Geometry of Secure Two-party Computation

Saugata Basu Hamidreza Amini Khorashgani Hemanta K. Maji
Hai H. Nguyen

Abstract

Characterizing the optimal round and communication complexity of secure computation is essential to minimize the overhead of security when computing over distributed data. In this context, the seminal results of Chor-Kushilevitz-Beaver (STOC–1989, FOCS–1989, DIMACS–1989) characterize all two-party computations with deterministic output that admit secure protocols, namely, the decomposable functions. However, the precise round and communication complexity have essentially remained unexplored for secure protocols of computations with randomized output. The space of all candidate private-coin secure protocols has an intricate structure that confounds intuition and has been challenging to reason.

Our work resolves this problem for two-party secure function evaluation functionalities with randomized output. We introduce an innovative geometric encoding of all candidate secure protocols for a given computation as points in a high-dimensional space. Next, we analyze the properties of these geometric sets of points using a real algebraic geometry toolkit and demonstrate their tameness. Consequently, the following decidability, search, and optimization results follow.

1. Determining whether a given computation admits a secure protocol within round or communication constraints is decidable.
2. If there is such a protocol, we can construct one such protocol.
3. Otherwise, we present a geometric obstruction to achieving security.

Tight new information complexity bounds for secure computation follow as corollaries of our technical contributions. We demonstrate the expressive power of our results by unifying the current state-of-the-art. The geometric sets that we study are new and natural generalizations of the convex hull of points, motivating exciting new foundational research in real algebraic geometry and topology.

1 Introduction

Consider the *privacy-preserving mechanism design* for (a variant of) the *facility location* problem: Determine a facility's location distributed according to a (discrete) Gaussian at the centroid of parties' private locations. Among various privacy metrics, *secure multi-party computation* (MPC), introduced by Yao [Yao86] and Goldreich-Micali-Wigderson [GMW87], facilitates the formalization of meaningful security where parties can interactively achieve this objective without revealing non-essential information, even a posteriori [NPS99].

Motivated by such applications, it is natural to study an abstraction where Alice and Bob have *private inputs* $x \in X$ and $y \in Y$. Their objective is to *interactively* compute their output sampled from the distribution $f(x, y)$ (over some sample space Z) without revealing additional information about their private inputs. The computation f, represented by the output distributions $\{f(x, y) \in \mathbb{R}^Z : x \in X, y \in Y\}$, is public knowledge. Both parties have an *unbounded computational power* and are *honest-but-curious*, i.e., they follow the prescribed protocol; however, they are curious to find additional information.

Question. Is there a secure protocol for a given computation?
What is its round and communication complexity?

Investigating this fundamental research problem is primarily restricted to computations with deterministic output or where at most one party's input influences the output. For example, among computations with deterministic output, the seminal works of Chor, Kushilevitz, and Beaver [CK89, Kus89, Bea89] characterized *decomposable functions* as ones admitting secure protocols. The case of functions with *randomized output* has remained unresolved ever since, barring highly specialized computations [MPR13, DP18] (c.f., the discussions in [MPR13, Bra21, Wei15]).

In particular, even the *decidability* of this problem is unknown, let alone resolving the search and optimization analogs. Systematically exploring the space of all candidate *private-coin* protocols to address such computability, search, or optimization problems has been a challenging hurdle to overcome.

Our contributions. We investigate the round and communication complexity of two-party secure function evaluation. Given a computation, we determine whether there is a secure protocol for the computation within specified round or communication constraints. We generate one such secure computation protocol if the feasibility test is affirmative. Otherwise, we demonstrate a (geometric) obstruction to secure realizability within these constraints. The following *technical innovations* underlie our results.

1. An innovative geometric encoding of candidate secure (private-coin) protocols for a given computation, and

2. Introducing (new and) natural generalizations of the convex hull of points to study the properties of appropriate sets of points (refer to Appendix I for details).

The round and communication studies generate (the encoding of) increasingly complex candidate (private-coin) protocols using an appropriate recursive *geometric action*, starting from initial points that encode the base case protocols. Our feasibility test translates into a membership test for a specific query point in these recursively-generated sets of points. The generative story of this membership yields a secure protocol for the computation. If the query point is outside these sets, then (a succinct description of) these sets represent a geometric obstruction to secure realizability.

We study the sets of points that this geometric action recursively generates through the lens of real algebraic geometry. We show that these sets are *tame* and support the features indicated above. Consequently, we obtain the following general feasibility, search, and optimization results.

Theorem 1 (Determining Round Complexity)**.** *There is a procedure that takes as input (a) the function $f\colon X \times Y \to \mathbb{R}^Z$, and (b) the interaction constraint $r \in \{1, 2, \dots, \}$. This procedure says yes if (and only if) there is a secure protocol for f with (at most) r rounds.*

If such a protocol exists, this procedure outputs one such secure protocol. If no such protocol exists, this procedure outputs a (geometric) certificate attesting to this fact.

Theorem 2 (Determining Communication Complexity)**.** *There is a procedure that takes as input (a) the function $f\colon X \times Y \to \mathbb{R}^Z$, and (b) the communication constraint $c \in \{1, 2, \dots, \}$. This procedure says yes if (and only if) there is a secure protocol for f with (at most) c-bit communication.*

If such a protocol exists, this procedure outputs one such secure protocol. If no such protocol exists, this procedure outputs a (geometric) certificate attesting to this fact.

Furthermore, our proof techniques establish the following consequences.

1. Appendix E and Appendix F: Our results subsume and unify the current state-of-the-art. For example, the characterization of Chor-Kushilevitz-Beaver [CK89, Kus89, Bea89] and Data-Prabhakaran [DP18] are particular cases of our general results.

2. Lemma 7: Even for $X = Y = \{0, 1\}$, for any $r \in \{1, 2, \dots\}$, there are functions $f\colon X \times Y \to \mathbb{R}^Z$ requiring r rounds of interaction, and, in turn, r bits of communication, for secure computation.

3. Corollary 1: If a function $f\colon X \times Y \to \mathbb{R}^Z$ has a secure r-round protocol, then there is an r-round secure protocol where Alice communicates $\lceil \lg(|X| + |Z|) \rceil$ bits, and Bob communicates $\lceil \lg(|Y| + |Z|) \rceil$ bits per round.

Overview of the paper. Section 2 introduces some minimal definitions and Section 3 presents our technical approach and illustrates it using an example. Section 4 summarizes the reduction of the cryptographic problem to a geometric problem. Section 5 and Section 6 demonstrate that the geometric problem is computable.

2 Preliminaries

This section defines our model and introduces basic definitions to facilitate our discussions.

System model. We consider the standard *two-party full information model* – Alice and Bob have *unbounded computation power*, and a *synchronous communication channel* connects them. Parties have access to an *unbounded number of independent private random bits* with *arbitrary biases*. For example, a party can have a private random bit that is 1 with a probability of $1/\pi$. In an interactive protocol, a *round* corresponds to one party sending a message to the other party.

Secure function evaluation functionalities. Alice and Bob have private inputs $x \in X$ and $y \in Y$, respectively. A *secure function evaluation* functionality samples (z_A, z_B) according to a distribution $f(x, y)$, and outputs z_A to Alice and z_B to Bob.

Among these functionalities, a *symmetric secure function evaluation* (SSFE) samples z according to a distribution $f(x, y)$ and outputs z to both Alice and Bob. Appendix H argues that

restricting our investigation to symmetric functions is sufficient. Therefore, the sequel investigates a randomized two-party function $f\colon X \times Y \to \mathbb{R}^Z$, where $f(x,y)_z$ represents the probability of the output being $z \in Z$ conditioned on the inputs $(x,y) \in X \times Y$. Furthermore, $f(x,y)$ represents the output distribution over Z for inputs $(x,y) \in X \times Y$.

Security model. We denote two identical distributions D and D' by $D \equiv D'$. Our work considers *perfect security* against *honest-but-curious (semi-honest)* adversaries, i.e., adversaries who follow the protocol honestly but are curious to find additional information about the honest party's input.

Definition 1 (Semi-honest Security)**.** Π *is a* perfectly semi-honest secure *protocol for a function* $f\colon X \times Y \to \mathbb{R}^Z$ *if the following conditions hold.*

1. ***Correctness.*** *Every complete transcript* τ *of the protocol* Π *is associated with an output* $\text{out}(\tau) \in Z$*. Let* $T(x,y)$ *represent the random variable corresponding to the complete transcript of the protocol* Π *when parties have private inputs* x *and* y*. Then, the following identity holds for every* $(x,y) \in X \times Y$*.*
$$\text{out}\left(T(x,y)\right) \equiv f(x,y).$$

2. ***Security against corrupt Alice.*** *The protocol transcript provides Alice with no additional information about Bob's private input beyond their output. That is, there is a simulator* Sim_A *such that the following identity holds for all* $(x,y) \in X \times Y$*.*
$$\text{Sim}_A(x, f(x,y)) \equiv T(x,y).$$
Intuitively, the Markov chain $Y - (X, f(X,Y)) - T(X,Y)$ *holds.*

3. ***Security against corrupt Bob.*** *There is a simulator* Sim_B *such that the following identity holds for all* $(x,y) \in X \times Y$*.*
$$\text{Sim}_B(y, f(x,y)) \equiv T(x,y).$$

This definition coincides with Canetti's *universally composable security* definition [Can00].

Round and communication complexity. Our work considers standard worst-case notions of round and communication complexity for interactive protocols. A protocol has round complexity (at most) r, if for all Alice input x and her private randomness, and Bob input y and his private randomness, the protocol Π exchanges (at most) r messages. Similarly, a protocol has communication complexity (at most) c, if for all Alice input x and her private randomness, and Bob input y and his private randomness, the protocol Π communicates (at most) c bits.

3 Overview: Our Technical Approach

This section presents a high-level summary of our technical ideas underlying our proof strategy to determine whether a given two-party SSFE has an r-round secure protocol or not. An illustrative worked-out representative example accompanies this presentation, showing that the example function of Figure 1 has a 4-round secure protocol and no 3-round secure protocol. The presentation below follows the actual proof closely, except for a definition where "division by 0 concerns" may arise, which the full proof in Appendix B subsequently addresses.

$f(1,0) = \frac{1}{216} \cdot (26, 40, 96, 54)$	$f(1,1) = \frac{1}{216} \cdot (13, 50, 72, 81)$
$f(0,0) = \frac{1}{216} \cdot (52, 80, 48, 36)$	$f(0,1) = \frac{1}{216} \cdot (26, 100, 36, 54)$

Figure 1: Definition of the representative example function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4\}}$.

Step 0: Standardization. Prior results [MPR13, DP18] show that one needs to consider only symmetric secure function evaluation (SSFE) $f\colon X \times Y \to \mathbb{R}^Z$ of a specific *standardized form*. Among all SSFE, one needs to consider only those where there are $A \in \mathbb{R}^{X \times Z}$, $B \in \mathbb{R}^{Y \times Z}$, and $V \in \mathbb{R}^Z$ such that the following identities hold (see Lemma 1 in Appendix B).

$$f(x,y)_z = A_{x,z} \cdot B_{y,z} \cdot V_z \qquad \text{(for all } x \in X, y \in Y, z \in Z\text{)}$$

$$\sum_{x \in X} A_{x,z} = 1 \text{ and } \qquad \sum_{y \in Y} B_{y,z} = 1 \qquad \text{(for all } z \in Z\text{)}$$

Consider our example SSFE $f\colon X \times Y \to \mathbb{R}^Z$ in Figure 1, where $X = Y = \{0,1\}$ and $Z = \{1,2,3,4\}$. This function satisfies the standardization constraints as evidenced by $A \in \mathbb{R}^{X \times Z}$, $B \in \mathbb{R}^{Y \times Z}$, and $V \in \mathbb{R}^Z$ below.

$$A = \begin{cases} A_1 = (1/3, 1/3, 2/3, 3/5) \in \mathbb{R}^Z \\ A_0 = (2/3, 2/3, 1/3, 2/5) \in \mathbb{R}^Z \end{cases} \qquad B = \begin{cases} B_1 = (1/3, 5/9, 3/7, 3/5) \in \mathbb{R}^Z \\ B_0 = (2/3, 4/9, 4/7, 2/5) \in \mathbb{R}^Z \end{cases} \tag{1}$$

$$V = (13/24, 5/4, 7/6, 25/24) \in \mathbb{R}^Z \tag{2}$$

Step 1: Security experiment. Suppose Π is a perfectly secure protocol for f. Let $\Pi^{(\tau)}$ represent the *residual protocol* of Π continuing from the partial transcript τ.[1] For example, when $\tau = \emptyset$ (the empty transcript), then $\Pi^{(\tau)} = \Pi$, and when τ is a complete transcript, then $\Pi^{(\tau)}$ is a 0-round protocol where the output is $\text{out}(\tau)$, irrespective of the parties' inputs.

Let $f^{(\tau)}\colon X \times Y \to \mathbb{R}^Z$ represent the randomized function such that $f^{(\tau)}(x,y)$ is identical to the output distribution of the protocol $\Pi^{(\tau)}(x,y)$, for all $(x,y) \in X \times Y$. For example, $f^{(\emptyset)} = f$ and, for a complete transcript τ, the function $f^{(\tau)} = e(z)$, a function that outputs z with probability 1 (irrespective of the inputs), where $z = \text{out}(\tau)$ and $e(z) \in \{0,1\}^Z$ is a vector indicating the output $z \in Z$.

Consider an *environment* that samples x uniformly at random from X, samples y uniformly (and independently) at random from Y, sends x to Alice and sends y to Bob. For a partial transcript τ of the protocol, let $\pi^{(\tau)} \in \mathbb{R}^X$ represent the conditional distribution of Alice's input conditioned on Π generating the partial transcript τ. Likewise, let $\rho^{(\tau)} \in \mathbb{R}^Y$ represent the conditional distribution of Bob input conditioned on Π generating τ.

We define the *pertinent information* corresponding to the partial transcript τ as $\left(\pi^{(\tau)}, \rho^{(\tau)}, f^{(\tau)}\right)$. Our objective is to characterize *all* candidate pertinent information systematically.

[1] The formal description of the protocol $\Pi^{(\tau)}(x,y)$ is as follows. Alice reverse-samples a random local private randomness consistent with her private input x and the public transcript τ. Bob reverse-samples a random local private randomness consistent with his private input y and the public transcript τ. Starting with these private views, Alice and Bob follow the protocol Π to generate the next messages and extend the protocol transcript τ.

Step 2: Structure for inductive geometric characterization. We inductively prove a *function structure* result showing that the following identity holds for some appropriate $V^{(\tau)} \in \mathbb{R}^Z$.

$$f^{(\tau)}(x,y)_z = \left(\frac{A_{x,z}}{\pi_x^{(\tau)}}\right) \cdot \left(\frac{B_{y,z}}{\rho_y^{(\tau)}}\right) \cdot V_z^{(\tau)}, \text{ for all } x \in X, y \in Y, z \in Z \tag{3}$$

That is, $\left(\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)}\right) \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z$ determines the function $f^{(\tau)}$, represented by $f^{(\tau)} \cong \left(\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)}\right)$. Consequently, henceforth, $\left(\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)}\right) \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z$ represents the pertinent information of τ.

Simultaneously, we inductively prove a *geometric embedding*. Let $\Omega^{(\tau)}$ represent the set of all partial transcripts that are one-round extensions of τ. Then, the following geometric embedding holds

$$\left(\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)}\right) = \sum_{\tau' \in \Omega^{(\tau)}} p^{(\tau')} \cdot \left(\pi^{(\tau')}, \rho^{(\tau')}, V^{(\tau')}\right),$$

where $\left\{p^{(\tau')}\right\}_{\tau' \in \Omega^{(\tau)}}$ is a probability distribution over $\Omega^{(\tau)}$.

