Secure Non-interactive Simulation: Feasibility & Rate

Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen

Department of Computer Science, Purdue University
West Lafayette, Indiana, USA

Abstract

Random samples from noisy channels, like binary erasure and binary symmetric channels, enable general secure computation. A key objective is to realize these secure computation tasks using the minimum number of samples from the noise source. However, even for elementary tasks, like converting one form of noisy channel samples into samples from another noisy channel, the precise characterization of achievable efficiency is not well-understood.

Motivated by secure two-party sampling and applications to building robust infrastructure for secure computation, this work introduces the concept of secure non-interactive simulation of joint distributions (SNIS). Parties receive samples from a noise source, and they, without any interaction, securely convert them into samples from another noise distribution. This primitive is a stronger version of (1) non-interactive simulation of joint distributions (NIS) in information theory, (2) non-interactive correlation distillation, and (3) one-way secure computation (OWSC). Our work algebraizes the simulation-based security definition of SNIS, making it more amenable to the Fourier analysis. After that, we study the feasibility and rate of SNIS.

This work studies random samples from the binary symmetric channel with noise parameter ε, represented by $\mathsf{BSS}(\varepsilon)$, and the binary erasure channel with erasure probability ε, represented by $\mathsf{BES}(\varepsilon)$.

Our work completely resolves the feasibility and rate of SNIS between these families of joint distributions. Realizing any BES sample from BSS samples is impossible in NIS and OWSC, which extends to SNIS. Furthermore, we prove the impossibility of a SNIS of any BSS sample from any BES samples, an open problem in NIS and OWSC.

Next, we prove that a SNIS of a $\mathsf{BES}(\varepsilon')$ sample from $\mathsf{BES}(\varepsilon)$ samples is feasible if and only if $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$. Additionally, in this context, we prove that all SNIS constructions must be linear. Furthermore, if $(1-\varepsilon') = (1-\varepsilon)^k$, then the rate of simulating multiple independent $\mathsf{BES}(\varepsilon')$ samples from $\mathsf{BES}(\varepsilon)$ samples is at most $1/k$, which is also achievable using (block) linear constructions.

Finally, we show that a SNIS of a $\mathsf{BSS}(\varepsilon')$ sample from $\mathsf{BSS}(\varepsilon)$ samples is feasible if and only if $(1-2\varepsilon') = (1-2\varepsilon)^k$, for some $k \in \mathbb{N}$. Interestingly, there are linear as well as (comparatively inefficient) non-linear SNIS constructions. However, if $(1-2\varepsilon') = (1-2\varepsilon)^k$, then the rate of simulating multiple $\mathsf{BSS}(\varepsilon')$ samples is at most $1/k$ (irrespective of linear or non-linear constructions), and this rate is achievable using (block) linear constructions.

Our technical innovation is the use of Fourier analytic tools to study feasibility and rate characterization problems in cryptographic protocols, explicitly incorporating the security constraint. The technical results rely on a new concentration of the Fourier spectrum unique to secure constructions. The authors believe that specifically developing new general analysis methodologies respecting security is of independent and broader interest.

Contents

1 Introduction

General secure computation [96, 44] is an exceptionally powerful cryptographic primitive that allows mutually distrusting parties to securely perform arbitrary computation over their private data, revealing only the respective outputs of each party, even if all adversarial parties are colluding. It is impossible to realize this cryptographic primitive solely from independent randomness and common shared randomness in the information-theoretic model [41, 64, 65]. On the other hand, *noisy*, albeit *correlated*, information is an incredible facilitator of cryptography. Rabin [81, 82] and Crépeau [30] demonstrated that erasure channels, referred to as Rabin Oblivious Transfer, enable performing general secure computation. In 1988, Crépeau and Kilian [31, 32] proved that noisy channels, particularly the binary symmetric channels, suffice for general secure computation. After that, a significant body of highly influential research demonstrated the feasibility of realizing general secure computation from diverse and unreliable noise sources [57, 58, 34, 59, 33, 92, 93, 56, 24]. In particular, random samples from these noisy channels suffice for general secure computation while incurring an slight increase in round and communication complexity [90].

Representative motivating example. Consider *secure two-party sampling* [78, 79, 80], i.e., the secure evaluation of an inputless randomized functionality. This cryptographic task enables Alice and Bob to generate private samples u and v, respectively, such that the joint distribution of their samples is (U, V). In the information-theoretic setting, even when parties have access to unbounded independent private randomness and common shared randomness, one can securely sample only cryptographically rudimentary joint distributions (U, V) (refer to the excellent thesis [91] for a survey of relevant works in this field). In particular, it is impossible to securely sample noisy correlations, for example, samples from binary erasure and symmetric source. On the other hand, given a *setup* that initializes Alice and Bob with correlated samples x^n and y^n, respectively, from (a different) joint distribution $(X, Y)^{\otimes n}$, they can interactively sample from any joint distribution (U, V) securely [96, 44, 59]. However, given a setup, the necessity of interaction for secure sampling is not apparent. In particular, which (U, V) can be securely sampled given which setup $(X, Y)^{\otimes n}$ without any communication (i.e., *non-interactively*) is unknown (as this work and the followup work [55] shows, this question turns out to be incredibly challenging with a significant potential for future research). Furthermore, if such a non-interactive secure simulation is feasible, the most efficient constructions' characterization is unknown.

Our work introduces the notion of *secure non-interaction simulation* (SNIS) to study the *feasibility* and *rate* of secure sampling without any communication between the parties.

Application of SNIS. Similar to the seminal works of Maurer [68, 69, 70], and Ahlswede and Csiszár [2, 3], who introduced the concept of building an infrastructure for shared private randomness using sources of noise, SNIS has applications to building a robust infrastructure for the *offline-online paradigm* of secure computation [67, 14, 35, 76]. In the offline-online paradigm, parties generate correlated private randomness in an offline phase and consume these samples during a fast online phase protocol, which is information-theoretically secure conditioned on the security of the offline phase. This model has resulted in several success stories in practical secure computation solutions, for example, private set intersection.

Consider an off-the-shelf MPC (online) protocol in the offline-online paradigm that uses multiple samples of (U, V) during its online phase. Alice and Bob are interested in using this MPC solution; however, they do not have access to samples from the exact noise distribution (U, V). Instead, Alice and Bob have access to multiple (independent) samples from a different noise source (X, Y), or, more generally, a sample from the distribution $(X_1, Y_1) \otimes (X_2, Y_2) \otimes \cdots \otimes (X_n, Y_n)$. Ideally, Alice and Bob would like to securely convert the samples of their available noise source into samples of (U, V) without any interaction, i.e., *silently* (see, for example, [19, 18] for the motivation for silent

computation). If this conversion is feasible, they can run the off-the-shelf MPC protocol using the available noise sources. Section 5 further elaborates this application.

1.1 Definition: Secure Non-Interactive Simulation

Let (X, Y) be a joint distribution over the sample space $(\mathcal{X}, \mathcal{Y})$, and (U, V) be a joint distribution over the sample space $(\mathcal{U}, \mathcal{V})$.[1] The intuitive definition of *secure non-interactive simulation of joint distributions* (SNIS) closely follows the presentation in Figure 1 (with parameter $m = 1$). Sample $(x^n, y^n) \xleftarrow{\$} (X, Y)^{\otimes n}$, i.e., draw n independent samples from the distribution (X, Y). Alice gets $x^n \in \mathcal{X}^n$, and Bob gets $y^n \in \mathcal{Y}^n$. Alice has private randomness $r_A \xleftarrow{\$} R_A$ and Bob has, independent, private randomness $r_B \xleftarrow{\$} R_B$, where R_A, R_B are random variables over the sample spaces $\mathcal{R}_A$ and $\mathcal{R}_B$, respectively. Suppose $f_n \colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{U}$ and $g_n \colon \mathcal{Y}^n \times \mathcal{R}_B \to \mathcal{V}$ are the (possibly randomized) *reduction functions* for Alice and Bob, respectively. Alice computes $u' = f_n(x^n, r_A)$ and Bob computes $v' = g_n(y^n, r_B)$.

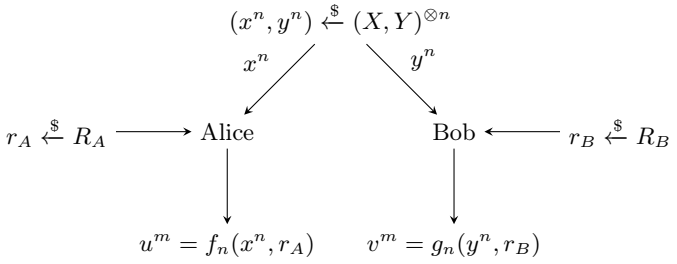

Figure 1: Our Model.

Let us gain some intuition regarding the definition of SNIS. For the ease of presentation, this section only considers deterministic reduction functions, i.e., there is no R_A and R_B. However, this choice for simplification in presentation does not incur any loss of generality. Looking ahead, Theorem 5 shall prove a derandomization result proving that one can assume reduction functions in SNIS to be deterministic, without loss of generality. However, such a derandomization result for the rate characterization is extremely subtle and depends on the proof strategy (paragraph "Subtlety" in Section 2.2 addresses this aspect of our work).

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 the 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 $u' = u$ and $v' = v$, is $\nu(n)$-close to being independent of v.[2]
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 $\nu(n)$-close to being independent of u.

To discuss rate, consider SNIS of the form $(U, V)^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n, g_n} (U, V)^{\otimes n}$. Here, the reduction functions output $m(n)$-independent samples from the distribution (U, V). Fixing (X, Y) and (U, V), our objective is to characterize the maximum achievable *production rate* $m(n)/n$ over all possible reductions (a standard single-letter characterization).

Remark 1. *Since we consider non-interactive protocols without private inputs, semi-honest and malicious security (with abort) are equivalent. So, for the simplicity, the presentation considers (statistical) security against semi-honest adversaries, that is, parties follow the protocol but are curious to find more information. Section 7 provides a formal (composable) simulation-based security*

[1] As is typical in this line of work in cryptography and information theory, the joint distributions (U, V) and (X, Y) assign probabilities to samples that are either 0 or at least a positive constant.

[2] The joint distribution $(A|B = b)$ is ν-close to being independent of b if there exists a distribution A^* such that $(A|B = b)$ is ν-close to A^* in the statistical distance, for all $b \in \mathrm{Supp}(B)$.

Input Joint Distribution	Output Joint Distribution	Feasible set of ε'		
		OWSC [39]	SNIS (Our Work)	NIS [97]
$\mathsf{BES}(\varepsilon)$	$\mathsf{BES}(\varepsilon')$	$(0,1)$	$\left\{1-(1-\varepsilon)^k :\ k\in\mathbb{N}\right\}$	$[\varepsilon,1)$
	$\mathsf{BSS}(\varepsilon')$	$\supseteq \emptyset$	$\emptyset$	$\supseteq [\varepsilon/2, 1/2)$ $\subseteq \left[\frac{1-\sqrt{1-\varepsilon}}{2}, 1/2\right)$
$\mathsf{BSS}(\varepsilon)$	$\mathsf{BES}(\varepsilon')$	$\emptyset$	$\emptyset$	$\emptyset$
	$\mathsf{BSS}(\varepsilon')$	$\supseteq \left\{\frac{1-(1-2\varepsilon)^k}{2} : k\in\mathbb{N}\right\}$	$\left\{\frac{1-(1-2\varepsilon)^k}{2} : k\in\mathbb{N}\right\}$	$[\varepsilon, 1/2)$

Table 1: Comparison of feasible parameters for OWSC, SNIS, and NIS involving reductions between BES and BSS families. A "$\supseteq S$" entry indicates that the feasible set is a superset of the set S. Therefore, a "$\supseteq \emptyset$" entry indicates that no characterization of the feasible set is known. Similarly, a "$\subseteq S$" entry indicates that the feasible set is a subset of the set S.

definition, sequential and parallel composition theorems, and the security of the projection operation.

1.2 Summary of our Results

Rabin and Crépeau [81, 82, 30] and Crépeau and Kilian [31, 32], respectively, proved that erasure and binary symmetric channels suffice for general secure computation. These elegant sources of noise provide an uncluttered access to abstracting the primary hurdles in achieving security. In a similar vein, to study the rate and capacity of SNIS, this paper considers samples from the following two families of distributions.

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

Comparison models. In information theory, *non-interactive simulation of joint distributions* (NIS) is a similar notion of simulating joint distributions [38, 94, 88, 52, 53, 43, 36, 42]. However, NIS only considers correctness (not security). Consequently, parties can generate independent private randomness, if rate is not a concern. Therefore, the NIS literature considers deterministic reductions when studying feasibility/infeasibility of reductions, without loss of generality. On the other hand, there is also research on performing secure computation using only one-way messages, a.k.a., *one-way secure computation* (OWSC) [39, 1]. This model considers secure protocols where only one party sends messages to the other party.

It is instructive to consider an example of SNIS, and an example of NIS that is *insecure*. Section 8 presents these examples for interested readers.

Remark 2. Non-interactive correlation distillation *[72, 71, 95, 15, 25] is a special case of SNIS where (U, V) is restricted to shared coin, i.e.,* $\mathsf{BSS}(0)$ *or* $\mathsf{BES}(0)$ *samples. This model has very strong impossibility results, so comparison with this model is not insightful.*

Technical Contribution: Concentration of Fourier Spectrum. Our work translates security into a "rank-one constraint" on an appropriate matrix (Theorem 6 and Theorem 7), and algebraizes the security definition of SNIS (Section 9.2, Section 10.1). These steps make the feasibility and rate characterization problem of SNIS amenable to an analytical approach.[3] Using this analytic formulation, our work identifies a *concentration of the Fourier spectrum for the reduction functions* for

[3]The inspiration stems from the fact that, at a high-level, the existing probabilistic, combinatorial, and extremal techniques employed to study characterization problems in cryptography are naturally generalized and unified by Fourier analytic techniques. The use of analytical techniques to study similar problems is commonplace in other fields of theoretical computer science and information theory (refer to Section 4); however, this analytical treatment is new to secure computation as per the authors' knowledge

SNIS (Theorem 1, Lemma 1). This phenomenon of secure reductions suffices to exclude insecure NIS constructions (see Section 8.2 for examples), and obtain tight feasibility and rate characterizations.

Feasibility results. Observe that the NIS and OWSC are relaxations of SNIS. Therefore, the impossibility results in either NIS or OWSC automatically imply an impossibility for SNIS. For example, in NIS, $\mathsf{BES}(\varepsilon')$ does not reduce to $\mathsf{BSS}(\varepsilon)^{\otimes n}$ with insecurity $\nu(n) = \mathsf{negl}(n)$[4] for any $\varepsilon \in (0, 1/2)$, and $\varepsilon' \in (0, 1)$ [53, 52, 39]. This impossibility result carries over to SNIS.

On the other hand, it is not known whether $\mathsf{BSS}(\varepsilon')$ reduces to $\mathsf{BES}(\varepsilon)^{\otimes n}$ with $\mathsf{negl}(n)$ insecurity via either NIS or OWSC. We resolve this problem for SNIS.[5] Table 1 summarizes our feasibility results (refer to Informal Theorem 1, Informal Theorem 2, Informal Theorem 3) and it positions them relative to the known results in NIS and OWSC. Additionally, for the perfect-SNIS case, our work characterizes the set of all possible secure reduction functions. This characterization results in the identification of exciting new reductions, which were not known earlier (see Equation 1 for such a reduction function).

Remark 3. *In fact, our feasibility results even hold for any $o(1)$ insecurity bound. Consequently, any BES–BES or BSS–BSS reduction is either (1) perfectly secure or (2) has constant insecurity. In particular, it is impossible to use more samples to achieve $o(1)$ insecurity in SNIS if perfect security is not achievable (which is possible in randomness extraction and interactive MPC).*

Rate results. The research in OWSC has not emphasized on characterizing the rate/capacity of these secure constructions. The authors are not aware of any rate/capacity results for NIS as well. For SNIS, we prove that if $\mathsf{BES}(\varepsilon')$ reduces to $\mathsf{BES}(\varepsilon)$, where $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$, then the rate of any secure construction is $\leqslant 1/k$. Similarly, if $\mathsf{BSS}(\varepsilon')$ reduces to $\mathsf{BSS}(\varepsilon)$, where $(1-2\varepsilon') = (1-2\varepsilon)^k$, for some $k \in \mathbb{N}$, then the rate of any secure construction is $\leqslant 1/k$. We present protocols demonstrating the tightness of these bounds (refer to Informal Theorem 2, Informal Theorem 3).

Tight rate/capacity results in secure computation are extremely rare [9, 37, 12, 85, 87, 78, 79, 80, 11]. Although the problem, in its full generality, seems insurmountable, there is a large body of highly influential research characterizing the feasibility of securely realizing functionalities given access to (ideal implementations of) other functionalities [57, 28, 63, 8, 26, 27, 13, 59, 66, 62, 61]. Surprisingly, even for (seemingly) analytically-manageable models like randomized polynomials/encoding [47, 7, 48, 50, 6] and cryptography using one-way communication [39, 1], just characterizing the feasibility of secure computation protocols is far from resolved. More generally, the current state-of-the-art has not made significant inroads into characterizing the rate/capacity of general secure computations. For instance, regarding the efficiency in using the noisy samples, referred to as the *sample complexity*, the current state-of-the-art constructs general secure computation from noisy channels at a (small) positive rate (as a consequence of [59, 90, 51, 49]), i.e., securely computing a functionality represented by a size-s circuit requires $O(s)$ random samples from a noisy channel. Consequently, the next logical frontier is the characterization of rate/capacity of general secure computation.

Remark 4. *Observe that independent coin samples are equivalent to $\mathsf{BSS}(1/2)$ samples. There is a NIS of independent coin from $\mathsf{BES}(\varepsilon)$, for any $\varepsilon \in (0, 1)$, using average min-entropy extraction techniques from a fixed source. However, we prove that a SNIS of independent coin from $\mathsf{BES}(\varepsilon)$ is impossible (see Informal Theorem 1).*

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

[5] The informal theorems in this section use $\nu(n) = \mathsf{negl}(n)$ only for ease of presentation. However, our results are significantly stronger. The actual theorem statements rule out any $\nu(n)$ that decays faster than an appropriate decreasing function in n. The interested readers are referred to the respective full theorems for the exact results.

Remark 5. *There is a NIS of independent coin from* $\mathsf{BSS}(\varepsilon)$*, for any* $\varepsilon \in (0, 1/2)$*, that achieves rate-*$1/2$ *(Alice outputs her first sample, and Bob outputs his second sample). Refer to Table 5 for the joint distribution table and Table 7 for the correctness of this NIS. Although the Fourier spectrum of each reduction is concentrated, the reduction functions have a lot of mismatches (vis-à-vis their input-output behavior). Therefore, Theorem 1 implies that this NIS cannot be secure (Table 6 violates the rank-one constraint). Furthermore, we can prove that any constant-rate SNIS of independent coins from* $\mathsf{BSS}(\varepsilon)$ *is impossible, where* $\varepsilon \in (0, 1/2)$*.*

Remark 6. *Overall, our constructions and hardness of computation results are the strongest possible in the following sense. All our constructions are perfectly secure (even against malicious adversaries), that is, they realize SNIS with zero insecurity. Furthermore, the constructions admit computationally efficient simulators. Moreover, all our feasibility and rate-achieving constructions hold whenever the number of input samples is sufficiently large (not just for infinitely-many values). On the other hand, our hardness of computation results extend to infinite families of reductions where (infinitely often) the insecurity falls faster than some* appropriate inverse-polynomial *of the number of input samples. Consequently, our results encompass the typical cryptographic contexts where the insecurity decays faster than* all *inverse-polynomials. Lastly, all our impossibility results hold against semi-honest adversaries and extend to the weaker game-based security definitions.*

2 Our Contribution: Technical Results

We introduce some intuitive terminology to present our results informally. A $\nu(n)$*-SNIS of* (U, V) *from* (X, Y) represents a family of SNIS, indexed by $n \in \mathbb{N}$, such that the insecurity of the construction is (at most) $\nu(n)$.[6] Finally, $R(\,(U, V), (X, Y)\,)$ represents the maximum achievable $m(n)/n$, as $n \to \infty$, when considering all SNIS of (U, V) from (X, Y) as illustrated in Figure 1.

