# Towards Characterizing Secure Samplability

**Hari Krishnan P. Anilkumar**
TIFR, Mumbai, India

**Keval Jain**
IIIT Hyderabad, India

**Manoj Prabhakaran**
IIT Bombay, Mumbai, India

**Vinod M. Prabhakaran**
TIFR, Mumbai, India

## Abstract

This work deals with the fundamental problem of characterizing which multiparty distributions can be securely sampled with information-theoretic security against passive corruption, when there is no setup or honest-majority. We focus on the case of 4-party distributions with boolean outputs for each party. We show that such a distribution is securely samplable if and only if every 2-party distribution derived from it by partitioning the parties into two sets is securely samplable. This extends a similar characterization previously known for 3-party distributions.

**2012 ACM Subject Classification** Security and privacy → Information-theoretic techniques

**Keywords and phrases** secure sampling, information-theoretic MPC

**Digital Object Identifier** 10.4230/LIPIcs.ITC.2026.6

**Funding** *Hari Krishnan P. Anilkumar*: supported by DAE, Govt. of India, under RTI4014.
*Keval Jain*: supported by IIT Bombay Trust Lab internship and by STCS, TIFR.
*Manoj Prabhakaran*: supported in part by IIT Bombay Trust Lab.
*Vinod M. Prabhakaran*: supported by DAE, Govt. of India, under RTI4014 and by ANRF through ANRF/ARGM/2025/000821/TS.

**Declaration on GenAI/LLM use** Computer searches and AI tools (specifically ChatGPT) were extensively used to arrive at conjectures and proof ideas throughout the project, but the final proofs were derived by hand.

## 1 Introduction

A fundamental question in the theory of secure multi-party computation (MPC) is to understand which functionalities can be securely realized. This question, posed in different settings, has led to a large and influential body of work in cryptography [7, 4, 5, 10, 3, 8, 9, 6, 11]. However, despite these major advances, a most basic question remains open:

> Which multi-party functions have information-theoretically secure protocols without any setup or restrictions on the set of parties that can be corrupted?

Here, by information-theoretic security we mean statistical security against passive corruption (but other variants are also interesting and remain open).

As a stepping stone towards answering this question, one can investigate this question restricted to functionalities which have no input – i.e., the setting of secure sampling. In this case, we fully understand the landscape of 2-party and 3-party distributions. Specifically, 2-party distributions that are securely samplable are exactly those which are "simple" – a combinatorial characterization which we define later (see [11] and references therein).

Further, 3-party distributions that are securely samplable are exactly those which when partitioned into 2-party distributions (by merging any two parties) always result in simple 2-party distributions [12]. However, these works leave open the question of 4 or more parties.

In this work we investigate the question of characterizing 4-party *boolean* distributions (i.e., each party receives a bit as its output). We show that the combinatorial characterization for 3-party distributions generalizes to this case.

Our proof involves a careful case analysis tailored to 4-party boolean distributions. In particular, our positive results (protocols for certain distributions) rely on sets satisfying a certain combinatorial condition having an "additive representation" over an abelian group. As we show in Appendix A, with a larger number of parties, not all securely samplable boolean distributions are additively representable.

## 1.1 Our Contribution

To state our result for securely samplable 4-party distributions, we recall that a 2-party distribution is securely samplable if and only if it is *simple*.[1] Given an $n$-party distribution, we can derive 2-party distributions by partitioning the set of parties into two; the original distribution is said to be *simple*$^*$ if every such partition results in a 2-party distribution that is simple.

Clearly, if an $n$-party distribution is securely samplable, so is every distribution derived using a 2-way partition; hence only simple$^*$ distributions are securely samplable. In [12] it was shown that 3-party distributions that are securely samplable are exactly simple$^*$ distributions, and the question of whether this characterization holds for a larger number of parties was raised.

In this work we show that for 4-party *boolean* distributions (i.e., where each party gets a single bit), this is a sufficient condition as well:

▶ **Theorem 1.** *A 4-party boolean distribution is statistically securely samplable against passive corruption of any number of parties if and only if it is simple*$^*$*.*

We leave open the question for 5-party distributions, as well as non-boolean 4-party distributions, whether being simple$^*$ is sufficient for secure samplability. Another open problem we leave is to extend our sufficiency results to *perfectly secure* sampling (as was done in [12] for 3-party distributions samplable using a circuit over uniformly random bits).

## 1.2 Related Work

As mentioned above, a large body of work has looked into the broader question of characterization of the class of 2-party and multi-party functions that can be information-theoretically securely computed, under several settings. Here we shall mention just a few of them which are closest in spirit to our setting.

In our setting of passive corruption without setup or honest-majority restrictions, the 2-party case is largely well understood (see [11] for a survey). However, for randomized 2-party functions there appear to be no simple combinatorial characterizations; instead a recent line of work has given algorithmic characterizations [1, 2].

[1] A 2-party distribution $P_{X,Y}$ is said to be simple if there exists a "common information" random variable Q (that is, Q can be expressed as a deterministic function of X and also as a deterministic function of Y), such that X and Y are independent conditioned on Q.

In the same setting, a characterization of securely computable multi-party functions (with more than 2 parties) remains elusive. Chor and Ishai [6] investigated a question similar to the one we explore, for deterministic functions (with inputs). Specifically, they asked if every 2-party function derived from an $m$-party function by partitioning the parties into two sets is securely computable, then whether the original function is guaranteed to be securely computable. In their case, they answered this problem in the negative. (For us, the answer is positive.)

The work most closely related to ours is [12], which considered the same sampling as ours. Their result in our setting (point-to-point channels and no setup) was limited to 3 parties, leaving the case of more parties open.

## 1.3 Overview

In this section, we give a detailed technical overview of our proof. Our main goal is to show that all simple$^*$ 4-party boolean distributions are securely samplable.

One may hope for a generic secure protocol for sampling from an $n$-party distribution that relies only on the fact that the distribution is simple$^*$. Indeed, in the case of 3-party distributions, such a generic protocol was identified in [12]. Unfortunately, for 4-party distributions we do not know if such a generic protocol is possible. Even restricted to boolean outputs, we rely on a careful case analysis to construct secure protocols for all simple$^*$ distributions. At a high level, there are two parts to our proof: (1) analyzing simple$^*$ 4-party boolean distributions, and identifying a small class of explicit distributions for which protocols do not follow from prior work, and (2) showing that each of these distributions does indeed have a secure sampling protocol. We give an overview of these two parts below.

