Abstract

In the last few years, applications such as practical verifiable computation, anonymous cryptocurrencies (e.g., Zcash), signature of knowledge and etc have made succinct non-interactive arguments (SNARGs) as an active research area for ground-breaking researchers. A non-interactive computationally sound argument (proof system) for $NP$ is succinct if its proof size is polylogarithmic the instance and witness sizes. The succinctness of an arguments makes it possible to verify the proof efficiently by low-power verifiers and clients. Recently, among wide range of prominent results on SNARGs, there was a basic research question regard to construction of SNARGs based on falsifiable cryptographic assumptions (e.g., DDH, RSA, LWE, OWFs, · · ·). Roughly speaking, the question was that "can we prove any SNARG construction secure under assumptions such as OWFs, DDH, RSA, LWE, and etc which are falsifiable assumptions". This question is answered by Gentry and Wichsy in 2011 [GW11], by showing that there is no black-box reduction security proof for any SNARG under falsifiable assumptions. Note that, a cryptographic assumption is called falsifiable if we can model it as a game between an adversary and an efficient challenger, which at the end of the game, the challenger can determine whether the adversary won the game. In this report, we aim to give a short overview on their result and highlight the key points of their paper.

1 Introduction

Proof systems and $\Sigma$-protocols are set of prominent tools which widely are used in cryptography to prove properties of particular information. Generally, suppose that $R$ be a polynomial time verifiable relation containing pairs $(x, w)$. First element of the pair $(x)$ is called statement, and the second one $(w)$ is called witness. Now, let the language $L_R$ be defined as the set of statements $x$ for which there exists a witness $w$ such that $(x, w) \in R$. Then, a proof system is a protocol between a prover $P$ and a verifier $V$ where the prover, who knows a witness $w$ for which $(x, w) \in R$ gives a proof to the verifier that $x \in L_R$. During last few years, some popular applications such as anonymous cryptocurrencies (e.g., Zcash [SCG+14]), commitment and prove schemes [Lip16], practical verifiable computation

\*This report is prepared in partial fulfillment of the requirements for the course Research Seminar in Cryptography (MTAT.07.022) in Fall 2017 and it is presented as a seminar at Institute of Computer Science, University of Tartu (on 28 November 2017).
systems (e.g. Pinocchio [PHGR13])\textsuperscript{1}, signatures of knowledge [GM17], and etc have made succinct non-interactive arguments (SNARGs) as an active research area for groundbreaking researchers. From communication point of view, a proof can be done in two different manners; including an interactive proof and a non-interactive proofs (see Fig. 1).

Following the original paper, in the report we will mostly focus on the non-interactive proofs. Generally, there are two models mainly used to get a non-interactive proof: the random oracle (RO) model, and the common reference string (CRS) model. In the RO model, it is assumed that there is one or more random oracles that give uniformly random responses. Using the Fiat-Shamir heuristic, these random responses can be used to replace every message a verifier sends to the prover. In the CRS model, it is assumed that there is a trusted third party that generates a common string that incorporates an honest verifier’s response in an interactive proof system. Once the string is generated, and a prover can use it during proof generation and proof verification [F\textsuperscript{+}17].

During past three decades, both interactive and non-interactive proof systems are studied from different point of views such as zero-knowledge (ZK) proofs, computationally soundness proofs, proof of knowledge, and probabilistically checkable proofs (PCPs).

From a different point of view, we always are interested to give a proof as short as possible. More precisely, in the interactive proofs, this could be considered to have succinct communication size which includes number of rounds and size of transmitted messages during the protocol execution. Equivalently, in the non-interactive proofs, we are interested to have a succinct proof. Accurately, a proof argument for \(NP\) is called succinct if given a statement \(x\) with a witness \(w\), the communication-complexity (proof size) of the argument is bounded by \(\text{poly}(n)(|x|+|w|^{o(1)})\), where \(n\) is a security parameter and soundness holds for all \(\text{poly}(n)\)-time bounded provers. Similarly, in the case that the proof size of an argument is bounded by \(\text{poly}(n)(|x|+|w|)^c + o(|x|+|w|)\), for \(c < 1\), the argument is considered as slightly succinct.

