Randomized Functions with High Round Complexity

Hai H. Nguyen

PURDUE UNIVERSITY ETH zürich

Joint work with

Saugata Basu

Hemanta K. Maji

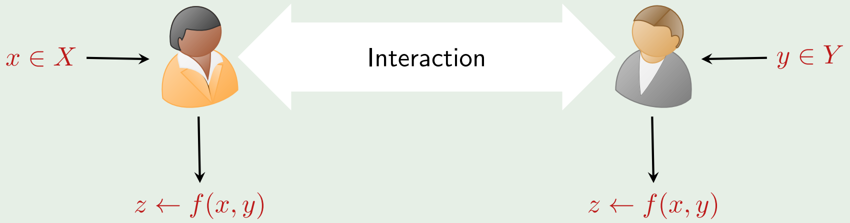
Hamidreza A. Khorasgani

PURDUE UNIVERSITY

Problem: Round Complexity of Secure Computation

Input: A function $f\colon X \times Y \to \mathbb{R}^Z$

Model: 2-party SFE in Information-theoretic Plain Model



Adversary: Honest-but-curious
Question: What is the round complexity of securely computing f?

Previous State-of-the-art

Question: What is the round complexity of $f\colon X \times Y \to \mathbb{R}^Z$?

Class of Functions	with Security	Upper Bound on $\mathsf{rc}(f)$
Any function	No	2

Previous State-of-the-art

Question: What is the round complexity of $f\colon X \times Y \to \mathbb{R}^Z$?

Class of Functions	with Security	Upper Bound on $\mathsf{rc}(f)$
Any function	No	2
Any deterministic decomposable function [Chor-Kushilevitz-Beaver-89]	Yes	$\min(\lvert Z\rvert, 2\cdot\lvert X\rvert, 2\cdot\lvert Y\rvert)-1$

Previous State-of-the-art

Question: What is the round complexity of $f\colon X \times Y \to \mathbb{R}^Z$?

Class of Functions	with Security	Upper Bound on $\mathsf{rc}(f)$
Any function	No	2
Any deterministic decomposable function [Chor-Kushilevitz-Beaver-89]	Yes	$\min(\lvert Z\rvert, 2\cdot\lvert X\rvert, 2\cdot\lvert Y\rvert) - 1$
A class of functions with $\lvert Z\rvert \leqslant 3$ [Data-Prabhakaran-18]	Yes	2

Previous State-of-the-art

Question: What is the round complexity of $f\colon X \times Y \to \mathbb{R}^Z$?

Class of Functions	with Security	Upper Bound on $\mathsf{rc}(f)$
Any function	No	2
Any deterministic decomposable function [Chor-Kushilevitz-Beaver-89]	Yes	$\min(\lvert Z\rvert, 2\cdot\lvert X\rvert, 2\cdot\lvert Y\rvert) - 1$
A class of functions with $\lvert Z\rvert \leqslant 3$ [Data-Prabhakaran-18]	Yes	2

Observation

The round complexity $\mathsf{rc}(f)$ in all these previous results

1. depends solely on the cardinality of its domain and range.
2. is independent of the probability distributions $f(x, y)$.

A Natural Conjecture:

$$\mathsf{rc}(f) = \mathsf{function}(\ \lvert X\rvert,\ \lvert Y\rvert,\ \lvert Z\rvert\ )$$

Our Contribution

Refute the Natural Conjecture:

$$\text{rc}(f) = \text{function}(|X|, |Y|, |Z|)$$

Our Contribution

Refute the Natural Conjecture:

$$\mathrm{rc}(f) = \mathrm{function}(|X|, |Y|, |Z|)$$

Theorem

1. *For any $r \in \mathbb{N}$, we construct a function $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^5$ such that $\mathrm{rc}(f) = r$.*
   - $\mathrm{rc}(f)$ *must involve the probabilities describing the function f.*
2. *Our construction is optimal.*
   - $\mathrm{rc}(f) \leqslant 4$ *for every function $f \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ satisfying $|Z| \leqslant 4$.*

Fascinating Connection Between Secure Computation & Hydrodynamics

Note

We learned about it at an Algebraic Geometry Workshop organized by [Basu-Kummer-Netzer-Vinzant-23].

