Secure Non-Interactive Reduction and Spectral Analysis of Correlations

Pratyush Agarwal[1], Varun Narayanan[2⋆], Shreya Pathak[1], Manoj Prabhakaran[1⋆⋆], Vinod M. Prabhakaran[3[0000−0001−7505−5303]⋆⋆⋆], and Mohammad Ali Rehan[1]

[1] Indian Institute of Technology Bombay, India
{pratyush,shreyapathak,mp,alirehan}@cse.iitb.ac.in
[2] Technion, Israel
varunnkv@gmail.com
[3] Tata Institute of Fundamental Research, India
vinodmp@tifr.res.in

Abstract. Correlated pairs of random variables are a central concept in information-theoretically secure cryptography. Secure reductions between different correlations have been studied, and completeness results are known. Further, the complexity of such reductions is intimately connected with circuit complexity and efficiency of locally decodable codes. As such, making progress on these complexity questions faces strong barriers. Motivated by this, in this work, we study a restricted form of secure reductions — namely, Secure *Non-Interactive* Reductions (SNIR) — which is still closely related to the original problem, and establish several fundamental results and relevant techniques for it.

We uncover striking connections between SNIR and linear algebraic properties of correlations. Specifically, we define the spectrum of a correlation, and show that a target correlation has a SNIR to a source correlation only if the spectrum of the latter contains the entire spectrum of the former. We also establish a "mirroring lemma" that shows an unexpected symmetry between the two parties in a SNIR, when viewed through the lens of spectral analysis. We also use cryptographic insights and elementary linear algebraic analysis to fully characterize the role of common randomness as well as local randomness in SNIRs. We employ these results to resolve several fundamental questions about SNIRs, and to define future directions.

1 Introduction

Correlated pairs of random variables — or correlations, for short — are central to information-theoretic cryptography. In particular, 2-party function evaluation

⋆ Supported by the Department of Atomic Energy, India project RTI4001, ERC Project NTSC (742754) and ISF Grants 1709/14 & 2774/20.
⋆⋆ Supported by a Ramanujan Fellowship and Joint Indo-Israel Project DST/INT/ISR/P-16/2017 of Dept. of Science and Technology, India.
⋆⋆⋆ Supported by the Department of Atomic Energy, India project RTI4001, and Science & Engineering Research Board, India project MTR/2020/000308.

can be *securely reduced* to sampling from such a correlation, with information-theoretic security, against passive or active corruption [16,17,24,20]. Among other things, such a reduction defines an important *cryptographic complexity* measure of a function [7,26,25,6,27] – namely, the number of samples of a correlation that need to be used in a secure 2-party computation protocol for the function[4]. Proving lower bounds for cryptographic complexity is a difficult problem, thanks to its implications to circuit complexity and locally decodable codes; even the existence of functions with super-linear cryptographic complexity remains open. As such, it is prudent to approach cryptographic complexity gently, through simplified problems and models. Taking a cue from circuit complexity, where simpler circuit models like AC^0 have served as a platform for developing new ideas and sophisticated techniques, here we consider a simplified model of secure *non-interactive* reductions (SNIR). Note that, without communication, it is impossible to *compute* non-trivial functions which take inputs from both parties;[5] hence we only consider the problem of *sampling* from a target correlation. In a non-interactive reduction of a target correlation D to a source correlation C, two parties receive correlated randomness from the source C; then they carry out a local computation (possibly randomized) and produce their outputs, which are to be jointly distributed according to D. The security requirement, informally, requires that a party should learn nothing more about the other party's output than is revealed by its own *output*, irrespective of what it receives from the source correlation.

Apart from being a simpler model to analyze, SNIR in fact isolates one of two components of an interactive secure reduction. A secure reduction can be viewed as consisting of two parts: Firstly, an interaction phase transforms the views of the two parties arbitrarily, subject only to the constraints of protocols (there is no element of security here); secondly, a local derivation step is used to transform the views resulting from this interaction to the outputs. The security condition solely applies to this second local derivation step. Thus the feasibility of an (interactive) secure reduction from D to C splits into the question of whether there exists a correlation C' such that (i) C' is the distribution of the views at the end of an interaction between the parties starting with C, and (ii) D has a SNIR to C'.

SNIR is also a natural and strictly stronger variant of a well-studied model in information-theory, namely, (non-secure) non-interactive reduction – or *non-interactive simulation* as it is more commonly known – which has attracted a significant amount of research in both information-theory and computer science literature [13,30,31,4,21,15,29].

[4] The choice of the exact correlation is not crucial and can be replaced by any finite complete functionality, without altering the complexity beyond constant factors [25].

[5] There does exist an alternate model of *Zero Communication Reductions* which allows non-interactive function computation conditioned on a predicate [27]. But here we consider the standard model of secure 2-party computation, except for the restriction of being non-interactive.

Our Contributions. We introduce a spectral analysis toolkit for (statistically) secure non-interactive reductions (SNIR), and use it to resolve several fundamental questions about SNIR.

As part of the toolkit, we derive the following results. The results refer to the *spectrum of a correlation*, $\mathbf{\Lambda}_C$ which we define as the multi-set of singular values of the *correlation operator* associated with the correlation C (see Section 2.2). Also they deal with "non-redundant" correlations (since, as we shall see, redundancies – which can be introduced or removed using local operations – do not have any effect on the existence of SNIRs).

Suppose there is a statistical SNIR, that reduces a non-redundant correlation D to a correlation C with ϵ error, then:

- D has a statistical SNIR to C using *deterministic* protocols (Lemma 7).
- $\mathbf{\Lambda}_D \subseteq \mathbf{\Lambda}_{C^{\otimes \ell}}$ for some $\ell \in \mathbb{N}$ (Theorem 4).
- the "spectral representation" of the SNIR satisfies a symmetry property, that we term *mirroring* (Theorem 5).

Furthermore, if D does not have a statistical SNIR to C, then it has no statistical SNIR to C even when both parties have access to unlimited common randomness (Theorem 6).

These general results can in turn be used to derive a variety of results. In particular, we show that there is *no complete correlation* for SNIR (Theorem 7). We also obtain a full characterization of all the parameter changes that are possible via SNIR for two correlation classes of interest, namely *doubly symmetric binary correlation* BSC (Theorem 8) and *binary erasure correlation* BEC (Theorem 9). For OLE correlations over finite fields, we obtain a necessary condition for SNIR (Theorem 10). We also derive results (Theorem 11 and Theorem 12) implied by impossibility results in the one-way secure computation model [14], that BEC and *oblivious transfer correlation* do not have a SNIR to BSC; we remark that the proof in [14], based on isoperimetric inequalities, yields a quantitatively weaker form that leaves open the possibility of inverse-polynomial security.

Finally, we also relate SNIR to secure (interactive) reductions of a correlation D to another C. Recall from the discussion earlier that a secure interactive protocol for D includes a SNIR from D to the view of the two parties at the end of the interaction. In fact, a stronger statement is possible: We show that when a correlation involves common information (as is the case with the view after interaction, which includes the transcript – and possibly more – as common information), then D should have a SNIR to one of the correlations obtained from C conditioned on a value for the common information. (Lemma 4 and Lemma 12). This motivates a challenging (non-cryptographic) problem of characterizing the spectrum of correlations that can be obtained as the view of an interaction starting with a given correlation C. We leave this as an open problem.

Related Work. As mentioned above, (interactive) secure reductions and non-interactive (non-secure) reductions have both been widely studied. In an independent, concurrent work Khorasgani et al. [23,22] also studied SNIRs. While these works also followed a linear-algebraic approach, their motivations and re-

sults were different. In particular, their results were mostly restricted to studying specific simple target correlations—the binary symmetric and binary erasure correlations—which admitted the use of Fourier analysis of boolean functions. In contrast, driven by the connections to circuit complexity lower bounds, we derive results that apply to arbitrary target correlations, including those which may have a high circuit complexity. On the other hand, for the simpler target correlations, [23,22] consider more fine-grained questions related to the rate of reduction, and the decidability of reduction to other correlations. We do not address these problems. Boyle et al. [9,10] introduced *pseudorandom correlation generators* which achieve the same objective against computationally bounded adversaries.

While perhaps not explicitly studied previously, the notions of a correlation operator and the spectrum of a correlation that are defined in this work have been implicitly present in spectral graph theory (by representing a correlation as a bipartite graph). An important element of the spectrum of a correlation was defined as maximal correlation by [30] for proving a seminal result of (non-secure) interactive reductions; in [2], it was observed that this proof can be cast in the language of spectral graph theory.

2 Technical Overview

Here we present an overview of the tools that we develop to derive impossibility results for SNIRs. Our starting point is a linear-algebraic formulation of a SNIR. For this, a distribution over $\mathcal{X} \times \mathcal{Y}$ is represented by a $|\mathcal{X}| \times |\mathcal{Y}|$ matrix whose entry with row indexed by $x \in \mathcal{X}$ and column indexed by $y \in \mathcal{Y}$ is simply the probability $\Pr[(x, y)]$ of Alice getting x and Bob getting y. In the following, we consider a SNIR from a *target* correlation represented by a matrix $D \in \mathbb{R}^{m_D \times n_D}$ to a *source* correlation represented by a matrix $C \in \mathbb{R}^{m_C \times n_C}$. Restricting here to the case of perfect security, a SNIR translates to a pair of stochastic "protocol" matrices (A, B) representing Alice and Bob's actions (mapping a symbol from the source to a symbol in the target), and a pair of "simulation" matrices (U, V) such that

$$A^\intercal \, C \, B = D \qquad A^\intercal \, C = D \, V \qquad C \, B = U^\intercal \, D. \tag{1}$$

The first identity is a straightforward linear algebraic interpretation of the correctness of the protocol, while the next two capture the security against a corrupt Bob and a corrupt Alice, respectively, as linear algebraic constraints. These identities are proved in Theorem 3, more generally, for statistical SNIR. As we would be interested in allowing access to arbitrarily many copies of a given correlation C_0, one should interpret C as the tensor power $C_0^{\otimes \ell}$ for an arbitrarily large integer ℓ. (However, w.l.o.g. we may consider D to be a single copy of the correlation we are interested in obtaining. As such, when considering statistical security, we shall use the $O_D(\cdot)$ notation to indicate an upper bound that hides a factor that is a function of D alone.)

Once viewed linear algebraically, we start obtaining consequences, which may not be evident *a priori*, through a series of steps that combine cryptographic intuition with linear algebraic manipulation. For ease of exposition, first we describe these steps for a *perfect* SNIR where many of the delicate technicalities disappear. We shall also sometimes focus on the case when the *marginal distributions* of Alice's and Bob's side of the correlations are uniform.

2.1 Restricting to Non-Redundant Correlations

Suppose two distinct symbols x_1, x_2 that Alice can obtain from D are such that conditioned on either, the distribution of the symbol obtained by Bob is the same. In this case, we may as well merge these two symbols into a single symbol, on obtaining which, Alice can probabilistically interpret it as x_1 or x_2 locally. We refer to the presence of such symbols, for either party, as *redundancy*. It is easily verified that for the purposes of secure sampling, every correlation is equivalent to a non-redundant correlation (obtained by merging groups of redundant symbols).

To understand the implications of having a SNIR from a non-redundant D to C, consider the following: Suppose Alice and Bob are given samples from D; then Alice outputs the value she got, but Bob locally samples an output based on the value he got as below.

- Bob's goal is that the joint distribution of what the two parties output should still correspond to D. The existence of a SNIR provides a way for Bob to do this: He first feeds the output from D to the *simulator* (V), to obtain a simulated view – i.e., his side of an output from C. The simulation guarantees that the joint distribution of Alice's output and Bob's view are as in a real execution of the protocol; now Bob applies his protocol (B) to the outcome of the simulation, to obtain his altered output.
- On the other hand, non-redundancy of D should imply – intuitively – that the only mapping Bob can use is the identity mapping.

Linear algebraically, the first statement corresponds to $DVB = A^{\intercal}CB = D$, and the latter is the assertion (which needs a proof) that, if D is non-redundant, then for any stochastic matrix X, $DX = D \Rightarrow X = I$. Taken together, this gives

$$VB = I, \qquad UA = I, \tag{2}$$

where the second identity follows from the same argument with Alice's and Bob's roles reversed. Thus, the protocol must in fact invert the simulation. This is possible only if the protocol is *deterministic*, as applying a randomized strategy to the output of a process (namely, the simulation) cannot guarantee that the output will match the input to simulation. That is, the protocol (on each party's side) could be viewed as simply a partition of the alphabet of C, with symbols in each part being mapped to a different symbol in the alphabet of D. This tells us further that the simulation should simply distribute each D symbol back to C symbols according to their relative probabilities. When the marginal distribution

for Alice (resp., Bob) from the correlations D and C are both uniform, this simplifies to

$$U = \frac{n_D}{n_C} A^\intercal \qquad \left(\text{resp., } V = \frac{m_D}{m_C} B^\intercal\right). \tag{3}$$

An Eigenvalue Condition. Our first result is a necessary condition for SNIR in terms of the eigenvalues of matrices associated with the two correlations. Here, we first discuss the case of uniform marginal distributions and perfect security, followed by the important extensions to the general case.

