Secure Non-interactive Simulation: Feasibility & Rate

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

Department of Computer Science, Purdue University
{haminikh,hmaji,nguye245}@purdue.edu

Abstract. A natural solution to increase the efficiency of secure computation will be to non-interactively and securely transform diverse inexpensive-to-generate correlated randomness, like, joint samples from noise sources, into correlations useful for secure computation protocols. Motivated by this general application for secure computation, our work introduces the notion of *secure non-interactive simulation* (SNIS). Parties receive samples of correlated randomness, and they, without any interaction, securely convert them into samples from another correlated randomness.

Our work presents a simulation-based security definition for SNIS and initiates the study of the feasibility and efficiency of SNIS. We also study SNIS among fundamental correlated randomnesses like random samples from the binary symmetric and binary erasure channels, represented by BSS and BES, respectively. We show the impossibility of interconversion between BSS and BES samples.

Next, we prove that a SNIS of a $\mathsf{BES}(\varepsilon')$ sample (a BES with noise characteristic ε') from $\mathsf{BES}(\varepsilon)$ is feasible if and only if $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$. 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 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 non-linear SNIS constructions. When $(1-2\varepsilon') = (1-2\varepsilon)^k$, we prove that the rate of a *perfectly secure* SNIS is at most $1/k$, which is achievable using linear and non-linear constructions.

Our technical approach algebraizes the definition of SNIS and proceeds via Fourier analysis. Our work develops general analysis methodologies for Boolean functions, explicitly incorporating cryptographic security constraints. Our work also proves strong forms of *statistical-to-perfect security* transformations: one can error-correct a statistically secure SNIS to make it perfectly secure. We show a connection of our research with *homogeneous Boolean functions* and *distance-invariant codes*, which may be of independent interest.

[⋆] The research effort is supported in part by an NSF CRII Award CNS–1566499, NSF SMALL Awards CNS–1618822 and CNS–2055605, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Awards (2019–2020, 2020–2021), a Ross-Lynn Research Scholars Grant, a Purdue Research Foundation (PRF) Award, and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

1 Introduction

Secure multi-party computation [52, 26] (MPC) allows mutually distrusting parties to compute securely over their private data. MPC protocols often offload most cryptographically and computationally intensive components to an offline procedure [38, 8, 17, 45]. The objective of this offline procedure is to output secure samples from highly structured correlated randomness, for example, Beaver triples [4]. The offline procedure relies on public-key cryptography to achieve this objective and, consequently, is computation and communication intensive.

On the other hand, there are diverse inexpensive-to-generate correlated randomness, like, joint samples from noise sources, that can also facilitate secure computation via interactive protocols [30]. A natural approach to increase the efficiency of this offline phase will be to non-interactively and securely transform such correlated randomness into correlations useful for secure computation while incurring low computational overhead. Motivated by this general application for secure computation, our work introduces the notion of *secure non-interactive simulation* (SNIS).

In SNIS, parties receive samples of correlated randomness, and they, without any interaction, securely convert them into samples from another correlated randomness. Section 1.1 defines this cryptographic primitive. SNIS is an information-theoretic analog of *pseudorandom correlation generators* (PCG) introduced by Boyle et al. [11, 12]. PCG is a *silent* local computation that transforms the input correlated private randomness into samples from a target correlation without any interaction. Boyle et al. [11, 12] construct this primitive based on various hardness of computation assumptions and illustrate their applications to increasing the efficiency of the preprocessing step of MPC protocols. SNIS shall convert diverse forms of correlated randomness sources into samples of a specific target correlation that is useful for the online phase of an MPC protocol with information-theoretic security.

SNIS is an extension of *non-interactive simulation of joint distribution* [21, 50, 49, 27, 28, 25, 18, 24] (NIS) and *non-interactive correlation distillation* [41, 40, 51, 9, 13] (NICD) from information theory. In NIS, the emphasis is on the correctness of simulation, and cryptographic security is not a concern. Consequently, erasing information from parties' views, for example, is permissible in NIS, which may not be cryptographically secure. NICD specifically aims to establish shared keys securely; however, shared keys alone do not suffice for general secure computation [23, 35, 36]. The objective of SNIS extends to securely simulating more general correlated randomness as well, referred to as the *complete correlations* [30], which are necessary for general secure computation. One can also interpret SNIS as the non-interactive version of *one-way secure computation* [22, 2] (OWSC) – secure computations where only one party sends messages.

Our work presents a simulation-based security definition for SNIS and initiates the study of the feasibility and efficiency of SNIS. Any hardness of computation results from NIS and OWSC automatically transfer to SNIS. This work initiates the study of tight feasibility and rate characterization in SNIS and considers the inter-conversion among fundamental correlated randomnesses like random samples from the binary symmetric and binary erasure channels. In this context, our work reveals strong forms of statistical-to-perfect security transformations where one can error-correct a statistically secure SNIS (with sufficiently small insecurity) to transform it into a perfect SNIS. In particular, there is a dichotomy: either (1) a perfect SNIS exists, or (2) every SNIS is constant insecure. For example, there are perfect rate-achieving SNIS; however, surpassing the maximum rate by how-so-ever small quantity immediately incurs constant-insecurity.

Our technical approach algebraizes the definition of SNIS and proceeds via Fourier analysis. A central contribution of our work is the development of general analysis methodologies for Boolean functions that explicitly incorporate the cryptographic security constraints. Our research uncovers fascinating new connections of SNIS with *homogeneous Boolean functions* and *distance-invariant codes*, which may be of independent interest (refer to Section 2.6).

Paper organization. Section 1.1 presents the SNIS model. Section 2 summarizes our contributions, connections to other research areas (Section 2.6). All our results consider SNIS with *randomized reductions* and *statistical security* (except Theorem 6, which considers only perfect security). Section 3 introduces the technical background for our proofs. Section 4, Section 5, and Section 6 present the technical outline and details of our proofs. A full version of this paper is available at [29].

Independent work. Independently, motivated by studying *cryptographic complexity* [7, 37, 33, 6, 44], Agarwal, Narayanan, Pathak, Prabhakaran, Prabhakaran, and Rehan [1] introduced SNIS as *secure non-interactive reduction*. They use spectral techniques to analyze this primitive. Determining tight rate of SNIS reductions and results pertaining to editing statistical reductions into perfect ones are beyond the scope of their work.

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 $(x^n, y^n) \overset{\$}{\leftarrow} (X, Y)^{\otimes n}$, 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 $r_A \overset{\$}{\leftarrow} R_A$ and Bob has, independent, private randomness $r_B \overset{\$}{\leftarrow} R_B$, 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 $v' = g_n(y^n, r_B)$.

[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.

$$\begin{tikzcd}
 & & (x^n, y^n) \xleftarrow{\$} (X,Y)^{\otimes n} \arrow[dl, "x^n"'] \arrow[dr, "y^n"] & & \\
r_A \xleftarrow{\$} R_A \arrow[r] & \text{Alice} \arrow[d] & & \text{Bob} \arrow[d] & r_B \xleftarrow{\$} R_B \arrow[l] \\
 & \mathcal{U}^{\otimes m} \ni u' = f_n(x^n, r_A) & & v' = g_n(y^n, r_B) \in \mathcal{V}^{\otimes m} &
\end{tikzcd}$$

Fig. 1. Model for secure non-interactive simulation: SNIS.

For the ease of presentation, this section only considers deterministic reduction functions, i.e., there is no R_A and R_B. All formal definitions and results in this work consider randomized reductions.

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 $(U,V)^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} (X,Y)^{\otimes n}$. 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). 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).

When n is clear from the context, then, instead of x^n and f_n, we shall only write x and f for brevity.

Remark 1 (Adversarial model). 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.

[2] The conditional 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 $b \in \mathrm{Supp}(B)$.

Remark 2 (Reasoning for providing private coins). In the cryptographic context, complete joint distributions [30] (X,Y) are the primary resources that one uses frugally. So, to define the rate with respect to the cryptographically expensive resource (namely, samples from the distribution $(X,Y)^{\otimes n}$), our definition of SNIS considers randomized reductions and provides private independent random coins as a free resource. If private coins are not free, they can be incorporated into the setup by considering the input joint distribution to be $(X,Y)^{\otimes n} \otimes \mathsf{Coins}$.

2 Our Contribution

Rabin and Crépeau [47, 48, 14] and Crépeau and Kilian [15, 16], 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 initiate the study of the feasibility and rate of SNIS, this paper considers samples from the following two families of distributions.

1. *Binary symmetric source.* X and Y are uniformly random bits $\{+1,-1\}$ 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 $\{+1,-1\}$, and $Y = X$ with probability $(1-\varepsilon)$, where $\varepsilon \in (0,1)$; otherwise, $Y = 0$. We represent this joint distribution by $\mathsf{BES}(\varepsilon)$.

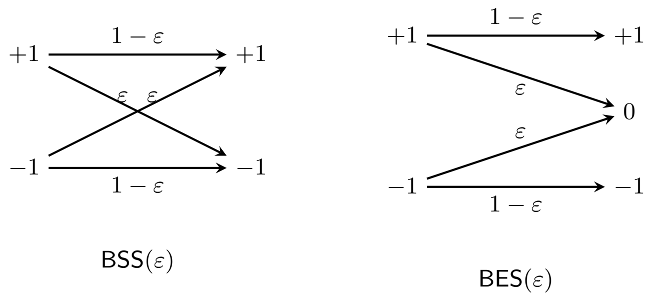

Fig. 2. Binary Symmetric Source (BSS) and Binary Erasure Source (BES) with noise characteristic ε.

Comparison models. In information theory, *non-interactive simulation of joint distributions* (NIS) is a similar notion of simulating joint distributions [21, 50, 49, 27, 28, 25, 18, 24]. However, NIS only considers correctness (not security). On the other hand, there is also research on performing secure computation using one-way messages, a.k.a., *one-way secure computation* (OWSC) [22, 2] – only one party sends messages to the other party. Table 1 compares our feasibility results to results in NIS and OWSC.

Remark 3. Non-interactive correlation distillation [41, 40, 51, 9, 13] 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 strong impossibility results and comparison with this model is not particularly insightful.

2.1 SNIS Composition and Projection

The following composition and projection results follow from the simulation-based definition of SNIS.

1. *Parallel Composition.* 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.* 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.* 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

There are a few flavors of derandomization results (for reductions) that are useful for different contexts like feasibility/rate results with perfect/statistical security.

For feasibility results. Let (X, Y) be a joint distribution such that the distribution $(X|Y)$ has average conditional min-entropy [20]. Then, Alice can extract (statistically) secure coins from a sufficiently large number of (X, Y) samples.[3] Analogously, if $(Y|X)$ has average conditional min-entropy, then Bob can also construct statistically secure coins using other (X, Y) samples. Complete joint distributions [30] (X, Y) have both these average conditional min-entropy properties.[4] Consequently, the following result is immediate.

[3] Alice can perform a random walk on an appropriate expander graph using her samples to get one random bit that is statistically secure conditioned on Bob's samples.

[4] A joint distribution (X, Y) is *complete* if there exists samples $x_0, x_1 \in \mathrm{Supp}(X)$ and $y_0, y_1 \in \mathrm{Supp}(Y)$ such that

1. $\Pr[X = x_0, Y = y_0], \Pr[X = x_1, Y = y_0], \Pr[X = x_1, Y = y_1] > 0$, and
2. $\Pr[X = x_0, Y = y_0] \cdot \Pr[X = x_1, Y = y_1] \neq \Pr[X = x_0, Y = y_1] \cdot \Pr[X = x_1, Y = y_0]$.

Proposition 1 (Derandomization: Feasibility results). *Let (X, Y) be a complete joint distribution. Consider a randomized SNIS $(U, V) \sqsubseteq^{\nu}_{f,g} (X, Y)^{\otimes n}$ with n_A and n_B Alice and Bob private randomness complexities, respectively. Then, there exists a deterministic SNIS $(U, V) \sqsubseteq^{\nu'}_{f',g'} (X, Y)^{\otimes n'}$ such that (for large-enough $k \in \mathbb{N}$)*

$$\begin{aligned} n' &= k \cdot n_A + k \cdot n_B + n, \text{ and} \\ \nu' &= (n_A + n_B) \cdot \exp(-\Theta(k)) + \nu. \end{aligned}$$

The reduction function f' uses the first kn_A samples to extract n_A private bits for Alice, each with $\exp(-\Theta(k))$ statistical security. The reduction function g' uses the next kn_B samples to extract n_B private bits for Bob. Finally, the reduction functions (f', g') restricted to the last n samples are identical to (f, g). This proposition effectively rules out the usefulness of independent private randomness in SNIS for feasibility results.