Lamination Hull

Given a set of points $\Lambda \subseteq \mathbb{R}^d$, and a set of initial point $S^{(0,\Lambda)} \subseteq \mathbb{R}^d$, recursively define:

$$S^{(i+1,\Lambda)} := \left\{ \lambda \cdot Q^{(1)} + (1-\lambda) \cdot Q^{(2)} : \begin{array}{c} Q^{(1)}, Q^{(2)} \in S^{(i,\Lambda)}, \\ \lambda \in [0,1], \text{ and} \\ Q^{(1)} - Q^{(2)} \in \Lambda \end{array} \right\}.$$

The lamination hull is the limit of the sequence $S^{(0,\Lambda)} \to S^{(1,\Lambda)} \to S^{(2,\Lambda)} \to \cdots$.
Our problem: $\Lambda = (0, \mathbb{R}, \dots, \mathbb{R}) \cup (\mathbb{R}, 0, \mathbb{R}, \dots, \mathbb{R}) \subseteq \mathbb{R}^d$

Tied to computing the stationary solutions to the following differential equations: do secure protocols manifest in physical processes in nature?

Incompressible Porous Media (IPM) Equations

Conservation of Mass, Incompressibility, Darcy's Law (ρ: fluid density, $\mathbf{v}$: velocity, g: gravity.)

$$\partial_t \rho + \nabla \cdot (\rho \mathbf{v}) = 0, \qquad \nabla \cdot \mathbf{v} = 0, \qquad \frac{\mu}{\kappa} \vec{v} = -\nabla p - \rho g.$$

Recap of Basu-Khorasgani-Maji-Nguyen (FOCS 2022)

Reduction: Round Complexity to a Geometric Problem

Consider a (possibly randomized) functionality $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$.

1. **Geometric Encoding:** $(\text{Alice Marginal}, \text{Bob Marginal}, \text{Function Encoding}) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}^{|Z|}$
2. **Rules for Bonding:** Convexly combine (X_1, Y_1, F) and (X_2, Y_2, F') if and only if $X_1 = X_2$ or $Y_1 = Y_2$

Recap of Basu-Khorasgani-Maji-Nguyen (FOCS 2022)

Reduction: Round Complexity to a Geometric Problem

Consider a (possibly randomized) functionality $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$.

1. **Geometric Encoding:** $(\text{Alice Marginal}, \text{Bob Marginal}, \text{Function Encoding}) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}^{|Z|}$
2. **Rules for Bonding:** Convexly combine (X_1, Y_1, F) and (X_2, Y_2, F') if and only if $X_1 = X_2$ or $Y_1 = Y_2$
3. **Base Case:** $S^{(0)}$ = Set of all Encoded "unsplit" Monochromatic Rectangles, $\left|S^{(0)}\right| = |Z|$
4. **Recursion (Geometric Action):** $S^{(i+1)}$ is the set of all *convex combination* of points in $S^{(i)}$ that satisfy the "Rules of Bonding"
5. **Target:** $Q(f) = (1/2, 1/2, \text{Encoding of } f)$

Recap of Basu-Khorasgani-Maji-Nguyen (FOCS 2022)

Reduction: Round Complexity to a Geometric Problem

Consider a (possibly randomized) functionality $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$.

1. **Geometric Encoding:** $(\text{Alice Marginal}, \text{Bob Marginal}, \text{Function Encoding}) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}^{|Z|}$
2. **Rules for Bonding:** Convexly combine (X_1, Y_1, F) and (X_2, Y_2, F') if and only if $X_1 = X_2$ or $Y_1 = Y_2$
3. **Base Case:** $S^{(0)} =$ Set of all Encoded "unsplit" Monochromatic Rectangles, $\left|S^{(0)}\right| = |Z|$
4. **Recursion (Geometric Action):** $S^{(i+1)}$ is the set of all *convex combination* of points in $S^{(i)}$ that satisfy the "Rules of Bonding"
5. **Target:** $Q(f) = (1/2, 1/2, \text{Encoding of } f)$
6. **Round Complexity:** $\mathsf{rc}(f) \leqslant r$ if and only if $Q(f) \in S^{(r)}$
   - **Protocol Construction:** If $Q(f) \in S^{(r)}$, then the *parse tree* of "how base cases generate $Q(f)$" translates into a secure protocol
   - **Obstruction Detection:** If $Q(f) \notin S^{(r)}$, then there is no secure protocol

Recap of Basu-Khorasgani-Maji-Nguyen (FOCS 2022)

Reduction: Round Complexity to a Geometric Problem

Consider a (possibly randomized) functionality $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$.

