Spectral Non-Interactive Reduction

and

Spectral Analysis of Correlations

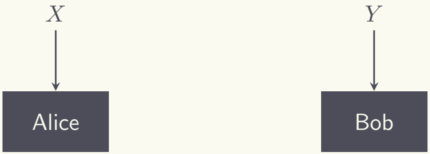
Pratyush Agarwal[1] Varun Narayanan [2] Shreya Pathak[1] Manoj Prabhakaran[1]
Vinod M. Prabhakaran[3] Mohammad Ali Rehan[1]

[1] Indian Institute of Technology Bombay, India

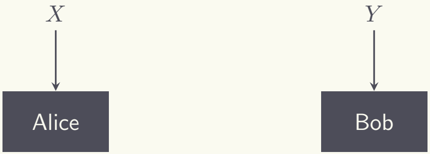
[2] Technion, Israel

[3] Tata Institute of Fundamental Research, India

Eurocrypt 2022

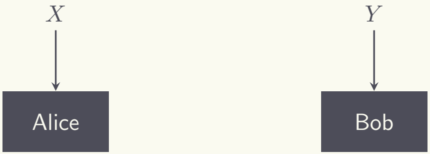


X
Y
Alice
Bob



$$\begin{pmatrix} C_{1,1} & \cdots & C_{1,y} & \cdots & C_{1,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{x,1} & \cdots & \boxed{C_{x,y}} & \cdots & C_{x,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{|\mathcal{X}|,1} & \cdots & C_{|\mathcal{X}|,y} & \cdots & C_{|\mathcal{X}|,|\mathcal{Y}|} \end{pmatrix}$$

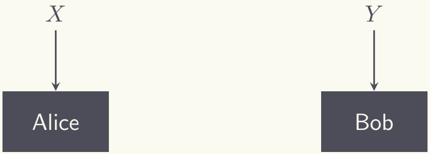
C is distribution over $\mathcal{X} \times \mathcal{Y}$



$$\begin{pmatrix} C_{1,1} & \cdots & C_{1,y} & \cdots & C_{1,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{x,1} & \cdots & \boxed{C_{x,y}} & \cdots & C_{x,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{|\mathcal{X}|,1} & \cdots & C_{|\mathcal{X}|,y} & \cdots & C_{|\mathcal{X}|,|\mathcal{Y}|} \end{pmatrix}$$

$\mathsf{Pr}[X = x, Y = y]$

C is distribution over $\mathcal{X} \times \mathcal{Y}$

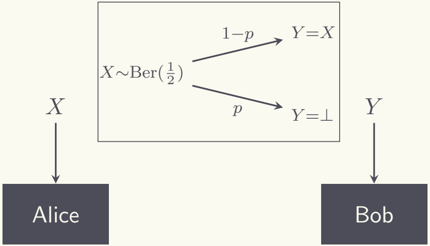


$$\begin{pmatrix} C_{1,1} & \cdots & C_{1,y} & \cdots & C_{1,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{x,1} & \cdots & \boxed{C_{x,y}} & \cdots & C_{x,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{|\mathcal{X}|,1} & \cdots & C_{|\mathcal{X}|,y} & \cdots & C_{|\mathcal{X}|,|\mathcal{Y}|} \end{pmatrix}$$

C is distribution over $\mathcal{X} \times \mathcal{Y}$

$$\mathrm{BEC}(p) = \begin{array}{cc} \begin{pmatrix} \frac{1-p}{2} & \frac{p}{2} & 0 \\ 0 & \frac{p}{2} & \frac{1-p}{2} \end{pmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \\ \begin{array}{ccc} 0 & \perp & 1 \end{array} & \end{array}$$

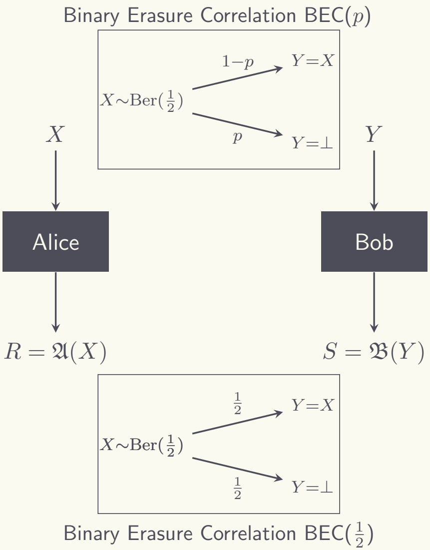
Binary Erasure Correlation BEC(p)

