Towards better SNARGs for P from Fiat-Shamir

Yiding Zhang
IIIS, Tsinghua University
Beijing, China
zhangyd19@mails.tsinghua.edu.cn

August 29, 2022

Abstract

We study the problem of constructing succinct non-interactive arguments (SNARGs), an important tool in cryptography for delegating computations. In recent years, several results related to SNARGs have appeared due to the progress in provably instantiating the Fiat-Shamir transformation. In this note, we show that some techniques used in constructing SNARGs can be improved to work in more general settings, which may be useful in constructing better SNARGs or in some other applications in cryptography.

1 Introduction

Succinct non-interactive arguments (SNARGs) are protocols for generating a short certificate for the correctness of a long computation. Such protocols are closely related to the problem of delegating computation: a client delegates the computation task to a untrusted server with more computational resources, and receives the result of the computation together with a short certificate that allows much faster verification than computing again. Efforts in constructing SNARGs are mainly motivated by the real-world applications like cloud services or block chains.

In this note, we focus on SNARGs for the complexity class P shown in [CJJ21b], which is based on the standard LWE assumption (see section 2.2.1). The main components of [CJJ21b] are a somewhere extractable (SE) commitment with local opening (section 3), a PCP (section 2.3), and a hash function for Fiat-Shamir (section 2.5). In the following sections, we study the constructions of these components respectively and try to extend them to more general settings.

1.1 Our results

Our main focus is to construct SNARGs based on assumptions different from or weaker than known results, e.g., SNARGs based on only (subexponential) DDH. Unfortunately, we only get some partial results in this direction. In section 3, we show that SE commitment is known from many standard assumptions, and present a relaxed version of this commitment scheme; in section 4, we show a different method of instantiating Fiat-Shamir, allowing us to instantiate Fiat-Shamir for a broader class of interactive protocols; then in section 5, we define a special PCP that is still not known to exist, which is the main barrier to get better results.

1.2 Related works

In addition to [CJJ21b], some other recent works also showed constructions of SNARGs based on different standard cryptographic assumptions, e.g., [HJKS22; CJJ21a] based on discrete Diffie-Hellman (DDH) and quadratic residue (QR), and [WW22] based on groups with bilinear maps. Note that most of the constructions are done by first constructing a (interactive) succinct argument, and then applying Fiat-Shamir securely on the argument, while an exception is [WW22], which constructs a non-interactive protocol directly without Fiat-Shamir.

More recently, [Kal22] showed a bootstrapping result for SNARGs, allowing us to get SNARGs with optimal communication complexity from any SNARG with non-trivial communication complexity. This solves the problem that SNARGs from [HJKS22; CJJ21a; WW22] can only achieve a weaker level of succinctness than [CJJ21b].

2 Preliminaries

2.1 Notations

For any positive integer n, we define $[n] := \{1, 2, \ldots, n\}$. For any vector $\mathbf{x}$ of length n, for any $i \in [n]$, we define $\mathbf{x}_i$ to be its i-th element; also for any $S \subset [n]$, we define $\mathbf{x}_S := \{\mathbf{x}_i\}_{i \in S}$.

2.2 Basic cryptographic assumptions

In this section, we present the basic cryptographic assumptions that we will use.

2.2.1 The Learning with Errors assumption

The learning with errors (LWE) problem, first introduced in [Reg05], is an extremely versatile basis for constructing cryptographic tools, and is believed to be hard even against quantum computers.

Definition 2.1 (The Learning with Errors (LWE) assumption). Let χ be an arbitrary error distribution over $\mathcal{Z}$. For any positive integer n, q, and $m = \mathsf{poly}(n)$, the Learning with Errors assumption states that for any non-uniform PPT adversary $\mathcal{D}$, there exists a negligible function $\nu(\cdot)$ such that

$$\left| \Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m \times n} \\ s \leftarrow \mathbb{Z}_q^n \\ e \leftarrow \chi^m}} [\mathcal{D}(A, As + e) = 1] - \Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m \times n} \\ y \leftarrow \mathbb{Z}_q^m}} [\mathcal{D}(A, y) = 1] \right| \leq \nu(n).$$

In the standard LWE assumption, χ is chosen to be the discrete Gaussian distribution with parameter $r = 2\sqrt{n}$. ♢

2.2.2 Number theoretical assumptions

We first state the DDH assumption [DH76], which is defined with respect to groups. We say $\mathcal{G}$ is a (prime-order) group generator if it is a PPT algorithm that takes as input the security parameter 1^λ, outputs $(\mathbb{G}, p, g)$ where $\mathbb{G}$ is the description of a multiplication cyclic group, $p = |\mathbb{G}|$ is a prime number, and g is a generator of $\mathbb{G}$. The DDH assumption is the following:

