Secure Non-interactive Simulation: Feasibility & Rate

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

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

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

Abstract

General secure computation is a powerful cryptographic primitive that allows mutually distrusting parties to compute securely over their private data. Random samples from noisy channels, like, binary erasure and binary symmetric channel, enable general secure computations using interactive protocols. A key research objective is to realize these constructions as efficiently as possible. For example, to realize a secure computation task, one strives to use the minimum number of samples of these noisy channels. Additionally, reducing the round and communication complexity of these interactive protocols is a well-established objective to minimize the impact of network latency. Even for elementary secure computation tasks, like converting one form of noisy channel samples into samples from another noisy channel, the precise characterization of achievable efficiency objectives mentioned above is not well-understood.

Towards this endeavor of understanding the limits of secure computation under limited interaction, this work introduces the concept of secure non-interactive simulation of joint distributions (SNIS), which reduces the round and communication complexity of secure computation protocols to the absolute minimum, and studies feasibility and rate characterization. In this setting, two parties begin with multiple independent samples from a correlated randomness source. This setup is akin to the preprocessing step of the offline-online paradigm of secure computation using sources of noise, which enables general secure computation even against parties with unbounded computational power. The objective of the parties is to non-interactively simulate samples of another joint distribution without any further communication. A non-interactive simulation is secure if a party's output samples are roughly as informative about the other party's output samples as its input samples. We define this security notion using standard simulation-based security. The fundamental research problem is to characterize the feasibility and the achievable rate of SNIS.

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

In this work, we study samples from the following two families of joint distributions. (1) $\mathsf{BSS}(\epsilon)$: A joint distribution (X, Y), where X is a uniform random bit and Y is a correlated bit such that $X \neq Y$ with probability $\epsilon \in (0, 1/2)$, and (2) $\mathsf{BES}(\epsilon)$ (a.k.a., (randomized) Rabin OT samples): A joint distribution (X, Y), where X is a uniform random bit, and $Y = X$ with probability $(1-\epsilon)$; otherwise $Y = \perp$, where $\epsilon \in (0, 1)$. These joint distributions are some of the most fundamental distributions that enable general secure computation at a constant rate using interactive protocols. However, even for these fundamental cryptographic resources, characterization of the optimal rate of enabling general secure computation is relatively not well explored.

Our work completely resolves the feasibility and rate of SNIS between these families of joint distributions. Note that the reverse hypercontractivity and OWSC already rule out the possibility of realizing any BES sample from BSS samples. This impossibility transfers to SNIS as well because it is a strictly stronger primitive. Furthermore, we prove the impossibility of a SNIS realization of any BSS sample from any BES samples. We highlight that this characterization problem remains open for NIS and OWSC.

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

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

Overall, our constructions and hardness of computation results are the strongest possible in the following sense. All our constructions are perfectly secure (even against malicious adversaries), that is, they realize SNIS with zero insecurity, and admit computationally efficient simulators. Moreover, all our feasibility and rate-achieving constructions hold whenever the number of input samples is sufficiently large. Additionally, our hardness of computation results extend to infinite families of reductions where (infinitely often) the insecurity falls faster than some appropriate inverse-polynomial of the number of input samples. Consequently, our results encompass the typical cryptographic contexts where the insecurity decays faster than all inverse-polynomials. Lastly, all our impossibility results hold against semi-honest adversaries and extend to the weaker game-based security definitions as well. Technically, our analysis relies on discrete Fourier analysis and an isoperimetric-type result on the Boolean hypercube.

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

Funding The research effort is supported in part by an NSF CRII Award CNS–1566499, an NSF SMALL Award CNS–1618822, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Award, a Purdue Research Foundation (PRF) Award, and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

1 Introduction

Noisy, albeit correlated, information is an incredible facilitator of cryptography. Rabin [Rab81, Rab05] and Crépeau [Cré88] demonstrated that erasure channels, referred to as Rabin Oblivious Transfer, enable performing *general secure computation* [Yao82, GMW87]. General secure computation is an exceptionally powerful cryptographic primitive that allows mutually distrusting parties to securely perform arbitrary computation over their private data revealing only the respective outputs of each party even if all adversarial parties are colluding. It is highly unlikely that one can realize this cryptographic primitive solely from common shared randomness [GKM$^+$00, MMP14a, MMP14b]. In 1988, Crépeau and Kilian [CK88, CK90] proved that noisy channels, in particular, 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 [Kil88, Kil91, DKS99, Kil00, CMW05, Wul07, Wul09, KMS16, CDLR16]. In particular, random samples from these noisy channels suffice for general secure computation while incurring a small increase in round and communication complexity [WW06].

There has been significant research into improving the efficiency of these interactive cryptographic protocols. For instance, in regards to efficiency in using the noisy samples, referred to as the sample complexity, the current state-of-the-art constructs general secure computation from noisy channels at a (small) positive rate [Kil00, WW06, IPS08, IKO$^+$11]. That is, securely computing a functionality represented by a size-s circuit requires $O(s)$ random samples from a noisy channel. However, a precise characterization of capacity and (achievable) rate for noisy channels is not well understood. Another bottleneck to these interactive protocols arises due to the significant overheads introduced by network latency (https://gist.github.com/hellerbarde/2843375). Consequently, there also has been a significant effort to reduce the round and the communication complexity of these interactive protocols [GMW87, BMR90, KOS03, KO04, Pas04, PW10, Wee10, Goy11, GMPP16, ACJ17, BHP17, COSV17b, COSV17a, BGJ$^+$18, HHPV18]. Even for elementary secure computation tasks where parties do not have any private inputs, like converting one form of noisy channel samples into samples from another noisy channel, the precise characterization of the achievable space of efficiency objectives mentioned above (vis-à-vis, sample, round, and communication complexity) is not known.

This work, continuing this extensive line of investigation, introduces *secure non-interactive simulation of joint distributions* against information-theoretic adversaries, a notion of secure computation relying on no communication between the parties, and considers tight *feasibility and rate* characterization. For motivation, consider the following representative application where this concept has promising potential for impact.

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

Unlike the prominent objective in information reconciliation of removing noise by leveraging multiple correlated observations, in cryptography, noise that is beyond the adversarial control is, surprisingly, a facilitator for non-trivial cryptographic tasks, like, key-agreement, and secure computation [CK90, Kil91, Kil00, IPS08, IKO$^+$11, KMPS14].[1] There has been

[1] This is the most appropriate opportunity to quote the following paragraphs from Crépeau and Kilian [CK90]. "Noisy channels have been extensively studied in the field of coding theory, and it is interesting to see how our perspective differs from the more traditional one. Coding theory adopts the viewpoint that noise is a bad thing, to be eliminated as efficiently as possible. Given a noisy channel, a coding theorist tries to simulate a pristine, noiseless communication line.
From our point of view (following Wyner [Wyn75]), an ideal communication line is a sterile, cryptograph-

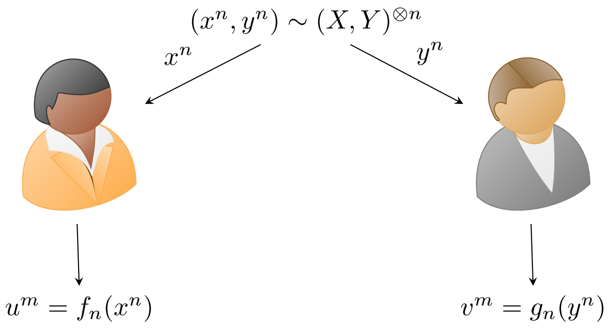

Figure 1 Our Model: Non-interactively simulating samples from the distribution $(U, V)^{\otimes m}$ using samples from the distribution $(X, Y)^{\otimes n}$ via reduction functions f_n and g_n. Alice and Bob obtain their respective input samples x^n and y^n sampled from the joint distribution $(x^n, y^n) \sim (X, Y)^{\otimes n}$. They apply local reduction functions f_n and g_n to their input samples and compute their output samples u^m and v^m, respectively. The parameter m possibly is a function of n, and the rate of this simulation is m/n. The correctness of this simulation guarantees that the joint distribution of (u^m, v^m), when $(x^n, y^n) \sim (X, Y)^{\otimes n}$, is close to the distribution $(U, V)^{\otimes m}$. The security against corrupt Alice insists that the information the output sample u^m provides about Bob's output sample v^m is roughly identical to the information that the input sample x^n provides about Bob's output samples v^m. An analogous requirement enforces the security against corrupt Bob. The feasibility question in SNIS studies the particular case of $m = 1$, while the rate question maximizes the achievable m as a function of n. Section 1.2 provides an intuitive definition and Section 3 provides the formal definition.

extensive research into the feasibility and efficiency of founding secure computation on such sources of noise. Within this ambit of research, out of efficiency concerns, the following natural question arises.

