $\lambda \in \mathbb{N}$, $x \in \text{Gen}(1^{\lambda})$, and $T \in \mathbb{N}$, it holds that

$$\langle \mathsf{Eval}(\mathsf{x}, 1^T), \mathsf{Verify}(\mathsf{x}, T) \rangle = 1.$$

Sequential Soundness. Let $\sigma : \mathbb{N} \to \mathbb{N}$ be parametrised by λ . The PoSW is said to be sequentialsound with sequentiality σ if, for any pair of PPT adversaries $(\mathcal{A}_0, \mathcal{A}_1)$, it holds that

$$\Pr\begin{bmatrix} \langle \mathcal{A}_1(\mathsf{x}), \mathsf{Verify}(\mathsf{x}, T) \rangle = 1 & \mathsf{x} \leftarrow \mathsf{Gen}(1^{\lambda}) \\ \wedge \mathsf{Depth}(\mathcal{A}_1) < \sigma(T)) & \mathsf{(st}, T) \leftarrow \mathcal{A}_0(1^{\lambda}) \end{bmatrix} \leq \mathsf{negl}(\lambda).$$

6.2 Construction

Let $S \subseteq \mathcal{R}$ be a subtractive set where ||r|| = 1 for all $r \in S$. We first construct a core protocol $\langle \mathcal{P}(\mathsf{params},\mathsf{stmt},\mathsf{wit}), \mathcal{V}(\mathsf{params},\mathsf{stmt}) \rangle$, where $\mathsf{params},\mathsf{stmt},\mathsf{wit}$ are respectively parameters, statements, and witnesses of the form

params =
$$\mathbf{A}$$
, stmt = $(\mathbf{x}, \mathbf{y}, \beta, T)$, wit = $(\mathbf{u}_i)_{i=0}^{T-1}$,

for proving the relation

$$\mathbf{A}_T \mathbf{u} = (-\mathbf{x}, \mathbf{0}, \dots, \mathbf{0}, \mathbf{y}) \mod q$$
 and $\mathbf{u} \in \mathcal{R}_{\beta}^{mT}$

recursively as follows:

• If T = 1, \mathcal{P} sends \mathbf{u}_0 and \mathcal{V} returns 1 if

$$\begin{pmatrix} \mathbf{G} \\ \mathbf{A} \end{pmatrix} \cdot \mathbf{u}_0 = \begin{pmatrix} -\mathbf{x} \\ \mathbf{y} \end{pmatrix} \mod q \qquad \text{and} \qquad \mathbf{u}_0 \in \mathcal{R}^m_\beta$$

• If T = 2t > 1:

- \mathcal{P} sends \mathbf{u}_{T-1} .
- \mathcal{V} checks that

$$\mathbf{A} \cdot \mathbf{u}_{T-1} = \mathbf{y} \mod q$$
 and $\mathbf{u}_{T-1} \in \mathcal{R}^m_\beta$

and returns 0 if not.

- $-\mathcal{P}$ and \mathcal{V} compute $\mathbf{y}' = -\mathbf{G} \cdot \mathbf{u}_{T-1}$ and set $\mathsf{stmt}' \coloneqq (\mathbf{x}, \mathbf{y}', \beta, T-1)$.
- \mathcal{P} sets wit' $\coloneqq (\mathbf{u}_i)_{i=0}^{T-2}$.
- Run $\langle \mathcal{P}(\mathsf{params},\mathsf{stmt}',\mathsf{wit}'), \mathcal{V}(\mathsf{params},\mathsf{stmt}') \rangle$.

• If T = 2t + 1 > 1:

- \mathcal{P} sends \mathbf{u}_t .
- \mathcal{V} checks that $\mathbf{u}_t \in \mathcal{R}^m_\beta$, returns 0 if not.
- $-\mathcal{V}$ samples $r \leftarrow S$ and sends r to \mathcal{P} .
- \mathcal{P} and \mathcal{V} compute the following:
 - * $\mathbf{x}' \coloneqq -\mathbf{x}_0 \mathbf{A} \cdot \mathbf{u}_t \cdot r \mod q.$
 - * $\mathbf{y}' \coloneqq \mathbf{x}_T \cdot r \mathbf{G} \cdot \mathbf{u}_t \mod q.$
 - * $\beta' \coloneqq 2 \gamma_{\mathcal{R}} \beta.$

$$* \mathsf{stmt}' \coloneqq (\mathbf{x}', \mathbf{y}', eta', t).$$

 $- \mathcal{P}$ computes

*
$$\mathbf{u}'_i \coloneqq \mathbf{u}_i + \mathbf{u}_{t+i+1} \cdot r$$
 for all $i \in \{0, \dots, t-1\}$
* wit' $\coloneqq (\mathbf{u}'_i)_{i=0}^{t-1}$.

 $- \operatorname{Run} \langle \mathcal{P}(\mathsf{params},\mathsf{stmt}',\mathsf{wit}'), \mathcal{V}(\mathsf{params},\mathsf{stmt}') \rangle.$

The PoSW protocol is then specified in Fig. 1.

Completeness. We show that the above core protocol and therefore the PoSW are complete.

It is easy to check that, given an instance (\mathbf{A}, \mathbf{x}) , the evaluator produces an output \mathbf{y} and a witness $\mathbf{u} = (\mathbf{u}_i)_{i=0}^{T-1}$ satisfying

$$\mathbf{A}_T \mathbf{u} = (-\mathbf{x}, \mathbf{0}, \dots, \mathbf{0}, \mathbf{y}) \mod q$$
 and $\mathbf{u} \in \mathcal{R}_p^{mT}$.

