Randomized Functions with High Round Complexity

Saugata Basu[1(✉)], Hamidreza Amini Khorasgani[1], Hemanta K. Maji[1], and Hai H. Nguyen[2]

[1] Department of Computer Science, Purdue University, West Lafayette, USA
{sbasu,haminikh,hmaji}@purdue.edu
[2] Department of Computer Science, ETH Zurich, Zürich, Switzerland
haihoang.nguyen@inf.ethz.ch

Abstract. Consider two-party secure function evaluation against an honest-but-curious adversary in the information-theoretic plain model. We study the round complexity of securely realizing a given secure function evaluation functionality.

Chor-Kushilevitz-Beaver (1989) proved that the round complexity of securely evaluating a deterministic function depends solely on the cardinality of its domain and range. A natural conjecture asserts that this phenomenon extends to functions with randomized output.

Our work falsifies this conjecture – revealing intricate subtleties even for this elementary security notion. For every r, we construct a function f_r with binary inputs and five output alphabets that has round complexity r. Previously, such a construction was known using $(r+1)$ output symbols. Our counter-example is optimal – we prove that any securely realizable function with binary inputs and four output alphabets has round complexity at most four.

We work in the geometric framework Basu-Khorasgani-Maji-Nguyen (FOCS–2022) introduced to investigate randomized functions' round complexity. Our work establishes a connection between secure computation and the lamination hull (geometric object originally motivated by applications in hydrodynamics). Our counterexample constructions are related to the "tartan square" construction in the lamination hull literature.

Keywords: Two-party secure computation · Information-theoretic security · Semi-honest adversary · Round complexity · Geometry of secure computation · Generalized convex hull · Lamination hull · Hydrodynamics

H. H. Nguyen—This work was done while the author was at Purdue.

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.

G. Rothblum and H. Wee (Eds.): TCC 2023, LNCS 14369, pp. 319–348, 2023.
https://doi.org/10.1007/978-3-031-48615-9_12

1 Introduction

Secure multi-party computation (MPC) [13,18] allows mutually distrusting parties to compute securely over their private data. In general, MPC requires an honest majority or oblivious transfer to compute tasks securely. Even if honest parties are not in the majority, several tasks are securely computable in the information-theoretic plain model without oblivious transfer or other hardness of computation assumptions. For example, the Dutch auction mechanism [6] securely performs auctions. These information-theoretic protocols, if they exist, are highly desirable – they are perfectly secure, fast, and require no setup or preprocessing. With rapid increases in the computational power of parties, the round complexity of these protocols becomes the primary bottleneck, significantly impacting their adoption.

This work studies the round complexity of MPC in the two-party information-theoretic plain model against honest-but-curious adversaries. Alice and Bob have private inputs $x \in X$ and $y \in Y$, respectively, and their objective is to securely sample an output z from the distribution $f(x, y)$ over the sample space Z. The distribution $f(x, y)$ is publicly known, and both parties must receive the identical output z. Parties have unbounded computational power and honestly follow the protocol; however, they are curious to obtain additional information about the other party's private input. An ideal communication channel connects the parties, and they send messages in alternating rounds.[1] The *round complexity* of securely computing f is the (worst-case) minimum number of rounds required to perform this sampling task securely.

We aim to investigate factors causing high round complexity for these secure sampling tasks. Increasing the size of the input or output sets would certainly lead to higher round complexity. However, even after fixing the input and output sets, the complexity of representing the probability distributions could influence the round complexity. There is a natural conjecture in this context.

It is conjectured that only the sizes of the input and output sets determine the round complexity. The complexity of representing the probability distributions $f(x, y)$ is absorbed within the private computation that parties perform, and it does not impact the round complexity.

This (extremely strong) conjecture is known to hold for (a) classical communication complexity where correctness (not security) is considered, (b) the secure computation tasks with deterministic output, and (c) randomized output tasks with a small output set. In the sequel, Sect. 1.1, Sect. 1.2, and Sect. 1.4 present evidence supporting the credibility of this conjecture. Our work refutes this conjecture. Section 2 presents our contributions and Sect. 3 highlights the underlying technical approach.

1.1 Discussion: Interaction in a World Without Security

Consider the *classical communication complexity* objective of correctly (possibly insecurely) evaluating a randomized output function with minimum interaction.

[1] Both parties know which party speaks in which round.

In this context, the following canonical interactive protocol is natural. Alice sends her input x to Bob. Bob samples $z \sim f(x, y)$ and sends the output z to Alice.[2] The round complexity of this (insecure) protocol is two. More generally, its communication complexity is $\log \operatorname{card}(X) + \log \operatorname{card}(Z)$, where $\operatorname{card}(S)$ represents the cardinality of the set S. These upper bounds on the interaction complexity hold irrespective of the complexity of representing the individual probabilities $f(x, y)_z$, the probability to output $z \in Z$ conditioned on the input $(x, y) \in X \times Y$. The computational complexity of sampling their output did not overflow into the interaction complexity because its impact was contained within the respective parties' private computation.

1.2 Round Complexity of Deterministic Functions

A particular class of functions widely studied in communication complexity and cryptography is the class of deterministic functions. The function f is deterministic if the support of the distribution $f(x, y)$ is a singleton set for every $(x, y) \in X \times Y$ – the output z is determined entirely by the parties' private inputs (x, y). For example, in an auction, the price is determined by all the bids.

Chor-Kushilevitz-Beaver [4,8,17] characterized all deterministic functions that are securely computable in the two-party information-theoretic plain model against honest-but-curious adversaries. The secure protocols for such functions follow a general template – parties rule out specific outputs in each round. Excluding outputs, in turn, rules out private input pairs (because each input pair produces one output). For example, the Dutch auction mechanism rules out the price that receives no bids. Such functions are called *decomposable functions* because these secure protocols incrementally decompose the feasible input-output space during their evolution. Decomposable functions are securely computable with *perfect security*.

Let us reason about the round complexity of a deterministic function $f\colon X \times Y \to Z$, represented by $\operatorname{round}(f)$. One has to exclude $\operatorname{card}(Z) - 1$ outputs so that only the output $z = f(x, y)$ remains feasible. So, if f has a secure protocol in this model, then

$$\operatorname{round}(f) \leqslant \operatorname{card}(Z) - 1.$$

Furthermore, the Markov property for interactive protocols holds in the information-theoretic plain model. The joint distribution of inputs conditioned on the protocol's evolution is always a product distribution. Excluding output also excludes private inputs of the parties. For example, if Alice sends a message in a round, she rules out some of her private inputs. This observation leads to the bound

$$\operatorname{round}(f) \leqslant 2 \cdot \operatorname{card}(X) - 1.$$

[2] We assume that parties have access to randomness with arbitrary bias; more concretely, consider the Blum-Schub-Smale model of computation [5]. For example, parties can have a random bit that is 1 with probability $1/\pi$.

Likewise, we also have

$$\text{round}\,(f) \leqslant 2 \cdot \text{card}\,(Y) - 1.$$

Combining these observations, Chor-Kushilevitz-Beaver [4,8,17] concluded that

$$\text{round}\,(f) \leqslant \min\left\{\text{card}\,(Z), 2 \cdot \text{card}\,(X), 2 \cdot \text{card}\,(Y)\right\} - 1. \tag{1}$$

The cardinalities of the private input and output sets determine the upper bound on the round complexity of f if it has a secure protocol. This phenomenon from the classical communication complexity extends to the cryptographic context for deterministic functions.

1.3 Round Complexity of Randomized Functions with Small Output Set

For functions with randomized output, the first conjecture already holds for small values of $\text{card}\,(Z)$. For example, $\text{card}\,(Z) \leqslant 3$ implies that $\text{round}\,(f) \leqslant 2$ [11]. In fact, this paper will prove that $\text{card}\,(Z) \leqslant 4$ implies $\text{round}\,(f) \leqslant 4$. It is fascinating that the complexity of sampling from the distributions $f(x, y)$ does not impact the round complexity; its role is localized to the parties' private computation.

1.4 Round Complexity of Randomized Functions (General Case)

For three decades, there was essentially no progress in determining the round complexity of securely computing general randomized functions – barring a few highly specialized cases [11]. Last year, Basu, Khorasgani, Maji, and Nguyen (FOCS 2022) [1] showed that determining "whether a randomized f has an r-round protocol or not" is decidable. They reduced this question to a geometric analog: "does a query point Q belong to a recursively-generated set $\mathcal{S}^{(r)}$." They start with an initial set of points $\mathcal{S}^{(0)}$, and recursively build $\mathcal{S}^{(i+1)}$ from the set $\mathcal{S}^{(i)}$ using a geometric action, for $i \in \{0, 1, \dots\}$. The function f has an (at most) r-round protocol if (and only if) a specific query point Q belongs to the set $\mathcal{S}^{(r)}$.

These set of points $\left\{\mathcal{S}^{(i)}\right\}_{i \geqslant 0}$ lie in the ambient space

$$\mathbb{R}^{\text{card}(X)-1} \times \mathbb{R}^{\text{card}(Y)-1} \times \mathbb{R}^{\text{card}(Z)}.$$

Again, the dimension of the ambient space (of their embedding) is determined entirely by the cardinalities of the inputs and output sets. This feature of their embedding added additional support to the conjecture.

Consider an analogy from geometry. Consider n initial points in $\mathbb{R}^d$, where $n \gg d$. At the outset, any point inside the convex hull can be expressed as a convex linear combination of the initial points that lie on the convex hull; their number can be $\gg d$. However, Carathéodory's theorem [7] states that every point in its interior is expressible as a convex linear combination of (at most) $(d + 1)$

initial points on the convex hull. At an abstract level: *canonical representations may have significantly lower complexity.* It is similar to the Pumping lemma for regular languages and (more generally) the Ogden lemma for context-free languages.

Likewise, a fascinating possibility opens up in the context of Basu et al.'s geometric problem. The canonical protocol for f could have round complexity determined solely by the dimension of their ambient space, which (in turn) is determined by the cardinality of the input and output sets. In fact, an optimistic conjecture of $\mathcal{O}\left(\operatorname{card}(Z)^2\right)$ upper bound on the round complexity appears in the full version of their paper [2, Section 7, Conjecture 1].

We Refute This Conjecture. The analogies break exactly at $|Z| = 5$. Represent a randomized function with input set $X \times Y$ and output set Z as $f\colon X \times Y \to \mathbb{R}^Z$. For every $r \in \{1, 2, \dots\}$, we construct a function $f_r\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4,5\}}$ with round complexity r. Previously, Basu et al. constructed functions $g_r\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,\dots,r+1\}}$ with round complexity r, i.e., their example had $\operatorname{card}(Z) = (r+1)$. In our example, $\operatorname{card}(Z) = 5$, a constant. Moreover, we prove the optimality of the counterexamples: Any $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4\}}$ has round complexity $\leqslant 4$.

Looking Ahead. Our results indicate that any upper bound on the round complexity of f must involve the complexity of representing (the probabilities appearing in) the function f. For example, consider a randomized function whose probabilities are integral multiples of $1/B$. Then, the round complexity of f should be upper bounded by some function of $\operatorname{card}(X)$, $\operatorname{card}(Y)$, $\operatorname{card}(Z)$, and B. The B-term represents (intuitively) "the condition number of the function f." If this dependence on B can, in fact, be a $\mathsf{poly}(\log(B))$ dependence, then it will lead to efficient secure algorithms, ones with round complexity of $\mathsf{poly}(\log B)$.

Our work considers the round complexity of perfectly secure protocols. The case of statistically secure protocols remains an interesting open problem. In fact, the decidability of the question: "Is there an r-round ε-secure protocol for f?" remains unknown, which is a more fundamental problem. Basu et al. [1] only considered the perfect security case. The technical machinery to handle statistical security for general randomized output functions *does not exist. This work does not contribute to these two research directions.*

1.5 Overview of the Paper

We discuss our contributions in Sect. 2. In Sect. 3, we provide a technical overview of our paper. In Sect. 4, we discuss the relation of our work with lamination hull. Section 5 presents the BKMN geometric framework. Section 6 introduces notations and preliminaries. Section 7 contains all results pertaining to constructing high-round complexity randomized functions. Section 8 shows that our counterexamples are optimal.

2 Our Contributions

Theorem 1 (Functions with arbitrarily high round complexity). *For any* $r \in \{1, 2, \dots, \}$, *there is a function* $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4,5\}}$ *such that* $\text{round}(f_r) = r$.

The function f_r has an r-round perfectly secure protocol (and r bits of communication) but no $(r-1)$-round perfectly secure protocol. This result proves that there are functions with arbitrary large round complexity with a constant input and output set size. Previously, Basu et al. [1] constructed functions with high round complexity with $(r+1)$ output alphabets. This result is a counterexample to the folklore conjecture. Section 7 presents the definition of the functions and the proof.