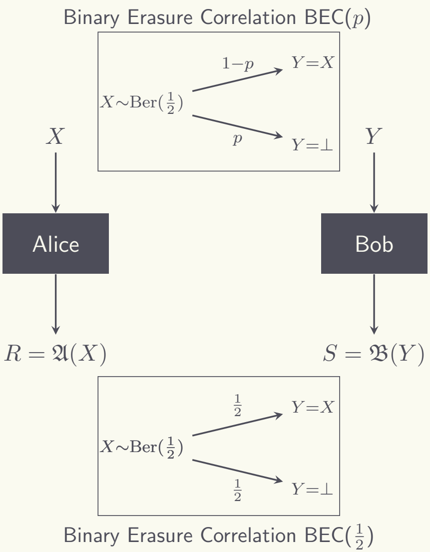


$$\begin{pmatrix} C_{1,1} & \cdots & C_{1,y} & \cdots & C_{1,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{x,1} & \cdots & \boxed{C_{x,y}} & \cdots & C_{x,|\mathcal{Y}|} \\ \vdots & & \vdots & & \vdots \\ C_{|\mathcal{X}|,1} & \cdots & C_{|\mathcal{X}|,y} & \cdots & C_{|\mathcal{X}|,|\mathcal{Y}|} \end{pmatrix}$$

C is distribution over $\mathcal{X} \times \mathcal{Y}$

$$\mathrm{BEC}(p) = \begin{array}{cc} \begin{pmatrix} \frac{1-p}{2} & \frac{p}{2} & 0 \\ 0 & \frac{p}{2} & \frac{1-p}{2} \end{pmatrix} & \begin{array}{c} 0 \\ 1 \end{array} \\ \begin{array}{ccc} 0 & \perp & 1 \end{array} & \end{array}$$

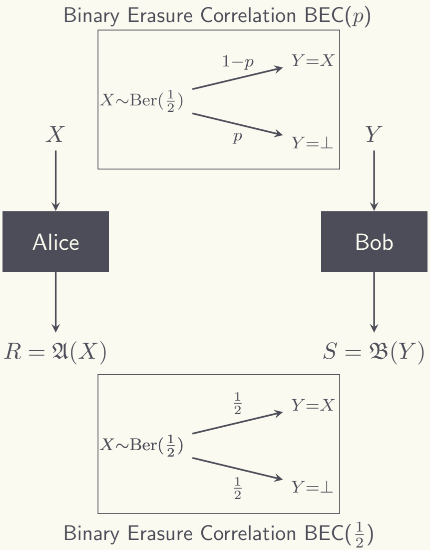

Binary Erasure Correlation BEC(p)
$1-p$
$Y=X$
$X \sim \mathrm{Ber}(\frac{1}{2})$
p
$Y=\perp$
X
Y
Alice
Bob
$R = \mathfrak{A}(X)$
$S = \mathfrak{B}(Y)$
$\frac{1}{2}$
$Y=X$
$X \sim \mathrm{Ber}(\frac{1}{2})$
$\frac{1}{2}$
$Y=\perp$
Binary Erasure Correlation BEC($\frac{1}{2}$)



Attempt 1 (for $p < \frac{1}{2}$)

1. Alice outputs X
2. Bob outputs Y w.p. $\frac{1}{2(1-p)}$; otherwise $\perp$

Correct but **not secure**



Attempt 1 (for $p < \frac{1}{2}$)

1. Alice outputs X
2. Bob outputs Y w.p. $\frac{1}{2(1-p)}$; otherwise $\perp$

Correct but **not secure**

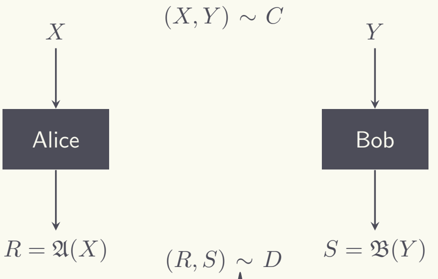
Attempt 2 (for $p = 1 - \frac{1}{\sqrt{2}}$)

Use 2 copies $(X_1, Y_1), (X_2, Y_2) \sim \mathrm{BEC}(p)$

1. Alice outputs $X_1 \oplus X_2$
2. Bob outputs $Y_1 \oplus Y_2$ if $Y_1, Y_2 \in \{0, 1\}$; otherwise $\perp$

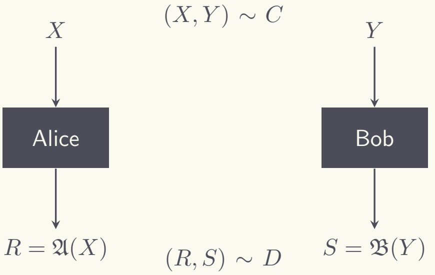
Correct and **secure**

Secure Non-Interactive Reduction (SNIR)



Non-Interactive Simulation (NIS)

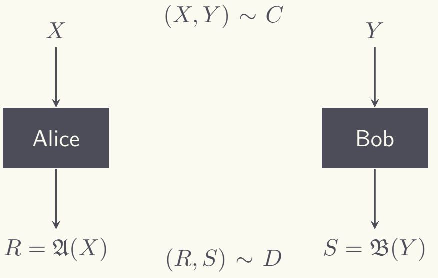
Secure Non-Interactive Reduction (SNIR)