Indeed, by construction, we have for $i \in \{0, \ldots, T-1\}$,

$$\mathbf{u}_i \in -\mathbf{G}^{-1}(\mathbf{x}_i) \in \mathcal{R}_2^m,$$
$$\mathbf{G}\mathbf{u}_i = -\mathbf{x}_i \mod q,$$
$$\mathbf{A}\mathbf{u}_i = \mathbf{x}_{i+1} \mod q.$$

Therefore, for $i \in \{0, ..., T - 2\}$,

$$\mathbf{A}\mathbf{u}_i + \mathbf{G}\mathbf{u}_{i+1} = \mathbf{0} \bmod q.$$

Finally, by construction, we have

$$\mathbf{y} = \mathbf{x}_T = \mathbf{A}\mathbf{u}_{T-1} \mod q.$$

It remains to check that the core protocol is complete for the relation

$$\mathbf{A}_T \mathbf{u} = (-\mathbf{x}, \mathbf{0}, \dots, \mathbf{0}, \mathbf{y}) \mod q$$
 and $\mathbf{u} \in \mathcal{R}_{\beta}^{mT}$

for any β .

The cases T = 1 and T = 2t > 1 are obvious. For the case T = 2t + 1 > 1, observe the relations

$$\mathbf{A}_t \begin{pmatrix} \mathbf{u}_0 & \mathbf{u}_{t-1} \\ \vdots & \vdots \\ \mathbf{u}_{t+1} & \mathbf{u}_{2t} \end{pmatrix} = \begin{pmatrix} -\mathbf{x}_0 & -\mathbf{A} \cdot \mathbf{u}_t \\ \vdots & \vdots \\ -\mathbf{G}\mathbf{u}_t & \mathbf{x}_T \end{pmatrix} \mod q,$$
$$\mathbf{A}_t \begin{pmatrix} \mathbf{u}_0 + \mathbf{u}_{t-1} \cdot r \\ \vdots \\ \mathbf{u}_{t+1} + \mathbf{u}_{2t} \cdot r \end{pmatrix} = \begin{pmatrix} -\mathbf{x}_0 - \mathbf{A} \cdot \mathbf{u}_t \cdot r \\ \vdots \\ -\mathbf{G}\mathbf{u}_t + \mathbf{x}_T \cdot r \end{pmatrix} \mod q$$

where the folded witness $(\mathbf{u}_i + \mathbf{u}_{t+i+1} \cdot r)$ is of norm at most $2\gamma_{\mathcal{R}}\beta$. The claim thus follows by induction.

Soundness. As mentioned in the beginning of Section 6, our security proof of the PoSW is vacuous since it relies on an instantiation of the SIS-sequentiality assumption with parameters vulnerable to known attacks. We keep the original soundness analysis below for completeness.

In the following we show that the core protocol is (2, 2, ..., 2)-special sound. First, we recall the definition of special soundness and a useful fact from [AL21].

Definition 6.2 $((k_1, \ldots, k_{\mu})$ -out-of- (N_1, \ldots, N_{μ}) -Special Soundness [AF22]). Let $k_1, \ldots, k_{\mu}, N_1, \ldots, N_{\mu} \in \mathbb{N}$. A $(2\mu + 1)$ -round public-coin protocol $(\mathcal{P}, \mathcal{V})$ for relation Φ , where \mathcal{V} samples the *i*-th challenge from a set of cardinality $N_i \geq k_i$ for $i \in [\mu]$, is (k_1, \ldots, k_{μ}) -out-of- (N_1, \ldots, N_{μ}) -special-sound if there exists a polynomial-time algorithm that, on input a statement stmt and a (k_1, \ldots, k_{μ}) -tree of accepting transcripts, outputs a witness wit such that $(\mathsf{stmt}; \mathsf{wit}) \in \Phi$. We also say $(\mathcal{P}, \mathcal{V})$ is (k_1, \ldots, k_{μ}) -special-sound.

For the (standard) definitions of public-coin protocol and trees of accepting transcripts we refer to [AF22].

Lemma 6.3 ([AL21]). Let $\mathcal{R} = \mathbb{Z}[\zeta_{d+1}]$ be the (d+1)-th cyclotomic ring where (d+1) is prime. The set $S = \{\mu_1, \ldots, \mu_d\} \subseteq \mathcal{R}^{\times}$ where $\mu_i = (\zeta^i - 1)/(\zeta - 1)$ is subtractive, i.e. for any $r_0, r_1 \in S$ it holds that $(r_1 - r_0)^{-1} \in \mathcal{R}$. Furthermore, for any $r_0, r_1 \in S$, we have $\frac{r_0}{r_1 - r_0}, \frac{r_1}{r_1 - r_0}, \frac{1}{r_1 - r_0} \in \mathcal{R}_2$.

Lemma 6.4 (Special Soundness). The above folding argument is (2, 2, ..., 2)-special sound for the relation

$$\left\{ ((\mathbf{A}, \mathbf{x}_0, \mathbf{x}_T); \mathbf{u}) : \mathbf{A}_T \mathbf{u} = (-\mathbf{x}_0, \mathbf{0}, \dots, \mathbf{0}, \mathbf{x}_T) \mod q \land \mathbf{u} \in \mathcal{R}^{mT}_{(2\gamma_{\mathcal{R}})^{2\log T}\beta} \right\}.$$

Proof. In this proof, we focus on the (more interesting) special case where $T = 2^{\mu+1} - 1$ for some $\mu \in \mathbb{N}$, so that $\frac{T-1}{2} = 2^{\mu} - 1$ is also an odd integer. It is clear that for such T the above folding argument is $(2\mu + 1)$ -round. The general case can be dealt with analogously.

