Secure Non-interactive Simulation from Arbitrary Joint Distributions

Hamidreza Amini Khorasgani * Hemanta K. Maji* Hai H. Nguyen*

Abstract

Secure non-interactive simulation (SNIS), introduced in EUROCRYPT 2022, is the information-theoretic analog of *pseudo-correlation generators*. SNIS allows parties, starting with samples of a source correlated private randomness, to non-interactively and securely transform them into samples from a different correlated private randomness. Determining the feasibility, rate, and capacity of SNIS is natural and essential for the efficiency of secure computation.

This work initiates the study of SNIS, where the target distribution (U, V) is a random sample from the *binary symmetric or erasure channels*; however, the source distribution can be arbitrary. In this context, our work presents:

1. The characterization of all sources that facilitate such SNIS,
2. An upper and lower bound on their maximum achievable rate, and
3. Exemplar SNIS instances where non-linear reductions achieve optimal efficiency; however, any linear reduction is insecure.

These results collectively yield the fascinating instances of *computer-assisted search* for secure computation protocols that identify ingenious protocols that are more efficient than all known constructions.

Our work generalizes the algebraization of the simulation-based definition of SNIS as an approximate eigenvector problem. The following foundational and general technical contributions of ours are the underpinnings of the results mentioned above.

1. Characterization of Markov and adjoint Markov operators' effect on the Fourier spectrum of reduction functions.
2. A new concentration phenomenon in the Fourier spectrum of reduction functions.
3. A powerful statistical-to-perfect lemma with broad consequences for feasibility and rate characterization of SNIS.

Our technical analysis relies on Fourier analysis over large alphabets with arbitrary measure, the orthogonal Efron-Stein decomposition, and junta theorems of Kindler-Safra and Friedgut. Our work establishes a fascinating connection between the rate of SNIS and the maximal correlation, a prominent information-theoretic property. Our technical approach motivates the new problem of "security-preserving dimension reduction" in harmonic analysis, which may be of independent and broader interest.

Keywords. Secure non-interactive simulation, information-theoretic security, pseudo-correlation generator, efficient secure computation, feasibility characterization, rate and capacity estimation, cryptographic complexity.

Technical keywords. Biased Fourier analysis, Fourier analysis over large alphabets with arbitrary measure, orthogonal Efron-Stein decomposition, Markov operator, Junta theorem.

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

1 Introduction

Recently, Khorasgani, Maji, and Nguyen [34] introduced *secure non-interactive simulation* (SNIS) as an information-theoretic analog of *pseudo-correlation generator* [10, 11]. In the two-party setting (refer to Figure 1), Alice and Bob start with n independent samples of *correlated private randomness* (X, Y), the *source distribution*. Non-interactively, Alice and Bob compute $U = f_n(X^n)$ and $V = g_n(Y^n)$, where $f_n(\cdot)$ and $g_n(\cdot)$ are reduction functions,[1] and the joint distribution (U, V) is the *target distribution*. This construction is a SNIS of the target distribution (U, V) from the source distribution (X, Y) if it is *simulation-secure* [13, 12, 14]. Note that SNIS security against semi-honest or malicious adversaries is identical.

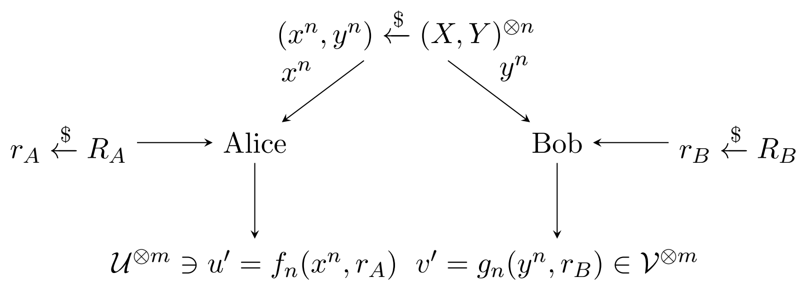

Figure 1: System model for secure non-interactive simulation: SNIS.

Motivating Application for SNIS: Correlation generators [34]. Secure computation [59, 26] protocols often offload most of their computationally and cryptographically expensive components to an offline procedure [41, 8, 17, 47]. This offline procedure has high computation and communication costs, and it generates structured correlated private randomness like Beaver triples [5]. However, several inexpensive sources of correlated private randomness also facilitate secure computation, like, correlated samples from noise sources [35]. Therefore, a natural solution is to *non-interactively* and *securely* convert these inexpensive correlations into ones used in secure computation protocols.

Boyle et al. [10, 11] introduced *pseudorandom correlation generators* to achieve this objective against computationally bounded adversaries. Recently, Khorasgani et al. [34] introduced the information-theoretic analog of this primitive, modeled by the system in Figure 1, to study the *feasibility* and *rate* of SNIS, which has straightforward consequences to the efficiency of secure computation.

Security & rate definition of SNIS [34]. Readers should follow the system in Figure 1 for the discussion below. For feasibility considerations, substitute $m = 1$ in Figure 1. Khorasgani et al. [34] said that a *SNIS of* (U, V) *from* $(X, Y)^{\otimes n}$ *using reduction functions* f_n, g_n *has insecurity* $\nu(n)$ if the following three conditions are satisfied.

1. *Correctness.* The joint distribution of the output samples (u', v') is $\nu(n)$-close to the target distribution (U, V) in statistical (i.e., total variational) distance.

[1]The reduction functions $f_n(\cdot)$ and $g_n(\cdot)$ are randomized and use independent private randomness; however, for brevity, the randomness is being excluded from the formal representation. Strong *sample-preserving* derandomization results (i.e., the derandomized reductions use an identical number of source samples and produce an identical number of target samples) for SNIS [34] indicate the uselessness of independent private randomness.

2. *Security against a corrupt Alice.* Fix any (u, v) in the support of the target 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] In other words, $X^n - U - V$ is an (approximate) Markov chain.

3. *Security against a corrupt Bob.* Likewise, for any (u, v) in the support of the target distribution (U, V), the conditional distribution $(Y^n | U' = u, V' = v)$ is $\nu(n)$-close to being independent of u. In other words, $Y^n - V - U$ is an approximate Markov chain.

[34] presented simulation-based security definition that unifies these three conditions. We represent this definition by the notation: "$(U, V) \sqsubseteq^{\nu(n)}_{f_n, g_n} (X, Y)^{\otimes n}$."

Fix the source (X, Y) and the target (U, V). To discuss (the single-letter characterization of) rate, Khorasgani et al. [34] consider a SNIS *family* of $(U, V)^{\otimes m(n)}$ from $(X, Y)^{\otimes n}$ using reduction function f_n, g_n with insecurity $\nu(n)$, parameterized by $n \in \{1, 2, \ldots\}$. The (production) *rate*, represented by $R(\ (U, V), (X, Y)\ )$, is the supremum of the maximum achievable $m(n)/n$ as $n \to \infty$ and $\nu(n) \to 0$ over all possible families of reductions.

This reduction-based investigation facilitates characterizing the efficiency limits of non-interactive secure computation irrespective of the origin of the source samples. For example, the source samples can originate from noisy physical processes, trusted hardware, or the output of a protocol relying on cryptographic hardness of computation assumptions.

Relation to other primitives and additional motivation. *One-way secure computation* [22, 2] uses one additional round of communication to transform the samples from source distributions into samples from a target distribution. *Non-interactive correlation distillation* [45, 44, 58, 9, 16] restricts SNIS to the target distribution (U, V) being the independent coin distribution. SNIS is the cryptographic extension of *non-interactive simulation of joint distribution* [21, 57, 53, 30, 31, 25, 18, 24] from information theory.

This non-cryptographic simulation problem (either non-interactive or with rate-limited communication) has diverse applications, for example, as discussed in [31], spanning from game-theoretic coordination in a network against an adversary to control a dynamical system over a distributed network. These applications naturally extend to the cryptographic context with adversarial agents, granting additional independent motivation to study SNIS.

Studying the *cryptographic complexity* [7, 40, 38, 6, 46] also motivates the study of SNIS, as done in the independent work of [1].

Our problem statement. This work considers the simulation of two particular target distributions (U, V) (refer to Figure 2).

1. *Noise from the binary symmetric channel.* Alice outputs uniformly random $u \in \{+1, -1\}$ and Bob outputs $v \in \{+1, -1\}$ such that, for each u, the probability of $u \neq v$ is $\varepsilon \in (0, 1/2)$. We represent this correlated private randomness by $\mathsf{BSS}(\rho)$, where $\rho = (1 - 2\varepsilon)$. Therefore, for example, $\mathsf{BSS}(1/2)$ is a distribution where Alice and Bob samples disagree with a probability of $1/4$.

2. *Noise from the binary erasure channel.* Alice outputs uniformly random $u \in \{+1, -1\}$ and Bob outputs $v \in \{u, 0\}$ such that, for each u, the probability of $v = 0$ is $\varepsilon \in (0, 1)$. We represent this correlated private randomness by $\mathsf{BES}(\rho)$, where $\rho = \sqrt{1 - \varepsilon}$. So, $\mathsf{BES}(\sqrt{1/2})$ has erasure probability $1/2$.

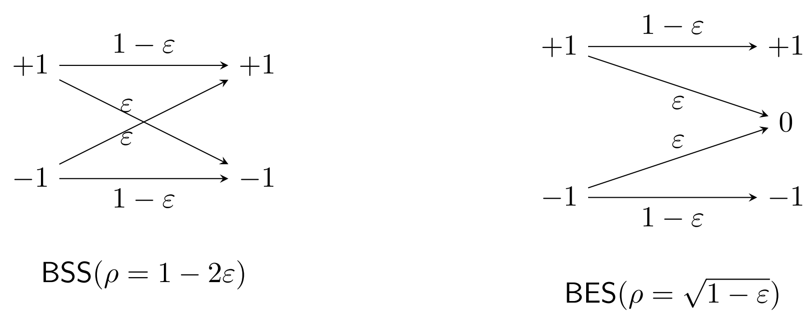

Figure 2: Random correlated noise generated by the binary symmetric channel (BSS) and the binary erasure channel (BES) with maximal correlation ρ.

This work parameterizes the channels by their *maximal correlation* ρ for brevity in our technical presentation (see Section 4.2 for formal definition). [34] proved that a SNIS of $\mathsf{BSS}(\rho')$ from $\mathsf{BSS}(\rho)$ exists if and only if $\rho' = \rho^k$, for some $k \in \{1, 2, \dots\}$. Furthermore, if this SNIS is feasible, it has a rate of $1/k$: each party outputs the product of k samples of their source – a linear reduction. Similarly, a SNIS of $\mathsf{BES}(\rho')$ from $\mathsf{BES}(\rho)$ exists if and only if $\rho' = \rho^k$, for some $k \in \{1, 2, \dots\}$. This SNIS also has a rate of $1/k$, and linear reductions are rate-achieving.

Our work considers the problem of determining the *feasibility* and *rate* of SNIS generating BSS/BES *target noise* from *arbitrary source distributions* and identifying corresponding *maximum rate-achieving* secure constructions. The source distribution (X, Y) can be arbitrary; they may have arbitrary-size sample spaces, and their marginal distributions need not be uniform or identical. Even the *decidability of the feasibility characterization is unknown*, let alone tackling the optimization and search versions to determine the rate and maximum rate-achieving constructions. For example, the non-cryptographic version of SNIS is also deceptively simple to formalize and is a foundational problem in information theory introduced in the early 1970s [21, 57, 53], which has been incredibly challenging to address. The recent breakthrough [25] in that research crucially hinged on developing analysis techniques for the particular case of BSS target.

Our work, along with [34], demonstrates that investigating the SNIS of the BSS/BES target is analytically tractable via the harmonic analysis toolkit. Beyond the feasibility characterization, we prove *non-trivial rate upper bounds* and discover optimal *non-linear SNIS* constructions using *computer-assisted exhaustive search*, which are more efficient than previously known constructions. Computer-assisted search has the potential of increasing the efficiency of secure computation by introducing unforeseen and unimaginable constructions. We conjecture that the technical innovations developed in these investigations shall be crucial to studying the SNIS of more sophisticated target correlations like the Beaver triple, which currently appears insurmountable.

Summary of our results. We present an exhaustive characterization of all source distributions that yield secure SNIS of BSS and BES target distributions. Furthermore, if the insecurity of a SNIS is sufficiently small, then one can slightly edit the reduction functions to convert them into perfectly secure SNIS. Next, we present (positive constant) lower and upper bounds on the production rate of such SNIS. Finally, we exhibit SNIS instances where non-linear reduction functions achieve optimal rate (also demonstrating the tightness of our rate estimates); however, every linear reduction is constant insecure. We efficiently searched the space of all reductions (guided by our technical

[2]The conditional distribution $(A|B = b)$ is ν-close to being independent of b if there is a distribution A^* such that the statistical distance between A^* and the conditional distribution $(A|B = b)$ is at most ν for any $b \in \mathrm{Supp}(B)$.

results) to identify these fascinating non-linear reductions – even the authors were unaware of their existence.

These cryptographic consequences rely on several foundational and technical contributions of ours, which may be of independent and broader interest. We generalize the [34]'s framework for algebraizing SNIS from arbitrary source distributions using the source's Markov and the adjoint Markov operators (refer to Section 4.4 and Section B for definition and illustrative examples). This algebraization translates SNIS into an *approximate eigenvector formulation* for appropriate linear operators, where the reduction functions are their eigenvectors. Next, we *quantify the impact* of these linear operators on the Fourier spectrum of the reduction functions. Our proof relies on a critical synergy between the linear operators and the reduction functions over the *orthogonal Efron-Stein basis*. Our work shows that this quantification entails a *concentration of the Fourier spectrum* of the reductions on low-degree terms. Fascinatingly, our bound on the degree depends on the *maximal correlations* of the source and the target distributions. Finally, we apply appropriate *junta theorems* (i.e., dimension reduction) to prove the closeness of SNIS reductions to juntas (a.k.a., *canonical reductions*).

Consequently, one obtains a potent technical tool: *the statistical to perfect lemma*. This lemma, for instance, implies the following highly non-trivial phenomena for any source and target pair.

1. One can error-correct any statistically-secure SNIS into a perfect SNIS.

2. The total number of canonical SNIS candidates is constant.

3. The rate of any feasible SNIS is a positive constant.

Such phenomena are rare in cryptography (cf. [28], and [34]).

The presentation above is only a high-level overview of our proof strategy, highlighting its primary landmarks. There are several subtleties to address and technical challenges to overcome, which we further elaborate in Section 2.2.

Computer-assisted search for optimal secure computation protocols. Although computer-assisted constructions are common while constructing error-correcting codes and combinatorial designs [39], their role in secure protocols is novel. Our work presents fascinating instances of computer-assisted search for finding *optimal* secure computation protocols that are *more efficient than known protocols*. [34] discovered new alternative constructions that achieve already-known efficiency parameters. [15] also used computer assistance to recover known garbling constructions. Typically idealized information-theoretic models yield hardness of computation results; however, the SNIS model also yields non-trivial positive results, i.e., optimal constructions that are more efficient than any known protocols. This research outcome indicates that one should be open to the possibility of relying on computer-assisted search to design new and more efficient secure computation protocols.

Subsequent independent work. Preliminary versions of our works publicly appeared in 2020 [32] and 2021 [33]. Subsequently (an independently), motivated by studying *cryptographic complexity* [7, 40, 38, 6, 46], Agarwal, Narayanan, Pathak, Prabhakaran, Prabhakaran, and Rehan [1] introduced SNIS as *secure non-interactive reduction* in EUROCRYPT–2022. They rely on spectral techniques to formalize and analyze this primitive. Lacking explicit dimension reduction tools for their basis (like the junta theorems in our Fourier basis), their technical approach seems to require a new dimension reduction theorem to investigate the rate of SNIS.

Overview of the paper. Section 2 presents an informal overview of our results and technical approach. Section 3 summarizes related works, and open problems and research directions (in cryptography, theoretical computer science, and harmonic analysis) motivated by our work. Section 4 introduces the preliminaries. Section 5 proves our results pertaining to determining the feasibility of SNIS. Section 6 presents our rate estimation results. Section 7 has results pertaining to 2×2 sources. Section 8 presents the remaining results. Omitted proofs are provided in the appendix.

2 Overview of our Contributions

2.1 Overview of Our Results

This section presents an informal summary of our results and a technical overview of the proof. In the presentation below, without loss of generality, we assume that the SNIS reductions are deterministic (see, for example, the derandomization results of Imported Theorem 7 and Imported Theorem 8 from [34]).

Feasibility characterization of SNIS from arbitrary sources. We present an efficient algorithm to determine whether a statistically secure SNIS of $\mathsf{BSS}/\mathsf{BES}$ from the source (X, Y) is feasible or not (see Corollary 1). Theorem 1 states that if the simulation error of a SNIS of $\mathsf{BSS}/\mathsf{BES}$ from the source (X, Y) is less than c/n, where c a suitable positive constant, one can edit the reduction functions into a perfect secure SNIS. Furthermore, these perfectly-secure reductions are canonical reductions that are *Boolean constant-juntas*. That is, they depend on a constant number of input variables, which entails that the total number of such canonical candidate reductions is only a constant. Therefore, one can exhaustively search for all such canonical reductions to determine if a SNIS of $\mathsf{BSS}/\mathsf{BES}$ from (X, Y) is possible.

This technical result entails the following consequence for *cryptographic contexts*. Efficient secure constructions in cryptography insist on achieving $\mathsf{negl}(\lambda)$ insecurity, where λ is the security parameter, using $n = \mathsf{poly}(\lambda)$ source samples. Therefore, given a source and target, our result proves that either (a) there is a perfectly secure SNIS or (b) every SNIS construction is insecure (because we show that the insecurity is at least inverse-polynomial in the security parameter). In particular, our result rules out the possibility of negligibly-insecure SNIS existing where there is no perfectly secure SNIS.

