Secure Non-interactive Simulation: Hardness & Feasibility

Hamidreza Amini Khorasgani
Department of Computer Science, Purdue University, USA
haminikh@purdue.edu

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

Hai H. Nguyen
Department of Computer Science, Purdue University, USA
nguye245@purdue.edu

Abstract

Network latency is a significant source of inefficiency in interactive protocols. This work contributes towards the possibility of reducing the round complexity and communication complexity of secure computation protocols to a minimum. We introduce the concept of secure non-interactive simulation of joint distributions.

Two parties begin with multiple independent samples from a correlated randomness source. Next, our objective is to investigate what forms of joint distributions can Alice and Bob securely simulate without any further communication. This offline preprocessing step fits perfectly within the offline-online paradigm of secure computation, which enables general secure computation even against parties with unbounded computational power.

One may interpret this concept as imbuing the notion of non-interactive simulation of joint distributions, which initiated from the seminal works of Gács and Körner (1972), and Wyner (1975), in information theory with cryptographic security. This concept is stronger than merely a secure version of non-interactive correlation distillation as introduced by Mossel, O'Donnell, Regev, Steif, and Sudakov (2004) because secure private keys alone do not suffice to facilitate general secure computation. Alternatively, secure non-interactive simulation is a natural restriction of performing cryptography with one-way communication introduced by Garg, Ishai, Kushilevitz, Ostrovsky, and Sahai (2015), which also serves as a naturally arising base case for inductively building cryptographic primitives with minimum communication complexity.

In this work, we study samples from (1) $\mathsf{BSS}(\epsilon)$, that is the joint distribution (X, Y), where X is a uniform random bit and Y is correlated bit such that $X \neq Y$ with probability $\epsilon \in (0, 1/2)$, and (2) $\mathsf{BES}(\epsilon)$, that is the joint distribution (X, Y), where X is a uniform random bit, and $Y = X$ with probability $(1 - \epsilon)$; otherwise $Y = \perp$, where $\epsilon \in (0, 1)$.

Note that the reverse hypercontractivity and hardness of cryptography with one-way messages both rule out the possibility of realizing any BES sample from BSS samples. This impossibility result carries over to our secure non-interactive simulation as well. Furthermore, we prove that it is also impossible to securely and non-interactively simulate samples of BSS from BES samples as well. Note that this impossibility result both in the setting of non-interactive simulation and cryptography with one-way communication remains open.

Next, we prove that we can simulate a sample of $\mathsf{BES}(\epsilon')$ from multiple samples of $\mathsf{BES}(\epsilon)$ if and only if $(1-\epsilon') = (1-\epsilon)^k$, for some $k \in \mathbb{N}$. We proceed by proving that all secure constructions must be linear, and, after that, the rate of the simulation is at most $1/k$.

Finally, we show the existence of securely and non-interactively simulating a sample of $\mathsf{BSS}(\epsilon')$ from $\mathsf{BSS}(\epsilon)$ if and only if $(1 - 2\epsilon') = (1 - 2\epsilon)^k$, for some $k \in \mathbb{N}$. Interestingly, there are linear as well as (comparatively inefficient) non-linear constructions.

Keywords and phrases Non-interactive Simulation, Secure Simulation, Binary Erasure Sample, Binary Symmetric Sample, Rate of Reduction

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

Network latency is a significant source of inefficiency in interactive protocols (https://gist.github.com/hellerbarde/2843375). Towards minimizing the impact of network latency on secure computation protocols, there is an increased investigation of the possibility of reducing the round complexity and the communication complexity of secure computation protocols [GMW87, BMR90, KOS03, KO04, Pas04, PW10, Wee10, Goy11, GMPP16, ACJ17, BHP17, COSV17b, COSV17a, BGJ^{+}18, HHPV18]. This work, continuing this general line of investigation, studies *secure non-interactive simulation of joint distributions* against information-theoretic adversaries. For motivation, consider the following representative application where this concept has promising potential for impact.

Representative Motivating Application. Frequently, one comes across signals arising from cataclysmic celestial events or their aftereffects that are well beyond human influence. For example, just from the recent past, we witnessed events like (1) Mysterious fast radio bursts that repeat every sixteen days, (2) Sudden and unexpected dimming of Betelgeuse indicating that it may go supernova, and (3) Gravitational waves originating from the merger of two neutron stars. Such signals, when observed from multiple observatories spread across the globe, yield large quantities of noisy correlated observations. Local atmospheric or electromagnetic noise perturb these observations. One does not have control over the exact noise introduced to the observations at these different locations, even when there are well-established models for these noises.

Unlike the prominent objective in information reconciliation of removing noise by leveraging multiple correlated observations, in cryptography, noise that is beyond the adversarial control is, surprisingly, a facilitator for non-trivial cryptographic tasks, like, key-agreement, and secure computation [CK90, Kil91, Kil00, IPS08, IKO^{+}11, KMPS14].[1] There has been extensive research into the feasibility and efficiency of founding secure computation on such sources of noise. Within this ambit of research, out of efficiency concerns, the following natural question arises.

“How to efficiently build an infrastructure for non-trivial cryptography
from correlated samples
without any additional interaction between the observatories?”

In particular, the *offline-online paradigm* of secure computation [MNPS04, BNP08, DPSZ12, NNOB12] typically relies on an offline phase to generate samples from a correlated randomness source and, later, uses these samples to perform a particular secure computation task during the fast online phase. One may securely realize the offline phase using computationally secure protocols (for example, using homomorphic encryption [Gen09] or somewhat homomorphic encryption [BGV12]). However, an increase in computational power due to shifts in computing paradigms or an improvement in the efficiency of adversarial attacks owing to recent mathematical advances may potentially render these protocols insecure. On

[1] This is the most appropriate opportunity to quote the following paragraphs from Crépeau and Kilian [CK90]. “Noisy channels have been extensively studied in the field of coding theory, and it is interesting to see how our perspective differs from the more traditional one. Coding theory adopts the viewpoint that noise is a bad thing, to be eliminated as efficiently as possible. Given a noisy channel, a coding theorist tries to simulate a pristine, noiseless communication line.
From our point of view (following Wyner [Wyn75]), an ideal communication line is a sterile, cryptographically uninteresting entity. Noise, on the other hand, breeds disorder, uncertainty, and confusion. Thus, it is the cryptographer’s natural ally. The question we consider is whether this primordial uncertainty can be sculpted into the more sophisticated uncertainty found in secure two-party protocols.”

the other hand, correlated randomness from noisy sources enables secure computation even against adversaries with unbounded (classical/quantum) computational power. Therefore, the motivating example above has the potential of generating highly efficient infrastructure for secure computation that never forfeits its security. Furthermore, the online phase may prefer to use samples from a noise source that has a particular parameter due to efficiency considerations (for example, this choice may arise from the particular multiplication friendly error-correcting code being used in the online protocol). Although the celestial source's noise parameter is beyond our control, it would be preferable if the parties can non-interactively simulate samples of a noise source with the more preferred parameter.

Positioning of our Research. In information theory, *non-interactive simulation of joint distributions* is the focus of intense curiosity and generates highly influential research (refer to the comprehensive survey [STW19]). Our study adds the additional feature of *security* to this direction of inquiry. As a consequence, for instance, randomized simulations or simulations where a party *erases* information from her view are ruled out in our secure simulation setting. Since shared private key is not sufficient for general secure computation, secure non-interactive simulation is *not* a straightforward generalization of *non-interactive correlation distillation* [MOR+06] with the cryptographic notion of security.

On the other hand, there has also been research in cryptography to perform secure computation using only one-way messages [GIK+15]. Our problem setting is even further restrictive; parties do not communicate with each other at all. However, looking ahead, our results demonstrate that several feasibility results in the one-way communication setting carry over to our non-interactive setting. In fact, the non-interactive simulation allows the parties to specify the infrastructure itself well after the correlated samples have been stored.

Furthermore, our research provides bounds on the efficiency of such computations, a.k.a., *upper bounds on the rate* of secure simulation of some fundamental joint distributions. Additionally, in the long run, our research forms the base case of building *communication-efficient* infrastructure for secure computation. For example, one can inductively build more sophisticated k-bit protocols from (comparatively) less expressive $(k-1)$-bit protocols; with the base case being $k = 0$, which is our research focus in this paper.

In this work, we primarily consider statistical security. However, a fine-grained security analysis, where one characterizes the minimum insecurity achievable for secure non-interactive simulation of arbitrary joint distributions has potential applications in cryptography as well. As indicated by the work of Ishai, Kushilevitz, Ostrovsky, Prabhakaran, Sahai, Wullschleger [IKO+11], any construction of noise samples with appropriately small constant insecurity suffices to perform general secure computation.

1.1 Our Contribution

We introduce some intuitive terminology to present our results informally. Section 4 and Section 5 present the formal results and their proofs. Let (X, Y) is a joint distribution over the sample space $(\mathcal{X}, \mathcal{Y})$, and (U, V) be a joint distribution over the sample space $(\mathcal{U}, \mathcal{V})$. Sample $(x^n, y^n) \overset{\$}{\leftarrow} (X, Y)^{\otimes n}$ (that is, one draws n independent samples from the distribution (X, Y)). Alice gets $x^n \in \mathcal{X}^n$ and Bob gets $y^n \in \mathcal{Y}^n$. Suppose $f_n \colon \mathcal{X}^n \to \mathcal{U}$ and $g_n \colon \mathcal{Y}^n \to \mathcal{V}$ be the *reduction functions* for Alice and Bob, respectively. Alice computes $u' = f_n(x^n)$ and Bob computes $v' = g_n(y^n)$.

We say that (U, V) *reduces to* $(X, Y)^{\otimes n}$ *via reduction functions* f_n, g_n *with insecurity* $\nu(n)$ (represented by, $(U, V) \sqsubseteq^{\nu(n)}_{f_n, g_n} (X, Y)^{\otimes n}$) if the following three conditions are satisfied.

1. Correctness: The distribution of the samples (u', v') is $\nu(n)$-close to the distribution

(U, V) in statistical distance.

2. Security against corrupt Alice: Consider any (u, v) in the support of the distribution (U, V). The distribution of x^n conditioned on the fact that $u' = u$ and $v' = v$ is independent of v.
3. Security against corrupt Bob: Consider any (u, v) in the support of the distribution (U, V). The distribution of y^n conditioned on the fact that $u' = u$ and $v' = v$ is independent of u.

We remark that, since we consider non-interactive protocols without private inputs, semi-honest and malicious security are identical. So, for the simplicity of presentation, we assume that we consider security against semi-honest adversaries, that is, parties follow the protocol but are curious to find more information. Section 3 provides a formal simulation-based security definition.

In this paper, we consider samples from two fundamental distributions.

1. Binary symmetric source. X and Y are uniformly random bits such that $X \neq Y$ with probability $\epsilon \in (0, 1/2)$. We represent this joint distribution by $\mathsf{BSS}(\epsilon)$.
2. Binary erasure source. X is a uniformly random bit, and $Y = X$ with probability $(1 - \epsilon)$, where $\epsilon \in (0, 1)$; otherwise, $Y = \perp$. We represent this joint distribution by $\mathsf{BES}(\epsilon)$.

Before we begin, note that the non-interactive simulation of joint distributions and cryptography with one-way communication are relaxations of secure non-interactive simulation of joint distributions, which we consider in this work. So, the impossibility results in either of these two settings automatically imply an impossibility in our context.

For example, it is impossible for $\mathsf{BES}(\epsilon')$ to reduce to $\mathsf{BSS}(\epsilon)^{\otimes n}$, for infinitely many $n \in \mathbb{N}$, with insecurity $\nu(n) = \mathsf{negl}(n)$,[2] for any $\epsilon \in (0, 1/2)$, and $\epsilon' \in (0, 1)$ [KA16, KA12, GIK⁺15]. On the other hand, it is not known whether $\mathsf{BSS}(\epsilon')$ reduces to $\mathsf{BES}(\epsilon)$ with $\mathsf{negl}(n)$ insecurity via either non-interactive simulations or one-way communication. We resolve this problem for secure non-interactive simulations.

▶ Informal Theorem 1 (Binary Symmetric Sample from Binary Erasure Samples). Fix $\epsilon' \in (0, 1/2)$ and $\epsilon \in (0, 1)$. For every infinite family of reduction functions $\{f_n, g_n\}_{n \in \mathbb{N}}$, insecurity bound $\nu(n) = \mathsf{negl}(n)$, and sufficiently large n, we have

$$\mathsf{BSS}(\epsilon') \not\sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\epsilon)^{\otimes n}.$$

Next, we consider the interconversion among binary erasure sources with different erasure probabilities.

▶ Informal Theorem 2 (Binary Erasure Samples: Feasibility & Rate). Fix any erasure probabilities $\epsilon', \epsilon \in (0, 1)$. Suppose, there exists an infinite family of reduction functions $\{f_n, g_n\}_{n \in \mathbb{N}}$ and insecurity bound $\nu(n) = \mathsf{negl}(n)$ such that, for infinitely many $n \in \mathbb{N}$ satisfying

$$\mathsf{BES}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\epsilon)^{\otimes n}.$$

Then, there exists $n^* \in \mathbb{N}$ and an infinite family of functions $\{f^*_n, g^*_n\}_{n \in \mathbb{N}}$ such that $\mathsf{BES}(\epsilon') \sqsubseteq^{0}_{f^*_n, g^*_n} \mathsf{BES}(\epsilon)^{\otimes n}$, for all $n \geq n^*$. Furthermore, there exists $k \in \{1, 2, \ldots, n^*\}$ such that $(1 - \epsilon') = (1 - \epsilon)^k$, $f^*_n(x) = g^*_n(x)$, for all $x \in \{0, 1\}^n$, and either f^*_n or $-f^*_n$ is the parity of some k input bits.

Moreover, if there exists an infinite family of functions $\{f_n, g_n\}_{n \in \mathbb{N}}$ and insecurity bound $\nu(n) = \mathsf{negl}(n)$ such that, for infinitely many $n \in \mathbb{N}$, we have $\mathsf{BES}(\epsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\epsilon)^{\otimes n}$. Then, we have $m(n) \leq n/k$.

[2] The function $f(n)$ is negligible in n if it becomes smaller than any inverse-polynomial in n, for sufficiently large $n \in \mathbb{N}$.

In the context of cryptography using one-way communication one can achieve ϵ' that is lower or higher than ϵ. On the other hand, in this work, we show that $\epsilon' \geq \epsilon$ is necessary for secure non-interactive simulation to exist.