Theorem 1 (Informal). *A uniform-marginal correlation with matrix $D \in \mathbb{R}^{m_D \times n_D}$ has an SNIR to a uniform-marginal correlation with matrix $C \in \mathbb{R}^{m_C \times n_C}$ only if all the eigenvalues of $m_D n_D DD^\intercal$ are also eigenvalues of $m_C n_C CC^\intercal$.*

Given our observations above, we have a short derivation of this result in the special case of uniform marginals. Using the two security conditions in (1) and the two equations in (3), we have

$$\begin{aligned} m_C n_C A^\intercal CC^\intercal = m_C n_C (DV) C^\intercal &= m_D n_C DB^\intercal C^\intercal \\ &= m_D n_C D(D^\intercal U) = m_D n_D DD^\intercal A^\intercal. \end{aligned}$$

Now, suppose λ is an eigenvalue of the symmetric matrix $m_D n_D DD^\intercal$, with a corresponding eigenvector $\boldsymbol{v}$. Then

$$(\boldsymbol{v}^\intercal A^\intercal) \cdot m_C n_C \cdot CC^\intercal = \boldsymbol{v}^\intercal (m_D n_D \cdot DD^\intercal) A^\intercal = \lambda \boldsymbol{v}^\intercal A^\intercal.$$

Hence we conclude that λ is an eigenvalue of $m_C n_C \cdot CC^\intercal$ as well (with eigenvector $A\boldsymbol{v}$).

2.2 Beyond Uniform Marginals: The Correlation Operator

So far, we represented a correlation of $\mathcal{X} \times \mathcal{Y}$ as a matrix M, with rows indexed by Alice's alphabet $\mathcal{X}$ and columns indexed by Bob's alphabet $\mathcal{Y}$, with $M_{x,y} = \Pr[(x, y)]$. However, when the marginal distributions of this correlation are not uniform, the above linear-algebraic arguments do not go through. This leads us to an alternate representation of a correlation in the form of what we call the **correlation operator**. It is a linear transformation defined by the matrix $\widetilde{M}$ as follows:[6]

$$\widetilde{M}_{x,y} = \frac{M_{x,y}}{\sqrt{\boldsymbol{a}_x \boldsymbol{b}_y}} \text{ where } \boldsymbol{a}_x = \sum_{y' \in \mathcal{Y}} M_{x,y'} \text{ and } \boldsymbol{b}_y = \sum_{x' \in \mathcal{X}} M_{x',y}.$$

A correlation operator transforms a $|\mathcal{Y}|$-dimensional (column) vector with entries of the form $\boldsymbol{q}_y / \sqrt{\boldsymbol{b}_y}$ into a $|\mathcal{X}|$-dimensional vector with entries of the

[6] Here we use the convention that symbols with 0 probability are omitted from the alphabets $\mathcal{X}$ and $\mathcal{Y}$, so that all the marginal probabilities $\boldsymbol{a}_x$ and $\boldsymbol{b}_y$ are strictly positive.

form $\boldsymbol{p}_x/\sqrt{\boldsymbol{a}_x}$, where $\boldsymbol{p}$ denotes the conditional distribution of Alice's symbol according to M when Bob's symbol is conditioned to be according to $\boldsymbol{q}$ (i.e., $\boldsymbol{p}_x = \sum_y \boldsymbol{q}_y \Pr[x|y] = \sum_y \boldsymbol{q}_y M_{x,y}/\boldsymbol{b}_y$). The transpose of this operator carries out a similar transformation in the reverse direction. Here, note that the correlation operator operates on vectors with "normalized probabilities" in their respective vector spaces; the probabilities over $\mathcal{X}$ (resp. $\mathcal{Y}$) lie on the plane tangential to the unit sphere, touching it at $\sqrt{\boldsymbol{a}}$ (resp. $\sqrt{\boldsymbol{b}}$), since $\langle \boldsymbol{p}/\sqrt{\boldsymbol{a}}, \sqrt{\boldsymbol{a}} \rangle = 1$ (and, $\langle \boldsymbol{q}/\sqrt{\boldsymbol{b}}, \sqrt{\boldsymbol{b}} \rangle = 1$). The marginal distributions $\boldsymbol{a}$ and $\boldsymbol{b}$ themselves are represented by unit vectors ($\sqrt{\boldsymbol{a}}$ and $\sqrt{\boldsymbol{b}}$).

Clearly, the correlation operator and the marginal distributions together completely specify the correlation. But in fact, as the geometric interpretation above may suggest, the correlation operator encodes the marginal distribution as well.[7] Indeed, as we shall see, the direction in which the transformation is non-shrinking corresponds to the marginals in the respective vector spaces (unit vectors $\sqrt{\boldsymbol{a}}, \sqrt{\boldsymbol{b}}$); the action of the transformation on the vector space orthogonal to the marginal encodes the dependence component of the correlation.

Singular Value Decomposition (SVD). SVD provides us with a powerful tool to analyze the linear-algebraic properties of a correlation operator. Given an $m \times n$ distribution matrix M, we apply SVD to its correlation operator, to get

$$\widetilde{M} = \boldsymbol{\Psi}_M^{\intercal} \boldsymbol{\Sigma}_M \boldsymbol{\Phi}_M$$

where $\boldsymbol{\Sigma}_M$ is an $m \times n$ dimensional non-negative diagonal matrix, $\boldsymbol{\Psi}_M$ and $\boldsymbol{\Phi}_M$ are orthogonal matrices of dimensions $m \times m$ and $n \times n$, respectively (i.e., $\boldsymbol{\Psi}_M^{-1} = \boldsymbol{\Psi}_M^{\intercal}$ and $\boldsymbol{\Phi}_M^{-1} = \boldsymbol{\Phi}_M^{\intercal}$). It would be convenient to define *the spectrum of* M, $\boldsymbol{\Lambda}_M$ as the *multi-set* of singular values of $\widetilde{M}$ (i.e., the non-zero entries in $\boldsymbol{\Sigma}_M$).

Correlation Operator and Normalized Laplacian. A natural representation of a correlation M is in the form of a weighted bipartite graph G_M, with Alice's and Bob's alphabets forming the two vertex sets, and symbols x and y connected by an edge of weight $M_{x,y}$. (By our convention of omitting 0-probability symbols, there are no isolated vertices in G_M.) This representation allows one to use spectral graph theory to explore the correlation M. Indeed, the correlation operator $\widetilde{M}$ is closely related to the "Normalized Laplacian" $\mathcal{L}(G_M)$ of the bipartite graph described above. Specifically, from the definitions it follows that

$$\mathcal{L}(G_M) = I - \begin{bmatrix} & \widetilde{M} \\ \widetilde{M}^{\intercal} & \end{bmatrix}$$

[7] There is a caveat: if the correlation involves common information – i.e., if it is over pairs that can be written as $((x,c),(y,c))$ where c indicates a piece of information available to both parties – then, the distribution of the common random variable itself is not captured by the correlation operator. But as we shall see, this component of the distribution can indeed be ignored when studying the feasibility of SNIRs.

Lemma 1. *For any correlation $M \in \mathbb{R}^{m\times n}$, the multi-set of eigenvalues of $\mathcal{L}(G_M)$ is given by* $\{1 \pm \sigma \mid \sigma \in \mathbf{\Lambda}_M\} \cup \{\underbrace{1, \cdots, 1}_{\substack{m+n-2|\mathbf{\Lambda}_M| \\ \text{times}}}\}$.

A formal proof of the lemma is deferred to the full version [1].

Using this connection, the basic properties of the spectrum of a correlation follow from well-known results in spectral graph theory [11]. In particular, we see that all the elements in the spectrum $\mathbf{\Lambda}_M$ lie in the range $[0, 1]$, and the largest one equals 1. The multiplicity of 1 in $\mathbf{\Lambda}_M$ is one, unless the correlation M involves non-trivial common information (i.e., multiple connected components in the bipartite graph G_M). This singular value corresponds to the transformations between unit vectors, $\sqrt{\boldsymbol{a}}^{\mathsf{T}}\widetilde{M} = \sqrt{\boldsymbol{b}}^{\mathsf{T}}$ and $\widetilde{M}\sqrt{\boldsymbol{b}} = \sqrt{\boldsymbol{a}}$. The second largest singular value, which indicates an upper bound on the extent to which M is not a product distribution of the marginals, has in fact been identified and used previously as *maximal correlation* by Witsenhausen in a seminal work that initiated the study of (non-secure) non-interactive reductions [30].

2.3 Spectral Protocols

Now we return to the question of generalizing Theorem 1 to correlations C and D whose marginals need not be uniform. A "spectral view" of SNIR, in terms of the correlation operators $\widetilde{C}$ and $\widetilde{D}$, and the spectra $\mathbf{\Lambda}_C$ and $\mathbf{\Lambda}_D$ provides us with just the right tools.

Given a SNIR (A, B) from D to C, we consider the singular value decompositions $\widetilde{C} = \mathbf{\Psi}_C^{\mathsf{T}}\mathbf{\Sigma}_C\mathbf{\Phi}_C$ and $\widetilde{D} = \mathbf{\Psi}_D^{\mathsf{T}}\mathbf{\Sigma}_D\mathbf{\Phi}_D$. Then, we can show that the linear algebraic conditions for correctness and privacy, originally formulated in the "probability domain," yields analogous conditions in the "spectral domain," where the protocols (A, B) are represented by their spectral counterparts, $(\widehat{A}, \widehat{B})$, defined as follows:

$$\widehat{A} = \mathbf{\Psi}_C\, \mathbf{\Delta}_{C^{\mathsf{T}}}^{1/2}\, A\, \mathbf{\Delta}_{D^{\mathsf{T}}}^{-1/2}\, \mathbf{\Psi}_D^{\mathsf{T}}, \qquad \widehat{B} = \mathbf{\Phi}_C\, \mathbf{\Delta}_C^{1/2}\, B\, \mathbf{\Delta}_D^{-1/2}\, \mathbf{\Phi}_D^{\mathsf{T}}.$$

Here, the notation $\mathbf{\Delta}_M$ denotes a diagonal matrix with the vector $\mathbf{1}^{\mathsf{T}}M$ along its diagonal; note that $\widetilde{M} = \mathbf{\Delta}_{M^{\mathsf{T}}}^{-1/2}\, M\, \mathbf{\Delta}_M^{-1/2}$. The following lemma summarizes the properties of a SNIR, viewed in the spectral domain.

Lemma 2. *If (A, B) is a perfect SNIR from a non-redundant correlation D to a correlation C, then*

$$\widehat{A}^{\mathsf{T}}\mathbf{\Sigma}_C\widehat{B} = \mathbf{\Sigma}_D \quad \widehat{A}^{\mathsf{T}}\mathbf{\Sigma}_C = \mathbf{\Sigma}_D\widehat{B}^{\mathsf{T}} \quad \mathbf{\Sigma}_C\widehat{B} = \widehat{A}\mathbf{\Sigma}_D \quad \widehat{A}^{\mathsf{T}}\widehat{A} = I, \qquad \widehat{B}^{\mathsf{T}}\widehat{B} = I. \tag{4}$$

The lemma is formally proved in the full version [1]. The condition $\widehat{A}^{\mathsf{T}}\mathbf{\Sigma}_C\widehat{B} = \mathbf{\Sigma}_D$ is obtained by simply rearranging the linear algebraic conditions for correctness and privacy in the "probability domain" and using the definitions of $\widehat{A}, \widehat{B}, \mathbf{\Sigma}_C$ and $\mathbf{\Sigma}_D$. (It is also implied by the other equations.) To show that

$\widehat{A}^\intercal\widehat{A}$ and $\widehat{B}^\intercal\widehat{B}$ are identity, we exploit the conditions $UA = I$ and $VB = I$, respectively, from (2). For the remaining two "privacy" conditions we use the generalization of (3) to the case of non-uniform marginals.

$$U = \boldsymbol{\Delta}_{D^\intercal}^{-1} A^\intercal \boldsymbol{\Delta}_{C^\intercal}, \qquad V = \boldsymbol{\Delta}_D^{-1} B^\intercal \boldsymbol{\Delta}_C. \tag{5}$$

Compared to (1), the condition (4) in the "spectral domain" involves the diagonal matrices $\boldsymbol{\Sigma}_C$ and $\boldsymbol{\Sigma}_D$ instead of C and D. Further, it is devoid of simulators (U, V), which are replaced by $(\widehat{A}^\intercal, \widehat{B}^\intercal)$. Further, $\widehat{A}$ and $\widehat{B}$ have orthonormal columns, rather than being stochastic and deterministic.

Spectral Criterion. The spectral formulation of the conditions for SNIR in Lemma 2 lead us to the following generalization of Theorem 1.