Definition 2.2 (The Decisional Diffie-Hellman (DDH) assumption). We say a group generator $\mathcal{G}$ satisfies the Decisional Diffie-Hellman assumption if for any non-uniform PPT adversary $\mathcal{D}$, there exists a negligible function $\nu(\cdot)$ such that

$$\left| \Pr_{\substack{(\mathbb{G},p,g)\leftarrow\mathcal{G}(1^\lambda)\\ x,y\leftarrow\mathbb{Z}_p}}[\mathcal{D}(1^\lambda,\mathbb{G},p,g,g^x,g^y,g^{xy})=1] - \Pr_{\substack{(\mathbb{G},p,g)\leftarrow\mathcal{G}(1^\lambda)\\ x,y,z\leftarrow\mathbb{Z}_p}}[\mathcal{D}(1^\lambda,\mathbb{G},p,g,g^x,g^y,g^z)=1] \right| \leq \nu(\lambda).$$

♢

Then we state the QR assumption [GM82]. We say N is a Blum integer if $N = p \cdot q$ where p, q are prime integers satisfying $p \equiv q \equiv 3 \pmod 4$. Let $\mathbb{Z}_N^*$ be the multiplication group of integers from $1, 2, \ldots, N$ that are co-prime with N. Then we define $\mathbb{J}_N$ as the subgroup of $\mathbb{Z}_N^*$ with Jacobi symbol $+1$, and define $\mathbb{QR}_N$ as the subgroup of $\mathbb{Z}_N^*$ consisting of all the quadratic residues. Note that if N is a Blum integer, then $\mathbb{J}_N$ can be written as $\{\pm 1\} \times \mathbb{QR}_N$. Then the QR assumption is as follows.

Definition 2.3 (The Quadratic Residuosity (QR) assumption). Let $N \leq 2^\lambda$ be a uniformly sampled Blum integer. The Quadratic Residuosity (QR) Assumption states that for any non-uniform PPT adversary $\mathcal{D}$, there exists a negligible function $\nu(\cdot)$ such that

$$\left| \Pr_{a\leftarrow\mathbb{J}_N}[\mathcal{D}(1^\lambda,N,a)=1] - \Pr_{a\leftarrow\mathbb{QR}_N}[\mathcal{D}(1^\lambda,N,a)=1] \right| \leq \nu(\lambda).$$

♢

Note that the above assumptions can be strengthened to sub-exponential assumptions. The corresponding sub-exponential assumptions additionally require that there exists a constant $\varepsilon \in (0,1)$ such that the function $\nu(\lambda)$ is bounded by $2^{-\lambda^\varepsilon}$ (stricter than $v(\cdot)$ being negligible).

2.3 Probabilistic Checkable Proofs

A probabilistic checkable proof (PCPs, see [AS98; ALMSS98]) is a proof system for a language that allows very fast verification. More precisely, the verifier can check the correctness by randomly probing very few bits of the proof. The definition of PCP is shown below.

Definition 2.4 (Probabilistic checkable proof). For a language L, a probabilistic checkable proof for L is a randomized algorithm V with the syntax $(I, D) \leftarrow V(x; r)$, where x is an instance, r is the random coins, I is a set of indices of size $|I| = q$, and $D : \{0,1\}^q \to \{0,1\}$ is the decision circuit. Furthermore, V should have the following properties:

- For any $x \in L$, there exists a proof string that make the verifier accept, i.e.,
$$\exists \pi \Pr_{(I,D)\leftarrow V(x;r)}[D(\pi_I)=1] = 1.$$
- For any $x \notin L$, any proof string can only make the verifier accept with very low probability, i.e.,
$$\forall \pi \Pr_{(I,D)\leftarrow V(x;r)}[D(\pi_I)=1] \leq \varepsilon.$$

In addition, q is called the query complexity, $|\pi|$ is the proof size, ε is the soundness error, and the size of the circuit D is the verification time. ♢

2.4 The Fiat-Shamir transformation

The Fiat-Shamir transformation [FS86] is a general method for eliminating interaction in public-coin interactive proofs (or arguments). Note that a proof system means that the prover is computationally unbounded, while an argument system means that the prover is comoputationally bounded (e.g., runs in polynomial time). In general, the Fiat-Shamir transformation can be used to convert any public-coin interactive proof (or argument) into a non-interactive argument. The transformation itself is quite simple: given a public-coin interactive proof protocol (P, V), the new prover P' and the new verifier V' first agree on a hash function h which is randomly chosen from a hash function family $\mathcal{H}$. Then the prover P' just runs the protocol by emulating P. Every time the protocol requires a verifier message (which is some random coins), the prover P' just replace the message with the hash of the transcript of the protocol so far. As a result, the verifier V' does not need to send anything (so (P', V') becomes non-interactive), and V' only needs to check that the prover message is an accepting transcript for V and the "verifier messages" are indeed the hash value. Figure 1 below is an illustration of the transformation.