If Alice extends the partial transcript τ, then $\rho^{(\tau)} = \rho^{(\tau')}$, for all $\tau' \in \Omega^{(\tau)}$, because she cannot reveal additional information about Bob's input beyond what the partial transcript τ already reveals. Similarly, if Bob extends the partial transcript τ, then $\pi^{(\tau)} = \pi^{(\tau')}$, for all $\tau' \in \Omega^{(\tau)}$.

We prove the function structure and the geometric embedding results simultaneously using induction on the *height* of the partial transcript τ, which is naturally defined. A complete transcript has height 0, and the height of any partial transcript is one more than the maximum height of the partial transcripts in $\Omega^{(\tau)}$.

Step 3: Base cases. Fix a complete transcript τ such that $\text{out}(\tau) = z \in Z$. By the security of the protocol, observe that $\pi_x^{(\tau)} = A_{x,z}$, for all $x \in X$, and $\rho_y^{(\tau)} = B_{y,z}$, for all $y \in Y$. Furthermore, the function $f^{(\tau)} = e(z)$, therefore $V^{(\tau)} = e(z)$ ensures that $f^{(\tau)} \cong \left(\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)}\right)$. Observe that the pertinent information of the complete transcript τ depends solely on f and is independent of the transcript itself.

For all output $z \in Z$, define the point

$$P^{(z)} = (\ (A_{x,z} \colon x \in X)\,, (B_{y,z} \colon y \in Y)\,, e(z)\ ) \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z. \tag{4}$$

For our example, we have (refer to Equation 1 for values of A and B)

$$P^{(1)} = ((2/3, 1/3), (2/3, 1/3), e(1))\,, \qquad P^{(2)} = ((2/3, 1/3), (4/9, 5/9), e(2))\,,$$
$$P^{(3)} = ((1/3, 2/3), (4/7, 3/7), e(3))\,, \qquad P^{(4)} = ((2/5, 3/5), (2/5, 3/5), e(4))\,.$$

Therefore, the pertinent information of all transcripts of height 0 (i.e., the complete transcripts) lie in the set

$$\mathcal{S}^{(0)} := \left\{P^{(z)} \colon z \in Z\right\} \subseteq \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z.$$

Step 4: Recursive generation of complex protocols. For $i \in \{0, 1, \dots\}$, let $\mathcal{S}^{(i)} \subseteq \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z$ represent the set of all candidate pertinent information of partial transcripts at height $\leqslant i$. Assume that we already have computed the set $\mathcal{S}^{(i)}$. Our objective is to define the set $\mathcal{S}^{(i+1)}$ recursively.

For $t \in \{1, 2, \dots\}$, consider arbitrary t points $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)} \in \mathcal{S}^{(i)}$, such that $Q^{(k)} = \left(\pi^{(k)}, \rho^{(k)}, V^{(k)}\right)$, for $k \in \{1, 2, \dots, t\}$. Let $Q = (\pi, \rho, V') = \sum_{k=1}^{t} p^{(k)} \cdot Q^{(k)}$ be a convex linear combination of the points $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)}$.

Suppose Alice extended the partial transcript corresponding to Q into the partial transcripts corresponding to $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)}$. Then, it must be the case that $\rho = \rho^{(1)} = \rho^{(2)} = \cdots = \rho^{(t)}$. We prove that the *converse is also true*. That is, if $\rho^{(1)} = \rho^{(2)} = \cdots = \rho^{(t)}$, then Alice can extend the partial transcript corresponding to Q into the partial transcripts $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)}$. For brevity, we say *Alice fuses the points* $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)}$. Likewise, if $\pi^{(1)} = \pi^{(2)} = \dots = \pi^{(t)}$, then *Bob fuses the points* $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)}$.

Define linear maps $\varphi_1 \colon \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z \to \mathbb{R}^X$ and $\varphi_2 \colon \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z \to \mathbb{R}^Y$ as follows.

$$\varphi_1(\pi, \rho, V') \;:=\; \pi \qquad\qquad \varphi_2(\pi, \rho, V') \;:=\; \rho. \tag{5}$$

Therefore, the set $\mathcal{S}^{(i+1)}$ is recursively defined below.

For $t \in \{1, 2, \dots\}$ and any points $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)} \in \mathcal{S}^{(i)}$ satisfying

$$\varphi_1(Q^{(1)}) = \varphi_1(Q^{(2)}) = \cdots = \varphi_1(Q^{(t)}), \text{ or}$$
$$\varphi_2(Q^{(1)}) = \varphi_2(Q^{(2)}) = \cdots = \varphi_2(Q^{(t)})$$

add all possible convex linear combinations of $Q^{(1)}, Q^{(2)}, \dots, Q^{(t)}$ to the set $\mathcal{S}^{(i+1)}$.

Figure 2 assists in visualizing the evolution of the sets $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \cdots$ for our example. In our case, these sets are subsets of $\mathbb{R}^{2+2+4}$, which is challenging to visualize. Consider the projection of a point $(\pi, \rho, V') \in \mathbb{R}^{\{0,1\}} \times \mathbb{R}^{\{0,1\}} \times \mathbb{R}^{\{1,2,3,4\}}$ to (π_1, ρ_1). Figure 2 demonstrates the evolution of the set $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \cdots \to \mathcal{S}^{(4)}$ under this projection. Observe that fusing $Q^{(1)}, \dots, Q^{(t)}$ is permissible if and only if $\pi^{(1)} = \cdots = \pi^{(t)}$ or $\rho^{(1)} = \cdots = \rho^{(t)}$. When, $X = Y = \{0, 1\}$, this constraint (equivalently) becomes: fusing $Q^{(1)}, \dots, Q^{(t)}$ is permissible if and only if $\pi_1^{(1)} = \cdots = \pi_1^{(t)}$ or $\rho_1^{(1)} = \cdots = \rho_1^{(t)}$.

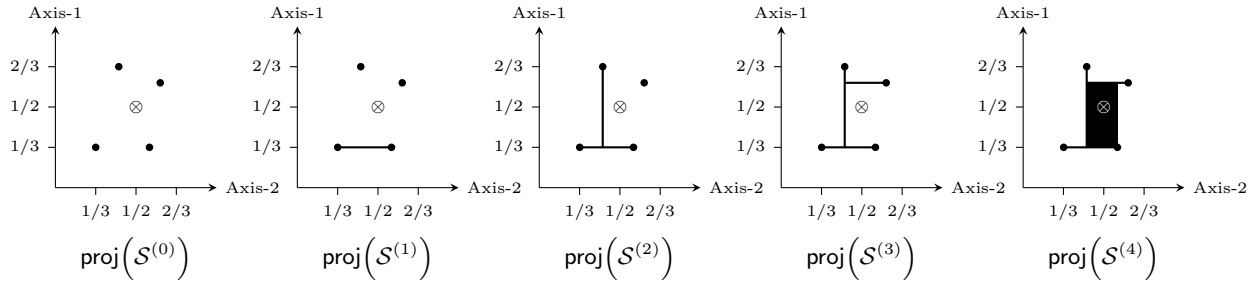


Figure 2: Plot of the projection of the points in $\mathcal{S}^{(i)}(f)$ for $0 \leqslant i \leqslant 4$. The $\otimes$ mark represents the projection of the query point $Q^{(f)}$ (defined in Equation 6), where f is defined in Figure 1. The geometric action allows joining the line segment between any two points with identical first or second coordinates.

Step 5: Protocol reconstruction. Recall that our objective is to determine whether f has an (at most) r-round protocol. The pertinent information of the empty transcript is represented by

$$Q^{(f)} \;:=\; \left(U_X, U_Y, \frac{1}{|X \times Y|} \cdot V\right) \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z, \tag{6}$$

where U_X is the uniform distribution over X, U_Y is the uniform distribution over Y, and V is the vector determined in Equation 2 of the standardization step.

In our example function, we have (refer to Equation 2 for the value of V)

$$Q^{(f)} = (\ (1/2, 1/2)\ ,\ (1/2, 1/2)\ ,\ (13/96, 5/16, 7/24, 25/96)\ ) \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z.$$

Therefore, f has an (at most) r-round protocol if and only if $Q^{(f)} \in \mathcal{S}^{(r)}$. If $Q^{(f)} \notin \mathcal{S}^{(r)}$, then the descriptions of the query point $Q^{(f)}$ and the set $\mathcal{S}^{(r)}$ are a novel geometric certificate that f does not have an r-round secure protocol. For our example, $Q^{(f)} \in \mathcal{S}^{(4)}$; however, $Q^{(f)} \notin \mathcal{S}^{(3)}$ (clear from Figure 2) – proving that our function has a 4 round protocol and 3 rounds are insufficient.

We show that every step of the inductive construction of a point $Q \in \mathcal{S}^{(i+1)}$ by fusing $Q^{(1)}, \ldots, Q^{(t)} \in \mathcal{S}^{(i)}$ translates into a protocol that extends a partial transcript corresponding to Q into partial transcripts corresponding to $Q^{(1)}, \ldots, Q^{(t)}$. These transition probabilities are determined by $\left\{p^{(k)}\right\}_{k\in\{1,2,\ldots,t\}}$ and $\left\{\pi^{(k)}\right\}_{k\in\{1,2,\ldots,t\}}$ (refer to Appendix C for the reconstruction algorithm). Using this step recursively, one recovers the protocol for f using a witness explaining the membership of the point $Q^{(f)} \in \mathcal{S}^{(r)}$.

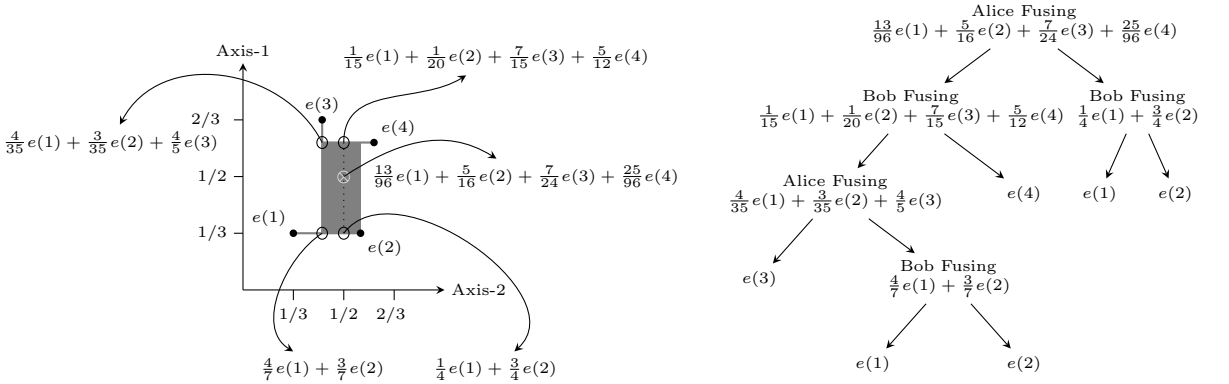


Figure 3: For the function f in Figure 1, this figure displays the payload of "critical points" in $\mathsf{proj}\left(\mathcal{S}^{(4)}\right)$. Recall that $e(1) = (1,0,0,0), e(2) = (0,1,0,0), e(3) = (0,0,1,0)$, and $e(4) = (0,0,0,1)$, the payloads of the points in the base case. Furthermore, note that $f(0,0) = \frac{13}{96}e(1) + \frac{5}{16}e(2) + \frac{7}{24}e(3) + \frac{25}{96}e(4)$. The tree presents the (shallowest tree) producing the payload from $e(1), e(2), e(3)$, and $e(4)$, generating the (unique) most efficient secure protocol for f.

For our example, let us visualize how $Q^{(f)} \in \mathcal{S}^{(4)}$. For points $(\pi, \rho, V') \in \mathbb{R}^{\{0,1\}} \times \mathbb{R}^{\{0,1\}} \times \mathbb{R}^{\{1,2,3,4\}}$ we continue to represent the projected point (π_1, ρ_1). For some critical points, we also mention the corresponding *payload* $V' \in \mathbb{R}^{\{1,2,3,4\}}$. Figure 3 demonstrates the witness of $Q^{(f)} \in \mathcal{S}^{(4)}$.

Challenges in Generalization. The presentation above relies on all probabilities $f(x,y)_z$ being positive. Generalizing to arbitrary f requires some modifications to definitions of pertinent information (specifically, refer to Equation 3, which risks "division by 0 concerns"). Appendix B presents the full proof of our result.

Functions with an arbitrarily high round complexity. Fix any $r \in \{1, 2, \ldots\}$. We show that there are functions $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ such that a secure protocol for f must have r rounds. In our example $|Z| = (r+1)$. The idea is to construct $\mathcal{S}^{(0)}$ such that the query point $Q^{(f)} = (1/2, 1/2, \cdot) \notin \mathcal{S}^{(r-1)}$, proving Lemma 7. Appendix D presents this function construction.

Modification: Addressing communication complexity. In the geometric problem, bounding $t \leqslant 2$ in the recursive definition ensures that $Q^{(f)} \in \mathcal{S}^{(c)}$ if and only if f has an (at most) c-bit secure protocol.

Remark: our novel perspective on security. Existing approaches analyze the (forwards) evolution of secure protocol over time – characterizing what safe information they can potentially reveal at any point in time. In contrast, we begin from a fully evolved state of a secure protocol and look back in time, characterizing all possible states that can lead the protocol to these final states. This difference in perspective is highlighted by comparing (1) Figure 7: Evolution of the secure protocol for Dutch auction as proposed by Kushilevitz [Kus89] and (2) Figure 8: Searching for the secure protocol for the Dutch auction using our perspective.

4 Cryptographic Reduction

Suppose we are investigating the round/communication complexity of a general (two-party) secure function evaluation. If this function has Kilian's obstruction [Kil91, Kil00], there is no secure protocol. However, avoiding Kilian's obstruction *does not* imply the existence of a secure protocol (for example, the famous Kushilevitz function of Figure 9 and the recent binary-input randomized function of Figure 13). If the function avoids Kilian's obstruction, then studying its round/communication complexity is equivalent to studying the round/communication complexity of a related standardized SSFE. Appendix H (following [MPR13, DP18]) provides additional details on this argument.

Consequently, without loss of generality, consider a standardized function $f\colon X \times Y \to \mathbb{R}^Z$ defined in step 0 of Section 3. Let $A \in \mathbb{R}^{X\times Z}, B \in \mathbb{R}^{Y\times Z}, V \in \mathbb{R}^Z$ be the appropriate vectors. Define $Q^{(f)}$ as in Equation 6. For every $z \in Z$, define $P^{(z)}$ as in Equation 4. Define the linear maps φ_1, φ_2 as in Equation 5.

Round Complexity. Initialize the set $\mathcal{S}^{(0)} := \left\{P^{(z)}\colon z \in Z\right\}$. For every $i \in \{0,1,\dots\}$, recursively define

$$\mathcal{S}^{(i+1)} := \left\{ \sum_{k=1}^{t} p^{(k)} \cdot Q^{(k)} \colon \begin{array}{c} t \in \{1,2,\dots\}, Q^{(1)}, Q^{(2)}, \dots, Q^{(t)} \in \mathcal{S}^{(i)} \\ p^{(1)}, p^{(2)}, \dots, p^{(t)} \geqslant 0, \sum_{k=1}^{t} p^{(k)} = 1 \\ \varphi_1(Q^{(1)}) = \cdots = \varphi_1(Q^{(t)}) \text{ or } \varphi_2(Q^{(1)}) = \cdots = \varphi_2(Q^{(t)}) \end{array} \right\} \tag{7}$$

The following statements hold.

