A Relationship between One-Wayness and Correlation Intractability *

Satoshi Hada † Toshiaki Tanaka ‡

March 31, 1999

Abstract

The notion of correlation intractability was introduced in an attempt to capture the "unpredictability" property of random oracles: It is assumed that if R is a random oracle then it is infeasible to find an input x such that the input-output pair $(x, R(x))$ has some desired property. It is desirable that a plausible construction of correlation intractable function ensembles will be provided since the unpredictability property is often useful to design many cryptographic applications in the random oracle model. However, no plausibility result has been proposed. In this paper, we show that proving the implication, "if uniform one-way functions exist then uniform correlation intractable function ensembles exist", is as hard as proving a claim regarding the triviality of 3-round auxiliary-input zero-knowledge Arthur-Merlin proofs without making any assumptions. We believe that it is unlikely that one can prove it unconditionally. Therefore, we conclude that it will be difficult to construct uniform correlation intractable function ensembles based solely on uniform one-way functions.

Keywords: One-way functions, correlation intractability, zero-knowledge, interactive proofs, round complexity, random oracle.

*An earlier version of this paper appeared in PKC'99 [HT99]. We reformulated our claims since our original ones were wrong.

†KDD R&D Laboratories, 2-1-15 Ohara, Kamifukuoka, Saitama 356-8502, Japan. `mailto:hada@lab.kdd.co.jp`.

‡KDD, 2-3-2 Nishishinjuku, Shinjuku-ku, Tokyo 163-8003, Japan. `mailto:tl-tanaka@kdd.co.jp`.

Contents

1 Introduction

In this paper, we investigate the round complexity of auxiliary-input zero-knowledge proofs and derive a relationship between one-wayness and correlation intractability.

1.1 Realizing Random Oracles

The random oracle model formulated in [BeRo93] is an ideal model in which all parties have oracle access to a truly random function (a random oracle). This model is very useful for designing cryptographic schemes such as public key encryption and digital signature since the schemes in this model are often very simple and efficient; Moreover, the security analysis is often clearer than in real life. The random oracle methodology consists of the following two steps. One first designs an ideal scheme in the random oracle model and proves the security of this ideal scheme. Next, one replaces the random oracle by a cryptographic hash function (such as MD5 or SHA) in order to obtain an implementation of this ideal scheme. Note that random oracles do not exist in real life.

Unfortunately, we do not have a general method of obtaining a good implementation which remains secure even in real life. Indeed, Canetti, Goldreich and Halevi showed that there exist digital signature and public key encryption schemes which are secure in the random oracle model, but for which any implementation yields insecure schemes [CGH98]. However, their result does not rule out the existence of an ideal scheme for which an implementation remains secure. Consider an ideal scheme whose security depends on some specific properties of random oracles. If one can construct cryptographic hash functions satisfying these properties in real life, it may be possible to obtain a good implementation which is secure even in real life. First attempts at identifying, defining and realizing the useful properties of random oracles have been made by Canetti [Ca97]. He roughly sketched two properties. One is "total secrecy": It is assumed that if $F(\cdot)$ is a random oracle, $F(x)$ gives no information on x. The other property is "unpredictability": It is assumed to be infeasible to find an input x such that the input-output pair $(x, F(x))$ has some desired property.

Canetti introduced a new primitive called "oracle hashing" (renamed "perfectly one-way hash functions" in [CMR98]) in an attempt to capture the total secrecy [Ca97]. Recently, it was shown that perfectly one-way hash functions can be constructed based on any one-way permutation [CMR98]. On the other hand, Canetti, Goldreich and Halevi introduced another new primitive called "correlation intractable function ensembles" in order to capture the unpredictability [CGH98] [1]. The requirement of this primitive seems to be much stronger than ones of other cryptographic primitives such as one-way functions, trapdoor permutations and collision-intractable hash functions. Indeed, they showed that there exist no correlation intractable function ensembles. However, their result leaves open the question of the existence of *restricted* correlation intractable function ensembles, where "restricted" means that each function will only be applied to inputs of pre-specified length. They described that it is interesting to either provide a negative result also for this restricted case or provide a plausible construction based on general complexity assumptions. In light of the above, it is important to investigate the relationships among restricted correlation intractable function ensembles and other cryptographic primitives.

This paper addresses the question of whether one can prove the following implication:

If one-way functions exist,
then restricted correlation intractable function ensembles exist.

Our answer is a negative one: It seems difficult to prove it. This relationship between one-wayness

[1]A weaker primitive called correlation free hash functions was introduced by Okamoto in [Ok92].

and restricted correlation intractability is obtained by investigating the lower bounds on the round complexity of auxiliary-input zero-knowledge proofs.

1.2 The Round Complexity of Auxiliary-Input Zero-Knowledge

Zero-knowledge (ZK) protocols introduced in [GMR85] play a central role in modern cryptography. The round complexity, the number of messages exchanged, is a standard complexity measure for the efficiency of ZK protocols [2]. The lower bounds on the round complexity have been investigated from the practical and theoretical viewpoint so far. Goldreich and Oren showed that only languages in $\mathcal{BPP}$ have 1-round GMR-ZK protocols [GoOr94], where GMR-ZK is the original definition of ZK [GMR85]. They also showed that only languages in $\mathcal{BPP}$ have 2-round auxiliary-input ZK (AIZK) protocols [GoOr94]. Furthermore, Goldreich and Krawczyk showed that only languages in $\mathcal{BPP}$ have 3-round black-box simulation ZK (BSZK) protocols [GoKr96] [3]. Since the argument in [GoKr96] uses the notion of black-box simulation in an essential way, their result does not apply to the weaker notions of GMR-ZK and AIZK. In fact, it is an interesting open problem whether there exist 3-round GMR-ZK or AIZK protocols for a non-trivial language.

With respect to secret-coin type protocols, it was shown that a 3-round AIZK protocol exists for any NP language under non-standard computational assumptions although they seem to be unreasonable [HT98]. In this paper, we focus on public-coin type protocols, so called *Arthur-Merlin* (AM) protocols [BaMo88]. Recall that in AM protocols, the prescribed verifier chooses all its messages at random, that is, all the messages sent by the verifier are (public) random coins. In 3-round AM protocols, a cheating verifier may choose its public-coin message (challenge message) as the value of a cryptographic hash function on the common input and the first message sent by the prover. Many researchers considered that the simulation for such a cheating verifier is difficult to do. Indeed, the only known way to complete the simulation is to repeat the black-box simulation of the cheating verifier until he outputs the desired (pre-determined) challenge message, but it seems to require an exponential number of trials. Therefore, we naturally conjecture that *assuming the existence of cryptographic hash functions*, only trivial languages such as $\mathcal{BPP}$ languages have 3-round ZK protocols [4].

In this paper, we consider the question of whether one can prove the following claim:

there exist 3-round GMR-ZK or AIZK AM proofs
only for trivial languages such as $\mathcal{BPP}$ languages.

As far as we know, proving it *unconditionally* is an open problem in the theory of zero-knowledge. We stress again that although Glodreich and Krawczyk proved that 3-round BSZK proofs exist only for BPP languages without making any assumptions, their argument does not apply to the weaker notions of GMR-ZK and AIZK which we consider here. We believe that it is unlikely that one can prove the above claim without making any assumptions. However, as described above, it may be possible to prove it *assuming the existence of cryptographic hash functions.* This paper shows what can be proven if we use restricted correlation intractable function ensembles as cryptographic hash functions.

[2] In this paper, we consider protocols with negligible error probability in completeness and soundness conditions.

[3] It is known that $Cl(BSZK) \subseteq Cl(AIZK) \subset Cl(GMR-ZK)$ where $Cl(def)$ denotes the class of all ZK protocols satisfying the requirements of definition def [GoOr94].

[4] Nevertheless, Goldreich and Krawczyk showed that only languages in $\mathcal{BPP}$ have 3-round BSZK protocols without making any assumptions [GoKr96]. Their proof uses the notion of black-box simulation in an essential way so that they can make use of a (deterministic) cheating verifier which behaves as a random oracle.

1.3 Our Results and Related Works

We show that assuming the existence of restricted *non-uniform* correlation intractable function ensembles, 3-round AIZK AM proofs exist only for $\mathcal{BPP}$ languages. Our proof of this result uses the non-uniformity of non-uniform correlation intractability in an essential way. We also show what can be proven if we only assume the existence of restricted *uniform* correlation intractable function ensembles. Our first feeling was that one can prove that 3-round AIZK AM proofs exist only for easy-to-approximate languages: We say that a language is easy to approximate if it can be recognized in probabilistic polynomial-time on average when the instance is generated from any polynomial sampleable distribution. Unfortunately, we don't know whether one can do it. Alternatively, we show a weaker result which says that assuming the existence of restricted uniform correlation intractable function ensembles, 3-round AIZK AM proofs with *perfect completeness* and 3-round auxiliary-input *statistical* ZK (AISZK) AM proofs exist only for easy-to-approximate languages. These triviality results are our main technical contributions. We argue that our results extend to both the argument model and the constant round case. Therefore, we may say that our results complement the ones of [GoKr96] with respect to AM protocols although the complexity assumptions are required.

We derive a relationship between uniform one-wayness and restricted uniform correlation intractability by combining the above triviality result in the uniform case with the result of Ostrovsky and Wigderson [OW93] which shows that uniform one-way functions are essential for zero-knowledge proofs for a hard-on-average language (See also [Go98, Theorem 4.5.4]). That is, we show that proving the implication, "if uniform one-way functions exist then restricted uniform correlation intractable function ensembles exist", is as hard as proving that "3-round AIZK AM proofs with perfect completeness and 3-round AISZK AM proofs exist only for easy-to-approximate languages." As described before, we believe that it is unlikely that one can prove the latter claim unconditionally although it is restricted to AIZK proofs with the perfect completeness or the statistical zero-knowledgeness. Therefore, we conclude that it will be difficult to construct restricted uniform correlation intractable function ensembles based solely on uniform one-way functions.