$(\mathfrak{A}, \mathfrak{B})$ is an SNIR of D to C if

- $(R, S) \sim D$
- R indep. of Y conditioned on S
- S indep. of X conditioned on R

Secure Non-Interactive Reduction (SNIR)



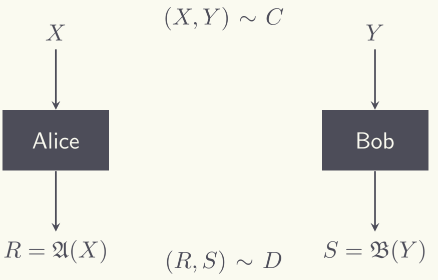
($\mathfrak{A}$,$\mathfrak{B}$) is an SNIR of D to C if

- $(R, S) \sim D$
- R indep. of Y conditioned on S
- S indep. of X conditioned on R

Fundamental question:

When can D have an SNIR to C?

Secure Non-Interactive Reduction (SNIR)



$(\mathfrak{A}, \mathfrak{B})$ is an SNIR of D to C if

- $(R, S) \sim D$
- R indep. of Y conditioned on S
- S indep. of X conditioned on R

Fundamental question:

When can D have an SNIR to C?

In this work

- A **spectral analysis toolkit** for (statistical) SNIR
- Exact characterizations for interesting classes of correlations

Why Study SNIR?

- Correlations are fundamental in information-theoretic cryptography
- SNIR is the most basic cryptographic question about correlations

Why Study SNIR?

- Correlations are fundamental in information-theoretic cryptography
- SNIR is the most basic cryptographic question about correlations

- Non-interactive variant of **secure computation**
  - Lowerbounds for secure computation is a deep complexity theoretic question
  - SNIR captures all the security aspects of secure computation of correlations. The latter has the form
    - Interaction phase (no security requirements)
    - **SNIR phase**

Why Study SNIR?

- Correlations are fundamental in information-theoretic cryptography
- SNIR is the most basic cryptographic question about correlations

- Non-interactive variant of **secure computation**
  - Lowerbounds for secure computation is a deep complexity theoretic question
  - SNIR captures all the security aspects of secure computation of correlations. The latter has the form
    - Interaction phase (no security requirements)
    - **SNIR phase**

- Secure variant of **(non-secure) non-interactive correlation simulation (NIS)**

Why Study SNIR?

- Correlations are fundamental in information-theoretic cryptography
- SNIR is the most basic cryptographic question about correlations

- Non-interactive variant of **secure computation**
  - Lowerbounds for secure computation is a deep complexity theoretic question
  - SNIR captures all the security aspects of secure computation of correlations. The latter has the form
    - Interaction phase (no security requirements)
    - **SNIR phase**

- Secure variant of **(non-secure) non-interactive correlation simulation (NIS)**

- Information theoretic variant of **pseudo-random correlation generators**

Our Results

Toolkit

When does D have a **statistical** SNIR $(\mathfrak{A},\mathfrak{B})$ to C?

- Enough to consider correlations without redundant symbols
- SNIR must be essentially **deterministic**
- **Spectrum** of $D \subseteq$ spectrum of C
- In the **spectral domain** $\mathfrak{A}$ and $\mathfrak{B}$ mirror each other
- Common information in C is only trivially useful

Our Results

Toolkit

When does D have a **statistical** SNIR $(\mathfrak{A},\mathfrak{B})$ to C?

- Enough to consider correlations without redundant symbols
- SNIR must be essentially **deterministic**
- **Spectrum** of $D \subseteq$ spectrum of C
- In the **spectral domain** $\mathfrak{A}$ and $\mathfrak{B}$ mirror each other
- Common information in C is only trivially useful

Applications

Exact characterizations of **statistical** SNIR for interesting classes of correlations

Our Results

Toolkit

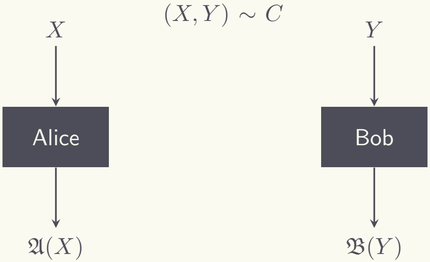
When does D have a **statistical** SNIR ($\mathfrak{A}$,$\mathfrak{B}$) to C?