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

The seminal works of Maurer [Mau91, Mau92, Mau93], and Ahlswede and Csisźar [AC93, AC98] introduced the concept of building an infrastructure for shared private randomness using sources of noise. Our emphasis is on enabling general secure computation, which is a strictly stronger cryptographic primitive [GKM$^+$00, MMP14b].

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

ically uninteresting entity. Noise, on the other hand, breeds disorder, uncertainty, and confusion. Thus, it is the cryptographer's natural ally. The question we consider is whether this primordial uncertainty can be sculpted into the more sophisticated uncertainty found in secure two-party protocols.”

motivating example above can generate highly efficient infrastructure for secure computation that never forfeits its security. In fact, the non-interactive simulation allows the parties to specify the infrastructure (say, the noise characteristics) itself well after the correlated samples have been stored. Furthermore, the online phase may prefer to use samples from a noise source with a particular noise characteristic due to efficiency considerations. For example, this choice may be guided by the particular multiplication friendly error-correcting code being used [Cra11] in the online protocol, or the probability of including servers on the *watchlist* [IPS08]. Although the celestial source's noise parameter is beyond our control, it would be preferable if the parties can non-interactively simulate samples of an alternate noise source with the more preferred parameter guided by the online protocol.

Positioning of our research. In information theory, *non-interactive simulation of joint distributions* (NIS) is the focus of intense curiosity and generates highly influential research (refer to the comprehensive survey [STW20]). Our study adds the additional feature of *security* to this direction of inquiry. As a consequence, for instance, randomized simulations or simulations where a party *erases* information from her view are ruled out in our secure simulation setting. Since shared private randomness is not sufficient for general secure computation, secure non-interactive simulation is *not* a straightforward generalization of *non-interactive correlation distillation* [MOR+06] with the cryptographic notion of security.

On the other hand, there is also research on performing secure computation using only one-way messages, a.k.a., *one-way secure computation* (OWSC) [GIK+15]. However, the emphasis of their work was on the feasibility/infeasibility and not characterizing the rate/capacity of these secure constructions. Our problem setting is even further restrictive; parties do not communicate with each other at all. However, looking ahead, our results demonstrate that, incidentally, several feasibility results in the OWSC setting carry over to our non-interactive setting.

Furthermore, our research provides bounds on the efficiency of such computations, a.k.a., *upper bounds on the rate* of secure simulation of some fundamental joint distributions. Additionally, in the long run, our research forms the base case of building *communication-efficient* infrastructure for secure computation. For example, similar research on zero-communication protocols and their connection to communication rectangles, communication complexity and information complexity is known [Jay10, KLL+12, Lov14, GR16]

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

1.1 Our Contribution

We introduce some intuitive terminology to present our results informally. Section 4, Section 5, and Section 6 present the formal theorem statements and their proofs.

The intuitive definition of *secure non-interactive simulation of joint distributions* (SNIS) closely follows the presentation in Figure 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 $(\mathcal{U},\mathcal{V})$. Sample $(x^n,y^n) \overset{\$}{\leftarrow} (X,Y)^{\otimes n}$ (that is, one draws n independent samples from the distribution (X,Y)). Alice gets $x^n \in \mathcal{X}^n$, and Bob gets $y^n \in \mathcal{Y}^n$. Suppose $f_n \colon \mathcal{X}^n \to \mathcal{U}$ and $g_n \colon \mathcal{Y}^n \to \mathcal{V}$ be the *reduction functions* for Alice and Bob, respectively. Alice computes $u' = f_n(x^n)$ and Bob computes $v' = g_n(y^n)$.

Input Joint Distribution	Output Joint Distribution	Feasible set of ϵ'		
		OWSC [GIK+15]	SNIS (Our Work)	NIS [YP14]
$\mathsf{BES}(\epsilon)$	$\mathsf{BES}(\epsilon')$	$(0,1)$	$\left\{1-(1-\epsilon)^k :\ k \in \mathbb{N}\right\}$	$[\epsilon, 1)$
	$\mathsf{BSS}(\epsilon')$	$\supseteq \emptyset$	$\emptyset$	$\supseteq [\epsilon/2, 1/2)$ $\subseteq \left[\frac{1-\sqrt{1-\epsilon}}{2}, 1/2\right)$
$\mathsf{BSS}(\epsilon)$	$\mathsf{BES}(\epsilon')$	$\emptyset$	$\emptyset$	$\emptyset$
	$\mathsf{BSS}(\epsilon')$	$\supseteq \left\{\frac{1-(1-2\epsilon)^k}{2} : k \in \mathbb{N}\right\}$	$\left\{\frac{1-(1-2\epsilon)^k}{2} : k \in \mathbb{N}\right\}$	$[\epsilon, 1/2)$

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

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

1. Correctness: The distribution of the samples (u', v') is $\nu(n)$-close to the distribution (U, V) in the statistical distance.
2. Security against corrupt Alice: Consider any (u, v) in the support of the distribution (U, V). The distribution of x^n, conditioned on the fact that $u' = u$ and $v' = v$, is independent of v.
3. Security against corrupt Bob: Consider any (u, v) in the support of the distribution (U, V). The distribution of y^n, conditioned on the fact that $u' = u$ and $v' = v$, is independent of u.

To discuss rate, one considers SNIS of the form $(U,V)^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} (U,V)^{\otimes n}$. Here, the reduction functions output $m(n)$-independent samples from the distribution (U, V). Fixing (X, Y) and (U, V), our objective is to characterize the reduction functions that maximize the production rate $m(n)/n$.

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

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

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

Before we begin the presentation of our results, note that the NIS and OWSC are relaxations of SNIS, which we consider in this work. Therefore, the impossibility results in either NIS or OWSC automatically imply an impossibility for SNIS. Table 1 summarizes our feasibility results and positions them relative to the known results in NIS and OWSC.

For example, in NIS, $\mathsf{BES}(\epsilon')$ does not reduce to $\mathsf{BSS}(\epsilon)^{\otimes n}$, for infinitely many $n \in \mathbb{N}$, with insecurity $\nu(n) = \mathsf{negl}(n)$,[2] for any $\epsilon \in (0, 1/2)$, and $\epsilon' \in (0, 1)$ [KA16, KA12, GIK+15]. On

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

the other hand, it is not known whether $\mathsf{BSS}(\epsilon')$ reduces to $\mathsf{BES}(\epsilon)^{\otimes n}$ with $\mathsf{negl}(n)$ insecurity via either NIS or OWSC. We resolve this problem for SNIS.[3]

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

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

Our proof also works for the SNIS of shared common randomness from $\mathsf{BES}(\epsilon)$, which provides an alternate combinatorial proof for this result proved using analytical techniques in [Yan04].

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

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

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

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

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

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

Typically, NIS literature's impossibility results rely on leveraging the reverse hypercontractivity theorem [KA12, KA16, NW17]. However, this approach encounters a significant hurdle for samples from the binary erasure channel [KA12]. The addition of the security constraint in our setting helps circumvent this hurdle. Essentially, we show that the *only* secure non-interactive simulation reduction among samples of the erasure channel is the following linear reduction. Alice outputs the parity of the first k-bits of her input x^n, and Bob outputs the parity of the first k-bits of $y^n \in \{0, 1\}^k \times \{0, 1, \perp\}^{n-k}$; otherwise Bob outputs $\perp$. This protocol is a perfect SNIS of $\mathsf{BES}(\epsilon')$ from $\mathsf{BES}(\epsilon)$, where $(1 - \epsilon') = (1 - \epsilon)^k$. Interestingly, this protocol is identical in spirit to the OWSC protocol, as presented in [GIK+15] when $(1 - \epsilon') \in \{(1 - \epsilon), (1 - \epsilon)^2, \ldots .\}$. However, all other values of ϵ' are feasible *only* for OWSC [GIK+15].

