Black-box use of One-way Functions is Useless for Optimal Fair Coin-Tossing

Hemanta K. Maji
Department of Computer Science, Purdue University, USA
hmaji@purdue.edu

Mingyuan Wang
Department of Computer Science, Purdue University, USA
wang1929@purdue.edu

Abstract

A two-party fair coin-tossing protocol is a coin-tossing protocol that guarantees output to the honest party even when the other party aborts during the protocol execution. Cleve (STOC–1986) demonstrated that, even when the parties are computationally bounded, a fail-stop adversary can alter the output distribution of the honest party by (roughly) $1/r$ (in the statistical distance) in an r-message coin-tossing protocol. An optimal fair coin-tossing protocol ensures that no adversary can alter the output distribution beyond $1/r$.

In a seminal result, Moran, Naor, and Segev (TCC–2009) constructed the first optimal fair coin-tossing protocol using oblivious transfer protocols. Whether the existence of oblivious transfer protocols is a necessary computational hardness assumption for optimal fair coin-tossing remains one of the most fundamental open problems in theoretical cryptography. Results of Impagliazzo and Luby (FOCS–1989) and Cleve and Impagliazzo (1993) together imply that the existence of one-way functions is necessary for optimal fair coin-tossing. However, the sufficiency of the existence of one-way functions is not known.

Towards this research endeavor, our work proves a black-box separation of optimal fair coin-tossing from the existence of one-way functions. That is, the black-box use of one-way functions is unlikely to enable optimal fair coin-tossing. Following the standard Impagliazzo and Rudich (STOC–1989) approach, our work considers any r-message fair coin-tossing protocol in the random oracle model where the parties have unbounded computational power. We demonstrate a fail-stop attack strategy for one of the parties to alter the output distribution of the honest party by $1/\sqrt{r}$. Our result, therefore, proves that the r-message coin-tossing protocol of Blum (COMPCON–1982) and Cleve (STOC–1986), which uses one-way functions in a black-box manner, is qualitatively the best possible protocol.

Several previous works, for example, Dachman–Soled, Lindell, Mahmoody, and Malkin (TCC–2011), Haitner, Omri, and Zarosim (TCC–2013), and Dachman–Soled, Mahmoody, and Malkin (TCC–2014), made partial progress on this research problem by proving this black-box separation assuming some restrictions on the coin-tossing protocol. Our work diverges significantly from these previous approaches to prove this black-box separation in its full generality. The starting point is the recently introduced potential-based inductive proof techniques for demonstrating large gaps in martingales in the information-theoretic plain model. Our technical contribution lies in identifying a global invariant that enables the extension of this technique to the random oracle model.

Keywords and phrases Fair Coin-Tossing, Black-box Separation, One-way Function, Random Oracle

Funding The research effort is supported in part by an NSF CRII Award CNS–1566499, an NSF SMALL Award CNS–1618822, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Award, a Purdue Research Foundation (PRF) Award, and

The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

Contents

1 Introduction

Ideally, in any cryptographic task, one would like to ensure that the honest parties receive their output when adversarial parties refuse to participate any further. The objective of guaranteed output delivery, or *fair computation*, is challenging to ensure even for fundamental cryptographic primitives like two-party coin-tossing. A *two-party fair coin-tossing protocol* assures that the honest party receives her output bit even when the adversary aborts during the protocol execution. Cleve [Cle86] demonstrated that, even for computationally bounded parties, a *fail-stop adversary*[1] could alter the output distribution by $1/r$ (in statistical distance) in any r-message interactive protocols. Intuitively, any r-message interactive protocol is $1/r$-*insecure*. An *optimal* r-message two-party fair coin-tossing protocol ensures that it is only $1/r$-insecure.

In a seminal result, nearly three decades after the introduction of optimal fair coin-tossing protocols, Moran, Naor, and Segev [MNS09] presented the first optimal coin-tossing protocol construction based on the existence of (unfair) secure protocols for the oblivious transfer functionality.[2] Shortly after that, in a sequence of exciting results, several optimal/near-optimal fair protocols were constructed for diverse two-party and multi-party functionalities [GHKL08, BOO10, GK10, BLOO11, ALR13, HT14, Ash14, Mak14, ABMO15, AO16, BHLT17]. However, each of these protocols assumes the existence of secure protocols for oblivious transfer as well.

In theoretical cryptography, a primary guiding principle of research is to realize a cryptographic primitive securely using the minimal computational hardness assumption. Consequently, the following fundamental question arises naturally.

Question: Is the existence of oblivious transfer
necessary
for constructing optimal fair coin-tossing protocols?

For example, the results of Impagliazzo and Luby [IL89] and Cleve and Impagliazzo [CI93] together imply that the existence of one-way functions is necessary for optimal fair coin-tossing. However, it is unclear whether one-way functions can help realize optimal fair coin-tossing or not. For instance, historically, for a long time, one-way functions were not known to imply several fundamental primitives like pseudorandom generators [ILL89, Hås90], and digital signatures [NY89, Rom90]; eventually, however, secure constructions were discovered. Therefore, is it just the case that we have not yet been able to construct optimal fair coin-tossing protocols securely from one-way functions, or are there inherent barriers to such constructions?

Among several possible approaches, a prominent technique to address the question above is to study it via the lens of black-box separations, as introduced by Impagliazzo and Rudich [IR89]. Suppose one "*black-box separates* the cryptographic primitive Q from another cryptographic primitive P." Then, one interprets this result as indicative of the fact that the primitive P is unlikely to facilitate the secure construction of Q using black-

[1] A fail-stop adversary behaves honestly and follows the prescribed protocol. However, based on her private view, she may choose to abort the protocol execution.

[2] Oblivious transfer takes $(x_0, x_1) \in \{0,1\}^2$ as input from the first party, and a choice bit $b \in \{0,1\}$ from the second party. The functionality outputs the bit x_b to the second party, and the first party receives no output. The security of this functionality ensures that the first party has no advantage in predicting the choice bit b. Furthermore, the second party has no advantage in predicting the other input bit x_{1-b}.

box constructions.[3] Consequently, to reinforce the necessity of the existence of oblivious transfer protocols for optimal fair coin-tossing, one needs to provide black-box separation of optimal fair coin-tossing protocols from computational hardness assumptions that are weaker than the existence of oblivious transfer protocols; for example, the existence of one-way functions [IL89, IR89].

Our results. In this work, we prove this (fully) black-box separation of optimal two-party fair coin-tossing protocol from the existence of one-way functions. In particular, we show that any r-message two-party coin-tossing protocol in the *random oracle model*, where parties have unbounded computational power, is $1/\sqrt{r}$-insecure. In turn, this result settles in the positive the longstanding open problem of determining whether the coin-tossing protocol of Blum [Blu82] and Cleve [Cle86] achieves the highest security while using one-way functions in a black-box manner.

Our proof relies on a potential-based argument that proceeds by identifying a global invariant across coin-tossing protocols in the random oracle model to guide the design of good fail-stop adversarial attacks. As a significant departure from previous approaches [DLMM11, DMM14], our analysis handles the entire sequence of *curious random oracle query-answer pairs* as one *single instance of information exposure*.

1.1 Our Contributions

Before we proceed to present a high-level informal summary of our results, we need an informal definition of two-party coin-tossing protocols in the random oracle model that are secure against fail-stop adversaries. An (r, n, X_0)-coin-tossing protocol is a *two-party interactive protocol* with final output $\in \{0, 1\}$, and parties have oracle access to a random oracle[4] such that the following conditions are satisfied.

1. Alice and Bob exchange a total of r messages (of arbitrary length) during the protocol.[5]
2. The oracle query complexity of both Alice and Bob is (at most) n in every execution of the protocol.
3. At the end of the protocol, parties always agree on the output $\in \{0, 1\}$. Furthermore, the expectation of the output over all possible protocol executions is $X_0 \in [0, 1]$.
4. We consider only fail-stop adversarial strategies. If one party aborts during the protocol execution, then the honest party outputs a defense coin $\in \{0, 1\}$ based on her view.

We emphasize that there are additional subtleties involved in defining coin-tossing protocols in the random oracle model, and Section 2.3 addresses them. In this section, we rely on a minimalist definition that suffices to introduce our results. Our main technical result is the following consequence for any (r, n, X_0)-coin-tossing protocol.

[3] Most constructions in theoretical computer science and cryptography are black-box in nature. That is, they rely only on the input-output behavior of the primitive P, and are oblivious to, for instance, the particular implementation of the primitive P. There are, however, some highly non-trivial non-black-box constructions in theoretical computer science, for example, [Coo71, Yao86, GMW87, Bar02]. However, an infeasibility of black-box constructions to realize Q from P indicates the necessity of new non-black-box constructions, which, historically, have been significantly infrequent.

[4] A random oracle is a function sampled uniformly at random from the set of all functions mapping $\{0, 1\}^n \to \{0, 1\}^n$.

[5] In this paper, we avoid the use of "round." Some literature assumes one round to contain only one message from some party. Other literature assumes that one round has one message from all the parties. Instead, for clarity, we refer to the total number of messages exchanged in the entire protocol.

▶ Informal Theorem 1 (Main Technical Result). There exists a universal constant $c > 0$ and a polynomial $p(\cdot)$ such that the following holds. Let π be any (r, n, X_0)-coin-tossing protocol in the information-theoretic random oracle model, where $r, n \in \mathbb{N}$ and $X_0 \in (0, 1)$. Then, there exists a fail-stop adversarial strategy for one of the parties to alter the expected output of the honest party by $\geq c \cdot X_0(1 - X_0)/\sqrt{r}$ and performs at most $p(nr/X_0(1 - X_0))$ additional queries to the random oracle.

We remark that X_0 may be a function of r and n itself. For example, the expected output X_0 may be an inverse polynomial of r (say).

This technical result directly yields the following (fully) black-box separation result using techniques in [IR89, RTV04].

▶ **Corollary 1** (Black-box Separation from One-way Functions). *There exists a universal constant $c > 0$ such that the following holds. Let π be any r-message two-party protocol that uses any one-way function in a fully black-box manner. Suppose, at the end of the execution of π, both parties agree on their output $\in \{0, 1\}$. Before the beginning of the protocol, let the expectation of their common output be $X_0 \in (0, 1)$. Then, there exists a fail-stop adversarial strategy for one of the parties to alter the expected output of the honest party by $\geq c \cdot X_0(1 - X_0)/\sqrt{r}$.*

We emphasize that the black-box separation extends to any primitive (and their exponentially-hard versions) that one can construct in a black-box manner from random oracles or ideal ciphers, which turn out to be closely related to random oracles [CPS08, HKT11]. Furthermore, the impossibility result in the random oracle model implies black-box separations from other (more structured) cryptographic primitives like regular one-way functions and one-way permutations as well. Although these primitives cannot be constructed from random oracles/ideal cipher in a black-box manner, using by-now well-establish techniques in this field (see, for example, [IR89]), the main technical result suffices to prove the separations from these structured primitives. As an aside, we remark that the full version of this paper shall also present a black-box separation from the existence of key-agreement protocols, which requires no additional new technical ideas and follows the general the techniques introduced in [MMP14b]. We chose to omit the proof of this result from this draft to ensure that the readability of the paper is not harmed.

This black-box separation from one-way functions indicates that the two-party coin-tossing protocol of Blum [Blu82] and Cleve [Cle86], which uses one-way functions in a black-box manner, achieves the best possible security for any r-message protocol. Their protocol is $1/\sqrt{r}$-insecure, and any r-message protocol cannot have asymptotically better security by only using one-way functions in a black-box manner, thus resolving this fundamental question after over three decades.

