Secure Non-Interactive Simulation: Feasibility & Rate

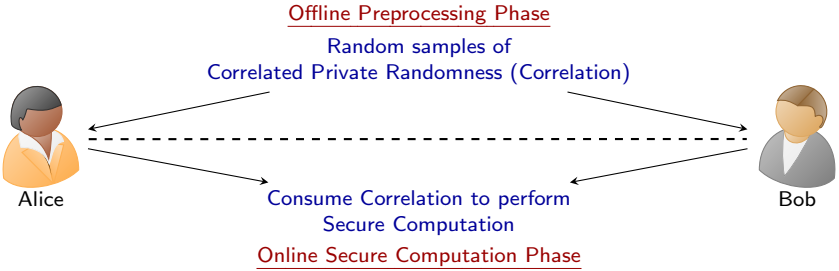
Hai H. Nguyen

Joint work with
Hamidreza Amini Khorasgani, Hemanta K. Maji

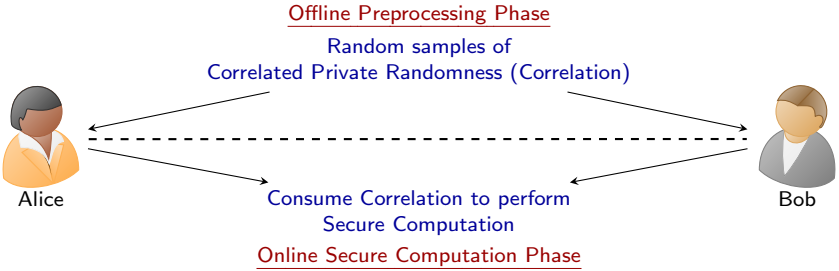
PURDUE
UNIVERSITY

June 3, 2022

Motivation


Offline Preprocessing Phase
Random samples of
Correlated Private Randomness (Correlation)
Alice
Bob
Consume Correlation to perform
Secure Computation
Online Secure Computation Phase

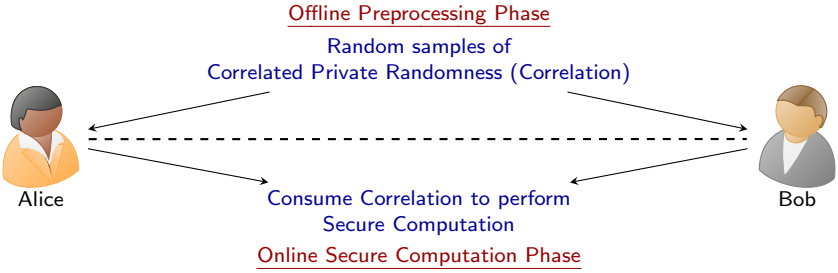
Motivation



Primary Concern

1. Online protocols need well-structured correlations that are computationally expensive to generate.
2. Online protocols using cheap correlations like noisy correlations are computationally expensive.

Motivation



Primary Concern

1. Online protocols need well-structured correlations that are computationally expensive to generate.
2. Online protocols using cheap correlations like noisy correlations are computationally expensive.

Ideal Resolution

Can we transform cheap correlations into well-structured ones?

- Non-interactively
- Efficiently

Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n

Alice

Bob

Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n

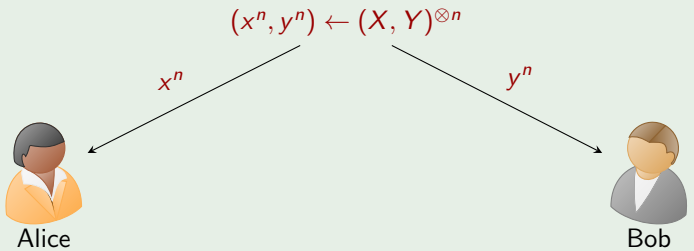
$$(x^n, y^n) \leftarrow (X, Y)^{\otimes n}$$

Alice

Bob

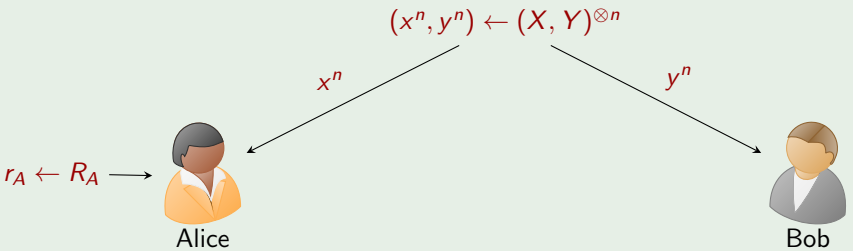
Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