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

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

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

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

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

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

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

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

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

Consider the following example when $(1-2\epsilon') = (1-2\epsilon)^2$. So, when $n = 2$, the linear reduction functions $f_2(x^2) = x^2_1 \oplus x^2_2$, and $g_2 = f_2$ suffice.[4] However, interestingly, there exists non-linear reduction functions $f_n = g_n$ for $n = 4$. For example, consider the reduction function below.

$$f_4(x^4) = \frac{2 - (-1)^{x^4_1+x^4_3} - (-1)^{x^4_2+x^4_3} - (-1)^{x^4_1+x^4_4} + (-1)^{x^4_2+x^4_4}}{4}.$$

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

Remark. Our proof techniques for Informal Theorem 2 and Informal Theorem 3 yield the following extensions as well. For Informal Theorem 2, we prove that $\mathsf{BES}(\epsilon_1) \otimes \cdots \otimes \mathsf{BES}(\epsilon_m) \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$ holds if and only if $(1-\epsilon_i) = (1-\epsilon)^{k_i}$, where $k_i \in \mathbb{N}$, and $1 \leq i \leq m$. Moreover, the rate is bounded by $k_1 + \cdots + k_m \leq n$. Here, $\epsilon_1, \ldots, \epsilon_m, \epsilon \in (0,1)$ are constants. Analogously, we prove for Informal Theorem 3 that $\mathsf{BSS}(\epsilon_1) \otimes \cdots \otimes \mathsf{BSS}(\epsilon_m) \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ holds if and only if $(1-2\epsilon_i) = (1-2\epsilon)^{k_i}$, where $k_i \in \mathbb{N}$ and $1 \leq i \leq m$, and $k_1 + \cdots + k_m \leq n$. Here, $\epsilon_1, \ldots, \epsilon_m, \epsilon \in (0,1/2)$ are constants. For ease of the presentation, we present the simpler form of our result. From the technical overview section, the extension of our results in this form is natural.

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

1.2 Prior Related Works

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

Non-interactive simulation. Information theory studies the possibility of simulating a sample from a joint distribution (U, V) given multiples samples from the joint distribution (X, Y), namely, *non-interactive simulation of joint distributions* (NIS). This line of research starts with the seminal works of Gács and Körner [GK73], Witsenhausen [Wit75], and Wyner [Wyn75]. The primary difference of this concept from our object of study is the omission of security. For example, it is permissible for parties to erase information from their views in this setting. On the other hand, in our setting, since we consider semi-honest and malicious security, erasure of information may be insecure. Let us consider an illustrative example highlighting this difference. Consider simulating one sample of $\mathsf{BSS}(\epsilon/2)$ from multiple samples of $\mathsf{BES}(\epsilon)$. Alice outputs the bit of her first sample. If Bob also received the bit in his first sample, then he outputs the bit; otherwise, if he received $\perp$ as his first sample, he outputs a uniformly random bit.[5] Note that this non-interactive simulation is not secure.[6] Even the decision version of the problem where one has to determine whether samples from one joint distribution may be non-interactively simulated from the samples of another joint distribution, in its full generality, is a difficult problem [GKS16, DMN18]. Technically, reverse hypercontractivity [AG76, Bor82, MOR$^+$06, MOS13, KA16, DMN18, BG15, MO05], and maximal correlation [Hir35, Wit75, AG76, Rén59, AGKN13] are few of the most prominent techniques employed to prove the impossibility of non-interactive simulations. We refer the interested reader to an exceptional survey by Sudan, Tyagi, and Watanabe [STW20] for a thorough introduction to this field.

There is a related notion of *non-interactive correlation distillation,* where the target joint distribution is the distribution of uniformly random private keys [MOR$^+$06, MO05, Yan04, BM11, CMN14].

Joint distributions useful for secure computation. Not all joint distribution (U, V) are useful for general secure computation. If the mutual information of (U, V) is 0, then clearly, this distribution does not suffice for key agreement, let alone secure computation, which is more complex to realize than key agreement. Even if the mutual information of (U, V) is > 0, then this joint distribution might enable key agreement, but not support general secure computation. However, random samples from noisy channels like binary erasure channels [Rab81, Rab05, Cré88], and binary symmetric channels [CK88] suffice for general secure computation [Yao82, GMW87, WW06] (relying on interactive protocols). Kilian [Kil00] exactly characterized all joint distributions that enable general secure computation. The benefit of secure computation based on samples of joint distributions is that these protocols are secure even against adversaries with unbounded computational power.

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

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

Secure computation with low interaction and communication. Alice and Bob, beginning from samples of any joint distribution useful for secure computation, may perform general secure computation in a constant number of rounds [IK00, IK02, AIK04, IPS08]. In fact, one can also perform secure computation at a constant rate[7] [IKO+11]. Recently, Garg, Ishai, Kushilevitz, Ostrovsky, and Sahai [GIK+15] explore the potential of secure computation using noisy channels and one-way communication. In their setting, they leave open several feasibility/infeasibility problems related to binary symmetric and binary erasure channels. The proposed notion of SNIS in this work permits no communication between the parties.

Bounding efficiency of secure constructions. There has been work on lower-bounding the efficiency of secure computations via interactive protocols, for example, the monotones of [WW05], and assisted common information [PP10, PP11, PP14, RP14].

1.3 Technical Overview

In this section we provide the intuition underlying the techniques used to prove our results.

Impossibility of SNIS of BSS from BES. Theorem 4 states our exact theorem statement, and Section 4.1 provides the full proof. Fix constant $\epsilon \in (0,1)$ and $\epsilon' \in (0,1/2)$. If possible let, there exists $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$. So, our reduction functions $f_n\colon \{0,1\}^n \to \{0,1\}$ and $g_n\colon \{0,1,\perp\}^n \to \{0,1\}$. Our argument proceeds along the following high-level intuition.

Part 1. We focus on elements $a^n \in \{0,1\}^n$ and $b^n \in \{0,1\}^n$ such that they differ exactly in one coordinate (i.e., they are neighbors in the Boolean hypercube), $f_n(a^n) = 0$, but $f_n(b^n) = 1$. We say that a^n is consistent with $y^n \in \{0,1,\perp\}^n$, represented by $a^n \vdash y^n$, if one can obtain y^n by passing a^n through an erasure channel. We define three disjoint subsets $T_0, T_1, T_{\text{both}} \subseteq \{0,1,\perp\}^n$ below.

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

One can argue that

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

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

We rely on an isoperimetric-type inequality on the Boolean hypercube to argue that there are (approximately) $2^n/\sqrt{n}$ pairs of points (a^n, b^n) that satisfy the above-mentioned

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

property [BL97].[8] Therefore, with $1/\sqrt{n}$ probability, one encounters the event of incurring constant insecurity. Consequently, all $\epsilon' \neq \epsilon/2$ are outrightly insecure.
Part 2. Next, our objective is to rule out the isolated case of $\epsilon' = \epsilon/2$ that survived the previous argument. We shall use the parallel composition of the original SNIS to obtain two samples of $\mathsf{BSS}(\epsilon')$. That is,

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

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

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

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

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

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

Characterization of SNIS feasibility and rate for BES from BES. Let us start by considering some SNIS reductions in this context. Suppose $(1-\epsilon') = (1-\epsilon)^k$, for some $k \in \mathbb{N}$. The input samples are over the sample space $(\mathcal{X}, \mathcal{Y}) = (\{0,1\}, \{0,1,\perp\})$ and the output sample space is $(\mathcal{U}, \mathcal{V}) = (\{1,-1\}, \{1,-1,0\})$.[9] For $n \geq k$, define the reduction function $f_n^*\colon \{0,1\}^n \to \{1,-1\}$ and $g_n^*\colon \{0,1,\perp\}^n \to \{1,-1,0\}$ as follows.