1.2 Prior Related Works and Comparison

There is a vast literature of defining and constructing fair protocols for two-party and multi-party functionalities [GHKL08, BOO10, GK10, BLOO11, ALR13, HT14, Ash14, Mak14, ABMO15, AO16, BHLT17]. In this paper, our emphasis is on the intersection of this literature with black-box separation results.

In a seminal result, Impagliazzo and Rudich [IR89] introduced the notion of black-box separation for cryptographic primitives. Intuitively, separating a primitive Q from a primitive P indicates that attempts to secure realize Q solely on the black-box use of P are unlikely to succeed. Reingold, Trevisan, and Vadhan [RTV04] highlighted the subtleties involved in defining black-box separations by delineating several variants of separations. In their terminology, this work pertains to a *fully black-box* separation where the construction uses P in a black-box manner, and the security reduction uses the adversary in a black-box manner as well. Since the inception of black-box separations in 1989, this research direction has been a fertile ground for highly influential research [Rud88, IR89, Rud92, Sim98, GKM$^+$00, GT00, GMR01, GGK03, GMM07, BPR$^+$08, BM09, Vah10, MM11, KSY11, DLMM11, HOZ13, MMP14a, MMP14b, DMM14, MM16, MMN$^+$16, GMM17a, GMM17b, GHMM18, GMMM18]. Among these results, in this paper, we elaborate on the hardness of computation results about fair computation protocols.

Furthermore, recent work of Haitner, Nissim, Omri, Shaltiel, and Silbak [HNO$^+$18] introduces the notion of the "computational essence of key-agreement." Haitner, Makriyannis, and Omri [HMO18] prove that r-message coin-tossing protocols imply key-agreement protocols if they are less than $1/\sqrt{r}$-insecure and r is very small. Observe that proving the implication that key-agreement protocol exists is a significantly stronger result as compared to demonstrating a black-box separation from key-agreement.

Among the related works in black-box separation, the most relevant to our problem are the following. Haitner, Omri, and Zarosim [HOZ13], for input-less functionalities, lift the hardness of computation results in the information-theoretic plain model against semi-honest adversaries to the random oracle model, i.e., random oracles are useless. However, coin-tossing is trivial to realize securely against semi-honest adversaries, and fail-stop adversarial strategies are not semi-honest. Dachman–Soled, Lindell, Mahmoody, and Malkin [DLMM11] proved that the random oracle could be "compiled away" if the coin-tossing protocol has $r = \mathcal{O}(n/\log n)$ messages. Therefore, the fail-stop adversarial strategy of Cleve and Impagliazzo [CI93] in the information-theoretic plain model also succeeds against the two-party coin-tossing protocol in the random oracle model. Finally, Dachman–Soled, Mahmoody, and Malkin [DMM14] show a fail-stop adversarial strategy against a particular class of fair coin-tossing protocols, namely, *function oblivious* protocols. An exciting feature of this work is that the attack performed by the adversarial party does not proceed by compiling away the random oracle, similar to [MMP14a, MMP14b].

Recently, there have been two works providing improvements to the fail-stop adversarial attacks of Cleve and Impagliazzo [CI93] in the information-theoretic plain model. These results proceed by induction on r and employ a potential argument to lower-bound the performance of the most devastating fail-stop adversarial strategy against a coin-tossing protocol. Khorasgani, Maji, and Mukherjee [KMM19] generalize (and improve) the fail-stop attack of Cleve and Impagliazzo [CI93] to arbitrary $X_0 \in (0, 1)$ and even when X_0 depends on r and tends to 0 or 1. Khorasgani, Maji, and Wang [KMW20] decouple the number of messages r in a coin-tossing protocol and the number of defense updates d the two parties perform. They show that a two-party coin-tossing protocol in the information-theoretic plain model is $1/\sqrt{d}$-insecure, independent of the number of messages r in the protocol.

Our work identifies a global invariant that enables the extension of the approach of [KMW20] to the random oracle model. Furthermore, we simplify the proof of their result as well.

1.3 Technical Overview

In this section, we introduce a fundamental technical idea underlying our approach to proving the main theorem. So, given an r-message coin-tossing protocol in the random oracle model, our objective is to design a fail-stop adversary who changes the output distribution of the honest party by $1/\sqrt{r}$.

Preprocessing. Let π be an r-message two-party fair coin-tossing protocol with query complexity n in the random oracle model, and parties have unbounded computational power. The primary difference between the random oracle model from the plain model is the following. In the plain model, conditioned on the public transcript, the joint distribution of Alice's and Bob's views consistent with the partial transcript is a product distribution. However, in the random oracle model, the joint distribution of their views might be correlated by the random oracle via their private query-answers. One needs to remove this correlation.[6]

Towards this objective, one uses a *heavy querier* [IR89, BM09, MMP14b]. A *heavy query* q is a query to the random oracle such that the probability of Alice or Bob performing this query (conditioned on the public transcript)[7] surpasses a fixed threshold ϵ. The heavy querier keeps performing heavy queries and adding their corresponding answer to the *augmented* public transcript. It stops when there are no more heavy queries left. It performs a total of $\mathcal{O}(n/\epsilon)$ queries in expectation, and, consequently (by an averaging argument), $\mathcal{O}\left(n/\epsilon^2\right)$ queries with probability (at least) $(1-\epsilon)$. Intuitively, once there are no heavy queries left, the joint distribution of Alice's and Bob's views conditioned on the augmented public transcript (which now also includes the query-answer pairs added by the heavy querier itself) is close to the product of the marginal distributions of Alice and Bob views.

Next, suppose we start from an augmented transcript where all queries are ϵ-*light* (that is, no query is ϵ-heavy). Alice performs some private queries and sends the next message in the protocol. Interestingly, the joint distribution of Alice-Bob views continues to be close to the product of their marginal distributions [BM09]; however, all queries may not be ϵ light anymore.[8] So, one needs to run the heavy querier at this point in the protocol. Furthermore, this process continues after every message that Alice and Bob exchange during the protocol evolution.

We refer to the protocol π augmented with heavy querier's sequence of query-answer pairs as the augmented protocol π^+. For the simplicity of presentation, in the sequel, we shall assume that the heavy querier always terminates after adding $\mathcal{O}\left(n/\epsilon^2\right)$ query-answer pairs over the entire protocol execution of π^+. Moreover, the distribution of Alice-Bob joint views conditioned on the augmented transcript immediately before and after Alice and Bob exchange messages prescribed in π is *identical* to the product distribution of their marginal distributions.

Bottleneck. Each party maintains a defense coin $\in \{0,1\}$ (in their private view) as a protection against the adversarial party aborting during the protocol execution.[9] The joint distribution of the defense coins of Alice and Bob in π^+ is a product distribution immediately before and after Alice/Bob sends their messages prescribed in π. We remind the readers that, in reality, the joint distribution is close to a product distribution; however, we have made the simplifying assumption above that, for intuitive purposes, we consider them to be a product distribution. This observation follows from the fact that the defense coins of the parties are a deterministic function of their respective private views.[10] The subsequent

[6] Otherwise, the oblivious transfer functionality is securely realizable in the random oracle model. After that, one can use the Moran–Naor–Segev [MNS09] protocol to realize optimal fair coin-tossing protocol securely.

[7] Using unbounded computational power, it is computationally efficient to calculate the heavy queries [JVV86, BGP00].

[8] For example, Alice may send to Bob one of her private queries (not the answer) that she performed during the next-message generation.

[9] Such protocols are referred to as *instantaneous protocols* in the literature [DLMM11]. One can assume, without loss of generality, that a fair protocol is an instantaneous protocol.

[10] This observation is very subtle. There are several other natural candidate characteristics of the protocol

query-answer pairs introduced by the heavy queries in π^+ may, however, reveal information about the parties' defense coins.

Cleve–Impagliazzo [CI93] fail-stop attack, which is the primary workhorse underlying the attacks on coin-tossing protocols by [DLMM11, DMM14], crucially relies on the following invariant during the evolution of π^+. Any information revealed by the transcript of the protocol keeps (at least) one party's expected defense unchanged. For example, when Alice sends a message in π^+, Bob's expected defense remains unchanged (due to the product distribution of their joint views). If there are D instances of such information revelations during the entire protocol execution, then Cleve–Impagliazzo [CI93] fail-stop attack guarantees an attack that alters the output distribution by $1/\sqrt{D}$.

Now, let us reason about how D compares to r. Observe that $D \geq r$ definitely, because parties may update their private defenses r times when they prepare the messages prescribed in π. However, it may be the case that $D \gg r$ in π^+ because the query-answer pairs added by the heavy querier has the potential of introducing several such information revelation instances.[11] There are, in fact, significantly worse concerns. The heavy queries may simultaneously reveal information about both Alice's and Bob's defense coins by discovering a query performed by both of them (namely, an *intersection query* [IR89]). If this event happens, then Cleve–Impagliazzo [CI93] breaks down entirely, and there is no way to salvage an attack on π^+. Therefore, a direct application of Cleve–Impagliazzo [CI93] to the augmented protocol π^+ is bound to fail.

A Stepping Stone: Khorasgani, Maji, and Wang [KMW20] Approach. Recently, Khorasgani, Maji, and Wang [KMW20] present a technique to remove one of the bottlenecks mentioned above. They propose an inductive approach (generalizing the approach of [KMM19]) to construct fail-stop attacks on coin-tossing protocols in the information-theoretic plain model. They use an appropriate potential function to control the insecurity introduced by various fail-stop attack strategies.

Observe that, in the information-theoretic plain model, when a party sends a message, the expected defense of the other party remains unchanged. Consider a D message protocol where parties update their defenses only r times. Cleve–Impagliazzo [CI93] attack would have indicated only a $1/\sqrt{D}$-insecurity. However, Khorasgani, Maji, and Wang [KMW20] demonstrate $1/\sqrt{r}$-insecurity.

We present a brief technical summary of one of their critical technical steps. Consider the following potential function used in [KMW20].

$$\Phi(x, a, b) := x(1-x) + (x-a)^2 + (x-b)^2.$$

▶ Remark 1. We provide some intuition underlying the choice of the potential function. The parameter x shall represent the expected output of the protocol, a shall represent the expected Alice defense, and b shall represent the expected Bob defense of a protocol. The potential function lower-bounds the most devastating fail-stop attack on this protocol. Intuitively, the potential function punishes Alice if her a is far from x, that is, when her expected defense deviates far from the expected output. The potential function, thus, incentivizes Alice to set her defense close to the expected color. Similarly, the potential has a symmetric term for expected Bob's defense that incentivizes him to set his expected defense close to the

that do not possess this unique "product distribution" property. For example, the expected output may depend on future random oracle query-answer pairs; thus, it need not have this property.

[11] For example, Bob performs n random oracle queries. The heavy querier might reveal all these queries sequentially. These queries may incrementally reveal information about Bob's defense coin. So, it is possible to have $D \geq n \gg r$.