The limits on the provable consequences of one-wayness were studied in [ImRu89]. Impagliazzo and Rudich showed that constructing a secure secret-key agreement protocol using any one-way permutation as a "black-box" is as hard as proving $\mathcal{P} \neq \mathcal{NP}$. That is, it is highly unlikely that secret-key agreement protocols can be constructed based on any one-way permutation. Recently, Simon showed that there is no "black-box" reduction from one-way permutations to collision intractable hash functions [Si98]. We note that both results leave open the question of the existence of *non-relativizing* reduction from one-way permutations to secret-key agreement protocols or collision intractable hash functions. In non-relativizing reductions, one can analyze the actual program for any one-way permutation, rather than only use it as a black-box. Our result can be viewed as a stronger type of limit since our result says that there does not seem to exist even a non-relativizing reduction from uniform one-way functions to restricted uniform correlation intractable function ensembles.

1.4 Organization

In Section 2, we give the definitions of the class of trivial languages, zero-knowledge protocols and restricted correlation intractability. In Section 3, we give the triviality results regarding 3-round AIZK AM proofs. Section 4 presents the relationship between uniform one-way functions and restricted uniform correlation intractable function ensembles. We conclude with some remarks in Section 5.

2 Preliminaries

We say that a function $\nu(\cdot) : \mathsf{N} \to \mathsf{R}$ is negligible in n if for every polynomial $poly(\cdot)$ and all sufficiently large n's, it holds that $\nu(n) < 1/poly(n)$. Also, we say that a function $f(\cdot) : \mathsf{N} \to \mathsf{R}$ is overwhelming in n if there exists a negligible (in n) function $\nu(\cdot)$ such that $f(\cdot) = 1 - \nu(\cdot)$. We often omit the expression "in n" when the definition of n will be clear by the context.

If S is any probability distribution then $x \leftarrow S$ denotes the operation of selecting an element uniformly at random according to S. If S is a set then we use the same notation to denote the operation of picking an element x uniformly from S. If A is a probabilistic machine then $A(x_1, x_2, \cdots, x_k)$ denotes the output distribution of A on inputs $(x_1, x_2, \cdots, x_k)$. Also, $\{x_1 \leftarrow S_1; x_2 \leftarrow S_2; \cdots x_k \leftarrow S_k : A(x_1, x_2, \cdots, x_k)\}$ denotes the output distribution of A on inputs $(x_1, x_2, \cdots, x_k)$ when the processes $x_1 \leftarrow S_1, x_2 \leftarrow S_2, \cdots, x_k \leftarrow S_k$ are performed in order. Let $\Pr[x \leftarrow S_1; x_2 \leftarrow S_2; \cdots; x_k \leftarrow S_k : E]$ denote the probability of the event E after the processes $x_1 \leftarrow S_1, x_2 \leftarrow S_2, \cdots, x_k \leftarrow S_k$ are performed in order.

Let S be a probabilistic distribution. Then we denote by $[S]$ the set of elements which S gives positive probability, i.e., $[S] = \{e \mid \Pr[b \leftarrow S : b = e] > 0\}$. We also denote by $\Pr[x = S]$ the probability that S associates with x, i.e., $\Pr[x = S] = \Pr[x' \leftarrow S : x' = x]$.

2.1 The Class of Trivial Languages

For any language L, we denote by χ_L the characteristic function of the language L, that is, $\chi_L(x) = \mathsf{Acc}$ if $x \in L$ and $\chi_L(x) = \mathsf{Rej}$ otherwise. $\mathcal{BPP}$ is a typical class of "trivial" languages.

Definition 2.1 [$\mathcal{BPP}$] We say that a language L is in $\mathcal{BPP}$ if there exists a probabilistic polynomial-time machine A such that for every polynomial $poly(\cdot)$ and all sufficiently long x's, $\Pr[b \leftarrow A(x) : b = \chi_L(x)] > 1 - 1/poly(|x|)$.

The class of trivial languages is not only $\mathcal{BPP}$. We define the class of easy-to-approximate languages which is a variant of the class of hard-to-approximate languages defined in [Go98, Definition 4.5.3 on p.180].

Definition 2.2 [$\mathcal{ETA}$] We say that a language L is easy to approximate if for every probabilistic polynomial-time machine X, there exists a probabilistic polynomial-time machine A such that for every polynomial $poly(\cdot)$ and all sufficiently large n's, $\Pr[x \leftarrow X(1^n); b \leftarrow A(x) : b = \chi_L(x)] > 1 - 1/poly(n)$, where $X(1^n)$ ranges over $\{0,1\}^n$. We denote by $\mathcal{ETA}$ the class of easy-to-approximate languages.

$\mathcal{BPP}$ requires that every instance is easy to recognize. On the other hand, $\mathcal{ETA}$ only requires that it is infeasible to find an instance which is hard to recognize. Therefore, it holds that $\mathcal{BPP} \subseteq \mathcal{ETA}$.

2.2 Interactive Proofs and Arguments

We consider two probabilistic interactive machines called the prover and the verifier. The verifier is always a probabilistic polynomial-time machine. Initially both machines have access to a common input tape which includes x of length n. The prover and the verifier send messages to one another through two communication tapes. After exchanging a polynomial number of messages, the verifier stops in an accept state or in a reject state. Each machine only sees its own tapes, namely, the common input tape, the random tape, the auxiliary-input tape and the communication tapes.

Let $\langle P_x^w, V_x^y \rangle$ denote the distribution of the decision (over $\{\mathsf{Acc}, \mathsf{Rej}\}$) of the verifier V having an auxiliary-input y when interacting on a common input x with the prover P having an auxiliary-input w, where the probability is taken over the random tapes of both machines.

We deal with two kinds of interactive protocols. One is "interactive proof" and the other is "interactive argument". The former requires that even a computationally unrestricted prover should be unable to make the verifier accept $x \notin L$, except with negligible probability [GMR85]. On the other hand, the latter requires that any cheating prover restricted to probabilistic polynomial-time should be unable to make the verifier accept $x \notin L$, except with negligible probability [BrCr86][BCC88]. In both definitions below, the verifier V does not take the auxiliary-input.

Definition 2.3 [interactive proofs [GMR85]] Let P, V be two probabilistic interactive machines. We say that (P, V) is an interactive proof for L if V is a probabilistic polynomial-time machine and the following two conditions hold:

- Completeness: For every polynomial $poly(\cdot)$, all sufficiently long $x \in L$,

$$\Pr[b \leftarrow \langle P_x, V_x \rangle : b = \mathsf{Acc}] > 1 - 1/poly(|x|).$$

- Statistical Soundness: For every machine $\widehat{P}$ (the computationally unrestricted cheating prover), every polynomial $poly(\cdot)$, all sufficiently long $x \notin L$,

$$\Pr[b \leftarrow \langle P_x, V_x \rangle : b = \mathsf{Rej}] > 1 - 1/poly(|x|).$$

Since the prover P and $\widehat{P}$ are computationally unrestricted, the auxiliary-inputs to them are omitted.

Definition 2.4 [interactive arguments [Go98]] Let P, V be two probabilistic polynomial-time interactive machines. We say that (P, V) is an interactive argument for L if the following two conditions hold:

- Efficient Completeness: For every polynomial $poly(\cdot)$, all sufficiently long $x \in L$, there exists an auxiliary-input w such that

$$\Pr[b \leftarrow \langle P_x^w, V_x \rangle : b = \mathsf{Acc}] > 1 - 1/poly(|x|).$$

- Computational Soundness: For every probabilistic polynomial-time machine $\widehat{P}$ (the polynomial-time bounded cheating prover), every polynomial $poly(\cdot)$, all sufficiently long $x \notin L$ and every auxiliary-input w,

$$\Pr[b \leftarrow \langle P_x^w, V_x \rangle : b = \mathsf{Rej}] > 1 - 1/poly(|x|).$$

We say that (P, V) is an interactive proof (resp., argument) with perfect completeness if the error probability in the completeness (resp., efficient completeness) condition is 0, that is, the verifier V always accepts $x \in L$.

2.3 Auxiliary-Input Zero-Knowledge

We recall the definition of auxiliary-input zero-knowledge. A *view* of the verifier is a distribution ensemble which consists of the common input, the verifier's auxiliary input, the verifier's random coins and the sequence of messages sent by the prover and the verifier during the interaction. Let $\mathsf{View}(P_x, V_x^y) = [x, y, m; R]$ denote V's view after interacting with P, where x is the common input, y the auxiliary input to V, R the random coins of V and m the sequence of messages sent by P and V. For simplicity, in the following definition, we omit the auxiliary-input to the prover P.

Definition 2.5 [auxiliary-input zero-knowledge (AIZK) [GoOr94]] Let P, V be two probabilistic interactive machines. We say that (P, V) is auxiliary-input zero-knowledge for L if for every probabilistic polynomial-time machine $\widehat{V}$ (the cheating verifier), there exists a probabilistic polynomial-time machine $S_{\widehat{V}}$ (the simulator) such that the following two distribution ensembles are computationally indistinguishable:

$$\{S_{\widehat{V}}(x, y)\}_{x \in L, y \in \{0,1\}^*} \text{ and } \{\mathsf{View}(P_x, \widehat{V}_x^y)\}_{x \in L, y \in \{0,1\}^*}.$$

Namely, for every polynomial-size circuit family $D = \{D_{x,y}\}_{x \in L, y \in \{0,1\}^*}$, every polynomial $poly(\cdot)$, all sufficiently long $x \in L$ and all $y \in \{0,1\}^*$,

$$|\Pr[v \leftarrow S_{\widehat{V}}(x, y) : D_{x,y}(v) = 1] - \Pr[v \leftarrow \mathsf{View}(P_x, \widehat{V}_x^y) : D_{x,y}(v) = 1]| < \frac{1}{poly(|x|)}.$$

We say that (P, V) is auxiliary-input statistical zero-knowledge (AISZK) for L if the above two distributions are statistically close.

