

On the Impossibility of Entropy Reversal, and Its Application to Zero-Knowledge Proofs

Shachar Lovett^(✉) and Jiapeng Zhang

University of California, San Diego, USA
slovett@cs.ucsd.edu, jpeng.zhang@gmail.com

Abstract. Zero knowledge proof systems have been widely studied in cryptography. In the statistical setting, two classes of proof systems studied are Statistical Zero Knowledge (SZK) and Non-Interactive Statistical Zero Knowledge (NISZK), where the difference is that in NISZK only very limited communication is allowed between the verifier and the prover. It is an open problem whether these two classes are in fact equal. In this paper, we rule out efficient black box reductions between SZK and NISZK.

We achieve this by studying algorithms which can reverse the entropy of a function. The problem of estimating the entropy of a circuit is complete for NISZK. Hence, reversing the entropy of a function is equivalent to a black box reduction of NISZK to its complement, which is known to be equivalent to a black box reduction of SZK to NISZK [Goldreich et al. CRYPTO 1999]. We show that any such black box algorithm incurs an exponential loss of parameters, and hence cannot be implemented efficiently.

Keywords: Entropy reversal · Statistical zero-knowledge proofs · Black-box reductions

1 Introduction

The notion of *Zero-Knowledge Proof Systems* was introduced in the seminal paper of Goldwasser et al. [11]. Informally, an interactive proof system is a protocol that involves a computational unbounded prover P and a polynomial time verifier V . The prover attempts to convince the verifier that an assertion is a YES instance x of some promise problem.

A promise problem Π consists of two disjoint sets Π_Y and Π_N , e.g., yes instances and no instances. A zero-knowledge proof system for the problem Π requires the following three conditions:

- *Completeness:* If $x \in \Pi_Y$, then $\Pr[(P, V)(x) \text{ accepts}] \geq 2/3$.
- *Soundness:* If $x \in \Pi_N$, then for every adversary P^* , $\Pr[(P^*, V)(x) \text{ accepts}] \leq 1/3$.

S. Lovett and J. Zhang—Research supported by NSF CAREER award 1350481.

- *Zero-knowledge*: There is a polynomial time simulator S such that $S(x)$ and $(P, V)(x)$ are “indistinguishable”, for every $x \in \Pi_Y$.

Different zero knowledge proof systems differ in the allowed communication protocol, and in the notion of indistinguishability applied to the simulator. In this paper, we restrict our attention to statistical proof systems (SZK and NISZK), where the corresponding notion is that of statistical indistinguishability.

Statistical zero knowledge (SZK). The complexity class SZK consists of the problems that have a statistical zero-knowledge proof, where any efficient interactive communication is allowed between the verifier and the prover. Surprisingly, there are complete problems for SZK which have nothing to do with interaction. This was first discovered by Sahai and Vadhan [17].

A distribution D over $\{0, 1\}^m$ is said to be *efficiently sampleable* if there exists a polynomial size boolean circuit $C : \{0, 1\}^n \rightarrow \{0, 1\}^m$, such that the distribution D can be obtained by applying C to uniformly sampled input bits. By an abuse of notation, we identify C with this distribution. Given two distributions C_1, C_2 over $\{0, 1\}^m$, we denote by $\text{dist}(C_1, C_2)$ their statistical distance. The following problem, called *Statistical Difference*, was shown by Sahai and Vadhan [17] to be complete for SZK.

Definition 1 (Statistical Difference [17]). *The promise problem Statistical Difference, denoted by $\text{SD} = (\text{SD}_Y, \text{SD}_N)$, consists of*

- $\text{SD}_Y = \{(C_1, C_2) : \text{dist}(C_1, C_2) \leq 1/3\}$
- $\text{SD}_N = \{(C_1, C_2) : \text{dist}(C_1, C_2) \geq 2/3\}$

Here C_1, C_2 denote polynomial size circuits with the same output length.

Theorem 1 [17]. *SD is SZK-complete.*

In a follow up work, Goldreich and Vadhan [10] gave another SZK-complete problem, called *Entropy Difference*. Below, $H(C)$ denotes the Shannon entropy of the distribution induced by C .

Definition 2 (Entropy Difference [10]). *The promise problem Entropy Difference, denoted by $\text{ED} = (\text{ED}_Y, \text{ED}_N)$, consists of*

- $\text{ED}_Y = \{(C_1, C_2) : H(C_1) \geq H(C_2) + 1\}$
- $\text{ED}_N = \{(C_1, C_2) : H(C_2) \geq H(C_1) + 1\}$

Here C_1, C_2 denote polynomial size circuits with the same output length.

Theorem 2 [10]. *The problem ED is SZK-complete.*

This in particular gives a slick proof to the fact that SZK is closed under complement, which might be hard to guess from the original definition. Given an input (C_1, C_2) to ED , one can simply reverse their order.

Non-interactive statistical zero knowledge (NISZK). The notion of *Non-Interactive Zero-Knowledge Proof Systems*, or NISZK was introduced by Blum et al. [2], allows for very restricted communication between the verifier and the prover. Both parties share a common uniformly random string (a random challenge), and the prover sends a single message to the verifier based on this random challenge.

Since the model has been introduced, several problems have been shown to be in NISZK. Originally these were problems arising in number theory, such as Quadratic Nonresiduosity and its variants [1, 2, 4, 6, 7]. More recently, this was extended to several natural problems in lattices [16].

The problem of finding complete problems for NISZK arose naturally. De Santis et al. [5], introduced a problem called *Image Density*, and proved that is complete for NISZK. Subsequently, Goldreich et al. [9] studied the following two problems and showed that they too are complete for NISZK.

Definition 3 (Statistical Difference from Uniform [9]). *The promise problem Statistical Difference from Uniform, denoted by $\text{SDU} = (\text{SDU}_Y, \text{SDU}_N)$, consists of*

- $\text{SDU}_Y = \{C : \text{dist}(C, \mathcal{U}) \leq 1/n\}$
- $\text{SDU}_N = \{C : \text{dist}(C, \mathcal{U}) \geq 1 - 1/n\}$

Here C denotes a polynomial size circuit which outputs n bits, and \mathcal{U} denotes the uniform distribution on $\{0, 1\}^n$.

Definition 4 (Entropy Approximation [9]). *The promise problem Entropy Approximation, denoted by $\text{EA} = (\text{EA}_Y, \text{EA}_N)$, consists of*

- $\text{EA}_Y = \{(C, k) : H(C) \geq k + 1\}$
- $\text{EA}_N = \{(C, k) : H(C) \leq k - 1\}$

Here C denotes a polynomial size circuit and $k \geq 1$ is an integer parameter.

Theorem 3 [9]. *SDU and EA are NISZK-complete.*

The main open problem that motivated the current paper is *what is the relationship between NISZK and SZK*. Goldreich et al. [9] made a significant progress towards resolving this problem.

Theorem 4 [9]. *The following statements are equivalent:*

- (1). $\text{SZK} = \text{NISZK}$.
- (2). NISZK is closed under complement.
- (3). NISZK is closed under NC^1 truth-table reductions.
- (4). ED , or SD Karp-reduces to EA , or SDU respectively.
- (5). EA or SDU Karp-reduces to its complement.

The main goal of the current paper is to show that these statements are all false, at least in a limited model of computation. Concretely, our goal is to rule out *black box reductions* between NISZK and its complement. When we consider black box reductions, the notion of efficient computation disappears, and we replace the study of circuits with the study of arbitrary functions (which can be seen as oracle functions).

1.1 Black-Box Reductions

We describe the notion of black box reductions of functions in this section.

Let $\mathcal{F}_{n,m}$ denote the family of functions $f : \{0,1\}^n \rightarrow \{0,1\}^m$. A promise problem Π over $\mathcal{F}_{n,m}$ consists of a family of yes instances Π_Y and a family of no instances Π_N , where $\Pi_Y, \Pi_N \subset \mathcal{F}_{n,m}$ and $\Pi_Y \cap \Pi_N = \emptyset$.

Definition 5 (Black-Box Reduction). *Let $\Pi = (\Pi_Y, \Pi_N)$ and $\Pi' = (\Pi'_Y, \Pi'_N)$ be promise problems over functions $\mathcal{F}_{n,m}$ and $\mathcal{F}_{n',m'}$, respectively. a black-box reduction from Π to Π' is an algorithm $A^{(\cdot)} : \{0,1\}^{n'} \rightarrow \{0,1\}^{m'}$ with oracle access to a function $f \in \mathcal{F}_{n,m}$, such that the following holds:*

- If $f \in \Pi_Y$ then $A^f \in \Pi'_Y$.
- If $f \in \Pi_N$ then $A^f \in \Pi'_N$.

Given an input $w \in \{0,1\}^{n'}$, the algorithm makes a number of queries to f (the query locations may depend on w and be adaptive), and outputs a value $z \in \{0,1\}^{m'}$. We define $A^f(w) = z$. The query complexity of A , denoted $QC(A)$, is the maximal number of queries to f performed over an input.

Our definition of black-box reduction does not relate to decidability, and instead relates to functionality. This type of black-box reduction is well studied in cryptography. Many reductions in the literature are in fact black-box reductions. Examples include the flattening lemma of [9], the polarization lemma of [17], the reduction from Statistical Difference to its complement [17], constructions of pseudorandom generators from one-way functions [12,13], constructions of pseudorandom functions from pseudorandom generators [8], and many more.