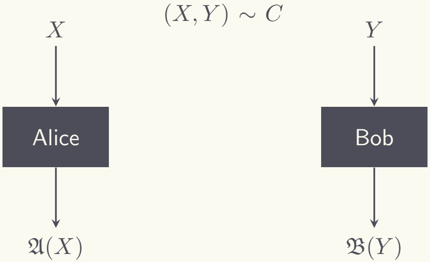
- Enough to consider correlations without redundant symbols
- SNIR must be essentially **deterministic**
- **Spectrum** of $D \subseteq$ spectrum of C
- In the **spectral domain** $\mathfrak{A}$ and $\mathfrak{B}$ mirror each other
- Common information in C is only trivially useful

BEC/BSC results also obtained by KMN22

Applications

Exact characterizations of **statistical** SNIR for interesting classes of correlations


$(X, Y) \sim C$
X
Alice
$\mathfrak{A}(X)$
Y
Bob
$\mathfrak{B}(Y)$



$(\mathfrak{A},\mathfrak{B})$ ϵ-SNIR of D to C iff, for $(R, S) \sim D$,

Correctness:

$$(\mathfrak{A}(X), \mathfrak{B}(Y)) \overset{\epsilon}{\approx} (R, S)$$

Security against Alice: $\exists$ simulator Sim_A:

$$(X, \mathfrak{B}(Y)) \overset{\epsilon}{\approx} (\mathsf{Sim}_A(R), S)$$

Security against Bob: $\exists$ simulator Sim_B:

$$(\mathfrak{A}(X), Y) \overset{\epsilon}{\approx} (R, \mathsf{Sim}_B(S))$$

(A,B) ϵ-SNIR of D to C iff:

Correctness:

$$A^\intercal C B \overset{\epsilon}{\approx} D$$

Security against Alice: $\exists U$:

$$CB \overset{\epsilon}{\approx} U^\intercal D$$

Security against Bob: $\exists V$:

$$A^\intercal C \overset{\epsilon}{\approx} DV$$

$(\mathfrak{A},\mathfrak{B})$ ϵ-SNIR of D to C iff, for $(R,S) \sim D$,

Correctness:

$$(\mathfrak{A}(X),\mathfrak{B}(Y)) \overset{\epsilon}{\approx} (R,S)$$

Security against Alice: $\exists$ simulator Sim_A:

$$(X,\mathfrak{B}(Y)) \overset{\epsilon}{\approx} (\mathsf{Sim}_A(R),S)$$

Security against Bob: $\exists$ simulator Sim_B:

$$(\mathfrak{A}(X),Y) \overset{\epsilon}{\approx} (R,\mathsf{Sim}_B(S))$$

(A,B) ϵ-SNIR of D to C iff:

Correctness:

$$A^\intercal C B \overset{\epsilon}{\approx} D$$

Security against Alice: $\exists U$:

$$CB \overset{\epsilon}{\approx} U^\intercal D$$

Security against Bob: $\exists V$:

$$A^\intercal C \overset{\epsilon}{\approx} DV$$

$$A[x,r] = \mathsf{Pr}_{\mathfrak{A}}[R = r | X = x]$$
$$U[r,x] = \mathsf{Pr}_{\mathsf{Sim}_A}[X = x | R = r]$$

$(\mathfrak{A},\mathfrak{B})$ ϵ-SNIR of D to C iff, for $(R,S) \sim D$,

Correctness:

$$(\mathfrak{A}(X), \mathfrak{B}(Y)) \overset{\epsilon}{\approx} (R,S)$$

Security against Alice: $\exists$ simulator Sim_A:

$$(X, \mathfrak{B}(Y)) \overset{\epsilon}{\approx} (\mathsf{Sim}_A(R), S)$$

Security against Bob: $\exists$ simulator Sim_B:

$$(\mathfrak{A}(X), Y) \overset{\epsilon}{\approx} (R, \mathsf{Sim}_B(S))$$

$$B[y,s] = \mathsf{Pr}_{\mathfrak{B}}[S = s | Y = y]$$
$$V[y,s] = \mathsf{Pr}_{\mathsf{Sim}_B}[Y = y | S = s]$$

(A, B) ϵ-SNIR of D to C iff:

Correctness:

$$A^{\intercal} C B \overset{\epsilon}{\approx} D$$

Security against Alice: $\exists U$:

$$C B \overset{\epsilon}{\approx} U^{\intercal} D$$

Security against Bob: $\exists V$:

$$A^{\intercal} C \overset{\epsilon}{\approx} D V$$

$(\mathfrak{A}, \mathfrak{B})$ ϵ-SNIR of D to C iff, for $(R, S) \sim D$,

Correctness:

$$(\mathfrak{A}(X), \mathfrak{B}(Y)) \overset{\epsilon}{\approx} (R, S)$$

Security against Alice: $\exists$ simulator Sim_A:

$$(X, \mathfrak{B}(Y)) \overset{\epsilon}{\approx} (\mathsf{Sim}_A(R), S)$$

Security against Bob: $\exists$ simulator Sim_B:

$$(\mathfrak{A}(X), Y) \overset{\epsilon}{\approx} (R, \mathsf{Sim}_B(S))$$

SNIR is Deterministic

An ϵ-SNIR of a non-redundant D to C can be converted into a **deterministic** $O_D(\sqrt{\epsilon})$-SNIR (A, B) with $U = \Delta_{D^{\intercal}}^{-1} A^{\intercal} \Delta_{C^{\intercal}}$ and $V = \Delta_D^{-1} B^{\intercal} \Delta_C$.