1. An r-round semi-honest secure protocol for f exists if and only if $Q^{(f)} \in \mathcal{S}^{(r)}$.
2. Given a witness for $Q^{(f)} \in \mathcal{S}^{(r)}$ one can construct an (at most) r-round secure protocol for f.
3. The descriptions of $Q^{(f)}$ and the set $\mathcal{S}^{(r)} \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z$ are a geometric obstruction for r-round secure protocols for f when $Q^{(f)} \notin \mathcal{S}^{(r)}$.

Communication Complexity. Initialize the set $\mathcal{T}^{(0)} := \left\{P^{(z)}\colon z \in Z\right\}$. For every $i \in \{0,1,\dots\}$, recursively define

$$\mathcal{T}^{(i+1)} := \left\{ p^{(1)} \cdot Q^{(1)} + p^{(2)} \cdot Q^{(2)} \colon \begin{array}{c} Q^{(1)}, Q^{(2)} \in \mathcal{T}^{(i)} \\ p^{(1)}, p^{(2)} \geqslant 0, p^{(1)} + p^{(2)} = 1 \\ \varphi_1(Q^{(1)}) = \varphi_1(Q^{(2)}) \text{ or } \varphi_2(Q^{(1)}) = \varphi_2(Q^{(2)}) \end{array} \right\} \tag{8}$$

The following statements hold.

1. An c-bit semi-honest secure protocol for f exists if and only if $Q^{(f)} \in \mathcal{T}^{(c)}$.

2. Given a witness for $Q^{(f)} \in \mathcal{T}^{(c)}$ one can construct an (at most) c-bit secure protocol for f.

3. The descriptions of $Q^{(f)}$ and the set $\mathcal{T}^{(c)} \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z$ are a geometric obstruction for c-bit secure protocols for f when $Q^{(f)} \notin \mathcal{T}^{(c)}$.

What remains? Since t is unbounded in the recursive definition of the set $\mathcal{S}^{(i+1)}$, it is unclear whether one can test $Q^{(f)} \in \mathcal{S}^{(r)}$. Section 5 upper bounds t in the recursive definition of $\mathcal{S}^{(i+1)}$. Subsequently, Section 6 demonstrates that membership testing, witness extraction, and the descriptions of the sets $\mathcal{S}^{(i)}$ and $\mathcal{T}^{(i)}$ are finite.

Proof overview of Theorem 1 and Theorem 2. Theorem 1 follows as a consequence of (a) the reduction of the round complexity problem to the geometric problem in this section, (b) the upper bound on t in the recursive definition of $\mathcal{S}^{(i+1)}$ in Section 5, and (c) Theorem 3 proving the tameness of the $\mathcal{S}^{(i)}$ sets. Theorem 2 follows as a consequence of (a) the reduction of the communication complexity problem to the geometric problem in this section and (b) Theorem 3 proving the tameness of the $\mathcal{T}^{(i)}$ sets.

5 Interlude: Bounding Complexity

Consider Equation 7. Define $d := |X| + |Y| + |Z|$. Let Q be a convex linear combination of $\left\{Q^{(k)}\right\}_{k\in\{1,2,\ldots,t\}}$, where $t \geqslant d+1$, such that $\varphi_b(Q^{(1)}) = \cdots = \varphi_b(Q^{(t)})$, for some $b \in \{1,2\}$. Carathéodory's theorem [Car11] states that there are $1 \leqslant i_1 < i_2 < \cdots < i_\ell \leqslant t$, where $1 \leqslant \ell \leqslant d+1$, such that Q is a convex linear combination of $Q^{(i_1)}, Q^{(i_2)}, \ldots, Q^{(i_\ell)}$. Furthermore, $\varphi_b\left(Q^{(i_1)}\right) = \cdots = \varphi_b\left(Q^{(i_\ell)}\right)$. Consequently, it suffices to consider $t \in \{1, 2, \ldots, d+1\}$ in Equation 7.

For the specific φ_1 and φ_2 being considered in Section 4 we can obtain a slightly better upper bound on t, whence the following corollary. Appendix J proves this corollary.

Corollary 1. *If the function $f\colon X \times Y \to \mathbb{R}^Z$ has an r-round semi-honest secure protocol then there is an r-round protocol where every message sent by Alice requires (at most) $\lceil \lg(|X| + |Z|) \rceil$ bits, and every message sent by Bob requires (at most) $\lceil \lg(|Y| + |Z|) \rceil$ bits.*

6 Real Algebraic Geometry Problem: Generalized Convex Hulls

In this section we consider only recursively generated sets $\left\{\mathcal{S}^{(i)}\right\}_{i\in\{0,1,\ldots\}}$, which suffice to prove the bounds on $\left\{\mathcal{T}^{(i)}\right\}_{i\in\{0,1,\ldots\}}$. Let $\varphi\colon \Omega \to \Omega'$ be an arbitrary function. The *fibre product* $\underbrace{\Omega \times_\varphi \Omega \times_\varphi \cdots \times_\varphi \Omega}_{\ell\text{-times}} := \left\{(\omega_1, \omega_2, \ldots, \omega_\ell)\colon \omega_1, \ldots, \omega_\ell \in \Omega, \varphi(\omega_1) = \cdots = \varphi(\omega_\ell)\right\}$.

Our ambient space is $\mathbb{R}^d$, where $d \in \{2, 3, \ldots\}$. Let $\varphi_1, \varphi_2\colon \mathbb{R}^d \to \mathbb{R}^{d'}$ be two linear maps, where $d' \in \{1, 2, \ldots\}$. Let $\mathcal{S}^{(0)} \subseteq \mathbb{R}^d$ be an arbitrary initial set of points. Define

$$\Lambda^{(d)} = \left\{\left(p^{(1)}, p^{(2)}, \ldots, p^{(d+1)}\right) : p^{(1)}, p^{(2)}, \ldots, p^{(d+1)} \geqslant 0, \text{ and } p^{(1)} + p^{(2)} + \ldots + p^{(d+1)} = 1\right\}.$$

Define the bilinear map $\langle\cdot,\cdot\rangle : \left(\mathbb{R}^d\right)^{d+1} \times \mathbb{R}^{d+1} \to \mathbb{R}^d$ as follows.

$$\left\langle\left(Q^{(1)}, Q^{(2)}, \ldots, Q^{(d+1)}\right), \left(p^{(1)}, p^{(2)}, \ldots, p^{(d+1)}\right)\right\rangle := \sum_{k=1}^{d+1} p^{(k)} \cdot Q^{(k)}.$$

For $i \in \{0, 1, \dots\}$, inductively define

$$\mathcal{S}^{(i+1)} = \left\langle \underbrace{\mathcal{S}^{(i)} \times_{\varphi_1} \mathcal{S}^{(i)} \times_{\varphi_1} \cdots \times_{\varphi_1} \mathcal{S}^{(i)}}_{(d+1)\text{-times}}, \Lambda^{(d)} \right\rangle \bigcup \left\langle \underbrace{\mathcal{S}^{(i)} \times_{\varphi_2} \mathcal{S}^{(i)} \times_{\varphi_2} \cdots \times_{\varphi_2} \mathcal{S}^{(i)}}_{(d+1)\text{-times}}, \Lambda^{(d)} \right\rangle.$$

Before we proceed, we remark that, if φ_1, φ_2 are relaxed to be arbitrary functions, then one can construct "ill-behaved" functions to ensure testing membership in $\mathcal{S}^{(i)}$ is undecidable. Therefore, the result below crucially relies on the fact that φ_1, φ_2 are "well-behaved", and also that the initial set $\mathcal{S}^{(i)}$ is tame (at least semi-algebraic). We recall here that a semi-algebraic (resp. semi-linear) subset of $\mathbb{R}^d$ is any subset that be defined by a Boolean formula with atoms of the form $P > 0, P = 0$, where $P \in R[X_1, \dots, X_k]$ (resp. with $\deg(P) \leqslant 1$).

Theorem 3. *Let $d \in \{2, 3, \dots\}$, $d' \in \{1, 2, \dots\}$, $\varphi_1, \varphi_2 \colon \mathbb{R}^d \to \mathbb{R}^{d'}$ be linear maps, $\mathcal{S}^{(0)} \subseteq \mathbb{R}^d$ a semi-algebraic subset, and $r \in \{0, 1, \dots\}$. Given a query point $Q \in \mathbb{R}^d$, the problem of determining whether $Q \in \mathcal{S}^{(r)}$ or not is decidable. Moreover, if $Q \in \mathcal{S}^{(r)}$, there exists an algorithm which outputs a witness tree, whose nodes are labelled by points in $\mathbb{R}^d$, and edges labelled by real numbers in $[0, 1]$ satisfying the following property:*

1. *The root node is labelled by Q;*
2. *each leaf node is labelled by a point in $\mathcal{S}^{(0)}$;*
3. *a node at height i is labelled by a point $\mathbf{x} \in \mathcal{S}^{(i)}$, and it has $(d+1)$ children each of which is labelled by points $\mathbf{y}^{(1)}, \dots, \mathbf{y}^{(d+1)} \in \mathcal{S}^{(i-1)}$, with the corresponding edges labelled by $p_1, \dots, p_{d+1} \in [0, 1]$, such that*

$$p_1 + \cdots + p_{d+1} = 1,$$
$$\mathbf{x} = p_1 \mathbf{y}^{(1)} + \cdots + p_{d+1} \mathbf{y}^{(d+1)}.$$

Moreover, the complexities of the decision problem and of the algorithm producing the witness tree are bounded by $(Nd)^{d^{\mathcal{O}(r)}}$, where N is the size of a quantifier-free formula describing the semi-algebraic set $\mathcal{S}^{(0)}$ measured by the product of the number of polynomials appearing in it and the maximum degree of these polynomials.

Proof. We will use the fact that the first order theory of the reals is decidable. Let $\Phi_0(\mathbf{X})$, where $\mathbf{X} = (X_1, \dots, X_d)$ denote the formula in the language of the first order theory of reals whose realization is the set $\mathcal{S}^{(0)} \subseteq \mathbb{R}^d$. Now, for $i > 0$, we will inductively define a formula $\Phi_i(\mathbf{X})$ whose realization is $\mathcal{S}^{(i)} \subseteq \mathbb{R}^d$. Suppose, $\Phi_{i-1}(\mathbf{X})$ has already being defined. We define $\Phi_i(\mathbf{X})$ as follows.

$$\Phi_i(\mathbf{X}) := \Phi_{i,1}(\mathbf{X}) \vee \Phi_{i,2}(\mathbf{X}),$$

where for $j = 1, 2$,

$$\Phi_{i,j}(\mathbf{X}) := (\exists \mathbf{Z})(\exists \mathbf{Y}^{(1)}) \cdots (\exists \mathbf{Y}^{(d+1)}) \Theta_1 \ \wedge \ \Theta_{2,j} \ \wedge \ \Theta_3$$

where

$$\begin{aligned} \mathbf{Y}^{(k)} &= (Y_1^{(k)}, \dots, Y_d^{(k)}), 1 \leqslant k \leqslant d+1, \\ \mathbf{Z} &= (Z_1, \dots, Z_{d+1}), \end{aligned}$$

and

$$\begin{aligned}
\Theta_1 &:= \bigwedge_{k=1}^{d+1} \Phi_{i-1}(\mathbf{Y}^{(k)}), \\
\Theta_{2,j} &:= \bigwedge_{k=1}^{d} \left(\phi_j(\mathbf{Y}^{(k)}) = \phi_j(\mathbf{Y}^{(k+1)})\right), \\
\Theta_3 &:= \bigwedge_{\ell=1}^{d} \left(\sum_{k=1}^{d+1} Z_k \cdot Y_\ell^{(k)} = X_\ell\right).
\end{aligned}$$

It is clear from the definition of Φ_i, that the realization of Φ_i in $\mathbb{R}^d$ equals $\mathcal{S}^{(i)} \subseteq \mathbb{R}^d$.

Note that each Φ_i is an (existential) formula in the first order theory of the reals. Using the Tarski-Seidenberg theorem there exists a quantifier-free formula $\Psi_i(\mathbf{X})$ (i.e. a quantifier-free Boolean formula whose atoms are polynomial equalities and inequalities) which is equivalent to Φ_i (i.e. their realizations in $\mathbb{R}^d$ are equal). Moreover, there exists effective algorithms to compute Ψ_i from Φ_i, which yields a procedure to check membership in $\mathcal{S}^{(i)} \subseteq \mathbb{R}^d$ since the truth of the formula Ψ_i can be decided directly given a point in $\mathbb{R}^d$ as input since it has no quantifiers.

The number N_r of existentially quantified variables in the formula Φ_r satisfies the recurrence

$$\begin{aligned}
N_r &= r(d+1)^2 + (d+1)N_{r-1}, \\
N_0 &= 0.
\end{aligned}$$

Hence,

$$N_r = r(d+1)^2 + (r-1)(d+1)^3 + \cdots = d^{\mathcal{O}(r)}.$$

The degrees of the polynomials appearing in Φ_r is bounded by $\max(2, N)$, and the number of polynomials is bounded by $Nd^{\mathcal{O}(r)}$. Using the effective version of quantifier-elimination in the theory of real closed field (see for instance [BPRon, Algorithm 14.5]), the complexity of computing Ψ_r, and also of deciding membership in $\mathcal{S}^{(r)}$ is bounded by

$$\left(Nd^{\mathcal{O}(r)}\right)^{d^{\mathcal{O}(r)}} = (Nd)^{d^{\mathcal{O}(r)}}.$$

In order to compute the witness tree, we observe that the formula $\Phi_r(Q)$ is an existential sentence. Using the algorithm for computing sample points ([BPRon, Theorem 13.22]) which is an intermediate step in the algorithm for deciding the existential theory of reals, it is possible to obtain a tuple of witness points and the corresponding probabilities giving the edge weights using the structure of the existential sentence Φ_r. These corresponds to the existentially quantified variables $\mathbf{Y}^{(i)}$'s giving the labels of the nodes in the witness tree, and the variables Z_i's giving the edge weights. Note that these are produced as real algebraic numbers whose descriptions are output as Thom encodings (see [BPRon, page 42] and Remark 1 below). □

Remark 1. *If in Theorem 3, we assumed that the initial set $\mathcal{S}^{(0)}$ is in fact a semi-linear set (for example, a finite set of points), then it is possible to show that each $\mathcal{S}^{(i)}$ remains a semi-linear set, and the points appearing in the witness tree can be chosen to be have coordinates which are rational in the coefficients of the at most linear polynomials defining $\mathcal{S}^{(0)}$.*

Starting from [CK89, Kus89], all works in this research area consider the functions to be constant-size, i.e., the sets X, Y, Z have constant size. Consequently, all parameters in the proof above are constants.

7 Future Research Directions

Our technical approach arises from a significantly different perspective on how security manifests in (private-coin) interactive protocols. The objective of this work is to introduce this new perspective via its application to a foundational (and long-standing open) problem, and develop technical tools to reason about the search space of all possible candidate (private-coin) protocols. Consequently, our work focuses on perfect security against honest-but-curious adversaries in the two-party setting. Our technical contribution identifies the new notion of generalized convex hulls, which is a fascinating new problem in mathematics (refer to Appendix I). We mention some additional representative potential research directions building upon our technical contributions below.

1. Specific to our problem setting, we conjecture that if $f\colon X \times Y \to \mathbb{R}^Z$ has a secure protocol, then there is a *canonical secure protocol* with round complexity $\mathcal{O}\left(|Z|^2\right)$ and communication complexity $\mathcal{O}\left(\log|X| + \log|Y| + |Z|^2\right)$. We emphasize that this bound is *independent* of the probabilities involved in defining the computation f. We foresee that resolving these conjectures shall involve understanding Carathéodory/Helly-numbers of collections of appropriate sets. Furthermore, we conjecture that if f *does not have a perfectly secure protocol*, then any protocol for f must be constant-insecure.