1.2 Our Results

We define the function version of the Entropy Approximation (EA) problem.

Definition 6 (Function Entropy Approximation). *The promise problem Function Entropy Approximation, denoted by $\text{FEA} = (\text{FEA}_Y, \text{FEA}_N)$, consists of*

- $\text{FEA}_Y = \{(f, k) : H(f) \geq k + 1\}$
- $\text{FEA}_N = \{(f, k) : H(f) \leq k - 1\}$

Here $n, m, k \geq 1$ and $f \in \mathcal{F}_{n,m}$. Note that the interesting regime of parameters (where the problem is not trivial) is when $1 \leq k \leq n - 1$.

A black box reduction from NISZK to its complement needs to map FEA to its complement. In particular, an efficient reduction would stay efficient even if we fix n, m, k to favourable values (we will later set $m = 3n$, $k = n - 3$). We call such a reduction an *Entropy Reverser*.

Definition 7 (Entropy Reverser). Let $n, m, k, n', m', k' \geq 1$. An $(n, m, k; n', m', k')$ entropy reverser is a black box reduction A from $\mathcal{F}_{n,m}$ to $\mathcal{F}_{n',m'}$ such that

- If $H(f) \geq k + 1$ then $H(A^f) \leq k' - 1$.
- If $H(f) \leq k - 1$ then $H(A^f) \geq k' + 1$.

Our main result is that entropy reversers require either exponential output length n', m' or exponential query complexity. In particular, when they are applied to a function f computed by a polynomial size circuit, their output A^f is computed by an exponential size circuit. We state and prove our result for a concrete setting of parameters $m = 3n$, $k = n - 3$. We note that our work can be extended to a much wider set of parameters. However, we did not see any applications of pursuing this.

Theorem 5 (Main theorem). Let A be an $(n, m, k; n', m', k')$ Entropy Reverser for $m = 3n, k = n - 3$. Then $QC(A) \geq 2^{n/5} / \text{poly}(n', m')$.

1.3 Related Works

Relations between zero knowledge proofs have been previously studied [14, 18], where certain black box reductions were ruled out. However, previous works only ruled out restricted forms of black box reductions, where the only access to a function f is via independent and uniform samples. In particular, these reductions are non adaptive. We note that this is a much weaker notion of black box reductions, and indeed some of the black box reductions we already mentioned (e.g. the reduction from Statistical Difference to its complement [17]) require the ability to correlate inputs. As far as we know, ours is the first work in this context which rules out general black box reductions without any restriction on the access pattern or adaptivity.

1.4 Proof Overview

Let $n \geq 1$ and fix $m = 3n, k = n - 3$.

The first step in our proof is to apply a black box reduction of Goldreich et al. [9], which converts high/low entropy distributions to distributions which are close to uniform, or supported on a small set, respectively (Lemma 1). This allows us to assume stronger properties of the functions generated by the supposed Entropy Reverser. Concretely, that we are given a black box reduction A from $\mathcal{F}_{n,m}$ to $\mathcal{F}_{n',m'}$ such that:

- If $H(f) \geq k + 1$ then A^f is distributed close to uniform (concretely, $\text{dist}(A^f, \mathcal{U}) \leq 0.1$).
- If $H(f) \leq k - 1$ then the distribution of A^f is supported on a small set (concretely, of size $\leq 0.1 \cdot 2^{m'}$).

As this black box reduction is efficient, it incurs a blowup of only $\text{poly}(n', m')$ in the query complexity. See Sect. 3.1 for the details. From now on, we focus on this stronger notion of an Entropy Reverser, and show that for it it holds that $QC(A) \geq \Omega(2^{n/5})$.

Next, we consider several distributions over functions $\mathcal{F}_{n,m}$. Fix $b = 256$. We denote by $\mathbf{B} = (B_1, \dots, B_s)$ a partition of the input space $\{0, 1\}^n$ into s blocks, each of size b . For $0 \leq j \leq s$ we define a distribution \mathcal{D}_j over $\mathcal{F}_{n,m}$ as follows:

- Sample a random partition $\mathbf{B} = (B_1, \dots, B_s)$ of $\{0, 1\}^n$.
- Sample $y_1, \dots, y_j \in \{0, 1\}^m$ uniformly and independently.
- If $x \in B_i$, $i \leq j$ then set $f_j(x) = y_i$.
- If $x \in B_i$, $i > j$ then sample $f_j(x) \in \{0, 1\}^m$ uniformly and independently.

It is not hard to show that as j increases, the entropy of $f_j \sim \mathcal{D}_j$ decreases. Concretely, we show (Claim 3.2) that with very high probability it holds that

$$H(f_{s/4}) = n - 2, \quad H(f_{s/2}) = n - 4.$$

Thus, by the assumptions of our Entropy Reverser (as we set $k = n - 3$), it should hold that $A^{f_{s/4}}$ is supported on a small set, while $A^{f_{s/2}}$ is distributed close to uniform. We show that this requires exponential query complexity. From now onwards, let $q = \text{QC}(A)$ denote this query complexity.

Let $z \in \{0, 1\}^{m'}$ be chosen uniformly, and let p_j for $0 \leq j \leq s$ denote the probability that z belongs to the support of A^{f_j} :

$$p_j = \Pr[\exists w \in \{0, 1\}^{n'}, z = A^{f_j}(w)].$$

By our assumptions, $p_{s/2} \geq 0.9$ while $p_{s/4} \leq 0.1$. Our goal is to apply a hybrid argument and show that if q is small then $p_{j-1} \approx p_j$ for all $s/4 \leq j \leq s/2$.

We can couple the choice of f_{j-1}, f_j , so that we jointly sample $\mathbf{B}, y_1, \dots, y_j$, and the only difference between f_{j-1} and f_j is that they differ on the block B_j (f_{j-1} maps each point in B_j to a uniformly chosen point in $\{0, 1\}^{m'}$, while f_j maps all the points in B_j to a single point). As the partition to blocks is random, the probability that a specific query belongs to the block B_j is $1/s$. As the algorithm makes q queries, this should “intuitively” give the bound

$$p_j - p_{j-1} \leq \frac{q}{s}.$$

(we say “intuitively” as the black box reduction is an adaptive algorithm, while the above analysis works straightforwardly only for non-adaptive algorithms). However, such a bound is useless for us, as we need to apply it $\Omega(s)$ times. Thus, we need a more refined analysis.

In order to do so, let $f \in \{f_{j-1}, f_j\}$. We say that an input w to A^f respects the block structure of \mathbf{B} if any block B_i in \mathbf{B} is queried at most once by $A^f(w)$. Intuitively, such an input should not be able to “distinguish” between f_{j-1} and f_j . On the other hand, the probability over a random partition that any two fixed points belong to B_j is $\approx 1/s^2$, and hence as there are q queries, this should “intuitively” give an improved bound of

$$p_j - p_{j-1} \leq \frac{q^2}{s^2}.$$

If such a bound is indeed true, then applying it $(s/2) - (s/4) = s/4$ times would give that $|p_{s/4} - p_{s/2}| \leq O(q^2/s)$, which would imply that $q^2 \geq \Omega(s) = \Omega(2^n)$, and hence we obtain an exponential lower bound on q .

Formalizing this intuition turns out to be quite delicate, as the algorithm A^f is an adaptive algorithm, and hence various choices are dependent on each other. Our main technical Lemma (Lemma 3) show that, if we restrict our attention to inputs which respect the block structure and define

$$p'_j = \Pr[\exists w \in \{0, 1\}^{n'}, z = A^{f_j}(w), w \text{ respects the block structure of } \mathbf{B}]$$

then p'_j is a good proxy for p_j (Lemma 2), for which a better bound can be obtained:

$$p'_j - p'_{j-1} \leq O\left(\frac{q^{5/3}}{s^{4/3}}\right).$$

While this bound is worse than the “intuitive” bound of q^2/s^2 , it still suffices for our purposes, as when we apply it $\Theta(s)$ times we obtain that $p'_{s/2} - p'_{s/4} \leq O(q^{5/3}/s^{1/3})$ and hence we still get an exponential lower bound on q , namely $q \geq \Omega(2^{n/5})$.

Paper organization. We give some preliminary definitions in Sect. 2. In Sect. 3 we formalize the above proof overview, and give the proof of our main theorem, Theorem 5, assuming our main technical lemma, Lemma 3. The proof of Lemma 3 is given in Sect. 4. We conclude with some open problems in Sect. 5.

2 Preliminaries

Let $\mathcal{F}_{n,m}$ denote the family of functions $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$. A *black box reduction* from $\mathcal{F}_{n,m}$ to $\mathcal{F}_{n',m'}$ with is an algorithm which, given query access to $f \in \mathcal{F}_{n,m}$, computes a function $A^f \in \mathcal{F}_{n',m'}$ as follows. Given an input $w \in \{0, 1\}^{n'}$, the algorithm makes a number of queries to f (the query locations can depend on w and be adaptive), and outputs a value $z \in \{0, 1\}^{m'}$. We define $A^f(w) = z$. The query complexity of A is the maximum number of queries to f performed over an input, which we denote by $\text{QC}(A)$.

Let X be a random variable taking values in $\{0, 1\}^m$. We recall some basic definitions. The support of X is $\text{supp}(X) = \{x : \Pr[X = x] > 0\}$. The Shannon entropy of X is

$$H(X) = \sum_x \Pr[X = x] \cdot \log_2(1/\Pr[X = x]).$$

The statistical distance of two random variables X, Y is

$$\text{dist}(X, Y) = \frac{1}{2} \sum_x |\Pr[X = x] - \Pr[Y = x]|.$$

We denote by \mathcal{U}_m the uniform distribution over $\{0, 1\}^m$.