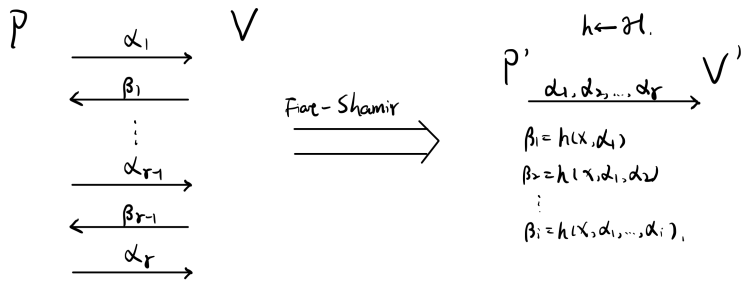

Figure 1: the Fiat-Shamir transformation, applied on an interactive proof proving $x \in L$

2.5 Correlation intractable hash functions

Correlation intractable (CI) hash functions are crucial for Fiat-Shamir. Together with round-by-round soundness (see section 4), they suffice to securely instantiate Fiat-Shamir for *proof*s. The formal definition is shown below.

Definition 2.5 (Correlation intractable hash family [CGH04]). A hash family $\mathcal{H} = \{\mathcal{H}_\lambda\}_{\lambda \in \mathbb{N}}$ has the following two algorithms:

- $K \leftarrow \mathcal{H}.\mathtt{Gen}(1^\lambda)$: $\mathtt{Gen}$ is a PPT algorithm that on input the security parameter 1^λ, outputs a hash key K;
- $y \leftarrow \mathcal{H}.\mathtt{Hash}(K, x)$: $\mathtt{Hash}$ is a deterministic polynomial-time algorithm that on input the hash key $K \in \mathtt{Gen}(1^\lambda)$ and the input $x \in \{0,1\}^{n(\lambda)}$, outputs the hash value $y \in \{0,1\}^\lambda$.

We say $\mathcal{H}$ is correlation intractable for a function family $\mathcal{F} = \mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ if the following holds:

- For any $\lambda \in \mathbb{N}$, any $f \in \mathcal{F}_\lambda$, and any $K \in \mathcal{H}.\mathtt{Gen}(1^\lambda)$, the functions $\mathcal{H}.\mathtt{Hash}(K, \cdot)$ and $f(\cdot)$ have the same domain and co-domain;

- For any non-uniform PPT adversary $\mathcal{A}$, for any $f \in \mathcal{F}_\lambda$, there exists a negligible function $\nu(\cdot)$ such that

$$\Pr_{\substack{K \leftarrow \mathcal{H}.\mathtt{Gen}(1^\lambda) \\ x \leftarrow \mathcal{A}(K)}} [\mathcal{H}.\mathtt{Hash}(K, x) = f(x)] \leq \nu(\lambda).$$

$\diamondsuit$

The results of CI hash family mainly used in constructing SNARGs are the following:

- CI for P assuming LWE [PS19];
- CI for TC^0 assuming subexponential DDH [JJ21];
- CI for efficiently verifiable product relations assuming LWE [HLR21].

3 Somewhere extractable commitment with local opening

In this section, we present the definition and constructions of somewhere extractable commitment with local opening, which is a crucial tool for constructing SNARGs. The constructions are known based on many standard assumptions by borrowing some works on private information retrieval.

Definition 3.1 (Somewhere extractable (SE) commitment, modified based on [CJJ21b]). A *somewhere extractable commitment* scheme is a tuple of algorithms $(\mathtt{Gen}, \mathtt{TGen}, \mathtt{Com}, \mathtt{Ext})$ with the following syntax:

- $K \leftarrow \mathtt{Gen}(1^\lambda, 1^N)$. The normal mode key generator $\mathtt{Gen}$ on input the security parameter λ and the message length N, outputs a commitment key K that is uniformly random over the key space.
- $(K^*, td) \leftarrow \mathtt{TGen}(1^\lambda, 1^N, i)$. The trapdoor mode key generator $\mathtt{TGen}$ on input the security parameter λ, the message length N, and the position of extraction $i \in [N]$, outputs a commitment key K^* together with an extraction trapdoor td.
- $c \leftarrow \mathtt{Com}(K, \mathbf{m})$. The commitment is a deterministic algorithm $\mathtt{Com}$ that on input the commitment key K, the message $\mathbf{m} \in \{0,1\}^N$, outputs a commitment c.
- $z \leftarrow \mathtt{Ext}(td, c)$. The extraction algorithm $\mathtt{Ext}$ on input a trapdoor td and a commitment c, outputs a bit z.

The above commitment scheme should have the following properties:

- **Succinct commitment.** The commitment key K (generated by either $\mathtt{Gen}$ or $\mathtt{TGen}$) and the commitment c should have length bounded by $\mathsf{poly}(\lambda, \log N)$.
- **Key indistinguishability.** For any $i \in [N]$, for any non-uniform PPT adversary $\mathcal{D}$, there exists a negligible function $\nu(\cdot)$ such that

$$\left| \Pr_{K \leftarrow \mathtt{Gen}(1^\lambda, 1^N)} [\mathcal{D}(K) = 1] - \Pr_{K^* \leftarrow \mathtt{TGen}(1^\lambda, 1^N, i)} [\mathcal{D}(K^*) = 1] \right| \leq \nu(\lambda).$$

- **Extraction correctness.** For any message $\mathbf{m} \in \{0,1\}^N$, any $i \in [N]$, there exists a negligible function $\nu(\cdot)$ such that

$$\Pr_{(K^*,td)\leftarrow \mathtt{TGen}(1^\lambda,1^N,i)}[\mathtt{Ext}(td, \mathtt{Com}(K^*, \mathbf{m})) = \mathbf{m}_i] \geq 1 - \nu(\lambda).$$