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

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

Next, let us move on to proving the feasibility and rate results. Theorem 5 provides the formal theorem statement, and Section 4.2 provides the full proof. Fix constants $\epsilon, \epsilon' \in (0,1)$. Suppose there exists $\mathsf{BES}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n, g_n} \mathsf{BES}(\epsilon)^{\otimes n}$.
Feasibility Characterization. This proof proceeds by Fourier analysis. We provide a very high-level intuition for the sequence of arguments that we use. The first step is to algebrize the notion of security and obtain a non-trivial restriction on the Boolean reduction function f_n. Define $\rho := (1-\epsilon)$ and $\rho' := (1-\epsilon')$. For a SNIS reduction between BES samples, relying on insecurity being $\nu(n) = o(1)$, we show that the following quantity is also $o(1)$.

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

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

[8] A naïve application of (vertex) isoperimetric inequality over the Boolean hypercube [Har66] yields $1/n^{3/2}$ probability instead of $1/n^{1/2}$, slightly worsening the upper-bound on $\nu(n)$.

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

main technical lemma: Lemma 2. This lemma proves that if the "rank-one constraint" holds for a Boolean function f_n, then ρ' is close to ρ^k for some $k \in \mathbb{N}$. Furthermore, the spectral weight of the Boolean function f_n is primarily concentrated on size-k (multi-)linear terms. After that, an analysis specific to SNIS for inter-converting BES samples proves that the function f_n must have most of its spectral weight on one single size-k (multi-)linear term. Then, one obtains the characterization of the function g_n from the security definition.
Rate Characterization. Suppose $(1-\epsilon') = (1-\epsilon)^k$ and we have $\mathsf{BES}(\epsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BES}(\epsilon)^{\otimes n}$.

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

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

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

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

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

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

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

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

$$(ii)\ \mathsf{BES}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n^{(j)},g_n^{(j)}} \mathsf{BES}(\epsilon)^{\otimes n},\ \text{and}$$

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

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

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

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

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

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

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

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

For every k, there are additional feasible SNIS reductions, however, they need more than k input samples to generate one output sample. Section 1.1 presents one such example. Computationally efficient simulators for these reductions can rely on rejection sampling (because ϵ' is a constant) to achieve statistical security (not, perfect security).

Theorem 7 provides the formal theorem statement, and Section 5 provides the full proof. In this case, the only change is that $\rho := (1-2\epsilon)$ and $\rho' := (1-2\epsilon')$. The rest of the proof intuition essentially remains identical to the SNIS involving BES case. Except that, for SNIS for inter-converting BSS samples, the Boolean reduction function f_n need not be linear. After that, one obtains the characterization that $g_n = f_n$ using the security definition.

2 Preliminaries

2.1 Notation

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

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

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

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

2.2 Correlated Random Sources and Noise Operator

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

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

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

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

2.3 Fourier Analysis for Boolean Functions: Preliminaries

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

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

For each $S \subseteq [n]$, the characteristic function $\chi_S(x^n) = (-1)^{S \cdot x^n} = (-1)^{\sum_{i \in S} x_i}$ is a linear function that computes the parity (that is, the exclusive-or) of of the bits $(x_i)_{i \in S}$. The set of all χ_S forms an orthonormal basis for the space of all real-valued functions on $\{0,1\}^n$. For any $S \subseteq [n]$, the Fourier coefficient of f at S is defined as $\widehat{f}(S) = \langle f, \chi_S\rangle$. Any function f can be uniquely expressed as $f = \sum_{S \subseteq [n]} \widehat{f}(S)\chi_S$ which is called Fourier expansion of f. The Fourier weight of f on a set $S \subseteq [n]$ is defined to be $\widehat{f}(S)^2$, and the Fourier weight of f at degree k is $W_k[f] = \sum_{S : |S| = k} \widehat{f}(S)^2$. We denote the set of all possible size-k subsets of the set $\{1, 2, \dots, n\}$ by $\mathcal{W}_k$. Parseval's Identity says that $\|f\|_2 = \mathbb{E}_{x^n \in \{0,1\}^n} f(x^n)^2 = \sum_{S \in [n]} \widehat{f}(S)^2$.

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

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

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

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

3 Secure Non-Interactive Simulation: Definition

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

We clarify that it is standard in the literature to assume that the sample spaces $\mathcal{X}, \mathcal{Y}, \mathcal{U}$, and $\mathcal{V}$ are constant sized (i.e., does not depend on n). All the probabilities $\Pr[(X, Y) = (x, y)]$

and $\Pr[(U,V)=(u,v)]$ are either 0 or at least a constant (i.e., for example, these probabilities do not tend to 0 as a function of n).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 3 The case of corrupt Alice for the reduction of $\mathsf{BES}(\epsilon')$ to $\mathsf{BES}(\epsilon)^{\otimes 2}$. The table illustrates the joint distribution of (X^2, V). It suffices to let $\mathrm{Sim}_A(0)$ be the uniform distribution over $\{00, 11\}$, and $\mathrm{Sim}_A(1)$ be the uniform distribution over $\{01, 10\}$.

Intuitively, the first constraint states that (on average) the conditional distribution $(X^n | f_n(X^n) = u, g_n(Y^n) = v)$ is independent of v, and the second constraint states that the conditional distribution $(Y^n | f_n(X^n) = u, g_n(Y^n) = v)$ is independent of u.

2. Consider a secure non-interactive simulation via reduction functions $\{f_n, g_n\}_{n\in\mathbb{N}}$ that has negligible insecurity, i.e., $\nu(n) = \mathsf{negl}(n)$. Then, using the fact that $\Pr[(U,V) = (u,v)]$ is either 0 or at least a constant, the security definition implies the following for every $(u,v) \in \mathrm{Supp}(U,V)$.

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

3. Consider the non-interactive simulation of $\mathsf{BES}(\epsilon')$ from $\mathsf{BES}(\epsilon)^{\otimes 2}$, where $(1-\epsilon') = (1-\epsilon)^2$, with 0 insecurity. In this case we use the reduction function $f_2(x^2) = x_1^2 \oplus x_2^2$ and $g_2(y^2) = \perp$ if $y_1^2 = \perp$, or $y_2^2 = \perp$; otherwise, $g_2(y^2) = y_1^2 \oplus y_2^2$. Let us first visualize the entire joint distribution in Table 2. We illustrate the consequences of the security definition using the tables below. Consider the case of corrupt Alice in Table 3 and the case of corrupt Bob in Table 4.

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

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

3.1 Composition

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

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

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

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

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

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

Then, the following holds.

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

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

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

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

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

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

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

Then, the following holds.

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

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

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

▶ **Theorem 3** (Projection). *For joint distribution P, Q, and R, suppose we have*

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

Then, the following holds.

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

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

4 Secure Non-interactive Simulation from Binary Erasure Source

In this section we consider reductions to BES.

4.1 Impossibility of Simulating Binary Symmetric Source from Binary Erasure Source

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

We begin by restating the Informal Theorem 1.

▶ **Theorem 4.** *Let $\epsilon' \in (0, 1/2)$, and $\epsilon \in (0, 1)$. For every infinite family of reduction functions $\{f_n, g_n\}_{n \in \mathbb{N}}$, insecurity bound $\nu(n) = o(n^{-1/2})$, and sufficiently large n, we have*

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

Proof. First, we shall rule out all $\epsilon' \neq \epsilon/2$. Let $S_0 \subseteq \{0,1\}^n$ be the set of all $x^n \in \{0,1\}^n$ such that $f_n(x^n) = 0$. Similarly, $S_1 = \{0,1\}^n \setminus S_0$ be the set of all $x^n \in \{0,1\}^n$ such that $f_n(x^n) = 1$. Let $\partial S_0 \subseteq S_0$ be the elements whose one of their neighbors on the boolean hypercube lies in S_1. Intuitively, ∂S_0 is the outermost shell of S_0 when embedded in the boolean hypercube. Analogously, define ∂S_1. Our objective is to find a large matching such that every edge has one endpoint in ∂S_0 and another endpoint in ∂S_1. Since $\min\{|S_0|, |S_1|\} \geq 2^{n-1}(1 - o(1))$, the size of such a matching is $\geq \Theta(2^n/\sqrt{n})$ [BL97].