2. In the two-party setting, the characterization of computations with randomized output that are (standalone) securely realizable against a malicious adversary is another long-standing open problem (refer to [MPR13]).

3. Extending our technical framework to the multi-party setting, where honest parties are *not in the majority*, is another natural research direction. In this setting, incorporating the communication infrastructure presents unique challenges; for example, considering budgets on broadcast channels, point-to-point communication channels, and the topology of the framework is non-trivial.

4. Another fascinating research direction in the multi-party setting is determining the *randomness complexity* of secure protocols [KOR96, KOP+19]. For example, can we determine the randomness complexity of securely computing AND and XOR of parties' private bits? Our technical approach demonstrates the possibility of obtaining the optimal protocol by exhaustive search techniques.

5. There are several (practically and theoretically well-motivated) analytically-tractable secure computations models like the *private simultaneous message* (PSM) [FKN94], *randomizing polynomial/randomized encoding* [IK00, IK02, AIK04], *conditional disclosure of secrets* [GIKM98], and *OT-complexity* [BM04]. Our techniques have the potential of providing new insights and technical approaches to determine the efficiency of computations in these models.

A Notation

We have some conventions in our notation throughout the paper. A functionality f with input domain $X \times Y$ is *deterministic* if for all $x \in X, y \in Y$, the function f always outputs a unique value. In this case, we represent the function with output space Z. So for a deterministic function $f\colon X \times Y \to Z$, we denote $f(x,y)$ as the output value on input (x,y).

A functionality f is *randomized* if on input $(x,y) \in X \times Y$ it outputs $z \in Z$ with some probability. We represent this function as $f\colon X \times Y \to \mathbb{R}^Z$. The notation $f(x,y) \in \mathbb{R}^Z$ represents the output distribution over Z on input (x,y), and $f(x,y)_z$ is the probability that the output is z conditioned on input being (x,y). This representation is also well-defined for deterministic functions. Let us give an example for the MAX function (a.k.a., the Dutch auction) with input domain $\{1,3\} \times \{2,4\}$. Using notation for deterministic, $\mathrm{MAX}\colon \{1,3\} \times \{2,4\} \to \{2,3,4\}$ satisfying

$$\mathrm{MAX}(1,2) = 2,\ \mathrm{MAX}(1,4) = 4,\ \mathrm{MAX}(3,2) = 3,\ \mathrm{MAX}(3,4) = 4.$$

Using notation for randomized, $\mathrm{MAX}\colon \{1,3\} \times \{2,4\} \to \mathbb{R}^4$ satisfying

$$\mathrm{MAX}(1,2) = (0,1,0,0),\ \mathrm{MAX}(1,4) = (0,0,0,1),\ \mathrm{MAX}(3,2) = (0,0,1,0),\ \mathrm{MAX}(3,4) = (0,0,0,1).$$

The secure protocol for MAX is the Dutch auction mechanism. Bob announces whether he his input is 4 or not. If not, then Alice announces whether she her input is 3 or not. If not, then Bob announces whether his input is 2 or not.

B Proof of Cryptographic Reduction

Let Π be a two-party protocol with private inputs $x \in X$ and $y \in Y$. For a partial transcript τ of the protocol Π, let $\pi^{(\tau)} \in \mathbb{R}^X$ represent the conditional distribution of Alice's input conditioned on Π generating the partial transcript τ when parties start with x drawn uniformly at random from X and y drawn uniformly at random from Y. Similarly, define the conditional distribution $\rho^{(\tau)} \in \mathbb{R}^Y$ of Bob's input.

Lemma 1. *Suppose a function $f\colon X \times Y \to \mathbb{R}^Z$ is maximally renamed and avoids Kilian's obstruction. Then, there are* unique *$A \in \mathbb{R}^X \times \mathbb{R}^Z$, $B \in \mathbb{R}^Y \times \mathbb{R}^Z$, and $V \in \mathbb{R}^Z$ such that the following identities hold.*

$$\begin{aligned} f(x,y) &= A_x * B_y * V \text{ for every } x \in X, y \in Y, \\ \sum_{x \in X} A_{x,z} &= 1 \text{ for every } z \in Z, \text{and} \\ \sum_{y \in Y} B_{y,z} &= 1 \text{ for every } z \in Z. \end{aligned}$$

Proof. Since f is maximally renamed and avoids Kilian's obstruction, it satisfies the strict cross product rule. This implies that, for each fixed $z \in Z$, the matrix $\{f(x,y)_z\}_{x,y} \in \mathbb{R}^{X \times Y}$ is rank one. By Proposition 1, there exist column vectors $u_z \in \mathbb{R}^X$ and $v_z \in \mathbb{R}^Y$ such that $\{f(x,y)_z\}_{x,y} = u_z \cdot v_z^T$, and u_z, v_z are non-zero vectors. For each $x \in X$ and $y \in Y$, let $A_x = ((u_z)_x\colon z \in Z)$ (or in other words the z^{th} column of matrix A is vector u_z) and $B_y = ((v_z)_y\colon z \in Z)$ (or in other words the z^{th} column of matrix B is v_z). Then, it holds that

$$f(x,y)_z = (u_z)_x \cdot (v_z)_y = A_{x,z} \cdot B_{y,z}.$$

Next, we normalize the matrix A and B so that the sum of elements in any column of A or B is 1, that is,

$$A_{x,z} \text{ is updated to } \frac{A_{x,z}}{\sum_x A_{x,z}}, \text{and } B_{y,z} \text{ is updated to } \frac{B_{y,z}}{\sum_x B_{y,z}}.$$

Observe that if $\sum_x A_{x,z} = 0$, then $f(x,y)_z = 0$, which is impossible for non-redundant output space. Therefore, the normalization step is always possible since $\sum_x A_{x,z} \neq 0$ and $\sum_y B_{y,z} \neq 0$. It is easy to see that there exists a unique $V \in \mathbb{R}^Z$, that is, each V_z is set to be 1 by the product of the two corresponding normalizing factors, such that

$$f(x,y)_z = A_{x,z} \cdot B_{y,z} \cdot V_z \text{ for every } x \in X, y \in Y, \text{ and } z \in Z.$$

This implies that $f(x,y) = A_x * B_y * V$ as desired. □

Proposition 1. *Let A be a matrix of size $m \times n$. Then, A is a rank one matrix if and only if there exist vectors u of size $m \times 1$ and v of size $n \times 1$ such that $A = u \cdot v^T$.*

Proposition 2. *For random variables X, Y, Z defined respectively over $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$, the Markov chain $X - Y - Z$ holds if and only if there exist functions $r\colon \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$ and $s\colon \mathcal{Y} \times \mathcal{Z} \to \mathbb{R}$ such that for each y that $\Pr[y] > 0$, we have $\Pr[x,y,z] = r(x,y) \times s(y,z)$.*

Lemma 2. *Suppose the environment chooses $x \in X$ and $y \in Y$ uniformly and independently at random. Then, for any partial transcript τ, the following identity holds.*

$$\Pr[x,y|\tau] = \pi_x^{(\tau)} \cdot \rho_y^{(\tau)}.$$

Proof. Let $\tau = (\tau_1, \ldots, \tau_r)$ denote the partial transcript such that τ_i denotes the message sent in round i. Without loss of generality, we assume that r is even and Alice sends messages $\tau_1, \tau_3, \ldots, \tau_{r-1}$ and Bob sends messages $\tau_2, \tau_4, \ldots, \tau_r$. In any round, the person who is going to send a message, chooses their message as a function of their private randomness, and their input and the partial transcript seen so far. This implies that $\Pr[\tau_j|x,y,\tau_{\leqslant j-1}] = \Pr[\tau_j|x,\tau_{\leqslant j-1}]$ whenever $j \in \{1,3,\ldots,r-1\}$ and $\Pr[\tau_j|x,y,\tau_{\leqslant j-1}] = \Pr[\tau_j|y,\tau_{\leqslant j-1}]$ whenever $j \in \{2,4,\ldots,r\}$. Since X and Y are independent, it follows from the chain rule that:

$$\begin{aligned}
\Pr[x,\tau,y] &= \Pr[x,y]\Pr[\tau_1|x,y]\Pr[\tau_2|\tau_1,x,y]\ldots\Pr[\tau_{r-1}|\tau_{\leqslant r-2},x,y]\Pr[\tau_r|\tau_{\leqslant r-1},x,y] \\
&= \Pr[x]\Pr[y]\Pr[\tau_1|x]\Pr[\tau_2|\tau_1,y]\ldots\Pr[\tau_{r-1}|\tau_{\leqslant r-2},x]\Pr[\tau_r|\tau_{\leqslant r-1},y] \\
&= r(x,\tau)\cdot s(y,\tau)
\end{aligned}$$

where

$$\begin{aligned}
r(x,\tau) &:= \Pr[x]\Pr[\tau_1|x]\Pr[\tau_3|\tau_{\leqslant 2},x]\ldots,\Pr[\tau_{r-1}|\tau_{\leqslant r-2},x] \\
s(x,\tau) &:= \Pr[y]\Pr[\tau_2|\tau_1,y]\Pr[\tau_4|\tau_{\leqslant 3},y]\ldots\Pr[\tau_r|\tau_{\leqslant r-1,y}].
\end{aligned}$$

Therefore, it follows from Proposition 2 that the Markov chain $X - T - Y$ holds which implies that for any x, y, τ it holds that $\Pr[x,y|\tau] = \Pr[x|\tau] \cdot \Pr[y|\tau] = \pi_x^{(\tau)} \cdot \rho_y^{(\tau)}$. □

Lemma 3. *For any partial transcript τ, let Ω represent the set of all one-round extension of τ. For $\tau' \in \Omega$, let $\lambda_{\tau'} = \Pr[\tau'|\tau]$ define a probability distribution over Ω. The following identities hold.*

1. $$\left(\pi^{(\tau)}, \rho^{(\tau)}\right) = \sum_{\tau' \in \Omega} \lambda_{\tau'} \cdot \left(\pi^{(\tau')}, \rho^{(\tau')}\right).$$

2. *If Bob extends the partial transcript τ, then $\pi^{(\tau)} = \pi^{(\tau')}$, for all $\tau' \in \Omega$. Analogously, if Alice extends the partial transcript τ, then $\rho^{(\tau)} = \rho^{(\tau')}$, for all $\tau' \in \Omega$.*

Proof. We shall first show that $\pi^{(\tau)} = \sum_{\tau' \in \Omega} \lambda_{\tau'} \cdot \pi^{(\tau')}$. By Bayes' rule, for any $x \in X$, we have

$$\pi_x^{(\tau)} = \Pr[x|\tau] = \sum_{\tau' \in \Omega} \Pr\big[x, \tau'|\tau\big] = \sum_{\tau' \in \Omega} \Pr\big[x|\tau, \tau'\big] \cdot \Pr\big[\tau'|\tau\big] = \sum_{\tau' \in \Omega} \Pr\big[x|\tau'\big] \cdot \Pr\big[\tau'|\tau\big] = \sum_{\tau' \in \Omega} \lambda_{\tau'} \cdot \pi_x^{(\tau')}.$$

This implies that $\pi^{(\tau)} = \sum_{\tau' \in \Omega} \lambda_{\tau'} \cdot \pi^{(\tau')}$. Similarly, it holds that $\rho^{(\tau)} = \sum_{\tau' \in \Omega} \lambda_{\tau'} \cdot \rho^{(\tau')}$.

Suppose Bob extends the partial transcript τ and sends a message m to Alice. Let $\tau' = (\tau, m)$. Observe that the message m is independent from x. Therefore, we have

$$\pi_x^{(\tau')} \overset{\text{(i)}}{=} \Pr\big[x|\tau'\big] \overset{\text{(ii)}}{=} \Pr[x|\tau, m] \overset{\text{(iii)}}{=} \frac{\Pr[x, m|\tau]}{\Pr[m|\tau]} \overset{\text{(iv)}}{=} \frac{\Pr[m|\tau, x] \cdot \Pr[x|\tau]}{\Pr[m|\tau]} \overset{\text{(v)}}{=} \frac{\Pr[m|\tau] \cdot \Pr[x|\tau]}{\Pr[m|\tau]} \overset{\text{(vi)}}{=} \pi_x^{(\tau)}.$$

In above, equality (i) is due to the definition of $\pi_x^{(\tau')}$, equality (ii) is due to the definition of τ', equality (iii) is due to the definition of conditional probability, equality (iv) is due to chain rule, equality (v) is due to the fact that the conditional distribution of message sent by Bob condition on the transcript seen so far is independent of Alice's input, equality (vi) is due to the definition of $\pi_x^{(\tau)}$.

This implies that $\pi^{(\tau)} = \pi^{(\tau')}$. With an analogous argument, one concludes that if Alice extends the partial transcript τ, then $\rho^{(\tau)} = \rho^{(\tau')}$, for all $\tau' \in \Omega$.

□

Lemma 4. *In a secure protocol, for a complete transcript τ, with associated output $z \in Z$, the following identities hold.*

1. *For any $x \in X$, we have $\pi_x^{(\tau)} = A_{x,z}$.*
2. *For any $y \in Y$, we have $\rho_y^{(\tau)} = B_{y,z}$.*

Proof. We first introduce some notation. Let $\mathbb{Z}_{\Pi,A}$, and $\mathbb{Z}_{\Pi,B}$ denote respectively the output of Alice and Bob in the protocol Π. It follows from the definition of security that $\mathbb{Z}_{\Pi,A} = \mathbb{Z}_{\Pi,B}$, so we use random variable $\mathbb{Z}_\Pi$ to denote both $\mathbb{Z}_{\Pi,A}$, and $\mathbb{Z}_{\Pi,B}$. Let $\mathbb{Z}_f$ denote the output of functionality f in the ideal world. Let $\mathbb{S}_A(x, z)$ denote the output of Alice's simulator. We define Bob's simulator $\mathbb{S}_B(y, z)$ similarly. We also use $\mathbb{T}$ to denote the transcript. It follows from the security definition that for any $x \in X$ and $y \in Y$, the joint distribution $(x, y, \mathbb{Z}_f, \mathbb{S}_B(y, z))$ is the same as the joint distribution $(x, y, \mathbb{Z}_{\Pi,A}, \mathbb{T})$. This implies that for any y, z, τ that $\Pr[\mathbb{Y} = y, \mathbb{Z}_A = z, \mathbb{T} = \tau] > 0$, we have:

$$\Pr[\mathbb{X} = x|\mathbb{Y} = y, \mathbb{Z}_f = z, \mathbb{S}_B(y, z) = \tau] = \Pr[\mathbb{X} = x|\mathbb{Y} = y, \mathbb{Z}_\Pi = z, \mathbb{T} = \tau] \tag{9}$$

Since $\Pr[\mathbb{Y} = y, \mathbb{Z}_A = z, \mathbb{T} = \tau] > 0$, we have $\Pr[\mathbb{Y} = y, \mathbb{Z}_f = z] > 0$, and so $B_{y,z} > 0$. We can rewrite the left hand side of Equation 9 as follows:

$$\begin{aligned}\Pr[\mathbb{X} = x|\mathbb{Y} = y, \mathbb{Z}_f = z, \mathbb{S}_B(y, z) = \tau] &= \Pr[\mathbb{X} = x|\mathbb{Y} = y, \mathbb{Z}_f = z] \\ &= \frac{A_{x,z}B_{y,z}}{\sum_x A_{x,z}B_{y,z}} = \frac{A_{x,z}}{\sum_x A_{x,z}}\end{aligned}$$

