Decidability of Secure Non-interactive Simulation of Doubly Symmetric Binary Source

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

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

Abstract

Noise, which cannot be eliminated or controlled by parties, is an incredible facilitator of cryptography. For example, highly efficient secure computation protocols based on independent samples from the doubly symmetric binary source (BSS) are known. A modular technique of extending these protocols to diverse forms of other noise without any loss of round and communication complexity is the following strategy. Parties, beginning with multiple samples from an arbitrary noise source, non-interactively, albeit securely, simulate the BSS samples. After that, they can use custom-designed efficient multi-party solutions using these BSS samples.

Khorasgani, Maji, and Nguyen (EPRINT–2020) introduce the notion of secure non-interactive simulation (SNIS) as a natural cryptographic extension of concepts like non-interactive simulation and non-interactive correlation distillation in theoretical computer science and information theory. In SNIS, the parties apply local reduction functions to their samples to produce samples of another distribution. This work studies the decidability problem of whether samples from the noise (X, Y) can securely and non-interactively simulate BSS samples. As is standard in analyzing non-interactive simulations, our work relies on Fourier-analytic techniques to approach this decidability problem. Our work begins by algebraizing the simulation-based security definition of SNIS. Using this algebraized definition of security, we analyze the properties of the Fourier spectrum of the reduction functions.

Given (X, Y) and BSS with noise parameter ε, the objective is to distinguish between the following two cases. (A) Does there exist a SNIS from $\mathsf{BSS}(\varepsilon)$ to (X, Y) with δ-insecurity? (B) Do all SNIS from $\mathsf{BSS}(\varepsilon)$ to (X, Y) incur δ'-insecurity, where $\delta' > \delta$? We prove that there is a bounded computable time algorithm achieving this objective for the following cases. (1) $\delta = \mathcal{O}(1/n)$ and $\delta' =$ positive constant, and (2) $\delta =$ positive constant, and $\delta' =$ another (larger) positive constant. We also prove that $\delta = 0$ is achievable only when (X, Y) is another BSS, where (X, Y) is an arbitrary distribution over $\{-1, 1\} \times \{-1, 1\}$. Furthermore, given (X, Y), we provide a sufficient test determining if simulating BSS samples incurs a constant-insecurity, irrespective of the number of samples of (X, Y).

Handling the security of the reductions in Fourier analysis presents unique challenges because the interaction of these analytical techniques with security is unexplored. Our technical approach diverges significantly from existing approaches to the decidability problem of (insecure) non-interactive reductions to develop analysis pathways that preserve security. Consequently, our work shows a new concentration of the Fourier spectrum of secure reduction functions, unlike their insecure counterparts. We show that nearly the entire weight of secure reduction functions' spectrum is concentrated on the lower-degree components. The authors believe that examining existing analytical techniques through the facet of security and developing new analysis methodologies respecting security is of independent and broader interest.

Contents

1 Introduction

Noise, which cannot be eliminated or controlled by parties, is an incredible facilitator of cryptography. Using interaction and private independent randomness, mutually distrusting parties can leverage such *correlated noise* to compute securely over their private data. For example, Rabin [44, 45] and Crépeau [9] constructed *general secure computation* [53, 23] protocols from erasure channels. Such correlated noise seems necessary for secure computation because it is impossible that shared randomness alone can enable general secure multi-party computation [20, 35, 36]. Crépeau and Kilian [10, 11] proved that samples from noisy channels, particularly the *binary symmetric channels*, suffice for general secure computation. After that, a significant body of highly influential research demonstrated the feasibility of realizing general secure computation from diverse and unreliable noise sources [30, 31, 13, 32, 12, 49, 50, 29, 7]. In particular, random samples from these noisy channels suffice for general secure computation while incurring a small increase in round and communication complexity [48].

There are highly efficient secure computation protocols from the correlated samples of the *doubly symmetric binary source*. A doubly symmetric binary source with parameter ε, represented by $\mathsf{BSS}(\varepsilon)$, provides the first party independent and uniformly random elements $x_1, \ldots, x_n \in \{-1, 1\}$. For every $i \in \{1, \ldots, n\}$, the second party gets a correlated $y_i \in \{-1, 1\}$ such that $y_i = x_i$ with probability $(1 - \varepsilon)$; otherwise, $y_i = -x_i$ with probability ε. These protocols efficiently use these samples (vis-à-vis, the number of samples required to compute an arbitrary circuit of fixed size securely) and have a small round and communication complexity [32, 48, 26, 25]. A modular technique of extending these protocols to diverse forms of other noise without any loss of round and communication complexity is the following strategy. Parties begin with multiple samples of an arbitrary noise source (X, Y), and they securely convert them into samples of $(U, V) = \mathsf{BSS}(\varepsilon)$ without any interaction, a.k.a., secure non-interactive simulation [28].[1]

Secure non-interactive simulation. Khorasgani, Maji, and Nguyen [28] introduced the notion of *secure non-interactive simulation* (SNIS) of joint distributions. The high-level objective of this cryptographic primitive is to *non-interactively* and *securely* simulate samples from a distribution (U, V) when the parties already have multiple independent samples from another distribution (X, Y). This cryptographic primitive is a natural cryptographic extension of highly influential concepts in theoretical computer science and information theory, like, non-interactive simulation (beginning with the seminal works of Gács and Körner [18], Witsenhausen [47], and Wyner [51]), and non-interactive correlation distillation [42, 40, 52, 4, 8]. This primitive is also a constrained version of one-way secure computation [19, 1], allowing no interaction between the parties. The sequel succinctly presents the intuition underlying this concept (for a formal simulation-based definition, refer to Appendix E).

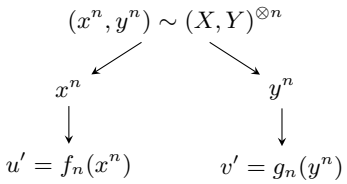

Figure 1: SNIS model.

Refer to Figure 1 for the following discussion. Let (X, Y) be a joint distribution over the sample space $\mathcal{X} \times \mathcal{Y}$. The system samples n independent samples drawn according to the distribution (X, Y). That is, $(x^n, y^n) \sim (X, Y)^{\otimes n}$. The system delivers the samples x^n to Alice and y^n to Bob. Alice applies a local *reduction function* $f_n \colon \mathcal{X}^n \to \mathcal{U}$ to her sample $x^n \in \mathcal{X}^n$ and outputs $u' = f_n(x^n)$. Similarly, Bob applies a local reduction function $g_n \colon \mathcal{Y}^n \to \mathcal{V}$ to his sample $y^n \in \mathcal{Y}^n$ and outputs $v' = g_n(y^n)$.

The case of private randomness. The definition of SNIS allows private randomness for the

[1] One can determine the noise characteristic of the BSS samples after gathering the samples of (X, Y).

parties. However one can assume that the reduction functions are deterministic, without loss of generality. The original work of [28] introduced a derandomization that is sample preserving.[2] This derandomization, however, increases the insecurity of the deterministic reduction to $\delta^{1/9}$, if the randomized reduction has insecurity δ. Some of our results shall rely on this derandomization result. However, for some of our applications we develop a new derandomization technique to obtain better results. This new derandomization result takes additional samples to securely and non-interactively simulate the private independent randomness of both parties (refer to Appendix F).[3] Henceforth, we assume that the reduction functions are deterministic, without loss of generality.

Intuitive definition. There exists a *secure non-interactive joint simulation (SNIS) of* (U, V) *from* (X, Y) *with insecurity tolerance* $\delta \in [0, 1]$ [28] if the following three conditions are satisfied.

1. The *correctness* of the non-interactive simulation ensures that the distribution of the joint samples (u', v') when $(x^n, y^n) \sim (X, Y)^{\otimes n}$ is δ-close to the distribution (U, V) (in the statistical distance).
2. The *security against an adversarial Alice* insists that there exists a (randomized) function $\mathrm{Sim}_A \colon \mathcal{U} \to \mathcal{X}^n$ such that the joint distribution $(X^n, f_n(X^n), g_n(Y^n))$ is δ-close to the joint distribution $(\mathrm{Sim}_A(U), U, V)$.
3. Similarly, the *security against an adversarial Bob* insists that there exists a function $\mathrm{Sim}_B \colon \mathcal{V} \to \mathcal{Y}^n$ such that the joint distribution $(f_n(X^n), g_n(Y^n), Y^n)$ is δ-close to the joint distribution $(U, V, \mathrm{Sim}_B(V))$.

Tersely, one represents this secure reduction as $(U, V) \sqsubseteq^{\delta}_{f_n, g_n} (X, Y)^{\otimes n}$. The general decidability problem of whether (U, V) reduces to $(X, Y)^{\otimes n}$ within a particular tolerance of insecurity remains unresolved (even for the gap-version).

Problem statement. In general, given two noise sources (X, Y) and (U, V), one needs to determine whether there exists a secure non-interactive simulation of (U, V) samples from the samples of (X, Y). More formally, given the source distribution (X, Y), the target distribution (U, V), and an insecurity tolerance $\delta \in [0, 1]$, does there exist $n \in \mathbb{N}$ and reduction functions f_n and g_n witnessing a secure non-interactive reduction? Our work studies this decidability problem (referred to as *decidability of SNIS*) specifically for the case where $(U, V) = \mathsf{BSS}(\varepsilon)$. The similar decidability problem for the (insecure) non-interactive reduction was extraordinarily challenging and was resolved only recently [22]. Consequently, exploring the particular case of $(U, V) = \mathsf{BSS}$ while simultaneously studying the (previously unexplored) interplay of Fourier-analytic techniques with security is already a complex undertaking.

Relation to the decidability of non-interactive simulation. Starting with the seminal works of Gács and Körner [18], Witsenhausen [47], and Wyner [51], deciding whether non-interactive simulation (NIS) of (U, V) using (X, Y) is possible or not has been a challenging problem. Only recently, progress on the decidability of (the gap-version of) the general problem was made [22, 14, 21].

Our decidability problem studies the general decidability of non-interactive simulation with the additional constraint of security. There is no outright evidence of whether our decidability problem reduces to this existing literature. In particular, the tests of [22] do not extend to the decidability

[2] If randomized reduction functions take n samples of (X, Y) as input to produce $m(n)$ samples of (U, V), then there are deterministic random functions that take n samples of (X, Y) as input and output $m(n)$ samples of (U, V).

[3] The idea of this derandomization result is the following. Assume that $(X|Y)$ has average min-entropy. Alice can use some samples to perform a suitably long random walk on an appropriate expander graph to deterministically extract the average min-entropy of $(X|Y)$ to generate her private randomness. Even the existence of such a graph suffices to demonstrate the existence of the deterministic reduction. Similarly, Bob uses some other samples to extract his private randomness.

of SNIS because they rely on generating samples from correlated Gaussians, which is insecure (see Appendix D for a discussion). This technical challenge requires our approach to diverge from the existing literature on non-interactive simulation's decidability [22, 14, 21]. Our work proves a concentration of the Fourier spectrum specific to secure reductions, distinguishing them from their insecure counterparts. The authors believe that examining existing analytical techniques through the facet of security and developing new analysis methodologies respecting security is of independent and broader interest. The specific problem of SNIS, owing to its significant similarity with (insecure) non-interactive simulation, is an appropriate representative target application to develop this analytic toolkit for secure constructions.

Comparison with [28]. Both our work and [28] consider (statistical) SNIS. However, there is a slight difference in the scope of the problems, and the techniques that these papers use. [28] considers the feasibility and rate characterization when (X, Y) and (U, V) are both noises from binary symmetric or erasure sources. Our work considers (the gap-decidability of) the feasibility problems pertaining to (U, V) being a binary symmetric noise source and (X, Y) can be an *arbitrary distribution*, which makes the analysis significantly challenging. For example, our work relies on the use of Markov operators, Efron-Stein (orthogonal) decomposition, and Junta theorems in addition to the Fourier analysis over general domains. [28] relies on Fourier analysis over the Boolean hypercube. Since our work does not consider rate, for some of our results, we employ a different derandomization of SNIS that does not degrade the security significantly. The derandomization of [28] emphasized preserving the sampling complexity, i.e., the number of samples of (X, Y) used in the derandomized reductions is identical to the number of samples before derandomization. Furthermore, similar to [28], we discover a Fourier concentration result as well. However, in our case, the spectrum of secure reductions is concentrated on lower weights (rather than exactly one weight, as in [28]).

1.1 Our Contribution

Our paper algebraizes the simulation-based security definition of SNIS to enable the algebraic treatment of our problem (refer to Claim 1). This algebraization ensures that the insecurity of simulation-secure SNIS is a two-factor approximation of the insecurity of algebraic-secure SNIS. For example, perfectly simulation-secure SNIS remains perfectly algebraic-secure SNIS, and statistically simulation-secure SNIS remains statistically algebraic-secure SNIS. In the sequel, consequently, we rely only on the algebraic definition of security.

Our results prove the feasibility to distinguish whether a SNIS with δ-insecurity exists or any SNIS must be δ'-insecure, where $\delta' > \delta$. That is, we solve the *gap-version* of the decidability problem, similar to the literature of decidability in NIS [22, 14, 21]. This gap is inherent to this area's technical tools (see, for example, the discussion in [14]).

Result I. A distribution is redundancy-free if both its marginal distributions have full support. We say that (X, Y) is a 2-by-2 distribution, if $\mathrm{Supp}(X) = \mathrm{Supp}(Y) = 2$. Unless specified, a *general* distribution (X, Y) has arbitrary support-size (even $\mathrm{Supp}(X) \neq \mathrm{Supp}(Y)$ is permitted).

Informal Theorem 1. *Given a redundancy-free general distribution (X, Y) and $(U, V) = \mathsf{BSS}(\varepsilon')$, we prove that there is a bounded computable time algorithm that distinguishes between the following two cases, for any positive constants α and β.*

1. *$\mathsf{BSS}(\varepsilon')$ reduces to $(X, Y)^{\otimes n}$ with $\delta_n \leq \alpha/n$ insecurity.*
2. *Any reduction of $\mathsf{BSS}(\varepsilon')$ to $(X, Y)^*$ has $\delta \geq \beta$ insecurity.*

[25] present techniques of using $\mathsf{BSS}(\varepsilon')$ samples that have constant β^* insecurity into (fully-secure) secure computation protocols. This result helps identify whether samples from the source (X, Y) can produce BSS samples below the constant β^* insecurity tolerance threshold of the [25]'s

protocol. If the insecurity of the $\mathsf{BSS}(\varepsilon')$ is at most α^*/n, then they can use a more efficient protocol of [25].

Typically, in cryptography, one insists on δ_n being negligible in n. Our result applies even for the case of $\delta_n = \mathcal{O}(1/n)$ insecurity as well. It is instructive to remind the reader that our result *does not* imply that either $\mathsf{BSS}(\varepsilon')$ reduces to (X, Y) with $\mathcal{O}(1/n)$-insecurity, or this reduction must incur constant insecurity. Our result states that it is possible to distinguish these two cases (we solve a promise problem). Theorem 6 presents the formal restatement of this result.

Furthermore, we prove that certain distributions (X, Y) can yield a SNIS to $\mathsf{BSS}(\varepsilon')$ only with constant-insecurity. The following result is a corollary of (the technical) Informal Theorem 4 discussed later in this section.

Corollary 1. *For any $\varepsilon' \in (0, \frac{1}{2})$, any $\rho \in [0, 1]$, and any 2-by-2 joint distribution (X, Y) of maximal correlation[4] ρ, the insecurity of any protocol for non-interactive secure simulation of $\mathsf{BSS}(\varepsilon')$ from (X, Y) using arbitrary number of independent samples is at least*

$$\frac{1}{4} \min\left(\left((1-2\varepsilon')^2 - \rho^{2k} \right)^2, \left((1-2\varepsilon')^2 - \rho^{2(k+1)} \right)^2 \right),$$

where $k \in \mathbb{N}$ such that $\rho^k \geq (1-2\varepsilon') > \rho^{k+1}$.

Observe that our result states that even using many samples of (X, Y) does not help securely realize $\mathsf{BSS}(\varepsilon')$ with statistically small insecurity. This result demonstrates the power of interaction in secure computation protocols because samples from any complete [32] (X, Y) can securely realize samples from $\mathsf{BSS}(\varepsilon')$ using an interactive protocol.

A similar phenomenon, where a functionality incurs constant insecurity irrespective of the protocol's complexity, occurs in other characterization problems in cryptography. For example, functions like the Kushilevitz function [34] or the oblivious transfer functionality [16] incur constant insecurity [37, 27] irrespective of the round or communication complexity of the secure computation protocol.

Result II. If one is interested in perfectly secure SNIS, then we prove that (X, Y) must be $\mathsf{BSS}(\varepsilon)$, such that $(1-2\varepsilon)^k = (1-2\varepsilon')$, where $k \in \mathbb{N}$ and (X, Y) is a joint distribution over $\{-1, 1\} \times \{-1, 1\}$.

Informal Theorem 2. *If a perfectly secure SNIS of $\mathsf{BSS}(\varepsilon')$ from a 2-by-2 joint distribution (X, Y) exists, then (X, Y) must be $\mathsf{BSS}(\varepsilon)$ and $(1-2\varepsilon') = (1-2\varepsilon)^k$, for some $k \in \mathbb{N}$.*

[28] proved a restricted version of this result. They show that if $(X, Y) = \mathsf{BSS}(\varepsilon)$, then $(1-2\varepsilon)^k = (1-2\varepsilon')$, and the parity reduction realizes the SNIS. Theorem 1 formally restates this informal theorem.

Result III. We know that efficiently general secure computation can be founded on (sufficiently small) constant-insecure samples of $\mathsf{BSS}(\varepsilon')$, see, for example, [25]. So, it suffices to realize $\mathsf{BSS}(\varepsilon')$ securely with constant insecurity. Towards this objective, we demonstrate that it is possible to distinguish whether $\mathsf{BSS}(\varepsilon')$ reduces to $(X, Y)^n$ with δ-insecurity, where δ is a constant, or any SNIS of $\mathsf{BSS}(\varepsilon')$ from $(X, Y)^*$ is $c \cdot \delta$-insecure, where $c > 1$ is a constant depending on (X, Y) and ε'.