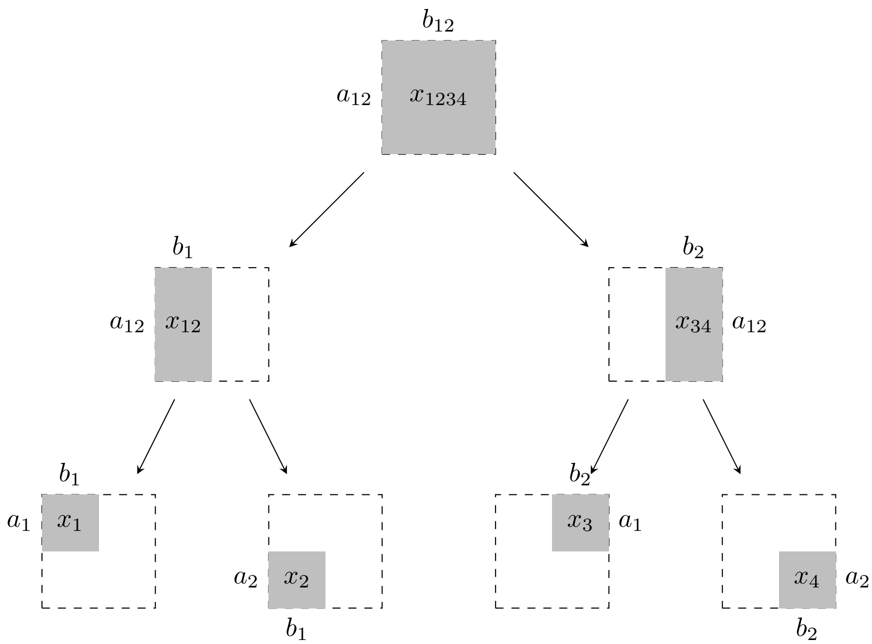

Figure 1 An intuitive pictorial summary of the potential argument of Khorasgani, Maji, and Wang [KMW20]. The shaded regions denote the pairs of consistent Alice and Bob views. The first message is sent by Bob, and the second message is sent by Alice. We denote the average of a_1 and a_2 by a_{12}. Similarly, b_{12} represents the average of b_1 and b_2. Finally, we define x_{12} as the average of x_1 and x_2, x_{34} as the average x_3 and x_4, and x_{1234} as the average of x_{12} and x_{34}. The potential at the root is $\Phi(x_{1234}, a_{12}, b_{12})$. The potential at the leaves are $\Phi(x_1, a_1, b_1)$, $\Phi(x_2, a_2, b_1)$, $\Phi(x_3, a_1, b_2)$, and $\Phi(x_4, a_2, b_2)$. The "expected potential of the parameters associated with the leaves" is at least the "potential of the expected parameters at the root" using the property of the potential function $\Phi(\cdot, \cdot, \cdot)$ and Jensen's inequality.

expected output. Finally, the last term is a variance of the expected output, which accounts for the quality of the fail-stop attack owing to x. For example, if x is already close to 0 or 1, any fail-stop attack may not be able to change the output distribution significantly.

Analytically, this function has the property that if a is a constant, then the potential is convex in x and b. Analogously, if b is a constant, then the potential is convex in x and a. However, one cannot handle the case where a, b, and x change simultaneously (Figure 3 presents a counterexample). In Figure 1 we demonstrate how one can lift the potential from the leaves of a communication protocol to its root across rounds where parties do not update their defense coins. This result crucially relies on the fact that one party's expected defense coin always remains unchanged in every step of the protocol evolution.

To summarize, the "expected potential of the parameters associated with the leaves" is at least the "potential of the expected parameters at the root." This property of the potential function suffices to demonstrate $1/\sqrt{r}$-insecurity using an inductive argument. This result makes us hopeful that π^+, where parties update their defenses only r times, also behaves similarly and has $1/\sqrt{r}$-insecurity. However, the fact that the heavy querier might simultaneously disclose information about both Alice's and Bob's private coins, prevents the use of this technique to π^+ in the random oracle model.

A Crucial Observation. Suppose Alice and Bob's expected defense coins are a and b, respectively. Assume that the heavy querier adds the transcript t_i with probability p_i.

Conditioned on the transcript t_i, the expected Alice's and Bob's defense coins are a_i and b_i, respectively.

We shall study the expectation of the product of Alice's and Bob's defense coins immediately before and after the sequence of query-answer pairs added by the heavy querier. Just before the heavy querier starts adding queries, the joint distribution of Alice-Bob views is product distribution. So, the expected product of Alice's and Bob's defense coins is $a \cdot b$. After the heavy querier terminates, the joint distribution of Alice and Bob views is product distribution again. So, the expected product of Alice's and Bob's defense coins conditioned on the the heavy querier adding t_i is $a_i \cdot b_i$. Overall, we have the following linearity constraint.

$$a \cdot b = \sum_i p_i \left(a_i \cdot b_i\right).$$

Observe, as a consequence of this constraint, the subtree inside the highlighted rectangle in Figure 3 is impossible to occur in *isolation*. The "complementary pieces" that help complete the product space need to show up elsewhere.

Our Approach. Our starting point is the potential function of Khorasgani, Maji, and Wang [KMW20], and we re-write their potential function as follows.

$$\begin{aligned}\Phi(x,a,b) &= x(1-x) + (x-a)^2 + (x-b)^2 \\ &= x + (x-a-b)^2 - 2ab\end{aligned}$$

Our crucial observation has already concluded that ab is a linear term. Furthermore, the term x represents the expected output of the protocol conditioned on the partial transcript, which is also a linear term. The term $(x-a-b)^2$ remains convex for x, a, and b.

Suppose before the heavy querier started, the expected output is x, the expected Alice defense is a, and the expected Bob defense is b. Furthermore, conditioning on the heavy querier generating the transcript t_i, the expected output is x_i, the expected Alice defense is a_i, and the expected Bob defense is b_i. Recall that immediately before and after the heavy querier execution, the joint distribution of Alice's and Bob's views is product distribution. Figure 2 pictorially elaborates on how to lift the potential of the leaves to the potential of the root.

Intuitively, at the root, the joint view of Alice and Bob is a product space. Conditioning on the sequence of query-answer pairs added by the heavy querier decomposes the view into small *combinatorial rectangles*. Under this new interpretation of the potential function $\Phi(x,a,b)$, Jensen's inequality helps us prove that the "average potential at individual leaves" is at least the "potential of the average parameters at the root." This observation suffices to translate the inductive argument of Khorasgani, Maji, Wang [KMW20] and apply it to π^+ in the random oracle model. Section 4 provides the full proof of our technical result. So, our technical result identifies a fail-stop adversarial strategy that demonstrates $1/\sqrt{r}$-insecurity, where r represents the number of times the parties update their defense coins. This argument completes the overview of our technical approach.

Discussion. Next, we present additional remarks positioning our technical approach relative to previous works, and highlighting how our techniques may help prove new separation results as well.

▶ Remark 2. There is no need for the existence of a communication protocol that realizes the decomposition into smaller combinatorial rectangles. For example, the decomposition in Figure 2 is inspired by the Kushilevitz function [KN], which has no communication protocol realizing the smaller combinatorial rectangles. We believe that this general property should facilitate demonstrating new black-box separations from cryptographic primitives

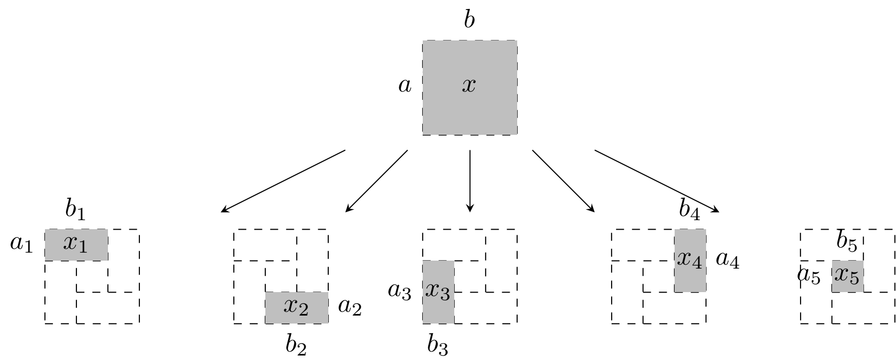

Figure 2 An pictorial summary of our potential argument in the random oracle model. The shaded regions denote the pairs of consistent Alice and Bob views. We denote the expectation of $\{a_1, \ldots a_5\}$ by a. Similarly, we define b as the expectation of $\{b_1, \ldots b_5\}$. Next, we define x is the expectation of $\{x_1, \ldots x_5\}$. The potential at root is $\Phi(x, a, b)$. The potential at the leaves are $\Phi(x_1, a_1, b_1)$, $\Phi(x_2, a_2, b_2)$, $\Phi(x_3, a_2, b_2)$, $\Phi(x_4, a_4, b_4)$, and $\Phi(x_5, a_5, b_5)$. The "expected potential of the parameters associated with the leaves" is at least the "potential of the expected parameters at the root" using the property of the potential function $\Phi(\cdot, \cdot, \cdot)$.

(even with private inputs) whose input-output behavior decomposes into monochromatic combinatorial rectangles (for example, the existence of semi-honest secure protocols for two-party deterministic functionalities that are *not decomposable* and do not have any OR-minor [Kus89, Bea89, MPR09]).

▶ Remark 3. Our analysis, in a significant divergence from existing approaches, considers the entire list of query-answers added by the heavy querier in π^+ immediately after a party sends a message as a *single instance of information exposure*. Even the technical approach of [KMW20] considers the rounds where no party updates their respective defense coins in an iterative manner (not as a single instance of information exposure).

Consequently, our proof translates into an alternate (and a more direct) proof for the result in [KMW20].

▶ Remark 4. Note that we are *not* ruling out the possibility of cases like Figure 3 occurring during the evolution of the heavy querier execution. We are merely stating that, overall, the (average) potential function increases from the leaves to the root, if the joint Alice-Bob views are (close to) product distribution immediately before and after the heavy querier adds all her query-answers. For example, this global argument automatically compensates adequately for any local harm to the potential caused by the subtree inside the rectangle of Figure 3 so that a local surplus somewhere else in the potential counterbalances this local deficit.

Note that previous works attempt to avoid the cases arising in Figure 3 (by ruling out intersection queries of parties with future queries that may influence the output). Our potential-based approach overcomes this challenge. Jensen's inequality typically is a local argument. However, the addition of the constraint that the product of expected Alice-Bob defense coins is conserved, introduces a global constraint sufficient to salvage the potential-based approach.

We want to highlight a subtlety at this point. The existence of views that occur as the internal nodes in Figure 3 do *not* imply the existence of key-agreement. Because, there exist public query-answers that make the joint distribution of Alice-Bob private views a product distribution.