GMR-ZK is defined in the same way, except that the verifier is not allowed to take the auxiliary-input y. We denote by $\mathcal{ZK}$ (resp., $\mathcal{AIZK}$) the class of languages that have GMR-ZK (resp., AIZK) interactive proofs. Also, we denote by $\mathit{3}\mathcal{R}$-$\mathcal{AIZK}$-$\mathcal{AM}$ the class of languages that have 3-round AIZK AM interactive proofs. Since all $\mathcal{BPP}$ languages have trivial AIZK proofs where any interaction is not carried out, it holds that $\mathcal{BPP} \subseteq \mathit{3}\mathcal{R}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM} \subseteq \mathcal{AIZK} \subseteq \mathcal{ZK}$.

2.4 Restricted Correlation Intractable Function Ensembles

We review the definition of *restricted* correlation intractable function ensembles introduced in [CGH98]. The original definitions were formalized in the uniform model. In this paper, we give not only the uniform definitions but also the non-uniform ones. Let $l_{in}, l_{out} : \mathsf{N} \to \mathsf{N}$ be length functions.

Definition 2.6 [function ensembles] An l_{out}-function ensemble is a sequence $\mathcal{F} = \{F_k\}_{k \in \mathsf{N}}$ of function family $F_k = \{f_s : \{0,1\}^* \to \{0,1\}^{l_{out}(k)}\}_{s \in \{0,1\}^k}$, so that the following two conditions hold:

- Length requirement: For every $s \in \{0,1\}^k$ and every $x \in \{0,1\}^*$, $|f_s(x)| = l_{out}(k)$.
- Efficiency: There exists a polynomial-time algorithm $Eval$ so that for all $s \in \{0,1\}^k$ and $x \in \{0,1\}^*$, $Eval(s, x) = f_s(x)$. In the sequel, we call s the *seed* or the *description* of the function f_s.

A machine M is called l_{in}-respectful if $|M(s)| = l_{in}(|s|)$ for all $s \in \{0,1\}^*$. A uniform function ensemble $\mathcal{U}_{l_{in}, l_{out}}$ is a sequence $\{U_{l_{in}(k), l_{out}(k)}\}_{k \in \mathsf{N}}$, where $U_{l_{in}(k), l_{out}(k)}$ is a set of all functions $f : \{0,1\}^{l_{in}(k)} \to \{0,1\}^{l_{out}(k)}$.

We say that a relation R is *evasive* if it is hard to find an input-output pair satisfying R under a truly random function (in the random oracle model). Note that there is a relation that is easy to satisfy even under a truly random function (e.g. $(x, y) \in R \Leftrightarrow y$ is an odd number).

Definition 2.7 [evasive relations] A binary relation R is uniformly evasive with respect to (l_{in}, l_{out}) if for every l_{in}-respectful probabilistic polynomial-time machine M, every polynomial $poly(\cdot)$ and all sufficiently large k's,

$$\Pr[\mathcal{O} \leftarrow U_{l_{in}(k),l_{out}(k)}; x \leftarrow M^{\mathcal{O}}(1^k) : (x, \mathcal{O}(x)) \in R] < \frac{1}{poly(k)}.$$

Also, we say that R is non-uniformly evasive with respect to (l_{in}, l_{out}) if the above condition holds for every l_{in}-respectful polynomial-size circuit family M.

A special case of non-uniformly evasive relations consists of R's for which for every polynomial $poly(\cdot)$ and all sufficiently large k's,

$$\max_{x \in \{0,1\}_{l_{in}(k)}} \{\Pr[y \leftarrow \{0,1\}^{l_{out}(k)} : (x, y) \in R]\} < \frac{1}{poly(k)}.$$

We say that a function ensemble $\mathcal{F}$ is (l_{in}, l_{out})*-restricted correlation intractable* if, given any evasive relation R with respect to (l_{in}, l_{out}) and a randomly chosen description of function f_s, it is hard to find an input-output pair satisfying R under f_s.

Definition 2.8 [restricted correlation intractability] We say that an l_{out}-function ensemble $\mathcal{F}$ is (l_{in}, l_{out})-restricted uniform correlation intractable if for every l_{in}-respectful probabilistic polynomial-time machine M, every uniformly evasive relation R with respect to (l_{in}, l_{out}), every polynomial $poly(\cdot)$ and all sufficiently large k's,

$$\Pr[s \leftarrow \{0,1\}^k; x \leftarrow M(s) : (x, f_s(x)) \in R] < \frac{1}{poly(k)}.$$

Also, we say that an l_{out}-function ensemble $\mathcal{F}$ is (l_{in}, l_{out})-restricted non-uniform correlation intractable if the above condition holds for every l_{in}-respectful polynomial-size circuit family M and every non-uniformly evasive relation R with respect to (l_{in}, l_{out}).

The following remarks apply to both the uniform case and the non-uniform case.

Remark 2.9 [Do such functions really exist ?] If $l_{out}(k) = O(\log k)$, there exist no (l_{in}, l_{out})-restricted correlation intractable function ensembles. Therefore, we always assume that $\omega(\log k) \leq l_{out}(k) \leq poly(k)$ in the sequel. Canetti, Goldreich and Halevi showed that if $l_{in}(k) \geq k - O(\log k)$ for infinitely many k's or if $l_{in}(k) + l_{out}(k) \geq k + \omega(\log k)$ for infinitely many k's, then there exist no (l_{in}, l_{out})-restricted correlation intractable function ensembles [CGH98, Proposition 11]. However, their results leave open the question of the existence of restricted correlation intractable function ensembles, for the case $l_{in}(k) + l_{out}(k) < k + O(\log k)$. Therefore, when we say that *there exist restricted correlation intractable function ensembles*, we mean that for any pair of length functions (l_{in}, l_{out}) such that $l_{in}(k) + l_{out}(k) < k + O(\log k)$, there exists an (l_{in}, l_{out})-restricted correlation intractable function ensemble.

Remark 2.10 [weak correlation intractability [CGH98, Remark 3]] Definition 2.8 quantifies over all evasive relations. A weaker notion, called restricted *weak* correlation intractability, is obtained by quantifying only over all *polynomial-time recognizable* evasive relations.

3 The Complexity of 3-Round AIZK AM Proofs

In this section, we prove the triviality results regarding 3-round AIZK AM proofs. In the non-uniform case, we show that assuming the existence of restricted non-uniform correlation intractable function ensembles, it holds that $\mathit{3}\mathcal{R}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM} = \mathcal{BPP}$. On the other hand, in the uniform case, we show that assuming the existence of restricted uniform correlation intractable function ensembles, 3-round AIZK AM proofs with perfect completeness and 3-round AISZK AM proofs exist only for $\mathcal{ETA}$ languages. We begin with the non-uniform case.

3.1 The Non-Uniform Case

Theorem 3.1 [$\mathcal{BPP}$ Version] Assume that there exist restricted non-uniform correlation intractable function ensembles. Then $\mathit{3}\mathcal{R}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM} = \mathcal{BPP}$.

Proof: As described before, it is clear that $\mathcal{BPP} \subseteq \mathit{3}\mathcal{R}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM}$. Therefore, we focus on the proof of $\mathit{3}\mathcal{R}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM} \subseteq \mathcal{BPP}$. We assume that a language L has a 3-round AIZK AM interactive proof (P, V) and then we show that L is in $\mathcal{BPP}$. Our proof uses the non-uniformity of restricted non-uniform correlation intractability in an essential way.

We use the following notations for 3-round AM proofs (P, V). Denote by x the common input and by n the length of x. The first and second messages sent by the prover P are denoted by α and γ, respectively. β denotes the challenge message of the verifier V. We denote by $l_\alpha(n)$ and $l_\beta(n)$ the length of α and β, respectively. Without loss of generality, we assume that the verifier chooses β uniformly at random in $\{0,1\}^{l_\beta(n)}$. The predicate computed by the verifier in order to decide whether to accept or reject is denoted by $\rho_V(x, \alpha, \beta, \gamma)$. That is, V accepts x if and only if $\rho_V(x, \alpha, \beta, \gamma) = \mathsf{Acc}$. We note that ρ_V may be a randomized function.

Firstly, we select an (l_{in}, l_{out})-restricted non-uniform correlation intractable function ensemble $\mathcal{F} = \{F_k\}_{k\in\mathsf{N}}$ and a seed length k such that $l_{in}(k) = n + l_\alpha(n)$ and $l_{out}(k) = l_\beta(n)$. We must select the length functions (l_{in}, l_{out}) satisfying the condition $k + O(\log k) > l_{in}(k) + l_{out}(k)$. Since the verifier is a polynomial-time machine, there exist constants c, d such that $n + l_\alpha(n) + l_\beta(n) < cn^d$. Therefore, if we set $k = cn^d$ and select (l_{in}, l_{out}) such that $l_{in}(k) = (k/c)^{1/d} + l_\alpha((k/c)^{1/d})$ and $l_{out}(k) = l_\beta((k/c)^{1/d})$, then the desired condition $k + O(\log k) > k > l_{in}(k) + l_{out}(k)$ is satisfied. We note that a function is negligible (resp., overwhelming) "in n" if and only if it is negligible (resp., overwhelming) "in k". Therefore, even if we omit the expressions "in n" and "in k", there is no ambiguity.

Next, we consider a (deterministic) cheating verifier $\widehat{V}$ which uses the selected (l_{in}, l_{out})-restricted non-uniform correlation intractable function ensemble $\mathcal{F} = \{F_k\}_{k\in\mathsf{N}}$ ($F_k = \{f_s\}_{s\in\{0,1\}^k}$) to compute the challenge message β from the common input x and the first message α. The key idea is to let $\widehat{V}$ use its auxiliary-input as a seed of $\mathcal{F}$.

Machine: The cheating verifier $\widehat{V}$.

Input: x of length n, the auxiliary-input y and the first message α.

Output: The challenge message $\beta = \widehat{V}(x, y, \alpha)$.

CV1: $\widehat{V}$ checks if y is of length $k = cn^d$. If this is false then $\widehat{V}$ aborts.