Since $\mathbb{Z}_\Pi$ is a deterministic function of $\mathbb{T}$, the Markov chain $\mathbb{X} - \mathbb{T} - \mathbb{Z}_\Pi$ holds and the Markov property $\mathbb{X} - \mathbb{T} - \mathbb{Y}$, mentioned in Lemma 2, implies that the Markov chain $\mathbb{X} - (\mathbb{T}, \mathbb{Z}_\Pi) - \mathbb{Y}$ holds. Now, we can simplify the right hand side of Equation 9 as follows:

$$\Pr[\mathbb{X} = x | \mathbb{Y} = y, \mathbb{Z}_\Pi = z, \mathbb{T} = \tau] = \Pr[\mathbb{X} = x | \mathbb{Z}_\Pi = z, \mathbb{T} = \tau] = \Pr[\mathbb{X} = x | \mathbb{T} = \tau] = \pi_x^{(\tau)}$$

Therefore, we have $\pi_x^{(\tau)} = A_{x,z} / \sum_x A_{x,z} = A_{x,z}$ since $\sum_x A_{x,z} = 1$. Similarly, it holds that $\rho_y^{(\tau)} = B_{y,z}$. □

Let us introduce some notation that is needed for our next lemma. The support of the pre-image of a functionality f at output z is defined as

$$\mathrm{Supp}\big(f^{-1}(z)\big) \;:=\; \{(x,y) \in X \times Y \colon \Pr[f(x,y) = z] > 0\}.$$

The support of the product distribution $\pi^{(\tau)} \times \rho^{(\tau)}$ is defined as

$$\mathrm{Supp}\Big(\pi^{(\tau)} \times \rho^{(\tau)}\Big) = \{(x,y) \in X \times Y \colon \pi_x^{(\tau)} > 0, \rho_y^{(\tau)} > 0\}.$$

Lemma 5. *For any partial transcript τ, we define $A^{(\tau)} \in \mathbb{R}^X \times \mathbb{R}^Z$, $B^{(\tau)} \in \mathbb{R}^Y \times \mathbb{R}^Z$, and $V^{(\tau)} \in \mathbb{R}^Z$ as follows.*

1. $A_x^{(\tau)} = \begin{cases} A_x / \pi_x^{(\tau)} & \text{if } \pi_x^{(\tau)} > 0, \\ \mathbf{0} & \text{otherwise.} \end{cases}$
2. $B_y^{(\tau)} = \begin{cases} B_y / \rho_y^{(\tau)} & \text{if } \rho_y^{(\tau)} > 0, \\ \mathbf{0} & \text{otherwise.} \end{cases}$
3. $V^{(\tau)} = \begin{cases} e(z) & \text{if } \tau \text{ is a complete transcript,} \\ \sum_{\tau' \in \Omega} \lambda_{\tau'} \cdot V^{(\tau')} & \text{otherwise.} \end{cases}$

Then, the following statements hold.

1. $f^{(\tau)} \equiv \big(A^{(\tau)}, B^{(\tau)}, V^{(\tau)}\big)$.
2. *If* $V_z^{(\tau)} > 0$, *then* $\mathrm{Supp}\big(f^{-1}(z)\big) \subseteq \mathrm{Supp}\big(\pi^{(\tau)} \times \rho^{(\tau)}\big)$.

Proof. We first note that the definitions of $A^{(\tau)}, B^{(\tau)}$, and $V^{(\tau)}$ are well-defined. We proceed by induction on the height of τ in a bottom-up fashion.

Base case. Let τ denote a complete transcript. Since τ is a complete transcript, the correctness of the protocol requires that the outputs of Alice and Bob are equal and so the functionality $f^{(\tau)}(x,y)$ is a deterministic function of only τ. This implies that there exists a z^* such that $f^{(\tau)}(x,y)_{z^*} = \Pr[z^* | x, y, \tau]$ equals 1 for any $(x,y) \in \mathrm{Supp}\big(\pi^{(\tau)} \times \rho^{(\tau)}\big)$ and $f^{(\tau)}(x,y)_z = 0$ for any other z. Now, notice that $\pi_x^{(\tau)} = A_{x,z^*}$ and $\rho_y^{(\tau)} = B_{y,z^*}$ according to Lemma 4 and so $A_{x,z^*}^{(\tau)} = B_{y,z^*}^{(\tau)} = 1$ according to our definition. Then, it is obvious that $f^{(\tau)}(x,y) = A_x^{(\tau)} * B_y^{(\tau)} * V^{(\tau)}$ where $V^{(\tau)} = e_{z^*}$ and $\mathrm{Supp}\big(f^{-1}(z^*)\big) = \mathrm{Supp}\big(\pi^{(\tau)} \times \rho^{(\tau)}\big)$.

Inductive step. Let $\sigma^{(\tau'|y)} := \Pr[\tau'|y,\tau]$, that is, the probability the extended transcript is τ' conditioned on the Bob's input being y and the partial transcript τ. Then, we have

$$\begin{aligned}
f^{(\tau)}(x,y) &= \sum_{\tau'\in\Omega} \sigma^{(\tau'|y)} \cdot f^{(\tau')}(x,y) \\
&= \sum_{\tau'\in\Omega} \sigma^{(\tau'|y)} \cdot A_x^{(\tau')} * B_y^{(\tau')} * V^{(\tau')} && \text{(by the inductive hypothesis)} \\
&= A_x^{(\tau)} * \sum_{\tau'\in\Omega} \sigma^{(\tau'|y)} \cdot B_y^{(\tau')} * V^{(\tau')} \\
& && \text{(For all } \tau'\in\Omega, \text{ we have } A^{(\tau)} = A^{(\tau')}, \text{ because } \pi^{(\tau)} = \pi^{(\tau')}) \\
&= A_x^{(\tau)} * \sum_{\substack{\tau'\in\Omega \\ \rho_y^{(\tau')}\neq 0}} \sigma^{(\tau'|y)} \cdot B_y^{(\tau')} * V^{(\tau')} \\
&= A_x^{(\tau)} * \sum_{\substack{\tau'\in\Omega \\ \rho_y^{(\tau')}\neq 0}} \frac{\sigma^{(\tau'|y)}}{\rho_y^{(\tau')}} \cdot B_y * V^{(\tau')} \\
&= A_x^{(\tau)} * \sum_{\substack{\tau'\in\Omega \\ \rho_y^{(\tau')}\neq 0}} \frac{\lambda_{\tau'}}{\rho_y^{(\tau)}} \cdot B_y * V^{(\tau')} && \text{(by Claim 1)} \\
&= A_x^{(\tau)} * B_y^{(\tau)} * \sum_{\substack{\tau'\in\Omega \\ \rho_y^{(\tau')}\neq 0}} \lambda_{\tau'} \cdot V^{(\tau')}
\end{aligned}$$

So it remains to prove that for any $x\in X, y\in Y, z\in Z$,

$$A_{x,z}^{(\tau)} \cdot B_{y,z}^{(\tau)} \cdot \sum_{\substack{\tau'\in\Omega \\ \rho_y^{(\tau')}\neq 0}} \lambda_{\tau'} \cdot V_z^{(\tau')} = A_{x,z}^{(\tau)} \cdot B_{y,z}^{(\tau)} \cdot \sum_{\tau'\in\Omega} \lambda_{\tau'} \cdot V_z^{(\tau')}.$$

It suffices to show that for any partial transcript $\tau'\in\Omega$ such that $\rho_y^{(\tau')} = 0$, we have

$$A_{x,z}^{(\tau)} \cdot B_{y,z}^{(\tau)} \cdot V_z^{(\tau')} = 0.$$

Since $y \notin \mathrm{Supp}\left(\rho^{(\tau')}\right)$, we have $(x',y) \notin \mathrm{Supp}\left(\pi^{(\tau')} \times \rho^{(\tau')}\right)$ for any x'. Suppose $V_z^{(\tau')} > 0$, then $\mathrm{Supp}\left(f^{-1}(z)\right) \subseteq \mathrm{Supp}\left(\pi^{(\tau')} \times \rho^{(\tau')}\right)$ by induction hypothesis. This implies that $(x',y) \notin \mathrm{Supp}\left(f^{-1}(z)\right)$ for any x'. It means that $f(x',y)_z = 0$ for any x'. This implies that $B_{y,z} = 0$ and therefore $B_{y,z}^{(\tau)} = 0$ and so $A_{x,z}^{(\tau)} \cdot B_{y,z}^{(\tau)} \cdot V_z^{(\tau')} = 0$.

Next, we prove the second statement. Without loss of generality, assume that Bob extends the transcript. Since $V_z^{(\tau)} > 0$ and $V_z^{(\tau)} = \sum_{\tau'\in\Omega} \lambda_{\tau'} \cdot V^{(\tau')}$, there is a transcript $\tau'\in\Omega$ such that $V_z^{(\tau')} > 0$. By induction hypothesis, $\mathrm{Supp}\left(f^{-1}(z)\right) \subseteq \mathrm{Supp}\left(\pi^{(\tau')} \times \rho^{(\tau')}\right)$. By Lemma 3, the following idetity holds.

$$\rho^{(\tau)} = \sum_{\tau'\in\Omega} \lambda_{\tau'} \cdot \rho^{(\tau')}.$$

This implies that $\mathrm{Supp}\big(\rho^{(\tau)}\big) = \bigcup_{\tau' \in \Omega} \mathrm{Supp}\Big(\rho^{(\tau')}\Big)$. Furthermore, Lemma 3 yields $\pi^{(\tau)} = \pi^{(\tau')}$, which implies that $\mathrm{Supp}\big(\pi^{(\tau)}\big) = \mathrm{Supp}\Big(\pi^{(\tau')}\Big)$. These facts imply that

$$\mathrm{Supp}\Big(\pi^{(\tau')} \times \rho^{(\tau')}\Big) \subseteq \mathrm{Supp}\Big(\pi^{(\tau)} \times \rho^{(\tau)}\Big).$$

Therefore, $\mathrm{Supp}\big(f^{-1}(z)\big) \subseteq \mathrm{Supp}\big(\pi^{(\tau)} \times \rho^{(\tau)}\big)$ as desired. □

Claim 1. *Let τ be a partial transcript and τ' be a one message extension of τ. Then, the following identity holds*

$$\rho_y^{(\tau)} \cdot \sigma^{(\tau'|y)} = \rho_y^{(\tau')} \cdot \lambda_{\tau'}.$$

Proof. This follows from definitions and Bayes' rule.

$$\begin{aligned}
\rho_y^{(\tau)} \cdot \sigma^{(\tau'|y)} &= \Pr[y|\tau] \cdot \Pr[\tau'|y,\tau] && \text{(definition)}\\
&= \Pr[y|\tau',\tau] \cdot \Pr[\tau'|\tau] && \text{(Bayes' rule)}\\
&= \Pr[y|\tau'] \cdot \Pr[\tau'|\tau] && (\tau' \text{ contains } \tau)\\
&= \rho_y^{(\tau')} \cdot \lambda_{\tau'} && \text{(definition)}
\end{aligned}$$

This completes the proof. □

Lemma 6. *Any point $(\pi, \rho, V') \in \mathcal{S}^{(i)}$ has a perfectly secure (at most) i-round protocol, where $i \in \{0, 1, 2, \dots\}$.*

Proof. We proceed by induction on $i \in \{0, 1, \dots\}$.
Base case. If $i = 0$, then $V = e(z)$. In this case, parties output z. It is trivial to see that the protocol is perfectly secure.
Inductive step. Suppose

$$\mathcal{S}^{(i)} \ni (\pi, \rho, V') = \sum_{k=1}^{t} \lambda_k \cdot \underbrace{(\pi^{(k)}, \rho^{(k)}, V^{(k)})}_{\in \mathcal{S}^{(i-1)}},$$

and $\pi = \pi^{(k)}$, for all $k \in \{1, 2, \dots, t\}$. Then, Bob sends the message in the protocol. By induction hypothesis, each point $(\pi^{(k)}, \rho^{(k)}, V^{(k)})$ has a perfectly secure (at most) $(i-1)$-round protocol, says $\Pi^{(k)}$. We use these protocols to construct a protocol for the point (π, ρ, V') as follows. Bob sends the first message to Alice so that then the sub-protocol that Alice and Bob execute after the first message is $\Pi^{(k)}$ with probability $\sigma^{(k|y)} := \lambda_k \cdot \rho_y^{(k)} / \rho_y$ conditioned on Bob's input is y. Clearly, this protocol has at most i-round. We will prove that this protocol is securely realizing the functionality g by constructing simulators for corrupted parties. Simulator for the case that Bob is corrupted is trivial since the simulator knows Bob's input y, therefore, can simulate Bob's first message exactly as the same as the message in the real protocol. So all remain is to construct a simulator for corrupted Alice. The simulator $\mathsf{Sim}_A(x, z)$ takes as input Alice's input x and the output z. And the simulator outputs symbol k with probability $\lambda_k V_z^{(k)} / V'_z$. This simulator works because the following expression is independent of y.

$$\begin{aligned}
\frac{\sigma^{(k|y)} f^{(k)}(x,y)_z}{f(x,y)_z} &= \frac{\sigma^{(k|y)} V_z^{(k)} \rho_y}{\rho_z^{(k)} V_z^{(k)}}\\
&= \frac{\lambda_k V_z^{(k)}}{V'_z}. && \text{(using Claim 1)}
\end{aligned}$$

This completes the proof. □

C Decidability and Witness to Protocol Recovery

This section presents the decidability results. The following IsRealizable(f, r) prodcedure takes as input a function $f\colon X \times Y \to \mathbb{R}^Z$ and a number $r \in \mathbb{N}$. It outputs Yes if there is a secure protocol for f with at most r rounds, and No otherwise. Furthermore, the procedure outputs a secure protocol by calling the sub-procedure Witness in the Yes instance and a certificate in the No instance. The certificate is the query point $Q^{(f)}$ and the description of the set $\mathcal{S}^{(r)}$. Note that the set $\mathcal{S}^{(r)}$ always has a succinct description since it is tame. In the following discussion, refer to Equation 4, Equation 5 for the definitions of $P^{(z)}, \varphi_1,$ and $, \varphi_2$.

IsRealizable(f, r):

1. **Ensure.** The function $f\colon X \times Y \to \mathbb{R}^Z$ and $r \in \{0, 1, \dots\}$
2. If the function f has Kilian's obstruction: **Return** False
3. Update f to be its standardized SSFE form as prescribed in [MPR13]
4. Initialize $\mathbb{R}^d \supseteq \mathcal{S}^{(0)} := \{P^{(z)}\colon z \in Z\}$ (see Equation 4)
5. Define linear maps φ_1, φ_2 as in Equation 5
6. For $i \in \{0, 1, \dots, r-1\}$, recursively define

$$\mathcal{S}^{(i+1)} := \left\{ \sum_{m=1}^{d+1} p_m \cdot Q^{(m)} : \begin{array}{c} p_1, \dots, p_{d+1} \geqslant 0,\ \sum_{m=1}^{d+1} p_m = 1,\ Q^{(1)}, \dots, Q^{(d+1)} \in \mathcal{S}^{(i)}, \\ \varphi_1(Q^{(1)}) = \cdots = \varphi_1(Q^{(d+1)}) \text{ or } \varphi_2(Q^{(1)}) = \cdots = \varphi_2(Q^{(d+1)}) \end{array} \right\}.$$

7. If $Q^{(f)} \in \mathcal{S}^{(r)}$: **Return** Yes, $\Pi :=$ Witness$(\mathcal{S}^{(0)}, Q^{(f)}, r)$
8. **Return** False, Certificate $:= Q^{(f)}, \mathcal{S}^{(r)}$

The witness procedure is defined recursively as follows.