Typically, the impossibility results in the non-interactive simulation of joint distributions literature relies on leveraging the reverse Hypercontractivity theorem [KA12, KA16, NW17]. However, for samples from the binary erasure channel, this approach encounters a major hurdle [KA12]. The addition of the security constraint in our setting helps us circumvent this hurdle. Essentially, we show that the *only* secure non-interactive simulation reduction among samples of the erasure channel is the following. Alice outputs a parity of her input x^n, and Bob outputs the parity of $y^n \in \{0,1\}^n$; otherwise Bob outputs $\perp$. Interestingly, this protocol is identical in spirit to the cryptography with one-way communication protocol as presented in [GIK$^+$15] when $(1-\epsilon') \in \{(1-\epsilon), (1-\epsilon)^2, \dots .\}$. However, all other ϵ' are feasible *only* with one-way communication [GIK$^+$15].

Finally, we consider the interconversion among binary symmetric samples with different flipping probabilities.

▶ Informal Theorem 3 (Binary Symmetric Samples: Feasibility). Fix any bit-flipping probabilities $\epsilon', \epsilon \in (0, 1/2)$. Suppose, there exists an infinite family of reduction functions $\{f_n, g_n\}_{n\in\mathbb{N}}$ and insecurity bound $\nu(n) = \mathsf{negl}(n)$ such that, for infinitely many $n \in \mathbb{N}$, we have

$$\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}.$$

Then, there exists $n^* \in \mathbb{N}$ and an infinite family of functions $\{f_n^*, g_n^*\}_{n\in\mathbb{N}}$ such that $\mathsf{BSS}(\epsilon') \sqsubseteq^{0}_{f_n^*,g_n^*} \mathsf{BSS}(\epsilon)^{\otimes n}$, for all $n \geq n^*$. Furthermore, there exists $k \in \{1, 2, \dots, n^*\}$ such that $(1-2\epsilon') = (1-2\epsilon)^k$, $f_n^* = g_n^*$, and either f_n^* or $-f_n^*$ is the parity of some k input bits.

Note that one cannot increase the reliability of the binary symmetric channel, which is identical to the result in [GIK$^+$15]. Furthermore, unlike [GIK$^+$15], we also rule out the possibility of secure non-interactive simulation for any $(1-2\epsilon') \notin \left\{(1-2\epsilon), (1-2\epsilon)^2, \dots\right\}$. For such ϵ', any non-interactive simulation is constant insecure.

At the outset, this theorem looks similar to the theorem for binary erasure channels; however, there are exciting subtleties involved. The theorem above states that one can securely non-interactively simulate samples of the binary symmetric channel as follows. Alice outputs the parity of her input x^n, and bob also outputs the parity of his input y^n. Interestingly, we prove that there are (non-trivial) *non-linear reduction functions* as well; however, they are inefficient for generating one sample. That is, for every non-linear reduction, there exists a more efficient linear reduction.

Consider the following example when $(1-2\epsilon') = (1-2\epsilon)^2$. So, when $n = 2$, the linear reduction functions $f_2(x^2) = x_1^2 \oplus x_2^2$, and $g_2 = f_2$ suffice.[3] However, interestingly, there exists non-linear reduction functions $f_n = g_n$ for $n = 4$. For example, consider the reduction function below.

$$f_4(x^4) = \frac{2 - (-1)^{x_1^4+x_3^4} - (-1)^{x_2^4+x_3^4} - (-1)^{x_1^4+x_4^4} + (-1)^{x_2^4+x_4^4}}{4}.$$

Although it is clear that the rate is upper bounded by $m(n) \leq n/2$ when linear reductions produce every output sample, it is not evident that the non-linear reductions cannot surpass this rate. We leave this question as an exciting open research direction.

[3] The symbol x_i^n represents the i-th bit in the n-bit string $x^n \in \{0,1\}^n$.

We remark that secure non-interactive simulation of shared private randomness (a.k.a., the secure version of non-interactive correlation distillation) is also impossible starting from multiple samples of BSS or BES because of the informal theorems above.

1.2 Prior Related Works

In this section, we discuss some of the closely related concepts in information theory and cryptography. It is impossible to do justice to these vast fields by providing every perspective into their respective research in this one section. Consequently, we cite and discuss only the most relevant literature to these concepts.

Non-interactive simulation. Information theory studies the possibility of simulating a sample from a joint distribution (U, V) given multiples samples from the joint distribution (X, Y). This concept is referred to as *non-interactive simulation of joint distributions.* This line of research starts from the seminal works of Gács and Körner [GK73] and Wyner [Wyn75]. The primary difference of this concept from our object of study is clearly the omission of security. For example, it is permissible for parties to erase information from their views in this setting. On the other hand, in our setting, since we consider semi-honest and malicious security, erasure of information gives rise to insecurity. Let us consider an illustrative example highlighting this difference. Consider simulating one sample of $\mathsf{BSS}(\epsilon/2)$ from multiple samples of $\mathsf{BES}(\epsilon)$. Alice outputs the bit of her first sample. If Bob also received the bit in his first sample, then he outputs the bit; otherwise, if he received $\perp$ as his first sample, he outputs a uniformly random bit.[4] Note that this non-interactive simulation is not secure.[5] Even the decision version of the problem where one has to determine whether samples from one joint distribution may be non-interactively simulated from the samples of another joint distribution, in its full generality, is a difficult problem [GKS16, DMN18]. Technically, reverse hypercontractivity [AG76, Bor82, MOR$^+$06, MOS13, KA16, DMN18, BG15, MO05a] and maximal correlation [Hir35, Wit75, AG76, Rén59, AGKN13] are few of the most prominent techniques employed to prove the impossibility of non-interactive simulations. We refer the interested reader to an exceptional survey by Sudan, Tyagi, and Watanabe [STW19] for a thorough introduction to this field.

There is a related notion of *non-interactive correlation distillation,* where the target joint distribution is the distribution of uniformly random private keys [MOR$^+$06, Yan04, MO05b].

Joint Distributions useful for Secure Computation. Not all joint distribution (U, V) are useful for general secure computation. If the mutual information of (U, V) is 0, then clearly this distribution does not suffice for key agreement, let alone secure computation, which is more complex to realize than key agreement. Even if the mutual information of (U, V) is > 0, then this joint distribution might enable key agreement, but not support general secure computation. Kilian [Kil00] exactly characterized all joint distributions that enable general secure computation. Samples from, for example, BSS and BES satisfy this characterization. The benefit of securely computation based on samples of joint distributions

[4] Bob can simulate a uniformly random bit from multiple samples of the $\mathsf{BES}(\epsilon)$ joint distribution.

[5] Consider the following case analysis when Bob is corrupt. Consider Alice's output being 0 and Bob's output being 0. The simulation strategy for Bob has to output $\perp$ with probability (close to) $\frac{\epsilon/2}{(1-\epsilon)+\epsilon/2}$ as the first simulated sample from $\mathsf{BES}(\epsilon)$, and output 0 with probability (close to) $\frac{1-\epsilon}{(1-\epsilon)+\epsilon/2}$ as the first simulated sample from $\mathsf{BES}(\epsilon)$; otherwise, the simulation is insecure. Now consider the case when Alice's output is 1 and Bob's output is 0. In this case, with probability (close to) $\frac{1-\epsilon}{(1-\epsilon)+\epsilon/2}$, Bob's simulated first sample of $\mathsf{BES}(\epsilon)$ is inconsistent with Alice's output. Therefore, no secure simulation strategy for Bob exists.

is that these protocols are secure even against adversaries with unbounded computational power.

Secure Computation with Low Interaction and Communication. Alice and Bob, beginning from samples of any joint distribution that is useful for secure computation, may perform general secure computation in a constant number of rounds [IK00, IK02, AIK04, IPS08]. In fact, one can also perform secure computation at a constant rate[6] [IKO$^+$11]. Recently, Garg, Ishai, Kushilevitz, Ostrovsky, and Sahai [GIK$^+$15] explore the potential of secure computation using noisy channels and one-way communication. In their setting, they leave open several feasibility/infeasibility problems related to binary symmetric and binary erasure channels. The proposed notion of secure non-interactive secure simulation in this work, permits no communication between the parties.

2 Preliminaries

2.1 Notations

We denote $[n]$ as the set $\{1, 2, \dots n\}$, and $N = 2^n$. The distribution $U_{\{0,1\}^n}$ is the uniform distribution over the set $\{0, 1\}^n$. For two functions f, g defined on the same domain, we use $f = g$ when the value of f and g are equal for each element of their domain. We use script letters $\mathcal{X}, \mathcal{Y}, \dots$ to denote finite sets, and μ usually denotes a probability distribution. $(\mathcal{X}, \mathcal{Y})$ is a joint probability space. We use X, Y to denote random variables. For $x^n \in \mathcal{X}^n$, we represent $x_i^n \in \mathcal{X}$ as the i-th coordinate of x^n.

Statistical Distance. The statistical distance between two distributions P and Q over a (discrete) sample space Ω is defined as the following.

$$\mathsf{SD}\left(P, Q\right) = \frac{1}{2} \sum_{x \in \Omega} \left|P(x) - Q(x)\right|.$$

2.2 Correlated Random Sources and Noise Operator

Binary Symmetric Source. A binary symmetric source with flipping probability $\epsilon \in (0, 1)$, denoted as $\mathsf{BSS}(\epsilon)$, is a joint distribution over the sample space $\{0, 1\} \times \{0, 1\}$ such that if $(X, Y) \overset{\$}{\leftarrow} \mathsf{BSS}(\epsilon)$, then $\Pr[X = 0, Y = 1] = \Pr[X = 1, Y = 0] = \epsilon/2$, and $\Pr[X = 0, Y = 0] = \Pr[X = 1, Y = 1] = (1 - \epsilon)/2$.

Binary Erasure Source. A binary erasure source with erasure probability $\epsilon \in (0, 1)$, denoted as $\mathsf{BES}(\epsilon)$, is a joint distribution over the sample space $\{0, 1\} \times \{0, 1, \perp\}$ such that if $(X, Y) \overset{\$}{\leftarrow} \mathsf{BES}(\epsilon)$, then $\Pr[X = 0, Y = 0] = \Pr[X = 1, Y = 1] = (1 - \epsilon)/2$, and $\Pr[X = 0, Y = \perp] = \Pr[X = 1, Y = \perp] = \epsilon/2$.

Noise Operator. Let $\rho \in [0, 1]$ be the parameter determining the noise. For each fixed bit string $x^n \in \{0, 1\}^n$, we write $y^n \overset{\$}{\leftarrow} N_\rho(x^n)$ to denote that the random string y^n is drawn as follows: for each $i \in [n]$, independently, y_i^n is equal to x_i^n with probability ρ and it is uniformly random with probability $1 - \rho$. The noise operator with parameter $\rho \in [0, 1]$ is the linear operator T_ρ on function $f : \{0, 1\}^n \to \mathbb{R}$ defined as $\mathsf{T}_\rho f(x^n) = \mathbb{E}_{y^n \sim N_\rho(x^n)}[f(y^n)]$. We say that y^n is ρ-correlated to x^n.

Note that if $(X^n, Y^n) \overset{\$}{\leftarrow} \mathsf{BSS}(\epsilon)$, then Y^n is ρ-correlated to X^n with parameter $\rho = 1 - 2\epsilon$.

[6] One can equivalently interpret constant rate as spending a constant number of samples to perform one multiplication/AND-gate secure in an ammortized sense.

2.3 Fourier Analysis for Boolean Functions: Preliminaries

We recall some background in Fourier analysis that will be useful for our analysis (see [O'D14] for more details). Let $f, g\colon \{0,1\}^n \to \mathbb{R}$ be two real-valued Boolean functions. We define the inner product as following.

$$\langle f, g\rangle = \frac{1}{N}\sum_{x\in\{0,1\}^n} f(x)\cdot g(x) = \mathop{\mathbb{E}}_{x}\left[f(x)\cdot g(x)\right]$$

For each $S \subseteq [n]$, the characteristic function $\chi_S(x) = (-1)^{S\cdot x} = (-1)^{\sum_{i\in S} x_i}$ is a linear function that computes the parity (that is, the exclusive-or) of of the bits $(x_i)_{i\in S}$. The set all χ_S forms an orthonormal basis for the space of all real-valued functions on $\{0,1\}^n$. For any $S \subseteq [n]$, the Fourier coefficient of f at S is defined as $\widehat{f}(S) = \langle f, \chi_S\rangle$. Any function f can be uniquely expressed as $f = \sum_{S\in[n]} \widehat{f}(S)\chi_S$, called Fourier expansion of f. The Fourier weight of f on a set $S \subseteq [n]$ is defined to be $\widehat{f}(S)^2$, and the Fourier weight of f at degree k is $W_k[f] = \sum_{S:|S|=k} \widehat{f}(S)^2$.

Next we summarize the basic Fourier analysis on Boolean function with *restriction* on the sub-cubes. Let J and $\bar{J}$ be a partition of the set $[n]$. Let $f_{J|z} : \{0,1\}^J \to \mathbb{R}$ denote the restriction of f to J when the coordinates in $\bar{J}$ are fixed to $z \in \{0,1\}^{\bar{J}}$. Let $\widehat{f_{J|z}}(S)$ be the Fourier coefficient of the function $f_{J|z}$ corresponding to the set S. Then, when we assume that $z \in \{0,1\}^{\bar{J}}$ is chosen uniformly at random, we have $\mathbb{E}_z[\widehat{f_{J|z}}(S)] = \widehat{f}(S)$, and $\mathbb{E}_z[\widehat{f_{J|z}}(S)^2] = \sum_{T\subseteq \bar{J}} \widehat{f}(S\cup T)^2$.

3 Secure Non-Interactive Simulation: Definition

In this section, we define the notion of secure non-interactive simulation of joint distributions using a simulation-based security definition [Can00b, Can00a, Can01]. Suppose (X, Y) is a joint distribution over the sample space $\mathcal{X} \times \mathcal{Y}$, and (U, V) be a joint distribution over the sample space $\mathcal{U} \times \mathcal{V}$. For $n \in \mathbb{N}$, suppose $f_n\colon \mathcal{X}^n \to \mathcal{U}$ and $g_n\colon \mathcal{Y}^n \to \mathcal{V}$ be two reduction functions.