Spectral analysis

simple case: perfect security, square matrices, uniform marginals

Suppose $\Delta_C = \Delta_{C^\intercal} = \frac{1}{m} I_{m\times m}$ and $\Delta_D = \Delta_{D^\intercal} = \frac{1}{n} I_{n\times n}$

$$
\begin{aligned}
A^\intercal C C^\intercal &= D V C^\intercal && \because A^\intercal C = DV \\
&= \frac{n}{m} D B^\intercal C^\intercal && \text{where } V = \Delta_D^{-1} B^\intercal \Delta_C = \frac{n}{m} B^\intercal \\
&= \frac{n}{m} D D^\intercal U && \because U^\intercal D = CB \\
&= D D^\intercal A^\intercal && \text{where } U = \Delta_{D^\intercal}^{-1} A^\intercal \Delta_{C^\intercal} = \frac{n}{m} A^\intercal
\end{aligned}
$$

If $\boldsymbol{v}^\intercal$ is an eigenvector corresponding to eigenvalue λ of $DD^\intercal$; i.e., $\boldsymbol{v}^\intercal D D^\intercal = \lambda \boldsymbol{v}^\intercal$,

$$
\boldsymbol{v}^\intercal A^\intercal C C^\intercal = \boldsymbol{v}^\intercal D D^\intercal A^\intercal = \lambda \boldsymbol{v}^\intercal A^\intercal,
$$

we get theorem

$$
\{ \text{ eigenvalues of } D^\intercal D \} \subseteq \{ \text{ eigenvalues of } C^\intercal C \}
$$

Spectrum Containment (simple case)

$\Delta_C = \Delta_{C^\intercal} = \frac{1}{m} I_{m \times m}$, $\Delta_D = \Delta_{D^\intercal} = \frac{1}{n} I_{n \times n} \implies D$ has a SNIR to C **only if**

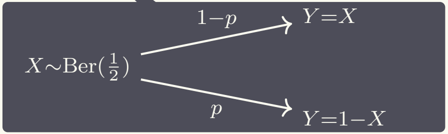
$$\{ \text{ eigenvalues of } D^\intercal D \ \} \subseteq \{ \text{ eigenvalues of } C^\intercal C \ \}$$

Spectrum Containment (simple case)

$\Delta_C = \Delta_{C^\intercal} = \frac{1}{m} I_{m\times m}$, $\Delta_D = \Delta_{D^\intercal} = \frac{1}{n} I_{n\times n} \implies$ D has a SNIR to C **only if**

$$\{ \text{ eigenvalues of } D^\intercal D \ \} \subseteq \{ \text{ eigenvalues of } C^\intercal C \ \}$$

For $D = \mathrm{BSC}(p)$, eigenvalues of $D^\intercal D$ are $\{1, 1-2p\}$



Spectrum Containment (simple case)

$\Delta_C = \Delta_{C^\intercal} = \frac{1}{m} I_{m\times m}$, $\Delta_D = \Delta_{D^\intercal} = \frac{1}{n} I_{n\times n} \implies D$ has a SNIR to C **only if**

$$\{ \text{ eigenvalues of } D^\intercal D \} \subseteq \{ \text{ eigenvalues of } C^\intercal C \}$$

For $D = \mathrm{BSC}(p)$, eigenvalues of $D^\intercal D$ are $\{1, 1-2p\}$
For $C = \mathrm{BSC}(q)^{\otimes \ell}$, eigenvalues of $C^\intercal C$ are $\{(1-2q)^k : 0 \le k \le \ell\}$

Spectrum Containment (simple case)

$\Delta_C = \Delta_{C^\intercal} = \frac{1}{m} I_{m\times m}$, $\Delta_D = \Delta_{D^\intercal} = \frac{1}{n} I_{n\times n} \implies D$ has a SNIR to C **only if**

$$\{\text{ eigenvalues of } D^\intercal D \ \} \subseteq \{ \text{ eigenvalues of } C^\intercal C \ \}$$

For $D = \mathrm{BSC}(p)$, eigenvalues of $D^\intercal D$ are $\{1, 1-2p\}$
For $C = \mathrm{BSC}(q)^{\otimes \ell}$, eigenvalues of $C^\intercal C$ are $\{(1-2q)^k : 0 \le k \le \ell\}$

Application

$\mathrm{BSC}(p)$ has a SNIR to $\mathrm{BSC}(q)^{\otimes \ell}$ **if and only if**, $\exists k \le \ell$, $1-2p = (1-2q)^k$, or equivalently, $p = q * \ldots * q$ (k times), where $q * q' = q(1-q') + q'(1-q)$.