For rate results with perfect security. To study rate of SNIS, one needs a *sample-preserving* derandomization. However, in the context of perfect security, such a result is immediate for complete joint distribution (U, V). Intuitively, one can fix Alice's local randomness to an arbitrary value, and Bob's local randomness to an arbitrary value. Then, the reduction functions (with these fixed random tapes) continue to be a perfectly secure SNIS.

Proposition 2 (Derandomization: Sample-preserving & Perfect security). *Let (U, V) be a complete joint distribution. For any randomized SNIS $(U, V) \sqsubseteq^{0}_{f,g} (X, Y)^{\otimes n}$, there is a deterministic SNIS $(U, V) \sqsubseteq^{0}_{f',g'} (X, Y)^{\otimes n}$.*

The deterministic reduction functions f', g' are the randomized reductions f, g with their random tapes arbitrarily fixed.

For rate results with statistical security. For a statistical SNIS, we prove a sample-preserving derandomization result of the following form.

Theorem 1 (Derandomization: Sample-preserving & Statistical security). *Fix (X, Y) and a complete joint distribution (U, V). There is a positive constant c such that the following holds. Consider a randomized SNIS $(U, V) \sqsubseteq^{\nu}_{f,g} (X, Y)^{\otimes n}$. Then, there is a deterministic SNIS $(U, V) \sqsubseteq^{\nu'}_{f',g'} (X, Y)^{\otimes n}$ such that (a) $\nu' = c \cdot \nu^{1/4}$, (b) the reduction function f is ν'-close to the reduction function f', and (c) the reduction function g is ν'-close to the reduction function g'.*

This theorem also yields Proposition 2 as a corollary.

The *closeness* of a randomized and a deterministic function is defined as follows. The function f, for example, has domain $\mathcal{X}^n \times \mathcal{R}_A$. Extend the domain

Multiple samples of a complete distributions can be used to (interactively) implement oblivious transfer [30], the atomic primitive for secure computation. The joint distribution $\mathsf{BES}(\varepsilon)$, for $\varepsilon \in (0, 1)$, and $\mathsf{BSS}(\varepsilon)$, for $\varepsilon \in (0, 1/2)$, are complete distributions. However, $\mathsf{BSS}(0) = \mathsf{BES}(0)$, $\mathsf{BES}(1)$, and $\mathsf{BSS}(1/2)$ are *not* complete distributions.

of the deterministic function f' from $\mathcal{X}^n$ to $\mathcal{X}^n \times \mathcal{R}_A$. The two functions are ν'-close if their outputs differ for (at most) ν' fraction of the inputs.

The constant c in the theorem depends on the joint distributions (X, Y) and (U, V); however, it is independent of n. So, one can, for example, meaningfully derandomize the statistically secure SNIS $\mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{\nu} \mathsf{BES}(\varepsilon)^{\otimes n}$ by considering $(U, V) = \mathsf{BES}(\varepsilon')^{\otimes 2}$ and $(X, Y) = \mathsf{BES}(\varepsilon)$. However, it may not be possible to meaningfully derandomize the statistically secure SNIS $\mathsf{BES}(\varepsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)} \mathsf{BES}(\varepsilon)^{\otimes n}$ by considering $(U, V) = \mathsf{BES}(\varepsilon')^{\otimes m(n)}$ and $(X, Y) = \mathsf{BES}(\varepsilon)$. Because the value of c depends on n (via its dependence on $m(n)$), and the resulting insecurity bound $c \cdot \nu(n)^{1/4}$ may be meaningless (it may be greater than one). This discussion highlights a subtlety in proving the rate result in Theorem 4.

2.3 BSS from BES Samples

Input Joint Distribution	Output Joint Distribution	Feasible set of ε'		
		OWSC [22]	SNIS (Our Work)	NIS [53]
$\mathsf{BES}(\varepsilon)$	$\mathsf{BES}(\varepsilon')$	$(0, 1)$	$\left\{1 - (1 - \varepsilon)^k \colon\ k \in \mathbb{N}\right\}$	$[\varepsilon, 1)$
	$\mathsf{BSS}(\varepsilon')$	$\supseteq \emptyset$	$\emptyset$	$\supseteq [\varepsilon/2, 1/2)$ $\subseteq \left[\frac{1-\sqrt{1-\varepsilon}}{2}, 1/2\right)$
$\mathsf{BSS}(\varepsilon)$	$\mathsf{BES}(\varepsilon')$	$\emptyset$	$\emptyset$	$\emptyset$
	$\mathsf{BSS}(\varepsilon')$	$\supseteq \left\{\frac{1-(1-2\varepsilon)^k}{2} : k \in \mathbb{N}\right\}$	$\left\{\frac{1-(1-2\varepsilon)^k}{2} : k \in \mathbb{N}\right\}$	$[\varepsilon, 1/2)$

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.

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. *Reverse-hypercontractivity* [3, 10, 41, 42, 28, 18, 5, 40] is a typical technical tool in NIS to show such impossibility results. Consider the feasibility of $(U, V) \sqsubseteq \mathsf{BSS}(\varepsilon)^{\otimes n}$. Reverse-hypercontractivity states that if there are two samples u and v such that $\Pr[U = u] > 0$ and $\Pr[V = v] > 0$, then $\Pr[U = u, V = v] > 0$. Therefore, for example, *correctly* constructing BES samples and random oblivious transfer samples are impossible, let alone securely.

The following result considers the reverse direction.

Theorem 2 (Infeasibility: BSS from BES). *Fix noise parameters $\varepsilon \in (0, 1)$ and $\varepsilon' \in (0, 1/2)$. There is a positive constant $c = c(\varepsilon, \varepsilon')$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu} \mathsf{BES}(\varepsilon)^{\otimes n}$, for any $n \in \mathbb{N}$, implies that $\nu \geqslant c$.*

Section 4 proves this theorem. This impossibility result remains open in NIS and OWSC. However, using the properties of security, we even rule out SNIS that are constant-insecure. In particular, one cannot use a larger number of $\mathsf{BES}(\varepsilon)$ samples to arbitrarily reduce the insecurity.

2.4 BES from BES Samples

Next, we consider the inter-conversion among binary erasure sources with different erasure probabilities. At the outset, let us begin with an example of perfectly secure SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)^{\otimes k}$, where $(1-\varepsilon') = (1-\varepsilon)^k$ for some $k \in \mathbb{N}$. Alice's reduction function $f \colon \{\pm 1\}^k \to \{\pm 1\}$ is defined by $f(x) = x_1 \cdot x_2 \cdots x_k$, a linear function. Bob's reduction function $g \colon \{\pm 1, 0\}^k \to \{\pm 1, 0\}$ is defined by $g(y) = y_1 \cdot y_2 \cdots y_k$. Observe that $g(y) = 0$ if and only if there is $i \in \{1, \dots, k\}$ such that $y_i = 0$. Such reductions (or their negations) shall be referred to as *k-linear* functions. One can verify that this reduction is a perfect SNIS.

Feasibility. We prove that, essentially, k-linear functions are the only reductions possible among BES samples.

Theorem 3 (Feasibility: BES-BES). *Fix erasure probabilities $\varepsilon, \varepsilon' \in (0,1)$.*

1. *If $(1-\varepsilon') \neq (1-\varepsilon)^k$, for all $k \in \mathbb{N}$: There is a positive constant $c = c(\varepsilon, \varepsilon')$ such that $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu} \mathsf{BES}(\varepsilon)^{\otimes n}$, for any $n \in \mathbb{N}$, implies that $\nu \geqslant c$.*
2. *If $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$: There are positive constants $c = c(\varepsilon, \varepsilon')$ and $d = d(\varepsilon, \varepsilon')$ such that the following result holds. If $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$, for any $n \in \mathbb{N}$, and $\nu \leqslant c$, then f is ν^d-close to a reduction function f^*, and g is ν^d-close to a reduction function g^* such that $\mathsf{BES}(\varepsilon') \sqsubseteq^{0}_{f^*,g^*} \mathsf{BES}(\varepsilon)^{\otimes n}$. Furthermore, f^* is a k-linear function.*

We remark that the "$\nu^{\Theta(1)}$-closeness" in the theorem above can be replaced by "$\Theta(\sqrt{\nu})$-closeness;" however, we forego this optimization as it does not change the qualitative nature of our results. This theorem intuitively states the following.

1. If $(1-\varepsilon') \notin \{(1-\varepsilon), (1-\varepsilon)^2, (1-\varepsilon)^3, \dots\}$, then any SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$ must be constant-insecure.
2. If $(1-\varepsilon') = (1-\varepsilon)^k$ and reduction functions f, g implement a SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$ with sufficient small insecurity, then the reduction functions f and g can be error-corrected (at at most ν^d-fraction of its inputs) to create reduction functions f^*, g^*, respectively, such that the new SNIS is a perfectly secure. Furthermore, the function $f^*(x) = \pm x_{i_1} \cdot x_{i_2} \cdots x_{i_k}$, for distinct $i_1, i_2, \dots, i_k \in \{1, \dots, n\}$. This result, intuitively, is a strong form of *statistical-to-perfect transformation*: reductions implementing SNIS with sufficiently small insecurity can be error-corrected into perfectly secure SNIS reductions. Furthermore, the lower the insecurity, the lesser amount of error-correction shall be needed.

In the context of OWSC, one can achieve erasure probability ε' that is either lower or higher than the erasure probability ε. For SNIS, however, we show that $\varepsilon' \geqslant \varepsilon$ is necessary. Interestingly, our linear SNIS construction is identical in spirit to the OWSC protocol, as presented in [22] when $(1-\varepsilon') \in \{(1-\varepsilon), (1-\varepsilon)^2, \dots .\}$. However, all other values of ε' are feasible *only* for OWSC [22]; not for SNIS.

Typically, NIS literature's impossibility results rely on leveraging the reverse hypercontractivity theorem [27, 28, 43]. However, this approach encounters a significant hurdle for samples from the binary erasure channel [27]. The addition of the security constraint in our setting helps overcome this hurdle.

Rate of Statistical SNIS. Observe that if $(1-\varepsilon') = (1-\varepsilon)^k$, for $k \in \mathbb{N}$, then a block-linear reduction achieves $1/k$-rate via a perfectly secure SNIS. Our rate result states that these reductions are, essentially, the only rate-achieving constructions. For rate results, we consider (possibly, randomized) reduction functions $\vec{f} \colon \{\pm1\}^n \to \{\pm1\}^m$ and $\vec{g} \colon \{\pm1, 0\}^n \to \{\pm1, 0\}^m$. We interpret these reductions as the concatenation of m reductions. For example, $\vec{f} = \left(f^{(1)}, f^{(2)}, \dots, f^{(m)}\right)$ such that $f^{(i)} \colon \{\pm1\}^n \to \{\pm1\}$, for each $i \in \{1, 2, \dots, m\}$. We refer to the function $f^{(i)}$ as the *i-th component of $\vec{f}$.*

Theorem 4 (Rate: BES-BES). *Let $\varepsilon, \varepsilon' \in (0,1)$ be erasure probabilities such that $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$. There are positive constants $c = c(\varepsilon, \varepsilon')$ and $d = d(\varepsilon, \varepsilon')$ such that the following result holds. Suppose $\mathsf{BES}(\varepsilon')^{\otimes m} \sqsubseteq^{\nu}_{\vec{f},\vec{g}} \mathsf{BES}(\varepsilon)^{\otimes n}$, for some $m, n \in \mathbb{N}$, and $\nu \leqslant c$. Then, there are deterministic reduction functions $\vec{f^*}$ and $\vec{g^*}$ such that the following conditions are satisfied.*

1. *$f^{(i)}$ is ν^d-close to ${f^*}^{(i)}$, for $i \in \{1, \dots, m\}$,*
2. *$g^{(i)}$ is ν^d-close to ${g^*}^{(i)}$, for $i \in \{1, \dots, m\}$,*
3. *Each ${f^*}^{(i)}$ is k-linear with disjoint support, for $i \in \{1, \dots, m\}$, and*
4. *$mk \leqslant n$, i.e., $R(\mathsf{BES}(\varepsilon'), \mathsf{BES}(\varepsilon)) \leqslant 1/k$.*

A block-linear construction achieves the rate as well. We emphasize that the reductions $\vec{f}$ and $\vec{g}$ are possibly randomized. Note that this theorem *does not* claim that the reduction function $\vec{f}$ is close to $\vec{f^*}$.