Informal Theorem 3. *Given a 2-by-2 redundancy-free distribution (X, Y) and $(U, V) = \mathsf{BSS}(\varepsilon')$, we prove that there is a bounded computable time algorithm that distinguishes between the following two cases, for any positive constant α.*

[4] The maximal correlation of (X, Y) is defined in Section 2.4 and is efficiently computable.

1. $\mathsf{BSS}(\varepsilon')$ *reduces to* $(X,Y)^{\otimes n}$ *with* $\delta \leq \alpha$ *insecurity.*
2. *Any reduction of* $\mathsf{BSS}(\varepsilon')$ *to* $(X,Y)^n$ *has insecurity* $\delta > c \cdot \alpha$ *insecurity.*

We emphasize that the constant c depends on the distribution (X,Y) and the noise parameter ε'. We remind the reader that $c \cdot \delta$ must be less than one; otherwise, item 2 above is always false. Theorem 4 is the formal restatement of this result.

1.2 Technical Contribution

We summarize two technical tools that are central to most of the results presented above. The authors think that these results highlighting analytical properties of cryptographically secure constructions are of independent and broader interest. First, we prove a necessary condition for SNIS of $\mathsf{BSS}(\varepsilon')$ from $(X,Y)^*$ with $\delta \to 0$ insecurity.

Informal Theorem 4. *Let* (X,Y) *be a 2-by-2 redundancy-free joint distribution with maximal correlation* ρ *and* $\mathsf{BSS}(\varepsilon')$*, where* $\varepsilon' \in (0, \frac{1}{2})$*, reduces to* $(X,Y)^{\otimes n}$ *with* $\delta_n \to 0$ *insecurity, then* $(1-2\varepsilon') = \rho^k$*, for some* $k \in \mathbb{N}$*.*

We emphasize that this test is not sufficient. Corollary 1, presented above, is a consequence of this result (formally restated as Theorem 3).

Finally, we prove a concentration of the Fourier spectrum for secure reductions.

Informal Theorem 5. *Let* (X,Y) *be a general joint distribution with maximal correlation* ρ *and* $\mathsf{BSS}(\varepsilon')$ *reduces to* $(X,Y)^{\otimes n}$ *with (any)* δ_n *insecurity via reduction functions* f_n *and* g_n*. Then, for some* $k \in \mathbb{N}$*, and the Fourier weight of both* f_n *and* g_n *on degrees* $> k$ *is at most* $c \cdot \delta_n$*.*

The constant c above depends on the maximal correlation ρ and the noise parameter ε'. Furthermore, we clarify that the Fourier weight of f_n and g_n is with respect to their input distributions being the marginal distributions X^n and Y^n, respectively. Our work extends the Fourier concentration property to the much more general case, that is, when the source is an arbitrary distribution and the target is a BSS, which requires biased Fourier analysis over larger alphabet set. The connection between secure simulation and the Fourier concentration is surprising and new. We show that the Fourier spectrum is concentrated on lower order terms. In particular, when the source is a 2-by-2 distribution, it is concentrated on one degree. This generalizes one of the Fourier concentration results of [28].

We use this result (Theorem 2 restates the formal version) to highlight how our technical approach diverges from the techniques of [22, 14, 21] for NIS-decidability. In NIS-decidability, [22, 14, 21] rely on the invariance principle [39] to arrive at a similar conclusion as Theorem 2. However, the invariance principle preserves correlation but *not the security* of the reduction. Consequently, our technical approach uses appropriate junta theorems [17, 33] to circumvent this bottleneck. (See Appendix D for more detailed discussions).

As evidenced from our technical approach, an essential contribution of our work is establishing analysis pathways that emphasize security preservation. Our work highlights new challenges in harmonic analysis introduced by the security constraints. In the algebraization of security, Markov operators are needed to capture security. The analytic properties of Markov operators does not combine well with the standard Fourier basis. Therefore, the Efron-Stein (orthogonal) decomposition is necessary. Advances in Fourier analysis for Markov operators and Junta's theorems shall naturally lead to improvements of our results.

1.3 Technical Overview

Our proof for general distributions (X,Y) also extend to the case of $\mathrm{Supp}(X) \neq \mathrm{Supp}(Y)$. However, for the simplicity of presentation, we consider $\mathrm{Supp}(X) = \mathrm{Supp}(Y)$ to present the main technical ideas.

The proofs of the decidability problems Informal Theorem 3 and Informal Theorem 1 follow a sequence of steps described below. Let $\varepsilon' \in (0, 1/2)$, $\rho' = 1 - 2\varepsilon'$ and (X, Y) be an arbitrary finite joint distribution with maximal correlation ρ (refer to Section 2.4 for the definition). Let π_x and π_y be the marginal distribution of X and Y, respectively. Let T be the Markov operator associated with (X, Y) (see Section 2.5 for the formal definition).

Step 0: Derandomization. As elaborated in the introduction, we can use the deradomization result of [28] or our derandomization result (Theorem 8) appropriately to assume that the reduction functions are deterministic without loss of generality. Informal Theorem 3 uses our derandomization result Theorem 8 and all other results use the derandomization result of [28].

Step 1: Algebraization of Security. We first give an algebraized definition of SNIS of BSS from any finite joint distribution (see Definition 1). We show that if the insecurity in the simulation-based definition is δ, then it is at most 2δ in the algebraic definition, and vice-versa (refer to Claim 1). This result implies that the gap version of SNIS with respect to the simulation-based definition is decidable if and only if the gap version of SNIS with respect to the algebraic definition is decidable.

For brevity, we shall use f_n to represent $f_n(X^n)$ and g_n to represent $g_n(Y^n)$ in this document.

Claim 1. *Let (X, Y) be a finite distribution over $(\mathcal{X}, \mathcal{Y})$ with probability mass distribution π. Let π_x and π_y be the two marginal distributions. Let $f_n, g_n \colon \mathcal{X}^n \to \{-1, 1\}$ such that $f_n \in L^2(\mathcal{X}^n, {\pi_x}^{\otimes n})$, $g_n \in L^2(\mathcal{Y}^n, {\pi_y}^{\otimes n})$, and δ is some insecurity parameter. Let T and $\overline{T}$, respectively, be the Markov operator and the adjoint Markov associated with the source distribution (X, Y). Then, the following statements hold.*

1. *If $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_n, g_n} (X, Y)^{\otimes n}$, then it holds that $\mathbb{E}[f_n] \leq \delta$, $\mathbb{E}[g_n] \leq \delta$, $\|T^{\otimes n} g_n - \rho' \cdot f_n\|_1 \leq 2\delta$, and $\left\|\overline{T}^{\otimes n} f_n - \rho' \cdot g_n\right\|_1 \leq 2\delta$.*
2. *If $\mathbb{E}[f_n] \leq \delta$, $\mathbb{E}[g_n] \leq \delta$, $\|T^{\otimes n} g_n - \rho' \cdot f_n\|_1 \leq \delta$, and $\left\|\overline{T}^{\otimes n} f_n - \rho' \cdot g_n\right\|_1 \leq \delta$, then it holds that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{2\delta}_{f_n, g_n} (X, Y)^{\otimes n}$.*

Appendix A proves Claim 1.

Step 2: Fourier Concentration of Reduction Functions. Consider a pair of reduction function $f_n, g_n \colon \Omega^n \to \{-1, 1\}$ that achieve δ insecurity. The Fourier tail of a function is the summation of the square of all high-degree Fourier coefficients. We show that the Fourier tail of the reduction functions f_n and g_n is $\mathcal{O}(\delta)$. The technical tool to prove this result relies on the orthogonal (Efron-Stein) decomposition technique (defined in Section 2.6). Suppose the maximal correlation of (X, Y) is strictly less than 1. Our result additionally relies on Fourier properties of Markov operators (refer to Proposition 5, Proposition 6) from [39] stating that the higher order terms in the Efron-Stein decomposition of $T^{\otimes n} g_n$ have significantly smaller L_2 norm compared to the L_2 norm of the corresponding higher order terms in the Efron-Stein decomposition of g_n. This ability of the Efron-Stein decomposition to exponentially degrade the higher-order terms of $T^{\otimes n} g_n$ is crucial to our proof strategy. The definition of security implies that when we apply the Markov operator and then adjoint operator on g_n, the result function $\overline{T} T^{\otimes n} g_n$ is close to a scaling of g_n. As a consequence, the Fourier tail of g_n is small.

In the setting of Informal Theorem 1 ($\delta_n = \mathcal{O}(1/n)$), it implies that the total influence (refer to Section 2.3) of the reduction function is bounded from above by a constant that does not depend on n (refer to Corollary 2). This step does not change the reduction functions but gives Fourier concentration property of the reduction functions.

Step 3: Dimension Reduction by Applying Junta Theorem. In Informal Theorem 3, when the insecurity bound δ is sufficiently small, the Fourier tails of reduction functions is small

enough so that we can apply Bourgain's Junta Theorem (over biased measures) [6, 33]. In Informal Theorem 1, applying the generalized Friedgut's Junta Theorem [17] for function with constant total influence also gives us two junta functions. In both cases, this step always gives us two constant-size junta functions $\tilde{f}_n, \tilde{g_n} \colon \Omega^n \to \{-1, 1\}$ that are close to the two original reduction functions f_n, g_n in L_1 norm, respectively. Our proof shows that if $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_n,g_n} (X,Y)^{\otimes n}$, then $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\Theta(\delta)}_{\tilde{f}_n,\tilde{g_n}} (X,Y)^{\otimes n}$. Since $\tilde{f}_n$ and $\tilde{g_n}$ are junta functions, it is clear that there exists $n_0 \in \mathbb{N}$ and functions $f_{n_0}, g_{n_0} \colon \Omega^{n_0} \to \{-1, 1\}$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta'}_{\tilde{f}_n,\tilde{g_n}} (X,Y)^{\otimes n}$ if and only if $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta'}_{f_{n_0},g_{n_0}} (X,Y)^{\otimes n_0}$ for any δ' (refer to Theorem 7, Theorem 5).

Step 4: Solving the Decidability Problems. This step is identical to the step in [22, 14, 21]. Once we have the constant n_0, an algorithm for deciding the SNIS problems works as follows. The algorithm brute forces over all possible reduction functions $f_{n_0}, g_{n_0} \colon \Omega^{n_0} \to \{-1, 1\}$. If the algorithm finds any functions f_{n_0}, g_{n_0} such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_{n_0},g_{n_0}} (X,Y)^{\otimes n_0}$, it outputs Yes. Otherwise, it returns No.

Remainder of the results. Finally, we give an overview for Informal Theorem 2 and Informal Theorem 4. Let $\varepsilon' \in (0, 1/2)$, $\rho' = 1 - 2\varepsilon'$ and (X, Y) be an arbitrary 2-by-2 joint distribution with maximal correlation ρ. Let π_x and π_y be the marginal distribution of X and Y, respectively. Let T be the Markov operator associated with (X, Y).

First, we show that if there exist a sequence δ_n converging to 0 and sequences of reduction functions f_n, g_n such that we can simulate $\mathsf{BSS}(\varepsilon')$ with δ_n insecurity using reduction functions f_n, g_n, then $(\rho')^2 = \rho^{2k}$ for some positive integer k using biased Fourier analysis over Boolean hypercube. The main technical tool is a generalization of the equation $T_\rho \chi_S = \rho \chi_S$ to correlated spaces, that is, $T\phi_S = \rho \cdot \psi_S$ and $\overline{T}\psi_S = \rho \cdot \phi_S$, where T_ρ is the Bonami-Beckner noise operator, T and $\overline{T}$ are the Markov operator and the adjoint operator associated with the source distribution (X, Y), and χ_S, ϕ_S, ψ_S are Fourier bases over the uniform measure, π_x-biased measure, and π_y-biased measure, respectively (Claim 4). With this additional technical tool, we can further prove that the Fourier spectrum of reduction functions (mostly) concentrated on a constant degree k. This helps us to show that there exists a constant c such that $\min_{S \subseteq [n]} (\rho'^2 - \rho^{|S|})^2 \leq c \cdot \delta_n$ for infinitely many n, which implies that $\rho'^2 = \rho^{2k}$ for some $k \in \mathbb{N}$ since δ_n converges to 0.

In the perfect security case, the Fourier spectrum of the reduction functions f_n, g_n over biased measures π_x, π_y, respectively, are all concentrated on some constant degree k (Claim 2). We show that there does not exist any such functions unless both the measures π_x, π_y are uniform (Claim 3).

Figure 2 summarizes the high-level overview of the dependence between our technical results, i.e., which results are used to prove which results. Since Subsection 1.1 presents the most sophisticated results first but our results are proven in a sequential manner, the informal theorem numbers do not align with the theorem numbers. To address this situation, we have a more elaborate version of Figure 2 in the appendix as Figure 3, which explicitly mentions the informal theorem along with their respective (formal) theorems.

1.4 Organization of the Paper

Section 2 introduces the preliminary notations and definitions. We present the perfect-SNIS characterization (Informal Theorem 2) in Section 3. The concentration of the Fourier spectrum for secure reductions (Informal Theorem 5) is presented in Section 4. The other technical contribution (Informal Theorem 4) and lower bound for minimum insecurity (Corollary 1) is given in Section 5. Section 6 and Section 7 present the decidability results Informal Theorem 3 and Informal Theorem 1, respectively.

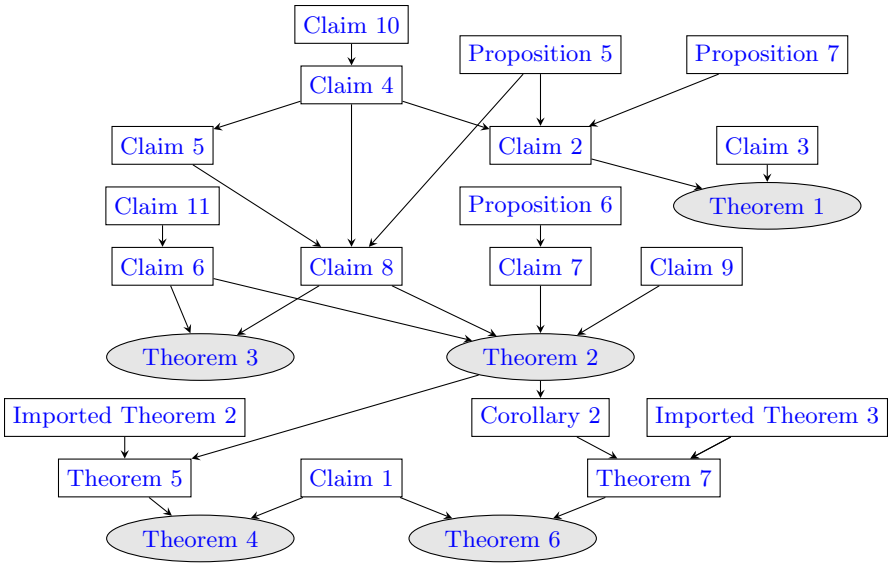

Figure 2: The diagram of claims, propositions and theorems. An arrow from one result to another result means that the first result is used to prove the second result. Highlighted nodes represent our final results.

2 Preliminaries

2.1 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 $f = g$ means that $f(x) = g(x)$ for every $x \in \Omega$. We use $\mathcal{X}, \mathcal{Y}, \mathcal{U}, \mathcal{V}$, or Ω to denote the sample spaces, and π usually denotes a probability distribution. $(\mathcal{X}, \mathcal{Y})$ is a joint probability space. For $x^n \in \mathcal{X}^n$, we represent $x_i \in \mathcal{X}$ as the i-th coordinate of x^n. A Boolean function is a $\{-1, 1\}$-valued function. Sometimes we omit the n when it is clear from the context.

Correlated Spaces. We usually use (X, Y) to denote the joint distribution over $(\mathcal{X}, \mathcal{Y})$ with probability mass function π, and π_x, π_y to denote the marginal probability distributions of X and Y, respectively. Sometimes we will use $(\mathcal{X} \times \mathcal{Y}, \pi)$ to denote the joint distribution. In this paper, we always use the following notation for the expectation of functions $f_n \in L^2(\mathcal{X}^n, {\pi_x}^{\otimes n}), g_n \in L^2(\mathcal{Y}^n, {\pi_y}^{\otimes n})$ over correlated spaces.

$$\mathbb{E}[f_n] := \mathop{\mathbb{E}}_{x^n \sim {\pi_x}^{\otimes n}} [f_n(x^n)], \ \mathbb{E}[g_n] := \mathop{\mathbb{E}}_{y^n \sim {\pi_y}^{\otimes n}} [g_n(x^n)]$$

$$\mathbb{E}[f_n g_n] := \mathop{\mathbb{E}}_{(x^n, y^n) \sim \pi^{\otimes n}} [f_n(x^n) \cdot g_n(y^n)]$$

We say that a joint distribution (X, Y) is *redundancy-free* if the sizes of the support of the two marginal distributions π_x, π_y are $|\mathcal{X}|$ and $|\mathcal{Y}|$, respectively. In this paper, we consider only redundancy-free joint distributions.

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

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

correlation of the source $\mathsf{BSS}(\varepsilon)$. If (X, Y) is a $\mathsf{BSS}(\varepsilon)$ source, then $(-X, Y)$ is a $\mathsf{BSS}(1-\varepsilon)$ source. So, without loss of generality, we can assume that $\varepsilon \in (0, \frac{1}{2}]$.

2.2 Secure Non-interactive Simulation: Definition

Appendix E recalls the notion of secure non-interactive simulation of joint distributions using a simulation-based security definition as defined in [28].

In this paper we are mainly focus on the case that the target distribution is a BSS. We give an algebrized definition of simulating BSS from any distribution as follows.