Our counterexample is also optimal, which is a consequence of our following result.

Theorem 2 (Bounded Round Complexity for $\text{card}(Z) \leqslant 4$**).** *Any function* $f \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ *with* $\text{card}(Z) \leqslant 4$ *has* $\text{round}(f) \leqslant 4$.

Section 8 proves this theorem.

3 Technical Overview of Our Results

The presentation in this work is entirely geometric. *No background in security is necessary.* We use the geometric embedding of BKMN [1] to translate round complexity problems into geometric problems. Security is already folded inside their geometric embedding.

3.1 High-Level Summary of the BKMN Geometric Framework

Section 5 presents a detailed version of this section. Consider a randomized output function $f \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$. BKMN approach considers the ambient space $\mathbb{R}^d$, where $d = \text{card}(Z) + 2$. They present the following maps

1. Function encoding. $f \mapsto (A, B, V)$, where the matrix $A \in \mathcal{M}_{2 \times \text{card}(Z)}(\mathbb{R})$[3], the matrix $B \in \mathcal{M}_{2 \times \text{card}(Z)}(\mathbb{R})$, and the vector $V \in \mathbb{R}^{\text{card}(Z)}$
2. Query point. $f \mapsto Q(f) \in \mathbb{R}^{\text{card}(Z)}$
3. Initial set. $(A, B) \mapsto \mathcal{S}^{(0)} \subseteq \mathbb{R}^d$ satisfying $\text{card}\left(\mathcal{S}^{(0)}\right) = \text{card}(Z)$.

They present the following recursive definition of $\mathcal{S}^{(i+1)} \subseteq \mathbb{R}^d$ from $\mathcal{S}^{(i)} \subseteq \mathbb{R}^d$, for all $i \in \{0, 1, \dots\}$.

$$\mathcal{S}^{(i+1)} = \left\{ \sum_{k=1}^{t} \lambda^{(k)} \cdot Q^{(k)} \;:\; \begin{array}{c} t \in \{1, 2, \dots\}, \\ \lambda^{(1)}, \lambda^{(2)}, \dots, \lambda^{(t)} \geqslant 0, \\ \lambda^{(1)} + \lambda^{(2)} + \cdots + \lambda^{(t)} = 1, \\ Q^{(1)}, Q^{(2)}, \dots, Q^{(t)} \in \mathcal{S}^{(i)}, \text{ and} \\ \left(Q_1^{(1)} = Q_1^{(2)} = \cdots = Q_1^{(t)} \text{ or} \right. \\ \left. Q_2^{(1)} = Q_2^{(2)} = \cdots = Q_2^{(t)} \right) \end{array} \right\}.$$

[3] $\mathcal{M}_{m \times n}(\mathbb{R})$ denotes the set of all m-by-n matrices with elements in $\mathbb{R}$.

Intuitively, this recursive definition ensures the following. Pick any t points $Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)} \in \mathcal{S}^{(i)}$, where $t \in \{1, 2, \ldots\}$. If the first coordinates of all these t points are identical, or the second coordinates of all these t points are identical, then add all possible convex linear combinations (i.e., the convex hull) of $\left\{Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)}\right\}$ to the set $\mathcal{S}^{(i+1)}$.

Remark 1 (Communication complexity). Restricting the recursive definition to $t = 2$ corresponds to investigating the communication complexity of f. This version of the recursion is closely connected to the lamination hull defined in Sect. 4.

Observe that, in the recursive definition, the points need not be distinct. Therefore, choosing $Q^{(1)} = Q^{(2)} = \cdots = Q^{(t)}$ ensures that $\mathcal{S}^{(i)} \subseteq \mathcal{S}^{(i+1)}$. Using this recursive definition, we have the following sequence of sets in $\mathbb{R}^d$:

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

Connection to Round Complexity of Secure Computation. BKMN [1] proved that, for all $r \in \{0, 1, \ldots\}$, $\operatorname{round}(f) \leqslant r$ if and only if $Q(f) \in \mathcal{S}^{(r)}$. Therefore, to prove $\operatorname{round}(f) = r$, it suffices to prove that $Q(f) \in \mathcal{S}^{(r)} \setminus \mathcal{S}^{(r-1)}$.

3.2 The "Tartan Square" Meets Secure Computation

Our objective is to prove that there is a function $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$, where $Z = \{1, 2, \ldots, 5\}$, such that $f_r \in \mathcal{S}^{(r)} \setminus \mathcal{S}^{(r-1)}$, for every $r \in \{1, 2, \ldots\}$. Recall that $\mathcal{S}^{(0)}$ is determined by f_r and $\operatorname{card}\left(\mathcal{S}^{(0)}\right) = \operatorname{card}(Z) = 5$. Furthermore, all the sets $\mathcal{S}^{(i)}$ are in ambient space $\mathbb{R}^7$, for $i \in \{0, 1, \ldots\}$.

A preliminary step towards designing such functions is to determine an initial set of points $\mathcal{S}^{(0)}$ such that we have

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

Otherwise, suppose $\mathcal{S}^{(i)} = \mathcal{S}^{(i+1)}$, for some $i \in \{0, 1, \ldots\}$. Then, $\mathcal{S}^{(j)} = \mathcal{S}^{(i)}$, for all $j \geqslant i$, and the round complexity cannot surpass i. So, our objective is to construct an *initial set $\mathcal{S}^{(0)}$ of constant size in an ambient space of constant dimension* such that the evolution of the sequence $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \cdots$ does not stabilize. It is unclear whether such an initial set $\mathcal{S}^{(0)}$ even exists.

Illustrative Example. We present an initial set $\mathcal{S}^{(0)} \subseteq \mathbb{R}^3$ such that the evolution of the recursively defined sets does not stabilize. We emphasize that this illustrative example is for intuition purposes only. The actual constructions are presented in Sect. 7, where the ambient space is $\mathbb{R}^7$.

We work in the ambient space $\mathbb{R}^3$ for the illustrative example. Consider an initial set of points

$$\mathbb{R}^3 \supseteq \mathcal{S}^{(0)} := \Big\{(2,0,0),\ (0,1,0),\ (1,3,0),\ (3,2,0),\ (2,1,1)\Big\}$$

1. For example, consider the points $(0, 1, 0)$ and $(2, 1, 1)$ in the set $\mathcal{S}^{(0)}$. The recursive definition allows the addition of the line segment $\overline{PQ}$ to the set $\mathcal{S}^{(1)}$. In particular, this line segment's midpoint $(1, 1, 1/2)$ is in the set $\mathcal{S}^{(1)}$.
2. Similarly, considering the points $(1, 3, 0)$ and $(1, 1, 1/2)$ in the set $\mathcal{S}^{(1)}$, we conclude that their midpoint $(1, 2, 1/4)$ is in the set $\mathcal{S}^{(2)}$.
3. Now, consider the points $(3, 2, 0)$ and $(1, 2, 1/4)$ in the set $\mathcal{S}^{(2)}$. Their midpoint $(2, 2, 1/8)$ is in the set $\mathcal{S}^{(3)}$.
4. Finally, the midpoint of the points $(2, 0, 0)$ and $(2, 2, 1/8)$ in the set $\mathcal{S}^{(3)}$ is $(2, 1, 1/16)$, which is in the set $\mathcal{S}^{(4)}$.

Let us summarize what we have achieved thus far. Beginning with the point $(2, 1, 1) \in \mathcal{S}^{(0)}$, we identified the point $(2, 1, 1/16) \in \mathcal{S}^{(4)}$. One can prove that this point $(2, 1, 1/16) \notin \mathcal{S}^{(3)}$. Therefore, we conclude that the point $(2, 1, 1/16) \in \mathcal{S}^{(4)} \setminus \mathcal{S}^{(3)}$.

Using analogous steps as above, starting instead with the point $(2, 1, 1/16) \in \mathcal{S}^{(4)} \setminus \mathcal{S}^{(3)}$ will lead to the point $\left(2, 1, 1/(16)^2\right) \in \mathcal{S}^{(8)} \setminus \mathcal{S}^{(7)}$ In general, using this construction, we will have

$$\left(2, 1, \frac{1}{16^k}\right) \in \mathcal{S}^{(4k)} \setminus \mathcal{S}^{(4k-1)}.$$

This sequence of points, for $k \in \{0, 1, 2, \dots\}$, demonstrate that the sequence $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \cdots$ does not stabilize. This example is the "tartan square" from the lamination hull literature; refer to Remark 2 in Sect. 4.

This illustrative example leads to the following conclusion. In an ambient space of constant dimension and starting with a suitable initial set $\mathcal{S}^{(0)}$ of constant size, the sequence $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \cdots$ may not stabilize.

3.3 Overview: Proof of Theorem 1

For $r \in \{1, 2, \dots\}$, we will appropriately choose the probabilities of the function $f_r \colon \{0, 1\} \times \{0, 1\} \to \mathbb{R}^Z$, such that $\operatorname{card}(Z) = 5$. Using the BKMN geometric framework (see Sect. 3.1), we will generate:

1. Function encoding (A, B, V_r). We emphasize that all our functions f_r are designed so that they map to the same (A, B); only V_r is different.
2. Query point $Q(f_r) \in \mathbb{R}^7$.
3. Initial point set $\mathcal{S}^{(0)} \subseteq \mathbb{R}^7$, which is identical for all f_r because (a) all functions map to identical (A, B), and (b) (A, B) alone determine $\mathcal{S}^{(0)}$.

Sect. 5.1 presents the definition of the function f_r.

Next, the choice of the $\mathcal{S}^{(0)}$ ensures that the evolution of the sets $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \cdots$ does not stabilize. It essentially mimics the tartan square construction of Sect. 3.2. However, we emphasize that in this section, the ambient space is $\mathbb{R}^7$ (the ambient space for the tartan square example was $\mathbb{R}^3$). Furthermore, we design our function f_r such that the corresponding query point $Q(f_r) \in \mathcal{S}^{(r)} \setminus \mathcal{S}^{(r-1)}$. Consequently, we have $\operatorname{round}(f_r) = r$.

3.4 Overview: Proof of Theorem 2

We aim to prove that round $(f) \leqslant 4$, for any function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ such that card $(Z) \leqslant 4$. Toward this objective, we begin with the following observations.

1. Recall that in the BKMN framework card $\left(\mathcal{S}^{(0)}\right) =$ card (Z).
2. Furthermore, if $\mathcal{S}^{(4)} = \mathcal{S}^{(5)}$, then $\mathcal{S}^{(j)} = \mathcal{S}^{(4)}$, for all $j \geqslant 4$. In this case, round $(f) \leqslant 4$, because $\mathcal{S}^{(r)} \setminus \mathcal{S}^{(r-1)} = \emptyset$, for all $r \in \{5, 6, \dots\}$.

To prove our theorem, it will suffice to prove that the evolution of the sets $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \cdots$ stabilizes by $i = 4$ when card $\left(\mathcal{S}^{(0)}\right) \leqslant 4$.[4] We prove this result using an exhaustive case analysis (see Sect. 8).

4 Lamination Hull

Consider an ambient space $\mathbb{R}^d$. The *lamination hull* is parameterized by a set of points $\Lambda \subseteq \mathbb{R}^d$. Given a set of initial point $\mathcal{S}^{(0,\Lambda)} \subseteq \mathbb{R}^d$, recursively define $\mathcal{S}^{(i+1,\Lambda)}$ from $\mathcal{S}^{(i)}$ as follows

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

Intuitively, one can add the line segment $\overline{Q^{(1)}Q^{(2)}}$ to the set $\mathcal{S}^{(i+1,\Lambda)}$ for any $Q^{(1)}, Q^{(2)} \in \mathcal{S}^{(i,\Lambda)}$ if $Q^{(1)} - Q^{(2)} \in \Lambda$. The lamination hull is the limit of the sequence $\mathcal{S}^{(0,\Lambda)} \to \mathcal{S}^{(1,\Lambda)} \to \mathcal{S}^{(2,\Lambda)} \to \cdots$. This hull is tied to computing the stationary solutions to the following differential equations underlying incompressible porous media [9,10,12,14].

Incompressible Porous Media (IPM) Equations

Conservation of Mass, Incompressibility, and Darcy's Law

$$\partial_t \rho + \nabla \cdot (\rho \boldsymbol{v}) = 0, \qquad \nabla \cdot \boldsymbol{v} = 0, \qquad \frac{\mu}{\kappa} \boldsymbol{v} = -\nabla p - \rho \boldsymbol{g}, \tag{2}$$

where ρ is the fluid density, $\boldsymbol{v}$ is the fluid velocity, and $\boldsymbol{g}$ is the gravity.