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

Define the following sets.

$$\begin{aligned} T_0 &= \{y^n : y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \not\vdash y^n\} \\ T_1 &= \{y^n : y^n \in \{0,1,\perp\}^n, a^n \not\vdash y^n, b^n \vdash y^n\} \\ T_{\text{both}} &= \{y^n : y^n \in \{0,1,\perp\}^n, a^n \vdash y^n, b^n \vdash y^n\} \end{aligned}$$

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

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

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

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

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

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

Then, by parallel composition, we have

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

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

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

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

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

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

4.2 Binary Erasure Source: Feasibility and Rate

We start by restating the Informal Theorem 2 as follows.

▶ **Theorem 5** (Binary Erasure Channel: Feasibility & Rate). *For constant $\epsilon', \epsilon \in (0,1)$, the following results hold.*

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

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

$$f_n^*(x^n) := (-1)^{x_1^n + x_2^n + \cdots + x_k^n}$$

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

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

   Furthermore, the production of $m(n)=\lfloor n/k\rfloor$ with $\nu(n)=0$ is achievable using block linear reduction functions for all $n\in\mathbb{N}$.[10]

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

4.2.1 Algebraic Definition

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

Suppose $(X^n,Y^n)\sim\mathsf{BES}(\epsilon)^{\otimes n}$, then P_ϵ denotes the marginal distribution of Y^n, and $Q_\epsilon(x^n)$ denotes the conditional distribution $(Y^n|X^n=x^n)$, and $M(y^n)$ denotes the conditional distribution $(X^n|Y^n=y^n)$. Note that we choose the range of reduction function f_n to be $\{-1,1\}$ and the range of g_n to be $\{-1,0,1\}$. We can rewrite the three conditions of the definition of secure non-interactive simulation, mentioned in Section 3, for BES, as the following.

From our discussion in Section 3, it follows from $\mathsf{BES}(\epsilon')\sqsubseteq^{\nu(n)}_{f_n,g_n}\mathsf{BES}(\epsilon)^{\otimes n}$, where $f\colon\{0,1\}^n\to\{-1,1\}, g\colon\{0,1,\perp\}^n\to\{-1,0,1\}$, the following algebraic constraints:

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

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

   which implies that $\mathbb{E}_{x^n\sim U_{\{0,1\}^n}}[f_n(x^n)]\le\nu(n)$, and $\mathbb{E}_{y^n\sim P_\epsilon}[g_n(y^n)]\le\nu(n)$.
2. Bob security:

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

3. Alice security:

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

Intuitively, the correctness implies that Alice can partition the set $\{0,1\}^n$ into two sets S_0,S_1 of (roughly) equal size such that whenever she gets $x^n\in S_i$, she outputs i for $i\in\{0,1\}$,

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

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

4.2.2 Proof of Feasibility Characterization

In this subsection, we shall prove the feasibility result in Theorem 5. First, we state all the lemmas that are needed for the proof. We provide the proofs of these lemmas in Appendix A.

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

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

▶ **Lemma 2** (Main Technical Lemma). *Let $\rho, \rho' \in (0,1)$, and let $f\colon \{0,1\}^n \to \{-1,1\}$ be a Boolean function. Suppose that*

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

Then, there there exists $k \in [n]$ such that $\left|\rho' - \rho^k\right| \leq \sqrt{(1+\rho')\delta}$. Furthermore, when $\rho' = \rho^k$ for some positive integer k the following bound holds.

$$\sum_{S \notin \mathcal{W}_k} \widehat{f}(S)^2 \leq \frac{(1+\rho')}{(1-\rho)^2 \rho'^2} \cdot \delta.$$

▶ **Lemma 3.** *Let $\{k(n)\}_{n\in I}$ be a sequence of positive integers and $\{\nu_n\}_{n \in I}$ be a sequence of positive real numbers such that $\lim_{n\to\infty} \nu(n) = 0$, where I is a subset of $\mathbb{N}$ with infinitely many elements. Let $\rho, \rho' \in (0,1)$ be fixed constants. Suppose that $\left|\rho' - \rho^{k(n)}\right| \leq \nu(n)$ for every $n \in I$. Then there exists $k \in \mathbb{N}$ such that $\rho' = \rho^k$.*

Proof of feasibility result in Theorem 5 . First we prove that statement (a) implies statement (b). For each n, applying Lemma 1 for $f = f_n, g = g_n$ and $\delta = \nu(n)$, we have

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

This allows us to invoke Lemma 2. So there exists $k(n) \in [n]$ such that

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

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

We can also verify that (b) implies (a) as a corollary of Theorem 6 which we shall prove in the next subsection. ◀

We present the proof of the rate result in Section 6.

4.2.3 Feasibility Characterization for Perfect Security Case

In the case of perfect security (when $\nu(n) = 0$), we can further characterize the set of all possible reduction functions f_n and g_n for any fixed n. More precisely, on input $x^n \in \{0,1\}^n$ Alice's reduction function f_n outputs the XOR of all the bits in x^n_S [11] for some $S \subseteq [n]$, and on input $y^n \in \{0,1,\perp\}^n$ Bob's reduction function g_n outputs the XOR of all the bits in y^n_S if y^n_S does not contain any bot symbols, otherwise it outputs zero. We state it formally as follow.

▶ **Theorem 6.** *For constant $\epsilon', \epsilon \in (0,1)$, and for any fixed $n \in \mathbb{N}$, the following two statements are equivalent.*

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

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

We provide the proof of Theorem 6 in Appendix A.

5 Simulation of BSS from BSS: Feasibility & Rate

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

▶ **Theorem 7** (Binary Symmetric Source to Binary Symmetric Source)**.** *For constants $\epsilon, \epsilon' \in (0, 1/2)$, the following results hold.*

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

   In particular, when $(1-2\epsilon') = (1-2\epsilon)^k$, the following linear reduction functions f^*_n, g^*_n realize $\mathsf{BSS}(\epsilon') \sqsubseteq^0_{f^*_n,g^*_n} \mathsf{BSS}(\epsilon)$ for all $n \geq k$.

$$f^*_n(x^n) := (-1)^{x^n_1 + x^n_2 + \cdots + x^n_k}, \text{ and} \qquad g^*_n = f^*_n.$$

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

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

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

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

5.1 Algebraic Definition

First we algebraize the definition of secure non-interactive simulation of $\mathsf{BSS}(\epsilon')$ from $\mathsf{BSS}(\epsilon)^{\otimes n}$. We denote $\rho = 1-2\epsilon$ and $\rho' = 1-2\epsilon'$. Recall that T_ρ is the linear noise operator. It takes as input a function, for example $f\colon \{0,1\}^n \to \{-1,1\}$, and returns a function $\mathsf{T}_\rho(f)\colon \{0,1\}^n \to \mathbb{R}$.

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

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

We describe some intuition here. Recall that for binary symmetric source $\mathsf{BSS}(\epsilon)$ each bit is flipped with probability ϵ, in other words, for each sample $(x,y) \xleftarrow{\$} \mathsf{BSS}(\epsilon)$, the bits x and y are ρ-correlated. By choosing the range of the two functions f_n, g_n appropriately, that is $\{-1,1\}$, we can rewrite the three conditions for the secure non-interactive simulation $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ nicely. The condition for corrupt Alice

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

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

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

This implies that

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

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

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

Analogously, the other security condition also holds.

5.2 Proof of the Feasibility Result

In this subsection, we shall prove the feasibility result in Theorem 5. First, we state all the lemmas that are needed for the proof. We provide the proofs of these lemmas in Appendix B.

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

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

At a high level idea, using the fact that the function $\mathsf{T}_\rho(f_n)$ is close to $\rho' g_n$ and that the function $\mathsf{T}_\rho(g_n)$ is close to $\rho' f_n$, it must be the case that the two functions f_n and g_n are also close. This together with the fact that f_n is a $\{-1, 1\}$-valued function imply that the function $\mathsf{T}_\rho(f_n)$ is close to the function $\rho' f_n$.

We are ready to describe the proof of feasibility result in Theorem 7 as follows. We emphasis that the security requirements of Alice and Bob are crucial to our proof. Moreover, we present the proof of rate result in Theorem 7 in Section 6.

