Secure Non-Interactive Simulation from Arbitrary Joint Distributions

Hamidreza Amini Khorasgani

Joint work with

Hemanta K. Maji

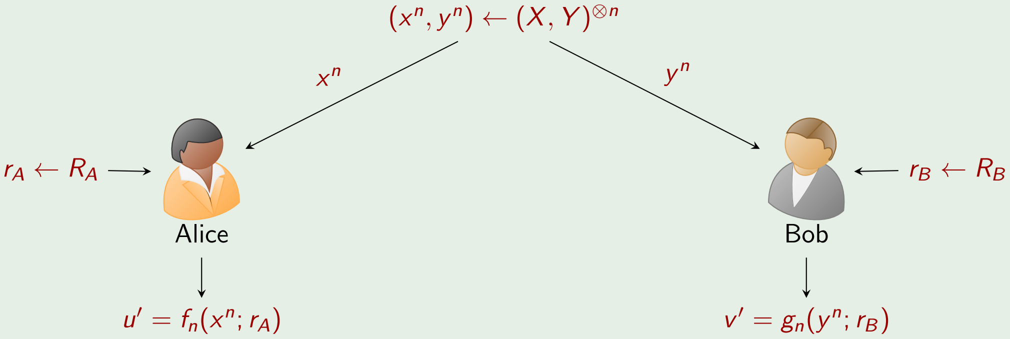
Hai H. Nguyen

PURDUE UNIVERSITY

TCC–2022

Secure Non-Interactive Simulation

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

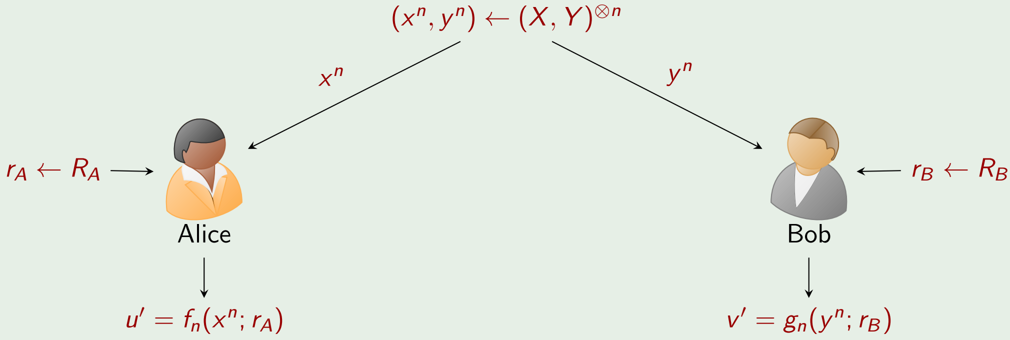


Simulation-based security

1. Correctness: $(U, V) \approx (U', V')$
2. Bob security: $(X^n | U' = u, V' = v) \approx \mathrm{Sim_A}(u)$ (X^n has no additional information about V' than U')
3. Alice security: $(Y^n | U' = u, V' = v) \approx \mathrm{Sim_B}(v)$ (Y^n has no additional information about U' than V')

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

Non-Interactive Simulation

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

Non-Interactive Correlation Distillation

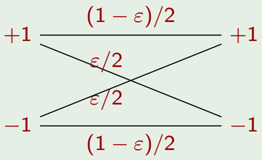
1. SNIS = Generalized targets for NICD
2. Target distribution is "shared keys" [Mossel-O'Donnell–2005, Mossel-O'Donnell-Regev-Steif-Sudakov–2006, Bogdanov-Mossel–2011, Chan-Mossel-Neeman–2014]

One-way Secure Computation

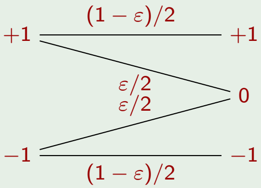
1. Secure computation with limited interaction: One party speaks and one party listens [Garg-Ishai-Kushilevitz-Ostrovsky-Sahai–2015, Agrawal-Ishai-Kushilevitz-Narayanan-Prabhakaran-Prabhakaran-Rosen–2020]
2. SNIS = Restriction of OWSC with no interaction