Definition 1 (Algebraic Definition)**.** *Let (X, Y) be correlated random variables distributed according to $(\mathcal{X} \times \mathcal{Y}, \pi)$. We say that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_n, g_n} (X, Y)$ if there exist reduction functions $f_n \in L^2(\mathcal{X}^n, {\pi_x}^{\otimes n})$, $g_n \in L^2(\mathcal{Y}^n, {\pi_y}^{\otimes n})$ such that*

1. ***Correctness:*** *$\mathbb{E}[f_n] \le \delta$, $\mathbb{E}[g_n] \le \delta$, and $\mathbb{E}[f_n g_n] \le \delta$.*
2. ***Corrupted Alice:***
$$\left\| T^{\otimes n} g_n - \rho' \cdot f_n \right\|_1 \le \delta,$$
where T is the Markov operator (defined in Section 2.5) associated with the source distribution (X, Y).
3. ***Corrupted Bob:***
$$\left\| \overline{T}^{\otimes n} f_n - \rho' \cdot g_n \right\|_1 \le \delta,$$
where $\overline{T}$ is the adjoint Markov operator(defined in Section 2.5) associated with (X, Y).

We provide a proof showing that this algebraic definition and the original (simulation-based) definition of SNIS are 2-approximate, in term of insecurity parameter, of each other in Appendix A. Next, we describe the decidability problem of SNIS as follows.

Problem 1. *Let (X, Y) be a joint distribution over the sample space $(\mathcal{X}, \mathcal{Y})$, and (U, V) be a joint distribution over the sample space $(\mathcal{U}, \mathcal{V})$, and let $\delta, \delta' > 0$ be some insecurity parameters, distinguish between the following two cases:*

1. *There exists a positive integer n, and functions $f_n \colon \mathcal{X}^n \to \mathcal{U}$ and $g_n \colon \mathcal{Y}^n \to \mathcal{V}$ such that $(U, V) \sqsubseteq^{\delta}_{f_n, g_n} (X, Y)^{\otimes n}$.*
2. *For every positive integer n, and for every reduction functions $f_n \colon \mathcal{X}^n \to \mathcal{U}$ and $g_n \colon \mathcal{Y}^n \to \mathcal{V}$, we have $(U, V) \not\sqsubseteq^{\delta'}_{f_n, g_n} (X, Y)^{\otimes n}$.*

Remark 1. *When $\delta' = c\delta$ for some constant $c > 1$, we call it multiplicative gap-SNIS. When $\delta' = \delta + \varepsilon$ for some $\varepsilon > 0$, we call it additive gap-SNIS. Note that $c\delta$ multiplicative gap is the same as $(c-1)\delta$ additive gap. When considering $\delta = o(1)$, the first item would be there exist a sequence of insecurity bound δ_n and a sequence of reduction functions f_n, g_n such that for infinitely many n, $(U, V) \sqsubseteq^{\delta_n}_{f_n, g_n} (X, Y)^{\otimes n}$, and the second item is the same.*

2.3 Fourier Analysis Basics

We recall some background in Fourier analysis over product measure that we will use in this paper. We follow the notation of [43].

2.3.1 Fourier Analysis over Higher Alphabet

Definition 2. *Let (Ω, π) be a finite probability space where $|\Omega| \ge 2$ and π denote a probability distribution over Ω. Let $\pi^{\otimes n}$ denote the product probability distribution on Ω^n such that $\pi^{\otimes n}(x_1 x_2 \dots x_n) = \prod_{i=1}^n \pi(x_i)$. 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*

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

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

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

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 $(\phi)_{\alpha \in \mathbb{N}^n_{<m}}$ (each $\alpha_i \in \{0, 1, \ldots, m-1\}$) is a Fourier basis for $L^2(\Omega^n, \pi^{\otimes n})$.

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 on 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 $\mathsf{Inf}(f) := \sum_{i=1}^n \mathsf{Inf}_i[f] = \sum_\alpha |\alpha| \widehat{f}(\alpha)^2 = \sum_{k=1}^n k \cdot W^k[f]$.

Proposition 1. *For any real-valued function $f \in L^2(\Omega^n, \pi^{\otimes n})$, if $\deg(f) = k$ for some $k \in \mathbb{N}$. Then $\mathsf{Inf}(f) \leq k$.*

2.3.2 Biased Fourier Analysis over Boolean Cube.

In the special case when $\Omega = \{-1, 1\}$, 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 $f \colon \Omega^n \to \{-1, 1\}$ 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 $\|f - h\|_1 \leq \varepsilon$.*

2.4 Maximal Correlation

We recall the definition of maximal correlation of a joint distribution and its properties in this subsection.

Definition 6 (Maximal Correlation [24, 47, 2, 46, 3])**.** *Let (X, Y) be a finite joint distribution over $(\mathcal{X}, \mathcal{Y})$ with probability mass function π. The Hirschfeld-Gebelein-Renyi maximal correlation of (X, Y) is defined as follows:*

$$\rho(X; Y) := \max_{(f,g) \in \mathcal{S}} \mathbb{E}[fg],$$

where $\mathcal{S}$ represents the set of all real-valued function $f \in L^2(\mathcal{X}, \pi_x)$ and $g \in L^2(\mathcal{Y}, \pi_y)$ satisfying the following two conditions:

$$\mathbb{E}[f] = \mathbb{E}[g] = 0,$$

$$\mathbb{E}[f^2] = \mathbb{E}[g^2] = 1.$$

In case that $\mathcal{S} = \emptyset$ (which happens precisely when at least one of X and Y is constant almost surely), $\rho(X;Y)$ is defined to be 0.

For example, the maximal correlation of $\mathsf{BSS}(\varepsilon)$ is $|1-2\varepsilon|$ for every $\varepsilon \in [0,1]$. Note that maximal correlation of any distribution is always between 0 and 1.

Imported Theorem 1 (Tensorization [47])**.** *If (X_1, Y_1) and (X_2, Y_2) are independent, then*

$$\rho(X_1, X_2; Y_1, Y_2) = \max\{\rho(X_1; Y_1), \rho(X_2, Y_2)\}$$

and so if $(X_1, Y_1), (X_2, Y_2)$ are i.i.d., then $\rho(X_1, X_2; Y_1, Y_2) = \rho(X_1; Y_1)$.

The following proposition shows that maximal correlation is an easily computable quantity.

Proposition 2 ([47])**.** *The maximal correlation of a finite joint distribution (X, Y) is the second largest singular value of the Markov operator T (defined in Section 2.5) associated with (X, Y), in other words, it is the square root of the second largest eigenvalue of the Markov operator $T\overline{T}$, where $\overline{T}$ is the adjoint Markov operator of T.*

2.5 Markov Operator

Definition 7 (Markov Operator [38])**.** *Let (X, Y) be a finite distribution over $(\mathcal{X}, \mathcal{Y})$ with probability mass distribution π. The Markov operator associated with this distribution, denoted by T, maps a function $g \in L^p(\mathcal{Y}, \pi_y)$ to a function $Tg \in L^p(\mathcal{X}, \pi_x)$ by the following map:*

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

where (X, Y) is distributed according to π. Furthermore, we define the adjoint operator of T, denoted as $\overline{T}$, maps a function $f \in L^p(\mathcal{X}, \pi_x)$ to a function $\overline{T}f \in L^p(\mathcal{Y}, \pi_y)$ by the following map:

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

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

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

The example below illustrates the Markov operator and its adjoint.

Example 1. *When $\mathcal{X} = \mathcal{Y} = \{-1, 1\}$ and $\pi(1,1) = a, \pi(1,-1) = b, \pi(-1,1) = c$, and $\pi(-1,-1) = d$, where $0 \le a, b, c, d \le 1$ 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 $f \in L^p(\{-1,1\}, \pi_x)$ and $g \in L^p(\{-1,1\}, \pi_y)$, we have*

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

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

Proposition 3. *[47] Let (X,Y) be a finite distribution over $(\mathcal{X},\mathcal{Y})$ with probability mass distribution π. Let T and $\overline{T}$ be the Markov operator and the adjoint Markov operator associated with (X,Y). Let $(\mathcal{X}\times\mathcal{X},\mu)$ be the distribution whose associated Markov operator is $T\overline{T}$ and $\mu_x=\pi_x$. Then, the marginal distributions of $(\mathcal{X}\times\mathcal{X},\mu)$ are the same, in other words, $\mu_x=\mu_y$. Furthermore, we have $\rho(\mathcal{X}\times\mathcal{X},\mu)=\rho^2$, where ρ is the maximal correlation of (X,Y).*

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

2.6 Efron-stein Decomposition

We shall use Efron-stein decomposition as one of the main technical tools to prove Informal Theorem 2 and Informal Theorem 5.

Definition 8 (Efron-Stein decomposition)**.** *Let $(\Omega_1,\mu_1),(\Omega_2,\mu_2),\ldots,(\Omega_\ell,\mu_\ell)$ 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:

- *$f^{=S}$ depends only on x_S.*
- *For all $S\not\subseteq S'$ and all $x_{S'}$, $\mathbb{E}[f^{=S}(X_{S'})|X_{S'}=x_{S'}]=0$*

Proposition 4 ([15])**.** *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 ([38, 39] Proposition 2.11)**.** *Let (X^n,Y^n) be a joint distribution over $(\mathcal{X}^n\times\mathcal{Y}^n,\pi^{\otimes n})$. Let T_i be the Markov operator associated with (X_i,Y_i). Let $T^{\otimes n}=\otimes_{i=1}^{n}T_i$, and consider a function $g_n\in L^p(\mathcal{Y}^n,{\pi_y}^{\otimes n})$. Then, the Efron-Stein decomposition of g_n satisfies:*

$$(T^{\otimes n}g_n)^{=S}=T^{\otimes n}(g_n^{=S}).$$

The next proposition shows that $T^{\otimes n}g_n$ depends on the low degree expansion of g_n.

Proposition 6 ([39] Proposition 2.12)**.** *Assuming the setting of Proposition 5 and let ρ be the maximal correlation of the distribution (X,Y). Then for all $g_n\in L^p(\mathcal{Y}^n,{\pi_y}^{\otimes n})$ it holds that*

$$\left\|T^{\otimes n}g_n^{=S}\right\|_2\le\rho^{|S|}\left\|g_n^{=S}\right\|_2.$$

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

Proposition 7 ([43] 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 $\Omega=\{-1,1\}$ 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 $W^{>k}[f]=\sum_{|S|>k}\left\|f^{=S}\right\|_2^2$.

3 SNIS Characterization: BSS from 2-by-2 Distribution

In this section we present the characterization result for SNIS of BSS from any arbitrary 2-by-2 distribution with 0-insecurity (perfect security). First we restate the Informal Theorem 2 as follows.

Theorem 1. *[Perfect-SNIS Characterization] Let $\varepsilon' \in (0, 1/2)$ and (X, Y) be an arbitrary 2-by-2 joint distribution. Suppose there exists $n \in \mathbb{N}$ and Boolean functions $f_n, g_n \colon \{-1,1\}^n \to \{-1,1\}$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^0_{f_n,g_n} (X,Y)^{\otimes n}$. Then, the distribution (X, Y) must be a BSS with flipping probability ε such that $(1-2\varepsilon') = (1-2\varepsilon)^k$ for some positive integer $k \leq n$.*

It follows from Theorem 1 that the perfect SNIS of BSS from any arbitrary 2-by-2 source distribution is decidable in polynomial time.

Remark 2. *The characterization of SNIS of BSS from arbitrary 2-by-2 distribution with $o(1)$ insecurity bound remains open.*

3.1 Claims needed for Theorem 1

We state all the claims that are needed to prove Theorem 1, and provide their proofs in Section 3.4.

Claim 2. *Let (X, Y) be a 2-by-2 joint distribution over $(\{-1,1\}, \{-1,1\})$ with probability mass distribution π and $\varepsilon' \in (0, 1/2)$. Suppose there exist $n \in \mathbb{N}$, and $f_n, g_n \colon \{-1,1\}^n \to \{-1,1\}$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^0_{f_n,g_n} (X,Y)$. Then, the following statements hold:*

1. *There exists a positive integer k such that $\rho' = \rho^k$, where ρ is the maximal correlation of the source distribution (X, Y) and $\rho' = 1 - 2\varepsilon'$.*
2. *Furthermore, the Fourier weights of both f_n, g_n are entirely concentrated on degree k, that is, $W^k[f_n] = W^k[g_n] = 1$, where the Fourier coefficients of f_n, g_n are with respect to the inner products over ${\pi_x}^{\otimes n}$ and ${\pi_y}^{\otimes n}$, respectively.*

Claim 3. *Suppose f is a Boolean function in $L^2(\{-1,1\}^n, \pi^{\otimes n})$ such that $W^k[f] = 1$. Then, it must be the case that the distribution π is the uniform distribution over $\{-1, 1\}$.*

3.2 Proof of Theorem 1

Suppose there exists $n \in \mathbb{N}$ and Boolean functions $f_n, g_n \colon \{-1,1\}^n \to \{-1,1\}$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^0_{f_n,g_n} (X,Y)^{\otimes n}$. Then, by Claim 2, we have $(1-2\varepsilon') = \rho^k$ for some $k \in \mathbb{N}$, and $W^k[f_n] = W^k[g_n] = 1$, where ρ is the maximal correlation of (X, Y). By Claim 3, both the marginal distribution π_x and π_y must be uniform distribution over $\{-1, 1\}$, which implies that the joint distribution (X, Y) is a $\mathsf{BSS}(\varepsilon)$ for some $\varepsilon \in (0, 1)$. Using the fact that the the maximal correlation of $\mathsf{BSS}(\varepsilon) = 1 - 2\varepsilon$, one concludes that $(1-2\varepsilon') = (1-2\varepsilon)^k$.

3.3 Technical Contribution: Properties of Markov Operators and Fourier Bases over Correlated Space

In this subsection, we prove some technical results showing relation between maximal correlation, Markov operators, and Fourier bases. We will use them as one of the main technical tools to prove Claim 2, Claim 3 and Theorem 3.

Let (X, Y) be a joint distribution over $(\{-1,1\}, \{-1,1\})$ with probability mass function π. Let T and $\overline{T}$ be the Markov operator and the adjoint Markov operator associated with (X, Y). Suppose $\pi = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ for $0 \leq a, b, c, d$ such that $a+b+c+d = 1$. Let $p = c+d$ and $q = b+d$. Let $\{\phi_S\}_{S \subseteq [n]}$ be

a biased Fourier basis for $L^2(\mathcal{X}^n, {\pi_x}^{\otimes n})$, and $\{\psi_S\}_{S\subseteq[n]}$ be a biased Fourier basis for $L^2(\mathcal{Y}^n, {\pi_y}^{\otimes n})$ defined as follows.

$$\phi_S(x) = \prod_{i=1}^{n} \left(\frac{x_i - \mu_x}{\sigma_x} \right), \text{ and } \psi_S(x) = \prod_{i=1}^{n} \left(\frac{y_i - \mu_y}{\sigma_y} \right),$$

where $\mu_x = 1-2p, \mu_y = 1-2q, \sigma_x = 2\sqrt{p}\sqrt{1-p}$, and $\sigma_y = 2\sqrt{q}\sqrt{1-q}$. Assuming these settings, we claim the following results.

Claim 4. *The following equalities hold.*

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

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

$$(T\overline{T})^{\otimes n}\phi_S = \rho^{2|S|} \cdot \phi_S, \text{ and } (\overline{T}T)^{\otimes n}\psi_S = \rho^{2|S|} \cdot \psi_S.$$

Remark 3. *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 ${T_\rho}^{\otimes n}\chi_S = \rho^{|S|} \cdot \chi_S$, where T_ρ is the Bonami-Beckner noise operator, and $\chi_S \colon \{-1,1\}^n \to \{-1,1\}$ is the function defined as $\chi_S = \prod_{i\in S} x_i$ (a Fourier basis over the uniform measure).*

We provide a proof of Claim 4 in Appendix B. The following result is a corollary of Claim 4.

Claim 5. *For any $S, H \subseteq [n]$, the following equalities hold.*

$$\widehat{T^{\otimes n}\psi_S}(H) = \widehat{\overline{T}^{\otimes n}\phi_S}(H) = \begin{cases} \rho^{|S|} & \text{if } H = S \\ 0 & \text{otherwise.} \end{cases}$$

$$\widehat{(T\overline{T})^{\otimes n}}\phi_S(H) = \widehat{(\overline{T}T)^{\otimes n}}\psi_S(H) = \begin{cases} \rho^{2|S|} & \text{if } H = S \\ 0 & \text{otherwise.} \end{cases}$$

3.4 Proofs of claims used in Theorem 1

In this subsection, we present the proofs of the two claims used to prove Theorem 1.

