2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS) | 978-1-6654-5519-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/FOCS54457.2022.00101

Geometry of Secure Two-party Computation

Saugata Basu
Purdue University
West Lafayette, USA
sbasu@purdue.edu

Hamidreza Amini Khorasgani
Purdue University
West Lafayette, USA
haminikh@purdue.edu

Hemanta K. Maji
Purdue University
West Lafayette, USA
hmaji@purdue.edu

Hai H. Nguyen
Purdue University
West Lafayette, USA
nguye245@purdue.edu

***Abstract*—What is the round and communication complexity of secure computation?**

The seminal results of Chor-Kushilevitz-Beaver (STOC–1989, FOCS–1989, DIMACS–1989) answer this question for computations with deterministic output. However, this question has remained unanswered for computations with randomized output. Our work answers this question for two-party secure function evaluation functionalities.

We introduce a geometric encoding of all candidate secure protocols for a given computation as points in a high-dimensional space. The following results follow by analyzing the properties of these sets of points.

1) **It is decidable to determine if a given computation has a secure protocol within round or communication constraints.**
2) **We construct one such protocol if it exists.**
3) **Otherwise, we present an obstruction to achieving security.**

Our technical contributions imply new information complexity bounds for secure computation.

***Index Terms*—secure computation, round complexity, communication complexity, information-theoretic security**

I. 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 [14] and Goldreich-Micali-Wigderson [8], facilitates the formalization of meaningful security where parties can interactively achieve this objective without revealing non-essential information, even a posteriori [13].

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 [2], [6], [11] characterized *decomposable functions* as ones admitting secure protocols. The case of functions with *randomized output* has remained unresolved ever since, barring highly specialized computations [7], [12] (c.f., the discussion in [12]). Data and Prabhakaran [7] characterized (1) securely realizable ternary output functions and (2) functions with 2-round secure protocols.

Even the *decidability* of this problem is unknown, let alone resolving the search and optimization analogs.

A. 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. Our main *technical idea* is an innovative geometric encoding of candidate secure (private-coin) protocols for a given computation.

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 parse tree of how this specific query point is generated from the base cases yields a secure protocol. 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*[1] and support the features in-

[1]The sets have an algebraic representation of bounded complexity.

Basu was partially supported by NSF grants CCF-1910441 and CCF-2128702.

Khorasgani, Maji, and Nguyen are supported in part by an NSF CRII Award CNS–1566499, NSF SMALL Awards CNS–1618822 and CNS–2055605, the IARPA HECTOR project, MITRE Innovation Program Academic Cybersecurity Research Awards (2019–2020, 2020–2021), a Ross-Lynn Research Scholars Grant, a Purdue Research Foundation (PRF) Award, and The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370.

978-1-6654-5519-0/22/$31.00 ©2022 IEEE
DOI 10.1109/FOCS54457.2022.00101

dicated above. Consequently, we obtain the following general feasibility, search, and optimization results.

Theorem 1 (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 (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) Lemma 1: 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.
2) 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 every round.

B. Overview of the paper.

Section II introduces the notation and some minimal definitions and Section III presents our technical approach and illustrates it using an example. Section IV summarizes the reduction of the cryptographic problem to a geometric problem. Section V and Section VI demonstrate that the geometric problem is computable. Section VIII provides secure functionalities with arbitrarily large round complexity. Section IX states all the key lemmas needed for the proof of our main results.

II. Preliminaries

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

A. System model

We consider the *Blum-Schub-Smale model of computation* [3] and the *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.

B. 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. It suffices to restrict our investigation to only symmetric functions [12], [7].

C. 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 $\mathrm{out}(\tau) \in Z$. 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 $(x, y) \in X \times Y$.
$$\mathrm{out}\,(T(x, y)) \equiv f(x, y).$$
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 $(x, y) \in X \times Y$.
$$\mathrm{Sim}_A(x, f(x, y)) \equiv T(x, y).$$
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 $(x, y) \in X \times Y$.
$$\mathrm{Sim}_B(y, f(x, y)) \equiv T(x, y).$$

This definition coincides with Canetti's *universally composable security* definition [4] where the simulator has an unbounded computational power.

D. Round and communication complexity

Our work considers 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.

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

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

III. Technical Overview

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.