CV2: $\widehat{V}$ computes $\beta = f_y(x\|\alpha)$ and outputs β. Note that we selected (l_{in}, l_{out}) so that $l_{in}(k) = |x\|\alpha|$ and $l_{out}(k) = |\beta|$.

Except for the computation of β, $\widehat{V}$ behaves in the same way as the prescribed verifier V.

Since we assumed that the language L has an AIZK interactive proof, there exists a simulator $S_{\widehat{V}}$ for this cheating verifier $\widehat{V}$. We construct a probabilistic polynomial-time machine A which uses $S_{\widehat{V}}$ to recognize L.

Machine: A.
Input: x of length n.
Output: Acc or Rej.
A1: A generates a string s uniformly at random in $\{0,1\}^k$, where $k = cn^d$.
A2: A runs $S_{\widehat{V}}(x, s)$ to get a view $[x, s, \alpha\beta\gamma; -]$, where the random coins of $\widehat{V}$ are empty since it is deterministic.
A3: A computes $\beta' = f_s(x\|\alpha)$.
A4: A outputs $\rho_V(x, \alpha, \beta', \gamma)$.

If $x \in L$ then the zero-knowledgeness of (P, V) guarantees that β is equal to β' with overwhelming probability. However, if $x \notin L$ then β may not be equal to β' with not negligible probability.

In order to complete the proof, we need to show that if $x \in L$ then A outputs Acc with overwhelming probability, otherwise A outputs Rej with overwhelming probability. That is, we will show that the probability

$$\Pr[s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha) : b \leftarrow \rho_V(x, \alpha, \beta', \gamma) : b = \chi_L(x)]$$

is overwhelming.

__**The case of $x \notin L$.**__ This part of the proof uses the statistical soundness of the protocol (P, V) and the restricted non-uniform correlation intractability of $\mathcal{F}$.

We consider a relation $R_{\notin L}$ defined as follows:

$$(x\|\alpha, \beta) \in R_{\notin L} \iff \begin{array}{l} x \notin L, \\ \exists\gamma, \Pr[b \leftarrow \rho_V(x, \alpha, \beta, \gamma) : b = \mathsf{Acc}] \text{ is not negligible.} \end{array}$$

Roughly speaking, $(x\|\alpha, \beta) \in R_{\notin L}$ is a prefix of a conversation where the verifier V accepts x in spite of the fact $x \notin L$.

Claim 3.2 $R_{\notin L}$ is non-uniformly evasive with respect to (l_{in}, l_{out}).

Proof: It follows from the statistical soundness, which requires that for every polynomial $poly(\cdot)$, all sufficiently long $x \notin L$ ($|x| = n$) and every $\alpha \in \{0,1\}^{l_\alpha(n)}$,

$$\Pr[\beta \leftarrow \{0,1\}^{l_\beta(n)} : (x\|\alpha, \beta) \in R_{\notin L}] < \frac{1}{poly(n)}.$$

Since $k = cn^d$, for every polynomial $poly(\cdot)$ and all sufficiently large k's, we have

$$\max_{x\|\alpha \in \{0,1\}^{l_{in}(k)}} \{\Pr[\beta \leftarrow \{0,1\}^{l_{out}(k)} : (x\|\alpha, \beta) \in R_{\notin L}]\} < \frac{1}{poly(k)}.$$

This means that $R_{\notin L}$ is non-uniformly evasive. ▮

Next, we claim that when s is chosen uniformly at random in $\{0,1\}^k$, the probability that $S_{\widehat{V}}$ outputs α satisfying $(x\|\alpha, f_s(x\|\alpha)) \in R_{\notin L}$ is negligible.

Claim 3.3 The probability

$$\Pr[s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha) : (x\|\alpha, \beta') \in R_{\notin L}]$$

is negligible.

Proof: Assume that this probability is not negligible. Then we can construct a polynomial-size circuit family $M = \{M_k\}_{k\geq 1}$ which violates the restricted non-uniform correlation intractability of $\mathcal{F}$. For simplicity, we describe M as a probabilistic polynomial-time algorithm with a non-uniform advice string. We note that M_k can take as the advice the common input $x \notin L$ which we care about now.

Circuit: M_k.
Input: The seed s chosen uniformly at random in $\{0,1\}^k$.
Advice: The common input $x \notin L$.
Output: $x\|\alpha$.
M1: M_k runs $S_{\widehat{V}}(x, s)$ to get a view $[x, s, \alpha\beta\gamma; -]$.
M2: M_k outputs $x\|\alpha$.

Clearly, the probability that M_k outputs $x\|\alpha$ satisfying $(x\|\alpha, f_s(x\|\alpha)) \in R_{\notin L}$ is not negligible when s is chosen uniformly at random in $\{0,1\}^k$. This contradicts the restricted non-uniform correlation intractability of $\mathcal{F}$ since $R_{\notin L}$ is non-uniformly evasive. ▮

By the definition of $R_{\notin L}$, Claim 3.3 means that the probability

$$\Pr[s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha) : b \leftarrow \rho_V(x, \alpha, \beta', \gamma) : b = \mathsf{Acc}]$$

is negligible. Therefore, we conclude that A outputs Rej with overwhelming probability.

<u>The case of $x \in L$.</u> This part of the proof uses the completeness, the zero-knowledgeness of the protocol (P, V) and the restricted non-uniform correlation intractability of $\mathcal{F}$.

Let $P_x(-)$ denote the probability distribution of P's first message α on the common input x. Let $P_x(\alpha\beta)$ denote the conditional distribution of the message γ assuming that P output the first message α. Therefore, the distribution $\langle P_x, V_x\rangle$ is identical to the distribution $\{\alpha \leftarrow P_x(-); \beta \leftarrow \{0,1\}^{l_\beta(n)}; \gamma \leftarrow P_x(\alpha\beta) : \rho_V(x, \alpha, \beta, \gamma)\}$.

We consider a relation $R_{\in L}$ defined as follows:

$$(x\|\alpha, \beta) \in R_{\in L} \iff \begin{array}{l} x \in L, \\ \alpha \in [P_x(-)], \\ \Pr[\alpha = P_x(-)] \cdot \Pr[\gamma \leftarrow P_x(\alpha\beta); b \leftarrow \rho_V(x, \alpha, \beta, \gamma) : b = \mathsf{Rej}] \text{ is not negligible.} \end{array}$$

Roughly speaking, $(x\|\alpha, \beta) \in R_{\in L}$ is a prefix of a conversation where the verifier V rejects x in spite of the fact that α is computed by the prover P on $x \in L$.

Claim 3.4 $R_{\in L}$ is non-uniformly evasive with respect to (l_{in}, l_{out}).

Proof: It follows from the completeness. The completeness requires that if for every polynomial $poly(\cdot)$, all sufficiently long $x \in L$ ($|x| = n$), and every $\alpha \in [P_x(-)]$,

$$\Pr[\beta \leftarrow \{0,1\}^{l_\beta(n)} : (x\|\alpha, \beta) \in R_{\in L}] < \frac{1}{poly(n)}.$$

Since $k = cn^d$, for every polynomial $poly(\cdot)$ and all sufficiently large k's, we have

$$\max_{x\|\alpha \in \{0,1\}^{l_{in}(k)}} \{\Pr[\beta \leftarrow \{0,1\}^{l_{out}(k)} : (x\|\alpha, \beta) \in R_{\in L}] < \frac{1}{poly(k)}\}.$$

This means that $R_{\in L}$ is non-uniformly evasive. ▮

We remark that if $R_{\in L}$ does not require the condition $\alpha \in [P_x(-)]$, $R_{\in L}$ is not necessarily non-uniformly evasive.

Next, we claim that when $\widehat{V}$'s auxiliary-input y is chosen uniformly at random in $\{0,1\}^k$, the cheating verifier $\widehat{V}$ accepts $x \in L$ with overwhelming probability after interacting with the prover P. This claim is given formally as follows:

Claim 3.5 The probability

$$\begin{aligned} & \Pr[y \leftarrow \{0,1\}^k; b \leftarrow \langle P_x, \widehat{V}_x^y \rangle : b = \mathsf{Rej}] \\ = \; & \Pr[s \leftarrow \{0,1\}^k; \alpha \leftarrow P_x(-); \beta = f_s(x\|\alpha); \gamma \leftarrow P_x(\alpha\beta); b \leftarrow \rho_V(x, \alpha, \beta, \gamma) : b = \mathsf{Rej}] \end{aligned}$$

is negligible.

Proof: Assume that this probability is not negligible. Then, by the definition of $R_{\in L}$, the probability

$$\Pr[s \leftarrow \{0,1\}^k; \alpha \leftarrow P_x(-); \beta = f_s(x\|\alpha) : (x\|\alpha, \beta) \in R_{x \in L}]$$

is not negligible. This means that there exists a string $\alpha \in [P_x(-)]$ such that

$$\Pr[s \leftarrow \{0,1\}^k; \beta = f_s(x\|\alpha) : (x\|\alpha, \beta) \in R_{\in L}]$$

is not negligible. We don't know whether one can produce such a string α in probabilistic polynomial-time, but it exists. Therefore, the following (trivial) polynomial-size circuit family $M = \{M_k\}_{k \geq 1}$ violates the restricted non-uniform correlation intractability of $\mathcal{F}$.

Circuit: M_k.
Input: The seed s chosen uniformly at random in $\{0,1\}^k$.
Advice: The common input $x \in L$ and the string $\alpha \in [P_x(-)]$.
Output: $x\|\alpha$.
M1: M_k outputs $x\|\alpha$.

Clearly, M_k outputs $x\|\alpha$ satisfying $(x\|\alpha, f_s(x\|\alpha)) \in R_{\in L}$ with not negligible probability. This contradicts the restricted non-uniform correlation intractability of $\mathcal{F}$ since $R_{\in L}$ is non-uniformly evasive. ▌

By combining Claim 3.5 and the zero-knowledgeness of (P, V), it follows that the probability

$$\Pr[s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); b \leftarrow \rho_V(x, \alpha, \beta, \gamma); b = \mathsf{Rej}]$$

is negligible. Furthermore, the zero-knowledgeness of (P, V) guarantees that the pair (α, β) output by $S_{\widehat{V}}$ satisfies $\beta = f_s(x\|\alpha)$ with overwhelming probability. This means that the probability

$$\Pr[s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha); b \leftarrow \rho_V(x, \alpha, \beta', \gamma) : b = \mathsf{Rej}]$$

is negligible. Therefore, we conclude that A outputs Acc with overwhelming probability.