Section 5 outlines the proof of Theorem 3 and Theorem 4.

2.5 BSS from BSS Samples

Finally, we consider the inter-conversion among binary symmetric samples with different noise characteristics. Observe that if $(1-2\varepsilon') = (1-2\varepsilon)^k$, for some $k \in \mathbb{N}$, then the following reduction functions $f, g \colon \{\pm1\}^k \to \{\pm1\}$ implement a perfectly secure SNIS of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BSS}(\varepsilon)^{\otimes k}$: $f(x) = x_1 \cdot x_2 \cdots x_k$ and $g(y) = y_1 \cdot y_2 \cdots y_k$. One can verify that this is a perfectly secure SNIS. However, surprisingly, unlike BES inter-conversions, linear functions are not the *only* secure reductions in BSS inter-conversions. For $k \geqslant 2$, consider the following non-linear reductions $f^{(1)}_{2k}, g^{(1)}_{2k} \colon \{\pm1\}^{2k} \to \{\pm1\}$, $g^{(1)}_{2k} = f^{(1)}_{2k}$ where $f^{(1)}_{2k}(x) = \frac{(x_1-x_2)}{2} \cdot \prod_{i=3}^{k+1} x_i + \frac{(x_1+x_2)}{2} \cdot \prod_{i=k+2}^{2k} x_i$. In fact, any *$k$-homogeneous* Boolean reduction function f and $g = f$ define a perfectly secure SNIS.

Although these non-linear constructions individually have worse efficiency than the linear constructions, they can achieve *rate* $1/k$, similar to the block-linear constructions. For example, consider another pair of reduction functions $f^{(2)}_{2k}, g^{(2)}_{2k} \colon \{\pm1\}^{2k} \to \{\pm1\}$, $g^{(2)}_{2k} = f^{(2)}_{2k}$ where $f^{(2)}_{2k}(x) = \frac{(x_1-x_2)}{2} \cdot \prod_{i=k+2}^{2k} x_i - \frac{(x_1+x_2)}{2} \cdot \prod_{i=3}^{k+1} x_i$. Now, interestingly, the two reductions $f^{(1)}_{2k} \| f^{(2)}_{2k}$ and $g^{(1)}_{2k} \| g^{(2)}_{2k}$ realize $\mathsf{BSS}(\varepsilon')^{\otimes 2} \sqsubseteq^{0} \mathsf{BSS}(\varepsilon)^{\otimes 2k}$ at rate $1/k$.

Feasibility. With this discussion as background, we mention our feasibility result.

Theorem 5 (Feasibility: BSS-BSS). *Fix noise characteristics $\varepsilon, \varepsilon' \in (0, 1/2)$.*

1. *If $(1-2\varepsilon') \neq (1-2\varepsilon)^k$, for all $k \in \mathbb{N}$: There is a positive constant $c = c(\varepsilon, \varepsilon')$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu} \mathsf{BSS}(\varepsilon)^{\otimes n}$, for any $n \in \mathbb{N}$, implies that $\nu \geqslant c$.*
2. *If $(1-2\varepsilon') = (1-2\varepsilon)^k$, for some $k \in \mathbb{N}$: There are positive constants $c = c(\varepsilon, \varepsilon')$ and $d = d(\varepsilon, \varepsilon')$ such that the following result holds. If $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$, for any $n \in \mathbb{N}$, and $\nu \leqslant c$, then f is ν^d-close to a reduction function f^* and g is ν^d-close to a reduction function g^* such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{0}_{f^*,g^*} \mathsf{BSS}(\varepsilon)^{\otimes n}$. Furthermore, $f^* = g^*$ is a k-homogeneous Boolean function.*

Similar to the theorem for binary erasure sources, this theorem also states a strong form of a statistical-to-perfect transformation. In the binary symmetric source case, the perfect reduction need not be a linear function; it may be a k-homogeneous Boolean function. Incidentally, as a consequence of the Kindler-Safra junta theorem [31, 32] (refer to Imported Theorem 1), the k-homogeneous Boolean functions implicitly are also juntas. This junta property shall be crucial in our proofs to show that the simulation error cannot be driven arbitrarily low by using larger number of input samples.

Note that one cannot increase the reliability of the binary symmetric source, which is identical to the result in [22]. However, unlike [22], we also rule out the possibility of SNIS for any $(1-2\varepsilon') \notin \left\{(1-2\varepsilon), (1-2\varepsilon)^2, \dots\right\}$. For such ε', any non-interactive simulation is *constant-insecure*.

Rate for Perfect SNIS. Unlike, the rate result for BES samples, we only prove a rate result for perfectly secure SNIS for BSS samples. We leave the rate result for statistically-secure SNIS as a fascinating open problem.

Theorem 6 (Perfect Security Rate: BSS-BSS). *Let $\varepsilon, \varepsilon' \in (0, 1/2)$ be noise characteristics such that $(1-2\varepsilon') = (1-2\varepsilon)^k$, for some $k \in \mathbb{N}$. If $\mathsf{BSS}(\varepsilon')^{\otimes m} \sqsubseteq^{0}_{\vec{f},\vec{g}} \mathsf{BSS}(\varepsilon)^{\otimes n}$, for some $m, n \in \mathbb{N}$, then $\vec{g} = \vec{f}$, each component of $\vec{f}$ is a k-homogeneous Boolean function, and $mk \leqslant n$, i.e., $R(\mathsf{BSS}(\varepsilon'), \mathsf{BSS}(\varepsilon)) \leqslant 1/k$.*

We emphasize that the components of the reduction $\vec{f}$ need not have disjoint input supports (as illustrated by the example above where we construct 2 output samples from $2k$ input samples using non-linear functions with identical input support). Both linear and non-linear rate-achieving perfect SNIS exist.

Section 6 outlines the proof of Theorem 5 and Theorem 6.

2.6 Technical Contribution and Connections

Homogeneous Boolean functions. A Boolean function $f\colon \{\pm 1\}^n \to \{\pm 1\}$ is k-homogeneous if its Fourier weight is entirely on degree-k (multi-)linear terms. For example, $f(x) = x_1 \cdots x_k$ is a k-homogeneous function and is *linear* as well (because its entire Fourier weight is concentrated on one character). Refer to the functions $f_{2k}^{(1)}, f_{2k}^{(2)}$ in Section 2.5 for examples of *non-linear* k-homogeneous functions. The algebraization of security in Claim 13 implies the following result.

Proposition 3. $\mathsf{BSS}(\varepsilon') \sqsubseteq_{f,g}^{0} \mathsf{BSS}(\varepsilon)^{\otimes n}$ *if and only if* $g = f$, f *is a* k*-homogeneous Boolean function, and* $(1 - 2\varepsilon') = (1 - 2\varepsilon)^k$.

In fact, we show a stronger result. If the reduction in the proposition above realizes a SNIS with sufficiently small insecurity, then the reduction can be error-corrected to obtain a perfect reduction (see Theorem 5).

This proposition presents a new application for the study of homogeneous Boolean functions. The characterization of k-homogeneous Boolean functions is not well-understood. For example, the Kindler-Safra junta theorem [31, 32] implies that such functions are juntas as well. A better understanding of the analytical properties of these functions shall help resolve the rate of statistical SNIS among BSS samples.

Distance-invariant codes. For a reduction function $f\colon \{\pm 1\}^n \to \{\pm 1\}$, one can equivalently identify it by the following code

$$\{\pm 1\}^n \supseteq C(f, +1) = \{x \colon f(x) = +1\}\,.$$

Analogously, the code $C(f, -1)$ is the complement of the set $C(f, +1)$.

A code $C \subseteq \{\pm 1\}^n$ is *distance-invariant* [34] if the number of codewords $A_i(c)$ at distance $i \in \{0, 1, \ldots, n\}$ from a codeword $c \in C$ is independent of c. For example, linear codes are distance-invariant. There are non-linear distance-invariant codes as well. For example, when $k = 2$, the function $f_{2k}^{(1)}$ in Section 2.5 yields the following code.

$$\{\pm 1\}^{2k} \supset C(f_{2k}^{(1)}, +1) = \left\{\begin{array}{ccccc} 1111, & 11{-}11, & 1{-}11{-}1, & -1{-}11{-}1, & -1{-}1{-}1{-}1 \\ & 1{-}111, & -11{-}11, & -11{-}1{-}1, & \end{array}\right\}.$$

The codewords are sorted based on their distance from the codeword 1111 (i.e., their Hamming weight). Observe that every codeword $c \in C(f_{2k}^{(1)}, +1)$ has 2 codewords at distance 1, 2, and 3; and 1 codeword at distance 0 and 4. That is, the *distance enumerator* $A(c, Z) := \sum_{i=1}^{2k} A_i(c) Z^i = 1 + 2Z + 2Z^2 + 2Z^3 + Z^4$, for any codeword $c \in C(f_{2k}^{(1)}, +1)$.

In fact, the code $C(f_{2k}^{(1)}, -1)$ is also distance-invariant (codewords are sorted by weight below) and has an *identical distance enumerator*.

$$\{\pm 1\}^{2k} \supset C(f_{2k}^{(1)}, -1) = \left\{\begin{array}{ccc} -1111, & -1{-}111, & 1{-}1{-}1{-}1, \\ 111{-}1, & -111{-}1, & -1{-}1{-}11, \\ & 1{-}1{-}11, & \\ & 11{-}1{-}1, & \end{array}\right\}.$$

Each codeword $c \in C(f_{2k}^{(1)}, -1)$ has 2 codewords at distance 1, 2, and 3; and 1 codeword at distance 0 and 4. These properties are no coincidence.

Proposition 4. $\mathsf{BSS}(\varepsilon') \sqsubseteq^0_{f,g} \mathsf{BSS}(\varepsilon)$, *for some* $\varepsilon, \varepsilon' \in (0, 1/2)$, *if and only if (a)* $f = g$, *and (b) the distance enumerators for any codeword in* $C(f, +1)$ *and* $C(f, -1)$ *are identical.*

Therefore, if distance-invariant codes $C(f, +1)$ and $C(f, -1)$ have identical distance enumerator then f is homogeneous.

3 Preliminaries

We denote $[n]$ as the set $\{1, 2, \dots n\}$. For two functions $f, g \colon \Omega \to \mathbb{R}$, the equation $f = g$ means that $f(x) = g(x)$ for every $x \in \Omega$. We use $\mathcal{X}, \mathcal{Y}, \mathcal{U}, \mathcal{V}$, or Ω to denote the sample spaces. We also use (X, Y) to denote the joint distribution over $(\mathcal{X}, \mathcal{Y})$ with probability mass function π, and π_x, π_y to denote the marginal probability distributions of X and Y, respectively. For $x \in \mathcal{X}^n$, we represent $x_i \in \mathcal{X}$ as the i-th coordinate of x.
Statistical Distance. The statistical distance (total variation distance) between two distributions P and Q over a finite sample space Ω is defined as $\mathsf{SD}(P, Q) = \frac{1}{2} \sum_{x \in \Omega} |P(x) - Q(x)|$.
Norms. We use $L^2(\Omega, \mu)$ to denote the real inner product space of functions $f : \Omega \to \mathbb{R}$ with inner product $\langle f, g \rangle_\mu = \mathbb{E}_{x \sim \mu} [f(x) \cdot g(x)]$. The p-norm of a function $f \in L^2(\Omega, \mu)$ is defined as $\|f\|_p := [\mathbb{E}_{x \sim \mu} |f(x)|^p]^{1/p}$.

3.1 Introductory Fourier Analysis over Boolean Hypercube

We recall some background in Fourier analysis that will be useful for our analysis (see [46] for more details). Let $f, g \colon \{\pm1\}^n \to \mathbb{R}$ be two real-valued functions. We define the inner product of two functions as following.

$$\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{\pm1\}^n} f(x) \cdot g(x) = \mathop{\mathbb{E}}_{x} [f(x) \cdot g(x)]$$

A function is *Boolean* if its range is $\{\pm1\}$. For each $S \subseteq [n]$, the characteristic function $\chi_S(x) = \prod_{i \in S} x_i$ is a *linear* function. The set of all χ_S forms an orthonormal basis for the space of all real-valued functions on $\{\pm1\}^n$. 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 *multi-linear 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 $\mathsf{W}^k[f] := \sum_{S : |S| = k} \widehat{f}(S)^2$. Similarly, the Fourier weight of f on all degrees except k is $\mathsf{W}^{\neq k}[f] := \sum_{S : |S| \neq k} \widehat{f}(S)^2$ and the Fourier weight of f on all degrees greater than k is $\mathsf{W}^{>k}[f] := \sum_{S : |S| > k} \widehat{f}(S)^2$. Parseval's Identity says that $\|f\|_2^2 = \sum_{S \subseteq [n]} \widehat{f}(S)^2$. In particular, if f is Boolean, it implies that $\sum_{S \subseteq [n]} \widehat{f}(S)^2 = 1$.