Theorem 2 (Informal). *A non-redundant correlation D has a perfect SNIR to C only if $\boldsymbol{\Lambda}_D \subseteq \boldsymbol{\Lambda}_C$ (as multi-sets).*

This result follows from the conditions in Lemma 2. Specifically, using the second and third conditions from (4), we have

$$\widehat{A}^\intercal \boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal = \boldsymbol{\Sigma}_D \widehat{B}^\intercal \boldsymbol{\Sigma}_C^\intercal = \boldsymbol{\Sigma}_D \boldsymbol{\Sigma}_D^\intercal \widehat{A}^\intercal.$$

Since $\boldsymbol{\Sigma}_D$ is a diagonal matrix, for $j \in [m_D]$, $\boldsymbol{\xi}_j^\intercal \boldsymbol{\Sigma}_D \boldsymbol{\Sigma}_D^\intercal = (\boldsymbol{\Sigma}_D)_{j,j}^2 \boldsymbol{\xi}_j^\intercal$. Hence, premultiplying the above expression by $\boldsymbol{\xi}_j^\intercal$, we get

$$(\widehat{A}_{\cdot,j})^\intercal \boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal = (\boldsymbol{\Sigma}_D)_{j,j}^2 (\widehat{A}_{\cdot,j})^\intercal.$$

Note that $\boldsymbol{\Sigma}_C\ \boldsymbol{\Sigma}_C^\intercal$ is a diagonal matrix, and in the LHS of the above equation, each coordinate of $\widehat{A}_{\cdot,j}$ is scaled by the corresponding element in the diagonal, whereas in the RHS, all coordinates are scaled by the same scalar value. Hence, for every i such that $\widehat{A}_{i,j} > 0$, we require $(\boldsymbol{\Sigma}_C)_{i,i} = (\boldsymbol{\Sigma}_D)_{j,j}$. Since $\widehat{A}^\intercal\widehat{A} = I$ and, consequently, $\|\widehat{A}_{\cdot,j}\| = 1$, there must be at least one $i \in [m_C]$ with $\widehat{A}_{i,j} > 0$. Thus, there exists $i \in [m_C]$ such that $(\boldsymbol{\Sigma}_C)_{i,i} = (\boldsymbol{\Sigma}_D)_{j,j}$. In fact, we can further argue that if a singular value appears multiple times in $\boldsymbol{\Sigma}_D$ it should appear at least as many times in $\boldsymbol{\Sigma}_C$. For $\lambda > 0$, let $S_\lambda = \{j \in [m_D] \mid (\boldsymbol{\Sigma}_D)_{j,j} = \lambda\}$, and $T_\lambda = \{i \in [m_C] \mid (\boldsymbol{\Sigma}_C)_{i,i} = \lambda\}$. Consider the set of columns $\{\widehat{A}_{\cdot,j} | j \in S_\lambda\}$; recall that they are orthogonal to each other (since $\widehat{A}^\intercal\widehat{A} = 1$). Now, for each $j \in S_\lambda$, we argued that $\widehat{A}_{\cdot,j}$ is supported entirely on rows i such that $(\boldsymbol{\Sigma}_C)_{i,i} = \lambda$, i.e., on rows indexed by T_λ. Hence, $\widehat{A}$ restricted to rows T_λ and columns S_λ has full column rank. Hence $|T_\lambda| \geq |S_\lambda|$.

Mirroring Lemma. Pursuing the implications of the above arguments further, we uncover a surprising symmetry in the spectral images of a SNIR.

Consider any $\lambda \in \boldsymbol{\Lambda}_D$ and $j \in S_\lambda$ as defined above. Consider the row j in the equation $\widehat{A}^\intercal \boldsymbol{\Sigma}_C = \boldsymbol{\Sigma}_D \widehat{B}^\intercal$ (from (4)). We have,

$$\left(\widehat{A}^\intercal \boldsymbol{\Sigma}_C\right)_{j,i} = \begin{cases} \lambda \cdot \widehat{A}_{i,j} & \text{if } i \in T_\lambda, \\ 0 & \text{otherwise,} \end{cases}$$

since $\widehat{A}_{\cdot,j}$ is supported only on rows in T_λ, and for $i \in T_\lambda$, we have $(\mathbf{\Sigma}_C)_{i,i} = \lambda$. On the other hand, $\left(\mathbf{\Sigma}_D \widehat{B}^\intercal\right)_{j,\cdot}$ is the j^{th} row of $\widehat{B}^\intercal$ scaled by $(\mathbf{\Sigma}_D)_{j,j}$, or equivalently, it is $\lambda \widehat{B}^\intercal_{\cdot,j}$. Thus, we obtain that for all $j \in S_\lambda$, and $i \in T_\lambda$, $\widehat{A}_{i,j} = \widehat{B}_{i,j}$, and for $i \notin T_\lambda$ whenever defined, $\widehat{A}_{i,j} = 0$ and $\widehat{B}_{i,j} = 0$. Note that here we may expand the range T_λ to $[\min(m_C, n_C)]$. Also, since this holds for any λ, we can consider j to be in the union of all S_λ, or equivalently, $j \in [\text{rank}(\mathbf{\Sigma}_D)]$. This gives us the following result:

Lemma 3 (Informal)**.** *Suppose a non-redundant correlation $D \in \mathbb{R}^{m_D \times n_D}$ has a perfect SNIR (A, B) to a correlation $C \in \mathbb{R}^{m_C \times n_C}$. Let $d = \text{rank}(\mathbf{\Sigma}_D)$ and $r = \text{rank}(\mathbf{\Sigma}_C)$. Then for each $(i, j) \in [d] \times [r]$, $\widehat{A}_{i,j} = \widehat{B}_{i,j}$. Further, for $i \notin [r]$ and $j \in [d]$, $\widehat{A}_{i,j} = 0$ and $\widehat{B}_{i,j} = 0$ (whenever defined).*

2.4 Effect of Common Information

An important aspect of correlations is the presence or absence of common information. We say that a correlation has (non-zero) common information if there is a bit of positive entropy on which Alice and Bob can non-interactively agree with probability 1 [13]. A correlation C has common information if and only if the bipartite graph G_C contains two (or more) connected components (the correlation corresponds to sampling an edge from the graph, and giving a node to each party; they can agree on which connected component the edge lies in, and nothing more). Equivalently, the matrix for C can be written as $C = \begin{bmatrix} \alpha C_0 & 0 \\ 0 & (1-\alpha) C_1 \end{bmatrix}$, where C_0, C_1 are two correlations and $0 < \alpha < 1$.

In the context of (non-secure) non-interactive reductions, common information is a *complete correlation*. That is, given common information in a source correlation, Alice and Bob can sample from any target correlation. Indeed, the tools for proving infeasibility in this area focus on how far source correlations are from having common information, measured using maximal correlation[18,30,3,28,4], or alternately, using the (reverse) hypercontractivity ribbon [3,8,21,12,5]. On the other hand, in the context of *interactive* secure reductions, common information is a trivial resource (against passive corruption) that does not help at all. Here we investigate the effect of common information in the source for secure and non-interactive reductions.

We note that $\widetilde{C} = \begin{bmatrix} \widetilde{C_0} & 0 \\ 0 & \widetilde{C_1} \end{bmatrix}$ (which remains invariant to α). Hence, $\mathbf{\Lambda}_C = \mathbf{\Lambda}_{C_0} \cup \mathbf{\Lambda}_{C_1}$ (as multi-sets). By Theorem 2, D has a perfect SNIR to C only if $\mathbf{\Lambda}_D \subseteq \mathbf{\Lambda}_{C_0} \cup \mathbf{\Lambda}_{C_1}$. But in fact, we can obtain the following (proven in Section 7):

Lemma 4. *Suppose $C = \begin{bmatrix} \alpha C_0 & 0 \\ 0 & (1-\alpha) C_1 \end{bmatrix}$ where C_0, C_1 are two correlations and $0 < \alpha < 1$. Then, a non-redundant correlation D devoid of common information has a perfect SNIR to C only if D has a perfect SNIR to C_0 as well as a perfect SNIR to C_1; in particular, $\mathbf{\Lambda}_D \subseteq \mathbf{\Lambda}_{C_0} \cap \mathbf{\Lambda}_{C_1}$.*

2.5 Statistical SNIR

Perfectly secure SNIR can often be impossible even due to "uninteresting" reasons; e.g. it is impossible to realize a common random bit with bias 1/3 using unbiased common random bits with perfect correctness, however, this can be realized with negligible error. As such it is important to extend our tools above to handle the case of statistical security. A significant part of the technical effort in this paper is directed towards this goal, as many of the several steps described above require a careful analysis to be applicable to statistical security.

For statistical security in cryptographic protocols, one usually asks for errors (in correctness and security) to be *negligible* in a security parameter k, while the protocol's complexity remains polynomial in k. A weaker security guarantee often considered settles for a protocol family where for any polynomial p, there is a protocol that achieves $1/p(k)$ error. Even weaker security guarantees are considered in the information-theory literature: the error can be $1/p(k)$ for a fixed polynomial p, or even any fixed function p such that $p(k) \to \infty$ as $k \to \infty$. It is this weakest form of security – security with (merely) vanishing error – that we shall rule out, thereby achieving a strong notion of impossibility. In this form, there is no restriction on the complexity of the protocol itself – which, in the case of a SNIR from D to C, corresponds to the *number of samples from* C used by the protocol. That is, we seek to show that there is an error lower bound ϵ such that for any $t \in \mathbb{N}$, D does not have a SNIR to $C^{\otimes t}$ (the tensor power notation indicating a correlation consisting of t independent samples from C).

In deriving our technical results, we lower bound the error in a SNIR from D to C, wherein only a single instance of C is allowed. Then, for this lower bound to be useful in the above sense, the error bound should be independent of the dimensions of C (but can depend on spectral properties that are invariant to tensor powering). As such, we keep track of the errors in our necessary conditions for a SNIR with an error ϵ in the form of $O_D(\epsilon)$, where the upper bound notation $O_D(\cdot)$ hides constants that can depend on D (but not on C).

We briefly sketch the arguments we need for extending our results to statistical SNIR.

- Firstly, the linear algebraic characterization of SNIR in (1) extends to the setting with statistical error, with a tight characterization in terms of the 1-norm of the error matrices (Theorem 3).
- Next, we extend (2) to the statistical setting, in Lemma 6. Recall that this was based on the non-redundancy of the correlation D; specifically, in the perfect security case, we relied on the fact that if $D = DT$ for a stochastic matrix T, then $T = I$. We show an analogous result that if $D \approx DT$, then $T \approx I$, in terms of the 1-norm of the error matrices. The proof of this result (provided in the full version [1]) relies on a purely linear-algebraic technical observation which requires a careful application of Gaussian elimination.
- For the case of perfect security, we had argued that a SNIR for a non-redundant correlation D must be deterministic. Clearly, this is not the case any more for statistically secure SNIR, as a protocol can incur a small error by behav-

ing arbitrarily with a small probability, and still remain secure. Nevertheless, we show that every (possibly randomized) SNIR protocol can be "rounded" to a deterministic protocol with an error of ϵ getting amplified to $O_D(\sqrt{\epsilon})$ (Lemma 7). The following steps are shown for a deterministic protocol.

- A robust version of Lemma 2 is proven as Lemma 10. Among other things, this requires a robust version of (5), which is proven as Lemma 8. Lemma 10 provides *multiple* error bounds in terms of the 1-norm of various matrices related to the error matrices (corresponding to $\theta \in \{0, 1\}$ in the lemma statement). The reason for this is that we cannot afford to multiply the bounds with quantities that relate to C; instead, the lemma gives bounds for matrix expressions that incorporate C in two different ways, as are required in the subsequent proofs.
- Theorem 4 extends the spectral criterion $\mathbf{\Lambda}_D \subseteq \mathbf{\Lambda}_{C^{\otimes t}}$ in Theorem 2 to the case of statistical security. While all other extensions result in statements that incorporate an error term, it is notable that the spectral criterion holds exactly! The reason for this is that if $\mathbf{\Lambda}_D$ is not exactly contained in $\mathbf{\Lambda}_{C^{\otimes t}}$ for any t, then there must be an element in $\mathbf{\Lambda}_D$ that maintains a constant gap from all of $\mathbf{\Lambda}_{C^{\otimes t'}}$, irrespective of how large t' is (Lemma 9). The proof of Theorem 4 also requires carefully keeping track of the how errors propagate in the spectral domain, using Lemma 10 mentioned above, as well as a technical bound proven as Lemma 11.
- Theorem 5 extends the Mirroring Lemma (Lemma 3) to the case of statistical security. For an ϵ-SNIR, the statement here incurs an error of the form $O_D(\sqrt{\epsilon})/\alpha^2$, where α denotes how close an element in $\mathbf{\Lambda}_C$ can approach an element in $\mathbf{\Lambda}_D$ without equaling it. Again, this proof relies on Lemma 10 and Lemma 11.
- Lemma 12 extends Lemma 4 to the case of statistical security. If a correlation D, devoid of common information, has an ϵ-SNIR to C, then, by Lemma 12, D has an SNIR to one of its component correlation with error $O_D(\epsilon)$. In the full version [1], we will also show that D has an SNIR to each of its component correlations, but with error scaled inversely with the probability of the component. Lemma 12 is used in Theorem 6 to show that common randomness does not aid in realizing SNIR; Theorem 7 uses this lemma to show that no correlation is *complete* in the SNIR setting.

2.6 Applications

We demonstrate the utility of the toolset we built for analyzing SNIR via a few fundamental examples.

Incompleteness in SNIR. Our first result addresses the question of completeness in the SNIR model and answers it in negative Theorem 7. There exist no finite correlation such that every target correlation has a statistical SNIR to possibly arbitrarily many copies of the correlation. This is in contrast with multiple other models of secure computation with simple complete primitives. Specifically, for interactive secure computation, all *non-trivial correlations* are complete (a

trivial correlation is one in which the variables are independent conditioned on common information); in the case of (non-secure) non-interactive reduction (NIR), the complete correlations are exactly those which have non-zero common information.

Our incompleteness result is a consequence of the ineffectiveness of common information in SNIR. Lemma 12 shows that SNIR to a correlation C implies SNIR to one of its component correlations. A correlation D has no (non-secure) non-interactive reduction to a correlation C with strictly smaller maximal correlation; this implies that, given any correlation C, we can always choose a correlation D with a larger maximal correlation than all the component correlations of C.