Theorem 3.1 follows from the above observations in two cases. ▌

Remark 3.6 [Interactive Argument] We show how to generalize the proof of Theorem 3.1 to obtain the same result in the argument model. We must consider the efficient completeness and the computational soundness instead of the completeness and the statistical soundness, respectively. This influences the non-uniform evasiveness of the relations $R_{\notin L}$ and $R_{\in L}$. Indeed, these relations are no longer non-uniformly evasive under such conditions. Therefore, we need to modify both relations. PPT stands for "probabilistic polynomial-time machine".

We define $R'_{\notin L}$ and $R'_{\in L}$ as follows:

$$(x\|\alpha, \beta) \in R'_{\notin L} \iff \begin{array}{l} x \notin L, \\ \exists \text{ PPT } \widehat{P}, \exists w, \Pr[\gamma \leftarrow \widehat{P}^w_x(\alpha\beta); b \leftarrow \rho_V(x, \alpha, \beta, \gamma) : b = \mathsf{Acc}] \text{ is not negligible.} \end{array}$$

Let $P_L(x)$ denote the set of string w satisfying the efficient completeness condition with respect to $x \in L$. We denote by $P^w_x(-)$ the distribution of the first message α of P and by $P^w_x(\alpha\beta)$ the conditional distribution of the message γ assuming P output α, where P takes the common input x and the auxiliary-input w.

$$(x\|\alpha, \beta) \in R'_{\in L} \iff \begin{array}{l} x \in L, \\ \forall w \in P_L(x) \text{ such that } \alpha \in [P^w_x(-)], \\ \quad \Pr[\alpha = P^w_x(-)] \cdot \Pr[\gamma \leftarrow P^w_x(\alpha\beta); b \leftarrow \rho_V(x, \alpha, \beta, \gamma) : b = \mathsf{Rej}] \\ \quad \text{is not negligible.} \end{array}$$

Both $R'_{\notin L}$ and $R'_{\in L}$ are non-uniformly evasive with respect to (l_{in}, l_{out}) by the computational soundness and the efficient completeness, respectively. Furthermore, we can prove the following claims similar to Claim 3.3 and 3.5.

- **In the case of $x \notin L$:** The probability

$$\Pr[s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s) : (x\|\alpha, \beta) \in R'_{\notin L}]$$

  is negligible.

- **In the case of $x \in L$:** The probability

$$\Pr[s \leftarrow \{0,1\}^k; \alpha \leftarrow P^w_x(-); \beta = f_s(x\|\alpha); \gamma \leftarrow P^w_x(\alpha\beta); b \leftarrow \rho_V(x, \alpha, \beta, \gamma) : b = \mathsf{Rej}]$$

  is negligible.

As a result, the same probabilistic polynomial-time machine A can recognize L.

Remark 3.7 [Constant Round Case] Theorem 3.1 extends to the constant-round case. But we require that the "constantly direct product" ensemble of the selected restricted correlation intractable function ensemble $\mathcal{F}$ satisfies the restricted correlation intractability as well. See Appendix A.

Remark 3.8 It does not seem that both $R_{\notin L}$ and $R_{\in L}$ can be recognized in probabilistic polynomial-time. Therefore, we don't know whether assuming the existence of restricted *weak* non-uniform correlation intractable function ensembles is sufficient for Theorem 3.1. The same is true in the following uniform case (Theorem 3.9).

3.2 The Uniform Case

The proof of Theorem 3.1 uses the non-uniformity of (l_{in}, l_{out})-restricted non-uniform correlation intractable function ensemble $\mathcal{F}$ in an essential way. Therefore, it does not seem that *uniform* correlation intractability is sufficient for Theorem 3.1. In this section, we will show what can be proven if we only assume uniform correlation intractability. Our first feeling was that we can prove that $\mathit{3}\mathcal{R}$-$\mathcal{AIZK}$-$\mathcal{AM} \subseteq \mathcal{ETA}$ assuming the existence of restricted uniform correlation intractable function ensembles. However, we can't prove it for the reason described in Remark 3.12. Alternatively, we show a weaker result which says that 3-round AIZK AM proofs with perfect completeness and 3-round AISZK AM proofs exist only for $\mathcal{ETA}$ languages. We denote by $\mathit{3}\mathcal{R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}}$ the class of languages having 3-round AIZK AM proofs with perfect completeness. We also denote by $\mathit{3}\mathcal{R}$-$\mathcal{AISZK}$-$\mathcal{AM}$ the class of languages having 3-round AISZK AM proofs.

Theorem 3.9 [$\mathcal{ETA}$ Version] Assume that there exist restricted uniform correlation intractable function ensembles. Then $(\mathit{3}\mathcal{R}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM}_{\mathsf{PC}} \cup \mathit{3}\mathcal{R}\text{-}\mathcal{AISZK}\text{-}\mathcal{AM}) \subseteq \mathcal{ETA}$.

Proof: We assume that a language L has an interactive proof (P, V) which is a 3-round AIZK AM proof with perfect completeness or a 3-round AISZK AM proof. Then we show that L is in $\mathcal{ETA}$. The basic idea is very similar to the proof of Theorem 3.1. However, we can no longer use the non-uniformity.

We use the same notations $\alpha, \beta, \gamma, l_\alpha, l_\beta$ and ρ_V for 3-round protocols. We use an (l_{in}, l_{out})-restricted *uniform* correlation intractable $\mathcal{F}$, where the length functions (l_{in}, l_{out}) and the seed length k are selected in the same way as in the non-uniform case. We consider the same cheating verifier $\widehat{V}$ who uses $\mathcal{F}$ to compute his challenge message β from $x\|\alpha$.

We want to show that L can be recognized by the same machine A as described in the proof of Theorem 3.1. But it is sufficient to show that A can recognize L only when the instance x is generated from any polynomial sampleable distribution. Therefore, in order to complete the proof, we need to show that for every probabilistic polynomial-time machine X, $\Pr[x \leftarrow X(1^n); b \leftarrow A(x) : b = \chi_L(x)]$ is overwhelming, where $X(1^n)$ ranges over $\{0,1\}^n$. That is, we need to show that for every probabilistic polynomial-time machine X, both

$$\Pr\left[x \leftarrow X_{\notin L}(1^n); b \leftarrow A(x) : b = \mathsf{Rej}\right] \text{ and } \Pr\left[x \leftarrow X_{\in L}(1^n); b \leftarrow A(x) : b = \mathsf{Acc}\right]$$

are overwhelming, where $X_{\notin L}(1^n)$ and $X_{\in L}(1^n)$ denote the distributions defined as follows:

$$\Pr[x = X_{\notin L}(1^n)] = \begin{cases} \Pr[x = X(1^n)] \text{ if } x \notin L, \\ 0 \text{ if } x \in L. \end{cases}$$

$$\Pr[x = X_{\in L}(1^n)] \quad = \quad \begin{cases} 0 \text{ if } x \notin L, \\ \Pr[x = X(1^n)] \text{ if } x \in L. \end{cases}$$

We note that both

$$\sum_{x \in \{0,1\}^n} \Pr[x = X_{\notin L}(1^n)] \text{ and } \sum_{x \in \{0,1\}^n} \Pr[x = X_{\in L}(1^n)]$$

are not necessarily equal to 1.

We consider the same (non-uniformly evasive) relations $R_{\notin L}$ and $R_{\in L}$ as defined in the proof of Theorem 3.1. Firstly, we claim that when s is chosen uniformly at random in $\{0,1\}^k$ and the common input x is generated by any probabilistic polynomial-time machine, the probability that $S_{\widehat{V}}$ outputs α satisfying $(x\|\alpha, f_s(x\|\alpha)) \in R_{\notin L}$ is negligible.

Claim 3.10 For any probabilistic polynomial-time machine X, the probability

$$\Pr[x \leftarrow X(1^n); s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha) : (x\|\alpha, \beta') \in R_{\notin L}]$$

is negligible.

Proof: Assume that this probability is not negligible. Then we can construct a probabilistic polynomial-time machine M which violates the restricted uniform correlation intractability of $\mathcal{F}$.

Machine: M.
Input: The seed s chosen uniformly at random in $\{0,1\}^k$.
Output: $x\|\alpha$.
M1: M runs $X(1^n)$ to get a common input x.
M2: M runs $S_{\widehat{V}}(x, s)$ to get a view $[x, s, \alpha\beta\gamma; -]$.
M3: M outputs $x\|\alpha$.

Clearly the probability that M outputs $x\|\alpha$ satisfying $(x\|\alpha, f_s(x\|\alpha)) \in R_{\notin L}$ is not negligible when s is chosen uniformly at random in $\{0,1\}^k$. This contradicts the restricted uniform correlation intractability of $\mathcal{F}$ since $R_{\notin L}$ is uniformly evasive (even non-uniformly evasive). ∎

Claim 3.10 means that for every probabilistic polynomial-time machine X, the probability

$$\Pr[x \leftarrow X_{\notin L}(1^n); s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha) : (x\|\alpha, \beta') \in R_{\notin L}]$$

is negligible. Furthermore, by the definition of $R_{\notin L}$, this means that for every probabilistic polynomial-time machine X, the probability

$$\begin{aligned} & \Pr\left[\begin{array}{l} x \leftarrow X_{\notin L}(1^n); s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \\ \beta' = f_s(x\|\alpha); b \leftarrow \rho_V(x, \alpha, \beta', \gamma) \end{array} : b = \mathsf{Acc}\right] \\ = \; & \Pr\left[x \leftarrow X_{\notin L}(1^n); b \leftarrow A(x) : b = \mathsf{Acc}\right] \end{aligned}$$

is negligible.