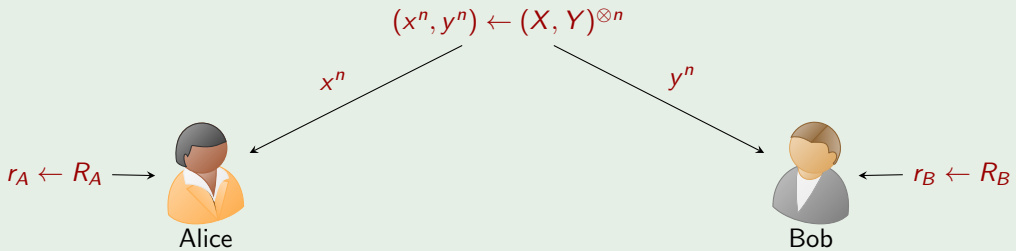
Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



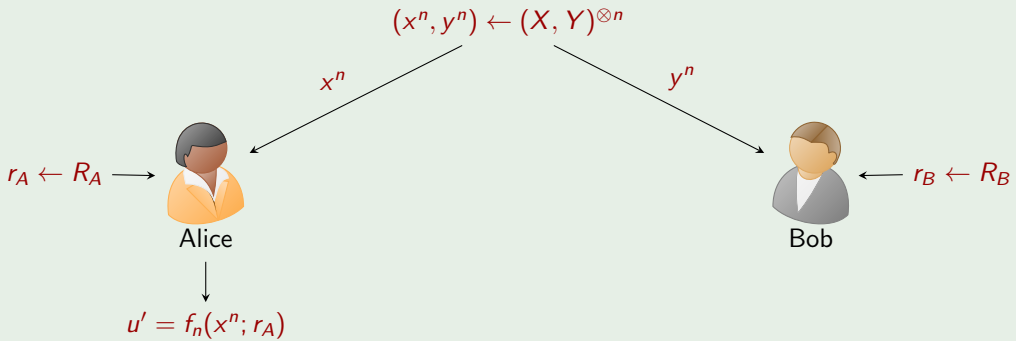
Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



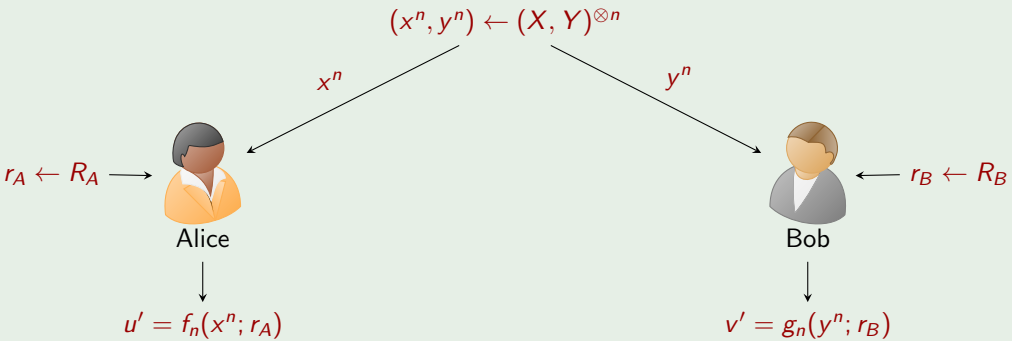
Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



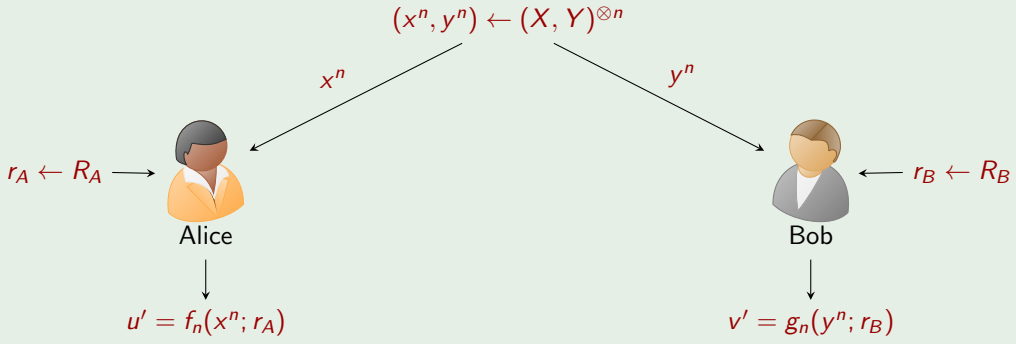
Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