### An Example of a Simple* Distribution

Before we proceed further, to familiarize the reader with the notions of simple and simple$^*$ distributions, we present an example.

It will be convenient to reinterpret a 2-party distribution $P_{\mathrm{X,Y}}$ as a distribution over edges in a bipartite graph: an edge $(x, y)$ corresponds to $P_{\mathrm{X,Y}}(x, y) > 0$.[2] If $P_{\mathrm{X,Y}}$ is a simple distribution, then this graph breaks up into connected components each of which is a complete bipartite graph (a.k.a. biclique). When the distribution is uniform over its support, this also is a sufficient condition for it to be simple.

Now, we consider an example of a 4-party simple$^*$ distribution: Let $(\mathrm{X}_1, \ldots, \mathrm{X}_4)$ be uniformly distributed over $S = \{(0,0,0,0), (0,0,1,1), (0,1,0,1), (1,0,0,1)\}$. To verify that it is simple$^*$, we consider each subset $J \subset \{1,2,3,4\}$ and check that the pair of random variables $(\mathrm{X}_J, \mathrm{X}_{\overline{J}})$ is simple.

For example, (see Figure 1) for $J = \{1\}$, the 2-party distribution of $(\mathrm{X}_1, \mathrm{X}_{\{2,3,4\}})$ is uniform over $\{(0,000), (0,011), (0,101), (1,001)\}$; the bipartite graph of this distribution has two connected components, each has a single node on the left-hand side and hence is a biclique. For $J = \{1,4\}$, we have $(\mathrm{X}_{\{1,4\}}, \mathrm{X}_{\{2,3\}})$ uniformly distributed over $\{(00,00), (01,01), (01,10), (11,00)\}$; in this case, the graph has two connected components – one component with 00 in the right-hand side and the other with 01 in the left-hand side – both of which are bicliques. Verifying this for all non-empty $J \subset \{1,2,3,4\}$ confirms that the distribution is simple$^*$.

[2] For simplicity, for now we consider distributions which are uniform over their support. In the more general case, we consider a weighted graph with the weight of the edge $(x, y)$ being $P_{\mathrm{X,Y}}(x, y)$.

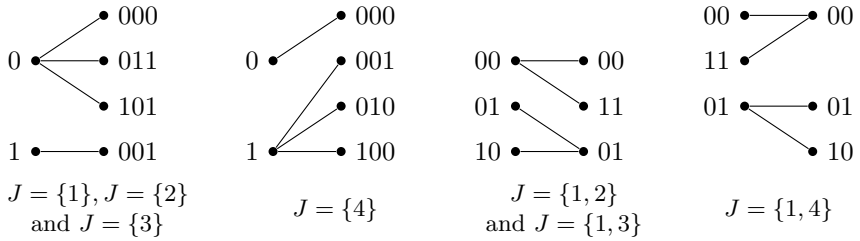


**Figure 1** Bipartite graphs corresponding to the different partitions $(\mathrm{X}_J, \mathrm{X}_{\bar{J}})$ for the support $S = \{(0,0,0,0), (0,0,1,1), (0,1,0,1), (1,0,0,1)\}$.

## Understanding 4-Party Boolean Simple* Distributions

### Reducible and Non-reducible Distributions

We start by dividing the simple* distributions into two cases: (1) *reducible* distributions which can be securely sampled using a secure sampling protocol for a 3−party distribution, and (2) *non-reducible* distributions, which we will analyze further.

Informally, a distribution is reducible if one of the parties has an output independent of the others, or if two parties have the same (or opposite) output. If a 4-party simple* distribution is reducible, it is easy to see that removing the independent/duplicate party results in a 3-party simple* distribution. Next, by [12], we obtain a secure sampling protocol for this 3-party distribution. Finally, this 3-party protocol can be readily transformed to a 4-party secure protocol for the original distribution.

Non-reducible simple* distributions require more work. We catalog all such 4-party boolean distributions, so that we can show that each one of them is securely samplable. We do this in two steps: first we characterize the support of such distributions ("admissible supports"), and then we characterize the probability mass over such a support.

### Support of Non-reducible Simple* Distributions

Firstly, for a 2-party simple distribution, the support can be identified with a bipartite graph whose connected components are bicliques. For a simple* distribution, the requirement on its support is that for every partition of the parties into two, the resulting 2-party distribution's support forms a disjoint collection of bicliques.

Being simple* *and non-reducible* imposes several combinatorial constraints on the support. In particular, we argue that the support, viewed as a subset of $\{0,1\}^4$, forms a "code" of distance at least 2, and it should be of size 4, 5, 6 or 8.

To be able to easily enumerate the supports, we consider two supports equivalent if they are related to each other by a permutation of the parties followed by complementing the outputs of a subset of the parties. Then, up to this equivalence (which we call relabeling), we exhaustively argue that there is only one support each of size 5, 6 and 8, and only two supports of size 4 that are possible for a 4-party boolean simple* distribution. In the sequel we refer to these five possible supports as the *admissible supports*.

### Non-reducible Simple* Distributions

To complete our explicit characterization of non-reducible simple* 4-party boolean distributions, we need to understand how probabilities could be assigned to the elements in an admissible support while maintaining simple* nature. One obvious choice is the uniform

distribution. This can be further generalized to a *product-form*: we associate a non-negative weight to each output (0 and 1) of each party, and the probability of any output tuple in the support is proportional to the product of the weights assigned to each party's outcome. If the uniform distribution is simple*, such a transformation over the same support keeps it simple*.

Remarkably, these product-form distributions turn out to be the only distributions that are simple*. We prove this by analyzing each of the five admissible supports separately.

## Protocols for Simple* Distributions

Since a secure protocol for a reducible 4-party simple* distribution can be obtained from the secure protocol for a simple* 3-party distribution (from [12]), we focus on the non-reducible 4-party boolean simple* distributions. Then it suffices to give a statistically secure protocol for simple* distributions with each of the 5 admissible supports identified above.

Firstly, we note that due to the product form of these distributions the following "sample-and-check" template suffices for a statistically secure protocol:

- Each party locally samples an independent bit according to its fixed marginal distribution.
- They will "semi-securely" compute whether the bits they collectively sampled lie in the support of the desired distribution. If it does, they output the sampled bits and terminate; else, they repeat the whole process. (After security parameter many attempts, one party may sample an element and send it to the others; this occurs with negligible probability.)