1.1 Motivation

In 1992, Kilian has showed that one can construct succinct interactive arguments with four rounds for \(NP\) based on the assumption that collision resistant hash functions (CRHFs)\textsuperscript{1}.

\textsuperscript{1} Pinocchio is one of the popular and near to practical system which is proposed for verifiable computations. Similar to this report, a short overview on the Pinocchio system can be found in [Bag16].
exist [Kil92]. Two years later, Micali showed that such succinct argument can be made non-interactive in the RO model [Mic94]. But until 2011, the question that whether succinct non-interactive arguments (SNARGs) exist in the standard model (under any simple cryptographic assumption), was considered as an open problem. Particularly, the SNARGs initialized with CRS elements, that these elements are used in the proof generation and verification procedures. In order to give a complete answer, one needed to show that if such a construction exists, which cryptographic assumption it needs to be relay on. In an interesting result Bitansky et al. [BCPR16] showed that indistinguishability obfuscation implies that for every candidate Succinct Non-Interactive Argument of Knowledge (SNARK), there are auxiliary output distributions that enable the adversary to create a valid proof without it being possible to extract the witness\(^2\). But, regard to the mentioned capital question, eventually, it was responded by Gentry and Wichsy [GW11]. It is shown that there is no construction of a SNARG with a formal security proof under any simple cryptographic assumption. In this report, we briefly go through to their results and address the dealing challenges. Before going through the details, lets have a short overview on their results, limitations and techniques.

1.2 Overview on Results, Limitations and Main Intuition

**Results.** In summary, the result of Gentry and Wichsy [GW11] is answering the stated question in the last part. To this end, they show that there is no SNARG with black-box reduction security proof under any non-false falsifiable cryptographic assumption.

Recall that the term black-box reduction refers to a proof technique that it is given oracle access to an arbitrary successful adversary which can be deployed to break some particular underlying cryptographic assumption. Giving oracle access to an arbitrary successful attacker means that the reduction only gives an input to the adversary in black-box manner and gets an output; and it does not know explicitly the description of the successful adversary. And as already mentioned, the term falsifiable assumption refers to the types of cryptographic assumptions that can be written as an interactive game between an efficient challenger \(C\) and an adversary \(\mathcal{A}\), and at the end of the game, \(C\) can determine whether \(\mathcal{A}\) won the game [Nao03]. In deed, a falsifiable assumption states that every efficient \(\mathcal{A}\) successes with a negligible probability. Majority of standard cryptographic notions such as One Way Functions, Trapdoor Permutations, Oblivious Transfer, Identity Based Encryption, Fully Homomorphic Encryption etc, and concrete cryptographic assumptions such as hardness of factoring, discrete logarithms, shortest vector problem, RSA, CDH, DDH, LWE and etc are categorized as a falsifiable assumption. Note that intuitively, this notion says that an efficient challenger can test whether an adversarial strategy falsifies (i.e. breaks) the assumption. This gives an evidence that falsifiable assumptions are more likable than non-falsifiable ones.

**Limitations.** The presented results in the paper hold for designated verifier SNARGs as well, which is a weaker notation of publicly verifiable ones. Precisely speaking, unlike the

\(^2\)A similar short report over the result can be found in [Bag17].
Techniques and Main Intuition. Basically, the main technique that Gentry and Wichsy [GW11] used to show the impossibility result, is the existence of a simulatable adversary. Roughly speaking, they show that for every SNARG for an $NP$ complete language $L$, there is a simulatable adversary $\mathcal{P}$. The adversary $\mathcal{P}$ is an inefficient adversarial prover which given a CRS comes up with a false statement $x \notin L$ and a proof $\pi$ for the false statement. But, in the other side, this adversary $\mathcal{P}$ comes with an efficient simulator $\mathcal{S}$ such that no efficient machine can distinguish whether it is interacting with $\mathcal{P}$ or $\mathcal{S}$. Fig. 2 shows a graphical illustration of a sample inefficient simulatable adversary $\mathcal{P}$ and its corresponding efficient simulator $\mathcal{S}$.