Protagonists

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 $\varepsilon \in (0, 1)$

Hirschfeld-Gebelein-Rényi Maximal Correlation [Hirschfeld–1935, Gebelein–1941, Rényi–1959, Witsenhausen–1975, Ahlswede-Gács–1976, Anantharam-Gohari-Kamath-Nair–2013]

$$\rho(X; Y) := \max_{\substack{\mathbb{E}[f]=\mathbb{E}[g]=0 \\ \mathbb{E}[f^2]=\mathbb{E}[g^2]=1}} \mathbb{E}[f(X) \cdot g(Y)]$$

Previous Results

Secure Non-interactive Simulation introduced by:

1. Hamidreza Amini Khorasgani, Hemanta K. Maji, Hai H. Nguyen: "Secure Non-interactive Simulation: Feasibility and Rate." (EUROCRYPT–2022)
2. 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)

Some of the Previous Results

1. A necessary condition for SNIS of a general target distribution from a general source distribution [Agarwal et al.-EC22]
2. Feasibility [Khorasgani et al.-EC22, Agarwal et al.-EC22] and Rate [Khorasgani et al.-EC22] of SNIS of $\mathrm{BSS}/\mathrm{BES}$ from $\mathrm{BSS}/\mathrm{BES}$
3. Statistical to Perfect Transformation: Error-correction of Reductions [Khorasgani et al.-EC22]
4. Dichotomy of SNIS: Either (a) Perfectly secure or (b) Constant insecure [Khorasgani et al.-EC22]

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

Theorem (Characterization)

1. *Dichotomy: Either (a) Perfectly secure or (b) c/n insecure*
2. *Algorithm to determine whether perfectly secure SNIS exists or not (only a few $constant$-juntas to test) (It returns a construction in YES instance)*

Theorem (Rate Estimate)

1. *Any feasible SNIS has constant rate*
2. *Rate $\leqslant 1/\log_{\sigma}\rho'$ (perfect security)*
   - σ^2*: The smallest (non-zero) magnitude eigenvalue of the $T\overline{T}$ operator for the source distributoin*
   - ρ'*: The maximal correlation of the target distribution*

Theorem (Power of Non-linear Reductions & Computer-assisted Search)

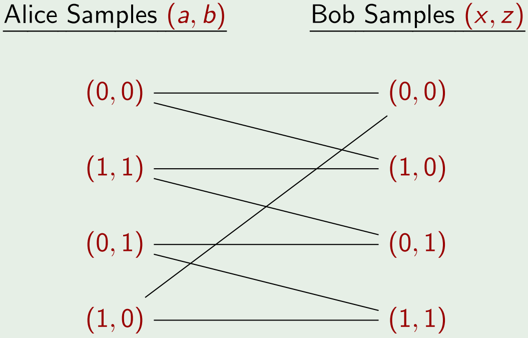
There is a source such that SNIS of $\mathrm{BSS}/\mathrm{BES}$ from this source has the following properties

1. *Any linear reduction is <u>infeasible</u>, and*
2. *There is a non-linear reduction achieving <u>optimal rate</u>*

Power of Non-linear Reductions & Computer-assisted Search

Random Oblivious Linear Function Evaluation (ROLE) [Wolf-Wullschleger–2006]

1. Sample $a, b, x \leftarrow F_2$
2. Compute $z = a \cdot x + b$
3. Give Alice (a, b) and Bob (x, z)



Fact

- Our rate upper bound for SNIS of $\mathrm{BSS}(\rho' = 1/2)$ from ROLE is $\leqslant 1/\log_\sigma \rho' = 1/2$

Question

Is this rate achievable?