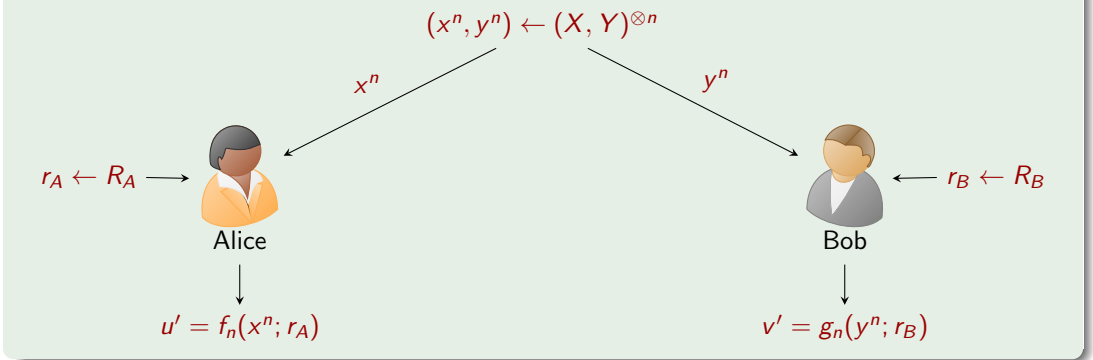
Correctness

Joint distribution of output (u', v') is close to the target distribution (U, V)

$$(U, V) \approx (U', V')$$

Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



(Information-theoretic) Security of Honest Bob against Corrupt Alice [Canetti-2000]

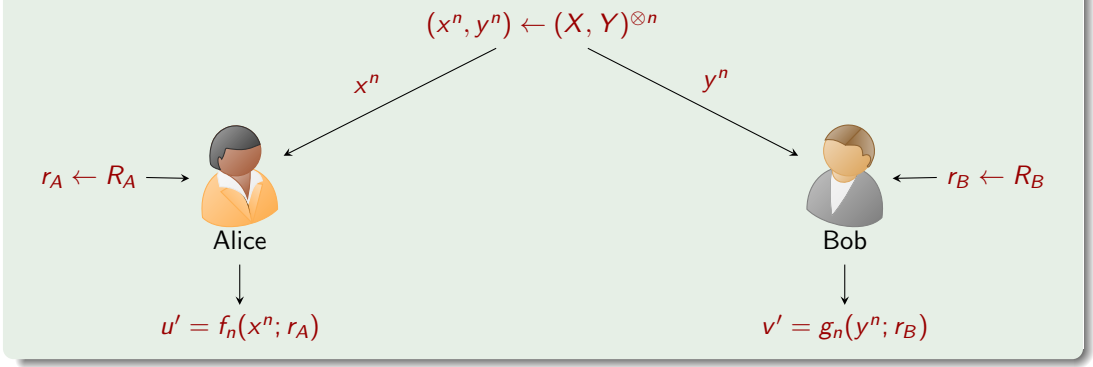
The distribution of x^n conditioned on $(u', v') = (u, v)$ is close to being independent of v

$$(X^n | U' = u, V' = v) \approx \mathrm{Sim}_{\mathrm{A}}(u)$$

Or, $V' - U' - X^n$ is an (approximate) Markov chain

Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



(Information-theoretic) Security of Honest Alice against Corrupt Bob [Canetti-2000]

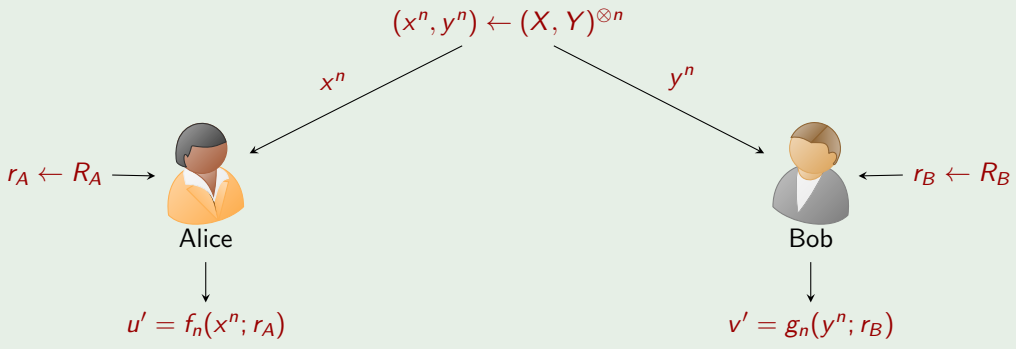
The distribution of y^n conditioned on $(u', v') = (u, v)$ is close to being independent of u