<u>Construction:</u>

When $(X^k, Y^k) \sim C^{\otimes k}$: Alice outputs $\bigoplus_{i=1}^{k} X_i$ and Bob outputs $\bigoplus_{i=1}^{k} Y_i$

Correlation Operator

A linear operator that transforms the distribution for one party (appropriately normalized) to that for the other party, conditioned on the former.

$$\widetilde{C} = \Delta_{C^\intercal}^{-1/2} C \Delta_C^{1/2}.$$

Correlation Operator

A linear operator that transforms the distribution for one party (appropriately normalized) to that for the other party, conditioned on the former.

$$\widetilde{C} = \Delta_{C^\intercal}^{-1/2} C \Delta_C^{1/2}.$$

Can use **Singular Value Decomposition** (SVD) to analyze a linear operator.

SVD views a linear operator as a sequence of 3 operations:

$\boxed{\text{Rotation/reflection}} \rightarrow \boxed{\text{Scaling along the axis}} \rightarrow \boxed{\text{Rotation/reflection}}$

Correlation Operator

A linear operator that transforms the distribution for one party (appropriately normalized) to that for the other party, conditioned on the former.

$$\widetilde{C} = \Delta_{C^\intercal}^{-1/2} C \Delta_{C}^{1/2}.$$

Can use **Singular Value Decomposition** (SVD) to analyze a linear operator.

SVD views a linear operator as a sequence of 3 operations:

$\boxed{\text{Rotation/reflection}} \rightarrow \boxed{\text{Scaling along the axis}} \rightarrow \boxed{\text{Rotation/reflection}}$

The scaling factors, called the **singular values**, capture several properties of a linear transform.

Correlation Operator

A linear operator that transforms the distribution for one party (appropriately normalized) to that for the other party, conditioned on the former.

$$\widetilde{C} = \Delta_{C^\intercal}^{-1/2} C \Delta_C^{1/2}.$$

Can use **Singular Value Decomposition** (SVD) to analyze a linear operator.

SVD views a linear operator as a sequence of 3 operations:

$\boxed{\text{Rotation/reflection}} \rightarrow \boxed{\text{Scaling along the axis}} \rightarrow \boxed{\text{Rotation/reflection}}$

The scaling factors, called the **singular values**, capture several properties of a linear transform.

Spectrum of a Correlation

We define Λ_C, the **spectrum** of C as the (non-zero) *singular values of* $\widetilde{C}$.

Spectrum of a Correlation

We define Λ_C, the **spectrum** of C as the (non-zero) *singular values of* $\widetilde{C}$.

- Can relate Λ_C to **spectral graph theoretic** quantities associated with a bipartite graph representing C
  - All entries in the spectrum fall in $(0, 1]$.
  - (Log) Multiplicity of 1 gives the **common information** (measured as max-entropy) in C
  - The second largest value in the spectrum is the **maximal correlation** of C [Wit75]

- Taking multiple copies of a correlation results in multiplication of the singular values, i.e.,

$$\Lambda_{C^{\otimes \ell}} = (\Lambda_C)^{\ell} := \left\{ \prod_{i=1}^{\ell} \lambda_i | \lambda_i \in \Lambda_C \right\}.$$

Spectral Protocol (for perfect SNIR)

If (A, B) is an SNIR from D to C, then there are **spectral protocols** $\widehat{A}, \widehat{B}$ such that

$$
\begin{array}{lcl}
A,\ B \text{ determinsitic} & \implies & \widehat{A}^\intercal \widehat{A} = I,\ \widehat{B}^\intercal \widehat{B} = I \\
A^\intercal C B = D & \implies & \widehat{A}^\intercal \Sigma_C \widehat{B} = \Sigma_D \\
\exists V : A^\intercal C = DV & \implies & \widehat{A}^\intercal \Sigma_C = \Sigma_D \widehat{B}^\intercal \\
\exists U : CC = U^\intercal D & \implies & \Sigma_C \widehat{B} = \widehat{A} \Sigma_D
\end{array}
$$

Spectral Protocol (for perfect SNIR)

If (A, B) is an SNIR from D to C, then there are **spectral protocols** $\widehat{A}, \widehat{B}$ such that

$$\begin{array}{lcl} A,\ B \text{ determinsitic} & \Longrightarrow & \widehat{A}^\intercal \widehat{A} = I,\ \widehat{B}^\intercal \widehat{B} = I \\ A^\intercal C B = D & \Longrightarrow & \widehat{A}^\intercal \Sigma_C \widehat{B} = \Sigma_D \\ \exists V : A^\intercal C = D V & \Longrightarrow & \widehat{A}^\intercal \Sigma_C = \Sigma_D \widehat{B}^\intercal \\ \exists U : C C = U^\intercal D & \Longrightarrow & \Sigma_C \widehat{B} = \widehat{A} \Sigma_D \end{array}$$

$$\boxed{\widehat{A}^\intercal \Sigma_C \Sigma_C^\intercal = \Sigma_D \widehat{B}^\intercal \Sigma_C^\intercal = \Sigma_D \Sigma_D^\intercal \widehat{A}^\intercal}$$

Spectral Protocol (for perfect SNIR)