Power of Non-linear Reductions & Computer-assisted Search

Known Construction: Rate 1/3 with One round communication

$\text{ROLE}^{\otimes 3}$ + One round of Communication $\rightarrow$ 1-out-of-4 (oblivious) Multiplexer

1. Alice sends a random permutation of $(u, u, u, 1-u)$, where $u \leftarrow F_2$, to the MUX
2. Bob chooses to receive a random bit v from the MUX

Rate 1/2 SNIS

Source Correlation.

$$(a_1, b_1), (a_2, b_2) \in \mathbb{F}_2 \times \mathbb{F}_2$$
$$A_i = (-1)^{a_i}, B_i = (-1)^{b_i}$$

$$(x_1, z_1), (x_2, z_2) \in \mathbb{F}_2 \times \mathbb{F}_2, \text{ where}$$
$$z_1 = a_1 \cdot x_1 + b_1, z_2 = a_2 \cdot x_2 + b_2$$
$$Z_i = (-1)^{z_i}, X_i = (-1)^{x_i}$$

Reduction Definition.

$$u = \begin{cases} +1, & \text{if } b_2 = a_1 \cdot a_2 + b_1 \\ -1, & \text{otherwise.} \end{cases}$$

$$v = \begin{cases} +1, & \text{if } z_2 = x_1 \cdot x_2 + z_1 \\ -1, & \text{otherwise.} \end{cases}$$

Rate 1/2 SNIS

Source Correlation.

$$(a_1, b_1), (a_2, b_2) \in \mathbb{F}_2 \times \mathbb{F}_2$$
$$A_i = (-1)^{a_i}, B_i = (-1)^{b_i}$$

$$(x_1, z_1), (x_2, z_2) \in \mathbb{F}_2 \times \mathbb{F}_2, \text{ where}$$
$$z_1 = a_1 \cdot x_1 + b_1, z_2 = a_2 \cdot x_2 + b_2$$
$$Z_i = (-1)^{z_i}, X_i = (-1)^{x_i}$$

Reduction Definition.

$$u = \begin{cases} +1, & \text{if } b_2 = a_1 \cdot a_2 + b_1 \\ -1, & \text{otherwise.} \end{cases}$$

$$v = \begin{cases} +1, & \text{if } z_2 = x_1 \cdot x_2 + z_1 \\ -1, & \text{otherwise.} \end{cases}$$

$$U = \frac{(1 + A_1 + A_2 - A_1 \cdot A_2) \cdot B_1 \cdot B_2}{2}$$

$$V = \frac{(1 + X_1 + X_2 - X_1 \cdot X_2) \cdot Z_1 \cdot Z_2}{2}$$

Power of Non-linear Reductions & Computer-assisted Search

Rate 1/2 SNIS

Source Correlation.

$$(a_1, b_1), (a_2, b_2) \in \mathbb{F}_2 \times \mathbb{F}_2$$

$$A_i = (-1)^{a_i}, B_i = (-1)^{b_i}$$

$$(x_1, z_1), (x_2, z_2) \in \mathbb{F}_2 \times \mathbb{F}_2, \text{ where}$$

$$z_1 = a_1 \cdot x_1 + b_1, z_2 = a_2 \cdot x_2 + b_2$$

$$Z_i = (-1)^{z_i}, X_i = (-1)^{x_i}$$

Reduction Definition.

$$u = \begin{cases} +1, & \text{if } b_2 = a_1 \cdot a_2 + b_1 \\ -1, & \text{otherwise.} \end{cases}$$

$$v = \begin{cases} +1, & \text{if } z_2 = x_1 \cdot x_2 + z_1 \\ -1, & \text{otherwise.} \end{cases}$$

$$U = \frac{(1 + A_1 + A_2 - A_1 \cdot A_2) \cdot B_1 \cdot B_2}{2}$$

$$V = \frac{(1 + X_1 + X_2 - X_1 \cdot X_2) \cdot Z_1 \cdot Z_2}{2}$$

Any linear reduction is constant insecure

Take-away

SNIS of BSC/BEC from General Sources:

1. Efficient algorithm to decide and find a construction if one exists
2. Upper and lower bounds on rate

SNIS of BSC from ROLE

1. There is a non-linear reduction that achieves optimal rate
   - Using computer-assisted search for protocol design
   - Achieve higher efficiency than previous constructions
2. Any linear reduction is constant insecure

Take-away

SNIS of BSC/BEC from General Sources:

1. Efficient algorithm to decide and find a construction if one exists
2. Upper and lower bounds on rate

SNIS of BSC from ROLE

1. There is a non-linear reduction that achieves optimal rate
    - Using computer-assisted search for protocol design
    - Achieve higher efficiency than previous constructions
2. Any linear reduction is constant insecure

Thanks!