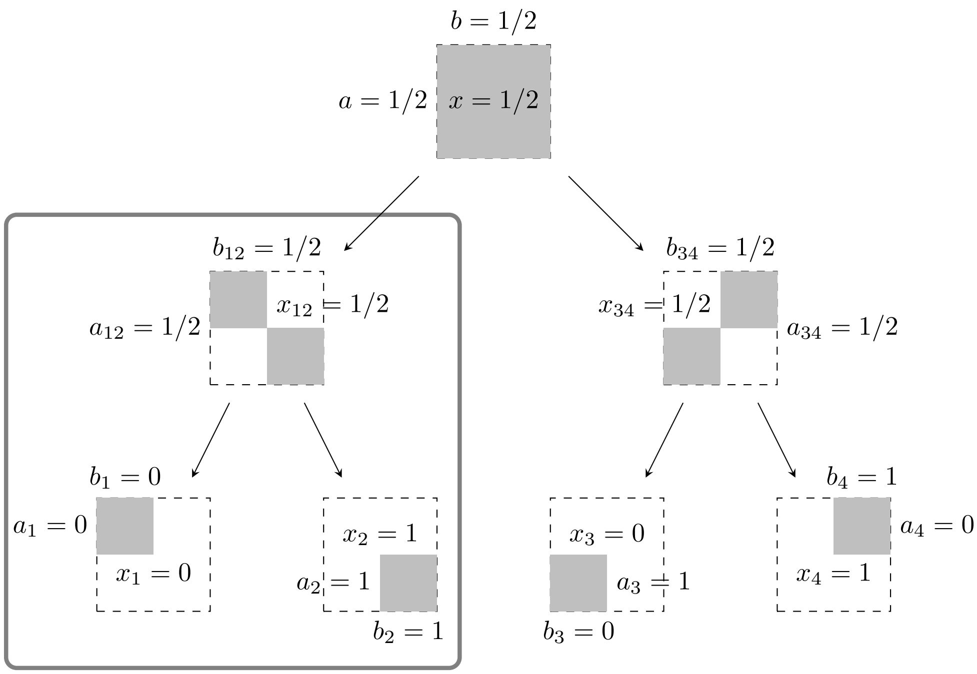

Figure 3 In certain situations, the potential $\Phi(\cdot,\cdot,\cdot)$ falls apart locally when x, a, and b change simultaneously. The shaded regions denote the pairs of consistent Alice and Bob views. We represent a_{12} as the average of a_1 and a_2, a_{34} as the average of a_3 and a_4, and a is the average of a_{12} and a_{34}. Similarly, b_{12} is the average of b_1 and b_2, b_{34} is the average of b_3 and b_4, and b is the average of b_{12} and b_{34}. Finally, x_{12} is the average of x_1 and x_2, x_{34} is the average of x_3 and x_4, and x is the average of x_{12} and x_{34}. Note that $\Phi(x, a, b) = 1/4$. At the leaves, we have $\Phi(x_1, a_1, b_1) = \Phi(x_2, a_2, b_2) = 0$, and $\Phi(x_3, a_3, b_3) = \Phi(x_4, a_4, b_4) = 1$. So, globally, the expected potential at the leaves is $1/2$ and is greater than the potential at the root, which is $1/4$. Now, focus into the local subtree inside the rectangle. The expected potential of the leaves inside the rectangle is 0, and the potential at their parent is $1/4$. Therefore, locally, the potential of the parent is *not* less than the expected potential of the leaves.

▶ Remark 5. It is not evident whether our attack "compiles away" the random oracle similar to the simulation lemma in [DLMM11]. Simulating the entire sequence of query-answer sequence added by the heavy querier may not be simulatable in the information-theoretic plain model. A primary source of difficulty lies in simulating the answers of queries that are intersection queries without actually revealing whether they are intersection queries or not. Therefore, similar to [MMP14a, MMP14b, DMM14] our result does not seem to compile away the random oracle.

To conclude this discussion, we emphasize that the technical overview enjoys the luxury of hindsight that the potential argument of [KMW20] applies to this setting. The identification of the actual invariant that ensures the counterbalances to the local harm caused to the potential by instances like Figure 3 was highly nontrivial. It is surprising (miraculous, perhaps) that considering the expected product of Alice's and Bob's defense coins turned out to be the critical invariant. In fact, beyond exploring the analytic properties, it would be interesting to investigate the intuition underlying the rewriting of the potential function as $\Phi(x, a, b) = x + (x - a - b)^2 - 2ab$.

2 Preliminaries

We use uppercase letters for random variables, lowercase letters for values, and calligraphic letters for sets. For a joint distribution (A, B), A and B represent the marginal distribution, and $A \times B$ represents the product distribution where one samples from the marginal distribution A and B independently. For a random variable A distributed over Ω, the *support* of A, denoted by $\mathrm{Supp}(A)$, is the set $\{x | \Pr[A = x] > 0\}$. For two random variables A, B distributed over (a discrete sample space) Ω, their *statistical distance* is defined as $\mathsf{SD}(A, B) := \frac{1}{2} \cdot \sum_{\omega \in \Omega} |\Pr[A = w] - \Pr[B = w]|$.

For a sequence $(X_1, X_2, \ldots)$, we use $X_{\leq i}$ to denote the distribution $(X_1, X_2, \ldots, X_i)$. Let $(M_1, M_2, \ldots, M_r)$ be a joint distribution over sample space $\Omega_1 \times \Omega_2 \times \cdots \times \Omega_r$, such that for any $i \in \{1, 2, \ldots, n\}$, M_i is a random variable over Ω_i. A random variable X_i is said to be $M_{\leq i}$ *measurable* if there exists a deterministic function $f \colon \Omega_1 \times \cdots \times \Omega_i \to \mathbb{R}$ such that $X_i = f(M_1, \ldots, M_i)$. A random variable $\tau \colon \Omega_1 \times \cdots \times \Omega_r \to \{1, 2, \ldots, r\}$ is called a *stopping time*, if random variable $\mathbb{1}_{\tau \leq i}$ is $M_{\leq i}$ measurable, where $\mathbb{1}$ is the indicator function. For a more formal treatment, refer to, for example, [Sch17].

The following inequality shall be helpful for our proof.

▶ **Theorem 1** (Jensen's inequality). *If f is a multivariate convex function, then $\mathrm{E}\left[f\left(\vec{X}\right)\right] \geq f\left(\mathrm{E}\left[\vec{X}\right]\right)$, for all probability distributions $\vec{X}$ over the domain of f.*

2.1 Two-party protocol in the random oracle model

Alice and Bob speak in alternate rounds. We denote the i^{th} message by M_i. For every message M_i, we denote Alice's private view immediately after sending/receiving message M_i as V_i^{A}, which consists of Alice's random tape R^{A}, her private queries, and the first i messages exchanged. We use V_0^{A} to represent Alice's private view before the protocol begins. Similarly, we define Bob's private view V_i^{B} and use R^{B} to denote his private random tape.

2.1.0.1 Query Operator $\mathcal{Q}$.

For any view V, we use $\mathcal{Q}(V)$ to denote the set of all queries contained in the view V.

2.2 Heavy Querier and the Augmented Protocol

For two-party protocols in the random oracle model, the heavy querier is a standard algorithm, which was introduced by [IR89, BM09]. In this paper, we shall use the following imported theorem.

▶ **Imported Theorem 1** (Guarantees of Heavy Querier [BM09, MMP14b]). *Let π be any two-party protocol between Alice and Bob in the random oracle model, in which both parties ask at most n queries. For all threshold $\epsilon \in (0, 1)$, there exists a public algorithm, called the heavy querier, who has access to the transcript between Alice and Bob. After receiving each message M_i, heavy querier will perform a set of queries and obtain its corresponding answers from the random oracle. Let H_i denote the sequence of query-answer pairs asked by the heavy querier after receiving message M_i. Let T_i be the union of the i^{th} message M_i and the i^{th} heavy querier message H_i. Heavy querier guarantees the following.*

- ***ϵ-Lightness.*** *For any i, any $t_{\leq i} \in \mathrm{Supp}(T_{\leq i})$, and query $q \notin \mathcal{Q}(h_{\leq i})$,*

$$\Pr\left[q \in \mathcal{Q}\left(V_i^{\mathsf{A}} \middle| T_{\leq i} = t_{\leq i}\right)\right] \leq \epsilon, \quad \text{and} \quad \Pr\left[q \in \mathcal{Q}\left(V_i^{\mathsf{B}} \middle| T_{\leq i} = t_{\leq i}\right)\right] \leq \epsilon.$$

- $n\epsilon$***-Dependence.*** *Fix any* i,

$$\mathop{\mathrm{E}}_{t_{\leq i} \leftarrow T_{\leq i}} \left[\mathsf{SD}\left(\left(V_i^{\mathsf{A}}, V_i^{\mathsf{B}} \middle| T_{\leq i} = t_{\leq i}\right), \left(V_i^{\mathsf{A}} \middle| T_{\leq i} = t_{\leq i}\right) \times \left(V_i^{\mathsf{B}} \middle| T_{\leq i} = t_{\leq i}\right)\right)\right] \leq n\epsilon.$$

  Intuitively, it states that on average*, the statistical distance between (1) the joint distribution of Alice's and Bob's private view, and (2) the product of the marginal distributions of Alice's private views and Bob's private views is small.*
- $\mathcal{O}(n/\epsilon)$***-Efficiency.*** *The expected number of queries asked by Eve is bounded by* $\mathcal{O}(n/\epsilon)$*. Moreover, it asks at most* $\mathcal{O}\left(n/\epsilon^2\right)$ *with probability (at least)* $(1-\epsilon)$ *by an averaging argument.*

We call the protocol with heavy querier's message attached, the augmented protocol. We call T_i the augmented message.

2.3 Coin-Tossing Protocol

We will prove our main result by induction on the message complexity of the protocol. Therefore, after any partial transcript $t_{\leq i}$, we will treat the remaining protocol starting from the $(i+1)^{th}$ message, as a protocol of its own. Hence, it is helpful to define the coin-tossing protocol where, before the beginning of the protocol, Alice's and Bob's private views are already correlated with the random oracle. However, note that, in the augmented protocol, after each augmented message t_i, the heavy querier has just ended. Thus, these correlations will satisfy Imported Theorem 1. Therefore, we need to define a general class of coin-tossing protocols in the random oracle model over which we shall perform our induction.

▶ **Definition 1** ($(\epsilon, \vec{\alpha}, r, n, X_0)$-Coin-Tossing)**.** An interactive protocol π between Alice and Bob with random oracle $O : \{0,1\}^\lambda \to \{0,1\}^\lambda$ is called an $(\epsilon, \vec{\alpha}, r, n, X_0)$-*coin-tossing protocol* if it satisfies the following.

- **Setup.** There is an arbitrary set $\mathcal{S} \subseteq \{0,1\}^\lambda$, which is publicly known, such that for all queries $s \in \mathcal{S}$, the query answers $O(s)$ are also publicly known. Let Ω^{A}, Ω^{B}, and Ω^{O} be the universes of Alice's random tape, Bob's random tape, and the random oracle, respectively. There are also publicly know sets $\mathcal{A} \subseteq \Omega^{\mathsf{A}} \times \Omega^{\mathsf{O}}$ and $\mathcal{B} \subseteq \Omega^{\mathsf{B}} \times \Omega^{\mathsf{O}}$. The random variables R^{A}, R^{B}, and O are sampled uniformly conditioned on that (1) $(R^{\mathsf{A}}, O) \in \mathcal{A}$, (2) $(R^{\mathsf{B}}, O) \in \mathcal{B}$, and (3) O is consistent with the publicly known answers at $\mathcal{S}$. Alice's (resp., Bob's) private view before the beginning of the protocol is a deterministic function of R^{A} (resp., R^{B}) and O, which might contain private queries.[12]
- **Agreement.** At the end of the protocol, both parties always agree on the output $\in \{0,1\}$. Without loss of generality, we assume the output is concatenated to the last message in the protocol.[13]
- **Defense preparation.** At message M_i, if Alice is supposed to speak, in addition to preparing the message M_i, she will also prepare a defense coin for herself as well. If Bob decides to abort the next message, she shall *not* make any additional queries to the random oracle, and simply output the defense she has just prepared. [DLMM11, DMM14]

[12] Basically, $\mathcal{S}$ is the set of all the queries that the heavy querier has published. $\mathcal{A}$ (resp., $\mathcal{B}$)is the set of all possible r^{A} (resp., r^{B}) and o pairs that are consistent with Alice's (resp., Bob's) messages before this protocol begins.