Estimating rate of SNIS from arbitrary sources. We prove that if a SNIS is feasible, it has a positive constant rate (see Corollary 2). Fix a $\mathsf{BSS}/\mathsf{BES}$ target. To lower-bound the rate of such SNIS by a positive constant, observe that if a SNIS of $\mathsf{BSS}/\mathsf{BES}$ from (X, Y) is feasible, there is a canonical SNIS, which is perfectly secure, and the reduction functions are constant-juntas. One can partition the samples of $(X, Y)^{\otimes n}$ into constant-size blocks, apply the canonical reduction to each block, and obtain one target sample from each block. This construction has a positive constant rate. Such results are rare in cryptography and challenging to prove for secure computation (cf., [29, 28, 34] for examples).

Theorem 5 upper-bounds the rate of SNIS of $\mathsf{BSS}/\mathsf{BES}$ from any target distribution using the *maximal correlation* [27, 53, 3, 52, 4] of the target distribution (refer to Section 4.2 for the definition of maximal correlation) and the eigenvalue of the Markov operator $\mathsf{T}\overline{\mathsf{T}}$ (refer to Section 4.4) of the source distribution. We emphasize that this upper bound is *only for perfectly secure SNIS*. This restriction is unsurprising because, as demonstrated in [34], even estimating the rate of simulating BSS from BSS is known only for perfectly secure SNIS. [34] present evidence that overcoming this hurdle may require advances in harmonic analysis.

Source. Alice gets (a_1, b_1, a_2, b_2) and Bob gets (c_1, d_2, c_2, d_2) such that $a_1, b_1, c_1, a_2, b_2, c_2$ are chosen uniformly and independently at random from the set $\{0, 1\}$ and $d_1 = a_1 \cdot c_1 \oplus b_1$ and $d_2 = a_2 \cdot c_2 \oplus b_2$.

Reductions.

1. Alice outputs $u = +1$, if $b_2 = a_1 \cdot a_2 \oplus b_1$; otherwise, $u = -1$.
2. Bob outputs $v = +1$, if $d_2 = c_1 \cdot c_2 \oplus d_1$; otherwise, $v = -1$.

Source. (In multiplicative notation.) Alice gets (A_1, B_1, A_2, B_2) and Bob gets (C_1, D_2, C_2, D_2) such that $A_1, B_1, C_1, A_2, B_2, C_2$ are chosen uniformly and independently at random from the set $\{+1, -1\}$ and $D_1 = \frac{1}{2} \cdot (1 + A_1 + C_1 - A_1 \cdot C_1) \cdot B_1$ and $D_2 = \frac{1}{2} \cdot (1 + A_2 + C_2 - A_2 \cdot C_2) \cdot B_2$.

Reductions.

1. Alice outputs $U = \frac{1}{2} \cdot (1 + A_1 + A_2 - A_1 \cdot A_2) \cdot B_1 \cdot B_2$.
2. Bob outputs $V = \frac{1}{2} \cdot (1 + C_1 + C_2 - C_1 \cdot C_2) \cdot D_1 \cdot D_2$.

Figure 3: SNIS of $\mathsf{BSS}(1/2)$ from ROLE achieving optimal production rate 1/2. The top half of the figure presents the reduction using ROLE as defined for elements in $\{0, 1\}$. The bottom half presents the equivalent reduction using the multiplicative notation $0 \mapsto +1$ and $1 \mapsto -1$. In the multiplicative representation, the Fourier spectrum of each reduction function is explicit. One can verify that the (1) reduction functions are non-linear and (2) their Fourier weights are not concentrated on terms of identical degree.

Our upper bounds for BSS and BES are tight as demonstrated by (1) the rate of self-simulation of BSS and BES [34], and (2) the reduction of $\mathsf{BSS}(1/2)$ and $\mathsf{BES}(\sqrt{1/2})$ from the ROLE correlation (defined below), whose maximal correlation is $\sqrt{1/2}$.

We clarify that this upper bound also extends to randomized perfectly-secure SNIS because the sample-preserving derandomization of [34] preserves perfect security.

Power of non-linear reductions and computer-assisted search. The *random oblivious linear-function evaluation* [55] (ROLE) source samples uniformly and independently random $a, b, c \in \{0, 1\}$, provides Alice $x = (a, b)$, and provides Bob $y = (c, d)$, where $d = a \cdot c \oplus b$. Section B shows that the maximal correlation of ROLE is $\sqrt{1/2}$. Recall that $\mathsf{BSS}(1/2)$ is a random correlated sample from the binary symmetric channel where parties' samples are different with probability 1/4.

We show that there is an *optimal* rate-1/2 SNIS of $\mathsf{BSS}(1/2)$ from ROLE using non-linear reductions (refer to the protocol in Figure 3 and the discussion in Section 8.3); however, any SNIS of $\mathsf{BSS}(1/2)$ from ROLE using linear reductions is constant-insecure (refer to Lemma 4).[3] The optimality of the rate follows from the upper bound of Theorem 5. In the optimal protocol each party's output indicates whether their source samples form a ROLE correlation or not.

The previous best construction (as far as the authors are aware) uses *three ROLEs* and *one round of communication* to implement a 1-out-of-4 bit-OT. Alice feeds a random permutation of $(u, u, u, 1 - u)$, where $u \xleftarrow{\$} \{0, 1\}$, into the 1-out-of-4 bit-OT. Bob chooses to receive the bit v at a random position $i \in \{1, 2, 3, 4\}$. In comparison, our construction uses one less ROLE sample and no communication, which significantly impacts the efficiency of this secure computation.[4]

Similarly, there is an *optimal* rate-1 SNIS of $\mathsf{BES}(\sqrt{1/2})$ from ROLE using non-linear reductions (refer to Section 8.3 and the protocol in Section E.4); however, any SNIS using linear reductions is constant-insecure (refer to Lemma 4). The optimality of this protocol follows from Theorem 5.

[3] Observe that "linearity" of a reduction may depend on how the samples of the source are "named." We prove our impossibility result is a strong sense. For any renaming of the samples, we show that linear constructions are constant insecure.

[4] We identified *all* reductions realizing this SNIS at an optimal rate. All the reductions were essentially equivalent to each other. However, we chose this particular reduction because it admits an elegant intuitive formulation.

Furthermore, the spectrums of these reduction functions are *not concentrated* on terms with an identical degree.

Additional Result: explicit characterization of SNIS of BSS from 2×2 sources. Let the target distribution be $\mathsf{BSS}(\rho')$ and (X, Y) be an arbitrary source such that the support size of both its marginals is two. We prove in Theorem 6 that if the source $(X, Y) \neq \mathsf{BSS}(\rho)$ or $(X, Y) = \mathsf{BSS}(\rho)$ but $\rho' \neq \rho^k$, for all $k \in \{1, 2, \dots\}$, then any SNIS of $\mathsf{BSS}(\rho')$ from (X, Y) is constant insecure. If $(X, Y) = \mathsf{BSS}(\rho)$, $\rho' = \rho^k$, for some $k \in \{1, 2, \dots\}$, and $\mathsf{BSS}(\rho') \sqsubseteq^{\nu}_{f,g} \mathsf{BSS}(\rho)$ for a sufficiently small ν, then one can slightly edit the reduction function to obtain new reduction functions f^*, g^* that are k-homogeneous[5] and $\mathsf{BSS}(\rho') \sqsubseteq^{0}_{f^*,g^*} \mathsf{BSS}(\rho)$ – a result already proved in [34]. The proof of Theorem 6 (additionally) depends on (1) Theorem 8: a statistical-to-perfect lemma for BSS target from arbitrary 2×2 source, and (2) Theorem 9: the characterization of sources facilitating perfect SNIS of BSS target.

Remark 1. *For 2×2 sources, our definition of "sufficiently small simulation error" is slightly different from the arbitrary source case. In the 2×2 source case, "sufficiently small simulation error" is a (global) constant. For arbitrary sources, "sufficiently small simulation error" is c/n, where c is a global constant. This variation is a consequence of the different junta theorems our analysis uses. Typically in cryptography, the security requires that the simulation error falls faster than any inverse polynomial. Our results even work when considering inverse polynomial simulation error.*

Additional Result: explicit characterization of SNIS of BES from 2×2 sources. We show that any SNIS of BES from a 2×2 source is constant insecure (refer to Theorem 7). This generalizes the impossibility of SNIS of BES from BSS [34].

Additional Result: necessary condition for SNIS feasibility. Theorem 11 presents easy-to-test necessary conditions for the feasibility of SNIS of BSS or BES from (eigenvalues of the) Markov operator of the source distribution. Our "eigenvalue test" (derived independently) is identical to the test introduced in [1].

Additional Result: Incompleteness of string OT. Random samples from the string oblivious transfer functionality, parameterized by $\ell \in \{1, 2, \dots\}$, gives Alice two random ℓ-bit strings $(x_0, x_1) \in \{0,1\}^{2\ell}$ and gives Bob $(b, x_b) \in \{0,1\}^{\ell+1}$, where b is a uniformly random bit (see Definition 8). Lemma 5 states that this family (for $\ell \in \{1, 2, \dots\}$) of random samples from the string oblivious transfer is not complete for SNIS because all of them have maximal correlation $\sqrt{1/2}$. This family cannot yield a SNIS of any target with maximal correlation $> \sqrt{1/2}$, because of Imported Theorem 2, and Imported Theorem 1.

This family is complete for one-way secure computation [22]. [1] show that a single source cannot be complete for SNIS.

2.2 Overview of Our Technical Contributions

This section presents a high-level intuition of our foundational and technical contributions. It is instructive to read this section with SNIS for BSS target as a representative example. SNIS for BES target encounters a technical subtlety, which we resolve towards the end. Although our work's analysis fits [34]'s high-level framework, achieving each of those high-level objectives involves unique and significant technical contributions.

[5] A homogeneous function is a linear combination of terms with an identical degree.

Our starting point. For a source $(X, Y) \in \{\mathsf{BSS}, \mathsf{BES}\}$, Khorasgani et al. [34] algebraically captured the simulation-based security definition of SNIS using the Markov (T) and the adjoint-Markov ($\overline{\mathsf{T}}$) operators associated with (X, Y). If a SNIS has a small simulation error, the reduction functions f and g are approximate eigenvectors of the linear operators $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$, respectively. We generalize this result to an arbitrary source (X, Y) using a similar idea. Furthermore, algebraization of security in [34] is not scalable. We perform a normalization change (relying on maximal-correlation-based notation) to make it scalable. For example, compare Theorem 4 in our paper with Claim 10 in [34].

Characterization of Markov operator's effect on the Fourier spectrum. It is essential to accurately characterize the impact on the Fourier spectrum when applying the $\mathsf{T}\overline{\mathsf{T}}$ linear operator on the reduction f and applying the $\overline{\mathsf{T}}\mathsf{T}$ linear operator on the reduction g. When the source is either BSS or BES as in [34], Fourier analysis over uniform measure suffices; both operators $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$ are the well-behaved noise (Bonami-Beckner) operators. Therefore, the impact of Fourier spectrum is well understood. In contrast, if the source is an arbitrary joint distribution, the marginal distributions of the source need not be uniform or identical to each other and the two operators need not be the Bonami-Beckner operators, complicating this technical challenge even further. If the source is a 2-by-2 distribution, we present an accurate characterization of Markov's operator's effect on the Fourier spectrum (see Lemma 1) using biased Fourier analysis. This result is a generalization to correlated space of the Bonami-Beckner operator's effect on the Fourier spectrum.

When the source is an arbitrary joint distribution, straightforward control of the Markov operator's effect is not evident even when using Fourier analysis over arbitrary product measure. Instead, we take a detour and use the Efron-Stein orthogonal decomposition for this analysis step (see Section 4.5). Our linear operators synergize well with the reduction functions over this decomposition, and one bounds the effect of these operators on the reduction functions using the maximal correlation of the source (X, Y) (see Proposition 5 and Proposition 6). Finally, we return to the Fourier basis and translate the bounds on the Fourier spectrum using Proposition 7.

Fourier concentration. The approximate eigenvector problem (a consequence of the SNIS definition) and the characterization of the Markov and adjoint-Markov operators' impact on the Fourier spectrum yields new Fourier concentration results. For 2×2 sources, we prove that the Fourier spectrum of the solutions of the approximate eigenvector problem (in particular, the reduction functions) are concentrated on terms of a fixed degree (see Theorem 10). [34] proved this concentration result for the particular cases of BSS and BES sources.

For arbitrary sources, we show that the Fourier spectrum is concentrated on low-degree terms (see Theorem 3). This relaxation in concentration is also necessary; i.e., we show perfectly secure reductions constructing $\mathsf{BSS}(1/2)$ and $\mathsf{BES}(\sqrt{1/2})$ from the ROLE source whose spectrums are *not concentrated on only one degree.* This Fourier concentration phenomenon is a manifestation of "security" and distinguishes our problems from those arising in non-interactive simulation (i.e., SNIS without security) [21, 57, 53, 30, 31, 25, 18, 24].

Statistical to perfect lemma. The set of all reductions with Fourier spectrum concentrated on low-degree multi-linear is still potentially huge. [6] Using appropriate junta theorems, Theorem 1 shows that Boolean functions satisfying such Fourier concentration properties are (close to) juntas. Since these juntas depend only on a constant number of inputs, the total number of such candidate

[6] A function whose Fourier spectrum is concentrated on low-degree multi-linear terms may depend on all the variables. So, without using any additional properties of low-degree Boolean functions, one cannot prune down the set of candidate functions. Therefore, their number may be exponential in the number of variables.

juntas is also a constant. Therefore, this result implies that (1) SNIS is either perfectly secure or constant-insecure, (2) The size of the set of all canonical SNIS of (U, V) from (X, Y) is a constant, and (3) Any feasible SNIS has a positive constant rate. Furthermore, these juntas yield perfectly-secure SNIS.

The consequences of this result are immense. For a particular number of source samples n and (sufficiently small constant) insecurity budget $\nu(n)$, our analysis determines whether such a SNIS exists or not. Furthermore, a constant-time algorithm can search for the witness reductions. For example, an *exhaustive search algorithm* discovered all SNIS of $\mathsf{BSS}(1/2)$ from ROLE, uncovering fascinating new reductions.

A technical subtlety. A careful reader would recognize that the junta theorems we mention apply only to Boolean functions. Therefore, the analysis outline above applies to Boolean reduction functions, for example, when the target is BSS.

However, when the target is BES, one encounters a technical hurdle. Although the reduction function f is Boolean, the reduction function g is *not* Boolean – it is three-valued. We assessed that general junta theorems for functions with a bounded number of different outputs were insufficient for our context. Consequently, we followed a different proof strategy relying on the security of SNIS.

1. First, using the proof outline above, one concludes that the reduction f is close to a constant-junta.

2. Next, the security condition states that $\overline{\mathsf{T}}f$ is close to (a scalar multiple of) the reduction function g, from which we conclude that g is itself close to a constant-junta.

3 Additional Discussion

3.1 Prior Related Works

Non-interactive simulation [21, 57, 53, 30, 31, 25, 18, 24], *non-interactive correlation distillation* [45, 44, 58, 9, 16], and *one-way secure computation* [22, 2] are well-studied research directions in information theory and cryptography. Recently, [34] and [1] motivated *secure non-interactive simulation* from efficiency considerations in secure computation and study of cryptographic complexity [7, 40, 38, 6, 46].

Non-interactive simulation considers the fundamental question of deciding whether a target distribution is simulatable from the source distribution. Security is not a concern in this primitive; therefore, erasure of information from parties' views is permissible. In particular, they consider the "gap" version of this question: one determines whether such simulation is possible under an error threshold δ, or any such simulation must have an error at least $c \cdot \delta$, where c is a constant greater than 1. The general Fourier concentration phenomenon for Boolean functions (discovered in [34] and our work) is unique to SNIS, which, the authors believe, distinguishes SNIS research from its insecure analog.

[34] introduced SNIS and studied the feasibility and rate of SNIS among BSS and BES distributions. Our work considers SNIS of BSS and BES distributions from arbitrary source distributions, a significant generalization of the research scope that requires new and more powerful harmonic analysis techniques.

Independently, [1] study SNIS through the lens of spectral analysis. They mainly focused on the feasibility of SNIS and showed a necessary condition of SNIS among arbitrary joint distributions based on the spectral correlations of the source and target. Our work focus on both the feasibility and rate of SNIS but restricted to BSS and BES target distributions. For the feasibility results, we are able to give a precise characterization for a subclass of all SNIS. For example, our characterization of BSS/BES from an arbitrary source distribution is not only necessary but also sufficient. In particular, our result implies that the necessary condition in [1] is not always sufficient (see Remark 3 for more detail).

3.2 Open Problems

Our work highlights the need to develop a more powerful harmonic analysis toolkit specific to cryptography. For example, a more powerful junta theorem for "secure" reduction functions would lead to stronger feasibility and rate characterizations and innovative secure protocol design (as illustrated by our rate-1/2 SNIS of BSS(1/2) from ROLE).

Another essential technical step in our analysis relied on the junta theorems to identify perfectly secure junta reductions if a SNIS had a *sufficiently small simulation error*. However, motivated by secure computation applications that can use *constant-insecure precomputation* (for example, [28]), it is meaningful to perform this dimension reduction even when the simulation error is a *constant that is not too small*. Towards this objective, a logical research direction is to seek a "security-preserving dimension reduction" (see Conjecture 1). For example, in non-interactive correlation research, "correlation-preserving dimension reduction" is an essential step. An analogous result in the cryptographic context shall help determine the feasibility of SNIS even when the insecurity budget is not too small.

The authors believe that it is not a coincidence that the upper bound on the SNIS rate depends on the maximal correlation and eigenvalues of the Markov operator. This raises the possibility that tight rate and capacity characterization of SNIS is closely related to the maximal correlation of the source and target distributions. This investigation is related to identifying *monotones for secure computation*, cf., [54, 56, 49, 50, 51].

This work primarily considers multiple samples from one source, and a natural extension would be to consider samples from a family of sources. For example, one can simultaneously consider a correlated source and independent coins to fold the derandomization results within the technical analysis itself. [34] and our work consider BSS and BES targets and discrete sources. A natural question is to extend the analysis to incorporate more complex targets or continuous sources, like the additive white Gaussian noise source.