WITNESS$(\mathcal{S}^{(0)}, Q, k)$:

1. If $k = 0$, it must hold that $Q = (U_X, U_Y, e(z))$ for some $z \in Z$. On any input $x \in X, y \in Y$, both parties always output z.
2. Else: Apply Theorem 3 to get $\lambda_1, \lambda_2, \cdots, \lambda_{d+1} \geqslant 0$ and $Q^{(1)}, Q^{(2)}, \cdots, Q^{(d+1)} \in \mathcal{S}^{(k-1)}$ such that

$$\lambda_1 + \lambda_2 + \cdots + \lambda_{d+1} = 1, \text{ and } Q = \lambda_1 \cdot Q^{(1)} + \lambda_2 \cdot Q^{(2)} + \cdots + \lambda_{d+1} \cdot Q^{(d+1)}$$

   Let $Q = (\pi, \rho, V')$, $Q^{(i)} = (\pi^{(i)}, \rho^{(i)}, V^{(i)})$.

   (a) If $\pi^{(1)} = \pi^{(2)} = \cdots = \pi^{(d+1)}$, then recall that $\rho_y = \lambda_1 \cdot \rho_y^{(1)} + \lambda_2 \cdot \rho_y^{(2)} + \cdots + \lambda_{d+1} \cdot \rho_y^{(d+1)}$. For any $y \in \text{Supp}(\rho)$, Bob sends message i to Alice with probability $\lambda_i \cdot \rho_y^{(i)} / \rho_y$ and recursively calls WITNESS$(\mathcal{S}^{(0)}, Q^{(i)}, k-1)$.

   (b) If $\rho^{(1)} = \rho^{(2)} = \cdots = \rho^{(d+1)}$, then recall that $\pi_x = \lambda_1 \cdot \pi_x^{(1)} + \lambda_2 \cdot \pi_x^{(2)} + \cdots + \lambda_{d+1} \cdot \pi_x^{(d+1)}$. For any $x \in \text{Supp}(\pi)$, Alice sends message i with probability $\lambda_i \cdot \pi_x^{(i)} / \pi_x$ to Bob and and recursively calls WITNESS$(\mathcal{S}^{(0)}, Q^{(i)}, k-1)$.

We emphasize that in Step 2 above, one cannot use *any* linear λ_is and $Q^{(i)}$s. Although it may generate a protocol, it may not be the optimal protocol one seeks. So, one needs to use Theorem 3 to get those values.

D Functions with Large Number of Rounds

This section shows that the round complexity of secure function evaluation could be arbitrarily large.

Lemma 7. *For any positive integer r, there is a function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{r+1}$ such that f has a r-round secure protocol but not any $(r-1)$-round secure protocol.*

Intuition. We give an intuitive description of the function and an informal proof using Figure 4. Fix any positive integer r. We construct an initial set $\mathcal{S}^{(0)} = \{q^{(0)}, q^{(1)}, \ldots, q^{(r)}\}$. Let q^* be the intersection of the vertical segment and the horizontal segment. For example, q^* is the intersection of the horizontal segment incident to $q^{(7)}$ and the vertical segment incident to $q^{(8)}$ when $r = 7$ or the intersection of the vertical segment incident to $q^{(8)}$ and the horizontal segment incident to $q^{(9)}$ when $r = 8$. Based on our cryptographic reduction, there is a function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{r+1}$ corresponding to the point q^*. We shall show that this function has a r-round secure protocol but no $(r-1)$-round secure protocol. One can prove this inductively using the observation that the vertical segment incident to $q^{(t)}$ when t is even or the horizontal segment incident to $q^{(t)}$ when t is odd is in $\mathcal{S}^{(t)}$ but not in $\mathcal{S}^{(t-1)}$ for any $t \leqslant r$.

However, the point q^* is not located at $(1/2, 1/2)$ which implies that the Alice's input distribution and Bob's input distribution are not uniform. To fix it, thank to the linear property of our geometric embedding, we can first scale Figure 4 to Figure 5 and then translate it to Figure 6 so that the point q^* is located at $(1/2, 1/2)$. This geometric transformation preserves the security and the number of rounds. That is, if the protocol constructed from Figure 4 is a secure protocol with r-round, then so does the protocol constructed from Figure 6.

For completeness, we present a formal proof below.

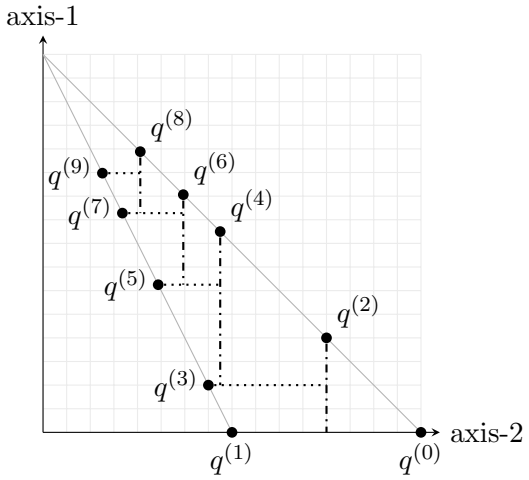


Figure 4: An illustrative example showing that for each r there exists a $\mathcal{S}^{(0)}$ such that $\mathcal{S}^{(r-1)} \subsetneq \mathcal{S}^{(r)}$. This implies that for each r there exists a function that has a r-round secure protocol but not any $(r-1)$-round secure protocol.

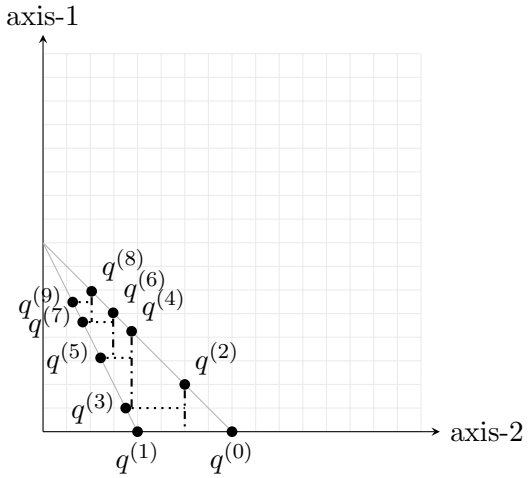


Figure 5: Scaling Figure 4 by an appropriate constant

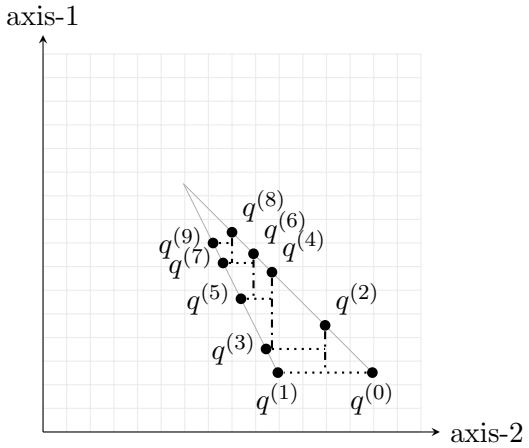


Figure 6: Translating Figure 5 so that f is located at $(1/2, 1/2)$.

Proof. Fix $r \in \mathbb{N}$. Let the output space be $Z = \{0, 1, \ldots, r\}$ and $e(z) \in \mathbb{R}^r$ be the indicator variable of z. We define a sequence of points $\{q^{(i)}\}_{i=0}^{r}$ in $\mathbb{R}^2$ (refer to Figure 4) as follows.

$$\begin{aligned}
q_1^{(2i+1)} &= \frac{q_1^{(2i+2)} + q_1^{(2i)}}{2},\ q_2^{(2i+1)} = \frac{1 - q_1^{(2i+1)}}{2},\\
q_2^{(2i+2)} &= \frac{q_2^{(2i+1)} + q_2^{(2i-1)}}{2},\ q_1^{(2i+2)} = 1 - q_2^{(2i+2)},\\
q^{(0)} &= (0,1), q^{(1)} = (0,1/2),\ q^{(2)} = (1/4, 3/4).
\end{aligned}$$

Intuitively, these points correspond to the leaves in the tree protocol of f. We shall show that the functionality $f \cong (A, B, V)$ has r-round protocol but no $(r-1)$-round protocol, where $A \in \mathbb{R}^2 \times \mathbb{R}^{r+1}, B \in \mathbb{R}^2 \times \mathbb{R}^{r+1}, V \in \mathbb{R}^{r+1}$ are defined as follows.

$$\begin{aligned}
A_1 &= (q_1^{(0)}, q_1^{(1)}, \ldots, q_1^{(r+1)}),\ A_0 = 1 - A_1,\\
B_1 &= (q_2^{(0)}, q_2^{(1)}, \ldots, q_2^{(r+1)}),\ B_0 = 1 - B_1,\\
V^{(2i+1)} &= \frac{q_2^{(2i+2)} - q_2^{(2i+1)}}{q_2^{(2i)} - q_2^{(2i+1)}} \cdot V^{(2i)} + \frac{q_2^{(2i)} - q_2^{(2i+2)}}{q_2^{(2i)} - q_2^{(2i+1)}} \cdot e(2i+1),\\
V^{(2i+2)} &= \frac{q_1^{(2i+2)} - q_1^{(2i+3)}}{q_1^{(2i+2)} - q_1^{(2i+1)}} \cdot V^{(2i+1)} + \frac{q_1^{(2i+3)} - q_1^{(2i+1)}}{q_1^{(2i+2)} - q_1^{(2i+1)}} \cdot e(2i+2),\\
V^{(0)} &= \frac{1}{2}e(0) + \frac{1}{2}e(1),\ V^{(1)} = \frac{1}{4}e(0) + \frac{1}{4}e(1) + \frac{1}{2}e(2),\\
V &= V^{(r)}.
\end{aligned}$$

Define $\mathcal{S}^{(0)} = \{(q^{(i)}, e(i)) \colon i \in Z\}$. Let $S^{(k)}$ be the projection of $\mathcal{S}^{(k)}$ on the first two coordinates for $k \in \mathbb{N}$. $S^{(0)} = \{q^{(0)}, q^{(1)}, \ldots, q^{(r)}\}$.

Claim 2. *Observe that*

1. *Both $\{q_1^{(2i+1)}\}_{i=0}$ and $\{q_1^{(2i)}\}_{i=0}$ are strictly increasing sequences, while both $\{q_2^{(2i+1)}\}_{i=0}$ and $\{q_2^{(2i)}\}_{i=0}$ are strictly decreasing sequences.*
2. *$q_1^{(2i+1)} < q_1^{(2i)} < q_1^{(2i+3)}$ for any $i \geqslant 1$.*
3. *$q_2^{(2i-1)} < q_2^{(2i)} < q_2^{(2i-3)}$ for any $i \geqslant 2$.*

For any $k \geqslant 1$, we define

$$\begin{aligned}
I_{2k} &= \{(x, q_2^{(2k)}) \colon q_1^{(2k-1)} < x < q_1^{(2k)}\},\ \text{and}\\
I_{2k+1} &= \{(q_1^{(2k+1)}, y) \colon q_2^{(2k+1)} < y < q_2^{(2k)}\}.
\end{aligned}$$

Note that I_r contains the query point q^*. We shall prove by induction on r stronger statements that

1. $I_r \in S_r^{(r)}$ and $I_r \notin S_r^{(r-1)}$.
2. Furthermore, it holds that (a) $q_2^{(r-1)} \leqslant q_2$, and $q_1^{(r)} \geqslant q_1$ if r is even, and (b) $q_1^{(r-1)} \geqslant q_1$, and $q_2^{(r)} \leqslant q_2$ if r is odd for any point $q \in S_r^{(r-1)} \setminus \{q^{(r)}\}$. In particular, $q_1^{(r+1)} > q_1$ and $q_2^{(r+1)} < q_2$ for any point $q \in S_r^{(r-1)} \setminus \{q^{(r)}\}$.

For $r = 2, 3$, it is easy to see that the statement is true. Suppose it holds for r, we will prove it is true for $r+1$. First, observe that $S_{r+1}^{(0)} = S_r^{(0)} \cup \{q^{(r+1)}\}$. By the induction hypothesis, we have $q_1^{(r+1)} > q_1$ and $q_2^{(r+1)} < q_2$ for any $q \in S_r^{(r-1)} \setminus \{q^{(r)}\}$. This implies that even when including the point $q^{(r+1)}$ in the set $S_r^{(r-1)}$, it does not add any new point to the set $S_r^{(r-1)}$ except the point $q^{(r+1)}$ itself, in other words, $S_{r+1}^{(r-1)} = S_r^{(r-1)} \cup \{q^{(r+1)}\}$. It also implies that the segment I_{r+1} is not in $S_{r+1}^{(r)}$. By the other induction hypothesis, $I_r \in S_r^{(r)}$ and $I_r \notin S_r^{(r-1)}$. Therefore, $I_r \in S_{r+1}^{(r)}$ and $I_r \notin S_{r+1}^{(r-1)}$. Observe that

1. $q_2^{(r+1)} < q_2^{(r)}$ and $q_1^{(r+1)} < q_1^{(r)}$ if r is even,
2. $q_2^{(r+1)} > q_2^{(r)}$ and $q_1^{(r+1)} > q_1^{(r)}$ if r is odd.

In either of the two cases, we can perform the geometric action from $q^{(r+1)}$ so that the segment I_{r+1} is added to $S_{r+1}^{(r+1)}$.

The second statement follows from the induction hypothesis and Claim 2. □

E Subsuming Kushilevitz and Beaver's Results

This section illustrates that our framework implies the decomposable theorem for deterministic function as in [CK89, Kus89, Bea89]. So, we shall consider only deterministic functions $f\colon X \times Y \to Z$ in this section. First, we state the definition of a decomposable function:

Definition 2 (**Decomposability [Kus89]**). *A deterministic function $f\colon X \times Y \to Z$ is decomposable if one of the following constraints holds:*

- ***Constant:*** *f is a constant function.*
- ***Row Decomposable:*** *We have $X = \bigcup_{i=1}^{s} X_i$, where the sets $\{X_i\}_{i=1}^{s}$ are non empty, and $X_i \cap X_j = \emptyset$ for any i, j, such that the two following occur:*
  - *For any i, j and any $x \in X_i, x' \in X_j$ and any $y \in Y$, we have $f(x, y) \neq f(x', y)$.*
  - *For any i, the restriction of f into $X_i \times Y$ is a constant function or column decomposable.*
- ***Column Decomposble:*** *We have $Y = \bigcup_{i=1}^{s} Y_i$, where the sets $\{Y_i\}_{i=1}^{s}$ are non empty, and $Y_i \cap Y_j = \emptyset$ for any i, j, such that the two following occur:*
  - *For any i, j and any $y \in Y_i, y' \in Y_j$ and any $x \in X$, we have $f(x, y) \neq f(x, y')$.*
  - *For any i, the restriction of f into $X \times Y_i$ is a constant function or row decomposable.*

Decomposable implies existence of a secure protocol. Figure 7 shows a secure protocol for the MAX function (Dutch auction) using Kushilevitz's decomposition strategy. This is a top-down approach. Using our bottom-up strategy, Figure 8 presents a secure protocol for that function.

Existence of a secure protocol implies decomposable. We show that if a deterministic function $f\colon X \times Y \to Z$ has a secure protocol, then it is decomposable using our techniques.

It follows from Lemma 2 that $\mathrm{Supp}\big(\pi^{(\tau)} \times \rho^{(\tau)}\big)$ is a combinatorial rectangle for any partial transcript τ. Observe that $f^{(\tau)}(x, y)$ is a constant for all $(x, y) \in \mathrm{Supp}\big(\pi^{(\tau)} \times \rho^{(\tau)}\big)$ if τ is a complete transcript. Let τ be a partial transcript of the protocol. Let Ω represent the set of all

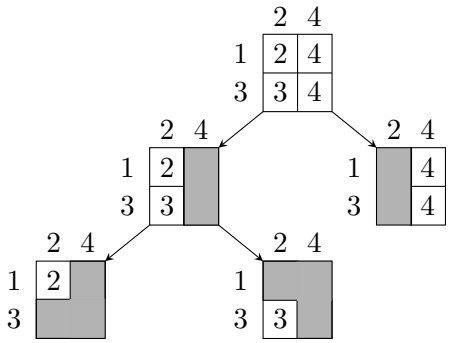


Figure 7: A secure protocol for Dutch auction (MAX) using Kushilevitz's decomposition strategy. Alice's input (rows) belongs to $\{1, 3\}$ and Bob's input (columns) belongs to $\{2, 4\}$. Each table represents a deterministic function. In each table, the area that is not shaded represents the range of the function corresponding to that table.