Proof of Claim 2. We shall use orthogonal (Efron-Stein) decomposition to prove this claim. We write f_n and g_n in terms of the orthogonal decomposition as follows.

$$f_n = \sum_{S\subseteq[n]} f_n^{=S}, \text{ and } g_n = \sum_{S\subseteq[n]} g_n^{=S}$$

By linearity of the Markov operator and by Proposition 5,

$$T^{\otimes n}g_n = T^{\otimes n}\left(\sum_{S\subseteq[n]} g_n^{=S} \right) = \sum_{S\subseteq[n]} T^{\otimes n} g_n^{=S} = \sum_{S\subseteq[n]} (T^{\otimes n} g_n)^{=S},$$

$$\overline{T}^{\otimes n}f_n = \overline{T}^{\otimes n}\left(\sum_{S\subseteq[n]} f_n^{=S} \right) = \sum_{S\subseteq[n]} \overline{T}^{\otimes n} f_n^{=S} = \sum_{S\subseteq[n]} (\overline{T}^{\otimes n} f_n)^{=S}$$

It follows from the perfect security assumption that $T^{\otimes n} g_n = \rho' \cdot f_n$ and $\overline{T}^{\otimes n} f_n = \rho' \cdot g_n$. Since $T^{\otimes n} g_n = \rho' \cdot f_n$ and by uniqueness of the orthogonal decomposition, it must be the case that $T^{\otimes n} g_n^{=S} = \rho' \cdot f_n^{=S}$ for every S. Similarly, we also have $\overline{T}^{\otimes n} f_n^{=S} = \rho' \cdot g_n^{=S}$ for every S. These two equations imply that

$$(T\overline{T})^{\otimes n} f_n^{=S} = \rho'^2 \cdot f_n^{=S}.$$

By Proposition 7 and Claim 4, we have

$$(T\overline{T})^{\otimes n} f_n^{=S} = (T\overline{T})^{\otimes n} (\widehat{f_n}(S) \cdot \phi_S) = \widehat{f_n}(S) \cdot (T\overline{T})^{\otimes n} \phi_S = \widehat{f_n}(S) \cdot \rho^{2|S|} \cdot \phi_S, \text{ and}$$
$$\rho'^2 \cdot f_n^{=S} = \rho'^2 \cdot \widehat{f_n}(S) \cdot \phi_S$$

It implies that $\widehat{f_n}(S) \cdot (\rho'^2 - \rho^{2|S|}) = 0$ for every S. So for every S either $\widehat{f_n}(S) = 0$ or $\rho'^2 = \rho^{2|S|}$. Since there exists S^* such that $\widehat{f_n}(S^*) \neq 0$, it must be the case that $\rho'^2 = \rho^{2k}$, where $k = |S^*|$. Furthermore, $\widehat{f_n}(S) = 0$ for every S satisfying $|S| \neq k$, in other words, $W^k[f_n] = 1$. Analogously, we can show that $W^k[g_n] = 1$. □

Proof of Claim 3. Let $\phi_S = \prod_{i \in S} \left(\frac{x_i - \mu}{\sigma}\right)$ be a Fourier basis over $L^2(\{-1,1\}^n, \pi^{\otimes n})$, where $p = Pr[\pi(x) = -1], \mu = 1 - 2p, \sigma = 2\sqrt{p}\sqrt{1-p}$. Since $W^k[f] = 1$, it can be written as

$$f(x) = \sum_{|S|=k} \widehat{f}(S)\phi_S(x) = \sum_{|S|=k} \widehat{f}(S) \left(\frac{x_i - \mu}{\sigma}\right).$$

Substitute $x = \mathbf{1} = (1, 1, \ldots, 1) \in \{-1,1\}^n$ and $x = -\mathbf{1} = (-1, -1, \ldots, -1) \in \{-1,1\}^n$ yields

$$f(\mathbf{1}) = \left(\frac{1-\mu}{\sigma}\right)^k \sum_{|S|=k} \widehat{f}(S), \text{ and} \qquad f(-\mathbf{1}) = \left(\frac{-1-\mu}{\sigma}\right)^k \sum_{|S|=k} \widehat{f}(S)$$

It it clearly that $\sum_{|S|=k} \widehat{f}(S) \neq 0$ since $f(\mathbf{1}) \neq 0$. Using the fact that f is boolean-valued function, we have $f(\mathbf{1})^2 = f(-\mathbf{1})^2$. Therefore, we have

$$\left(\frac{1-\mu}{\sigma}\right)^{2k} \left(\sum_{|S|=k} \widehat{f}(S)\right)^2 = \left(\frac{-1-\mu}{\sigma}\right)^{2k} \left(\sum_{|S|=k} \widehat{f}(S)\right)^2$$

It implies that

$$\left(\frac{1-\mu}{\sigma}\right)^{2k} = \left(\frac{-1-\mu}{\sigma}\right)^{2k},$$

which can happen only when $\mu = 0$. In other words, π is a uniform distribution over $\{-1,1\}$, which completes the proof. □

4 Concentration of the Fourier Spectrum for Secure Reductions

We restate Informal Theorem 5 formally as the following theorem in this section, which will be used as a main technical lemma to prove Informal Theorem 3 and Informal Theorem 1.

Theorem 2. *Let $\rho \in [0,1]$ and $\varepsilon' \in (0, 1/2)$. Suppose there exists $n \in \mathbb{N}$, a finite joint distribution (X, Y) over (Ω, Ω) with probability mass function π and reduction functions $f_n, g_n \colon \Omega^n \to \{-1,1\}$*

such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta_n}_{f_n,g_n} (X,Y)^{\otimes n}$ *for some* $\delta_n \geq 0$ *and the maximal correlation of* (X,Y) *is* ρ. *Then, the following bounds hold.*

$$W^{>k}[f_n] := \sum_{S\colon |S|>k} \widehat{f_n}(S)^2 \leq \frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2}\cdot\delta_n, \text{ and}$$

$$W^{>k}[g_n] := \sum_{S\colon |S|>k} \widehat{g_n}(S)^2 \leq \frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2}\cdot\delta_n,$$

where $\rho' = 1-2\varepsilon'$, $f_n \in L^2(\Omega^n, {\pi_x}^{\otimes n})$, $g_n \in L^2(\Omega^n, {\pi_y}^{\otimes n})$, *and* $k \in \mathbb{N}$ *such that* $\rho^k \geq \rho' > \rho^{k+1}$.

We provide the proof of Theorem 2 in Subsection 4.2. Intuitively, Theorem 2 says that the Fourier spectrum of reduction functions are mostly concentrated on low degree weights. As a consequence, when $\delta_n = O(1/n)$, the total influences of reduction functions are bounded from above. We state it as following and prove it in Subsection 4.3.

Corollary 2. *Assuming the setting of Theorem 2, if* $\delta_n = c_0/n$ *for some constant* $c_0 > 0$, *then we have*

$$\mathsf{Inf}(f_n) \leq k + \frac{(1+\rho')^2 c_0}{(\rho^{2(k+1)}-\rho'^2)^2}, \text{ and } \mathsf{Inf}(g_n) \leq k + \frac{(1+\rho')^2 c_0}{(\rho^{2(k+1)}-\rho'^2)^2}$$

4.1 Required Claims for Theorem 2

Assuming the setting of Theorem 2 and the following notation, we state the claims that are needed to prove Theorem 2. We provide the proofs of these claims in Appendix C. Let T and $\overline{T}$ denote respectively the Markov operator and the corresponding adjoint operator associated with the distribution (X,Y). Note that $f_n \in L^2(\Omega^n, {\pi_x}^{\otimes n})$, $g_n \in L^2(\Omega^n, {\pi_y}^{\otimes n})$, $T^{\otimes n} g_n \in L^2(\Omega^n, {\pi_x}^{\otimes n})$, and $\overline{T}^{\otimes n} f_n \in L^2(\Omega^n, {\pi_y}^{\otimes n})$. Let $f_n = \sum_{S\subseteq[n]} f_n^{=S}$, and $g_n = \sum_{S\subseteq[n]} g_n^{=S}$ be the Efron-stein decompositions of f_n and g_n.

Claim 6. $\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2\cdot f_n\right\|_1 \leq (1+\rho')\delta_n$, *and* $\left\|(\overline{T}T)^{\otimes n} g_n - \rho'^2\cdot g_n\right\|_1 \leq (1+\rho')\delta_n$. *Furthermore, we have* $\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2\cdot f_n\right\|_2^2 \leq (1+\rho')^2\delta_n$, *and* $\left\|(\overline{T}T)^{\otimes n} g_n - \rho'^2\cdot g_n\right\|_2^2 \leq (1+\rho')^2\delta_n$.

Intuitively, Claim 6 says that a noisy version of reduction functions is close to their scaling version in both L_1 and L_2 norms.

Claim 7. *For every* $S \subseteq [n]$ *such that* $|S| > k$, *the following bound holds.*

$$\left|\left\|T^{\otimes n} f_n^{=S}\right\|_2 - \rho'^2\cdot\left\|f_n^{=S}\right\|_2\right| \geq \left|\rho^{2|S|}\cdot\left\|f_n^{=S}\right\|_2 - \rho'^2\cdot\left\|f_n^{=S}\right\|_2\right|$$

Claim 8. *The following equation holds.*

$$\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2\cdot f_n\right\|_2^2 = \sum_{S\subseteq[n]}\left\|(T\overline{T})^{\otimes n} f_n^{=S} - \rho'^2\cdot f_n^{=S}\right\|_2^2$$

In particular, when $\Omega = \{-1,1\}$, *we have*

$$\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2\cdot f_n\right\|_2^2 = \sum_{S\subseteq[n]}\widehat{f_n}(S)^2\left(\rho^{2|S|}-\rho'^2\right)^2$$

The identities in Claim 8 are Parseval-like equations for the composition of Markov operator and its adjoint operator applying on a function. The next claim says that the both operators T and $\overline{T}$ are contractive.

Claim 9. *The following inequalities hold.*

$$\left\|T^{\otimes n} g_n\right\|_1 \leq \|g_n\|_1 = 1, \text{ and } \left\|\overline{T}^{\otimes n} f_n\right\|_1 \leq \|f_n\|_1 = 1.$$

4.2 Proof of Theorem 2

Assuming Claim 6, Claim 7, Claim 8, we present a proof of Theorem 2 as follows. Clearly, the function $(T\overline{T})^{\otimes n} f_n - \rho' \cdot f_n$ is bounded from above by $1+\rho'$. So it follows from Claim 6 and that

$$\left\|(T\overline{T})^{\otimes n} f_n - \rho' \cdot f_n\right\|_2^2 \leq (1+\rho')^2 \delta_n.$$

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

$$\begin{aligned}
\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2 \cdot f_n\right\|_2^2 &= \sum_{S\subseteq[n]} \left\|(T\overline{T})^{\otimes n} f_n^{=S} - \rho'^2 \cdot f_n^{=S}\right\|_2^2 && \text{Claim 8} \\
&\geq \sum_{S:\ |S|>k} \left\|(T\overline{T})^{\otimes n} f_n^{=S} - \rho'^2 \cdot f_n^{=S}\right\|_2^2 \\
&\geq \sum_{S:\ |S|>k} \left|\left\|(T\overline{T})^{\otimes n} f_n^{=S}\right\|_2 - \rho'^2 \cdot \left\|f_n^{=S}\right\|_2\right|^2 && \text{Triangle Inq.} \\
&\geq \sum_{S:\ |S|>k} \left|\rho^{2|S|} \cdot \left\|f_n^{=S}\right\|_2 - \rho'^2 \cdot \left\|f_n^{=S}\right\|_2\right|^2 && \text{Claim 7} \\
&\geq \sum_{S:\ |S|>k} (\rho^{2(k+1)} - \rho'^2)^2 \cdot \left\|f_n^{=S}\right\|_2^2 \\
&= (\rho^{2(k+1)} - \rho'^2)^2 \sum_{S:\ |S|>k} \left\|f_n^{=S}\right\|_2^2
\end{aligned}$$

Recall that $W^{>k}[f_n] = \sum_{S:\ |S|>k} \left\|f_n^{=S}\right\|$, therefore $W^{>k}[f_n] \leq \frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2} \cdot \delta_n$. Similarly, $W^{>k}[g_n] \leq \frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2} \cdot \delta_n$, which completes the proof.

4.3 Proof of Corollary 2

Let m be the size the domain Ω. From the basic formula of total influence and the fact that $\sum_{\alpha\in\mathbb{N}_n^{<m}} \widehat{f}(\alpha)^2 = \sum_{i=1}^n W^i(f_n) = 1$, we have

$$\begin{aligned}
\mathsf{Inf}(f_n) &= \sum_{\alpha\in\mathbb{N}_n^{<m}} |\alpha| \widehat{f_n}(\alpha)^2 \\
&= \sum_{i=1}^n i \cdot W^i(f_n) \\
&\leq k \cdot \sum_{i=1}^k W^i(f_n) + n \cdot W^{>k}(f_n) \\
&\leq k \cdot 1 + n \cdot \frac{c}{n} \cdot \frac{(1+\rho')^2}{(\rho^{2(k+1)} - \rho'^2)^2} && \text{Theorem 2} \\
&= k + c \cdot \frac{(1+\rho')^2}{(\rho^{2(k+1)} - \rho'^2)^2}
\end{aligned}$$

Analogously, $\mathsf{Inf}(g_n) \leq k + \frac{(1+\rho')^2 c}{(\rho^{2(k+1)}-\rho'^2)^2}$, which completes the proof.

5 Lower Bound for Minimum Insecurity

We restate both Informal Theorem 4 and Corollary 1 as the following theorem.

Theorem 3. *Let $\varepsilon' \in (0, 1/2)$ and let (X, Y) be a* redundancy-free *2-by-2 joint distribution with maximal correlation ρ. Suppose there exists a sequence $\delta_n \in [0, 1]$ converging to 0, and a sequence of reduction functions f_n, g_n such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta_n}_{f_n,g_n} (X, Y)^{\otimes n}$. Then, there exists $k \in \mathbb{N}$ such that $(1 - 2\varepsilon') = \rho^k$.*

On the other hand, if $(1 - 2\varepsilon') \neq \rho^k$ for any $k \in \mathbb{N}$, then the insecurity of any protocol for non-interactive secure simulation of $\mathsf{BSS}(\varepsilon')$ from (X, Y) using arbitrary number of independent samples is at least

$$\frac{1}{4} \min\left(\left((1-2\varepsilon')^2 - \rho^{2k}\right)^2, \left((1-2\varepsilon')^2 - \rho^{2(k+1)}\right)^2\right),$$

where $k \in \mathbb{N}$ such that $\rho^k > (1 - 2\varepsilon') > \rho^{k+1}$.

Theorem 3 gives a necessary condition for SNIS of $\mathsf{BSS}(\varepsilon')$ from an arbitrary 2-by-2 source distribution with $o(1)$-insecurity. As consequences, if $(1 - 2\varepsilon')^2 \neq \rho^{2k}$ for every $k \in \mathbb{N}$, any secure protocol simulating $\mathsf{BSS}(\varepsilon')$ has constant insecurity. Furthermore, using our proof technique we can derive an explicit lower bound for the minimum insecurity.

Proof of Theorem 3. Let $\rho' = 1 - 2\varepsilon'$. Let T and $\overline{T}$ denote, respectively, the Markov operator and the corresponding adjoint operator associated with the distribution (X, Y). Let π be the probability mass function of (X, Y). Moreover, note that $f_n \in L^2(\Omega^n, {\pi_x}^{\otimes n})$ and $g_n \in L^2(\Omega^n, {\pi_y}^{\otimes n})$. Applying Claim 8 yields

$$\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2 \cdot f_n\right\|_2^2 = \sum_{S\subseteq[n]} \left\|(T\overline{T})^{\otimes n} f_n^{=S} - \rho'^2 \cdot f_n^{=S}\right\|_2^2 = \sum_{S\subseteq[n]} \widehat{f_n}(S)^2 \left(\rho^{2|S|} - \rho'^2\right)^2$$

Together with Claim 6, it implies that

$$\min_{S\subseteq[n]} \left(\rho^{2|S|} - \rho'^2\right)^2 \leq \frac{(1+\rho')^2}{1 - \frac{(1+\rho')^2\delta_n}{\rho^{2(k+1)} - \rho^{2k}}} \cdot \delta_n.$$

Now, since $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta_n}_{f_n,g_n}$ for infinitely many n and $\lim_{n\to\infty} \delta_n = 0$, we have

$$\min_{S} \left(\rho^{2|S|} - \rho'^2\right)^2 \leq \lim_{n\to\infty} \frac{(1+\rho')^2}{1 - \frac{(1+\rho')^2\delta_n}{\rho^{2(k+1)} - \rho^{2k}}} \cdot \delta_n = \lim_{n\to\infty} \delta_n = 0.$$

Therefore, it must be the case that there exists S^* such that $\rho'^2 = \rho^{2k}$, where $k = |S^*|$.

Next, applying Claim 8 yields

$$\left\|(T\overline{T})^{\otimes n} f_n - \rho' \cdot f_n\right\|_2^2 = \sum_{S\subseteq[n]} \widehat{f_n}(S)^2 \left(\rho^{2|S|} - \rho'^2\right)^2 \geq \min_{S\subseteq[n]} \left(\rho^{2|S|} - \rho'^2\right)^2$$

By Claim 6, we have $(1 + \rho')^2\delta_n \geq \min_{S\subseteq[n]} \left(\rho^{2|S|} - \rho'^2\right)^2$. This implies that

$$\delta_n \geq \frac{1}{4} \min\left(\left(\rho'^2 - \rho^{2k}\right)^2, \left(\rho'^2 - \rho^{2(k+1)}\right)^2\right).$$

□

6 Decidability of SNIS: BSS from 2-by-2 Distribution

In this section, we formally restate Informal Theorem 3.

Theorem 4 (Decidability-Multiplicative-Gap-2-by-2)**.** *Let (X,Y) be a 2-by-2 distribution over $(\{-1,1\},\{-1,1\})$ with maximal correlation ρ and probability mass function π. Let $p=\pi_x(-1)$ and $q=\pi_y(-1)$. Let $\varepsilon'\in(0,1/2)$, $\rho'=1-2\varepsilon'$, $\kappa=\frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2}$, where $k\in\mathbb{N}$ such that $\rho^k\geq(1-2\varepsilon')>\rho^{k+1}$. There exist $c>0,\delta_0>0$, and $n_0\in\mathbb{N}$, such that the following statement holds. For any insecurity parameter $\delta<\delta_0$, there is an algorithm running in bounded computable time $O(2^{2^{n_0}})$ that distinguishes between the following two cases.*

1. *There exist $n\in\mathbb{N}$ and reduction functions $f_n,g_n\colon\{-1,1\}^n\to\{-1,1\}$ such that $\mathsf{BSS}(\varepsilon')\sqsubseteq^{\delta}_{f_n,g_n}(X,Y)^{\otimes n}$.*
2. *For all $n\in\mathbb{N}$, and reduction functions $f_n,g_n\colon\{-1,1\}^n\to\{-1,1\}$, it must be the case that $\mathsf{BSS}(\varepsilon')\not\sqsubseteq^{c\cdot\delta}_{f_n,g_n}(X,Y)^{\otimes n}$.*

One can set δ_0,c,n_0 as follows:

$$
\begin{aligned}
&n_0=2kM/\eta_p^{16k}+2kM/\eta_q^{16k}\,,\delta_0=\min(\delta_0(p),\delta_0(q))\,,\\
&\delta_0(p):=\min(\eta_p^{16k}/(M\cdot\kappa),(d/\kappa-1)^4\cdot\eta_p^{16k}/(2\kappa\cdot 1064^4))\,,\\
&\delta_0(q):=\min(\eta_q^{16k}/(M\cdot\kappa),(d/\kappa-1)^4\cdot\eta_q^{16k}/(2\kappa\cdot 1064^4))\,,\\
&c=5(\kappa+1)\,,\eta_p=(1+p^{-1/2}(1-p)^{-1/2})^{-1/2}\,,\eta_q=(1+q^{-1/2}(1-q)^{-1/2})^{-1/2}\,,
\end{aligned}
$$

and M is a global constant (refer to Imported Theorem 2). Furthermore, in the first case, the algorithm outputs a pair of reduction functions f_{n_0},g_{n_0} such that $\mathsf{BSS}(\varepsilon')\sqsubseteq^{c\delta}_{f_{n_0},g_{n_0}}(X,Y)^{\otimes n_0}$.