Once it is shown that there is such a simulatable $\mathcal{P}$, one can show that there is no SNARG with black-box reduction security proof under any non-false falsifiable cryptographic assumption. Basically, this result comes from the discussed fact that an efficient oracle-access machine $\mathcal{R}^{(\cdot)}$, given access to a successful adversary $\mathcal{P}$, breaks a falsifiable assumption. Now, as already mentioned, since an efficient distinguisher of a falsifiable assumption cannot distinguish $\mathcal{P}$ from $\mathcal{S}$, so if a machine $\mathcal{R}^{(\mathcal{P})}$ breaks a particular falsifiable assumption, $\mathcal{R}^{(\mathcal{S})}$ will also be able to break the same assumption (see Fig. 2). Note that this is equivalent to showing that if there is a black-box reduction from a falsifiable assumption to soundness.
proof of a SNARG, then the assumption must already be false.

In the above discussions, it is assumed that there is a simulatable adversary $\mathcal{P}$. But, in fact the existence of such an adversary needs to be proved. In order to prove the existence of a simulatable adversary $\mathcal{P}$, they prove a lemma regard to indistinguishability with auxiliary information which will be discussed latter. Intuitively, the lemma proves that assuming two computationally indistinguishable distributions $L$ over the set $L$ and $\bar{L}$ over the set $\bar{L}$, where $\bar{L} = \{0,1\}^* \setminus L$, then for any auxiliary information $\pi$ that we can give about $x \leftarrow L$, there exists some auxiliary information $\bar{\pi}$ that we can give about $\bar{x} \leftarrow \bar{L}$ such that $(x, \pi)$ and $(\bar{x}, \bar{\pi})$ are also computationally indistinguishable from each other. Fig. 3 depicts a graphical view of the described procedure. In this setting, the security degrades (exponentially) with the size of auxiliary information $\pi$. It is worth to mention that the result of lemma does not depend on the witness; in other words, the lemma holds even if the auxiliary information $\pi$ is not efficiently computable from $x$, and similarly $\bar{\pi}$ may not be efficiently computable from $\bar{x}$. The proof of lemma extremely relies on Neumann’s min-max theorem [Neu28].

Finally, given result of the discussed lemma, one can show the existence of a simulatable adversary $\mathcal{P}$ and its corresponding simulator $S$. Precisely speaking, assuming the existence of a sub-exponentially hard subset-membership problem, there is an $\mathcal{NP}$ language $L$ along with two distributions $L$ and $\bar{L}$ as above, that are computationally indistinguishable. This will be shown as a lemma in the upcoming sections of the report. Intuitively, the simulator $S$ efficiently samples $x \leftarrow L$ along with a witness $w$ and efficiently computes an honest proof $\pi$ for the sampled $x$. The unbounded simulatable adversary $\mathcal{P}$ samples $\bar{x} \leftarrow \bar{L}$ with some inefficiently samplable auxiliary information $\bar{\pi}$, as defied by the lemma. Now, since the proofs $\pi$ of a SNARG are sufficiently short, the distributions $(x, \pi)$ produced by $\mathcal{P}$ and $(\bar{x}, \bar{\pi})$ produced by $S$ are computationally indistinguishable by efficient parties. It means that $\mathcal{P}$ produces valid proofs for false statements, and hence is a successful adversary, but it can also be simulated by the efficient simulator $S$. There are some key points in the structure of simulator $S$, which will be discuss in the later.

Structure of the report: Section 2 reviews some relevant definitions which are used in the rest of report. In section 3, we will briefly review the main results of the paper which contains
the concept of indistinguishability with auxiliary information, existence of a simulatable adversary for any SNARG and also describes the black-box separation of SNARGs from falsifiable assumptions. Finally, we conclude the report in section 4.