[13] This generalization shall not make the protocol any more vulnerable. Any attack in this protocol shall also exist in the original protocol with the same amount of deviation. This only helps simplify the presentation of our proof.

introduced this constraint as the "instant construction." They showed that, without loss of generality, one can assume this property for all the defense preparations except for the first defense (see Remark 7). We shall refer to this defense both as Alice's i^{th} defense and also as her $(i+1)^{th}$ defense. Consequently, Alice's defense for every i is well-defined. Bob's defense is defined similarly. We assume the party who receives the first message has already prepared her defense for the first message before the protocol begins.

- **ϵ-Lightness at Start.** For any query $q \notin \mathcal{S}$, the probability that Alice (resp., Bob) has asked query q before the protocol begins is upper bounded by $\epsilon \in [0, 1]$.
- **$\vec{\alpha}$-Dependence.** For all $i \in \{0, 1, \ldots, r\}$, Alice's and Bob's private view after message T_i are α_i-dependent on average . That is, the following condition is satisfied for every i.

$$\alpha_i := \mathop{\mathrm{E}}_{t_{\leq i} \leftarrow T_{\leq i}} \left[\mathsf{SD}\left(\left(V_i^{\mathsf{A}}, V_i^{\mathsf{B}} \middle| T_{\leq i} = t_{\leq i}\right), \left(V_i^{\mathsf{A}} \middle| T_{\leq i} = t_{\leq i}\right) \times \left(V_i^{\mathsf{B}} \middle| T_{\leq i} = t_{\leq i}\right)\right)\right]$$

- **r-Message complexity.** The number of messages of this protocol is $r = \mathsf{poly}(\lambda)$. We emphasize that the length of the message could be arbitrarily long.
- **n-Query complexity.** For all possible complete executions of the protocol, the number of queries that Alice (resp., Bob) asks (including the queries asked before the protocol begins) is at most $n = \mathsf{poly}(\lambda)$. This also includes the queries that are asked for the preparation of the defense coins.
- **X_0-Color.** The expectation of the output, referred to as the color, is $X_0 \in (0, 1)$.

▶ Remark 6. Let us justify the necessity of $\vec{\alpha}$-dependence in the definition. We note that when heavy querier stops, Alice's and Bob's view are not necessarily close to the product of their respective marginal distributions.[14] However, to prove any meaningful bound on the susceptibility of this protocol, we have to treat $\vec{\alpha}$ as an additional error term. Therefore, we introduce this parameter in our definition. However, the introduction of this error shall not be a concern globally, because the heavy querier guarantees that over all possible executions this dependence is at most $n\epsilon$ (on average), which we shall ensure to be sufficiently small.

▶ Remark 7. We note that, after every heavy querier message, the remaining sub-protocol always satisfies the definition above. However, the original coin-tossing protocol might not meet these constraints. For example, consider a one-message protocol where Alice queries $O(0^\lambda)$, and sends the parity of this string to Bob as the output. On the other hand, Bob also queries $O(0^\lambda)$ and uses the parity of this string as his defense. This protocol is perfectly secure in the sense that no party can deviate the output of the protocol at all. However, the query 0^λ is 1-heavy in Bob's private view even before the protocol begins. Prior works [DLMM11, DMM14] rule out such protocols by banning Bob from making any queries when he prepares his first defense. In this paper, we consider protocols such that no queries are more than ϵ-heavy when Bob prepares his first defense. We call this the *ϵ-lightness at start assumption*. The set of protocols that prior works consider is exactly the set of protocols that satisfies 0-lightness at start assumption.

To justify our ϵ-lightness at start assumption, we stress that one could always run a heavy querier with a threshold ϵ before the beginning of the protocol as a pre-processing step. Note that this fixes only a small part (of size n/ϵ) of the random oracle, and, hence, the random

[14] For instance, suppose Alice samples a uniform string $u_1 \xleftarrow{\$} \{0,1\}^\lambda$ and sends $O(u_1)$ to Bob. Next, Bob samples a uniform string $u_2 \xleftarrow{\$} \{0,1\}^\lambda$ and sends $O(u_2)$ to Alice. Assume the first message and the second message are the same, i.e., $O(u_1) = O(u_2)$. Then, there are no heavy queries, but Alice's and Bob's private are largely correlated.

oracle is still an "idealized" one-way function. If this protocol is a black-box construction of a coin-tossing protocol with any one-way function, the choice of the one-way function should not change its color. Therefore, by running a heavy querier before the beginning of the protocol, it should not alter the color of the protocol. And now all queries are ϵ-light in Bob's view before the protocol begins. Hence our proof will follow.

2.3.0.1 Notation.

Let X_i represent the expected output conditioned on the first i augmented messages, i.e., $T_{\leq i}$. Let D_i^{A} (resp., D_i^{B}) be the expectation of Alice's (resp., Bob's) i^{th} defense conditioned on the first i augmented messages.[15] Note that the variables $X_i, D_i^{\mathsf{A}}, D_i^{\mathsf{B}}$ are $T_{\leq i}$ measurable.

3 Our Results

Given an $(\epsilon, \vec{\alpha}, r, n, X_0)$-coin-tossing protocol π and a stopping time τ, we define the following score function that captures the susceptibility of this protocol with respect to this particular stopping time.

▶ **Definition 2.** Let π be an $(\epsilon, \vec{\alpha}, r, n, X_0)$-coin tossing protocol. Let $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ be the party who sends the last message of the protocol. For any stopping time τ, define

$$\mathsf{Score}(\pi, \tau) := \mathrm{E}\left[\mathbb{1}_{(\tau \neq r) \vee (\mathsf{P} \neq \mathsf{A})} \cdot \left|X_\tau - D_\tau^{\mathsf{A}}\right| + \mathbb{1}_{(\tau \neq r) \vee (\mathsf{P} \neq \mathsf{B})} \cdot \left|X_\tau - D_\tau^{\mathsf{B}}\right|\right].$$

We clarify that the binary operator $\vee$ in the expression above represents the boolean OR operation.

To provide additional perspectives to this definition, we make the following remarks similar to [KMW20].

1. Suppose Alice is about to send (m_i^*, h_i^*) as the i^{th} message. In the information-theoretic plain model, prior works [CI93, KMM19] consider the gap between the expected output before and after this message. Intuitively, since Alice is sending this message, she could utilize this gap to attack Bob, because Bob's defense can not keep abreast of this new information. However, in the random oracle model, both parties are potentially vulnerable to this gap. This is due to the fact that the heavy querier message might also reveal information about Bob. For instance, it might reveal Bob's commitments sent in previous messages. Then, Alice's defense cannot keep abreast of this new information either and thus Alice is potentially vulnerable.
2. Due to the reasons above, for every message, we consider the potential deviations that *both* parties can cause by aborting appropriately. Suppose we are at transcript $T_{\leq i} = t^*_{\leq i}$, which belongs to the stopping time, i.e., $\tau = i$. And Alice sends the last message (m_i^*, h_i^*). Naturally, Alice can abort without sending this message to Bob when she finds out her i^{th} message is (m_i^*, h_i^*). This attack causes a deviation of $\left|X_\tau - D_\tau^{\mathsf{B}}\right|$. On the other hand, Bob can also attack by aborting when he receives Alice's message (m_i^*, h_i^*). This attack ensures a deviation of $\left|X_\tau - D_{\tau+1}^{\mathsf{A}}\right|$. Note that for the $(i+1)^{th}$ message, Alice is not supposed to speak, her $(i+1)^{th}$ defense is exactly her i^{th} defense. Hence this deviation can be also written as $\left|X_\tau - D_\tau^{\mathsf{A}}\right|$.

[15] Recall that in the Definition 1, Alice's i^{th} defense is defined for all $i \in \{1, 2, \ldots, r\}$.

3. The above argument has a boundary case, which is the last message of the protocol. Suppose Alice sends the last message. Then, Bob, who receives this message, cannot abort anymore because the protocol has ended. Therefore, if our stopping time $\tau = n$, the score function must exclude $\left|X_\tau - D_\tau^{\mathsf{A}}\right|$. This explains why we have the indicator function $\mathbb{1}$ in our score function.
4. Lastly, we illustrate how one can translate this score function into a fail-stop attack strategy. Suppose we find a stopping time τ^* that witnesses a large score $\mathsf{Score}(\pi, \tau^*)$. For Alice, we will partition the stopping time into two partitions depending on whether $X_\tau \geq D_\tau^{\mathsf{B}}$ or not. Similarly, for Bob, we partition the stopping time into two partitions depending on whether $X_\tau \geq D_\tau^{\mathsf{A}}$. These four attack strategies correspond to Alice or Bob deviating towards 0 or 1. And the summation of the deviations caused by these four attacks are exactly $\mathsf{Score}(\pi, \tau^*)$. Hence there must exist a fail-stop attack strategy with deviation $\geq \frac{1}{4} \cdot \mathsf{Score}(\pi, \tau^*)$.

Given the definition of our score function, we are interested in finding the stopping time that witnesses the largest score. This motivates the following definition.

▶ **Definition 3.** For any $(\epsilon, \vec{\alpha}, r, n, X_0)$-coin-tossing protocol π, define

$$\mathsf{Opt}(\pi) := \max_{\tau} \ \mathsf{Score}(\pi, \tau).$$

Intuitively, $\mathsf{Opt}(\pi)$ represents the susceptibility of the protocol π. And our main theorem states the following.

▶ **Theorem 2** (Main Technical Result in the Random Oracle Model)**.** *For any $(\epsilon, \vec{\alpha}, r, n, X_0)$-coin-tossing protocol π, the following holds.*

$$\mathsf{Opt}(\pi) \geq \Gamma_r \cdot X_0\left(1 - X_0\right) - \left(nr \cdot \epsilon + \alpha_0 + 2\sum_{i=1}^{r} \alpha_i\right),$$

where $\Gamma_r := \sqrt{\frac{\sqrt{2}-1}{r}}$ for all $r \in \mathbb{N}^*$.

We defer the proof to Section 4. In light of the remarks above, this theorem implies the following corollary.

▶ **Corollary 2.** *Let π be a coin-tossing protocol in the random oracle model that satisfies the ϵ-lightness at start assumption.*[16] *Suppose π is an r-message protocol, and Alice and Bob ask at most n queries. The expected output of π is X_0. Then, either Alice or Bob has a fail-stop attack strategy that deviates the output by*

$$\Omega\left(\frac{X_0\left(1 - X_0\right)}{\sqrt{r}}\right).$$

In expectation, this attack strategy asks $\mathcal{O}\left(\frac{n^2r^2}{X_0(1-X_0)}\right)$ queries.

This corollary is obtained by simply setting $\epsilon = \frac{X_0(1-X_0)}{nr^2}$ in Theorem 2. Imported Theorem 1 guarantees that, for all i, the average dependences after the i^{th} message are bounded by $n\epsilon$. Hence, the error term is $\mathrm{o}\left(\frac{X_0(1-X_0)}{\sqrt{r}}\right)$.

---

[16] See Remark 7.