1. **Geometric Encoding:** $(\text{Alice Marginal}, \text{Bob Marginal}, \text{Function Encoding}) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}^{|Z|}$
2. **Rules for Bonding:** Convexly combine (X_1, Y_1, F) and (X_2, Y_2, F') if and only if $X_1 = X_2$ or $Y_1 = Y_2$
3. **Base Case:** $S^{(0)} =$ Set of all Encoded "unsplit" Monochromatic Rectangles, $\left|S^{(0)}\right| = |Z|$
4. **Recursion (Geometric Action):** $S^{(i+1)}$ is the set of all *convex combination* of points in $S^{(i)}$ that satisfy the "Rules of Bonding"
5. **Target:** $Q(f) = (1/2, 1/2, \text{Encoding of } f)$
6. **Round Complexity:** $\mathsf{rc}(f) \leqslant r$ if and only if $Q(f) \in S^{(r)}$
   - **Protocol Construction:** If $Q(f) \in S^{(r)}$, then the *parse tree* of "how base cases generate $Q(f)$" translates into a secure protocol
   - **Obstruction Detection:** If $Q(f) \notin S^{(r)}$, then there is no secure protocol

Corollary

$\mathsf{rc}(f) = r$ *if and only if* $Q(f) \in S^{(r)} \setminus S^{(r-1)}$

Overview of Our Construction

High-Level Idea

Objective: For every r, construct a function $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^5$ such that $\mathsf{rc}(f_r) = r$.

BKMN's Reduction: Construct f_r such that $Q(f_r) \in S^{(r)}$ and $Q(f_r) \notin S^{(r-1)}$

Overview of Our Construction

High-Level Idea

Objective: For every r, construct a function $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^5$ such that $\mathrm{rc}(f_r) = r$.

BKMN's Reduction: Construct f_r such that $Q(f_r) \in S^{(r)}$ and $Q(f_r) \notin S^{(r-1)}$

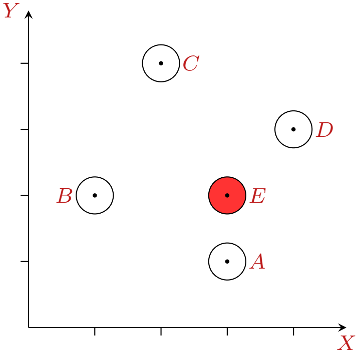
Our Main Idea: Construct a set $S^{(0)}$ of *constant size* in an ambient space of *constant dimension* such that

$$S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$$

- Otherwise, if $S^{(t)} = S^{(t+1)}$, for some $t \in \{0,1,2,\ldots\}$, then $\mathrm{rc}(f) \leqslant t$

Our Illustrative Example: Tartar Square

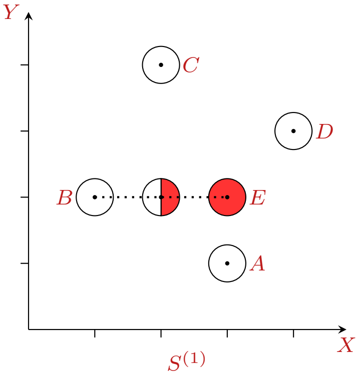
Objective: Construct $S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$



$$\mathbb{R}^3 \supseteq S^{(0)} = \{A = (3,1,0), B = (1,2,0), C = (2,4,0), D = (4,3,0), E = (3,2,1)\}$$

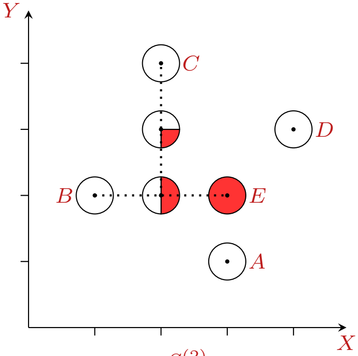
Our Illustrative Example: Tartar Square

Objective: Construct $S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$



Our Illustrative Example: Tartar Square

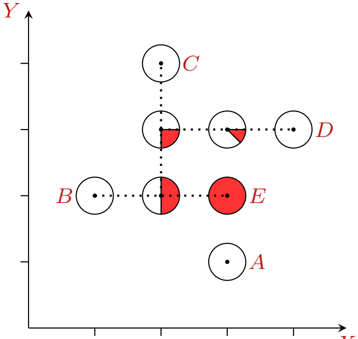
Objective: Construct $S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$



$S^{(2)}$

Our Illustrative Example: Tartar Square

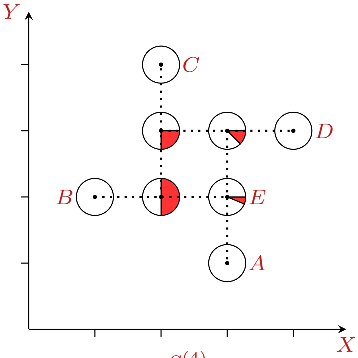
Objective: Construct $S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$