The following result is the main technical lemma for the proof of the above theorem.

Theorem 5 (Dimension Reduction 2-by-2)**.** *Let (X,Y) be a 2-by-2 distribution over $(\{-1,1\},\{-1,1\})$ with maximal correlation ρ and probability mass function π. Let $p=\pi_x(-1)$ and $q=\pi_y(-1)$. Let $\varepsilon'\in(0,1/2)$, $\rho'=1-2\varepsilon'$, $\kappa=\frac{(1+\rho')^2}{(\rho^{2(k+1)}-\rho'^2)^2}$, where $k\in\mathbb{N}$ such that $\rho^k\geq(1-2\varepsilon')>\rho^{k+1}$ and fix $d\geq\kappa$. There exists $0<\delta_0<1$, $n_0\in\mathbb{N}$, such that for any $0<\delta<\delta_0$, for any $n\in\mathbb{N}$, any reduction functions $f_n,g_n\colon\{-1,1\}^n\to\{-1,1\}$ satisfying $\mathsf{BSS}(\varepsilon')\sqsubseteq^{\delta}_{f_n,g_n}(X,Y)^{\otimes n}$, there exist functions $f_{n_0},g_{n_0}\colon\{-1,1\}^{n_0}\to\{-1,1\}$ such that $\mathsf{BSS}(\varepsilon')\sqsubseteq^{(1+4d)\delta}_{f_{n_0},g_{n_0}}(X,Y)^{\otimes n_0}$. Furthermore, n_0 is a computable function in the parameters of the problem. In particular, one may take $n_0=2kM/\eta_p^{16k}+2kM/\eta_q^{16k}$ and $\delta_0=\min(\delta_0(p),\delta_0(q))$, where*

$$
\begin{aligned}
\delta_0(p)&:=\min(\eta_p^{16k}/(M\cdot\kappa),(d/\kappa-1)^4\cdot\eta_p^{16k}/(2\kappa\cdot 1064^4))\\
\delta_0(q)&:=\min(\eta_q^{16k}/(M\cdot\kappa),(d/\kappa-1)^4\cdot\eta_q^{16k}/(2\kappa\cdot 1064^4))
\end{aligned}
$$

where $k\in\mathbb{N}$ such that $\rho^k\geq(1-2\varepsilon')>\rho^{k+1}$, and M is a global constant (refer to Imported Theorem 2) and

$$\eta_p=(1+p^{-1/2}(1-p)^{-1/2})^{-1/2},\ \text{and}\ \eta_q=(1+q^{-1/2}(1-q)^{-1/2})^{-1/2}.$$

We provide the proof of Theorem 5 in Section 6.2 and the proof of Theorem 4 in Section 6.1. We highlight that the following junta theorem is the key to prove Theorem 5.

Imported Theorem 2 (Kindler and Safra[33])**.** *There exists a constant M such that for every $k\in\mathbb{N}$ the following holds. Let $f\colon\{-1,1\}^n\to\{-1,1\}$ be a Boolean function, define $\varepsilon:=\sum_{|S|>k}\left|\widehat{f}(S)\right|^2$, where $\widehat{f}(S)$ is with respect to p biased measure, denote $\tau:=\eta_p^{16k}/M$ (where $\eta_p=(1+p^{-1/2}(1-p)^{-1/2})^{-1/2}=O(p^{1/4})$). If $\varepsilon<\tau$ then f is $(1+1064\eta_p^{-4k}(2\varepsilon)^{1/4})\varepsilon$-close to a (k/τ)-junta.*

6.1 Proof of Theorem 4

Assuming Theorem 5, we prove the Theorem 4 as follows. According to Claim 1, it suffices to decide the problem with respect to our algebraic definition.

In the following, assuming (X, Y) is a 2-by-2 distribution, we prove that we can decide the problem for the constant $c = 5(1+\kappa)$ and any $\delta < \delta_0$ where δ_0 is introduced in Theorem 5. For YES instance, there exists $n \in \mathbb{N}$ and reduction functions $f_n, g_n \colon \{-1,1\}^n \to \{-1,1\}$ satisfying $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_n,g_n} (X,Y)^{\otimes n}$. Then, for an appropriate choice of parameters in Theorem 5, there exists functions $f_{n_0}, g_{n_0} \colon \{-1,1\}^{n_0} \to \{-1,1\}$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{(1+4d)\delta}_{f_{n_0},g_{n_0}} (X,Y)^{\otimes n_0}$ where n_0 is introduced in that theorem. Moreover, we set $d = 1+\kappa$ in Theorem 5. This implies the following:

$$\mathbb{E}[f_{n_0}] \le (5+4\kappa)\delta, \;\; \mathbb{E}[g_{n_0}] \le (5+4\kappa)\delta, \;\; \mathbb{E}[f_{n_0} g_{n_0}] \le (5+4\kappa)\delta \,,$$
$$\left\|T^{\otimes n_0} g_{n_0} - \rho' \cdot f_{n_0}\right\|_1 \le (5+4\kappa)\delta \,, \text{ and} \left\|\overline{T}^{\otimes n_0} f_{n_0} - \rho' \cdot g_{n_0}\right\|_1 \le (5+4\kappa)\delta \,,$$

for $\delta < \delta_0$ (for δ_0 refer to Theorem 5).

For NO instance, for all n, in particular $n = n_0$, there are no reduction functions $f_{n_0}, g_{n_0} \colon \{-1,1\}^{n_0} \to \{-1,1\}$ satisfying the following inequalities:

$$E[f_{n_0}] \le (5+5\kappa)\delta, \;\; \mathbb{E}[g_{n_0}] \le (5+5\kappa)\delta, \;\; \mathbb{E}[f_{n_0} g_{n_0}] \le (5+5\kappa)\delta \,,$$
$$\left\|T^{\otimes n_0} g_{n_0} - \rho' \cdot f_{n_0}\right\|_1 \le (5+5\kappa)\delta \,, \text{ and} \left\|\overline{T}^{\otimes n_0} f_{n_0} - \rho' \cdot g_{n_0}\right\|_1 \le (5+5\kappa)\delta.$$

Now, we brute force over all possible functions $f_{n_0}, g_{n_0} \colon \{-1,1\}^{n_0} \to \{-1,1\}$ to check if there exists any function satisfying $\mathsf{BSS}(\varepsilon') \sqsubseteq^{(5+4\kappa)\delta}_{f_{n_0},g_{n_0}} (X,Y)^{\otimes n_0}$ or not. If such reduction functions exist, then the algorithm outputs YES, and outputs NO otherwise. This brute force can be done in $\mathcal{O}\big(2^{2^{n_0}}\big)$ time.

6.2 Dimension Reduction

The proof of Theorem 5 follows from the step 2 and step 3 as described in Subsection 1.3. Let (X, Y) be a 2-by-2 distribution over $(\{-1,1\}, \{-1,1\})$ such that X and Y are respectively p-biased and q-biased distribution, and $\varepsilon' \in (0, 1/2)$. Let $\delta < \delta_0$, which will be specified later. We denote k to be the positive integer such that $\rho^k \ge \rho' > \rho^{k+1}$. Let M be the global constant in the Imported Theorem 2. It follows from Theorem 2 that $W^{>k}[f_n] \le \kappa\delta$ and $W^{>k}[g_n] \le \kappa\delta$, where $\kappa = \frac{(1+\rho')^2}{(\rho^{2(k+1)} - \rho'^2)^2}$.

We shall apply Imported Theorem 2 on function f_n. First, we set $\varepsilon = \kappa \cdot \delta$. We require $\delta \le (d/\kappa - 1)^4 \cdot \eta_p^{16k}/(2\kappa \cdot 1064^4)$ (for $d \ge \kappa$) to have $\kappa(1 + 1064\eta_p^{-4k}(2\kappa\delta)^{1/4}) \le d$ and so $(1 + 1064\eta_p^{-4k}(2\varepsilon)^{1/4})\varepsilon < d\delta$. Moreover, we need to have $\delta < \eta_p^{16k}/(M \cdot \kappa)$ to satisfy the condition $\varepsilon < \tau$ in the theorem. So we set $\delta_0(p) := \min(\eta_p^{16k}/(M \cdot \kappa), (d/\kappa - 1)^4 \cdot \eta_p^{16k}/(2\kappa \cdot 1064^4))$. Moreover, $J_p = k/\tau = kM/\eta_p^{16k}$. Similarly, we can apply Imported Theorem 2 on g_n and get $\delta_0(q) := \min(\eta_q^{16k}/(M \cdot \kappa), (d/\kappa - 1)^4 \cdot \eta_q^{16k}/(2\kappa \cdot 1064^4))$ and $J_q = k/\tau = kM/\eta_q^{16k}$. We set $\delta_0 = \min(\delta_0(p), \delta_0(q))$. It implies that there exist two junta functions $\tilde{f}_n, \tilde{g}_n \colon \{-1,1\}^n \to \{-1,1\}$ such that they are $2d\delta$-close to f_n, g_n in L_1 norm, respectively.

$$\left\|f_n - \tilde{f}_n\right\|_1 = 2\Pr[f_n(x^n) \ne \tilde{f}_n(x^n)] \le 2d\delta \,, \text{ and} \|g_n - \tilde{g}_n\|_1 = 2\Pr[g_n(x^n) \ne \tilde{g}_n(x^n)] \le 2d\delta.$$

Furthermore, $\tilde{f}_n$ and $\tilde{g}_n$ depend on $J_p = kM/\eta_p^{16k}$ and $J_q = kM/\eta_q^{16k}$ variables, respectively. Next, we show that the insecurity obtained when simulating $\mathsf{BSS}(\varepsilon')$ from (X, Y) using the reduction

functions $\tilde{f}_n, \tilde{g_n}$ is at most $(1+4d)\delta$. By triangle inequality and the contraction property of averaging operator, in particular Markov operator, we have

$$\begin{aligned}\left\|T^{\otimes n}\tilde{g_n} - \rho'\tilde{f}_n\right\|_1 &\le \left\|T^{\otimes n}\tilde{g_n} - T^{\otimes n}g_n\right\|_1 + \left\|T^{\otimes n}g_n - \rho' f_n\right\|_1 + \left\|\rho' f_n - \rho'\tilde{f}_n\right\|_1 \\ &\le \|g_n - \tilde{g_n}\|_1 + \left\|T^{\otimes n}g_n - \rho' f_n\right\|_1 + \rho'\left\|(f_n - \tilde{f}_n)\right\|_1 \\ &\le 2d\delta + \delta + 2\rho' d\delta = (1 + (2+2\rho')d)\delta \le (1+4d)\delta\end{aligned}$$

Similarly, we have $\left\|\overline{T}^{\otimes n}\tilde{f}_n - \rho'\tilde{g_n}\right\|_1 \le (1+4d)\delta$. Since f_n, g_n are $2d\delta$-close in L_1-norm to $\tilde{f}_n, \tilde{g_n}$, and $\mathbb{E}[f_n] \le \delta$, $\mathbb{E}[g_n] \le \delta$, it follows that $\mathbb{E}[\tilde{f}_n] \le (1+2d)\delta$ and $\mathbb{E}[\tilde{f}_n] \le (1+2d)\delta$. Using the fact that $\tilde{f}_n$ and $\tilde{g_n}$ are respectively J_p-junta and J_q-junta, there exist $n_0 = J_p + J_q = \mathcal{O}(k)$ and two functions $f_{n_0}, g_{n_0} \colon \Omega^{n_0} \to \{-1,1\}$ such that

$$\begin{aligned}&\left\|T^{\otimes n}\tilde{g_n} - \rho'\tilde{f}_n\right\|_1 = \left\|T^{\otimes n_0}g_{n_0} - \rho' f_{n_0}\right\|_1 \le (1+4d)\delta, \\ &\left\|T^{\otimes n}\tilde{f}_n - \rho'\tilde{g_n}\right\|_1 = \left\|T^{\otimes n_0}f_{n_0} - \rho' g_{n_0}\right\|_1 \le (1+4d)\delta, \text{ and} \\ &\mathbb{E}[f_{n_0}] = \mathbb{E}[\tilde{f}_n] \le (1+2d)\delta,\ \mathbb{E}[g_{n_0}] = \mathbb{E}[\tilde{g_n}] \le (1+2d)\delta.\end{aligned}$$

It implies that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{(1+4d)\delta}_{f_{n_0}, g_{n_0}} (X,Y)^{\otimes n_0}$, which completes the proof.

7 Decidability of SNIS: BSS from Arbitrary m-by-m Source

In this section, we shall restate and prove Informal Theorem 1.

Theorem 6 (Decidability-Additive-Gap)**.** *Let (X,Y) be a* redundancy-free *finite distribution over (Ω,Ω) with maximal correlation ρ and probability mass function π. Let $\varepsilon' \in (0,1/2)$ and $\delta > 0$ be an arbitrary insecurity parameter. There exists an algorithm running in bounded computable time $O(2^{|\Omega|^{n_0}})$ that distinguishes between the following two cases:*

1. *There exist a sequence of insecurity parameters $\delta_n = O(1/n)$ and a sequence of reduction functions $f_n, g_n \colon \Omega^n \to \{-1,1\}$ such that for infinitely many n, we have $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta_n}_{f_n,g_n} (X,Y)^{\otimes n}$.*
2. *For all $n \in \mathbb{N}$, and reduction functions $f_n, g_n \colon \Omega^n \to \{-1,1\}$, it is the case that $\mathsf{BSS}(\varepsilon') \not\sqsubseteq^{\delta}_{f_n,g_n} (X,Y)^{\otimes n}$.*

One may take $n_0 = (1/\lambda)^{\mathcal{O}((k+\kappa\cdot c_0)/\delta)}$, where $k \in \mathbb{N}$ satisfying $\rho^k \ge \rho' > \rho^{k+1}, \rho' = 1-2\varepsilon'$, $\kappa = \frac{(1+\rho')^2}{\rho^{2(k+1)} - \rho'^2}$, and λ is such that any outcome over (Ω,π_x) and (Ω,π_y) has probability at least λ.

The following result is the main technical lemma for the proof of the above theorem.

Theorem 7. *Let (X,Y) be a* redundancy-free *finite distribution over (Ω,Ω) with maximal correlation ρ and probability mass function π. Let $\varepsilon' \in (0,1/2)$. For any constant $\delta' > 0$, there exists $n_0 \in \mathbb{N}$ such that for any sequence of insecurity parameters $\delta_n \le c_0/n$, for some constant $c_0 > 0$, and any sequence of reduction functions $f_n, g_n \colon \Omega^n \to \{-1,1\}$ satisfying $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta_n}_{f_n,g_n} (X,Y)^{\otimes n}$, there exist functions $f_{n_0}, g_{n_0} \colon \Omega^{n_0} \to \{-1,1\}$ such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{5\delta'}_{f_{n_0},g_{n_0}} (X,Y)^{\otimes n_0}$.*

Furthermore, n_0 is a computable function in the parameters of the problem. In particular, one may take $n_0 = (1/\lambda)^{\mathcal{O}((k+\kappa\cdot c_0)/\delta')}$, where $k \in \mathbb{N}$ satisfying $\rho^k \ge 1-2\varepsilon' > \rho^{k+1}$, $\kappa = \frac{(1+\rho')^2}{\rho^{2(k+1)} - \rho'^2}$, and λ is such that any outcome over (Ω,π_x) and (Ω,π_y) has probability at least λ.

To prove this, we shall apply Imported Theorem 3. Intuitively, it says that, for any Boolean-valued functions with the total influence at most K, there exits a $2^{\mathcal{O}(K)}$-junta function that is close to the given function in L_1-norm.

Imported Theorem 3. ***Friedgut's Junta Theorem for general product space domains****[17, 43]: 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 $\{-1, 1\}$ and $0 < \varepsilon \leq 1$, then f is ε-close to a $(1/\lambda)^{O(I[f]/\varepsilon)}$-junta $h\colon \Omega^n \to \{-1, 1\}$, i.e., $\Pr_{x^n \sim \pi^{\otimes n}}[f(x^n) \neq h(x^n)] \leq \varepsilon$.*

7.1 Proof of Theorem 6

Assuming Theorem 7, we present the proof of Theorem 6 as follows. At a high level idea the proof is similar to the proof of Theorem 4. Suppose we are in YES instance, then let $\delta' = \delta/5$ and invoke Theorem 7 to get the constant $n_0 \in \mathbb{N}$. Then, we are sure that there exist reduction functions f_{n_0} and g_{n_0} such that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_{n_0}, g_{n_0}} (X, Y)^{\otimes n_0}$.

Now, suppose we are in NO instance, then for any n (in particular for $n = n_0$) we have $\mathsf{BSS}(\varepsilon') \not\sqsubseteq^{\delta}_{f_n, g_n} (X, Y)^{\otimes n}$. We brute force over all functions $f_{n_0}, g_{n_0}\colon \Omega^n \to \{-1, 1\}$ for n_0 mentioned in Theorem 7. If there exists any pair of reduction functions f_{n_0}, g_{n_0} satisfying $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_{n_0}, g_{n_0}} (X, Y)^{\otimes n_0}$, output YES, otherwise output NO. The running time of this algorithm is $O(2^{|\Omega|^{n_0}})$.