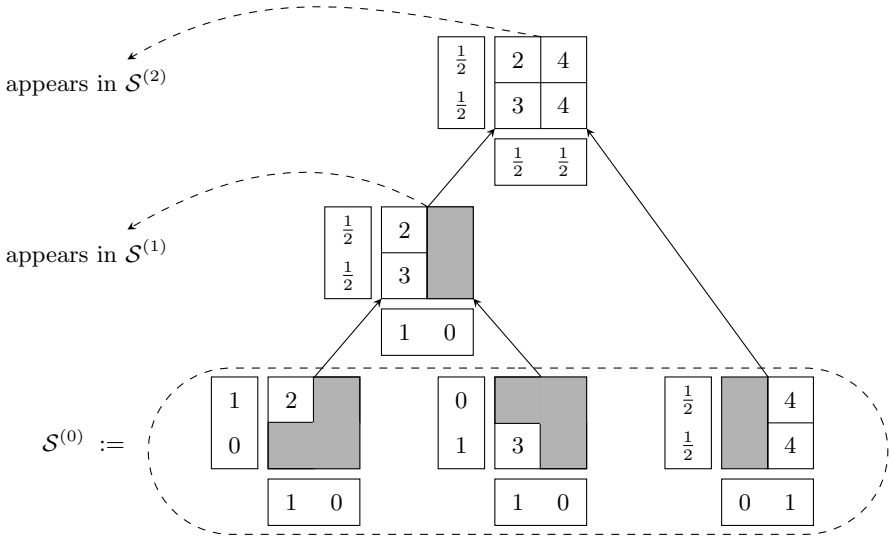


Figure 8: A secure protocol for the Dutch auction (MAX) function using our framework. Alice's input (rows) belongs to $\{1, 3\}$ and Bob's input (columns) belongs to $\{2, 4\}$. Each table represents a deterministic function. The column next to each table represents Alice's input distribution and the row below each table represents Bob's input distribution. The area in each table that is not shaded represents the range of the function corresponding to that table. Alice fuses two of leaves securely because the marginal distribution of Bob's input for those leaves are the same (equal to $(1, 0)$). Then Bob can fuse the other leaf with the internal node to realize the main function securely because the marginal distribution of Alice's input for those two nodes are the same (equal to $(1/2, 1/2)$).

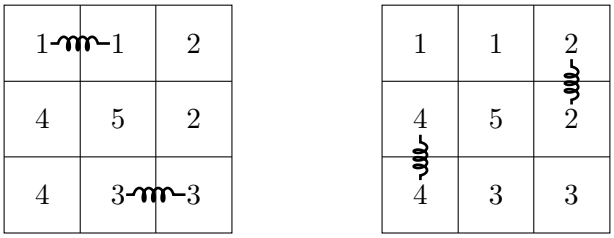


Figure 9: Illustration of the Kushilevitz function that is not decomposable. There is no way to partition the rows or the columns of the output matrix so that resulting matrices are decomposable.

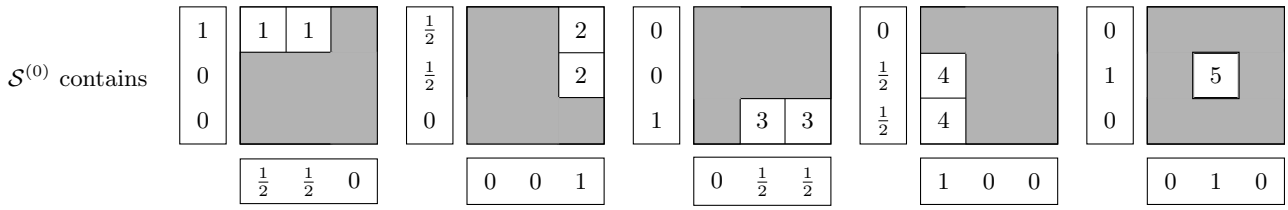


Figure 10: Illustration of why there is no secure protocol for the Kushilevitz function [Kus89] using our framework. The marginal distributions of the base cases are mentioned and no fusing is possible because no pair of the base cases have either identical Alice's input distribution or Bob's input distribution. The columns represent Alice's input distribution and the row represents the corresponding Bob's input distribution. Each square matrix represents the output value of the corresponding (deterministic) function whose domain is defined over the white color cells only.

one-round extension of τ. Suppose Alice extends the partial transcript τ. By Lemma 3, for all $\tau' \in \Omega$, $\rho^{(\tau)} = \rho^{(\tau')}$ and

$$\pi^{(\tau)} = \sum_{\tau' \in \Omega} \lambda_{\tau'} \cdot \pi^{(\tau')}.$$

This implies that all combinatorial rectangles $\text{Supp}\left(\pi^{(\tau')} \times \rho^{(\tau')}\right)$ have the same width and

$$\text{Supp}\left(\pi^{(\tau)} \times \rho^{(\tau)}\right) = \bigcup_{\tau' \in \Omega} \text{Supp}\left(\pi^{(\tau')} \times \rho^{(\tau')}\right).$$

We note that it is possible that these rectangles are not disjoint. However, based on the equation above, it is always possible to partition the rectangle $\text{Supp}\left(\pi^{(\tau)} \times \rho^{(\tau)}\right)$ into disjoint rectangles with the same width $\text{Supp}\left(\rho^{(\tau)}\right)$, in other words, it is row-decomposalbe. We make a convention that if a rectangle is an intersection of some of these rectangles, then keep that intersection in the rectangle of the left most partial transcript. Note that this partition will preserve the decomposable property. Similarly, if Bob extends the partial transcript, the rectangle $\text{Supp}\left(\pi^{(\tau)} \times \rho^{(\tau)}\right)$ is column-decomposable. Applying this argument top-down, one concludes that f is decomposable.

No secure protocol for the spiral function. Figure 9 shows that the Kushilevitz function is not row decomposable and column decomposable as well. In Figure 10, we illustrate that the Kushilevitz function does not have any secure protocol using our framework.

F Subsuming Data-Prabhakaran's results [DP18]

This section illustrates that our results subsume the results in [DP18].

Characterizing ternary output symmetric functions. [DP18] gave the following characterization for ternary output functionality.

Theorem 4. *A ternary output functionality $f\colon X \times Y \to \mathbb{R}^Z$ has a secure protocol if and only if f does not have Kilian's obstruction and there are some ordering of output space Z as (z_1, z_2, z_3) and two functions $\phi\colon X \to [0,1]$ and $\psi\colon Y \to [0,1]$ such that*

1. $f(x,y)_{z_1} = \phi(x)$, $f(x,y)_{z_2} = (1-\phi(x)) \cdot \psi(y)$, *and* $f(x,y)_{z_3} = (1-\phi(x)) \cdot (1-\psi(y))$, *or*
2. $f(x,y)_{z_1} = \psi(y)$, $f(x,y)_{z_2} = (1-\psi(y)) \cdot \phi(x)$, *and* $f(x,y)_{z_3} = (1-\psi(y)) \cdot (1-\phi(y))$.

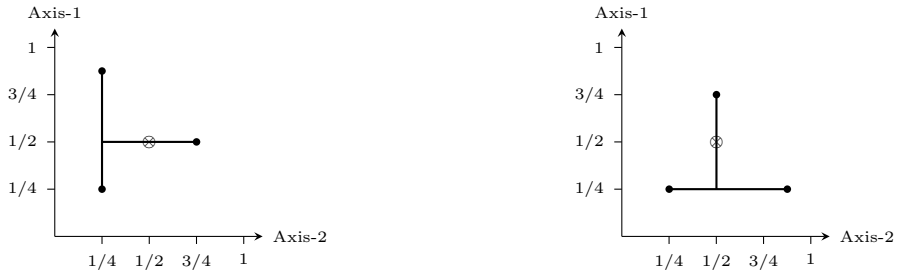


Figure 11: Illustration of our geometric action for a ternary output function.

It follows from our cryptographic reduction that any secure protocol for ternary output symmetric function has exactly 3 points in the initial set $\mathcal{S}^{(0)}$ which implies that $\mathcal{S}^{(2)} = \mathcal{S}^{(3)} = \cdots$. To see that our framework also implies this result, it suffices to show that the query point $Q^{(f)} \in \mathcal{S}^{(2)}$ if and only if the conditions in item 1 or item 2 (in the above theorem) hold. Figure 11 visualizes this statement. If the conditions on the first item holds, then there is a secure protocol in which Alice either sends z_1 to Bob with probability $\phi(x)$ or asks Bob to pick the output with probability $(1-\phi(x))$; if Bob is asked to pick the output, he sends z_2 with probability $\psi(y)$ and z_3 with probability $(1-\psi(y))$ to Alice. This protocol is exactly the protocol corresponding to the right figure (see our Witness procedure in Appendix C). Similarly, the second item corresponds to the left figure. Therefore, our results also imply the theorem above. We have the following result as a consequence.

Corollary 2. *Any secure protocol for a ternary output function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ has at most 2 rounds.*

Negative Result. [DP18] also showed that the following functionality $\ell\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ is not securely computable, where $Z = \{1,2,3\}$. We shall show this using our technique.

$\ell(1,0) = (2/9, 4/9, 1/3)$	$\ell(1,1) = (5/18, 2/9, 1/2)$
$\ell(0,0) = (1/3, 5/12, 1/4)$	$\ell(0,1) = (5/12, 5/24, 3/8)$

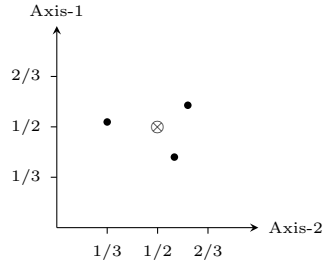
By Lemma 1, there exist $A \in \mathbb{R}^2 \times \mathbb{R}^3, B \in \mathbb{R}^2 \times \mathbb{R}^3$, and $V \in \mathbb{R}^3$ such that $\ell(x,y) = A_x * B_y * V$, where A, B, V are defined as

$$A = \begin{array}{|c|}\hline A_0 = (3/5, 15/31, 3/7) \\ \hline A_1 = (2/5, 16/31, 4/7) \\ \hline \end{array}, B = \begin{array}{|c|}\hline B_0 = (4/9, 2/3, 2/5) \\ \hline B_1 = (5/9, 1/3, 3/5) \\ \hline \end{array}, V = (5/4, 31/24, 35/24).$$

Figure 12 and Figure 13 illustrate that function ℓ is not securely computable using our geometric technique. In fact, our technique implies that there are infinite many ternary output functions that do not has a secure protocol by choosing any 3 points with coordinates in $(0,1)$ that are not axis-aligned and their convex hull contains the query point.

$A_1 = (2/5, 16/31, 4/7)$

$B_1 = (5/9, 1/3, 3/5)$



$\mathsf{proj}\big(\mathcal{S}^{(0)}(\ell)\big)$

Figure 12: The figure on the right shows the projection of $\mathcal{S}^{(0)}(\ell)$ to its first two coordinates. Our geometric action cannot add any further points to $\mathcal{S}_0(\ell)$ because no two points in the figure on the right is axis-aligned. Therefore, $\mathcal{S}^{(0)} = \mathcal{S}^{(1)} = \mathcal{S}^{(2)} = \cdots$.

$\mathcal{S}^{(0)}$ contains

$\frac{2}{5}$	$e(1)$	$e(1)$
$\frac{3}{5}$	$e(1)$	$e(1)$
	$\frac{4}{9}$	$\frac{5}{9}$

$\frac{16}{31}$	$e(2)$	$e(2)$
$\frac{15}{31}$	$e(2)$	$e(2)$
	$\frac{2}{3}$	$\frac{1}{3}$

$\frac{4}{7}$	$e(3)$	$e(3)$
$\frac{3}{7}$	$e(3)$	$e(3)$
	$\frac{2}{5}$	$\frac{3}{5}$

Figure 13: Illustration of why there is no secure protocol for the function ℓ using our framework. The marginal distributions of the base cases are mentioned and no fusing is possible because no pair of the base cases have either identical Alice's input distribution or Bob's input distribution. The column next to each square matrix represents the corresponding Alice's input distribution and the row below represents the corresponding Bob's input distribution. Each square matrix represents the output distributions of the corresponding function using the notation for randomized functions.

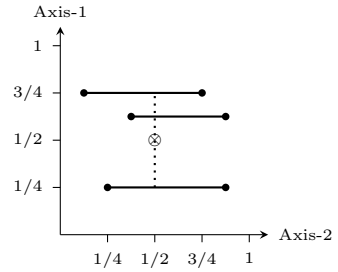


Figure 14: Characterization of symmetric functions with 2-round secure protocols using our geometric technique assuming Alice sends the first message.

Characterizing functions with 2-round protocols. [DP18] gave the following characterization for symmetric functions with 2-round secure protocols.

Theorem 5. *A symmetric function $f\colon X \times Y \to \mathbb{R}^Z$ that avoids Kilian's obstruction has a two round-protocol with Alice sending the first message if and only if there is a surjective map $\phi\colon Z \to W$ such that $\Pr[z|w,y] = 0$ if $w \neq \phi(z)$, and for all $x \in X, y \in Y, z \in Z$,*

$$f(x,y)_z \;:=\; \Pr[z|x,y] = \Pr[\phi(z)|x] \cdot \Pr[z|\phi(z),y].$$

Futhermore, f has a unique-transcript secure protocol in which Alice sends w with probability $\Pr[w|x]$, and Bob sends back z with probability $\Pr[z|w,y]$.

Figure 14 visualizes that Alice first sends a message w to Bob with probability based on the convex combination of the query point (marked $\otimes$) using the 3 points that are intersection of the vertical segment with the 3 horizontal segments, then Bob sends back z with probability based on the intersection and the convex combination of this intersection. This protocol is basically identical to the protocol in the theorem above and has unique-transcript.

G UC Semi-honest Security Definition

This section presents the security definition of secure symmetric function evaluation following the universal composable framework [Can00]. Intuitively, a protocol securely realizes a (possibly randomized) function if Alice or Bob does not learn any additional information beyond what she/he can learn from her/his input and output at the end of the protocol. More formally, there are two worlds named real world and ideal world in the definition.

Real World Experiment. There are three participants in real world: Alice, Bob, and an environment $\mathcal{E}$. The environment $\mathcal{E}$ decides which party to corrupt and also the private input x of Alice and the private input y of Bob. Alice and Bob run the protocol Π honestly and return their outputs z_A, z_B to $\mathcal{E}$. In addition, the corrupt party sends her complete view to $\mathcal{E}$.

1. If the environment corrupts no party, the distribution of environment's view is $\mathbb{V}_{\mathcal{E}}^{(real)} = (x, Z_A, y, Z_B)$.
2. If the environment corrupts Alice, environment's view is $\mathbb{V}_{\mathcal{E}}^{(real)} = (x, V_A, y, Z_B)$.
3. If the environment corrupts Bob, environment's view is $\mathbb{V}_{\mathcal{E}}^{(real)} = (x, Z_A, y, V_B)$.

Ideal World Experiment. There are four participants: Alice, Bob, the environment, and the ideal functionality that takes as input x from Alice and y from Bob, and outputs the (random variable) $Z = f(x, y)$ to both parties. The environment remains identical to the one in the real world. Honest parties send their output they received from the ideal functionality to the environment.