2.1 SNIS Composition and Projection

Section 7 provides the simulation-based definition of SNIS and proves the following composition and projection results, where the reduction functions may be randomized (the main difference is that the simulation-based definition requires an efficient simulator, while the game-based definition does not).

1. *Parallel Composition (Theorem 2).* Let P, P', Q, and Q' be joint distributions. If ν-SNIS of P from Q and ν'-SNIS of P' from Q' exist, then a $(\nu + \nu')$-SNIS of $(P\|P')$ from $(Q\|Q')$ exists. The distribution $(P\|P')$ generates samples from both the joint distributions P and P', and $(Q\|Q')$ generates samples from both the joint distributions Q and Q'.
2. *Sequential Composition (Theorem 3).* Let P, Q, and R be joint distributions. If ν-SNIS of P from Q and ν'-SNIS of Q from R exist, then a $(\nu + \nu')$-SNIS of P from R exists.
3. *Projection (Theorem 4).* Let P, Q, and R be joint distributions. If a ν-SNIS of $(P\|Q)$ from R exists, then a ν-SNIS of P from R also exists.

These composition and projection theorems shall assist in proving our feasibility and rate results.

2.2 Derandomization

Recall that our definition of SNIS allows the reduction functions to use private randomness drawn from arbitrary distributions as well (refer to Figure 1). However, for cryptographic notions

[6] We highlight a subtlety in this notation. When we state a positive result that $\nu(n)$-SNIS of (U, V) from (X, Y) exists, then we imply that the reduction exists for all sufficiently large n. On the other hand, when we state a negative result that $\nu(n)$-SNIS of (U, V) from (X, Y) is impossible, then we imply that the reduction does not exist even for infinitely many n.

of security, we prove that if there exists a ν-SNIS of P from $Q^{\otimes n}$ using randomized reduction functions, then there exists a $\nu^{1/9}$-SNIS of P from $Q^{\otimes n}$ using deterministic reduction functions that is *sample preserving* (refer to Theorem 5). If the original reduction uses n samples of Q to generate the sample of P, then the deterministic reduction functions also use (a subset of) these n samples to generate the sample of P. Furthermore, observe that for cryptographic notion of security, the insecurity ν is a negligible function of n, represented as $\nu = \mathsf{negl}(n)$. When $\nu = \mathsf{negl}(n)$, note that $\nu^{1/9} = \mathsf{negl}(n)$ as well. Consequently, henceforth, we consider the reduction functions to be deterministic, without loss of generality for feasility characterization problems. However, there are subtleties involved for the rate characterization problem, which we discuss them in the paragraph below.

Remark 7. *This sample-preserving derandomization crucially relies on the security of the reduction. Insecure NIS need not admit a sample-preserving derandomization. For example, consider the example in Section 8.2.*

Remark 8. *Observe that the argument above also works for the receiver in the OWSC model. Consequently, without loss of generality, in the feasibility results of OWSC, the receiver is deterministic.*

Subtlety: Rate Characterization Problems. The derandomization above holds only for *constant-size* P; however, the result does not depend on the number of samples of Q. Let us consider an example to appreciate this subtlety, followed by a discussion on how our technical contributions uses this derandomization result.

Consider (U, V) and (X, Y) that are constant-size joint distributions. When considering a *feasibility result* where we consider SNIS of (U, V) from $(X, Y)^{\otimes n}$, we can use the derandomization result and assume that the reduction functions are deterministic, without loss of generality.

However, we *cannot* directly apply the derandomization result to the SNIS of $(U, V)^{\otimes m(n)}$ from $(X, Y)^{\otimes n}$ when considering a *rate result*. To circumvent this hurdle, as will be evident in our technical approach, we never consider m independent samples of (U, V) simultaneously in our analysis. We follow the following proof-strategy instead.

1. Suppose there is a SNIS of $(U, V)^{\otimes m(n)}$ from $(X, Y)^{\otimes n}$ using (possibly randomized) reduction functions.
2. We use the projection operator, which is secure even for randomized reductions, to argue that considering only the samples i and j of the output is secure, where $i, j \in \{1, \ldots, m(n)\}$.
3. Now, we consider this projected SNIS of $(U, V)^{\otimes 2}$ from (X, Y). Here, $(U, V)^{\otimes 2}$ has constant size; therefore, this projected SNIS admits derandomization.
4. We apply our "feasibility technical results" to this derandomized projected SNIS, and draw conclusions about this derandomized project SNIS, which is also sample preserving.

For brevity, we shall refer to these four-step arguments in our proof as "assuming that the SNIS of $(U, V)^{\otimes m(n)}$ from (X, Y) is deterministic, without loss of generality."

2.3 BSS from BES Samples

Recall that it is impossible to have a SNIS of $\mathsf{BES}(\varepsilon')$ from any number of $\mathsf{BSS}(\varepsilon)$ samples, for any $n \in \mathbb{N}$, $\varepsilon \in (0, 1/2)$, and $\varepsilon' \in (0, 1)$, because this reduction is already impossible in NIS and OWSC. Here we consider the other direction.

Informal Theorem 1 (Impossibility of BSS from BES)**.** *There is an universal constant c such that $c/\sqrt{n}$-SNIS of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$ does not exist, for any $\varepsilon' \in (0, 1/2)$ and $\varepsilon \in (0, 1)$.*

Refer to Theorem 8 for a formal statement. We prove this result using a combinatorial technique and an isoperimetric inequality on the Boolean hypercube (refer to Section 6.3 for an overview and

Section 9.1 for the proof). Our proof also works for the SNIS of shared common randomness from $\mathsf{BES}(\varepsilon)$, which provides an alternate combinatorial proof for this result proved using analytical techniques in [95].

2.4 BES from BES Samples

Next, we consider the inter-conversion among binary erasure sources with different erasure probabilities.

Informal Theorem 2 (BES Samples: Feasibility & Rate)**.** *Fix erasure probabilities $\varepsilon, \varepsilon' \in (0,1)$.*
Feasibility characterization. *The following statements are equivalent.*

1. *There is a $o(1)$-SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$.*
2. *There is a 0-SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$ (a perfectly secure SNIS).*
3. *There exists $k \in \mathbb{N}$ satisfying $(1-\varepsilon') = (1-\varepsilon)^k$.*

Rate characterization. *Fix any erasure probabilities $\varepsilon, \varepsilon' \in (0,1)$, such that $(1-\varepsilon') = (1-\varepsilon)^k$ and $k \in \mathbb{N}$. If a $o\big(1/n^{36+9k/2}\big)$-SNIS of $\mathsf{BES}(\varepsilon')^{\otimes m(n)}$ from $\mathsf{BES}(\varepsilon)^{\otimes n}$ exists, then $m(n)/n \leqslant 1/k$ and the production rate $R(\,\mathsf{BES}(\varepsilon'), \mathsf{BES}(\varepsilon)\,) = 1/k$.*

In fact, we prove an extension of Informal Theorem 2 in Appendix A where the target can be $\mathsf{BES}(\varepsilon_1) \otimes \mathsf{BES}(\varepsilon_2) \otimes \cdots \otimes \mathsf{BES}(\varepsilon_m)$ instead of $\mathsf{BES}(\varepsilon')^{\otimes m}$.

The results above are for an infinite family of reductions $\{f_n, g_n\}_{n\in\mathbb{N}}$. However, if there is even one reduction pair with perfect security, then we can directly conclude that $(1-\varepsilon') = (1-\varepsilon)^k$ and characterize the reduction functions precisely (see Theorem 10).

In the context of OWSC, one can achieve erasure probability ε' that is either lower or higher than the erasure probability ε. On the other hand, for SNIS, we show that $\varepsilon' \geqslant \varepsilon$ is necessary.

Typically, NIS literature's impossibility results rely on leveraging the reverse hypercontractivity theorem [52, 53, 74]. However, this approach encounters a significant hurdle for samples from the binary erasure channel [52]. The addition of the security constraint in our setting helps overcome this hurdle. Essentially, we show that the *only* secure non-interactive simulation reduction among samples of the erasure channel is the following linear reduction. Alice outputs the parity of the first k-bits of her input x^n, and Bob outputs the parity of the first k-bits of $y^n \in \{0,1\}^k \times \{0,1,\perp\}^{n-k}$; otherwise Bob outputs $\perp$. This protocol is a perfect SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$, where $(1-\varepsilon') = (1-\varepsilon)^k$. Interestingly, this protocol is identical in spirit to the OWSC protocol, as presented in [39] when $(1-\varepsilon') \in \{(1-\varepsilon), (1-\varepsilon)^2, \dots\}$. However, all other values of ε' are feasible *only* for OWSC [39].

This linear construction achieves the optimal rate as well. To obtain multiple output samples, one treats each consecutive k input samples as a block and extracts one $\mathsf{BES}(\varepsilon')$ sample from each block using the linear reduction function above.

Remark 9. *Informal Theorem 2 implies that if there is a statistically secure SNIS then there is also a perfectly secure SNIS. This type of results have also been discovered previously in the context of various other characterization problems in cryptography. For example, [63, 8] characterized all two-party symmetric deterministic function evaluations that have a perfectly secure protocol in the information-theoretic model. Incidentally, this characterization also extends to the statistical security case [66, 62]. However, a general result showing the equivalence of "perfect security" and "statistical security" is not known.*

2.5 BSS from BSS Samples

Finally, we consider the inter-conversion among binary symmetric samples with different noise characteristics.

Informal Theorem 3 (BSS Samples: Feasibility & Rate)**.** *Fix noise parameters $\varepsilon, \varepsilon' \in (0, 1/2)$.*
Feasibility characterization. *The following statements are equivalent.*

1. *There is a $o(1)$-SNIS of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BSS}(\varepsilon)$.*
2. *There is a 0-SNIS of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BSS}(\varepsilon)$ (a perfectly secure SNIS).*
3. *There exists $k \in \mathbb{N}$ satisfying $(1-2\varepsilon') = (1-2\varepsilon)^k$.*

Rate characterization. *Fix any noise parameters $\varepsilon, \varepsilon' \in (0, 1/2)$, such that $(1-2\varepsilon') = (1-2\varepsilon)^k$ and $k \in \mathbb{N}$. If a $o\big(1/n^{36+9k/2}\big)$-SNIS of $\mathsf{BSS}(\varepsilon')^{\otimes m(n)}$ from $\mathsf{BSS}(\varepsilon)^{\otimes n}$ exists, then $m(n)/n \leqslant 1/k$ and the production rate $R(\,\mathsf{BSS}(\varepsilon'), \mathsf{BSS}(\varepsilon)\,) = 1/k$.*

In fact, we prove an extension of Informal Theorem 3 in Appendix A where the target can be $\mathsf{BSS}(\varepsilon_1) \otimes \mathsf{BSS}(\varepsilon_2) \otimes \cdots \otimes \mathsf{BSS}(\varepsilon_m)$ instead of $\mathsf{BSS}(\varepsilon')^{\otimes m}$.

We prove that if there is one pair of reduction functions that is perfectly secure then the conclusion above hold as well (see Theorem 1).

Note that one cannot increase the reliability of the binary symmetric channel, which is identical to the result in [39]. However, unlike [39], we also rule out the possibility of secure non-interactive simulation for any $(1-2\varepsilon') \notin \big\{(1-2\varepsilon), (1-2\varepsilon)^2, \dots\big\}$. 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 the first k-bits of her input x^n, and Bob also outputs the parity of the first k-bits 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 $(1-2\varepsilon') = (1-2\varepsilon)^2$. 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.[7] However, interestingly, there exists non-linear reduction functions $f_n = g_n$ for $n = 4$. For example, consider the reduction function below.

$$\begin{aligned}
&\text{Function definition:} && f_4(x^4) = \frac{2 - (-1)^{x_1^4+x_3^4} - (-1)^{x_2^4+x_3^4} - (-1)^{x_1^4+x_4^4} + (-1)^{x_2^4+x_4^4}}{4} \\
&\text{The preimage of 0:} && f_4^{-1}(0) = \{0000, 0001, 1000, 0110, 1001, 1011, 1110, 1111\} \\
&\text{The preimage of 1:} && f_4^{-1}(1) = \{0010, 1000, 0011, 0101, 1010, 1100, 0111, 1101\}\,.
\end{aligned} \tag{1}$$

However, even using non-linear reductions, we prove that the rate cannot surpass $1/k$, when $(1-2\varepsilon') = (1-2\varepsilon)^k$. Similar to the case for the reduction among BES samples, the natural protocol that treats each consecutive k input samples as a block and extracts one $\mathsf{BSS}(\varepsilon')$ sample from each block using the parity reduction function achieves the optimal rate.

2.6 Technical Contribution: Fourier Spectrum Concentration

For the presentation in this section, consider SNIS of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BSS}(\varepsilon)$. We prove the following technical result that captures an essential property of SNIS. Our feasibility result, and, in turn, our rate results rely on similar Fourier spectrum concentration bounds.

Theorem 1 (Fourier Spectrum Concentration)**.** *For any constants $\varepsilon', \varepsilon \in (0, 1/2)$, and for any fixed $n \in \mathbb{N}$, the following two statements are equivalent.*

1. *There exist reduction functions $f, g\colon \{0,1\}^n \to \{-1, 1\}$, such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^0_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$.*
2. *There is a constant $k \in [n]$ such that $(1-2\varepsilon') = (1-2\varepsilon)^k$, (a) $f = g$, and (b) $W_k[f] = W_k[g] = 1$.*

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

Observe that this result is an *equivalent* characterization of perfect-SNIS using Fourier analytic properties of Boolean functions. Perfect-SNIS is equivalent to the Fourier spectrum being concentrated at one degree $k \in \mathbb{N}$. Consequently, if there is a pair of Boolean reduction functions f, g satisfying condition (2) above, then it shall define a secure SNIS. We emphasize that the Fourier concentration is *not* necessarily on one function, it is on functions of identical weight (refer to the reduction function in Equation 1).

Furthermore, extending the result of Theorem 1 to any insecurity $\nu(n) \geqslant 0$, we show a necessary condition on the Fourier spectrum concentration of reduction functions. That is, if there are reduction functions $f, g\colon \{0,1\}^n \to \{-1,1\}$ satisfying $\mathsf{BSS}(\varepsilon') \sqsubseteq_{f,g}^{\nu(n)} \mathsf{BSS}(\varepsilon)^{\otimes n}$, then there is a constant $k \in [n]$ such that (1) $(1-2\varepsilon')$ is δ-close to $(1-2\varepsilon)^k$, (2) the outputs of f and g agree at $(1-\delta)$ fraction of inputs, (3) $W_k[f] \geqslant 1-\delta$, and (4) $W_k[g] \geqslant 1-\delta$, where $\delta = \Theta(\mathsf{poly}(\nu(n)))$ (see Lemma 4 and Lemma 1 for the formal results).

For SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$, a similar analysis applies to Alice's reduction function f. After that, we capture the properties of Bob's reduction function, which has domain $\{-1,0,+1\}$ representing $\{1,\perp,0\}$, respectively, using restrictions of f on sub-cubes (refer to Theorem 10, Lemma 2, Lemma 1).

3 Technical Overview

In this section we provide the intuition underlying our proof techniques.

3.1 Derandomization

Suppose $(U,V) \sqsubseteq_{f_n,g_n} (X,Y)^{\otimes n}$, such that the reduction functions f_n and g_n are randomized. For the ease of presentation, assume that there is no insecurity in this reduction. Fix $Y^n = y^n$ such that $y^n \in \mathrm{Supp}(Y^n)$. Consider the distribution $D = (f_n(X^n, R_A) \mid Y^n = y^n)$. Note that the distribution D has to be identical to some conditional distribution $(U|V=v)$, where $v \in \mathrm{Supp}(V)$. Otherwise, the statistical distance of D from each of the conditional distributions $(U|V=v)$, where $v \in \mathrm{Supp}(V)$, is a constant. In which case, for $Y^n = y^n$, the reduction incurs a constant insecurity.

Assume that $D = (U|V=v^*)$. Observe that for all Bob randomness r_B such that $g_n(y^n, r_B) \neq v^*$, the reduction again incurs constant insecurity. Consequently, one assumes that the function $g_n(y^n, r_B)$ does not depend on r_B. Therefore, the deterministic function $g'_n(y^n) = v^*$ is a faithful simulation of the random variable $g_n(y^n, R_B)$.

The actual proof, proceeds by averaging arguments, a.k.a., the Markov inequality. Theorem 5 presents the actual statement and Appendix C presents the full proof. Henceforth, we assume that all reduction functions are deterministic, without loss of generality (refer to the "Subtlety" paragraph in Section 2.2 regarding this assumption for rate characterization problems).

3.2 Impossibility of SNIS of BSS from BES

Theorem 8 states our exact theorem statement, and Section 9.1 provides the full proof. Fix constant $\varepsilon \in (0,1)$ and $\varepsilon' \in (0,1/2)$. If possible let, there exists $\mathsf{BSS}(\varepsilon') \sqsubseteq_{f_n,g_n}^{\nu(n)} \mathsf{BES}(\varepsilon)^{\otimes n}$. So, our reduction functions $f_n\colon \{0,1\}^n \to \{0,1\}$ and $g_n\colon \{0,1,\perp\}^n \to \{0,1\}$. Our argument proceeds along the following high-level intuition.

Part 1. We focus on elements $a^n \in \{0,1\}^n$ and $b^n \in \{0,1\}^n$ such that they differ exactly in one coordinate (i.e., they are neighbors in the Boolean hypercube), $f_n(a^n) = 0$, but $f_n(b^n) = 1$. We say that a^n is consistent with $y^n \in \{0,1,\perp\}^n$, represented by $a^n \vdash y^n$, if one can obtain y^n by passing

a^n through an erasure channel. We define three disjoint subsets $T_0, T_1, T_{\text{both}} \subseteq \{0,1,\perp\}^n$ below.

$$T_0 = \{y^n : y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \nvdash y^n\}$$
$$T_1 = \{y^n : y^n \in \{0,1,\perp\}^n, a^n \nvdash y^n, b^n \vdash y^n\}$$
$$T_{\text{both}} = \{y^n : y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \vdash y^n\}$$

One can argue that

$$\Pr[Y^n \in T_0 | X^n = a^n] = \Pr[Y^n \in T_1 | X^n = b^n] = (1-\varepsilon)$$
$$\Pr[Y^n \in T_{\text{both}} | X^n = a^n] = \Pr[Y^n \in T_{\text{both}} | X^n = b^n] = \varepsilon$$

Consider the partition $W_0 = g_n^{-1}(0)$ and $W_1 = g_n^{-1}(1)$. When one passes a^n through the erasure channel, it should generate elements in W_0 with probability $(1-\varepsilon')$, and elements in W_1 with probability ε'. Similarly, one passes b^n through the erasure channel, it should generate elements in W_1 with probability $(1-\varepsilon')$ and elements in W_0 with probability ε'. Roughly, this can be achieved by setting $T_0 \subseteq W_0$, $T_1 \subseteq W_1$ and equally partitioning T_{both} across W_0 and W_1, when $\varepsilon' = \varepsilon/2$. However, when $\varepsilon' \neq \varepsilon/2$, any partition strategy shall contribute to the insecurity of the reduction, which is proportional to $|\varepsilon' - \varepsilon/2|$. Consequently, for every pair of witness (a^n, b^n), any $\varepsilon' \neq \varepsilon/2$ shall account for a "constant insecurity."