When $\Lambda = (0, \mathbb{R}, \dots, \mathbb{R}) \cup (\mathbb{R}, 0, \mathbb{R}, \dots, \mathbb{R}) \subseteq \mathbb{R}^d$, the sequence $\mathcal{S}^{(0,\Lambda)} \to \mathcal{S}^{(1,\Lambda)} \to \mathcal{S}^{(2,\Lambda)} \to \cdots$ is identical to the sequence defined by Basu et al. [1] for the communication complexity case (see Remark 1). Basu et al. [1] proved that the points in the recursively defined sets are related to secure computation protocols. As a consequence of this connection, secure computation protocols manifest in physical processes in nature. This connection is mentioned in [3, Page 20].

[4] We highlight a subtlety. We only need to prove that $\mathcal{S}^{(4)} = \mathcal{S}^{(5)}$. It is inconsequential if they have stabilized even earlier. For example, it may be the case that $\mathcal{S}^{(j)} = \mathcal{S}^{(j+1)}$ for some $j \in \{0, 1, 2, 3\}$.

Remark 2 (Independent discovery of the "tartan square" construction). Our work independently discovered the "tartan square" construction in the lamination hull literature [16, Figure 2, Page 3]. Consider ambient dimension $\mathbb{R}^3$ and $\Lambda = (0, \mathbb{R}, \mathbb{R}) \cup (\mathbb{R}, 0, \mathbb{R}) \subseteq \mathbb{R}^d$. The "tartan square" is a set of 5 points in $\mathbb{R}^3$ such that the sequence $\mathcal{S}^{(0,\Lambda)} \to \mathcal{S}^{(1,\Lambda)} \to \mathcal{S}^{(2,\Lambda)} \to \cdots$ does not stabilize. Section 3 uses this example to provide the intuition underlying our counterexample constructions.

5 BKMN Geometric Framework: A Formal Introduction

Basu-Khorasgani-Maji-Nguyen [1] presents a new approach for studying the round complexity of any (symmetric) functionality $f\colon X \times Y \to \mathbb{R}^Z$. In the following discussion, we shall recall this approach for the particular case where the input domain satisfies $X = Y = \{0, 1\}$.

From the given functionality f, BKMN22 defines the following maps.

1. Function encoding: $f \mapsto (A, B, V)$
2. Query point: $f \mapsto Q(f)$
3. Initial set: $(A, B) \mapsto \mathcal{S}^{(0)}$
4. Recursive construction: $\mathcal{S}^{(i)} \mapsto \mathcal{S}^{(i+1)}$ for any $i \in \{0, 1, 2, \dots\}$.

Function Encoding

There are matrices $A \in \mathcal{M}_{2\times \mathrm{card}(Z)}(\mathbb{R})$, $B \in \mathcal{M}_{2\times \mathrm{card}(Z)}(\mathbb{R})$, and vector $V \in \mathbb{R}^{\mathrm{card}(Z)}$ such that

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

$$\sum_{x \in X} A_{x,z} = 1, \qquad \sum_{y \in Y} B_{y,z} = 1 \text{ for all } z \in Z.^{a}$$

[a] If such an encoding does not exist, there is no secure protocol for f [15].

The query point $Q(f)$ is constructed as follows.

Query Point Construction

$$Q(f) := \left(1/2,\ 1/2,\ \frac{1}{4} \cdot V\right) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}^{\mathrm{card}(Z)}$$

The initial set $\mathcal{S}^{(0)}$ is constructed from (A, B) as follows.

Constructing the initial set $\mathcal{S}^{(0)}$ from (A, B)

$$\mathcal{S}^{(0)} := \{(A_{0,z},\ B_{0,z},\ e(z)) \colon z \in Z\} \subseteq \mathbb{R}^d,$$

where $d := \text{card}\,(Z) + 2$, and $e(z)$ is the standard unit vector whose coordinates are all zeros except that the z-th coordinate is one.

They consider the sequence $\mathcal{S}^{(0)}, \mathcal{S}^{(1)}, \ldots, \mathcal{S}^{(i)}, \ldots$ where for any $i \in \{0, 1, \ldots\}$, the geometric action that recursively generates $\mathcal{S}^{(i+1)}$ from $\mathcal{S}^{(i)}$ is defined as follows:

Geometric Action: Constructing $\mathcal{S}^{(i+1)}$ from $\mathcal{S}^{(i)}$

For any $t \in \{1, 2, \ldots\}$ and points $Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)} \in \mathcal{S}^{(i)}$, add all convex linear combinations of the points $\{Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)}\}$ to the set $\mathcal{S}^{(i+1)}$ if (and only if)

1. $Q_1^{(1)} = Q_1^{(2)} = \cdots = Q_1^{(t)}$, or
2. $Q_2^{(1)} = Q_2^{(2)} = \cdots = Q_2^{(t)}$.

For a point $Q \in \mathbb{R}^d$, Q_1 represents the first coordinate of Q, and Q_2 represents the second coordinate of Q.

Some Clarifications.

1. A convex linear combination of the points $Q^{(1)}, \ldots, Q^{(t)}$, is a point of the form $\lambda^{(1)} \cdot Q^{(1)} + \cdots + \lambda^{(t)} \cdot Q^{(t)}$, where $\lambda^{(1)}, \ldots, \lambda^{(t)} \geqslant 0$ and $\sum_{i=1}^{t} \lambda^{(i)} = 1$. All possible convex linear combinations consider all possible such $\lambda^{(1)}, \ldots \lambda^{(t)}$ values.
2. The points $Q^{(1)}, \ldots, Q^{(t)}$ in the definition need not be distinct
3. Considering $t = 1$ in the definition above ensures that $\mathcal{S}^{(i)} \subseteq \mathcal{S}^{(i+1)}$.
4. Since efficiency is not a consideration in the current context, we consider $t \in \{1, 2, \ldots\}$. Otherwise, by Carathéodory's theorem [7], it suffices to consider only $t = (d + 1)$.

BKMN's Reduction. Given the initial set $\mathcal{S}^{(0)}$, one constructs the sequence $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \ldots$ recursively based on the geometric action. Basu et al. reduce the problem of the round complexity of secure computation of randomized functions to the problem of testing whether a point belongs to a set in a high dimensional space.

BKMN's Reduction

For any $r \in \{1, 2, \dots\}$,

1. $\text{round}(f) \leqslant r$ if and only if $Q(f) \in \mathcal{S}^{(r)}$.
2. $\text{round}(f) = r$ if and only if $Q(f) \in \mathcal{S}^{(r)} \setminus \mathcal{S}^{(r-1)}$.

5.1 An Example

In this section, we consider an example and find the corresponding encoding, query point, and sets $\mathcal{S}^{(0)}, \mathcal{S}^{(1)}, \dots$ based on BKMN's approach. For any $r = 4k+1$ where $k \in \{0, 1, \dots\}$, we construct a functionality $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4,5\}}$ and then show in Sect. 7 that $\text{round}(f_r) = r$. We emphasize that it is also possible to construct such functionality for the cases that $r = 4k$ or $r = 4k+2$ or $r = 4k+3$ where $k \in \{0, 1, 2, \dots\}$.

Consider the following functionality

$$
\begin{aligned}
f_{4k+1}(0,0) &= \left(\frac{3}{16} \cdot \sigma_k,\ \frac{1}{4} \cdot \sigma_{k+1},\ \frac{1}{8} \cdot \sigma_k,\ \frac{3}{8} \cdot \sigma_k,\ \frac{3}{2^{4k+2}} \right), \\
f_{4k+1}(0,1) &= \left(\frac{9}{16} \cdot \sigma_k,\ \frac{1}{4} \cdot \sigma_{k+1},\ 0 \cdot \sigma_k,\ \frac{1}{8} \cdot \sigma_k,\ \frac{3}{2^{4k+2}} \right), \\
f_{4k+1}(1,0) &= \left(\frac{1}{16} \cdot \sigma_k,\ \frac{3}{4} \cdot \sigma_{k+1},\ \frac{1}{8} \cdot \sigma_k,\ 0 \cdot \sigma_k,\ \frac{1}{2^{4k+2}} \right), \\
f_{4k+1}(1,1) &= \left(\frac{3}{16} \cdot \sigma_k,\ \frac{3}{4} \cdot \sigma_{k+1},\ 0 \cdot \sigma_k,\ 0 \cdot \sigma_k,\ \frac{1}{2^{4k+2}} \right),
\end{aligned}
$$

where $\sigma_k := \frac{1-(1/16)^k}{1-1/16}$ for $k \in \{0, 1, 2, \dots\}$. Following BKMN's approach (refer to Sect. 5), the encoding of f_{4k+1} is the triplet (A, B, V_{4k+1}), where

$$
\begin{aligned}
A &= \begin{pmatrix} 3/4, & 1/4, & 1/2, & 1, & 3/4 \\ 1/4, & 3/4, & 1/2, & 0, & 1/4 \end{pmatrix} \in \mathcal{M}_{2\times 5}(\mathbb{R}), \\
B &= \begin{pmatrix} 1/4, & 1/2, & 1, & 3/4, & 1/2 \\ 3/4, & 1/2, & 0, & 1/4, & 1/2 \end{pmatrix} \in \mathcal{M}_{2\times 5}(\mathbb{R}), \\
V_{4k+1} &= \left(\sigma_k, 2\sigma_{k+1}, \frac{\sigma_k}{4}, \frac{\sigma_k}{2}, \frac{1}{2^{4k-1}} \right) \in \mathbb{R}^5.
\end{aligned}
$$

Note that the first row of matrix A corresponds to input $X = 0$, and its second row corresponds to $X = 1$. Similarly, the first row of B corresponds to input $Y = 0$, and the other row corresponds to $Y = 1$. The initial set $\mathcal{S}^{(0)}$ is derived from (A, B, V_{4k+1}) as follows.

$$
\begin{aligned}
\mathcal{S}^{(0)} &= \{P^{(z)} \colon z \in \{1, 2, 3, 4, 5\}\}, \text{ where} \\
P^{(1)} &= (3/4,\ 1/4,\ 1, 0, 0, 0, 0),
\end{aligned}
$$

$$P^{(2)} = (1/4,\ 1/2,\ 0,1,0,0,0),$$
$$P^{(3)} = (1/2,\quad 1\ ,\ 0,0,1,0,0),$$
$$P^{(4)} = (\ 1\ ,\ 3/4,\ 0,0,0,1,0),$$
$$P^{(5)} = (3/4,\ 1/2,\ 0,0,0,0,1).$$

Note that $\mathcal{S}^{(i)} \subseteq \mathbb{R}^7$ for all $i \in \{0,1,\dots\}$. The query point is defined as

$$Q(f_{4k+1}) = \left(\frac{1}{2},\ \frac{1}{2},\ \frac{1}{4}\cdot\frac{\sigma_k}{4},\ \frac{\sigma_{k+1}}{2},\ \frac{\sigma_k}{16},\ \frac{\sigma_k}{8},\ \frac{1}{2^{4k+1}}\right) \in \mathbb{R}^7.$$

To prove that $round(f_{4k+1}) = 4k+1$, it suffices to prove the following result.

Lemma 1. *It holds that* $Q(f_{4k+1}) \in \mathcal{S}^{(4k+1)} \setminus \mathcal{S}^{(4k)}$.

We provide a proof for Lemma 1 in Sect. 7 (refer to the proof of Theorem 3).

6 Preliminaries

This section introduces some notations and definitions to facilitate our presentation.

6.1 Notations

We will use the following notations for a point $p \in \mathbb{R}^d$, a scalar $c \in \mathbb{R}$, and a set $\mathcal{S} \subseteq \mathbb{R}^d$.

$$p + \mathcal{S} \ :=\ \{p + q\colon q \in \mathcal{S}\}, \quad c \cdot \mathcal{S} \ :=\ \{c \cdot q\colon q \in \mathcal{S}\}.$$

We use the standard notations $\setminus, \cup, \cap$ to denote the minus, union, and intersection operators on sets, respectively.

6.2 Convex Geometry

For any two points $x, y \in \mathbb{R}^d$, the *line segment* between x and y, denoted as $\overline{xy}$, is the set of all points $t \cdot x + (1-t) \cdot y$ for $t \in [0,1]$. A subset of $\mathbb{R}^d$ is a *convex set* if, given any two points in the subset, the subset contains the whole line segment joining them. A *convex combination* is a linear combination of points in which all coefficients are non-negative and sum up to 1. An *extreme point* of a convex set $S \subseteq \mathbb{R}^d$ is a point that does not lie on any open line segment joining two distinct points of S.

Definition 1 (Convex Hull). *For any set* $S \subseteq \mathbb{R}^d$*, the convex hull of* S*, denoted as* $\mathsf{conv}(S)$*, is the set of all convex combinations of points in* S*.*

For example, every line segment is the convex hull of the two endpoints. The following facts follow directly from the definition of the convex hull.

Fact 1. *For any subset* $\mathcal{S} \subseteq \mathbb{R}^d$*, it holds that* $\mathsf{conv}(\mathsf{conv}(\mathcal{S})) = \mathsf{conv}(\mathcal{S})$.