Characterization of SNIR between Binary Symmetric Correlations. A binary symmetric correlation with crossover probability p, denoted by BSC_p, is a symmetric Boolean correlation that corresponds to giving a uniform random bit to Alice, and then giving the same bit to Bob with probability $1-p$ and the opposite bit with probability p. Consider a protocol in which, given k instances of BSC_p, Alice and Bob each output the XOR of their k bits. It is not hard to show that this is in fact a (perfect) SNIR from BSC_q to BSC_p, where $q = p*\ldots*p$ (k times) with the operator $*$ defined by $p*p' = p(1-p')+p'(1-p)$. Surprisingly, these are the only values of q for which there is a (possibly statistical) SNIR from BSC_q to BSC_p. This result, which fully resolves the question of SNIR between BSCs, follows directly from analyzing the spectra of the correlations of the form BSC_p and applying our spectral criterion for SNIRs.

Characterization of SNIR between Binary Erasure Correlations. BEC_p is a correlation which can be defined as picking a random bit for Alice, and sampling Bob's output based on it; here Bob gets an erasure symbol $\perp$ with probability p and the same bit as Alice got with probability $1-p$. Consider a protocol in which, given k instances of BEC_p, Alice outputs the XOR of all her bits, and Bob outputs $\perp$ if at least one of the symbols he received is $\perp$ and otherwise outputs the XOR of all the bits. This is a SNIR from BEC_q to BEC_p, where $1-q = (1-p)^k$. Again, surprisingly, these are the only values of q for which there is a (possibly statistical) SNIR from BEC_q to BEC_p. Again, this result follows directly from our spectral criterion.

Necessary Conditions for SNIR between OLE Correlations. We demonstrate the usefulness of spectral criterion by showing that it is impossible to obtain SNIR between OLE correlations over finite fields with different characteristics.

Application of Mirroring Lemma. We show that there is no statistical SNIR from binary erasure correlation or *oblivious transfer correlation* (OT) (see (6)) to binary symmetric correlation. These results do not follow from the spectral criterion, but can be based on the Mirroring Lemma. In this case, the source correlation C (BSC) has a certain symmetry ($\mathbf{\Psi}_C = \mathbf{\Phi}_C$) whereas the target correlation D (BEC and OT) have markedly different entries in $\mathbf{\Psi}_D$ and $\mathbf{\Phi}_D$; this, we show, makes it impossible for a spectral protocol to satisfy the Mirroring Lemma. Indeed, we provide a much more general implication of mirroring lemma for symmetric sources in Lemma 13.

We remark that our impossibility result rules out an error lower than a positive constant, no matter how many copies of BSC are used. In contrast, a quantitatively weaker result is implied by a known impossibility result for One-Way Secure Computation [14].

We remark that independently, [23] also considered these problems regarding SNIR between BSC and BEC correlations (using techniques tailored for these correlations). They obtain the above three results, with two caveats: their definition of a SNIR allowed only deterministic protocols, and required negligible security error. While the first caveat can be removed using our result in Lemma 7, the second one appears inherent to their techniques. We also remark that [23] also shows that BSC does not have a SNIR to BEC, using techniques similar to those in [14]; we have not obtained this result, as our approach relying on the mirroring lemma seems to require a tedious analysis for this example. This example gives a possible direction in which our toolkit could be expanded.

2.7 Future Directions

Our results and techniques suggest several exciting questions at the intersection of cryptography, linear-algebra and complexity of functions. We mention a few of these directions here.

1. As mentioned at the beginning, SNIR forms one part of a pair of questions about the feasibility of an (interactive) secure reduction from D to C. The question we do not address here is the (non-cryptographic) question regarding what correlations can be created as the views of two parties in an interaction. This is a purely "communication" problem, that fits in with the rich literature of communication complexity, which also studies the properties of communication protocols, albeit the goals are very different.

Apart from this broad direction, our results open up some concrete questions. Consider Alice sending a single bit to Bob, based (probabilistically) on her sample from the correlation C. The resulting view is described by the following correlation, where Q encodes Alice's communication strategy as a diagonal matrix (with Q_{xx} being the probability of sending 0 on receiving x):

$$\begin{bmatrix} QC & 0 \\ 0 & (I-Q)C \end{bmatrix}.$$

How is the spectrum of this new correlation related to that of C, over all possible choices of Q? If C corresponds to a (possibly noisy) string-OT, where Bob receives two strings (y_0, y_1) and Alice receives (b, y_b), if Alice sends b to Bob, then the maximal correlation greatly increases. However, if C is of the form $C_1^{\otimes t}$ it would appear that sending a single bit will have only limited effect on the spectrum. Can this be quantified?

2. How "complex" can the spectrum of a correlation be, in terms of the complexity of sampling from it, or computing the probabilities? In particular, if a correlation is the tensor power of a smaller correlation, all the values in the spectrum can be computed as monomials of a few variables.

3. The correlation operator $\widetilde{M}$ essentially captures all the information about a correlation M (other than the distribution of the common information). However, the spectrum of a correlation discards the orthogonal transformations $\mathbf{\Psi}_M$ and $\mathbf{\Phi}_M$ that are part of the singular value decomposition of the correlation operator $\widetilde{M}$. Can we obtain tighter criteria for SNIR based on them?

4. The correlation operator is a tool worthy of study on its own. We have not explored some natural mathematical questions that would arise in such a study.

- Which linear transformations correspond to valid correlation operators? In particular, given a valid correlation operator, can it be altered – say, by truncating the spectrum – to obtain the correlation operator of meaningfully "simpler" correlations? (Truncating the spectrum to retain only the top singular value yields the correlation operator corresponding to the product distribution with the same marginal.)
- The correlation operator is quite symmetric in its definition (e.g., $\widetilde{M^\intercal} = \widetilde{M}^\intercal$). While not as versatile as the correlation operator, asymmetric variants of it does capture certain interesting details of a correlation. For instance, one can define $\mathbf{\Delta}_{M^\intercal}^{-\alpha} M \mathbf{\Delta}_M^{-(1-\alpha)}$ for any $0 \leq \alpha \leq 1$. We leave it to future work to explore such variants.

5. Finally, there are information-theoretic problems on SNIR that we have not explored. For instance, as pursued in [23], one may explore the exact constant rate at which a SNIR between specific correlations is possible. Also, as pursued in [22], one may consider the question of decidability (or even, efficient decidability) of the existence of SNIR between such a pair of correlations.

3 Preliminaries

In this section, we set up the notation and make the necessary definitions and formally define the notion of non-interactive secure reduction.

Notation. Throughout the paper, we only consider finite sets. Finite sets are denoted as $\mathcal{X}, \mathcal{Y}$, and so on; a random variable over set $\mathcal{X}$ is denoted as X and a member of $\mathcal{X}$ is denoted as x. For convenience, we consider vectors with elements indexed by elements $x \in \mathcal{X}$ for a arbitrary set $\mathcal{X}$; hence it makes sense to define an $\mathcal{X}$ dimensional column vector. For an $\mathcal{X}$ dimensional column (or row) vector $\boldsymbol{v}$, the entry at the position x is denoted by $(\boldsymbol{v})_x$. Similarly, for sets $\mathcal{X}$ and $\mathcal{Y}$, consider an $\mathcal{X} \times \mathcal{Y}$ dimensional matrix H. The row of H indexed by x and the column indexed by y are denoted as vectors $(H)_{x,\cdot}$ and $(H)_{\cdot,y}$, respectively, and the element indexed by (x, y) is denoted as $(H)_{x,y}$. The transpose is denoted by $H^\intercal$. Finally, $|H|$ denotes the absolute value of H, *i.e.*, $(|H|)_{i,j} = |(H)_{i,j}|$, for all $i \in [m]$ and $j \in [n]$. We remove the parentheses whenever there is no scope for confusion and the vector/matrix itself is subscripted; *i.e.*, $(\boldsymbol{v})_x, (H)_{\cdot,x}$ and $(H)_{x,y}$ are simplified to $\boldsymbol{v}_x, H_{\cdot,x}$ and $H_{x,y}$, respectively.

For $n \in \mathbb{N}$, an n dimensional column vector with all elements being 1 (resp. 0) is denoted by $\mathbf{1}^n$ (resp. $\mathbf{0}^n$). For $i \in [n]$, $\boldsymbol{\xi}_i^n$ denotes the n dimensional unit vector

along the 'direction i'. That is, $(\boldsymbol{\xi}_i^n)_i = 1$ and $(\boldsymbol{\xi}_i^n)_j = 0$ for all $j \neq i$. We drop the superscript when there is no scope for confusion regarding the dimension of the vector. $n \times n$ dimensional identity matrix is denoted $I^{n\times n}$ and the 'zero matrix' (with all elements being 0) is denoted by $0^{n\times n}$.

We write $O_D(\epsilon)$ to denote an upper bound of the form $f(D) \cdot \epsilon$, for some fixed non-negative function f.

Definition 1 (Norms)**.** For a $m\times n$ dimensional matrix H, 1-norm of the matrix, denoted by $\|H\|$, is the sum of the absolute value of all elements in H, *i.e.,*

$$\|H\| = \sum_{(i,j)\in[m]\times[n]} |H_{i,j}| = (\mathbf{1}^m)^\intercal |H| \mathbf{1}^n.$$

The 2-norm of an n dimensional vector $\boldsymbol{v}$ is defined as $\|\boldsymbol{v}\|_2 = \left(\sum_{i\in[n]} \boldsymbol{v}_i^2\right)^{\frac{1}{2}}$. ◁

Definition 2. Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be vectors of dimensions m and n, respectively. Then,

$$\delta(\boldsymbol{u}, \boldsymbol{v}) = \hat{\boldsymbol{u}} - \hat{\boldsymbol{v}},$$

where $\hat{\boldsymbol{u}}$ and $\hat{\boldsymbol{v}}$ are the $\max(m, n)$ dimensional zero-paddings of vector $\boldsymbol{u}$ and $\boldsymbol{v}$, respectively. ◁

Definition 3. A matrix T with non-negative entries is said to be *stochastic* if $T\mathbf{1} = \mathbf{1}$. A stochastic matrix in which every entry is either 0 or 1 is called a *deterministic* stochastic matrix or simply a deterministic matrix. ◁

Definition 4. For an $m \times n$ dimensional matrix M, we define $\boldsymbol{\Delta}_M$ as the $n \times n$ diagonal matrix, such that

$$(\boldsymbol{\Delta}_M)_{i,j} = \begin{cases} (\mathbf{1}^\intercal M)_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$ ◁

Probability. Let X be a random variable distributed over a domain $\mathcal{X}$. Probability with which X takes on the value $x \in \mathcal{X}$ is denoted by $\mathrm{P}_X(x)$ or simply as $\mathrm{P}(x)$, when the distribution is apparent. Given two random variables X, X' over the same domain, we write $\mathrm{SD}(X, X')$ to denote the statistical difference (a.k.a. total variation distance) between the two, which is computed as

$$\sum_{x\in\mathcal{X}} |\mathrm{P}_X(x) - \mathrm{P}_{X'}(x)|.$$

Throughout this paper, we would be interested in correlations, which are joint distributions over a product of two sets. For finite sets $\mathcal{X}$ and $\mathcal{Y}$, a $\mathcal{X} \times \mathcal{Y}$ dimensional matrix H with non-negative entries is a joint distribution matrix or simply a distribution matrix if

$$\sum_x \sum_y H_{x,y} = 1.$$

We write $(X, Y) \sim H$ to imply that the random variables (X, Y) are distributed according to the distribution law H; *i.e.,* $\mathrm{P}_{XY}(x, y) = H_{x,y}$ for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$. In the sequel, we will always refer to a pair of random variables by its joint distribution matrix. We drop all-zero rows (and all-zero columns) from joint distribution matrices, i.e., elements in $\mathcal{X}$ (and $\mathcal{Y}$) which occur with zero probability are suppressed.

When we say Alice and Bob receive a correlation (X, Y), we mean Alice and Bob receive random variables X and Y respectively. The objective of non-interactive secure reductions is for Alice and Bob to *securely realize* a desired correlation among themselves using (potentially many copies) of the correlation at hand without communicating with each other.

Some Correlations of Interest. Below, we define some correlations that are extensively studied in information theory and cryptography which we use to illustrate the implications of our main results.

For $p \in [0, 1]$, the **Binary Symmetric Correlation** with crossover probability p over the alphabet $\{0, 1\} \times \{0, 1\}$, and the **symmetric Binary Erasure Correlation** with erasure probability p over the alphabet $\{0, 1\} \times \{0, 1, \perp\}$ are given by the following probability distribution matrices, respectively.

$$\mathsf{BSC}_p = \begin{bmatrix} \frac{1-p}{2} & \frac{p}{2} \\ \frac{p}{2} & \frac{1-p}{2} \end{bmatrix}. \qquad \mathsf{BEC}_p = \begin{bmatrix} \frac{1-p}{2} & \frac{p}{2} & 0 \\ 0 & \frac{p}{2} & \frac{1-p}{2} \end{bmatrix}.$$

The **OLE correlation** (for Oblivious Linear-function Evaluation) over a finite field (or ring) $\mathbb{F}$ is the correlation $\mathsf{OLE}_{\mathbb{F}}$ over the domain $\mathbb{F}^2 \times \mathbb{F}^2$ such that, for all $a, b, x, y \in \mathbb{F}$,

$$(\mathsf{OLE}_{\mathbb{F}})_{(a,x),(b,y)} = \begin{cases} \frac{1}{|\mathbb{F}|^3} & \text{if } a \cdot b = x + y, \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

OLE correlation over $\mathbb{F}_2$ is alternately called the **Oblivious Transfer correlation** or OT for short.