In the following, we construct an extractor \mathcal{E} which extracts a witness **u** given a $(2, \ldots, 2)$ -tree of accepting transcripts recursively from depth $i = \mu$ to depth i = 1. Let $T_i := 2^{\mu-i+1} - 1$ for $i \in \{0, \ldots, \mu\}$ so that $T_0 = T$ and $T_{\mu} = 1$. Note that $T_{i-1} = 2T_i + 1$ for all $i \in [\mu]$. Let node₀ and node₁ be siblings at depth-*i* associated with the challenges r_0 and r_1 respectively, and let node_{ϵ} be the parent node of node₀ and node₁. From the tree of accepting transcripts, \mathcal{E} fetches the vectors $\mathbf{x}_0^{(node)}, \mathbf{x}_{T_{depth(node)}}^{(node)}, \mathbf{u}_t^{(node)}$ associated to each node node $\in \{\text{node}_{\epsilon}, \text{node}_0, \text{node}_1\}$ recursively defined such that $\mathbf{x}_0^{\text{root}} = \mathbf{x}_0, \mathbf{x}_{T_0}^{\text{root}} = \mathbf{x}_T$, and

$$\begin{pmatrix} \mathbf{x}_0^{(\mathsf{node}_b)} \\ \mathbf{x}_{T_i}^{(\mathsf{node}_b)} \end{pmatrix} = \begin{pmatrix} \mathbf{x}_0^{(\mathsf{node}_\epsilon)} \\ -\mathbf{G} \cdot \mathbf{u}_{T_i}^{(\mathsf{node}_\epsilon)} \end{pmatrix} + \begin{pmatrix} \mathbf{A} \cdot \mathbf{u}_{T_i}^{(\mathsf{node}_\epsilon)} \\ \mathbf{x}_{T_{i-1}}^{(\mathsf{node}_\epsilon)} \end{pmatrix} \cdot r_b \bmod q.$$

Suppose the vector $(\mathbf{u}_0^{\mathsf{node}_b}, \ldots, \mathbf{u}_{T_i-1}^{\mathsf{node}_b})$ extracted at node_b for $b \in \{0, 1\}$ satisfies

$$\mathbf{A}_{T_i} \cdot \begin{pmatrix} \mathbf{u}_0^{\mathsf{node}_b} \\ \vdots \\ \mathbf{u}_{T_i-1}^{\mathsf{node}_b} \end{pmatrix} = \begin{pmatrix} -\mathbf{x}_0^{(\mathsf{node}_b)} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{x}_{T_i}^{(\mathsf{node}_b)} \end{pmatrix} \mod q \qquad \text{and} \qquad \begin{pmatrix} \mathbf{u}_0^{\mathsf{node}_b} \\ \vdots \\ \mathbf{u}_{T_i-1}^{\mathsf{node}_b} \end{pmatrix} \in \mathcal{R}_{(2\,\gamma_{\mathcal{R}})^{2\mu-i}\cdot\beta}^{mT_i}.$$

Expanding the expressions, the L.H.S. becomes

$$\mathbf{A}_{T_i} \cdot \begin{pmatrix} \mathbf{u}_0^{\mathsf{node}_b} \\ \vdots \\ \mathbf{u}_{T_i-1}^{\mathsf{node}_b} \end{pmatrix} = \begin{pmatrix} -\mathbf{x}_0^{(\mathsf{node}_\epsilon)} \\ \mathbf{0} \\ \vdots \\ \vdots \\ \mathbf{0} \\ -\mathbf{G} \cdot \mathbf{u}_{T_i}^{(\mathsf{node}_\epsilon)} \end{pmatrix} + \begin{pmatrix} -\mathbf{A} \cdot \mathbf{u}_{T_i}^{(\mathsf{node}_\epsilon)} \\ \mathbf{0} \\ \vdots \\ \vdots \\ \mathbf{0} \\ \mathbf{x}_T^{(\mathsf{node}_\epsilon)} \end{pmatrix} \cdot r_b \bmod q.$$

Let

$$\begin{pmatrix} \mathbf{u}_0 & \mathbf{u}_{t+1} \\ \vdots & \vdots \\ \mathbf{u}_{T_i-1} & \mathbf{u}_{T_{i-1}-1} \end{pmatrix} = \begin{pmatrix} \mathbf{u}_0^{\mathsf{node}_0} & \mathbf{u}_0^{\mathsf{node}_1} \\ \vdots & \vdots \\ \mathbf{u}_{T_i-1}^{\mathsf{node}_0} & \mathbf{u}_{T_i-1}^{\mathsf{node}_1} \end{pmatrix} \cdot \begin{pmatrix} \frac{r_1}{r_1-r_0} & \frac{-1}{r_1-r_0} \\ \frac{-r_0}{r_1-r_0} & \frac{1}{r_1-r_0} \end{pmatrix}.$$

It follows that

$$\mathbf{A}_{T_i} \cdot \begin{pmatrix} \mathbf{u}_0 & \mathbf{u}_{t+1} \\ \vdots & \vdots \\ \mathbf{u}_{T_i-1} & \mathbf{u}_{T_{i-1}-1} \end{pmatrix} = \begin{pmatrix} -\mathbf{x}_0^{(\mathsf{node}_{\epsilon})} & -\mathbf{A} \cdot \mathbf{u}_t^{(\mathsf{node}_{\epsilon})} \\ \mathbf{0} & \mathbf{0} \\ \vdots & \vdots \\ \mathbf{0} & \mathbf{0} \\ -\mathbf{G} \cdot \mathbf{u}_{T_i}^{(\mathsf{node}_{\epsilon})} & \mathbf{x}_{T_{i-1}}^{(\mathsf{node}_{\epsilon})} \end{pmatrix} \bmod q,$$

or equivalently

$$\mathbf{A}_{T_{i-1}} \cdot \begin{pmatrix} \mathbf{u}_0 \\ \vdots \\ \mathbf{u}_{T_{i-1}-1} \end{pmatrix} = \begin{pmatrix} -\mathbf{x}_0^{(\mathsf{node}_{\epsilon})} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{x}_{T_{i-1}}^{(\mathsf{node}_{\epsilon})} \end{pmatrix} \mod q,$$

and $(\mathbf{u}_0, \ldots, \mathbf{u}_{T-1}) \in \mathcal{R}_{(2\gamma_{\mathcal{R}})^{2\mu-i+1} \cdot \beta}$, where the inclusion is due to Lemma 6.3.