Fact 2. *For any* $\mathcal{S} \subseteq \mathcal{T} \subseteq \mathbb{R}^d$*, it holds that* $\mathsf{conv}(\mathcal{S}) \subseteq \mathsf{conv}(\mathcal{T})$.

7 Functions with High Round Complexity

This section provides a formal proof for Theorem 1 restated as follows.

Theorem 3. *For every $r \in \mathbb{N}$, there exists a function $f_r\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ such that* $\mathrm{card}\,(Z) = 5$ *and f_r has r-round perfectly secure protocol but no $(r-1)$-round secure protocol.*

We begin with introducing some notations. Let $P = (P_1, P_2, P_3, P_4, P_5, P_6, P_7)$ denote a point in $\mathbb{R}^2 \times \mathbb{R}^5$. We define the following projections

$$\begin{aligned} &\pi\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}^2, && \pi(P) \;:=\; (P_1, P_2)\\ &\pi_1\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}, && \pi_1(P) \;:=\; P_1\\ &\pi_2\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}, && \pi_2(P) \;:=\; P_2\\ &\rho\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}^5, && \rho(P) \;:=\; (P_3, P_4, P_5, P_6, P_7) \end{aligned}$$

We use $e_i \in \mathbb{R}^5$, where $i \in \{1, \ldots, 5\}$, to represent the i^{th} vector of the standard basis for $\mathbb{R}^5$. All coordinates of e_i are 0 except the i^{th} coordinate, which is equal to 1. For example, if $P = (1/4, 1/2, 0, 1, 0, 0, 0)$, then

$$\pi(P) = (1/4, 1/2), \quad \pi_1(P) = 1/4, \pi_2(P) = 1/2, \quad \rho(P) = (0, 1, 0, 0, 0) = e_2.$$

Our Initial Set of Points. We define the following five points in $\mathbb{R}^2$

$$a_1 = (3/4, 1/4),\ a_2 = (1/4, 1/2),\ a_3 = (1/2, 1),\ a_4 = (1, 3/4),\ a_5 = (3/4, 1/2).$$

The initial set $\mathcal{S}^{(0)}$ is defined as

$$\mathcal{S}^{(0)} \;:=\; \{P \in \mathbb{R}^2 \times \mathbb{R}^5 \colon \exists\ i \in \{1,2,3,4,5\},\ \pi(P) = a_i \text{ and } \rho(P) = e_i\}.$$

Recursive construction of $\mathcal{S}^{(i)}$. For $i \in \{1, 2, \ldots\}$, let $\mathcal{S}^{(i)} \subseteq \mathbb{R}^2 \times \mathbb{R}^5$ be the set defined recursively from $\mathcal{S}^{(i-1)}$ according to Fig. 1.

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

$$\pi_1(Q^{(1)}) = \pi_1(Q^{(2)}) = \cdots = \pi_1(Q^{(t)}),\ \text{or}$$
$$\pi_2(Q^{(1)}) = \pi_2(Q^{(2)}) = \cdots = \pi_2(Q^{(t)})$$

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

Fig. 1. Recursive procedure to construct $\mathcal{S}^{(i)}$ from $\mathcal{S}^{(i-1)}$ for $i \in \{1, 2, \ldots\}$.

In addition to Theorem 3, we shall also prove the following result.

Theorem 4 (Does not Stabilize). *For all $i \in \{1, 2, \ldots\}$, $\mathcal{S}^{(i-1)} \subsetneq \mathcal{S}^{(i)}$.*

Intuitively, the choice of the $\mathcal{S}^{(0)}$ ensures that the evolution of the sets $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \cdots$ does not stabilize.

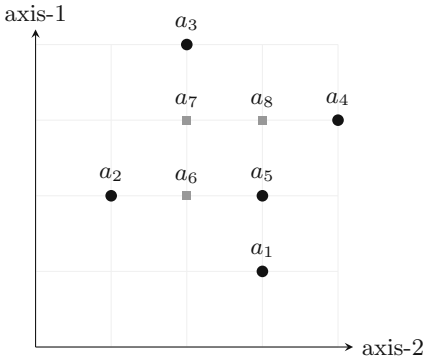


Fig. 2. An example showing that the sequence $\{\mathcal{S}^{(i)}\}_{i=0}^{\infty}$ does not stabilize.

Additional points and notations. We define the following additional points for our analysis (refer to Fig. 2).

$$a_6 = (1/2, 1/2),\ a_7 = (1/2, 3/4),\ a_8 = (3/4, 3/4)$$

Let $\overline{a_1 a_8}$ denote the set of points on the line segment that connects the point a_1 to the point a_8. The segments $\overline{a_2 a_5}, \overline{a_3 a_6}, \overline{a_4 a_7}$ are defined similarly. For any set $\Omega \subseteq \mathbb{R}^2$, we define the set $\mathcal{S}_{\Omega}^{(i)}$ as follows.

$$\mathcal{S}_{\Omega}^{(i)} \ := \ \{Q \in \mathcal{S}^{(i)} : \pi(Q) \in \Omega\}$$

Whenever Ω is a singleton set, we omit the brackets. For example,

$$\begin{aligned}
&\mathcal{S}_{a_1}^{(0)} = \{(3/4, 1/4, 1, 0, 0, 0, 0)\}, \quad \mathcal{S}_{a_2}^{(0)} = \{(1/4, 1/2, 0, 1, 0, 0, 0)\},\\
&\mathcal{S}_{a_3}^{(0)} = \{(1/2, \quad 1, 0, 0, 1, 0, 0)\}, \quad \mathcal{S}_{a_4}^{(0)} = \{(1, 3/4, 0, 0, 0, 1, 0)\},\\
&\mathcal{S}_{a_5}^{(0)} = \{(3/4, 1/2, 0, 0, 0, 0, 1)\}, \quad \mathcal{S}_{a_6}^{(0)} = \mathcal{S}_{a_7}^{(0)} = \mathcal{S}_{a_8}^{(0)} = \emptyset.
\end{aligned}$$

Moreover, for any set $\Omega \subseteq \mathbb{R}^2 \times \mathbb{R}^5$, we define $\rho(\Omega) \ := \ \{\rho(P) : P \in \Omega\}$. For example, $\rho(\mathcal{S}_{a_4}^{(0)}) = \{(0, 0, 0, 1, 0)\} = \{e_4\}$.

For $i \in \{0, 1, 2, \dots\}$, we define

$$\begin{aligned}
\sigma_i \ &:= \ \sum_{k=0}^{i-1} \frac{1}{16^k} = \frac{1 - (1/16)^i}{1 - 1/16},\\
\alpha_i \ &:= \quad \sigma_i \cdot \frac{e_1}{2} + \quad \sigma_i \cdot \frac{e_4}{4} + \quad \sigma_i \cdot \frac{e_3}{8} + \sigma_i \cdot \frac{e_2}{16} + \frac{e_5}{16^i},\\
\beta_i \ &:= \ \sigma_{i+1} \cdot \frac{e_2}{2} + \quad \sigma_i \cdot \frac{e_1}{4} + \quad \sigma_i \cdot \frac{e_4}{8} + \sigma_i \cdot \frac{e_3}{16} + \frac{e_5}{2^{4i+1}},\\
\gamma_i \ &:= \ \sigma_{i+1} \cdot \frac{e_3}{2} + \sigma_{i+1} \cdot \frac{e_2}{4} + \quad \sigma_i \cdot \frac{e_1}{8} + \sigma_i \cdot \frac{e_4}{16} + \frac{e_5}{2^{4i+2}},\\
\delta_i \ &:= \ \sigma_{i+1} \cdot \frac{e_4}{2} + \sigma_{i+1} \cdot \frac{e_3}{4} + \sigma_{i+1} \cdot \frac{e_2}{8} + \sigma_i \cdot \frac{e_1}{16} + \frac{e_5}{2^{4i+3}}.
\end{aligned}$$

Moreover, $\alpha^*, \beta^*, \gamma^*, \delta^*$ are defined as the limit of sequences $\alpha_i, \beta_i, \gamma_i, \delta_i$ respectively (refer to Proposition 4). We prove some algebraic properties of $\alpha_i, \beta_i, \gamma_i, \delta_i$ in Sect. 7.4.

Now, we state all claims needed for the proof of Theorem 3. Assuming these claims, we first prove Theorem 3 in Sect. 7.1. Then, we prove these claims in Sect. 7.2

Lemma 2. *For every $i \in \{0, 1, 2, \dots\}$, the following identities hold.*

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(4i)}) = \rho(\mathcal{S}_{a_5}^{(4i+1)}) = \rho(\mathcal{S}_{a_5}^{(4i+2)}) = \rho(\mathcal{S}_{a_5}^{(4i+3)}),\\
\rho(\mathcal{S}_{a_6}^{(4i+1)}) = \rho(\mathcal{S}_{a_6}^{(4i+2)}) = \rho(\mathcal{S}_{a_6}^{(4i+3)}) = \rho(\mathcal{S}_{a_6}^{(4i+4)}),\\
\rho(\mathcal{S}_{a_7}^{(4i+2)}) = \rho(\mathcal{S}_{a_7}^{(4i+3)}) = \rho(\mathcal{S}_{a_7}^{(4i+4)}) = \rho(\mathcal{S}_{a_5}^{(4i+5)}),\\
\rho(\mathcal{S}_{a_8}^{(4i+3)}) = \rho(\mathcal{S}_{a_8}^{(4i+4)}) = \rho(\mathcal{S}_{a_8}^{(4i+5)}) = \rho(\mathcal{S}_{a_8}^{(4i+6)}).
\end{aligned}$$

Lemma 3. *For all $i \in \{0, 1. \dots\}$,*

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(4i)}) = \mathsf{conv}(\{\alpha_0, \alpha_i)\}),\ \rho(\mathcal{S}_{a_6}^{(4i+1)}) = \mathsf{conv}(\{\beta_0, \beta_i\}),\\
\rho(\mathcal{S}_{a_7}^{(4i+2)}) = \mathsf{conv}(\{\gamma_0, \gamma_i\}),\ \rho(\mathcal{S}_{a_8}^{(4i+3)}) = \mathsf{conv}(\{\delta_0, \delta_i\}).
\end{aligned}$$

Lemma 4. *For any $i \in \{0, 1, 2, \dots\}$, it holds that*

$$\alpha_{i+1} \notin \rho(\mathcal{S}_{a_5}^{(4i)}),\ \beta_{i+1} \notin \rho(\mathcal{S}_{a_6}^{(4i+1)}),\ \gamma_{i+1} \notin \rho(\mathcal{S}_{a_7}^{(4i+2)}),\ \delta_{i+1} \notin \rho(\mathcal{S}_{a_8}^{(4i+3)}).$$

7.1 Proofs of Theorem 3 and Theorem 4

Proof (of Theorem 3). Suppose $r = 4k + 1$, where $k \in \{0, 1, 2, \dots\}$. Recall the functionality f_{4k+1} defined in Sect. 5.1

$$\begin{aligned}
f_{4k+1}(0,0) &= \left(\frac{3}{16}\cdot\sigma_k, \frac{1}{4}\cdot\sigma_{k+1}, \frac{1}{8}\cdot\sigma_k, \frac{3}{8}\cdot\sigma_k, \frac{3}{2^{4k+2}}\right)\\
f_{4k+1}(0,1) &= \left(\frac{9}{16}\cdot\sigma_k, \frac{1}{4}\cdot\sigma_{k+1}, 0\cdot\sigma_k, \frac{1}{8}\cdot\sigma_k, \frac{3}{2^{4k+2}}\right)\\
f_{4k+1}(1,0) &= \left(\frac{1}{16}\cdot\sigma_k, \frac{3}{4}\cdot\sigma_{k+1}, \frac{1}{8}\cdot\sigma_k, 0\cdot\sigma_k, \frac{1}{2^{4k+2}}\right)\\
f_{4k+1}(1,1) &= \left(\frac{3}{16}\cdot\sigma_k, \frac{3}{4}\cdot\sigma_{k+1}, 0\cdot\sigma_k, 0\cdot\sigma_k, \frac{1}{2^{4k+2}}\right)
\end{aligned}$$

where $\sigma_k := \frac{1-(1/16)^k}{1-1/16}$ for $k \in \{0, 1, 2, \dots\}$. As we discussed in Sect. 5.1, the encoding of f_{4k+1} is the triplet (A, B, V_{4k+1}), where

$$\begin{aligned}
A &= \begin{pmatrix} 3/4, & 1/4, & 1/2, & 1, & 3/4 \\ 1/4, & 3/4, & 1/2, & 0, & 1/4 \end{pmatrix} \in \mathcal{M}_{2\times 5}(\mathbb{R}),\\
B &= \begin{pmatrix} 1/4, & 1/2, & 1, & 3/4, & 1/2 \\ 3/4, & 1/2, & 0, & 1/4, & 1/2 \end{pmatrix} \in \mathcal{M}_{2\times 5}(\mathbb{R}),\\
V_{4k+1} &= \left(\sigma_k, 2\sigma_{k+1}, \frac{\sigma_k}{4}, \frac{\sigma_k}{2}, \frac{1}{2^{4k-1}}\right) \in \mathbb{R}^5.
\end{aligned}$$

and the query point is the following:

$$Q(f_{4k+1}) = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{4}\cdot\frac{\sigma_k}{4}, \frac{\sigma_{k+1}}{2}, \frac{\sigma_k}{16}, \frac{\sigma_k}{8}, \frac{1}{2^{4k+1}}\right) \in \mathbb{R}^7.$$