We will identify $f \in \mathcal{F}_{n,m}$ with the random variable of its output distribution in $\{0,1\}^m$, given a uniformly sampled input in $\{0,1\}^n$. As such, we extend the definition of support, Shannon entropy and statistical distance to functions. In the special case where f is computable by a circuit $C : \{0,1\}^n \rightarrow \{0,1\}^m$ of size $\text{poly}(m)$, we say that this distribution is an *efficiently sampleable distribution*.

3 Proof of Main Theorem: Theorem 5

3.1 A Useful Reduction

As a first step towards proving Theorem 5, we make use of a black box reduction of Goldreich et al. [9]. It allows us to strengthen the assumptions in Theorem 5.

Lemma 1 [9]. *Let $n', m', k' \geq 1$. There exists a black box reduction A_1 from $\mathcal{F}_{n',m'}$ to $\mathcal{F}_{n'',m''}$, where n'', m'' , $QC(A_1) \leq \text{poly}(n', m')$, such that the following holds for any $f \in \mathcal{F}_{n',m'}$:*

- If $H(f) \geq k' + 1$ then $\text{dist}(A_1^f, \mathcal{U}_{m''}) \leq 0.1$.
- If $H(f) \leq k' - 1$ then $|\text{supp}(A_1^f)| \leq 0.1 \cdot 2^{m''}$.

Let A_5 denote the black box reduction from $\mathcal{F}_{n,m}$ to $\mathcal{F}_{n',m'}$ assumed in Theorem 5. Let A_1 denote the black box from $\mathcal{F}_{n',m'}$ to $\mathcal{F}_{n'',m''}$ given in Lemma 1. Let A be their composition. Namely, A is a black box reduction from $\mathcal{F}_{n,m}$ to $\mathcal{F}_{n'',m''}$, obtained by first applying A_5 and then A_1 . That is,

$$A^f = A_1^{A_5^f}.$$

Observe that $QC(A) \leq QC(A_5)QC(A_1) \leq QC(A_5)\text{poly}(n', m')$, that $n'', m'' \leq \text{poly}(n', m')$, and that A satisfies the following:

- If $H(f) \geq k + 1$ then $|\text{supp}(A^f)| \leq 0.1 \cdot 2^{m''}$.
- If $H(f) \leq k - 1$ then $\text{dist}(A^f, \mathcal{U}_{m''}) \leq 0.1$.

We will prove a lower bound on the query complexity of A , which would then imply a lower bound on the query complexity of A_5 .

3.2 Preparations

In order to prove Theorem 5, we will exhibit two distributions over functions, one of high entropy functions, the other of low entropy functions, and show that black box reductions with low query complexity cannot “reverse” the entropy relation between them.

Definition 8 (Sample distribution). Let $n, m \geq 1$ and let $b \geq 2$ be a parameter (block size) to be determined later, and set $s = 2^n/b$. We denote by $\mathbf{B} = (B_1, \dots, B_s)$ a partition of $\{0, 1\}^n$ into s blocks of equal size $2^n/s = b$. For any $0 \leq j \leq s$ we define a distribution over partitions \mathbf{B} and functions $f_j \in \mathcal{F}_{n,m}$ as follows:

- Sample a random partition $\mathbf{B} = (B_1, \dots, B_s)$ of $\{0, 1\}^n$.
- Sample $y_1, \dots, y_j \in \{0, 1\}^m$ uniformly and independently.
- If $x \in B_i$, $i \leq j$ then set $f_j(x) = y_i$.
- If $x \in B_i$, $i > j$ then sample $f_j(x) \in \{0, 1\}^m$ uniformly and independently.

We denote the joint distribution of (\mathbf{B}, f_j) as \mathcal{D}_j . With an abuse of notation, when we write $f_j \sim \mathcal{D}_j$, we simply omit the block structure from the sample. Note that $f_0 \sim \mathcal{D}_0$ is uniformly distributed over $\mathcal{F}_{n,m}$. The following simple claim argues that as we increase j , the entropy of $f_j \sim \mathcal{D}_j$ decreases. It is specialized to our desired application.

Claim. Let $m = 3n$. Sample $f_j \sim \mathcal{D}_j$. Then with probability $1 - 2^{-n}$ over the choice of f_j , it holds that

$$H(f_j) = n - (j/s) \log b.$$

In particular, if we set $b = 256$ then

$$H(f_{s/4}) = n - 2, \quad H(f_{s/2}) = n - 4.$$

Proof. Let $0 \leq j \leq s$ and sample $f_j \sim \mathcal{D}_j$. Let y_1, \dots, y_j be the single value that f_j obtains on blocks B_1, \dots, B_j . Consider $y_1, \dots, y_j, (f_j(x) : x \in B_i, i > j)$. Lets denote by E_0 the event that no two values in this list collide. The probability that any two of these values are equal is 2^{-m} . As there are $\leq 2^n$ values, the probability that any two intersect is bounded by $2^{2n-m} \leq 2^{-n}$. Thus $\Pr[E_0] \geq 1 - 2^{-n}$.

Lets assume that E_0 holds. Then, the distribution of f_j is as follows: there are j values (namely, y_1, \dots, y_j) that each is obtained with probability $1/s = b/2^n$. All other $2^n - bj$ values are each obtained with probability 2^{-n} . Thus

$$H(f_j|E_0) = j \cdot (b/2^n) \cdot \log(2^n/b) + (2^n - bj) \cdot 2^{-n} \cdot \log(2^n) = n - (j/s) \log b.$$

We treat $\mathcal{D}_{s/4}$ as a distribution over (mostly) high entropy functions, and $\mathcal{D}_{s/2}$ as a distribution over (mostly) lower entropy functions.

3.3 Block Compatible Inputs

Given $w \in \{0, 1\}^{n''}$ and $f \in \mathcal{F}_{n,m}$, we denote by $\text{Query}(A^f(w)) \subset \{0, 1\}^n$ the set of inputs of f queried by A^f on input w . To recall, the functions that we focus attention on are defined together with a block structure $\mathbf{B} = (B_1, \dots, B_s)$. Below, we specialize our attention to inputs and their corresponding outputs, for which at most one value in each block is queried.

Definition 9 (Block compatible inputs). Let $\mathbf{B} = (B_1, \dots, B_s)$ be a partition of $\{0, 1\}^n$, $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$. We say that $w \in \{0, 1\}^{n''}$ is a block compatible input with respect to (f, \mathbf{B}) if, when computing $A^f(w)$, each block of \mathbf{B} is queried at most once. We denote by $I(f, \mathbf{B})$ the set of all block compatible inputs:

$$I(f, \mathbf{B}) = \{w \in \{0, 1\}^{n''} : |\text{Query}(A^f(w)) \cap B_i| \leq 1 \quad \forall i = 1, \dots, s\}$$

Definition 10 (Block compatible outputs). Let \mathbf{B} be a partition of $\{0, 1\}^n$, $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$. We say that $z \in \{0, 1\}^{m''}$ is a block compatible output with respect to (f, \mathbf{B}) if $A^f(w) = z$ for a block compatible input w . We denote by $O(f, \mathbf{B})$ the set of all block compatible outputs:

$$O(f, \mathbf{B}) = \{z \in \{0, 1\}^{m''} : \exists w \in I(f, \mathbf{B}), A^f(w) = z\}.$$

Observe that the definition of $I(f, \mathbf{B}), O(f, \mathbf{B})$ does not depend on the order of the blocks in \mathbf{B} . This will turn out to be crucial later on in the analysis. Thus, for $\mathbf{B} = (B_1, \dots, B_s)$ define $\{\mathbf{B}\} = \{B_1, \dots, B_s\}$ (that is, forgetting the order of the blocks) and note that

$$I(f, \mathbf{B}) = I(f, \{\mathbf{B}\}) \quad O(f, \mathbf{B}) = O(f, \{\mathbf{B}\}).$$

It is obvious that $O(f, \mathbf{B}) \subset \text{supp}(A^f)$. Next, we argue that if the distribution of A^{f_j} is close to uniform, then $O(f_j, \mathbf{B})$ is large.

Lemma 2. *Sample $(\mathbf{B}, f_j) \sim \mathcal{D}_j$, and assume that*

$$\Pr_{f_j} [\text{dist}(A^{f_j}, \mathcal{U}_{m''}) \leq \varepsilon] \geq 1 - \delta.$$

Then

$$\mathbb{E}[|O(f_j, \mathbf{B})|] \geq \left(1 - \frac{q^2}{s} - \varepsilon - 3\delta\right) 2^{m''}.$$

Proof. We first argue that for each fixed w ,

$$\Pr_{(\mathbf{B}, f_j) \sim \mathcal{D}_j} [w \in I(f_j, \mathbf{B})] \geq 1 - \frac{q^2}{s}.$$

To see that, let $Q = \{(x_1, y_1, \dots, x_q, y_q)\} \subset \{0, 1\}^{q(n+m)}$ be all possible queries and answers made by $A^f(w)$. That is, $x_1 = x_1(w)$ is the first query made. If $f(x_1) = y_1$ then x_2 is the second query made, and so on. Note that each x_i is determined by $w, x_1, y_1, \dots, x_{i-1}, y_{i-1}$, while y_i can take any value in $\{0, 1\}^m$. In particular, $|Q| = 2^{mq}$.