We rely on an isoperimetric-type inequality on the Boolean hypercube to argue that there are (approximately) $2^n/\sqrt{n}$ pairs of points (a^n, b^n) that satisfy the above-mentioned property [16].[8] Therefore, with $1/\sqrt{n}$ probability, one encounters the event of incurring constant insecurity. Consequently, all $\varepsilon' \neq \varepsilon/2$ are outrightly insecure.

Part 2. Next, our objective is to rule out the isolated case of $\varepsilon' = \varepsilon/2$ that survived the previous argument. We shall use the parallel composition of the original SNIS to obtain two samples of $\mathsf{BSS}(\varepsilon')$. That is,

$$\mathsf{BSS}(\varepsilon')^{\otimes 2} \sqsubseteq^{2\nu(n)} \mathsf{BES}(\varepsilon)^{\otimes 2n}.$$

We know that the parity reduction functions realizes the following perfectly secure SNIS.

$$\mathsf{BSS}(\varepsilon'') \sqsubseteq^{0} \mathsf{BSS}(\varepsilon'),$$

where $(1-2\varepsilon'') = (1-2\varepsilon')^2 = (1-\varepsilon)^2$. That is, we have $\varepsilon'' = \varepsilon - \varepsilon^2/2$. By the sequential composition of these two SNIS, we obtain

$$\mathsf{BSS}(\varepsilon - \varepsilon^2/2) \sqsubseteq^{2\nu(n)} \mathsf{BES}(\varepsilon)^{\otimes 2n}.$$

Now, since $\varepsilon - \varepsilon^2/2 \neq \varepsilon/2$, for all $\varepsilon \in (0,1)$, the final SNIS contradicts the result in the first part of the proof, which ruled out all constant $\varepsilon' \neq \varepsilon/2$.

3.3 Characterization of SNIS feasibility and rate for BES from BES

Let us begin by considering some SNIS construction in this context. Suppose $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$. The input samples are over the sample space $(\mathcal{X}, \mathcal{Y}) = (\{0,1\}, \{0,1,\perp\})$ and the output sample space is $(\mathcal{U}, \mathcal{V}) = (\{1,-1\}, \{1,-1,0\})$.[9] For $n \geqslant k$, define the reduction function $f_n^* : \{0,1\}^n \to \{1,-1\}$ and $g_n^* : \{0,1,\perp\}^n \to \{1,-1,0\}$ as follows.

$$f_n^*(x^n) = (-1)^{x_1^n + x_2^n + \cdots + x_k^n}$$
$$g_n^*(y^n) = \begin{cases} (-1)^{y_1^n + y_2^n + \cdots + y_k^n}, & \text{if } y^n \in \{0,1\}^k \times \{0,1,\perp\}^{n-k} \\ 0, & \text{otherwise.} \end{cases}$$

[8] A naïve application of (vertex) isoperimetric inequality over the Boolean hypercube [45] yields $1/n^{3/2}$ probability instead of $1/n^{1/2}$, slightly worsening the upper-bound on $\nu(n)$.

[9] The output samples use the *multiplicative* notation. Intuitively, the bit 0 is mapped to $(-1)^0 = 1$, the bit 1 is mapped to $(-1)^1 = -1$, and one defines $(-1)^\perp$ to be 0.

One observes that $\mathsf{BES}(\varepsilon') \sqsubseteq^{0}_{f_n^*, g_n^*} \mathsf{BES}(\varepsilon)^{\otimes n}$. The simulators for these reduction functions are computationally efficient because the reduction functions are linear. We shall prove that these k-term (multi-)linear reduction functions are the *only* reductions possible when $(1-\varepsilon') = (1-\varepsilon)^k$.

Next, let us move on to proving the feasibility and rate results. Theorem 9 provides the formal theorem statement, and Section 9.2 provides the full proof. In the following, suppose $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\varepsilon)^{\otimes n}$ for fixed constants $\varepsilon, \varepsilon' \in (0,1)$.

Feasibility Characterization. This proof proceeds by Fourier analysis. We provide a very high-level intuition for the sequence of arguments that we use. The first step is to algebraize the notion of security and obtain a non-trivial restriction on the Boolean reduction function f_n. Define $\rho := (1-\varepsilon)$ and $\rho' := (1-\varepsilon')$. For a SNIS reduction between BES samples, relying on insecurity being $\nu(n) = o(1)$, we show that the following quantity is also $o(1)$.

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

That is, the ρ-noisy version of f_n is (close to) the ρ' scaling of f_n itself in the L_1-norm. We refer to this technical constraint as the "rank-one constraint" for brevity. Then, we apply the following main technical lemma.

Lemma 1. *Let $\rho, \rho' \in (0,1)$, and let $f_n \colon \{0,1\}^n \to \{-1,1\}$ be a Boolean function. Suppose that*

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

Then, there is $k \in [n]$ such that $\left|\rho' - \rho^k\right| \leqslant \sqrt{(1+\rho')\delta}$. Furthermore, the following bound holds.

$$W_k[f_n] := \sum_{|S|=k} \widehat{f_n}(S)^2 \geqslant 1 - \frac{(1+\rho')}{(1-\rho)^2 \rho'^2} \cdot \delta.$$

This lemma proves that if the "rank-one constraint" holds for a Boolean function f_n, then ρ' is close to ρ^k for some $k \in \mathbb{N}$. Furthermore, the spectral weight of the Boolean function f_n is primarily concentrated on size-k (multi-)linear terms. After that, an analysis specific to SNIS for inter-converting BES samples proves that the function f_n must have most of its spectral weight on one single size-k (multi-)linear term. Then, one obtains the characterization of the function g_n from the security definition.

Rate Characterization. At the outset we remind the readers that there is a subtlety of using the derandomization result for rate characterization problems (refer to the paragraph "Subtlety" in Section 2.2). Our actual proof outline will follow the steps outlined in that section. For simplicity, in the presentation below, we assume that the reduction functions are deterministic. Suppose $(1-\varepsilon') = (1-\varepsilon)^k$ and we have $\mathsf{BES}(\varepsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\varepsilon)^{\otimes n}$.

Incorrect "proof." Let us begin the technical overview with an incorrect "proof" to highlight additional subtleties. We know that using the linear reduction functions, the following SNIS holds.

$$\mathsf{BES}(\varepsilon'') \sqsubseteq^{0} \mathsf{BES}(\varepsilon')^{\otimes m(n)},$$

where $(1-\varepsilon'') = (1-\varepsilon')^{m(n)} = (1-\varepsilon)^{k \cdot m(n)}$. By the sequential composition of these two SNIS, we obtain that

$$\mathsf{BES}(\varepsilon'') \sqsubseteq^{\nu(n)} \mathsf{BES}(\varepsilon)^{\otimes n}.$$

Therefore, we must have $k \cdot m(n) \leqslant n \implies m(n) \leqslant \lfloor n/k \rfloor$.

There is a *major flaw* in this argument. The parameter ε'' is *not* a constant in $(0,1)$. In fact, we have $(1-\varepsilon'') = (1-\varepsilon)^{k \cdot m(n)}$, which is negligible in n. The feasibility argument mentioned above does not apply to this ε''.

Correct proof. Now, let us proceed with the outline of the correct proof. Let $f_n^{(i)}, g_n^{(i)}$ be the projections of f_n, g_n, respectively, that output only the i-th output samples, where $1 \leqslant i \leqslant m(n)$. Similarly, for $1 \leqslant i < j \leqslant m(n)$, $f_n^{(i,j)}, g_n^{(i,j)}$ be the projections of f_n, g_n, respectively, that output only the i-th and the j-th output samples. By the projection of the SNIS, one concludes the following three SNIS holds for all $1 \leqslant i < j \leqslant m(n)$.

$$\text{(i) } \mathsf{BES}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n^{(i)}, g_n^{(i)}} \mathsf{BES}(\varepsilon)^{\otimes n},$$
$$\text{(ii) } \mathsf{BES}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n^{(j)}, g_n^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}, \text{ and}$$
$$\text{(iii) } \mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{\nu(n)}_{f_n^{(i,j)}, g_n^{(i,j)}} \mathsf{BES}(\varepsilon)^{\otimes n}.$$

We know that $\mathsf{BES}(\varepsilon'') \sqsubseteq^0 \mathsf{BES}(\varepsilon')^{\otimes 2}$ using the linear reduction functions, where $(1-\varepsilon'') = (1-\varepsilon')^2 = (1-\varepsilon)^{2k}$. We shall represent the reductions functions for this SNIS as $f_n^{(i)} \cdot f_n^{(j)}$ and $g_n^{(i)} \cdot g_n^{(j)}$. Therefore, the sequential composition with SNIS (iii) above yields the following SNIS

$$\text{(iv) } \mathsf{BES}(\varepsilon'') \sqsubseteq^{\nu(n)}_{f_n^{(i)} \cdot f_n^{(j)}, g_n^{(i)} \cdot g_n^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}.$$

Now, let us consider the SNIS (i), (ii), and (iv). SNIS (i) implies that the Fourier spectrum of $f_n^{(i)}$ is concentrated on k-term (multi-)linear functions. Similarly, SNIS (ii) implies that the Fourier spectrum of $f_n^{(j)}$ is concentrated on k-term (multi-)linear functions. Finally, the spectrum of $f_n^{(i)} \cdot f_n^{(j)}$ is the convolution of the Fourier spectrum of $f_n^{(i)}$ and $f_n^{(j)}$, which, by SNIS (iv) is concentrated on $2k$-term (multi-)linear functions. These observations imply that the k-term linear functions in the Fourier spectrum of $f_n^{(i)}$ are essentially disjoint from the k-term linear functions in the Fourier spectrum of $f_n^{(j)}$; otherwise, the Fourier spectrum of $f_n^{(i)} \cdot f_n^{(j)}$ would have observable weight on $(< 2k)$-term (multi-)linear functions.

Once, we have this conclusion for every pair of $1 \leqslant i < j \leqslant m(n)$, using union bound, one shows that f_n must have $k \cdot m(n)$ inputs, which implies $m(n) \leqslant \lfloor n/k \rfloor$.

3.4 Characterization of SNIS feasibility and rate for BSS from BSS

First, we begin by considering some SNIS constructions. Suppose $(1-2\varepsilon') = (1-2\varepsilon)^k$, for some $k \in \mathbb{N}$. The input samples are from the sample space $(\mathcal{X}, \mathcal{Y}) = (\{0,1\}, \{0,1\})$, and the output sample space is $(\mathcal{U}, \mathcal{V}) = (\{1,-1\}, \{1,-1\})$. For $n \geqslant k$, define the reduction function $f_n^*\colon \{0,1\}^n \to \{1,-1\}$ and $g_n^*\colon \{0,1\}^n \to \{1,-1\}$, as follows.

$$f_n^*(x^n) = (-1)^{x_1^n + x_2^n + \cdots + x_k^n}, \qquad g_n^* = f_n^*.$$

Note that $\mathsf{BSS}(\varepsilon') \sqsubseteq^0_{f_n^*, g_n^*} \mathsf{BSS}(\varepsilon)^{\otimes n}$. These k-term (multi-)linear reduction functions are the *most efficient* reductions possible when $(1-\varepsilon') = (1-\varepsilon)^k$. Similar to the previous case, the simulators for these linear reductions are efficient as well.

For every k, there are additional feasible SNIS reductions, however, they need more than k input samples to generate one output sample. Equation 1 presents one such example. Computationally efficient simulators for these reductions can rely on rejection sampling (because ε' is a constant) to achieve statistical security (not, perfect security).

Theorem 11 provides the formal theorem statement, and Section 10 provides the full proof. In this case, the only change is that $\rho := (1-2\varepsilon)$ and $\rho' := (1-2\varepsilon')$. The rest of the proof intuition essentially remains identical to the SNIS involving BES case. Except that, for SNIS for inter-converting BSS samples, the Boolean reduction function f_n need not be linear. After that, one obtains the characterization that $g_n = f_n$ using the security definition.

4 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 in this one section. Consequently, we cite and discuss only the most relevant literature on 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), namely, *non-interactive simulation of joint distributions* (NIS). This line of research starts with the seminal works of Gács and Körner [38], Witsenhausen [88], and Wyner [94]. The primary difference of this concept from our object of study is 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 may be insecure. Let us consider an illustrative example highlighting this difference. Consider simulating one sample of $\mathsf{BSS}(\varepsilon/2)$ from multiple samples of $\mathsf{BES}(\varepsilon)$. 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.[10] Note that this non-interactive simulation is not secure.[11] 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 [43, 36]. Technically, reverse hypercontractivity [4, 17, 72, 73, 53, 36, 10, 71], and maximal correlation [46, 88, 4, 84, 5] 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 [86] 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 [72, 71, 95, 15, 25].

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. However, random samples from noisy channels like binary erasure channels [81, 82, 30], and binary symmetric channels [31] suffice for general secure computation [96, 44, 90] (relying on interactive protocols). Kilian [59] exactly characterized all joint distributions that enable general secure computation. The benefit of secure computation based on samples of joint distributions 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 useful for secure computation, may perform general secure computation in a constant number of rounds [47, 48, 7, 51]. In fact, one can also perform secure computation at a constant rate[12] [49]. Recently, Garg, Ishai, Kushilevitz, Ostrovsky, and Sahai [39] 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

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

[11] 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) $\frac{\varepsilon/2}{(1-\varepsilon)+\varepsilon/2}$ as the first simulated sample from $\mathsf{BES}(\varepsilon)$, and output 0 with probability (close to) $\frac{1-\varepsilon}{(1-\varepsilon)+\varepsilon/2}$ as the first simulated sample from $\mathsf{BES}(\varepsilon)$; 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) $\frac{1-\varepsilon}{(1-\varepsilon)+\varepsilon/2}$, Bob's simulated first sample of $\mathsf{BES}(\varepsilon)$ is inconsistent with Alice's output. Therefore, no secure simulation strategy for Bob exists.

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

symmetric and binary erasure channels. Agrawal et al. [1] prove the completeness of finite channels (with inverse polynomial error) by realizing string-ROT from bit-OT. To complement this result, they also show that no finite channel is complete with negligible error. The proposed notion of SNIS in our work permits no communication between the parties. Recently, Narayanan, Prabhakaran, and Prabhakaran [75] introduced a new primitive called Zero-communication Reduction (ZCR) that is different from SNIS. In ZCR, each party is given an independent input and has access to a correlation. Their goal is to locally produce an output candidate along with an input to a predicate. The correctness requires that when the predicate outputs "acccepts", the output candidates produced by the two parties must be correct, and correctness is not guaranteed when the predicate outputs "rejects". Moreover, a typically exponentially small lower bound on the probability of acceptance is required. They defined three variants corresponding to different levels of security. The primitive ZCR is an extension of zero-communication protocols used for studying communication and information complexity (see [54]).

Bounding efficiency of secure constructions. There has been work on lower-bounding the efficiency of secure computations via interactive protocols, for example, the monotones of [89], and assisted common information [78, 79, 80, 83].

5 Application: Versatile Offline Phase for Secure Computation

This section presents the problem of deploying off-the-shelf secure computation solutions using diverse noise sources, which SNIS can enable without additional communication.

Representative motivating scenario. Frequently, one comes across signals arising from cataclysmic celestial events or their aftereffects that are well beyond human influence. For example, 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 (more generally) secure computation [32, 58, 59, 51, 49, 60].[13] There has been extensive research into the feasibility and efficiency of founding secure computation on such noise sources. Within this research, out of efficiency concerns, the following natural question arises.

"How to efficiently build a versatile infrastructure for cryptography
from correlated samples
without any additional interaction between the observatories?"

[13] This is the most appropriate opportunity to quote the following paragraphs from Crépeau and Kilian [32]. "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 [94]), 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 seminal works of Maurer [68, 69, 70], and Ahlswede and Csiszár [2, 3] introduced the concept of building an infrastructure for shared private randomness using sources of noise. Our emphasis is on enabling general secure computation, which is a strictly stronger cryptographic primitive [41, 65].

Offline-online paradigm. The *offline-online paradigm* of secure computation [67, 14, 35, 76] 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 [40] or somewhat homomorphic encryption [20]). However, an increase in computational power due to shifts in computing paradigms or an improvement in adversarial attacks' efficiency due to new mathematical advances may potentially render these protocols insecure. On the other hand, correlated randomness from noisy sources enables secure computation even against adversaries with unbounded (classical/quantum) computational power. Therefore, the motivating scenario above can generate highly efficient infrastructure for secure computation that never forfeits its security.

Application. In fact, the non-interactive simulation allows the parties to specify the infrastructure (say, the noise characteristics) well after the correlated samples have been observed. Furthermore, the online phase may prefer to use samples from a noise source with a *particular noise characteristic* due to efficiency considerations. For example, this choice may be guided by the particular multiplication friendly error-correcting code being used [29] in the online protocol, or the probability of including servers on the *watchlist* [51]. Although the celestial source's noise parameter is beyond our control, it would be desirable if the parties can non-interactively simulate samples of an alternate noise source with a noise characteristics that the online protocol prefers. Enabling this non-interactive conversion, allows parties to deploy off-the-shelf secure computation solutions using samples from diverse noise sources without any increase in round or communication complexity.

6 Preliminaries

6.1 Notation

We denote $[n]$ as the set $\{1, 2, \dots n\}$, and N as 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 write $f = g$ to denote that 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 $(\mathcal{X}, \mathcal{Y})$ to denote a joint probability space. We use capital letters $X, Y, \dots$ to denote random variables. For $x^n \in \mathcal{X}^n$, $x_i^n \in \mathcal{X}$ represents the i-th coordinate of x^n.

For a function $f\colon \mathcal{D} \to \mathcal{R}^m$, the function $f^{(i)}\colon \mathcal{D} \to \mathcal{R}$, where $i \in [m]$, denotes the mapping that on input $x \in \mathcal{D}$ returns the ith coordinate of $f(x) \in \mathcal{R}^m$. The function $f^{(i)}$ is called the projection of f on the i-th coordinate.

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

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

6.2 Correlated Random Sources and Noise Operator

Binary Symmetric Source. A binary symmetric source with flipping probability $\varepsilon \in (0,1)$, denoted as $\mathsf{BSS}(\varepsilon)$, is a joint distribution over the sample space $\{-1,1\} \times \{-1,1\}$ such that if $(X,Y) \xleftarrow{\$} \mathsf{BSS}(\varepsilon)$, then $\Pr[X = 1, Y = -1] = \Pr[X = -1, Y = 1] = \varepsilon/2$, and $\Pr[X = 1, Y = 1] = \Pr[X = -1, Y = -1] = (1 - \varepsilon)/2$. We write ρ to denote the correlation of the source $\mathsf{BES}(\varepsilon)$. Note that $\rho = 1 - 2\varepsilon$.