$$(Y^n | U' = u, V' = v) \approx \mathrm{Sim}_B(v)$$

Or, $U' - V' - Y^n$ is an (approximate) Markov chain

Our Model: Secure Non-Interactive Simulation

Secure Non-Interactive Simulation of (U, V) from $(X, Y)^{\otimes n}$ using reduction functions f_n, g_n



Rate: SNIS of $(U, V)^{\otimes m}$ from $(X, Y)^{\otimes n}$

Maximum achievable m/n

Positioning of this Research Problem

Pseudorandom Correlation Generators

1. Introduced by [Boyle-Couteau-Gilboa-Ishai-Kohl-Scholl–2019, Boyle-Couteau-Gilboa-Ishai-Kohl-Scholl–2020]
2. SNIS = Information-theoretic analog of PCG

Non-Interactive Simulation

1. Classical problem in information theory [Gács-Körner–1972, Wyner–1975, Witsenhausen–1975]
2. SNIS = Cryptographic extension of "Non-Interactive Simulation"

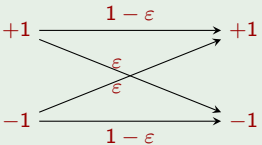
Non-Interactive Correlation Distillation

1. Target distribution is "shared keys" [Mossel-O'Donnell–2005, Mossel-O'Donnell-Regev-Steif-Sudakov–2006, Bogdanov-Mossel–2011, Chan-Mossel-Neeman–2014]
2. SNIS = Generalized targets for NICD

One-way Secure Computation

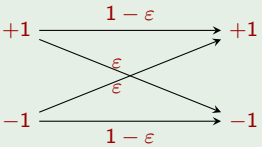
1. One party speaks and one party listens [Garg-Ishai-Kushilevitz-Ostrovsky-Sahai–2015, Agrawal-Ishai-Kushilevitz-Narayanan-Prabhakaran-Prabhakaran-Rosen–2020]
2. SNIS = Restriction of OWSC to no interaction

Representative Correlated Noise Sources

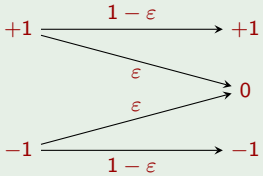


Correlated Noise from the
Binary Symmetric Source
$\mathrm{BSS}(\rho = 1 - 2\varepsilon)$, where $\varepsilon \in (0, 1/2)$

Representative Correlated Noise Sources



Correlated Noise from the
Binary Symmetric Source
$\mathrm{BSS}(\rho = 1 - 2\varepsilon)$, where $\varepsilon \in (0, 1/2)$



Correlated Noise from the
Binary Erasure Source
$\mathrm{BES}(\rho = \sqrt{1 - \varepsilon})$, where $\varepsilon \in (0, 1)$

Insecure Reduction: Example

Insecure NIS of (Target) $\mathrm{BSS}(\rho' = 1 - 2 \cdot (\varepsilon/2))$ from (Source) $\mathrm{BES}(\rho = \sqrt{1-\varepsilon})$

$$X \leftarrow \{+1, -1\} \qquad\qquad Y = \begin{cases} X, & \text{w.p. } 1-\varepsilon \\ 0, & \text{otherwise.} \end{cases}$$

$$\downarrow \qquad\qquad \downarrow$$

$$U' = X \qquad\qquad V' = \begin{cases} Y, & \text{if } Y \in \{+1, -1\} \\ \leftarrow \{+1, -1\}, & \text{otherwise.} \end{cases}$$