We clarify that it is standard in the literature to assume that the sample spaces $\mathcal{X}, \mathcal{Y}, \mathcal{U}$, and $\mathcal{V}$ are constant sized (i.e., does not depend on n). All the probabilities $\Pr[(X, Y) = (x, y)]$ and $\Pr[(U, V) = (u, v)]$ are either 0 or at least a constant (i.e., for example, these probabilities do not tend to 0 as a function of n).

We shall define simulation-based security for secure non-interactive reductions. In the real world, we have the following experiment.

1. A trusted third party samples $(x^n, y^n) \xleftarrow{\$} (X, Y)^{\otimes n}$, and delivers $x^n \in \mathcal{X}^n$ to Alice and $y^n \in \mathcal{Y}^n$ to Bob.
2. Alice outputs $u' = f_n(x^n)$, and Bob outputs $v' = g_n(y^n)$.

For inputless functionalities and non-interactive computation, semi-honest and malicious adversaries are identical. Furthermore, static and adaptive corruption are also identical for this setting. So, for simplicity, one can always consider semi-honest static corruption to interpret the security definitions. All forms of adversary mentioned above shall turn out to be equivalent in our setting.

1. **The case of no corruption.** Suppose the environment does not corrupt any party. So, it receives (U, V) as output from the two parties in the ideal world. In the real world,

the simulator receives $(f_n(X^n), g_n(Y^n))$ as output. If this reduction has at most $\nu(n)$ insecurity, then the following must hold.

$$\mathsf{SD}\left(\ (U,V)\ ,\ (f_n(X^n), g_n(Y^n))\ \right) \leq \nu(n).$$

2. **The case of Corrupt Alice.** Suppose the environment statically corrupt Alice. In the real world, the simulator receives $(X^n, f_n(X^n), g_n(Y^n))$. In the ideal world, we have a simulator $\mathrm{Sim}_A\colon \mathcal{U} \to \mathcal{X}^n$ that receives u from the ideal functionality, and outputs $(\mathrm{Sim}_A(u), u)$ to the environment. The environment's view is the random variable $(\mathrm{Sim}_A(U), U, V)$. If this reduction has at most $\nu(n)$ insecurity, then the following must hold.
$$\mathsf{SD}\left(\ (\mathrm{Sim}_A(U), U, V)\ ,\ (X^n, f_n(X^n), g_n(Y^n))\ \right) \leq \nu(n).$$
3. **The case of Corrupt Bob.** Analogously, there exists a simulator for Bob $\mathrm{Sim}_B\colon \mathcal{V} \to \mathcal{Y}^n$ and the following must hold if this reduction has at most $\nu(n)$ insecurity.
$$\mathsf{SD}\left(\ (U, V, \mathrm{Sim}_B(V))\ ,\ (f_n(X^n), g_n(Y^n), Y^n)\ \right) \leq \nu(n).$$

If there exists reductions functions f_n, g_n such that the insecurity is at most $\nu(n)$ as defined above then we say that (U,V) *reduces to* $(X,Y)^{\otimes n}$ *via reduction functions* f_n, g_n *with insecurity at most* $\nu(n)$. In our presentation, all secure reductions admit *computationally efficient* simulators Sim_A and Sim_B. Moreover, all our impossibility results even rule out simulators with unbounded computational power. We say that $\nu(n)$ is *negligible* in n if it decays faster than any inverse-polynomial in n for sufficiently large values of n.

To make our paper accessible to a wider audience, we add a discussion on some consequences of the definition of secure non-interactive simulation presented above.

1. The security definition above may be reinterpreted using averaging over $(u,v) \xleftarrow{\$} (U,V)$ as follows.

$$\text{Alice corruption:}\quad \mathop{\mathbb{E}}_{(u,v)\xleftarrow{\$}(U,V)} \mathsf{SD}\left(\ \mathrm{Sim}_A(u)\ ,\ (X^n | f_n(X^n) = u, g_n(Y^n) = v)\ \right) \leq \nu(n)$$
$$\text{Bob corruption:}\quad \mathop{\mathbb{E}}_{(u,v)\xleftarrow{\$}(U,V)} \mathsf{SD}\left(\ \mathrm{Sim}_B(v)\ ,\ (Y^n | f_n(X^n) = u, g_n(Y^n) = v)\ \right) \leq \nu(n)$$

   Intuitively, the first constraint states that (on average) the conditional distribution $(X^n | f_n(X^n) = u, g_n(Y^n) = v)$ is independent of v, and the second constraint states that the conditional distribution $(Y^n | f_n(X^n) = u, g_n(Y^n) = v)$ is independent of u.
2. Consider a secure non-interactive simulation via reduction functions $\{f_n, g_n\}_{n\in\mathbb{N}}$ that has negligible insecurity, i.e., $\nu(n) = \mathsf{negl}(n)$. Then, using the fact that $\Pr[(U,V) = (u,v)]$ is either 0 or at least a constant, the security definition implies the following for every $(u,v) \in \mathrm{Supp}(U,V)$.

$$\mathsf{SD}\left(\ \mathrm{Sim}_A(u)\ ,\ (X^n | f_n(X^n) = u, g_n(Y^n) = v)\ \right) \leq \mathsf{negl}(n)$$
$$\mathsf{SD}\left(\ \mathrm{Sim}_B(v)\ ,\ (Y^n | f_n(X^n) = u, g_n(Y^n) = v)\ \right) \leq \mathsf{negl}(n)$$

3. Consider the non-interactive simulation of $\mathsf{BES}(\epsilon')$ from $\mathsf{BES}(\epsilon)^{\otimes 2}$, where $(1-\epsilon') = (1-\epsilon)^2$, with 0 insecurity. In this case we use the reduction function $f_2(x^2) = x_1^2 \oplus x_2^2$ and $g_2(y^2) = \perp$ if $y_1^2 = \perp$, or $y_2^2 = \perp$; otherwise, $g_2(y^2) = y_1^2 \oplus y_2^2$. Let us first visualize the entire joint distribution in Table 1. We illustrate the consequences of the security definition using the tables below. Consider the case of corrupt Alice in Table 2 and the case of corrupt Bob in Table 3.

		$v=0$		$v=\perp$					$v=1$	
		00	11	$0\perp$	$\perp 0$	$1\perp$	$\perp 1$	$\perp\perp$	01	10
$u=0$	00	$\frac{(1-\epsilon)^2}{4}$		$\frac{(1-\epsilon)\epsilon}{4}$	$\frac{\epsilon(1-\epsilon)}{4}$			$\frac{\epsilon^2}{4}$		
	11		$\frac{(1-\epsilon)^2}{4}$			$\frac{(1-\epsilon)\epsilon}{4}$	$\frac{\epsilon(1-\epsilon)}{4}$	$\frac{\epsilon^2}{4}$		
$u=1$	01			$\frac{(1-\epsilon)\epsilon}{4}$			$\frac{\epsilon(1-\epsilon)}{4}$	$\frac{\epsilon^2}{4}$	$\frac{(1-\epsilon)^2}{4}$	
	10				$\frac{\epsilon(1-\epsilon)}{4}$	$\frac{(1-\epsilon)\epsilon}{4}$		$\frac{\epsilon^2}{4}$		$\frac{(1-\epsilon)^2}{4}$

Table 1 Joint distribution induced by the reduction of $\mathsf{BES}(\epsilon')$ to $\mathsf{BES}(\epsilon)^{\otimes 2}$. Rows have elements in $\mathcal{X}^2 = \{0,1\}^2$, and columns have elements in $\mathcal{Y}^2 = \{0,1,\perp\}^2$. The (x^2, y^2)-th entry in this matrix represents the probability $\Pr\left[(X,Y)^{\otimes 2} = (x^2, y^2)\right]$, and no-entry implies that the probability is 0.

		$v=0$	$v=\perp$	$v=1$
$u=0$	00	$\frac{(1-\epsilon)^2}{4}$	$\frac{2\epsilon-\epsilon^2}{4}$	
	11	$\frac{(1-\epsilon)^2}{4}$	$\frac{2\epsilon-\epsilon^2}{4}$	
$u=1$	01		$\frac{2\epsilon-\epsilon^2}{4}$	$\frac{(1-\epsilon)^2}{4}$
	10		$\frac{2\epsilon-\epsilon^2}{4}$	$\frac{(1-\epsilon)^2}{4}$

Table 2 The case of corrupt Alice for the reduction of $\mathsf{BES}(\epsilon')$ to $\mathsf{BES}(\epsilon)^{\otimes 2}$. The table illustrates the joint distribution of (X^2, V). It suffices to let $\mathrm{Sim}_A(0)$ be the uniform distribution over $\{00, 11\}$, and $\mathrm{Sim}_A(1)$ be the uniform distribution over $\{01, 10\}$.

	$v=0$		$v=\perp$					$v=1$	
	00	11	$0\perp$	$\perp 0$	$1\perp$	$\perp 1$	$\perp\perp$	01	10
$u=0$	$\frac{(1-\epsilon)^2}{4}$	$\frac{(1-\epsilon)^2}{4}$	$\frac{(1-\epsilon)\epsilon}{4}$	$\frac{\epsilon(1-\epsilon)}{4}$	$\frac{(1-\epsilon)\epsilon}{4}$	$\frac{\epsilon(1-\epsilon)}{4}$	$\frac{2\epsilon^2}{4}$		
$u=1$			$\frac{(1-\epsilon)\epsilon}{4}$	$\frac{\epsilon(1-\epsilon)}{4}$	$\frac{(1-\epsilon)\epsilon}{4}$	$\frac{\epsilon(1-\epsilon)}{4}$	$\frac{2\epsilon^2}{4}$	$\frac{(1-\epsilon)^2}{4}$	$\frac{(1-\epsilon)^2}{4}$

Table 3 The case of corrupt Bob for the reduction of $\mathsf{BES}(\epsilon')$ to $\mathsf{BES}(\epsilon)^{\otimes 2}$. The table illustrates the joint distribution of (U, Y^2). It suffices to let $\mathrm{Sim}_B(0)$ be the uniform distribution over $\{00, 11\}$, $\mathrm{Sim}_B(1)$ be the uniform distribution over $\{01, 10\}$, and $\mathrm{Sim}_B(\perp)$ be the distribution that outputs $0\perp$, $1\perp$, $\perp 0$, and $\perp 1$ (each) with probability $\epsilon(1-\epsilon)/(4\epsilon - 2\epsilon^2)$, and outputs $\perp\perp$ with probability $2\epsilon^2/(4\epsilon - 2\epsilon^2)$.

3.1 Composition

In this section, we shall prove the sequential and parallel composition theorems for secure non-interactive joint simulations.

As a first step, we introduce a few notations. Suppose P, Q are joint distributions (X, Y) and (X', Y') on sample spaces $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{X}' \times \mathcal{Y}'$, respectively. The notation $(P\|Q)$ represents a joint distribution over the sample space $(\mathcal{X} \times \mathcal{X}') \times (\mathcal{Y} \times \mathcal{Y}')$ defined by the following procedure. Sample $(x, y) \overset{\$}{\leftarrow} (X, Y)$, sample $(x', y') \overset{\$}{\leftarrow} (X', Y')$, give the sample (x, x') to Alice and (y, y') to Bob.

For reduction functions, we shall need the following notation. Suppose $f_n \colon \Omega_1 \to \Omega_2$, and $f'_n \colon \Omega'_1 \to \Omega'_2$. The function $f_n \| f'_n$ is a function $\Omega_1 \times \Omega'_1 \to \Omega_2 \times \Omega'_2$ defined by the following mapping $(x, x') \mapsto (f_n(x), f'_n(x'))$.

We remark that, in the composition theorems below, the distribution $P, P'Q, Q'$, and R may depend on n itself.

▶ **Theorem 1** (Parallel Composition)**.** *For joint distributions P, P', Q, and Q', suppose we have*

$$P \sqsubseteq^{\nu(n)}_{f_n, g_n} Q \text{ and } P' \sqsubseteq^{\nu'(n)}_{f'_n, g'_n} Q'.$$

Then, the following holds.

$$(P\|P') \sqsubseteq^{\nu(n)+\nu'(n)}_{f_n\|f'_n,g_n\|g'_n} (Q\|Q').$$

Proof. Suppose the environment does not corrupt any party. Then, the bound follows from a hybrid argument.

Suppose the environment corrupts Alice. Let Sim_A and Sim'_A be the simulators for corrupt Alice for $P \sqsubseteq^{\nu(n)}_{f_n,g_n} Q$ and $P' \sqsubseteq^{\nu'(n)}_{f'_n,g'_n} Q'$, respectively. We consider the simulator $\mathrm{Sim}_A\|\mathrm{Sim}'_A$ for $(P\|P') \sqsubseteq^{\nu(n)+\nu'(n)}_{f_n\|f'_n,g_n\|g'_n} (Q\|Q')$. The result is immediate from a hybrid argument.

Similarly, when the environment corrupts Bob, the simulator $\mathrm{Sim}_B\|\mathrm{Sim}'_B$ serves as a the simulator for the composed reduction, where Sim_B and Sim'_B are simulators for corrupt Bob in the reductions $P \sqsubseteq^{\nu(n)}_{f_n,g_n} Q$ and $P' \sqsubseteq^{\nu'(n)}_{f'_n,g'_n} Q'$, respectively. ◀

We need one more notation for the sequential composition. Suppose $f_n\colon \Omega \to \Omega'$, and $f'_n\colon \Omega' \to \Omega''$. The function $f'_n \circ f_n$ is a function $\Omega \to \Omega''$ defined by the mapping $x \mapsto f'_n(f_n(x))$.

▶ **Theorem 2** (Sequential Composition). *For joint distribution P, Q, and R, suppose we have*

$$P \sqsubseteq^{\nu(n)}_{f_n,g_n} Q, \ \textit{and}\ Q \sqsubseteq^{\nu'(n)}_{f'_n,g'_n} R.$$

Then, the following holds.

$$P \sqsubseteq^{\nu(n)+\nu'(n)}_{f_n\circ f'_n,g_n\circ g'_n} R.$$

Proof. The only non-trivial case is when the environment corrupts one of the parties, say, Alice. Suppose Sim_A and Sim'_A be the simulators when Alice is corrupted by the environment in the reduction $P \sqsubseteq^{\nu(n)}_{f_n,g_n} Q$ and $Q \sqsubseteq^{\nu'(n)}_{f'_n,g'_n} R$. Then, the simulator $\mathrm{Sim}'_A \circ \mathrm{Sim}_A$ suffices to prove the security of the reduction $P \sqsubseteq^{\nu(n)+\nu'(n)}_{f_n\circ f'_n,g_n\circ g'_n} R$ using a hybrid argument. ◀

4 Secure Non-interactive Simulation from Binary Erasure Source

4.1 Impossibility of Simulating Binary Symmetric Source from Binary Erasure Source

We begin with a relatively simple proof that rules out the possibility of securely non-interactively simulating samples of $\mathsf{BSS}(\epsilon)$ from $\mathsf{BES}(\epsilon)^{\otimes n}$. We emphasize that this reduction is not ruled out by (insecure) non-interactive simulation literature and cryptography with one-way messages for *any* choice of ϵ, ϵ' parameters. This result highlights the crucial role that the notion of "security" plays in the proofs.