The efficiency of the heavy querier is guaranteed by Imported Theorem 1. One can transform the average-case efficiency to worst-case efficiency by forcing the heavy querier to stop when it asks more than $\frac{n^2r^3}{(X_0(1-X_0))^2}$ queries. By Markov's inequality, this happens with probability at most $\mathcal{O}\left(\frac{X_0(1-X_0)}{r}\right) = \mathrm{o}\left(\frac{X_0(1-X_0)}{\sqrt{r}}\right)$, and thus the quality of this attack is essentially identical to the averge-case attack.

4 Proof of Theorem 2

In this section, we prove Theorem 2 using induction on message complexity r. We first provide some useful lemmas in Section 4.1. Next, we prove the base case in Section 4.2. Finally, Section 4.3 proves the inductive step.

Throughout this section, without loss of generality, we shall assume that Alice sends the first message in the protocol.

4.1 Useful Technical Lemmas

Firstly, it is implicit in [BM09] that if (1) Alice's and Bob's private view before the protocol begins are α_0-dependent, (2) all the queries are ϵ-light for Bob, and (3) Alice asks at most n queries to prepare her first message, then after the first message, Alice's and Bob's private view are $(\alpha_0 + n\epsilon)$-dependent.

▶ **Lemma 1** (Technical Lemma [BM09]). *We have*

$$\mathsf{SD}\left(\left(V_1^{\mathsf{A}}, V_0^{\mathsf{B}}\right), \left(V_1^{\mathsf{A}} \times V_0^{\mathsf{B}}\right)\right) \leq \alpha_0 + n\epsilon.$$

In addition, the following inequality from [KMW20] shall be useful for our proof.

▶ **Lemma 2** (Technical Lemma, Lemma 1 in [KMW20]). *For all $P \in [0,1]$ and $Q \in [0,1/2]$, if P, Q satisfies*

$$Q \leq \frac{P}{1+P^2},$$

then for all $x, \alpha, \beta \in [0,1]$, we have

$$\max\left(P \cdot x(1-x)\ ,\ |x-\alpha| + |x-\beta|\right) \geq Q \cdot \left(x(1-x) + (x-\alpha)^2 + (x-\beta)^2\right).$$

In particular, for all $r \geq 1$, the constraints are satisfied if we set $P = \Gamma_r$ and $Q = \Gamma_{r+1}$, where $\Gamma_r := \sqrt{\frac{\sqrt{2}-1}{r}}$.

4.2 Base case: $r = 1$

Let π be an $(\epsilon, \vec{\alpha}, r, n, X_0)$-coin-tossing protocol with $r = 1$. In this protocol, Alice sends the only message M_1. We shall pick the stopping time τ to be 1. Note that this is the last message of the protocol and hence Bob who receives it cannot abort any more. Therefore, our score function is the following

$$\mathsf{Score}(\pi, \tau) = \mathrm{E}\left[\left|X_1 - D_1^{\mathsf{B}}\right|\right].$$

Let $D_0^{\mathsf{B}} = \mathrm{E}\left[D_1^{\mathsf{B}}\right]$, which is the expectation of Bob's first defense before the protocol begins. Recall that in the augmented protocol $T_1 = (M_1, H_1)$, and X_1 and D_1^{B} are T_1 measurable.

We have

$$\begin{aligned}
\mathrm{E}\left[\left|X_1 - D_1^{\mathsf{B}}\right|\right] &= \mathop{\mathrm{E}}_{m_1 \leftarrow M_1}\left[\mathop{\mathrm{E}}_{h_1 \leftarrow (H_1|M_1=m_1)}\left[\left|X_1 - D_1^{\mathsf{B}}\right|\right]\right]\\
&\overset{\text{(i)}}{\geq} \mathop{\mathrm{E}}_{m_1 \leftarrow M_1}\left[\left|\mathrm{E}[X_1|M_1=m_1] - \mathrm{E}\left[D_1^{\mathsf{B}}|M_1=m_1\right]\right|\right]\\
&\overset{\text{(ii)}}{\geq} \mathop{\mathrm{E}}_{m_1 \leftarrow M_1}\left[\left|\mathrm{E}[X_1|M_1=m_1] - D_0^{\mathsf{B}}\right| - \left|D_0^{\mathsf{B}} - \mathrm{E}\left[D_1^{\mathsf{B}}|M_1=m_1\right]\right|\right]\\
&\overset{\text{(iii)}}{\geq} \mathop{\mathrm{E}}_{m_1 \leftarrow M_1}\left[\left|\mathrm{E}[X_1|M_1=m_1] - D_0^{\mathsf{B}}\right|\right] - \alpha_0 - n\epsilon\\
&\overset{\text{(iv)}}{\geq} X_0 \cdot \left(1 - D_0^{\mathsf{B}}\right) + (1 - X_0) \cdot D_0^{\mathsf{B}} - \alpha_0 - n\epsilon\\
&\geq X_0\left(1 - X_0\right) + \left(X_0 - D_0^{\mathsf{B}}\right)^2 - \alpha_0 - n\epsilon\\
&\geq X_0\left(1 - X_0\right) - \alpha_0 - n\epsilon.
\end{aligned}$$

In the above inequality, (i) and (ii) are because of triangle inequality. Since we assume the output is concatenated to the last message of the protocol, $\mathrm{E}[X_1|M_1 = m_1] \in \{0, 1\}$. And by the definition of X_0, the probability of the output being 1 is X_0. Hence we have (iv).

To see (iii), note that

$$\begin{aligned}
\mathrm{E}\left[D_1^{\mathsf{B}}|M_1=m_1\right] &= \sum_{v_1^{\mathsf{A}}, v_0^{\mathsf{B}}} \Pr\left[V_1^{\mathsf{A}} = v_1^{\mathsf{A}}, V_0^{\mathsf{B}} = v_0^{\mathsf{B}}|M_1 = m_1\right]\mathrm{E}\left[D_1^{\mathsf{B}}|V_0^{\mathsf{B}} = v_0^{\mathsf{B}}\right]\\
&\leq \sum_{\mathcal{Q}(v_1^{\mathsf{A}}) \cap \mathcal{Q}(v_0^{\mathsf{B}}) = \emptyset} \Pr\left[V_1^{\mathsf{A}} = v_1^{\mathsf{A}}|M_1 = m_1\right] \cdot \Pr\left[V_0^{\mathsf{B}} = v_0^{\mathsf{B}}\right]\mathrm{E}\left[D_1^{\mathsf{B}}|V_0^{\mathsf{B}} = v_0^{\mathsf{B}}\right]\\
&\quad + \sum_{\mathcal{Q}(v_1^{\mathsf{A}}) \cap \mathcal{Q}(v_0^{\mathsf{B}}) \neq \emptyset} \Pr\left[V_1^{\mathsf{A}} = v_1^{\mathsf{A}}, V_0^{\mathsf{B}} = v_0^{\mathsf{B}}|M_1 = m_1\right]\mathrm{E}\left[D_1^{\mathsf{B}}|V_0^{\mathsf{B}} = v_0^{\mathsf{B}}\right]
\end{aligned}$$

Hence,

$$\left|\mathrm{E}\left[D_1^{\mathsf{B}}|M_1=m_1\right] - D_0^{\mathsf{B}}\right| \leq \Pr_{(v_1^{\mathsf{A}}, v_0^{\mathsf{B}}) \leftarrow (V_1^{\mathsf{A}}, V_0^{\mathsf{B}})|M_1=m_1}\left[\mathcal{Q}\left(v_1^{\mathsf{A}}\right) \cap \mathcal{Q}\left(v_0^{\mathsf{B}}\right) \neq \emptyset\right].$$

Therefore,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{m_1 \leftarrow M_1}\left[\left|\mathrm{E}\left[D_1^{\mathsf{B}}|M_1=m_1\right] - D_0^{\mathsf{B}}\right|\right]\\
&\leq \mathop{\mathrm{E}}_{m_1 \leftarrow M_1}\left[\Pr_{(v_1^{\mathsf{A}}, v_0^{\mathsf{B}}) \leftarrow (V_1^{\mathsf{A}}, V_0^{\mathsf{B}})|M_1=m_1}\left[\mathcal{Q}\left(v_1^{\mathsf{A}}\right) \cap \mathcal{Q}\left(v_0^{\mathsf{B}}\right) \neq \emptyset\right]\right]\\
&\leq \Pr_{(v_1^{\mathsf{A}}, v_0^{\mathsf{B}}) \leftarrow (V_1^{\mathsf{A}}, V_0^{\mathsf{B}})}\left[\mathcal{Q}\left(v_1^{\mathsf{A}}\right) \cap \mathcal{Q}\left(v_0^{\mathsf{B}}\right) \neq \emptyset\right] \leq \alpha_0 + n\epsilon.
\end{aligned}$$

This completes the proof for the base case.

4.3 Inductive Step

Suppose the theorem is true for $r = r_0 - 1$, we are going to prove it for $r = r_0$. Let π be an arbitrary $(\epsilon, \vec{\alpha}, r_0, n, X_0)$-coin-tossing protocol. Assume the first augmented message is $(M_1, H_1) = (m_1^*, h_1^*)$, and conditioned on that, $X_1 = x_1^*$, $D_1^{\mathsf{A}} = d_1^{\mathsf{A},*}$, and $D_1^{\mathsf{B}} = d_1^{\mathsf{B},*}$. Moreover, the remaining sub-protocol π^* is an $(\epsilon, \vec{\alpha}^*, r_0 - 1, n, x_1^*)$-coin-tossing protocol. By our induction hypothesis,

$$\mathsf{Opt}\left(\pi^*\right) \geq \Gamma_{r_0-1} \cdot x_1^*\left(1 - x_1^*\right) - \left(n(r_0 - 1)\epsilon + \alpha_0^* + \sum_{i=1}^{r_0-1} \alpha_i^*\right).$$

(For simplicity, we shall use $\mathsf{Err}\left(\vec{\alpha}, n, r\right)$ to represent $\alpha_0 + \sum_{i=1}^{r} \alpha_i + nr\epsilon$ in the rest of the proof.) That is, there exists a stopping time τ^* for sub-protocol π^*, whose score is lower bounded by the quantity above. On the other hand, we may choose not to continue by picking this message $(M_1, H_1) = (m_1^*, h_1^*)$ as our stopping time. This would yield a score of

$$\left|x_1^* - d_1^{\mathsf{A},*}\right| + \left|x_1^* - d_1^{\mathsf{B},*}\right|.$$

Hence, the optimal stopping time would decide on whether to abort now or defer the attack to sub-protocol π^* by comparing which one of those two quantities is larger. This would yield a score of

$$\begin{aligned} &\max\left(\mathsf{Opt}\left(\pi^*\right)\ ,\ \left|x_1^* - d_1^{\mathsf{A},*}\right| + \left|x_1^* - d_1^{\mathsf{B},*}\right|\right) \\ \geq\ &\max\left(\Gamma_{r_0-1} \cdot x_1^*\left(1 - x_1^*\right)\ ,\ \left|x_1^* - d_1^{\mathsf{A},*}\right| + \left|x_1^* - d_1^{\mathsf{B},*}\right|\right) - \mathsf{Err}\left(\vec{\alpha}^*, n, r_0 - 1\right) \\ \overset{\text{(i)}}{\geq} &\Gamma_{r_0}\left(x_1^*\left(1 - x_1^*\right) + \left(x_1^* - d_1^{\mathsf{A},*}\right)^2 + \left(x_1^* - d_1^{\mathsf{B},*}\right)^2\right) - \mathsf{Err}\left(\vec{\alpha}^*, n, r_0 - 1\right), \end{aligned}$$

where inequality (i) is because of Lemma 2. Now that we have a lower bound on how much score we can yield at every first augmented message, we are interested in how much do they sum up to.