Here a "semi-secure" membership test is a protocol which provides privacy guarantees when the inputs do form a member of the set (i.e., if two distinct elements of the set have the same bits restricted to a subset of the parties, then their views are distributed identically when the protocol is executed with those two inputs). When the inputs form an element outside the set, there is no privacy guarantee. Note that such a protocol suffices in the above template since we reject samples which are not elements of the support.

To instantiate the second step of this template, we need a *semi-secure set-membership test*, for each of the five admissible supports. The key to our protocols is the observation that all the admissible supports are "additively representable," as defined below. (In our case, $\mathcal{X}_i = \{0, 1\}$ and $n = 4$.)

▶ **Definition 2.** *A set $S \subseteq \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ is said to be* additively representable *if there exist a finite abelian group $G$, a set of maps $\mu_i : \mathcal{X}_i \to G$ and an element $g \in G$, such that $S = \{(x_1, \ldots, x_n) | \sum_{i=1}^{n} \mu_i(x_i) = g\}$.*

We note that every additively representable set has a simple semi-secure membership protocol (against passive corruption). It is well known that the summation task over any finite abelian group can be securely computed. To check membership in an additively representable set $S$, each party locally maps their input $x_i$ to $\mu_i(x_i)$, and then they securely compute the sum $\sum_{i=1}^{n} \mu_i(x_i)$. If this sum equals $g$, then the parties only learn that their inputs form an element of the set; otherwise, they do learn information beyond the fact that the inputs are not in the set, but this is permitted in a semi-secure protocol.

To complete our proof, we need to show that each of the five admissible supports we identified as supports for simple* distributions are additively representable. We show that this is indeed the case (using groups $\mathbb{Z}_2, \mathbb{Z}_3$ and $\mathbb{Z}_6$). In particular, for the example from the beginning of this section, $S = \{(0,0,0,0), (0,0,1,1), (0,1,0,1), (1,0,0,1)\}$, we use the group $\mathbb{Z}_6$, the target element $g = 0$, and maps $\mu_1 = \mu_2 = \mu_3$ which map $0 \mapsto 0$ and $1 \mapsto 1$, and $\mu_4 : 0 \mapsto 0$ and $\mu_4 : 1 \mapsto -1$.

## 2 Preliminaries

For any positive integer $n$, we write $[n]$ to denote the set $\{1, \ldots, n\}$. We use uppercase letters in italics to denote sets and uppercase letters in upright to denote random variables.

### Multi-Party Distributions

A distribution $P$ over a (finite) alphabet $\mathcal{X}$ is simply a function $P : \mathcal{X} \to [0, 1]$ such that $\sum_{x \in \mathcal{X}} P(x) = 1$. The basic objects of interest in this work are $n$-party distributions. These are simply distributions defined over some alphabet $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$, with the connotation that an element $(x_1, \ldots, x_n)$ sampled from this distribution will be distributed among $n$ parties $\mathsf{P}_1, \ldots, \mathsf{P}_n$, so that $\mathsf{P}_i$ gets $x_i$. We shall often write such a distribution as $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$, where the random variable $\mathrm{X}_i$ denotes the element given to $\mathsf{P}_i$. The distribution $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ is said to be *boolean* if each $\mathrm{X}_i$ is a boolean random variable – i.e., its alphabet is $\{0, 1\}$.

For any $J \subseteq [n]$, we will use $\mathrm{X}_J$ to denote the tuple of variables $(\mathrm{X}_i)_{i \in J}$. We also define, for $x \in \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ and subset $J \subseteq [n]$, the element $x_J$ to be the tuple obtained by restricting $x$ to the indices in $J$. When there is no ambiguity, we shall often represent a tuple by a string (e.g., 0000 instead of $(0, 0, 0, 0)$).

### Protocols

The other basic object in this work is a secure sampling protocol. In an (inputless) protocol, parties $\mathsf{P}_1, \ldots, \mathsf{P}_n$ have access to private randomness at the beginning of the protocol. The protocol proceeds in rounds; in every round, each party sends a message to each of the other parties, where the message is a function of the sender's private randomness and all the messages that it received in all the previous rounds in the protocol. After a finite number of rounds, the protocol should terminate and each party $\mathsf{P}_i$ should produce an output.

For a protocol $\Pi$, the random variable $\mathsf{View}_i^{\Pi}$ denotes the view of a party $\mathsf{P}_i$, which consists of the private randomness of $\mathsf{P}_i$ and all the messages received by $\mathsf{P}_i$ during the entire protocol. The random variable $\mathsf{out}_i^{\Pi}$ denotes the output produced by $\mathsf{P}_i$. $\mathsf{out}_i^{\Pi}$ is a deterministic function of $\mathsf{View}_i^{\Pi}$.

The statistical distance (total variation distance) $\mathrm{SD}(\mathrm{X}_1, \mathrm{X}_2)$ between two random variables $\mathrm{X}_1$ and $\mathrm{X}_2$ defined on some alphabet $\mathcal{X}$ is

$$\mathrm{SD}(\mathrm{X}_1, \mathrm{X}_2) = \frac{1}{2} \sum_{x \in \mathcal{X}} |\Pr[\mathrm{X}_1 = x] - \Pr[\mathrm{X}_2 = x]| = \max_{T \subseteq \mathcal{X}} (\Pr[\mathrm{X}_1 \in T] - \Pr[\mathrm{X}_2 \in T]).$$

The support of an $n$-party distribution $P$ over $\mathcal{X}_1 \times \ldots \mathcal{X}_n$ is $\mathrm{supp}(P) = \{x \in \mathcal{X}_1 \times \ldots \times \mathcal{X}_n : P(x) > 0\}$. For any distribution $P_{\mathrm{X,Y,Q}}$, the statement that X and Y are independent conditioned on Q will be denoted by the Markov chain $\mathrm{X} \leftrightarrow \mathrm{Q} \leftrightarrow \mathrm{Y}$.

▶ **Definition 3** (Securely Samplable Distribution). *For $\epsilon > 0$, a protocol $\Pi$ is said to $\epsilon$-securely sample from $P_{X_1,\ldots,X_n}$ if for each $C \subset [n]$ there exists a random variable $\mathsf{Sim}_C$ (jointly distributed with the ideal outputs $\mathrm{X}_{[n]}$) such that*

$$\mathsf{Sim}_C \leftrightarrow \mathrm{X}_C \leftrightarrow \mathrm{X}_{\overline{C}}, \text{ and} \tag{1}$$

$$\mathrm{SD}\left(\left(\mathrm{X}_{\overline{C}}, \mathsf{Sim}_C\right), \left(\mathsf{out}_{\overline{C}}^{\Pi}, \mathsf{View}_C^{\Pi}\right)\right) \leq \epsilon. \tag{2}$$

*$P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ is said to be* securely samplable *if for every $\epsilon > 0$ there exists a protocol that $\epsilon$-securely samples from it.*

When $\epsilon = 0$, we say that $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ is samplable under perfect security.