Now, recall that

$$\beta_k = \sigma_{k+1}\cdot\frac{e_2}{2} + \quad \sigma_k\cdot\frac{e_1}{4} + \quad \sigma_k\cdot\frac{e_4}{8} + \sigma_k\cdot\frac{e_3}{16} + \frac{e_5}{2^{4k+1}}$$

This implies $\rho(Q(f_{4k+1})) = \beta_k$. Thus, it follows from Lemma 3 and Lemma 4 that $\rho(Q(f_{4k+1})) \in \mathcal{S}_{a_6}^{(4k+1)}$ but $\rho(Q(f_{4k+1})) \notin \mathcal{S}_{a_6}^{(4(k-1)+1)}$. Moreover, Lemma 2 implies that $\mathcal{S}_{a_6}^{(4(k-1)+1)} = \mathcal{S}_{a_6}^{(4k)}$. Thus, we conclude that

$$Q(f_{4k+1}) \in \mathcal{S}^{(4k+1)} \setminus \mathcal{S}^{(4k)}$$

which is what we promised to prove in Lemma 1. This implies that f_r has r round secure protocol but no $(r-1)$ secure protocol.

We can extend the proof to the case that $r \neq 4k+1$ for any k. The idea is similar. We can find 3 different family of functions corresponding to $r = 4k, r = 4k+2, r = 4k+3$. We only need to choose a different query point in Fig. 2, a_5, a_7, or a_8 and scale that figure and transfer it appropriately such that query points $(1/2, 1/2)$ is on a_5, a_7, or a_8 depending on the remainder of division of r by 4. Then, we can find appropriate functionalities. This completes the proof of the theorem.

Proof (of Theorem 4). Theorem 4 follows directly from Lemma 3 and Lemma 2.

7.2 Proofs of Claims Needed for Theorem 3

This section proves all the claims needed for Theorem 3 assuming other results that will be proved in Sect. 7.3.

Proof (of Lemma 2). We prove by induction on i.

Base Case. From the recursion in Lemma 6, one can verify that

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(0)}) = \rho(\mathcal{S}_{a_5}^{(1)}) = \rho(\mathcal{S}_{a_5}^{(2)}) = \rho(\mathcal{S}_{a_5}^{(3)}) &= \{e_5\},\\
\rho(\mathcal{S}_{a_6}^{(1)}) = \rho(\mathcal{S}_{a_6}^{(2)}) = \rho(\mathcal{S}_{a_6}^{(3)}) = \rho(\mathcal{S}_{a_6}^{(4)}) &= \frac{e_2+e_5}{2},\\
\rho(\mathcal{S}_{a_7}^{(2)}) = \rho(\mathcal{S}_{a_7}^{(3)}) = \rho(\mathcal{S}_{a_7}^{(4)}) = \rho(\mathcal{S}_{a_7}^{(5)}) &= \frac{e_3}{2} + \frac{e_2+e_5}{4},\\
\rho(\mathcal{S}_{a_8}^{(3)}) = \rho(\mathcal{S}_{a_8}^{(4)}) = \rho(\mathcal{S}_{a_8}^{(5)}) = \rho(\mathcal{S}_{a_8}^{(6)}) &= \frac{e_4}{2} + \frac{e_3}{4} + \frac{e_2+e_5}{8}.
\end{aligned}$$

Induction Step. Suppose the induction hypothesis holds for $(i-1)$. It follows from Lemma 6 that

$$\rho(\mathcal{S}_{a_5}^{(4i+3)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+2)}) \cup \frac{1}{2}\cdot\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+2)})\right)\right)$$

$$= \mathsf{conv}\left(\mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+1)}) \cup \frac{1}{2}\cdot\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+1)})\right)\right) \cup \frac{1}{2}\cdot\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+2)})\right)\right)$$

By the induction hypothesis, $\rho(\mathcal{S}_{a_8}^{(4i+2)}) = \rho(\mathcal{S}_{a_8}^{(4i+1)})$. Therefore, we have

$$\frac{1}{2}\cdot\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+1)})\right) = \frac{1}{2}\cdot\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+2)})\right)$$

This, together with Fact 1 and Lemma 6, implies that

$$\rho(\mathcal{S}_{a_5}^{(4i+3)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+1)}) \cup \frac{1}{2}\cdot\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+1)})\right)\right) = \rho(\mathcal{S}_{a_5}^{(4i+2)}).$$

Likewise, one can show that $\rho(\mathcal{S}_{a_5}^{(4i+2)}) = \rho(\mathcal{S}_{a_5}^{(4i+1)})$ and $\rho(\mathcal{S}_{a_5}^{(4i+1)}) = \rho(\mathcal{S}_{a_5}^{(4i)})$. These imply that

$$\rho(\mathcal{S}_{a_5}^{(4i)}) = \rho(\mathcal{S}_{a_5}^{(4i+1)}) = \rho(\mathcal{S}_{a_5}^{(4i+2)}) = \rho(\mathcal{S}_{a_5}^{(4i+3)}).$$

The proof of other equalities is similar.

Proof (of Lemma 3). We prove by induction on i (refer to Fig. 3).

Base Case. For $i = 0$,

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(0)}) &= \{\alpha_0\} = \{e_5\},\\
\rho(\mathcal{S}_{a_6}^{(1)}) &= \{\beta_0\} = \left\{\frac{e_2+e_5}{2}\right\},\\
\rho(\mathcal{S}_{a_7}^{(2)}) &= \{\gamma_0\} = \left\{\frac{e_3}{2} + \frac{e_2+e_5}{4}\right\},\\
\rho(\mathcal{S}_{a_8}^{(3)}) &= \{\delta_0\} = \left\{\frac{e_4}{2} + \frac{e_3}{4} + \frac{e_2+e_5}{8}\right\}.
\end{aligned}$$

Induction Step. Suppose the lemma is true for i. We shall show that it is true for $i+1$.

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(4i+4)}) &= \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+3)}) \cup \frac{1}{2}\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+3)})\right)\right) && (\textit{Lemma 6})\\
&= \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i)}) \cup \frac{1}{2}\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+3)})\right)\right) && (\textit{Lemma 2})\\
&= \mathsf{conv}\left(\mathsf{conv}(\{\alpha_0,\alpha_i\}) \cup \frac{1}{2}\left(e_1 + \mathsf{conv}(\{\delta_0,\delta_i\})\right)\right) && (\text{Induction hypothesis})\\
&= \mathsf{conv}\left(\{\alpha_0,\alpha_i\} \cup \left\{\frac{e_1+\delta_0}{2}, \frac{e_1+\delta_i}{2}\right\}\right) && (\textit{Fact 1})\\
&= \mathsf{conv}\left(\{\alpha_0,\alpha_i\} \cup \{\alpha_1,\alpha_{i+1}\}\right) && \textit{Proposition 2}\\
&= \mathsf{conv}(\{\alpha_0,\alpha_{i+1}\}) && (\textit{Proposition 5 and Fact 2})
\end{aligned}$$

Similarly, it holds that

$$\begin{aligned}
\rho(\mathcal{S}_{a_6}^{(4i+5)}) &= \mathsf{conv}(\{\beta_0,\beta_{i+1}\}),\\
\rho(\mathcal{S}_{a_7}^{(4i+6)}) &= \mathsf{conv}(\{\gamma_0,\gamma_{i+1}\}),\\
\rho(\mathcal{S}_{a_8}^{(4i+7)}) &= \mathsf{conv}(\{\delta_0,\delta_{i+1}\}),
\end{aligned}$$

which completes the proof.

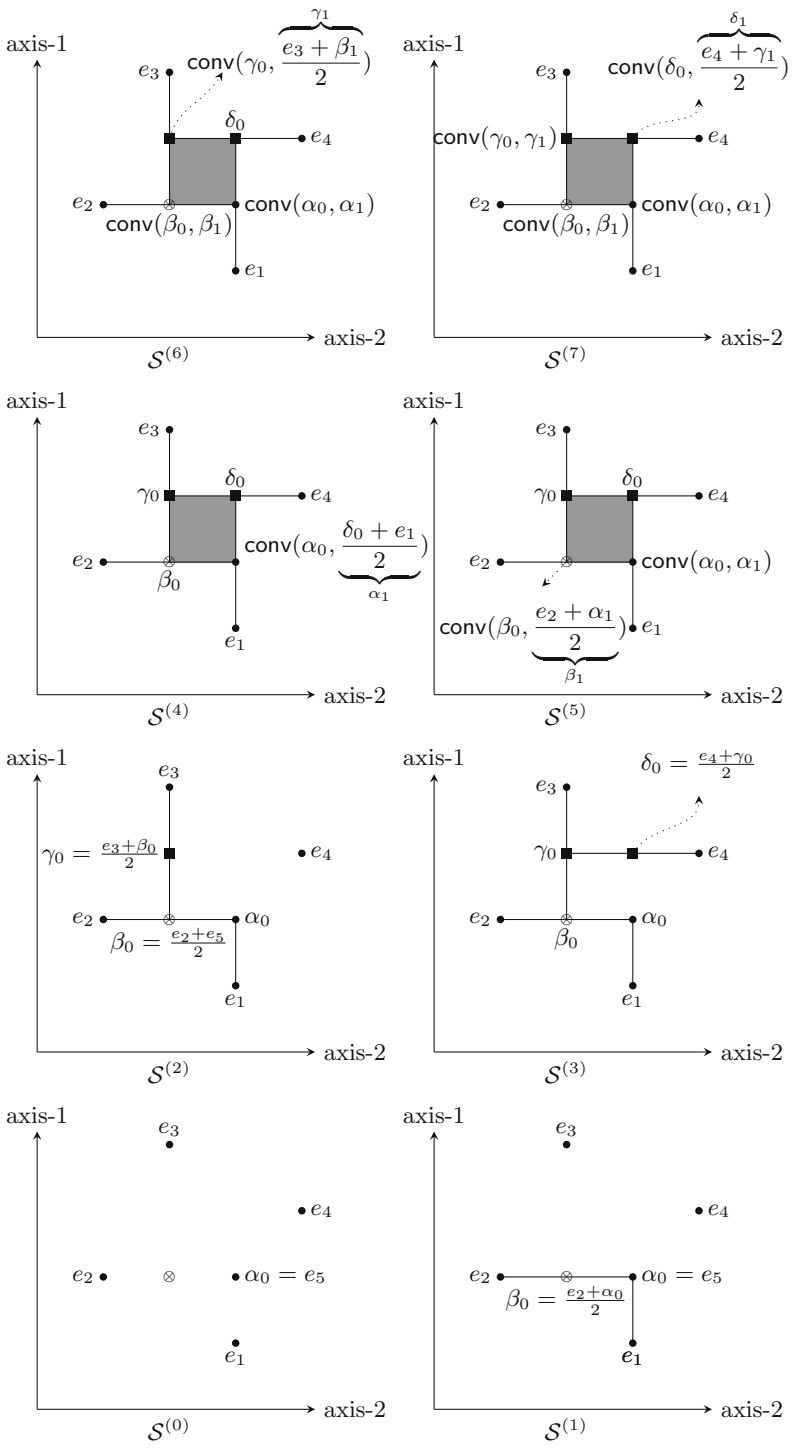


Fig. 3. The evolution of $\rho(\mathcal{S}^{(i)}_{a_5}), \rho(\mathcal{S}^{(i)}_{a_6}), \rho(\mathcal{S}^{(i)}_{a_7}), \rho(\mathcal{S}^{(i)}_{a_8})$ up to step eight.

Proof (of Lemma 4). Lemma 4 follows directly from Lemma 3 and Proposition 5.

7.3 Proof of Claims Needed for Lemma 2, Lemma 3, and Lemma 4

This section proves results that are needed for the proof of Lemma 2, Lemma 3, and Lemma 4. The result below follows directly from the definition of the sequence $\{\mathcal{S}_i\}_{i=0}^{\infty}$.