Next, we summarize the basic Fourier analysis of Boolean function with *restriction* on the sub-cubes. Let J and $\bar{J}$ be a partition of the set $[n]$. Let

$f_{J|z} : \{\pm 1\}^J \to \mathbb{R}$ denote the restriction of f to J when the coordinates in $\bar{J}$ are fixed to $z \in \{\pm 1\}^{|\bar{J}|}$. 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 $z \in \{\pm 1\}^{|\bar{J}|}$ is chosen uniformly at random, we have

$$\mathop{\mathbb{E}}_{z}[\widehat{f_{J|z}}(S)] = \widehat{f}(S) \tag{1}$$

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

For any $y \in \{\pm 1, 0\}^n$, we define $J_y := \{i \in [n] : y_i = 0\}$, $\bar{J}_y := [n] \setminus J_y$, and we also define z_y as the concatenation of all non-zero symbols of y. For example, if $y = (1, 0, -1, 0)$, then $J_y = \{2, 4\}$, $\bar{J}_y = \{1, 3\}$ and $z_y = (1, -1)$.

Degree of a Function. The *degree* of a function $f : \{\pm 1\}^n \to \mathbb{R}$ is the degree of its multilinear expansion, i.e., $\max\{|S| : \widehat{f}(S) \neq 0\}$.

Homogeneous Functions. A function $f : \{\pm 1\}^n \to \mathbb{R}$ is *k-homogeneous* if every term in the multi-linear expansion of f has degree k.

Junta Functions. A function $f : \{\pm 1\}^n \to \mathbb{R}$ is *d-junta* if the output of the function f depends on at most d inputs, where d is usually a constant independent of n.

Linear Functions. A function f is *linear* if $f = \pm \chi_S$ for some $S \subseteq [n]$.

3.2 Noise and Markov Operators

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

Markov Operator [39]. Let (X, Y) be a finite distribution over $(\mathcal{X}, \mathcal{Y})$ with probability distribution π. The *Markov operator* associated with this distribution, denoted by T, maps a function $g \in L^2(\mathcal{Y}, \pi_y)$ to a function $Tg \in L^2(\mathcal{X}, \pi_x)$ by $(\mathsf{T}g)(x) := \mathbb{E}[g(Y) \mid X = x]$, where (X, Y) is distributed according to π. Furthermore, we define the *adjoint operator* of T, denoted as $\overline{\mathsf{T}}$, maps a function $f \in L^2(\mathcal{X}, \pi_x)$ to a function $\overline{\mathsf{T}}f \in L^2(\mathcal{Y}, \pi_y)$ by $(\overline{\mathsf{T}}f)(y) = \mathbb{E}[f(X) \mid Y = y]$.

Example 1. For $\mathsf{BSS}(\varepsilon)$, both marginal distributions π_x and π_y are the uniform distribution over $\{\pm 1\}$. Both the Markov operator T and its adjoint $\overline{\mathsf{T}}$ associated with $\mathsf{BSS}(\varepsilon)$ are identical to the noise operator T_ρ, where $\rho = 1 - 2\varepsilon$.

Example 2. For $\mathsf{BES}(\varepsilon)$, the marginal distribution π_x is the uniform distribution over $\{\pm 1\}$, and π_y satisfies $\pi_y(+1) = \pi_y(-1) = (1 - \varepsilon)/2$ and $\pi_y(0) = \varepsilon$. For any functions $f \in L^2(\{\pm1\}, \pi_x)$ and $g \in L^2(\{\pm1, 0\}, \pi_y)$, the Markov operator and its adjoint associated with $\mathsf{BES}(\varepsilon)$ are as follows.

$$(\mathsf{T}g)(x) = (1-\varepsilon)\cdot g(x) + \varepsilon \cdot g(0) \text{ for every } x \in \{\pm1\}$$
$$(\overline{\mathsf{T}}f)(y) = \begin{cases} f(y) & \text{if } y \in \{\pm1\} \\ 1/2 \cdot f(1) + 1/2 \cdot f(-1) & \text{if } y = 0 \end{cases}$$

3.3 Imported Theorems

This section present results that are useful for our proofs. We use the following version of Kindler-Safra junta theorem (Theorem 1.1 in [19]).

Imported Theorem 1 (Kindler-Safra Junta Theorem [31, 32]) *Fix $d \geqslant 0$. There exists $\varepsilon_0 = \varepsilon_0(d)$ and constant C such that for every $\varepsilon < \varepsilon_0$, if $f\colon \{\pm1\}^n \to \{\pm1\}$ satisfies $\mathsf{W}^{>d}[f] = \varepsilon$ then there exists a C^d-junta and degree d function $\tilde{f}\colon \{\pm1\}^n \to \{\pm1\}$ such that $\left\| f - \tilde{f} \right\|_2^2 \leqslant (\varepsilon + C^d \varepsilon^{5/4})$.*

This theorem says that any Boolean function whose Fourier spectrum is concentrated on low degree multi-linear terms is close to a low degree Boolean Junta.

Lemma 1 (Exercise 1.11 Chapter 1 [46]). *Suppose that $f\colon \{\pm1\}^n \to \{\pm1\}$ has degree $d \geqslant 1$. Then, for every $S \subseteq [n]$, the Fourier coefficient $\widehat{f}(S)$ is an integer multiple of $2/2^d$.*

This lemma states that a bounded-degree function's spectrum is coarse-grained.

4 Technical Overview: BSS from BES Samples

We outline the proof of Theorem 2 below.

Infeasibility Outline. Consider a randomized SNIS $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$, where $\varepsilon \in (0,1)$ and $\varepsilon' \in (0,1/2)$. Using Proposition 1 (the derandomization result for feasibility results), we can, without loss of generality, assume that f and g are deterministic functions. Therefore, we have $f\colon \{\pm1\}^n \to \{\pm1\}$ and $g\colon \{\pm1, 0\}^n \to \{\pm1\}$. Define $\rho = (1-\varepsilon)$ and $\rho' = (1-2\varepsilon')$.

Step 1: Algebraization of security. The simulation-based definition of SNIS of BSS from BES samples can be algebraized as follows.

Claim 1 (BSS-BES Algebraization of Security) *For any $\varepsilon \in (0,1)$ and $\varepsilon' \in (0,1/2)$, the following statements hold.*

1. *If $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$, then $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\|\overline{\mathsf{T}}f - \rho' g\right\|_1 \leqslant 4\nu$, and $\left\|\mathsf{T}g - \rho' f\right\|_1 \leqslant 4\nu$.*
2. *If $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\|\overline{\mathsf{T}}f - \rho' g\right\|_1 \leqslant \nu$, and $\left\|\mathsf{T}g - \rho' f\right\|_1 \leqslant \nu$, then $\mathsf{BSS}(\varepsilon') \sqsubseteq^{2\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$.*

Recall that T and $\overline{\mathsf{T}}$ are the Markov and the adjoint Markov operators associated with the $\mathsf{BES}^{\otimes n}$ joint distribution. This claim shows the qualitative equivalence of the simulation-based security definition and the algebraized definition (they incur only a multiplicative constant loss in insecurity during interconversion). Furthermore, this claim preserves perfect security.

Step 2: Approximate eigenvector problem. Let us focus on the reduction function $f\colon \{\pm1\}^n \to \{\pm1\}$. Composing the two constraints (a) $\left\|\overline{\mathsf{T}}f - \rho' g\right\|_1 \leqslant 4\nu$, and (b) $\left\|\mathsf{T}g - \rho' f\right\|_1 \leqslant 4\nu$, we get that $\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 \leqslant 8\nu$. This property is an eigenvector problem for the $\mathsf{T}\overline{\mathsf{T}} = \mathsf{T}_\rho$ operator.

Claim 2 ("Noisy Close-to-Scaling" Constraint) *If* $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$, *then it holds that* $\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 = \left\|\mathsf{T}_\rho f - {\rho'}^2 f\right\|_1 \leqslant 8\nu$.

Step 3: Homogeneous property. Recall that T_ρ operator scales $\widehat{f}(S)$ proportional to $\rho^{|S|}$. If ${\rho'}^2 \not\in \{\rho, \rho^2, \rho^3, \dots\}$, then $\mathsf{T}_\rho f$ cannot be close to ${\rho'}^2 f$. In this case, when f is Boolean, there shall always be a constant gap between $\mathsf{T}_\rho f$ and ${\rho'}^2 f$. That is, ν is at least a constant. The proof is done.

On the other hand, suppose ${\rho'}^2 = \rho^k$, for some $k \in \mathbb{N}$. In this case, any weight on $\widehat{f}(S)$ such that $|S| \neq k$ contributes to the gap between $\mathsf{T}_\rho f$ and ${\rho'}^2 f$. Consequently, most of the Fourier-weight of f must be on the degree-k (multi-)linear terms. The following claim formalizes this argument.

Claim 3 (Properties of Reduction Functions) *Suppose* $\left\|\mathsf{T}_\rho f - \rho^k f\right\|_1 \leqslant \delta$, *then there exists* $D = D(k)$ *such that the following statements hold.*

1. *The function f is $\frac{2\delta}{(1-\rho)\rho^{2k}}$-close to k-homogeneous.*
2. *There exists a Boolean k-homogeneous D-junta function $\tilde{f}\colon \{\pm1\}^n \to \{\pm1\}$ such that $\left\|f - \tilde{f}\right\|_2^2 \leqslant \sigma + D\sigma^{5/4}$, where $\sigma = \frac{2}{(1-\rho)^2\rho^{2k}} \cdot \delta$.*

The result that (the Boolean) f is close to a Boolean junta function is a consequence of Kindler-Safra junta theorem [31, 32] (refer to Imported Theorem 1) and this property of f shall be crucial for our strong statistical-to-perfect transformation. Due to the qualitative equivalence of simulation-based and algebraic definition of security, if f, g witness a secure SNIS with ν insecurity, then $\widetilde{f}, g$ witness a secure SNIS with comparable insecurity (say, $\mathsf{poly}(\nu)$-insecurity). Henceforth, we shall use the k-homogeneous D-junta (Boolean) reduction function $\widetilde{f}$ instead of the reduction f. The proof of the entire argument presented in this step relies on Theorem 8 and Theorem 9.

Step 4: Infeasibility. This step is the continuation of the case that ${\rho'}^2 = \rho^k$, for $k \in \mathbb{N}$. In this step, we shall use the properties of the reduction function $g\colon \{\pm1, 0\}^n \to \{\pm1\}$ and security to conclude that the reduction must be constant-insecure.

Theorem 7 (Insecurity Lower Bound). *Let $\overline{\mathsf{T}}$ be the adjoint Markov operator associated with the joint distribution $\mathsf{BES}(\varepsilon)^{\otimes n}$. Suppose $h\colon \{\pm1\}^n \to \{\pm1\}$ is a Boolean k-homogeneous D-junta function, and $g\colon \{\pm1, 0\}^n \to \{\pm1\}$ be any arbitrary function. Then $\left\|\overline{\mathsf{T}}h - \rho' g\right\|_1 \geqslant \rho' \cdot \min\left(\left(\frac{1-\varepsilon}{2}\right)^D, \varepsilon^D\right)$.*

Observe that without the junta property of h, we would not have obtained a constant lower bound to the insecurity. Section 4.2 proves this theorem.

4.1 Our Technical Results

This section presents our technical results that are crucial to the proofs of the feasibility and rate results (for not only SNIS of BSS from BES but also SNIS of BES from BES and BSS from BSS). The following theorem basically solves the "approximate eigenvector problem". Intuitively, it says that if the noisy version of a Boolean function is sufficiently-close to a scaling of that function, then (1) the scaling factor must be an eigenvalue of the noise operator and (2) the Fourier spectrum of that function is concentrated on some particular degree, i.e., it is close to a homogeneous (not necessarily Boolean) function.