▶ **Definition 4** (Bipartite Graph of a 2-Party Distribution)**.** *The bipartite graph of a 2-party probability distribution $P_{\mathrm{XY}}$ over the alphabet $\mathcal{X} \times \mathcal{Y}$ is defined as the weighted graph $G_{P_{\mathrm{XY}}} = (\mathcal{X}, \mathcal{Y}, P_{\mathrm{XY}})$. That is, the weight of an edge $(x, y) \in \mathcal{X} \times \mathcal{Y}$ is $P_{\mathrm{XY}}(x, y)$.*

▶ **Definition 5** (Simple 2-Party Distribution)**.** *A 2-party distribution $P_{\mathrm{X,Y}}$ over the alphabet $\mathcal{X} \times \mathcal{Y}$ is said to be* simple *if there are functions $w_1 : \mathcal{X} \to \mathbb{R}^+$, $w_2 : \mathcal{Y} \to \mathbb{R}^+$, $q_1 : \mathcal{X} \to \mathbb{Z}$ and $q_2 : \mathcal{Y} \to \mathbb{Z}$ such that for all $x \in \mathcal{X}, y \in \mathcal{Y}$,*

$$P_{\mathrm{X,Y}}(x, y) = \begin{cases} w_1(x)w_2(y) & \text{if } q_1(x) = q_2(y) \\ 0 & \text{otherwise} \end{cases}. \tag{3}$$

The following alternate view of a simple distribution is often convenient: $P_{\mathrm{X,Y}}$ is simple if and only if there exists a random variable Q over $\mathbb{Z}$ jointly distributed with X and Y such that

1. Q is a deterministic function of X and a deterministic function of Y.
2. The Markov chain $\mathrm{X} \leftrightarrow \mathrm{Q} \leftrightarrow \mathrm{Y}$ holds; i.e., X and Y are independent conditioned on Q.

Indeed, if $P_{\mathrm{XY}}$ is simple as defined, taking $\mathrm{Q} = q_1(\mathrm{X})$ it holds that $\mathrm{Q} = q_2(\mathrm{Y})$ also w.p. 1. Further, for a given $q$, for all $x, y$ s.t. $q_1(x) = q_2(y) = q$, $P_{\mathrm{X,Y|Q}}(x, y|q) = \frac{w_1(x)w_2(y)}{P_{\mathrm{Q}}(\mathrm{Q}=q)} = \frac{w_1(x)w_2(y)}{(\sum_{x':q_1(x')=q} w_1(x'))(\sum_{y':q_2(y')=q} w_2(y'))}$ and 0 for all other $x, y$; then $P_{\mathrm{X|Q}}(x|q) = \sum_{y:q_2(y)=q} P_{\mathrm{X,Y|Q}}(x, y|q) = \frac{w_1(x)}{\sum_{x':q_1(x')=q} w_1(x')}$, and similarly $P_{\mathrm{Y|Q}}(y|q) = \frac{w_2(y)}{\sum_{y':q_2(y')=q} w_2(y')}$, so that $P_{\mathrm{X,Y|Q}}(x, y|q) = P_{\mathrm{X|Q}}(x|q)P_{\mathrm{Y|Q}}(y|q)$. (This factorization also holds for $(x, y)$ for which it is not the case that $q_1(x) = q_2(y) = q$, as the LHS and at least one of the factors in the RHS are 0.)

Conversely, if such a Q exists, we use the given deterministic functions that define Q as $q_1, q_2$ and set $w_1(x) = P_{\mathrm{X}}(x), w_2(y) = P_{\mathrm{Y|Q}}(y|q_2(y))$, so that, for $x, y$ pairs such that $P_{\mathrm{X,Y}}(x, y) > 0$, we have

$$\begin{aligned} P_{\mathrm{X,Y}}(x, y) = P_{\mathrm{X,Y,Q}}(x, y, q_1(x) = q_2(y)) = P_{\mathrm{X,Q}}(x, q_1(x))P_{\mathrm{Y|Q}}(y|q_2(y)) \\ = P_{\mathrm{X}}(x)P_{\mathrm{Y|Q}}(y|q_2(y)) = w_1(x)w_2(y). \end{aligned} \tag{4}$$

We will often refer to the variable Q as the *common information* for a simple $P_{\mathrm{X,Y}}$.

▶ **Proposition 6** ([13])**.** *A two-party distribution is simple if and only if it is securely samplable.*

The notion of a simple distribution can be extended to $n$-party distributions for $n \geq 2$ as follows.

▶ **Definition 7** (Simple* Distributions)**.** *An $n$-party distribution $P_{\mathrm{X}_{[n]}}$ is a simple$^*$ distribution if for every set $J \subset [n]$, the 2-party distribution $P_{\mathrm{X}_J\mathrm{X}_{\overline{J}}}$ is a simple distribution.*

More explicitly, a distribution $P_{\mathrm{X}_{[n]}}$ is simple$^*$ if, for every non-empty $J \subset [n]$, there is a weight function $w_J : \mathrm{X}_J \to \mathbb{R}^+$ and an index function $q_J : \mathrm{X}_J \to \mathbb{Z}$ such that

$$P_{\mathrm{X}_{[n]}}(x) = \begin{cases} w_J(x_J)w_{\overline{J}}(x_{\overline{J}}) & \text{if } q_J(x_J) = q_{\overline{J}}(x_{\overline{J}}) \\ 0 & \text{otherwise.} \end{cases}$$

▶ **Lemma 8.** *If an $n$-party distribution is securely samplable, then it is simple$^*$.*

**Proof.** If an $n$-party distribution $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ is securely samplable using a protocol $\Pi$, for every $J \subset [n]$, consider the 2-party protocol in which one party simulates the parties $(\mathsf{P}_i)_{i\in J}$ in $\Pi$, and the other party simulates $(\mathsf{P}_i)_{i\in\overline{J}}$. This is a secure sampling protocol for $P_{\mathrm{X}_J\mathrm{X}_{\overline{J}}}$. By Proposition 6, it follows that for every $J \subset [n]$, the distribution $P_{\mathrm{X}_J\mathrm{X}_{\overline{J}}}$ is simple, which means that $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ is simple$^*$. ◀

## 3 4-Party Boolean Simple* Distributions are Securely Samplable

In this section we present the overall structure of our proof of Theorem 1, that a 4-party boolean distribution is securely samplable if and only if it is simple$^*$.