The introductory works on SNIS ([34, 1] and this work) consider two-party SNIS. Extending SNIS to the multi-party setting motivated by applications to multi-party computation is natural. Instead of the non-interactive setting, one can also consider the rate-limited communication model motivated by applications to leakage-resilient secure computation.

Beyond SNIS, feasibility, rate, and capacity questions are pertinent in the one-way secure computation model [22]. There are several open problems in feasibility, and no non-trivial rate/capacity results are known. The gap between non-linear and linear reduction functions in SNIS further increases the challenge of analyzing this model.

4 Preliminaries

4.1 Notation

We denote $[n]$ as the set $\{1, 2, \ldots, n\}$ and $\mathbb{N}_{<m} = \{0, 1, \ldots, m-1\}$. For two functions $f, g \colon \Omega \to \mathbb{R}$, the equation $f = g$ implies that $f(x) = g(x)$, for every $x \in \Omega$. We use Ω to denote the sample spaces, and π usually denotes a probability distribution. (Ω_x, Ω_y) is a joint probability space. For

$x \in \Omega_x^n$, we represent $x_i \in \Omega_x$ as the i-th coordinate of x. A Boolean function is a $\{\pm 1\}$-valued function.

Correlated Spaces. We use (X, Y) to denote the joint distribution over (Ω_x, Ω_y) with probability mass function π, and π_x, π_y to denote the marginal probability distributions of X and Y, respectively. Sometimes we will use $(\Omega_x \times \Omega_y, \pi)$ to denote the joint distribution. We sometimes use notation $(X, Y)_\rho$ to emphasize that its maximal correlation (defined in Section 4.2) is ρ. We always use the following notation for the expectation of functions $f \in L^2(\Omega_x^n, {\pi_x}^{\otimes n}), g \in L^2(\Omega_y^n, {\pi_y}^{\otimes n})$ over correlated spaces.

$$\mathbb{E}[f] := \mathop{\mathbb{E}}_{x \sim {\pi_x}^{\otimes n}}[f(x)],\ \mathbb{E}[g] := \mathop{\mathbb{E}}_{y \sim {\pi_y}^{\otimes n}}[g(y)],\ \mathbb{E}[fg] := \mathop{\mathbb{E}}_{(x,y) \sim \pi^{\otimes n}}[f(x) \cdot g(y)]$$

Statistical Distance. The statistical distance (total variation distance) between two distributions P and Q over a finite sample space Ω is defined as $\mathsf{SD}\left(P, Q\right) = \frac{1}{2} \sum_{x \in \Omega} |P(x) - Q(x)|$.

4.2 Maximal Correlation

We define maximal correlation and its properties in this subsection.

Definition 1 (Maximal Correlation [27, 23, 53, 3, 52, 4])**.** *The Hirschfeld-Gebelein-Rényi maximal correlation of (X, Y) is defined as*

$$\rho(X; Y) := \max_{\substack{\mathbb{E}[f]=\mathbb{E}[g]=0 \\ \mathbb{E}[f^2]=\mathbb{E}[g^2]=1}} \mathbb{E}[f(X)g(Y)]$$

For example, the maximal correlation of BSS with flipping probability ε is $|1-2\varepsilon|$ for every $\varepsilon \in [0,1]$, and the maximal correlation of BES with erasure probability ε is $\sqrt{1-\varepsilon}$ [60]. Note that maximal correlation of any distribution is always between 0 and 1.

Imported Theorem 1 (Tensorization [53])**.** *If $(X_1, Y_1)_{\rho_1}$ and $(X_2, Y_2)_{\rho_2}$ are independent, then the maximal correlation of $(X_1, X_2; Y_1, Y_2)$ is equal to $\max(\rho_1, \rho_2)$ and so if $(X_1, Y_1), (X_2, Y_2)$ are i.i.d., then it is equal to $\rho_1 = \rho_2$.*

Imported Theorem 2 (Data Processing [53])**.** *Let (X, Y) be a joint distribution. Then, for any pair of (even randomized) functions, we $\rho(f(X), g(Y)) \leqslant \rho(X, Y)$.*

One can compute maximal correlation as follows.

Proposition 1 ([53])**.** *The maximal correlation of a finite joint distribution (X, Y) is the square root of the second largest eigenvalue of the Markov operator $\mathsf{T}\overline{\mathsf{T}}$, where T and $\overline{\mathsf{T}}$ are Markov and adjoint Markov operator associated with (X, Y).*

4.3 Fourier Analysis Basics

We follow the notation of [48] to introduce some background in Fourier analysis over product measure.

4.3.1 Fourier Analysis over Higher Alphabet

Definition 2. *Let (Ω, π) be a finite probability space where $|\Omega| \geqslant 2$ and π denote a probability distribution over Ω. Let $\pi^{\otimes n}$ denote the product probability distribution on Ω^n such that*

$\pi^{\otimes n}(x_1 x_2 \ldots x_n) = \prod_{i=1}^n \pi(x_i)$. *For* $n \in \mathbb{N}$, *we write* $L^2(\Omega^n, \pi^{\otimes n})$ *to denote the real inner product space of functions* $f \colon \Omega^n \to \mathbb{R}$ *with inner product*

$$\langle f, g\rangle_{\pi^{\otimes n}} = \mathop{\mathbb{E}}_{x \sim \pi^{\otimes n}}[f(x)g(x)].$$

Moreover, the L_p*-norm of a function* $f \in L^2(\Omega^n, \pi^{\otimes n})$ *is defined as*

$$\|f\|_p := \mathop{\mathbb{E}}_{x \sim \pi^{\otimes n}}[|f(x)|^p]^{1/p}.$$

We define the distance between two functions $f, g \in L^2(\Omega, \mu)$ as $\|f - g\|_1$. Note that if f, g are bounded i.e. $|f(x)| \leqslant \alpha$ and $|g(x)| \leqslant \alpha$ for every $x \in \Omega$, then $\|f - g\|_2^2 \leqslant 2\alpha\|f - g\|_1$. In particular, for Boolean valued functions f, g, $\|f - g\|_2^2 \leqslant 2\|f - g\|_1 = 4\Pr_{x \sim \mu}[f(x) \neq g(x)]$. Therefore,

Claim 1. *Suppose* $f \in L^2(\Omega, \mu)$ *such that* $|f(x)| \leqslant \alpha$ *for every* $x \in \Omega$. *Then, we have* $\|f\|_2^2 \leqslant \alpha \cdot \|f\|_1$.

Definition 3. *A Fourier basis for an inner product space* $L^2(\Omega, \pi)$ *is an orthonormal basis* $\phi_0, \phi_1, \ldots, \phi_{m-1}$ *with* $\phi_0 \equiv 1$, *where by orthonormal, we mean that for any* $i \neq j$, $\langle \phi_i, \phi_j\rangle = 0$ *and for any* i, $\langle \phi_i, \phi_i\rangle = 1$.

It can be shown that if $\phi_0, \phi_1, \ldots, \phi_{m-1}$ is a Fourier basis for $L^2(\Omega, \pi)$, then the collection $(\phi)_{\alpha \in \mathbb{N}^n_{<m}}$ where $\phi_\alpha(x) := \prod_{i=1}^n \phi_{\alpha_i}(x_i)$ (each $\alpha_i \in \{0, 1, \ldots, m-1\}$) is a Fourier basis for $L^2(\Omega^n, \pi^{\otimes n})$. Note that the size of the basis $(\phi)_{\alpha \in \mathbb{N}^n_{<m}}$ is m^n.

Definition 4. *Fix a Fourier basis* $\phi_0, \phi_1, \ldots, \phi_{m-1}$ *for* $L^2(\Omega, \pi)$, *then every* $f \in L^2(\Omega^n, \pi^{\otimes n})$ *can be uniquely written as* $f = \sum_{\alpha \in \mathbb{N}^n_{<m}} \widehat{f}(\alpha)\phi_\alpha$ *where* $\widehat{f}(\alpha) = \langle f, \phi_\alpha\rangle$. *The real number* $\widehat{f}(\alpha)$ *is called the Fourier coefficient of* f *at* α.

For $\alpha \in \mathbb{N}^n_{<m}$, we denote $|\alpha| := |\{i \in [n] \colon \alpha_i \neq 0\}|$. The *Fourier weight* of f at degree k is defined as $W^k[f] := \sum_{\alpha : |\alpha| = k} \widehat{f}(\alpha)^2$. The Fourier weight of f at degree strictly greater than k is defined as $W^{>k}[f] := \sum_{\alpha : |\alpha| > k} \widehat{f}(\alpha)^2$. We say that the *degree* of a function $f \in L^2(\Omega^n, \pi^{\otimes n})$, denoted by $\deg(f)$, is the largest value of $|\alpha|$ such that $\widehat{f}(\alpha) \neq 0$. For every coordinate $i \in [n]$, the *i-th influence* of f, denoted by $\mathsf{Inf}_i[f]$, is defined as $\mathsf{Inf}_i[f] := \sum_{\alpha \colon \alpha_i \neq 0} \widehat{f}(\alpha)^2$. And the *total influence* is defined as $\mathsf{Inf}(f) := \sum_{i=1}^n \mathsf{Inf}_i[f] = \sum_\alpha |\alpha| \widehat{f}(\alpha)^2 = \sum_{k=1}^n k \cdot W^k[f]$.

4.3.2 Biased Fourier Analysis over Boolean Cube.

In the special case when $\Omega = \{\pm 1\}$, we define the product Fourier basis functions ϕ_S for $S \subseteq [n]$ as

$$\phi_S(x) = \prod_{i \in S} \phi(x_i) = \prod_{i \in S} \left(\frac{x_i - \mu}{\sigma}\right),$$

where $p = \pi(-1), \mu = 1 - 2p, \sigma = 2\sqrt{p}\sqrt{1-p}$.

Definition 5 (Junta Function)**.** *A function* $f \colon \Omega^n \to \{\pm 1\}$ *is called a* k*-junta for* $k \in \mathbb{N}$ *if it depends on at most* k *of its inputs coordinates; in other words,* $f(x) = g(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$, *where* $i_1, i_2, \ldots, i_k \in [n]$. *Informally, we say that* f *is a "junta" if it depends on only a constant number of coordinates. We also say that* f *is* ε*-close to a* k*-junta function* h *if* $\|f - h\|_1 \leqslant \varepsilon$.

4.4 Markov Operator

Definition 6 (Markov Operator [42])**.** *The Markov operator associated with joint distribution (X, Y), denoted by T, maps a function $g \in L^p(\Omega_y, \pi_y)$ to a function $\mathsf{T}g \in L^p(\Omega_x, \pi_x)$ by the following map:*

$$(\mathsf{T}g)(x) := \mathbb{E}[g(Y) \mid X = x],$$

where (X, Y) is distributed according to π.

Furthermore, we define the adjoint operator of T, denoted as $\overline{\mathsf{T}}$, maps a function $f \in L^p(\Omega_x, \pi_x)$ to a function $\overline{\mathsf{T}}f \in L^p(\Omega_y, \pi_y)$ by the following map:

$$(\overline{\mathsf{T}}f)(y) = \mathbb{E}[f(X) \mid Y = y].$$

Note that the two operators T and $\overline{\mathsf{T}}$ have the following property.

$$\langle Tg, f\rangle_{\pi_x} = \langle g, \overline{\mathsf{T}}f\rangle_{\pi_y} = \mathbb{E}[f(X^n)g(Y^n)].$$

Moreover, both Markov operators T and $\overline{\mathsf{T}}$ are linear operators. Both $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$ are also Markov operator. We want to emphasize that the largest eigenvalue of any Markov operator is always 1.

Proposition 2. *Let $\mathsf{T}, \overline{\mathsf{T}}$ be respectively the Markov and adjoint operator associated with the 2-by-2 distribution $(X, Y)_\rho^{\otimes n}$. Let $1 = \lambda_0 \geqslant \lambda_1 > 0$ be the eigenvalues of $\mathsf{T}\overline{\mathsf{T}}^{(1)}$ (multiplication of Markov and adjoint operators for $n = 1$). Then, it holds that $\rho = \sqrt{\lambda_1}$. Moreover, the set of all eigenvalues of $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$ is $\{1, \rho^2, \rho^4, \dots, \rho^{2n}\}$.*

Proposition 3. *[53] Suppose (X, Y) is a finite joint distribution over (Ω_x, Ω_y). Let π denote the probability mass function of (X, Y) and T and $\overline{\mathsf{T}}$ respectively denote the Markov operator and the adjoint Markov operator associated with (X, Y). Let (X, X') be the joint distribution over $(\Omega_x \times \Omega_x, \mu)$ such that the marginal distribution μ_x is the same as π_x and the associated Markov operator of (X, X') is $\mathsf{T}\overline{\mathsf{T}}$. Then, the marginal distributions of (X, X') are the same, in other words, $\mu_x = \mu_{x'}$. Furthermore, we have $\rho(\Omega_x \times \Omega_x, \mu) = \rho^2$, where ρ is the maximal correlation of (X, Y).*

This result shows that for $f \in L^2(\Omega_x, \pi_x)$, we have $(\mathsf{T}\overline{\mathsf{T}})f \in L^2(\Omega_x, \pi_x)$.

4.5 Efron-Stein Decomposition

We shall use the orthogonal Efron-stein decomposition as one of the main technical tools.

Definition 7 (Efron-Stein decomposition (Chapter 8 of [48]))**.** *Let $\{(\Omega_i, \mu_i)\}_{i=1}^{\ell}$ be discrete probability spaces and let $(\Omega, \mu) = \prod_{i=1}^{\ell}(\Omega_i, \mu_i)$. The Effron-Stein decomposition of $f \colon \Omega \to \mathbb{R}$ is defined as $f = \sum_{S \subseteq [n]} f^{=S}$ where the functions $f^{=S}$ satisfy (1) $f^{=S}$ depends only on x_S, and (2) for all $S \not\subseteq S'$ and all $x_{S'}$, $\mathbb{E}[f^{=S} | X_{S'} = x_{S'}] = 0$.*

Proposition 4 ([19])**.** *Efron-Stein decomposition exists and is unique.*

The following propositions give the relation between Markov operators and Efron-stein decompositions. The first proposition shows that the Efron-Stein decomposition commutes with Markov Operator.

Proposition 5 ([42, 43] Proposition 2.11)**.** *Let (X^n, Y^n) be a joint distribution over $(\Omega_x^n \times \Omega_y^n, \pi^{\otimes n})$. Let $\mathsf{T}^{(i)}$ be the Markov operator associated with (X_i, Y_i). Let $\mathsf{T} = \otimes_{i=1}^n \mathsf{T}^{(i)}$, and consider a function $g \in L^2(\Omega_y^n, {\pi_y}^{\otimes n})$. Then, the Efron-Stein decomposition of g satisfies $(\mathsf{T}g)^{=S} = \mathsf{T}(g^{=S})$.*

The next proposition shows that $\mathsf{T}g$ depends on the low degree expansion of g.

Proposition 6 ([43] Proposition 2.12)**.** *Assuming the setting of Proposition 5 and let ρ be the maximal correlation of the distribution (X, Y). Then for all $g \in L^2(\Omega_y^n, {\pi_y}^{\otimes n})$ it holds that $\left\|\mathsf{T}g^{=S}\right\|_2 \leqslant \rho^{|S|}\left\|g^{=S}\right\|_2$.*

The next proposition shows the connection between Fourier decomposition and Efron-Stein decomposition.

Proposition 7 ([48] Proposition 8.36)**.** *Let $f \in L^2(\Omega^n, \pi^{\otimes n})$ have the orthogonal decomposition $f = \sum_{S \subseteq [n]} f^{=S}$, and let $\{\phi_H\}_{H \in \Omega^n}$ be an orthonormal Fourier basis for $L^2(\Omega^n, \pi^{\otimes n})$. Then $f^{=S} = \sum_{\alpha\colon \mathrm{Supp}(\alpha)=S} \widehat{f}(\alpha)\phi_\alpha$. In particular, when $\Omega = \{\pm 1\}$ we have $f^{=S} = \widehat{f}(S)\phi_S$.*

This implies that $\left\|f^{=S}\right\|_2^2 = \sum_{\alpha\colon \mathrm{Supp}(\alpha)=S} \widehat{f}(\alpha)^2$. Therefore, it holds that $W^k[f] = \sum_{|S|=k}\left\|f^{=S}\right\|_2^2$, and $W^{>k}[f] = \sum_{|S|>k}\left\|f^{=S}\right\|_2^2$.

4.6 Imported Theorems

Imported Theorem 3 (Kindler-Safra Junta Theorem [36, 37])**.** *Fix $d \geqslant 0$. There exists $\varepsilon_0 = \varepsilon_0(d)$ and constant C such that for every $\varepsilon < \varepsilon_0$, if $f\colon \{\pm 1\}^n \to \{\pm 1\}$ satisfies $\mathsf{W}^{>d}[f] = \varepsilon$ then there exists a C^d-junta and degree d function $\tilde{f}\colon \{\pm 1\}^n \to \{\pm 1\}$ such that $\left\|f - \tilde{f}\right\|_2^2 \leqslant (\varepsilon + C^d \varepsilon^{5/4})$.*

Imported Theorem 4 (Friedgut's Junta Theorem [20, 48])**.** *There exists a global constant M such that the following holds. Let (Ω, π) be a finite probability space such that every outcome has probability at least λ. If $f \in L^2(\Omega^n, \pi^n)$ has range $\{\pm 1\}$ and $0 < \varepsilon \leqslant 1$, then f is ε-close to a $(1/\lambda)^{M \cdot \mathsf{Inf}(f)/\varepsilon}$-junta $h\colon \Omega^n \to \{\pm 1\}$, i.e., $\Pr_{x \sim \pi^{\otimes n}}[f(x) \neq h(x)] \leqslant \varepsilon$.*

5 Characterization of SNIS from arbitrary Sources

This section presents our feasibility characterization of SNIS from arbitrary joint distributions stated below.