Next, fix x_1, \dots, x_q and let \mathbf{B} be a randomly chosen partition. Then

$$\Pr_{\mathbf{B}} [x_1, \dots, x_q \text{ in distinct blocks}] \geq 1 - \sum_{i \neq j} \Pr_{\mathbf{B}} [x_i, x_j \text{ in the same block}] \geq 1 - \frac{q^2}{s}.$$

Note that if x_1, \dots, x_q are in distinct blocks, then $f_j(x_1), \dots, f_j(x_q)$ are independently and uniformly chosen in $\{0, 1\}^m$. Thus

$$\begin{aligned}
& \Pr_{(\mathbf{B}, f_j) \sim \mathcal{D}_j} [w \in I(f_j, \mathbf{B})] \\
&= \sum_{(x_1, y_1, \dots, x_q, y_q) \in Q} \Pr[w \in I(f_j, \mathbf{B}) \wedge f_j(x_1) = y_1 \wedge \dots \wedge f_j(x_q) = y_q] \\
&= \sum_{(x_1, y_1, \dots, x_q, y_q) \in Q} \Pr[x_1, \dots, x_q \text{ in distinct blocks} \wedge f_j(x_1) = y_1 \wedge \dots \wedge f_j(x_q) = y_q] \\
&= \sum_{(x_1, y_1, \dots, x_q, y_q) \in Q} \Pr[x_1, \dots, x_q \text{ in distinct blocks}] \cdot \\
&\quad \Pr[f_j(x_1) = y_1 \wedge \dots \wedge f_j(x_q) = y_q | x_1, \dots, x_q \text{ in distinct blocks}] \\
&\geq \sum_{(x_1, y_1, \dots, x_q, y_q) \in Q} \left(1 - \frac{q^2}{s}\right) 2^{-mq} \\
&= 1 - \frac{q^2}{s}.
\end{aligned}$$

We next consider $O(f_j, \mathbf{B})$. Recall that we assume that the distribution of A^{f_j} is ε -close in statistical distance to the uniform distribution $\mathcal{U}_{m''}$. Let $w \in \{0, 1\}^{n''}$ be chosen uniformly and consider the random variable $z = A^{f_j}(w)$. We have

$$\Pr_{(\mathbf{B}, f_j) \sim \mathcal{D}_j, w \in \{0, 1\}^{n''}} [z \in O(f_j, \mathbf{B})] \geq \Pr[w \in I(f_j, \mathbf{B})] \geq 1 - \frac{q^2}{s}.$$

On the other hand, let $u \in \{0, 1\}^{m''}$ be chosen uniformly and independently of all other random variables. Let $E = E(f_j)$ denote the event

$$E := [\text{dist}(A^{f_j}, \mathcal{U}_{m''}) \leq \varepsilon].$$

If we condition that E holds then $\text{dist}(z, u) = \text{dist}(A^{f_j}, \mathcal{U}_{m''}) \leq \varepsilon$. Thus for every fixing of \mathbf{B}, f_j for which E holds we get

$$\Pr[u \in O(f_j, \mathbf{B}) | \mathbf{B}, f_j, E] \geq \Pr[z \in O(f_j, \mathbf{B}) | \mathbf{B}, f_j, E] - \varepsilon.$$

Averaging over the choices of \mathbf{B}, f_j we obtain that

$$\Pr[u \in O(f_j, \mathbf{B}) | E] \geq \Pr[z \in O(f_j, \mathbf{B}) | E] - \varepsilon.$$

We next remove the conditioning on E . As $\Pr[E] \geq 1 - \delta$, we can bound

$$\Pr[u \in O(f_j, \mathbf{B})] \geq \Pr[u \in O(f_j, \mathbf{B}) | E] \Pr[E] \geq \Pr[u \in O(f_j, \mathbf{B}) | E] - \delta$$

and

$$\begin{aligned}
\Pr[z \in O(f_j, \mathbf{B})] &\leq \frac{\Pr[z \in O(f_j, \mathbf{B})]}{\Pr[E]} \\
&\leq \Pr[z \in O(f_j, \mathbf{B}) | E] + \Pr[\neg E] / \Pr[E] \\
&\leq \Pr[z \in O(f_j, \mathbf{B}) | E] + 2\delta.
\end{aligned}$$

Thus

$$\Pr[u \in O(f_j, \mathbf{B})] \geq \Pr[z \in O(f_j, \mathbf{B})] - 3\delta \geq 1 - \frac{q^2}{s} - \varepsilon - 3\delta.$$

This concludes the proof as

$$\mathbb{E}[|O(f_j, \mathbf{B})|] = 2^{m''} \Pr[u \in O(f_j, \mathbf{B})] \geq \left(1 - \frac{q^2}{s} - \varepsilon - 4\delta\right) 2^{m''}.$$

3.4 Main Technical Lemma

The main step in proving Theorem 5 is showing that $O(f_{j-1}, \mathbf{B})$ is not much smaller than $O(f_j, \mathbf{B})$.

Definition 11. *Let us jointly sample \mathbf{B}, f_{j-1}, f_j as follows:*

- Sample $(\mathbf{B}, f_{j-1}) \sim \mathcal{D}_{j-1}$.
- Sample $y_j \in \{0, 1\}^m$ independently and uniformly, and set

$$f_j(x) = \begin{cases} f_{j-1}(x) & x \notin B_j \\ y_j & x \in B_j. \end{cases}$$

We denote this joint distribution over \mathbf{B}, f_{j-1}, f_j by $\mathcal{D}_{j-1,j}$. Observe that if we omit f_{j-1} , then the marginal distribution over (\mathbf{B}, f_j) is indeed \mathcal{D}_j .

Lemma 3 (Main lemma). *Assume that $\delta s \leq j \leq (1 - \delta)s$ and sample $(\mathbf{B}, f_{j-1}, f_j) \sim \mathcal{D}_j$. Then for any $z \in \{0, 1\}^{m''}$ it holds that*

$$\Pr[z \in O(f_{j-1}, \mathbf{B})] \geq \Pr[z \in O(f_j, \mathbf{B})] - \varepsilon,$$

where $\varepsilon = \frac{4q^{5/3}b^{2/3}}{\delta^{4/3}s^{4/3}}$. In particular, if we set $b = 256$ and $\delta = 1/4$ then $\varepsilon = O(q^{5/3}/s^{4/3})$. Averaging over a uniform choice of z gives that

$$\mathbb{E}[|O(f_{j-1}, \mathbf{B})|] \geq \mathbb{E}[|O(f_j, \mathbf{B})|] - \varepsilon 2^{m''}.$$

We note that it is crucial in Lemma 3 that $\varepsilon \ll 1/s$, as we will apply it to relate $O(f_{s/4}, \mathbf{B})$ to $O(f_{s/2}, \mathbf{B})$, which will incur an additional factor of s . Most of the technical challenge in proving Lemma 3 is achieving that, as achieving weaker bounds of the form $\varepsilon = \text{poly}(q)/s$ is much easier. We defer the proof of Lemma 3 to Sect. 4, and next show how it implies Theorem 5.

3.5 Deducing Theorem 5

Let A_5 be the assumed black box reduction given in Theorem 5, specialized for $m = 3n, k = n - 3$. Let n', m' denote the input and output size of A_5^f in this case and let $k' = k'(n, m, k)$. Let A be the black box reduction obtained by first applying A_5 to $f \in \mathcal{F}_{n,m}$, then applying A_1 to A_5^f . Thus $A^f \leq \mathcal{F}_{n'', m''}$ where $n'', m'' \leq \text{poly}(n', m')$. We have $\text{QC}(A) \leq \text{QC}(A_5)\text{QC}(A_1) \leq \text{QC}(A_5)\text{poly}(n', m')$.

Definition 12 (Hybrid distribution). *Sample $(f_j : j = 0, \dots, s)$ jointly as follows:*

- Sample a random partition $\mathbf{B} = (B_1, \dots, B_s)$ of $\{0, 1\}^n$.
- Sample $y_1, \dots, y_s \in \{0, 1\}^m$ uniformly and independently.
- Sample a uniform function $g : \{0, 1\}^n \rightarrow \{0, 1\}^m$.
- If $x \in B_i$, $i \leq j$ then set $f_j(x) = y_i$.
- If $x \in B_i$, $i > j$ then sample $f_j(x) = g(x)$.

Observe that the marginal distribution of (\mathbf{B}, f_j) is \mathcal{D}_j , and moreover, the marginal distribution of $(\mathbf{B}, f_{j-1}, f_j)$ is $\mathcal{D}_{j-1,j}$. According to Claim 3.2, we have the following statements by setting $b = 256$,

- $\Pr_{f_{s/4} \sim \mathcal{D}_{s/4}}[H(f_{s/4}) = n - 2] \geq 1 - 2^{-n}$.
- $\Pr_{f_{s/2} \sim \mathcal{D}_{s/2}}[H(f_{s/2}) = n - 4] \geq 1 - 2^{-n}$.

By the guarantees of A we have that

- If $H(f_{s/4}) \geq (n - 3) + 1$ then $|\text{supp}(A^{f_{s/4}})| \leq 0.1 \cdot 2^{m''}$.
- If $H(f_{s/2}) \leq (n - 3) - 1$ then $\text{dist}(A^{f_{s/2}}, U_{m''}) \leq 0.1$.