1. If the environment does not corrupt any party, then its view is $\mathbb{V}_{\mathcal{E}}^{(ideal)} = (x, Z, y, Z)$.
2. If the environment corrupts Alice, then we need to design a simulator Sim_A that takes over the control of Alice in the ideal world. The simulator takes input x from the environment, forwards x to the ideal functionality, and receives the output Z. Then, the simulator Sim_A generates a view V_A based on its view (x, Z). The distribution of environment's view is $\mathbb{V}_{\mathcal{E}}^{(ideal)} = (x, \mathsf{Sim}_A(x, Z), y, Z)$.
3. Similarly, if the environment corrupts Bob, then we need to design a simulator Sim_B that takes over the control of Bob in the ideal world. The simulator takes input y from the environment, forwards y to the ideal functionality, and receives the output Z. Then, the simulator Sim_B generates a view V_B based on its view (y, Z). The distribution of environment's view is $\mathbb{V}_{\mathcal{E}}^{(ideal)} = (x, Z, y, \mathsf{Sim}_B(y, Z))$.

Security Definition. We say that a protocol realizes a functionality f with simulation error ϵ, if there exist simulators Sim_A and Sim_B such that for any environment $\mathcal{E}$, the distributions of environment's views in the real world and ideal world are indistinguishable, that is, the statistical distance between $\mathbb{V}_{\mathcal{E}}^{(real)}$ and $\mathbb{V}_{\mathcal{E}}^{(ideal)}$ is at most ϵ. The protocol has perfect simulation error when $\epsilon = 0$.

H Maximally Renamed Symmetric Functions Without Kilian's Obstruction

A generalized function evaluation $g\colon X \times Y \to \mathbb{R}^{Z_A, Z_B}$ obtains input x from Alice and y from Bob. It samples (z_A, z_B) according to the probability distribution $g(x, y)$. Then, it outputs z_A to Alice and z_B to Bob.

Kilian's obstruction [Kil91, Kil00]. Kilian [Kil91, Kil00] presented a combinatorial characterization of two-party secure function evaluations that suffice to perform *oblivious transfer* [EGL85], which we shall refer to as *Kilian's obstruction*. A function with Kilian's obstruction has no secure protocol in the full information model (otherwise, oblivious transfer will be possible, which is impossible).

Although avoiding Kilian's obstruction is necessary, it is not sufficient for a function to have a secure protocol, for example, Kushilevitz function in Appendix E and Data-Prabhakaran function in Appendix F. For functions avoiding Kilian's obstruction, a standardization argument is possible.

Proposition 3 (Standardization [MPR13])**.** *If a general function g avoids Kilian's obstruction then there is a symmetric function $f\colon X \times Y \to \mathbb{R}^Z$ such that*

1. *For every $x, x' \in X$, $y, y' \in Y$, and $z \in Z$ the following identity holds.*

$$f(x, y)_z \cdot f(x', y')_z = f(x, y')_z \cdot f(x', y)_z.$$

2. *There is an r-round c-bit protocol for g if and only if there is an r-round c-bit protocol for the function f.*

Consequently, without loss of generality, the functions we investigate are symmetric functions in this standardized form – referred to as *(maximally renamed) symmetric functions avoiding Kilian's obstruction*. Analytically, for every output $z \in Z$, the matrices $M^{(z)}(f) := \{f(x,y)_z\}_{x,y \in X \times Y} \in \mathbb{R}^{X \times Y}$ are rank-one, which yields the standardization result of Step 0 of Section 3.

I Generalized Convex Hull

We elaborate the rationale behind referring to our recursively defined sets $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \cdots$ in Section 3 as *generalized convex hulls*. For simplicity, instead of linear maps, consider linear functionals $\varphi_1, \varphi_2 \colon \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z \to \mathbb{R}$.

Case 1. $\varphi_1 = \varphi_2 = 0$**.** In this case $\mathcal{S}^{(1)}$ is the *convex hull* of the initial set of points $\mathcal{S}^{(0)}$. Furthermore, $\mathcal{S}^{(1)} = \mathcal{S}^{(2)} = \cdots$.

Case 2. $\varphi_1 \neq 0$ **and** φ_2 **is a scalar multiple of** φ_1**.** Partition $\mathcal{S}^{(0)}$ into sets $\mathcal{S}^{(0,1)}, \mathcal{S}^{(0,2)}, \ldots, \mathcal{S}^{(0,\ell)}$ such that

1. $\varphi_1(X) = \varphi_1(Y)$, for all $X, Y \in \mathcal{S}^{(0,k)}$ and $k \in \{1, 2, \ldots, \ell\}$, and
2. $\varphi_1(X) \neq \varphi(Y)$, for all $X \in \mathcal{S}^{(0,k)}$, $Y \in \mathcal{S}^{(0,k')}$, and distinct $k, k' \in \{1, 2, \ldots, \ell\}$.

Now, $\mathcal{S}^{(1)}$ is the union of the convex hulls of the points in $\mathcal{S}^{(0,k)}$, where $k \in \{1, 2, \ldots, \ell\}$. Furthermore, $\mathcal{S}^{(1)} = \mathcal{S}^{(2)} = \cdots$.

Case 3. The linear functionals φ_1 **and** φ_2 **are linearly independent.** The non-triviality of our generalized convex hull problem arises only when φ_1 and φ_2 are linearly independent, which is the case for our research problem. Our work motivates fascinating new research problems in mathematics.

J Proof of Corollary 1

Suppose there is a secure r-round protocol for the function f. Then, it must hold that $Q^{(f)} \in \mathcal{S}^{(r)}$. Let Π be a secure protocol constructed from the WITNESS procedure with (at most) r-round for f. Suppose Alice extended τ to τ' and $f^{(\tau)} \cong (\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)}) =: Q$. Suppose that Q is a convex linear combination of $\{Q^{(k)}\}_{k=1}^{t} \in \mathcal{S}^{(r-1)}$, where $t \geqslant |X|+|Z|$. Recall that when Alice extends τ to τ', then the marginal distribution $\rho_y^{(\tau')} = \rho_y^{(\tau)}$ for any τ'. Let Q_A denote the projection of point Q on the first $|X|-1$ and last $|Z|$ coordinates. Then, Q_A is also a convex linear combination of $\{Q_A^{(k)}\}_{k \in \{1,2,\ldots,t\}}$. According to Carathéodory's theorem [Car11], there exist $1 \leqslant i_1 < i_2 < \ldots < i_\ell \leqslant t$, where $1 \leqslant \ell \leqslant |X| + |Z|$, such that Q_A is a convex linear combination of $Q_A^{(i_1)}, \ldots, Q_A^{(i_\ell)} \in \mathcal{S}^{(r-1)}$. So, it suffices to consider $t \in \{1, 2, \ldots, |X| + |Z|\}$ in Equation 7. Since corresponding to any point in $\mathcal{S}^{(r-1)}$, there exists a secure protocol of at most $r-1$ rounds realizing the function defined by that point, we can still recursively construct a secure protocol for function f. Similarly, it suffices to consider $t \in \{1, 2, \ldots, |Y| + |Z|\}$ if Bob extends the transcript. Therefore, there exists a r-round secure protocol for f such that in each round Alice needs to select a message among at most $|X|+|Z|$ messages, and so Alice needs to sends at most $\lceil \lg(|X| + |Z|) \rceil$. Furthermore, every message sent by Bob requires at most $\lceil \lg(|Y| + |Z|) \rceil$. This completes the proof.

K Examples

This section presents some additional figures visualizing our techniques. For binary input function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$, we define the projection of a point $f^{(\tau)} \cong (\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)})$ as $\mathsf{proj}\big(\pi^{(\tau)}, \rho^{(\tau)}, V^{(\tau)}\big) = (\pi_1^{(\tau)}, \rho_1^{(\tau)})$.

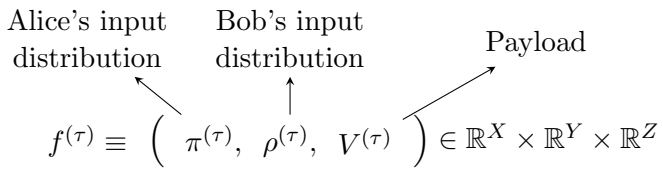


Figure 15: Pictorial encoding of the functionality given the partial transcript τ. The first component $\pi^{(\tau)}$ contains Alice's input distribution, and the second component $\rho^{(\tau)}$ contains Bob's input distribution. The last $|Z|$ coordinates carry a payload $V^{(\tau)} \in \mathbb{R}^Z$.

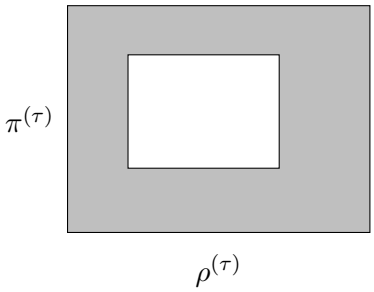


Figure 16: Support of the product distribution $\pi^{(\tau)} \times \rho^{(\tau)}$ is a combinatorial rectangle.

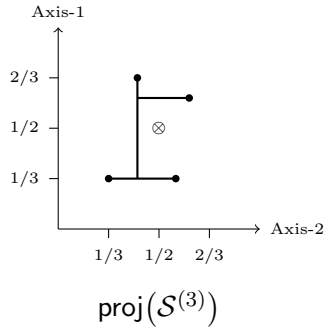


Figure 17: An example showing that there is no secure protocol for the function f defined in Figure 1 such that there is a unique transcript associated with every output symbol $z \in Z$ (a.k.a., the "unique transcript" constraint) . Under this constraint, $\mathcal{S}_i = \mathcal{S}_3$, for any $i \geqslant 4$, because any further progress needs at least two distinct transcripts associated with the output $z = 2$. Because the query point is outside $\mathcal{S}_3$, there is no secure protocol for f under the "unique transcript" constraint.

References

[AIK04] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. In *45th Annual Symposium on Foundations of Computer Science*, pages 166–175, Rome, Italy, October 17–19, 2004. IEEE Computer Society Press. doi:10.1109/FOCS.2004.20. 12

[Bea89] Donald Beaver. Perfect privacy for two-party protocols. In Joan Feigenbaum and Michael Merritt, editors, *Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey, USA, October 4-6, 1989*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 65–78. DIMACS/AMS, 1989. doi:10.1090/dimacs/002/03. 1, 2, 23

[BM04] Amos Beimel and Tal Malkin. A quantitative approach to reductions in secure computation. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 238–257, Cambridge, MA, USA, February 19–21, 2004. Springer, Heidelberg, Germany. doi:10.1007/978-3-540-24638-1_14. 12

[BPRon] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006 (second edition). 11

[Bra21] Mark Braverman. Information complexity, 2021. https://mbraverm.princeton.edu/research/information-complexity/. 1

[Can00] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, January 2000. doi:10.1007/s001459910006. 3, 28

[Car11] Constantin Carathéodory. Über den variabilitätsbereich der fourier'schen konstanten von positiven harmonischen funktionen. *Rendiconti Del Circolo Matematico di Palermo (1884-1940)*, 32(1):193–217, 1911. 9, 30

[CK89] Benny Chor and Eyal Kushilevitz. A zero-one law for Boolean privacy (extended abstract). In *21st Annual ACM Symposium on Theory of Computing*, pages 62–72, Seattle, WA, USA, May 15–17, 1989. ACM Press. doi:10.1145/73007.73013. 1, 2, 11, 23

[DP18] Deepesh Data and Manoj Prabhakaran. Towards characterizing securely computable two-party randomized functions. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018: 21st International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 10769 of *Lecture Notes in Computer Science*, pages 675–697, Rio de Janeiro, Brazil, March 25–29, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-76578-5_23. 1, 2, 4, 8, 25, 26, 28

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985. URL: http://doi.acm.org/10.1145/3812.3818, doi:10.1145/3812.3818. 29

[FKN94] Uriel Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation (extended abstract). In *26th Annual ACM Symposium on Theory of Computing*, pages 554–563, Montréal, Québec, Canada, May 23–25, 1994. ACM Press. doi:10.1145/195058.195408. 12

[GIKM98] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. In *30th Annual ACM Symposium on Theory of Computing*, pages 151–160, Dallas, TX, USA, May 23–26, 1998. ACM Press. doi:10.1145/276698.276723. 12

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, NY, USA, May 25–27, 1987. ACM Press. doi:10.1145/28395.28420. 1

[IK00] Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *41st Annual Symposium on Foundations of Computer Science*, pages 294–304, Redondo Beach, CA, USA, November 12–14, 2000. IEEE Computer Society Press. doi:10.1109/SFCS.2000.892118. 12

[IK02] Yuval Ishai and Eyal Kushilevitz. Perfect constant-round secure computation via perfect randomizing polynomials. In Peter Widmayer, Francisco Triguero Ruiz, Rafael Morales Bueno, Matthew Hennessy, Stephan Eidenbenz, and Ricardo Conejo, editors, *ICALP 2002: 29th International Colloquium on Automata, Languages and Programming*, volume 2380 of *Lecture Notes in Computer Science*, pages 244–256, Malaga, Spain, July 8–13, 2002. Springer, Heidelberg, Germany. doi:10.1007/3-540-45465-9_22. 12

[Kil91] Joe Kilian. A general completeness theorem for two-party games. In *23rd Annual ACM Symposium on Theory of Computing*, pages 553–560, New Orleans, LA, USA, May 6–8, 1991. ACM Press. doi:10.1145/103418.103475. 8, 29

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd Annual ACM Symposium on Theory of Computing*, pages 316–324, Portland, OR, USA, May 21–23, 2000. ACM Press. doi:10.1145/335305.335342. 8, 29

[KOP+19] Eyal Kushilevitz, Rafail Ostrovsky, Emmanuel Prouff, Adi Rosén, Adrian Thillard, and Damien Vergnaud. Lower and upper bounds on the randomness complexity of private computations of AND. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019: 17th Theory of Cryptography Conference, Part II*, volume 11892 of *Lecture Notes in Computer Science*, pages 386–406, Nuremberg, Germany, December 1–5, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-36033-7_15. 12

[KOR96] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Characterizing linear size circuits in terms of privacy. In *28th Annual ACM Symposium on Theory of Computing*, pages 541–550, Philadephia, PA, USA, May 22–24, 1996. ACM Press. doi:10.1145/237814.238002. 12

[Kus89] Eyal Kushilevitz. Privacy and communication complexity. In *30th Annual Symposium on Foundations of Computer Science*, pages 416–421, Research Triangle Park, NC, USA, October 30 – November 1, 1989. IEEE Computer Society Press. doi:10.1109/SFCS.1989.63512. 1, 2, 8, 11, 23, 25

[MPR13] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation functionalities. In Manoj Prabhakaran and Amit Sahai, editors, *Secure Multi-Party Computation*, volume 10 of *Cryptology and Information Security Series*, pages 249–283. IOS Press, 2013. doi:10.3233/978-1-61499-169-4-249. 1, 4, 8, 12, 19, 29

[NPS99] Moni Naor, Benny Pinkas, and Reuban Sumner. Privacy preserving auctions and mechanism design. In Stuart I. Feldman and Michael P. Wellman, editors, *Proceedings of the First ACM Conference on Electronic Commerce (EC-99), Denver, CO, USA, November 3-5, 1999*, pages 129–139. ACM, 1999. doi:10.1145/336992.337028. 1

[Wei15] Omri Weinstein. *Interactive Information Complexity and Applications*. PhD thesis, Princeton University, 2015. 1

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th Annual Symposium on Foundations of Computer Science*, pages 162–167, Toronto, Ontario, Canada, October 27–29, 1986. IEEE Computer Society Press. doi:10.1109/SFCS.1986.25. 1