By recursion, \mathcal{E} extracts at the root node a vector $(\mathbf{u}_0, \ldots, \mathbf{u}_{T-1})$ satisfying

$$\mathbf{A}_{T}\begin{pmatrix}\mathbf{u}_{0}\\\vdots\\\vdots\\\mathbf{u}_{T-1}\end{pmatrix} = \begin{pmatrix}-\mathbf{x}_{0}\\\mathbf{0}\\\vdots\\\mathbf{0}\\\mathbf{x}_{T}\end{pmatrix} \mod q, \ \begin{pmatrix}\mathbf{u}_{0}\\\vdots\\\vdots\\\mathbf{u}_{T-1}\end{pmatrix} \in \mathcal{R}_{(2\gamma_{\mathcal{R}})^{2\mu}\beta}^{mT} \subset \mathcal{R}_{(2\gamma_{\mathcal{R}})^{2\log T}\beta}^{mT}$$

as desired.

Finally, we are ready to show that the construction is sound, which follows by invoking the extractor of the above protocol, which returns a valid computation transcript. Since the extractor runs in time sublinear in T, this contradicts the sequentiality of our function.

Theorem 6.5 (Soundness (Vacuous due to [PT23])). There exists $p(\lambda) \in \text{poly}(\lambda)$ and $\sigma'(T) = \sigma(T) \cdot p(\lambda)$ such that if $SIS_{\mathcal{R},n,m,q,\beta}$ assumption and the SIS-sequentiality assumption with sequentiality σ' hold, then the PoSW constructed in Fig. 1 is sequentially sound with sequentiality σ .

Sketch. The theorem follows from Lemma 6.4 and standard techniques. We provide a proof sketch. Since the above folding argument is (2, 2, ..., 2)-special-sound with a challenge set size of $\Omega(\lambda)$, it follows from [AF22] that the $(\lambda/\log \lambda)$ -fold parallel repetition of it is knowledge-sound with negligible knowledge error. Furthermore, we observe that the extractor constructed in [AF22] is depth-preserving, i.e. there exists a polynomial $p(\lambda) \in poly(\lambda)$ such that the knowledge extractor $\mathcal{E}_{\mathcal{A}}$ has depth $\mathsf{Depth}(\mathcal{E}_{\mathcal{A}}) \leq p(\lambda) \cdot \mathsf{Depth}(\mathcal{A})$. Suppose there exists a polynomial-size adversary \mathcal{A} which breaks the sequential-soundness of the PoSW with sequentiality σ , then the above shows that $\mathcal{E}_{\mathcal{A}}$ is a polynomial-size adversary which breaks the SIS-sequentiality assumption with sequentiality σ' . \Box

In Appendix B, we discuss challenges of formally proving the security of our PoSW against quantum adversaries.

Acknowledgments

The authors wish to thank Andrej Bogdanov and Alon Rosen for insightful discussions and for comments on an earlier draft of this work. The authors are also grateful to the anonymous reviewers for suggesting the preprocessing attack described in Section 5.2. G.M. wishes to thank Chis Peikert for discussions on the sequentiality assumption. R.L. wishes to thank Thomas Attema for sharing an earlier draft of his attack. G.M. is partially funded by the German Federal Ministry of Education and Research (BMBF) in the course of the 6GEM research hub under grant number 16KISK038, by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972, and by the European Research Council through an ERC Starting Grant (Grant agreement No. 101077455, ObfusQation).

References

- [ACK21] Thomas Attema, Ronald Cramer, and Lisa Kohl. A compressed Σ-protocol theory for lattices. In Tal Malkin and Chris Peikert, editors, CRYPTO 2021, Part II, volume 12826 of LNCS, pages 549–579, Virtual Event, August 2021. Springer, Heidelberg.
- [AD23] Thomas Attema and Léo Ducas. Personal communication, 2023.
- [AF22] Thomas Attema and Serge Fehr. Parallel repetition of (k_1, \ldots, k_{μ}) -special-sound multi-round interactive proofs. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 415–443. Springer, Heidelberg, August 2022.
- [AFK22] Thomas Attema, Serge Fehr, and Michael Klooß. Fiat-shamir transformation of multiround interactive proofs. In Eike Kiltz and Vinod Vaikuntanathan, editors, TCC 2022, Part I, volume 13747 of LNCS, pages 113–142. Springer, Heidelberg, November 2022.
- [Ajt96] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In 28th ACM STOC, pages 99–108. ACM Press, May 1996.
- [AL21] Martin R. Albrecht and Russell W. F. Lai. Subtractive sets over cyclotomic rings limits of Schnorr-like arguments over lattices. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part II*, volume 12826 of *LNCS*, pages 519–548, Virtual Event, August 2021. Springer, Heidelberg.
- [BBBF18] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In Hovav Shacham and Alexandra Boldyreva, editors, CRYPTO 2018, Part I, volume 10991 of LNCS, pages 757–788. Springer, Heidelberg, August 2018.
- [BCH⁺22] Nir Bitansky, Arka Rai Choudhuri, Justin Holmgren, Chethan Kamath, Alex Lombardi, Omer Paneth, and Ron D. Rothblum. PPAD is as hard as LWE and iterated squaring. In Eike Kiltz and Vinod Vaikuntanathan, editors, TCC 2022, Part II, volume 13748 of LNCS, pages 593–622. Springer, Heidelberg, November 2022.
- [BD21] Jeffrey Burdges and Luca De Feo. Delay encryption. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 302–326. Springer, Heidelberg, October 2021.