If (A, B) is an SNIR from D to C, then there are **spectral protocols** $\widehat{A}, \widehat{B}$ such that

$$
\begin{array}{lcl}
A,\ B \text{ determinsitic} & \Longrightarrow & \widehat{A}^\intercal \widehat{A} = I,\ \widehat{B}^\intercal \widehat{B} = I \\
A^\intercal C B = D & \Longrightarrow & \widehat{A}^\intercal \Sigma_C \widehat{B} = \Sigma_D \\
\exists V : A^\intercal C = DV & \Longrightarrow & \widehat{A}^\intercal \Sigma_C = \Sigma_D \widehat{B}^\intercal \\
\exists U : CC = U^\intercal D & \Longrightarrow & \Sigma_C \widehat{B} = \widehat{A} \Sigma_D
\end{array}
$$

$$\boxed{\widehat{A}^\intercal \Sigma_C \Sigma_C^\intercal = \Sigma_D \widehat{B}^\intercal \Sigma_C^\intercal = \Sigma_D \Sigma_D^\intercal \widehat{A}^\intercal}$$

Necessary conditions for Perfect SNIR (non-redundant D)

Determinisim:	A and B must be deterministic
Spectral criterion:	$\Lambda_D \subseteq \Lambda_C$
Mirroring property:	$\widehat{A} = \widehat{B}$ (after zero-padding)

Results for ϵ-SNIR

Necessary conditions for ϵ-SNIR (non-redundant D)

- There is a **deterministic** $O_D(\sqrt{\epsilon})$-SNIR
- Each element in Λ_D is close to some element in Λ_C
- $\|\widehat{A} - \widehat{B}\|$ is small (after zero-padding)

Results for Statistical SNIR

D has a **statistical** SNIR to C if, $\forall \epsilon > 0 \; \exists \ell$ s.t. D has an ϵ-secure SNIR to $C^{\otimes \ell}$.

Necessary conditions for Statistical SNIR (non-redundant D)

Determinisim:	*W.l.o.g.* A and B are deterministic
Spectral criterion:	$\Lambda_D \subseteq \Lambda_C$ (same as for perfect SNIR!)
Mirroring property:	$\|\widehat{A} - \widehat{B}\| \to 0$ (after zero-padding)

Results for Statistical SNIR

D has a **statistical** SNIR to C if, $\forall \epsilon > 0 \; \exists \ell$ s.t. D has an ϵ-secure SNIR to $C^{\otimes \ell}$.

Necessary conditions for Statistical SNIR (non-redundant D)

Determinisim:	*W.l.o.g.* A and B are deterministic
Spectral criterion:	$\Lambda_D \subseteq \Lambda_C$ (same as for perfect SNIR!)
Mirroring property:	$\|\widehat{A} - \widehat{B}\| \to 0$ (after zero-padding)

D \ C	BSC(q)		BEC(q)	
	secure	non-secure	**secure**	non-secure
BSC(p)	$p = q^{*k}$	$p \geq q$	impossible [KMN22]	$p \geq q$
BEC(p)	impossible	impossible	$p = q^k$	$p \geq q$

Results for Statistical SNIR

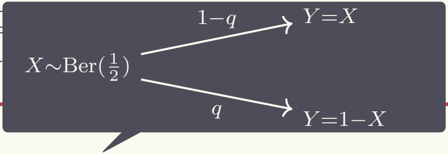
D has a **statistical** SNIR to C if, $\forall \epsilon > 0\ \exists \ell$ s.t. D has an ϵ-secure SNIR to $C^{\otimes \ell}$.

Necessary conditions for Statistical SNIR (non-redundant D)

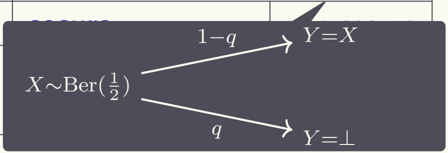
Determinisim: *W.l.o.g.* A and B are deterministic

Spectral criterion: $\Lambda_D \subseteq$

Mirroring property: $\|\widehat{A} -$



D \ C	BSC(q)		BEC(q)	
	secure	non-secure		
BSC(p)	$p = q^{*k}$	$p \geq q$		
BEC(p)	impossible	impossible		



Results for Statistical SNIR

D has a **statistical** SNIR to C if, $\forall \epsilon > 0\ \exists \ell$ s.t. D has an ϵ-secure SNIR to $C^{\otimes \ell}$.