We begin by restating the Informal Theorem 1.

▶ **Theorem 3.** *Let $\epsilon' \in (0,1/2)$, and $\epsilon \in (0,1)$. For every infinite family of reduction functions $\{f_n, g_n\}_{n\in\mathbb{N}}$, insecurity bound $\nu(n) = o(n^{-3/2})$, and sufficiently large n, we have*

$$\mathsf{BSS}(\epsilon') \not\sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}.$$

Proof. First, we shall rule our all $\epsilon' \neq \epsilon/2$. Let $S_0 \subseteq \{0,1\}^n$ be the set of all $x^n \in \{0,1\}^n$ such that $f_n(x^n) = 0$. Similarly, $S_1 = \{0,1\}^n \setminus S_0$ be the set of all $x^n \in \{0,1\}^n$ such that $f_n(x^n) = 1$. Let $\partial S_0 \subseteq S_0$ be the elements whose neighbors on the boolean hypercube lie in S_1. Intuitively, ∂S_0 is the outermost shell of S_0 when embedded in the boolean hypercube. Analogously, define ∂S_1.

Without loss of generality, assume that $|\partial S_0| \leq |\partial S_1|$. By the isoperimetric inequality on the boolean hypercube, we know that $|\partial S_0| \geq \Theta(2^n/\sqrt{n})$, because $|S_0|$ is close to 2^{n-1}. Greedily match elements in ∂S_0 with elements in ∂S_1 such that the matched elements are neighbors in the boolean hypercube; there may be elements in ∂S_1 that are left unmatched. The matching is of size at least $\Theta\left(2^n/n^{3/2}\right)$ because every vertex in the hypercube has degree n.

Consider any $a^n \in \partial S_0$ and its matched neighbor $b^n \in \partial S_1$. Note that a^n and b^n differ in exactly one position. Consider any $y^n \in \{0,1,\perp\}^n$. We say that $a^n \vdash y^n$. (read, a^n is consistent with y^n) if for all $1 \leq i \leq n$ we have $y_i^n = \perp$ or $y_i^n = a_i^n$. Intuitively, $a^n \vdash y^n$ if it is possible to obtain y^n by passing a^n through an erasure channel.

Define the following sets.

$$\begin{aligned} T_0 &= \{y^n \colon y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \nvdash y^n\} \\ T_1 &= \{y^n \colon y^n \in \{0,1,\perp\}^n, a^n \nvdash y^n, b^n \vdash y^n\} \\ T_{\text{both}} &= \{y^n \colon y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \vdash y^n\} \end{aligned}$$

Note that T_0 is the set of all y^n such that the index where a^n and b^n differed survived, and it agrees with the entry in a^n. Similarly, the set T_1 is the set of all y^n such that the index where a^n and b^n differed survived, and it agrees with the entry in b^n. Finally, the set T_{both} is the set of all y^n such that the index where a^n and b^n differed was erased. Therefore, we conclude that $\Pr[Y^n \in T_0 | X^n = a^n] = (1-\epsilon)$, $\Pr[Y^n \in T_1 | X^n = b^n] = (1-\epsilon)$, and $\Pr[Y^n \in T_{\text{both}} | X^n = a^n] = \Pr[Y^n \in T_{\text{both}} | X^n = b^n] = \epsilon$.

Let $W_0 \subseteq \{0,1,\perp\}^n$ is the set of all entries $y^n \in \{0,1,\perp\}^n$ such that $g_n(y^n) = 0$. Similarly define $W_1 = \{0,1,\perp\}^n \setminus W_0$. Our objective is to *partition* T_0, T_{both}, and T_1 and allocate the elements to W_0 and W_1 such that the following constraints hold simultaneously.

1. $\Pr[Y^n \in W_0 | X^n = a^n] \approx (1-\epsilon')$, and $\Pr[Y^n \in W_1 | X^n = a^n] \approx \epsilon'$.
2. $\Pr[Y^n \in W_1 | X^n = b^n] \approx (1-\epsilon')$, and $\Pr[Y^n \in W_0 | X^n = b^n] \approx \epsilon'$.

Any deviation from these probabilities contribute to simulation error for corrupt Alice. Note that the simulation error (for corrupt Alice) shall be at least $\frac{1}{2}\left|\epsilon' - \frac{\epsilon}{2}\right|$ conditioned on $X^n \in \{a^n, b^n\}$. Therefore, the simulation error when $X^n \in \partial S_0 \cup \partial S_1$ is at least $\frac{1}{2}\left|\epsilon' - \frac{\epsilon}{2}\right| \cdot \Pr[X^n \in \partial S_0] \geq \Theta\left(|\epsilon - 2\epsilon'|/n^{3/2}\right) = \Theta\left(n^{-3/2}\right)$. Therefore, it is impossible to have $\nu(n) = o(n^{-3/2})$ insecurity.

At this point, we have ruled out secure non-interactive reduction for all $\epsilon' \neq \epsilon/2$. If possible let there exists a secure non-interactive simulation

$$\mathsf{BSS}(\epsilon/2) \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}.$$

Then, by parallel composition, we have

$$\mathsf{BSS}(\epsilon/2)^{\otimes 2} \sqsubseteq^{2\nu(n)}_{f_n \| f_n, g_n \| g_n} \mathsf{BES}(\epsilon)^{\otimes 2n}.$$

We know that $\mathsf{BSS}(\epsilon - \epsilon^2/2) \sqsubseteq^{0}_{\text{parity}_2,\text{parity}_2} \mathsf{BSS}(\epsilon/2)^{\otimes 2}$ using the parity reductions (refer to the results in Section 5). By sequential composition, we have

$$\mathsf{BSS}(\epsilon - \epsilon^2/2) \sqsubseteq^{2\nu(n)}_{f_n \oplus f_n, g_n \oplus g_n} \mathsf{BES}(\epsilon)^{\otimes 2n}.$$

Note that $\epsilon - \epsilon^2/2 \neq \epsilon/2$, for all $\epsilon \in (0,1)$. Therefore, we have shown the secure non-interactive simulation of $\mathsf{BSS}(\epsilon')$, for some $\epsilon' \neq \epsilon/2$, from samples of $\mathsf{BES}(\epsilon)$, which contradicts the first part of the proof. Consequently, our initial assumption that $\mathsf{BSS}(\epsilon/2) \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$ must be false.

This argument completes the proof ruling out all $\epsilon' \in (0,1/2)$. ◀

We emphasize that the case of corrupt Alice suffices to rule out all secure non-interactive simulation of a $\mathsf{BSS}(\epsilon')$ sample, where $\epsilon' \neq \epsilon/2$.

4.2 Binary Erasure Source: Feasibility and Rate

We start with restating the Informal Theorem 2 as follows.

▶ **Theorem 4** (Binary Erasure Channel: Feasibility & Rate). *Let $\epsilon', \epsilon \in (0,1)$. Suppose there exists an infinite family of reduction functions $f_n\colon \{0,1\}^n \to \{-1,1\}, g_n\colon \{0,1,\perp\}^n \to \{-1,0,1\}$, and insecurity bound $\nu(n) = o(1)$ such that $\mathsf{BES}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$ for infinitely many $n \in \mathbb{N}$. Then, the following holds:*

1. *There exists $n^* \in \mathbb{N}$ and an infinite family of reduction functions $f^*_n\colon \{0,1\}^n \to \{-1,1\}$, $g^*_n\colon \{0,1,\perp\}^n \to \{-1,0,1\}$ such that $\mathsf{BES}(\epsilon') \sqsubseteq^{0}_{f^*_n,g^*_n} \mathsf{BES}(\epsilon)^{\otimes n}$ for all $n \geq n^*$.*
2. *Furthermore, there exists $k \in [n^*]$ such that $(1-\epsilon') = (1-\epsilon)^k$, $f^*_n(x) = g^*_n(x)$, for all $x \in \{0,1\}^n$, and either f^*_n or $-f^*_n$ is the parity of a set of k input bits.*
3. *Moreover, if there exists an infinite family of functions $\{f_n, g_n\}_{n\in\mathbb{N}}$ and insecurity bound $\nu(n) = o(1)$ such that, for infinitely many $n \in \mathbb{N}$, we have $\mathsf{BES}(\epsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$. Then, we have $m(n) \leq n/k$.*

Before proving Theorem 4, we introduce some new notations that we will use in this section.

Let $A \subseteq [n]$, then define $y^n_A \in \{0,1,\perp\}^n$ as a string achieved from $y^n \in \{0,1,\perp\}^n$ by erasing all bits y^n_j for $j \in A$ and keeping all bits y^n_j for $j \notin A$. For example, if $y^6 = (0,1,\perp,1,\perp,0)$ then $y^6_{\{1,4,5\}} = (\perp,1,\perp,\perp,\perp,0)$. We call y^n_A as an erased version of y^n_A and y^n as a refined version of y^n_A. Moreover, we say that z^n is a complete refined version of y^n if $z^n \in \{0,1\}^n$ and it is a refined version of y^n. For example, if $y^5 = (0,\perp,1,1,\perp)$, then the set of all refined versions of y^5 is the following set:

$$\{(0,0,1,1,0),(0,1,1,1,0),(0,0,1,1,1),(0,1,1,1,1),$$
$$(0,\perp,1,1,0),(0,\perp,1,1,1),(0,0,1,1,\perp),(0,1,1,1,\perp)\}$$

while the set of all complete refined versions of y^5 is the following set:

$$\{(0,0,1,1,0),(0,1,1,1,0),(0,0,1,1,1),(0,1,1,1,1)\}$$

We call the set of all complete refined versions of y^n as the span of y^n and we denote it by $Sp(y^n)$. More formally, $Sp(y^n) = \{a^n \in \{0,1\}^n : a^n \vdash y^n\}$. For instance, if $y^5 = (0,\perp,1,1,\perp)$, then

$$Sp(y^5) = \{(0,0,1,1,0),(0,1,1,1,0),(0,0,1,1,1),(0,1,1,1,1)\}$$

Suppose $(X^n, Y^n) \sim \mathsf{BES}(\epsilon)^{\otimes n}$ (Y^n denotes the distribution of the output of the channel $\mathsf{BES}(\epsilon)^{\otimes n}$ when the input string is chosen uniformly at random i.e. $X^n \sim U_{\{0,1\}^n}$). For each $y^n \in \{0,1,\perp\}^n$, we define $M(y^n)$ as the uniform distribution over $Sp(y^n)$ (the set of all $a^n \in \{0,1\}^n$ such that a^n is consistent with y^n i.e. $a^n \vdash y^n$).

For example, when $n = 4$ and $y^4 = 01\perp\perp$, $M(y^4)$ denotes the uniform distribution over the set $Sp(y^4) = \{0100, 0101, 0110, 0111\}$. For each $x^n \in \{0,1\}^n$, let $Q_\epsilon(x^n)$ denotes the conditional distribution over $\{0,1,\perp\}^n$ when the input is x^n. We also use P_ϵ to denote the marginal distribution of Y^n over $\{0,1,\perp\}^n$.

Note that we choose the range of reduction function f_n to be $\{-1,1\}$ and the range of g_n to be $\{-1,0,1\}$, so we can rewrite the three conditions of the definition of secure non-interactive simulation, mentioned in Section 3, for BES as the following algebraic constraints.

From our discussion in Section 3, it follows from $\mathsf{BES}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$ the following three conditions:

1. Correctness: Assuming $(X^n, Y^n) \sim \mathsf{BES}(\epsilon)^{\otimes n}$, we have:

$$\mathsf{SD}\left((f_n(X^n), g_n(Y^n)), (U, V)\right) \leq \nu(n)$$

   which imply $\mathbb{E}_{x^n \sim U_{\{0,1\}^n}}[f_n(x^n)] \leq \nu(n)$, and $\mathbb{E}_{y^n \sim P_\epsilon}[g_n(y^n)] \leq \nu(n)$.
2. Bob security: $\mathbb{E}_{x^n \sim U_{\{0,1\}^n}} \left| E_{y^n \sim Q_\epsilon(x^n)} g_n(y^n) - (1-\epsilon') f_n(x^n) \right| \leq \nu(n)$.
3. Alice security: $\mathbb{E}_{y^n \sim P_\epsilon} \left| \mathbb{E}_{x^n \sim M(y^n)} f_n(x^n) - g_n(y^n) \right| \leq \nu(n)$.

Intuitively, the correctness implies that Alice can partition the set $\{0,1\}^n$ into two sets S_0, S_1 of (roughly) equal size such that whenever she gets $x^n \in S_i$, she outputs i for $i \in \{0,1\}$, and Bob can partition the set $\{0,1,\perp\}^n$ into 3 sets $T_0, T_1, T_\perp$ such that $\Pr[y^n \in T_0]$, and $\Pr[y^n \in T_1]$ are almost equal and whenever he gets $y^n \in T_j$, he outputs j. Alice security implies that if Bob receives some $y^n \in T_i$ for $i \in \{0,1\}$, then most of x^n consistent with y^n must belong to S_i, and if $y^n \in T_\perp$, (roughly) half of them must belong to S_0 and the other half must belong to S_1.

We show in Lemma 1 that when we have perfect security (the case that $\nu(n) = 0$), Alice's reduction function f_n must be a linear function and there exists some $k \in [n]$ such that $1 - \epsilon' = (1-\epsilon)^k$.