7.2 Dimension Reduction

The proof of Theorem 7 is similar to the proof of Theorem 5 except applying Friedgut's junta theorem instead of Kindler and Safra's junta theorem in the dimension reduction step.

This section presents the proof of Theorem 7. Let (X, Y) be a finite distribution over (Ω, Ω), and $\varepsilon' \in (0, 1/2)$. Let $\delta' > 0$. For any $n \geq c_0/\delta'$, which implies that $\delta_n = c_0/n \leq \delta'$, satisfying $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta_n}_{f_n, g_n} (X, Y)^{\otimes n}$, it follows from Corollary 2 that the total influence of both f_n and g_n are at most $k + \kappa \cdot c_0$. By Imported Theorem 3, there exist two J-junta functions $\tilde{f_n}, \tilde{g_n}\colon \Omega^n \to \{-1, 1\}$ such that

$$\left\| f_n - \tilde{f_n} \right\|_1 = 2 \Pr[f_n(x^n) \neq \tilde{f_n}(x^n)] \leq 2\delta' \,, \|g_n - \tilde{g_n}\|_1 = 2 \Pr[g_n(x^n) \neq \tilde{g_n}(x^n)] \leq 2\delta' \,,$$

and $|J| = (1/\lambda)^{\mathcal{O}((k+\kappa \cdot c_0)/\delta')}$, where λ is the constant defined in Imported Theorem 3. Next, we show that the insecurity obtained when simulating $\mathsf{BSS}(\varepsilon')$ from (X, Y) using the reduction functions $\tilde{f_n}, \tilde{g_n}$ is at most $5\delta'$. By Triangle inequality and the contraction property of averaging operator, in particular Markov operator, we have

$$\begin{aligned}
\left\| T^{\otimes n} \tilde{g_n} - \rho' \tilde{f_n} \right\|_1 &\leq \left\| T^{\otimes n} \tilde{g_n} - T^{\otimes n} g_n \right\|_1 + \left\| T^{\otimes n} g_n - \rho' f_n \right\|_1 + \left\| \rho' f_n - \rho' \tilde{f_n} \right\|_1 \\
&= \left\| T^{\otimes n} (\tilde{g_n} - g_n) \right\|_1 + \left\| T^{\otimes n} g_n - \rho' f_n \right\|_1 + \left\| \rho' (f_n - \tilde{f_n}) \right\|_1 \\
&\leq \|g_n - \tilde{g_n}\|_1 + \left\| T^{\otimes n} g_n - \rho' f_n \right\|_1 + \rho' \left\| (f_n - \tilde{f_n}) \right\|_1 \\
&\leq 2\delta' + \frac{c_0}{n} + \rho'(2\delta') \leq 5\delta'
\end{aligned}$$

Similarly, we have $\left\| \overline{T}^{\otimes n} \tilde{f_n} - \rho' \tilde{g_n} \right\|_1 \leq 5\delta'$. Since f_n, g_n are δ'-close in L_1-norm to $\tilde{f_n}, \tilde{g_n}$, and $\mathbb{E}[f_n] \leq 2\delta'$, $\mathbb{E}[g_n] \leq 2\delta'$, it follows that $\mathbb{E}[\tilde{f_n}] \leq 3\delta'$ and $\mathbb{E}[\tilde{f_n}] \leq 3\delta'$. Using the fact that $\tilde{f_n}$ and $\tilde{g_n}$ are junta functions, there exist $n_0 = (1/\lambda)^{\mathcal{O}((k+\kappa \cdot c_0)/\delta')}$ and two functions $f_{n_0}, g_{n_0}\colon \Omega^{n_0} \to \{-1, 1\}$ such that

$$\left\| T^{\otimes n} \tilde{g_n} - \rho' \tilde{f_n} \right\|_1 = \left\| T^{\otimes n_0} g_{n_0} - \rho' f_{n_0} \right\|_1, \text{ and}$$

$$\left\| T^{\otimes n} \tilde{f}_n - \rho' \tilde{g_n} \right\|_1 = \left\| T^{\otimes n_0} f_{n_0} - \rho' g_{n_0} \right\|_1, \text{ and}$$
$$\mathbb{E}[f_{n_0}] = \mathbb{E}[\tilde{f}_n] \leq 3\delta', \text{ and } \mathbb{E}[g_{n_0}] = \mathbb{E}[\tilde{g_n}] \leq 3\delta'.$$

It implies that $\mathsf{BSS}(\varepsilon') \sqsubseteq^{5\delta'}_{f_{n_0}, g_{n_0}} (X, Y)^{\otimes n_0}$, which completes the proof.

References

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

[2] 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. 10

[3] 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. 10

[4] Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *IEEE Trans. Inf. Theory*, 57(10):6351–6355, 2011. 1

[5] Christer Borell. Geometric bounds on the ornstein-uhlenbeck velocity process. *Probability Theory and Related Fields*, 70(1):1–13, 1985. 32

[6] Jean Bourgain. On the distribution of the fourier spectrum of boolean functions. *Israel Journal of Mathematics*, 131(1):269–276, 2002. 7

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

[8] 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. 1

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

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

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

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

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

[14] Anindya De, Elchanan Mossel, and Joe Neeman. Non interactive simulation of correlated distributions is decidable. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2728–2746. SIAM, 2018. 2, 3, 5, 7, 32

[15] Bradley Efron and Charles Stein. The jackknife estimate of variance. *The Annals of Statistics*, pages 586–596, 1981. 12

[16] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *CRYPTO'82*, pages 205–210. Plenum Press, New York, USA, 1982. 4

[17] Ehud Friedgut. Boolean functions with low average sensitivity depend on few coordinates. *Comb.*, 18(1):27–35, 1998. 5, 7, 22

[18] Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973. 1, 2

[19] 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. 1

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

[21] 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-Zentrum für Informatik, 2018. 2, 3, 5, 7, 32

[22] Badih Ghazi, Pritish Kamath, and Madhu Sudan. Decidability of non-interactive simulation of joint distributions. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 545–554. IEEE, 2016. 2, 3, 5, 7, 32, 33

[23] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987. 1

[24] 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. 10

[25] 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. 1, 3, 4

[26] 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. 1

[27] Amisha Jhanji, Hemanta K. Maji, and Raphael Arkady Meyer. Characterizing optimal security and round-complexity for secure OR evaluation. In *2017 IEEE International Symposium on Information Theory, ISIT 2017, Aachen, Germany, June 25-30, 2017*, pages 2703–2707. IEEE, 2017. 4

[28] 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. 1, 2, 3, 4, 5, 6, 9, 34

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

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

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

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

[33] Guy Kindler and Shmuel Safra. Noise-resistant boolean functions are juntas. *preprint*, 2002. 5, 7, 19

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

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

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

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

[38] 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. 11, 12

[39] Elchanan Mossel. Gaussian bounds for noise correlation of functions. *Geometric and Functional Analysis*, 19(6):1713–1756, 2010. 5, 6, 12, 32

[40] Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Structures & Algorithms*, 26(4):418–436, 2005. 1

[41] Elchanan Mossel, Ryan O'Donnell, and Krzysztof Oleszkiewicz. Noise stability of functions with low infuences: Invariance and optimality. In *46th FOCS*, pages 21–30. IEEE Computer Society Press, October 2005. 32

[42] 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. 1

[43] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. 9, 12, 22

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

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

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

[47] Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975. 1, 2, 10, 11, 12, 32, 33

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

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

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

[51] Aaron Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975. 1, 2

[52] 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. 1

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

A Proof of Claim 1

We use a hybrid-argument to prove this claim. Without loss of generality, we can assume that the simulator will reverse sample x^n from the input u. That is, for every $u \in \{-1,1\}$ the Sim_A outputs x^n with probability 0 if $x^n \notin f_n^{-1}(u)$ since if there is such an x^n we can construct a new simulator that shifts the probability of that x^n to the probability of some other element in $f^{-1}(u)$ and achieve the security at least as good as the original simulator. Observe that on an input $u \in \{-1,1\}$ a "good" simulator should reverse sample x^n, which implies that any "good" simulator behaves almost the same as $\overline{\mathrm{Sim}_A}$.

From these observations, we define a $\overline{\mathrm{Sim}_A}(u)$ as follows. On input u, it outputs x^n with probability $2\Pr[X^n = x^n]$ if $x^n \in f_n^{-1}(u)$ and with probability 0 otherwise. Effectively, $\mathrm{Sim}_A(U)$ outputs x^n with $\Pr[X^n = x^n]$. First, we claim that

$$\mathsf{SD}\left(\left(\overline{\mathrm{Sim}_A}(U), U, V\right) , \ (X^n, f_n(X^n), g_n(Y^n)) \right) = \left\| T^{\otimes n} g_n - \rho' f_n \right\|_1.$$

Intuitively, the quantity $|T^{\otimes n} g_n(x^n) - \rho' f_n(x^n)|$ measures how good the simulation is on input x^n. Note that it might be the case that $\overline{\mathrm{Sim}_A(x)}$ is not a valid simulator if for any $u \in \{-1,1\}$, $2\sum_{x^n \in f^{-1}(u)} \Pr[X^n = x^n] \neq 1$.

Forward Implication. If $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta}_{f_n, g_n} (X,Y)^{\otimes n}$, there exists a simulator $\mathrm{Sim}_A \colon \{-1,1\} \to \Omega^n$ such that

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

By the discussion above, it must be the case that $\mathrm{Sim}_(A)$ is δ-close to $\overline{\mathrm{Sim}_A}$. Therefore, by triangle inequality, one can conclude that

$$\left\| T^{\otimes n} g_n - \rho' f_n \right\|_1 \leq \mathsf{SD}\left(\left(\mathrm{Sim}_A(U), U, V\right) , \ (X^n, f_n(X^n), g_n(Y^n)) \right) + \delta \leq 2\delta$$

The inequalities $\mathbb{E}[f_n] \leq \delta$ follows from the fact that $f_n(X^n)$ is δ-close to U, which is a uniform distribution for BSS. Similarly, we have $\mathbb{E}[g_n] \leq \delta$ and $\left\| \overline{T}^{\otimes n} f_n - \rho' g_n \right\|_1 \leq 2\delta$.

Reverse Implication. Suppose there exist function f_n, g_n such that $\mathbb{E}[f_n] \leq \delta$, $\mathbb{E}[g_n] \leq \delta$, $\|T^{\otimes n} g_n - \rho' \cdot f_n\|_1 \leq \delta$, and $\left\| \overline{T}^{\otimes n} f_n - \rho' \cdot g_n \right\|_1 \leq \delta$. Recall that if $2\sum_{x^n \in f^{-1}(u)} \Pr[X^n = x^n] \neq 1$, then $\overline{\mathrm{Sim}_A}$ is not a valid simulator. However, this will not be an issue since from the fact that $\mathbb{E}[f_n] \leq \delta$, we can construct a valid simulator Sim_A from $\overline{\mathrm{Sim}_A}$ with incurring at most additional δ insecurity. Therefore, the simulation error is at most 2δ.

We provide more details of the discussion above as follows. Suppose $\mathrm{Sim}_A(u)$ outputs x^n with probability $2(\Pr[X^n = x^n] + \varepsilon_{x^n})$ if $x^n \in f_n^{-1}(u)$, and with probability 0 otherwise, where $\varepsilon_{x^n} \in [0,1]$. This implies that $\mathrm{Sim}_A(U)$ outputs x^n with probability $\Pr[X^n = x^n] + \varepsilon_{x^n}$. Clearly $\mathsf{SD}\left(\mathrm{Sim}_A(U), X^n\right) \leq \delta$, which implies that $\sum_{x^n} |\varepsilon_{x^n}| \leq \delta$. Similarly, $\mathbb{E}[f_n(X^n)] \leq \delta$ since $\mathsf{SD}\left(f_n(X^n), U\right) \leq \delta$.

Observe that, for a fixed $x^n \in f^{-1}(1)$, the three quantities $\frac{1}{2}|(T^{\otimes n} g_n)(x^n) - \rho' f_n(x^n)|$, and $|\Pr[g_n(Y^n) = 1 | X^n = x^n,] - (1 - \varepsilon')|$, and $|\Pr[g_n(Y^n) = -1 | X^n = x^n] - \varepsilon'|$ are the same. Using this fact, we have

$$\begin{aligned}
&\left\| T^{\otimes n} g_n - \rho' \cdot f_n \right\|_1 \\
&= \mathbb{E}\left| (T^{\otimes n} g_n - \rho' \cdot f_n)(X^n) \right| \\
&= \sum_{x^n} \Pr[X^n = x^n] \cdot \left| (T^{\otimes n} g_n)(x^n) - \rho' \cdot f_n(x^n) \right| \\
&= \sum_{x^n} \Pr[X^n = x^n] \cdot \left| (T^{\otimes n} g_n)(x^n) - \rho' \cdot f_n(x^n) \right|
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{x^n} \Pr[X^n = x^n] \cdot \left|\Pr[g_n(Y^n) = 1 | X^n = x^n] - (1-\varepsilon')\right| \\
&+ \sum_{x^n} \Pr[X^n = x^n] \cdot \left|\Pr[g_n(Y^n) = -1 | X^n = x^n] - \varepsilon'\right| \\
&= \mathsf{SD}\left(\left(\overline{\mathrm{Sim}_A}(U), U, V\right) , \ (X^n, f_n(X^n), g_n(Y^n)) \right)
\end{aligned}
$$

Using this equation, one can verify that, by triangle inequality,

$$
\begin{aligned}
&\mathsf{SD}\left(\left(\mathrm{Sim}_A(U), U, V\right) , \ (X^n, f_n(X^n), g_n(Y^n)) \right) \\
&\geq \mathsf{SD}\left(\left(\overline{\mathrm{Sim}_A}(U), U, V\right) , \ (X^n, f_n(X^n), g_n(Y^n)) \right) - \sum_{x^n} |\varepsilon_{x^n}| \\
&= \left\| T^{\otimes n} g_n - \rho' \cdot f_n \right\|_1 - \sum_{x^n} |\varepsilon_{x^n}|
\end{aligned}
$$

which implies that $\|T^{\otimes n} g_n - \rho' \cdot f_n\|_1 \leq 2\delta$ since $\sum_{x^n} |\varepsilon_{x^n}| \leq \delta$. With an analogous argument, one can show that $\left\| \overline{T}^{\otimes n} f_n - \rho' \cdot g_n \right\|_1 \leq 2\delta$ and $\mathbb{E}[g_n] \leq \delta$.
The proof of the other direction is similar.

B Omitted Proofs in Section 3

B.1 Proof of Claim 4

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

$$
\begin{aligned}
T^{\otimes n} \psi_S(x^n) &= \mathbb{E}[\psi_S(Y^n) | X^n = x^n] \\
&= \mathop{\mathbb{E}}_{y^n \sim (Y^n | X^n = x^n)} \prod_{i \in S} \left(\frac{y_i - \mu_y}{\sigma_y} \right) \\
&= \prod_{i \in S} \mathop{\mathbb{E}}_{y_i \sim (Y_i | X_i = x_i)} \left(\frac{y_i - \mu_y}{\sigma_y} \right) \\
&= \prod_{i \in S} \rho \cdot \left(\frac{x_i - \mu_x}{\sigma_x} \right) && \textit{Claim 10} \\
&= \rho^{|S|} \phi_S(x^n)
\end{aligned}
$$

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

Claim 10. *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

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

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

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 either of the cases, it's always the case 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 proof.

C Omitted Proofs in Section 4

First we prove that if a real-valued function is bounded and its L_1 norm is bounded, then the L_2 norm of this function is also bounded.

Claim 11. *Suppose $f \in L^2(\Omega, \mu)$ such that $\|f\|_1 \le \alpha$ and $|f(x)| \le \beta$ for every $x \in \Omega$. Then, we have $\|f\|_2^2 \le \alpha\beta$.*

Proof. We have

$$\|f\|_2^2 = \mathbb{E}[f(x)^2] = \mathbb{E}[|f(x)|^2] \le \mathbb{E}[|f(x)| \cdot \beta] = \beta \cdot \mathbb{E}[|f(x)|] = \beta \cdot \|f\|_1 \le \alpha\beta.$$

□

C.1 Proof of claims needed in Theorem 2

First we recall the notation. Let $\rho \in [0,1]$ and $\varepsilon' \in (0,1/2)$. Let (X,Y) be a joint distribution over (Ω,Ω) with probability mass function π and maximal correlation ρ. Let T and $\overline{T}$ denote respectively the Markov operator and the corresponding adjoint operator associated with the distribution (X,Y). Note that $f_n \in L^2(\Omega^n, {\pi_x}^{\otimes n})$, $g_n \in L^2(\Omega^n, {\pi_y}^{\otimes n})$, $T^{\otimes n} g_n \in L^2(\omega^n, {\pi_x}^{\otimes n})$, and $\overline{T}^{\otimes n} f_n \in L^2(\omega^n, {\pi_y}^{\otimes n})$. Let $f_n = \sum_{S\subseteq[n]} f_n^{=S}$, and $g_n = \sum_{S\subseteq[n]} g_n^{=S}$ be the Efron-stein decompositions of f_n and g_n.