2 Preliminaries

This section provides notation and some background which are three essential concepts for the rest of the report. Given a security parameter $n$, efficient algorithms are identified with $\text{poly}(n)$-sized randomized circuits or, equivalently, probabilistic $\text{poly}(n)$-time Turing Machines with $\text{poly}(n)$-sized advice. A function $\epsilon(n)$ is called negligible if $\epsilon(n) = \frac{1}{\text{poly}(n)}$ and it is written as $\epsilon(n) = \text{negl}(n)$ for short. Two distributions $X_1$ and $X_2$ are called $(s(n),\epsilon(n))$-indistinguishable if for every circuit $D$ of size $s(n)$, we have $|\Pr[D(X_1 = 1)] - \Pr[D(X_2 = 1)]| \leq \epsilon(n)$. And similarly, they are called computationally indistinguishable if for every $s(n) = \text{poly}(n)$ there is some $\epsilon(n) = \text{negl}(n)$ such that the distributions are $(s(n);\epsilon(n))$-indistinguishable.

2.1 Succinct Non-Interactive Arguments (SNARGs)

In general a SNARG $\Pi = (G, P, V)$ consists of three efficient algorithms $\Pi = (G, P, V)$, which are called generator, prover, and verifier, respectively. Given the security parameter $n$, the generation algorithm $(\text{crs}, \text{priv}) \leftarrow G(1^n)$ generates a common reference string $\text{crs}$ and the trapdoors $\text{priv}$. The prover algorithm $\pi \leftarrow P(\text{crs}, x, w)$ generates a proof $\pi$ for a statement $x$ using a witness $w$. The (designated) verifier algorithm decides if $\pi$ is a valid proof for $x$ as $(\{0, 1\} \leftarrow V(x, \pi, \text{crs}, \text{priv})) \{0, 1\} \leftarrow V(x, \pi, \text{crs})$. Not that in the designated verifier case, verifier also need secret keys $\text{priv}$ of $\text{crs}$ to verify the proof. Fig. 4 represents the discussed algorithms.

Definition 1. We say that $\pi = (G, P, V)$ is a succinct non-interactive argument (SNARG) for an $NP$ language $L$ with a corresponding $NP$ relation $R$, if it satisfies the following three properties:
Completeness: \( \forall (x, w) \in R, \text{Pr} \left[ V(x, \pi, \text{crs}, \text{priv}) = 0 \mid (\text{crs}, \text{priv}) \leftarrow G(1^n), \pi \leftarrow P(\text{crs}, x, w) \right] = \text{negl}(n) \).

Soundness: For all efficient \( P \), \( \text{Pr} \left[ V(x, \pi, \text{crs}, \text{priv}) = 1 \mid (\text{crs}, \text{priv}) \leftarrow G(1^n), x \notin L \mid (x, \pi) \leftarrow P(1^n, \text{crs}) \right] = \text{negl}(n) \).

Succinctness: The length of a proof is given by \(|\pi| = \text{poly}(n)(|x| + |w|)^{o(1)}\). Note that, there is a weaker notion of the succinctness which is called slightly succinct and it that case there is some constant \( c < 1 \) such that the length of a proof is given by \(|\pi| = \text{poly}(n)(|x| + |w|)^{c} + o(|x| + |w|)\).

Intuitively, one can consider the succinctness as a case that there is a fixed polynomial bound on the size of the proof \( \pi \), independent of the size of statement/witness.

2.2 Falsifiable Cryptographic Assumptions

The next essential concept which needs to be review is falsifiable assumptions that is introduced by [Nao03]. Following Gentry and Wichsy paper [GW11], this reports uses the following definition.

Definition 2. A falsifiable cryptographic assumption consists of an efficient interactive challenger \( C \) and a constant \( c \in [0, 1) \). The challenger \( C(1^n) \) interacts with a machine \( A(1^n) \) (\( n \) is security parameter) and finally outputs a special symbol win or \( \bot \). If the outputs win, we say \( A(1^n) \) wins \( C(1^n) \).