Theorem 8 (Constant Insecurity or Close to Homogeneous). *Fix parameters $\rho, \rho' \in (0,1)$. Let $f\colon \{\pm1\}^n \to \{\pm1\}$ be a Boolean function, and let $\delta = \|\mathsf{T}_\rho f - \rho' f\|_1$. Then, the following statement hold.*

1. *If $\rho^{t+1} < \rho' < \rho^t$ for some $t \in [n]$, then $\delta \geqslant \frac{1}{2}\min((\rho' - \rho^t)^2, (\rho' - \rho^{t+1})^2)$.*
2. *If $\rho' = \rho^k$ for some $k \in [n]$, then $\mathsf{W}^k[f] \geqslant 1 - \frac{2}{(1-\rho)^2 \rho'^2} \cdot \delta$.*

Proof. Since $|(\mathsf{T}_\rho f)(x)| \leqslant 1$ and $f(x) \in \{\pm1\}$ for every x, we have

$$|(\mathsf{T}_\rho f)(x) - \rho' \cdot f(x)| \leqslant 1 + \rho' \leqslant 2 \text{ for every } x.$$

This implies that

$$\|(\mathsf{T}_\rho f)(x) - \rho' f\|_2^2 = \mathop{\mathbb{E}}_x [(\mathsf{T}_\rho f)(x) - \rho' \cdot f(x)]^2 \leqslant 2 \mathop{\mathbb{E}}_x |(\mathsf{T}_\rho f)(x) - \rho' \cdot f(x)| \leqslant 2\delta.$$

Case 1: If $\rho^{t+1} < \rho' < \rho^t$ for some $t \in [n]$, then $\delta = \|(\mathsf{T}_\rho f)(x) - \rho' f\|_1$ is bounded from below by

$$\frac{1}{2}\|(\mathsf{T}_\rho f)(x) - \rho' f\|_2^2 = \frac{1}{2}\sum_{S \subseteq [n]} (\rho^{|S|} - \rho')^2 \widehat{f}(S)^2 \geqslant \frac{1}{2}\min((\rho' - \rho^t)^2, (\rho' - \rho^{t+1})^2).$$

Case 2: $\rho' = \rho^k$ for some $k \in \mathbb{N}$. Observe that $\left|\rho^{|S|} - \rho'\right| \geqslant \left|\rho^{k+1} - \rho^k\right|$ for any $|S| \neq k$. Therefore, we have

$$\sum_{|S| \neq k} (\rho^{k+1} - \rho^k)^2 \widehat{f}(S)^2 \leqslant \sum_{|S| \neq k} (\rho^{|S|} - \rho^k)^2 \widehat{f}(S)^2 = \left\|(\mathsf{T}_\rho f)(x) - \rho^k f\right\|_2^2 \leqslant 2\delta.$$

This implies that $\mathsf{W}^{\neq k}[f] = \sum_{S\colon |S| \neq k} \widehat{f}(S)^2 \leqslant \frac{2\delta}{\rho^{2k}(1-\rho)^2}$, as desired.

Next, we show that if a noisy version of a Boolean function is close to that function scaled by an eigenvalue of the noise operator, then the function is close to a homogeneous junta Boolean function.

Theorem 9 (Close to Homogeneous and Junta). *Let $\rho \in (0,1)$ and $k \in \mathbb{N}$. There exist constants $D = D(k) > 0$, $\delta_0 = \delta_0(\rho, k) > 0$ such that the following statement holds. For any $\delta < \delta_0$, if the function $f \colon \{\pm1\}^n \to \{\pm1\}$ satisfies $\left\| \mathsf{T}_\rho f - \rho^k f \right\|_1 = \delta$, then there exists a k-homogeneous D-junta function $\tilde{f} \colon \{\pm1\}^n \to \{\pm1\}$ such that $\left\| f - \tilde{f} \right\|_2^2 \leqslant \sigma + D\sigma^{5/4}$, where $\sigma = \frac{2}{(1-\rho)^2\rho^{2k}} \cdot \delta$.*

We use the Kindler-Safra junta theorem (Imported Theorem 1) and the following claim to prove this theorem.

Claim 4 *Let $f, \tilde{f} \colon \{\pm1\}^n \to \{\pm1\}$ be two Boolean functions. Suppose $\mathsf{W}^k[f] \geqslant 1 - \delta$ and $\left\| f - \tilde{f} \right\|_2 \leqslant \gamma$. Then it holds that $\mathsf{W}^k[\tilde{f}] \geqslant 1 - \delta - 2\gamma$.*

Basically, the claim tells us that if a Boolean function $\tilde{f}$ is close to another Boolean function that is also close to a homogeneous (not necessarily Boolean) function, then $\tilde{f}$ is also close to a homogeneous function.

Proof (of Theorem 9). Applying Theorem 8 for the reduction function f satisfying $\left\| \mathsf{T}_\rho f - \rho^k f \right\|_1 \leqslant \delta$ yields $\mathsf{W}^{\neq k}[f] = 1 - \mathsf{W}^k[f] \leqslant \frac{2}{(1-\rho)^2\rho^{2k}} \cdot \delta$. Let $\varepsilon_0 = \varepsilon_0(k)$ be the constant achieved by applying Imported Theorem 1. Let $\delta_1 = \frac{(1-\rho)^2\rho^{2k}}{2} \cdot \varepsilon_0$. Note that δ_1 depends only on k and $\delta_1 \leqslant \varepsilon_0$. This implies that, for any $\delta < \delta_1$, we have $\mathsf{W}^{\neq k}[f] \leqslant \varepsilon_0$. Invoking Imported Theorem 1, there exists a C^k-junta and degree k function $\tilde{f} \colon \{\pm1\}^n \to \{\pm1\}$ such that $\left\| f - \tilde{f} \right\|_2^2 \leqslant \sigma + C^k\sigma^{5/4}$, where $\sigma = \frac{2}{(1-\rho)^2\rho^{2k}} \cdot \delta$. Next, we show that $\tilde{f}$ is k-homogeneous, i.e., $\mathsf{W}^k[\tilde{f}] = 1$. By Claim 4, we have $\mathsf{W}^k[\tilde{f}] \geqslant 1 - \sigma - 2\sqrt{\sigma + C^k\sigma^{5/4}}$. We choose δ_2 to be a constant such that $\sigma + 2\sqrt{\sigma + C^k\sigma^{5/4}} < \frac{1}{2^{2(k-1)}}$ for every $\delta < \delta_2$. Note that δ_2 depends only on ρ and k. If $\mathsf{W}^k[\tilde{f}] \neq 1$, it follows from Lemma 1 that $\mathsf{W}^{=k}[\tilde{f}]$ is far from 1, in other words, $\mathsf{W}^k[\tilde{f}] \leqslant 1 - 1/2^{2(k-1)} < 1 - \sigma - 2\sqrt{\sigma + C^k\sigma^{5/4}}$, which is a contradiction. So it must be the case that $\mathsf{W}^k[\tilde{f}] = 1$ when $\delta \leqslant \delta_2$. Choosing $\delta_0 = \min(\delta_1, \delta_2)$ completes the proof.

Finally, the following result says that two low-degree Boolean functions cannot be too close. We use the granularity property of low-degree Boolean function (see Lemma 1) to prove this lemma.

Lemma 2 (Low-degree Boolean Functions are Far). *If $h, \ell \colon \{\pm1\}^n \to \{\pm1\}$ are distinct Boolean functions of degree (at most) d, then $\|h - \ell\|_2 \geqslant 2/2^d$.*

Proof. Since h and ℓ are two distinct functions, there exists a $S^* \subseteq [n]$ such that $\widehat{h}(S^*) \neq \widehat{\ell}(S^*)$. Invoking Lemma 1 for low degree functions h and ℓ yields that the Fourier coefficients of h and ℓ are integer multiple of $1/2^{d-1}$. This implies that $\left|\widehat{h}(S^*) - \widehat{\ell}(S^*)\right| \geqslant 1/2^{d-1}$. Therefore, we have

$$\|h-\ell\|_2^2 = \sum_{S\subseteq[n]} (\widehat{h}(S) - \widehat{\ell}(S))^2 \geqslant (\widehat{h}(S^*) - \widehat{\ell}(S^*))^2 \geqslant 1/2^{2(d-1)},$$

which completes the proof.

As a consequence, we have the following corollary.

Corollary 1. *Fix noise parameter $\rho \in (0,1)$. Suppose $h, \ell \colon \{\pm1\}^n \to \{\pm1\}$ are two distinct d-homogeneous Boolean functions. Then, $\left\|\mathsf{T}_\rho h - \rho^d \ell\right\|_2 \geqslant 2\rho^d/2^d$.*

4.2 Proof of Theorem 7

First, we state some claims that are needed for the proof of Theorem 7. Recall that $J_y := \{i \in [n] : y_i = 0\}$ and z_y denotes the concatenation of all non-zero symbols of y as defined in Section 3.2.

Claim 5 (Connection with Restriction of Functions) *Let $\overline{\mathsf{T}}$ be the adjoint Markov operator of $\mathsf{BES}(\varepsilon)^{\otimes n}$, and let $f \colon \{\pm1\}^n \to \{\pm1\}$. Then, for every $y \in \{\pm1, 0\}^n$, it holds that $(\overline{\mathsf{T}}f)(y) = \widehat{f_{J_y|z_y}}(\emptyset)$.*

Proof. Since the distribution of (X, Y) is $\mathsf{BES}(\varepsilon)$, for any $i \in [n]$ that $y_i = 1$, $\Pr[X_i = 1 | Y_i = y_i = 1] = 1$ and for any $i \in [n]$ that $y_i = -1$, $\Pr[X_i = -1 | Y_i = y_i = -1] = 1$; while for any $i \in [n]$ that $y_i = 0$, $\Pr[X_i = 1 | Y_i = y_i = 0] = \Pr[X_i = -1 | Y_i = y_i = 0] = 1/2$. This implies that conditioned on non-zero symbols of y, i.e., z_y, the conditional distribution over the corresponding symbols of x is deterministic while over the rest of symbols is uniform. Therefore, we have

$$\begin{aligned}
(\overline{\mathsf{T}}f)(y) &= \mathbb{E}[f(X)|Y = y] && \text{(Definition of adjoint operator)}\\
&= \mathbb{E}[f(X)|J_y, z_y] && (J_y, z_y \text{ implies } y)\\
&= \mathbb{E}[f_{J_y|z_y}(X)] && \text{(Definition of restriction function)}\\
&= \widehat{f}_{J_y|z_y}(\emptyset).
\end{aligned}$$

Claim 6 (Fourier Property of Homogeneous Functions) *Let f be a Boolean k-homogeneous function. Then, for every $y \in \{\pm1, 0\}^n$ satisfying $\left|\bar{J}_y\right| < k$, it holds that $\widehat{f}_{J_y|z_y}(\emptyset) = 0$.*

Proof. First, note that $\widehat{f}(S) = 0$ for every $|S| \neq k$. This together with equation (2) implies that, for every $y \in \{\pm1, 0\}^n$ satisfying $\left|\bar{J}_y\right| < k$,

$$\mathop{\mathbb{E}}_{z_y}\left[\widehat{f}_{J_y|z_y}(\emptyset)^2\right] = \sum_{T\subseteq \bar{J}_y} \widehat{f}(T)^2 = 0.$$

Therefore, it must hold that $\widehat{f}_{J_y|z_y}(\emptyset) = 0$ as desired.

Now, we are ready to prove the main theorem.