C.1.1 Proof of Claim 6

Since $\mathsf{BSS}(\varepsilon') \sqsubseteq^{\delta_n}_{f_n,g_n} (X,Y)^{\otimes n}$, we have two inequalities $\|T^{\otimes n} g_n - \rho' f_n\|_1 \le \delta_n$ and $\left\|\overline{T}^{\otimes n} f_n - \rho' g_n\right\|_1 \le \delta_n$. Note that $(T\overline{T})^{\otimes n} f_n \in L^2(\Omega^n, {\pi_x}^{\otimes n})$. Applying triangle inequality and contraction property of averaging operator, we get

$$\begin{aligned}
&\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2 f_n\right\|_1 \\
&\le \left\|(T\overline{T})^{\otimes n} f_n - \rho' T^{\otimes n} g_n\right\|_1 + \left\|\rho' T^{\otimes n} g_n - \rho'^2 f_n\right\|_1 \\
&= \left\|T^{\otimes n}\left(\overline{T}^{\otimes n} f_n - \rho' g_n\right)\right\|_1 + \rho' \left\|T^{\otimes n} g_n - \rho' f_n\right\|_1 \\
&\le \left\|\overline{T}^{\otimes n} f_n - \rho' g_n\right\|_1 + \rho' \left\|T^{\otimes n} g_n - \rho' f_n\right\|_1 \\
&\le (1+\rho')\delta_n
\end{aligned}$$

Similarly, we have $\left\|(\overline{T}T)^{\otimes n} g_n - \rho'^2 \cdot g_n\right\|_1 \le (1+\rho')\delta_n$. Next, by a direct application of Claim 11 yields

$$\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2 \cdot f_n\right\|_2^2 \le (1+\rho')^2\delta_n, \text{ and } \left\|(\overline{T}T)^{\otimes n} g_n - \rho'^2 \cdot g_n\right\|_2^2 \le (1+\rho')^2\delta_n.$$

C.1.2 Proof of Claim 7

By Proposition 6, we have $\left\|T^{\otimes n} f_n^{=S}\right\|_2 \le \rho^{|S|}\left\|f_n^{=S}\right\|_2$, which implies that $\left\|T^{\otimes n} f_n^{=S}\right\|_2 \le \rho^{|S|}\left\|f_n^{=S}\right\|_2 \le \rho'\left\|f_n^{=S}\right\|_2$ when $|S| > k$. Therefore, we have

$$\left\|T^{\otimes n} f_n^{=S}\right\|_2 - \rho'^2 \cdot \left\|f_n^{=S}\right\|_2 \le \rho^{2|S|} \cdot \left\|f_n^{=S}\right\|_2 - \rho'^2 \cdot \left\|f_n^{=S}\right\|_2 \le 0$$

Taking the absolute value of both sides yields

$$\left|\left\|T^{\otimes n} f_n^{=S}\right\|_2 - \rho'^2 \cdot \left\|f_n^{=S}\right\|_2\right| \ge \left|\rho^{2|S|} \cdot \left\|f_n^{=S}\right\|_2 - \rho'^2 \cdot \left\|f_n^{=S}\right\|_2\right|.$$

C.1.3 Proof of Claim 8

By orthogonal property of Efron-Stein decomposition and the commute property (Proposition 5), we have

$$\begin{aligned}
\left\|(T\overline{T})^{\otimes n} f_n - \rho'^2 \cdot f_n\right\|_2^2 &= \left\|(T\overline{T})^{\otimes n}\left(\sum_S f_n^{=S}\right) - \rho'^2 \cdot \sum_{S\subseteq[n]} f_n^{=S}\right\|_2^2 \\
&= \left\|\sum_{S\subseteq[n]}\left((T\overline{T})^{\otimes n} f_n^{=S} - \rho'^2 \cdot f_n^{=S}\right)\right\|_2^2
\end{aligned}$$

$$= \sum_{S\subseteq[n]} \left\| (T\overline{T})^{\otimes n} f_n^{=S} - \rho'^2 \cdot f_n^{=S} \right\|_2^2$$

When $\Omega = \{-1, 1\}$, let ϕ_S and ψ_S be two Fouier basis with respect to π_x and π_y respectively. We have

$$\begin{aligned}
&\sum_{S\subseteq[n]} \left\| (T\overline{T})^{\otimes n} f_n^{=S} - \rho'^2 \cdot f_n^{=S} \right\|_2^2 \\
&= \sum_{S\subseteq[n]} \left\| (T\overline{T})^{\otimes n} \left(\widehat{f_n}(S) \cdot \phi_S \right) - \rho'^2 \cdot \widehat{f_n}(S) \cdot \phi_S \right\|_2^2 && \textit{Claim 4} \\
&= \sum_{S\subseteq[n]} \widehat{f_n}(S)^2 \cdot \left\| (T\overline{T})^{\otimes n} \phi_S - \rho'^2 \cdot \phi_S \right\|_2^2 \\
&= \sum_{S\subseteq[n]} \widehat{f_n}(S)^2 \cdot \sum_{R\subseteq[n]} \left(\widehat{(T\overline{T})^{\otimes n}} \phi_S(R) - \rho'^2 \cdot \widehat{\phi_S}(R) \right)^2 && \text{Parseval} \\
&= \sum_{S\subseteq[n]} \widehat{f_n}(S)^2 \left(\rho^{2|S|} - \rho'^2 \right)^2 && \textit{Claim 5}
\end{aligned}$$

which completes the proof.

C.1.4 Proof of Claim 9

By triangle inequality, we have

$$\left\| T^{\otimes n} g_n \right\|_1 = \mathop{\mathbb{E}}_{x^n \in \pi_x{}^{\otimes n}} |\mathbb{E}[g_n(Y^n)|X^n = x^n]| \le \mathop{\mathbb{E}}_{x^n \in \pi_x{}^{\otimes n}} \mathbb{E}[|g_n(Y^n)||X^n = x^n] = \mathop{\mathbb{E}}_{x^n \in \pi_x{}^{\otimes n}} 1 = 1$$

where (X^n, Y^n) is sampled according to π. Since the range of g_n is $\{-1, 1\}$, it is clearly that $\|g_n\|_1 = 1$. Similarly $\left\| \overline{T}^{\otimes n} f_n \right\|_1 \le \|f_n\|_1 = 1$.

D Discussion on The Techniques Used in Related Work

In this section, we shall first review the approaches used in [22, 14, 21] to prove that the non-interactive simulation (NIS) problem is decidable and then discuss the bottlenecks of using them to prove the decidability of the secure non-interactive simulation (SNIS) problem.

In [22], for the first time, the authors prove that the gap version of NIS is decidable. They solve this problem for the case that the target distribution is a 2-by-2 joint distribution. Their main contribution is reducing the problem to the case that the source distribution is one sample of correlated Gaussian distribution. Then, combining Witsenhausen [47], and an invariance principle introduced in [41, 39] (inspired by Borell's noise stability theorem [5]) provides them with a precise characterization of joint distributions that can be simulated from a correlated Gaussian distribution. However, when the target distribution is k-by-k for some $k > 2$, then their approach is not enough for two main reasons: First, Borrel's theorem is not available for $k > 2$, second, for $k > 2$ it is not the case that a distribution (U, V) can be specified by $\mathbb{E}[U], \mathbb{E}[V]$ and $\Pr[U = V]$.

The authors of [14] manage to address this issue by following a similarly high-level framework of using regularity lemma and invariance principle introduced in [22] and some more advanced techniques like a new smoothing argument inspired by learning theory and potential function argument in complexity theory. In [21], the authors use a different approach from [14], and they combine the

framework of [22] with a new result (NIS from Gaussian sources) to solve the problem for general $k \geq 2$.

Finally, they use Witsenhausen's theorem to simulate this threshold function applied on a Gaussian sample using a constant number of source samples.

Next, we discuss the bottlenecks of using these approaches to proving the decidability of SNIS problem. We do not see a straightforward way of applying these approaches to SNIS problem. All three papers reduce the reduction functions to low degree functions by a smoothening step. However, this step does not seem to apply to the SNIS setting. The first reason is that smoothening might not preserve the security conditions. Moreover, the second reason is that it changes the range of functions to non-Boolean values, preventing Friedgut's junta theorem used in our technique. Consequently, we need to do rounding in the later step. While rounding preserves the correlation in NIS, it likely does not maintain the security conditions in secure-NIS. Furthermore, simulating correlated Gaussians from independent samples using the central limit theorem is insecure. It is unclear whether one can simulate correlated Gaussian samples securely or not.

Finally, we discuss in more detail the bottleneck of applying the approach in [22] to SNIS problem. The invariance principle guarantees that the correlation of two low-influential functions is almost the same as the correlation of appropriate threshold functions applied on one sample of a ρ-correlated Gaussian distribution. Lemma 1 is one of the key steps in [22].

Definition 9 (Gaussian Stability)**.** *[22] Let Φ be the cumulative distribution function (CDF) of a standard $\mathcal{N}(0,1)$ gaussian distribution and (G_1, G_2) be a ρ-correlated gaussian distribution. Given $\rho \in [-1,1]$ and $\mu, \nu \in [-1,1]$, define*

$$\overline{P}_\mu(G_1) := sign\left(\Phi^{-1}\left(\frac{1+\mu}{2}\right) - G_1\right)$$

$$\overline{Q}_\nu(G_2) := sign\left(\Phi^{-1}\left(\frac{1+\nu}{2}\right) - G_2\right)$$

$$\overline{\Gamma}_\rho(\mu,\nu) := \mathbb{E}[\overline{P}_\mu(G_1) \cdot \overline{Q}_\nu(G_2)]$$

$$\underline{\Gamma}_\rho(\mu,\nu) := -\mathbb{E}[\overline{P}_\mu(G_1) \cdot \overline{Q}_{-\nu}(G_2)].$$

Note that $\mathbb{E}[\overline{P}_\mu(G_1)] = \mu$ and $\mathbb{E}[\overline{Q}_\nu(G_2)] = \nu = \mathbb{E}[-\overline{Q}_{-\nu}(G_2)]$.

Lemma 1 (Simulating Threshold on gaussians)**.** *[47] For any joint distribution (X,Y) with maximal correlation ρ, any arbitrary $\zeta > 0$, there exists $n \in \mathbb{N}$ ($n = O(\frac{1+\rho}{\alpha\cdot(1-\rho)^3\cdot\zeta^2})$) such that for all $\mu, \nu \in [-1,1]$, there exist functions $P_\mu \colon X^n \to [-1,1]$ and $Q_\nu \colon Y^n \to [-1,1]$ such that $|\mathbb{E}[P_\mu] - \mu| \leq \zeta/2, |\mathbb{E}[Q_\nu] - \nu| \leq \zeta/2$ and*

$$\left|\mathbb{E}[P_\mu(X^n)Q_\nu(Y^n)] - \overline{\Gamma}_\rho(\mu,\nu)\right| \leq \zeta$$

Now, we claim that above lemma does not necessarily provide us with a secure simulation. The reason is that for $\mu = \nu = \frac{1}{2}$, the joint distribution $(\overline{P}_\mu(G_1), \overline{Q}_\nu(G_2))$ is BSS when (G_1, G_2) is a ρ-correlated Gaussian distribution. Suppose that the parameter of this BSS is ε'. Now, if we choose (X,Y) to be a redundancy-free 2-by-2 joint distribution with a maximal correlation τ such that there is no integer k satisfying $\tau^{2k} = (1-2\varepsilon')^2$, according to Corollary 1 there will be a lower bound on minimum insecurity. This implies that the constructions in Lemma 1 might be insecure.

E Secure Non-Interactive Simulation: Definition

We recall the notion of secure non-interactive simulation of joint distributions using a simulation-based security definition as defined in [28].

If there exists reductions functions f_n, g_n such that the insecurity is at most $\delta(n)$ as defined above then we say that (U,V) *reduces to* $(X,Y)^{\otimes n}$ *via reduction functions* f_n, g_n *with insecurity at most* $\delta(n)$, represented by $(U,V) \sqsubseteq^{\delta(n)}_{f_n,g_n} (X,Y)^{\otimes n}$. Suppose (X,Y) is a joint distribution over the sample space $\mathcal{X} \times \mathcal{Y}$, and (U,V) be a joint distribution over the sample space $\mathcal{U} \times \mathcal{V}$. For $n \in \mathbb{N}$, suppose $f_n \colon \mathcal{X}^n \to \mathcal{U}$ and $g_n \colon \mathcal{Y}^n \to \mathcal{V}$ be two reduction functions.

In the real world, we have the following experiment.

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

The following conditions are required for the security.

1. **The case of no corruption.** Suppose the environment does not corrupt any party. So, it receives (U,V) as output from the two parties in the ideal world. In the real world, the simulator receives $(f_n(X^n), g_n(Y^n))$ as output. If this reduction has at most $\delta(n)$ insecurity, then the following must hold.

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

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

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

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

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

Definition 10 (Secure Non-interactive Simulation)**.** *Let (X,Y) be a joint distribution over the sample space $(\mathcal{X}, \mathcal{Y})$, and (U,V) be a joint distribution over the sample space $(\mathcal{U}, \mathcal{V})$. We say that the distribution (U,V) can be securely and non-interactively simulated using distribution (X,Y), denoted as $(U,V) \sqsubseteq (X,Y)$, if there exists $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$ there exist reduction functions $f_n \colon \mathcal{X}^n \to \mathcal{U}$, $g_n \colon \mathcal{Y}^n \to \mathcal{V}$, and insecurity bound $\delta(n)$ satisfying*

$$(U,V) \sqsubseteq^{\delta(n)}_{f_n,g_n} (X,Y)^{\otimes n}, \ \textit{and} \ \lim_{n \to \infty} \delta(n) = 0.$$

F Derandomization

In this section, we shall show that without loss of generality, we can assume that the reduction functions are deterministic.

Theorem 8. *Let (U,V) and (X,Y) be two joint distributions. Let $n \in \mathbb{N}$ and $\nu(n) \geq 0$. Suppose there exist randomized reduction functions $f\colon \mathcal{X}^n \times \mathcal{R}_A \to \mathcal{V}$, and $g\colon \mathcal{Y}^n \times \mathcal{R}_B \to \mathcal{U}$ such that $(U,V) \sqsubseteq_{f,g}^{\nu(n)} (X,Y)^{\otimes n}$. Then, there exist $\eta \in \mathbb{N}$, and deterministic reduction functions $f'\colon \mathcal{X}^\eta \to \mathcal{U}$, and $g'\colon \mathcal{Y}^\eta \to \mathcal{V}$ such that $(U,V) \sqsubseteq_{f',g'}^{4\nu(n)} (X,Y)^{\otimes \eta}$. In particular, when $\mathcal{R}_A = \mathcal{R}_B = \{0,1\}^k$ (uniform bits), where $k \leq n^c$ for some constant c, and $\nu(n) \geq 2^{-n^c}$, then $\eta = O(n^c)$.*

Theorem 8 shows that for any two randomized reduction functions whose insecurity bound is $\nu(n)$, there always exist deterministic reductions using more samples while the insecurity bound is guaranteed to be $4\nu(n)$. This result implies that in order to solve gap decidability of SNIS, it suffices to assume that the reductions are deterministic.

F.1 Preliminaries

First, we mention some tools that we will use in our proofs.
The min-entropy of a random variable X is defined as follows:

$$H_\infty(X) = \min_x \left(\log \frac{1}{\Pr[X = x]} \right).$$

Let (X,Y) be a joint distribution. The average min-entropy of the conditional distribution $X|Y$ is defined as

$$H_\infty(X|Y) = \log \left(\frac{1}{\mathbb{E}_y[\max_x(\Pr[X = x|Y = y])]} \right),$$

which is equal to $-\log\left(\mathbb{E}_y[2^{-H_\infty(X|Y=y)}]\right)$.

The convolution of two functions $f, g\colon \{0,1\}^n \to \mathbb{R}$ is a function $(f * g)\colon \{0,1\}^n \to \mathbb{R}$ defined as

$$(f * g)(x^n) = \frac{1}{2^n} \sum_{y^n \in \{0,1\}^n} f(y^n) g(x^n \oplus y^n).$$

Suppose X and Y are two functions which represents the probability distribution over $\{0,1\}^n$, then $2^n(X * Y)$ is the function that corresponds to the probability distribution of $X \oplus Y$. It can be verified that $\widehat{(f * g)}(S) = \widehat{f}(S) \cdot \widehat{g}(S)$. This implies that $\widehat{(X \oplus Y)}(S) = 2^n \cdot \widehat{X}(S) \cdot \widehat{Y}(S)$. Therefore, if $X_1, X_2, \ldots, X_\eta$ are η random variables defined over $\{0,1\}^n$, then

$$\widehat{\bigoplus_{i=1}^\eta X_i}(S) = 2^{n(\eta-1)} \prod_{i=1}^\eta \widehat{X_i}(S). \tag{1}$$

Moreover, it follows from Cauchy-Schwarz inequality and Parseval's identity that

$$2\mathrm{SD}\left(X,Y\right) \leq 2^n \sqrt{\sum_{S \neq \emptyset} (\widehat{X}(S) - \widehat{Y}(S))^2}.$$

In particular, we have:

$$2\mathrm{SD}\left(X,\mathbb{U}^n\right) \leq 2^n \sqrt{\sum_{S \neq \emptyset} \widehat{X}(S)^2}. \tag{2}$$

F.2 Proof of Theorem 8

We will use the following lemma to to prove Theorem 8.

Lemma 2. *Let $\varepsilon > 0$ and let $\mathbb{U}^k$ denote the uniform distribution over $\{0,1\}^k$. Suppose (X,Y) is a joint distribution over $\mathcal{X} \times \mathcal{Y}$ such that $H_\infty(X|Y) \neq 0$. Then, there exist $\eta \in \mathbb{N}$, and a deterministic extractor $Ext\colon \mathcal{X}^\eta \to \{0,1\}^k$ such that*

$$\mathrm{SD}\left((Ext(X^\eta), Y^\eta), (\mathbb{U}^k, Y^\eta)\right) \leq \varepsilon,$$

where (X^η, Y^η) denotes η i.i.d samples of the joint distribution (X,Y).