▶ **Lemma 1.** *Let n be a positive integer. Suppose $\mathsf{BES}(\epsilon') \sqsubseteq^{0}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$ for some functions $f_n \colon \{0,1\}^n \to \{-1,1\}$ and $g_n \colon \{0,1,\perp\}^n \to \{-1,0,1\}$. Then, there exists $S \subseteq [n]$ such that $f_n(x^n) = \chi_S(x^n)$ for all $x^n \in \{0,1\}^n$. Moreover, $g_n(y^n) = \chi_S(y^n)$ if $y^n_i \neq \perp$ for all $i \in S$, otherwise if there exists at least $j \in S$ such that $y^n_j = \perp$, then $g_n(y^n) = 0$. Finally, we have $(1-\epsilon') = (1-\epsilon)^k$ where $|S| = k$.*

We shall present two proofs for this lemma. The first one is a combinatorial proof while the second one is a proof in which Fourier analysis is used. We use Claim 1 to prove *Lemma* 1. We define $S_i = \{x^n \in \{0,1\}^n : f_n(x^n) = i\}$ for $i \in \{-1,1\}$ and $T_j = \{y^n \in \{0,1,\perp\}^n : g_n(y^n) = j\}$ for $j \in \{-1,0,1\}$.

▶ **Claim 1.** *Suppose $\mathsf{BES}(\epsilon') \sqsubseteq^{0}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$ for $\epsilon \leq \frac{1}{2}$, then $S_0 \subseteq T_{+1}$ and $S_1 \subseteq T_{-1}$.*

Proof. Based on definition of security, we have

$$\mathop{\mathbb{E}}_{y^n \sim P_\epsilon} \left| \mathop{\mathbb{E}}_{x^n \sim M(y^n)} f_n(x^n) - g_n(y^n) \right| \leq \nu(n).$$

Fix $y^n \in \{0,1\}^n$, then $\mathbb{E}_{x^n \sim M(y^n)} f_n(X^n) = f_n(y^n)$ because for $y^n \in \{0,1\}^n$, we know that $\Pr[X^n = y^n | Y^n = y^n] = 1$ according to the distribution of $\mathsf{BES}(\epsilon)^{\otimes n}$. This implies that $\mathbb{E}_{y^n \sim P_\epsilon}[|f_n(y^n) - g_n(y^n)|\,|y^n \in \{0,1\}^n] \leq \frac{\nu(n)}{\Pr[y^n \in \{0,1\}^n]} = \frac{\nu(n)}{2^n \times (1-\epsilon)^n} \leq \nu(n)$. In case of perfect secrecy $\nu(n) = 0$ which implies that $f_n(y^n) = g_n(y^n)$ for any $y^n \in \{0,1\}^n$. This completes the proof. ◀

Now, we start proving Lemma 1:

Perfect security implies linearity of f_n. Recall from Subsection 2.3 that $f_{J_{y^n}|z_{y^n}} : \{0,1\}^{|J_{y^n}|} \to \mathbb{R}$ denotes the restriction of f_n to J_{y^n} when the coordinates in $\bar{J}_{y^n}$ are fixed to be equal to the non erased bits of y^n, denoted by the string z_{y^n}. More precisely, for each $y^n \in \{0,1,\perp\}$, we define $J_{y^n} = \{i \in [n] \colon y^n_i = \perp\}^n$ and z_{y^n} is the concatenation of all non-bot (non erased) symbols in y^n. For example, when $y^4 = 01\perp\perp$, $J_{y^4} = \{3,4\}$ and

$z_{y^4} = 01$. Since J_{y^n} and z_{y^n} are well defined for any $y^n \in \{0,1,\perp\}^n$, we use f_{y^n} instead of $f_{J_{y^n}|z_{y^n}}$.

The condition on Bob security implies that $\widehat{f_{y^n}}(\emptyset) = \mathbb{E}_{x^n \sim M(y^n)} f_n(x^n)$ must agree with $g_n(y^n)$ on every input $y^n \in \{0,1,\perp\}^n$. This implies that $\widehat{f_{y^n}}(\emptyset)$ is always 0, 1, or -1 for any y^n. Note that for $y^n = \perp\perp\ldots\perp$, we have $\widehat{f_{y^n}}(\emptyset) = \mathbb{E}_{x^n \sim U_{\{0,1\}^n}} f_n(x^n) = 0$ due to correctness and for any $y^n \in \{0,1\}^n$, $\widehat{f_{y^n}}(\emptyset) \in \{-1,1\}$ based on Claim 1 (refer to Observation 1).

This implies that there exists some $S \subseteq [n]$ and $z^n \in \{0,1,\perp\}^n$ such that $J_{z^n} = S$ and $\widehat{f_{z^n}}(\emptyset) \neq 0$ but $\widehat{f_{y^n}}(\emptyset) = 0$ for any $y^n \in \{0,1,\perp\}^n$ such that $S \subsetneq J_{y^n}$.

For each permutation π of $(1,2,\ldots,n)$, we construct a complete binary tree of height n inductively as follows. We call this tree T_π.

1. Let $\widehat{f_{\perp\perp\ldots\perp}}(\emptyset) = \widehat{f}(\emptyset)$ be the root.
2. For each node $\widehat{f_{y^n}}$ at level i, create two children $\widehat{f_{y^{(l)}}}(\emptyset)$ and $\widehat{f_{y^{(r)}}}(\emptyset)$, where $y_j^{(l)} = y_j^{(r)} = y_j^n$ for every $j \neq \pi(i+1)$, and $y_{\pi(i+1)}^{(l)} = 0$, and $y_{\pi(i+1)}^{(r)} = 1$.

In *Figure* 1, an example of the complete binary tree corresponding to the permutation $\pi(i) = i$ for every $i \in [n]$, has been provided. Note that there are exactly $n!$ of such binary trees corresponding to $n!$ different permutations.

▶ **Observation 1.** For each leaf $y \in \{0,1\}^n$ in any tree T_π, we have $\widehat{f_y}(\emptyset) \in \{1,-1\}$.

Proof. This is true according to Claim 1. ◀

▶ **Observation 2.** For each π, each internal node in T_π is the average of its children, so T_π corresponds to a martingale.

Proof. This is can be seen by applying the law of total expectation:

$$\widehat{f_{y^n}}(\emptyset) = \mathop{\mathbb{E}}_{x^n \sim M(y^n)} f_n(x^n) = \frac{1}{2} \times \mathop{\mathbb{E}}_{x^n \sim M(y^{(l)})} f_n(x^n) + \frac{1}{2} \times \mathop{\mathbb{E}}_{x^n \sim M(y^{(r)})} f_n(x^n)$$

◀

▶ **Observation 3.** For any $y \in \{0,1,\perp\}^n$, the value $\widehat{f_y}(\emptyset)$ appears in exactly $k!(n-k)!$ trees, where k is the number of non-erased bits in y.

In the perfect security case, for every $y^n \in \{0,1,\perp\}^n$, we have $\widehat{f_{y^n}}(\emptyset) = g(y^n)$. This together with Observation 1, imply that there exists $y^n \in \{0,1,\perp\}^n$ such that $\widehat{f_y}(\emptyset) = g(y) = 1$ or -1. Let $y^n \in \{0,1,\perp\}^n$ be an string with the minimum number of non-erased bits such that $\widehat{f_{y^n}}(\emptyset) \neq 0$. Without loss of generality, we can assume that $g(y^n) = \widehat{f_{y^n}}(\emptyset) = 1$ and let k be the number of non-erased bits of such y^n. Recall that $J_{y^n} = \{i \in [n] \colon y_i^n = \perp\}$ and z_{y^n} is the concatenation of all non-bot symbols in y^n.

▶ **Claim 2.** *Let $y^n \in \{0,1,\perp\}^n$ be a string with the minimum number of non-erased bits such that $\widehat{f_{y^n}}(\emptyset) \neq 0$. For every $z^n \in \{0,1,\perp\}^n$ such that $J_{z^n} = J_{y^n}$ it holds that $\widehat{f_{z^n}}(\emptyset) \in \{1,-1\}$.*

Proof. Suppose that $|\bar{J}_{y^n}| = k$. Let A_{y^n} denote the set of all $z^n \in \{0,1,\perp\}^n$ such that $J_{y^n} = J_{z^n}$. We assign each string in A_{y^n} to some node of the sub-cube Q_k such that there is an edge between two nodes in Q_k if and only if the Hamming distance between the corresponding two strings is exactly 1. We know that Q_k has a Hamiltonian cycle and so it has a Hamiltonian path starting from node y^n. Let $y^{(1)}, y^{(2)}, \ldots, y^{(2^k)}$ (to make our notation simpler, we drop n from $y^{(j)}$'s) be that Hamiltonian path where $y^{(1)} = y^n$. Note that for each j, $y^{(j)}$ and $y^{(j+1)}$ are different in exactly one element and there exists at least one tree

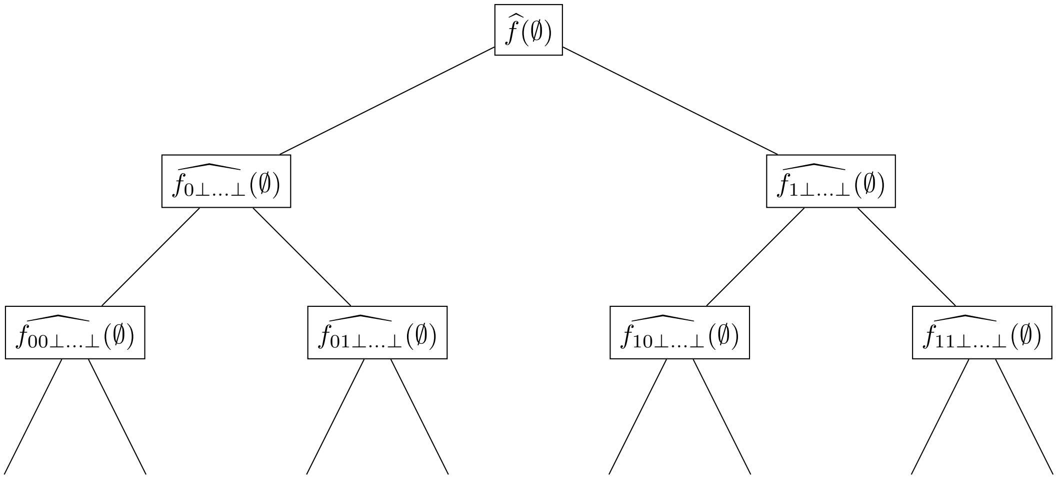
$\widehat{f}(\emptyset)$
$\widehat{f_{0\perp\ldots\perp}}(\emptyset)$
$\widehat{f_{1\perp\ldots\perp}}(\emptyset)$
$\widehat{f_{00\perp\ldots\perp}}(\emptyset)$
$\widehat{f_{01\perp\ldots\perp}}(\emptyset)$
$\widehat{f_{10\perp\ldots\perp}}(\emptyset)$
$\widehat{f_{11\perp\ldots\perp}}(\emptyset)$

Figure 1 The first two levels of the tree corresponding to the permutation $1, 2, 3, \ldots, n$

T_π such that these two nodes are siblings at level k, so if z^n denotes the parent of these two nodes in T_π, we have $\frac{1}{2} \times \widehat{f_{y^{(j)}}}(\emptyset) + \frac{1}{2} \times \widehat{f_{y^{(j+1)}}}(\emptyset) = \widehat{f_{z^n}}(\emptyset)$, but since $|J_{z^n}| = k-1$, $\widehat{f_{z^n}}(\emptyset) = 0$ which implies that $\widehat{f_{y^{(j)}}}(\emptyset) = -\widehat{f_{y^{(j+1)}}}(\emptyset)$ for each j. Since $\widehat{f_{y^{(1)}}}(\emptyset) = \widehat{f_{y^n}}(\emptyset) = 1$ it follows that $\widehat{f_{z^n}}(\emptyset) \in \{1, -1\}$ for any $z^n \in A_{y^n}$. ◀

We can use combinatorial argument or Fourier analysis to complete the proof of Lemma 1.

Combinatorial argument for perfect security: In the last step of the proof of Claim 2, we are assigning $+1$ and -1 to all nodes in the same level of the trees T_π such that the values assigned to any two neighbour nodes on the sub-cube Q_k, must be different(one of them is $+1$ and the other is -1). We know that Q_k is a bipartite graph and has a Hamiltonian cycle. Neighbours on this cycle belong to different two parts of this bipartite graph. This means that the parity of weight of (the number of bits 1 of) the nodes on this cycle are different. According to the proof of Claim 2, perfect security implies that there exists a level k such that the values of g for the nodes y^n at this level are $+1$ or -1 and for all nodes (or strings) with the same parity the value of g is the same. In perfect security, whenever the value of a node on a tree T_π is $+1$ or -1, then all the descendants of that node are $+1$ or -1 respectively. This implies that g is a linear function of the k bits in the set $\bar{J}_{y^n}$ such that $g_n(z^n) = (-1)^{\sum_{j \in \bar{J}_{y^n}} z_j^n}$ for each $z^n \in \{0, 1, \perp\}^n$ that $z_j^n \neq \perp$ for $j \in \bar{J}_{y^n}$ and $g_n(z^n) = 0$ if there exists at least an index $j \in \bar{J}_{y^n}$ such that $z_j^n = \perp$. This means that in the simulated source a simulated bit is not erased if and only if all the bits with indices in the set $\bar{J}_{y^n}$ are not erased; this happens with probability $(1-\epsilon)^{|\bar{J}_{y^n}|} = (1-\epsilon)^k$, so $1 - \epsilon' = (1-\epsilon)^k$.

Since in perfect security for each string $y^n \in \{0,1\}^n$, $f(y^n) = g(y^n)$ (refer to Claim 1), it implies that f is linear on its domain.

Proof of perfect security by Fourier analysis: By using Claim 2 and equation $\mathbb{E}_z[\widehat{f_{J|z}}(S)^2] = \sum_{T \subseteq \bar{J}} \widehat{f}(S \cup T)^2$, we have

$$\sum_{T \subseteq \bar{J}_{y^n}} \widehat{f}(T)^2 = \mathbb{E}\,\widehat{f_{y^n}}(\emptyset)^2 = 1. \tag{1}$$

By the way that we choose y^n, it must be the case that $\widehat{f_{z^n}}(\emptyset) = 0$ for every $z^n \in \{0, 1, \perp\}^n$ such that $|J_{z^n}| > |J_{y^n}| = n - k$. Again applying the same equation, for all previous levels

$1, 2, \ldots, k-1$ of the $k! \times (n-k)!$ different trees, we get the following:

$$\sum_{T \subseteq S} \widehat{f}(T)^2 = \mathbb{E}\, \widehat{f_{y'}}(\emptyset)^2 = 0 \text{ for every } S \subsetneq \bar{J}_{y^n}.$$

This implies that $\widehat{f}(S) = 0$ for every $S \subsetneq \bar{J}_{y^n}$. Now, from equation 1, we can conclude that $\widehat{f}(\bar{J}_{y^n})^2 = 1$, which means that f is a linear function.