Next, we show that the probability $\Pr[x \leftarrow X_{\in L}(1^n); b \leftarrow A(x) : b = \mathsf{Acc}]$ is overwhelming. To do so, we claim that the cheating verifier $\widehat{V}$ accepts with overwhelming probability when s is chosen uniformly at random in $\{0,1\}^k$ and the common input x generated by any probabilistic polynomial-time machine belongs to L.

Claim 3.11 For every probabilistic polynomial-time machine X, the probability

$$\begin{aligned} & \Pr[x \leftarrow X_{\in L}(1^n); y \leftarrow \{0,1\}^k; b \leftarrow \langle P_x, \widehat{V}_x^y \rangle : b = \mathsf{Acc}] \\ = \ & \Pr\left[\begin{array}{l} x \leftarrow X_{\in L}(1^n); s \leftarrow \{0,1\}^k; \alpha \leftarrow P_x(-); \\ \beta = f_s(x\|\alpha); \gamma \leftarrow P_x(\alpha\beta); b \leftarrow \rho_V(x,\alpha,\beta,\gamma) \end{array} : b = \mathsf{Acc} \right] \end{aligned}$$

is overwhelming.

Proof: When (P, V) satisfies the perfect completeness, $\widehat{V}$ always accepts $x \in L$ since the challenge message β is always an element of $\{0,1\}^{l_\beta(n)} = \{0,1\}^{l_{in}(k)}$. Therefore, we focus on the case that (P, V) is a 3-round AISZK AM proof. Assume that the claim does not hold. Then there exists a probabilistic polynomial-time machine X such that the probability

$$\Pr\left[\begin{array}{l} x \leftarrow X_{\in L}(1^n); s \leftarrow \{0,1\}^k; \alpha \leftarrow P_x(-); \\ \beta = f_s(x\|\alpha); \gamma \leftarrow P_x(\alpha\beta); b \leftarrow \rho_V(x,\alpha,\beta,\gamma) \end{array} : b = \mathsf{Rej} \right]$$

is not negligible. By the definition of $R_{\in L}$, this means that the probability

$$\Pr\left[\begin{array}{l} x \leftarrow X(1^n); s \leftarrow \{0,1\}^k; \\ \alpha \leftarrow P_x(-); \beta = f_s(x\|\alpha) \end{array} : (x\|\alpha, \beta) \in R_{\in L} \right]$$

is not negligible. From the statistical zero-knowledgeness [5] of (P, V), it follows that the probability

$$\Pr\left[\begin{array}{l} x \leftarrow X(1^n); s \leftarrow \{0,1\}^k; \\ [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha) \end{array} : (x\|\alpha, \beta') \in R_{\in L} \right]$$

is not negligible, where $S_{\widehat{V}}$ is the simulator for $\widehat{V}$. Therefore, we can construct a probabilistic polynomial-time machine M which violates the restricted uniform correlation intractability of $\mathcal{F}$.

Machine: M.
Input: The seed s chosen uniformly at random in $\{0,1\}^k$.
Output: $x\|\alpha$.
M1: M runs $X(1^n)$ to get a common input x.
M2: M runs $S_{\widehat{V}}(x, s)$ to get a view $[x, s, \alpha\beta\gamma; -]$.
M3: M outputs $x\|\alpha$.

Clearly the probability that M outputs $x\|\alpha$ satisfying $(x\|\alpha, f_s(x\|\alpha)) \in R_{\in L}$ is not negligible when s is chosen uniformly at random in $\{0,1\}^k$. This contradicts the restricted uniform correlation intractability of $\mathcal{F}$ since $R_{\in L}$ is uniformly evasive (even non-uniformly evasive). ∎

[5] If $R_{\in L}$ can be recognized in probabilistic polynomial-time, the computational zero-knowledgeness is sufficient for Claim 3.11. But we don't know whether it can be. As described in Remark 3.12, we believe that it is an open problem whether or not it is sufficient.

By combining Claim 3.11 and the zero-knowledgeness of (P, V), it follows that for every probabilistic polynomial-time machine X, the probability

$$\Pr[x \leftarrow X_{\in L}(1^n); s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); b \leftarrow \rho_V(x, \alpha, \beta, \gamma) : b = \mathsf{Acc}]$$

is overwhelming. Furthermore, the zero-knowledgeness of (P, V) guarantees that the pair (α, β) output by $S_{\widehat{V}}$ satisfies $\beta = f_s(x\|\alpha)$ with overwhelming probability. Therefore, for every probabilistic polynomial-time machine X, the probability

$$\Pr[x \leftarrow X_{\in L}(1^n); s \leftarrow \{0,1\}^k; [x, s, \alpha\beta\gamma; -] \leftarrow S_{\widehat{V}}(x, s); \beta' = f_s(x\|\alpha); b \leftarrow \rho_V(x, \alpha, \beta', \gamma) : b = \mathsf{Acc}]$$

is overwhelming. This means that for every probabilistic polynomial-time machine X, the probability $\Pr[x \leftarrow X_{\in L}(1^n); b \leftarrow A(x) : b = \mathsf{Acc}]$ is overwhelming. ▮

Remark 3.12 [Open Problem] We don't know whether one can prove Claim 3.11 under the weaker assumption that (P, V) is just a 3-round AIZK AM proof. Of course, it is possible if $\mathcal{F}$ is a restricted *non-uniform* correlation intractable function ensemble as we have shown in Claim 3.5. However, we don't know whether one can prove it when we only assume that $\mathcal{F}$ is a restricted *uniform* correlation intractable function ensemble. The problem is in that the prescribed prover P is computationally unrestricted and so there is no way of producing $\alpha \in [P_x(-)]$ in probabilistic polynomial-time. That is why we required that (P, V) satisfies the additional properties: Perfect completeness or statistical zero-knowledgeness. We believe that it is an open problem whether it holds that $3\mathcal{R}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM} \subseteq \mathcal{ETA}$ assuming the existence of restricted uniform correlation intractable function ensembles.

4 One-Wayness and Restricted Correlation Intractability

In this section, we show the relationship between uniform one-way functions and restricted uniform correlation intractable function ensembles. We start by reviewing the result of Ostrovsky and Wigderson [OW93].

It is well-known that assuming the existence of non-uniform one-way functions, it holds that $\mathcal{NP} \subseteq \mathcal{ZK}$ [GMW91] [6]. Ostrovsky and Wigderson considered the question of whether this sufficient condition is also necessary. They showed that the existence of GMR-ZK interactive proofs for languages outside $\mathcal{ETA}$ implies the existence of uniform one-way functions (but not of non-uniform one-way functions).

Definition 4.1 [uniform one-way functions] A function $f : \{0,1\}^* \to \{0,1\}^*$ is uniform one-way if the following two conditions hold:

- Easy to compute: There exists a (deterministic) polynomial-time machine A so that on input x, A outputs $f(x)$.
- Hard to invert: For every probabilistic polynomial-time machine A', every polynomial $poly(\cdot)$ and all sufficient large n's, $\Pr[x \leftarrow \{0,1\}^n; y = f(x); x' \leftarrow A'(y) : y = f(x')] < 1/poly(n)$.

Theorem 4.2 [Ostrovsky-Wigderson [OW93][Go98, Theorem 4.5.4]] Assume that there exists a $\mathcal{ZK}$ language outside $\mathcal{ETA}$. Then there exist uniform one-way functions.

[6] Furthermore, it is well-known that $\mathcal{IP}=\mathcal{ZK}=\mathcal{PSPACE}$ assuming the existence of non-uniform one-way functions [ImYu87][BGG+88][Sh92]

Now we derive the relationship between uniform one-wayness and restricted uniform correlation intractability by combining Theorem 3.9 and 4.2.

Theorem 4.3 Proving the implication, "if uniform one-way functions exist then restricted uniform correlation intractable function ensembles exist", is as hard as proving ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) $\subseteq \mathcal{ETA}$.

Proof: Recall that ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) $\subseteq \mathcal{AIZK} \subseteq \mathcal{ZK}$. Therefore, Theorem 4.2 says that assuming that there exists a ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) language outside $\mathcal{ETA}$, uniform one-way functions exist. On the other hand, Theorem 3.9 says that if there exist restricted uniform correlation intractable function ensembles, it holds that ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) $\subseteq \mathcal{ETA}$.

Assume that if uniform one-way functions exist then restricted uniform correlation intractable function ensembles exist. Then, it follows that if there exists a ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) language outside $\mathcal{ETA}$, then ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) $\subseteq \mathcal{ETA}$. This means that it unconditionally holds that ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) $\subseteq \mathcal{ETA}$. ∎

Theorem 4.3 does not imply the non-existence of restricted uniform correlation intractable function ensembles. There may exist uniform one-way functions and restricted uniform correlation intractable function ensembles, simultaneously. As mentioned before, the assumption of the existence of restricted *weak* uniform correlation intractable function ensembles does not seem to be sufficient for Theorem 3.9. Therefore, Theorem 4.3 does not extend to restricted *weak* uniform correlation intractable function ensembles.

5 Concluding Remarks

In this paper, we have shown that assuming the existence of restricted non-uniform correlation intractable function ensembles, 3-round AIZK AM proofs exist only for $\mathcal{BPP}$ languages. We have also shown that assuming the existence of restricted uniform correlation intractable function ensembles, 3-round AIZK AM proofs with perfect completeness and 3-round AISZK AM proofs exist only for $\mathcal{ETA}$ languages. Our proofs use the verifier's auxiliary-input in an essential way: It is used as the seed of restricted correlation intractable function ensembles. Therefore, our results do not apply to the notion of GMR-ZK, where the cheating verifiers are not allowed to take the auxiliary-inputs. One may think that if we define the restricted correlation intractability in the single-function model rather than in the function ensemble model, we can prove analogous triviality results with respect to GMR-ZK. However, as described in [CGH98, Section 1.1.2], such functions do not exist.