Necessary conditions for Statistical SNIR (non-redundant D)

Determinisim:	*W.l.o.g.* A and B are deterministic
Spectral criterion:	$\Lambda_D \subseteq \Lambda_C$ (same as for perfect SNIR!)
Mirroring property:	$\|\widehat{A} - \widehat{B}\| \to 0$ (after zero-padding)

D \ C	BSC(q)		BEC(q)	
	secure	non-secure	**secure**	non-secure
BSC(p)	$p = q^{*k}$	$p \geq q$	impossible [KMN22]	$p \geq q$
BEC(p)	impossible	impossible	$p = q^k$	$p \geq q$

Other Results in the Paper

- OLE over field $\mathbb{F}$ has an SNIR to OLE over $\mathbb{F}'$ only if $\mathbb{F}$ and $\mathbb{F}'$ have the same *characteristic*
  - Characteristic of $\mathbb{F}$ is a prime number p such that $|\mathbb{F}| = p^k$ for some integer k.
  - Spectrum of OLE over field $\mathbb{F}$ has $\{1, \frac{1}{|\mathbb{F}|}\}$.
  - $\sqrt{|\mathbb{F}|} = \sqrt{|\mathbb{F}'|}^{\ell}$ only if $\mathbb{F}$ and $\mathbb{F}'$ have same characteristic.

Other Results in the Paper

- OLE over field $\mathbb{F}$ has an SNIR to OLE over $\mathbb{F}'$ only if $\mathbb{F}$ and $\mathbb{F}'$ have the same *characteristic*
  - Characteristic of $\mathbb{F}$ is a prime number p such that $|\mathbb{F}| = p^k$ for some integer k.
  - Spectrum of OLE over field $\mathbb{F}$ has $\{1, \frac{1}{|\mathbb{F}|}\}$.
  - $\sqrt{|\mathbb{F}|} = \sqrt{|\mathbb{F}'|}^{\ell}$ only if $\mathbb{F}$ and $\mathbb{F}'$ have same characteristic.
- OT has no SNIR to BSC
  - A quantitatively weaker version is implied by a (qualitatively stronger) impossibility result in the one-way secure computation model [GIKOS15]

Other Results in the Paper

- OLE over field $\mathbb{F}$ has an SNIR to OLE over $\mathbb{F}'$ only if $\mathbb{F}$ and $\mathbb{F}'$ have the same *characteristic*
  - Characteristic of $\mathbb{F}$ is a prime number p such that $|\mathbb{F}| = p^k$ for some integer k.
  - Spectrum of OLE over field $\mathbb{F}$ has $\{1, \frac{1}{|\mathbb{F}|}\}$.
  - $\sqrt{|\mathbb{F}|} = \sqrt{|\mathbb{F}'|}^{\ell}$ only if $\mathbb{F}$ and $\mathbb{F}'$ have same characteristic.
- OT has no SNIR to BSC
  - A quantitatively weaker version is implied by a (qualitatively stronger) impossibility result in the one-way secure computation model [GIKOS15]
- There are **no SNIR-complete correlations**

Other Results in the Paper

- OLE over field $\mathbb{F}$ has an SNIR to OLE over $\mathbb{F}'$ only if $\mathbb{F}$ and $\mathbb{F}'$ have the same *characteristic*
  - Characteristic of $\mathbb{F}$ is a prime number p such that $|\mathbb{F}| = p^k$ for some integer k.
  - Spectrum of OLE over field $\mathbb{F}$ has $\{1, \frac{1}{|\mathbb{F}|}\}$.
  - $\sqrt{|\mathbb{F}|} = \sqrt{|\mathbb{F}'|}^{\ell}$ only if $\mathbb{F}$ and $\mathbb{F}'$ have same characteristic.
- OT has no SNIR to BSC
  - A quantitatively weaker version is implied by a (qualitatively stronger) impossibility result in the one-way secure computation model [GIKOS15]
- There are **no SNIR-complete correlations**
- Role of common information in SNIR from D to C:

  Perfect/Statistical SNIR: "Not useful" unless D has common information

  ϵ-**SNIR:** Conditioned on common randomness in C, it remains an $O_D(\epsilon)$-SNIR

Conclusion and Open Problems

- Spectral analysis reveals structure in SNIR
- Characterized SNIR between natural correlations
- Towards decidability of SNIR

Conclusion and Open Problems

- Spectral analysis reveals structure in SNIR
- Characterized SNIR between natural correlations
- Towards decidability of SNIR (settled in upcoming follow-up work)

Conclusion and Open Problems

- Spectral analysis reveals structure in SNIR
- Characterized SNIR between natural correlations
- Towards decidability of SNIR (settled in upcoming follow-up work)
- Towards secure *interactive* reductions

Conclusion and Open Problems

- Spectral analysis reveals structure in SNIR
- Characterized SNIR between natural correlations
- Towards decidability of SNIR (settled in upcoming follow-up work)
- Towards secure *interactive* reductions
  - Decidability is long settled, with a combinatorial characterization
    - Open for one-way communication

Conclusion and Open Problems

- Spectral analysis reveals structure in SNIR
- Characterized SNIR between natural correlations
- Towards decidability of SNIR (settled in upcoming follow-up work)
- Towards secure *interactive* reductions
  - Decidability is long settled, with a combinatorial characterization
    - Open for one-way communication
  - Rate (how many copies of C per copy of D) is open, but faces circuit-complexity barriers
    - Rate of SNIR?

Thank you