Step 0: Standardization. Prior results [7], [12] 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 2 in Section IX).

$$f(x,y)_z = A_{x,z} \cdot B_{y,z} \cdot V_z \quad \text{(for all } x \in X, y \in Y, z \in Z\text{)}$$
$$\sum_{x\in X} A_{x,z} = 1 \qquad \text{(for all } z \in Z\text{)}$$
$$\sum_{y\in Y} B_{y,z} = 1 \qquad \text{(for all } z \in Z\text{)}$$

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.

$$A = \begin{cases} A_1 = (1/3, 1/3, 2/3, 3/5) \in \mathbb{R}^Z \\ A_0 = (2/3, 2/3, 1/3, 2/5) \in \mathbb{R}^Z \end{cases} \tag{1}$$

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

$$V = (13/24, 5/4, 7/6, 25/24) \in \mathbb{R}^Z \tag{3}$$

What does the state-of-the-art tell us about this function? This function avoids Kilian's obstruction [10] and does not have a 2-round protocol [7].

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.[2] 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 $\mathrm{out}(\tau)$, irrespective of the parties' inputs.

[2]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.

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 $z = \mathrm{out}(\tau)$ and $e(z) \in \{0,1\}^Z$ is the 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.

Remark 1: Security in cryptographic context is inherently a worst case notion – a protocol's insecurity is the maximum insecurity over all possible inputs of the parties. However, for perfect security, a distribution notion of security is also equivalent to the worst case security. When the environment samples the inputs independently and uniformly at random for the two parties, each input pair is picked with probability $1/|X| \cdot |Y|$. So, if a protocol is ε insecure in the worst case, then it is at least $\varepsilon/|X|\cdot|Y|$ insecure when interacting with our environment. Therefore, for perfect security, these two notions are identical.

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.

Step 2: Structure for inductive geometric characterization. We inductively prove a *function structure* result showing that the following *invariant* holds for some appropriate $V^{(\tau)} \in \mathbb{R}^Z$, and for all $x \in X, y \in Y, z \in Z$ (see Lemma 6).

$$f^{(\tau)}(x,y)_z = A^{(\tau)}_{x,z} \cdot B^{(\tau)}_{y,z} \cdot V^{(\tau)}_z, \text{ where} \tag{4}$$

$$A^{(\tau)}_{x,z} = \begin{cases} A_{x,z}/\pi^{(\tau)}_x & \text{if } \pi^{(\tau)}_x > 0 \\ 0 & \text{otherwise,} \end{cases}$$

$$B^{(\tau)}_{y,z} = \begin{cases} B_{x,z}/\rho^{(\tau)}_x & \text{if } \rho^{(\tau)}_x > 0 \\ 0 & \text{otherwise,} \end{cases}$$

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 $\Omega^{(\tau)}$ (see Lemma 4).

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 $\mathrm{out}(\tau) = z \in Z$. 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 $y \in Y$ (see Lemma 5). 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

$$P^{(z)} := \Big((A_{x,z} \colon x \in X),\ (B_{y,z} \colon y \in Y),\ e(z) \Big) \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z. \quad (5)$$

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

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

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 increasingly 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 *securely 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.

$$\varphi_1(\pi, \rho, V') := \pi \qquad \varphi_2(\pi, \rho, V') := \rho. \quad (6)$$

Therefore, the set $\mathcal{S}^{(i+1)}$ is recursively defined in Figure 2.

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 $\mathcal{S}^{(i+1)}$.

Fig. 2: Recursive procedure to construct $\mathcal{S}^{(i+1)}$ from $\mathcal{S}^{(i)}$.

Figure 3 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 3 demonstrates the evolution of the sets $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \cdots \to \mathcal{S}^{(4)}$ 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 $\rho_1^{(1)} = \cdots = \rho_1^{(t)}$.

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

$$Q^{(f)} := \left(U_X, U_Y, \frac{1}{|X \times Y|} \cdot V \right) \in \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z, \quad (7)$$

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 3 of the standardization step.

In our example function, we have (refer to Equation 3 for the value of V)