Using the triviality result in the uniform case, we have shown that, proving the implication, "if uniform one-way functions exist then restricted uniform correlation intractable function ensembles exist", is as hard as proving the claim ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) $\subseteq \mathcal{ETA}$ without making any assumptions. We believe that it is unlikely that one can prove the latter claim unconditionally. Therefore, we conclude that it will be difficult to construct restricted uniform correlation intractable function ensembles based solely on uniform one-way functions.

It is interesting to investigate how hard it is to prove that $\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM} = \mathcal{BPP}$ or ($\mathcal{3R}$-$\mathcal{AIZK}$-$\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{3R}$-$\mathcal{AISZK}$-$\mathcal{AM}$) $\subseteq \mathcal{ETA}$ without making any assumptions.

Acknowledgments

We would like to thank Shai Halevi, Oded Goldreich and Takeshi Koshiba for pointing out several errors in an earlier version. We would like to thank Rafail Ostrovsky for answering our questions regarding the results of [OW93]. We also thank Masahiro Wada and Kenji Suzuki for their encouragement.

References

[BaMo88] L. Babai and S. Moran, "Arthur-Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes," J. Comput. System Sci., 36, pp.254-276, 1988.

[BeRo93] M. Bellare and P. Rogaway, "Random Oracles are Practical: a paradigm for designing efficient protocols, " Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 62-73, 1993.

[BGG+88] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali and P. Rogaway, "Everything Provable is Provable in Zero-Knowledge," Proceedings of CRYPTO'88, 1990.

[BCC88] G. Brassard, D. Chaum and C. Crépeau, "Minimum Disclosure Proofs of Knowledge, " Journal of Computer and System Sciences, Vol. 37, No. 2, pp. 156-189, 1988.

[BrCr86] G. Brassard and C. Crépeau, "Non-Transitive Transfer of Confidence : A Perfect Zero-Knowledge Interactive Protocol for SAT and Beyond, " Proceedings of 27th FOCS, 1986.

[Ca97] R. Canetti, "Towards Realizing Random Oracles: Hash Functions that Hide All Partial Information," Proceedings of CRYPTO'97, pp.455-469, 1997.

[CGH98] R. Canetti, O. Goldreich and S. Halevi, "The Random Oracle Model, Revisited," A preliminary version dated March 31, 1998 is available as Theory of Cryptography Library: Record 98-11.

[CMR98] R. Canetti, D. Micciancio and O. Reingold, "Perfectly One-Way Probabilistic Hash Functions," Proceedings of 30th STOC, 1998.

[Go93] O. Goldreich, "A Uniform-Complexity Treatment of Encryption and Zero-Knowledge," Journal of Cryptology, Vol.6, No. 1, pp.21-53, 1993.

[Go98] O. Goldreich, "Foundations of Cryptography (Fragments of a Book - Version 2.03)," February 27, 1998.

[GoKr96] O. Goldreich and H. Krawczyk, "On the Composition of Zero-Knowledge Proof Systems," SIAM Journal on Computing, Vol.25, No.1, pp.169-192, 1996.

[GMW91] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems," Journal of the ACM, Vol.38, No.1, pp.691-729, 1991.

[GoOr94] O. Goldreich and Y. Oren, "Definitions and Properties of Zero-Knowledge Proof Systems," Journal of Cryptology, Vol.7, No. 1, pp.1-32, 1994.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proofs," Proceedings of 17th STOC, pp.291-304, 1985.

[HT98] S. Hada and T. Tanaka, "On the Existence of 3-Round Zero-Knowledge Protocols, " Available as Theory of Cryptography Library: Record 99-?. An earlier version appeared in the proceedings of CRYPTO'98, pp. 408-423, 1998.

[HT99] S. Hada and T. Tanaka, "A Relationship between One-Wayness and Correlation Intractability, " Proceedings of PKC'99, 1999.

[ImRu89] R. Impagliazzo and S. Rudich, "Limits on the provable consequences of one-way permutations," Proceedings of 21st STOC, 1989.

[ImYu87] R. Impagliazzo and M. Yung, " Direct Minimum-Knowledge Computations," Proceedings of CRYPTO'87, pp. 40–51, 1987.

[Ok92] T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," Proceedings of CRYPTO'92, pp.31–53, 1993.

[OW93] R. Ostrovsky and A. Wigderson, "One-Way Functions are Essential for Non-Trivial Zero-Knowledge," Technical Report in ICSI, TR-93-073, 1993.

[Sh92] A. Shamir, "IP=PSPACE, " Journal of ACM, Vol. 39, No. 4, pp. 869-877, 1992.

[Si98] D. R. Simon, "Finding Collisions on a One-Way Street: Can Secure Hash Functions Be Based on General Assumptions," Proceedings of Eurocrypt'98, pp.334-345, 1998.

A The Extension to Constant-Round AIZK

In this appendix, we extend Theorem 3.1 and 3.9 to the constant-round case.

Canetti, Goldreich and Halevi commented that even if an (l_{in}, l_{out})-restricted correlation intractable function ensemble $\mathcal{F}$ exists, it is very non-robust constructs in [CGH98, Proposition 12]. They considered the "direct product" ensemble $\mathcal{F}^m$ of $\mathcal{F}$ defined as follows:

$$\mathcal{F}^m = \{f'_{s_1\|s_2\|\cdots\|s_{m(k)}} : |s_1| = |s_2| = \cdots = |s_{m(k)}| = k\}_{k\in\mathsf{N}},$$

where, for $x_1\|x_2\|\cdots\|x_{m(k)} \in \{0,1\}^{m(k)l_{in}(k)}$ such that $|x_1| = |x_2| = \cdots = |x_{m(k)}| = l_{in}(k)$,

$$f'_{s_1\|s_2\|\cdots\|s_{m(k)}}(x_1\|x_2\|\cdots\|x_{m(k)}) = f_{s_1}(x_1)\|f_{s_2}(x_2)\|\cdots\|f_{s_{m(k)}}(x_{m(k)}).$$

They showed that for sufficiently large m (e.g. $m(k) \geq k/l_{in}(k)$), $\mathcal{F}^m$ is not (l_{in}^m, l_{out}^m)-restricted correlation intractable, where $l_{xx}^m(m(k)\cdot k) = m(k)\cdot l_{xx}(k)$ for $xx \in \{in, out\}$. However, for sufficiently small m (e.g. m is a constant), their result does not rule out the existence of (l_{in}, l_{out})-restricted correlation function ensembles of which direct product ensembles are (l_{in}^m, l_{out}^m)-restricted correlation intractable function ensembles.

We say that (l_{in}, l_{out})-restricted correlation intractable function ensembles $\mathcal{F}$ is *constantly robust* if for every constant m, its direct product ensemble $\mathcal{F}^m$ is (l_{in}^m, l_{out}^m)-restricted correlation intractable. We denote by $\mathcal{CR}$-$\mathcal{AIZK}$-$\mathcal{AM}$ the class of languages that have constant-round AIZK AM interactive proofs.

Theorem A.1 [$\mathcal{BPP}$ Version] Assume that there exist constantly robust restricted non-uniform correlation intractable function ensembles. Then $\mathcal{CR}$-$\mathcal{AIZK}$-$\mathcal{AM} = \mathcal{BPP}$.

Proof: Clearly, it holds that $\mathcal{BPP} \subseteq \mathcal{CR}$-$\mathcal{AIZK}$-$\mathcal{AM}$. Therefore, we focus on the proof of $\mathcal{CR}$-$\mathcal{AIZK}$-$\mathcal{AM} \subseteq \mathcal{BPP}$. We assume that a language L has a constant-round AIZK AM proof (P, V). Then we show that L is in $\mathcal{BPP}$.

We use the following notations for constant-round AM proofs. Denote by x the common input and by n the length of x. For simplicity of the exposition we make some assumptions on the form of the protocol without loss of generality. We consider protocols in which both the first and last messages are sent by the prover P. By adding dummy message any protocol can be converted into one of this form. Note that in such a protocol, the number of rounds is always an odd number $2m + 1$, where m is a constant. The messages sent by the prover P are denoted by $\alpha_1, \alpha_2, \cdots, \alpha_m$ and γ. The messages sent by the verifier V are denoted by $\beta_1, \beta_2, \cdots, \beta_m$. We assume that for every i, α_i and β_i have length $l_\alpha(n)$ and $l_\beta(n)$, respectively. We also assume that for every i, the verifier chooses β_i uniformly at random in $\{0,1\}^{l_\beta(n)}$. The predicate computed by the verifier in order to decide whether to accept or reject is denoted by $\rho_V(x, \alpha_1, \beta_1, \cdots, \alpha_m, \beta_m, \gamma)$. That is, V accepts x if and only if $\rho_V(x, \alpha_1, \beta_1, \cdots, \alpha_m, \beta_m, \gamma) = \mathsf{Acc}$. This predicate may be a randomized function.

Let $\mathcal{F} = \{F_k\}_{k \in \mathsf{N}}$ be the same restricted non-uniform correlation intractable function ensembles as selected in the proof of Theorem 3.1. We consider a cheating verifier $\widehat{V}$ who computes, for every i, its message β_i as follows:

Machine: The cheating verifier $\widehat{V}$.

Input: The common input x of length n, the auxiliary-input y and the messages $\alpha_1, \beta_1, \cdots, \alpha_i$.

Output: The message β_i.

CV1: $\widehat{V}$ checks if y is of length mk, where $k = cn^d$. If this is true, $\widehat{V}$ splits y into m blocks $y = y_1 \| y_2 \| \cdots \| y_m$ (each block y_i is of length k), otherwise $\widehat{V}$ aborts.

CV2: $\widehat{V}$ outputs $\beta_i = f_{y_i}(x \| \alpha_i)$.

Except for the above computation of β_i, this cheating verifier $\widehat{V}$ behaves in the same way as the prescribed verifier V.

The rest of the proof is essentially equivalent to the proof of Theorem 3.1. Let $P_x(\alpha_1\beta_1 \cdots \alpha_{i-1}\beta_{i-1})$ denote the conditional distribution of the message α_i (for $1 \le i \le m$) assuming P output the messages $\alpha_1\alpha_2 \cdots \alpha_{i-1}$.