- [BGJ⁺16] Nir Bitansky, Shafi Goldwasser, Abhishek Jain, Omer Paneth, Vinod Vaikuntanathan, and Brent Waters. Time-lock puzzles from randomized encodings. In Madhu Sudan, editor, *ITCS 2016*, pages 345–356. ACM, January 2016.
- [BJRW20] Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. Towards classical hardness of module-LWE: The linear rank case. In Shiho Moriai and Huaxiong Wang, editors, ASIACRYPT 2020, Part II, volume 12492 of LNCS, pages 289–317. Springer, Heidelberg, December 2020.
- [BLNS20] Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. A non-PCP approach to succinct quantum-safe zero-knowledge. In Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO 2020, Part II, volume 12171 of LNCS, pages 441–469. Springer, Heidelberg, August 2020.
- [BN00] Dan Boneh and Moni Naor. Timed commitments. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 236–254. Springer, Heidelberg, August 2000.
- [BR23] Andrej Bogdanov and Alon Rosen. Personal communication, 2023.
- [BSCG⁺19] Eli Ben-Sasson, Alessandro Chiesa, Lior Goldberg, Tom Gur, Michael Riabzev, and Nicholas Spooner. Linear-size constant-query iops for delegating computation. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography (TCC)*, 2019.
- [CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta. Lattice-based succinct arguments from vanishing polynomials - (extended abstract). In Helena Handschuh and Anna Lysyanskaya, editors, CRYPTO 2023, Part II, volume 14082 of LNCS, pages 72–105. Springer, Heidelberg, August 2023.
- [CLMQ21] Yilei Chen, Alex Lombardi, Fermi Ma, and Willy Quach. Does fiat-shamir require a cryptographic hash function? In Tal Malkin and Chris Peikert, editors, CRYPTO 2021, Part IV, volume 12828 of LNCS, pages 334–363, Virtual Event, August 2021. Springer, Heidelberg.
- [CMS19] Alessandro Chiesa, Peter Manohar, and Nicholas Spooner. Succinct arguments in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, TCC 2019, Part II, volume 11892 of LNCS, pages 1–29. Springer, Heidelberg, December 2019.
- [CP18] Bram Cohen and Krzysztof Pietrzak. Simple proofs of sequential work. In Jesper Buus Nielsen and Vincent Rijmen, editors, EUROCRYPT 2018, Part II, volume 10821 of LNCS, pages 451–467. Springer, Heidelberg, April / May 2018.
- [CSRT22] Jorge Chávez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi. Verifiable isogeny walks: Towards an isogeny-based postquantum VDF. In Riham AlTawy and Andreas Hülsing, editors, SAC 2021, volume 13203 of LNCS, pages 441–460. Springer, Heidelberg, September / October 2022.
- [DGMV20] Nico Döttling, Sanjam Garg, Giulio Malavolta, and Prashant Nalini Vasudevan. Tight verifiable delay functions. In Clemente Galdi and Vladimir Kolesnikov, editors, SCN 20, volume 12238 of LNCS, pages 65–84. Springer, Heidelberg, September 2020.

- [DLM19] Nico Döttling, Russell W. F. Lai, and Giulio Malavolta. Incremental proofs of sequential work. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part II*, volume 11477 of *LNCS*, pages 292–323. Springer, Heidelberg, May 2019.
- [DMPS19] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai, editors, ASIACRYPT 2019, Part I, volume 11921 of LNCS, pages 248–277. Springer, Heidelberg, December 2019.
- [FS87] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, CRYPTO'86, volume 263 of LNCS, pages 186–194. Springer, Heidelberg, August 1987.
- [GGH96] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Collision-free hashing from lattice problems. Cryptology ePrint Archive, Report 1996/009, 1996. https://eprint.iacr. org/1996/009.
- [GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, CRYPTO 2013, Part I, volume 8042 of LNCS, pages 75–92. Springer, Heidelberg, August 2013.
- [JMRR21] Samuel Jaques, Hart Montgomery, Razvan Rosie, and Arnab Roy. Time-release cryptography from minimal circuit assumptions. In Avishek Adhikari, Ralf Küsters, and Bart Preneel, editors, *INDOCRYPT 2021*, volume 13143, pages 584–606. Springer, 2021.
- [LM23] Russell W. F. Lai and Giulio Malavolta. Lattice-based timed cryptography. In Helena Handschuh and Anna Lysyanskaya, editors, CRYPTO 2023, Part V, volume 14085 of LNCS, pages 782–804. Springer, Heidelberg, August 2023.
- [LMS22] Russell W. F. Lai, Giulio Malavolta, and Nicholas Spooner. Quantum rewinding for many-round protocols. In Eike Kiltz and Vinod Vaikuntanathan, editors, TCC 2022, Part I, volume 13747 of LNCS, pages 80–109. Springer, Heidelberg, November 2022.
- [LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, EUROCRYPT 2010, volume 6110 of LNCS, pages 1–23. Springer, Heidelberg, May / June 2010.
- [LPS17] Huijia Lin, Rafael Pass, and Pratik Soni. Two-round and non-interactive concurrent non-malleable commitments from time-lock puzzles. In Chris Umans, editor, 58th FOCS, pages 576–587. IEEE Computer Society Press, October 2017.
- [MMV13] Mohammad Mahmoody, Tal Moran, and Salil P. Vadhan. Publicly verifiable proofs of sequential work. In Robert D. Kleinberg, editor, *ITCS 2013*, pages 373–388. ACM, January 2013.
- [MT19] Giulio Malavolta and Sri Aravinda Krishnan Thyagarajan. Homomorphic time-lock puzzles and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 620–649. Springer, Heidelberg, August 2019.