Proof of the Feasibility Result in Theorem 7 . First we prove the forward direction by showing that if $\mathsf{BSS}(\epsilon') \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ holds for infinitely many $n \in \mathbb{N}$, then $\rho' = \rho^k$. For each n, applying Lemma 4 for $f = f_n$, $g = g_n$, $\delta = \nu(n)$, we have the following

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

Furthermore, we have

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

Applying Lemma 2 for $f = f_n, g = g_n$ and $\delta = \nu(n) + 5\sqrt{\nu(n)}$, there exists $k(n) \in [n]$ such that

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

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

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

5.3 Feasibility Characterization for Perfect Secuirty Case

In the case of perfect security, we can further characterize the set of all possible reduction functions f_n and g_n for any fixed n. More precisely, on input $x^n \in \{0,1\}^n$ Alice's reduction function f_n outputs the XOR of all the bits in x^n_S for some $S \subseteq [n]$, and on input $y^n \in \{0,1\}^n$ Bob's reduction function g_n outputs the XOR of all the bits in y^n_S. We state it formally as follow.

▶ **Theorem 8.** *For constant $\epsilon', \epsilon \in (0, 1/2)$, and for any fixed $n \in \mathbb{N}$, the following two statements are equivalent.*

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

We provide the proof of Theorem 8 in Appendix B.

6 Proof of the Rate Results

First, we state all the claims that are needed for the proof of the rate results for both BES and BSS as stated in Theorem 5 and Theorem 7. We provide their proof in Appendix C.

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

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

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

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

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

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

Then, the following probability bound holds.

$$\Pr_{\substack{S \sim \mathcal{S}(h^{(1)}) \\ T \sim \mathcal{S}(h^{(2)})}} [S, T \in \mathcal{W}_k, S \cap T = \emptyset] \geq 1 - \delta \left(3 + \sqrt{\binom{n}{k}} \right).$$

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

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

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

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

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

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

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

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

Proof of the Rate Result in Theorem 7 . Suppose $\mathsf{BSS}(\epsilon')^{\otimes m(n)} \sqsubseteq^{\nu(n)}_{f_n,g_n} \mathsf{BSS}(\epsilon)^{\otimes n}$ for an infinite family of functions $\{f_n, g_n\}_{n\in\mathbb{N}}$. Let ϵ'' such that $1-2\epsilon'' = (1-2\epsilon')^2$. Let $f_n^{(i)}$ and $g_n^{(i)}$ be respectively the i-th projection of the function $f_n\colon \{0,1\}^n \to \{-1,1\}^{m(n)}$ and $g_n\colon \{0,1\}^n \to \{-1,1\}^{m(n)}$ ($m(n) \le n$), for $1 \le i \le m(n)$. For each i, we have

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

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

$$\mathop{\mathbb{E}}_{x^n}\left[\left|(\mathsf{T}_\rho f_n^{(i)})(x^n) - \rho' \cdot f_n^{(i)}(x^n)\right|\right] \le \nu'(n) \tag{3}$$

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

$$\sum_{S \notin \mathcal{W}_k} \widehat{{f_n}^{(i)}}(S)^2 \le \delta(n) \qquad \forall i \in [m(n)]. \tag{4}$$

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

Define ${p_{m(n)}}^{(i,j)}\colon \{-1,1\}^{m(n)} \to \{-1,1\}$ as a function that maps $(u_1, u_2, \ldots, u_{m(n)}) \in \{-1,1\}^{m(n)}$ to $u_i \cdot u_j$. It is easy to verify that $\mathsf{BSS}(\epsilon'') \sqsubseteq^{0}_{{p_{m(n)}}^{(i,j)},{p_{m(n)}}^{(i,j)}} \mathsf{BSS}(\epsilon')^{\otimes m(n)}$ for each $1 \le i < j \le m(n)$. Sequential composition (Theorem 2), implies that

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

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

$$\mathop{\mathbb{E}}_{x^n}\left[\left|(\mathsf{T}_\rho {f_n}^{(i,j)})(x^n) - \rho'' \cdot {f_n}^{(i,j)}(x^n)\right|\right] \le \nu'(n) \tag{5}$$

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

$$\sum_{S \notin \mathcal{W}_{2k}} \widehat{{f_n}^{(i,j)}}(S)^2 \leq \delta'(n) \qquad \forall\ 1 \leq i < j \leq m(n). \tag{6}$$

where $\delta'(n) = \frac{(1+\rho'')\nu'(n)}{(1-\rho)^2 {\rho''}^2}$. Now, by applying Corollary 1, we conclude that if we choose $\nu(n)$ such that $\binom{n}{2}\left(\delta(n)\left(3 + \sqrt{\binom{n}{k}}\right) + \delta'(n)\right) < 1$, then $\frac{m(n)}{n} \leq \frac{1}{k}$. Since $\binom{n}{k} = O(n^k)$, there exists a constant c, which depends on only ϵ and ϵ', such that if $\nu(n) = o(\frac{1}{n^c})$, then $\frac{m(n)}{n} \leq \frac{1}{k}$ for large enough n. ◀

Proof of the Rate Result in Theorem 5 . The proof of rate result in Theorem 5 is very similar to the proof of rate result in Theorem 7. This is due to the fact that the proof of Theorem 7 is based on Lemma 4. Now, by the use of Lemma 1 which is similar to Lemma 4, we can prove the rate result in Theorem 5. ◀

References

AC93 Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - I: secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, 1993. doi:10.1109/18.243431. 4

AC98 Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - part II: CR capacity. *IEEE Trans. Inf. Theory*, 44(1):225–240, 1998. doi:10.1109/18.651026. 4

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

AG76 Rudolf Ahlswede and Peter Gács. Spreading of sets in product spaces and hypercontraction of the markov operator. *The annals of probability*, pages 925–939, 1976. 9

AGKN13 Venkat Anantharam, Amin Gohari, Sudeep Kamath, and Chandra Nair. On maximal correlation, hypercontractivity, and the data processing inequality studied by erkip and cover. *arXiv preprint arXiv:1304.6133*, 2013. 9

AIK04 Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. In *45th Annual Symposium on Foundations of Computer Science*, pages 166–175, Rome, Italy, October 17–19, 2004. IEEE Computer Society Press. doi:10.1109/FOCS.2004.20. 10

BG15 Salman Beigi and Amin Gohari. On the duality of additivity and tensorization. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2381–2385. IEEE, 2015. doi:10.1109/ISIT.2015.7282882. 9

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

BGV12 Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012: 3rd Innovations in Theoretical Computer Science*, pages 309–325, Cambridge, MA, USA, January 8–10, 2012. Association for Computing Machinery. doi:10.1145/2090236.2090262. 4

BHP17 Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou. Four round secure computation without setup. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017: 15th Theory of Cryptography Conference, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 645–677, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_22. 3

BL97 Béla Bollobás and Imre Leader. Matchings and paths in the cube. *Discret. Appl. Math.*, 75(1):1–8, 1997. doi:10.1016/S0166-218X(96)00076-5. 11, 18

BM11 Andrej Bogdanov and Elchanan Mossel. On extracting common random bits from correlated sources. *IEEE Trans. Inf. Theory*, 57(10):6351–6355, 2011. doi:10.1109/TIT.2011.2134067. 9

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

BNP08 Assaf Ben-David, Noam Nisan, and Benny Pinkas. FairplayMP: a system for secure multi-party computation. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *ACM CCS 2008: 15th Conference on Computer and Communications Security*, pages 257–266, Alexandria, Virginia, USA, October 27–31, 2008. ACM Press. doi:10.1145/1455770.1455804. 4

Bor82 Christer Borell. Positivity improving operators and hypercontractivity. *Mathematische Zeitschrift*, 180(3):225–234, 1982. doi:10.1007/BF01318906. 9

Can00a Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, January 2000. doi:10.1007/s001459910006. 14

Can00b Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2000. http://eprint.iacr.org/2000/067. 14

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

CDLR16 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: 14th Theory of Cryptography Conference, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 204–234, Beijing, China, October 31 – November 3, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-53641-4_9. 3

CK88 Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *29th Annual Symposium on Foundations of Computer Science*, pages 42–52, White Plains, NY, USA, October 24–26, 1988. IEEE Computer Society Press. doi:10.1109/SFCS.1988.21920. 3, 9