First, we define two relations $R_{\notin L}$ and $R_{\in L}$ as follows:

$$\begin{aligned} & (x_1 \| \alpha_1 \| x_2 \| \alpha_2 \| \cdots \| x_m \| \alpha_m, \beta_1 \| \beta_2 \| \cdots \| \beta_m) \in R_{\notin L} \\ \iff & x_1 = x_2 = \cdots = x_m = x \notin L, \\ & \exists \gamma, \Pr[b \leftarrow \rho_V(x, \alpha_1, \beta_1, \alpha_2, \beta_2, \cdots, \alpha_m, \beta_m, \gamma) : b = \mathsf{Acc}] \text{ is not negligible.} \end{aligned}$$

And,

$$\begin{aligned} & (x_1 \| \alpha_1 \| x_2 \| \alpha_2 \| \cdots \| x_m \| \alpha_m, \beta_1 \| \beta_2 \| \cdots \| \beta_m) \in R_{\in L} \\ \iff & x_1 = x_2 = \cdots = x_m = x \in L, \\ & \text{For } 1 \le i \le m,\ \alpha_i \in [P_x(\alpha_1\beta_1 \cdots \alpha_{i-1}\beta_{i-1})], \\ & \prod_{i=1}^{m} \Pr[\alpha_i = P_x(\alpha_1\beta_1 \cdots \alpha_{i-1}\beta_{i-1})] \times \end{aligned}$$

$$\Pr\left[\begin{array}{l}\gamma \leftarrow P_x(\alpha_1\beta_1\alpha_2\beta_2\cdots\alpha_m\beta_m);\\ b \leftarrow \rho_V(x,\alpha_1,\beta_1,\alpha_2,\beta_2,\cdots,\alpha_m,\beta_m,\gamma)\end{array} : b = \mathsf{Rej}\right] \text{ is not negligible.}$$

They are non-uniformly evasive with respect to (l_{in}^m, l_{out}^m) by the statistical soundness and the completeness, respectively.

We want to show that the following probabilistic polynomial-time machine A can recognize L.

Machine: A.

Input: x of length n.

Output: Acc or Rej.

A1: A generates a seed $s = s_1\|s_2\|\cdots\|s_m$ uniformly at random in $\{0,1\}^{mk}$ ($k = cn^d$), where s_i is of length k for every $1 \le i \le m$.

A2: A runs $S_{\widehat{V}}(x,s)$ to get a view $[x,s,\alpha_1\beta_1\alpha_2\beta_2\cdots\gamma;-]$, where the random coins of $\widehat{V}$ are empty since it is deterministic.

A3: For $1 \le i \le m$, A computes $\beta_i' = f_{s_i}(x\|\alpha_i)$.

A4: A outputs $\rho_V(x,\alpha_1,\beta_1',\alpha_2,\beta_2',\cdots,\alpha_m,\beta_m',\gamma)$.

In order to complete the proof, we need to show that the probability

$$\Pr\left[\begin{array}{l}s \leftarrow \{0,1\}^{mk}; [x,s,\alpha_1\beta_1\alpha_2\beta_2\cdots\gamma;-] \leftarrow S_{\widehat{V}}(x,s);\\ \text{For } 1 \le i \le m,\ \beta_i' = f_{s_i}(x\|\alpha_i);\\ b \leftarrow \rho_V(x,\alpha_1,\beta_1',\alpha_2,\beta_2',\cdots,\gamma)\end{array} : b = \chi_L(x)\right]$$

is overwhelming.

<u>**The case of $x \notin L$.**</u> We claim that when s is chosen uniformly at random in $\{0,1\}^{mk}$, the probability that $S_{\widehat{V}}$ outputs $\alpha_1\cdots\alpha_m$ satisfying $(x\|\alpha_1\|\cdots x\|\alpha_m, f_{s_1}(x\|\alpha_1)\|\cdots\|f_{s_m}(x\|\alpha_m)) \in R_{\notin L}$ is negligible.

Claim A.2 The probability

$$\Pr\left[\begin{array}{l}s \leftarrow \{0,1\}^{mk};\\ [x,s,\alpha_1\beta_1\cdots\alpha_m\beta_m\gamma;-] \leftarrow S_{\widehat{V}}(x,s);\\ \text{For } 1 \le i \le m,\ \beta_i' = f_{s_i}(x\|\alpha_i)\end{array} : (x\|\alpha_1\|\cdots\|x\|\alpha_m, \beta_1'\|\cdots\|\beta_m') \in R_{\notin L}\right]$$

is negligible.

Proof: As in the proof of Claim 3.3, we can construct a polynomial-size circuit family which violates the restricted non-uniform correlation intractability of $\mathcal{F}^m$. ▮

By the definition of $R_{\notin L}$, Claim A.2 means that the probability

$$\Pr\left[\begin{array}{l}s \leftarrow \{0,1\}^{mk};\\ [x,s,\alpha_1\beta_1\cdots\alpha_m\beta_m\gamma;-] \leftarrow S_{\widehat{V}}(x,s);\\ \text{For } 1 \le i \le m,\ \beta_i' = f_{s_i}(x\|\alpha_i);\\ b \leftarrow \rho_V(x,\alpha_1,\beta_1',\cdots,\alpha_m,\beta_m',\gamma)\end{array} : b = \mathsf{Acc}\right]$$

is negligible. Therefore, we conclude that A outputs Rej with overwhelming probability.

<u>The case of $x \in L$.</u> We claim that when $\widehat{V}$'s auxiliary-input y is chosen uniformly at random in $\{0,1\}^{mk}$, the cheating verifier $\widehat{V}$ accepts $x \in L$ with overwhelming probability after interacting with the prover P. This claim is given formally as follows:

Claim A.3 The probability

$$\begin{aligned}
& \Pr[y \leftarrow \{0,1\}^{mk}; b \leftarrow \langle P_x, \widehat{V}_x^y\rangle; b = \mathsf{Rej}] \\
= \ & \Pr\left[\begin{array}{ll} s \leftarrow \{0,1\}^{mk}; & \\ \alpha_1 \leftarrow P_x(-); \beta_1 = f_{s_1}(x\|\alpha_1); & \\ \alpha_2 \leftarrow P_x(\alpha_1\beta_1); \beta_2 = f_{s_2}(x\|\alpha_2); & \\ \cdots; & : b = \mathsf{Rej} \\ \alpha_m \leftarrow P_x(\alpha_1\beta_1\cdots\alpha_{m-1}\beta_{m-1}); \beta_m = f_{s_m}(x\|\alpha_m); & \\ \gamma \leftarrow P_x(\alpha_1\beta_1\cdots\alpha_m\beta_m); & \\ b \leftarrow \rho_V(x, \alpha_1, \beta_1, \cdots \gamma) & \end{array}\right]
\end{aligned}$$

is negligible.

Proof: As in the proof of Claim 3.5, we can construct a polynomial-size circuit family which violates the restricted non-uniform correlation intractability of $\mathcal{F}^m$. ▮

By combining Claim A.3 and the zero-knowledgeness of (P, V), it follows that the probability

$$\Pr[s \leftarrow \{0,1\}^{mk}; [x, s, \alpha_1\beta_1\cdots\alpha_m\beta_m\gamma; -] \leftarrow S_{\widehat{V}}(x, s); b \leftarrow \rho_V(x, \alpha_1, \beta_1, \cdots, \alpha_m, \beta_m, \gamma); b = \mathsf{Rej}]$$

is negligible. Since by the zero-knowledgeness of (P, V) it holds that $\beta_i = f_{s_i}(x\|\alpha_i)$ for $1 \le i \le m$ with overwhelming probability, the probability

$$\Pr\left[\begin{array}{ll} s \leftarrow \{0,1\}^{mk}; & \\ [x, s, \alpha_1\beta_1\cdots\alpha_m\beta_m\gamma; -] \leftarrow S_{\widehat{V}}(x, s); & : b = \mathsf{Rej} \\ \text{For } 1 \le i \le m,\ \beta_i' = f_{s_i}(x\|\alpha_i); b \leftarrow \rho_V(x, \alpha_1, \beta_1', \cdots, \alpha_m, \beta_m', \gamma) & \end{array}\right]$$

is negligible. Therefore, we conclude that A outputs Acc with overwhelming probability.

Theorem A.1 follows from the above arguments in two cases. ▮

It is easy to see that Theorem 3.9 can be extended to the constant round case using the same idea. We denote by $\mathcal{CR}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM}_{\mathsf{PC}}$ the class of languages that have constant-round AIZK AM proofs with perfect completeness and by $\mathcal{CR}\text{-}\mathcal{AISZK}\text{-}\mathcal{AM}$ the class of languages that have constant-round AISZK AM proofs.

Theorem A.4 [$\mathcal{ETA}$ Version] Assume that there exist constantly robust restricted uniform correlation intractable function ensembles. Then $(\mathcal{CR}\text{-}\mathcal{AIZK}\text{-}\mathcal{AM}_{\mathsf{PC}} \cup \mathcal{CR}\text{-}\mathcal{AISZK}\text{-}\mathcal{AM}) \subseteq \mathcal{ETA}$.

Proof: Omitted. ▮

Theorem A.1 and A.4 extend to the argument model in the same way as described in Remark 3.6.

B Flaws in PKC'99 Version [HT99]

In [HT99], we wrongly claimed that assuming that there exist restricted uniform correlation intractable function ensembles, it holds that $\mathit{3}\mathcal{R}$-$\mathcal{AIZK}$-$\mathcal{AM}\subseteq \mathcal{ETA}$ (Theorem 1 in [HT99]). Indeed, the proof of Theorem 1 includes many errors. As a result, we wrongly claimed that proving the implication, "if uniform one-way functions exist then restricted uniform correlation intractable function ensembles exist", is as hard as proving $\mathit{3}\mathcal{R}$-$\mathcal{AIZK}$-$\mathcal{AM} \subseteq \mathcal{ETA}$.