So far, we have given a necessary condition for perfectly secure non-interactive simulation of $\mathsf{BES}(\epsilon')$ from $\mathsf{BES}(\epsilon)$. In Lemma 2, we present a perfectly secure protocol which realizes the necessary conditions.

▶ **Lemma 2.** *Let $\epsilon \in (0,1)$ and k be some positive integer. Let n be a positive integer such that $n \geq k$. Let $f_n = \chi_S$ be a linear function, where $S \subseteq [n]$ and $|S| = k$. We define $g_n \colon \{0,1,\perp\}^n \to \{-1,0,1\}$ as following.*

$$g_n(y^n) = \begin{cases} 0 & \text{if } \exists i \in S \text{ such that } y_i^n = \perp \\ \chi_S(y^n) & \text{otherwise.} \end{cases}$$

Then, we have $\mathsf{BES}(\epsilon') \sqsubseteq^0_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$, where $\rho' = 1 - \epsilon' = (1-\epsilon)^k = \rho^k$.

Proof. The value $g_n(y^n)$ is equal to 0 if and only if there exists at least an index i such that $y_i^n = \perp$. So, we have the following:

$$\begin{aligned} \Pr[g_n(y^n) = 0] &= \Pr[\exists i \in S \text{ such that } y_i^n = \perp] = 1 - \Pr[\forall i \in S, y_i^n \neq \perp] \\ &= 1 - \prod_{i \in S} \Pr[y_i^n \neq \perp] = 1 - \prod_{i \in S} (1 - Pr[y_i^n = \perp]) \\ &= 1 - (1-\epsilon)^{|S|} = 1 - (1-\epsilon)^k \end{aligned}$$

Since whenever $g_n(y^n) \neq \perp$, we have $g_n(y^n) = f_n(y^n)$, we conclude that the given construction simulates $\mathsf{BES}(\epsilon')$ where $\epsilon' = \Pr[g_n(y^n) = 0] = 1 - (1-\epsilon)^k$. We need to prove that it is perfectly secure. For each x^n,

$$\mathop{\mathbb{E}}_{y^n \sim Q_\epsilon(x^n)} g_n(y^n) = (1-\epsilon)^k \times f_n(x^n) + (1 - (1-\epsilon)^k) \times 0 = (1-\epsilon') f_n(x^n)$$

and for each $y^n \in \{0,1,\perp\}^n$ such that for each $i \in S$, $y_i^n \neq \perp$,

$$\mathop{\mathbb{E}}_{x^n \sim M(y^n)} f_n(x^n) = f_n(y^n) = g_n(y^n)$$

and for each $y^n \in \{0,1,\perp\}^n$ such that for at least an index $i \in S$, $y_i^n = \perp$, we have:

$$\mathop{\mathbb{E}}_{x^n \sim M(y^n)} f_n(x^n) = \mathop{\mathbb{E}}_{x^n \sim M(y^n)} \chi_S(x^n) = 0.$$

This completes the proof. ◀

We shall first prove some useful claims and then complete the proof of Theorem 4.

▶ **Claim 3.** *We have*

$$\mathop{\mathbb{E}}_{x^n \sim U_{\{0,1\}^n}} \left| \mathop{\mathbb{E}}_{y^n \sim Q_\epsilon(x^n)} \mathop{\mathbb{E}}_{z^n \sim M(y^n)} f_n(z^n) - (1-\epsilon') f_n(x^n) \right| \leq 2\nu(n).$$

Proof. By triangle inequality we have

$$\begin{aligned}
&\mathop{\mathbb{E}}_{x^n\sim U_{\{0,1\}^n}}\left|\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)}\mathop{\mathbb{E}}_{z^n\sim M(y^n)} f_n(z^n)-(1-\epsilon')f_n(x^n)\right|\\
&\overset{\text{(i)}}{\leq}\mathop{\mathbb{E}}_{x^n\sim U_{\{0,1\}^n}}\left|\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)}\mathop{\mathbb{E}}_{z^n\sim M(y^n)} f_n(z^n)-\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)} g_n(y^n)\right|+\\
&\quad\mathop{\mathbb{E}}_{x^n\sim U_{\{0,1\}^n}}\left|\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)} g_n(y^n)-(1-\epsilon')f_n(x^n)\right|\\
&\overset{\text{(ii)}}{\leq}\mathop{\mathbb{E}}_{x^n\sim U_{\{0,1\}^n}}\left|\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)}\mathop{\mathbb{E}}_{z^n\sim M(y^n)} f_n(z^n)-\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)} g_n(y^n)\right|+\nu(n)\\
&\overset{\text{(iii)}}{\leq}\mathop{\mathbb{E}}_{x^n\sim U_{\{0,1\}^n}}\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)}\left|\mathop{\mathbb{E}}_{z^n\sim M(y^n)} f_n(z^n)-g_n(y^n)\right|+\nu(n)\\
&\overset{\text{(iv)}}{=}\mathop{\mathbb{E}}_{y^n\sim P_\epsilon}\left|\mathop{\mathbb{E}}_{z^n\sim M(y^n)} f_n(z^n)-g_n(y^n)\right|+\nu(n)\\
&\overset{\text{(v)}}{\leq}\nu(n)+\nu(n)\\
&=2\nu(n)
\end{aligned}$$

In above, inequalities (i) and (iii) are true due to triangle inequality. Inequalities (ii) and (v) are implied by Bob security and Alice security respectively. Equality (iv) is due to the definitions of distributions P_ϵ and Q_ϵ: drawing y^n from marginal distribution P_ϵ of the distribution $(x^n,y^n)\sim\mathsf{BES}(\epsilon)^{\otimes n}$ is equivalent to drawing x^n uniformly at random and then drawing y^n from conditional distribution $Q_\epsilon(\epsilon)$ induced by the distribution $(x^n,y^n)\sim\mathsf{BES}(\epsilon)^{\otimes n}$. ◀

Recall that the noise operator is defined as $\mathsf{T}_\rho(f_n)(x^n)=\mathbb{E}_{y^n\sim N_\rho(x^n)} f_n(y^n)$.

▶ **Claim 4.** *Let $\rho=1-\epsilon$, then we have*

$$\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)}\mathop{\mathbb{E}}_{z^n\sim M(y^n)} f_n(z^n)=\mathsf{T}_\rho(f_n)(x^n).$$

Proof. Fix $x^n\in\{0,1\}^n$. Drawing y^n from the distribution $Q_\epsilon(x^n)$ and then drawing z^n from the distribution $M(y^n)$ is equivalent to the following experiment: Erase each bit x_i^n with probability ϵ and do not erase it with probability $1-\epsilon$ to get y_i^n. Now, if $y_i^n\neq\perp$ (which means that $y_i^n=x_i^n$), then $z_i^n=y_i^n$ (so $z_i^n=x_i^n$), otherwise $z_i^n=0$ with probability $\frac{1}{2}$. This means that for each x_i^n, we have

$$\begin{aligned}
\Pr[z_i^n=x_i^n]&=\Pr[z_i^n=x_i^n|y_i^n=x_i^n]\Pr[y_i^n=x_i^n]+\Pr[z_i^n=x_i^n|y_i^n=\perp]\Pr[y_i^n=\perp]\\
&=1\times(1-\epsilon)+\frac{1}{2}\times\epsilon=1-\frac{\epsilon}{2}
\end{aligned}$$

And so $\Pr[z_i^n=1-x_i^n]=\frac{\epsilon}{2}$. This completes the proof. ◀

▶ **Claim 5.** *Let $f_n\colon\{0,1\}^n\to\{-1,1\}$. Suppose that*

$$\mathop{\mathbb{E}}_{x^n\sim U_{\{0,1\}^n}}|\mathsf{T}_\rho(f_n)(x^n)-\rho' f_n(x^n)|\leq 2\nu(n).$$

Then, there exists $k(n)\in[n]$ such that $\left|\rho'-\rho^{k(n)}\right|\leq(50\cdot\nu(n))^{1/4}$.

Proof. This claim can be easily verified by using Claim 8 for $\delta=2\nu(n)$. We will prove Claim 8 in the next section. ◀

Proof of Theorem 4: It follows from Lemma 5 (proved in the next section) and Claim 5 that $\rho' = \rho^k$ for some integer k. This completes the proof of the second part of Theorem 4. So we know that there exists integer k such that $\rho' = \rho^k$. Moreover, we have shown a perfectly secure construction in Lemma 2 such that $\rho' = \rho^k$ and we also proved that if we have perfect security, then the only construction is parity. This completes the proof of the first part. Finally, we present a proof for the third part of Theorem 4 in the following.

Upper bound on the rate. Observe that for any n, if $\mathsf{BES}(\epsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$, there exists reduction functions f_n^*, g_n^* such that $\mathsf{BES}(\epsilon')^{\otimes s(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$ for any $s(n) \leq m(n)$. In particular for $s(n) = 1$, if we just look at the first bit of the $m(n)$ bits $a_1, \dots, a_{m(n)}$ output by function f_n^*, we realize that $\mathsf{BES}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$. Now, according to the first part and second part of Theorem 4, for sufficiently large n, there exists some $k \in [n^*]$ such that $(1-\epsilon') = (1-\epsilon)^k$ and also a subset of size k of the n bits $x_1, \dots, x_n$ whose parity determines the first bit simulated by Alice a_1. This is also true for each bit a_i. Now, suppose $m(n) \geq n/k$, there exists at least two subsets of size k of the n bits given to Alice whose intersection is not empty. Without loss of generality, assume that $x_1, \dots, x_k$ determines the first bit a_1 and $x_{k+1}, \dots, x_{2k}$ determines the second bit a_2. Notice that whenever x_k is $\perp$, both a_1 and a_2 are $\perp$. This implies that the distribution of a_1 and a_2 is not independent which is a contradiction.

5 Simulation of BSS from BSS

In this section, we shall present our results for secure non-interactive simulation from binary symmetric source, including both feasibility and rate results as in the Informal Theorem 3. We begin with restating it formally as follows.

▶ **Theorem 5** (Binary Symmetric Source to Binary Symmetric Source). *Let $\epsilon, \epsilon' \in (0, 1/2)$. Suppose there exists a family of reduction functions $f_n, g_n \colon \{0,1\}^n \to \{-1,1\}$ for infinitely many $n \in \mathbb{N}$ and security bound $\nu(n)$ such that $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ and $\lim_{n\to\infty} \nu(n) = 0$. Then, the following holds:*

1. *There exists $n^* \in \mathbb{N}$ and an infinite family of functions $\{f_n^*, g_n^*\}_n$ such that $\mathsf{BSS}(\epsilon') \sqsubseteq^{0}_{f_n^*,g_n^*} \mathsf{BSS}(\epsilon)^{\otimes n}$ for all $n \geq n^*$.*
2. *Furthermore, there exists $S \subseteq [n]$ such that for every $n \geq n^*$, $f_n^* = g_n^* = \chi_S$, where χ_S is the characteristic function. Moreover, $\rho' = \rho^k$ where $k = |S|$.*

We begin with some notations and terminology that will use in this section. We denote $\rho = 1 - 2\epsilon$ and $\rho' = 1 - 2\epsilon'$. We say that two functions are close if they agree on most of the inputs, more concretely, for functions with the range over $\{-1, 1\}$, they are close if their inner product is close to 1. Recall that T_ρ is the linear noise operator. It takes as input a function, for example $f \colon \{0,1\}^n \to \{-1,1\}$, and returns a function $\mathsf{T}_\rho(f) \colon \{0,1\}^n \to \mathbb{R}$. We state and prove all the lemmas that are needed for the proof of Theorem 5.

First the three conditions for secure non-interactive simulation $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ can be algebraized as follows.

▶ **Lemma 3.** *Let n be any positive integer, and let $\epsilon', \epsilon \in (0, 1/2)$. Suppose $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ for some functions $f_n, g_n \colon \{0,1\}^n \to \{-1,1\}$ and $\nu(n) \geq 0$. Then, the following holds*

1. *Correctness: $\mathbb{E}[f_n(x^n)] \leq \nu(n)$, $\mathbb{E}[g_n(x^n)] \leq \nu(n)$, and $|\mathbb{E}\left[f_n(x^n) \cdot g_n(y^n)\right] - \rho'| \leq \nu(n)$, where $(x^n, y^n) \overset{\$}{\leftarrow} \mathsf{BSS}(\epsilon)^{\otimes n}$.*

2. *Alice security:* $\mathbb{E}_{y^n \sim U_{\{0,1\}^n}} \left|\mathsf{T}_\rho(f_n)(y^n) - \rho' \cdot g_n(y^n)\right| \leq \nu(n)$.
3. *Bob security:* $\mathbb{E}_{x^n \sim U_{\{0,1\}^n}} \left|\mathsf{T}_\rho(g_n)(x^n) - \rho' \cdot f_n(x^n)\right| \leq \nu(n)$.