Corollary 1 (Feasibility Characterization)**.** *There is an algorithm that takes as input a constant $c > 0$, a source (X, Y), and a target $(U, V) \in \{\mathsf{BSS}(\rho'), \mathsf{BES}(\rho')\}$, and*

1. *outputs YES, if there is an infinite family of reduction functions $\{f_n, g_n\}$ satisfying $(U, V) \sqsubseteq_{f_n, g_n}^{\nu_n} (X, Y)^{\otimes n}$ and $\nu_n \leqslant c/n$, and*
2. *outputs NO, otherwise.*

In the YES instance, the algorithm additionally outputs a pair of reduction functions $f^*\colon \Omega_x^{n_0} \to \{\pm 1\}$ and $g^*\colon \Omega_y^{n_0} \to \{\pm 1\}$ that witness a perfect-SNIS construction for some $n_0 = n_0(c, \rho, \rho') \in \mathbb{N}$ where ρ represents the maximal correlation of source (X, Y). Furthermore, the algorithm's running time is bounded and computable.

This theorem says that there is an algorithm that can determine whether there is a statistically SNIS of $\mathsf{BSS}/\mathsf{BES}$ from a given source. The algorithm also outputs a canonical (perfect) SNIS construction in the YES instance. Corollary 1 follows from the following statistical to perfect results.

Theorem 1 (Statistical-to-perfect)**.** *Let (X, Y) be an arbitrary joint distribution and $(U, V) \in \{\mathsf{BSS}(\rho'), \mathsf{BES}(\rho')\}$. For any $c > 0$, there are positive constants n_0, d, D such that the following result holds. If $(U, V) \sqsubseteq^{\nu}_{f,g} (X, Y)^{\otimes n}$, for some $n \geqslant n_0$, and $\nu \leqslant c/n$, then f is ν^d-close to a D-junta reduction function f^*, and g is ν^d-close to a D-junta reduction function g^* such that $(U, V) \sqsubseteq^{0}_{f^*,g^*} (X, Y)^{\otimes n}$.*

We remark that the constant D does not depend on n but might depend on the source, the target, the constant c, and the implicit constant in the Friedgut's junta theorem (Imported Theorem 4). Assuming this theorem, Figure 4 gives an algorithm for Corollary 1. We provide the proof of

$\mathsf{SNISFeasChar}\,((X, Y), (U, V), c)$:

1. Let $D = D(\rho', (X, Y), c)$ be the constant defined in Theorem 1.
2. Consider all functions $f : \Omega_x^D \to \{\pm 1\}$, and $g : \Omega_y^D \to \{\pm 1\}$
   - Return YES, if there exist f^*, g^* such that $\mathsf{BSS}(\rho') \sqsubseteq^{0}_{f^*,g^*} (X, Y)^{\otimes D}$.
   - Return NO, otherwise.

Figure 4: An algorithm to decide the feasibility of SNIS of $\mathsf{BSS}(\rho')$ from samples of (X, Y)

Theorem 1 when $(U, V) = \mathsf{BSS}(\rho')$ in Section 5.1, and when $(U, V) = \mathsf{BES}(\rho')$ in Section 5.2. At a high level, our proof strategy for BES is similar to the strategy for BSS except one technical challenge due to Bob's reduction function, which is not a Boolean-valued function.

5.1 Statistical to Perfect: BSS target

Consider a SNIS of $\mathsf{BSS}(\rho') \sqsubseteq^{\nu}_{f,g} {(X, Y)_\rho}^{\otimes n}$ where (X, Y) is an arbitrary joint distribution, $f \in L^2(\Omega_x^n, {\pi_x}^{\otimes n})$ and $g \in L^2(\Omega_y^n, {\pi_y}^{\otimes n})$.

Step 1: Algebraization of SNIS and approximate eigenvalue problem. Following a similar idea as in [34], we extend the algebraization of simulation-based SNIS to arbitrary source distribution as follows.

Theorem 2 (BSS Algebraization of Security)**.** *For any $\rho' \in (0, 1)$ and any joint distribution (X, Y), the following statements hold.*

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

This theorem gives a qualitative equivalence of the simulation-based definition and the algebraized definition. Next, composing the two L_1-norm constraints yields $\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 \leqslant 8\nu$ and $\left\|\overline{\mathsf{T}}\mathsf{T}g - {\rho'}^2 g\right\|_1 \leqslant 8\nu$. This implies that f and g are an approximate eigenvector of the two operators $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$, respectively.

Claim 2 (Approximate eigenvalue constraint)**.** *Suppose $\mathsf{BSS}(\rho') \sqsubseteq^{\nu}_{f,g} (X, Y)^{\otimes n}$, then $\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 \leqslant 8\nu$, and $\left\|\overline{\mathsf{T}}\mathsf{T}g - {\rho'}^2 g\right\|_1 \leqslant 8\nu$.*[7]

[7]Note that in general the operator $\overline{\mathsf{T}}\mathsf{T}$ (or $\mathsf{T}\overline{\mathsf{T}}$) is not equal to the noise operator T_ρ.

Step 2: Effect of Markov operators on Fourier spectrum of reduction functions. Let $\{\phi_\alpha\}$ and $\{\psi_\alpha\}$ be some Fourier bases for $L^2(\Omega_x^n, {\pi_x}^{\otimes n})$ and $L^2(\Omega_y^n, {\pi_y}^{\otimes n})$, respectively. As common in Fourier analysis, it is natural to look at the effect of the Markov operators on the Fourier characters. However, we don't know how to control the behavior of $\mathsf{T}\overline{\mathsf{T}}\phi_\alpha$ and $\overline{\mathsf{T}}\mathsf{T}\psi_\alpha$. To circumvent this bottleneck, we take a detour and look at the effect of these operators on the orthogonal (Efron-Stein) decomposition. Let $f = \sum_{S\subseteq[n]} f^{=S}$ and $g = \sum_{S\subseteq[n]} g^{=S}$ be the orthogonal decomposition. [43] showed that the decomposition has two important properties: (1) it commutes with the Markov operators (Proposition 5) and (2) the higher order terms in the decomposition of $\mathsf{T}\overline{\mathsf{T}}f = \sum_{S\subseteq[n]}(\mathsf{T}\overline{\mathsf{T}}f)^{=S}$ have significantly smaller L_2 norm compared to the L_2 norm of the corresponding higher order terms in the decomposition of f (Proposition 6 and similarly for $\overline{\mathsf{T}}\mathsf{T}g$ and g). This help us first to rewrite

$$(\mathsf{T}\overline{\mathsf{T}}f)^{=S} = (\mathsf{T}\overline{\mathsf{T}})f^{=S} = \mathsf{T}\overline{\mathsf{T}}f^{=S}, \text{and } (\overline{\mathsf{T}}\mathsf{T}g)^{=S} = \overline{\mathsf{T}}\mathsf{T}g^{=S},$$

and then bound them as:

$$\left\|\mathsf{T}\overline{\mathsf{T}}f^{=S}\right\|_2 \leqslant \rho^{2|S|}\|f\|_2, \text{and } \left\|\overline{\mathsf{T}}\mathsf{T}g^{=S}\right\|_2 \leqslant \rho^{2|S|}\|g\|_2$$

Step 3: Fourier concentration, low total influence, and junta properties of reduction functions. Those inequalities above together with the connection between orthogonal decomposition and the Fourier decomposition (Proposition 7) yields that Fourier spectrum of f and g are concentrated on low-degree terms.

Theorem 3. *Suppose there exist reduction functions $f\colon \Omega_x^n \to \{\pm 1\}$ and $g\colon \Omega_y^n \to \{\pm 1\}$ such that $\mathsf{BSS}(\rho') \sqsubseteq^{\delta}_{f,g} (X,Y)^{\otimes n}$ for some $\delta \geqslant 0$.*[8] *Then, the following bounds hold.*

$$\mathsf{W}^{>k}[f] := \sum_{\alpha\colon |\alpha|>k} \widehat{f}(\alpha)^2 \leqslant \frac{(1+\rho')^2}{(\rho^{2(k+1)} - {\rho'}^2)^2}\cdot\delta, \text{ and}$$
$$\mathsf{W}^{>k}[g] := \sum_{\alpha\colon |\alpha|>k} \widehat{g}(\alpha)^2 \leqslant \frac{(1+\rho')^2}{(\rho^{2(k+1)} - {\rho'}^2)^2}\cdot\delta,$$

where $k \in \mathbb{N}$ such that $\rho^k \geqslant \rho' > \rho^{k+1}$.

Observe that if the Fourier weight of a function is mostly concentrated on low-degree terms, then the function has small total influence (Claim 3).

Claim 3 (Concentrated on low degree implies low influence)**.** *Let f be a Boolean-valued function in $L^2(\Omega^n, \mu^{\otimes n})$. If $\mathsf{W}^{>k}[f] \leqslant \delta$, then $\mathsf{Inf}[f] \leqslant k + n\delta$.*

In particular, when δ is sufficiently small, the total influence of reduction functions f, g are constant (not depend on n). This allows us to invoke the Friedgut's junta theorem (Imported Theorem 4) and conclude that reduction functions are close to some junta functions.

Step 4: Must be Perfect. Since junta functions $\tilde{f}$ and $\tilde{g}$ depend on a constant number of variables, so does $\overline{\mathsf{T}}\tilde{f}$ and $\mathsf{T}\tilde{g}$. Observe that two distinct bounded junta functions are always constant far (Claim 4).

[8] It is possible that δ depends on n.

Claim 4 (Distinct Bounded Junta are Far)**.** *Suppose $h\colon \Omega_x^n \to \{\pm 1\}$ and $\ell\colon \Omega_y^n \to \{\pm 1\}$ are two D-junta Boolean functions in $L^2(\Omega_x^n, \pi_x)$ and $L^2(\Omega_y^n, \pi_y)$, respectively. If $\overline{\mathsf{T}}h \neq \rho'\ell$, then there exists a constant c that depends only on $\rho', D, (X,Y)$ such that $\left\|\overline{\mathsf{T}}h - \rho'\ell\right\|_2 \geqslant c$. Similarly, if $\mathsf{T}\ell \neq \rho' h$, then there exists a constant d that depends only on $\rho', D, (X,Y)$ such that $\|\mathsf{T}\ell - \rho' h\|_2 \geqslant d$.*

In particular, if $\overline{\mathsf{T}}\tilde{f} \neq \rho'\tilde{g}$, then they are constant far, which implies a constant insecurity; similarly, if $\mathsf{T}\tilde{g} \neq \rho'\tilde{f}$, then they are constant far, which also implies a constant insecurity. Thus, it must hold that $\overline{\mathsf{T}}\tilde{f} = \rho'\tilde{g}$ and $\overline{\mathsf{T}}\tilde{g} = \rho'\tilde{f}$. The junta property of $\tilde{f}$, $\tilde{f}$ and f are close, and $\mathbb{E}[f]$ is small imply that $\mathbb{E}[\tilde{f}] = 0$. Similarly, it holds that $\mathbb{E}[\tilde{g}] = 0$. Therefore, $\tilde{f}$ and $\tilde{g}$ witness a perfect construction.

Proof of Theorem 3. Observe that $\left|(\mathsf{T}\overline{\mathsf{T}}f - \rho'^2 f)(x)\right| \leqslant 2$, and $\left|(\overline{\mathsf{T}}\mathsf{T}g - \rho'^2 g)(x)\right| \leqslant 2$ for every x by the contraction property of Markov operator and boundedness of functions f and g. Observe that if a bounded function has small L_1 norm so does its L_2 norm square. Thus, we have

$$\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_2^2 \leqslant 2\delta, \text{ and} \left\|\overline{\mathsf{T}}\mathsf{T}g - {\rho'}^2 g\right\|_2^2 \leqslant 2\delta. \tag{1}$$

Let $f = \sum_{S \subseteq [n]} f^{=S}$ be the orthogonal decomposition of f. Then, we have

$$\begin{aligned}
\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_2^2 &= \sum_{S\subseteq[n]} \left\|\mathsf{T}\overline{\mathsf{T}}f^{=S} - {\rho'}^2 f^{=S}\right\|_2^2 && \text{(Orthogonal property)}\\
&\geqslant \sum_{S\colon |S|>k} \left\|\mathsf{T}\overline{\mathsf{T}}f^{=S} - {\rho'}^2 f^{=S}\right\|_2^2 && \text{(Property of norms)}\\
&\geqslant \sum_{S\colon |S|>k} \left|\, \left\|\mathsf{T}\overline{\mathsf{T}}f^{=S}\right\|_2 - {\rho'}^2 \left\|f^{=S}\right\|_2 \,\right|^2 && \text{(Triangle inequality)}
\end{aligned}$$

By Proposition 6, we have $\left\|\mathsf{T}\overline{\mathsf{T}}f^{=S}\right\|_2 \leqslant \rho^{2|S|}\left\|f^{=S}\right\|_2$. This implies that, for every $S \subseteq [n]$ satisfying $|S| > k$,

$$\left\|\mathsf{T}\overline{\mathsf{T}}f^{=S}\right\|_2 - \rho'^2\left\|f^{=S}\right\|_2 \leqslant (\rho^{2|S|} - \rho'^2)\left\|f^{=S}\right\|_2 \leqslant 0, \tag{2}$$

where the last inequality follows from $\rho^{2|S|} - \rho'^2 \leqslant \rho^{2(k+1)} - \rho'^2 \leqslant 0$ for every $|S| > k$, and $\left\|f^{=S}\right\|_2 \geqslant 0$. Thus, squaring both sides of inequality 2 for each $|S| > k$ yields

$$\begin{aligned}
\left\|\mathsf{T}\overline{\mathsf{T}}f - \rho'^2 f\right\|_2^2 &\geqslant \sum_{S\colon |S|>k} (\rho^{2|S|} - \rho'^2)^2 \left\|f^{=S}\right\|_2^2\\
&\geqslant \min_{S\colon |S|>k} (\rho^{2|S|} - \rho'^2)^2 \sum_{S\colon |S|>k} \left\|f^{=S}\right\|_2^2\\
&= (\rho^{2(k+1)} - \rho'^2)^2\ \mathsf{W}^{>k}[f]
\end{aligned}$$

This together with the inequality (1) implies that $\mathsf{W}^{>k}[f] \leqslant \frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2} \cdot \delta$. Similarly, it also holds that $\mathsf{W}^{>k}[g] \leqslant \frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2} \cdot \delta$, as desired.

5.2 Statistical to Perfect: BES target

Consider a SNIS of $\mathsf{BES}(\rho') \sqsubseteq_{f,g}^{\nu} (X,Y)_\rho^{\otimes n}$ where (X,Y) is an arbitrary joint distribution, $f \in L^2(\Omega_x^n, {\pi_x}^{\otimes n})$ and $g \in L^2(\Omega_y^n, {\pi_y}^{\otimes n})$. Step 2 and step 4 basically are the same as these steps in Section 5.1. So we shall discuss steps 1 and 3 only.

Step 1: Algebraization of SNIS and approximate eigenvalue problem. We use a similar idea as in [34] to extend the algebraization to arbitrary source.

Theorem 4 (BES target Algebraization of Security)**.** *For any $\rho' \in (0,1)$, and any joint distribution (X,Y), the following statements hold.*

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

Claim 5 (Approximate eigenvalue constraint)**.** *Suppose $\mathsf{BES}(\rho') \sqsubseteq^{\nu}_{f,g} (X,Y)^{\otimes n}$, then $\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 \leqslant 8\nu$, and $\left\|\overline{\mathsf{T}}\mathsf{T}g - {\rho'}^2 g\right\|_1 \leqslant 8\nu$.*

Step 3: Fourier concentration, low total influence, and junta properties. When the target is a BSS both the ranges of reduction functions are Boolean, so the junta theorems can be applied for both functions. On the other hand, when the target is a BES, the existing junta theorem for functions with more than two values is not good enough for us. To overcome this barrier, we first use the same idea to show that Alice's reduction function f is close to a junta function $f^*\colon \Omega_x^n \to \{\pm 1\}$, and then prove that Bob's reduction function g is also close to a junta function using the security constraint $\left\|\overline{\mathsf{T}}f^* - g\right\|_1 \leqslant \nu$. More concretely, since f^* is a junta function, so does $\overline{\mathsf{T}}f^*$. This together with the security constraint imply that g is close to a the junta function $\overline{\mathsf{T}}f^*$ whose range is not necessarily $\{\pm 1, 0\}$. However, we can round each value of $(\overline{\mathsf{T}}f^*)(y)$ to the closest value in $\{\pm 1, 0\}$. The rounded function is still a junta function and close to the original function $\overline{\mathsf{T}}f^*$. Therefore, g is close to the rounded junta function by triangle inequality. We formalize this step at follows.

Claim 6. *Suppose $f^*\colon \Omega_x^n \to \{\pm 1\}$ is a junta function and $g\colon \Omega_y^n \to \{\pm 1, 0\}$ is an arbitrary function such that $\left\|\overline{\mathsf{T}}f^* - g\right\|_1 \leqslant \delta$ for some $\delta \geqslant 0$. Then, there exists a junta function $g^*\colon \Omega_y^n \to \{\pm 1, 0\}$ such that g is $\Theta(\sqrt{\delta})$-close to g^*.*

6 Estimation of Rate from arbitrary Sources

As a consequence of the statistical to perfect theorem (Theorem 1), we can lower bound the rate by a positive constant, if it is feasible.

Corollary 2 (Constant Rate Lower Bound)**.** *Fix a constant $c > 0$, a source (X,Y), and a target $(U,V) \in \{\mathsf{BSS}(\rho'), \mathsf{BES}(\rho')\}$ for $\rho' \in (0,1)$. If there exists an infinite family of reduction functions $\{f_n, g_n\}$ such that $(U,V) \sqsubseteq^{\nu(n)}_{f_n,g_n} (X,Y)^{\otimes n}$, and $\nu(n) \leqslant c/n$, then the production rate $R(\,(U,V),(X,Y)\,) \geqslant 1/D$ for some constant $D = D((X,Y),\rho',c)$.*

We note that the constant D is the number of input variables that perfect reduction functions depend on. Next, we prove an upper bound the rate of perfect SNIS.