  We say the extraction correctness is perfect if $\nu(\cdot) \equiv 0$. ♢

Note that we can always open the commitment by directly revealing the message $\mathbf{m}$ and letting the verifier re-compute the commitment. However, in many applications, we need to locally open a single element of $\mathbf{m}$ in a more efficient way. So, we have the following definition of local opening:

Definition 3.2 (Somewhere extractable commitment with local opening). A *somewhere extractable commitment with local opening* is a tuple of algorithms $(\mathtt{Gen}, \mathtt{TGen}, \mathtt{Com}, \mathtt{Open}, \mathtt{Verify}, \mathtt{Ext})$ such that $(\mathtt{Gen}, \mathtt{TGen}, \mathtt{Com}, \mathtt{Ext})$ is a SE commitment, and the extra $\mathtt{Open}$ and $\mathtt{Verify}$ have the following syntax:

- $\pi \leftarrow \mathtt{Open}(K, \mathbf{m}, i)$. On input the commitment key K, the message $\mathbf{m} \in \{0,1\}^N$, and an index $i \in [N]$, the deterministic algorithm $\mathtt{Open}$ generates an opening π to $\mathbf{m}_i$.
- $0/1 \leftarrow \mathtt{Verify}(K, c, i, z, \pi)$. The verification algorithm $\mathtt{Verify}$ gets as input the commitment key K, the commitment c, the index $i \in [N]$ to open, the value z claimed to be $\mathbf{m}_i$, and an opening π for it. Then it decides to either accept (output 1) or reject (output 0) the opening.

Furthermore, the commitment scheme should also have the following properties:

- **Succinct opening.** The length of the opening π and the running time of $\mathtt{Verify}$ should be bounded by $\mathsf{poly}(\lambda, \log N)$.
- **Opening completeness.** For any commitment key K, any message $\mathbf{m} \in \{0,1\}^N$, and any index $i \in [N]$, we have

$$\mathtt{Verify}(K, \mathtt{Com}(K, \mathbf{m}), i, \mathbf{m}_i, \mathtt{Open}(K, \mathbf{m}, i)) = 1.$$

- **Opening soundness.** For any extraction index $i \in [N]$, there exists a negligible function $\nu(\cdot)$ such that

$$\Pr_{(K^*,td)\leftarrow \mathtt{TGen}(1^\lambda,1^N,i)}[\exists c, z, \pi : \mathtt{Verify}(K^*, c, i, z, \pi) = 1 \wedge \mathtt{Ext}(td, c) \neq z] \leq \nu(\lambda).$$

♢

Remark. The definition here is a bit different from the definition in [CJJ21b]. The differences and why our definition suffices are as follows:

1. Our commitment is deterministic given the commitment key. Note that [CJJ21b] fixes the randomness when using the commitment, so we directly define a deterministic one.
2. We only define extraction w.r.t. a single index instead of a subset of indices. In fact, a SE commitment scheme w.r.t a subset S can be constructed easily by using $|S|$ different SE commitment schemes, each constructed w.r.t one of the extraction index in S (also, [CJJ21b] has another step of randomly shuffling the S commitments to achieve another required property called no-signaling). Therefore, our definition suffices.

3. In *extraction correctness* (and hence also in *opening soundness*), we allow a negligible error probability, while [CJJ21b] requires perfect correctness. One can easily find that extraction is only used in the proof of soundness, and it never appears in the real protocol. Therefore, the negligible error probability incurs only an extra negligible soundness error, since the soundness error can be bounded in the following way: for any wrong claim, the probability that the protocol accepts (i.e., the soundness error) is

$$\Pr[\text{protocol accepts}] \leq \Pr[\text{protocol accepts} \mid \text{extraction works}] + \Pr[\text{extraction fails}].$$

This problem will be discussed in detail when we construct the commitments (see section 3.2 and 3.3).

3.1 Private information retrieval

In this subsection, we define private information retrieval (PIR), which is closely related to SE commitment but is much more well-studied. The formal definition is shown below.

Definition 3.3 (Private information retrieval (PIR), modified based on [Döt+19]). A private information retrieval is a two-message protocol between a sender and a receiver. The sender has a long vector $\mathbf{m} \in \{0,1\}^N$, while the receiver wants to retrieve $\mathbf{m}_i$. The protocol consists of a triple of PPT algorithms $\Pi = (\Pi_1, \Pi_2, \Pi_3)$ with the following syntax:

- $(\mathtt{st}, \mathtt{msg1}) \leftarrow \Pi_1(1^\lambda, i)$. Π_1 takes as input the security parameter and the index i, and outputs a receiver message $\mathtt{msg1}$ together with a receiver state $\mathtt{st}$.
- $\mathtt{msg2} \leftarrow \Pi_2(\mathtt{msg1}, m)$. Π_2 takes as input the receiver message $\mathtt{msg1}$ and the vector $\mathbf{m}$, and outputs the sender message $\mathtt{msg2}$.
- $z \leftarrow \Pi_3(\mathtt{st}, \mathtt{msg2})$. Π_3 takes as input the state $\mathtt{st}$ and the sender message $\mathtt{msg2}$, and outputs the receiver output z.