Proof (of Theorem 7). We say that a node $y \in \{\pm1, 0\}^n$ is "bad" if it incurs a large simulation error, in other words, $\left|(\overline{\mathsf{T}}h)(y^*) - \rho' g(y^*)\right|$ is large. First, we show that there exists a "bad" $y^* \in \{\pm1, 0\}^n$. Let $y^* \in \{\pm1, 0\}^n$ be such that $\left|\bar{J}_{y^*}\right| < k$. It follows from Claim 5 and Claim 6 that $(\overline{\mathsf{T}}h)(y^*) = \widehat{h}_{J_{y^*}|z_{y^*}}(\emptyset) = 0$. Now, since the $g(y^*) \in \{\pm1\}$, we have $\left|(\overline{\mathsf{T}}h)(y^*) - \rho' g(y^*)\right| = \rho'$. Next, we construct a large set $\mathcal{S}(y^*)$ such that every $y \in \mathcal{S}(y^*)$ is bad. Let I denote the set of the D coordinates that (might) have influence on the output of h. Since h is a D-junta function, every coordinate in $\bar{I} = [n] \setminus I$ does not have any influence on the output of the function. We construct a set of bad nodes as follow.

$$\mathcal{S}(y^*) := \{y \in \{\pm1, 0\}^n \colon y_I = y^*_I\}$$

Here, y_I denotes the concatenation of all y_i where $i \in I$. It follows from the junta property of h that $(\overline{\mathsf{T}}h)(y) = (\overline{\mathsf{T}}h)(y^*) = (\overline{\mathsf{T}}_I h)(y_I)$ for every $y \in \mathcal{S}(y^*)$, where $\overline{\mathsf{T}}_I$ denotes the adjoint Markov operator associated with $\mathsf{BES}(\varepsilon)^{\otimes|I|}$. So it holds that $\left|(\overline{\mathsf{T}}h)(y) - \rho' g(y)\right| = \rho'$ for every $y \in \mathcal{S}(y^*)$. Note that $|\mathcal{S}(y^*)| = 3^{n-D}$. Thus, we have

$$\begin{aligned}
\left\|\overline{\mathsf{T}}h - \rho' g\right\|_1 &= \mathop{\mathbb{E}}_y \left|(\overline{\mathsf{T}}h)(y) - \rho' g(y)\right| && \text{(by definition)}\\
&\geqslant \sum_{y \in \mathcal{S}(y^*)} \Pr[Y = y] \cdot \left|(\overline{\mathsf{T}}h)(y) - \rho' g(y)\right| \\
&= \sum_{y \in \mathcal{S}(y^*)} \Pr[Y = y] \cdot \rho' && \text{(identity transformation)}\\
&= \rho' \cdot \Pr[Y_I = y^*_I] && \text{(identity transformation)}\\
&= \rho' \cdot \left(\frac{1-\varepsilon}{2}\right)^{D-t} \cdot \varepsilon^t && (t \text{ is the number of zeros in } y^*_I)\\
&\geqslant \rho' \cdot \min\left(\left(\frac{1-\varepsilon}{2}\right)^D, \varepsilon^D\right).
\end{aligned}$$

5 Technical Overview: BES from BES Samples

First, we outline the proof of Theorem 3 below, then Theorem 4.

Feasibility Outline. Consider a randomized SNIS $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$, where $\varepsilon, \varepsilon' \in (0, 1)$. Using Proposition 1, we can, without loss of generality, assume that f and g are deterministic functions. Therefore, we have $f \colon \{\pm1\}^n \to \{\pm1\}$ and $g \colon \{\pm1, 0\}^n \to \{\pm1, 0\}$. Define $\rho = (1 - \varepsilon)$ and $\rho' = (1 - \varepsilon')$.

Step 1: Algebraization of security. We show that simulation-based SNIS definition is qualitatively equivalent to the algebraized definition of SNIS.

Claim 7 (BES-BES Algebraization of Security) *For any $\varepsilon, \varepsilon' \in (0, 1)$, the following statements hold.*

1. *If* $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$*, then* $\mathbb{E}[f] \leqslant \nu$*,* $\mathbb{E}[g] \leqslant \nu$*,* $\left\|\overline{\mathsf{T}}f - g\right\|_1 \leqslant 4\nu$*, and* $\left\|\mathsf{T}g - \rho' f\right\|_1 \leqslant 4\nu$*.*
2. *If* $\mathbb{E}[f] \leqslant \nu$*,* $\mathbb{E}[g] \leqslant \nu$*,* $\left\|\overline{\mathsf{T}}f - g\right\|_1 \leqslant \nu$*, and* $\left\|\mathsf{T}g - \rho' f\right\|_1 \leqslant \nu$*, then* $\mathsf{BES}(\varepsilon') \sqsubseteq^{2\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$*.*

Step 2: Approximate eigenvector problem. Focusing on the reduction function and the guarantees (a) $\left\|\overline{\mathsf{T}}f - g\right\|_1 \leqslant 4\nu$, and (b) $\left\|\mathsf{T}g - \rho' f\right\|_1 \leqslant 4\nu$, we obtain the following result.

Claim 8 ("Noisy Close-to-Scaling" Constraint) *If* $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$*, then it holds that* $\left\|\mathsf{T}\overline{\mathsf{T}}f - \rho' f\right\|_1 = \left\|\mathsf{T}_\rho f - \rho' f\right\|_1 \leqslant 8\nu$*.*

Step 3: Homogeneous property. There are two cases to consider. If $\rho' \not\in \{\rho, \rho^2, \dots\}$, then the reduction is constant insecure (and the proof is done). However, if $\rho' = \rho^k$, for some $k \in \mathbb{N}$, then the reduction function must be close to a k-homogeneous D-junta Boolean function f^* (using Claim 3). We remark that if security is perfect then f is identical to f^*. Intuitively, the set of all possible junta functions has constant size and f can be *error-corrected* to the unique closest f^*.

Step 4: Only linear functions. Now it remains to prove that f^* is linear.

Theorem 10 (Must be Linear). *Let* $\overline{\mathsf{T}}$ *be the adjoint Markov operator associated with the joint distribution* $\mathsf{BES}(\varepsilon)^{\otimes n}$*. Suppose* $h\colon \{\pm 1\}^n \to \{\pm 1\}$ *is a Boolean* k*-homogeneous* D*-junta function, and* $g\colon \{\pm 1, 0\}^n \to \{\pm 1, 0\}$ *be any arbitrary function. There is a constant* $c = c(\varepsilon, D, k)$ *such that if* $\left\|\overline{\mathsf{T}}h - g\right\|_1 \leqslant c$*, then* h *must be a linear function.*

Section 5.1 proves this theorem. The proof proceeds by considering an appropriate martingale of the Fourier-coefficients of the restrictions of the reduction function.

It is instructive to compare this theorem with Theorem 7, where we proved that any reduction is constant-insecure. In the theorem here, our objective is to characterize h such that $\left\|\overline{\mathsf{T}}h - g\right\|_1$ is small. In Theorem 7, the constraint was $\left\|\overline{\mathsf{T}}h - \rho' g\right\|_1$ instead, where $\rho' \in (0,1)$. This additional ρ' factor made every reduction function constant-insecure.

Once we conclude that f is close to a k-linear f^*, we can argue that g is also close to g^* such that f^*, g^* witness a perfect SNIS of $\mathsf{BES}(\varepsilon')$ from $\mathsf{BES}(\varepsilon)$ samples. The following claim formalizes this reasoning.

Claim 9 *Suppose* $\mathsf{BES}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$*, where* $(1-\varepsilon') = (1-\varepsilon)^k$ *for some* $k \in \mathbb{N}$*. Suppose also that* $h\colon \{\pm 1\}^n \to \{\pm 1\}$ *is a* k*-linear character* χ_S *for some* $S \subseteq [n]$ *and* $\|f - h\|_1 \leqslant \delta$*. Let* $\ell\colon \{\pm 1, 0\}^n \to \{\pm 1, 0\}^n$ *be defined as* $\ell(y) = \prod_{i \in S} y_i$*. Then, it holds that* $\mathsf{BES}(\varepsilon') \sqsubseteq^{0}_{h,\ell} \mathsf{BES}(\varepsilon)^{\otimes n}$ *and* $\|g - \ell\|_1 \leqslant 4\nu + \delta$*.*

Finally, we emphasize that if $\nu = 0$, then f and g are identical to f^* and g^*.

Outline: Rate of Statistical SNIS. The discussion below is the outline for the proof of Theorem 4. Fix erasure probabilities $\varepsilon, \varepsilon' \in (0,1)$. Consider a randomized SNIS $\mathsf{BES}(\varepsilon')^{\otimes m} \sqsubseteq^{\nu}_{\vec{f},\vec{g}} \mathsf{BES}(\varepsilon)^{\otimes n}$. We require a sample-preserving derandomization (for statistical SNIS) to prove the rate result. However, we cannot directly derandomize this SNIS using Theorem 1 (refer to the discussion following Theorem 1). Consequently, we have to follow a different strategy.

Let $f^{(i)}, g^{(i)}$ represent the i-th component of the reductions $\vec{f}, \vec{g}$, where $i \in \{1, \dots, m\}$. Let $f^{(i)} \| f^{(j)}$, for $1 \leqslant i < j \leqslant m$, represent the pair of components $f^{(i)}$ and $f^{(j)}$. Similarly, define $g^{(i)} \| g^{(j)}$. Observe that $\mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{\nu}_{f^{(i)} \| f^{(j)}, g^{(i)} \| g^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}$ (by projecting on the i-th and j-th output samples). We can derandomize this construction using Theorem 1 (our sample-preserving derandomization for statistical SNIS). So, we get deterministic reduction function $\widetilde{f}^{(i)} \| \widetilde{f}^{(j)}$ that is close to $f^{(i)} \| f^{(j)}$ and deterministic $\widetilde{g}^{(i)} \| \widetilde{g}^{(j)}$ that is close to $g^{(i)} \| g^{(j)}$ such that $\mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{\nu'}_{\widetilde{f}^{(i)} \| \widetilde{f}^{(j)}, \widetilde{g}^{(i)} \| \widetilde{g}^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}$, where $\nu' = \Theta\big(\nu^{1/4}\big)$.

We show that there are deterministic functions ${f^*}^{(i)}$ and ${f^*}^{(j)}$ such that ${f^*}^{(i)}$ is close to $\widetilde{f}^{(i)}$ (which is in turn close to $f^{(i)}$) and ${f^*}^{(j)}$ is close to $\widetilde{f}^{(j)}$ (which is in turn close to $f^{(j)}$). Furthermore, there are reduction functions ${g^*}^{(i)}$ and ${g^*}^{(j)}$ such that $\mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{0}_{{f^*}^{(i)} \| {f^*}^{(j)}, {g^*}^{(i)} \| {g^*}^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}$. We emphasize that ${f^*}^{(i)}$ is independent of the choice of $j \in \{1, \dots, m\}$.

At this point, we can conclude that ${f^*}^{(i)}$ and ${f^*}^{(j)}$ are both k-linear (because reductions for perfect BES-from-BES SNIS are linear). We can use a linear construction to obtain one sample of $\mathsf{BES}(\varepsilon'')$ from $\mathsf{BES}(\varepsilon')^{\otimes 2}$ with perfect security, where $(1-\varepsilon'') = (1-\varepsilon')^2$. We compose these two constructions to obtain a perfectly secure SNIS of $\mathsf{BES}(\varepsilon'')$ from $\mathsf{BES}(\varepsilon)^n$, where $(1-\varepsilon'') = (1-\varepsilon')^2 = (1-\varepsilon)^{2k}$. So, the reduction of the composed SNIS must be $2k$-linear; i.e., ${f^*}^{(i)} \cdot {f^*}^{(j)}$ is $2k$-linear. We conclude that ${f^*}^{(i)}$ and ${f^*}^{(j)}$ are k-linear such that they do not share any input variables.

So, we have ${f^*}^{(1)}, \dots, {f^*}^{(m)} \colon \{\pm 1\}^n \to \{\pm 1\}$ such that each function is k-linear with pairwise disjoint inputs. Therefore, $mk \leqslant n$. This entire reasoning describes the proof of Claim 10.

Claim 10 *Let $\varepsilon, \varepsilon' \in (0,1)$ be erasure probabilities satisfying $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$. There is a constant $c = c(\varepsilon, \varepsilon')$ such that the following holds. Suppose $\mathsf{BES}(\varepsilon')^{\otimes m} \sqsubseteq^{\nu}_{\vec{f},\vec{g}} \mathsf{BES}(\varepsilon)^{\otimes n}$ for some $\nu \leqslant c$. For each pair $1 \leqslant i < j \leqslant m$, let $\widetilde{f}_{ij}^{(i)} \| \widetilde{f}_{ij}^{(j)}$ and $\widetilde{g}_{ij}^{(i)} \| \widetilde{g}_{ij}^{(j)}$ be the deterministic functions obtained by derandomizing the SNIS of $\mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{\nu}_{f^{(i)} \| f^{(j)}, g^{(i)} \| g^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}$ using Theorem 1. Let ${f_{ij}^*}^{(i)}$ and ${f_{ij}^*}^{(j)}$ be k-linear Boolean functions that are close to $\widetilde{f}_{ij}^{(i)}$ and $\widetilde{f}_{ij}^{(i)}$, respectively. It holds that*

1. *${f_{ij}^*}^{(i)} = {f_{ij'}^*}^{(i)}$ for any distinct triple $i, j, j' \in \{1, 2, \dots, m\}$. For any $j \neq i$, represent ${f^*}^{(i)} := {f_{ij}^*}^{(i)}$.*
2. *There exists a unique $g^* = ({g^*}^{(1)}, {g^*}^{(2)}, \dots, {g^*}^{(m)})$ such that, for any $1 \leqslant i < j \leqslant m$,*

$$\mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{0}_{{f^*}^{(i)} \| {f^*}^{(j)},\ {g^*}^{(i)} \| {g^*}^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}.$$

3. *Furthermore, for distinct $i, j \in \{1, \dots, m\}$, the input support of ${f^*}^{(i)}$ and the support of ${f^*}^{(j)}$ are disjoint. Consequently, $mk \leqslant n$.*

5.1 Proof of Theorem 10

The following claim is crucial to the proof of the theorem.