Theorem 5 (Perfect Security Rate). *Let $(U,V) \in \{\mathsf{BSS}(\rho'), \mathsf{BES}(\rho')\}$ for $\rho' \in (0,1)$. If $(U,V)^{\otimes m} \sqsubseteq^{0}_{\vec{f},\vec{g}} (X,Y)^{\otimes n}_{\rho}$ for some $m,n \in \mathbb{N}$, then $m/n \leqslant 1/\lfloor \log_\sigma \rho' \rfloor$, where σ^2 is the smallest non-zero eigenvalue of the operator $\mathsf{T}\overline{\mathsf{T}}$ for the source (X,Y).*

Remark 2. *For the SNIS self-reduction of* BSS *or* BES*, [34] showed that* $\rho' = \rho^k$ *for some* $k \in \mathbb{N}$ *and the rate* $m/n \leqslant 1/k$ *matching our bound here since* $\sigma = \rho$*, where* ρ *is the maximal correlation of the source* (X, Y)*. The* ROLE *distribution has maximal correlation* $\rho = 1/\sqrt{2}$ *and* $\sigma = 1/\sqrt{2}$*. Thus, when* $(X, Y) = \mathsf{ROLE}$*, the rate is upper bounded by* $1/2$*. Our new construction realizes this bound, demonstrating its optimality.*

Proof of Theorem 5. We shall prove for the case $(U, V) = \mathsf{BSS}$. The proof for the case $(U, V) = \mathsf{BES}$ is almost identical. Suppose $\mathsf{BSS}(\rho')^{\otimes m} \sqsubseteq^0_{\vec{f},\vec{g}} (X, Y)^{\otimes n}$ for some $m, n \in \mathbb{N}$ and (deterministic) reduction functions $\vec{f} = (f_1, \cdots, f_m)$ and $\vec{g} = (g_1, \cdots, g_m)$. For $\rho'' = {\rho'}^m$, there is a linear deterministic construction realizing $\mathsf{BSS}(\rho'') \sqsubseteq^0 \mathsf{BSS}(\rho')$. By sequential composition Imported Theorem 5, it holds that $\mathsf{BSS}(\rho'') \sqsubseteq^0 (X, Y)^{\otimes n}$. Let $\mathsf{T}, \overline{\mathsf{T}}$ denote the Markov operator and the adjoint Markov operator associated with (X, Y). Note that $\mathsf{T}\overline{\mathsf{T}}$ is non-negative definite (see [53] for a proof). Let $1 = \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_t = \sigma^2 > 0$ are all non-zero eigenvalues of $\mathsf{T}\overline{\mathsf{T}}$. Then, according to Theorem 1, we have ${\rho''}^2 = \prod_{i=2}^t \lambda_i^{k_i}$, where $k_i \in \mathbb{N}$ such that $\sum_{i=2}^t k_i \leqslant n$. This implies that

$$
{\rho''}^2 = {\rho'}^{2m} = \prod_{i=2}^{t} \lambda_i^{k_i} \geqslant \lambda_t^{k_2+\ldots+k_t} = \sigma^{2(k_2+\ldots+k_t)} \geqslant \sigma^{2n}.
$$

Taking the logarithm of base $\sigma < 1$ of both sides yields $2m \log_\sigma \rho' \leqslant 2n$ which implies that $m/n \leqslant 1/\log_\sigma \rho'$ as desired.

7 Characterization of BSS/ BES from 2-by-2 Distributions

In this section, we present a succinct characterization of BSS/BES from a 2-by-2 source. The following theorem states that SNIS of $\mathsf{BSS}(\rho')$ from $(X, Y)_\rho$ is possible if and only if the source is a $\mathsf{BSS}(\rho)$ such that $\rho' = \rho^k$ for some positive integer k.

Theorem 6 (Characterization of BSS from 2-by-2)**.** *Fix a 2-by-2 distribution* $(X, Y)_\rho$*, and also* $\mathsf{BSS}(\rho')$*.*

1. *If* $(X, Y)_\rho \neq \mathsf{BSS}(\rho)$ *or* $\rho' \neq \rho^k$ *for all* $k \in \mathbb{N}$*: There is a positive constant* $c = c(\rho, \rho')$ *such that* $\mathsf{BSS}(\rho') \sqsubseteq^\nu (X, Y)^{\otimes n}$*, for any* $n \in \mathbb{N}$*, implies that* $\nu \geqslant c$*.*

2. *If* $(X, Y)_\rho = \mathsf{BSS}(\rho)$ *and* $\rho' = \rho^k$*, for some* $k \in \mathbb{N}$*: There are positive constants* $c = c(\rho, \rho')$ *and* $d = d(\rho, \rho')$ *such that the following result holds. If* $\mathsf{BSS}(\rho') \sqsubseteq^\nu_{f,g} \mathsf{BSS}(\rho)^{\otimes n}$*, 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* $\mathsf{BSS}(\rho') \sqsubseteq^0_{f^*,g^*} \mathsf{BSS}(\rho)^{\otimes n}$*. Furthermore,* $f^* = g^*$ *is a* k*-homogeneous*[9] *Boolean function.*

Remark 3. *It is shown in [1] that* $\mathsf{BES}(\rho') \sqsubseteq^{\nu_n}_{f_n,g_n} (X, Y)^{\otimes n}$ *(where* $\nu_n = o(1)$*) only if the spectrum* [10] *of* (U, V) *is contained in the spectrum of the* $(X, Y)^{\otimes n}$ *for some* n*. Note that Theorem 6 implies that the necessary condition mentioned in [1] is not sufficient since there exists a 2-by-2 distribution* $(X, Y)_\rho \neq \mathsf{BSS}(\rho)$ *and* $(U, V) = \mathsf{BSS}(\rho')$ *such that* $\rho' = \rho^k$*, the spectrum of* (U, V) *is contained in the spectrum of* $(X, Y)^{\otimes n}$*, but there is no SNIS of* (U, V) *from* (X, Y)*.*

[9] A function $f\colon \{\pm 1\}^n \to \{\pm 1\}$ is k-homogeneous if all the terms in the multi-linear expansion of f has degree k.

[10] Spectrum of a distribution matrix M is defined in [1] as the multi-set of non-zero singular values of the matrix $\Delta_{M^T}^{-1/2} M \Delta_M^{-1/2}$ where Δ_M represents a diagonal matrix with the vector $\mathbf{1}^T M$ along its diagonal.

Next, we show that SNIS of BES from a 2-by-2 source is impossible. This result implies that, for example, any construction of BES from a Z-channel with randomized input has constant security.

Theorem 7 (Characterization of BES from 2-by-2)**.** *Fix a 2-by-2 distribution $(X,Y)_\rho$, and also $\mathsf{BES}(\rho')$. There are positive constants $c = c(\rho,\rho')$ such that if $\mathsf{BES}(\rho') \sqsubseteq^{\nu}_{f,g} (X,Y)^{\otimes n}$ for some $n \in \mathbb{N}$, then the simulation error ν is at least c.*

We shall first prove the Theorem 6, and then we provide a proof of Theorem 7 in Section 7.3.
Proof outline of Theorem 6. First, we show that if there is a statistical SNIS of $\mathsf{BSS}(\rho')$ from $(X,Y)^{\otimes n}$, then a perfect construction exists (Theorem 8). Next, we characterize for which 2-by-2 distribution (X,Y) there exists a perfect-SNIS of $\mathsf{BSS}(\rho')$ from $(X,Y)^{\otimes n}$. Theorem 9 says that (X,Y) must be a BSS. Finally we conclude the proof by using the characterization of SNIS between BSS distributions in [34].

Theorem 8 (Statistical-to-perfect of BSS from 2-by-2)**.** *Let $\rho' \in (0,1)$ and $(X,Y)_\rho$ be an arbitrary 2-by-2 joint distribution. There are positive constants $c = c((X,Y)_\rho,\rho')$, $d = d((X,Y)_\rho,\rho')$, and $D = D((X,Y)_\rho,\rho')$ such that the following result holds. If $\mathsf{BSS}(\rho') \sqsubseteq^{\nu}_{f,g} (X,Y)^{\otimes n}_\rho$, for any $n \in \mathbb{N}$, and $\nu \leqslant c$, then f is ν^d-close to a D-junta reduction function f^*, and g is ν^d-close to a D-junta reduction function g^* such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{0}_{f^*,g^*} (X,Y)^{\otimes n}_\rho$. Furthermore, $\rho' = \rho^k$, and $\mathsf{W}^k[f^*] = \mathsf{W}^k[g^*] = 1$.*

Informally, there is a statistical SNIS of $\mathsf{BSS}(\varepsilon')$ from (X,Y) if and only if $(X,Y)_\rho = \mathsf{BSS}(\rho)$ for some ρ satisfying $\rho' = \rho^k$ for some $k \in \mathbb{N}$. Furthermore, any statistical reduction functions can be error-corrected to junta ones that witness a perfect construction.

Theorem 9 (Characterization of Perfect-SNIS of BSS from 2-by-2)**.** *Suppose there exists $n \in \mathbb{N}$ and Boolean functions $f,g\colon \{\pm1\}^n \to \{\pm1\}$ such that $\mathsf{BSS}(\rho') \sqsubseteq^{0}_{f,g} (X,Y)^{\otimes n}$. Then, the distribution (X,Y) must be a $\mathsf{BSS}(\rho)$ such that $\rho' = \rho^k$ for some positive integer $k \leqslant n$.*

As a consequence of Theorem 6, the rate for perfect SNIS of BSS from an arbitrary 2-by-2 distribution is completely settled, while the rate for statistical security (even if the source is BSS) is still open.

Corollary 3. *If $(X,Y) \neq \mathsf{BSS}(\rho)$ for all $\rho \in (0,1)$ or $\rho' \neq \rho^k$ for all $k \in \mathbb{N}$, then the rate of $\mathsf{BSS}(\rho')$ from (X,Y) is zero. Otherwise, it is shown in [34] that the maximum achievable rate is $1/k$ in perfect SNIS.*

7.1 Statistical to Perfect

This section presents the proof of the statistical to perfect (Theorem 8) when the source is a 2-by-2 distribution. The proof idea is similar to the general case. For 2-by-2 distribution, we are able to precisely characterize the effect of Markov operators on Fourier coefficients. We remark that Fourier basis and the orthogonal Efron-Stein basis are the same in this case.

7.1.1 Proof Outline of Theorem 8.

Consider a SNIS of $\mathsf{BSS}(\rho') \sqsubseteq^{\nu}_{f,g} {(X,Y)_\rho}^{\otimes n}$ where (X,Y) is a 2-by-2 distribution and $f,g\colon \{\pm1\}^n \to \{\pm1\}$.

Step 1: Algebraization of SNIS and approximate eigenvalue problem. This step is identical to the first step in the case (X,Y) is a 2-by-2 distribution discussed in Section 7.1.

Step 2: Effect of Markov operators on Fourier spectrum of reduction functions. If $\mathsf{T}\overline{\mathsf{T}}$ and/or $\overline{\mathsf{T}}\mathsf{T}$ is equal to the Bonami-Beckner operator T_γ for some appropriate γ, which happens when $(X, Y) = \mathsf{BSS}$, then the T_γ operator scales $\widehat{f}(S)$ proportional to $\gamma^{|S|}$, which, in turn, solves the approximate eigenvalue problem nicely as done in [34]. However, both $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$ are not equal to T_ρ in general. We overcome this bottleneck by characterizing the effect of these Markov operators on the Fourier coefficients as follows.

Lemma 1. *Let $\{\phi_S\}_{S\subseteq[n]}$ be a biased Fourier basis for $L^2(\Omega_x^n, \pi_x{}^{\otimes n})$, and $\{\psi_S\}_{S\subseteq[n]}$ be a biased Fourier basis for $L^2(\Omega_y^n, \pi_y{}^{\otimes n})$. Then, for any $S \subseteq [n]$, it holds that*

$$\mathsf{T}\overline{\mathsf{T}}\phi_S = \rho^{2|S|}\phi_S, \text{ and } \overline{\mathsf{T}}\mathsf{T}\psi_S = \rho^{2|S|}\psi_S.$$

Consequently, for any real-valued functions $f \in L^2(\mathcal{X}^n, \pi_x{}^{\otimes n})$ and $g \in L^2(\Omega_y^n, \pi_y{}^{\otimes n})$, the Fourier expansion of $\mathsf{T}\overline{\mathsf{T}}f$ and $\overline{\mathsf{T}}\mathsf{T}g$ is given by

$$\mathsf{T}\overline{\mathsf{T}}f = \sum_{S\subseteq[n]} \rho^{2|S|}\widehat{f}(S)\phi_S, \text{ and } \overline{\mathsf{T}}\mathsf{T}g = \sum_{S\subseteq[n]} \rho^{2|S|}\widehat{g}(S)\psi_S.$$

One can view this lemma as an analog/extension of $\mathsf{T}_\rho\chi_S = \rho^{|S|}\chi_S$ and $\mathsf{T}_\rho f = \sum_S \rho^{|S|}\widehat{f}(S)\chi_S$ to correlated space. Intuitively, the $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$ operator scales $\widehat{f}(S)$ and $\widehat{g}(S)$ proportional to $\rho^{2|S|}$, respectively. Lemma 1 is crucial to prove the concentration of Fourier spectrum of reduction functions.

Step 3: Fourier concentration and junta properties of reduction functions. Recall that the maximal correlation ρ is the square root of the second largest eigenvalue of $\mathsf{T}\overline{\mathsf{T}}$ and $\overline{\mathsf{T}}\mathsf{T}$ as well, and $\{1, \rho^2, \rho^4, \ldots\}$ are the set of all eigenvalues of the two Markov operators as well (Proposition 2). Consequently, if ${\rho'}^2 \notin \{\rho^2, \rho^4, \ldots\}$, then $\mathsf{T}\overline{\mathsf{T}}f$ and $\overline{\mathsf{T}}\mathsf{T}g$ cannot be close to ${\rho'}^2 f$ and ${\rho'}^2 g$, respectively. When f and g are Boolean functions, there will be constant gap between $\mathsf{T}\overline{\mathsf{T}}f$ and ${\rho'}^2 f$, which implies that the simulation error ν is at least a constant.

On the other hand, if ${\rho'}^2 = \rho^{2k}$ or equivalently $\rho' = \rho^k$ for some $k \in \mathbb{N}$, for any $|S| \neq k$, the weight on $\widehat{f}(S)$ contributes to the gap between $\mathsf{T}\overline{\mathsf{T}}f$ and ${\rho'}^2 f$. As a consequence, most of the Fourier weight of f is concentrated on S such that $|S| = k$. We formalize this argument as follows.

Theorem 10 (Constant Insecurity or Close to Low Degree Junta)**.** *Suppose that $\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 = \delta_1$, $\left\|\overline{\mathsf{T}}\mathsf{T}g - {\rho'}^2 g\right\|_1 = \delta_2$. Then the following statements hold.*

1. *If $\rho^{t+1} < \rho' < \rho^t$, then $\min(\delta_1, \delta_2) \geqslant \frac{1}{2}\min(({\rho'}^2 - \rho^{2t})^2, ({\rho'}^2 - \rho^{2(t+1)})^2)$.*
2. *If $\rho' = \rho^k$ for some $k \in [n]$, then there exists $D = D(k)$ such that*
   (a) *The functions f and g are $\frac{2\delta_1}{(1-\rho^2)^2\rho^{4k}}$, and $\frac{2\delta_2}{(1-\rho^2)^2\rho^{4k}}$ concentrated on degree k, respectively.*
   (b) *There exist Boolean degree-k D-junta functions $\tilde{f}, \tilde{g}\colon \{\pm 1\}^n \to \{\pm 1\}$ such that $\left\|f - \tilde{f}\right\|_2^2 \leqslant \sigma_1 + D\sigma_1^{5/4}$, and $\|g - \tilde{g}\|_2^2 \leqslant \sigma_2 + D\sigma_2^{5/4}$, where $\sigma_1 = \frac{2}{(1-\rho^2)^2\rho^{4k}} \cdot \delta_1$ and $\sigma_2 = \frac{2}{(1-\rho^2)^2\rho^{4k}} \cdot \delta_2$.*

In the above claim, we use the Kindler-Safra junta theorem [37, 36] (see Imported Theorem 3) to infer that f is close to a junta function from the Fourier concentration property. The junta property is crucial to show the existence of a perfect construction.

Step 4: Must be perfect. This step is similar to the step 4 in the general case. Using the junta properties, one conclude that there exists a perfect construction.

7.2 Perfect-SNIS Characterization

In this section, we prove Theorem 9. We need the following result for the proof.

Claim 7. *Suppose f is a Boolean function in $L^2(\{\pm 1\}^n, \pi^{\otimes n})$ such that $\mathsf{W}^k[f] = 1$. Then, the distribution π must be the uniform distribution over $\{\pm 1\}$.*

The following result is needed to prove Claim 7. First let us introduce some notation. Let $f\colon \{\pm 1\}^n \to \{\pm 1\}$ be a Boolean function. For each $p \in (0,1)$, we write a Boolean function f as $f^{(p)}$ when viewing f as an element of $L^2(\{\pm 1\}^n), {\pi_p}^{\otimes n})$, where π_p is a distribution over $\{\pm 1\}$ such that $\pi_p(-1) = p$ and $\pi_p(1) = 1-p$. Observe that $\sigma = 2\sqrt{p}\sqrt{1-p}$ is the standard deviation of the distribution.

Claim 8. *If $\mathsf{W}^{\leqslant k}[f^{(p)}] = 1$, then $\mathsf{W}^k[f^{(1/2)}] = \mathsf{W}^k[f^{(p)}]/\sigma^{2k}$ where $\sigma = 2\sqrt{p(1-p)}$.*

Intuitively, this claim says that the Fourier weight measured over the p-biased distribution on a particular degree is equal to the product of the Fourier weight measured over the uniform distribution on the same degree and a power of the standard deviation the p-biased distribution.