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

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 $y^n \xleftarrow{\$} N_\rho(x^n)$ 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 chosen uniformly at random with probability $1-\rho$. We say that y^n is ρ-correlated to x^n. 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 $\mathsf{T}_\rho f(x^n) = \mathbb{E}_{y^n \sim N_\rho(x^n)}[f(y^n)]$.

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

6.3 Fourier Analysis for Boolean Functions: Preliminaries

We recall some background in Fourier analysis that will be useful for our analysis (see [77] 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.

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

For each $S \subseteq [n]$, the characteristic function $\chi_S(x^n) = (-1)^{S \cdot x^n} = (-1)^{\sum_{i \in S} x_i}$ is a linear function that computes the parity (that is, the exclusive-or) of the bits $(x_i)_{i \in S}$. The set of 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 $f = \sum_{S \subseteq [n]} \widehat{f}(S)\chi_S$ which is 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 $W_k[f] = \sum_{S:|S|=k} \widehat{f}(S)^2$. We denote the set of all possible size-k subsets of the set $\{1,2,\ldots,n\}$ by $\mathcal{W}_k$. Parseval's Identity says that $\|f\|_2^2 = \mathbb{E}_{x^n \sim \mathbb{U}_{\{0,1\}^n}} f(x^n)^2 = \sum_{S \subseteq [n]} \widehat{f}(S)^2$ where $\mathbb{U}_{\{0,1\}^n}$ denotes uniform distribution over $\{0,1\}^n$.

Next we summarize the basic Fourier analysis on Boolean function with *restriction* on the subcubes. 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 $S \subseteq J$. Then, when we assume that $z \in \{0,1\}^{|\bar{J}|}$ is chosen uniformly at random, we have

$$\mathop{\mathbb{E}}_{z}[\widehat{f_{J|z}}(S)] = \widehat{f}(S) \tag{2}$$

$$\mathop{\mathbb{E}}_{z}[\widehat{f_{J|z}}(S)^2] = \sum_{T \subseteq \bar{J}} \widehat{f}(S \cup T)^2 \tag{3}$$

Definition 1 (Spectral Sample)**.** *For each function $f\colon \{0,1\}^n \to \mathbb{R}$, the spectral sample for f, denoted as $\mathcal{S}(f)$, is the probability distribution on subsets of $[n]$ in which the set S has probability $\widehat{f}(S)^2 / \sum_{T \subseteq [n]} \widehat{f}(T)^2$. In particular, if $f\colon \{0,1\}^n \to \{-1,1\}$ is a boolean function then its associated spectral sample $\mathcal{S}(f)$ is the distribution where the probability of sampling any set $S \subseteq [n]$ is given by $\widehat{f}(S)^2$.*

7 Secure Non-Interactive Simulation: Simulation-based Definition

In this section, we define the notion of secure non-interactive simulation of joint distributions using a simulation-based security definition [22, 21, 23]. 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 $f \colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{U}$ and $g \colon \mathcal{Y}^n \times \mathcal{R}_B \to \mathcal{V}$ be two reduction functions where $\mathcal{R}_A$ and $\mathcal{R}_B$ denote respectively the space of private random used by Alice and Bob.

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 samples private randomness r_A from $\mathcal{R}_A$ and outputs $u' = f(x^n, r_A)$.
3. Bob samples private randomness r_B from $\mathcal{R}_B$ and outputs $v' = g(y^n, r_B)$.

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

$$\mathsf{SD}\left(\ (U, V) \ , \ (f(X^n, R_A), g(Y^n, R_B)) \ \right) \leqslant \nu(n).$$

2. **The case of Corrupt Alice.** Suppose the environment statically corrupt Alice. In the real world, the simulator receives $((X^n, R_A), f(X^n, R_A), g(Y^n, R_B))$. In the ideal world, we have a simulator $\mathrm{Sim}_A \colon \mathcal{U} \to \mathcal{X}^n \times \mathcal{R}_A$ 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.

$$\mathsf{SD}\left(\ (\mathrm{Sim}_A(U), U, V) \ , \ ((X^n, R_A), f(X^n, R_A), g(Y^n, R_B)) \ \right) \leqslant \nu(n).$$

3. **The case of Corrupt Bob.** Analogously, there exists a simulator for Bob $\mathrm{Sim}_B \colon \mathcal{V} \to \mathcal{Y}^n \times \mathcal{R}_B$ and the following must hold if this reduction has at most $\nu(n)$ insecurity.

$$\mathsf{SD}\left(\ (U, V, \mathrm{Sim}_B(V)) \ , \ (f(X^n, R_A), g(Y^n, R_B), (Y^n, R_B)) \ \right) \leqslant \nu(n).$$

If there exists reductions functions f, g 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.

7.1 Composition

In this section, we shall prove the sequential and parallel composition theorems, and the security of projection operation for SNIS.

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 $(x, y) \xleftarrow{\$} (X, Y)$, sample $(x', y') \xleftarrow{\$} (X', Y')$, 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 2 (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 3 (Sequential Composition)**.** *For joint distribution P, Q, and R, suppose we have*

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

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. □

Suppose $f_n \colon \Omega \to \Omega' \times \Omega''$, then the projection function $f^{(1)}_n \colon \Omega \to \Omega'$ is defined by the mapping $x \mapsto y$ if $f_n(x) = (y, z)$, for some $z \in \Omega''$. Next, we formally state that projections preserve security.

Theorem 4 (Projection). *For joint distribution P, Q, and R, suppose we have*

$$(P\|Q) \sqsubseteq^{\nu(n)}_{f_n,g_n} R.$$

Then, the following holds.

$$P \sqsubseteq^{\nu(n)}_{f_n^{(1)},g_n^{(1)}} R.$$

Proof. The proof is a corollary of statistical distance satisfying the triangle inequality. □

7.2 Derandomization of Reductions

In this section, we state the drandomization of reduction functions formally as follows. We provide the proof in Appendix C.

Theorem 5 (Rate-preserving Derandomization of Reduction Functions). *Let (U, V) and (X, Y) be two joint distributions. Let $n \in \mathbb{N}$ and $\nu(n) \geqslant 0$. Suppose there exist randomized reduction functions $f\colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{V}$, and $g\colon \mathcal{Y}^n \times \mathcal{R}_B \to \mathcal{U}$ such that $(U, V) \sqsubseteq^{\nu(n)}_{f,g} (X, Y)^{\otimes n}$. Then, there exists a constant γ (which depends on the target distribution (U, V)), and (deterministic) reduction functions $f'\colon \mathcal{X}^n \to \mathcal{U}$, and $g'\colon \mathcal{Y}^n \to \mathcal{V}$ such that $(U, V) \sqsubseteq^{\gamma\nu(n)^{1/9}}_{f',g'} (X, Y)^{\otimes n}$.*

Intuitively, Theorem 5 says that if there exists a ν-SNIS of (U, V) from (X, Y) using randomized reduction functions, then there exists a $\Theta(\nu^{1/9})$-SNIS of (U, V) from (X, Y) using deterministic reduction functions that uses the same number of samples.

7.3 Rank-characterization of Security

Suppose there exist $n \in \mathbb{N}$, $f\colon \mathcal{X}^n \to \mathcal{U}$, and $g\colon \mathcal{Y}^n \to \mathcal{V}$ such that $(U, V) \sqsubseteq^{\nu(n)}_{f,g} (X, Y)^{\otimes n}$. Let M denote the matrix that represents the probability mass function of the joint distribution $(X, Y)^{\otimes n}$ i.e. M has $|\mathcal{X}|^n$ rows and $|\mathcal{Y}|^n$ columns and each row in M is indexed by a unique $x^n \in \mathcal{X}^n$ and each column in M is indexed by a unique $y^n \in \mathcal{Y}^n$ and $M(x^n, y^n)$, the element at row x^n and column y^n, is equal to $\Pr[X^n = x^n, Y^n = y^n]$ (refer to Table 2). For $u \in \mathcal{U}$, let $\mathcal{A}_f(u) := \{x^n \in \mathcal{X}^n | f(x^n) = u\}$ and for $v \in \mathcal{V}$ let $\mathcal{B}_g(v) := \{y^n \in \mathcal{Y}^n | g(y^n) = v\}$. Let M_A denote the matrix of size $|\mathcal{U}| \times |\mathcal{Y}|^n$ achieved by collapsing all the rows whose indices are mapped by f to the same element in $\mathcal{U}$ i.e. for $u \in \mathcal{U}$ and $y^n \in \mathcal{Y}^n$, $M_A(u, y^n) = \sum_{x^n \in \mathcal{A}_f(u)} M(x^n, y^n)$ (refer to Table 4). Similarly, we define M_B as the matrix of size $|\mathcal{X}|^n \times |\mathcal{V}|$ achieved by collapsing all the columns whose indices are mapped by g to the same element in $\mathcal{V}$ i.e. for $v \in \mathcal{V}$ and $x^n \in \mathcal{X}^n$, $M_B(x^n, v) = \sum_{y^n \in \mathcal{B}_g(v)} M(x^n, y^n)$ (refer to Table 3).

Let M_A^v denote the submatrix of M_A achieved by selecting those columns of M_A whose indices belong to $\mathcal{B}_g(v)$. Note that the size of M_A^v is $|\mathcal{U}| \times |\mathcal{B}_g(v)|$. Similarly, let M_B^u denote the submatrix of M_B achieved by selecting those rows of M_B whose indices belong to $\mathcal{A}_f(u)$. Note that the size of M_B^u is $|\mathcal{A}_f(u)| \times |\mathcal{V}|$.

For two matrices P and Q of size $r \times t$, define

$$\mathrm{SD}\,(P, Q) := \frac{1}{2} \sum_{i \in [r]} \sum_{j \in [t]} |P(i, j) - Q(i, j)|.$$

Notice that if both matrices P and Q are representing joint distributions over $[r] \times [t]$, then $\mathrm{SD}\,(P, Q)$ is in fact the statistical distance of the two corresponding distributions.

Theorem 6 and Theorem 7 prove that one can express the security of SNIS as an appropriate rank-one constraint. Appendix B proves these theorems.

Theorem 6. *Suppose there exist $n \in \mathbb{N}$, $f\colon \mathcal{X}^n \to \mathcal{U}$, and $g\colon \mathcal{Y}^n \to \mathcal{V}$ such that $f(U,V) \sqsubseteq_{f,g}^{\nu(n)} (X,Y)^{\otimes n}$, then the two following conditions hold together:*

- *For each $v \in \mathcal{V}$, there exists a rank one matrix T^v of size $|\mathcal{U}| \times |\mathcal{B}_g(v)|$ such that $\mathrm{SD}\left(T^v, M_A^v\right) \leqslant \nu(n)$ and for each $u \in \mathcal{U}$, $\sum_{y^n \in \mathcal{B}_g(v)} T^v(u, y^n) = \Pr[U = u, V = v]$.*
- *For each $u \in \mathcal{U}$, there exists a rank one matrix T^u of size $|\mathcal{A}_f(u)| \times |\mathcal{V}|$ such that $\mathrm{SD}\left(T^u, M_B^u\right) \leqslant \nu(n)$ and for each $v \in \mathcal{V}$, $\sum_{x^n \in \mathcal{A}_f(u)} T^u(x^n, v) = \Pr[U = u, V = v]$.*

Theorem 7. *Suppose there exist $n \in \mathbb{N}$, $f\colon \mathcal{X}^n \to \mathcal{U}$, and $g\colon \mathcal{Y}^n \to \mathcal{V}$ such that the two following conditions hold together:*

- *For each $v \in \mathcal{V}$, there exists a rank one matrix T^v of size $|\mathcal{U}| \times |\mathcal{B}_g(v)|$ such that $\mathrm{SD}\left(T^v, M_A^v\right) \leqslant \nu(n)$ and for each $u \in \mathcal{U}$, we have $\sum_{y^n \in \mathcal{B}_g(v)} T^v(u, y^n) = \Pr[U = u, V = v]$.*
- *For each $u \in \mathcal{U}$, there exists a rank one matrix T^u of size $|\mathcal{A}_f(u)| \times |\mathcal{V}|$ such that $\mathrm{SD}\left(T^u, M_B^u\right) \leqslant \nu(n)$ and for each $v \in \mathcal{V}$, we have $\sum_{x^n \in \mathcal{A}_f(u)} T^u(x^n, v) = \Pr[U = u, V = v]$.*

then, $(U,V) \sqsubseteq_{f,g}^{d \times \nu(n)} (X,Y)^{\otimes n}$ where $d = \max(|\mathcal{U}|, |\mathcal{V}|)$.

8 Examples

This section presents an example of SNIS and an insecure NIS. Section 8.1 presents a SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$, where $(1-\varepsilon') = (1-\varepsilon)^2$. Section 8.2 presents a NIS of $\mathsf{BES}(\varepsilon/2)$ from $\mathsf{BES}(\varepsilon)$, where $\varepsilon \in (0,1)$. However, this NIS is *insecure*. The reason underlying its insecurity highlights the additional constraints needed to ensure security.

8.1 SNIS Example

Consider the secure non-interactive simulation of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)^{\otimes 2}$, where $(1-\varepsilon') = (1-\varepsilon)^2$, with 0 insecurity. For notation, we use x_i^n to represent the coordinate i of a length-n vector. In this case we use the reduction functions $f_2(x^2) = x_1^2 \oplus x_2^2$ 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 2.

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

Table 2: Joint distribution induced by SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)^{\otimes 2}$. 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.

Consider a corrupt Alice (refer to Table 3). The security constraint states that the conditional distribution $(X^n | f_n(X^n) = u, g_n(Y^n) = v)$ is independent of v, Bob's output. Similarly, when Bob is corrupt (refer to Table 4). The security constraint states that the conditional distribution $(Y^n | f_n(X^n) = u, g_n(Y^n) = v)$ is independent of u. Theorem 6 and Theorem 7 abstract these security constraints as equivalent "rank-one constraints" on an appropriate matrix.

8.2 Insecure NIS Example

Consider the non-interactive simulation of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$, where $\varepsilon' = \varepsilon/2$ and $\varepsilon \in (0,1)$. Alice's reduction function is $u = f_1(x^1) = x_1^1$. The reduction function for Bob is randomized (it

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

Table 3: The case of corrupt Alice for SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)^{\otimes 2}$. 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
$u=0$	$\frac{(1-\varepsilon)^2}{4}$	$\frac{(1-\varepsilon)^2}{4}$	$\frac{(1-\varepsilon)\varepsilon}{4}$	$\frac{\varepsilon(1-\varepsilon)}{4}$	$\frac{(1-\varepsilon)\varepsilon}{4}$	$\frac{\varepsilon(1-\varepsilon)}{4}$	$\frac{2\varepsilon^2}{4}$		
$u=1$			$\frac{(1-\varepsilon)\varepsilon}{4}$	$\frac{\varepsilon(1-\varepsilon)}{4}$	$\frac{(1-\varepsilon)\varepsilon}{4}$	$\frac{\varepsilon(1-\varepsilon)}{4}$	$\frac{2\varepsilon^2}{4}$	$\frac{(1-\varepsilon)^2}{4}$	$\frac{(1-\varepsilon)^2}{4}$

Table 4: The case of corrupt Bob for the reduction of $\mathsf{BES}(\varepsilon')$ to $\mathsf{BES}(\varepsilon)^{\otimes 2}$. 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 $\varepsilon(1-\varepsilon)/(4\varepsilon-2\varepsilon^2)$, and outputs $\perp\perp$ with probability $2\varepsilon^2/(4\varepsilon-2\varepsilon^2)$.

takes one additional random bit as input). Bob's reduction function is $g_1(y^1, r_B)$ is defined as follows, where $r_B \in \{0,1\}$. If $y_1^1 \in \{0,1\}$, then $v = y_1^1$, and, if $y_1^1 = \perp$, then $v = r_A$. Observe that $u \neq v$ with probability $\varepsilon/2$. However, this NIS is insecure when Bob is corrupt (this reduction is secure against a corrupt Alice).

Fix Bob's output v. Conditioned on this output, with probability $(1-\varepsilon)$, Bob knows Alice's output exactly. With the remaining ε probability, Bob has no advantage is predicting Alice's output. A secure $\mathsf{BSS}(\varepsilon/2)$ sample needs to ensure that conditioned on Bob's *entire view*, the probability of Alice output being $u = v$ is $(1-\varepsilon/2)$ always. To summarize, NIS allows reduction functions to erase information, which is not allowed by SNIS.

Remark 10. *Note that the NIS above is randomized. One cannot derandomize this while preserving the rate of the reduction. For example, for example Bob can use additional* $\mathsf{BES}(\varepsilon)$ *samples as input to simulate the bit* r_A*. However, the rate worsens. We shall prove that SNIS, on the other hand, admits a sample-preserving derandomization.*

9 SNIS from Binary Erasure Source Samples

In this section we consider reductions to BES.

9.1 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 $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)^{\otimes n}$. 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 $\varepsilon, \varepsilon'$ parameters. This result highlights the crucial role that the notion of "security" plays in the proofs.

		$v=0$		$v=1$	
		00	10	01	11
$u=0$	00	a	b	b	c
	01	b	c	a	b
$u=1$	10	b	a	c	b
	11	c	b	b	a

Table 5: The joint distribution induced by the reduction $f(x_1, x_2) = x_1, g(y_1, y_2) = y_2$ which is used to simulate $\mathsf{BSS}(1/2)$ from $\mathsf{BSS}(\varepsilon)^{\otimes 2}$. Note that $a = \frac{(1-\varepsilon)^2}{4}, b = \frac{\varepsilon(1-\varepsilon)}{4}, c = \frac{\varepsilon^2}{4}$ where $\varepsilon \in (0, \frac{1}{2})$. This reduction is perfectly correct (refer to Table 7) but not perfectly secure (refer to Table 6). Note that the Fourier spectrum of both functions f and g are concentrated on degree one but not the same support (see Theorem 1).

	$v=0$		$v=1$	
	00	10	01	11
$u=0$	α	$\frac{1}{4}-\alpha$	α	$\frac{1}{4}-\alpha$
$u=1$	$\frac{1}{4}-\alpha$	α	$\frac{1}{4}-\alpha$	α

Table 6: The joint distribution achieved after collapsing the rows of the matrix of Table 5. Note that $\alpha = a + b = \frac{1-\varepsilon}{4}$, where $\varepsilon \in (0, \frac{1}{2})$, $a = (1-\varepsilon)/4$, and $b = \varepsilon(1-\varepsilon)/4$. The submatrix restricted to $v = 0$ has rank 2. Therefore, according to Theorem 6, this reduction is not perfectly secure against a corrupt Bob.

We begin by restating the Informal Theorem 1.