Tensor product. When G and H are $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{X}' \times \mathcal{Y}'$ dimensional matrices, *tensor (Kronecker) product* of G and H, denoted as $G \otimes H$ is an $(\mathcal{X} \times \mathcal{X}') \times (\mathcal{Y} \times \mathcal{Y}')$ dimensional matrix such that, for all $(x, x') \in \mathcal{X} \times \mathcal{X}'$ and $(y, y') \in \mathcal{Y} \times \mathcal{Y}'$,

$$(G \otimes H)_{(x,x'),(y,y')} = G_{x,y} \cdot H_{x',y'}.$$

$G \otimes H$ is essentially the product distribution of G and H, *i.e.,* independent draws from distributions G and H. We will use the following well known result about Kronecker product [19].

Claim 1. *For matrices G, H and $t \in \mathbb{N}$, $(GH)^{\otimes t} = G^{\otimes t} H^{\otimes t}$.*

4 Definitions

We define the notion of secure non-interactive reduction (SNIR) in this section. Non-interactive reduction of a distribution to another without the security guarantee called non-interactive reduction (NIR) is well studied. We formally define NIR and discuss some of its properties before defining SNIR.

Definition 5. Let C and D be correlations over $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{R} \times \mathcal{S}$, respectively. For any $\epsilon \geq 0$, an *ϵ-non-interactive reduction* (ϵ-NIR) from D to C is a pair of probabilistic algorithms $\mathfrak{A} : \mathcal{X} \to \mathcal{R}$ and $\mathfrak{B} : \mathcal{Y} \to \mathcal{S}$ such that, when $(X, Y) \sim C$ and $(R, S) \sim D$,

$$\mathrm{SD}\left((\mathfrak{A}(X), \mathfrak{B}(Y)), (R, S)\right) \leq \epsilon. \tag{7}$$

0-NIR is alternatively called a perfect NIR. ◁

Definition 6. Let C and D be correlations over $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{R} \times \mathcal{S}$, respectively. D is said to have a statistical NIR to C if for all $\epsilon > 0$, there exists a sufficiently large n for which, D has an ϵ-NIR to $C^{\otimes n}$. ◁

Definition 7. Let C and D be correlations over $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{R} \times \mathcal{S}$, respectively. For any $\epsilon \geq 0$, a *ϵ-secure non-interactive reduction* (ϵ-SNIR) from D to C is a pair of probabilistic algorithms $\mathfrak{A} : \mathcal{X} \to \mathcal{R}$ and $\mathfrak{B} : \mathcal{Y} \to \mathcal{S}$ such that, when $(X, Y) \sim C$ and $(R, S) \sim D$, in addition to condition (7), the following security conditions hold.

There exist a pair of probabilistic algorithms, $\mathsf{Sim}_A : \mathcal{R} \to \mathcal{X}$ and $\mathsf{Sim}_B : \mathcal{S} \to \mathcal{Y}$ such that,

$$\mathrm{SD}\left((X, \mathfrak{B}(Y)), (\mathsf{Sim}_A(R), S)\right) \leq \epsilon, \tag{8}$$

$$\mathrm{SD}\left((\mathfrak{A}(X), Y), (R, \mathsf{Sim}_B(S))\right) \leq \epsilon. \tag{9}$$

0-SNIR is alternatively called a perfect SNIR. ◁

Definition 8. Let C and D be distributions over $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{R} \times \mathcal{S}$, respectively. D is said to have a statistical SNIR to C if for all $\epsilon > 0$, there exists a sufficiently large n for which, D has an ϵ-SNIR to $C^{\otimes n}$. ◁

We begin with a linear algebraic characterization of secure non-interactive reductions (SNIR). The following theorem is proved in the full version [1].

Theorem 3. *Let $\epsilon \geq 0$, and let C and D be correlations over $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{R} \times \mathcal{S}$, respectively. D has a ϵ-SNIR to C if and only if there exist stochastic matrices A, B, U, and V of dimensions $\mathcal{X} \times \mathcal{R}$, $\mathcal{Y} \times \mathcal{S}$, $\mathcal{R} \times \mathcal{X}$, and $\mathcal{S} \times \mathcal{Y}$, respectively, such that*

$$A^{\intercal}\, C\, B = D + E \qquad A^{\intercal}\, C = D\, V + E_A \qquad C\, B = U^{\intercal}\, D + E_B,$$

where E, E_A, and E_B are matrices of dimensions $\mathcal{R} \times \mathcal{S}$, $\mathcal{R} \times \mathcal{Y}$, and $\mathcal{X} \times \mathcal{S}$, respectively, such that $\|E\|, \|E_A\|, \|E_B\| \leq \epsilon$.

Going forward, given distribution matrices C and D of dimensions $m_C \times n_C$ and $m_D \times n_D$, respectively, and stochastic matrices A and B of dimensions $m_C \times m_D$ and $n_C \times n_D$, respectively; we say that (A, B) is a ϵ-SNIR of D to C if the conditions in Theorem 3 are satisfied for some stochastic matrices U and V of dimensions $m_D \times m_C$ and $n_D \times n_C$, respectively.

5 Basic Properties of SNIR

In this section, we will establish some fundamental properties of SNIR that will be crucially used in arriving at the main results in the paper. In Lemma 5, we show that it is sufficient to study SNIR between correlations in which there are no redundant symbols (see Definition 9) in Alice's or Bob's side. Lemma 6 establishes a relation between SNIR protocols and their simulators (used for proving the security conditions) of a secure reduction. This relation is later used in Lemma 7 to show that protocols inducing SNIR are necessarily deterministic. This allows us to focus on SNIR with deterministic protocols in the sequel. Finally, the main result of this section characterizes the simulators (U and V) for a secure reduction in terms of the protocols (respectively, A and B).

We formally define redundant correlations and the core of a correlation.

Definition 9. A distribution matrix H over $\mathcal{X} \times \mathcal{Y}$ is said to be *redundant* if there exist distinct $x, x' \in \mathcal{X}$ and $\alpha \in \mathbb{R}_{\geq 0}$ such that $H_{x,\cdot} = \alpha \cdot H_{x',\cdot}$ or there exist $y, y' \in \mathcal{Y}$ and $\beta \in \mathbb{R}_{\geq 0}$ such that $H_{\cdot,y} = \beta \cdot H_{\cdot,y'}$. $\triangleleft$

By this definition, both the marginal distributions of a non-redundant distribution have full support since an all zero column (or row) is trivially a scalar multiple of any other column (or row).

Consider a (potentially redundant) distribution matrix H over $\mathcal{X} \times \mathcal{Y}$. Consider the partition $\mathcal{X}_1, \ldots, \mathcal{X}_m$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ of $\mathcal{X}$ and $\mathcal{Y}$, respectively, such that $x, x' \in \mathcal{X}_i$ (resp. $y, y' \in \mathcal{Y}_j$) if and only $H_{x,\cdot}$ and $H_{x',\cdot}$ (resp. $H_{\cdot,y}$ and $H_{\cdot,y'}$) are non-zero scalar multiples of each other. Additionally, we include all zero columns and rows in $\mathcal{X}_1$ and $\mathcal{Y}_1$, respectively. The distribution over such a partition induced by H is called the *core of the distribution* H. Formally, the non-redundant core of H, denoted by H_{core}, is the $m \times n$ dimensional matrix such that, for all $i \in [m]$ and $j \in [n]$,

$$(H_{\text{core}})_{i,j} = \sum_{x \in \mathcal{X}_i} \sum_{y \in \mathcal{Y}_j} H_{x,y}.$$

It is easy to verify that the core of any distribution is non-redundant and unique up to relabelling.

Lemma 5, Lemma 6 and Lemma 7 are formally proved in the full version [1].

Lemma 5. *Consider distributions C and D over $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{R} \times \mathcal{S}$, respectively. For any $\epsilon \geq 0$, D has an ϵ-SNIR to C if and only if D_{core} has an ϵ-SNIR to C_{core}.*

Lemma 6. *Let C be a $m_C \times n_C$ dimensional distribution matrix and D be a $m_D \times n_D$ dimensional non-redundant distribution matrix. For any $\epsilon \geq 0$, if stochastic matrices A, B, U, V are such that*

$$\|A^\intercal C B - D\| \leq \epsilon \qquad \|A^\intercal C - D V\| \leq \epsilon \qquad \|C B - U^\intercal D\| \leq \epsilon,$$

then $\|VB - I\| \leq O_D(\epsilon)$ and $\|UA - I\| \leq O_D(\epsilon)$.

Lemma 7. *Let C and D be non-redundant distribution matrices of dimensions $m_C \times n_C$ and $m_D \times n_D$, respectively. For any $\epsilon \geq 0$, if there exist stochastic matrices A, B, U and V such that*

$$\|A^\intercal CB - D\| \leq \epsilon \qquad \|A^\intercal C - DV\| \leq \epsilon \qquad \|CB - U^\intercal D\| \leq \epsilon,$$

then there exist deterministic stochastic matrices $\bar{A}, \bar{B}$ such that,

$$\|\bar{A}^\intercal C\bar{B} - D\| \leq O_D\big(\sqrt{\epsilon}\big) \quad \|\bar{A}^\intercal C - DV\| \leq O_D\big(\sqrt{\epsilon}\big) \quad \|C\bar{B} - U^\intercal D\| \leq O_D\big(\sqrt{\epsilon}\big)\,.$$

The following is the main result of this section that characterizes the simulators for a secure reduction in terms of the protocols.

Lemma 8. *Let C and D be non-redundant distribution matrices of dimensions $m_C \times n_C$ and $m_D \times n_D$, respectively. For any $\epsilon \geq 0$, if there exist deterministic stochastic matrices A and B, and stochastic matrices U and V such that*

$$\|A^\intercal CB - D\| \leq \epsilon \qquad \|A^\intercal C - DV\| \leq \epsilon \qquad \|CB - U^\intercal D\| \leq \epsilon,$$

then,

$$\|V - \boldsymbol{\Delta}_D^{-1} B^\intercal \boldsymbol{\Delta}_C\| \leq O_D(\epsilon) \qquad \|U - \boldsymbol{\Delta}_{D^\intercal}^{-1} A^\intercal \boldsymbol{\Delta}_{C^\intercal}\| \leq O_D(\epsilon)\,.$$

Proof: For $i \in [n_C]$, define $j_i^* \in [n_D]$ as the unique index (since B is deterministic) such that $B_{i,j_i^*} = 1$. Define row vectors $\boldsymbol{c} = \mathbf{1}^\intercal C$ and $\boldsymbol{d} = \mathbf{1}^\intercal D$ of dimensions n_C and n_D, respectively. It can be verified that for all $i \in [n_C]$, for all $j \neq j_i^*$, $\left(\boldsymbol{\Delta}_D^{-1} B^\intercal \boldsymbol{\Delta}_C\right)_{j,i} = 0$, and $\left(\boldsymbol{\Delta}_D^{-1} B^\intercal \boldsymbol{\Delta}_C\right)_{j_i^*,i} = \frac{\boldsymbol{c}_i}{\boldsymbol{d}_{j_i^*}}$. Hence, for each $i \in [n_C]$,

$$\sum_{j \in [n_D]} \left| \left(\boldsymbol{\Delta}_D^{-1} B^\intercal \boldsymbol{\Delta}_C\right)_{j,i} - V_{j,i} \right| = \left| \frac{\boldsymbol{c}_i}{\boldsymbol{d}_{j_i^*}} - V_{j_i^*,i} \right| + \sum_{j \neq j_i^*} V_{j,i}. \tag{10}$$

Let $A^\intercal C - DV = E$; by our assumption, $\|E\| \leq \epsilon$. Define n_C dimensional row vector $\boldsymbol{e} = \mathbf{1}^\intercal E$. Since A is a stochastic matrix, $\mathbf{1}^\intercal A^\intercal = \mathbf{1}^\intercal$. Consequently,

$$\boldsymbol{e} = \mathbf{1}^\intercal E = \mathbf{1}^\intercal A^\intercal C - \mathbf{1}^\intercal DV = \boldsymbol{c} - \sum_{j=1}^{n_D} \boldsymbol{d}_j V_{j,\cdot}$$

Hence, for all $i \in n_C$,

$$\boldsymbol{c}_i - \boldsymbol{d}_{j_i^*} V_{j_i^*,i} = \boldsymbol{e}_i + \sum_{j \neq j_i^*} \boldsymbol{d}_j V_{j,i}.$$

Since D is non-redundant all entries of $\boldsymbol{d}$ are non zero. Hence, for all $i \in [n_C]$,

$$\left| \frac{\boldsymbol{c}_i}{\boldsymbol{d}_{j_i^*}} - V_{j_i^*,i} \right| \leq \frac{1}{\min\limits_{j \in [n_D]} \boldsymbol{d}_j} \left(|\boldsymbol{e}_i| + \sum_{j \neq j_i^*} V_{j,i} \right).$$