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

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

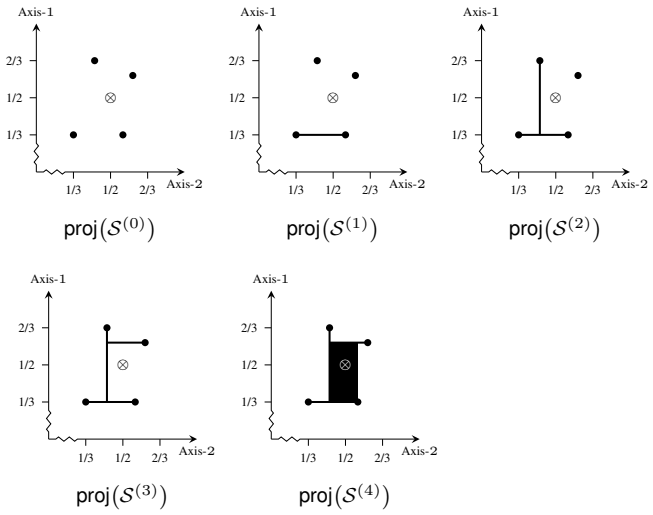

Fig. 3: Plot of the projection of the points in $\mathcal{S}^{(i)}(f)$ for $0 \leqslant i \leqslant 4$. The $\otimes$ mark represents the projection of the query point $Q^{(f)}$ (defined in Equation 7), where f is defined in Figure 1. The geometric action allows the following. For any two points in $\mathcal{S}^{(i)}$, one can add the line segment joining them to $\mathcal{S}^{(i+1)}$ if the two points have identical first or second coordinates.

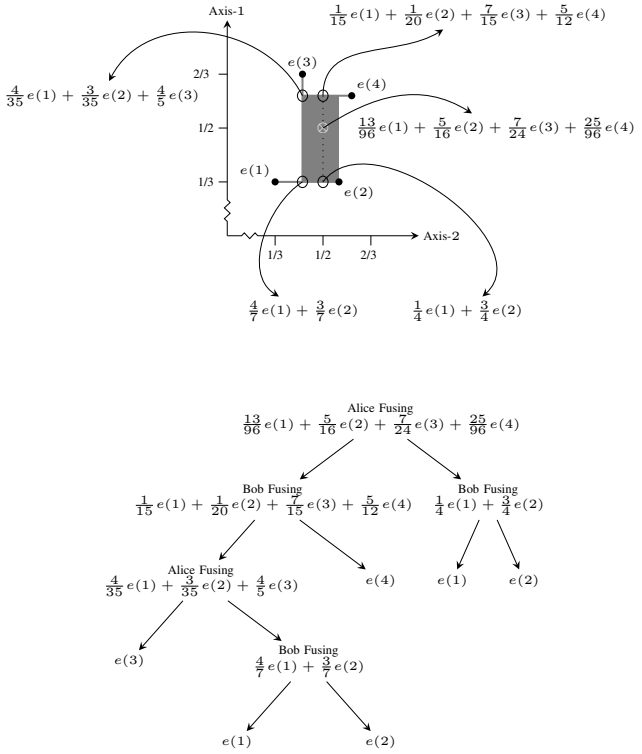

Fig. 4: For the function f in Figure 1, this figure displays the payload of "critical points" in $\mathsf{proj}\left(\mathcal{S}^{(4)}\right)$. Recall that $e(1) = (1,0,0,0), e(2) = (0,1,0,0), e(3) = (0,0,1,0)$, and $e(4) = (0,0,0,1)$, the payloads of the points in the base case. Furthermore, note that $V^{(\emptyset)} = \frac{1}{2} \times \frac{1}{2} \times V = \frac{13}{96}e(1) + \frac{5}{16}e(2) + \frac{7}{24}e(3) + \frac{25}{96}e(4)$. 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.

Figure 3) – 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 Section VII for the reconstruction algorithm). Using this step recursively, one recovers the protocol for f using a witness explaining the membership of the point $Q^{(f)} \in \mathcal{S}^{(r)}$.

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 4 demonstrates the witness of $Q^{(f)} \in \mathcal{S}^{(4)}$.

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 1. Section VIII presents this function construction.

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

IV. 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 [9], [10], 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). 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 [7], [12].

Consequently, without loss of generality, consider a standardized function $f\colon X \times Y \to \mathbb{R}^Z$ defined in step 0 of Section III. 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 7. For every $z \in Z$, define $P^{(z)}$ as in Equation 5. Define the linear maps φ_1, φ_2 as in Equation 6.

Round Complexity. Initialize the base case set $\mathcal{S}^{(0)} :=$

$\left\{P^{(z)} \colon z \in Z\right\}$. For every $i \in \{0,1,\dots\}$, recursively define

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

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 the point $Q^{(f)}$ and the set $\mathcal{S}^{(r)} \subseteq \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z$ 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

$$\mathcal{T}^{(i+1)} := \left\{ p^{(1)} Q^{(1)} + p^{(2)} Q^{(2)} \colon \begin{array}{c} Q^{(1)}, Q^{(2)} \in \mathcal{T}^{(i)}, \\ p^{(1)}, p^{(2)} \geqslant 0, \\ p^{(1)} + p^{(2)} = 1, \\ \varphi_1(Q^{(1)}) = \varphi_1(Q^{(2)}) \text{ or} \\ \varphi_2(Q^{(1)}) = \varphi_2(Q^{(2)}) \end{array} \right\} \tag{9}$$

The following statements hold.