Let $q = \text{QC}(A)$. Applying Lemma 2 to $f_{s/2}$, and assuming that $q^2/s \leq 0.1$ gives that

$$\mathbb{E}[|O(A^{f_{s/2}}, \mathbf{B})|] \geq 0.8 \cdot 2^{m''}.$$

On the other hand,

$$\mathbb{E}[|O(A^{f_{s/4}}, \mathbf{B})|] \leq |\text{supp}(A^{f_{s/4}})| \leq 0.1 \cdot 2^{m''}.$$

Lemma 3, applied for $s/4 \leq j \leq s/2$, gives that

$$\mathbb{E}[|O(A^{f_{j-1}}, \mathbf{B})|] \geq [|O(A^{f_j}, \mathbf{B})|] - \varepsilon 2^{m''},$$

where $\varepsilon = O(q^{5/3}/s^{4/3})$. For all these to hold we need to have

$$\varepsilon(s/2 - s/4) \geq 0.7$$

which gives the required bound

$$\text{QC}(A) = q \geq \Omega(s^{1/5}).$$

This then gives us the bound

$$\text{QC}(A_5^f) \geq \Omega(2^{n/5}/\text{poly}(n', m')).$$

4 Proof of Main Technical Lemma: Lemma 3

We prove Lemma 3 in this section. To recall, A is a black box reduction from $\mathcal{F}_{n,m}$ to $\mathcal{F}_{n'',m''}$. We fix $1 \leq j \leq s$ and $z \in \{0,1\}^{m''}$ from here onwards. We sample $(\mathbf{B}, f_{j-1}, f_j) \sim \mathcal{D}_{j-1,j}$ and wish to compare $\Pr[z \in O(f_{j-1}, \mathbf{B})]$ and $\Pr[z \in O(f_j, \mathbf{B})]$. To simplify notations define

$$O(f_{j-1}) = O(f_{j-1}, \mathbf{B}) \quad I(f_{j-1}) = I(f_{j-1}, \mathbf{B}).$$

Define the events

$$X := [z \in O(f_{j-1})] \quad Y := [z \in O(f_j)].$$

Our goal is to show that if Y holds, then with high probability also X holds. The “common information” between X, Y is captured by the random variable

$$\mathcal{C} := (\{(B_i, f_j|_{B_i})\}_{1 \leq i \leq j-1}, B_j, \{(B_i, f_j|_{B_i})\}_{j+1 \leq i \leq s}).$$

Observe that $\{\mathbf{B}\}$ can be computed from \mathcal{C} , which we denote as $\{\mathbf{B}\} = \{\mathbf{B}\}(\mathcal{C})$, and that furthermore

$$f_{j-1} = f_{j-1}(\mathcal{C}, f_{j-1}|_{B_j}) \quad f_j = f_j(\mathcal{C}, f_j|_{B_j}).$$

Thus

$$X = X(\mathcal{C}, f_{j-1}|_{B_j}) \quad Y = Y(\mathcal{C}, f_j|_{B_j}).$$

In particular, given any fixing of \mathcal{C} , we have that $f_{j-1}|_{B_j}$ is a uniform function from B_j to $\{0,1\}^m$, that $f_j|_{B_j}$ is a random constant function, and that the two are independent of each other. We obtain the following claim:

Claim. For any fixing of \mathcal{C} , the random variables $X|\mathcal{C}$ and $Y|\mathcal{C}$ are independent.

Recall that f_{j-1} and f_j differ only in their evaluation on the block B_j . We define a partial function \hat{f} to be the set of inputs where f_{j-1} and f_j agree, namely all inputs outside B_j , and outputs “?” otherwise. Formally, we define the function $\hat{f} : \{0,1\}^n \rightarrow (\{0,1\}^m \cup \{?\})$ as follows:

$$\hat{f}(x) = \begin{cases} f_{j-1}(x) & \text{if } x \notin B_j \\ ? & \text{if } x \in B_j \end{cases}$$

if $x \notin B_j$ then $\hat{f}(x) = f_{j-1}(x) = f_j(x)$. As we now allow for partial functions, we will also need to allow running the black box reduction A on partial functions. We do so by outputting a “?” if the black box reduction queries a point where the partial function is not defined. Observe that \hat{f} can be computed given \mathcal{C} :

$$\hat{f} = \hat{f}(\mathcal{C}).$$

Definition 13 (Black box reduction of a partial function). Let A be a black box reduction from $\mathcal{F}_{n,m}$ to $\mathcal{F}_{n'',m''}$. Let $f : \{0,1\}^n \rightarrow (\{0,1\}^m \cup \{?\})$ be a partial function. We define $A^f : \{0,1\}^{n''} \rightarrow (\{0,1\}^{m''} \cup \{?\})$ to be the following partial function. When computing $A^f(w)$, follows the queries made by A as if f was a total function. However, if at any point we query a point x where $f(x) = ?$ then we abort and output $?$.

We also extend the definition of block compatible inputs and outputs to partial functions in the obvious manner. Define $O(\hat{f}) := O(\hat{f}, \{\mathbf{B}\})$ and define the event E_1 as

$$E_1 = E_1(\mathcal{C}) := [z \in O(\hat{f})].$$

Claim. If E_1 holds then both X and Y also hold: $E_1 \Rightarrow X \wedge Y$.

Proof. If E_1 holds then by definition, there exists $w \in I(\hat{f})$ for which $A^{\hat{f}}(w) = z$. This implies that $A^{f_{j-1}}(w) = A^{f_j}(w) = z$, as since $A^{\hat{f}}(w)$ didn't return a "?", it only queried locations outside B_j , where f_{j-1}, f_j agree. Also, as $w \in I(\hat{f})$ this means that $A^{\hat{f}}(w)$ queries each block B_i at most once, while block B_j is never queried. Thus also $w \in I(f_{j-1}), w \in I(f_j)$. This implies that $z \in O(f_{j-1}), z \in O(f_j)$ which means that X, Y hold.

According to Claim 4 we have,

$$\Pr[X \wedge E_1] = \Pr[Y \wedge E_1] = \Pr[E_1]$$

and hence

$$\begin{aligned} & \Pr[X] - \Pr[Y] \\ &= \Pr[X \wedge E_1] + \Pr[X \wedge \neg E_1] - \Pr[Y \wedge E_1] - \Pr[Y \wedge \neg E_1] \\ &= \Pr[X \wedge \neg E_1] - \Pr[Y \wedge \neg E_1] \end{aligned}$$

Thus, from now on we focus on the case that $\neg E_1$ holds.

4.1 Analyzing the Case that E_1 Doesn't Hold

For each $x \in B_j, y \in \{0,1\}^m$ we define the following extension of \hat{f} . Define a partial function $\hat{f}_{x,y} : \{0,1\}^n \rightarrow (\{0,1\}^m \cup \{?\})$ as follows:

$$\hat{f}_{x,y}(x') := \begin{cases} \hat{f}(x') & \text{if } x' \notin B_j \\ y & \text{if } x' = x \\ ? & \text{if } x' \in B_j \text{ and } x' \neq x \end{cases}$$

For each $x \in B_j$ define

$$R(x) = R_{\hat{f}}(x) := \{y \in \{0,1\}^m : z \in O(f_{x,y})\}.$$

Namely, $R(x)$ is the set of values y for which, if we allow the algorithm to make a single query to B_j at point x which returns y , then z becomes a block compatible output. Observe that the definition of $R(x)$ depends only on \hat{f} , and hence on \mathcal{C} . Crucially, it does not depend on the values of either f_{j-1} or f_j on B_j . We further define

$$r(x) := \Pr_{y \in \{0,1\}^m} [y \in R(x)] = \frac{|R(x)|}{2^m}.$$

As $R(x), r(x)$ depend only on \mathcal{C} , we may consider the following experiment: first sample \mathcal{C} and then sample f_{j-1}, f_j conditioned on \mathcal{C} . That is, f_{j-1}, f_j are equal to $\hat{f} = \hat{f}(\mathcal{C})$ outside $B_j = B_j(\mathcal{C})$, and on B_j we sample f_{j-1} as a random function, while $f_j(x) = y_j$ for all $x \in B_j$, where y_j is randomly chosen. Recall that $E_1 = E_1(\mathcal{C})$.

Claim. For any fixing of \mathcal{C} sample $f_{j-1}, f_j | \mathcal{C}$. Then

$$\Pr[X | \mathcal{C}, \neg E_1] = 1 - \prod_{x \in B_j} (1 - r(x))$$

and

$$\Pr[Y | \mathcal{C}, \neg E_1] \leq \sum_{x \in B_j} r(x).$$

Proof. Consider any fixing of \mathcal{C} and sample f_{j-1}, f_j conditioned on it. Recall that $r(x)$ is a function of \mathcal{C} .

Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$ be any function which agrees with \hat{f} on all $x \notin B_j$. If $z \in O(f)$ then there exists $w \in I(f)$ for which $A^f(w) = z$. As we assume that $\neg E_1$ holds, for any such w , $A^f(w)$ must query the block B_j at least once, and since $w \in I(f)$ it is exactly once, say at point $x_w \in B_j$. But then also $z \in O(\hat{f}_{x_w, f(x_w)})$, which means that $f(x_w) \in R(x_w)$. The converse direction also holds: if $f(x) \in R(x)$ for any $x \in B_j$ then by definition of $R(x)$, there exists w_x such that $w_x \in I(f)$ and $A^f(w_x) = z$ (and moreover $A^f(w_x)$ queries the block B_j exactly at x) and in particular $z \in O(f)$. Thus

$$z \in O(f) \iff \bigvee_{x \in B_j} [f(x) \in R(x)].$$

Next, we apply this logic to both f_{j-1} and f_j . For f_{j-1} , each point $f_{j-1}(x)$ for $x \in B_j$ is uniformly and independently chosen, hence

$$\begin{aligned} \Pr[X | \mathcal{C}, \neg E_1] &= \Pr[z \in O(f_{j-1}) | \mathcal{C}, \neg E_1] \\ &= 1 - \Pr[f_{j-1}(x) \notin R(x) \forall x \in B_j] \\ &= 1 - \prod_{x \in B_j} (1 - r(x)). \end{aligned}$$

For f_j , all the evaluations $\{f_j(x) : x \in B_j\}$ are equal to a uniformly chosen point y_j . Hence by the union bound

$$\begin{aligned} \Pr[Y|\mathcal{C}, \neg E_1] &= \Pr[z \in O(f_j)|\mathcal{C}, \neg E_1] \\ &\leq \sum_{x \in B_j} \Pr[y_j \in R(x)] \\ &\leq \sum_{x \in B_j} r(x). \end{aligned}$$

The following definition allow us to compare the two bounds appearing in Claim 4.1.

Definition 14. Let $\gamma > 0$. A sequence of numbers $r_1, \dots, r_b \in [0, 1]$ is said to be γ -balanced if

$$(1 - \gamma) \sum r_i \leq 1 - \prod (1 - r_i).$$

Let $\gamma > 0$ to be determined later, and define the event E_2 as

$$E_2 = E_2(\mathcal{C}) := [(r(x) : x \in B_j) \text{ is } \gamma\text{-balanced}].$$

The following is a corollary of Claim 4.1 and the definition of X, Y .

Claim. For any fixing of \mathcal{C} for which $\neg E_1, E_2$ hold, it holds that

$$\Pr[X|\mathcal{C}, \neg E_1, E_2] \geq (1 - \gamma) \Pr[Y|\mathcal{C}, \neg E_1, E_2].$$

Proof. Fix \mathcal{C} such that $\neg E_1, E_2$ hold. This fixes in particular B_j and $(r(x) : x \in B_j)$. As E_2 holds, we obtain by Claim 4.1 that

$$\Pr[X|\mathcal{C}] = 1 - \prod_{x \in B_j} (1 - r(x)) \geq (1 - \gamma) \sum_{x \in B_j} r(x) \geq (1 - \gamma) \Pr[Y|\mathcal{C}].$$

Following up on (1), we have

$$\begin{aligned} \Pr[X] - \Pr[Y] &= (\Pr[X \wedge \neg E_1 \wedge E_2] - \Pr[Y \wedge \neg E_1 \wedge E_2]) \\ &\quad + (\Pr[X \wedge \neg E_1 \wedge \neg E_2] - \Pr[Y \wedge \neg E_1 \wedge \neg E_2]) \end{aligned}$$

The second term can simply be bounded by $\Pr[\neg E_1 \wedge \neg E_2]$, which we bound in the next section. For now, let's focus on the first term. Consider any fixing of \mathcal{C} for which $\neg E_1, E_2$ hold. By Claim 4.1 we have that $\Pr[X|\mathcal{C}] \geq (1 - \gamma) \Pr[Y|\mathcal{C}]$. By averaging over such \mathcal{C} , we obtain that

$$\Pr[X \wedge \neg E_1 \wedge E_2] - \Pr[Y \wedge \neg E_1 \wedge E_2] \geq -\gamma \Pr[Y \wedge \neg E_1 \wedge E_2].$$

We can bound the right hand side by

$$\Pr[Y \wedge \neg E_1 \wedge E_2] \leq \Pr[Y \wedge \neg E_1] = \Pr[Y] \Pr[\neg E_1|Y].$$

Claim. $\Pr[\neg E_1|Y] \leq q/j$.

Proof. Sample $(\mathbf{B}, f_{j-1}, f_j) \sim \mathcal{D}_{j-1,j}$. In addition, sample $t \in \{1, \dots, j\}$ uniformly. We will define a “proxy” f'_{j-1} obtained from f_j by changing the value on B_t to a random function. We will then argue that with high probability, this misses any specific set of queries. To that end, define the following random variables:

- $f'_{j-1} : \{0, 1\}^n \rightarrow \{0, 1\}^m$ is a random function defined as follows: if $x \notin B_t$ then $f'_{j-1}(x) = f_j(x)$; and if $x \in B_t$ then $f'_{j-1}(x)$ is a uniformly random element in $\{0, 1\}^m$.
- $\hat{f}' : \{0, 1\}^n \rightarrow (\{0, 1\}^m \cup \{?\})$ is a partial function defined as follows: $\hat{f}'(x) = f'_{j-1}(x) = f_j(x)$ if $x \notin B_t$, and $\hat{f}'(x) = ?$ if $x \in B_t$.
- \mathbf{B}' is equal to \mathbf{B} with blocks B_t, B_j swapped. Namely,

$$\mathbf{B}' = (B_1, \dots, B_{t-1}, B_j, B_{t+1}, \dots, B_{j-1}, B_t, B_{j+1}, \dots, B_s).$$

Observe that the joint distributions of $(\mathbf{B}, f_j, f_{j-1}, \hat{f})$ and $(\mathbf{B}', f_j, f'_{j-1}, \hat{f}')$ are identical. Next, define the following events:

- $Y' := [z \in O(f_j, \{\mathbf{B}'\})]$.
- $E'_1 := [z \in O(\hat{f}', \{\mathbf{B}'\})]$.

Observe that $Y' = Y$ since $\{\mathbf{B}'\} = \{\mathbf{B}\}$, and that the joint distributions of (E_1, Y) and $(E'_1, Y) = (E'_1, Y')$ are identical. Next, fix \mathbf{B}, f_j such that Y holds. This means that there exists $w \in I(f_j, \{\mathbf{B}\}) = I(f_j, \{\mathbf{B}'\})$ such that $A^{f_j}(w) = z$. Let $Q = \text{Query}(A^{f_j}(w))$ be the set of queries made by the algorithm, where $|Q| \leq q$. Observe that if $B_t \cap Q = \emptyset$ then E'_1 holds, and that Q, t are independent random variables. Let $T = T(\mathbf{B}, f_j) = \{i \in \{1, \dots, j\} : B_i \cap Q \neq \emptyset\}$, where $|T| \leq |Q| \leq q$. Thus

$$\Pr[\neg E'_1 | \mathbf{B}, f_j, Y] \leq \Pr[B_t \cap Q \neq \emptyset | \mathbf{B}, f_j, Y] = \Pr[t \in T | \mathbf{B}, f_j, Y] \leq \frac{|T|}{j} \leq \frac{q}{j}.$$

By averaging over \mathbf{B}, f_j , we obtain that $\Pr[\neg E'_1 | Y] \leq q/j$. Thus also

$$\Pr[\neg E_1 | Y] = \Pr[\neg E'_1 | Y] \leq \frac{q}{j}.$$

We thus have

$$\Pr[X \wedge \neg E_1 \wedge E_2] - \Pr[Y \wedge \neg E_1 \wedge E_2] \geq -\gamma(q/j) \Pr[Y]$$

which implies that

$$\Pr[X] - \Pr[Y] \geq -\gamma(q/j) \Pr[Y] - \Pr[\neg E_1 \wedge \neg E_2]$$

which in turn gives the bound

$$\Pr[X] \geq (1 - \gamma(q/j)) \Pr[Y] - \Pr[\neg E_1 \wedge \neg E_2]. \quad (1)$$

To conclude, we need to upper bound $\Pr[\neg E_1 \wedge \neg E_2]$, which is what we do in the next section.

4.2 Bounding the Probability that both E_1, E_2 Don't Hold

We first need a simple corollary of the definition of γ -balanced.

Claim. Let $r_1, \dots, r_b \in [0, 1]$ be a sequence which is not γ -balanced. Then there exist distinct $1 \leq i, j \leq b$ such that $r_i, r_j \geq \gamma/b$.

Proof. Assume not. Then without loss of generality, $r_2, \dots, r_b \leq \gamma/b$. By the inclusion-exclusion principle

$$1 - \prod(1 - r_i) \geq \sum r_i - \sum_{i < j} r_i r_j$$

and by our assumption

$$\sum_{i < j} r_i r_j \leq \left(\sum_{j \geq 2} r_j \right) \left(\sum_{i \geq 1} r_i \right) \leq \gamma \sum r_i.$$

Thus

$$1 - \prod(1 - r_i) \geq (1 - \gamma) \sum r_i,$$

which means that the sequence r_1, \dots, r_b is γ -balanced.

We next define the notion of critical blocks. Informally, a block B_j is critical if all block compatible input w for which $A^f(w) = z$, $A^f(w)$ queries exactly one point in B_j .

Definition 15 (Critical block). Given $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ and a partition $\mathbf{B} = (B_1, \dots, B_s)$ of $\{0, 1\}^n$, we say that the block B_j is critical for f if

$$(A^f(w) = z) \wedge (w \in I(f, \mathbf{B})) \Rightarrow |\text{Query}(A^f(w)) \cap B_j| = 1.$$

A double critical block is a critical block where the output z can be obtained by two block compatible inputs w_1, w_2 which query different points x_1, x_2 in the block.