By Lemma 8, the "only if" direction is immediate. Therefore, it remains to prove that every simple$^*$ 4-party boolean distribution is securely samplable.

The proof is divided into two parts. In this section we first identify families of simple$^*$ 4-party distributions whose secure samplability can be obtained from the secure samplability of a suitable 3-party distribution. We call these distributions reducible. In the next section we then analyze the remaining simple$^*$ 4-party distributions.

▶ **Definition 9.** *An $n$-party distribution $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ is said to* reduce to *the $(n-1)$-party distribution $P_{\mathrm{X}_{[n]\setminus\{i\}}}$ for an $i \in [n]$ if either of the following conditions hold:*

1. *$\mathrm{X}_i$ is distributed independently of the other variables, i.e., $\mathrm{X}_i \perp\!\!\!\perp \mathrm{X}_{[n]\setminus\{i\}}$*
2. *For some $i' \neq i$ and some deterministic function $f$, $\mathrm{X}_i = f(\mathrm{X}_{i'})$.*

*$P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ is said to be* reducible *if it reduces to $P_{\mathrm{X}_{[n]\setminus\{i\}}}$ for some $i \in [n]$. Otherwise, we call it* non-reducible.

We shall establish that if a 4-party simple$^*$ distribution is reducible then it is securely samplable. For this, we first need the following lemma.

▶ **Lemma 10.** *Suppose $P$ reduces to $P'$. Then,*

1. *If $P$ is simple$^*$, then so is $P'$.*
2. *If $P'$ is securely samplable, so is $P$.*

**Proof.** Suppose $P$ is $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ and $P'$ is $P_{\mathrm{X}_{[n]\setminus\{i\}}}$. W.l.o.g, we shall take $i = n$, so that $P'$ is $P_{\mathrm{X}_{[n-1]}}$. We prove each of the items in the claim.

***$P$ simple$^*$ $\implies$ $P'$ simple$^*$.*** To show that $P'$ is simple$^*$, for any subset $J \subset [n-1]$ and its complement $\overline{J} = [n-1] \setminus J$, we need to show that the 2-party distribution $P_{\mathrm{X}_J,\mathrm{X}_{\overline{J}}}$ is simple. For this we can use the fact that $P_{\mathrm{X}_J,\mathrm{X}_{\overline{J}\cup\{n\}}}$ is simple. We fix a $J$ now.

Recall that there are two ways in which $P$ can reduce to $P'$ – either $\mathrm{X}_n$ is independent of $\mathrm{X}_{[n-1]}$, or $\mathrm{X}_n$ is a function of $\mathrm{X}_{i'}$ for some $i' \neq n$.

In the former case, we invoke the following claim, with $\mathrm{U} = \mathrm{X}_J, \mathrm{V} = \mathrm{X}_{\overline{J}}$ and $\mathrm{W} = \mathrm{X}_n$, to conclude that $P_{\mathrm{X}_J,\mathrm{X}_{\overline{J}}}$ is simple.

▷ Claim 11. Let $P_{\mathrm{UVW}} = P_{\mathrm{UV}}P_{\mathrm{W}}$. Then, if the two party distribution $P_{\mathrm{U,VW}}$ is simple, so is the two-party distribution $P_{\mathrm{U,V}}$.

Proof. Let Q be common information of $P_{\mathrm{U,VW}}$. Note that since $\mathrm{W} \perp\!\!\!\perp (\mathrm{U},\mathrm{V})$, $\mathrm{U} \leftrightarrow \mathrm{V} \leftrightarrow \mathrm{W}$, which further implies that $\mathrm{Q} \leftrightarrow \mathrm{V} \leftrightarrow \mathrm{W}$ as Q is a function of U. Using this conditional independence, we have that since, Q is a function of $(\mathrm{V},\mathrm{W})$, Q must be a function of only V. Moreover, Q is a function of U. This, along with the fact that $\mathrm{U} \leftrightarrow \mathrm{Q} \leftrightarrow (\mathrm{V},\mathrm{W}) \implies \mathrm{U} \leftrightarrow \mathrm{Q} \leftrightarrow \mathrm{V}$ completes the proof that $P_{\mathrm{U,V}}$ is simple. ◁

In case $\mathrm{X}_n$ is a function of $\mathrm{X}_{i'}$ for some $i' \neq n$, we invoke the following claim, again with $\mathrm{X}_J = \mathrm{U}$, $\mathrm{X}_{\overline{J}} = \mathrm{V}$ and $\mathrm{X}_n = \mathrm{W}$, and assuming w.l.o.g, that $i' \in J$ (swapping the roles of $J, \overline{J}$ if necessary).

▷ Claim 12. Suppose $P_{\mathrm{UW,V}}$ defined on $\mathcal{U} \times \mathcal{V} \times \mathcal{W}$ is simple, where $\mathrm{W} = f(\mathrm{U})$ for a deterministic function $f : \mathcal{U} \to \mathcal{W}$. Then $P_{\mathrm{U,V}}$ is simple.

Proof. Let Q be the common information for $P_{\mathrm{UW,V}}$. Since Q is a function of $(\mathrm{U}, \mathrm{W})$, it is a function of U as well; and Q is also a function of V since it is the common information. Furthermore, since $(\mathrm{U}, \mathrm{W}) \leftrightarrow \mathrm{Q} \leftrightarrow \mathrm{V}$, therefore, $\mathrm{U} \leftrightarrow \mathrm{Q} \leftrightarrow \mathrm{V}$. ◁

Thus in either case, if $P$ is simple$^*$, so is $P'$.

**$P'$ securely samplable $\implies$ $P$ securely samplable.** Given an $(n-1)$-party secure protocol for sampling $P'$, we shall upgrade it to an $n$-party protocol for $P$. Again, we separately consider the two different ways in which $P$ can reduce to $P'$.