We say the protocol is a PIR if the following properties holds:

- **Correctness:** Π is correct if for all $\mathbf{m} \in \{0,1\}^N$ and $i \in [N]$, there exists a negligible function $\nu(\cdot)$ such that
$$\Pr_{\substack{(\mathtt{st},\mathtt{msg1})\leftarrow\Pi_1(1^\lambda,i)\\ \mathtt{msg2}\leftarrow\Pi_2(\mathtt{msg1},\mathbf{m})\\ z\leftarrow\Pi_3(\mathtt{st},\mathtt{msg2})}}[z \neq \mathbf{m}_i] \leq \nu(\lambda).$$
- **Receiver privacy:** For any $i, j \in [N]$, for any non-uniform PPT adversary $\mathcal{D}$, there exists a negligible function $\nu(\cdot)$ such that
$$\left| \Pr_{(\mathtt{st},\mathtt{msg1})\leftarrow\Pi_1(1^\lambda,i)}[\mathcal{D}(1^\lambda, \mathtt{msg1}) = 1] - \Pr_{(\mathtt{st},\mathtt{msg1})\leftarrow\Pi_1(1^\lambda,j)}[\mathcal{D}(1^\lambda, \mathtt{msg1}) = 1] \right| \leq \nu(\lambda).$$

♢

By taking a closer look at the definition, we have the following result:

Proposition 3.4. The following two things are equivalent:

1. PIR with $\mathsf{poly}(\lambda, \log N)$ communication complexity;
2. SE commitment. ♢

Proof. The proof is straightforward. In the definition of PIR and SE commitment, we take Π_1 as $\mathtt{TGen}$, Π_2 as $\mathtt{Com}$, and Π_3 as $\mathtt{Ext}$. Then the correctness of PIR is the same as the extraction correctness of SE commitment, receiver privacy is the same as key indistinguishability, and $\mathsf{poly}(\lambda, \log N)$ communication complexity is the same as the commitment being succinct. □

Due to the equivalence, we can get SE commitments directly from the constructions of PIR, and then check whether they have local opening. We check the constructions in the following subsections.

3.2 Constructions based on LWE or QR

In order to construct SE commitments with local opening, we borrow the results from [Döt+19], which presents constructions of PIR based on LWE, DDH, or QR. Due to the equivalence, we can directly obtain SE commitments from these assumptions. Furthermore, all the constructions in [Döt+19] have a special Merkle tree structure, allowing us to locally open a single element. In general, the opening algorithm simply reveals the path from the root to the position to open on the tree structure, together with the sibling of each node on the path. Then the verifier just checks that each node on the path is correct.

The completeness of such an opening is straightforward. However, the soundness might be problematic due to the different settings of PIR and commitments. When we use the commitment in a protocol, we need to consider a malicious prover: it may try to forge a commitment after receiving the commitment key. Therefore, the definition of *opening soundness* requires that with high probability over a randomly chosen key, even an unbounded prover cannot find a commitment with a wrong local opening (like adaptive security). However, in a PIR, the correctness only requires that for any message to commit, the extraction can work with high probability over a randomly chosen key (like non-adaptive security). As a result, a cheating prover may be able to find a commitment given the commitment key and make the extraction fail.

Note that the constructions based on LWE or QR have perfect extraction correctness, so we at least have the following theorem:

Theorem 3.5. If either LWE or QR holds, we have SE commitments with local opening. ♢

For the construction based on DDH, we show in the next subsection that it may satisfy a relaxed property that suffices for constructing SNARGs.

3.3 Possible weaker construction based on DDH

There is an observation of the DDH-based PIR from [Döt+19]: when extracting the commitment, we can efficiently check whether the extraction fails or not. It means we can either perfectly extract the correct value or find that the extraction does not work. Due to this property, we can allow the extraction algorithm to output a special symbol representing "fail", and define the following relaxed version of soundness:

Definition 3.6 (Weak opening soundness). Consider a commitment scheme $(\mathtt{Gen}, \mathtt{TGen}, \mathtt{Com}, \mathtt{Open}, \mathtt{Verify}, \mathtt{Ext})$. We say it is a SE *commitment with weak local opening* if it satisfies all other definitions of SE commitment with local opening, except that the definition of *opening soundness* is relaxed to *weak opening soundness*: the extraction algorithm $\mathtt{Ext}$ is allowed to output a special symbol $\perp$ meaning the extraction fails, and the following two properties are satisfied:

- For any non-uniform PPT adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that

$$\Pr_{\substack{(K^*,td)\leftarrow\mathtt{TGen}(1^\lambda,1^N,i)\\ c\leftarrow\mathcal{A}(K^*)}}[\mathtt{Ext}(td,c)=\perp] \leq \mu(\lambda).$$

- There exists a negligible function $\nu(\cdot)$ such that

$$\Pr_{(K^*,td)\leftarrow\mathtt{TGen}(1^\lambda,1^N,i)}[\exists c,z,\pi : \mathtt{Verify}(K^*,c,i,z,\pi)=1 \wedge \mathtt{Ext}(td,c)\neq z \wedge \mathtt{Ext}(td,c)\neq\perp] \leq \nu(\lambda).$$

$\diamondsuit$

In fact, the error probability $\nu(\lambda)$ in the second inequality can be 0. Therefore, we only need to bound the probability of finding a "non-extractable" commitment given a random key. However, this problem is related to too many details of the DDH-based PIR, and is still not very clear. Also, there should be simpler proofs/constructions, or even constructions with standard soundness. So, we just skip the complicated analysis here.