Note that the assumption associated with the tuple \( (C, c) \) states that for any efficient \( A \), we have \( \text{Pr}[A(1^n) \text{ wins } C(1^n)] \leq c + \text{negl}(n) \). A (possibly inefficient) machine \( A \) considered as an assumption breaker if its probability of winning exceeds that of the assumption.

Note that definition covers different cryptographic assumptions by appropriate parameter settings. E.g. with \( c = 0 \), it captures assumptions such as (strong) RSA, discrete-logarithm (DL), computational Diffie-Hellman (CDH) etc. And with \( c = \frac{1}{2} \), it can model various decisional assumptions such as the Decisional Diffie-Hellman (DDH), the decisional Learning with Errors (LWE) assumptions and so on.

There are some examples of cryptographic assumptions that cannot be modeled as an interactive game and consequently they are not obviously falsifiable. As a instance, assuming that a proof system is zero knowledge, is not falsifiable. Because it is not clear how to state it as an interactive game between an efficient challenger and an adversary (the definition of ZK requires the existence of a simulator for every adversary). As another example which is related to this work and are not obviously falsifiable are the various version of Knowledge assumptions such as Knowledge of Exponent [Dam91] or BDH-KE [ABLZ17].

2.3 Black-Box Reductions

The result of Gentry and Wichsy [GW11], is considers black-box reductions that prove the soundness of a SNARG \( \Pi \) based on a falsifiable assumption \( (C, c) \).
Definition 3. A (possibly inefficient) machine $\mathcal{P}$ is a $\Pi$-adversary if there exists a polynomial $p(\cdot)$ and many $n \in \mathbb{N}$ s.t. $\Pr\left[ V(x, \pi, \text{crs}, \text{priv}) = 1 \mid (\text{crs}, \text{priv}) \leftarrow G(1^n) \wedge x \notin L \mid (x, \pi) \leftarrow \mathcal{P}(1^n, \text{crs}) \right] \geq \frac{1}{p(n)}$.

Definition 4. A black-box reduction which proves the soundness of a SNARK $\Pi$ under a falsifiable assumption $(C, c)$ is an efficient oracle-access machine $R^{(\cdot)}$ such that, for every (not necessarily efficient) $\Pi$-adversary $\mathcal{P}$ the machine $R^{\mathcal{P}}$ breaks the assumption.

In this report we will see stateless adversaries $\mathcal{P}$ and it is assumed that the reduction $R^{\mathcal{P}}$ can only query the adversary with arbitrarily many inputs of the form $(1^m, \text{crs})$ with fresh random coins; where $m$ is a security parameter and it does not necessarily equal to the actual security parameter $n$.

2.4 Hard Subset Membership Problems

A subset membership problem consists of an $\mathcal{NP}$ language $L$ with a corresponding relation $R$ along with:

- A distribution-ensemble $\mathcal{L} = \{L_n\}_{n \in \mathbb{N}}$ over the language $L$ and $\bar{\mathcal{L}} = \{\bar{L}_n\}_{n \in \mathbb{N}}$ over the language $\bar{L} = \{0, 1\}^* / L$ which is outside of the language.

- An efficient sampling algorithm $(x, w) \leftarrow \text{Sam}(1^n)$ whose support lies in the relation $R$ and whose projection to the first coordinate yields the distributions $\mathcal{L} = \{L_n\}_{n \in \mathbb{N}}$.

Definition 5. Let $(\mathcal{L}, \bar{\mathcal{L}}, \text{Sam})$ be a subset-membership problem over the $\mathcal{NP}$ language $L$. The problem is called hard if the distribution-ensembles $\mathcal{L}, \bar{\mathcal{L}}$ are computationally indistinguishable. It is $(s(n), \epsilon(n))$-hard if the distributions $L_n, \bar{L}_n$ are $(s(n), \epsilon(n))$-indistinguishable. It is sub-exponentially hard if there exists some constant $\delta > 0$ such that the problem is $(s(n), \epsilon(n))$-hard with $s(n) = 2^{\Omega(n^\delta)}$, $\epsilon(n) = \frac{1}{2^{2^{\Omega(n^\delta)}}}$.