Using this, along with (10), we get,

$$\begin{aligned}\|\boldsymbol{\Delta}_D^{-1} B^\intercal \boldsymbol{\Delta}_C - V\| &= \sum_{i\in[n_C]} \sum_{j\in[n_D]} \left| \left(\boldsymbol{\Delta}_D^{-1} B^\intercal \boldsymbol{\Delta}_C - V\right)_{j,i} \right| \\ &\leq \sum_{i\in[n_C]} \frac{|\boldsymbol{e}_i|}{\min_{j\in[n_D]} \boldsymbol{d}_j} + \sum_{j\neq j_i^*} V_{j,i} \left(1 + \frac{1}{\min_{j\in[n_D]} \boldsymbol{d}_j}\right) \\ &\leq \frac{1}{\min_{j\in[n_D]} \boldsymbol{d}_j} \cdot \left(\epsilon + \sum_{i\in[n_C]} \sum_{j\neq j_i^*} 2V_{j,i}\right).\end{aligned}$$

In the last inequality, we used $1 \leq \frac{1}{\min_i \boldsymbol{d}_i}$, and since $\|E\| \leq \epsilon$, $\sum_{i\in[n_D]} |\boldsymbol{e}_i| \leq \epsilon$. To bound the sum in the RHS, we proceed as follows. Since each row $i \in [n_C]$ of B has a unique non-zero entry (1 in the column j_i^*),

$$\sum_{j\in[n_D]} (VB)_{j,j} = \sum_{j\in[n_D]} \sum_{i\in[n_C]} V_{j,i} B_{i,j} = \sum_{i\in[n_C]} \sum_{j\in[n_D]} V_{j,i} \cdot B_{i,j} = \sum_{i\in[n_C]} V_{j_i^*,i}.$$

By Lemma 6, $\|VB - I\| = O_D(\epsilon)$. Furthermore, since V is stochastic matrix with n_D rows, all entries of V add up to n_D. Hence,

$$\begin{aligned}O_D(\epsilon) &\geq \sum_{j\in[n_D]} (I - VB)_{j,j} = n_D - \sum_{j\in[n_D]} (VB)_{j,j} = n_D - \sum_{i\in[n_C]} V_{j_i^*,i} \\ &= \sum_{i\in[n_C]} \sum_{j\in[n_D]} V_{j,i} - \sum_{i\in[n_C]} V_{j_i^*,i} = \sum_{i\in[n_C]} \sum_{j\neq j_i^*} V_{j,i}.\end{aligned}$$

This concludes the proof. □

6 Spectral Protocols

The properties of SNIR that were established in the previous section are used in this section to analyze the protocols in the so called *spectral domain*. We then show that these spectral protocols reveal more of the underlying structures in secure reductions that are not obvious when we analyze the protocols themselves. The properties of secure reductions revealed by analyzing the secure reductions in the spectral domain tend to be *robust*, in that, they easily extend to the statistical case. First, we make the following definitions.

Definition 10 (Spectrum of a Correlation)**.** For any distribution matrix M of dimension $m \times n$, define[8]

$$\widetilde{M} = \boldsymbol{\Delta}_{M^\intercal}^{-1/2} M \boldsymbol{\Delta}_M^{-1/2}.$$

[8] Recall that we use the convention that a distribution matrix does not have an all-0 row or column, and hence the diagonal matrices $\boldsymbol{\Delta}_{M^\intercal}$ and $\boldsymbol{\Delta}_M$ have strictly positive entries in their diagonals.

Further define $\mathbf{\Sigma}_M$, $\mathbf{\Psi}_M$ and $\mathbf{\Phi}_M$ to be given by a canonical singular value decomposition of M, so that $\mathbf{\Sigma}_M$ is an $m \times n$ dimensional non-negative diagonal matrix with the diagonal sorted in descending order, $\mathbf{\Psi}_M$ and $\mathbf{\Phi}_M$ are unitary matrices of dimensions $m \times m$ and $n \times n$, respectively, and

$$\widetilde{M} = \mathbf{\Psi}_M^{\intercal} \mathbf{\Sigma}_M \mathbf{\Phi}_M.$$

The multi-set of *non-zero* singular values of $\widetilde{M}$ is called the *spectrum of* M, and is denoted by $\mathbf{\Lambda}_M$. ◁

We now describe the spectrum of the correlations of interest in this paper.

Binary Symmetric Correlation. For $0 < p < \frac{1}{2}$, $\mathsf{BSC}_p = \begin{bmatrix} \frac{1-p}{2} & \frac{p}{2} \\ \frac{p}{2} & \frac{1-p}{2} \end{bmatrix}$

$$\mathbf{\Sigma}_{\mathsf{BSC}_p} = \begin{bmatrix} 1 & 0 \\ 0 & 1-2p \end{bmatrix} \qquad \mathbf{\Psi}_{\mathsf{BSC}_p} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} \end{bmatrix} \qquad \mathbf{\Phi}_{\mathsf{BSC}_p} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} \end{bmatrix}. \quad (11)$$

Binary Erasure Correlation. For $0 < p < 1$, when $q = 1-p$, $\mathsf{BEC}_p = \begin{bmatrix} \frac{q}{2} & \frac{p}{2} & 0 \\ 0 & \frac{p}{2} & \frac{q}{2} \end{bmatrix}$

$$\mathbf{\Sigma}_{\mathsf{BEC}_p} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \sqrt{q} & 0 \end{bmatrix} \quad \mathbf{\Psi}_{\mathsf{BEC}_p} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} \end{bmatrix} \quad \mathbf{\Phi}_{\mathsf{BEC}_p} = \begin{bmatrix} \sqrt{\frac{q}{2}} & \sqrt{p} & \sqrt{\frac{q}{2}} \\ \sqrt{\frac{1}{2}} & 0 & -\sqrt{\frac{1}{2}} \\ \sqrt{\frac{p}{2}} & -\sqrt{q} & \sqrt{\frac{p}{2}} \end{bmatrix}. \quad (12)$$

Oblivious Transfer Correlation $\mathsf{OT} = \frac{1}{8} \cdot \begin{bmatrix} 1\,0\,1\,0 \\ 1\,0\,0\,1 \\ 0\,1\,1\,0 \\ 0\,1\,0\,1 \end{bmatrix}$

$$\mathbf{\Sigma}_{\mathsf{OT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \mathbf{\Psi}_{\mathsf{OT}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{-1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{2} & \frac{-1}{2} & \frac{-1}{2} & \frac{1}{2} \end{bmatrix} \mathbf{\Phi}_{\mathsf{OT}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{-1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{-1}{2} \\ \frac{-1}{2} & \frac{1}{2} & \frac{-1}{2} & \frac{1}{2} \\ \frac{-1}{2} & \frac{-1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}. \quad (13)$$

In the full version [1], we will show that the spectrum of the OLE correlation over a finite field $\mathbb{F}$ consists of only the values 1 and $\frac{1}{\sqrt{|\mathbb{F}|}}$.

Definition 11 (Spectral Image of SNIR)**.** Given correlations $C \in \mathbb{R}^{m_C \times n_C}$ and $D \in \mathbb{R}^{m_D \times n_D}$, and a SNIR from D to C given by (A, B), where $A \in \mathbb{R}^{m_C \times m_D}$ and $B \in \mathbb{R}^{n_C \times n_D}$, we define its *spectral image* $(\widehat{A}, \widehat{B})$ (where $\widehat{A} \in \mathbb{R}^{m_C \times m_D}$ and $\widehat{B} \in \mathbb{R}^{n_C \times n_D}$) by

$$\widehat{A} = \mathbf{\Psi}_C \, \mathbf{\Delta}_{C^{\intercal}}^{1/2} \, A \, \mathbf{\Delta}_{D^{\intercal}}^{-1/2} \, \mathbf{\Psi}_D^{\intercal}, \qquad \widehat{B} = \mathbf{\Phi}_C \, \mathbf{\Delta}_C^{1/2} \, B \, \mathbf{\Delta}_D^{-1/2} \, \mathbf{\Phi}_D^{\intercal}. \qquad \triangleleft$$

Note that above, for brevity we have suppressed C and D in the notation for $\widehat{A}$ and $\widehat{B}$, as they will be evident from context. Before turning to our main results, below we summarize a few properties of the spectrum of a correlation (see the full version [1] for the proof).

Lemma 9. *Let M be a distribution matrix of dimension $m \times n$. Then,*

(i) Elements of $\mathbf{\Lambda}_M$ lie in the range $(0,1]$, and $\max(\mathbf{\Lambda}_M) = 1$. Furthermore, if M has no common information, then the second largest element of $\mathbf{\Lambda}_M$ is strictly less than 1.

(ii) For all $\ell \in \mathbb{N}$, $\mathbf{\Lambda}_{M^{\otimes \ell}} \subseteq \mathbf{\Lambda}_{M^{\otimes(\ell+1)}}$.

(iii) For all $\lambda \in (0,1)$, there exists $\beta > 0$ such that for all $\ell \in \mathbb{N}$ and for all $\sigma \in \mathbf{\Lambda}_{M^{\otimes \ell}}$, either $\lambda = \sigma$ or $|\lambda - \sigma| > \beta$.

Our goal in this section is to prove robust versions of the Spectral Criterion (Theorem 2) and the Mirroring Lemma (Lemma 3) as Theorem 4 and Theorem 5, respectively. Before proving those theorems, we state the following lemmas that are crucially used in the proofs of the theorems. The lemmas are formally proved in the full version [1].

The first lemma is the statistical equivalent of the results in Lemma 2 for perfect SNIR.

Lemma 10. *Suppose a non-redundant correlation $D \in \mathbb{R}^{m_D \times n_D}$ has a deterministic ϵ-SNIR (A,B) to a correlation $C \in \mathbb{R}^{m_C \times n_C}$, for $\epsilon \geq 0$. Then,*

(i). There exist matrices E_1, E_2 such that $\|E_1\| = O_D(\epsilon)$ and $\|E_2\| = O_D(\epsilon)$, and

$$\widehat{A}^\intercal \widehat{A} = I^{m_D \times m_D} + E_1 \qquad \widehat{B}^\intercal \widehat{B} = I^{n_D \times n_D} + E_2.$$

(ii). There exist matrices $\hat{E}, \hat{E}_A, \hat{E}_B$ such that

$$\widehat{A}^\intercal \mathbf{\Sigma}_C \widehat{B} = \mathbf{\Sigma}_D + \hat{E}, \quad \widehat{A}^\intercal \mathbf{\Sigma}_C = \mathbf{\Sigma}_D \widehat{B}^\intercal + \hat{E}_A, \quad \widehat{B}^\intercal \mathbf{\Sigma}_C^\intercal = \mathbf{\Sigma}_D^\intercal \widehat{A}^\intercal + \hat{E}_B,$$

where $\|\hat{E}\| = O_D(\epsilon)$, and for all $\theta \in \{0,1\}$,

$$\|\hat{E}_A (\mathbf{\Sigma}_C^\intercal \mathbf{\Sigma}_C)^\theta \mathbf{\Sigma}_C^\intercal \widehat{A}\| = O_D(\epsilon)\,, \|\hat{E}_A (\mathbf{\Sigma}_C^\intercal \mathbf{\Sigma}_C)^\theta \widehat{B}\| = O_D(\epsilon)\,,$$
$$\|\hat{E}_B (\mathbf{\Sigma}_C \mathbf{\Sigma}_C^\intercal)^\theta \mathbf{\Sigma}_C \widehat{B}\| = O_D(\epsilon)\,, \|\hat{E}_B (\mathbf{\Sigma}_C \mathbf{\Sigma}_C^\intercal)^\theta \widehat{A}\| = O_D(\epsilon)\,.$$

Next is a technical lemma that will be needed in both the proofs.

Lemma 11. *Suppose a non-redundant correlation $D \in \mathbb{R}^{m_D \times n_D}$ has a deterministic ϵ-SNIR (A,B) to a correlation $C \in \mathbb{R}^{m_C \times n_C}$ for $\epsilon \geq 0$. Then, for all $i \in [m_D]$,*

$$\left\| \left(\mathbf{\Sigma}_C \mathbf{\Sigma}_C^\intercal - (\mathbf{\Sigma}_D \mathbf{\Sigma}_D^\intercal)_{i,i} \cdot I \right) \widehat{A}_{\cdot,i} \right\|_2 = O_D\big(\sqrt{\epsilon}\big)\,.$$

Similarly, for $i \in [n_D]$,

$$\left\| \left(\mathbf{\Sigma}_C^\intercal \mathbf{\Sigma}_C - (\mathbf{\Sigma}_D^\intercal \mathbf{\Sigma}_D)_{i,i} \cdot I \right) \widehat{B}_{\cdot,i} \right\|_2 = O_D\big(\sqrt{\epsilon}\big)\,.$$

6.1 Spectral Criterion

Theorem 4. *A non-redundant correlation D has a statistically secure SNIR to C only if, there exists $\ell \in \mathbb{N}$ such that $\mathbf{\Lambda}_D \subseteq \mathbf{\Lambda}_{C^{\otimes \ell}}$.*

Proof: For all $\epsilon > 0$, there exist a large enough ℓ, and deterministic matrices A and B and stochastic matrices U and V such that,

$$\|A^\intercal C^{\otimes \ell} B - D\| \leq \epsilon, \qquad \|A^\intercal C^{\otimes \ell} - DV\| \leq \epsilon, \qquad \|C^{\otimes \ell} B - U^\intercal D\| \leq \epsilon. \quad (14)$$