4 Fiat-Shamir compatible protocols

In this section, we relax the definition of Fiat-Shamir compatible protocols in order to deal with the faulted extraction in SE commitment. The idea is that for an interactive argument that the prover is computationally bounded, a small fraction of prover messages that are hard for the prover to find can be ignored.

Definition 4.1 (Relaxed round by round soundness, modified based on [Can+19]). Let $\Pi = (P, V)$ be an interactive argument under the common reference string model for a language L, and crs be the common reference string. We say Π is *relaxed round by round sound* if there exists a deterministic function $\mathtt{State}$ (can be inefficient) that takes as input an instance $x \in \{0,1\}^*$ and a prefix of the transcript of the protocol τ, and outputs one of $0/1/\perp$ (representing "reject", "accept", and "abort" respectively). $\mathtt{State}$ should have the following properties:

- Let ϕ be the empty transcript prefix. For any $x \in L$, we have $\mathtt{State}(x,\phi)=1$; for any $x \notin L$, we have $\mathtt{State}(x,\phi)=0$.
- For any instance x, any transcript prefix $\tau = (\mathrm{crs}, \alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_{i-1}, \beta_{i-1})$ such that $\mathtt{State}(x,\tau)=0$, and any prover message α_i such that $\mathtt{State}(x,\tau|\alpha_i)\neq\perp$, there exists a negligible function $\nu(\cdot)$ such that

$$\Pr_{\beta_i\leftarrow V(x,\tau|\alpha_i)}[\mathtt{State}(x,\tau|\alpha_i|\beta_i)=1] \leq \nu(\lambda).$$

- For any instance x, any complete protocol transcript τ, we have

$$\mathtt{State}(x,\tau)=0 \Rightarrow V(x,\tau)=0.$$

- For any instance x and transcript prefix τ, if any prefix τ' of τ satisfies $\texttt{State}(x, \tau') = \perp$, then we must have $\texttt{State}(x, \tau) = \perp$.
- For any instance $x \notin L$, any non-uniform PPT adversary $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that

$$\Pr_{\substack{\text{crs} \leftarrow \{0,1\}^* \\ \tau \leftarrow \mathcal{A}(x, \text{crs})}} [\texttt{State}(x, \text{crs}|\tau) = \perp] \leq \nu(\lambda).$$

$\diamondsuit$

Similar to a standard RBR-sound protocol, we can also define the bad relation $\mathcal{B}$ for an interactive argument $\Pi = (P, V)$ with relaxed RBR soundness. $\mathcal{B}$ is defined as

$$\mathcal{B} = \{((x, \tau|\alpha), \beta) : \texttt{State}(x, \tau) = 0 \wedge \texttt{State}(x, \tau|\alpha|\beta) = 1\}.$$

We can show that the relaxed version of RBR soundness can also work with correlation intractability to securely instantiate Fiat-Shamir.

Theorem 4.2 (FS-compatible interactive arguments). Let $\Pi = (P, V)$ be an interactive argument for L with relaxed round-by-round soundness, and let $\mathcal{H}$ be a hash function family that is correlation intractable for the bad relation $\mathcal{B}$ of Π. Then the new protocol $\Pi' = (P', V')$ defined below is a non-interactive argument for L with negligible soundness error.

- Common reference string crs': the new crs' has the form $crs' = (crs, h)$, where crs is the common reference string of Π, and $h \leftarrow \mathcal{H}$ is the description of a hash function from the hash family $\mathcal{H}$.
- Prover P': P' emulates P and replaces each message β_i from V with $\beta'_i = h(x, crs|\alpha_1|\alpha_2|\cdots|\alpha_i)$. Then it sends the transcript to V'.
- Verifier V': V' checks that the transcript is consistent with h and V accepts the transcript. $\diamondsuit$

Proof. If there exists a non-uniform PPT cheating prover P^* for the new protocol Π', it means there exists an instance $x \notin L$ and an inverse-polynomial function $p(\cdot)$ such that

$$\Pr_{\substack{crs \leftarrow \{0,1\}^* \\ h \leftarrow \mathcal{H} \\ \tau \leftarrow P^*(x, crs, h)}} [V'(x, h, \tau) = 1] \geq p(\lambda).$$