Theorem 8. *Let $\varepsilon' \in (0, 1/2)$, and $\varepsilon \in (0, 1)$. There exists a constant c such that, for any $n \in \mathbb{N}$, for any reduction functions f_n, g_n satisfying $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\varepsilon)^{\otimes n}$, it holds that $\nu(n) \geqslant c/\sqrt{n}$.*

Proof. First, we shall rule out all $\varepsilon' \neq \varepsilon/2$. 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 one of their neighbors on the boolean hypercube lies in S_1. Intuitively, ∂S_0 is the outermost shell of S_0 when embedded in the boolean hypercube. Analogously, define ∂S_1. Our objective is to find a large matching such that every edge has one endpoint in ∂S_0 and another endpoint in ∂S_1. Since $\min\{|S_0|, |S_1|\} \geqslant 2^{n-1}(1 - o(1))$, the size of such a matching is $\geqslant \Theta(2^n/\sqrt{n})$ [16].

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 $1 \leqslant i \leqslant n$ we have $y^n_i = \perp$ or $y^n_i = a^n_i$. 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.

$$T_0 = \{y^n : y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \nvdash y^n\}$$
$$T_1 = \{y^n : y^n \in \{0,1,\perp\}^n, a^n \nvdash y^n, b^n \vdash y^n\}$$
$$T_{\text{both}} = \{y^n : y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \vdash y^n\}$$

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

	$v=0$	$v=1$
$u=0$	$\frac{1}{4}$	$\frac{1}{4}$
$u=1$	$\frac{1}{4}$	$\frac{1}{4}$

Table 7: The joint distribution achieved after collapsing the rows and columns of the matrix of Table 5. This table shows that the reduction introduced in Table 5 is perfectly correct.

$\Pr[Y^n \in T_0 | X^n = a^n] = (1-\varepsilon)$, $\Pr[Y^n \in T_1 | X^n = b^n] = (1-\varepsilon)$, and $\Pr[Y^n \in T_{\text{both}} | X^n = a^n] = \Pr[Y^n \in T_{\text{both}} | X^n = b^n] = \varepsilon$.

Let $W_0 \subseteq \{0,1,\perp\}^n$ be 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. $\Pr[Y^n \in W_0 | X^n = a^n] \approx (1-\varepsilon')$, and $\Pr[Y^n \in W_1 | X^n = a^n] \approx \varepsilon'$.
2. $\Pr[Y^n \in W_1 | X^n = b^n] \approx (1-\varepsilon')$, and $\Pr[Y^n \in W_0 | X^n = b^n] \approx \varepsilon'$.

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

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

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

Then, by parallel composition, we have

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

We know that $\mathsf{BSS}(\varepsilon - \varepsilon^2/2) \sqsubseteq^{0}_{\text{parity}_2, \text{parity}_2} \mathsf{BSS}(\varepsilon/2)^{\otimes 2}$ using the parity reductions (refer to the results in Section 10). By sequential composition, we have

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

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

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

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

9.2 Binary Erasure Source: Feasibility and Rate

We start by restating the Informal Theorem 2 as follows.

Theorem 9 (Binary Erasure Channel: Feasibility & Rate)**.** *For constant $\varepsilon', \varepsilon \in (0,1)$, the following results hold.*

1. ***Feasibility characterization.*** *The following two statements are equivalent.*
   (a) *There exists a 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 $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\varepsilon)^{\otimes n}$ for infinitely many $n \in \mathbb{N}$.*

(b) There exists a constant $k \in \mathbb{N}$, such that $(1-\varepsilon') = (1-\varepsilon)^k$.

In particular, when $(1-\varepsilon') = (1-\varepsilon)^k$, the following linear reduction functions f_n^*, g_n^* realize $\mathsf{BES}(\varepsilon') \sqsubseteq^0_{f_n^*, g_n^*} \mathsf{BES}(\varepsilon)$ for all $n \geqslant k$.

$$f_n^*(x^n) := (-1)^{x_1^n + x_2^n + \cdots + x_k^n}$$
$$g_n^*(y^n) := \begin{cases} (-1)^{y_1^n + y_2^n + \cdots + y_k^n}, & \text{if } y^n \in \{0,1\}^k \times \{0,1,\perp\}^{n-k} \\ 0, & \text{otherwise.} \end{cases}$$

2. ***Rate characterization:*** *Suppose $(1-\varepsilon') = (1-\varepsilon)^k$ for some constant $k \in \mathbb{N}$. There exists a positive constant c such that the first statement implies the second statement below.*
   (a) There exists an infinite family of functions $f_n \colon \{0,1\}^n \to \{-1,1\}^{m(n)}$, $g_n \colon \{0,1,\perp\}^n \to \{-1,0,1\}^{m(n)}$ such that $\mathsf{BES}(\varepsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\varepsilon)^{\otimes n}$, where $\nu(n) = o(1/n^{36+9k/2})$.
   (b) The production is bounded by $m(n) \leqslant \lfloor n/k \rfloor$, for large enough $n \in \mathbb{N}$.

   Furthermore, the production of $m(n) = \lfloor n/k \rfloor$ with $\nu(n) = 0$ is achievable using block linear reduction functions for all $n \in \mathbb{N}$.[14]

Our theorem gives the full characterization of the feasible region of secure non-interactive simulation of a binary erasure source from another one. That is, $o(1)$-secure non-interactive simulation of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$ is possible if and only if the erasure probabilities ε and ε' satisfy that $(1-\varepsilon')$ is a power of $(1-\varepsilon)$. Furthermore, when the erasure probabilities are in the feasible region, in other words, $(1-\varepsilon') = (1-\varepsilon)^k$ for some constant $k \in \mathbb{N}$, the rate of reduction is at most $\frac{1}{k}$. Conversely, this rate is achievable for infinitely many n that are multiples of k by using block-wise linear constructions.

9.2.1 Algebraic Definition

In this subsection, we algebraize the definition of security of secure non-interactive simulation of a BES source from another BES source. Moreover, we introduce some new notations that we will use in this subsection.

Suppose $(X^n, Y^n) \sim \mathsf{BES}(\varepsilon)^{\otimes n}$, then P_ε denotes the marginal distribution of Y^n, and $Q_\varepsilon(x^n)$ denotes the conditional distribution $(Y^n | X^n = x^n)$, and $M(y^n)$ denotes the conditional distribution $(X^n | Y^n = y^n)$. Note that we choose the range of reduction function f_n to be $\{-1,1\}$ and the range of g_n to be $\{-1,0,1\}$. We can rewrite the three conditions of the definition of secure non-interactive simulation, mentioned in Section 7, for BES, as the following.

From our discussion in Section 7, it follows from $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\varepsilon)^{\otimes n}$, where $f_n \colon \{0,1\}^n \to \{-1,1\}, g_n \colon \{0,1,\perp\}^n \to \{-1,0,1\}$, the following algebraic constraints:

1. Correctness: Assuming $(X^n, Y^n) \sim \mathsf{BES}(\varepsilon)^{\otimes n}$, we have:
$$\mathsf{SD}\left((f_n(X^n), g_n(Y^n)), (U, V)\right) \leqslant \nu(n)$$
which implies that $\mathbb{E}_{x^n \sim U_{\{0,1\}^n}}[f_n(x^n)] \leqslant \nu(n)$, and $\mathbb{E}_{y^n \sim P_\varepsilon}[g_n(y^n)] \leqslant \nu(n)$.
2. Bob security:
$$\mathop{\mathbb{E}}_{x^n \sim U_{\{0,1\}^n}} \left| \mathop{\mathbb{E}}_{y^n \sim Q_\varepsilon(x^n)} g_n(y^n) - (1-\varepsilon') f_n(x^n) \right| \leqslant \nu(n).$$

[14] A block linear reduction partitions the input samples into size-k $\lfloor n/k \rfloor$ blocks, and applies the linear reduction functions f_k^*, g_k^* mentioned above on *each* block to produce an output sample.

3. Alice security:

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

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 condition says that if Bob receives some $y^n \in T_i$ for $i \in \{0,1\}$, then most of x^n that are 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. Bob security condition says that if Alice has some input $x^n \in S_i$, then $(1-\varepsilon')$ fraction of y^n that are consistent with x^n is in T_i and ε' fraction of them is in $T_\perp$.

9.2.2 Proof of Feasibility Characterization

In this subsection, we shall prove the feasibility result in Theorem 9. First, we state all the lemmas that are needed for the proof. We provide the proofs of these lemmas in Appendix D.1.

Lemma 2. *Let n be a positive integer. Suppose that there exist reduction functions $f\colon \{0,1\}^n \to \{-1,1\}, g\colon \{0,1,\perp\}^n \to \{-1,0,1\}$, and insecurity bound δ such that $\mathsf{BES}(\varepsilon') \sqsubseteq^{\delta}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$. Then, the following inequality holds.*

$$\mathop{\mathbb{E}}_{x^n \sim U_{\{0,1\}^n}} \left| (\mathsf{T}_\rho f)(x^n) - \rho' f(x^n) \right| \leqslant 2\delta.$$

Lemma 3. *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 $\left|\rho' - \rho^{k(n)}\right| \leqslant \nu(n)$ for every $n \in I$. Then there exists $k \in \mathbb{N}$ such that $\rho' = \rho^k$.*

Proof of feasibility result in Theorem 9. First we prove that statement (a) implies statement (b). For each n, applying Lemma 2 for $f = f_n, g = g_n$ and $\delta = \nu(n)$, we have

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

This allows us to invoke Lemma 1. So there exists $k(n) \in [n]$ such that

$$\left|\rho' - \rho^{k(n)}\right| \leqslant \sqrt{2(1+\rho')\nu(n)}.$$

It is clear that $\lim_{n\to\infty} \sqrt{2(1+\rho')\nu(n)} = 0$ since $\lim_{n\to\infty} \nu(n) = 0$. Using the fact that $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\varepsilon)^{\otimes n}$ holds for infinitely many $n \in \mathbb{N}$, we can apply Lemma 3 to conclude that $\rho' = \rho^k$ for some positive integer k.

We can also verify that (b) implies (a) as a corollary of Theorem 10 which we shall prove in the next subsection. □

We present the proof of the rate result in Section 11.

9.2.3 Feasibility Characterization for Perfect Security Case

In the case of perfect security (when $\nu(n) = 0$), we can further characterize the set of all possible reduction functions f_n and g_n for any fixed n. More precisely, on input $x^n \in \{0,1\}^n$ Alice's reduction function f_n outputs the XOR of all the bits in x^n_S [15] for some $S \subseteq [n]$, and on input $y^n \in \{0,1,\perp\}^n$

[15] x^n_S denotes the string obtained from x^n by concatenating of all the bits x^n_i such that $i \in S$.

Bob's reduction function g_n outputs the XOR of all the bits in y_S^n if y_S^n does not contain any bot symbols, otherwise it outputs zero. We state it formally as follow.

Theorem 10. *For constants $\varepsilon', \varepsilon \in (0,1)$, and for any fixed $n \in \mathbb{N}$, the following two statements are equivalent.*

1. *There exist reduction functions $f\colon \{0,1\}^n \to \{-1,1\}$, $g\colon \{0,1,\perp\}^n \to \{-1,0,1\}$ such that $\mathsf{BES}(\varepsilon') \sqsubseteq^0_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$.*
2. *There exists a constant $k \in [n]$ such that $(1-\varepsilon') = (1-\varepsilon)^k$, and there exists some size-k subset S of $[n]$ such that*

$$f(x^n) := (-1)^{\sum_{i\in S} x_i^n}$$
$$g(y^n) := \begin{cases} (-1)^{\sum_{i\in S} y_i^n}, & \text{if } y_S^n \in \{0,1\}^k \\ 0, & \text{otherwise.} \end{cases}$$

We provide the proof of Theorem 10 in Appendix D.1.

10 SNIS of BSS from BSS: Feasibility & Rate

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 11 (Binary Symmetric Source to Binary Symmetric Source)**.** *For constants $\varepsilon, \varepsilon' \in (0, 1/2)$, the following results hold.*

1. ***Feasibility characterization.*** *The following two statements are equivalent.*
   (a) *There exists a family of reduction functions $f_n, g_n\colon \{0,1\}^n \to \{-1,1\}$ and insecurity bound $\nu(n) = o(1)$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\varepsilon)^{\otimes n}$ for infinitely many $n \in \mathbb{N}$.*
   (b) *There exists a constant $k \in \mathbb{N}$, such that $(1-2\varepsilon') = (1-2\varepsilon)^k$.*

   In particular, when $(1-2\varepsilon') = (1-2\varepsilon)^k$, the following linear reduction functions f_n^*, g_n^* realize $\mathsf{BSS}(\varepsilon') \sqsubseteq^0_{f_n^*,g_n^*} \mathsf{BSS}(\varepsilon)$ for all $n \geqslant k$.

$$f_n^*(x^n) := (-1)^{x_1^n + x_2^n + \cdots + x_k^n}, \text{ and} \qquad g_n^* = f_n^*.$$

2. ***Rate characterization:*** *Suppose $(1-2\varepsilon') = (1-2\varepsilon)^k$ for some constant $k \in \mathbb{N}$. There exists a positive constant c such that the first statement implies the second statement below.*
   (a) *There exists an infinite family of functions $f_n, g_n\colon \{0,1\}^n \to \{-1,1\}^{m(n)}$, such that $\mathsf{BSS}(\varepsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\varepsilon)^{\otimes n}$, where $\nu(n) = o(1/n^{36+9k/2})$.*
   (b) *The production is bounded by $m(n) \leqslant \lfloor n/k \rfloor$, for large enough $n \in \mathbb{N}$.*

   Furthermore, the production of $m(n) = \lfloor n/k \rfloor$ with $\nu(n) = 0$ is achievable using block linear reduction functions for all $n \in \mathbb{N}$.

Our theorem gives the full characterization of the feasible region of secure non-interactive simulation between binary symmetric sources. That is, $o(1)$-secure non-interactive simulation of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BSS}(\varepsilon)$ is possible if and only if the erasure probabilities ε and ε' satisfy that $(1-2\varepsilon') = (1-2\varepsilon)^k$ for some constant $k \in \mathbb{N}$. Furthermore, when the erasure probabilities are in the feasible region, in other words, $(1-2\varepsilon') = (1-2\varepsilon)^k$ for some constant $k \in \mathbb{N}$, the rate of reduction is at most $\frac{1}{k}$. Conversely, this rate is achievable for infinitely many n that are multiples of k by using block-wise linear constructions.

10.1 Algebraic Definition

First we algebraize the definition of secure non-interactive simulation of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BSS}(\varepsilon)^{\otimes n}$. We denote $\rho = 1-2\varepsilon$ and $\rho' = 1-2\varepsilon'$. 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 $\mathsf{T}_\rho(f)\colon \{0,1\}^n \to \mathbb{R}$.

The three conditions for SNIS of $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\varepsilon)^{\otimes n}$, where $f_n, g_n\colon \{0,1\}^n \to \{-1,1\}$, implies the following algebraic constraints.

1. Correctness: Assuming $(X^n, Y^n) \sim \mathsf{BSS}(\varepsilon)^{\otimes n}$, we have:
$$\mathsf{SD}\left((f_n(X^n), g_n(Y^n)), (U,V)\right) \leqslant \nu(n)$$
which implies that $\mathbb{E}_{x^n \sim U_{\{0,1\}^n}}[f_n(x^n)] \leqslant \nu(n)$, and $\mathbb{E}_{y^n \sim U_{\{0,1\}^n}}[g_n(y^n)] \leqslant \nu(n)$.
2. Alice security:
$$\mathop{\mathbb{E}}_{y^n \sim U_{\{0,1\}^n}} \left|(\mathsf{T}_\rho f_n)(y^n) - \rho' \cdot g_n(y^n)\right| \leqslant \nu(n).$$
3. Bob security:
$$\mathop{\mathbb{E}}_{x^n \sim U_{\{0,1\}^n}} \left|(\mathsf{T}_\rho g_n)(x^n) - \rho' \cdot f_n(x^n)\right| \leqslant \nu(n).$$

We describe some intuition here. Recall that for binary symmetric source $\mathsf{BSS}(\varepsilon)$ each bit is flipped with probability ε, in other words, for each sample $(x,y) \xleftarrow{\$} \mathsf{BSS}(\varepsilon)$, 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 $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\varepsilon)^{\otimes n}$ nicely. The condition for corrupt Alice

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

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

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

This implies that

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

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

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

Analogously, the other security condition also holds.

10.2 Proof of the Feasibility Result

In this subsection, we shall prove the feasibility result in Theorem 9. First, we state all the lemmas that are needed for the proof. We provide the proofs of these lemmas in Appendix D.2.

Lemma 4. *Let n be any positive integer, and let $\varepsilon', \varepsilon \in (0,1/2)$. Suppose $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$ for some functions $f, g\colon \{0,1\}^n \to \{-1,1\}$ and $\delta \geqslant 0$. Then, f and g agree on most of the inputs $x \in \{0,1\}^n$, that is, $\langle f, g\rangle \geqslant 1 - \frac{5\sqrt{\delta}}{2\rho'}$.*
Furthermore, we have
$$\mathop{\mathbb{E}}_{x} \left|\mathsf{T}_\rho f(x) - \rho' f(x)\right| \leqslant \delta + 5\sqrt{\delta}.$$

At a high level idea, 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 a $\{-1,1\}$-valued function imply that the function $\mathsf{T}_\rho(f_n)$ is close to the function $\rho' f_n$.

We are ready to describe the proof of feasibility result in Theorem 11 as follows. We emphasis that the security requirements of Alice and Bob are crucial to our proof. Moreover, we present the proof of rate result in Theorem 11 in Section 11.

Proof of the Feasibility Result in Theorem 11. First we prove the forward direction by showing that if $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\varepsilon)^{\otimes n}$ holds for infinitely many $n \in \mathbb{N}$, then $\rho' = \rho^k$. For each n, applying Lemma 4 for $f = f_n$, $g = g_n$, $\delta = \nu(n)$, we have the following

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

Furthermore, we have

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

Applying Lemma 1 for $f = f_n, g = g_n$ and $\delta = \nu(n) + 5\sqrt{\nu(n)}$, there exists $k(n) \in [n]$ such that

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

It is clear that $\lim_{n\to\infty} \sqrt{(1+\rho')(\nu(n) + 5\sqrt{\nu(n)})} = 0$ since $\lim_{n\to\infty} \nu(n) = 0$. Using the fact that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\varepsilon)^{\otimes n}$ holds for infinitely many $n \in \mathbb{N}$, we can apply Lemma 3 to conclude that $\rho' = \rho^k$ for some positive integer k.

Conversely, when $\rho' = \rho^k$, for each $n \geqslant k$, we define $f_n^* = g_n^* = \chi_S$, where S is some subset of size k of $[n]$. By Lemma 9, we have $\mathsf{BSS}(\varepsilon') \sqsubseteq^{0}_{f_n^*,g_n^*} \mathsf{BSS}(\varepsilon)^{\otimes n}$. Thus, there exists a family of infinitely many functions $\{f_n^*, g_n^*\}$ as desired. □

Feasibility Characterization for Perfect Secuirty Case. In the case of perfect security, we can further characterize the set of all possible reduction functions f_n and g_n for any fixed n. More precisely, on input $x^n \in \{0,1\}^n$ Alice's reduction function f_n outputs the XOR of all the bits in x^n_S for some $S \subseteq [n]$, and on input $y^n \in \{0,1\}^n$ Bob's reduction function g_n outputs the XOR of all the bits in y^n_S. We provide the proof of Theorem 1 in Appendix D.2.

11 Proof of the Rate Results

First, we state all the claims that are needed for the proof of the rate results for both BES and BSS as stated in Theorem 9 and Theorem 11. We provide their proofs in Appendix D.3.