Proof of Claim 7. Let $p := \pi(-1)$. It follows from Claim 8 that $\mathsf{W}^k[f^{(p)}] \leqslant \sigma^{2k}\mathsf{W}^k[f^{(1/2)}]$. Since f is Boolean it follows from Parseval identity that $\mathsf{W}^k[f^{(1/2)}] \leqslant 1$, and so $1 = \mathsf{W}^k[f^{(p)}] \leqslant \sigma^{2k}$ which implies that $\sigma = 1$ and so $p = 1/2$. Therefore, the distribution π is uniform. □

Now we are ready to prove Theorem 9 as follow.

of Theorem 9. Suppose there exists $n \in \mathbb{N}$ and Boolean functions $f, g\colon \{\pm 1\}^n \to \{\pm 1\}$ such that $\mathsf{BSS}(\rho') \sqsubseteq^0_{f,g} (X,Y)^{\otimes n}$. Then, applying Theorem 1 for insecurity bound $\nu = 0$ yields $\rho' = \rho^k$ for some $k \in \mathbb{N}$, and $\mathsf{W}^k[f] = \mathsf{W}^k[g] = 1$, where ρ is the maximal correlation of (X,Y). By Claim 7, both the marginal distributions π_x and π_y must be uniform distribution over $\{\pm 1\}$. This implies that the joint distribution (X,Y) is a $\mathsf{BSS}(\varepsilon)$ for some $\varepsilon \in (0,1/2)$. Using the fact that the the maximal correlation of $\mathsf{BSS}(\varepsilon) = \rho$ and the result from [34], one concludes that $\rho' = \rho^k$. □

7.3 Proof Outline of Theorem 7

The proof of Theorem 7 is similar to the proof of Theorem 6 except that here we again use the same idea that we applied in BES from arbitrary to deal with the non-binary range of Bob's reduction function. Again, we have a statistical to perfect result. Similar to Theorem 9, we can show that the source must be a BSS. We conclude the proof by using the impossibility result of simulating BES from BSS even in the (non-secure) NIS due to reverse hypercontractivity.

8 Additional Results and Discussions

8.1 Necessary Condition on Eigenvalues

Theorem 11. *Let (X,Y) be an arbitrary joint distribution whose Markov operator and adjoint are respectively $\mathsf{T}^{(1)}$ and $\overline{\mathsf{T}}^{(1)}$, and let $(U,V) \in \{\mathsf{BSS}(\rho'), \mathsf{BES}(\rho')\}$ for $\rho' \in (0,1)$. For any $c > 0$, there are positive constants n_0 and $d = d((X,Y),\rho')$ such that the following result holds. If $(U,V) \sqsubseteq^{\nu}_{f,g} (X,Y)^{\otimes n}$, for some $n \geqslant n_0$, and $\nu \leqslant c/n$, then ${\rho'}^2 = \prod_{i=1}^t \lambda_i^{k_i}$, where $1 = \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_t$ are all eigenvalues of $(\mathsf{T}\overline{\mathsf{T}})^{(1)}$, and $k_i \in \mathbb{N}$ such that $\sum_{i=1}^t k_i = n$.*

By the reduction of statistical to perfect (Theorem 1), without loss of generality, assume that $\mathsf{BSS}(\rho') \sqsubseteq^0_{f,g} (X,Y)^{\otimes n}$. Theorem 2 and Claim 2 imply that $\mathsf{T}\overline{\mathsf{T}} f = {\rho'}^2 f$. This means that ${\rho'}^2$ is an eigenvalue of the Markov operator $\mathsf{T}\overline{\mathsf{T}}$. Suppose $1 = \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_t$ be all eigenvalues of $(\mathsf{T}\overline{\mathsf{T}})^{(1)}$, then it follows from tensorization property of eigenvalues (Lemma 6) that ${\rho'}^2 = \prod_{i=1}^t \lambda_i^{k_i}$ for some $k_i \in \mathbb{N}$ such that $k_1 + k_2 + \cdots + k_t = n$, as desired. As a consequence, we have the following result.

Corollary 4. *There is no complete joint distribution in SNIS.*

8.2 Decidability

Corollary 1 gives an algorithm to decide whether there is a statistical SNIS of $\mathsf{BSS}(\rho')$ from (X,Y) with insecurity bound $\nu(n) = \mathcal{O}(1/n)$. In (non-secure) NIS, [25, 18, 24] considered a different problem of decidability called gap decidability. Given a constant $\delta > 0$, a source (X,Y) and a target (U,V), the goal is to distinguish between (1) there exists a $n_0 \in \mathbb{N}$ such that (U,V) can be non-interactively simulated (not necessarily secure) from $(X,Y)^{\otimes n_0}$ with error at most δ and (2) for any $n \in \mathbb{N}$, any simulation of (U,V) from $(X,Y)^{\otimes n}$ has error at least $c\delta$, where c is some constant. The gap decidability of BSS from an arbitrary source in SNIS is still open. We formulate this problem as follows.

SNIS gap decidability problem. Given any $c > 1, \delta > 0$, a source (X,Y), and a target $\mathsf{BSS}(\rho')$. Distinguish between the following 2 cases:

1. There exist $n_0 \in \mathbb{N}$ and functions $f\colon \Omega_x^{n_0} \to \{\pm 1\}$ and $g\colon \Omega_y^{n_0} \to \{\pm 1\}$ such that SNIS of $\mathsf{BSS}(\rho)$ from $(X,Y)^{\otimes n_0}$ has simulation error at most δ.
2. For any $n \in \mathbb{N}$ and $f\colon \Omega_x^{n} \to \{\pm 1\}$ and $g\colon \Omega_y^{n} \to \{\pm 1\}$, SNIS of $\mathsf{BSS}(\rho)$ from $(X,Y)^{\otimes n}$ has simulation error at least $c\delta$.

When the source is a 2-by-2 distribution, our characterization solves this problem and we know for sure it is a Yes instance when the threshold δ is less than the constant in our Theorem 8. We conjecture the following "junta theorem over correlated space"/"dimension reduction preserving security" that would help to solve the gap decidability problem. In the following, we abuse the notation and let $\mathsf{T}, \overline{\mathsf{T}}$ denote the Markov operator and adjoint Markov operator of both $(X,Y)^{\otimes n}$ and $(X,Y)^{\otimes n_0}$.

Conjecture 1. *Given any $\delta \geqslant 0$, and $f\colon \Omega_x^n \to \{\pm 1\}$ and $g\colon \Omega_y^n \to \{\pm 1\}$ satisfying $\mathbb{E}[f] \leqslant \delta, \mathbb{E}[g] \leqslant \delta$, $\left\|\overline{\mathsf{T}} f - \rho' g\right\|_1 \leqslant \delta$ and $\|\mathsf{T} g - \rho' f\|_1 \leqslant \delta$, there exist $n_0 = n_0((X,Y), \rho', \delta)$, functions $f^*\colon \Omega_x^{n_0} \to \{\pm 1\}$ and $g^*\colon \Omega_y^{n_0} \to \{\pm 1\}$ such that*

$$(i)\ |\mathbb{E}[f^*] - \mathbb{E}[f]| \leqslant 2\delta, \quad (ii)\ |\mathbb{E}[g^*] - \mathbb{E}[g]| \leqslant 2\delta,$$
$$(iii)\ \left\|\overline{\mathsf{T}} f^* - \rho' g^*\right\|_1 \leqslant 2\delta, \text{ and } (iv)\ \left\|\mathsf{T} g^* - \rho' f^*\right\|_1 \leqslant 2\delta.$$

The conjecture holds true when the source is 2-by-2 and δ is a small enough constant due to our characterization theorem.

The requirement that both f^* and g^* remains Boolean-valued functions is unique to security constraint in SNIS. In contrast, the reduction functions in NIS setting [25] only need to be bounded functions since they only need to preserve the correlation (see Theorem 3.1 in [25]) not the security.

8.3 On Power of Non-linear Constructions

Lemma 2 (Non-linear constructions of $\mathsf{BSS}(1/2)$ from ROLE)**.** *There are exactly 16 perfect non linear SNIS constructions of* $\mathsf{BSS}(1/2)$ *from two samples of* ROLE*.*

By implementing our exhaustive search algorithm, we found 16 perfect constructions provided in Appendix E.3.

Lemma 3. *There is a perfect non linear SNIS construction of* $\mathsf{BES}(\sqrt{1/2})$ *from one sample of* ROLE*.*

Next, we shall show that there is no SNIS construction of $\mathsf{BSS}(1/2)/\mathsf{BES}(\sqrt{1/2})$ from n independent samples of ROLE for any $n \in \mathbb{N}$.

Lemma 4. *For any naming of the samples from the* ROLE *distribution, any* $n \in \mathbb{N}$*, any SNIS of* $\mathsf{BSS}(1/2)$ *or* $\mathsf{BES}(\sqrt{1/2})$ *from* $\mathsf{ROLE}^{\otimes n}$ *with linear reductions has a constant simulation error.*

We provide a proof of Lemma 4 in Appendix E.3

Corollary 5. *Fix a constant* $c > 0$*, then the following statements hold.*

1. *There exists an infinite family of reduction functions* $\{f_n, g_n\}$ *such that* $\mathsf{BSS}(\rho') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{ROLE}^{\otimes n}$ *and* $\nu(n) \leqslant c/n$ *if and only if* $\rho' = 1/2^k$ *for some* $k \in \mathbb{N}$*.*

2. *There exists an infinite family of reduction functions* $\{f_n, g_n\}$ *such that* $\mathsf{BES}(\rho') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{ROLE}^{\otimes n}$ *and* $\nu(n) \leqslant c/n$ *if and only if* $\rho' = 1/\sqrt{2}^k$ *for some* $k \in \mathbb{N}$*.*

8.4 Incompleteness of string-ROT

Garg et al. [22] initiated the study of one way secure computation (OWSC). One of the results they proved was that the family of string-ROT is complete in OWSC when considering negligible error. An open question in [22] was the completeness of finite channels in OWSC which has been recently solved by [2]. They provide a construction of string-ROT using bit-ROT with inverse polynomial error. This means that bit-ROT can be used to realize randomized functionalities with inverse polynomial error in OWSC. [2] also rule out the existence of any complete finite channel when considering negligible error. [1] show that there is no complete joint distribution in SNIS setting. We show that even the family of string-ROT is not complete.

Definition 8. *The* ℓ*-bit string random oblivious transfer source, represented as* $ROT(\ell)$*, samples uniformly and independently random* $x_1, x_2 \in \{0,1\}^\ell$ *and a bit* $b \in \{0,1\}^n$*, provides Alice* (x_1, x_2)*, and provides Bob* (b, x_b)*.*

In contrast to the completeness result in OWSC, we show that the family of string-ROT is not complete.

Lemma 5. *The family of string-ROT is not complete for SNIS.*

This lemma follows from the fact that the maximal correlation of $ROT(\ell) = 1/\sqrt{2}$ for every $\ell \in \mathbb{N}$ (Claim 16) and the data processing inequality (Imported Theorem 2).

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. 2, 4, 7, 9, 10, 19, 24

[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. doi:10.1007/978-3-030-64840-4_22. 2, 9, 24

[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. 5, 11

[4] Venkat Anantharam, Amin Gohari, Sudeep Kamath, and Chandra Nair. On maximal correlation, hypercontractivity, and the data processing inequality studied by erkip and cover. *arXiv preprint arXiv:1304.6133*, 2013. 5, 11

[5] 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. doi:10.1007/3-540-46766-1_34. 1

[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. doi:10.1007/978-3-642-54242-8_14. 2, 4, 9

[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. doi:10.1007/978-3-540-24638-1_14. 2, 4, 9

[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. doi:10.1145/1455770.1455804. 1

[9] Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *IEEE Trans. Inf. Theory*, 57(10):6351–6355, 2011. doi:10.1109/TIT.2011.2134067. 2, 9

[10] 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. doi:10.1007/978-3-030-26954-8_16. 1

[11] 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. doi:10.1007/978-3-030-56880-1_14. 1

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

[13] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2000. https://eprint.iacr.org/2000/067. 1

[14] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd FOCS*, pages 136–145. IEEE Computer Society Press, October 2001. doi:10.1109/SFCS.2001.959888. 1

[15] Brent Carmer and Mike Rosulek. Linicrypt: A model for practical cryptography. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 416–445. Springer, Heidelberg, August 2016. doi:10.1007/978-3-662-53015-3_15. 4

[16] 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. doi:10.1109/TIT.2014.2301155. 2, 9

[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. doi:10.1007/978-3-642-32009-5_38. 1

[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. doi:10.1137/1.9781611975031.174. 2, 8, 9, 23

[19] Bradley Efron and Charles Stein. The jackknife estimate of variance. *The Annals of Statistics*, pages 586–596, 1981. 13

[20] Ehud Friedgut. Boolean functions with low average sensitivity depend on few coordinates. *Comb.*, 18(1):27–35, 1998. doi:10.1007/PL00009809. 14

[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, 3, 8, 9

[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. doi:10.1007/978-3-662-48000-7_10. 2, 7, 9, 10, 24

[23] Hans Gebelein. Das statistische problem der korrelation als variations-und eigenwertproblem und sein zusammenhang mit der ausgleichsrechnung. *ZAMM-Journal of Applied Mathematics and Mechanics/Zeitschrift für Angewandte Mathematik und Mechanik*, 21(6):364–379, 1941. 11

[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. URL: https://doi.org/10.4230/LIPIcs.CCC.2018.28, doi:10.4230/LIPIcs.CCC.2018.28. 2, 8, 9, 23

[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. doi:10.1109/FOCS.2016.65. 2, 3, 8, 9, 23

[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. doi:10.1145/28395.28420. 1

[27] Hermann O Hirschfeld. A connection between correlation and contingency. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 520–524. Cambridge University Press, 1935. doi:10.1017/S0305004100013517. 5, 11

[28] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 667–684. Springer, Heidelberg, August 2011. doi:10.1007/978-3-642-22792-9_38. 4, 5, 10

[29] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 572–591. Springer, Heidelberg, August 2008. doi:10.1007/978-3-540-85174-5_32. 5

[30] 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, 8, 9

[31] Sudeep Kamath and Venkat Anantharam. On non-interactive simulation of joint distributions. *IEEE Transactions on Information Theory*, 62(6):3419–3435, 2016. 2, 8, 9

[32] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation: Feasibility & rate. Cryptology ePrint Archive, Report 2020/252, 2020. https://eprint.iacr.org/2020/252. 4

[33] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Decidability of secure non-interactive simulation of doubly symmetric binary source. Cryptology ePrint Archive, Report 2021/190, 2021. https://eprint.iacr.org/2021/190. 4

[34] Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation: Feasibility & rate. *To appear at EUROCRYPT 2022*, 2022. URL: https://eprint.iacr.org/2020/252.pdf. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15, 18, 19, 20, 21, 22, 31

[35] Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd ACM STOC*, pages 316–324. ACM Press, May 2000. doi:10.1145/335305.335342. 1

[36] Guy Kindler. *Property Testing PCP*. PhD thesis, Tel-Aviv University, 2002. 14, 21

[37] Guy Kindler and Shmuel Safra. Noise-resistant boolean functions are juntas. *preprint*, 2002. 14, 21

[38] 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. doi:10.1007/978-3-642-55220-5_36. 2, 4, 9

[39] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977. 4

[40] 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. doi:10.3233/978-1-61499-169-4-249. 2, 4, 9

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

[42] 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. doi:10.1109/FOCS.2008.44. 13

[43] Elchanan Mossel. Gaussian bounds for noise correlation of functions. *Geometric and Functional Analysis*, 19(6):1713–1756, 2010. 13, 14, 16

[44] Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Structures & Algorithms*, 26(4):418–436, 2005. doi:10.1002/rsa.20062. 2, 9

[45] 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, 9

[46] 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. doi:10.1007/978-3-030-64381-2_10. 2, 4, 9

[47] 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. doi:10.1007/978-3-642-32009-5_40. 1

[48] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. 11, 13, 14

[49] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2602–2606. IEEE, 2010. doi:10.1109/ISIT.2010.5513743. 10

[50] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information: Further results. In Alexander Kuleshov, Vladimir M. Blinovsky, and Anthony Ephremides, editors, *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011*, pages 2861–2865. IEEE, 2011. doi:10.1109/ISIT.2011.6034098. 10

[51] Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information with an application to secure two-party sampling. *IEEE Trans. Inf. Theory*, 60(6):3413–3434, 2014. doi:10.1109/TIT.2014.2316011. 10

[52] Alfréd Rényi. On measures of dependence. *Acta mathematica hungarica*, 10(3-4):441–451, 1959. doi:10.1007/BF02024507. 5, 11

[53] Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975. doi:doi.org/10.1137/0128010. 2, 3, 5, 8, 9, 11, 13, 19

[54] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. In Victor Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 467–477. Springer, Heidelberg, August 2005. doi:10.1007/11535218_28. 10

[55] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 222–232. Springer, Heidelberg, May / June 2006. doi:10.1007/11761679_14. 6

[56] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. *IEEE Trans. Inf. Theory*, 54(6):2792–2797, 2008. doi:10.1109/TIT.2008.921674. 10

[57] Aaron Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975. doi:10.1109/TIT.1975.1055346. 2, 3, 8, 9

[58] 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, 9

[59] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd FOCS*, pages 160–164. IEEE Computer Society Press, November 1982. doi:10.1109/SFCS.1982.38. 1

[60] Zi Yin and Youngsuk Park. Hypercontractivity, maximal correlation and non-interactive simulation. 2014. 11, 30, 31