Now we consider the state function. The state can only be "accept" or "abort" if the verifier accepts. Therefore,

$$\begin{aligned} &\Pr_{\substack{crs \leftarrow \{0,1\}^* \\ h \leftarrow \mathcal{H} \\ \tau \leftarrow P^*(x, crs, h)}} [\texttt{State}(x, \tau) = 1] + \Pr_{\substack{crs \leftarrow \{0,1\}^* \\ h \leftarrow \mathcal{H} \\ \tau \leftarrow P^*(x, crs, h)}} [\texttt{State}(x, \tau) = \perp] \geq p(\lambda) \\ \Rightarrow &\Pr_{\substack{crs \leftarrow \{0,1\}^* \\ h \leftarrow \mathcal{H} \\ \tau \leftarrow P^*(x, crs, h)}} [\texttt{State}(x, \tau) = 1] \geq p(\lambda) - \texttt{negl}(\lambda). \end{aligned}$$

This step is because the probability of aborting must be negligible according to the definition of relaxed RBR soundness. Now we have been back to the situation without aborting, and the proof using standard RBR soundness and correlation intractability can just go through. $\square$

5 Towards better SNARGs for P

Based on the results in previous sections, we want to weaken the assumptions required for SNARGs, e.g., SNARGs based on only (subexponential) DDH. However, there are still some problems related to PCP. In this section, we present the ideas and problems of constructing better SNARGs with techniques in [CJJ21b].

5.1 Weak local opening and Fiat-Shamir

We first show that if we use SE commitment with weak local opening in the protocol in [CJJ21b], relaxed RBR soundness can be satisfied. The original protocol proves somewhere statistical soundness by switching the commitment key to trapdoor mode, and extracting the commitment to define the state function. With weak local opening, we first let the state function output "abort" if the prover sends a commitment that cannot be extracted by the trapdoor, and then define the state function in the same way as the original protocol. Due to the definition of weak opening soundness, such a commitment is hard to find, and thus the relaxed RBR soundness is satisfied.

5.2 The need of better PCPs

Note that in [CJJ21b], the construction requires the result of CI for fancier relations from [HLR21]. However, such kind of results are only known from LWE. The major technique used in [HLR21] is list-recoverable codes, which are roughly used to derandomize the protocol and then apply the CI for P result. Although we also have CI for TC^0 assuming (sub-exponential) DDH [JJ21], we still do not know list-recoverable codes that can meet the TC^0-computable requirement.

In order to have SNARGs from assumptions other than LWE, we need to either have similar results from other assumptions (which are still unknown), or avoid such kind of relations by constructing better PCPs. For example, to get a DDH-based SNARG using the same technique, we need a PCP with $\mathsf{negl}(\lambda)$ soundness error with the following properties:

- **Few bad randomness.** For any $x \notin L$, any PCP proof π, the number of bad randomness is polynomially bonded, i.e., $|\{r : (I, D) \leftarrow V(x; r), D(\pi_I) = 1\}| \leq \mathsf{poly}(\lambda)$.
- **Efficient bad function.** There exists an efficient algorithm in TC^0 such that given the PCP proof π for $x \notin L$, the algorithm samples a bad randomness r of the PCP query that leads to accept.

Such a PCP is still unknown. To make the problem easier, we can try to relax some properties of PCPs. An observation of [CJJ21b] is that the requirements on the query complexity and verification time is not as strict as traditional PCPs: we only need the verification circuit to be a little bit smaller than the original NP statement, but traditional PCPs usually shrink a lot, say $\mathsf{poly}(\log |C|, \lambda)$. Therefore, here we can relax the verification time (and thus the query complexity) to be smaller than only a non-trivial bound, say, $|C|^{\varepsilon} \cdot \mathsf{poly}(\lambda)$ for a small enough constant ε.

Note that there are boosting techniques for PCP to reduce the query complexity, like composing PCPs (see, e.g., [AS98]). However, composition of PCPs has additional requirements, e.g., robustness and proof of proximity. Also, the soundness error after composing two PCPs is the sum of the two original PCPs. Since we may not be able to boost the query complexity for free, relaxing the query complexity can make sense.

6 Conclusion

This work is only a partial result of SNARGs based solely on (subexponential) DDH. We summarized some results from PIR showing that SE commitment (with local opening) is known from several standard cryptographic assumptions. Also, we tried to relax the requirement of local opening, and presented a new relaxed version of RBR soundness. However, there still remains a barrier of constructing either better PCPs or DDH-based correlation-intractable hash functions for fancier relations. Also, the DDH-based commitment requires further examination. In addition to solving this problem, we can also try to apply the relaxed RBR soundness to other applications.

References

[ALMSS98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. "Proof Verification and the Hardness of Approximation Problems". In: *J. ACM* 45.3 (1998), pp. 501–555. DOI: 10.1145/278298.278306. URL: https://doi.org/10.1145/278298.278306 (cit. on p. 3).

[AS98] Sanjeev Arora and Shmuel Safra. "Probabilistic Checking of Proofs: A New Characterization of NP". In: *J. ACM* 45.1 (1998), pp. 70–122. DOI: 10.1145/273865.273901. URL: https://doi.org/10.1145/273865.273901 (cit. on pp. 3, 11).