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

CMN14 Siu On Chan, Elchanan Mossel, and Joe Neeman. On extracting common random bits from correlated sources on large alphabets. *IEEE Trans. Inf. Theory*, 60(3):1630–1637, 2014. doi:10.1109/TIT.2014.2301155. 9

CMW05 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: 4th International Conference on Security in Communication Networks*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59, Amalfi, Italy, September 8–10, 2005. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-30598-9_4. 3

COSV17a Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Delayed-input non-malleable zero knowledge and multi-party coin tossing in four rounds. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017: 15th Theory of Cryptography Conference, Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 711–742, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_24. 3

COSV17b Michele Ciampi, Rafail Ostrovsky, Luisa Siniscalchi, and Ivan Visconti. Round-optimal secure two-party computation from trapdoor permutations. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017: 15th Theory of Cryptography Conference,* *Part I*, volume 10677 of *Lecture Notes in Computer Science*, pages 678–710, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_23. 3

Cra11 Ronald Cramer. The arithmetic codex: Theory and applications (invited talk). In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, page 1, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-20465-4_1. 5

Cré88 Claude Crépeau. Equivalence between two flavours of oblivious transfers. In Carl Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 350–354, Santa Barbara, CA, USA, August 16–20, 1988. Springer, Heidelberg, Germany. doi:10.1007/3-540-48184-2_30. 2, 9

DKS99 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, *Advances in Cryptology – EUROCRYPT'99*, volume 1592 of *Lecture Notes in Computer Science*, pages 56–73, Prague, Czech Republic, May 2–6, 1999. Springer, Heidelberg, Germany. doi:10.1007/3-540-48910-X_5. 3

DMN18 Anindya De, Elchanan Mossel, and Joe Neeman. Non interactive simulation of correlated distributions is decidable. In Artur Czumaj, editor, *29th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2728–2746, New Orleans, LA, USA, January 7–10, 2018. ACM-SIAM. doi:10.1137/1.9781611975031.174. 9

DPSZ12 Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 643–662, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-32009-5_38. 4

Gen09 Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Computing*, pages 169–178, Bethesda, MD, USA, May 31 – June 2, 2009. ACM Press. doi:10.1145/1536414.1536440. 4

GIK$^+$15 Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with one-way communication. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 191–208, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-48000-7_10. 5, 6, 7, 8, 10

GK73 Peter Gács and János Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973. 9

GKM$^+$00 Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan. The relationship between public key encryption and oblivious transfer. In *41st Annual Symposium on Foundations of Computer Science*, pages 325–335, Redondo Beach, CA, USA, November 12–14, 2000. IEEE Computer Society Press. doi:10.1109/SFCS.2000.892121. 3, 4

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

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

GMW87 Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, NY, USA, May 25–27, 1987. ACM Press. doi:10.1145/28395.28420. 2, 3, 9

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

GR16 Venkatesan Guruswami and Jaikumar Radhakrishnan. Tight bounds for communication-assisted agreement distillation. In Ran Raz, editor, *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, volume 50 of *LIPIcs*, pages 6:1–6:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPIcs.CCC.2016.6. 5

Har66 Lawrence H Harper. Optimal numberings and isoperimetric problems on graphs. *Journal of Combinatorial Theory*, 1(3):385–393, 1966. 11

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

Hir35 Hermann O Hirschfeld. A connection between correlation and contingency. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 520–524. Cambridge University Press, 1935. doi:10.1017/S0305004100013517. 9

IK00 Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *41st Annual Symposium on Foundations of Computer Science*, pages 294–304, Redondo Beach, CA, USA, November 12–14, 2000. IEEE Computer Society Press. doi:10.1109/SFCS.2000.892118. 10

IK02 Yuval Ishai and Eyal Kushilevitz. Perfect constant-round secure computation via perfect randomizing polynomials. In Peter Widmayer, Francisco Triguero Ruiz, Rafael Morales Bueno, Matthew Hennessy, Stephan Eidenbenz, and Ricardo Conejo, editors, *ICALP 2002: 29th International Colloquium on Automata, Languages and Programming*, volume 2380 of *Lecture Notes in Computer Science*, pages 244–256, Malaga, Spain, July 8–13, 2002. Springer, Heidelberg, Germany. doi:10.1007/3-540-45465-9_22. 10

IKO$^+$11 Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 667–684, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-22792-9_38. 3, 5, 10

IPS08 Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 572–591, Santa Barbara, CA, USA, August 17–21, 2008. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-85174-5_32. 3, 5, 10

Jay10 T. S. Jayram. Information complexity: a tutorial. In Jan Paredaens and Dirk Van Gucht, editors, *Proceedings of the Twenty-Ninth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, PODS 2010, June 6-11, 2010, Indianapolis, Indiana, USA*, pages 159–168. ACM, 2010. doi:10.1145/1807085.1807108. 5

KA12 Sudeep Kamath and Venkat Anantharam. Non-interactive simulation of joint distributions: The hirschfeld-gebelein-rényi maximal correlation and the hypercontractivity ribbon. In *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1057–1064. IEEE, 2012. 6, 7

KA16 Sudeep Kamath and Venkat Anantharam. On non-interactive simulation of joint distributions. *IEEE Transactions on Information Theory*, 62(6):3419–3435, 2016. 6, 7, 9

Kil88 Joe Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing*, pages 20–31, Chicago, IL, USA, May 2–4, 1988. ACM Press. doi:10.1145/62212.62215. 3

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

Kil00 Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd Annual ACM Symposium on Theory of Computing*, pages 316–324, Portland, OR, USA, May 21–23, 2000. ACM Press. doi:10.1145/335305.335342. 3, 9

KLL$^+$12 Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. In *53rd Annual Symposium on Foundations of Computer Science*, pages 500–509, New Brunswick, NJ, USA, October 20–23, 2012. IEEE Computer Society Press. doi:10.1109/FOCS.2012.68. 5

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

KMS16 Dakshita Khurana, Hemanta K. Maji, and Amit Sahai. Secure computation from elastic noisy channels. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 184–212, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-49896-5_7. 3

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

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

Lov14 Shachar Lovett. Communication is bounded by root of rank. In David B. Shmoys, editor, *46th Annual ACM Symposium on Theory of Computing*, pages 842–846, New

York, NY, USA, May 31 – June 3, 2014. ACM Press. doi:10.1145/2591796.2591799. 5

Mau91 Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In *23rd Annual ACM Symposium on Theory of Computing*, pages 561–571, New Orleans, LA, USA, May 6–8, 1991. ACM Press. doi:10.1145/103418.103476. 4

Mau92 Ueli M. Maurer. A universal statistical test for random bit generators. *Journal of Cryptology*, 5(2):89–105, January 1992. doi:10.1007/BF00193563. 4

Mau93 Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39(3):733–742, 1993. doi:10.1109/18.256484. 4

MMP14a Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. Limits of random oracles in secure computation. In Moni Naor, editor, *ITCS 2014: 5th Conference on Innovations in Theoretical Computer Science*, pages 23–34, Princeton, NJ, USA, January 12–14, 2014. Association for Computing Machinery. doi:10.1145/2554797.2554801. 3

MMP14b Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran. On the power of public-key encryption in secure computation. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 240–264, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-54242-8_11. 3, 4

MNPS04 Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - secure two-party computation system. In Matt Blaze, editor, *USENIX Security 2004: 13th USENIX Security Symposium*, pages 287–302, San Diego, CA, USA, August 9–13, 2004. USENIX Association. 4

MO05 Elchanan Mossel and Ryan O'Donnell. Coin flipping from a cosmic source: On error correction of truly random bits. *Random Structures & Algorithms*, 26(4):418–436, 2005. doi:10.1002/rsa.20062. 9

MOR$^+$06 Elchanan Mossel, Ryan O'Donnell, Oded Regev, Jeffrey E Steif, and Benny Sudakov. Non-interactive correlation distillation, inhomogeneous markov chains, and the reverse bonami-beckner inequality. *Israel Journal of Mathematics*, 154(1):299–336, 2006. 5, 9

MOS13 Elchanan Mossel, Krzysztof Oleszkiewicz, and Arnab Sen. On reverse hypercontractivity. *Geometric and Functional Analysis*, 23(3):1062–1097, 2013. 9