Proof. Basically, this lemma follows from the discussions as mentioned in Section 3. We describe some intuition here. Recall that for binary symmetric source $\mathsf{BSS}(\epsilon)$ each bit is flipped with probability ϵ, in other words, for each sample $(x, y) \xleftarrow{\$} \mathsf{BSS}(\epsilon)$, the bits x and y are ρ-correlated. By choosing the range of the two functions f_n, g_n appropriately, that is $\{-1, 1\}$, we can rewrite the three conditions for the secure non-interactive simulation $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ nicely. More concretely, the condition for the no corruption case, that is,

$$\mathsf{SD}\left((f_n(X^n), g_n(Y^n)), (U, V)\right) \leq \nu(n)$$

implies that $\mathbb{E}[f_n] \leq \nu(n)$, $\mathbb{E}[g_n] \leq \nu(n)$, and $|\mathbb{E}[f_n(X^n) \cdot g_n(Y^n) - \rho'| \leq \nu(n)]$ by simple applications of triangle inequalities. Next, the condition for corrupt Alice

$$\mathop{\mathbb{E}}_{(u,v) \xleftarrow{\$} \mathsf{BSS}(\epsilon')} \mathsf{SD}\left(\ \mathrm{Sim}_A(u)\ ,\ (X^n | f_n(X^n) = u, g_n(Y^n) = v)\ \right) \leq \nu(n),$$

implies that on average the conditional distribution $(X^n | f_n(X^n) = u, g_n(Y^n) = v)$ is independent of v. Let S_0 be the set of all entries $x^n \in \{0,1\}^n$ such that $f_n(x^n) = 1$ and S_1 be the set of all entries $x^n \in \{0,1\}^n$ such that $f_n(y^n) = -1$. We define T_0 and T_1 similarly for g_n. Then, we have

$$\Pr[Y^n \in T_0 | X^n = x^n] \approx 1 - \epsilon' \text{ and} \Pr[Y^n \in T_1 | X^n = x^n] \approx \epsilon' \text{ for every } x^n \in S_0.$$

This implies that

$$\Pr[Y^n \in T_0 | X^n = x^n] - \Pr[Y^n \in T_1 | X^n = x^n] \approx 1 - 2\epsilon' \text{ for every } x^n \in S_0,$$

or equivalently, $\mathsf{T}_\rho(g_n)(x^n) \approx \rho' f_n(x^n)$ for every $x^n \in S_0$. Similarly, we have $\mathsf{T}_\rho(g_n)(x^n) \approx \rho' f_n(x^n)$ for every $x^n \in S_1$. Therefore, we have

$$\mathop{\mathbb{E}}_{x^n \sim U_{\{0,1\}^n}} \left|\mathsf{T}_\rho(g_n)(x^n) - \rho' \cdot f_n(x^n)\right| \leq \nu(n).$$

Analogously, the other security condition also holds. ◀

Next, we state and prove our main technical lemma of this section. Briefly, using the fact that the function $\mathsf{T}_\rho(f_n)$ is close to $\rho' g_n$ and that the function $\mathsf{T}_\rho(g_n)$ is close to $\rho' f_n$, it must be the case that the two functions f_n and g_n are also close. This together with the fact that f_n is $\{-1, 1\}$-valued function imply that the function $\mathsf{T}_\rho(f_n)$ is close to the function $\rho' f_n$ that allows us to conclude that ρ' is close to $\rho^{k(n)}$ for some $k(n) \in [n]$.

▶ **Lemma 4.** *Let n be any positive integer, and let $\epsilon', \epsilon \in (0, 1/2)$. Suppose $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ for some functions $f_n, g_n \colon \{0,1\}^n \to \{-1, 1\}$ and $\nu(n) \geq 0$. Then, f_n and g_n agree on most of the inputs $x^n \in \{0,1\}^n$, that is, $\langle f_n, g_n \rangle \geq 1 - \frac{5\sqrt{\nu(n)}}{2\rho'}$. Furthermore, there exists $k(n) \in [n]$ such that*

$$\left|\rho' - \rho^{k(n)}\right| \leq \sqrt{5}\left(\nu(n) + 5\sqrt{\nu(n)}\right)^{1/4}.$$

We prove the following claims that are needed for the proof of Lemma 4.

▶ **Claim 6.** *For any functions $f, g \colon \{0,1\}^n \to \mathbb{R}$, and any $\rho > 0$, the following holds*

$$\frac{\langle f, \mathsf{T}_\rho f \rangle + \langle g, \mathsf{T}_\rho g \rangle}{2} \geq |\langle f, \mathsf{T}_\rho g \rangle| = |\langle g, \mathsf{T}_\rho f \rangle|$$

Proof. Recall that $\widehat{\mathsf{T}_\rho f}(S) = \rho^{|S|}\widehat{f}(S)$ for every $S \subseteq [n]$. So we have the following equations

$$\langle f, \mathsf{T}_\rho g\rangle = \langle g, \mathsf{T}_\rho f\rangle = \sum_S \rho^{|S|}\widehat{f}(S)\widehat{g}(S),$$
$$\langle f, \mathsf{T}_\rho f\rangle = \sum_S \rho^{|S|}\widehat{f}(S)^2,$$
$$\langle g, \mathsf{T}_\rho g\rangle = \sum_S \rho^{|S|}\widehat{g}(S)^2.$$

Using term-wise AM-GM, we have

$$\frac{\langle f, \mathsf{T}_\rho f\rangle + \langle g, \mathsf{T}_\rho g\rangle}{2} \geq |\langle f, \mathsf{T}_\rho g\rangle| = |\langle g, \mathsf{T}_\rho f\rangle|,$$

which give us the inequality as desired. ◀

▶ **Claim 7.** *Let n be any positive integer, and let $\epsilon', \epsilon \in (0, 1/2)$. Suppose $\mathsf{BSS}(\epsilon') \sqsubseteq^{\delta}_{f,g} \mathsf{BSS}(\epsilon)^{\otimes n}$ for some functions $f, g\colon \{0,1\}^n \to \{-1,1\}$ and $\delta \geq 0$. Then, f and g agree on most of the inputs $x \in \{0,1\}^n$, that is, $\langle f, g\rangle \geq 1 - \frac{5\sqrt{\delta}}{2\rho'}$.*
Furthermore, we have

$$\mathop{\mathbb{E}}_x |\mathsf{T}_\rho f(x) - \rho' f(x)| \leq \delta + 5\sqrt{\delta}.$$

Proof. Let $a = |A|/N$, and $A = \{x \in \{0,1\}^n : f(x) = g(x)\}$. Note that $\langle f, g\rangle = 2a - 1$. We shall show that a is close to 1. By Claim 6 we have

$$\frac{\langle f, \mathsf{T}_\rho f\rangle + \langle g, \mathsf{T}_\rho g\rangle}{2} \geq |\langle f, \mathsf{T}_\rho g\rangle| = |\langle g, \mathsf{T}_\rho f\rangle| \tag{2}$$

The main idea is that we will upper bound the left hand side and lower bound the right hand side of the inequality above to get an inequality constraint for a, from which we can conclude that a is close to 1.

Upper bound for the left hand side. By the security requirement, we have

$$\mathop{\mathbb{E}}_{x \sim U_{\{0,1\}^n}} |\mathsf{T}_\rho g(x) - \rho' f(x)| \leq \delta,$$

which is equivalent to

$$\mathop{\mathbb{E}}_{x \sim U_{\{0,1\}^n}} |f(x)\mathsf{T}_\rho g(x) - \rho'| \leq \delta.$$

By an averaging argument, there exists a least $1 - \sqrt{\delta}$ fraction of $x \in \{0,1\}^n$ such that $|f(x)\mathsf{T}_\rho g(x) - \rho'| \leq \sqrt{\delta}$, and at most $\sqrt{\delta}$ fraction such that $|f(x)\mathsf{T}_\rho g(x) - \rho'| > \sqrt{\delta}$. Clearly $|f(x)\mathsf{T}_\rho g(x) - \rho'| \leq 1$. Therefore

$$\begin{aligned}
\langle f, \mathsf{T}_\rho f\rangle &= \mathop{\mathbb{E}}_{x \in \{0,1\}^n} f(x)\mathsf{T}_\rho f(x) \\
&= \frac{1}{N}\left(\sum_{x: f(x)=g(x)} f(x)\mathsf{T}_\rho f(x) + \sum_{x: f(x)=-g(x)} f(x)\mathsf{T}_\rho f(x)\right) \\
&= \frac{1}{N}\left(\sum_{x \in A} f(x)\mathsf{T}_\rho g(x) - \sum_{x \notin A} f(x)\mathsf{T}_\rho g(x)\right) \\
&\leq \frac{1}{N}\left(\sum_{x \in A}(\rho' + \sqrt{\delta}) + \sum_{x \notin A}(-\rho' - \sqrt{\delta})\right) + \sqrt{\delta} \cdot 1 \\
&= (2a-1)\rho' + \sqrt{\delta} + \sqrt{\delta} \\
&= (2a-1)\rho' + 2\sqrt{\delta}
\end{aligned}$$

Similarly, we get $\langle g, \mathsf{T}_\rho g\rangle \leq (2a-1)\rho' + 2\sqrt{\delta}$.
Lower bound for the right hand side.

$$|\langle f, \mathsf{T}_\rho g\rangle| \geq (1-\sqrt{\delta})(\rho' - \sqrt{\delta}) + \sqrt{\delta}\cdot(-1) = \rho' + \sqrt{\delta} - \sqrt{\rho}(\rho' - \sqrt{\delta} + 1) \geq \rho' - 3\sqrt{\delta}$$

Putting things together. Therefore, we have $(2a-1)\rho' + 2\sqrt{\delta} \geq \rho' - 3\sqrt{\delta}$, which implies that $a \geq 1 - \frac{5\sqrt{\delta}}{2\rho'}$. Next, by triangle inequality,

$$\mathop{\mathbb{E}}_x |\mathsf{T}_\rho f(x) - \rho' f(x)| \leq \mathop{\mathbb{E}}_x |\mathsf{T}_\rho f(x) - \rho' g(x)| + \rho' \mathop{\mathbb{E}}_x |g(x) - f(x)| \quad \leq \delta + 2\rho' \frac{5\sqrt{\delta}}{2\rho'} = \delta + 5\sqrt{\delta},$$

which completes our proof of Claim 7. ◀

▶ **Claim 8.** *Let $f\colon \{0,1\}^n \to \{-1,1\}$. Suppose that $\mathbb{E}_x |\mathsf{T}_\rho f(x) - \rho' f(x)| \leq \delta$. Then there exists $k \in [n]$ such that $\left|\rho' - \rho^k\right| \leq \sqrt{5}\cdot\delta^{1/4}$.*

Proof. By an averaging argument, we have

$$\mathop{\mathbb{E}}_x (\mathsf{T}_\rho f(x) - \rho' f(x))^2 \leq (1-\sqrt{\delta})\delta + \sqrt{\delta}\cdot 2^2 \leq 5\sqrt{\delta}$$

By Parseval's identity,

$$\mathop{\mathbb{E}}_x (\mathsf{T}_\rho f(x) - \rho' f(x))^2 = \sum_{S\subseteq[n]} \mathsf{T}_\rho \widehat{f - \rho'} \cdot f(S)^2 = \sum_S \left(\widehat{\mathsf{T}_\rho f}(S) - \rho' \widehat{f}(S)\right)^2 = \sum_S (\rho^{|S|} - \rho')^2 \widehat{f}(S)^2$$

Let $\gamma = \min_{k\in[n]} \left|\rho' - \rho^k\right|$, then

$$\sum_S (\rho^{|S|} - \rho')^2 \widehat{f}(S)^2 \geq \sum_S \gamma^2 \widehat{f}(S)^2 = \gamma$$

So it must be the case that $\gamma^2 \leq 5\sqrt{\delta}$, which implies that $\left|\rho' - \rho^k\right| \leq \sqrt{5}\cdot\delta^{1/4}$. ◀

Now, we are ready to prove Lemma 4.

Proof of Lemma 4 . Applying Claim 7 for $f = f_n$, $g = g_n$, $\delta = \nu(n)$, we have the following

$$\langle f_n, g_n\rangle \geq 1 - \frac{5\sqrt{\nu(n)}}{2\rho'}$$

Furthermore,

$$\mathop{\mathbb{E}}_{x^n} |\mathsf{T}_\rho(f_n)(x^n) - \rho' f_n(x^n)| \leq \nu(n) + 5\sqrt{\nu(n)}.$$

Applying Claim 8 for $f = f_n, g = g_n$ and $\delta = \nu(n) + 5\sqrt{\nu(n)}$, there exists $k(n) \in [n]$ such that

$$\left|\rho' - \rho^{k(n)}\right| \leq \sqrt{5}\left(\nu(n) + 5\sqrt{\nu(n)}\right)^{1/4},$$

which completes our proof. ◀

▶ **Lemma 5.** *Let $\{k(n)\}_{n\in I}$ be a sequence of positive integers and $\{\nu_n\}_{n\in I}$ be a sequence of positive real numbers such that $\lim_{n\to\infty} \nu(n) = 0$, where I is a subset of $\mathbb{N}$ with infinitely many elements. Let $\rho, \rho' \in (0,1)$ be fixed constants. Suppose that $\left|\rho' - \rho^{k(n)}\right| \leq \nu(n)$ for every $n \in I$. Then there exists $k \in \mathbb{N}$ such that $\rho' = \rho^k$.*

Proof. Let $\{k(n)\}_{n\in I}$ be a sequence of positive integers and $\{\nu_n\}_{n\in I}$ be a sequence of positive real numbers such that $\lim_{n\to\infty}\nu(n) = 0$, where I is a subset of $\mathbb{N}$ with infinitely many elements. Let $\rho, \rho' \in (0,1)$ be fixed constants. Suppose that $\left|\rho' - \rho^{k(n)}\right| \le \nu(n)$ for every $n \in I$. Then, there exists $k \in \mathbb{N}$ such that $\rho' = \rho^k$. ◀

▶ **Lemma 6.** *Let $\epsilon \in (0, 1/2)$ and k be some positive integer. For any positive integer $n \ge k$, for any functions $f_n = g_n$ in the set of linear function $\{\chi_S \colon S \subseteq [n], |S| = k\}$, we have $\mathsf{BSS}(\epsilon') \sqsubseteq^0_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$, where $\rho' = 1 - 2\epsilon' = (1-2\epsilon)^k = \rho^k$.*

Proof. Suppose $f_n = g_n = \chi_S$ for some $S \subseteq [n]$ with $|S| = k$. We shall show that all there algebraic conditions are satisfied, namely,

1. Correctness: $\mathbb{E}[f_n(x^n)] = \mathbb{E}[g_n(x^n)] = 0$, and $|\mathbb{E}\left[f_n(x^n)\cdot g_n(y^n)\right] - \rho'| = 0$.
2. Alice security: $\mathbb{E}_{y^n\sim U_{\{0,1\}^n}} \left|\mathsf{T}_\rho(f_n)(y^n) - \rho'\cdot g_n(y^n)\right| = 0$.
3. Bob security: $\mathbb{E}_{x^n\sim U_{\{0,1\}^n}} \left|\mathsf{T}_\rho(g_n)(x^n) - \rho'\cdot f_n(x^n)\right| = 0$.

It is clear that χ_S is a balanced function, therefore

$$\mathbb{E}[f_n] = \mathbb{E}[g_n] = \mathbb{E}[\chi_S] = 0.$$

Now, by basic Fourier analysis, we have

$$\mathsf{T}_\rho(f_n) = \mathsf{T}_\rho(g_n) = \mathsf{T}_\rho(\chi_S) = \rho^k\chi_S = \rho'\chi_S = \rho' f_n = \rho' g_n.$$

From these equations, it is straightforward to see that all three conditions are satisfied, which implies $\mathsf{BSS}(\epsilon') \sqsubseteq^0_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ as desired. ◀

We are ready to describe the proof of Theorem 5 as follows. We emphasis that the security requirements of Alice and Bob are crucial to our proof.