- [Pie19] Krzysztof Pietrzak. Simple verifiable delay functions. In Avrim Blum, editor, ITCS 2019, volume 124, pages 60:1–60:15. LIPIcs, January 2019.
- [PT23] Chris Peikert and Yi Tang. Cryptanalysis of lattice-based sequentiality assumptions and proofs of sequential work. *IACR Cryptol. ePrint Arch.*, page 1880, 2023.
- [Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, 37th ACM STOC, pages 84–93. ACM Press, May 2005.
- [RSW96] Ronald L. Rivest, Adi Shamir, and David A. Wagner. Time-lock puzzles and timedrelease crypto. Technical report, 1996.
- [Unr16] Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 497–527. Springer, Heidelberg, May 2016.
- [Val08] Paul Valiant. Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In Ran Canetti, editor, TCC 2008, volume 4948 of LNCS, pages 1–18. Springer, Heidelberg, March 2008.
- [vdf19] Vdf alliance, 2019. Accessed in June 2023.

A Attacks against SIS-Sequentiality

In [LM23], it was implicitly assumed that the SIS-sequentiality assumption (Assumption 5.1) holds for any choice of β and σ with $\sigma(T) = (1 - \omega(1)) \cdot T \cdot \text{poly}(\lambda)$. In particular, the sequential-soundness of the PoSW was proven in [LM23] based on the assumption with $\beta = (2\gamma_R)^{2\log T} \cdot p$. Below, we discuss attacks against the SIS-sequentiality assumption and its "offline" variant.

Offline Preprocessing Attack. This attack is suggested to us by anonymous reviewers. Let us start with the simplified settings where we *fix* the matrix **A**, instead of sampling it as part of the instance (\mathbf{A}, \mathbf{x}) . The idea of the attack is to precompute a witness for $(\mathbf{A}, p^i \cdot \mathbf{e}_j)$, for $i = 0, \ldots, \lceil \log_p q \rceil - 1$ and $j = 1, \ldots, n$ and where $\mathbf{e}_j \in \{0, 1\}^n$ denotes the *j*-th unit vector. Let us denote the (i, j)-th precomputed witness by $(\mathbf{u}_0^{(i,j)}, \ldots, \mathbf{u}_{T-1}^{(i,j)}, \mathbf{y}^{(i,j)})$. Note that $\mathbf{u}_k^{(i,j)} \in \mathcal{R}_p^m$. Upon receiving $\mathbf{x} \in \mathcal{R}_q^n$, decompose \mathbf{x} into

$$\mathbf{x} = \sum_{i=0}^{\left|\log_{p} q\right| - 1} \sum_{j=1}^{n} x^{(i,j)} \cdot p^{i} \cdot \mathbf{e}_{j}$$

where $x^{(i,j)} \in \mathcal{R}_p$. Set the witness to

$$(\mathbf{u}_0, \dots, \mathbf{u}_{T-1}, \mathbf{y}) := \sum_{i=0}^{\lceil \log_p q \rceil - 1} \sum_{j=1}^n x^{(i,j)} \cdot (\mathbf{u}_0^{(i,j)}, \dots, \mathbf{u}_{T-1}^{(i,j)}, \mathbf{y}^{(i,j)}).$$

Note that $\mathbf{u}_k \in \mathcal{R}^m_{\gamma_{\mathcal{R}}mp}$, and furthermore the parallel runtime of the attack (after the preprocessing phase) is $\log T \cdot \mathsf{poly}(\lambda)$. This would break a hypothetical version of our sequentiality assumption, where we fix **A** for all instances, for $\beta = \gamma_{\mathcal{R}}mp$ and $\sigma = \log T \cdot \mathsf{poly}(\lambda)$.

Online Preprocessing Attack. Next, we describe an online attack by Attema and Ducas [AD23] which, given an instance (\mathbf{A}, \mathbf{x}) , finds a solution (\mathbf{y}, \mathbf{u}) with $\mathbf{u} \in \mathcal{R}_{\gamma \mathcal{R} m p}^{mT}$ in depth $\sqrt{T} \log T \cdot \mathsf{poly}(\lambda)$.

The attack consists of a preprocessing phase and an iterative phase. Upon receiving (\mathbf{A}, \mathbf{x}) and denoting $\mathbf{x}_0 \coloneqq \mathbf{x}$, perform the above preprocessing on \mathbf{A} for \sqrt{T} steps to compute witnesses $(\mathbf{u}_0^{(i,j)}, \ldots, \mathbf{u}_{\sqrt{T-1}}^{(i,j)}, \mathbf{y}^{(i,j)})$ for $i = 0, \ldots, \lceil \log_p q \rceil - 1$ and $j = 1, \ldots, n$. Then, in the iterative phase, for $\ell = 1, \ldots, \sqrt{T}$, decompose

$$\mathbf{x}_{(\ell-1)\sqrt{T}} = \sum_{i=0}^{\left\lceil \log_p q \right\rceil - 1} \sum_{j=1}^n x_{(\ell-1)\sqrt{T}}^{(i,j)} \cdot p^i \cdot \mathbf{e}_j$$

and compute

$$(\mathbf{u}_{(\ell-1)\sqrt{T}},\ldots,\mathbf{u}_{\ell\sqrt{T}-1},\mathbf{x}_{\ell\sqrt{T}}) := \sum_{i=0}^{\lceil \log_p q \rceil - 1} \sum_{j=1}^n x_{(\ell-1)\sqrt{T}}^{(i,j)} \cdot (\mathbf{u}_0^{(i,j)},\ldots,\mathbf{u}_{\sqrt{T}-1}^{(i,j)},\mathbf{y}^{(i,j)})$$

Finally, output $(\mathbf{x}_T, \mathbf{u})$, where $\mathbf{u}^{\mathsf{T}} := (\mathbf{u}_0^{\mathsf{T}}, \dots, \mathbf{u}_{T-1}^{\mathsf{T}})$.