Proposition 1. *For any set Ω and any $i \in \{0, 1, \dots\}$, the following property holds.*

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

The following result says that for any $i \in \{0, 1, \dots\}$, all the points in the line segment $\overline{a_1 a_8}$ at round $(i+1)$ except the new ones at the point a_8 are constructed solely from the points at a_1, a_8, a_5 at round i, and similarly for others.

Lemma 5. *For every $i \in \{0, 1, \dots\}$,*

$$\mathcal{S}_{\overline{a_1 a_8}}^{(i+1)} \setminus \left(\mathcal{S}_{a_8}^{(i+1)} \setminus \mathcal{S}_{a_8}^{(i)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_1}^{(i)} \cup \mathcal{S}_{a_8}^{(i)} \cup \mathcal{S}_{a_5}^{(i)}\right),$$

$$\mathcal{S}_{\overline{a_2 a_5}}^{(i+1)} \setminus \left(\mathcal{S}_{a_5}^{(i+1)} \setminus \mathcal{S}_{a_5}^{(i)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_2}^{(i)} \cup \mathcal{S}_{a_5}^{(i)} \cup \mathcal{S}_{a_6}^{(i)}\right),$$

$$\mathcal{S}_{\overline{a_3 a_6}}^{(i+1)} \setminus \left(\mathcal{S}_{a_6}^{(i+1)} \setminus \mathcal{S}_{a_6}^{(i)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_3}^{(i)} \cup \mathcal{S}_{a_6}^{(i)} \cup \mathcal{S}_{a_7}^{(i)}\right),$$

$$\mathcal{S}_{\overline{a_4 a_7}}^{(i+1)} \setminus \left(\mathcal{S}_{a_7}^{(i+1)} \setminus \mathcal{S}_{a_7}^{(i)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_4}^{(i)} \cup \mathcal{S}_{a_7}^{(i)} \cup \mathcal{S}_{a_8}^{(i)}\right).$$

Proof (of Lemma 5). We prove by induction on i.

Base Case. For $i = 0$, we have

$$\mathcal{S}_{a_1}^{(0)} = \{(3/4, 1/4, 1, 0, 0, 0, 0, 0)\},\ \mathcal{S}_{a_5}^{(0)} = \{(3/4, 1/2, 0, 0, 0, 0, 1)\},\ \mathcal{S}_{a_8}^{(0)} = \emptyset.$$

It implies that

$$\mathsf{conv}\left(\mathcal{S}_{a_1}^{(0)} \cup \mathcal{S}_{a_8}^{(0)} \cup \mathcal{S}_{a_5}^{(0)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_1}^{(0)} \cup \mathcal{S}_{a_5}^{(0)}\right).$$

Observe that $\pi_1(P) = 3/4$, for any point $P \in \mathcal{S}_{a_1}^{(0)} \cup \mathcal{S}_{a_5}^{(0)}$. Therefore, any convex combination of a point in $\mathcal{S}_{a_1}^{(0)}$ and a point in $\mathcal{S}_{a_5}^{(0)}$ is in the set $\mathcal{S}_{\overline{a_1 a_8}}^{(1)}$. Notice that $\mathcal{S}_{a_8}^{(0)} = \mathcal{S}_{a_8}^{(1)} = \emptyset$. This shows that

$$\mathsf{conv}\left(\mathcal{S}_{a_1}^{(0)} \cup \mathcal{S}_{a_8}^{(0)} \cup \mathcal{S}_{a_5}^{(0)}\right) \subseteq \mathcal{S}_{\overline{a_1 a_8}}^{(1)} = \mathcal{S}_{\overline{a_1 a_8}}^{(1)} \setminus \left(\mathcal{S}_{a_8}^{(1)} \setminus \mathcal{S}_{a_8}^{(0)}\right).$$

To prove the other direction, observe that any point in $\mathcal{S}_{\overline{a_1 a_8}}^{(1)}$ except for the points in $\mathcal{S}_{a_8}^{(1)} \setminus \mathcal{S}_{a_8}^{(0)}$ is a convex combination of a set of points in $\mathcal{S}_{\overline{a_1 a_8}}^{(0)} = \mathcal{S}_{a_1}^{(0)} \cup \mathcal{S}_{a_5}^{(0)}$ by definition. Thus, it follows that

$$\mathcal{S}_{\overline{a_1 a_8}}^{(1)} \setminus \left(\mathcal{S}_{a_8}^{(1)} \setminus \mathcal{S}_{a_8}^{(0)}\right) = \mathcal{S}_{\overline{a_1 a_8}}^{(1)} \subseteq \mathsf{conv}\left(\mathcal{S}_{a_1}^{(0)} \cup \mathcal{S}_{a_5}^{(0)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_1}^{(0)} \cup \mathcal{S}_{a_8}^{(0)} \cup \mathcal{S}_{a_5}^{(0)}\right).$$

Induction Hypothesis. We assume that

$$\mathcal{S}^{(i)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i)}_{a_8} \setminus \mathcal{S}^{(i-1)}_{a_8}\right) = \mathsf{conv}\left(\mathcal{S}^{(i-1)}_{a_1} \cup \mathcal{S}^{(i-1)}_{a_8} \cup \mathcal{S}^{(i-1)}_{a_5}\right),$$

and similarly for other equations.

Induction Step. Note that for any point P in the set $\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}$, we have $\pi_1(P) = 3/4$. Therefore,

$$\mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right) \subseteq \mathcal{S}^{(i+1)}_{\overline{a_1 a_8}}$$

Since $\overline{a_4 a_7}$ is the only line segment that contains a_8 such that a_8 is not an end point of it, we have:

$$\left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) \cap \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right) = \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) \cap \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_8}\right) = \emptyset.$$

Therefore, we conclude that

$$\mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right) \subseteq \mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right).$$

To prove the other direction, note that any point in $\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i+1)}_{a_8}$ is constructed from a convex combination of the points in $\mathcal{S}^{(i)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i)}_{a_8}$. Thus, we have

$$\begin{aligned}
\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i+1)}_{a_8} &\subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i)}_{a_8}\right) \\
&\subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i)}_{a_8} \setminus \mathcal{S}^{(i-1)}_{a_8}\right)\right) && (\textit{Fact } 2) \\
&= \mathsf{conv}\left(\mathsf{conv}\left(\mathcal{S}^{(i-1)}_{a_1} \cup \mathcal{S}^{(i-1)}_{a_8} \cup \mathcal{S}^{(i-1)}_{a_5}\right)\right) && (\text{Induction hypothesis}) \\
&= \mathsf{conv}\left(\mathcal{S}^{(i-1)}_{a_1} \cup \mathcal{S}^{(i-1)}_{a_8} \cup \mathcal{S}^{(i-1)}_{a_5}\right) && (\textit{Fact } 1) \\
&\subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right), && (\textit{Proposition } 1 \text{ and } \textit{Fact } 2)
\end{aligned}$$

Since $\mathcal{S}^{(i)}_{a_8} \subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right)$, it follows that

$$\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) = \left(\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i+1)}_{a_8}\right) \cup \mathcal{S}^{(i)}_{a_8} \subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right).$$

We have shown that

$$\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) = \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right).$$

We prove other equations in a similar manner, which completes the proof.

Next, using Lemma 5, we prove a recursive construction of the projection ρ at the points a_i for $1 \leqslant i \leqslant 8$.

Lemma 6. *For all* $i \in \{0, 1, \dots\}$,

$$\rho(\mathcal{S}_{a_1}^{(i)}) = \{e_1\},\ \rho(\mathcal{S}_{a_2}^{(i)}) = \{e_2\},\ \rho(\mathcal{S}_{a_3}^{(i)}) = \{e_3\},\ \rho(\mathcal{S}_{a_4}^{(i)}) = \{e_4\}.$$

Furthermore, for all $i \in \{1, 2, \dots, \}$,

$$\rho(\mathcal{S}_{a_5}^{(0)}) = \{e_5\},\ \rho(\mathcal{S}_{a_5}^{(i+1)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(i)}) \cup \frac{1}{2} \cdot \left(e_1 + \rho(\mathcal{S}_{a_8}^{(i)})\right)\right),$$

$$\rho(\mathcal{S}_{a_6}^{(0)}) = \emptyset,\ \rho(\mathcal{S}_{a_6}^{(i+1)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_6}^{(i)}) \cup \frac{1}{2} \cdot \left(e_2 + \rho(\mathcal{S}_{a_5}^{(i)})\right)\right),$$

$$\rho(\mathcal{S}_{a_7}^{(0)}) = \emptyset,\ \rho(\mathcal{S}_{a_7}^{(i+1)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_7}^{(i)}) \cup \frac{1}{2} \cdot \left(e_3 + \rho(\mathcal{S}_{a_6}^{(i)})\right)\right),$$

$$\rho(\mathcal{S}_{a_8}^{(0)}) = \emptyset,\ \rho(\mathcal{S}_{a_8}^{(i+1)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_8}^{(i)}) \cup \frac{1}{2} \cdot \left(e_4 + \rho(\mathcal{S}_{a_7}^{(i)})\right)\right).$$

Proof (of Lemma 6). Initially, $\rho(\mathcal{S}_{a_1}^{(0)}) = \{e_1\}$. At any round $i \in \{1, 2 \dots\}$, there is no new point constructed at a_1, since a_1 is an extreme point of $\mathsf{conv}(a_1, a_2, a_3, a_4, a_5)$. Therefore, $\rho(\mathcal{S}_{a_1}^{(i)}) = \{e_1\}$. Similarly, we have

$$\rho(\mathcal{S}_{a_2}^{(i)}) = \{e_2\},\ \rho(\mathcal{S}_{a_3}^{(i)}) = \{e_3\},\ \rho(\mathcal{S}_{a_4}^{(i)}) = \{e_4\},\ \text{for every } i \in \{0, 1, \dots\}.$$

Let $P \in \mathcal{S}_{a_5}^{(i+1)}$. It follows from Lemma 5 that there are points $P_{a_1} \in \mathcal{S}_{a_1}^{(i)}$, $P_{a_8} \in \mathcal{S}_{a_8}^{(i)}$, $P_{a_5} \in \mathcal{S}_{a_5}^{(i)}$, and $\lambda_1, \lambda_8, \lambda_5 \geqslant 0$ such that

$$P = \lambda_1 \cdot P_{a_1} + \lambda_8 \cdot P_{a_8} + \lambda_5 \cdot P_{a_5},\ \text{and}\ \lambda_1 + \lambda_8 + \lambda_5 = 1.$$

Projecting these points into the second coordinate, we have

$$\pi_2(P) = \lambda_1 \cdot \pi_2(P_{a_1}) + \lambda_8 \cdot \pi_2(P_{a_8}) + \lambda_5 \cdot \pi_2(P_{a_5}).$$

This together with $\pi_2(P) = \pi_2(P_{a_5}) = \frac{1}{2}(\pi_2(P_{a_1}) + \pi_2(P_{a_8}))$ implies that $\lambda_1 = \lambda_8$. Thus, the point P is in the set $\mathsf{conv}\left(\mathcal{S}_{a_5}^{(i)} \cup \frac{1}{2} \cdot \left(\mathcal{S}_{a_1}^{(i)} + \mathcal{S}_{a_8}^{(i)}\right)\right)$. This implies that

$$\mathcal{S}_{a_5}^{(i+1)} \subseteq \mathsf{conv}\left(\mathcal{S}_{a_5}^{(i)} \cup \frac{1}{2} \cdot \left(\mathcal{S}_{a_1}^{(i)} + \mathcal{S}_{a_8}^{(i)}\right)\right).$$

Projecting this fact into coordinates $\{3, 4, 5, 6, 7\}$ yields

$$\begin{aligned}\rho(\mathcal{S}_{a_5}^{(i+1)}) &\subseteq \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(i)}) \cup \frac{1}{2} \cdot \left(\rho(\mathcal{S}_{a_1}^{(i)}) \cup \rho(\mathcal{S}_{a_8}^{(i)})\right)\right) \\ &= \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(i)}) \cup \frac{1}{2} \cdot \left(e_1 + \rho(\mathcal{S}_{a_8}^{(i)})\right)\right) \qquad (\text{since } \rho(\mathcal{S}_{a_1}^{(i)}) = \{e_1\}).\end{aligned}$$

Conversely, it suffices to show that

$$\mathsf{conv}\left(\mathcal{S}_{a_5}^{(i)} \cup \frac{1}{2} \cdot \left(\mathcal{S}_{a_1}^{(i)} + \mathcal{S}_{a_8}^{(i)}\right)\right) \subseteq \mathcal{S}_{a_5}^{(i+1)}.$$

This follows directly from the fact that a_5 is the midpoint of the segment $\overline{a_1 a_8}$. We have proved that

$$\rho(\mathcal{S}^{(i+1)}_{a_5}) = \mathsf{conv}\left(\rho(\mathcal{S}^{(i)}_{a_5}) \cup \frac{1}{2} \cdot \left(e_1 + \rho(\mathcal{S}^{(i)}_{a_8})\right)\right).$$

Similarly, the other three equations for a_6, a_7, a_8 also hold.