$S^{(3)}$

Our Illustrative Example: Tartar Square

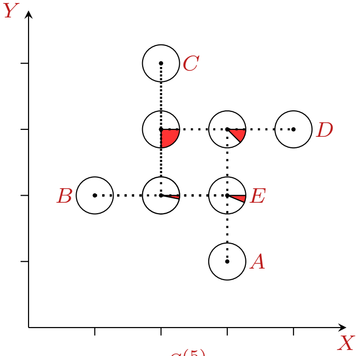
Objective: Construct $S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$



$S^{(4)}$

Our Illustrative Example: Tartar Square

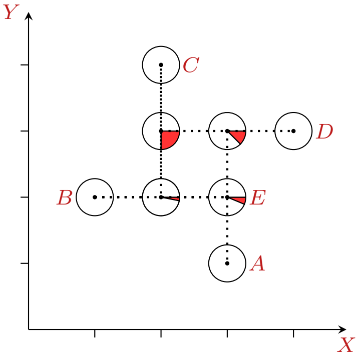
Objective: Construct $S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$



$S^{(5)}$

Our Illustrative Example: Tartar Square

Objective: Construct $S^{(0)} \subsetneq S^{(1)} \subsetneq S^{(2)} \subsetneq \cdots$



Notes

1. Constructed a sequence of points $P^{(1)}, P^{(2)}, P^{(3)}, P^{(4)}, \ldots \in \mathbb{R}^3$ such that
   - the third coordinate of $P^{(i)}$ is $1/2^i$ that tends to but never reaches 0,
   - $P^{(i)} \in S^{(i)} \setminus S^{(i-1)}$ for every i.
2. Similar to the famous Tartar square in Mathematics.

Functions with High Round Complexity

	$y=0$					$y=1$				
$x=1$	$\frac{1}{16}\sigma_k$	$\frac{3}{4}\sigma_{k+1}$	$\frac{1}{8}\sigma_k$	0	$\frac{1}{2^{4k+2}}$	$\frac{3}{16}\sigma_k$	$\frac{3}{4}\sigma_{k+1}$	0	0	$\frac{1}{2^{4k+2}}$
$x=0$	$\frac{3}{16}\sigma_k$	$\frac{1}{4}\sigma_{k+1}$	$\frac{1}{8}\sigma_k$	$\frac{3}{8}\sigma_k$	$\frac{3}{2^{4k+2}}$	$\frac{9}{16}\sigma_k$	$\frac{1}{4}\sigma_{k+1}$	0	$\frac{1}{8}\sigma_k$	$\frac{3}{2^{4k+2}}$

Construction of $f_{4k+1} \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^5$ such that $\mathrm{rc}(f_{4k+1}) = 4k+1$, where $\sigma_k = \frac{1-(1/16)^k}{1-1/16}$.

Geometric Encoding

Initial Set: Let e_i be the i-th standard basis of $\mathbb{R}^5$

$$S^{(0)} = \left\{ \left(\frac{3}{4}, \frac{1}{4}, e_1\right), \left(\frac{1}{4}, \frac{2}{4}, e_2\right), \left(\frac{2}{4}, \frac{4}{4}, e_3\right), \left(\frac{4}{4}, \frac{3}{4}, e_4\right), \left(\frac{3}{4}, \frac{2}{4}, e_5\right) \right\} \subseteq \mathbb{R}^7$$

Query Point:

$$Q(f_{4k+1}) = \left(1/2, 1/2, \frac{\sigma_k}{4}, \frac{\sigma_{k+1}}{2}, \frac{\sigma_k}{16}, \frac{\sigma_k}{8}, \frac{1}{2^{4k+1}}\right) \in S^{(4k+1)} \setminus S^{(4k)}$$

Conclusion

Theorem

1. *For any* $r \in \mathbb{N}$, *there is a function* $f_r\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^5$ *such that* $\mathsf{rc}(f) = r$.
2. $\mathsf{rc}(f) \leqslant 4$ *for every function* $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ *satisfying* $|Z| \leqslant 4$.

Question

Does a 2-party function, possibly with randomized output, have a secure protocol?

Conclusion

Theorem

1. *For any* $r \in \mathbb{N}$, *there is a function* $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^5$ *such that* $\mathsf{rc}(f) = r$.
2. $\mathsf{rc}(f) \leqslant 4$ *for every function* $f \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ *satisfying* $|Z| \leqslant 4$.

Question

Does a 2-party function, possibly with randomized output, have a secure protocol?

On-going Work

The above question is *decidable* (Technical machinery: Tropical Geometry)

Thank you!