Lemma 5. *Let $f^{(1)}, f^{(2)} \colon \{0,1\}^n \to \{-1,1\}$ be two Boolean functions satisfying*

$$\sum_{S \notin \mathcal{W}_k} \widehat{f^{(i)}}(S)^2 \leqslant \delta,$$

for both $i \in \{1,2\}$, and for some positive integer $1 \leqslant k \leqslant n$. We define the truncated version of $f^{(i)}$ as following.

$$h^{(i)}(x) = \sum_{S \in \mathcal{W}_k} \widehat{f^{(i)}}(S) \chi_S(x)$$

Let $f^{(1,2)}\colon \{0,1\}^n \to \{-1,1\}$ be the product of the two functions $f^{(1)}$ and $f^{(2)}$, and let $h^{(1,2)}\colon \{0,1\}^n \to \mathbb{R}$ be the product of the two functions $h^{(1)}$ and $h^{(2)}$. Suppose that the following bound holds on the spectral mass of the function $f^{(1,2)}$.

$$\sum_{S \notin \mathcal{W}_{2k}} \widehat{f^{(1,2)}}(S)^2 \leqslant \delta'$$

Then, the following probability bound holds.

$$\Pr_{\substack{S \sim \mathcal{S}(h^{(1)}) \\ T \sim \mathcal{S}(h^{(2)})}} [S, T \in \mathcal{W}_k, S \cap T = \emptyset] \geqslant 1 - \delta \left(3 + \sqrt{\binom{n}{k}}\right) - \delta'.$$

Intuitively, the claim states the following result in a quantitative fashion. Let $f^{(1)}$ and $f^{(2)}$ be Boolean functions such that the spectral mass of $f^{(1)}$ and $f^{(2)}$ are essentially concentrated on the subsets in $\mathcal{W}_k$. Let $h^{(1)}$ and $h^{(2)}$ be the truncated version of $f^{(1)}$ and $f^{(2)}$, respectively, so that all the Fourier spectrum of them are entirely concentrated on $\mathcal{W}_k$. Suppose the product of the two functions, represented by $f^{(1,2)}$, is a Boolean function whose most spectral mass concentrated on $\mathcal{W}_{2k}$. Let $h^{(1,2)}$ be the product of $h^{(1)}$ and $h^{(2)}$, then $h^{(1,2)}$ is close to $f^{(1,2)}$, which implies that the spectral mass of $h^{(1,2)}$ is concentrated on $\mathcal{W}_{2k}$. The claim concludes that two samples drawn (independently) from the distributions $\mathcal{S}(h^{(1)})$ and $\mathcal{S}(h^{(2)})$ lie in $\mathcal{W}_k$, and are disjoint with high probability.

Corollary 1. *Let $f^{(i)}$ be the i-th projection of the reduction function $f\colon \{0,1\}^n \to \{-1,1\}^m$ ($m \leqslant n$), for $1 \leqslant i \leqslant m$. Let $f^{(i,j)}$ be the product of $f^{(i)}$ and $f^{(j)}$, where $1 \leqslant i < j \leqslant m$. Suppose for each $1 \leqslant i \leqslant m$,*

$$\sum_{S \notin \mathcal{W}_k} \widehat{f^{(i)}}(S)^2 \leqslant \delta$$

and for each $1 \leqslant i < j \leqslant m$,

$$\sum_{S \notin \mathcal{W}_{2k}} \widehat{f^{(i,j)}}(S)^2 \leqslant \delta'.$$

Let $h^{(i)}(x) = \sum_{S \in \mathcal{W}_k} \widehat{f^{(i)}}(S)\chi_S(x)$ and let $h^{(i,j)} = h^{(i)} \cdot h^{(j)}$. Then, the following bound holds.

$$\Pr_{(S^{(1)}, S^{(2)}, \ldots, S^{(m)}) \sim \bigotimes_{i=1}^m \mathcal{S}(h^{(i)})} \left[\left|\bigcup_{i=1}^m S^{(i)}\right| \geqslant mk\right] \geqslant 1 - \binom{m}{2}\left(\delta\left(3 + \sqrt{\binom{n}{k}}\right) + \delta'\right).$$

In particular, if δ and δ' are such that $\binom{m}{2}\left(\delta\left(3 + \sqrt{\binom{n}{k}}\right) + \delta'\right) < 1$, then it follows that $n \geqslant mk$.

Proof of the Rate Result in Theorem 11. Suppose $\mathsf{BSS}(\varepsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BSS}(\varepsilon)^{\otimes n}$ for an infinite family of functions $\{f_n, g_n\}_{n \in \mathbb{N}}$. Let ε'' such that $1 - 2\varepsilon'' = (1 - 2\varepsilon')^2$. Let $f_n^{(i)}$ and $g_n^{(i)}$ be respectively the i-th projection of the function $f_n\colon \{0,1\}^n \to \{-1,1\}^{m(n)}$ and $g_n\colon \{0,1\}^n \to \{-1,1\}^{m(n)}$ ($m(n) \leqslant n$), for $1 \leqslant i \leqslant m(n)$. For each i, we have

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

Therefore, according to Lemma 4, the following inequality holds,

$$\mathop{\mathbb{E}}_{x^n}\left[\left|(\mathsf{T}_\rho f_n^{(i)})(x^n) - \rho' \cdot f_n^{(i)}(x^n)\right|\right] \leqslant \nu'(n) \tag{4}$$

where $\nu' = \nu(n) + 5\sqrt{\nu(n)}$ and $\rho' = 1 - 2\varepsilon'$. Now, by applying Lemma 1, we conclude that:

$$\sum_{S \notin \mathcal{W}_k} \widehat{f_n{}^{(i)}}(S)^2 \leqslant \delta(n) \qquad \forall i \in [m(n)]. \tag{5}$$

where $\delta(n) = \frac{(1+\rho')\nu'(n)}{(1-\rho)^2\rho'^2}$ and k is an integer such that $\rho' = \rho^k$.

Define $p_{m(n)}{}^{(i,j)} \colon \{-1,1\}^{m(n)} \to \{-1,1\}$ as a function that maps $(u_1, u_2, \ldots, u_{m(n)}) \in \{-1,1\}^{m(n)}$ to $u_i \cdot u_j$. It is easy to verify that $\mathsf{BSS}(\varepsilon'') \sqsubseteq^0_{p_{m(n)}{}^{(i,j)}, p_{m(n)}{}^{(i,j)}} \mathsf{BSS}(\varepsilon')^{\otimes m(n)}$ for each $1 \leqslant i < j \leqslant m(n)$. Sequential composition (Theorem 3), implies that

$$\mathsf{BSS}(\varepsilon'') \sqsubseteq^{\nu(n)}_{f_n{}^{(i,j)}, g_n{}^{(i,j)}} \mathsf{BSS}(\varepsilon)^{\otimes n}$$

for each i, j, where $f_n{}^{(i,j)} = p_{m(n)}{}^{(i,j)} \circ f_n$ and $g_n{}^{(i,j)} = p_{m(n)}{}^{(i,j)} \circ g_n$. Note that $f_n{}^{(i,j)} = f_n{}^{(i)} \cdot f_n{}^{(j)}$ and $g_n{}^{(i,j)} = g_n{}^{(i)} \cdot g_n{}^{(j)}$. According to Lemma 4, the following inequality holds for each n,

$$\mathop{\mathbb{E}}_{x^n}\left[\left|(\mathsf{T}_\rho f_n{}^{(i,j)})(x^n) - \rho'' \cdot f_n{}^{(i,j)}(x^n)\right|\right] \leqslant \nu'(n) \tag{6}$$

where $\rho'' = (1 - 2\varepsilon'') = \rho'^2 = \rho^{2k}$. Again, by applying Lemma 1, we have:

$$\sum_{S \notin \mathcal{W}_{2k}} \widehat{f_n{}^{(i,j)}}(S)^2 \leqslant \delta'(n) \qquad \forall\ 1 \leqslant i < j \leqslant m(n). \tag{7}$$

where $\delta'(n) = \frac{(1+\rho'')\nu'(n)}{(1-\rho)^2\rho''^2}$. Now, by applying Corollary 1, we conclude that if we choose $\nu(n)$ such that $\binom{n}{2}\left(\delta(n)\left(3 + \sqrt{\binom{n}{k}}\right) + \delta'(n)\right) < 1$, then $\frac{m(n)}{n} \leqslant \frac{1}{k}$. Since $\binom{n}{k} = O(n^k)$, when $\nu(n) = o(\frac{1}{n^c})$ for the choice of $c = 4 + k/2$ for deterministic reduction functions and $c = 36 + 9k/2$ for randomized ones, we observe that $\frac{m(n)}{n} \leqslant \frac{1}{k}$ for large enough n. □

Proof of the Rate Result in Theorem 9. The proof of rate result in Theorem 9 is very similar to the proof of rate result in Theorem 11. This is due to the fact that the proof of Theorem 11 is based on Lemma 4. Now, by the use of Lemma 2 which is similar to Lemma 4, we can prove the rate result in Theorem 9. □

References

[1] Shweta Agrawal, Yuval Ishai, Eyal Kushilevitz, Varun Narayanan, Manoj Prabhakaran, Vinod M. Prabhakaran, and Alon Rosen. Cryptography from one-way communication: On completeness of finite channels. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 653–685. Springer, Heidelberg, December 2020. 3, 4, 14

[2] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - I: secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, 1993. 1, 15

[3] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - part II: CR capacity. *IEEE Trans. Inf. Theory*, 44(1):225–240, 1998. 1, 15

[4] 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. 13

[5] 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. 13

[6] Benny Applebaum. Garbled circuits as randomized encodings of functions: a primer. Cryptology ePrint Archive, Report 2017/385, 2017. https://eprint.iacr.org/2017/385. 4

[7] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. In *45th FOCS*, pages 166–175. IEEE Computer Society Press, October 2004. 4, 13

[8] Donald Beaver. Perfect privacy for two-party protocols. In Joan Feigenbaum and Michael Merritt, editors, *Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey, USA, October 4-6, 1989*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 65–78. DIMACS/AMS, 1989. 4, 7

[9] Donald Beaver. Correlated pseudorandomness and the complexity of private computations. In *28th ACM STOC*, pages 479–488. ACM Press, May 1996. 4

[10] 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. 13

[11] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 317–342. Springer, Heidelberg, February 2014. 4

[12] Amos Beimel and Tal Malkin. A quantitative approach to reductions in secure computation. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 238–257. Springer, Heidelberg, February 2004. 4

[13] Amos Beimel, Tal Malkin, and Silvio Micali. The all-or-nothing nature of two-party secure computation. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 80–97. Springer, Heidelberg, August 1999. 4

[14] 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*, pages 257–266. ACM Press, October 2008. 1, 15

[15] Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *IEEE Trans. Inf. Theory*, 57(10):6351–6355, 2011. 3, 13

[16] Béla Bollobás and Imre Leader. Matchings and paths in the cube. *Discret. Appl. Math.*, 75(1):1–8, 1997. 10, 22

[17] Christer Borell. Positivity improving operators and hypercontractivity. *Mathematische Zeitschrift*, 180(3):225–234, 1982. 13

[18] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Rindal, and Peter Scholl. Efficient two-round OT extension and silent non-interactive secure computation. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*, pages 291–308. ACM, 2019. 1

[19] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators: Silent OT extension and more. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 489–518. Springer, Heidelberg, August 2019. 1

[20] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012*, pages 309–325. ACM, January 2012. 15

[21] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, January 2000. 17

[22] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2000. https://eprint.iacr.org/2000/067. 17

[23] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd FOCS*, pages 136–145. IEEE Computer Society Press, October 2001. 17

[24] Ignacio Cascudo, Ivan Damgård, Felipe Lacerda, and Samuel Ranellucci. Oblivious transfer from any non-trivial elastic noisy channel via secret key agreement. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part I*, volume 9985 of *LNCS*, pages 204–234. Springer, Heidelberg, October / November 2016. 1

[25] Siu On Chan, Elchanan Mossel, and Joe Neeman. On extracting common random bits from correlated sources on large alphabets. *IEEE Trans. Inf. Theory*, 60(3):1630–1637, 2014. 3, 13

[26] Benny Chor, Mihály Geréb-Graus, and Eyal Kushilevitz. Private computations over the integers (extended abstract). In *31st FOCS*, pages 335–344. IEEE Computer Society Press, October 1990. 4

[27] Benny Chor, Mihály Geréb-Graus, and Eyal Kushilevitz. On the structure of the privacy hierarchy. *Journal of Cryptology*, 7(1):53–60, December 1994. 4

[28] Benny Chor and Eyal Kushilevitz. A zero-one law for Boolean privacy (extended abstract). In *21st ACM STOC*, pages 62–72. ACM Press, May 1989. 4

[29] Ronald Cramer. The arithmetic codex: Theory and applications (invited talk). In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, page 1. Springer, Heidelberg, May 2011. 15

[30] Claude Crépeau. Equivalence between two flavours of oblivious transfers. In Carl Pomerance, editor, *CRYPTO'87*, volume 293 of *LNCS*, pages 350–354. Springer, Heidelberg, August 1988. 1, 3, 13

[31] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th FOCS*, pages 42–52. IEEE Computer Society Press, October 1988. 1, 3, 13

[32] Claude Crépeau and Joe Kilian. Weakening security assumptions and oblivious transfer (abstract). In Shafi Goldwasser, editor, *CRYPTO'88*, volume 403 of *LNCS*, pages 2–7. Springer, Heidelberg, August 1990. 1, 3, 14

[33] Claude Crépeau, Kirill Morozov, and Stefan Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In Carlo Blundo and Stelvio Cimato, editors, *SCN 04*, volume 3352 of *LNCS*, pages 47–59. Springer, Heidelberg, September 2005. 1

[34] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 56–73. Springer, Heidelberg, May 1999. 1

[35] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 643–662. Springer, Heidelberg, August 2012. 1, 15

[36] Anindya De, Elchanan Mossel, and Joe Neeman. Non interactive simulation of correlated distributions is decidable. In Artur Czumaj, editor, *29th SODA*, pages 2728–2746. ACM-SIAM, January 2018. 3, 13

[37] Yevgeniy Dodis and Silvio Micali. Lower bounds for oblivious transfer reductions. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 42–55. Springer, Heidelberg, May 1999. 4

[38] Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973. 3, 13

[39] 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, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 191–208. Springer, Heidelberg, August 2015. 3, 4, 7, 8, 13

[40] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 169–178. ACM Press, May / June 2009. 15

[41] Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan. The relationship between public key encryption and oblivious transfer. In *41st FOCS*, pages 325–335. IEEE Computer Society Press, November 2000. 1, 15

[42] Badih Ghazi, Pritish Kamath, and Prasad Raghavendra. Dimension reduction for polynomials over gaussian space and applications. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*, volume 102 of *LIPIcs*, pages 28: 1–28: 37. Schloss Dagstuhl - Leibniz Center for "u r Computer Science, 2018. 3

[43] Badih Ghazi, Pritish Kamath, and Madhu Sudan. Decidability of non-interactive simulation of joint distributions. In Irit Dinur, editor, *57th FOCS*, pages 545–554. IEEE Computer Society Press, October 2016. 3, 13

[44] 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 ACM STOC*, pages 218–229. ACM Press, May 1987. 1, 13

[45] Lawrence H Harper. Optimal numberings and isoperimetric problems on graphs. *Journal of Combinatorial Theory*, 1(3):385–393, 1966. 10

[46] 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. 13

[47] Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *41st FOCS*, pages 294–304. IEEE Computer Society Press, November 2000. 4, 13

[48] 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*, volume 2380 of *LNCS*, pages 244–256. Springer, Heidelberg, July 2002. 4, 13

[49] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 667–684. Springer, Heidelberg, August 2011. 4, 13, 14

[50] Yuval Ishai, Eyal Kushilevitz, and Anat Paskin-Cherniavsky. From randomizing polynomials to parallel algorithms. In Shafi Goldwasser, editor, *ITCS 2012*, pages 76–89. ACM, January 2012. 4

[51] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 572–591. Springer, Heidelberg, August 2008. 4, 13, 14, 15

[52] 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. 3, 4, 7

[53] Sudeep Kamath and Venkat Anantharam. On non-interactive simulation of joint distributions. *IEEE Transactions on Information Theory*, 62(6):3419–3435, 2016. 3, 4, 7, 13

[54] Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. *SIAM J. Comput.*, 44(5):1550–1572, 2015. 14

[55] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Decidability of secure non-interactive simulation of doubly symmetric binary source. Cryptology ePrint Archive, Report 2021/190, 2021. https://eprint.iacr.org/2021/190. 1

[56] Dakshita Khurana, Hemanta K. Maji, and Amit Sahai. Secure computation from elastic noisy channels. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 184–212. Springer, Heidelberg, May 2016. 1

[57] Joe Kilian. Founding cryptography on oblivious transfer. In *20th ACM STOC*, pages 20–31. ACM Press, May 1988. 1, 4

[58] Joe Kilian. A general completeness theorem for two-party games. In *23rd ACM STOC*, pages 553–560. ACM Press, May 1991. 1, 14

[59] Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd ACM STOC*, pages 316–324. ACM Press, May 2000. 1, 4, 13, 14

[60] 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, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 659–676. Springer, Heidelberg, May 2014. 14

[61] Gunnar Kreitz. A zero-one law for secure multi-party computation with ternary outputs. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 382–399. Springer, Heidelberg, March 2011. 4

[62] Robin Künzler, Jörn Müller-Quade, and Dominik Raub. Secure computability of functions in the IT setting with dishonest majority and applications to long-term security. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 238–255. Springer, Heidelberg, March 2009. 4, 7

[63] Eyal Kushilevitz. Privacy and communication complexity. In *30th FOCS*, pages 416–421. IEEE Computer Society Press, October / November 1989. 4, 7

[64] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. Limits of random oracles in secure computation. In Moni Naor, editor, *ITCS 2014*, pages 23–34. ACM, January 2014. 1

[65] Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. On the power of public-key encryption in secure computation. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 240–264. Springer, Heidelberg, February 2014. 1, 15

[66] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 256–273. Springer, Heidelberg, March 2009. 4, 7

[67] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - secure two-party computation system. In Matt Blaze, editor, *USENIX Security 2004*, pages 287–302. USENIX Association, August 2004. 1, 15

[68] Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In *23rd ACM STOC*, pages 561–571. ACM Press, May 1991. 1, 15

[69] Ueli M. Maurer. A universal statistical test for random bit generators. *Journal of Cryptology*, 5(2):89–105, January 1992. 1, 15

[70] Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39(3):733–742, 1993. 1, 15

[71] 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. 3, 13

[72] 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. 3, 13

[73] Elchanan Mossel, Krzysztof Oleszkiewicz, and Arnab Sen. On reverse hypercontractivity. *Geometric and Functional Analysis*, 23(3):1062–1097, 2013. 13

[74] 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. 7

[75] Varun Narayanan, Manoj Prabhakaran, and Vinod M. Prabhakaran. Zero-communication reductions. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part III*, volume 12552 of *LNCS*, pages 274–304. Springer, Heidelberg, November 2020. 14

[76] 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, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 681–700. Springer, Heidelberg, August 2012. 1, 15

[77] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. 16

[78] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2602–2606. IEEE, 2010. 1, 4, 14

[79] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information: Further results. In Alexander Kuleshov, Vladimir M. Blinovsky, and Anthony Ephremides, editors, *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011*, pages 2861–2865. IEEE, 2011. 1, 4, 14