Insecure Reduction: Example

Insecure NIS of (Target) $\mathrm{BSS}(\rho' = 1 - 2 \cdot (\varepsilon/2))$ from (Source) $\mathrm{BES}(\rho = \sqrt{1-\varepsilon})$

$$X \leftarrow \{+1, -1\} \qquad Y = \begin{cases} X, & \text{w.p. } 1-\varepsilon \\ 0, & \text{otherwise.} \end{cases}$$

$$\downarrow \qquad\qquad \downarrow$$

$$U' = X \qquad V' = \begin{cases} Y, & \text{if } Y \in \{+1, -1\} \\ \leftarrow \{+1, -1\}, & \text{otherwise.} \end{cases}$$

Verdict: Correct, Secure against Corrupt Alice, but Insecure against Corrupt Bob

$$(Y|U' = +1, V' = +1) \equiv \begin{cases} +1, & \text{w.p. } \frac{1-\varepsilon}{1-\varepsilon/2} \\ 0, & \text{w.p. } \frac{\varepsilon/2}{1-\varepsilon/2} \end{cases}$$

$$(Y|U' = -1, V' = +1) \equiv \begin{cases} +1, & \text{w.p. } 0 \\ 0, & \text{w.p. } 1. \end{cases}$$

The distribution is NOT independent of U'

Secure Reduction: Example

Secure NIS of (Target) $\mathrm{BSS}(\rho' = \rho^2)$ from (Source) $\mathrm{BSS}(\rho = 1 - 2\varepsilon)$

$$X^2 \leftarrow \{+1, -1\}^2 \qquad\qquad Y^2 = X^2 \odot N_\rho^{\otimes 2}$$

$$\downarrow \qquad\qquad \downarrow$$

$$U' = X_1^2 \cdot X_2^2 \qquad\qquad V' = Y_1^2 \cdot Y_2^2$$

Where, the noise

$$N_\rho = \begin{cases} +1, & \text{w.p. } 1 - \varepsilon \\ -1, & \text{w.p. } \varepsilon. \end{cases}$$

Intuition

$(Y^2 | U' = +1, V' = +1)$ and $(Y^2 | U' = -1, V' = +1)$ are uniformly random over $\{(+1, +1), (-1, -1)\}$

Research Question. Given a source and target distribution, is the SNIS feasible? What is the most efficient SNIS?

Independent Work

Pratyush Agarwal, Varun Narayanan, Shreya Pathak, Manoj Prabhakaran, Vinod M. Prabhakaran, Mohammad Ali Rehan: "Secure Non-Interactive Reduction and Spectral Analysis of Correlations" (EUROCRYPT–2022)

1. Motivated by cryptographic complexity [Beimel-Malkin–2004, Maji-Prabhakaran-Rosulek–2013, Kraschewski-Maji-Prabhakaran-Sahai–2014, Beimel-Ishai-Kumaresan-Kushilevitz–2014, Narayanan-Prabhakaran-Prabhakaran–2020]

Our Results: Derandomization

Theorem (Derandomization for Feasibility Results)

If there is a (randomized) SNIS of P from $Q^{\otimes n}$ with insecurity ν, then there is a (deterministic) SNIS of P from $Q^{\otimes \Theta(n)}$ with insecurity $\nu + \exp(-n)$.

Theorem (Sample-preserving Derandomization)

If there is a (randomized) SNIS of P from $Q^{\otimes n}$ with insecurity ν, then there is a (deterministic) SNIS of P from $Q^{\otimes n}$ with insecurity $\nu^{\Theta(1)}$.

Our Results: BSS/BES Sources and Targets

Theorem (SNIS of (1) BES from BSS or (2) BSS from BES)

Impossible

Our Results: $\mathrm{BSS}/\mathrm{BES}$ Sources and Targets

Theorem (SNIS of (1) BES from BSS or (2) BSS from BES)

Impossible

Theorem (SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BSS}(\rho)$)

1. *Feasible for* $\rho' = \rho^k$, *for* $k \in \{1, 2, \dots\}$
2. *In this context, rate* $\leqslant 1/k$
3. *Statistical to Perfect Transformation: Error-correction of Reductions*
4. *Dichotomy of SNIS: Either (a) Perfect secure or (b) Constant insecure*

Our Results: $\mathrm{BSS}/\mathrm{BES}$ Sources and Targets

Theorem (SNIS of (1) BES from BSS or (2) BSS from BES)

Impossible

Theorem (SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BSS}(\rho)$)

1. *Feasible for $\rho' = \rho^k$, for $k \in \{1, 2, \dots\}$*
2. *In this context, rate $\leqslant 1/k$*
3. *Statistical to Perfect Transformation: Error-correction of Reductions*
4. *Dichotomy of SNIS: Either (a) Perfect secure or (b) Constant insecure*