1) A 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 the point $Q^{(f)}$ and the set $\mathcal{T}^{(c)} \subseteq \mathbb{R}^X \times \mathbb{R}^Y \times \mathbb{R}^Z$ 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 V upper bounds t in the recursive definition of $\mathcal{S}^{(i+1)}$. Subsequently, Section VI 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 V, 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.

V. Interlude: Bounding Complexity

Consider Equation 8. Define $d := |X| + |Y| + |Z|$. Let Q be a convex linear combination of $\left\{Q^{(k)}\right\}_{k \in \{1,2,\dots,t\}}$, 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 [5] 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 $Q^{(i_1)}, Q^{(i_2)}, \dots, Q^{(i_\ell)}$. Furthermore, $\varphi_b\left(Q^{(i_1)}\right) = \cdots = \varphi_b\left(Q^{(i_\ell)}\right)$. Consequently, it suffices to consider $t \in \{1,2,\dots,d+1\}$ in Equation 8 and in Figure 2.

For the specific φ_1 and φ_2 being considered in Section IV we can obtain a better upper bound on t, whence the following 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.

VI. Real Algebraic Geometry Problem

In this section, we consider only recursively generated sets $\left\{\mathcal{S}^{(i)}\right\}_{i \in \{0,1,\dots\}}$, which suffice to prove the bounds on $\left\{\mathcal{T}^{(i)}\right\}_{i \in \{0,1,\dots\}}$. Let $\varphi \colon \Omega \to \Omega'$ be an arbitrary function. The (ℓ-fold) *fibre product*, represented by $\underbrace{\Omega \times_\varphi \Omega \times_\varphi \cdots \times_\varphi \Omega}_{\ell\text{-times}}$, is defined to be the set below.

$$\left\{(\omega_1, \omega_2, \dots, \omega_\ell) \colon \omega_1, \dots, \omega_\ell \in \Omega, \varphi(\omega_1) = \cdots = \varphi(\omega_\ell)\right\}.$$

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

$$\Lambda^{(d)} := \left\{ \left(p^{(1)}, \dots, p^{(d+1)}\right) : \begin{array}{c} p^{(1)}, \dots, p^{(d+1)} \geqslant 0, \\ p^{(1)} + \ldots + p^{(d+1)} = 1 \end{array} \right\}.$$

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.

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

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

$$\mathcal{S}^{(i+1)} := \bigcup_{b=1}^{2} \left\langle \underbrace{\mathcal{S}^{(i)} \times_{\varphi_b} \mathcal{S}^{(i)} \times_{\varphi_b} \cdots \times_{\varphi_b} \mathcal{S}^{(i)}}_{(d+1)\text{-times}}, \Lambda^{(d)} \right\rangle$$

Recall that a semi-algebraic subset of $\mathbb{R}^d$ is any subset that is defined by a Boolean formula with atoms of the form $P > 0, P = 0$, where $P \in R[X_1, \dots, X_k]$. A semi-linear subset additionally has $\deg(P) \leqslant 1$.

Remark 2: 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).

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 $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(d+1)} \in \mathcal{S}^{(i-1)}$, with the corresponding edges labelled by $p_1, \ldots, p_{d+1} \in [0,1]$, 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 1: We will use the fact that the first order theory of the reals is decidable. Let $\Phi_0(\mathbf{X})$, where $\mathbf{X} = (X_1, \ldots, X_d)$ 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

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

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 [1, 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 ([1, 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 [1, page 42] and Remark 3 below).

Remark 3: 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 $\mathcal{S}^{(0)}$, which is consistent with the Blum-Schub-Smale computation model [3].

Starting from [6], [11], 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.

VII. 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 5, Equation 6 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 [12]
4) Define $d := |X| + |Y| + |Z|$.
5) Initialize $\mathbb{R}^d \supseteq \mathcal{S}^{(0)} := \{P^{(z)}\colon z \in Z\}$ (as in Equation 5)
6) Define linear maps φ_1, φ_2 as in Equation 6
7) For $i \in \{0, 1, \dots, r-1\}$, recursively define

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

8) If $Q^{(f)} \in \mathcal{S}^{(r)}$: **Return** Yes, $\Pi :=$ Witness$(\mathcal{S}^{(0)}, Q^{(f)}, r)$ as defined in Figure 6
9) **Return** False, Certificate $:= \left(Q^{(f)}, \mathcal{S}^{(r)}\right)$

Fig. 5: Procedure to decide the realizability.

The witness procedure is defined recursively in Figure 5.

We emphasize that in Step 2 above, one cannot use *any* linear λ_ks and $Q^{(k)}$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.