Clearly, for each k = 1, ..., T, we have $\mathbf{u}_k \in \mathcal{R}^m_{\gamma_{\mathcal{R}}mp}$ as in the preprocessing attack. For the runtime, note that the preprocessing of \mathbf{A} for \sqrt{T} steps takes takes depth $\sqrt{T} \cdot \mathsf{poly}(\lambda)$. Then, each of

the \sqrt{T} iterative steps takes $\log T \cdot \mathsf{poly}(\lambda)$ depth. The entire attack therefore takes $\sqrt{T} \log T \cdot \mathsf{poly}(\lambda)$ depth.

We remark that the above attack seems to rely on the sparsity of the image

$$\begin{pmatrix} -\mathbf{x}_0^{\mathsf{T}} & \mathbf{0}^{\mathsf{T}} & \dots & \mathbf{0}^{\mathsf{T}} & \mathbf{x}_T^{\mathsf{T}} \end{pmatrix}^{\mathsf{T}}$$

and in particular that it can be decomposed into

$$\sum_{\ell=1}^{\sqrt{T}} \begin{pmatrix} \mathbf{0}^{\mathsf{T}} & \dots & \mathbf{0}^{\mathsf{T}} & -\mathbf{x}_{(\ell-1)\sqrt{T}}^{\mathsf{T}} & \mathbf{0}^{\mathsf{T}} & \dots & \mathbf{0}^{\mathsf{T}} & \mathbf{x}_{\ell\sqrt{T}}^{\mathsf{T}} & \mathbf{0}^{\mathsf{T}} & \dots & \mathbf{0}^{\mathsf{T}} \end{pmatrix}^{\mathsf{T}}.$$

Preimage Sampling Attack. We summarise a family of preimage sampling attacks by Peikert and Tang [PT23] which, given an instance (\mathbf{A}, \mathbf{x}) , finds a solution (\mathbf{y}, \mathbf{u}) with $\mathbf{u} \in \mathcal{R}_{(\gamma_{\mathcal{R}}m)^{(\log_k T)/2}}^{mT}$ in depth $k \log_k T \cdot \mathsf{poly}(\lambda)$, for any $1 \le k \le T$. Note that the family of attacks is parameterised by a parameter k which describes a tradeoff between the parallel runtime and the norm of the solution. In particular, when $k = \sqrt{T}$, this attack has the same performance as that of Attema and Ducas.

In essence, the attack works by first computing a trapdoor of the matrix



and then using the trapdoor to sample a short preimage $\mathbf{u}^{\mathrm{T}} = (\mathbf{u}_{0}^{\mathrm{T}}, \dots, \mathbf{u}_{T-1}^{\mathrm{T}})$ such that

$$\mathbf{B}_T \mathbf{u} = (-\mathbf{x}_0^\mathsf{T}, \mathbf{0}^\mathsf{T}, \dots, \mathbf{0}^\mathsf{T})^\mathsf{T} \bmod q.$$

The output is then (\mathbf{y}, \mathbf{u}) where $\mathbf{y} := \mathbf{A}\mathbf{u}_{T-1} \mod q$.

The computation of a trapdoor of \mathbf{B}_T is based on the following observation. For $i \in [k]$, let $\mathbf{C}_i \in \mathcal{R}_q^{nt_i \times mt_i}$ be matrices with trapdoors $\mathbf{R}_i \in \mathcal{R}^{mt_i \times mt_i}$ so that $\mathbf{C}_i \mathbf{R}_i = \mathbf{I}_{t_i} \otimes \mathbf{G} \mod q$. For $i, j \in [k]$ with i > j, let $\mathbf{W}_{i,j} \in \mathcal{R}_q^{nt_i \times mt_j}$ be arbitrary matrices. Define

$$\mathbf{C} := \begin{pmatrix} \mathbf{C}_1 & & \\ \mathbf{W}_{2,1} & \mathbf{C}_2 & \\ \vdots & \vdots & \ddots & \\ \mathbf{W}_{k,1} & \mathbf{W}_{k,2} \dots \dots \mathbf{C}_k \end{pmatrix}$$

Observe that the matrix

$$\mathbf{R} := \begin{pmatrix} \mathbf{R}_1 & & \\ & \mathbf{R}_2 & \\ & & \ddots & \\ & & & \mathbf{R}_k \end{pmatrix} \begin{pmatrix} \mathbf{I}_{mt_1} & & \\ \mathbf{S}_{2,1} & \mathbf{I}_{mt_2} & \\ \vdots & \vdots & \ddots & \\ \mathbf{S}_{k,1} & \mathbf{S}_{k,2} & \dots & \mathbf{I}_{mt_k} \end{pmatrix} = \begin{pmatrix} \mathbf{R}_1 & & \\ \mathbf{R}_2 \mathbf{S}_{2,1} & \mathbf{R}_2 & \\ \vdots & \vdots & \ddots & \\ \mathbf{R}_k \mathbf{S}_{k,1} & \mathbf{R}_k \mathbf{S}_{k,2} & \dots & \mathbf{R}_k \end{pmatrix}$$

where

$$\mathbf{S}_{i,j} := -(\mathbf{I}_{t_i} \otimes \mathbf{G})^{-1} (\mathbf{W}_{i,j} \mathbf{R}_j + \sum_{j < j' < i} \mathbf{W}_{i,j'} \mathbf{R}_{j'} \mathbf{S}_{j',j})$$

is a trapdoor of **C**, i.e. $\mathbf{CR} = \mathbf{I}_{\sum_{i=1}^{k} t_i} \otimes \mathbf{G} \mod q$. Given the above observation, the idea is to recursively decompose \mathbf{B}_T into k-by-k block matrices until arriving at the block matrix



whose diagonal blocks admit trivial trapdoors, i.e. $\mathbf{GI}_m = \mathbf{G}$.