7.4 Properties of the Four Sequences

We first recall the definition of the four sequences $\alpha_i, \beta_i, \gamma_i, \sigma_i$ as follows. For $i \in \{0, 1, 2, \dots\}$,

$$\begin{aligned}
\sigma_i &:= \sum_{k=0}^{i-1} \frac{1}{16^k} = \frac{1-(1/16)^i}{1-1/16}, \\
\alpha_i &:= \quad \sigma_i \cdot \frac{e_1}{2} + \quad \sigma_i \cdot \frac{e_4}{4} + \quad \sigma_i \cdot \frac{e_3}{8} + \sigma_i \cdot \frac{e_2}{16} + \frac{e_5}{16^i}, \\
\beta_i &:= \sigma_{i+1} \cdot \frac{e_2}{2} + \quad \sigma_i \cdot \frac{e_1}{4} + \quad \sigma_i \cdot \frac{e_4}{8} + \sigma_i \cdot \frac{e_3}{16} + \frac{e_5}{2^{4i+1}}, \\
\gamma_i &:= \sigma_{i+1} \cdot \frac{e_3}{2} + \sigma_{i+1} \cdot \frac{e_2}{4} + \quad \sigma_i \cdot \frac{e_1}{8} + \sigma_i \cdot \frac{e_4}{16} + \frac{e_5}{2^{4i+2}}, \\
\delta_i &:= \sigma_{i+1} \cdot \frac{e_4}{2} + \sigma_{i+1} \cdot \frac{e_3}{4} + \sigma_{i+1} \cdot \frac{e_2}{8} + \sigma_i \cdot \frac{e_1}{16} + \frac{e_5}{2^{4i+3}}.
\end{aligned}$$

Proposition 2. *For all $i \in \{0, 1, \dots\}$,*

$$\alpha_{i+1} = \frac{e_1 + \delta_i}{2},\ \beta_i = \frac{e_2 + \alpha_i}{2},\ \gamma_i = \frac{e_3 + \beta_i}{2},\ \delta_i = \frac{e_4 + \gamma_i}{2}.$$

Proof. By definition,

$$\begin{aligned}
\frac{e_2 + \alpha_i}{2} &= \frac{e_2}{2} + \frac{\sigma_i}{2} \cdot (\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}) + \frac{e_5}{2 \cdot 16^i} \\
&= \frac{e_2}{2} + \frac{\sigma_i}{2} \cdot (\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}) + \frac{e_5}{2 \cdot 16^i} \\
&= \left(1 + \frac{\sigma_i}{16}\right) \cdot \frac{e_2}{2} + \sigma_i \cdot (\frac{e_1}{4} + \frac{e_4}{8} + \frac{e_3}{16}) + \frac{e_5}{2 \cdot 16^i} \\
&= \sigma_{i+1} \cdot \frac{e_2}{2} + \sigma_i \cdot (\frac{e_1}{4} + \frac{e_4}{8} + \frac{e_3}{16}) + \frac{e_5}{2 \cdot 16^i} \qquad (\textit{Proposition 3}) \\
&= \beta_i
\end{aligned}$$

The proofs of the other equations are similar.

The following proposition follows from the definition of σ_i.

Proposition 3. *For all $i \in \{1, 2, \dots\}$,*

$$\sigma_i = 1 + \frac{1}{16}\sigma_{i-1}.$$

Proposition 4. *The following statements hold.*

$$\begin{aligned}
\lim_{i\to\infty} \alpha_i &= \frac{8}{15}e_1 + \frac{4}{15}e_4 + \frac{2}{15}e_3 + \frac{1}{15}e_2 \;=:\; \alpha^*,\\
\lim_{i\to\infty} \beta_i &= \frac{8}{15}e_2 + \frac{4}{15}e_1 + \frac{2}{15}e_4 + \frac{1}{15}e_3 \;=:\; \beta^*,\\
\lim_{i\to\infty} \gamma_i &= \frac{8}{15}e_3 + \frac{4}{15}e_2 + \frac{2}{15}e_1 + \frac{1}{15}e_4 \;=:\; \gamma^*,\\
\lim_{i\to\infty} \delta_i &= \frac{8}{15}e_4 + \frac{4}{15}e_3 + \frac{2}{15}e_2 + \frac{1}{15}e_1 \;=:\; \delta^*.
\end{aligned}$$

Proof. First, note that

$$\lim_{i\to\infty} \sigma_{i-1} = \lim_{i\to\infty} \sigma_i = \lim_{i\to\infty} \frac{1-(1/16)^i}{1-1/16} = 16/15.$$

Now, we have

$$\begin{aligned}
\lim_{i\to\infty} \alpha_i &= \lim_{i\to\infty} \sigma_i \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^i}\\
&= \frac{16}{15} \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right)\\
&= \frac{8}{15}e_1 + \frac{4}{15}e_4 + \frac{2}{15}e_3 + \frac{1}{15}e_2 = \alpha^*.
\end{aligned}$$

Similarly, we can find the $\lim_{i\to\infty} \beta_i = \beta^*, \lim_{i\to\infty} \gamma_i = \gamma^*$, and $\lim_{i\to\infty} \delta_i = \delta^*$ (Fig. 4).

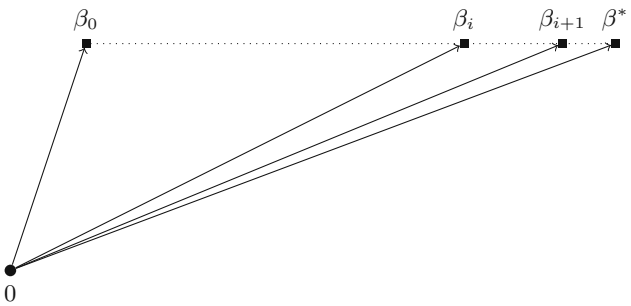


Fig. 4. Visualization of sequence $\{\beta_i\}_{i=1}^{\infty}$ (refer to Proposition 5)

Proposition 5. *For all* $i \in \{0, 1, \dots\}$,

$$\begin{aligned}
\alpha_{i+1} &= \frac{15}{16} \cdot \alpha^* + \frac{1}{16} \cdot \alpha_i, \quad & \beta_{i+1} &= \frac{15}{16} \cdot \beta^* + \frac{1}{16} \cdot \beta_i,\\
\gamma_{i+1} &= \frac{15}{16} \cdot \gamma^* + \frac{1}{16} \cdot \gamma_i, \quad & \delta_{i+1} &= \frac{15}{16} \cdot \delta^* + \frac{1}{16} \cdot \delta_i.
\end{aligned}$$

Consequently, α_i is on the line segment between $\alpha_0 = e_5$ and α_{i+1}; and α_{i+1} is on the line segment between α_i and α^*. More formally,

$$\begin{aligned}
&\alpha_i \in \mathsf{conv}(\alpha_0, \alpha_{i+1}),\ \alpha_{i+1} \in \mathsf{conv}(\alpha_i, \alpha^*),\\
&\beta_i \in \mathsf{conv}(\beta_0, \beta_{i+1}),\ \beta_{i+1} \in \mathsf{conv}(\beta_i, \beta^*),\\
&\gamma_i \in \mathsf{conv}(\gamma_0, \gamma_{i+1}),\ \gamma_{i+1} \in \mathsf{conv}(\gamma_i, \gamma^*),\\
&\delta_i \in \mathsf{conv}(\delta_0, \delta_{i+1}),\ \delta_{i+1} \in \mathsf{conv}(\delta_i, \delta^*).
\end{aligned}$$

Proof. By definition,

$$\alpha_i = \sigma_i \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^i}.$$

So, we have

$$\begin{aligned}
\alpha_{i+1} &= \sigma_{i+1} \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^{i+1}}\\
&= \left(1 + \frac{\sigma_i}{16}\right) \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^{i+1}} && (\textit{Proposition}\ 3)\\
&= \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{1}{16} \cdot \left(\sigma_i \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^i}\right)\\
&= \frac{15}{16} \cdot \alpha^* + \frac{1}{16} \cdot \alpha_i
\end{aligned}$$

The proofs of the three other equations are similar.

8 On the Optimality of Our Constructions

This section proves Theorem 2 mentioned in Sect. 2. It suffices to prove the following Theorem 5.

Theorem 5. *Let $\mathcal{S}^{(0)}$ be a subset of $\mathbb{R}^6$ of size 4. Then, there exists an $i^* \in \{0, 1, 2, 3, 4\}$ such that $\mathcal{S}^{(i^*)} = \mathcal{S}^{(i^*+1)}$.*

According to the above theorem, if the initial set $\mathcal{S}^{(0)}$ is a subset of $\mathbb{R}^6$ of size 4, the sequence $\mathcal{S}^{(0)} \to \mathcal{S}^{(1)} \to \mathcal{S}^{(2)} \to \dots$ stabilizes after at most 4 rounds. The following result is a consequence of the above theorem and [1,11].

Corollary 1. *Let $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ such that $\mathrm{card}\,(Z) \leqslant 4$. If f has a perfectly secure protocol, then there is a perfectly secure protocol for f with at most 4 rounds.*

8.1 Proof of Theorem 5

To prove Theorem 5, We will enumerate over all possible cases for $\mathcal{S}^{(0)}$ and show that in each case the sequence $\mathcal{S}^{(0)}, \mathcal{S}^{(1)}, \dots$ stabilizes in at most four rounds i.e. $\mathcal{S}^{(4)} = \mathcal{S}^{(5)}$. It was already shown in [11] that there is an at most two-round secure protocol for a secure function with $\mathrm{card}\,(Z) \leqslant 3$. Therefore, without loss

of generality, we only need to enumerate over the cases that the final result in $\mathcal{S}^{(\infty)}$ is connected. Moreover, we only need to consider one case among a set of cases that are similar. For example, in case 1, we consider 4 horizontally aligned points. The case that 4 points are aligned vertically is similar to case 1 and we do not need to consider it. We complete the proof by stating and proving the following lemma (Lemma 7).

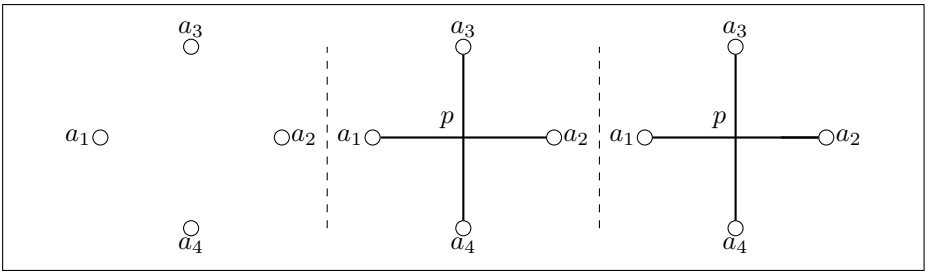
Lemma 7. *The following table states the values of i^* (defined in Theorem 5) for each enumerated case (Table 1).*

Table 1. The number of rounds needed to stabilize the sequence $\mathcal{S}^{(0)}, \mathcal{S}^{(1)}, \ldots$ for each enumerated case.

Case Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
i^*	1	1	2	1	2	2	1	2	2	1	2	2	4	2	3	3	2

Proof. In all cases except case 6, one can easily verify that $\mathcal{S}^{(i^*)} = \mathcal{S}^{(i^*+1)}$ for the i^* mentioned in the table. The reason is that in all those cases, when the final shape in the projected space (projection under π) stabilizes, then the whole shape stabilizes. More formally, in all cases except case 6, one can verify that $\pi(\mathcal{S}^{(i^*)}) = \pi(\mathcal{S}^{(i^*+1)})$ implies that $\mathcal{S}^{(i^*)} = \mathcal{S}^{(i^*+1)}$. For all cases except case 6, we show in the following that $\pi(\mathcal{S}^{(i^*)}) = \pi(\mathcal{S}^{(i^*+1)})$.

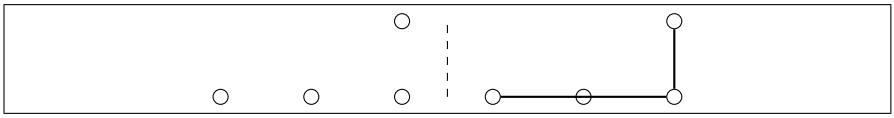
Now, we discuss case 6 in the following figure. At time 0, there are four points. Suppose $\rho(\mathcal{S}^{(0)}_{a_i}) = e_i$ where $e_i \in \mathbb{R}^4$ represents the i-th standard basis vector in $\mathbb{R}^4$. The points a_1 and a_2 are axis aligned, so $\rho(\mathcal{S}^{(1)}_{\frac{a_1 a_2}{}}) = \mathsf{conv}(e_1, e_2)$. Similarly, $\rho(\mathcal{S}^{(1)}_{\frac{a_3 a_4}{}}) = \mathsf{conv}(e_3, e_4)$. Now, notice that at the end of time 1, there are two objects at point p. One of them is $(p, \frac{e_1+e_2}{2})$ and the other one is $(p, \frac{e_3+e_4}{2})$. They are both axis aligned. So, we have $\rho(\mathcal{S}^{(2)}_p) = \mathsf{conv}(\frac{e_1+e_2}{2}, \frac{e_3+e_4}{2})$ and the shape stabilizes at step 2.