[80] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information with an application to secure two-party sampling. *IEEE Trans. Inf. Theory*, 60(6):3413–3434, 2014. 1, 4, 14

[81] Michael O. Rabin. How to exchange secrets by oblivious transfer. *Technical Memo TR-81*, 1981. 1, 3, 13

[82] Michael O. Rabin. How to exchange secrets with oblivious transfer. Cryptology ePrint Archive, Report 2005/187, 2005. https://eprint.iacr.org/2005/187. 1, 3, 13

[83] K. Sankeerth Rao and Vinod M. Prabhakaran. A new upperbound for the oblivious transfer capacity of discrete memoryless channels. In *2014 IEEE Information Theory Workshop, ITW 2014, Hobart, Tasmania, Australia, November 2-5, 2014*, pages 35–39. IEEE, 2014. 14

[84] Alfréd Rényi. On measures of dependence. *Acta mathematica hungarica*, 10(3-4):441–451, 1959. 13

[85] Louis Salvail, Christian Schaffner, and Miroslava Sotáková. On the power of two-party quantum cryptography. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 70–87. Springer, Heidelberg, December 2009. 4

[86] Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for generating correlation: A unifying survey. *IEEE Trans. Inf. Theory*, 66(1):5–37, 2020. 13

[87] Severin Winkler and Jürg Wullschleger. On the efficiency of classical and quantum oblivious transfer reductions. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 707–723. Springer, Heidelberg, August 2010. 4

[88] Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975. 3, 13

[89] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. In Victor Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 467–477. Springer, Heidelberg, August 2005. 14

[90] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 222–232. Springer, Heidelberg, May / June 2006. 1, 4, 13

[91] Jürg Wullschleger. Oblivious-transfer amplification. *CoRR*, abs/cs/0608076, 2006. 1

[92] Jürg Wullschleger. Oblivious-transfer amplification. In Moni Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 555–572. Springer, Heidelberg, May 2007. 1

[93] Jürg Wullschleger. Oblivious transfer from weak noisy channels. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 332–349. Springer, Heidelberg, March 2009. 1

[94] Aaron Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975. 3, 13, 14

[95] Ke Yang. On the (im)possibility of non-interactive correlation distillation. In Martin Farach-Colton, editor, *LATIN 2004*, volume 2976 of *LNCS*, pages 222–231. Springer, Heidelberg, April 2004. 3, 7, 13

[96] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd FOCS*, pages 160–164. IEEE Computer Society Press, November 1982. 1, 13

[97] Zi Yin and Youngsuk Park. Hypercontractivity, maximal correlation and non-interactive simulation. 2014. 3

A Extension to Multiple Channel Parameters

Our proof techniques for Informal Theorem 2 and Informal Theorem 3 yield the following extensions as well. For Informal Theorem 2, we prove that $\mathsf{BES}(\varepsilon_1) \otimes \cdots \otimes \mathsf{BES}(\varepsilon_m) \sqsubseteq_{f_n,g_n}^{\nu(n)} \mathsf{BES}(\varepsilon)^{\otimes n}$ holds if and only if $(1-\varepsilon_i) = (1-\varepsilon)^{k_i}$, where $k_i \in \mathbb{N}$, and $1 \leqslant i \leqslant m$. Moreover, the rate is bounded by $k_1 + \cdots + k_m \leqslant n$. Here, $\varepsilon_1, \ldots, \varepsilon_m, \varepsilon \in (0,1)$ are constants. Analogously, we prove for Informal Theorem 3 that $\mathsf{BSS}(\varepsilon_1) \otimes \cdots \otimes \mathsf{BSS}(\varepsilon_m) \sqsubseteq_{f_n,g_n}^{\nu(n)} \mathsf{BSS}(\varepsilon)^{\otimes n}$ holds if and only if $(1-2\varepsilon_i) = (1-2\varepsilon)^{k_i}$, where $k_i \in \mathbb{N}$ and $1 \leqslant i \leqslant m$, and $k_1 + \cdots + k_m \leqslant n$. Here, $\varepsilon_1, \ldots, \varepsilon_m, \varepsilon \in (0, 1/2)$ are constants. For ease of the presentation, we present the simpler form of our result. From the technical overview section, the extension of our results in this form is natural.

B Rank One Characterization of SNIS

B.1 Proof of Theorem 6

Suppose $(U,V) \sqsubseteq_{f,g}^{\nu(n)} (X,Y)^{\otimes n}$, then we shall prove the first condition. The proof of the second condition is similar. Our assumption implies that there exists simulator $\mathrm{Sim}_B \colon \mathcal{V} \to \mathcal{Y}^n$ such that

$$\mathrm{SD}\left(\left(U, V, \mathrm{Sim}_B(V)\right) , \left(f(X^n), g(Y^n), Y^n\right) \right) \leqslant \nu(n)$$

which in turn implies the following for each $v^* \in \mathcal{V}$.

$$\mathrm{SD}\left(\left(U, V = v^*, \mathrm{Sim}_B(V)\right) , \left(f(X^n), g(Y^n) = v^*, Y^n\right) \right) \leqslant \nu(n) \tag{8}$$

Now, notice that for each $u \in \mathcal{U}$, and $y^n \in \mathcal{Y}^n$,

$$\begin{aligned} \Pr[U = u, V = v^*, \mathrm{Sim}_B(V) = y^n] &= \Pr[U = u, V = v^*, \mathrm{Sim}_B(v^*) = y^n] && (9)\\ &= \Pr[U = u, V = v^*] \times \Pr[\mathrm{Sim}_B(v^*) = y^n] && (10) \end{aligned}$$

We define the matrix T^{v^*} of size $|\mathcal{U}| \times |\mathcal{B}_g(v^*)|$ as follows:

For $y^n \in \mathcal{B}_g(v^*)$ and $u \in \mathcal{U}$, define $T^{v^*}(u, y^n)$ (the element at row u and column y^n) as $\Pr[U = u, V = v^*] \times \Pr[\mathrm{Sim}_B(v^*) = y^n]$.

The rank of T^{v^*} is one because each column of it, is a scale (with scale value $\Pr[\mathrm{Sim}_B(v^*) = y^n]$ for column indexed by y^n) of a column vector of size $|\mathcal{U}|$ whose element at row indexed by u, is $\Pr[U = u, V = v^*]$.

Moreover, it follows from (8) and (9) that $\mathrm{SD}\left(T^{v^*}, M_A^{v^*}\right) \leqslant \nu(n)$. Finally,

$$\begin{aligned} \sum_{y^n \in \mathcal{B}_g(v^*)} T^{v^*}(u, y^n) &= \sum_{y^n \in \mathcal{B}_g(v^*)} \Pr[U = u, V = v^*] \times \Pr[\mathrm{Sim}_B(v^*) = y^n] && (11)\\ &= \Pr[U = u, V = v^*] \sum_{y^n \in \mathcal{B}_g(v^*)} \Pr[\mathrm{Sim}_B(v^*) = y^n] && (12)\\ &= \Pr[U = u, V = v^*] && (13) \end{aligned}$$

Note that in (12), we assume without loss of generality that simulator Sim_B on input v^* outputs some y^n in the set $\mathcal{B}_g(v^*)$[17]. This completes the proof of first condition. The proof of second condition is similar.

[17] This assumption is true because otherwise we can modify simulator to get a new simulator which has this property and its insecurity is still at most $\nu(n)$.

B.2 Proof of Theorem 7

We need to define simulators Sim_A and Sim_B such that satisfy the definitions of security. Define random function $\mathrm{Sim}_B \colon \mathcal{V} \to \mathcal{Y}^n$ such that

$$\Pr[\mathrm{Sim}_B(v) = y^n] = \frac{T^v(u, y^n)}{\Pr[U = u, V = v]} \times \mathbf{1}_{\{y^n \in \mathcal{B}_g(v)\}}$$

where $\mathbf{1}_{\{y^n \in \mathcal{B}_g(v)\}} = 1$ when $y^n \in \mathcal{B}_g(v)$ and $\mathbf{1}_{\{y^n \in \mathcal{B}_g(v)\}} = 0$ when $y^n \notin \mathcal{B}_g(v)$. Note that the condition $\sum_{y^n \in \mathcal{B}_g(v)} T^v(u, y^n) = \Pr[U = u, V = v]$ guarantees that $\sum_{y^n \in \mathcal{B}_g(v)} \Pr[\mathrm{Sim}_B(v) = y^n] = 1$. Moreover, the condition $\mathrm{SD}\left(T^v, M_A^v\right) \leqslant \nu(n)$ implies that for $v \in \mathcal{V}$,

$$\begin{aligned}
&\frac{1}{2} \sum_{u \in \mathcal{U}, y^n \in \mathcal{B}_g(v)} |T^v(u, y^n) - M_A^v(u, y^n)| \leqslant \nu(n) \\
\iff &\frac{1}{2} \sum_{u \in \mathcal{U}, y^n \in \mathcal{B}_g(v)} |\Pr[U = u, V = v] \Pr[\mathrm{Sim}_B(v) = y^n] - \Pr[f(X^n) = u, Y^n = y^n]| \leqslant \nu(n) \\
\iff &\frac{1}{2} \sum_{u \in \mathcal{U}, y^n \in \mathcal{B}_g(v)} |\Pr[U = u, V = v, \mathrm{Sim}_B(V) = y^n] - \Pr[f(X^n) = u, Y^n = y^n]| \leqslant \nu(n) \\
\iff &\frac{1}{2} \sum_{u \in \mathcal{U}, y^n \in Y^n} |\Pr[U = u, V = v, \mathrm{Sim}_B(V) = y^n] - \Pr[f(X^n) = u, g(Y^n) = v, Y^n = y^n]| \leqslant \nu(n)
\end{aligned}$$

which implies the following:

$$\begin{aligned}
&\frac{1}{2} \sum_{u \in \mathcal{U}, v \in \mathcal{V}, y^n \in Y^n} |\Pr[U = u, V = v, \mathrm{Sim}_B(V) = y^n] - \Pr[f(X^n) = u, g(Y^n) = v, Y^n = y^n]| \leqslant |\mathcal{V}| \nu(n) \\
&\quad \iff \mathrm{SD}\left((U, V, \mathrm{Sim}_B(V)), f(X^n), g(Y^n), Y^n\right) \leqslant |\mathcal{V}| \nu(n)
\end{aligned}$$

Similarly, we can define Sim_A satisfying the following:

$$\mathrm{SD}\left(\ (U, V, \mathrm{Sim}_A(U))\ ,\ (f(X^n), g(Y^n), X^n)\ \right) \leqslant |\mathcal{U}| \nu(n)$$

So, the insecurity is at most $\max(|\mathcal{U}|, |\mathcal{V}|) \times \nu(n)$.

C Deterministic Protocols from Randomized Protocols

In this section, we will show that, without loss of generality, one can assume the reduction functions in SNIS are deterministic, in other words, parties do not use any private randomness by proving Theorem 5.

of Theorem 5. Suppose there exist $n \in \mathbb{N}$ and two functions $f \colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{U}$, and $g \colon \mathcal{Y}^n \times \mathcal{R}_B \to \mathcal{V}$ such that $(U, V) \sqsubseteq_{f,g}^{\nu} (X, Y)^{\otimes n}$. Define the function $g' \colon \mathcal{Y}^n \to \mathcal{V}$ as the following:

$$g'(y^n) := \operatorname*{argmin}_{v \in \mathcal{V}} \mathrm{SD}\left((f(X^n, R_A) | g(Y^n, R_B) = v, (Y^n = y^n, R_B)), \left(U | V = v, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right)$$

where Sim_B is the simulator used to simulate the view of corrupt Bob in the definition. Note that we have:

$$g'(y^n) \quad = \operatorname*{argmin}_{v \in\ \mathcal{V}} \mathrm{SD}\left(\ f(X^n, R_A) \mid Y^n = y^n\ ,\ U \mid V = v\ \right)$$

due to the fact that the random variable $f(X^n, R_A)$ condition of Y^n, is independent of R_B and $g(Y^n, R_B)$ (Markov chain $f(X^n, R_A) \leftrightarrow Y^n \leftrightarrow (Y^n, R_B) \leftrightarrow g(Y^n, R_B)$) and the other fact that the random variable U condition on V is independent of $\mathrm{Sim}_B(V)$ (Markov chain $U \leftrightarrow V \leftrightarrow g(Y^n, R_B)$).

Note that $|\mathcal{V}|$ and $|\mathcal{U}|$ are constant and they do not depend on n. Therefore, it must be the case that $\mathrm{SD}\left((U|V = v_1) , (U|V = v_2) \right)$ is a constant value (does not depend on ε) for any two different $v_1, v_2 \in \mathcal{V}$.

We can assume that for any $v_1, v_2 \in \mathcal{U}$, $\mathrm{SD}\left((U|V = v_1) , (U|V = v_2) \right) \neq 0$ [18]. Therefore, there exists a constant α such that for any two different elements $v_1, v_2 \in \mathcal{U}$, the following inequality holds.

$$\mathrm{SD}\left((U|V = v_1) , (U|V = v_2) \right) \geqslant \alpha.$$

For any two different elements $v_1, v_2 \in \mathcal{V}$, we have

$$\begin{aligned} & \mathrm{SD}\left((U|V = v_1, \mathrm{Sim}_B(V)) , (U|V = v_2, \mathrm{Sim}_B(V)) \right) \\ = \ & \mathrm{SD}\left((U|V = v_1) , (U|V = v_2) \right) \\ \geqslant \ & \alpha \end{aligned}$$

Suppose $g'(y^n) = v^*$, then according to the definition of g', we have,

$$\begin{aligned} & \mathrm{SD}\left((f(X^n, R_A) \mid g(y^n, R_B) = v, (y^n, R_B)) , \left(U \mid V = v, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \geqslant \\ & \mathrm{SD}\left((f(X^n, R_A) \mid g(y^n, R_B) = v^*, (y^n, R_B)) , \left(U \mid V = v^*, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \end{aligned}$$

then we claim that for any $v \neq v^*$,

$$\mathrm{SD}\left((f(X^n, R_A) \mid g(y^n, R_B) = v, (y^n, R_B)) , \left(U \mid V = v, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \geqslant \frac{\alpha}{2}$$

because otherwise, by triangle inequality, we have,

$$\begin{aligned} & \mathrm{SD}\left((U|V = v) , (U|V = v^*) \right) \\ = \ & \mathrm{SD}\left(\left(U \mid V = v, \mathrm{Sim}_B(V) = (y^n, R'_B)\right), \left(U \mid V = v^*, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \\ \leqslant \ & \mathrm{SD}\left((f(X^n, R_A) \mid Y^n = y^n)) , \left(U \mid V = v, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \\ & + \mathrm{SD}\left((f(X^n, R_A) \mid Y^n = y^n)) , \left(U \mid V = v^*, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \\ = \ & \mathrm{SD}\left((f(X^n, R_A) \mid g(y^n, R_B) = v, (y^n, R_B)) , \left(U \mid V = v, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \\ & + \mathrm{SD}\left((f(X^n, R_A) \mid g(y^n, R_B) = v^*, (y^n, R_B)) , \left(U \mid V = v^*, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \\ \leqslant \ & 2\mathrm{SD}\left((f(X^n, R_A) \mid g(y^n, R_B) = v, (y^n, R_B)) , \left(U \mid V = v, \mathrm{Sim}_B(V) = (y^n, R'_B)\right)\right) \\ \leqslant \ & \alpha \end{aligned}$$

which is a contradiction. We say that y^n is bad if $\Pr[g(y^n, R_B) \neq g'(y^n)] \geqslant \delta = \nu^{2/3}$ (note that the probability is over randomness $\mathcal{R}_B$). It follows from average argument that for any bad y^n, there exists $v_{y^n} \in \mathcal{V}$ such that $v_{y^n} \neq g'(y^n)$ and $\Pr[g(y^n, R_B) = v_{y^n}] \geqslant \frac{\nu^{2/3}}{|\mathcal{V}|}$. Let $\mathrm{BAD} \subseteq \mathcal{Y}^n$ denote the subset of all bad strings y^n. Define $\rho := \Pr[Y^n \in \mathrm{BAD}]$.

Therefore, the insecurity of simulating (U, V) by using functions $f\colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{U}$, and $g\colon \mathcal{Y}^n \times$

[18] Otherwise v_1 and v_2 can be combined together and considered as one element.

$\mathcal{R}_B \to \mathcal{V}$ is at least $\rho \times \frac{\nu^{2/3}}{|\mathcal{V}|} \times \frac{\alpha}{2}$. Therefore, we should have $\rho \leqslant \frac{2|\mathcal{V}|\nu^{1/3}}{\alpha}$. Now, we have

$$\begin{aligned}\Pr[g(Y^n, R_B) \neq g'(Y^n)] &= Pr[g(Y^n, R_B) \neq g'(Y^n) | Y^n \in \text{BAD}] \times \Pr[Y^n \in \text{BAD}] \\ &\quad + Pr[g(Y^n, R_B) \neq g'(Y^n) | Y^n \notin \text{BAD}] \times \Pr[Y^n \notin \text{BAD}] \\ &\leqslant 1 \times \frac{2|\mathcal{V}|\nu^{1/3}}{\alpha} + \nu^{2/3} \times 1 \\ &\leqslant \nu^{1/3} \times (1 + \frac{2|\mathcal{V}|}{\alpha})\end{aligned}$$

By the way that we defined function g', the new scheme defined by the simulation functions f, g' is more secure than the scheme f, g (with respect to a corrupt Bob); however, it guarantees correctness with a looser bound. So far, we have shown that given two functions $f\colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{U}$, and $g\colon \mathcal{Y}^n \times \mathcal{R}_B \to \mathcal{V}$ such that $(U, V) \sqsubseteq^{\nu}_{f,g} (X, Y)^{\otimes n}$, there exists $g'\colon \mathcal{Y}^n \to \mathcal{V}$ and constant β (which depends on distribution (U, V)) such that $(U, V) \sqsubseteq^{\beta\nu^{1/3}}_{f,g'} (X, Y)^{\otimes n}$. Now, we can use a similar argument to show that there exists a function $f'\colon \mathcal{X}^n \to \mathcal{U}$ and constant γ such that $(U, V) \sqsubseteq^{\gamma\nu^{1/9}}_{f',g'} (X, Y)^{\otimes n}$. This completes the proof. □

D Omitted Proofs

D.1 Omitted Proofs in Section 9

D.1.1 Proof of Lemma 2

Proof. First we show that

$$\mathop{\mathbb{E}}_{x^n \sim U_{\{0,1\}^n}} \left| \mathop{\mathbb{E}}_{y^n \sim Q_\varepsilon(x^n)} \mathop{\mathbb{E}}_{z^n \sim M(y^n)} f(z^n) - (1 - \varepsilon') f(x^n) \right| \leqslant 2\delta. \tag{14}$$

By triangle inequality we have

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

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 $(x^n, y^n) \sim \mathsf{BES}(\varepsilon)^{\otimes n}$ is equivalent to drawing x^n uniformly at random and then drawing y^n from conditional distribution $Q_\varepsilon(\varepsilon)$ induced by the distribution $(x^n, y^n) \sim \mathsf{BES}(\varepsilon)^{\otimes n}$.