NNOB12 Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. A new approach to practical active-secure two-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 681–700, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-32009-5_40. 4

NW17 Chandra Nair and Yan Nan Wang. Reverse hypercontractivity region for the binary erasure channel. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 938–942. IEEE, 2017. doi:10.1109/ISIT.2017.8006666. 7

O'D14 Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. 14

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

PP10 Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2602–2606. IEEE, 2010. doi:10.1109/ISIT.2010.5513743. 10

PP11 Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information: Further results. In Alexander Kuleshov, Vladimir M. Blinovsky, and Anthony Ephremides, editors, *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011*, pages 2861–2865. IEEE, 2011. doi:10.1109/ISIT.2011.6034098. 10

PP14 Vinod M. Prabhakaran and Manoj Prabhakaran. Assisted common information with an application to secure two-party sampling. *IEEE Trans. Inf. Theory*, 60(6):3413–3434, 2014. doi:10.1109/TIT.2014.2316011. 10

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

Rab81 Michael O. Rabin. How to exchange secrets by oblivious transfer. *Technical Memo TR-81*, 1981. 2, 9

Rab05 Michael O. Rabin. How to exchange secrets with oblivious transfer. Cryptology ePrint Archive, Report 2005/187, 2005. http://eprint.iacr.org/2005/187. 2, 9

Rén59 Alfréd Rényi. On measures of dependence. *Acta mathematica hungarica*, 10(3-4):441–451, 1959. doi:10.1007/BF02024507. 9

RP14 K. Sankeerth Rao and Vinod M. Prabhakaran. A new upperbound for the oblivious transfer capacity of discrete memoryless channels. In *2014 IEEE Information Theory Workshop, ITW 2014, Hobart, Tasmania, Australia, November 2-5, 2014*, pages 35–39. IEEE, 2014. doi:10.1109/ITW.2014.6970787. 10

STW20 Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for generating correlation: A unifying survey. *IEEE Trans. Inf. Theory*, 66(1):5–37, 2020. doi:10.1109/TIT.2019.2946364. 5, 9

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

Wit75 Hans S Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975. doi:doi.org/10.1137/0128010. 9

Wul07 Jürg Wullschleger. Oblivious-transfer amplification. In Moni Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 555–572, Barcelona, Spain, May 20–24, 2007. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-72540-4_32. 3

Wul09 Jürg Wullschleger. Oblivious transfer from weak noisy channels. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 332–349. Springer, Heidelberg, Germany, March 15–17, 2009. doi:10.1007/978-3-642-00457-5_20. 3

WW05 Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 467–477, Santa Barbara, CA, USA, August 14–18, 2005. Springer, Heidelberg, Germany. doi:10.1007/11535218_28. 10

WW06 Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232, St. Petersburg, Russia, May 28 – June 1, 2006. Springer, Heidelberg, Germany. doi:10.1007/11761679_14. 3, 9

Wyn75 Aaron Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975. doi:10.1109/TIT.1975.1055346. 3, 9

Yan04 Ke Yang. On the (im)possibility of non-interactive correlation distillation. In Martin Farach-Colton, editor, *LATIN 2004: Theoretical Informatics, 6th Latin American Symposium*, volume 2976 of *Lecture Notes in Computer Science*, pages 222–231, Buenos Aires, Argentina, April 5–8, 2004. Springer, Heidelberg, Germany. 7, 9

Yao82 Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science*, pages 160–164, Chicago, Illinois, November 3–5, 1982. IEEE Computer Society Press. doi:10.1109/SFCS.1982.38. 2, 9

YP14 Zi Yin and Youngsuk Park. Hypercontractivity, maximal correlation and non-interactive simulation. 2014. 6

A Omitted Proofs in Section 4

A.1 Proof of Lemma 1

Proof. First we show that

$$\mathop{\mathbb{E}}_{x^n\sim U_{\{0,1\}^n}} \left| \mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)} \mathop{\mathbb{E}}_{z^n\sim M(y^n)} f(z^n) - (1-\epsilon')f(x^n) \right| \leq 2\delta. \tag{7}$$

By triangle inequality we have

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

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

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

$$\mathop{\mathbb{E}}_{y^n\sim Q_\epsilon(x^n)} \mathop{\mathbb{E}}_{z^n\sim M(y^n)} f(z^n) = \mathsf{T}_\rho(f)(x^n). \tag{8}$$

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

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

And so $\Pr[z_i^n = 1 - x_i^n] = \frac{\epsilon}{2}$. This completes the proof of equation(8). Finally, substituting equation (8) in to inequality (7) gives the desired inequality. ◀

A.2 Proof of Lemma 2

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

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

It implies that

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

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

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

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

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

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

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

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

A.3 Proof of Lemma 3

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

A.4 Proof of Theorem 6

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

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

Proof. For each $y^n \in \{0,1,\perp\}^n$, we define $J(y^n) := \{i \in [n] \colon y^n_i = \perp\}$, $\overline{J(y^n)} = [n] \setminus J(y^n)$, and $z(y^n)$ as the concatenation of all non-bot symbols in y^n. For example, when $y^4 = 0\perp1\perp$, $J(y^4) = \{2,4\}$, $\overline{J(y^4)} = \{1,3\}$, and $z(y^4) = 01$. For $x^n, y^n \in \{0,1,\perp\}^n$, we say that they are neighbor (sibling) of each other if $J(x^n) = J(y^n)$, and $z(x^n), z(y^n)$ are different at exactly one coordinate (their Hamming distance is one). Suppose $z(x^n)$ and $z(y^n)$ differ at coordinate j. We define the parent of x^n, y^n is the vector obtained by replacing the coordinate j of x^n by the bot symbol. For instance, $00\perp\perp$ is a neighbor of $01\perp\perp$, and their parent is $0\perp\perp\perp$. Recall the definition of restriction of function to sub-cubes from Subsection 2.3 that the function $f_{J(y^n)|z(y^n)} \colon \{0,1\}^{|J(y^n)|} \to \{-1,1\}$ denotes the restriction of f to $J(y^n)$ when the coordinates in $\overline{J(y^n)}$ is fixed to $z(y^n)$. For ease of presentation, we denote $f_{J(y^n)|z(y^n)}$ as f_{y^n}. When $\nu(n) = 0$, Alice security condition implies that

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

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

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

$$y^n_* = \mathop{\mathrm{argmin}}_{y^n \colon \left|\widehat{f_{y^n}}(\emptyset)\right| = 1} |J(y^n)|\,.$$

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

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

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

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

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

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

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

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

▶ **Lemma 7.** *In Theorem 6, statement (2) implies statement (1).*

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

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

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

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

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

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

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

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

This completes the feasibility of the proof of Theorem 5 when $\nu(n) = 0$. ◀

B Omitted Proofs in Section 5

B.1 Proof of Lemma 4

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

$$\frac{\langle f, \mathsf{T}_\rho f\rangle + \langle g, \mathsf{T}_\rho g\rangle}{2} \geq |\langle f, \mathsf{T}_\rho g\rangle| = |\langle g, \mathsf{T}_\rho f\rangle| \tag{9}$$

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

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

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

which is equivalent to

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

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

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

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

Lower bound for the right hand side.

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

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

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

which completes our proof of Lemma 4. ◀

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

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

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

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

Using term-wise AM-GM, we have

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

which give us the inequality as desired. ◀

B.2 Proof of Theorem 8

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

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

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

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

$$\mathsf{T}_\rho f(x) = \sum_{S \subseteq [n]} \rho^{|S|} \widehat{f}(S) \chi_S(x)$$

$$\rho' f(x) = \rho' \sum_{S \subseteq [n]} \widehat{f}(S) \chi_S(x) = \sum_{S \subseteq [n]} \rho' \widehat{f}(S) \chi_S(x)$$

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

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

▶ **Lemma 9.** *In Theorem 8, statement (2) implies statement (1).*

Proof. Note that

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

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

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

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

   which implies that

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

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

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

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

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

C Omitted Proofs in Section 6

C.1 Proof of Lemma 5

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

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

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

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

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

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

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

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

◀

C.2 Proof of Corollary 1

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

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

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