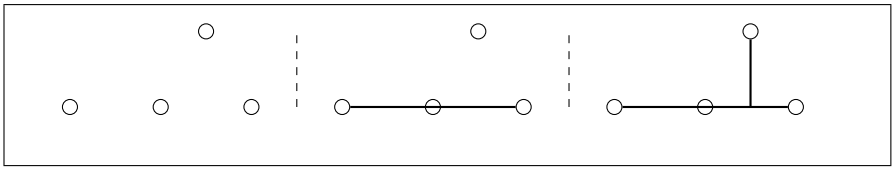


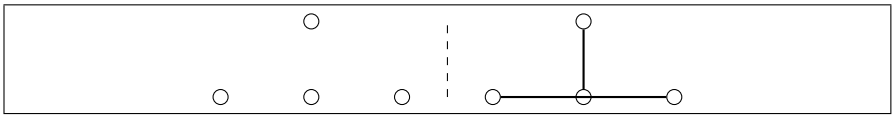
In the following, we enumerate over all possible cases and study the evolution of the sequence $\mathcal{S}^{(0)}, \mathcal{S}^{(1)}, \ldots$.

If There are 3 Collinear Points. There will be 4 cases as follows.

1.

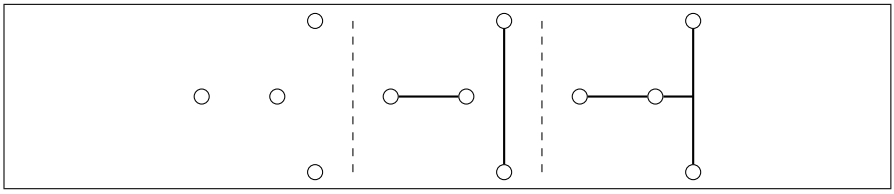

2.


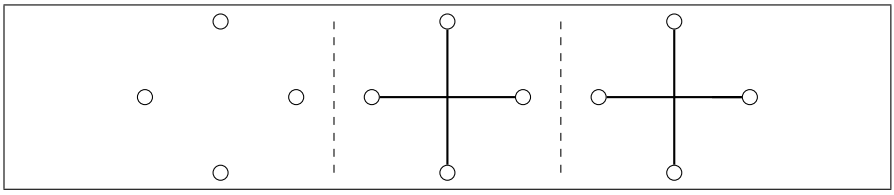
3.


4.


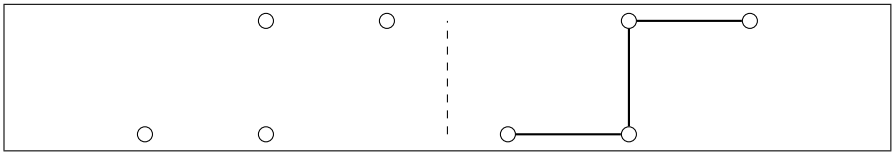
There are No 3 Collinear Points

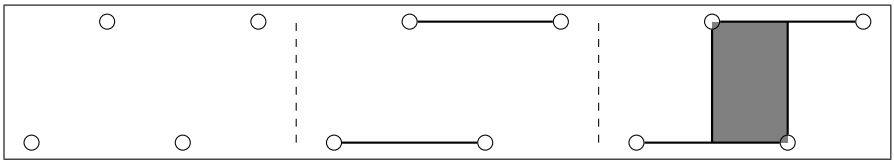
Subcase 1: Two points are horizontally collinear and the other two points are vertically collinear. There are 2 cases as follows.

5.


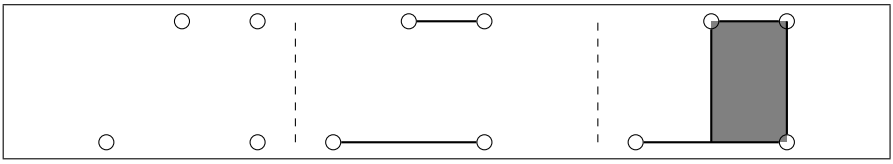
6.


Subcase 2: Two points are horizontally collinear and the other two are also horizontally collinear.

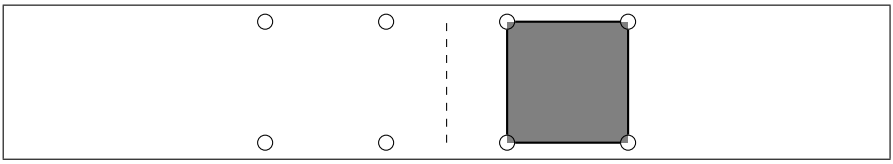
7.


8.


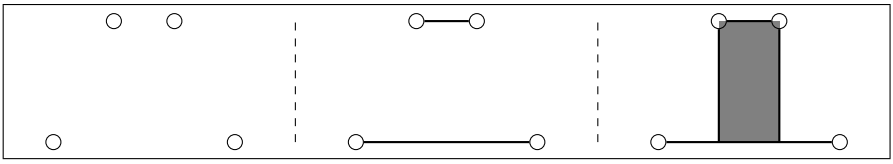
9.



10.

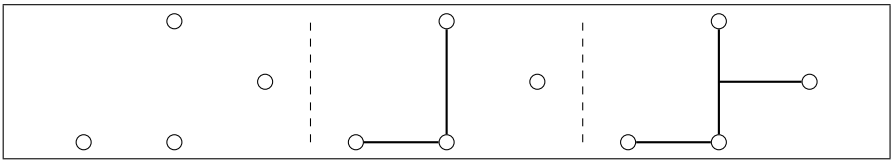


11.

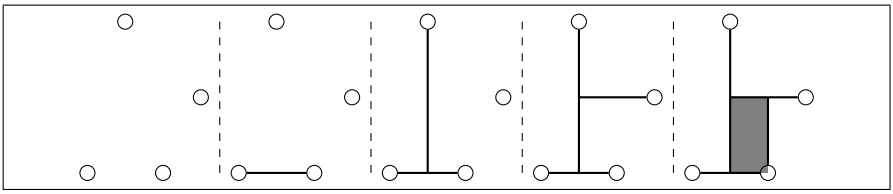


Subcase 3: Two points are horizontally collinear, and the other two points are not collinear.

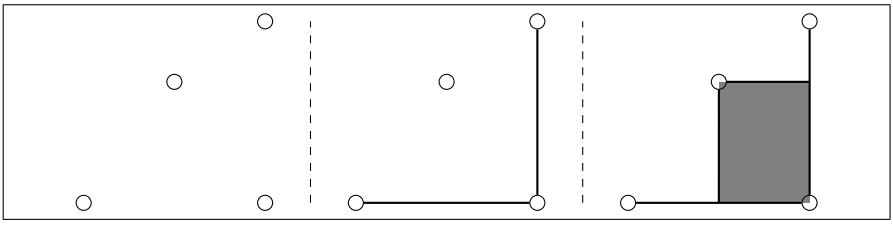
12.



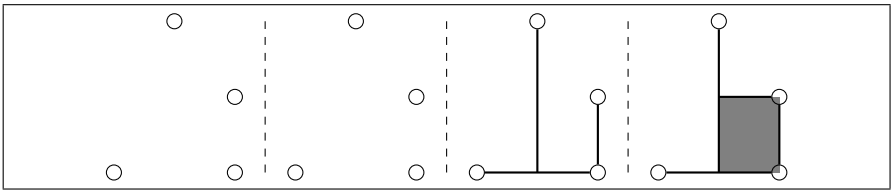
13.



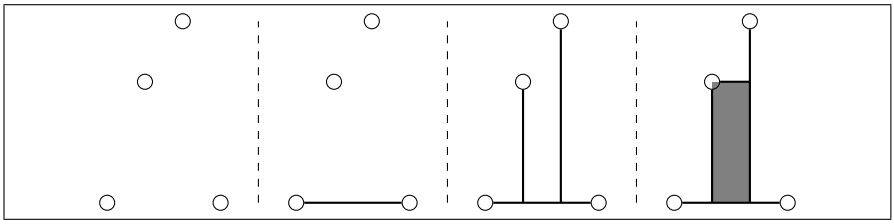
14.



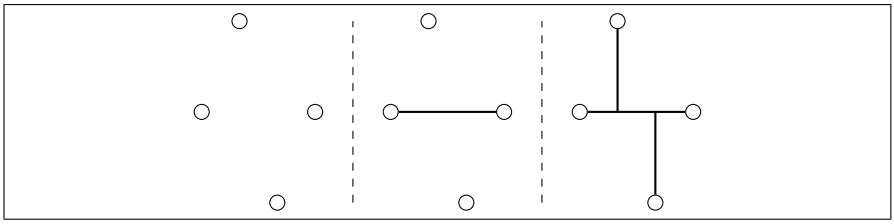
15.



16.



17.



We have exhaustively enumerated all possible cases and proved that the sequence $\mathcal{S}^{(0)}, \mathcal{S}^{(1)}, \ldots$ stabilizes after at most four rounds, which completes the proof.

References

1. Basu, S., Khorasgani, H.A., Maji, H.K., Nguyen, H.H.: Geometry of secure two-party computation. In: 63rd FOCS, pp. 1035–1044. IEEE Computer Society Press, October/November 2022
2. Basu, S., Khorashgani, H.A., Maji, H.K., Nguyen, H.H.: Geometry of secure two-party computation (2022). https://www.cs.purdue.edu/homes/hmaji/papers/BKMN22.pdf. Accessed 15 Feb 2023
3. Basu, S., Kummer, M., Netzer, T., Vinzan, C.: New directions in real algebraic geometry. https://publications.mfo.de/bitstream/handle/mfo/4031/OWR_2023_15.pdf?sequence=-1&isAllowed=y
4. Beaver, D.: Perfect privacy for two-party protocols. In: Proceedings of DIMACS Workshop on Distributed Computing and Cryptography, vol. 2, pp. 65–77 (1991)
5. Blum, L., Shub, M., Smale, S.: On a theory of computation and complexity over the real numbers: Np-completeness, recursive functions and universal machines (1989)
6. Bogetoft, P., et al.: Secure multiparty computation goes live. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 325–343. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03549-4_20
7. Carathéodory, C.: Über den variabilitätsbereich der fourier'schen konstanten von positiven harmonischen funktionen. Rendiconti Del Circolo Matematico di Palermo (1884–1940), **32**(1), 193–217 (1911)
8. Chor, B., Kushilevitz, E.: A zero-one law for Boolean privacy (extended abstract). In: 21st ACM STOC, pp. 62–72. ACM Press, May 1989
9. Cordoba, D., Faraco, D., Gancedo, F.: Lack of uniqueness for weak solutions of the incompressible porous media equation. Arch. Ration. Mech. Anal. **200**, 725–746 (2011)
10. Córdoba, D., Gancedo, F.: Contour dynamics of incompressible 3-d fluids in a porous medium with different densities. Commun. Math. Phys. **273**, 445–471 (2007)

11. Data, D., Prabhakaran, M.: Towards characterizing securely computable two-party randomized functions. In: Abdalla, M., Dahab, R. (eds.) PKC 2018. LNCS, vol. 10769, pp. 675–697. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76578-5_23
12. De Lellis, C., Székelyhidi Jr., L.: The Euler equations as a differential inclusion. Ann. Math. 1417–1436 (2009)
13. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or A completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th ACM STOC, pp. 218–229. ACM Press, May 1987
14. Hitruhin, L., Lindberg, S.: Lamination convex hull of stationary incompressible porous media equations. SIAM J. Math. Anal. **53**(1), 491–508 (2021)
15. Kilian, J.: More general completeness theorems for secure two-party computation. In: 32nd ACM STOC, pp. 316–324. ACM Press, May 2000
16. Kolář, J.: Non-compact lamination convex hulls. In: Annales de l'Institut Henri Poincaré C, Analyse non linéaire, vol. 20, pp. 391–403. Elsevier (2003)
17. Kushilevitz, E.: Privacy and communication complexity. In: 30th FOCS, pp. 416–421. IEEE Computer Society Press, October/November 1989
18. Yao, A.C.-C.: How to generate and exchange secrets (extended abstract). In: 27th FOCS, pp. 162–167. IEEE Computer Society Press, October 1986