Without loss of generality, assume there are totally ℓ possible first augmented messages, namely $t_1^{(1)}, t_1^{(2)}, \ldots, t_1^{(\ell)}$. The probability of the first message being $t_1^{(i)}$ is $p^{(i)}$ and conditioned that, $X_1 = x_1^{(i)}$, $D_1^{\mathsf{A}} = d_1^{\mathsf{A},(i)}$, and $D_1^{\mathsf{B}} = d_1^{\mathsf{B},(i)}$. Moreover, the remaining $r_0 - 1$ protocol has dependence vector $\vec{\alpha}^{(i)}$. Therefore, we are interested in,

$$\sum_{i=1}^{\ell} p^{(i)}\left(\Gamma_{r_0}\left(x_1^{(i)}\left(1 - x_1^{(i)}\right) + \left(x_1^{(i)} - d_1^{\mathsf{A},(i)}\right)^2 + \left(x_1^{(i)} - d_1^{\mathsf{B},(i)}\right)^2\right) - \mathsf{Err}\left(\vec{\alpha}^{(i)}, n, r_0 - 1\right)\right)$$

Define the tri-variate function Φ as

$$\Phi(x, y, z) := x(1 - x) + (x - y)^2 + (x - z)^2.$$

We make the crucial observation that this function can also be rewritten as

$$\Phi(x, y, z) = x + (x - y - z)^2 - 2yz.$$

Therefore, we can rewrite the above quantity as

$$\sum_{i=1}^{\ell} p^{(i)}\left(\Gamma_{r_0}\left(x_1^{(i)} + \left(x_1^{(i)} - d_1^{\mathsf{A},(i)} - d_1^{\mathsf{B},(i)}\right)^2 + d_1^{\mathsf{A},(i)} \cdot d_1^{\mathsf{B},(i)}\right) - \mathsf{Err}\left(\vec{\alpha}^{(i)}, n, r_0 - 1\right)\right)$$

We observe the following

1. For the x term, we observe that the expectation of $x_1^{(i)}$ is X_0, i.e., we have $\sum_{i=1}^{\ell} p^{(i)} \cdot x_1^{(i)} = X_0$.
2. For the $(x - y - z)^2$ term, we note that it is a convex tri-variate function. Hence, Jensen's inequality is applicable.
3. For the $y \cdot z$ term, we have the following claim.

▶ **Claim 1.** $\left|\sum_{i=1}^{\ell} p^{(i)} \cdot d_1^{\mathsf{A},(i)} \cdot d_1^{\mathsf{B},(i)} - \mathrm{E}\left[D_1^{\mathsf{A}}\right]\mathrm{E}\left[D_1^{\mathsf{B}}\right]\right| \leq (\alpha_0 + n\epsilon) + \alpha_1.$

Proof. To see this, consider the expectation of the product of Alice and Bob defense when we sample from $\left(V_1^{\mathsf{A}}, V_0^{\mathsf{B}}\right)$. This expectation is $\alpha_0 + n\epsilon$ close to $\mathrm{E}\left[D_1^{\mathsf{A}}\right]\mathrm{E}\left[D_1^{\mathsf{B}}\right]$ because joint distribution $\left(V_1^{\mathsf{A}}, V_0^{\mathsf{B}}\right)$ is $\alpha_0 + n\epsilon$ close to the product of its marginal distribution by Lemma 1.

On the other hand, this expectation is identical to the average (over all possible messages) of the expectation of the product of Alice and Bob defense when we sample from $\left(V_1^{\mathsf{A}}, V_0^{\mathsf{B}} \middle| T_1 = t_1^{(i)}\right)$. Conditioned on first message being $t_1^{(i)}$, this expectation is $\alpha_0^{(i)}$-close to $d_1^{\mathsf{A},(i)} \cdot d_1^{\mathsf{B},(i)}$ because $\left(V_1^{\mathsf{A}}, V_0^{\mathsf{B}} \middle| T_1 = t_1^{(i)}\right)$ has $\alpha_0^{(i)}$-dependence by definition.

Finally, we note that, by definition, $\sum_{i=1}^{\ell} p^{(i)}\alpha_0^{(i)} = \alpha_1$. Note that the indices between α and $\alpha^{(i)}$ are shifted by 1. This because of that the dependence after the first message of the original protocol is the average of the dependence before each sub-protocol begins.

This proves that $\sum_{i=1}^{\ell} p^{(i)} \cdot d_1^{\mathsf{A},(i)} d_1^{\mathsf{B},(i)}$ and $\mathrm{E}\left[D_1^{\mathsf{A}}\right]\mathrm{E}\left[D_1^{\mathsf{B}}\right]$ are $(\alpha_0 + n\epsilon) + \alpha_1$ close. ◀

Given these observations, we can push the expectation inside each term, and they imply that our score is lower bounded by

$$\Gamma_{r_0}\Big(X_0 + \left(X_0 - \mathrm{E}\left[D_1^{\mathsf{A}}\right] - \mathrm{E}\left[D_1^{\mathsf{B}}\right]\right)^2 + \mathrm{E}\left[D_1^{\mathsf{A}}\right] \cdot \mathrm{E}\left[D_1^{\mathsf{B}}\right] - (\alpha_0 + \alpha_1 + n\epsilon)\Big) - \sum_{i=1}^{\ell} p^{(i)} \cdot \mathsf{Err}\left(\vec{\alpha}^{(i)}, n, r_0 - 1\right)$$

We note that by definition (again note that the indices of α and $\alpha^{(i)}$ are shifted by 1),

$$(\alpha_0 + \alpha_1 + n\epsilon) + \sum_{i=1}^{\ell} p^{(i)} \cdot \mathsf{Err}\left(\vec{\alpha}^{(i)}, n, r_0 - 1\right) = \mathsf{Err}\left(\vec{\alpha}, n, r_0\right).$$

Therefore, our score is at least

$$\Gamma_{r_0}\left(X_0 + \left(X_0 - \mathrm{E}\left[D_1^{\mathsf{A}}\right] - \mathrm{E}\left[D_1^{\mathsf{B}}\right]\right)^2 + \mathrm{E}\left[D_1^{\mathsf{A}}\right] \cdot \mathrm{E}\left[D_1^{\mathsf{B}}\right]\right) - \mathsf{Err}\left(\vec{\alpha}, n, r_0\right).$$

Switching back to the form of $x(1-x) + (x-y)^2 + (x-z)^2$, we get

$$\begin{aligned}
&\Gamma_{r_0}\left(X_0\left(1 - X_0\right) + \left(X_0 - \mathrm{E}\left[D_1^{\mathsf{A}}\right]\right)^2 + \left(X_0 - \mathrm{E}\left[D_0^{\mathsf{B}}\right]\right)^2\right) - \mathsf{Err}\left(\vec{\alpha}, n, r_0\right) \\
&\geq \Gamma_{r_0} \cdot X_0\left(1 - X_0\right) - \mathsf{Err}\left(\vec{\alpha}, n, r_0\right) \\
&= \Gamma_{r_0} \cdot X_0\left(1 - X_0\right) - \left(n r_0 \epsilon + \alpha_0 + 2\sum_{i=1}^{r_0} \alpha_i\right).
\end{aligned}$$

This completes the proof of the inductive step and hence the proof of Theorem 2.

References

ABMO15 Gilad Asharov, Amos Beimel, Nikolaos Makriyannis, and Eran Omri. Complete characterization of fairness in secure two-party computation of Boolean functions. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015: 12th Theory of Cryptography Conference, Part I*, volume 9014 of *Lecture Notes in Computer Science*, pages 199–228, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-46494-6_10. 3, 5

ALR13 Gilad Asharov, Yehuda Lindell, and Tal Rabin. A full characterization of functions that imply fair coin tossing and ramifications to fairness. In Amit Sahai, editor, *TCC 2013: 10th Theory of Cryptography Conference*, volume 7785 of *Lecture Notes in Computer Science*, pages 243–262, Tokyo, Japan, March 3–6, 2013. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-36594-2_14. 3, 5

AO16 Bar Alon and Eran Omri. Almost-optimally fair multiparty coin-tossing with nearly three-quarters malicious. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 307–335, Beijing, China, October 31 – November 3, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-53641-4_13. 3, 5

Ash14 Gilad Asharov. Towards characterizing complete fairness in secure two-party computation. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 291–316, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_13. 3, 5

Bar02 Boaz Barak. Constant-round coin-tossing with a man in the middle or realizing the shared random string model. In *43rd Annual Symposium on Foundations of Computer Science*, pages 345–355, Vancouver, BC, Canada, November 16–19, 2002. IEEE Computer Society Press. doi:10.1109/SFCS.2002.1181957. 4

Bea89 Donald Beaver. *Perfect privacy for two-party protocols*. Harvard University, Center for Research in Computing Technology, Aiken . . . , 1989. 11

BGP00 Mihir Bellare, Oded Goldreich, and Erez Petrank. Uniform generation of np-witnesses using an np-oracle. *Information and Computation*, 163(2):510–526, 2000. 7

BHLT17 Niv Buchbinder, Iftach Haitner, Nissan Levi, and Eliad Tsfadia. Fair coin flipping: Tighter analysis and the many-party case. In Philip N. Klein, editor, *28th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2580–2600, Barcelona, Spain, January 16–19, 2017. ACM-SIAM. doi:10.1137/1.9781611974782.170. 3, 5

BLOO11 Amos Beimel, Yehuda Lindell, Eran Omri, and Ilan Orlov. $1/p$-Secure multiparty computation without honest majority and the best of both worlds. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 277–296, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-22792-9_16. 3, 5

Blu82 Manuel Blum. Coin flipping by telephone. *Proc. of COMPCON, IEEE, 1982*, 1982. 4, 5

BM09 Boaz Barak and Mohammad Mahmoody-Ghidary. Merkle puzzles are optimal - an $O(n^2)$-query attack on any key exchange from a random oracle. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 374–390, Santa Barbara, CA, USA, August 16–20, 2009. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-03356-8_22. 6, 7, 13, 18

BOO10 Amos Beimel, Eran Omri, and Ilan Orlov. Protocols for multiparty coin toss with dishonest majority. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 538–557, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-14623-7_29. 3, 5

BPR+08 Dan Boneh, Periklis A. Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, and Brent Waters. On the impossibility of basing identity based encryption on trapdoor permutations. In *49th Annual Symposium on Foundations of Computer Science*, pages 283–292, Philadelphia, PA, USA, October 25–28, 2008. IEEE Computer Society Press. doi:10.1109/FOCS.2008.67. 6

CI93 Richard Cleve and Russell Impagliazzo. Martingales, collective coin flipping and discrete control processes. *In other words*, 1:5, 1993. 3, 6, 8, 16

Cle86 Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In *18th Annual ACM Symposium on Theory of Computing*, pages 364–369, Berkeley, CA, USA, May 28–30, 1986. ACM Press. doi:10.1145/12130.12168. 3, 4, 5

Coo71 Stephen A Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158, 1971. 4

CPS08 Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin. The random oracle model and the ideal cipher model are equivalent. In David Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 1–20, Santa Barbara, CA, USA, August 17–21, 2008. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-85174-5_1. 5

DLMM11 Dana Dachman-Soled, Yehuda Lindell, Mohammad Mahmoody, and Tal Malkin. On the black-box complexity of optimally-fair coin tossing. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 450–467, Providence, RI, USA, March 28–30, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-19571-6_27. 4, 6, 7, 8, 12, 14, 15