If $\mathrm{X}_n$ is independent of $\mathrm{X}_{[n-1]}$, we obtain a secure protocol for $P$ in which the $n^{\text{th}}$ party simply outputs a sample from the marginal distribution $P_{\mathrm{X}_n}$ and independently, the other $n-1$ parties run the given protocol for sampling from $P_{\mathrm{X}_{[n-1]}}$.

If $\mathrm{X}_n$ is a function of $\mathrm{X}_{i'}$ for some $i' \neq n$, say, $\mathrm{X}_n = f(\mathrm{X}_{i'})$, we obtain a secure protocol for $P$ in which the first $n-1$ parties run the given protocol for sampling from $P_{\mathrm{X}_{[n-1]}}$, after which party $i'$ sends the value $f(\mathrm{X}_{i'})$ to the $n^{\text{th}}$ party, who outputs it.

It is easy to see that in either case, the protocol obtained above is a secure protocol for sampling from $P$. ◀

We now need the following result about secure samplability of 3-party distributions from [12].

▶ **Proposition 13** ([12]). *A 3-party boolean distribution is securely samplable against passive corruption of any subset of parties if and only if it is simple$^*$.*

Now we state the main result of this section.

▶ **Lemma 14.** *If a 4-party distribution is simple$^*$ and reducible, then, it is securely samplable.*

**Proof.** Suppose a 4-party distribution $P$ is simple$^*$ and reduces to a 3-party distribution $P'$. Then by Lemma 10 (item 1), $P'$ is simple$^*$. Then, by Proposition 13, $P'$ is securely samplable. Invoking Lemma 10 (item 2), we conclude that $P$ is securely samplable, as desired. ◀

## 4 Supports of Simple* Non-Reducible 4-Party Boolean Distributions

▶ **Definition 15** (Relabeling a Distribution). *A* relabeling *of $n$-party distributions over $\mathcal{X}^n$ is a bijection $\Phi_\varphi : \mathcal{X}^n \to \mathcal{X}^n$ specified by a tuple $\varphi = (\pi, \sigma_1, \ldots, \sigma_n)$ where $\pi : [n] \to [n]$ is a permutation and, for each $i \in [n]$, each $\sigma_i : \mathcal{X} \to \mathcal{X}$ is a bijection. The bijection $\Phi_\varphi : \mathcal{X}^n \to \mathcal{X}^n$ is defined as $\Phi_\varphi(x_1, \ldots, x_n) := \big(\sigma_1(x_{\pi(1)}), \ldots, \sigma_n(x_{\pi(n)})\big)$. We define the relabeled distribution $\varphi(P)$ by*

$$\varphi(P)(v) := P\big(\Phi_\varphi^{-1}(v)\big), \qquad \forall\, v \in \mathcal{X}^n.$$

**Example.** Let $\mathcal{X} = \{0,1\}$ and $n = 4$. Let $\pi$ swap coordinates 1 and 2 (so $\pi(1) = 2, \pi(2) = 1$), let $\sigma_1$ be bit-flip ($\sigma_1(b) = 1 - b$), and let $\sigma_2, \sigma_3, \sigma_4$ be the identity. Then $\Phi_\varphi(x_1, x_2, x_3, x_4) = (1-x_2,\, x_1,\, x_3,\, x_4)$, so for any $(v_1, v_2, v_3, v_4) \in \{0,1\}^4$ we have $\varphi(P)(v_1, v_2, v_3, v_4) = P(v_2,\, 1-v_1,\, v_3,\, v_4)$. It is easy to see that relabeling does not affect the combinatorial property of being simple$^*$, nor the cryptographic property of being securely samplable. We record this in the following lemma.

▶ **Lemma 16** (Invariance under relabeling). *Let $P$ be an $n$-party distribution $P_{\mathrm{X}_1,\ldots,\mathrm{X}_n}$ and $\varphi$ a relabeling for it. Then $P$ is simple$^*$ if and only if $\varphi(P)$ is simple$^*$, and $P$ is securely samplable if and only if $\varphi(P)$ is securely samplable.*

In this section we show that a simple$^*$ non-reducible 4-party boolean distribution, up to relabeling, must have one of the following five sets as its support. In the sequel, we shall refer to them as the *admissible supports*.

$$
\begin{aligned}
S_1 &:= \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\},\\
S_2 &:= \{0000, 0011, 0101, 1010, 1100, 1111\},\\
S_3 &:= \{0000, 0011, 0101, 1001, 1110\},\\
S_4 &:= \{0000, 0011, 0101, 1001\},\\
S_5 &:= \{0000, 0011, 0101, 1110\}.
\end{aligned} \tag{5}
$$

▶ **Proposition 17.** *Let $P$ be a simple$^*$ non-reducible 4-party boolean distribution. Then, up to relabeling, supp$(P)$ must be one of $S_1, S_2, S_3, S_4, S_5$ defined in Equation* (5).

The proof proceeds by a case analysis on $|\mathrm{supp}(P)|$. We first rule out supports of size smaller than 4, then analyze the cases of support sizes 4 through 8, and finally rule out supports of size larger than 8. This yields Proposition 17.

## Case Analysis of Supports of Different Sizes

Before proceeding with our analysis, we introduce the following unweighted bipartite graph for representing the support of a 2-party distribution derived from an $n$-party distribution with a given support.

▶ **Definition 18** (Support graph). *Let $S \subseteq \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$ and let $J \subset [n], J \neq \emptyset$. The support graph $B_J^S$ is the bipartite graph whose left vertex set is $\mathcal{X}_J$, whose right vertex set is $\mathcal{X}_{[n]\setminus J}$, and whose edge set is $E\big(B_J^S\big) := \{(x_J, x_{[n]\setminus J}) : x \in S\}$.*

We shall also refer to a few combinatorial properties of the support of a simple$^*$ non-reducible boolean distribution. For this it will be useful to define minimum Hamming distance of a subset $S \subseteq \{0,1\}^n$ as $\Delta(S) = \min_{\substack{x,y\in S\\ x\neq y}} d_H(x,y)$, where, $d_H(x,y)$ denotes the Hamming distance between $x$ and $y$, namely, the number of coordinates on which $x$ and $y$ differ.