A More on Preliminaries

Proposition 8 (Maximal correlation of a 2-by-2 distribution)**.** *Suppose* $\Omega_x = \Omega_y = \{\pm 1\}$ *and* $\pi(1,1) = a, \pi(1,-1) = b, \pi(-1,1) = c,$ *and* $\pi(-1,-1) = d,$ *where* $0 \leqslant a,b,c,d \leqslant 1$ *and* $a+b+c+d=1$. *The maximal correlation of* (X,Y) *is the following:*

$$\rho = \frac{|ad-bc|}{\sqrt{(a+b)(c+d)(a+c)(b+d)}}.$$

Proof. When $\Omega_x = \Omega_y = \{\pm 1\}$ and $\pi(1,1) = a, \pi(1,-1) = b, \pi(-1,1) = c,$ and $\pi(-1,-1) = d,$ where $0 \leqslant a,b,c,d \leqslant 1$ and $a+b+c+d=1$. Then $\pi_x(1) = a+b, \pi(-1) = c+d,$ $\pi_y(1) = a+c, \pi(-1) = b+d$. For any function $f \in L^p(\{\pm 1\}, \pi_x)$ and $g \in L^p(\{\pm 1\}, \pi_y)$, we have

$$\begin{aligned}
(\mathsf{T}g)(1) &= \frac{a}{a+b}\cdot g(1) + \frac{b}{a+b}\cdot g(-1)\\
(\mathsf{T}g)(-1) &= \frac{c}{c+d}\cdot g(1) + \frac{d}{c+d}\cdot g(-1)\\
(\overline{\mathsf{T}}f)(1) &= \frac{a}{a+c}\cdot f(1) + \frac{c}{a+c}\cdot f(-1)\\
(\overline{\mathsf{T}}f)(-1) &= \frac{b}{b+d}\cdot f(1) + \frac{d}{b+d}\cdot f(-1)
\end{aligned}$$

Note that, in this case, the maximal correlation of (X,Y) is

$$\rho = \frac{|ad-bc|}{\sqrt{(a+b)(c+d)(a+c)(b+d)}}.$$

When $a = d = (1+\gamma)/4$ and $b = c = (1-\gamma)/4$, the operator T is the *Bonami-Beckner operator*, denoted as T_γ. ☐

Lemma 6. *Let* $\{\lambda_i\}_{i=1}^m$ *and* $\{\mu_j\}_{j=1}^n$ *represent respectively the set of all eigenvalues of the real matrices* $A_{m\times m}$ *and* $B_{n\times n}$, *then the set of eigenvalues of* $A \otimes B$ *is* $\{\lambda_i\mu_j\}_{i=1}^m{}_{j=1}^n$. *Moreover, if* v *is an eigenvector of* A *corresponding to eigenvalue* λ *and* w *is an eigenvector of* B *corresponding to eigenvalue* μ, *then* $v \otimes w$ *is an eigenvector of* $A \otimes B$ *corresponding to the eigenvalue* $\lambda \cdot \mu$. *Furthermore, if* $\{v_i\}_{i=1}^p$ *and* $\{w_j\}_{j=1}^q$ *represent respectively a basis for the eigenspace of* A *and* B, *then the set* $\{v_i \otimes w_j\}_{i=1}^p{}_{j=1}^q$ *is a basis of the eigenspace of* $A \otimes B$.

Claim 9 (Contraction Property)**.** *Suppose* T *is a Markov operator. Then, for any function* g, *we have* $\|\mathsf{T}g\|_1 \leqslant \|g\|_1$.

B Examples: Markov operator, adjoint-Markov operator, and Maximal Correlation

Maximal Correlation of BSS: For BSS with noise characteristics ε, we have

$$\mathsf{T} = \overline{\mathsf{T}} = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}.$$

The eigenvalues of $\mathsf{T}\overline{\mathsf{T}}$ are 1 and $(1-2\varepsilon)^2$. Therefore, the maximal correlation of BSS with noise characteristic ε is $\rho = 1-2\varepsilon$ [60].

For BES with erasure probability ε, we have

$$\mathsf{T} = \begin{bmatrix} 1-\varepsilon & \varepsilon & 0 \\ 0 & \varepsilon & 1-\varepsilon \end{bmatrix}, \text{ and } \overline{\mathsf{T}} = \begin{bmatrix} 1 & 0 \\ 1/2 & 1/2 \\ 0 & 1 \end{bmatrix}.$$

The eigenvalues of $\mathsf{T}\overline{\mathsf{T}}$ are 1 and $(1-\varepsilon)$. Therefore, the maximal correlation of BES with erasure probability ε is $\rho = \sqrt{1-\varepsilon}$ [60].

For ROLE, we have

$$\mathsf{T} = \begin{bmatrix} 1/2 & 1/2 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 1/2 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix}, \text{ and } \overline{\mathsf{T}} = \begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 1/2 & 1/2 \end{bmatrix}.$$

The eigenvalues of

$$\mathsf{T}\overline{\mathsf{T}} = \begin{bmatrix} 1/2 & 1/4 & 0 & 1/4 \\ 1/4 & 1/2 & 1/4 & 0 \\ 0 & 1/4 & 1/2 & 1/4 \\ 1/4 & 0 & 1/4 & 1/2 \end{bmatrix}$$

are $1, 1/2, 1/2, 0$. So, the maximal correlation of ROLE is $\sqrt{1/2}$.

C Other Imported Theorems

Imported Theorem 5 (Sequential Composition [34])**.** *For joint distribution P, Q, and R, suppose we have*

$$P \sqsubseteq^{\nu}_{f,g} Q, \text{ and } Q \sqsubseteq^{\nu'}_{f,g} R.$$

Then, the following holds.

$$P \sqsubseteq^{\nu+\nu'}_{f\circ f', g\circ g'} R.$$

Imported Theorem 6 (Projection [34])**.** *Suppose P, Q are two joint distributions. Suppose $P^{\otimes m} \sqsubseteq^{\nu}_{f,g} Q$. Then, it holds that $P \sqsubseteq^{\nu}_{f,g} Q$.*

Derandomization theorem: we had the following two derandomization theorems where the second one is the one that we want to use:

Imported Theorem 7 (Derandomization: Feasibility results[34])**.** *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 $k \in \mathbb{N}$)*

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

Imported Theorem 8 (Derandomization of Reduction Functions[34])**.** *Let (U,V) and (X,Y) be two joint distributions over $\mathcal{U}\times\mathcal{V}$ and $\mathcal{X}\times\mathcal{Y}$ respectively such that (U,V) is a redundancy-free joint distribution. Let $n \in \mathbb{N}$ and $\nu \in [0,1]$. Let R_A and R_B be two random variables defined respectively over $\mathcal{R}_A$ and $\mathcal{R}_B$ such that R_A is independent of both R_B and X^n; R_B is independent of both Y^n and*

R_A. *Suppose there exist randomized reduction functions* $f\colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{U}$, *and* $g\colon \mathcal{Y}^n \times \mathcal{R}_B \to \mathcal{V}$ *such that* $(U,V) \sqsubseteq_{f,g}^{\nu} (X,Y)^{\otimes n}$. *Then, there exists a constant* γ*(which depends on the target distribution* (U,V)*), and (deterministic) reduction functions* $f'\colon \mathcal{X}^n \to \mathcal{U}$, *and* $g'\colon \mathcal{Y}^n \to \mathcal{V}$ *such that:*

1. $(U,V) \sqsubseteq_{f',g'}^{\gamma\nu^{1/4}} (X,Y)^{\otimes n}$.
2. $\mathrm{SD}\left(f(X^n,R_A), f'(X^n)\right) \leqslant \gamma \times \nu^{\frac{1}{4}}$ *and* $\mathrm{SD}\left(g(Y^n,R_B), g'(Y^n)\right) \leqslant \gamma \times \nu^{\frac{1}{4}}$.

D Omitted Proofs

D.1 Proof of Claim 3

Let m be the size the domain Ω. Applying Parseval's identity for function f yields $\sum_{\alpha\in\mathbb{N}_n^{<m}} \widehat{f}(\alpha)^2 = \sum_{i=1}^{n} \mathsf{W}^i[f] = 1$. From the basic formula of total influence, we have

$$\begin{aligned}\mathsf{Inf}[f] &= \sum_{i=1}^{n} i\cdot \mathsf{W}^i[f] \\ &= \sum_{i=1}^{k} i\cdot \mathsf{W}^i[f] + \sum_{i=k+1}^{n} i\cdot \mathsf{W}^i[f] \\ &\leqslant k\cdot \sum_{i=1}^{k} \mathsf{W}^i[f] + n\cdot \sum_{i=k+1}^{n} \mathsf{W}^i[f] \\ &\leqslant k\cdot 1 + n\cdot\delta,\end{aligned}$$

which completes the proof.

D.2 Proof of Claim 6

Note that $\overline{\mathsf{T}}f^*\colon {\Omega_y}^n \to [-1,1]$. We define the function $g^*\colon {\Omega_y}^n \to \{\pm1,0\}$ whose output is achieved by rounding the output of $\overline{\mathsf{T}}f^*$ to the closest value in $\{\pm1,0\}$. Since f^* is a junta it follows that $\overline{\mathsf{T}}f^*$ is also a junta. Note that $\Pr_{y\sim\Omega_y}\left[\left|g(y)-\overline{\mathsf{T}}f^*(y)\right| \geqslant \sqrt{\delta}\right] \leqslant \sqrt{\delta}$ and so $\left\|g^*-\overline{\mathsf{T}}f^*\right\| \leqslant 2\sqrt{\delta}$. Therefore, it follows from triangle inequality that $\left\|g-g^*\right\|_1 \leqslant 2\sqrt{\delta}+\delta \leqslant 3\sqrt{\delta}$.

D.3 Proof of Lemma 1

It suffices to prove the following claim.

Claim 10. *The following equalities hold.*

$$\mathsf{T}\psi_S = \rho^{|S|}\cdot\phi_S, \text{ and } \overline{\mathsf{T}}\phi_S = \rho^{|S|}\cdot\psi_S,$$

where $\rho = \frac{ad-bc}{\sqrt{pq(1-p)(1-q)}}$. *Furthermore, the following equations hold.*

$$\mathsf{T}\overline{\mathsf{T}}\phi_S = \rho^{2|S|}\cdot\phi_S, \text{ and } \overline{\mathsf{T}}\mathsf{T}\psi_S = \rho^{2|S|}\cdot\psi_S.$$

Remark 4. *The quantity* ρ *defined in the above claim has the same magnitude as the maximal correlation of the joint distribution* (X,Y). *When* $ad > bc$, *it is exactly the maximal correlation of* (X,Y). *This result can be viewed as a generalization of equation* $\mathsf{T}_\rho\chi_S = \rho^{|S|}\cdot\chi_S$, *where* T_ρ *is the Bonami-Beckner noise operator, and* $\chi_S\colon \{\pm1\}^n \to \{\pm1\}$ *is the function defined as* $\chi_S = \prod_{i\in S} x_i$ *(a Fourier basis over the uniform measure).*

D.3.1 Proof of Claim 10

In the following expressions, (X^n, Y^n) is always sampled from $\pi^{\otimes n}$. For every $x^n \in \Omega^n$, we have

$$\begin{aligned}
\mathsf{T}\psi_S(x^n) &= \mathbb{E}[\psi_S(Y^n)|X^n = x^n] \\
&= \mathop{\mathbb{E}}_{y^n \sim (Y^n|X^n=x^n)} \prod_{i\in S} \left(\frac{y_i - \mu_y}{\sigma_y}\right) \\
&= \prod_{i\in S} \mathop{\mathbb{E}}_{y_i \sim (Y_i|X_i=x_i)} \left(\frac{y_i - \mu_y}{\sigma_y}\right) \\
&= \prod_{i\in S} \rho \cdot \left(\frac{x_i - \mu_x}{\sigma_x}\right) && \text{(Claim 11)} \\
&= \rho^{|S|}\phi_S(x^n)
\end{aligned}$$

Similarly, we also have $\overline{\mathsf{T}}\phi_S = \rho^{|S|}\psi_S$.

Claim 11. *The following equation holds.*

$$\mathop{\mathbb{E}}_{y_i \sim Y_i|X_i=x_i} \left(\frac{y_i - \mu_y}{\sigma_y}\right) = \rho \cdot \left(\frac{x_i - \mu_x}{\sigma_x}\right)$$

Proof. We do case analysis on x_i.

Case 1: If $x_i = 1$, the left hand side can be simplified as

$$\begin{aligned}
\mathop{\mathbb{E}}_{y_i \sim Y_i|X_i=1} \left(\frac{y_i - \mu_y}{\sigma_y}\right) &= \frac{a}{a+b} \cdot \frac{1-\mu_y}{\sigma_y} + \frac{b}{a+b} \cdot \frac{-1-\mu_y}{\sigma_y} \\
&= \frac{a}{a+b} \cdot \frac{2(b+d)}{2\sqrt{b+d}\sqrt{a+c}} + \frac{b}{a+b} \cdot \frac{-2(a+c)}{\sqrt{b+d}\sqrt{a+c}} \\
&= \frac{ad-bc}{(a+b)\sqrt{b+d}\sqrt{a+c}}
\end{aligned}$$

The right hand side can be rewritten as

$$\begin{aligned}
\rho \cdot \left(\frac{1-\mu_x}{\sigma_x}\right) &= \rho \cdot \frac{2(c+d)}{2\sqrt{a+b}\sqrt{c+d}} \\
&= \frac{ad-bc}{\sqrt{(a+b)(c+d)(a+c)(b+d)}} \cdot \frac{(c+d)}{\sqrt{a+b}\sqrt{c+d}} \\
&= \frac{ad-bc}{(a+b)\sqrt{b+d}\sqrt{a+c}}
\end{aligned}$$

Case 2: If $x_i = -1$, the left hand side can be simplified as

$$\begin{aligned}
\mathop{\mathbb{E}}_{y_i \sim Y_i|X_i=-1} \left(\frac{y_i - \mu_y}{\sigma_y}\right) &= \frac{c}{c+d} \cdot \frac{1-\mu_y}{\sigma_y} + \frac{d}{c+d} \cdot \frac{-1-\mu_y}{\sigma_y} \\
&= \frac{c}{c+d} \cdot \frac{2(b+d)}{2\sqrt{b+d}\sqrt{a+c}} + \frac{d}{c+d} \cdot \frac{-2(a+c)}{\sqrt{b+d}\sqrt{a+c}} \\
&= \frac{bc-ad}{(c+d)\sqrt{b+d}\sqrt{a+c}}
\end{aligned}$$

The right hand side can be rewritten as

$$\begin{aligned}\rho \cdot \left(\frac{-1-\mu_x}{\sigma_x}\right) &= \rho \cdot \frac{-2(a+b)}{2\sqrt{a+b}\sqrt{c+d}} \\ &= \frac{ad-bc}{\sqrt{(a+b)(c+d)(a+c)(b+d)}} \cdot \frac{-(a+b)}{\sqrt{a+b}\sqrt{c+d}} \\ &= \frac{bc-ad}{(c+d)\sqrt{b+d}\sqrt{a+c}}\end{aligned}$$

In both cases, it holds that $\mathbb{E}_{y_i \sim Y_i | X_i = x_i}\left(\frac{y_i-\mu_y}{\sigma_y}\right) = \rho \cdot \left(\frac{x_i-\mu_x}{\sigma_x}\right)$, which completes the first part of the claim.

Next, we prove the second part of the claim.

$$\mathsf{T}\overline{\mathsf{T}}\phi_S = \mathsf{T}(\overline{\mathsf{T}}\phi_S) = \mathsf{T}(\rho^{|S|}\psi_S) = \rho^{|S|} \cdot \mathsf{T}\psi_S = \rho^{|S|} \cdot \rho^{|S|}\psi_S = \rho^{2|S|} \cdot \phi_S$$

Similarly, it also holds that $\overline{\mathsf{T}}\mathsf{T}\psi_S = \rho^{|S|}\phi_S$, which completes the proof. □

D.4 Proof of Theorem 6

By Theorem 2, it holds that $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\|\overline{\mathsf{T}}f - g\right\|_1 \leqslant 4\nu$, and $\|\mathsf{T}g - \rho' f\|_1 \leqslant 4\nu$. Applying triangle inequality for the the last two constraints yields $\left\|\mathsf{T}\overline{\mathsf{T}}f - \rho' f\right\|_1 \leqslant 8\nu$. Now, consider two cases as follows.

Case 1: $\rho^{t+1} < \rho' < \rho^t$ for some $t \in [n]$, then by the first case of Theorem 10,

$$\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 \geqslant \frac{1}{2}\min(({\rho'}^2 - \rho^{2t})^2, ({\rho'}^2 - \rho^{2(t+1)})^2).$$

This implies that the insecurity ν is at least $\frac{1}{16}\min(({\rho'}^2 - \rho^{2t})^2, ({\rho'}^2 - \rho^{2(t+1)})^2)$, which is a constant.

Case 2: $\rho' = \rho^k$ for some $k \in \mathbb{N}$. Then by Theorem 10, there exist degree-k D-junta functions $f^*, g^* \colon \{\pm 1\}^n \to \{\pm 1\}$ such that $f^* \in L^2(\{\pm 1\}, \pi_x)$, $g^* \in L^2(\{\pm 1\}^n, \pi_y)$, and

$$\|f - f^*\|_2^2 \leqslant \sigma_1 + D\sigma_1^{5/4}, \tag{3}$$

$$\|g - g^*\|_2^2 \leqslant \sigma_2 + D\sigma_2^{5/4}, \tag{4}$$

where $\sigma_1 = \frac{2}{(1-\rho^2)^2\rho^{4k}} \cdot \delta_1$ and $\sigma_2 = \frac{2}{(1-\rho^2)^2\rho^{4k}} \cdot \delta_2$, and $\mathsf{W}^k[f^*] \geqslant 1 - \frac{2\delta_1}{(1-\rho^2)^2\rho^{4k}}$, $\mathsf{W}^k[g^*] \geqslant 1 - \frac{2\delta_2}{(1-\rho^2)^2\rho^{4k}}$. Using these facts and triangle inequality, it is easy to see that f^*, g^* witness a statistical SNIS of $\mathsf{BSS}(\rho')$ from $(X,Y)^{\otimes n}$. Next, it follows from Claim 4 that f^*, g^* witness a perfect SNIS of $\mathsf{BSS}(\rho')$ from $(X,Y)^{\otimes n}$, and $\mathsf{W}^k[f^*] = \mathsf{W}^k[g^*] = 1$.