Proof of Theorem 5 . First we show that $\rho' = \rho^k$. For each n such that $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$, by Lemma 4, we have

$$\left|\rho' - \rho^{k(n)}\right| \le \sqrt{5}\left(\nu(n) + 5\sqrt{\nu(n)}\right)^{1/4}.$$

It is clear that $\lim_{n\to\infty}\sqrt{5}\left(\nu(n) + 5\sqrt{\nu(n)}\right)^{1/4} = 0$ since $\lim_{n\to\infty}\nu(n) = 0$. Using the fact that $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ holds for infinitely many $n \in \mathbb{N}$, we can apply Lemma 5 to conclude that $\rho' = \rho^k$ for some positive integer k.

Next, when $\rho' = \rho^k$, for each $n \ge k$, we define $f^*_n = g^*_n = \chi_S$, where S is some subset if size k of $[n]$. By Lemma 6, we have $\mathsf{BSS}(\epsilon') \sqsubseteq^0_{f^*_n,g^*_n} \mathsf{BSS}(\epsilon)^{\otimes n}$. Thus, there exists a family of infinitely many functions $\{f^*_n, g^*_n\}$ as desired. ◀

Remarks. In fact, in the perfect secure reduction $\mathsf{BSS}(\epsilon') \sqsubseteq^0_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$, we can characterize the set of all possible reduction functions f_n, g_n and the set of all possible values of ϵ' for any *fixed* value n as follows.

▶ **Lemma 7.** *Let n be a positive integer and $\epsilon', \epsilon \in (0, 1/2)$. Suppose that $\mathsf{BSS}(\epsilon') \sqsubseteq^0_{f,g} \mathsf{BSS}(\epsilon)^{\otimes n}$ for some functions $f, g \colon \{0,1\}^n \to \{-1,1\}$. Then $f = g$ and there exists some positive integer k such that $\rho' = \rho^k$. Furthermore, the two functions f and g have the Fourier weights at the degree k only, that is, $W_k[f] = W_k[g] = 1$.*

Proof. Apply Claim 7 for $\delta = 0$, we have

$$\langle f, g \rangle \geq 1 - 0 = 1,$$

which means that $f = g$. This implies that $\mathsf{T}_\rho f = \rho' f$. We have the following equations

$$\mathsf{T}_\rho f(x) = \sum_{S \subseteq [n]} \rho^{|S|} \widehat{f}(S) \chi_S(x)$$
$$\rho' f(x) = \rho' \sum_{S \subseteq [n]} \widehat{f}(S) \chi_S(x) = \sum_{S \subseteq [n]} \rho' \widehat{f}(S) \chi_S(x)$$

Now by the uniqueness of Fourier expansion, we must have $\rho^{|S|} \widehat{f}(S) = \rho' \widehat{f}(S)$ for every $S \subseteq [n]$. Since $\sum_{S \subseteq [n]} \widehat{f}(S)^2 = 1$, there exists some $S^* \subseteq [n]$ such that $\widehat{f}(S^*) \neq 0$. Let $k = |S^*|$, then $\rho^k \widehat{f}(S^*) = \rho' \widehat{f}(S^*)$, which implies that $\rho' = \rho^k$. Furthermore, when $|S| \neq k$, it must be the case that $\widehat{f}(S) = 0$. Therefore, $W_k[f] = W_k[g] = 1$, which completes the proof. ◀

We notice that there are non-linear functions f such that it puts all Fourier weights at one degree k of f (see the example in the introduction).

References

ACJ17 Prabhanjan Ananth, Arka Rai Choudhuri, and Abhishek Jain. A new approach to round-optimal secure multiparty computation. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 468–499, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-63688-7_16. 3

AG76 Rudolf Ahlswede and Peter Gács. Spreading of sets in product spaces and hypercontraction of the markov operator. *The annals of probability*, pages 925–939, 1976. 7

AGKN13 Venkat Anantharam, Amin Gohari, Sudeep Kamath, and Chandra Nair. On maximal correlation, hypercontractivity, and the data processing inequality studied by erkip and cover. *arXiv preprint arXiv:1304.6133*, 2013. 7

AIK04 Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. In *45th Annual Symposium on Foundations of Computer Science*, pages 166–175, Rome, Italy, October 17–19, 2004. IEEE Computer Society Press. doi:10.1109/FOCS.2004.20. 8

BG15 Salman Beigi and Amin Gohari. On the duality of additivity and tensorization. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2381–2385. IEEE, 2015. doi:10.1109/ISIT.2015.7282882. 7

BGJ$^+$18 Saikrishna Badrinarayanan, Vipul Goyal, Abhishek Jain, Yael Tauman Kalai, Dakshita Khurana, and Amit Sahai. Promise zero knowledge and its applications to round optimal MPC. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 459–487, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-96881-0_16. 3

BGV12 Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012: 3rd Innovations in Theoretical Computer Science*, pages 309–325, Cambridge, MA, USA, January 8–10, 2012. Association for Computing Machinery. doi:10.1145/2090236.2090262. 3

BHP17 Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou. Four round secure computation without setup. 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 645–677, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_22. 3

BMR90 Donald Beaver, Silvio Micali, and Phillip Rogaway. The round complexity of secure protocols (extended abstract). In *22nd Annual ACM Symposium on Theory of Computing*, pages 503–513, Baltimore, MD, USA, May 14–16, 1990. ACM Press. doi:10.1145/100216.100287. 3

BNP08 Assaf Ben-David, Noam Nisan, and Benny Pinkas. FairplayMP: a system for secure multi-party computation. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM CCS 2008: 15th Conference on Computer and Communications Security*, pages 257–266, Alexandria, Virginia, USA, October 27–31, 2008. ACM Press. doi:10.1145/1455770.1455804. 3

Bor82 Christer Borell. Positivity improving operators and hypercontractivity. *Mathematische Zeitschrift*, 180(3):225–234, 1982. doi:10.1007/BF01318906. 7

Can00a Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, January 2000. doi:10.1007/s001459910006. 9

Can00b Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2000. http://eprint.iacr.org/2000/067. 9

Can01 Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science*, pages 136–145, Las Vegas, NV, USA, October 14–17, 2001. IEEE Computer Society Press. doi:10.1109/SFCS.2001.959888. 9

CK90 Claude Crépeau and Joe Kilian. Weakening security assumptions and oblivious transfer (abstract). In Shafi Goldwasser, editor, *Advances in Cryptology – CRYPTO'88*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7, Santa Barbara, CA, USA, August 21–25, 1990. Springer, Heidelberg, Germany. doi:10.1007/0-387-34799-2_1. 3

COSV17a Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Delayed-input non-malleable zero knowledge and multi-party coin tossing in four rounds. 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 711–742, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_24. 3

COSV17b Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Round-optimal secure two-party computation from trapdoor permutations. 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 678–710, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_23. 3

DMN18 Anindya De, Elchanan Mossel, and Joe Neeman. Non interactive simulation of correlated distributions is decidable. In Artur Czumaj, editor, *29th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2728–2746, New Orleans, LA, USA, January 7–10, 2018. ACM-SIAM. doi:10.1137/1.9781611975031.174. 7

DPSZ12 Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 643–662, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-32009-5_38. 3

Gen09 Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Computing*, pages 169–178, Bethesda, MD, USA, May 31 – June 2, 2009. ACM Press. doi:10.1145/1536414.1536440. 3

GIK$^+$15 Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with one-way communication. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 191–208, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-48000-7_10. 4, 5, 6, 8

GK73 Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973. 7

GKS16 Badih Ghazi, Pritish Kamath, and Madhu Sudan. Decidability of non-interactive simulation of joint distributions. In Irit Dinur, editor, *57th Annual Symposium on Foundations of Computer Science*, pages 545–554, New Brunswick, NJ, USA, October 9–11, 2016. IEEE Computer Society Press. doi:10.1109/FOCS.2016.65. 7

GMPP16 Sanjam Garg, Pratyay Mukherjee, Omkant Pandey, and Antigoni Polychroniadou. The exact round complexity of secure computation. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 448–476, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-49896-5_16. 3

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. 3

Goy11 Vipul Goyal. Constant round non-malleable protocols using one way functions. In Lance Fortnow and Salil P. Vadhan, editors, *43rd Annual ACM Symposium on Theory of Computing*, pages 695–704, San Jose, CA, USA, June 6–8, 2011. ACM Press. doi:10.1145/1993636.1993729. 3

HHPV18 Shai Halevi, Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam. Round-optimal secure multi-party computation. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 488–520, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-96881-0_17. 3

Hir35 Hermann O Hirschfeld. A connection between correlation and contingency. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 520–524. Cambridge University Press, 1935. doi:10.1017/S0305004100013517. 7

IK00 Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *41st Annual Symposium on Foundations of Computer Science*, pages 294–304, Redondo Beach, CA, USA, November 12–14, 2000. IEEE Computer Society Press. doi:10.1109/SFCS.2000.892118. 8

IK02 Yuval Ishai and Eyal Kushilevitz. Perfect constant-round secure computation via perfect randomizing polynomials. In Peter Widmayer, Francisco Triguero Ruiz, Rafael Morales Bueno, Matthew Hennessy, Stephan Eidenbenz, and Ricardo Conejo, editors, *ICALP 2002: 29th International Colloquium on Automata, Languages and Programming*, volume 2380 of *Lecture Notes in Computer Science*, pages 244–256, Malaga, Spain, July 8–13, 2002. Springer, Heidelberg, Germany. doi:10.1007/3-540-45465-9_22. 8

IKO$^+$11 Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 667–684, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-22792-9_38. 3, 4, 8

IPS08 Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 572–591, Santa Barbara, CA, USA, August 17–21, 2008. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-85174-5_32. 3, 8

KA12 Sudeep Kamath and Venkat Anantharam. Non-interactive simulation of joint distributions: The hirschfeld-gebelein-rényi maximal correlation and the hypercontractivity ribbon. In *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1057–1064. IEEE, 2012. 5, 6

KA16 Sudeep Kamath and Venkat Anantharam. On non-interactive simulation of joint distributions. *IEEE Transactions on Information Theory*, 62(6):3419–3435, 2016. 5, 6, 7

Kil91 Joe Kilian. A general completeness theorem for two-party games. In *23rd Annual ACM Symposium on Theory of Computing*, pages 553–560, New Orleans, LA, USA, May 6–8, 1991. ACM Press. doi:10.1145/103418.103475. 3

Kil00 Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd Annual ACM Symposium on Theory of Computing*, pages 316–324, Portland, OR, USA, May 21–23, 2000. ACM Press. doi:10.1145/335305.335342. 3, 7

KMPS14 Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai. A full characterization of completeness for two-party randomized function evaluation. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 659–676, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-55220-5_36. 3

KO04 Jonathan Katz and Rafail Ostrovsky. Round-optimal secure two-party computation. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 335–354, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-28628-8_21. 3

KOS03 Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Round efficiency of multi-party computation with a dishonest majority. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 578–595, Warsaw, Poland, May 4–8, 2003. Springer, Heidelberg, Germany. doi:10.1007/3-540-39200-9_36. 3

MNPS04 Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - secure two-party computation system. In Matt Blaze, editor, *USENIX Security 2004: 13th USENIX Security Symposium*, pages 287–302, San Diego, CA, USA, August 9–13, 2004. USENIX Association. 3

MO05a Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Structures & Algorithms*, 26(4):418–436, 2005. doi:10.1002/rsa.20062. 7

MO05b Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Struct. Algorithms*, 26(4):418–436, 2005. doi:10.1002/rsa.20062. 7

MOR$^+$06 Elchanan Mossel, Ryan O'Donnell, Oded Regev, Jeffrey E Steif, and Benny Sudakov. Non-interactive correlation distillation, inhomogeneous markov chains, and the reverse bonami-beckner inequality. *Israel Journal of Mathematics*, 154(1):299–336, 2006. 4, 7

MOS13 Elchanan Mossel, Krzysztof Oleszkiewicz, and Arnab Sen. On reverse hypercontractivity. *Geometric and Functional Analysis*, 23(3):1062–1097, 2013. 7

NNOB12 Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. A new approach to practical active-secure two-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 681–700, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-32009-5_40. 3

NW17 Chandra Nair and Yan Nan Wang. Reverse hypercontractivity region for the binary erasure channel. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 938–942. IEEE, 2017. doi:10.1109/ISIT.2017.8006666. 6

O'D14 Ryan O'Donnell. *Analysis of boolean functions.* Cambridge University Press, 2014. 9

Pas04 Rafael Pass. Bounded-concurrent secure multi-party computation with a dishonest majority. In László Babai, editor, *36th Annual ACM Symposium on Theory* *of Computing*, pages 232–241, Chicago, IL, USA, June 13–16, 2004. ACM Press. doi:10.1145/1007352.1007393. 3

PW10 Rafael Pass and Hoeteck Wee. Constant-round non-malleable commitments from sub-exponential one-way functions. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 638–655, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-13190-5_32. 3

Rén59 Alfréd Rényi. On measures of dependence. *Acta mathematica hungarica*, 10(3-4):441–451, 1959. doi:10.1007/BF02024507. 7

STW19 Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for generating correlation: A unifying survey. *IEEE Transactions on Information Theory*, 66(1):5–37, 2019. doi:10.1109/TIT.2019.2946364. 4, 7

Wee10 Hoeteck Wee. Black-box, round-efficient secure computation via non-malleability amplification. In *51st Annual Symposium on Foundations of Computer Science*, pages 531–540, Las Vegas, NV, USA, October 23–26, 2010. IEEE Computer Society Press. doi:10.1109/FOCS.2010.87. 3

Wit75 Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975. doi:doi.org/10.1137/0128010. 7

Wyn75 Aaron Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975. doi:10.1109/TIT.1975.1055346. 3, 7

Yan04 Ke Yang. On the (im)possibility of non-interactive correlation distillation. In Martin Farach-Colton, editor, *LATIN 2004: Theoretical Informatics, 6th Latin American Symposium*, volume 2976 of *Lecture Notes in Computer Science*, pages 222–231, Buenos Aires, Argentina, April 5–8, 2004. Springer, Heidelberg, Germany. 7