Claim 11 *Let $h\colon \{\pm 1\}^n \to \{\pm 1\}$ be a k-homogeneous Boolean function such that $\left|\widehat{h}_{J|z}(\emptyset)\right| = 1$ for some $J \subseteq [n]$ satisfying $\left|\bar{J}\right| = k$, and for some $z \in \{\pm 1\}^{\left|\bar{J}\right|}$. Then h is the linear character function $\chi_{\bar{J}}$ or $-\chi_{\bar{J}}$.*

Remark 4. This claim still holds even if we replace the k-homogeneous constraint by $\mathsf{W}^{<k}[h] = 0$.

Intuitively, it says that if there is a size-k restriction of a k-homogeneous Boolean function f such that the restriction function is the constant function 1, then the function f must be a linear function. We provide proof using the Martingale structure of restriction function (implied by equations 1) as follows.

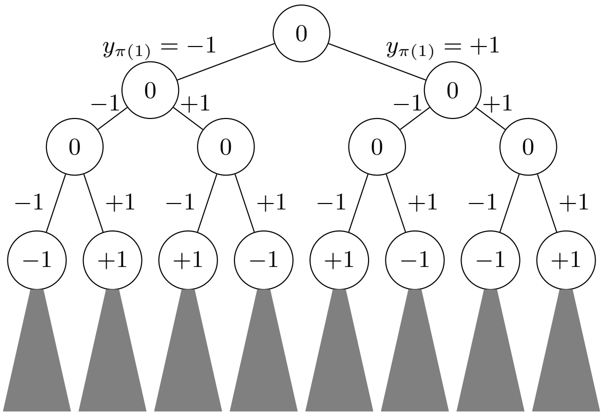

Fig. 3. The representation of a binary tree $\mathcal{T}_\pi$ of depth n with respect to a permutation π, and $k = 3$. Any edge between depth d and depth $d+1$ denotes $y_{\pi(d)} \in \{\pm 1\}$. We assign the value $\alpha_\emptyset = \widehat{h}(\emptyset) = \mathbb{E}[h(X)]$ to the root and the value $\alpha_v = \widehat{h}_{J_v|v}(\emptyset) \in [-1, 1]$ to the node v. The value of any node is the average of the values of its children. The constraint $\mathsf{W}^{<k}[h] = 0$ implies that the value of any node at depth $< k$ is 0. If some node at depth k has a non-zero value then h must be χ_S or $-\chi_S$ where $S = \{\pi(i)\}_{i=1}^k$.

Proof. First, let us introduce some notation. Corresponding to each permutation $\pi\colon [n] \to [n]$, we define a binary tree $\mathcal{T}_\pi$ of depth n (refer to Figure 3) such that each edge between a node and its left child is labeled by -1 and other edges are labeled by 1. This allows us to address each node v at depth $t \in [n]$ with a string

$v = v_1 v_2 \dots v_t$ of length $|v| = t$ which is the string of labels assigned to the edges of the path from root to that node. We assign to a node $v = v_1 v_2 \dots v_t$, the value $\alpha_v := \widehat{h}_{J_v|z}(\emptyset)$ where $z = v$ and $J_v = [n] \setminus \bar{J}_v$ where $\bar{J}_v = \{\pi(1), \pi(2), \dots, \pi(t)\}$.

Martingale Property. According to Claim 5, $\alpha_v = \mathbb{E}[h(X)|Y = y]$ where y is the unique string for which $z_y = v, J_y = J_v$ i.e. $y_{\pi(1)} = v_1, \dots, y_{\pi(t)} = v_t$ and $y_j = 0$ whenever $j \notin \{\pi(1), \dots, \pi(t)\}$ (J_y, z_y are defined in Claim 5). Therefore, $\alpha_v = \frac{\alpha_u + \alpha_w}{2}$ whenever nodes u, w are children of v in the tree $\mathcal{T}_\pi$, i.e. the values α_v (for all v) assigned to the nodes of $\mathcal{T}_\pi$ forms a Martingale.

Since $\mathsf{W}^{<k}[h] = 0$, for each $T \subseteq [n]$ of size $|T| < k$, $\widehat{h}(T) = 0$. Therefore, it follows from (2) that for each $\bar{J}_1$ of size $k-1$, and for any π that $\bar{J}_1 = \{\pi(j)\}_{j=1}^{k-1}$ the following holds

$$\begin{aligned} &\mathop{\mathbb{E}}_{v \in \mathcal{T}_\pi : |v| = k-1}[\alpha_v^2] = \mathop{\mathbb{E}}_{v}[\widehat{h_{J_1|v}}(\emptyset)^2] = \sum_{T \subseteq \bar{J}_1} \widehat{h}(T)^2 = 0 \\ \implies\ &\alpha_v = 0 \quad \forall v \in \mathcal{T}_\pi : |v| \leqslant k-1 \qquad \text{(Due to Martingale property)} \end{aligned}$$

Without of loss of generality, we assume that $\widehat{h}_{J|z}(\emptyset) = 1$. This means that for some π and some node u of length $|u| = k$, we have $\alpha_u = 1$. Let v represent the parent of u in $\mathcal{T}_\pi$, then since $|v| = k-1$, $\alpha_v = 0$, and by applying Martingale property, $\alpha_w = -1$ where w is the sibling of v. Similarly, we can show that the sibling of w in any other tree is 1. By applying this argument iteratively, one can argue that for any permutation π such that $\bar{J} = \{\pi(i)\}_{i=1}^{k}$, any $v \in \mathcal{T}_\pi$ that $|v| = k$, we have $\alpha_v^2 = 1$. Therefore, it follows from (2) that:

$$1 = \mathop{\mathbb{E}}_{v \in \mathcal{T}_\pi : |v| = k}[\alpha_v^2] = \mathop{\mathbb{E}}_{v}[\widehat{h_{J|v}}(\emptyset)^2] = \sum_{T \subseteq \bar{J}} \widehat{h}(T)^2 = \widehat{h}(\bar{J})^2 + \sum_{\substack{T \subseteq \bar{J} \\ |T| < k}} \widehat{h}(T)^2 = \widehat{h}(\bar{J})^2$$

which implies that $\widehat{h}(\bar{J}) = \pm 1$. So it must be the case that $h = \chi_{\bar{J}}$ or $h = -\chi_{\bar{J}}$.

Now we are ready to prove the main theorem.

Proof (of Theorem 10). It follows from Claim 5 and Claim 6 that $(\mathsf{T}h)(y) = \widehat{h}_{J_y|z_y}(\emptyset) = 0$ for any $y \in \{\pm 1, 0\}^n$ such that $\left|\bar{J}_y\right| < k$. Let y^* be the filtration corresponding to the largest Fourier coefficient in level k, i.e., $y^* = \operatorname*{argmax}_{y\colon \left|\bar{J}_y\right| = k} \left|\widehat{h}_{J_y|z_y}(\emptyset)\right|$. First, observe that $\widehat{h}_{J_{y^*}|z_{y^*}}(\emptyset)$ must be non-zero because otherwise h is the constant function 0.

Next, we claim that $\left|\widehat{h}_{J_{y^*}|z_{y^*}}(\emptyset)\right| = 1$ if c is sufficiently small, which is chosen later. For the sake of contradiction, suppose it is not. We will show that

$$\left|(\mathsf{T}h)(y^*) - g(y^*)\right| = \left|\widehat{h}_{J_{y^*}|z_{y^*}}(\emptyset) - g(y^*)\right| \geqslant 1/2^{k-1}. \tag{3}$$

Observe that the Boolean function $h_{J_y|z_y}$ has degree at most k since it is a restriction of a degree-k Boolean function. According to Lemma 1, $\widehat{h}_{J_{y^*}|z_{y^*}}(\emptyset)$

is an integer multiple of $1/2^{k-1}$. Since it is not equal to 0 or ± 1, it holds that $1/2^{k-1} \leqslant \left|\widehat{h}_{J_{y^*}|z_{y^*}}(\emptyset)\right| \leqslant 1 - 1/2^{k-1}$. Note that $g(y^*) \in \{\pm 1, 0\}$. Therefore, the inequality (3) must hold. Using the same idea as in the proof of Theorem 7 yields

$$\left\|\mathsf{T}h - g\right\|_1 \geqslant \frac{1}{2^{k-1}} \cdot \min\left(\left(\frac{1-\varepsilon}{2}\right)^D, \varepsilon^D\right).$$

Now, choose $c < \frac{1}{2^{k-1}} \cdot \min\left(\left(\frac{1-\varepsilon}{2}\right)^D, \varepsilon^D\right)$, then we have reach a contradiction. Thus, it must be the case that $\left|\widehat{h}_{J_{y^*}|z_{y^*}}(\emptyset)\right| = 1$. Applying Claim 11 for the k-homogeneous Boolean function h implies that h is a linear function.

5.2 Proof of the Rate Result

This section provides a proof of Theorem 4. It suffices to prove Claim 10. The following results are needed for the proof.

Claim 12 *Let $f^{(1)}, f^{(2)}, h^{(1)}, h^{(2)} \colon \{\pm 1\}^n \to \{\pm 1\}$ be Boolean functions such that $\left\|f^{(1)} - h^{(1)}\right\|_1 \leqslant \delta_1$ and $\left\|f^{(2)} - h^{(2)}\right\|_1 \leqslant \delta_2$. Then, it holds that*

$$\left\|f^{(1)} \cdot f^{(2)} - h^{(1)} \cdot h^{(2)}\right\|_1 \leqslant \delta_1 + \delta_2.$$

Proposition 5. $\mathsf{BES}(\varepsilon') \sqsubseteq^0_{f,g} \mathsf{BES}(\varepsilon)^{\otimes n}$ *if and only if (1) $(1-\varepsilon') = (1-\varepsilon)^k$, for some $k \in \mathbb{N}$, (2) f is a linear Boolean function $\sigma \cdot \chi_S$ for some size-k subset S of $[n]$, and (3) $g(y) = \sigma \cdot \prod_{i \in S} y_i$, where $\sigma \in \{\pm 1\}$.*

Proof (of Claim 10). The notation $f \approx \widetilde{f}$ means that f and $\widetilde{f}$ are close in which the closeness is always $\mathsf{poly}(\nu)$. The notation $\mathsf{poly}(\nu)$ is always means that the constant in the polynomial is zero and all other coefficients depend only on $\varepsilon, \varepsilon'$. Let $1 \leqslant i < j \leqslant m$. Recall that $\widetilde{f}^{(i)}_{ij} \| \widetilde{f}^{(j)}_{ij}$ and $\widetilde{g}^{(i)}_{ij} \| \widetilde{g}^{(j)}_{ij}$ is the deterministic functions obtained by derandomizing the SNIS $\mathsf{BES}(\varepsilon')^{\otimes 2} \sqsubseteq^{\nu}_{f^{(i)} \| f^{(j)}, g^{(i)} \| g^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}$. By Theorem 1, $\widetilde{f}^{(i)}_{ij}$ is close to $f^{(j)}$ and $\widetilde{f}^{(j)}_{ij}$ is close to $f^{(j)}$. By the feasibility result, $\widetilde{f}^{(i)}_{ij}$ is close to some k-linear function ${f^*_{ij}}^{(i)}$. The relation between these function can be summarized as ${f^*_{ij}}^{(i)} \approx \widetilde{f}^{(i)}_{ij} \approx f^{(i)}$.