Theorem (SNIS of $\mathrm{BES}(\rho')$ from $\mathrm{BES}(\rho)$)

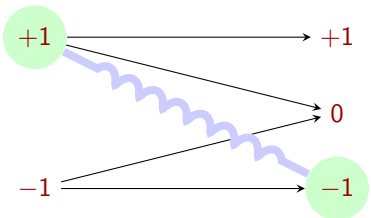
1. *Feasible for $\rho' = \rho^k$, for $k \in \{1, 2, \dots\}$, and only linear reductions*
2. *In this context, rate $\leqslant 1/k$*
3. *Statistical to Perfect Transformation: Error-correction of Reductions*
4. *Dichotomy of SNIS: Either (a) Perfectly secure or (b) Constant insecure*

Warmup: Impossibility of (Target) BES from (Source) BSS

Impossibility from NIS and OWSC extend to SNIS

1. NIS Impossibility: Reverse Hypercontractivity
2. OWSC Impossibility: Harris–Kleitman Inequality [Garg-Ishai-Kushilevitz-Ostrovsky-Sahai–2015]

Proof Intuition.



Impossibility of (Target) BSS from (Source) BES

Remark

Characterizing Feasibility/Infeasibility Parameters: This problem is incredibly challenging and remains open in NIS and OWSC

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

Step 0: Derandomization (for Feasibility/Infeasibility Results)

Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ using reduction functions $f\colon \{+1, -1\}^n \to \{+1, -1\}$ and $g\colon \{+1, 0, -1\}^n \to \{+1, -1\}$

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

- Consider reduction functions $f\colon \{+1,-1\}^n \to \{+1,-1\}$ and $g\colon \{+1,0,-1\}^n \to \{+1,-1\}$

Step 1: Algebraization of Security

The T and $\overline{T}$ are the Markov and the adjoint Markov operators associated with the $\mathrm{BES}^{\otimes n}$ joint distribution

1. $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$
2. $\left\| \overline{T} f - \rho' g \right\|_1 \leqslant 4\nu$
3. $\left\| Tg - \rho' f \right\|_1 \leqslant 4\nu$

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

- Consider reduction functions $f\colon \{+1,-1\}^n \to \{+1,-1\}$ and $g\colon \{+1,0,-1\}^n \to \{+1,-1\}$
- $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\| \overline{T} f - \rho' g \right\|_1 \leqslant 4\nu$, $\left\| Tg - \rho' f \right\|_1 \leqslant 4\nu$

Step 2: Approximate Eigenvector Problem

$$\left\| T\overline{T} f - \rho'^2 f \right\|_1 \leqslant 8\nu$$

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

- Consider reduction functions $f\colon \{+1,-1\}^n \to \{+1,-1\}$ and $g\colon \{+1,0,-1\}^n \to \{+1,-1\}$
- $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\| \overline{T} f - \rho' g \right\|_1 \leqslant 4\nu$, $\| Tg - \rho' f \|_1 \leqslant 4\nu$
- $\left\| T\overline{T} f - {\rho'}^2 f \right\|_1 \leqslant 8\nu$

Step 3: Homogeneous Property

1. Observation: $T\overline{T} = T_{\rho^2}$ (the Bonami-Beckner Noise Operator)
2. It must be the case that ${\rho'}^2 \in \left\{ \rho^2, \left(\rho^2\right)^2, \left(\rho^2\right)^3, \dots \right\}$
3. Suppose $\rho' = \rho^k$, for some constant $k \in \{1, 2, 3, \dots\}$
4. **Spectral Concentration.** Nearly all spectral weight of f is on "degree-k terms"

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

- Consider reduction functions $f\colon \{+1,-1\}^n \to \{+1,-1\}$ and $g\colon \{+1,0,-1\}^n \to \{+1,-1\}$
- $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\| \overline{T} f - \rho' g \right\|_1 \leqslant 4\nu$, $\left\| Tg - \rho' f \right\|_1 \leqslant 4\nu$
- $\left\| T\overline{T} f - \rho'^2 f \right\|_1 \leqslant 8\nu$
- $\rho' = \rho^k$ and $W^{=k}[f] \approx 1$

Step 4: Dimension Reduction

1. **Junta Theorem.** [Kindler-Safra–2002] $f \approx h$ such that h is a constant-junta