If $\mathbf{\Lambda}_D \not\subseteq \mathbf{\Lambda}_{C^{\otimes t}}$ for all $t \in \mathbb{N}$, by Lemma 9 (ii), there exists $i \in [\min(m_D, n_D)]$ such that for all t, $(\mathbf{\Sigma}_D)_{i,i} \notin \mathbf{\Lambda}_{C^{\otimes t}}$. Then, by Lemma 9 (iii), there exists $\beta > 0$ such that for all $t \in \mathbb{N}$ and all $\lambda \in \mathbf{\Lambda}_{C^{\otimes t}}$, $|(\mathbf{\Sigma}_D)_{i,i} - \lambda| > \beta$. Hence, when $\boldsymbol{a} = \widehat{A}_{\cdot,i}$,

$$\boldsymbol{a}^\intercal \cdot \left(\mathbf{\Sigma}_C^{\otimes \ell} (\mathbf{\Sigma}_C^{\otimes \ell})^\intercal - (\mathbf{\Sigma}_D \mathbf{\Sigma}_D^\intercal)_{i,i} \cdot I\right)^2 \cdot \boldsymbol{a} \geq \beta^4 (\boldsymbol{a}^\intercal \cdot \boldsymbol{a}). \quad (15)$$

But, (14) and Lemma 11 imply that

$$\boldsymbol{a}^\intercal \cdot \left(\mathbf{\Sigma}_C^{\otimes \ell} (\mathbf{\Sigma}_C^{\otimes \ell})^\intercal - (\mathbf{\Sigma}_D \mathbf{\Sigma}_D^\intercal)_{i,i} \cdot I\right)^2 \cdot \boldsymbol{a} = O_D(\epsilon)\,. \quad (16)$$

By (i) in Lemma 10, $\boldsymbol{a}^\intercal \cdot \boldsymbol{a} = 1 - O_D(\epsilon)$. This along with (15) and (16) imply that $\beta^4 = O_D(\epsilon)$. However, this yields a contradiction (since $\beta > 0$ is a constant while ϵ can be arbitrarily small), proving the theorem. □

6.2 Mirroring Lemma

Theorem 5. *Suppose a non-redundant correlation $D \in \mathbb{R}^{m_D \times n_D}$ has a deterministic ϵ-SNIR (A, B) to a correlation $C \in \mathbb{R}^{m_C \times n_C}$ for $\epsilon \geq 0$. Then, for $i \in \min(m_D, n_D)$ such that $(\mathbf{\Sigma}_D)_{i,i} > 0$,*

$$\|\delta\left(\widehat{A}_{\cdot,i}, \widehat{B}_{\cdot,i}\right)\|_2 = \frac{O_D(\sqrt{\epsilon})}{\alpha_i^2},$$

where

$$\alpha_i = \min_{j:(\mathbf{\Sigma}_C)_{j,j} \neq (\mathbf{\Sigma}_D)_{i,i}} |(\mathbf{\Sigma}_C)_{j,j} - (\mathbf{\Sigma}_D)_{i,i}|.$$

Proof: By Lemma 10, we have matrix $\hat{E}_A$ such that

$$\widehat{A}^\intercal \mathbf{\Sigma}_C = \mathbf{\Sigma}_D \widehat{B}^\intercal + \hat{E}_A,$$

where $\|\hat{E}_A \mathbf{\Sigma}_C^\intercal \widehat{A}\| = O_D(\epsilon)$ and $\|\hat{E}_A \widehat{B}\| = O_D(\epsilon)$. Fix $i \in \min(m_D, n_D)$ such that $(\mathbf{\Sigma}_D)_{i,i} > 0$, and define $\lambda_i = (\mathbf{\Sigma}_D)_{i,i}$. Since $(\boldsymbol{\xi}_i)^\intercal \mathbf{\Sigma}_D = \lambda_i (\boldsymbol{\xi}_i)^\intercal$, denoting $\widehat{A}_{\cdot,i}$ and $\widehat{B}_{\cdot,i}$ by $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively,

$$(\boldsymbol{\xi}_i)^\intercal \widehat{A}^\intercal \mathbf{\Sigma}_C - (\boldsymbol{\xi}_i)^\intercal \mathbf{\Sigma}_D \widehat{B} = \boldsymbol{a}^\intercal \mathbf{\Sigma}_C - \lambda_i \boldsymbol{b}^\intercal = (\boldsymbol{\xi}_i)^\intercal \hat{E}_A. \quad (17)$$

Post-multiplying the above equation by the transpose of the LHS, we get,

$$(\boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - \lambda_i \boldsymbol{b})^\intercal \cdot (\boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - \lambda_i \boldsymbol{b}) = (\boldsymbol{\xi}_i)^\intercal \hat{E}_A \boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - (\boldsymbol{\xi}_i)^\intercal \hat{E}_A \lambda_i \boldsymbol{b}. \tag{18}$$

But,

$$\begin{aligned}(\boldsymbol{\xi}_i)^\intercal \hat{E}_A \boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - (\boldsymbol{\xi}_i)^\intercal \hat{E}_A \lambda_i \boldsymbol{b} &= (\boldsymbol{\xi}_i)^\intercal \hat{E}_A \boldsymbol{\Sigma}_C^\intercal \widehat{A} \boldsymbol{\xi}_i + (\boldsymbol{\xi}_i)^\intercal \hat{E}_A \widehat{B} \boldsymbol{\xi}_i \\ &= \left(\hat{E}_A \boldsymbol{\Sigma}_C^\intercal \widehat{A}\right)_{i,i} + \left(\hat{E}_A \widehat{B}\right)_{i,i} \leq \|\hat{E}_A \boldsymbol{\Sigma}_C^\intercal \widehat{A}\| + \|\hat{E}_A \widehat{B}\| = O_D(\epsilon)\,.\end{aligned}$$

The above bound implies that, (18) can be written as,

$$(\boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - \lambda_i \boldsymbol{b})^\intercal \cdot (\boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - \lambda_i \boldsymbol{b}) = O_D(\epsilon)\,. \tag{19}$$

Define the set $\mathcal{S} \subset [m_C]$ and the m_C dimensional vector $\boldsymbol{a}|_{\mathcal{S}}$ as follows.

$$\mathcal{S} = \{j \in [m_C] : (\boldsymbol{\Sigma}_C)_{j,j} = \lambda_i\}, \text{ and } (\boldsymbol{a}|_s)_j = \begin{cases} (\boldsymbol{a})_j & \text{if } j \in \mathcal{S}, \\ 0 & \text{otherwise.} \end{cases}$$

Let Σ be a $m_C \times n_C$ dimensional matrix such that,

$$(\Sigma)_{i,j} = \begin{cases} 1 \text{ if } i = j \in [\min(m_C, n_C)], \\ 0 \text{ otherwise.} \end{cases}$$

Define $\hat{\boldsymbol{a}}^\intercal = \boldsymbol{a}^\intercal \Sigma$ and $(\hat{\boldsymbol{a}}|_{\mathcal{S}})^\intercal = (\boldsymbol{a}|_{\mathcal{S}})^\intercal \Sigma$. We have $(\boldsymbol{a}|_{\mathcal{S}})^\intercal (\boldsymbol{\Sigma}_C - \lambda_i \Sigma) = 0$ since $(\boldsymbol{a}|_{\mathcal{S}})_j = 0$ if $(\boldsymbol{\Sigma}_C)_{j,j} \neq \lambda_i$. Hence,

$$\boldsymbol{a}^\intercal \boldsymbol{\Sigma}_C = \lambda_i \boldsymbol{a}^\intercal \Sigma + \boldsymbol{a}^\intercal (\boldsymbol{\Sigma}_C - \lambda_i \Sigma) = \lambda_i \hat{\boldsymbol{a}}^\intercal + (\boldsymbol{a}^\intercal - (\boldsymbol{a}|_{\mathcal{S}})^\intercal)(\boldsymbol{\Sigma}_C - \lambda_i \Sigma).$$

By Lemma 11, since $(\boldsymbol{a}|_{\mathcal{S}})^\intercal \left(\boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal - \lambda_i^2 I\right) = 0$,

$$\begin{aligned}(\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}})^\intercal \left(\boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal - \lambda_i^2 I\right) \left(\boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal - \lambda_i^2 I\right)^\intercal (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}}) &= \boldsymbol{a}^\intercal \left(\boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal - \lambda_i^2 I\right)^2 \boldsymbol{a} \\ &\overset{(a)}{=} O_D(\epsilon)\,.\end{aligned}$$

For all $j \notin \mathcal{S}$, $|(\boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal)_{j,j} - \lambda_i^2| \geq \alpha^4$. That is, for all j such that $(\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}})_j \neq 0$, $|(\boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal)_{j,j} - \lambda_i^2| \geq \alpha^4$. Since $\alpha > 0$ by definition,

$$\begin{aligned}O_D(\epsilon) = (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}})^\intercal \cdot (\boldsymbol{\Sigma}_C \boldsymbol{\Sigma}_C^\intercal - \lambda_i I)^2 \cdot (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}}) &\geq \alpha^4 \cdot (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}})^\intercal \cdot (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}}) \\ \Rightarrow (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}})^\intercal \cdot (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}}) = \frac{O_D(\epsilon)}{\alpha^4} &\Rightarrow \|\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}}\|_2 = \frac{O_D(\sqrt{\epsilon})}{\alpha^2}.\end{aligned}$$

$\boldsymbol{\Sigma}_C - \lambda_i \Sigma$ is a $m \times n$ dimensional matrix with zero as non-diagonal entries and the absolute value of each diagonal entry is at most 1. This follows from Lemma 9, which established that each diagonal entry is at most 1. Hence,

$$\|(\boldsymbol{\Sigma}_C - \lambda_i \Sigma)^\intercal (\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}})\|_2 \leq 2\|\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}}\|_2 = \frac{O_D(\sqrt{\epsilon})}{\alpha^2}.$$

For brevity, denote $(\boldsymbol{\Sigma}_C - \lambda_i \Sigma)^\intercal(\boldsymbol{a} - \boldsymbol{a}|_{\mathcal{S}})$ by $\boldsymbol{v}$. Then, by (19),

$$\begin{aligned} O_D(\epsilon) &= (\boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - \lambda_i \boldsymbol{b})^\intercal \cdot (\boldsymbol{\Sigma}_C^\intercal \boldsymbol{a} - \lambda_i \boldsymbol{b}) = (\lambda_i(\hat{\boldsymbol{a}} - \boldsymbol{b}) + \boldsymbol{v})^\intercal \cdot (\lambda_i(\hat{\boldsymbol{a}} - \boldsymbol{b}) + \boldsymbol{v}) \\ &\geq \lambda_i^2 (\hat{\boldsymbol{a}} - \boldsymbol{b})^\intercal \cdot (\hat{\boldsymbol{a}} - \boldsymbol{b}) + 2\lambda_i \boldsymbol{v}^\intercal \cdot (\hat{\boldsymbol{a}} - \boldsymbol{b}). \end{aligned}$$

Using Cauchy's inequality,

$$\lambda_i^2 (\hat{\boldsymbol{a}} - \boldsymbol{b})^\intercal \cdot (\hat{\boldsymbol{a}} - \boldsymbol{b}) \leq O_D(\epsilon) + 2\|\boldsymbol{v}\|_2 \cdot \|\hat{\boldsymbol{a}} - \boldsymbol{b}\|_2 \leq O_D(\epsilon) + \frac{O_D(\sqrt{\epsilon})}{\alpha^2} \cdot \|\hat{\boldsymbol{a}} - \boldsymbol{b}\|_2.$$

By definition of $\hat{\boldsymbol{a}}$, $\|\hat{\boldsymbol{a}}\|_2 = \|\boldsymbol{a}\|_2$. By the statement (i) of Lemma 10, $\boldsymbol{a}^\intercal \cdot \boldsymbol{a} = 1 - O_D(\epsilon)$ and $\boldsymbol{b}^\intercal \cdot \boldsymbol{b} = 1 - O_D(\epsilon)$. Hence $\|\hat{\boldsymbol{a}} - \boldsymbol{b}\|_2$ is upper bounded by 2. Using this bound,

$$(\hat{\boldsymbol{a}} - \boldsymbol{b})^\intercal \cdot (\hat{\boldsymbol{a}} - \boldsymbol{b}) \leq O_D(\epsilon) + \frac{O_D(\sqrt{\epsilon})}{\alpha^2}.$$

This concludes the proof. □

7 Common Information and SNIR

In this section, we study the role of common information in SNIR and establish that it does not aid in secure reductions. Intuition suggests that the common information available to both parties cannot be exploited to achieve SNIR. Specifically, having access to common randomness does not aid in SNIR; this is shown in the following theorem.

Theorem 6. *Let C_w be 1-bit common randomness correlation; i.e., $C_w = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$. If a non-redundant correlation D without common information has a statistical SNIR to $C_w \otimes C_0$ for a correlation C_0, then D also has a statistical SNIR to C_0.*

In the full version [1], we state and prove a robust variant of Lemma 4, which shows that if a correlation D devoid of common information has an ϵ-SNIR to C, then it has a SNIR to each of its component distribution with error that depends inversely on the probability of the component. But when the reduction use arbitrarily large number of copies of common random bits, this dependence makes the lemma ineffective in proving the theorem. However, the following lemma (also proven in the full version [1]) implies that if D has an ϵ-SNIR to $C^{\otimes \ell}$, then it has a $O_D(\epsilon)$-SNIR to $C_0^{\otimes \ell}$ proving the theorem.