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. "The random oracle methodology, revisited". In: *J. ACM* 51.4 (2004), pp. 557–594. DOI: 10.1145/1008731.1008734. URL: https://doi.org/10.1145/1008731.1008734 (cit. on p. 4).

[Can+19] Ran Canetti et al. "Fiat-Shamir: from practice to theory". In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019*. Ed. by Moses Charikar and Edith Cohen. ACM, 2019, pp. 1082–1090. DOI: 10.1145/3313276.3316380. URL: https://doi.org/10.1145/3313276.3316380 (cit. on p. 9).

[CJJ21a] Arka Rai Choudhuri, Abhishek Jain, and Zhengzhong Jin. "Non-interactive Batch Arguments for NP from Standard Assumptions". In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part IV*. Ed. by Tal Malkin and Chris Peikert. Vol. 12828. Lecture Notes in Computer Science. Springer, 2021, pp. 394–423. DOI: 10.1007/978-3-030-84259-8_14. URL: https://doi.org/10.1007/978-3-030-84259-8%5C_14 (cit. on p. 2).

[CJJ21b] Arka Rai Choudhuri, Abhishek Jain, and Zhengzhong Jin. "SNARGs for \mathcal{P} from LWE". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 68–79. DOI: 10.1109/FOCS52979.2021.00016. URL: https://doi.org/10.1109/FOCS52979.2021.00016 (cit. on pp. 1, 2, 5, 6, 7, 11).

[DH76] Whitfield Diffie and Martin E. Hellman. "New directions in cryptography". In: *IEEE Trans. Inf. Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638. URL: https://doi.org/10.1109/TIT.1976.1055638 (cit. on p. 2).

[Döt+19] Nico Döttling et al. "Trapdoor Hash Functions and Their Applications". In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11694. Lecture Notes in Computer Science. Springer, 2019, pp. 3–32. DOI: 10.1007/978-3-030-26954-8_1. URL: https://doi.org/10.1007/978-3-030-26954-8%5C_1 (cit. on pp. 7, 8).

[FS86] Amos Fiat and Adi Shamir. "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*. Ed. by Andrew M. Odlyzko. Vol. 263. Lecture Notes in Computer Science. Springer, 1986, pp. 186–194. DOI: 10.1007/3-540-47721-7_12. URL: https://doi.org/10.1007/3-540-47721-7%5C_12 (cit. on p. 4).

[GM82] Shafi Goldwasser and Silvio Micali. "Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information". In: *Proceedings of the 14th Annual ACM Symposium on Theory of Computing, May 5-7, 1982, San Francisco, California, USA*. Ed. by Harry R. Lewis, Barbara B. Simons, Walter A. Burkhard, and Lawrence H. Landweber. ACM, 1982, pp. 365–377. DOI: 10.1145/800070.802212. URL: https://doi.org/10.1145/800070.802212 (cit. on p. 3).

[HLR21] Justin Holmgren, Alex Lombardi, and Ron D. Rothblum. "Fiat-Shamir via list-recoverable codes (or: parallel repetition of GMW is not zero-knowledge)". In: *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM, 2021, pp. 750–760. DOI: 10.1145/3406325.3451116. URL: https://doi.org/10.1145/3406325.3451116 (cit. on pp. 5, 11).

[HJKS22] James Hulett, Ruta Jawale, Dakshita Khurana, and Akshayaram Srinivasan. "SNARGs for P from Sub-exponential DDH and QR". In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part II*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13276. Lecture Notes in Computer Science. Springer, 2022, pp. 520–549. DOI: 10.1007/978-3-031-07085-3_18. URL: https://doi.org/10.1007/978-3-031-07085-3%5C_18 (cit. on p. 2).

[JJ21] Abhishek Jain and Zhengzhong Jin. "Non-interactive Zero Knowledge from Sub-exponential DDH". In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12696. Lecture Notes in Computer Science. Springer, 2021, pp. 3–32. DOI: 10.1007/978-3-030-77870-5_1. URL: https://doi.org/10.1007/978-3-030-77870-5%5C_1 (cit. on pp. 5, 11).

[Kal22] Yeal Taumen Kalai. "Delegating Computation: Simple at Last". Milan theory workshop. 2022. URL: https://lucatrevisan.github.io/mtw.html (cit. on p. 2).

[PS19] Chris Peikert and Sina Shiehian. "Noninteractive Zero Knowledge for NP from (Plain) Learning with Errors". In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11692. Lecture Notes in Computer Science. Springer, 2019, pp. 89–114. DOI: 10.1007/978-3-030-

26948-7_4. URL: https://doi.org/10.1007/978-3-030-26948-7%5C_4 (cit. on p. 5).

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*. Ed. by Harold N. Gabow and Ronald Fagin. ACM, 2005, pp. 84–93. DOI: 10.1145/1060590.1060603. URL: https://doi.org/10.1145/1060590.1060603 (cit. on p. 2).

[WW22] Brent Waters and David J. Wu. "Batch Arguments for NP and More from Standard Bilinear Group Assumptions". In: *IACR Cryptol. ePrint Arch.* (2022), p. 336. URL: https://eprint.iacr.org/2022/336 (cit. on p. 2).