Next, for any $j' \neq j$, a similar argument also yields ${f^*_{ij'}}^{(i)} \approx \widetilde{f}^{(i)}_{ij'} \approx f^{(i)}$. By a simple application of triangle inequalities, it holds that ${f^*_{ij}}^{(i)} \approx {f^*_{ij'}}^{(i)}$. Now, using the fact that both ${f^*_{ij}}^{(i)}$ and ${f^*_{ij'}}^{(i)}$ are k-linear functions, we can conclude that they must be the same when ν is chosen sufficiently small because if they are different they are constant far apart (the constant is at least 1). Therefore, it holds that ${f^*_{ij}}^{(i)} = {f^*_{ij'}}^{(i)}$ for every distinct triple $i, j, j' \in [m]$. According to Proposition 5, there is a unique ${g^*_{ij}}^{(i)}$ such that $\mathsf{BES}(\varepsilon') \sqsubseteq^0_{{f^*_{ij}}^{(i)}, {g^*_{ij}}^{(i)}} \mathsf{BES}(\varepsilon)^{\otimes n}$. By Claim 9, ${g^*_{ij}}^{(i)}$ is close to $\widetilde{g}^{(i)}_{ij}$, which is also close to $g^{(i)}$. With a similar argument, one conclude that ${g^*_{ij}}^{(i)} = {g^*_{ij'}}^{(i)}$ for every distinct triple $i, j, j' \in [m]$.

Represent ${f^*}^{(i)} := {f^*_{ij}}^{(i)}$ and ${g^*}^{(i)} := {g^*_{ij}}^{(i)}$ for any $j \neq i$. By sequential composition, we have $\mathsf{BES}(\varepsilon'') \sqsubseteq^{\nu}_{\widetilde{f}^{(i)}_{ij}\cdot\widetilde{f}^{(j)}_{ij},\ \widetilde{g}^{(i)}_{ij}\cdot\widetilde{g}^{(i)}_{ij}} \mathsf{BES}(\varepsilon)^{\otimes n}$ where $(1-\varepsilon'') = (1-\varepsilon')^2 = (1-\varepsilon)^{2k}$. Note that ${f^*}^{(i)} \approx \widetilde{f}^{(i)}_{ij}$ and ${f^*}^{(j)} \approx \widetilde{f}^{(j)}_{ij}$. Therefore, it follows from Claim 12 that ${f^*}^{(i)} \cdot {f^*}^{(j)} \approx \widetilde{f}^{(i)}_{ij} \cdot \widetilde{f}^{(j)}_{ij}$. Similarly, ${g^*}^{(i)} \cdot {g^*}^{(j)} \approx \widetilde{g}^{(i)}_{ij} \cdot \widetilde{g}^{(j)}_{ij}$. By triangle inequality, we have $\mathsf{BES}(\varepsilon'') \sqsubseteq^{\mathsf{poly}(\nu)}_{{f^*}^{(i)}\cdot{f^*}^{(j)},\ {g^*}^{(i)}\cdot{g^*}^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}$. This implies that ${f^*}^{(i)} \cdot {f^*}^{(j)}$ is $\mathsf{poly}(\lambda)(\nu)$-close to a $2k$-homogeneous function. Next, we argue that, in fact, $\mathsf{BES}(\varepsilon'') \sqsubseteq^{0}_{{f^*}^{(i)}\cdot{f^*}^{(j)},\ {g^*}^{(i)}\cdot{g^*}^{(j)}} \mathsf{BES}(\varepsilon)^{\otimes n}$, and the input supports of ${f^*}^{(i)}$ and ${f^*}^{(j)}$ are disjoint. For the sake of contradiction suppose that the input supports of ${f^*}^{(i)}$ intersects the input supports of ${f^*}^{(j)}$. Then ${f^*}^{(i)} \cdot {f^*}^{(j)}$ is a $<2k$-linear function that is a contradiction with the requirement that it is close to a $2k$-homogeneous function. Therefore, it must hold that the input supports of ${f^*}^{(i)}$ and ${f^*}^{(j)}$ are disjoint for every distinct i, j. Note that the domain of ${f^*}^{(i)}$ is still $\{\pm 1\}^n$ for every $i \in [m]$. Consequently, we have $mk \leqslant n$.

6 Technical Overview: BSS from BSS Samples

We outline the proof of Theorem 5 and Theorem 6 below.

Feasibility Outline. Consider a randomized SNIS $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$, where $\varepsilon, \varepsilon' \in (0,1)$. Using Proposition 1, we can, without loss of generality, assume that f and g are deterministic functions. Therefore, we have $f \colon \{\pm 1\}^n \to \{\pm 1\}$ and $g \colon \{\pm 1\}^n \to \{\pm 1\}$. Define $\rho = (1-2\varepsilon)$ and $\rho' = (1-2\varepsilon')$.

Step 1: Algebraization of security. We show that simulation-based SNIS definition is qualitatively equivalent to the algebraized definition of SNIS.

Claim 13 (BSS-BSS **Algebraization of Security)** *For any $\varepsilon, \varepsilon' \in (0, 1/2)$, the following statements hold.*

1. *If $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$, then $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\| \mathsf{T}_\rho f - \rho' g \right\|_1 \leqslant 4\nu$, and $\left\| \mathsf{T}_\rho g - \rho' f \right\|_1 \leqslant 4\nu$.*
2. *If $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\| \mathsf{T}_\rho f - \rho' g \right\|_1 \leqslant \nu$, and $\left\| \mathsf{T}_\rho g - \rho' f \right\|_1 \leqslant \nu$, then $\mathsf{BSS}(\varepsilon') \sqsubseteq^{2\nu}_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$.*

We remark that the Markov and the adjoint Markov operators associated with $\mathsf{BSS}(\varepsilon)^{\otimes n}$ are both identical to the noise operator T_ρ.

Step 2: Approximate eigenvector problem. Focusing on the reduction function and the guarantees (a) $\left\| \overline{\mathsf{T}} f - g \right\|_1 \leqslant 4\nu$, and (b) $\left\| \mathsf{T} g - \rho' f \right\|_1 \leqslant 4\nu$, we obtain the following result.

Claim 14 ("Noisy Close-to-Scaling" Constraint) *If $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$, then it holds that $\left\| \mathsf{T}_\rho \mathsf{T}_\rho f - {\rho'}^2 f \right\|_1 = \left\| \mathsf{T}_{\rho^2} f - {\rho'}^2 f \right\|_1 \leqslant 8\nu$.*

Step 3: Homogeneous property. There are two cases to consider. If $\rho' \notin \{\rho, \rho^2, \dots\}$, then the reduction is constant insecure. However, if $\rho' = \rho^k$, then the reduction function must be close to a k-homogeneous D-junta Boolean function f^* (using Claim 3). Observe that when $\nu = 0$, then $f = g$ is a k-homogeneous function. In fact, any k-homogeneous Boolean function $f = g$ satisfies the algebraic security definition of SNIS perfectly when $\rho' = \rho^k$. Section 2.6 shows that such functions are related to special types of distance-invariant codes. Once we conclude that f is close to a k-homogeneous f^*, we can argue that g is also close to $g^* := f^*$ and that f^*, g^* witness a perfect SNIS of $\mathsf{BSS}(\varepsilon')$ from $\mathsf{BSS}(\varepsilon)$ samples. The following claim formalizes the argument.

Claim 15 *Suppose* $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\nu}_{f,g} \mathsf{BSS}(\varepsilon)^{\otimes n}$, *where* $(1-2\varepsilon') = (1-2\varepsilon)^k$ *for some* $k \in \mathbb{N}$, *and* $h\colon \{\pm1\}^n \to \{\pm1\}$ *is a k-homogeneous Boolean function satisfying* $\|f - h\|_1 \leqslant \delta$. *Then, it holds that* $\mathsf{BSS}(\varepsilon') \sqsubseteq^{0}_{h,h} \mathsf{BSS}(\varepsilon)^{\otimes n}$ *and* $\|g - h\|_1 \leqslant 4\nu + \delta$.

Rate Outline. For reduction among BSS samples, we only prove a rate result for *perfect* SNIS. Consider a randomized SNIS $\mathsf{BSS}(\varepsilon')^{\otimes m} \sqsubseteq^{0}_{\vec{f},\vec{g}} \mathsf{BSS}(\varepsilon)^{\otimes n}$, where $(1 - 2\varepsilon') = (1 - 2\varepsilon)^k$ and $k \in \mathbb{N}$. By Proposition 2 (the sample-preserving derandomization for perfect SNIS), we can assume, without loss of generality, that $\vec{f}, \vec{g}$ are deterministic. For $(1 - 2\varepsilon'') = (1 - 2\varepsilon')^m$, there is a (deterministic) linear construction realizing $\mathsf{BSS}(\varepsilon'') \sqsubseteq^{0}_{f',g'} \mathsf{BSS}(\varepsilon')^{\otimes m}$. By the sequential composition of these two SNIS, we get a new SNIS $\mathsf{BSS}(\varepsilon'') \sqsubseteq^{0} \mathsf{BSS}(\varepsilon)^{\otimes n}$, where $(1 - 2\varepsilon'') = (1 - 2\varepsilon')^m = (1 - 2\varepsilon)^{mk}$. The reduction functions of this new SNIS must be mk-homogeneous; consequently, $mk \leqslant n$.

References

1. Pratyush Agarwal, Varun Narayanan, Shreya Pathak, Manoj Prabhakaran, Vinod Prabhakaran, and Mohammad Ali Rehan. Secure non-interactive reduction and spectral analysis of correlations. *To appear at EUROCRYPT 2022*, 2022. 3
2. 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. 2, 5
3. 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. 8
4. Donald Beaver. Efficient multiparty protocols using circuit randomization. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 420–432. Springer, Heidelberg, August 1992. 2
5. 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. 8
6. 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. 3

7. 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. 3
8. 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. 2
9. Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *IEEE Trans. Inf. Theory*, 57(10):6351–6355, 2011. 2, 6
10. Christer Borell. Positivity improving operators and hypercontractivity. *Mathematische Zeitschrift*, 180(3):225–234, 1982. 8
11. 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. 2
12. Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators from ring-LPN. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 387–416. Springer, Heidelberg, August 2020. 2
13. 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. 2, 6
14. 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. 5
15. 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. 5
16. 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. 5
17. 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. 2
18. 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. 2, 5, 8
19. Irit Dinur, Yuval Filmus, and Prahladh Harsha. Low degree almost boolean functions are sparse juntas. *Electron. Colloquium Comput. Complex.*, page 180, 2017. 15
20. Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008. 6
21. Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973. 2, 5
22. 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. 2, 5, 8, 9, 11

23. 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. 2
24. 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. 2, 5
25. 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. 2, 5
26. 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. 2
27. 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. 2, 5, 9
28. Sudeep Kamath and Venkat Anantharam. On non-interactive simulation of joint distributions. *IEEE Transactions on Information Theory*, 62(6):3419–3435, 2016. 2, 5, 8, 9
29. Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation: Feasibility & rate. Cryptology ePrint Archive, Report 2020/252, 2020. https://ia.cr/2020/252. 3
30. Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd ACM STOC*, pages 316–324. ACM Press, May 2000. 2, 5, 6, 7
31. Guy Kindler. *Property Testing PCP*. PhD thesis, Tel-Aviv University, 2002. 11, 12, 15, 16
32. Guy Kindler and Shmuel Safra. Noise-resistant boolean functions are juntas. *preprint*, 2002. 11, 12, 15, 16
33. 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. 3
34. Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977. 12
35. 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. 2
36. 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. 2
37. Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation functionalities. In Manoj Prabhakaran and Amit Sahai, editors, *Secure Multi-Party Computation*, volume 10 of *Cryptology and Information Security Series*, pages 249–283. IOS Press, 2013. 3
38. 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. 2

39. Elchanan Mossel. Gaussian bounds for noise correlation of functions and tight analysis of long codes. In *49th FOCS*, pages 156–165. IEEE Computer Society Press, October 2008. 14
40. 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. 2, 6, 8
41. 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. 2, 6, 8
42. Elchanan Mossel, Krzysztof Oleszkiewicz, and Arnab Sen. On reverse hypercontractivity. *Geometric and Functional Analysis*, 23(3):1062–1097, 2013. 8
43. 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. 9
44. 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. 3
45. 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. 2
46. Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. 13, 15
47. Michael O. Rabin. How to exchange secrets by oblivious transfer. *Technical Memo TR-81*, 1981. 5
48. Michael O. Rabin. How to exchange secrets with oblivious transfer. Cryptology ePrint Archive, Report 2005/187, 2005. https://eprint.iacr.org/2005/187. 5
49. Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975. 2, 5
50. Aaron Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975. 2, 5
51. 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. 2, 6
52. Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd FOCS*, pages 160–164. IEEE Computer Society Press, November 1982. 2
53. Zi Yin and Youngsuk Park. Hypercontractivity, maximal correlation and non-interactive simulation. 2014. 8