Definition 16 (Double critical block). Given $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ and a partition $\mathbf{B} = (B_1, \dots, B_s)$ of $\{0, 1\}^n$, we say that the block B_j is double critical for f if

- (i) B_j is a critical block for f .
- (ii) There exist distinct $w_1, w_2 \in I(f, \mathbf{B})$ and distinct $x_1, x_2 \in B_j$ such that

$$(A^f(w_i) = z) \wedge (\text{Query}(A^f(w_i)) \cap B_j = \{x_i\}) \quad i = 1, 2.$$

Lemma 4. Sample $(\mathbf{B}, f_{j-1}) \sim \mathcal{D}_{j-1}$. Then

$$\Pr[B_j \text{ is double critical for } f_{j-1}] \leq \frac{2q^3}{(s - j + 1)^2}.$$

Proof. We can jointly sample \mathbf{B}, f_{j-1} as follows:

- (1) Sample disjoint blocks B_1, \dots, B_{j-1} and $y_1, \dots, y_{j-1} \in \{0, 1\}^m$, and set $f_{j-1}(x) = y_i$ if $x \in B_i$, $i < j$.
- (2) Let $U := \{0, 1\}^m \setminus (B_1 \cup \dots \cup B_{j-1})$. Sample $f_{j-1}(x) \in \{0, 1\}^m$ uniformly and independently for all $x \in U$.
- (3) Sample B_j, \dots, B_s a random partition of U to $s - j + 1$ blocks of size b .

From now on, we fix f_{j-1}, U and consider only the randomness in step (3), namely the random partition of U . For simplicity of notation we say that B_j is critical, or double critical, where in both cases we refer with respect to f_{j-1} .

Define

$$W := \{w \in \{0, 1\}^{n''} : A^{f_{j-1}}(w) = z, |\text{Query}(A^{f_{j-1}}(w)) \cap B_i| \leq 1 \ \forall i = 1, \dots, j-1\}.$$

The set W is the set of *potential* elements in $I(f_{j-1}, \mathbf{B})$, in the sense that they satisfy the requirement $|\text{Query}(A^{f_{j-1}}(w)) \cap B_i| \leq 1$ for the blocks defined so far, namely B_1, \dots, B_{j-1} . If W is empty then no block can be critical, and the lemma follows. So, we assume that W is nonempty. For simplicity of notation define $Q(w) := \text{Query}(A^{f_{j-1}}(w)) \cap U$. Note that so far these definitions do not depend on the choice of the partition of U to B_j, \dots, B_s .

Next, sample a random partition (B_j, \dots, B_s) of U . We say that an input w is *legal* if $A^{f_{j-1}}(w)$ queries each block at most once:

$$W_{\text{legal}} := \{w \in W : |Q(w) \cap B_i| \leq 1 \ \forall i = j, \dots, s\}.$$

Equivalently, $W_{\text{legal}} = \{w \in I(f, \mathbf{B}) : A^{f_{j-1}}(w) = z\}$. The definitions of critical and double critical can then be cast as

$$\begin{aligned} B_j \text{ is critical} &\Leftrightarrow |B_j \cap Q(w)| = 1, \ \forall w \in W_{\text{legal}}; \\ B_j \text{ is double critical} &\Leftrightarrow B_j \text{ is critical and } |B_j \cap (\cup_{w \in W_{\text{legal}}} Q(w))| \geq 2. \end{aligned}$$

Fix $w_1 \in W$ and assume for now that $w_1 \in W_{\text{legal}}$. We will handle the case that $w_1 \notin W_{\text{legal}}$ later.

If B_j is critical then $|B_j \cap Q(w_1)| = 1$. Say $B_j \cap Q(w_1) = \{x_1\}$. If B_j is double critical then there must be another legal $w_2 \in W_{\text{legal}}$ such that $B_j \cap Q(w_2) = \{x_2\}$ where $x_2 \neq x_1$. In particular, $x_1 \notin Q(w_2)$. Thus, for each $x_1 \in Q(w_1)$ define

$$W_{x_1} := \{w \in W : x_1 \notin Q(w)\}.$$

Note that if W_{x_1} is empty then it is impossible that B_j is double critical, w_1 is legal and $B_j \cap Q(w_1) = \{x_1\}$. Thus let

$$Q'(w_1) := \{x_1 \in Q(w_1) : |W_{x_1}| \geq 1\}.$$

For each $x_1 \in Q'(w_1)$ fix an arbitrary $w_{x_1} \in W_{x_1}$. By definition, $x_1 \notin Q(w_{x_1})$. We can bound the probability that B_j is double critical and w_1 is legal by requiring

that $B_j \cap Q(w_1) = \{x_1\}$ and $B_j \cap Q(w_{x_1}) = \{x_2\}$, where by definition $x_1 \neq x_2$, and summing over all choices for x_1, x_2 :

$$\begin{aligned} & \Pr[B_j \text{ is double critical} \wedge w_1 \in W_{\text{legal}}] \\ & \leq \sum_{x_1 \in Q'(w_1)} \sum_{x_2 \in Q(w_{x_1})} \Pr[x_1, x_2 \in B_j] \\ & \leq \frac{q^2}{(s-j+1)^2} \end{aligned}$$

where the bound follows from the union bound and the fact that as B_j, \dots, B_s is a random partition of U , for any fixed distinct $x_1, x_2 \in U$ it holds that $\Pr[x_1, x_2 \in B_j] \leq 1/(s-j+1)^2$.

To conclude the proof, we need to handle the event that w_1 is not legal. First, note that

$$\Pr[w_1 \notin W_{\text{legal}}] \leq \sum_{x_1, x_2 \in Q(w_1), x_1 \neq x_2} \Pr[x_1, x_2 \text{ in the same block}] \leq \frac{q^2}{s-j+1}.$$

We will bound $\Pr[B_j \text{ is double critical} | w_1 \notin W_{\text{legal}}]$. To do that, let's condition on which block does every element of $Q(w_1)$ belong to. Let H_1 denote the family of all functions $h : Q(w_1) \rightarrow \{j, \dots, s\}$. Let F_h denote the event

$$F_h := [x \in B_{h(x)} \quad \forall x \in Q(w_1)].$$

Note that the events F_h are disjoint, and that the event $w_1 \notin W_{\text{legal}}$ is equivalent to F_h holding where h has at least one collision. Thus let

$$H_2 := \{h \in H_1 : \exists x_1, x_2 \in Q(w_1), h(x_1) = h(x_2)\}.$$

We have $w_1 \notin W_l \iff \cup_{h \in H_2} F_h$.

For each $h \in H_2$ let W_h denote the set of $w \in W$ for which $Q(w)$ is not already illegal given h , namely

$$W_h := \{w \in W : \neg \exists x_1, x_2 \in Q_w \cap Q_{w_1}, h(x_1) = h(x_2)\}.$$

If W_h is empty then it is impossible that B_j is double critical and that F_h holds, as there are no legal inputs. Thus let

$$H_3 := \{h \in H_2 : |W_h| \geq 1\}.$$

For each $h \in H_3$ fix an arbitrary $w_h \in W_h$. By definition, if B_j is double critical then we must have $|B_j \cap Q(w_h)| = 1$. We can thus bound

$$\begin{aligned} \Pr[B_j \text{ is double critical} | w_1 \notin W_{\text{legal}}] &= \sum_{h \in H_3} \Pr[B_j \text{ is double critical} | F_h] \Pr[F_h | w_1 \notin W_{\text{legal}}] \\ &\leq \sum_{h \in H_3} \sum_{x \in Q(w_h)} \Pr[x \in B_j | F_h] \Pr[F_h | w_1 \notin W_{\text{legal}}]. \end{aligned}$$

In order to help bound this expression, note that both $h \in H_3$ and $\Pr[F_h|w_1 \notin W_{\text{legal}}]$ are invariant to permutations of the output of h . That is, if we replace $h(x)$ with $\pi(h)(x) = \pi(h(x))$ for any permutation π on $\{j, \dots, s\}$, then $h \in H_3 \iff \pi(h) \in H_3$ and $\Pr[F_h|w_1 \notin W_{\text{legal}}] = \Pr[F_{\pi(h)}|w_1 \notin W_{\text{legal}}]$. Thus

$$\begin{aligned} & \Pr[B_j \text{ is double critical} | w_1 \notin W_{\text{legal}}] \\ & \leq \mathbb{E}_\pi \sum_{h \in H_3} \sum_{x \in Q(w_h)} \Pr[x \in B_j | F_{\pi(h)}] \Pr[F_{\pi(h)} | w_1 \notin W_{\text{legal}}] \\ & = \mathbb{E}_\pi \sum_{h \in H_3} \sum_{x \in Q(w_h)} \Pr[x \in B_{\pi^{-1}(j)} | F_h] \Pr[F_h | w_1 \notin W_{\text{legal}}]. \end{aligned}$$

When we average over π we get that $\Pr[x \in B_{\pi^{-1}(j)} | F_h] = \frac{1}{s-j+1}$, and hence

$$\Pr[B_j \text{ is double critical} | w_1 \notin W_{\text{legal}}] \leq \frac{1}{s-j+1} \sum_{h \in H_3} \sum_{x \in Q(w_h)} \Pr[F_h | w_1 \notin W_{\text{legal}}] = \frac{q}{s-j+1}.$$