DMM14 Dana Dachman-Soled, Mohammad Mahmoody, and Tal Malkin. Can optimally-fair coin tossing be based on one-way functions? In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 217–239, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_10. 4, 6, 8, 12, 14, 15

GGK03 Rosario Gennaro, Yael Gertner, and Jonathan Katz. Lower bounds on the efficiency of encryption and digital signature schemes. In *35th Annual ACM Symposium on Theory of Computing*, pages 417–425, San Diego, CA, USA, June 9–11, 2003. ACM Press. doi:10.1145/780542.780604. 6

GHKL08 S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete fairness in secure two-party computation. In Richard E. Ladner and Cynthia Dwork, editors, *40th Annual ACM Symposium on Theory of Computing*, pages 413–422, Victoria, BC, Canada, May 17–20, 2008. ACM Press. doi:10.1145/1374376.1374436. 3, 5

GHMM18 Sanjam Garg, Mohammad Hajiabadi, Mohammad Mahmoody, and Ameer Mohammed. Limits on the power of garbling techniques for public-key encryption. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 335–364, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-96878-0_12. 6

GK10 S. Dov Gordon and Jonathan Katz. Partial fairness in secure two-party computation. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 157–176, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-13190-5_8. 3, 5

GKM+00 Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan. The relationship between public key encryption and oblivious transfer. In *41st Annual Symposium on Foundations of Computer Science*, pages 325–335, Redondo Beach, CA, USA, November 12–14, 2000. IEEE Computer Society Press. doi:10.1109/SFCS.2000.892121. 6

GMM07 Yael Gertner, Tal Malkin, and Steven Myers. Towards a separation of semantic and CCA security for public key encryption. In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 434–455, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-70936-7_24. 6

GMM17a Sanjam Garg, Mohammad Mahmoody, and Ameer Mohammed. Lower bounds on obfuscation from all-or-nothing encryption primitives. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 661–695, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-63688-7_22. 6

GMM17b Sanjam Garg, Mohammad Mahmoody, and Ameer Mohammed. When does functional encryption imply obfuscation? In Yael Kalai and Leonid Reyzin, editors, *TCC 2017: 15th Theory of Cryptography Conference, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 82–115, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_4. 6

GMMM18 Sanjam Garg, Mohammad Mahmoody, Daniel Masny, and Izaak Meckler. On the round complexity of OT extension. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 545–574, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-96878-0_19. 6

GMR01 Yael Gertner, Tal Malkin, and Omer Reingold. On the impossibility of basing trapdoor functions on trapdoor predicates. In *42nd Annual Symposium on Foundations of Computer Science*, pages 126–135, Las Vegas, NV, USA, October 14–17, 2001. IEEE Computer Society Press. doi:10.1109/SFCS.2001.959887. 6

GMW87 Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, NY, USA, May 25–27, 1987. ACM Press. doi:10.1145/28395.28420. 4

GT00 Rosario Gennaro and Luca Trevisan. Lower bounds on the efficiency of generic cryptographic constructions. In *41st Annual Symposium on Foundations of Computer Science*, pages 305–313, Redondo Beach, CA, USA, November 12–14, 2000. IEEE Computer Society Press. doi:10.1109/SFCS.2000.892119. 6

Hås90 Johan Håstad. Pseudo-random generators under uniform assumptions. In *22nd Annual ACM Symposium on Theory of Computing*, pages 395–404, Baltimore, MD, USA, May 14–16, 1990. ACM Press. doi:10.1145/100216.100270. 3

HKT11 Thomas Holenstein, Robin Künzler, and Stefano Tessaro. The equivalence of the random oracle model and the ideal cipher model, revisited. In Lance Fortnow and Salil P. Vadhan, editors, *43rd Annual ACM Symposium on Theory of Computing*, pages 89–98, San Jose, CA, USA, June 6–8, 2011. ACM Press. doi:10.1145/1993636.1993650. 5

HMO18 Iftach Haitner, Nikolaos Makriyannis, and Eran Omri. On the complexity of fair coin flipping. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018: 16th Theory of Cryptography Conference, Part I*, volume 11239 of *Lecture Notes in Computer Science*, pages 539–562, Panaji, India, November 11–14, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-03807-6_20. 6

HNO$^+$18 Iftach Haitner, Kobbi Nissim, Eran Omri, Ronen Shaltiel, and Jad Silbak. Computational two-party correlation: A dichotomy for key-agreement protocols. In Mikkel Thorup, editor, *59th Annual Symposium on Foundations of Computer Science*, pages 136–147, Paris, France, October 7–9, 2018. IEEE Computer Society Press. doi:10.1109/FOCS.2018.00022. 6

HOZ13 Iftach Haitner, Eran Omri, and Hila Zarosim. Limits on the usefulness of random oracles. In Amit Sahai, editor, *TCC 2013: 10th Theory of Cryptography Conference*, volume 7785 of *Lecture Notes in Computer Science*, pages 437–456, Tokyo, Japan, March 3–6, 2013. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-36594-2_25. 6

HT14 Iftach Haitner and Eliad Tsfadia. An almost-optimally fair three-party coin-flipping protocol. In David B. Shmoys, editor, *46th Annual ACM Symposium on Theory of Computing*, pages 408–416, New York, NY, USA, May 31 – June 3, 2014. ACM Press. doi:10.1145/2591796.2591842. 3, 5

IL89 Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th Annual Symposium on Foundations of Computer Science*, pages 230–235, Research Triangle Park, NC, USA, October 30 – November 1, 1989. IEEE Computer Society Press. doi:10.1109/SFCS.1989.63483. 3, 4

ILL89 Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions (extended abstracts). In *21st Annual ACM Symposium on Theory of Computing*, pages 12–24, Seattle, WA, USA, May 15–17, 1989. ACM Press. doi:10.1145/73007.73009. 3

IR89 Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *21st Annual ACM Symposium on Theory of Computing*, pages 44–61, Seattle, WA, USA, May 15–17, 1989. ACM Press. doi:10.1145/73007.73012. 3, 4, 5, 6, 7, 8, 13

JVV86 Mark R Jerrum, Leslie G Valiant, and Vijay V Vazirani. Random generation of combinatorial structures from a uniform distribution. *Theoretical Computer Science*, 43:169–188, 1986. 7

KMM19 Hamidreza Amini Khorasgani, Hemanta K. Maji, and Tamalika Mukherjee. Estimating gaps in martingales and applications to coin-tossing: Constructions and hardness. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019: 17th Theory of Cryptography Conference, Part II*, volume 11892 of *Lecture Notes in Computer Science*, pages 333–355, Nuremberg, Germany, December 1–5, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-36033-7_13. 6, 8, 16

KMW20 Hamidreza Amini Khorasgani, Hemanta K. Maji, and Mingyuan Wang. Coin tossing with lazy defense: Hardness of computation results. 2020. https://eprint.iacr.org/2020/131. 6, 8, 9, 10, 11, 12, 16, 18

KN Eyal Kushilevitz and Noam Nisan. Communication complexity. 1997. *Google Scholar Google Scholar Digital Library Digital Library*. 10

KSY11 Jonathan Katz, Dominique Schröder, and Arkady Yerukhimovich. Impossibility of blind signatures from one-way permutations. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 615–629, Providence, RI, USA, March 28–30, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-19571-6_37. 6

Kus89 Eyal Kushilevitz. Privacy and communication complexity. In *30th Annual Symposium on Foundations of Computer Science*, pages 416–421, Research Triangle Park, NC, USA, October 30 – November 1, 1989. IEEE Computer Society Press. doi:10.1109/SFCS.1989.63512. 11

Mak14 Nikolaos Makriyannis. On the classification of finite Boolean functions up to fairness. In Michel Abdalla and Roberto De Prisco, editors, *SCN 14: 9th International Conference on Security in Communication Networks*, volume 8642 of *Lecture Notes in Computer Science*, pages 135–154, Amalfi, Italy, September 3–5, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-10879-7_9. 3, 5

MM11 Takahiro Matsuda and Kanta Matsuura. On black-box separations among injective one-way functions. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 597–614, Providence, RI, USA, March 28–30, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-19571-6_36. 6

MM16 Mohammad Mahmoody and Ameer Mohammed. On the power of hierarchical identity-based encryption. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 243–272, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-49896-5_9. 6

MMN+16 Mohammad Mahmoody, Ameer Mohammed, Soheil Nematihaji, Rafael Pass, and abhi shelat. Lower bounds on assumptions behind indistinguishability obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A: 13th Theory of Cryptography Conference, Part I*, volume 9562 of *Lecture Notes in Computer Science*, pages 49–66, Tel Aviv, Israel, January 10–13, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-49096-9_3. 6

MMP14a Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. Limits of random oracles in secure computation. In Moni Naor, editor, *ITCS 2014: 5th Conference on Innovations in Theoretical Computer Science*, pages 23–34, Princeton, NJ, USA, January 12–14, 2014. Association for Computing Machinery. doi:10.1145/2554797.2554801. 6, 12

MMP14b Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. On the power of public-key encryption in secure computation. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 240–264, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_11. 5, 6, 7, 12, 13

MNS09 Tal Moran, Moni Naor, and Gil Segev. An optimally fair coin toss. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 1–18. Springer, Heidelberg, Germany, March 15–17, 2009. doi:10.1007/978-3-642-00457-5_1. 3, 7

MPR09 Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 256–273. Springer, Heidelberg, Germany, March 15–17, 2009. doi:10.1007/978-3-642-00457-5_16. 11

NY89 Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *21st Annual ACM Symposium on Theory of Computing*, pages 33–43, Seattle, WA, USA, May 15–17, 1989. ACM Press. doi:10.1145/73007.73011. 3

Rom90 John Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd Annual ACM Symposium on Theory of Computing*, pages 387–394, Baltimore, MD, USA, May 14–16, 1990. ACM Press. doi:10.1145/100216.100269. 3

RTV04 Omer Reingold, Luca Trevisan, and Salil P. Vadhan. Notions of reducibility between cryptographic primitives. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages

1–20, Cambridge, MA, USA, February 19–21, 2004. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-24638-1_1. 5

Rud88 Steven Rudich. Limits on the provable consequences of one-way functions. 1988. 6

Rud92 Steven Rudich. The use of interaction in public cryptosystems (extended abstract). In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 242–251, Santa Barbara, CA, USA, August 11–15, 1992. Springer, Heidelberg, Germany. doi:10.1007/3-540-46766-1_19. 6

Sch17 René L Schilling. *Measures, integrals and martingales*. Cambridge University Press, 2017. 13

Sim98 Daniel R. Simon. Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? In Kaisa Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 334–345, Espoo, Finland, May 31 – June 4, 1998. Springer, Heidelberg, Germany. doi:10.1007/BFb0054137. 6

Vah10 Yevgeniy Vahlis. Two is a crowd? A black-box separation of one-wayness and security under correlated inputs. In Daniele Micciancio, editor, *TCC 2010: 7th Theory of Cryptography Conference*, volume 5978 of *Lecture Notes in Computer Science*, pages 165–182, Zurich, Switzerland, February 9–11, 2010. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-11799-2_11. 6

Yao86 Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th Annual Symposium on Foundations of Computer Science*, pages 162–167, Toronto, Ontario, Canada, October 27–29, 1986. IEEE Computer Society Press. doi:10.1109/SFCS.1986.25. 4