D.5 Proof of Claim 4

Since h is a J-junta function, so does $\overline{\mathsf{T}}h$. Observe that $\overline{\mathsf{T}}h$ is bounded function, that is, $\left|(\overline{\mathsf{T}}h)(x)\right| \leqslant 1$ for every $x \in \{\pm 1\}$. Note that $\rho' \cdot \ell$ is also a bounded J-junta function because ℓ is a Boolean J-junta function and $\rho' \in (0,1)$. Therefore, if $\overline{\mathsf{T}}h \neq \rho' \cdot \ell$, then $\left\|\overline{\mathsf{T}}h - \rho' \cdot \ell\right\|_2$ must be a constant value that depends only on $J, \varepsilon', (X,Y)$.

D.5.1 Proof of Theorem 10.

First, note that $\mathsf{T}\overline{\mathsf{T}}$ is a Markov operator. Since $\left|(\mathsf{T}\overline{\mathsf{T}}f)(x)\right| \leqslant 1$ and $f(x) \in \{\pm 1\}$ for every x, we have

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

It implies that

$$\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_2^2 = \mathop{\mathbb{E}}_x \left[(\mathsf{T}\overline{\mathsf{T}}f)(x) - {\rho'}^2 \cdot f(x)\right]^2 \leqslant 2 \mathop{\mathbb{E}}_x \left|(\mathsf{T}\overline{\mathsf{T}}f)(x) - {\rho'}^2 \cdot f(x)\right| \leqslant 2\delta_1$$

Now, consider 2 cases as follows.

Case 1: If $\rho^{t+1} < \rho' < \rho^t$ for some $t \in [n]$. We have

$$\begin{aligned}
\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_1 &\geqslant \frac{1}{2}\left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_2^2 && \text{(Claim 1)}\\
&= \frac{1}{2}\left\|\mathsf{T}\overline{\mathsf{T}}\left(\sum_{S \subseteq [n]} \widehat{f}(S)\phi_S\right) - {\rho'}^2\left(\sum_{S\subseteq[n]} \widehat{f}(S)\phi_S\right)\right\|_2^2 && \text{(Fourier expansion)}\\
&= \frac{1}{2}\left\|\sum_{S\subseteq[n]} \widehat{f}(S)\left(\mathsf{T}\overline{\mathsf{T}}\phi_S - {\rho'}^2\phi_S\right)\right\|_2^2 && \text{(Linearity of Markov Operator.)}\\
&= \frac{1}{2}\left\|\sum_{S\subseteq[n]} \widehat{f}(S)\left(\rho^{2|S|}\phi_S - {\rho'}^2\phi_S\right)\right\|_2^2 && \text{(Claim 10)}\\
&= \frac{1}{2}\sum_{S\subseteq[n]} (\rho^{2|S|} - {\rho'}^2)^2 \widehat{f}(S)^2 && \text{(Orthonormality of Fourier Basis)}\\
&\geqslant \frac{1}{2}\min(({\rho'}^2 - \rho^{2t})^2, ({\rho'}^2 - \rho^{2(t+1)})^2) \cdot \sum_{S\subseteq[n]} \widehat{f}(S)^2\\
&= \frac{1}{2}\min(({\rho'}^2 - \rho^{2t})^2, (\rho' - \rho^{2(t+1)})^2) && \text{(Parseval)}
\end{aligned}$$

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

$$\begin{aligned}
\sum_{S\colon |S|\neq k} (\rho^{2(k+1)} - \rho^{2k})^2 \widehat{f}(S)^2 &\leqslant \sum_{S\colon |S|\neq k} (\rho^{2|S|} - \rho^{2k})^2 \widehat{f}(S)^2\\
&= \sum_{S\subseteq[n]} (\rho^{2|S|} - \rho^{2k})^2 \widehat{f}(S)^2\\
&= \left\|\mathsf{T}\overline{\mathsf{T}}f - {\rho'}^2 f\right\|_2^2\\
&\leqslant 2\delta_1.
\end{aligned}$$

This implies that $\mathsf{W}^{\neq k}[f] = \sum_{S\colon |S|\neq k} \widehat{f}(S)^2 \leqslant \frac{2\delta_1}{(1-\rho^2)^2\rho^{4k}}$, as desired. Similarly, it also holds that $\mathsf{W}^{\neq k}[g] \leqslant \frac{2\delta_2}{(1-\rho^2)^2\rho^{4k}}$. Finally, by Imported Theorem 3, there exist Boolean degree-k D-junta functions $\tilde{f}, \tilde{g}\colon \{\pm1\}^n \to \{\pm 1\}$ such that $\left\|f - \tilde{f}\right\|_2^2 \leqslant \sigma_1 + D\sigma_1^{5/4}$, and $\|g - \tilde{g}\|_2^2 \leqslant \sigma_2 + D\sigma_2^{5/4}$, where $\sigma_1 = \frac{2}{(1-\rho^2)^2\rho^{4k}} \cdot \delta_1$ and $\sigma_2 = \frac{2}{(1-\rho^2)^2\rho^{4k}} \cdot \delta_2$, which completes the proof.

D.6 Proof of Claim 8

Let $\chi_S(x) = \prod_{i\in S} x_i$ be the Fourier basis of $L^2(\{\pm 1\}^n, {\pi_{1/2}}^{\otimes n})$. Let $\phi_S(x) = \prod_{i\in S}\left(\frac{x_i-\mu}{\sigma}\right)$ be the Fourier basis of $L^2(\{\pm 1\}^n, {\pi_p}^{\otimes n})$. We use these two bases to express the same function f in two different ways. Since $\mathsf{W}^{\leqslant k}[f^{(p)}] = 1$, we have $\widehat{f^{(p)}}(S) = 0$ when $|S| > k$. Therefore, we have the following:

$$f(x) = f^{(p)}(x) = \sum_{|S|\leqslant k} \widehat{f^{(p)}}(S) \prod_{i\in S}\left(\frac{x_i - \mu}{\sigma}\right)$$

$$f(x) = f^{(1/2)}(x) = \sum_{S\subseteq[n]} \widehat{f^{(1/2)}}(S) \prod_{i\in S} x_i$$

This implies that $\widehat{f^{(1/2)}}(S) = \frac{1}{\sigma^k}\widehat{f^{(p)}}(S)$ for every $S \subseteq [n]$ such that $|S| = k$. Therefore, we complete the proof by

$$\mathsf{W}^k[f^{(1/2)}] = \sum_{|S|=k} \widehat{f^{(1/2)}}(S)^2 = \frac{1}{\sigma^{2k}} \sum_{|S|=k} \widehat{f^{(p)}}(S)^2 = \frac{1}{\sigma^{2k}}\mathsf{W}^k[f^{(p)}].$$

E New Constructions

E.1 SNIS of BSS from a 3-by-3 distribution

		$v=+1$	$v=-1$	
		0	1	2
$u=+1$	0	3/8	1/12	1/24
$u=-1$	1	1/12	3/16	1/16
	2	1/24	1/16	1/16

Table 1: SNIS of $\mathsf{BSS}(\varepsilon' = 1/4)$ from one sample of a distribution (X, Y) over $\mathcal{X} \times \mathcal{Y}$ where $|\mathcal{X}| = |\mathcal{Y}| = 3$.

Suppose Alice has (a_1, b_1) and (a_2, b_2), and Bob has (c_1, d_1) and (c_2, d_2) such that $d_i = a_i c_i \oplus b_i$. We are using bit representation $\{0, 1\}$.

E.2 SNIS of BSS from a 4-by-4 distribution

Let (X, Y) be the the distribution with the following probability mass distribution. One can verify

a	b	c	d
b	a	d	c
c	d	a	b
d	c	b	a

Table 2: A 4-by-4 distribution, where $a, b, c, d \geqslant 0$ and $a + b + c + d = 1/4$

that the above matrix has four eigenvalues $\lambda_1 = 1, \lambda_2 = a + b - c - d, \lambda_3 = a + c - b - d, \lambda_4 = a+d-b-c$ with associated eigenvectors $v_1 = (1, 1, 1, 1), v_2 = (1, 1, -1, -1), v_3 = (1, -1, 1, -1), v_4 = (1, -1, -1, 1)$, respectively.

Claim 12. *There is a perfect SNIS of* $\mathsf{BSS}(\varepsilon')$ *from one sample of* (X, Y) *if and only if* $\rho' = \lambda_i$ *for some* $i \in \{2, 3, 4\}$*, where* $\rho' = 1 - 2\varepsilon'$*.*

Proof. The forward direction follows from Theorem 11. For the backward direction, suppose $\rho' = \lambda_i$, one can verify that the reduction functions $f = g = v_i$ witness a perfect construction. □

We can generalize this as follows.

Claim 13. *There is a perfect SNIS of* $\mathsf{BSS}(\varepsilon')$ *from* n *samples of* (X, Y) *if and only if* $\rho' = \prod_{i=1}^{4} \lambda_i^{t_i}$*, where* $\rho' = 1 - 2\varepsilon'$*, and* $\sum_{i=1}^{4} t_i = n$*.*

This claim follows from parallel and sequential compositions theorems.

E.3 SNIS of BSS from ROLE

Non-linear constructions. We list 4 constructions (following ROLE notation) found by exhaustive search.

$$
\begin{aligned}
f_1(a_1, b_1, a_2, b_2) &= 0.5(-1 - (-1)^{a_1} - (-1)^{a_2} + (-1)^{a_1+a_2})(-1)^{b1+b2} \\
g_1(c_1, d_1, c_2, d_2) &= 0.5(-1 - (-1)^{c_1} - (-1)^{c_2} + (-1)^{c_1+c_2})(-1)^{d_1+d_2} \\
f_2(a_1, b_1, a_2, b_2) &= 0.5(-1 - (-1)^{a_1} + (-1)^{a_2} - (-1)^{a_1+a_2})(-1)^{b_1+b_2} \\
g_2(c_1, d_1, c_2, d_2) &= 0.5(-1 + (-1)^{c_1} - (-1)^{c_2} - (-1)^{c_1+c_2})(-1)^{d_1+d_2} \\
f_3(a_1, b_1, a_2, b_2) &= 0.5(-1 + (-1)^{a_1} - (-1)^{a_2} - (-1)^{a_1+a_2})(-1)^{b_1+b_2} \\
g_3(c_1, d_1, c_2, d_2) &= 0.5(-1 - (-1)^{c_1} + (-1)^{c_2} - (-1)^{c_1+c_2})(-1)^{d_1+d_2} \\
f_4(a_1, b_1, a_2, b_2) &= 0.5(+1 - (-1)^{a_1} - (-1)^{a_2} - (-1)^{a_1+a_2})(-1)^{b_1+b_2} \\
g4(c_1, d_1, c_2, d_2) &= 0.5(-1 + (-1)^{c_1} + (-1)^{c_2} + (-1)^{c_1+c_2})(-1)^{d_1+d_2}
\end{aligned}
$$

Observe that if a pair of reduction functions (f, g) witnesses secure construction, so does $(f, -g), (-f, g)$, or $(-f, -g)$. Thus, there are 16 perfect SNIS constructions of $\mathsf{BSS}(1/2)$ from bit ROLE in total.

No linear construction exists. We show that there does not exist any linear construction of BSS from ROLE.

Definition 9 (Linear Construction)**.** *We say that there is a linear SNIS of* $\mathsf{BSS}(\varepsilon)$ *from* ROLE *if there exist reduction functions* $f, g\colon \{00, 01, 10, 11\}^n \to \{\pm 1\}$ *such that* $\mathsf{BSS}(\varepsilon) \sqsubseteq_{f,g}^{0} \mathsf{ROLE}^{\otimes n}$ *and at least one of the four sets*

$$f^{-1}(+1), f^{-1}(1), g^{-1}(+1), g^{-1}(-1)$$

is a vector space over $\{0, 1\}$*, where the probability mass distribution of* ROLE *is one the two following matrices corresponding to two different namings.*

$$
\begin{bmatrix} 1/2 & 0 & 1/2 & 0 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 1/2 & 0 & 1/2 \end{bmatrix} \quad or \quad \begin{bmatrix} 1/2 & 0 & 1/2 & 0 \\ 0 & 1/2 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{bmatrix}
$$

Reduction. Without loss of generality, we can change to the reduction function $f, g\colon \{+1+1, +1-1, -1+1, -1-1\}^n \to \{\pm 1\}$. So f, g witness a linear construction if $\mathsf{BSS}(\varepsilon) \sqsubseteq^0_{f,g} \mathsf{ROLE}^{\otimes n}$ and at least one of the four sets $f^{-1}(+1), f^{-1}(1), g^{-1}(+1), g^{-1}(-1)$ is a vector space over $\{\pm 1\}$. Here a set $V \subseteq \{\pm 1\}^{2n}$ is a vector space if it is close under coordinate-wise multiplication.

Claim 14. *Reduction functions $f, g\colon \{\pm 1\}^{2n} \to \{\pm 1\}$ witness a linear SNIS of $\mathsf{BSS}(\varepsilon)$ from $\mathsf{ROLE}^{\otimes n}$ if and only if $f = \chi_S$ or $g = \chi_S$ for some $S \subseteq [n]$, where $\chi_S(x) = \prod_{i \in S} x_i$.*

Proof. W.L.O.G, suppose $f^{-1}(+1)$ is a vector space. It follows from the algebraic definition of SNIS that f must be a balanced function. This implies that $f^{-1}(+1)$ is a vector space of dimension $2n-1$ of $\{\pm 1\}^{2n}$, and $f^{-1}(-1)$ is its coset. It is easy to see that f must be a non-zero character χ_S for some S. □

There will be $4! = 24$ different ways of naming the ROLE distribution, each of them corresponds to a permutation of rows of the following matrix.

$$\mathsf{ROLE} = \begin{bmatrix} 1/2 & 0 & 1/2 & 0 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 1/2 & 0 & 1/2 \end{bmatrix}$$

Using the claim above, we can see that linear function f or g (in the vector form) is the tensorization of the following basis functions (vectors) $e_0, e_1, e_2, e_3, : \{\pm 1\}^2 \to \{\pm 1\}$.

$$e_0(x) = 1,\ e_1 = x_1,\ e_2(x) = x_2,\ e_3(x) = x_1 \cdot x_2.$$

Note that in the vector form $e_1 = [1, 1, -1, -1]^T, e_2 = [1, -1, 1, -1]^T, e_3 = [1, -1, -1, 1]^T$. Let r_1, r_2, r_3, r_4 be the rows of ROLE. Observe that

$$\begin{aligned} r_1 \cdot e_1 = 0, r_1 \cdot e_2 = 1, r_1 \cdot e_3 = 0 \\ r_2 \cdot e_1 = 0, r_2 \cdot e_2 = 0, r_2 \cdot e_3 = 1 \\ r_3 \cdot e_1 = 0, r_3 \cdot e_2 = 0, r_3 \cdot e_3 = -1 \\ r_4 \cdot e_1 = 0, r_4 \cdot e_2 = -1, r_4 \cdot e_3 = 0 \end{aligned}$$

Suppose g is a linear function. Let p be a permutation of $\{1, 2, 3, 4\}$. Let ROLE_p be the matrix obtained by permuting the rows of ROLE according to p. Let T and $\overline{\mathsf{T}}$ be the Markov and associated Markov operators of ROLE_p. Since T is a Markov matrix, $\mathsf{T}e_0 = e_0$. From the observation above, it is easy to see that $\mathsf{T}e_1 = [0, 0, 0, 0]^T$, and both vectors $\mathsf{T}e_2$ and $\mathsf{T}e_3$ satisfy that two coordinates of them are 0, one coordinate is 1, and the other is -1. This together with g is $\{\pm 1\}$-valued function imply that for any non-constant linear function g, at least half of the coordinates of the vector $\mathsf{T}f$ are 0. Therefore, $\|\mathsf{T}g - \rho' f\|_1 \geqslant \frac{1}{2} \cdot \frac{1}{2} = 1/4$. Similarly, one can argue that if f is a linear function, then $\left\|\overline{\mathsf{T}}f - \rho' g\right\|_1 \geqslant 1/4$. The proof for BES is similar.

E.4 SNIS of BES from ROLE

In this subsection, we present a SNIS simulation of $\mathsf{BES}(\sqrt{1/2})$ from ROLE (ROLE) with rate 1. Suppose Alice is given $(a, b) \in \{0, 1\}^2$ and Bob is given $(c, d) \in \{0, 1\}^2$ where (a, b) and (c, d) is a sample of ROLE construction. Then, the reduction function of Alice is $f(a, b) = (-1)^b$ and the reduction function of Bob is $g(c, d) = \frac{((-1)^c + 1)(-1)^d}{2}$.

E.5 On the In-completeness of String-ROT Distributions

This section shows that even the family of string-ROT is not complete in SNIS.

Claim 15. *For any $\ell \in \mathbb{N}$, it holds that $\rho_m(ROT(\ell)) = \frac{1}{\sqrt{2}}$.*

To prove this claim, it suffices this to prove the following result.

Claim 16. *Let T and $\overline{\mathsf{T}}$ be the Markov and assosiated Markov's operator of $ROT(\ell)$, respectively. Let $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_{2L}$ be the eigenvalues of the matrix $\overline{\mathsf{T}} \cdot \mathsf{T}$, where $L = 2^\ell$. Then, it holds that $\lambda_1 = 1, \lambda_{2L} = 0$ and $\lambda_i = 1/2$ for every $1 < i < 2L$.*

Proof. Let I_n denote the $n \times n$ identity matrix. Let $\mathsf{1}_n$ denote the $n \times n$ matrix with all one entries. First, note that $\overline{\mathsf{T}} \cdot \mathsf{T}$ is a $2L \times 2L$ square matrix. One can verify that

$$\overline{\mathsf{T}} \cdot \mathsf{T} = \left[\begin{array}{c|c} (1/2) \cdot I_L & (1/2L) \cdot \mathsf{1}_L \\ \hline (1/2L) \cdot \mathsf{1}_L & (1/2) \cdot I_L \end{array}\right]$$

Then, Claim 16 follows from basic algebra. □