Next, recall that the noise operator is defined as $(\mathsf{T}_\rho f)(x^n) = \mathbb{E}_{y^n \sim N_\rho(x^n)} f(y^n)$. We shall show that

$$\mathop{\mathbb{E}}_{y^n \sim Q_\varepsilon(x^n)} \mathop{\mathbb{E}}_{z^n \sim M(y^n)} f(z^n) = \mathsf{T}_\rho(f)(x^n). \tag{15}$$

Fix $x^n \in \{0,1\}^n$. Drawing y^n from the distribution $Q_\varepsilon(x^n)$ 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 $1-\varepsilon$ 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

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

And so $\Pr[z_i^n = 1 - x_i^n] = \frac{\varepsilon}{2}$. This completes the proof of equation(15). Finally, substituting equation (15) in to inequality (14) gives the desired inequality. □

D.1.2 Proof of Lemma 1

Proof. Since $|(\mathsf{T}_\rho f)(x^n)| \leqslant 1$ and $f(x^n) \in \{-1, 1\}$ for every x^n, we have

$$\left|(\mathsf{T}_\rho f)(x^n) - \rho' \cdot f(x^n)\right| \leqslant 1 + \rho' \text{ for every } x^n.$$

It implies that

$$\begin{aligned}\mathop{\mathbb{E}}_{x^n} \left[(\mathsf{T}_\rho f)(x^n) - \rho' \cdot f(x^n)\right]^2 &\leqslant \mathop{\mathbb{E}}_{x^n} \left[(1+\rho')\left|(\mathsf{T}_\rho f)(x^n) - \rho' \cdot f(x^n)\right|\right] \\ &= (1+\rho') \mathop{\mathbb{E}}_{x^n} \left|(\mathsf{T}_\rho f)(x^n) - \rho' \cdot f(x^n)\right| \\ &\leqslant (1+\rho') \cdot \delta\end{aligned}$$

We use the Parseval's identity to evaluate the left hand side of this expression in another fashion.

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

Let $\gamma := \min_{k \in [n]} \left|\rho' - \rho^k\right|$. Recall that we already know that $\mathbb{E}_{x^n} \left[(\mathsf{T}_\rho f)(x^n) - \rho' \cdot f(x^n)\right]^2 \leqslant (1 + \rho')\delta$. Consequently, we have:

$$(1+\rho')\delta \geqslant \sum_S (\rho^{|S|} - \rho')^2 \widehat{f}(S)^2 \geqslant \sum_S \gamma^2 \widehat{f}(S)^2 = \gamma^2, \text{ because} \sum_S \widehat{f}(S)^2 = 1.$$

So it must be the case that $\gamma^2 \leqslant (1+\rho')\delta$, which implies that $\min_{k \in [n]} \left|\rho' - \rho^k\right| \leqslant \sqrt{(1+\rho')\delta}$. Next, we have

$$\sum_{S \notin \mathcal{W}_k} (\rho^{|S|} - \rho^k)^2 \widehat{f}(S)^2 \leqslant \sum_{S \subseteq [n]} (\rho^{|S|} - \rho^k)^2 \widehat{f}(S)^2 = \mathop{\mathbb{E}}_{x^n} \left[(\mathsf{T}_\rho f)(x^n) - \rho^k \cdot f(x^n)\right]^2 \leqslant (1+\rho')\delta.$$

Since $0 < \rho < 1$, we have $(\rho^{|S|} - \rho^k)^2 \geqslant \rho^{2k}(1-\rho)^2 = \rho'^2(1-\rho)^2$ for each $S \notin \mathcal{W}_k$. Therefore, we have $\sum_{S \notin \mathcal{W}_k} \widehat{f}(S)^2 \leqslant \frac{(1+\rho')\delta}{(1-\rho)^2 \rho'^2}$. □

D.1.3 Proof of Lemma 3

Proof. The sequence $\left|\rho' - \rho^{k(n)}\right|$ are bounded below by 0 and bounded above by $\nu(n)$, which also converges to 0. By squeeze theorem, the sequence $\rho' - \rho^{k(n)}$ also converges to 0. Now, since $k(n)$ is an integer for any $n \in I$, the sequence $k(n)$ must converge. Therefore, there exists some positive number k sucht that $\rho' = \rho^k$ as desired. □

D.1.4 Proof of Theorem 10

Lemma 6. *In Theorem 10, statement (1) implies statement (2).*

The proof of this lemma crucially relies on the Alice security condition and the fact that f is a balanced function. We use the Fourier analysis to prove this. For convenience, we omit n from f_n, g_n in this subsection.

Proof. For each $y^n \in \{0,1,\perp\}^n$, we define $J(y^n) := \{i \in [n] \colon y_i^n = \perp\}$, $\overline{J(y^n)} = [n] \backslash J(y^n)$, and $z(y^n)$ as the concatenation of all non-bot symbols in y^n. For example, when $y^4 = 0\perp1\perp$, $J(y^4) = \{2,4\}$, $\overline{J(y^4)} = \{1,3\}$, and $z(y^4) = 01$. For $x^n, y^n \in \{0,1,\perp\}^n$, we say that they are neighbor (sibling) of each other if $J(x^n) = J(y^n)$, and $z(x^n), z(y^n)$ are different at exactly one coordinate (their Hamming distance is one). Suppose $z(x^n)$ and $z(y^n)$ differ at coordinate j. We define the parent of x^n, y^n is the vector obtained by replacing the coordinate j of x^n by the bot symbol. For instance, $00\perp\perp$ is a neighbor of $01\perp\perp$, and their parent is $0\perp\perp\perp$. Recall the definition of restriction of function to sub-cubes from Section 6.3 that the function $f_{J(y^n)|z(y^n)} \colon \{0,1\}^{|J(y^n)|} \to \{-1,1\}$ denotes the restriction of f to $J(y^n)$ when the coordinates in $\overline{J(y^n)}$ is fixed to $z(y^n)$. For ease of presentation, we denote $f_{J(y^n)|z(y^n)}$ as f_{y^n}. When $\nu(n) = 0$, Alice security condition implies that

$$\mathop{\mathbb{E}}_{x^n \sim M(y^n)} f(x^n) = g(y^n) \text{ for every } y^n \in \{0,1,\perp\}^n.$$

Note that the left side is the expectation of the restriction function of f to $J(y^n)$ using $z(y^n)$, so $\mathbb{E}_{x^n \sim M(y^n)} f(x^n) = \widehat{f_{y^n}}$. Therefore, we have $\widehat{f_{y^n}}(\emptyset) = g(y^n)$ for every $y^n \in \{0,1,\perp\}^n$. Since the range of function g is $\{-1,0,1\}$, the value $\widehat{f_{y^n}}(\emptyset)$ is also in $\{-1,0,1\}$ for every $y^n \in \{0,1,\perp\}^n$.

When $y^n = \perp\perp\cdots\perp$, we have $\widehat{f_{y^n}}(\emptyset) = \widehat{f}(\emptyset) = 0$ since f is a balanced function. Clearly, $\widehat{f_{y^n}}(\emptyset)$ cannot be zero for every y^n. This together with the fact that $\widehat{f_{y^n}}(\emptyset) \in \{-1,0,1\}$ implies that there exists a $y^n \in \{0,1,\perp\}^n$ such that $\left|\widehat{f_{y^n}}(\emptyset)\right| = 1$. Let y_*^n be a such one with minimum number of bot symbols, more precisely,

$$y_*^n = \mathop{\text{argmin}}_{y^n : \left|\widehat{f_{y^n}}(\emptyset)\right| = 1} |J(y^n)|.$$

To prove that f is a linear function, it suffices to show that $\widehat{f}(S^*)^2 = 1$, where $S^* = \overline{J(y_*^n)}$. By the choice of y_*^n, we have $\widehat{f_{y^n}}(\emptyset) = 0$ for every $y^n \in \{0,1,\perp\}^n$ such that $|J(y^n)| < |J(y_*^n)|$. For each $S \subseteq [n]$, let $\mathcal{V}(S) = \{y^n \in \{0,1,\perp\}^n \colon \overline{J(y^n)} = S\}$, and let $k = |S^*|$. We shall show that $\left|\widehat{f_{y^n}}(\emptyset)\right| = 1$ for every $y^n \in \mathcal{V}(S^*)$. Observe that the set $\{z(y^n) \colon y^n \in \mathcal{V}(S^*)\}$ is a sub-cube of $\{0,1\}^n$. We know that this sub-cube has a Hamiltonian cycle. This implies that there is a Hamiltonian path starting from y_*^n, says $(y_*^n = y^{(1)}, y^{(2)}, \ldots, y^{(2^k)})$, in which every two consecutive vertices $y^{(i)}$ and $y^{(i+1)}$ are neighbor of each other. Now, by the the basic Fourier property (2) we have

$$\frac{1}{2}\widehat{f_{y^{(i)}}}(\emptyset) + \frac{1}{2}\widehat{f_{y^{(i+1)}}}(\emptyset) = \widehat{f_p}(\emptyset) \text{ for every } i = 1, \ldots 2^k,$$

where p is the parent of $y^{(i)}$ and $y^{(i+1)}$. We know that $\widehat{f_p}(\emptyset) = 0$, so $\widehat{f_{y^{(i)}}}(\emptyset) = -\widehat{f_{y^{(i+1)}}}(\emptyset)$. Now applying this argument iteratively for $i = 1, 2, \ldots, 2^k$, we can conclude that $\left|\widehat{f_{y^n}}(\emptyset)\right| = 1$ for every $y^n \in \mathcal{V}(S^*)$. Applying equation (3), we have

$$\sum_{S \subseteq S^*} \widehat{f}(S)^2 = \mathop{\mathbb{E}}_{y^n \in \mathcal{V}(S^*)} \widehat{f_{y^n}}(\emptyset)^2 = 1$$
$$\sum_{S \subseteq T} \widehat{f}(S)^2 = \mathop{\mathbb{E}}_{y^n \in \mathcal{V}(T)} \widehat{f_{y^n}}(\emptyset)^2 = 0 \text{ for every } T \subsetneq S^*$$

These equations imply that $\widehat{f}(S^*)^2 = 1$. Next, observe that if $\widehat{f_{y^n}}(\emptyset) = \pm 1$, then $\widehat{f_{x^n}}(\emptyset) = \widehat{f_{y^n}}(\emptyset)$ for every $x^n \in \{0,1,\perp\}^n$ such that $x^n \vdash y^n$. Using this fact together with the equations (2) and (3), and the fact that $g(y^n) = \widehat{f_{y^n}}(\emptyset)$, we can verify that

$$g(y^n) := \begin{cases} (-1)^{\sum_{i \in S^*} y_i^n}, & \text{if } y^n_{S^*} \in \{0,1\}^k \\ 0, & \text{otherwise.} \end{cases}$$

Finally, by a simple calculation, we can conclude that $(1 - \varepsilon') = (1 - \varepsilon)^k$.

□

Lemma 7. *In Theorem 10, statement (2) implies statement (1).*

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:

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

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 $\mathsf{BES}(\varepsilon')$ where $\varepsilon' = \Pr[g_n(y^n) = 0] = 1 - (1-\varepsilon)^k$. We need to prove that it is perfectly secure. For each x^n,

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

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 feasibility of the proof of Theorem 9 when $\nu(n) = 0$. □

D.2 Omitted Proofs in Section 10

D.2.1 Proof of Lemma 4

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

$$\frac{\langle f, \mathsf{T}_\rho f\rangle + \langle g, \mathsf{T}_\rho g\rangle}{2} \geqslant |\langle f, \mathsf{T}_\rho g\rangle| = |\langle g, \mathsf{T}_\rho f\rangle| \tag{16}$$

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

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

which is equivalent to

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

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

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

Similarly, we get $\langle g, \mathsf{T}_\rho g\rangle \leqslant (2a-1)\rho' + 2\sqrt{\delta}$.

Lower bound for the right hand side.

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

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

$$\begin{aligned}
\mathop{\mathbb{E}}_x\left|\mathsf{T}_\rho f(x) - \rho' f(x)\right| &\leqslant \mathop{\mathbb{E}}_x\left|\mathsf{T}_\rho f(x) - \rho' g(x)\right| + \rho'\mathop{\mathbb{E}}_x|g(x) - f(x)| \\
&\leqslant \delta + 2\rho'\frac{5\sqrt{\delta}}{2\rho'} = \delta + 5\sqrt{\delta},
\end{aligned}$$

which completes our proof of Lemma 4. □

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

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

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

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

Using term-wise AM-GM, we have

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

which give us the inequality as desired. □

D.2.2 Proof of Theorem 1

Lemma 8. *In Theorem 1, statement (1) implies statement (2).*

Proof. Apply Lemma 4 for $\delta = 0$, we have

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

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

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

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 emphasis 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).

Lemma 9. *In Theorem 1, statement (2) implies statement (1).*

Proof. Note that

$$\mathsf{T}_\rho f(x^n) = \sum_{S\subseteq[n]} \rho^{|S|}\widehat{f}(S)\chi_S(x^n) = \rho^k \sum_{S\in\mathcal{W}_k} \widehat{f}(S)\chi_S(x^n) = \rho^k f(x^n) = \rho' g(x^n).$$

We shall show that all the algebraic conditions are satisfied, namely,

1. Correctness: $\mathbb{E}[f(x^n)] = \mathbb{E}[g(x^n)] = 0$, according to the assumption. Moreover,

$$\left|\mathbb{E}\left[f(x^n) \cdot g(y^n)\right] - \rho'\right| = \left|(f\mathsf{T}_\rho g)(x^n) - \rho'\right| = \left|f\mathsf{T}_\rho f - \rho'\right| = 0,$$

   which implies that

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

2. Alice security: Similarly, we have $\mathbb{E}_{y^n \sim U_{\{0,1\}^n}} |\mathsf{T}_\rho(f)(y^n) - \rho' \cdot g(y^n)| = 0$.
3. Bob security: Similarly, we have $\mathbb{E}_{x^n \sim U_{\{0,1\}^n}} |\mathsf{T}_\rho(g)(x^n) - \rho' \cdot f(x^n)| = 0$.

It is clear that χ_S is a balanced function, and when $|S| = k$ satisfies the mentioned constraints.

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

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

D.3 Omitted Proofs in Section 11

D.3.1 Proof of Lemma 5

Proof. First we prove that the L-infinity norm of $h^{(2)}$ is bounded above. For every $x \in \{0,1\}^n$, by Cauchy-Schwartz we have

$$h^{(2)}(x)^2 = \left(\sum_{S \in \mathcal{W}_k} \widehat{f^{(2)}}(S)\chi_S(x)\right)^2 \leqslant \left(\sum_{S \in \mathcal{W}_k} \widehat{f^{(2)}}(S)^2\right)\left(\sum_{S \in \mathcal{W}_k} \chi_S(x)^2\right) = \binom{n}{k}$$

since $\sum_{S \in \mathcal{W}_k} \widehat{f^{(2)}}(S)^2 \leqslant 1$ and $\chi_S(x)^2 = 1$. It implies that $\left\|h^{(2)}\right\|_\infty \leqslant \sqrt{\binom{n}{k}}$. Second, we show that $f^{(1,2)}$ is close to $h^{(1,2)}$. Let $\|f\|_2$ denote the L-2 norm of function f. By triangle inequality, we have

$$\begin{aligned}
\left\|f^{(1,2)} - h^{(1,2)}\right\|_2 &= \left\|f^{(1)}f^{(2)} - h^{(1)}h^{(2)}\right\|_2 \\
&\leqslant \left\|f^{(1)}f^{(2)} - f^{(1)}h^{(2)}\right\|_2 + \left\|f^{(1)}h^{(2)} - h^{(1)}h^{(2)}\right\|_2 \\
&= \left\|f^{(1)}(f^{(2)} - h^{(2)})\right\|_2 + \left\|h^{(2)}(f^{(1)} - h^{(1)})\right\|_2 \\
&= \left\|f^{(2)} - h^{(2)}\right\|_2 + \left\|h^{(2)}(f^{(1)} - h^{(1)})\right\|_2 \\
&\leqslant \delta + \left\|h^{(2)}\right\|_\infty \cdot \left\|f^{(1)} - h^{(1)}\right\|_2 \\
&\leqslant \delta\left(1 + \left\|h^{(2)}\right\|_\infty\right) \\
&\leqslant \delta\left(1 + \sqrt{\binom{n}{k}}\right)
\end{aligned}$$

This together with the fact that the Fourier spectral of $f^{(1,2)}$ are mostly concentrated on the set $\mathcal{W}_{2k}$ implies that

$$\sum_{S \notin \mathcal{W}_{2k}} \widehat{h^{(1,2)}}(S)^2 \leqslant \delta' + \delta\left(1 + \sqrt{\binom{n}{k}}\right).$$

Note that the event $S, T \in \mathcal{W}_k, S \cap T = \emptyset$ is equivalent to the event $S, T \in \mathcal{W}_k, |S \triangle T| = 2k$. Therefore, by union bound we have

$$\begin{aligned}
&\Pr_{\substack{S\sim\mathcal{S}(h^{(1)})\\T\sim\mathcal{S}(h^{(2)})}}[S, T \in \mathcal{W}_k, S \cap T = \emptyset] \\
&\geqslant 1 - \Pr_{S\sim\mathcal{S}(h^{(1)})}[S \notin \mathcal{W}_k] - \Pr_{T\sim\mathcal{S}(h^{(2)})}[T \notin \mathcal{W}_k] - \Pr_{\substack{S\sim\mathcal{S}(h^{(1)})\\T\sim\mathcal{S}(h^{(2)})}}[S \cap T \neq \emptyset, S, T \in \mathcal{W}_k] \\
&\geqslant 1 - \delta - \delta - \delta' - \delta\left(1 + \sqrt{\binom{n}{k}}\right) = 1 - \delta\left(3 + \sqrt{\binom{n}{k}}\right) - \delta'
\end{aligned}$$

□

D.3.2 Proof of Corollary 1

Proof. Note that the event $S^{(i)} \cap S^{(j)} = \emptyset \;\; \forall\, 1 \leqslant i < j \leqslant m, \left|S^{(i)}\right| = k \;\forall i \in [m]$ implies the event $\left|\bigcup_{i=1}^{m} S^{(i)}\right| \geqslant mk$. Now, according to Lemma 5, and by using union bound, the following bound holds.

$$\begin{aligned}
&\Pr_{(S^{(1)},S^{(2)},\ldots,S^{(m)})\sim\bigotimes_{i=1}^{m}\mathcal{S}(h^{(i)})}\left[\left|\bigcup_{i=1}^{m} S^{(i)}\right| \geqslant mk\right] \\
&\geqslant \Pr_{(S^{(1)},S^{(2)},\ldots,S^{(m)})\sim\bigotimes_{i=1}^{m}\mathcal{S}(h^{(i)})}\left[S^{(i)} \cap S^{(j)} = \emptyset \;\; \forall i, j, \left|S^{(i)}\right| = k \;\forall i\right] \\
&\geqslant 1 - \binom{m}{2}\left(\delta\left(3 + \sqrt{\binom{n}{k}}\right) + \delta'\right)
\end{aligned}$$

When $\binom{m}{2}\left(\delta\left(3 + \sqrt{\binom{n}{k}}\right) + \delta'\right) < 1$, there exists at least m subsets $S^{(1)}, S^{(2)}, \ldots, S^{(m)} \subseteq [n]$ such that $\left|S^{(1)} \cup S^{(2)} \cup \cdots \cup S^{(n)}\right| \geqslant mk$. This implies that $n \geqslant mk$. □