▶ **Lemma 19.** *Let $S$ be the support of a simple$^*$ non-reducible boolean distribution. Then:*

1. *$\Delta(S) \geq 2$;*
2. *no coordinate is constant on $S$, i.e., there is no $i \in [n]$ such that for a fixed $b$, $x_i = b$ for all $x \in S$.*
3. *no two coordinates are identical on all of $S$ or complementary on all of $S$.*

**Proof.** Let $P$ be a non-reducible simple$^*$ distribution over $\{0,1\}^n$ such that $S = \mathrm{supp}(P)$. For item (1), suppose there exist distinct $x, y \in S$ such that $d_H(x,y) = 1$. Let $i \in [n]$ be the unique coordinate on which $x$ and $y$ differ, and let $r := x_{[n]\setminus\{i\}} = y_{[n]\setminus\{i\}}$. Since $P$ is simple$^*$,

the two-party distribution $(\mathrm{X}_i, \mathrm{X}_{[n]\setminus\{i\}})$ is simple. Let Q be its common information. Then Q is a deterministic function of $\mathrm{X}_i$, and also of $\mathrm{X}_{[n]\setminus\{i\}}$. Since both $\Pr[(\mathrm{X}_i, \mathrm{X}_{[n]\setminus\{i\}}) = (0, r)] > 0$ and $\Pr[(\mathrm{X}_i, \mathrm{X}_{[n]\setminus\{i\}}) = (1, r)] > 0$, it follows that the two values $\mathrm{X}_i = 0$ and $\mathrm{X}_i = 1$ give rise to the same value of Q and hence Q is constant. Therefore $\mathrm{X}_i \perp\!\!\!\perp \mathrm{X}_{[n]\setminus\{i\}}$, so $P$ is reducible which gives a contradiction.

For item (2), if some coordinate $i$ were constant on $S$, then $\mathrm{X}_i$ would be constant, and hence independent of $X_{[n]\setminus\{i\}}$. Thus $P$ would be reducible, a contradiction.

For item (3), if coordinates $i$ and $j$ were identical on $S$ or complementary on $S$, then $\mathrm{X}_i$ would be a deterministic function of $\mathrm{X}_j$. Thus again $P$ would be reducible, a contradiction. ◀

Now we are ready to start our case analysis of supports of non-reducible simple* 4-party boolean distributions, organized by the size of the support. We start by ruling out supports of size smaller than 4.

▶ **Lemma 20.** *Let $P$ be a simple* non-reducible 4-party boolean distribution, and let $S := supp(P)$. Then $|S| \geq 4$.*

**Proof.** By Lemma 19, no coordinate is constant on $S$, and no two coordinates are identical or complementary on $S$.

Suppose $|S| \leq 3$, and write $S = \{x^{(1)}, \ldots, x^{(t)}\}$ with $t \leq 3$. For each coordinate $i \in [4]$, consider the length-$t$ bitstring $\left(x_i^{(1)}, \ldots, x_i^{(t)}\right) \in \{0,1\}^t$. Since no coordinate is constant on $S$, this bitstring is neither all-0 nor all-1. Hence there are at most $2^t - 2$ possibilities. Identifying a bitstring with its complement leaves at most $\frac{2^t-2}{2} \leq 3$ equivalence classes. Since there are 4 coordinates, two coordinates lie in the same class, so they are identical or complementary on $S$, a contradiction. ◀

▶ **Lemma 21.** *Let $S \subseteq \{0,1\}^4$ be such that $\Delta(S) \geq 2$, and let $J \subseteq [4]$ satisfy $|J| = 2$. Then every vertex of $B_J^S$ has degree at most 2.*

**Proof.** Let $u$ be a left vertex of $B_J^S$. If $u$ had three distinct neighbors $v^{(1)}, v^{(2)}, v^{(3)}$, then among the three 2-bit strings $v^{(1)}, v^{(2)}, v^{(3)}$ there would be two that differ in exactly one coordinate. The corresponding two points of $S$ would then differ in exactly one coordinate, contradicting the assumption that $\Delta(S) \geq 2$. The same argument applies to the right vertices. ◀

▶ **Lemma 22.** *Let $P$ be a simple* non-reducible 4-party boolean distribution, and let $S := supp(P)$. If $|S| = 4$, then, up to relabeling, $S$ is either $S_4$ or $S_5$.*

**Proof.** By Lemma 19, $\Delta(S) \geq 2$, no coordinate is constant on $S$, and no two coordinates are identical or complementary on $S$.

Since $|S| = 4$, $\Delta(S) \leq 2$. Indeed, if $\Delta(S) \geq 3$, then the radius-1 Hamming balls around the four points of $S$ would be disjoint, each of size 5, which is impossible in $\{0,1\}^4$. Thus there exist $x, y \in S$ with $d_H(x, y) = 2$. Up to relabeling, we may assume that $0000, 0011 \in S$.

Consider the support graph $B_{\{1,2\}}^S$. The left vertex 00 is adjacent to the right vertices 00 and 11. If some other point $z \in S$ satisfied $z_{\{3,4\}} \in \{00, 11\}$, then the connected component containing the left vertex 00 would contain a second left vertex adjacent to both 00 and 11 (to both 00 and 11 due to the fact that $P$ is a simple* distribution). Since no coordinate is constant on $S$, this second left vertex cannot be 01 or 10, and hence it must be 11. Therefore $\{0000, 0011, 1100, 1111\} \subseteq S$. But then the coordinates 1 and 2 are identical on $S$, a contradiction. Let $x, y$ be the two points in $S \setminus \{0000, 0011\}$. We have $x_{\{3,4\}}, y_{\{3,4\}} \in \{01, 10\}$.

If $x_{\{3,4\}} = y_{\{3,4\}}$, then, after swapping coordinates 3 and 4 if necessary, this common value is 01. Since $\Delta(S) \geq 2$, the points $x$ and $y$ must then be 0101 and 1001. Thus $S = S_4$.

Suppose instead that $x_{\{3,4\}} \neq y_{\{3,4\}}$. Then $\{x_{\{3,4\}}, y_{\{3,4\}}\} = \{01, 10\}$. Neither $x_{\{1,2\}}$ nor $y_{\{1,2\}}$ is 00 since $x, y \in S \setminus \{0000, 0011\}$ and $\Delta(S) \geq 2$. If $\{x_{\{1,2\}}, y_{\{1,2\}}\} = \{01, 10\}$, then, up to relabeling, $S = \{0000, 0011, 0101, 1010\}$. In $B^S_{\{1,3\}}$, the left vertices 00 and 11 have neighborhoods $\{00, 11\}$ and $\{00\}$, respectively. These two left vertices have a common neighbor but different neighborhoods, so this graph is not a union of bicliques, contradicting that $P$ is simple$^*$. Hence, one of the points $x, y$ satisfies $x_{\{1,2\}} = 11$ or $y_{\{1,2\}} = 11$. Up to swapping coordinates 3 and 4, we may assume that $1110 \in S$. The remaining point must then be 0101 or 1001, and a further swap of coordinates 1 and 2 if necessary, gives 0101. Hence, $S$ is a relabeling of $S_5$. ◀

▶ **Lemma 23.** *Let $P$ be a simple$^*$ non-reducible 4-party boolean distribution, and let $S := supp(P)$. If $|S| = 5$, then, up to relabeling, $S = S_3$.*

**Proof.** By Lemma 19, $\Delta(S) \geq 2$, no coordinate is constant on $S$, and no two coordinates are identical or complementary on $S$.