We remark that the above attack, as pointed out by Peikert and Tang [PT23], is oblivious (up to minor optimisation) to the form of the image

$$\begin{pmatrix} -\mathbf{x}^{\mathsf{T}} & \mathbf{0}^{\mathsf{T}} & \dots & \mathbf{0}^{\mathsf{T}} \end{pmatrix}^{\mathsf{T}}$$

On Post-Quantum Security of our PoSW В

Formally showing that our PoSW is secure against quantum adversaries requires more work than what is presented in Section 6.2. A recent work [LMS22] shows that protocols that satisfy special soundness and a particular notion of binding for the hash function (called collapsing) can be proven secure against quantum adversary (when sequentially repeated). Unfortunately, their result is not sufficient for our purposes, since the depth of the extractor scales with the size of the extraction tree. which in particular means that it is polynomial in T. Thus, we cannot hope to use this extractor to derive a contradiction against the sequentiality of our function. We leave proving a precise statement in the quantum settings as a fascinating open question. As a first step towards this, in the following we show that the hash function used at each round of our protocol is collapsing. Here we assume familiarity with the basics of quantum information and we refer the reader to [LMS22] for precise definitions of the notions used here. First we recall below the notion of collapsing for hash functions [Unr16].

Definition B.1 (Collapsing). Let H be a (keyed) hash function. We say that H is collapsing if for any efficient (quantum) adversary \mathcal{A}

$$\left| \Pr \Big[\mathsf{Collapsing}^0_{\mathcal{A}}(1^{\lambda}) = 1 \Big] - \Pr \Big[\mathsf{Collapsing}^1_{\mathcal{A}}(1^{\lambda}) = 1 \Big] \right| \le \mathsf{negl}(\lambda),$$

where the experiment $\mathsf{Collapsing}^b_{\mathcal{A}}$ is defined as follows:

Collapsing $^{b}_{A}(1^{\lambda})$:

- Sample a key k and send it over to \mathcal{A} .
- \mathcal{A} replies with a classical bitstring y and a quantum state on a register \mathcal{X} .
- Let $U_{k,y}$ be the unitary that acts on \mathcal{X} and a fresh ancilla, and CNOTs into the fresh ancilla the bit that determines whether the output of $H_k(\cdot)$ equals y and the input belongs to the appropriate domain. Apply $U_{k,y}$, measure the ancilla, and apply $U_{k,y}^{\dagger}$.

- If the output of the measurement is 0, then abort the experiment. Else proceed.
- If b = 0 do nothing.
- If b = 1 measure the register \mathcal{X} in the computational basis, discard the result.
- Return to \mathcal{A} all registers and output whichever bit \mathcal{A} outputs.

In [LMS22] it is shown that the SIS-based hash function is collapsing, assuming the hardness of the LWE problem.

Lemma B.2 ([LMS22]). If the LWE problem is hard, then the function H_A defined as

$$\mathsf{H}_{\mathbf{A}}(\mathbf{u}) = \mathbf{A} \cdot \mathbf{u} \bmod q$$

where $\mathbf{A} \leftarrow \mathcal{R}_q^{n \times m}$, is collapsing.

We are now ready to prove that the hash function used in our folding argument is collapsing.

Lemma B.3 (Collapsing). Let t be a polynomial in the security parameter. If the LWE problem is hard, then the function H_A defined as



where $\mathbf{A} \leftarrow \mathcal{R}_q^{n \times m}$, is collapsing.

Proof. The proof follows by a standard hybrid argument. Let us split the input $\mathbf{u} \in \mathcal{R}_p^{tm}$ in t blocks $(\mathbf{u}_1, \ldots, \mathbf{u}_t)$ where $\mathbf{u}_i \in \mathcal{R}_p^m$ and let $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_t$ be the corresponding registers. In the last hybrid, the challenger does not measure any of the registers (this corresponds to $\mathsf{Collapsing}_{\mathcal{A}}^1$). The *i*-th hybrid is defined as the previous one, except that the challenger only measures registers $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_t$ in the computational basis. Note that the 0-th hybrid corresponds to the experiment $\mathsf{Collapsing}_{\mathcal{A}}^0$. What is left to be shown is that consequent hybrids are computationally indistinguishable.

For hybrids t and t - 1, indistinguishability follows directly from the collapsing property of **A** (Lemma B.2). For other hybrids, it suffices to observe that the *i*-th block of the output $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_t)$ is computed as:

$$\mathbf{y}_i = \mathbf{A} \cdot \mathbf{u}_i + \mathbf{G} \cdot \mathbf{u}_{i+1} \mod q$$
$$\mathbf{y}_i - \mathbf{G} \cdot \mathbf{u}_{i+1} = \mathbf{A} \cdot \mathbf{u}_i \mod q$$

and therefore indistinguishability follows one again by Lemma B.2, since \mathbf{u}_{i+1} can be computed as the result of the measurement on register \mathcal{X}_{i+1} (which we assume it is measured).