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

- Consider reduction functions $f\colon \{+1,-1\}^n \to \{+1,-1\}$ and $g\colon \{+1,0,-1\}^n \to \{+1,-1\}$
- $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\| \overline{T} f - \rho' g \right\|_1 \leqslant 4\nu$, $\| Tg - \rho' f \|_1 \leqslant 4\nu$
- $\left\| T\overline{T} f - \rho'^2 f \right\|_1 \leqslant 8\nu$
- $\rho' = \rho^k$ and $W^{=k}[f] \approx 1$
- $f \approx h$ such that h is a constant-junta

Step 5: Infeasibility

"Random restrictions" technique to prove that $\left\| \overline{T} h - \rho' g \right\| \geqslant \text{constant} > 0$

Impossibility of (Target) BSS from (Source) BES

Proof by Contradiction. Fix $\mathrm{BES}(\rho)$ and $\mathrm{BSS}(\rho')$. Suppose there is a SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BES}(\rho)^{\otimes n}$ (for some $n \in \{1, 2, \dots\}$) with insecurity ν

- Consider reduction functions $f\colon \{+1,-1\}^n \to \{+1,-1\}$ and $g\colon \{+1,0,-1\}^n \to \{+1,-1\}$
- $\mathbb{E}[f] \leqslant \nu$, $\mathbb{E}[g] \leqslant \nu$, $\left\| \overline{T} f - \rho' g \right\|_1 \leqslant 4\nu$, $\| Tg - \rho' f \|_1 \leqslant 4\nu$
- $\left\| T\overline{T} f - \rho'^2 f \right\|_1 \leqslant 8\nu$
- $\rho' = \rho^k$ and $W^{=k}[f] \approx 1$
- $f \approx h$ such that h is a constant-junta
- (Some *technical manipulation* to reach) CONTRADICTION!

High-level Analysis Template. Derandomization $\to$ Algebraization of Security $\to$ Approximate Eigenvector Problem $\to$ Fourier Concentration $\to$ Dimension Reduction

Feasibility of (Target) BSS from (Source) BSS

Feasibility Characterization

- $\rho' = \rho^k$, where $k \in \{1, 2, \dots\}$
- $W^{=k}[f] \approx 1$, $f \approx h \approx g$, where h is constant-junta Boolean function

Feasibility of (Target) BSS from (Source) BSS

Feasibility Characterization

- $\rho' = \rho^k$, where $k \in \{1, 2, \dots\}$
- $W^{=k}[f] \approx 1$, $f \approx h \approx g$, where h is constant-junta Boolean function

Example 1: $\mathrm{BSS}(\rho' = \rho^2)$ from $\mathrm{BSS}(\rho)$

Linear Reduction:

$$f(X^2) := X_1^2 \cdot X_2^2$$
$$g(Y^2) := Y_1^2 \cdot Y_2^2.$$

Feasibility of (Target) BSS from (Source) BSS

Feasibility Characterization

- $\rho' = \rho^k$, where $k \in \{1, 2, \dots\}$
- $W^{=k}[f] \approx 1$, $f \approx h \approx g$, where h is constant-junta Boolean function

Example 2: $\mathrm{BSS}(\rho' = \rho^2)$ from $\mathrm{BSS}(\rho)$

Non-Linear Reduction:

$$f(X^4) := \begin{cases} X_1^4 \cdot X_4^4, & \text{if } X_1^4 = X_2^4 \\ X_1^4 \cdot X_3^4, & \text{otherwise.} \end{cases}$$

$$= \frac{(X_1^4 - X_2^4) \cdot X_3^4 + (X_1^4 + X_2^4) \cdot X_4^4}{2}$$

$$g := f.$$

Feasibility of (Target) BSS from (Source) BSS

Feasibility Characterization

- $\rho' = \rho^k$, where $k \in \{1, 2, \dots\}$
- $W^{=k}[f] \approx 1$, $f \approx h \approx g$, where h is constant-junta Boolean function

Example 2: $\mathrm{BSS}(\rho' = \rho^2)$ from $\mathrm{BSS}(\rho)$

Non-Linear Reduction:

$$f(X^4) := \begin{cases} X_1^4 \cdot X_4^4, & \text{if } X_1^4 = X_2^4 \\ X_1^4 \cdot X_3^4, & \text{otherwise.} \end{cases}$$

$$= \frac{(X_1^4 - X_2^4) \cdot X_3^4 + (X_1^4 + X_2^4) \cdot X_4^4}{2}$$

$$g := f.$$

Question

Are non-linear reductions *always worse* than linear reductions?