We obtained the bound

$$\begin{aligned} & \Pr[B_j \text{ is double critical} \wedge w_1 \notin W_{\text{legal}}] \\ & = \Pr[B_j \text{ is double critical} | w_1 \notin W_{\text{legal}}] \Pr[w_1 \notin W_{\text{legal}}] \\ & \leq \frac{q}{s-j+1} \cdot \frac{q^2}{s-j+1} = \frac{q^3}{(s-j+1)^2}. \end{aligned}$$

Combining the two bounds we obtained, we conclude that

$$\begin{aligned} & \Pr[B_j \text{ is double critical}] \\ & = \Pr[B_j \text{ is double critical} \wedge w_1 \in W_{\text{legal}}] + \Pr[B_j \text{ is double critical} \wedge w_1 \notin W_{\text{legal}}] \\ & \leq \frac{q^2}{(s-j+1)^2} + \frac{q^3}{(s-j+1)^2} \leq \frac{2q^3}{(s-j+1)^2}. \end{aligned}$$

Claim. Let \mathcal{C} be such that $\neg E_1, \neg E_2$ hold. Sample $f_{j-1} | \mathcal{C}$. Then

$$\Pr[B_j \text{ is double critical for } f_{j-1} | \mathcal{C}] \geq (\gamma/b)^2.$$

In particular,

$$\Pr[B_j \text{ is double critical for } f_{j-1} | \neg E_1, \neg E_2] \geq (\gamma/b)^2.$$

Proof. Fix any \mathcal{C} such that $\neg E_1, \neg E_2$ hold. By Claim 4.2 there are distinct $x_1, x_2 \in B_j$ such that $r(x_i) \geq \gamma/b$. Note that if $f_{j-1}(x_i) \in R(x_i)$ for both $i = 1, 2$, then B_j is double critical for f_{j-1} . As $f_{j-1}(x_i)$ are sampled independently, we have

$$\Pr[B_j \text{ is double critical for } f_{j-1} | \mathcal{C}] \geq \Pr[f_{j-1}(x_i) \in R(x_i), i = 1, 2 | \mathcal{C}] \geq (\gamma/b)^2.$$

Combining Lemma 4 and Claim 4.2 gives a bound on the probability that both E_1, E_2 don't hold.

Corollary 1. $\Pr[\neg E_1 \wedge \neg E_2] \leq \frac{2q^3b^2}{\gamma^2(s-j+1)^2}$.

Proof. Let $F := [B_j \text{ is double critical for } f_{j-1}]$. We have

$$\Pr[\neg E_1 \wedge \neg E_2] = \frac{\Pr[\neg E_1 \wedge \neg E_2 \wedge F]}{\Pr[F|\neg E_1 \wedge \neg E_2]} \leq \frac{\Pr[F]}{\Pr[F|\neg E_1, \neg E_2]} \leq \frac{2q^3b^2}{\gamma^2(s-j+1)^2}.$$

The claim then follows.

We can finally prove Lemma 3. Appealing to (1) we have that

$$\Pr[X] \geq \left(1 - \frac{\gamma q}{j}\right) \Pr[Y] - \frac{2q^3b^2}{\gamma^2(s-j+1)^2} \geq \Pr[Y] - \left(\frac{\gamma q}{j} + \frac{2q^3b^2}{\gamma^2(s-j+1)^2}\right). \quad (2)$$

Let us denote

$$\varepsilon = \frac{\gamma q}{j} + \frac{2q^3b^2}{\gamma^2(s-j+1)^2}.$$

We now choose γ to minimize ε . Let us assume (as we have) that $\delta s \leq j \leq (1-\delta)s$ for some absolute constant $\delta > 0$. Then

$$\varepsilon \leq \frac{\gamma q}{\delta s} + \frac{2q^3b^2}{\gamma^2\delta^2s^2}.$$

We choose $\gamma = (2q^2b^2/\delta s)^{1/3}$ to equate the two terms, so that

$$\varepsilon \leq \frac{4q^{5/3}b^{2/3}}{\delta^{4/3}s^{4/3}}.$$

In particular, as we choose b, δ to be absolute constants, we have $\varepsilon \leq O(q^{5/3}/s^{4/3})$.

5 Conclusions and Open Problems

In this paper, we studied impossibility of reversing entropy in black-box constructions. An obvious question that remains open is whether our result can be extended to the computational setting, given some complexity assumptions. Note that if we assume that $P = NP$ then $P = \text{NISZK} = \text{SZK} = \text{NP}$.

Besides considering the relationship between NISZK and SZK, it is also interesting to explore relationships between other non-computational zero-knowledge proof systems. Concretely, what are the relationships between NIPZK and PZK, the perfect statistical analogs of NISZK and SZK, and the statistical versions. In particular, Malka [15] gave a complete problem for NIPZK, which can be a good starting point to apply the techniques developed in this paper and separate NISZK and NIPZK. In a recent work of Bouland et al. [3] gave an oracle to separate NISZK and NIPZK, however we are still interested in whether we can separate them in random oracle model.

Acknowledgement. We would like to thank Iftach Haitner and Salil Vadhan for helpful discussion, and we would also like to thank anonymous TCC reviewers for their comments. Jiapeng Zhang would also like to thank his wife, Yingcong Li.

References

1. Blum, M., De Santis, A., Micali, S., Persiano, G.: Noninteractive zero-knowledge. *SIAM J. Comput.* **20**(6), 1084–1118 (1991)
2. Blum, M., Feldman, P., Micali, S.: Non-interactive zero-knowledge and its applications. In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pp. 103–112. ACM (1988)
3. Bouland, A., Chen, L., Holden, D., Thaler, J., Vasudevan, P.N.: On SZK and PP. *arXiv preprint [arXiv:1609.02888](https://arxiv.org/abs/1609.02888)* (2016)
4. De Santis, A., Di Crescenzo, G., Persiano, G.: The knowledge complexity of quadratic residuosity languages. *Theoret. Comput. Sci.* **132**(1–2), 291–317 (1994)
5. De Santis, A., Di Crescenzo, G., Persiano, G., Yung, M.: Image density is complete for non-interactive-SZK. In: Larsen, K.G., Skyum, S., Winskel, G. (eds.) *ICALP 1998*. LNCS, vol. 1443, pp. 784–795. Springer, Heidelberg (1998). doi:[10.1007/BFb0055102](https://doi.org/10.1007/BFb0055102)
6. De Santis, A., Di Crescenzo, G., Persiano, P.: Randomness-efficient non-interactive zero knowledge. In: Degano, P., Gorrieri, R., Marchetti-Spaccamela, A. (eds.) *ICALP 1997*. LNCS, vol. 1256, pp. 716–726. Springer, Heidelberg (1997). doi:[10.1007/3-540-63165-8_225](https://doi.org/10.1007/3-540-63165-8_225)
7. Gennaro, R., Micciancio, D., Rabin, T.: An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products. In: *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pp. 67–72. ACM (1998)
8. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. *J. ACM (JACM)* **33**(4), 792–807 (1986)
9. Goldreich, O., Sahai, A., Vadhan, S.: Can statistical zero knowledge be made non-interactive? or on the relationship of SZK and *NISZK*. In: Wiener, M. (ed.) *CRYPTO 1999*. LNCS, vol. 1666, pp. 467–484. Springer, Heidelberg (1999). doi:[10.1007/3-540-48405-1_30](https://doi.org/10.1007/3-540-48405-1_30)
10. Goldreich, O., Vadhan, S.: Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In: *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity*, pp. 54–73. IEEE (1999)
11. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. *SIAM J. Comput.* **18**(1), 186–208 (1989)
12. Haitner, I., Harnik, D., Reingold, O.: On the power of the randomized iterate. In: Dwork, C. (ed.) *CRYPTO 2006*. LNCS, vol. 4117, pp. 22–40. Springer, Heidelberg (2006). doi:[10.1007/11818175_2](https://doi.org/10.1007/11818175_2)
13. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. *SIAM J. Comput.* **28**(4), 1364–1396 (1999)
14. Holenstein, T., Renner, R.: One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption. In: Shoup, V. (ed.) *CRYPTO 2005*. LNCS, vol. 3621, pp. 478–493. Springer, Heidelberg (2005). doi:[10.1007/11535218_29](https://doi.org/10.1007/11535218_29)
15. Malka, L.: How to achieve perfect simulation and a complete problem for non-interactive perfect zero-knowledge. In: Canetti, R. (ed.) *TCC 2008*. LNCS, vol. 4948, pp. 89–106. Springer, Heidelberg (2008). doi:[10.1007/978-3-540-78524-8_6](https://doi.org/10.1007/978-3-540-78524-8_6)

16. Peikert, C., Vaikuntanathan, V.: Noninteractive statistical zero-knowledge proofs for lattice problems. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 536–553. Springer, Heidelberg (2008). doi:[10.1007/978-3-540-85174-5_30](https://doi.org/10.1007/978-3-540-85174-5_30)
17. Sahai, A., Vadhan, S.: A complete problem for statistical zero knowledge. J. ACM (JACM) **50**(2), 196–249 (2003)
18. Vadhan, S.: Personal Communication (2016)

Theory of Cryptography

15th International Conference, TCC 2017, Baltimore,
MD, USA, November 12-15, 2017, Proceedings, Part I

Tauman Kalai, Y.; Reyzin, L. (Eds.)

2017, XVII, 812 p. 80 illus., Softcover

ISBN: 978-3-319-70499-9