Proof. First, we prove the case $k = 1$. Since $H_\infty(X|Y)$ is non-zero, there always exists a hash function $h\colon \mathcal{X} \to \{0,1\}$ such that $H_\infty(h(X)|Y)$ is non-zero. Define $Ext(X^\eta) = \bigoplus_{i=1}^{\eta} h(X_i)$. By convolution property of Fourier coefficients,

$$\widehat{(\bigoplus h(X_i)|Y^\eta = y^\eta)}(S) = 2^{\eta-1} \prod \widehat{(h(X_i)|Y_i = y_i)}(S)$$

We have

$$\begin{aligned}
\mathrm{SD}\left((Ext(X^\eta), Y^\eta), (\mathbb{U}^1, Y^\eta)\right) &= \mathop{\mathbb{E}}_{y^\eta} \mathrm{SD}\left((Ext(X^\eta)|Y^\eta = y^\eta), (\mathbb{U}^1|Y^\eta = y^\eta)\right) \\
&\overset{\text{(i)}}{\leq} \mathop{\mathbb{E}}_{y^\eta} \sqrt{\sum_{S \neq \emptyset} \widehat{(\bigoplus h(X_i)|Y^\eta = y^\eta)}(S)^2} \\
&\overset{\text{(ii)}}{=} 2^{\eta-1} \mathop{\mathbb{E}}_{y^\eta} \sqrt{\sum_{S \neq \emptyset} \prod \widehat{(h(X_i)|Y_i = y_i)}(S)^2} \\
&\overset{\text{(iii)}}{\leq} 2^{\eta-1} \sqrt{\mathop{\mathbb{E}}_{y^\eta} \sum_{S \neq \emptyset} \prod \widehat{(h(X_i)|Y_i = y_i)}(S)^2} \\
&\overset{\text{(iv)}}{=} 2^{\eta-1} \sqrt{\sum_{S \neq \emptyset} \prod \mathop{\mathbb{E}}_{y_i} \widehat{(h(X_i)|Y_i = y_i)}(S)^2} \\
&\overset{\text{(v)}}{=} 2^{\eta-1} \sqrt{\sum_{S \neq \emptyset} \left(\mathop{\mathbb{E}}_{y_1} \widehat{(h(X_1)|Y_1 = y_1)}(S)^2\right)^\eta} \\
&\overset{\text{(vi)}}{=} 2^{\eta-1} \sqrt{\left(\mathop{\mathbb{E}}_{y_1} \widehat{(h(X_1)|Y_1 = y_1)}(\{1\})^2\right)^\eta}
\end{aligned}$$

In above, (i) is achieved from (2) for $n = 1$, (ii) is achieved from (1) for $n = 1$, (iii) is achieved from Jensen's inequality, (iv) holds because of the linearity property of expectation and the fact that the samples are independent, (v) holds because the samples have identical distribution, (vi) holds because $n = 1$ and the only non empty set S is $\{1\}$.

Therefore, if $\mathbb{E}_{y_1} \widehat{(h(X_1)|Y_1 = y_1)}(\{1\})^2 < \frac{1}{4}$ (strictly less than $\frac{1}{4}$), then we can choose η sufficiently large to make

$$\mathrm{SD}\left((Ext(X^\eta), Y^\eta), (\mathbb{U}^1, Y^\eta)\right)$$

arbitrarily small.

We claim that if $h(X_1)$ is not a deterministic function of Y_1, then

$$\mathop{\mathbb{E}}_{y_1} \widehat{(h(X_1)|Y_1 = y_1)}(\{1\})^2 < \frac{1}{4}.$$

Suppose that $\Pr[h(X_1)=1|Y_1=y_1]=p_{y_1}$ and $\Pr[h(X_1)=0|Y_1=y_1]=1-p_{y_1}$, then $\widehat{(h(X_1)|Y_1=y_1)}(\{1\})^2=(\frac{1}{2}-p_{y_1})^2\leq\frac{1}{4}$ and equality holds if and only if $p_{y_1}=0$ or 1. Therefore, $\mathbb{E}_{y_1}\widehat{(h(X_1)|Y_1=y_1)}(\{1\})^2\leq\frac{1}{4}$ and equality holds if and only if for each y_1, we have $\widehat{(h(X_1)|Y_1=y_1)}(\{1\})^2=\frac{1}{4}$ if and only if for each y_1, it happens that $p_{y_1}=0$ or 1 if and only if $h(X_1)$ is a deterministic function of Y_1 if and only if $H_\infty(h(X)|Y)=0$.

For extracting k random bits, the error will be k times the error of extracting 1 random bit (according to the inequality $\mathrm{SD}\left((A,B),(C,D)\right)\leq\mathrm{SD}\left(A,C\right)+\mathrm{SD}\left(B,D\right)$ when A and B are independent and C and D are independent because we use different disjoint blocks of bits to extract the random bits.) □

Remark. Suppose $\mathbb{E}_{y_1}\widehat{(h(X_1)|Y_1=y_1)}(\{1\})^2=\frac{1}{4}-\varepsilon$ for some constant $\varepsilon>0$. Then

$$\mathrm{SD}\left((Ext(X^\eta),Y^\eta),(\mathbb{U}^1,Y^\eta)\right)\leq\frac{(1-4\varepsilon)^{\eta/2}}{2}.$$

If we set $\frac{(1-4\varepsilon)^{\eta/2}}{2}=\nu(n)/k$, then we need $\eta=O(\log(\frac{k}{\nu(n)}))$ samples to produce k random bits with error at most $\nu(n)$.

Now, we are ready to prove Theorem 8.

of Theorem 8. In the following, for any distributions A,B, we use the notation $A\overset{\nu}{\approx}B$ whenever the statistical distance between A and B is at most ν. Moreover, without loss of generality we assume that private randomness of each party is a set of uniform independent bits. We also use $\mathbb{U}^k$ to denote uniform distribution over set $\{0,1\}^k$.

Since $(U,V)\sqsubseteq_{f,g}^{\nu(n)}(X,Y)^{\otimes n}$, there exist $m_A,m_B\in\mathbb{N}$ and simulators $\mathrm{Sim}_A\colon\mathcal{U}\to\mathcal{X}^n\times\{0,1\}^{m_A}$ and $\mathrm{Sim}_B\colon\mathcal{V}\to\mathcal{Y}^n\times\{0,1\}^{m_B}$ such that

$$(\,U,V\,)\overset{\nu(n)}{\approx}(\,f(X^n,\mathbb{U}^{m_A}),g(Y^n,\mathbb{U}^{m_B})\,)$$

$$(\,\mathrm{Sim}_A(U),U,V\,)\overset{\nu(n)}{\approx}(\,(X^n,\mathbb{U}^{m_A}),f(X^n,\mathbb{U}^{m_A}),g(Y^n,\mathbb{U}^{m_B})\,)$$

$$(\,U,V,\mathrm{Sim}_B(V)\,)\overset{\nu(n)}{\approx}(\,f(X^n,\mathbb{U}^{m_A}),g(Y^n,\mathbb{U}^{m_B}),(Y^n,\mathbb{U}^{m_B})\,)$$

Suppose that there is an extractor Ext such that

$$(\mathsf{Ext}(X^{n_A}),Y^{n_A})\overset{\nu(n)}{\approx}(\mathbb{U}^{m_A},Y^{n_A})$$

and

$$(X^{n_B},\mathsf{Ext}(Y^{n_B}))\overset{\nu(n)}{\approx}(X^{n_B},\mathbb{U}^{m_B})$$

for $n_A,n_B\in\mathbb{N}$. Let

$$\begin{aligned}m&=n+n_A+n_B\\I_1&=\{1,\ldots,n\}\\I_2&=\{n+1,\ldots,n+n_A\}\\I_3&=\{n+n_A+1,\ldots,m\}\end{aligned}$$

$$J_1 = \{n+1, \ldots, n+m_A\}$$
$$J_2 = \{n+1, \ldots, n+m_B\}$$

and define deterministic functions $f' \colon \mathcal{X}^m \to \mathcal{U}$ and $g' \colon \mathcal{Y}^m \to \mathcal{V}$ such that for any $\mathbf{x} \in \mathcal{X}^m$, $f'(\mathbf{x}) = f(\mathbf{x}_{I_1}, \mathsf{Ext}(\mathbf{x}_{I_2}))$ (where $\mathbf{x}_{I_1}$ and $\mathbf{x}_{I_2}$ denote the respectively $\mathbf{x}_1, \ldots, \mathbf{x}_n$ and $\mathbf{x}_{n+1}, \ldots, \mathbf{x}_{n+n_A}$) and for any $\mathbf{y} \in \mathcal{Y}^m$, $g'(\mathbf{y}) = f(\mathbf{y}_{I_1}, \mathsf{Ext}(\mathbf{y}_{I_3}))$.

Define $\mathrm{Sim}_A^* \colon \mathcal{U} \to \mathcal{X}^m$ and $\mathrm{Sim}_B^* \colon \mathcal{V} \to \mathcal{Y}^m$ such that for each $u \in \mathcal{U}$,

$$\mathrm{Sim}_A^*(u) = (\mathrm{Sim}_A(u)_{I_1}, \mathbf{x}', \mathbf{x}'')$$

where $\mathrm{Sim}_A(u)_{I_1}$ denotes the first n bits of the output string of simulator Sim_A on input u, and $\mathbf{x}' \sim \mathsf{Ext}^{-1}(\mathrm{Sim}_A(u)_{J_1})$ and $\mathbf{x}'' \sim X^{n_B}$ and for each $v \in \mathcal{V}$,

$$\mathrm{Sim}_B^*(v) = (\mathrm{Sim}_B(v)_{I_1}, \mathbf{y}'', \mathbf{y}')$$

where $\mathbf{y}'' \sim Y^{n_A}$ and $\mathbf{y}' \sim \mathsf{Ext}^{-1}(\mathrm{Sim}_B(v)_{J_2})$. We shall prove the following:

$$(U, V) \overset{4\nu(n)}{\approx} (f'(X^m), g'(Y^m)) \tag{3}$$

$$(\mathrm{Sim}_A^*(U), U, V) \overset{4\nu(n)}{\approx} (X^m, f'(X^m), g'(Y^m)) \tag{4}$$

$$(U, V, \mathrm{Sim}_B^*(V)) \overset{4\nu(n)}{\approx} (f'(X^m), g'(Y^m), Y^m) \tag{5}$$

We have:

$$(f'(X^m), g'(Y^m)) = (f(X_{I_1}^m, \mathsf{Ext}(X_{I_2}^m)), g(Y_{I_1}^m, \mathsf{Ext}(Y_{I_3}^m)))$$

Note that since $I_2 \cap I_3 = \emptyset$, $\mathsf{Ext}(X_{I_2}^m)$ is independent of $\mathsf{Ext}(Y_{I_3}^m)$. According to the data processing inequality ($\mathrm{SD}(f(A), f(B)) \leq \mathrm{SD}(A, B)$), and the inequality $\mathrm{SD}((A, B), (C, D)) \leq \mathrm{SD}(A, C) + \mathrm{SD}(B, D)$ (when A and B are independent and C and D are independent), we have:

$$\begin{aligned}
&\mathrm{SD}\left(f(X_{I_1}^m, \mathsf{Ext}(X_{I_2}^m)), g(Y_{I_1}^m, \mathsf{Ext}(Y_{I_3}^m)),\ f(X_{I_1}^m, \mathbb{U}_A^{m_A}), g(Y_{I_1}^m, \mathbb{U}_B^{m_B})\right) \\
&\leq \mathrm{SD}\left((X_{I_1}^m, \mathsf{Ext}(X_{I_2}^m)), (Y_{I_1}^m, \mathsf{Ext}(Y_{I_3}^m)),\ (X_{I_1}^m, \mathbb{U}_A^{m_A}), (Y_{I_1}^m, \mathbb{U}_B^{m_B})\right) \\
&\leq \mathop{\mathbb{E}}_{\mathbf{x}_{I_1}, \mathbf{y}_{I_1}} \mathrm{SD}\left(\left(\mathsf{Ext}(X_{I_2}^m) \mid \mathbf{x}_{I_1},\ \mathsf{Ext}(Y_{I_3}^m) \mid \mathbf{y}_{I_1}\right),\ (\mathbb{U}_A^{m_A} \mid \mathbf{x}_{I_1}, \mathbb{U}_B^{m_B} \mid \mathbf{y}_{I_1})\right) \\
&\leq \mathrm{SD}\left(\mathsf{Ext}(X_{I_2}^m), \mathbb{U}_A^{m_A})\right) + \mathrm{SD}\left(\mathsf{Ext}(Y_{I_3}^m), \mathbb{U}_B^{m_B}\right) \\
&\leq 2\nu
\end{aligned}$$

This implies that

$$\begin{aligned}
(f'(X^m), g'(Y^m)) &= (f(X_{I_1}^m, \mathsf{Ext}(X_{I_2}^m)), g(Y_{I_1}^m, \mathsf{Ext}(Y_{I_3}^m))) \\
&\overset{2\nu}{\approx} (f(X_{I_1}^m, \mathbb{U}_A^{m_A}), g(Y_{I_1}^m, \mathbb{U}_B^{m_B})) \\
&\overset{\nu}{\approx} (U, V)
\end{aligned}$$

which implies (3) by using triangle inequality. Moreover, let $f(X_{I_1}^m, \mathbb{U}_A^{m_A}) = F$, and $g(Y_{I_1}^m, \mathbb{U}_B^{m_B}) = G$

$$\mathrm{SD}\left((\mathrm{Sim}_A^*(U), U, V), (X^m, f'(X^m), g'(Y^m))\right)$$

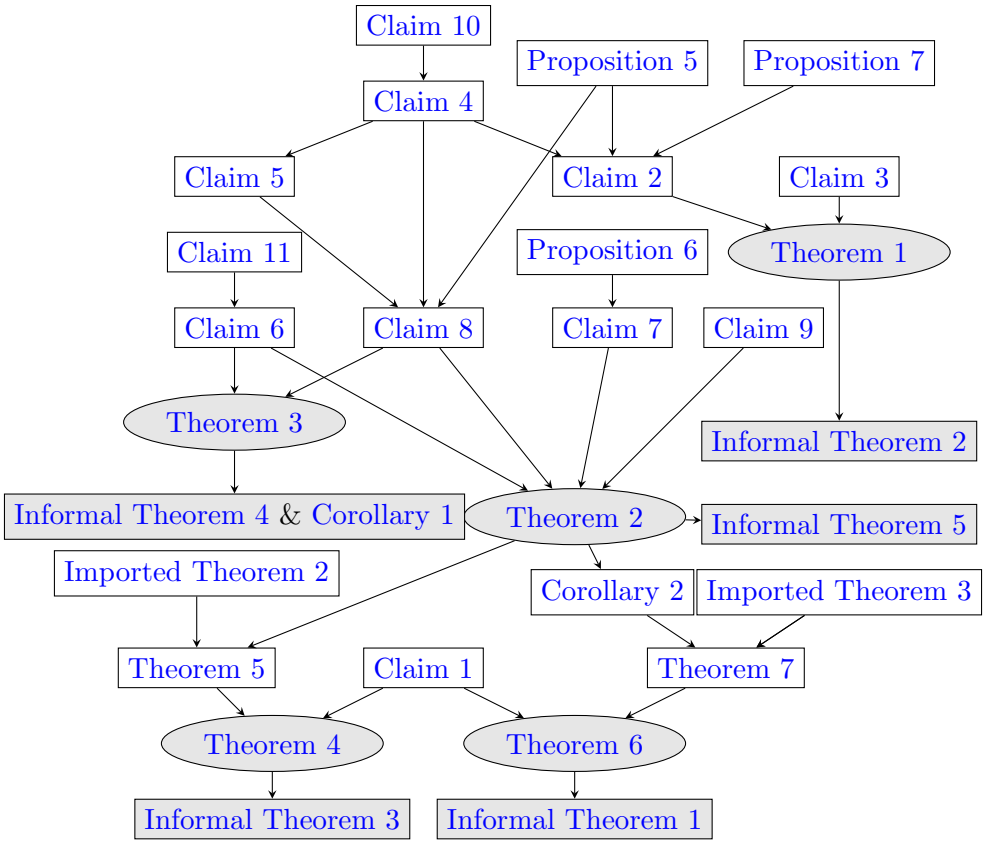

Figure 3: The diagram of claims, propositions, theorems and informal theorems. An arrow from one result to another result means that the first result is used to prove the second result. Highlighted nodes represent our final results.

$$
\begin{aligned}
&= \mathrm{SD}\left(\left(\left(\mathrm{Sim}_A(U)_{I_1}, \mathsf{Ext}^{-1}(\mathrm{Sim}_A(U)_{J_1}), X^{n_B}\right), U, V \right), \left(X^m, f'(X^m), g'(Y^m) \right) \right) \\
&\le \mathrm{SD}\left(\left(\left(\mathrm{Sim}_A(U)_{I_1}, \mathsf{Ext}^{-1}(\mathrm{Sim}_A(U)_{J_1}), X^{n_B}\right), U, V \right), \left(X^m, F, G \right) \right) \\
&+ \mathrm{SD}\left(\left(X^m, F, G \right), \left(X^m, f'(X^m), g'(Y^m) \right) \right) \\
&\le \mathrm{SD}\left(\left(\mathrm{Sim}_A(U)_{I_1}, \mathsf{Ext}^{-1}(\mathrm{Sim}_A(U)_{J_1}), X^{n_B}\right), U, V \right) \\
&\qquad \left((X^m_{I_1}, X^m_{I_2}, X^m_{I_3}), f(X^m_{I_1}, \mathbb{U}_A^{m_A}), g(Y^m_{I_1}, \mathbb{U}_B^{m_B}) \right) + 2\nu \\
&\le \mathrm{SD}\left(\left(\mathrm{Sim}_A(U)_{I_1}, U, V \right), \left(X^m_{I_1}, f(X^m_{I_1}, \mathbb{U}_A^{m_A}), g(Y^m_{I_1}, \mathbb{U}_B^{m_B}) \right) \right) \\
&+ \mathrm{SD}\left(\left(\mathsf{Ext}^{-1}(\mathrm{Sim}_A(U)_{J_1}), X^{n_B} \right), (X^m_{I_2}, X^m_{I_3}) \right) + 2\nu \\
&\le \nu + \nu + 2\nu = 4\nu,
\end{aligned}
$$

which implies the security definition for corrupt Alice (4). The proof of security for corrupt Bob (5)) is similar and we skip it. This completes the proof. □