As an example for existence of hard subset membership problems, one can see that any pseudorandom generator (PRG) gives a subset membership problem by considering that $L$ is the output-distribution of the PRG and $\bar{L}$ would be uniform over all other strings.

3 Black-Box Separation of SNARGs

In this section, we will briefly go through the main result of the paper which in summary aims to show that there is no black-box reduction security proof for any SNARG construction under any kind of falsifiable assumptions (i.e. DDH, CDH, RSA, LWE, · · ·) [GW11]. This result will be proved as a theorem. But, before going through the main theorem, introducing two lemmas are necessary that show two prominent partial results of the main theorem.

The first lemma shows a result regard to indistinguishability with auxiliary information. Consider two distributions $\mathcal{L}$ and $\bar{L}$ which are computationally indistinguishable. They show that for any short auxiliary information $\pi$ that is given about samples $x \leftarrow \mathcal{L}$, there exists
some "lie" $\overline{\pi}$ that one can give about samples $\overline{\pi} \leftarrow L$ such that that $(x, \pi)$ and $(\overline{x}, \overline{\pi})$ are computationally indistinguishable as well. This result is presented as the following lemma,

**Lemma 1.** There is some polynomial poly for which the following statement holds. Assume that $L_n, \overline{L}_n$ be two arbitrary distributions that are $(s(n), \epsilon(n))$-indistinguishable. Let $L^*_n$ be some augmented distribution on tuples $(x, \pi)$, where $x$ is distributed according to $L_n$ and $\pi$ is some arbitrary correlated auxiliary information of length $|\pi| = l_n$. Then there exists an augmented distribution $\overline{L}^*_n$ on tuples $(\overline{x}, \overline{\pi})$ which similarly $\overline{x}$ distributed according to $\overline{L}_n$, such that $L^*_n$ and $\overline{L}^*_n$ are $(s^*(n), \epsilon^*(n))$-indistinguishable for $s^*(n) = s(n)poly(\epsilon(n)/2^{L(n)}, \epsilon^*(n) = 2\epsilon(n)$.

**Note on Lemma.** It is worth highlight that in the mentioned destinations $L_n, \overline{L}_n, L^*_n$ and $\overline{L}^*_n$ are not efficiently samplable. Indeed, the result of lemma will be trivial if the distribution $L^*_n$ allows us to sample $\pi$ efficiently for a particular given $x$. Similarly, if the distributions would be efficiently sampleable, trivially $\overline{L}^*_n$ can just sample $\overline{x} \in \overline{L}$ and sample $\pi$ honestly using $\overline{x}$. In the case that $\pi$ is not efficiently sampleable for $x$ (e.g. the case that $x$ depends on a witness $w$ to the fact that $x \in L_n$) it is not clear how to define the augmented distribution $\overline{L}^*_n$ on tuples $(\overline{x}, \overline{\pi})$. It is worth to mention that, the proof of lemma does not give explicit description of the augmented distribution $\overline{L}^*_n$ on tuples $(\overline{x}, \overline{\pi})$, and instead it uses von Neumann’s minmax theorem [Neu28] and shows that there exists such a distribution.

**Proof.** The detailed proof is in [GW11].

The second basic concept which has essential rule in the main result, is the existence of a simulatable adversary for any SNARG. To show that they use the result of **Lemma 1**, and show that prove this result. This result is presented as the following lemma,

**Lemma 2.** Suppose that $L$ is a language with a sub-exponentially hard subset-membership problem. Let $\Pi = (G, P, V)$ is a non-interactive proof system for the language $L$ that satisfies the completeness and succinctness properties. Then, there is a machine $\mathcal{P}$, called a simulatable $\Pi$-adversary satisfying the following:

- $\mathcal{P}$ is a stateless and computationally unbounded $\Pi$-adversary. On input $(1^n, crs)$ it always outputs some $(x, \pi)$ with $x \notin L$ of size $|x| = l_{st}(m)$, for some polynomial $l_{st}$, and:

$$\Pr[V(x, \pi, crs, priv) = 1|(crs, priv) \leftarrow \mathcal{G}(1^n), (x, \pi) \leftarrow \mathcal{P}(1^n, crs)] \geq 1 - \text{negl}(n).$$