VIII. Functions with Large Number of Rounds

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

Lemma 1: For any $r \in \{1, 2, \dots\}$, there is a function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$, where $Z = \{1, 2, \dots, r+1\}$, such that f has an r-round secure protocol but no $(r-1)$-round secure protocol.

Construction and proof sketch. We give an intuitive description of the function and an informal proof using Figure 7. Fix any positive integer r. We construct an initial set $\mathcal{S}^{(0)} = \{q^{(0)}, q^{(1)}, \dots, q^{(r)}\}$ as in the figure. 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^*.

Witness$(\mathcal{S}^{(0)}, Q, r)$:

1) If $r = 0$, 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 $Q^{(1)}, Q^{(2)}, \cdots, Q^{(d+1)} \in \mathcal{S}^{(r-1)}$ 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 $Q = (\pi, \rho, V')$, $Q^{(k)} = (\pi^{(k)}, \rho^{(k)}, V^{(k)})$ for $k \in \{1, 2, \dots, d+1\}$.

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 k to Alice with probability $\lambda_k \cdot \rho_y^{(k)} / \rho_y$ and recursively calls Witness$(\mathcal{S}^{(0)}, Q^{(k)}, r-1)$.
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 k with probability $\lambda_k \cdot \pi_x^{(k)} / \pi_x$ to Bob and and recursively calls Witness$(\mathcal{S}^{(0)}, Q^{(k)}, r-1)$.

Fig. 6: Procedure to recover a secure protocol.

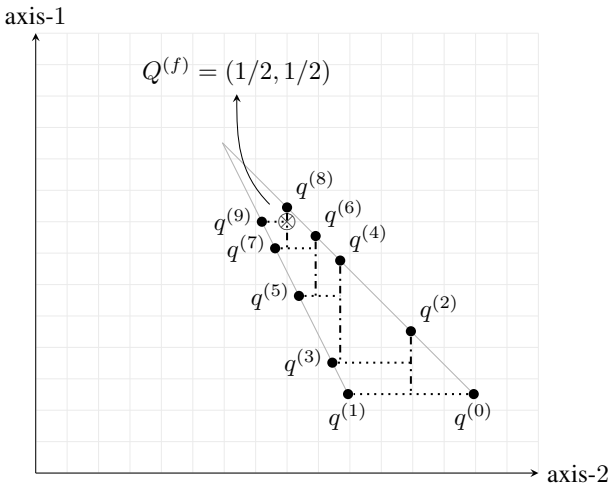

Fig. 7: An illustrative example showing that for each $r \in \{1, 2, \dots\}$ there is a $\mathcal{S}^{(0)}$ such that $\mathcal{S}^{(r-1)} \subsetneq \mathcal{S}^{(r)}$. This implies that for each r there exists a function that has a r-round secure protocol but not any $(r-1)$-round secure protocol.

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 $t \leqslant r$.

IX. Lemmas needed for the Cryptographic Reduction

This section states all the lemmas that are needed for our cryptographic reduction. The proofs of these can be found in our full version. We first recall some notations. 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 2: Suppose a function $f\colon X \times Y \to \mathbb{R}^Z$ is maximally renamed (as defined in [12]) 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.

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

Lemma 3: 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.

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

Lemma 4: 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 $\tau' \in \Omega$.

Lemma 5: In the perfectly secure protocol Π, 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 $\rho_y^{(\tau)} = B_{y,z}$.

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

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

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

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

Lemma 6: 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) $f^{(\tau)} \cong \left(A^{(\tau)}, B^{(\tau)}, V^{(\tau)}\right)$.
2) If $V_z^{(\tau)} > 0$, then $\mathrm{Supp}\left(f^{-1}(z)\right) \subseteq \mathrm{Supp}\left(\pi^{(\tau)} \times \rho^{(\tau)}\right)$.

Lemma 7: Any point $(\pi, \rho, V') \in \mathcal{S}^{(i)}$ has a perfectly secure (at most) i-round protocol, where $i \in \{0, 1, 2, \dots\}$.

References

[1] 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). 7

[2] 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. 1

[3] Lenore Blum, Mike Shub, and Steve Smale. On a theory of computation and complexity over the real numbers: NP–completeness, recursive functions and universal machines. *American Mathematical Society*, 21(1), 1989. 2, 7

[4] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, January 2000. 2

[5] 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. 6

[6] 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. 1, 7

[7] 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. 1, 2, 3, 5

[8] 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. 1

[9] 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. 5

[10] 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. 3, 5

[11] 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. 1, 7

[12] 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. 1, 2, 3, 5, 8, 9

[13] 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. 1

[14] 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. 1