Lemma 12. *Consider a non-redundant correlation $D \in \mathbb{R}^{m_D \times n_D}$ with zero common information. For correlations $C_1, \ldots, C_k$ and positive numbers $\alpha_1, \ldots, \alpha_k$ such that $\alpha_1 + \ldots + \alpha_k = 1$, let*

$$C = \begin{bmatrix} \alpha_1 C_1 & 0 & 0 & \ldots & 0 \\ 0 & \alpha_2 C_2 & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \alpha_k C_k \end{bmatrix}. \tag{20}$$

If D has an ϵ-SNIR to C, then for some $1 \leq i \leq k$, D has a $O_D(\epsilon)$-SNIR to C_i.

8 Applications

In this section, we demonstrate the use of the results above in studying SNIR between various interesting classes of correlations.

Our first result shows that no finite correlation is complete for SNIR even when Alice and Bob share common information.

Theorem 7. ***[Incompleteness]*** *For any correlation C, there exists a correlation D such that D does not have a statistical SNIR to C.*

Proof: We shall set D to be BSC_p for an appropriately chosen p.

For correlations $C_1, \ldots, C_k$ without common information and positive constants $\alpha_1, \ldots, \alpha_k$, suppose C can be represented as in (20). By Lemma 12, D has a ϵ-SNIR to $C^{\otimes \ell}$ only if it has a $O_D(\epsilon)$-SNIR to one of its component correlations; specifically, by Lemma 12, D has a $O_D(\epsilon)$-SNIR to $C_{a_1} \otimes C_{a_2} \otimes \ldots \otimes C_{a_k}$, for some $(a_1, \ldots, a_\ell) \in [k]^\ell$. This, trivially, implies that D has a $O_D(\epsilon)$-SNIR to $C_0^{\otimes \ell}$, where $C_0 = C_1 \otimes C_2 \otimes \ldots \otimes C_k$. Thus, D has a statistical SNIR to C_0 if it has a statistical SNIR to C. Choose $0 < p < \frac{1}{2}$ such that $1 - 2p > \max(\mathbf{\Lambda}_{C_0})$; by Lemma 9 (i), such a p exists since $C_1, \ldots, C_k$ have no common information. By (11), $\mathbf{\Lambda}_{\mathsf{BSC}_p} = \{1, 1-2p\}$; hence, by Theorem 4, BSC_p has no statistical SNIR to C_0 and hence to C; this proves the theorem. □

8.1 Applications of the Spectral Criterion

The spectral criterion in Theorem 4 can be used to analyze self-reductions of binary symmetric, binary erasure and OLE correlations.

The first couple of results *characterize* self-reductions of binary symmetric correlations and binary erasure correlations. Define the operator $*$ such that for $p, q \in [0, 1]$,

$$p * q = p(1-q) + q(1-p).$$

Naturally, for all $k \in \mathbb{N}$, we can extend this notion to define p^{*k} as $p * p * \ldots * p$ (k times). We prove the following two theorems in the full version [1].

Theorem 8. *For $p, q \in (0, \frac{1}{2})$, BSC_q has a statistical SNIR to BSC_p if and only if $q = p^{*\ell}$ for some $\ell \in \mathbb{N}$.*

The necessity of the condition is shown using the spectral criterion. As observed in (11), $\mathbf{\Lambda}_{\mathsf{BSC}_p} = \{1, (1-2p)\}$. Hence, by Theorem 4, BSC_q has a statistical SNIR to BSC_p only if $(1-2q) = (1-2p)^\ell$ for some $\ell \in \mathbb{N}$. Necessity of the condition now follows from the fact that if $(1-2q) = (1-2p)^\ell$ then $q = p^{*\ell}$. The protocol for SNIR of $\mathsf{BSC}_{p^{*\ell}}$ to $\mathsf{BSC}_p^{\otimes \ell}$ described in Section 2.6 shows the sufficiency of the condition.

Theorem 9. *For $p, q \in (0, 1)$, BEC_q has a statistical SNIR to BEC_p if and only if $1 - q = (1-p)^\ell$ for some $\ell \in \mathbb{N}$.*

The proof is similar to that of the previous theorem. As observed in (12), $\mathbf{\Lambda}_{\mathsf{BEC}_p} = \{1, \sqrt{1-p}\}$. Necessity of the condition follows from the fact that if $\sqrt{1-q} = \sqrt{1-q}^{\ell}$ then $q = p^{\ell}$. The protocol for SNIR of BEC_{p^ℓ} to $\mathsf{BEC}_p^{\otimes \ell}$ described in Section 2.6 shows the sufficiency of the condition.

Next, we show a necessary condition for self-reductions between OLE correlations over finite fields.

Theorem 10. $\mathsf{OLE}_{\mathbb{F}}$ *has a statistical SNIR to* $\mathsf{OLE}_{\mathbb{F}'}$ *only if both* $\mathbb{F}$ *and* $\mathbb{F}'$ *have the same characteristic.*

In the full version [1], we will show that the spectrum of the OLE correlation over a finite field $\mathbb{F}$ consists exclusively of the values 1 and $1/\sqrt{|\mathbb{F}|}$. Now, recall that $|\mathbb{F}| = p^k$ for some prime p and $k \in \mathbb{N}$, where p is the characteristic of the field. Hence, the only values in the spectrum of $\mathsf{OLE}_{\mathbb{F}}^{\otimes \ell}$, for a characteristic-$p$ field $\mathbb{F}$, are of the form $p^{t/2}$ for integers t. Hence, together with Theorem 4, this implies Theorem 10.

8.2 Applications of the Mirroring Lemma

In this section, we employ the mirroring lemma in Theorem 5 to argue impossibility of SNIR which cannot be inferred using only the spectral criterion. To this end, we derive a strong necessary condition for statistical SNIR to correlations with uniform marginals and positive semi-definite distribution matrices. A formal proof of the lemma is given in the full version [1].

Lemma 13. *Let* C *be a correlation with uniform marginals and* $\mathbf{\Psi}_C = \mathbf{\Phi}_C$. *A non-redundant distribution* D *over* $m_D \times n_D$ *has a statistical SNIR to* C *only if, there exist partitions* $S_1 \sqcup S_2 \sqcup \ldots \sqcup S_l = [m_D]$ *and* $T_1 \sqcup T_2 \sqcup \ldots \sqcup T_l = [n_D]$ *such that*

$$\sum_{i \in S_k} (D\mathbf{1})_i = \sum_{i \in T_k} (D^{\intercal}\mathbf{1})_i \,, \text{ for all } k \in [l],$$

and, for each $j \in [\min(m_D, n_D)]$ *such that* $(\mathbf{\Sigma}_D)_{j,j} > 0$,

$$\left(\mathbf{\Delta}_{D^{\intercal}}^{-1/2} \mathbf{\Psi}_D^{\intercal} \right)_{i,j} = \left(\mathbf{\Delta}_D^{-1/2} \mathbf{\Phi}_D^{\intercal} \right)_{i',j} \text{ for all } k \in [l], i \in S_k, i' \in T_k.$$

As a direct consequence of this result, BEC does not have statistical SNIR to BSC. In the case of perfect SNIR, this impossibility is trivial to see: it is impossible to arrange for Bob to output only 0 or $\perp$, whenever Alice outputs 0 (perfect correctness).

Theorem 11. *For all values* $p, q \in (0, 1)$, BEC_q *has no statistical SNIR to* BSC_p.

Proof: We observe that, for all $0 < p < 1$, BSC_p has uniform marginal and, as described in (11), $\mathbf{\Psi}_{\mathsf{BSC}_p} = \mathbf{\Phi}_{\mathsf{BSC}_p}$. Furthermore, for $0 < q < 1$, it can be verified

using (12) that

$$\left(\mathbf{\Delta}_{\mathsf{BEC}_q^\intercal}^{-1/2}\,\mathbf{\Psi}_{\mathsf{BEC}_q}^{\intercal}\right)_{\cdot,2}=\begin{bmatrix}1\\-1\end{bmatrix}\qquad\left(\mathbf{\Delta}_{\mathsf{BEC}_q}^{-1/2}\,\mathbf{\Phi}_{\mathsf{BEC}_q}^{\intercal}\right)_{\cdot,2}=\begin{bmatrix}\sqrt{\frac{1}{1-q}}\\0\\-\sqrt{\frac{1}{1-q}}\end{bmatrix}.$$

Impossibility follows directly from Lemma 13 as $(\mathbf{\Sigma}_D)_{2,2}=\sqrt{1-q}>0$ as given in (12). □

Theorem 12. OT *has no statistical SNIR to* BSC_p *for any* $0<p<\frac{1}{2}$.

Proof: Inspecting (13), $(\mathbf{\Sigma}_{\mathsf{OT}})_{2,2}=\frac{1}{\sqrt{2}}>0$ and

$$\left(\mathbf{\Delta}_{\mathsf{OT}^\intercal}^{-1/2}\,\mathbf{\Psi}_{\mathsf{OT}}^{\intercal}\right)_{\cdot,2}=\begin{bmatrix}0\\-\sqrt{2}\\\sqrt{2}\\0\end{bmatrix}\qquad\left(\mathbf{\Delta}_{\mathsf{OT}}^{-1/2}\,\mathbf{\Phi}_{\mathsf{OT}}^{\intercal}\right)_{\cdot,2}=\begin{bmatrix}-1\\1\\1\\-1\end{bmatrix}.$$

Impossibility follows directly from Lemma 13. □

References

1. Pratyush Agarwal, Varun Narayanan, Shreya Pathak, Manoj Prabhakaran, Vinod M. Prabhakaran, and Mohammad Ali Rehan. Secure non-interactive reduction and spectral analysis of correlations. Cryptology ePrint Archive, 2022.
2. Shashank Agrawal and Manoj Prabhakaran. On fair exchange, fair coins and fair sampling. In *CRYPTO*, 2013.
3. Rudolf Ahlswede and Peter Gacs. Spreading of sets in product spaces and hypercontraction of the markov operator. *The Annals of Probability*, 4(6):925–939, 1976.
4. Venkat Anantharam, Amin Aminzadeh Gohari, Sudeep Kamath, and Chandra Nair. On maximal correlation, hypercontractivity, and the data processing inequality studied by erkip and cover. *CoRR*, abs/1304.6133, 2013.
5. Salman Beigi and Amin Gohari. On the duality of additivity and tensorization. In *ISIT*, pages 2381–2385. IEEE, 2015.
6. Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *TCC*, pages 317–342, 2014.
7. Amos Beimel and Tal Malkin. A quantitative approach to reductions in secure computation. In *TCC*, pages 238–257, 2004.
8. C. Borell. Positivity improving operators and hypercontractivity. *Mathematische Zeitschrift*, 180:225–234, 1982.
9. Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators: Silent ot extension and more. In *CRYPTO*, pages 489–518. Springer, 2019.
10. Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators from ring-lpn. In *CRYPTO*, pages 387–416. Springer, 2020.

11. F. R. K. Chung. *Spectral Graph Theory*. American Mathematical Society, 1997.
12. Anindya De, Elchanan Mossel, and Joe Neeman. Non interactive simulation of correlated distributions is decidable. In *SODA 2018*, pages 2728–2746. SIAM, 2018.
13. P. Gács and J. Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149–162, 1973.
14. Sanjam Garg, Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with one-way communication. In *CRYPTO 2015*, pages 191–208, 2015.
15. Badih Ghazi, Pritish Kamath, and Madhu Sudan. Decidability of non-interactive simulation of joint distributions. In *FOCS*, pages 545–554. IEEE Computer Society, 2016.
16. Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play ANY mental game. In *STOC*, pages 218–229, 1987. See [**?**, Chap. 7] for more details.
17. Oded Goldreich and Ronen Vainish. How to solve any protocol problem - an efficiency improvement. In *CRYPTO*, pages 73–86, 1987.
18. H. O. Hirschfeld and J. Wishart. A Connection between Correlation and Contingency. *Proceedings of the Cambridge Philosophical Society*, 31(4):520, January 1935.
19. Roger A. Horn and Charles R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, 1991.
20. Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In *CRYPTO*, pages 572–591, 2008.
21. Sudeep Kamath and Venkat Anantharam. On non-interactive simulation of joint distributions. *IEEE Trans. Inf. Theory*, 62(6):3419–3435, 2016.
22. Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Decidability of secure non-interactive simulation of doubly symmetric binary source. Cryptology ePrint Archive, Report 2021/190, 2021. https://eprint.iacr.org/2021/190.
23. Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Secure non-interactive simulation: Feasibility & rate. In *CRYPTO*, 2022. To appear.
24. Joe Kilian. Founding cryptography on oblivious transfer. In *STOC*, pages 20–31, 1988.
25. Daniel Kraschewski, Hemanta Maji, Manoj Prabhakaran, and Amit Sahai. A full characterization of completeness for two-party randomized function evaluation. In *EUROCRYPT*, 2014.
26. Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. *Complexity of Multi-Party Computation Functionalities*, volume 10 of *Cryptology and Information Security Series*, pages 249 – 283. IOS Press, Amsterdam, 2013.
27. Varun Narayanan, Manoj Prabhakaran, and Vinod M. Prabhakaran. Zero-communication reductions. In *TCC*, volume 12552, pages 274–304. Springer, 2020.
28. A. Rènyi. On measures of dependence. *Acta Mathematica Hungarica*, 10(3-4), 1959.
29. Madhu Sudan, Himanshu Tyagi, and Shun Watanabe. Communication for generating correlation: A unifying survey. *IEEE Trans. Inf. Theory*, 66(1):5–37, 2020.
30. H. S. Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, 1975.
31. A. D. Wyner. The common information of two dependent random variables. *IEEE Transactions on Information Theory*, 21(2):163–179, 1975.