Example 3: $\mathrm{BSS}(\rho' = \rho^2)$ from $\mathrm{BSS}(\rho)$

Non-Linear Reduction:

$$f^{(1)}(X^4) := \frac{(X_1^4 - X_2^4) \cdot X_3^4 + (X_1^4 + X_2^4) \cdot X_4^4}{2}$$
$$f^{(2)}(X^4) := \frac{(X_1^4 - X_2^4) \cdot X_4^4 - (X_1^4 + X_2^4) \cdot X_3^4}{2}$$
$$g^{(1)} := f^{(1)}$$
$$g^{(2)} := f^{(2)}.$$

Rate of (Target) BSS from (Source) BSS

Observations

Rate of Constructing $\mathrm{BSS}(\rho' = \rho^2)$ from $\mathrm{BSS}(\rho)$.

1. Block-linear reductions achieve $1/2$ rate
2. Non-linear reductions can also achieve $1/2$ rate

Question

Can non-linear reductions surpass rate $1/2$?

Rate of (Target) BSS from (Source) BSS

Rate of Perfect SNIS

If $\rho' = \rho^k$, for $k \in \{1, 2, \dots\}$, then the rate of SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BSS}(\rho)$ is (at most) $1/k$

Proof outline.

1. "SNIS of $\mathrm{BSS}(\rho' = \rho^k)^{\otimes m}$ from $\mathrm{BSS}(\rho)^{\otimes n}$" implies that there is a "SNIS of $\mathrm{BSS}(\rho'' = \rho^{m \cdot k})$ from $\mathrm{BSS}(\rho)^{\otimes n}$"
2. Reduction must be $m \cdot k$ homogeneous
3. $m \cdot k \leqslant n \iff m/n \leqslant 1/k$

Rate of (Target) BSS from (Source) BSS

Rate of Perfect SNIS

If $\rho' = \rho^k$, for $k \in \{1, 2, \dots\}$, then the rate of SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BSS}(\rho)$ is (at most) $1/k$

Problem remains open for Statistical SNIS.

Rate of (Target) BSS from (Source) BSS

Rate of Perfect SNIS

If $\rho' = \rho^k$, for $k \in \{1, 2, \dots\}$, then the rate of SNIS of $\mathrm{BSS}(\rho')$ from $\mathrm{BSS}(\rho)$ is (at most) $1/k$

Problem remains open for Statistical SNIS.

Conjecture

Local-to-Global Structure for Homogeneous Boolean Functions. Let $f, g, h\colon \{+1, -1\}^n \to \{+1, -1\}$ be Boolean functions satisfying

1. f is u-homogeneous, g is v-homogeneous, and h is w-homogeneous, and
2. $f \cdot g$ is $(u + v)$-homogeneous, $g \cdot h$ is $(v + w)$-homogeneous, and $h \cdot f$ is $(w + u)$-homogeneous.

Then, the function $f \cdot g \cdot h$ is $(u + v + w)$-homogeneous.

This conjecture shall prove that the rate for statistical SNIS is at most $1/k$

Connection to Distance-Invariant Codes

Definition (Distance-Invariant Codes)

A code $C \subseteq \{+1, -1\}^n$ is *distance-invariant* if the number of codewords $A_i(c)$ at distance $i \in \{0, 1, ..., n\}$ from a codeword $c \in C$ is independent of c.

Theorem (Connection between Homogeneous Boolean Functions and Distance-Invariant Codes)

There is a SNIS of $\mathrm{BSS}(\rho')$ *from* $\mathrm{BSS}(\rho)$ *if and only if*

1. *The reduction functions are identical (i.e.,* $f = g$*), and*
2. *The distance enumerators for any codeword in* $f^{-1}(+1)$ *and* $f^{-1}(-1)$ *are identical.*

Conclusions

Summary

1. Introducing SNIS and initiating the study the feasibility and rate of SNIS.
2. Giving a complete characterization of feasibility and rate among BSS and BES samples except the statistical rate of BSS from BSS.
   - Proving strong forms of statistical to perfect reductions
   - Showing a connection of SNIS among BSS samples with homogeneous Boolean functions and distance-invariant codes

Thank You!