- $\mathcal{P}$ is poly-time simulatable. That is, for every efficient distinguisher $D$ there exists some efficient simulator $S$ such that:

$$\Pr[D^{\mathcal{P}(1^n)} = 1] - \Pr[D^{S(1^n)} = 1] \leq \text{negl}(n).$$
Note that the distinguisher $D^{S}(1^n)$ can make its oracle any query $(1^m, \text{crs})$ and $m$ does not need to be equal to actual security parameter $n$. The simulator $S$ is given $1^n$ as input and can run in time polynomial in $n$ on any query.

**Proof Intuition.** Given the result of Lemma 1, the main idea of the constriction of machines $\overline{P}$ and $S$ is not complicated: on query $(1^m, \text{crs})$, the machine $S$ efficiently samples $(x, w) \leftarrow \text{Sam}(1^m)$ and computes an honest proof $\pi$ as defined in the SNARG. In the other side, $P$ samples from the corresponding fake distribution $(\overline{x}, \overline{\pi}) \leftarrow \overline{L}_{\text{crs}}$ defined in Lemma 1.

The only concern that they had is that, if the value $m$, which is used as the security parameter in the query, is small enough compared to the actual security parameter $n$, then the answers from $S$ and $P$ can be distinguished. To cope with this concern, they modify the structure of already described simulator. More precisely, they give an advice table of hard-coded responses (given as polynomial-sized non-uniform advice) to the simulator which uses it to answer all queries with a sufficiently small $m$. After enclosing the advice table, the structure of final simulator which reacts based on the value of $m$ (security parameter in query) is shown in Fig. 5. In the advice table of figure, $m^*(n) \approx \log(n)$ is a threshold value for each security parameter $n$.

**Proof.** Full proof is given in original paper [GW11].

Now, given Lemma 1 and Lemma 2, we can go trough to the main result with the following Theorem.

**Theorem 1.** Suppose that $L$ is a language with a sub-exponentially hard subset-membership problem. Let $\Pi = (G, \mathcal{P}, V)$ be a candidate non-interactive proof system for the language $L$
that satisfies the completeness and succinctness properties. Then, for any falsifiable assumption \((C, c)\), one of the two following states must holds,

- The falsifiable assumption \((C, c)\) if not true (is false).
- There is no black-box reduction to prove the soundness of \(\Pi\) based on the falsifiable assumption \((C, c)\).

**Proof.** By contradiction, suppose that there is a black-box reduction \(R\) proving the soundness property of an SNARK \(\Pi\) based on the falsifiable assumption \((C, c)\).

Now, using the result of Lemma 2, assume that \(P\) be the simulatable \(\Pi\)-adversary. Then there exists some polynomial \(q(\cdot)\) and large number of \(n \in \mathbb{N}\) for which \(\Pr[\mathcal{R}^P \text{ wins } C(1^n)] \geq c + 1/q(n)\). Now, since the challenger \(C\) is efficient, we can think of \(R\) and \(C\) together as a single efficient oracle-access distinguisher \(D^{(\cdot)}\) and, then using the result of Lemma 2, we know that there is a poly-time simulator \(S\) (See Fig. 5) such that \(\Pr[\mathcal{R}^S \text{ wins } C(1^n)] \geq c + 1/q(n) - \text{negl}(n)\).

As a result, the efficient \(\mathcal{R}^S\) will be an efficient assumption attacker which implies that the underlying falsifiable assumption \((C, c)\) is not true.

4 Conclusion

Succinct Non-Interactive Arguments are of the powerful tools in cryptography which are found in various fancy and prominent applications. In 2011, Gentry and Wichsy [GW11] presented a negative result on the construction of SNARGs in the standard model. Their result states that one cannot prove the security of SNARGs under any falsifiable assumption via a black-box reduction. In this report we presented a short overview on their research and summarized the key points of their result.

References