Consider the support graph $B^S_{\{1,2\}}$. By Lemma 21, every connected component is one of $K_{1,1}$, $K_{1,2}$, $K_{2,1}$, or $K_{2,2}$. Let $n_{11}$ be the number of $K_{1,1}$ components, let $n_{12}$ be the number of components which are either $K_{1,2}$ or $K_{2,1}$, and let $n_{22}$ be the number of $K_{2,2}$ components. Counting edges gives $n_{11}+2n_{12}+4n_{22} = 5$, and counting vertices gives $2n_{11}+3n_{12}+4n_{22} \leq 8$. The only nonnegative integer solutions are $(n_{11}, n_{12}, n_{22}) = (1, 0, 1)$ and $(1, 2, 0)$.

Assume first that $(n_{11}, n_{12}, n_{22}) = (1, 0, 1)$. Because $\Delta(S) \geq 2$, the two left vertices in the $K_{2,2}$ component are opposite vertices of $\{0, 1\}^2$, and the same holds on the right. Up to relabeling, we may therefore assume that $S = \{0000\} \cup \{0101, 0110, 1001, 1010\}$. In $B^S_{\{1,3\}}$, the left vertices 00 and 11 have neighborhoods $\{00, 11\}$ and $\{00\}$, respectively. These two left vertices have a common neighbor but different neighborhoods, so this graph is not a union of bicliques, contradicting that $P$ is simple$^*$. Hence $(n_{11}, n_{12}, n_{22}) = (1, 2, 0)$. Up to relabeling, this forces $S = \{0001, 0010\} \cup \{0100, 1000\} \cup \{1111\}$. Flipping coordinate 4 maps this set to $S_3$. ◀

▶ **Lemma 24.** *Let $P$ be a simple$^*$ non-reducible 4-party boolean distribution, and let $S := supp(P)$. If $|S| = 6$, then, up to relabeling, $S = S_2$.*

**Proof.** By Lemma 19, $\Delta(S) \geq 2$, no coordinate is constant on $S$, and no two coordinates are identical or complementary on $S$.

Consider the support graph $B^S_{\{1,2\}}$. By Lemma 21, every connected component is one of $K_{1,1}$, $K_{1,2}$, $K_{2,1}$, or $K_{2,2}$. Let $n_{11}$, $n_{12}$, and $n_{22}$ be the corresponding component counts. Counting edges gives $n_{11}+2n_{12}+4n_{22} = 6$, and counting vertices gives $2n_{11}+3n_{12}+4n_{22} \leq 8$. The only nonnegative integer solutions are $(n_{11}, n_{12}, n_{22}) = (0, 1, 1)$ and $(2, 0, 1)$.

Assume first that $(n_{11}, n_{12}, n_{22}) = (0, 1, 1)$. Because $\Delta(S) \geq 2$, the two left vertices in the $K_{2,2}$ component are opposite, and the same holds on the right. Up to relabeling, we may assume that $S = \{0000, 0011\} \cup \{0101, 0110, 1001, 1010\}$. In $B^S_{\{1,3\}}$, the left vertices 01 and 10 have neighborhoods $\{01, 10\}$ and $\{01\}$, respectively. These two left vertices have a common neighbor but different neighborhoods, so this graph is not a union of bicliques, contradicting that $P$ is simple$^*$.

Hence $(n_{11}, n_{12}, n_{22}) = (2, 0, 1)$. Up to relabeling, this forces

$S = \{0011\} \cup \{1100\} \cup \{0101, 0110, 1001, 1010\}$. Flipping coordinates 2 and 3 maps this set to $S_2$. ◀

▶ **Lemma 25.** *There is no set $S \subseteq \{0,1\}^4$ with $|S| = 7$ such that $\Delta(S) \geq 2$ and $B^S_J$ is a union of bicliques for every $J \subseteq [4]$ with $|J| = 2$.*

**Proof.** Consider the support graph $B^S_{\{1,2\}}$. By Lemma 21, every connected component is one of $K_{1,1}$, $K_{1,2}$, $K_{2,1}$, or $K_{2,2}$. Let $n_{11}$ be the number of $K_{1,1}$ components, let $n_{12}$ be the number of $K_{1,2}$ or $K_{2,1}$ components, and let $n_{22}$ be the number of $K_{2,2}$ components. Counting edges gives $n_{11} + 2n_{12} + 4n_{22} = 7$, while counting vertices gives $2n_{11} + 3n_{12} + 4n_{22} \leq 8$. Subtracting yields $n_{11} + n_{12} \leq 1$.

If $n_{22} \geq 2$, then $|S| \geq 8$, a contradiction. If $n_{22} = 1$, then $n_{11} + 2n_{12} = 3$, but $n_{11} + n_{12} \leq 1$ implies $n_{11} + 2n_{12} \leq 2$, a contradiction. If $n_{22} = 0$, then $n_{11} + 2n_{12} = 7$, but again $n_{11} + 2n_{12} \leq 2$, a contradiction. Thus no such set $S$ exists. ◀

▶ **Lemma 26.** *Let $S \subseteq \{0,1\}^4$ be such that $\Delta(S) \geq 2$. Then $|S| \leq 8$. Moreover, if $|S| = 8$, then, up to relabeling, $S = S_1$.*

**Proof.** Join two strings in $\{0,1\}^4$ by an edge if they differ in exactly one coordinate. Since $\Delta(S) \geq 2$, no such edge has both endpoints in $S$. Every point of $S$ has exactly four neighbors in $\{0,1\}^4$, so the number of edges with one endpoint in $S$ and the other in $\{0,1\}^4 \setminus S$ is $4|S|$. On the other hand, every point of $\{0,1\}^4 \setminus S$ is incident to at most four such edges, so

$$4|S| \leq 4(16 - |S|).$$

Hence $|S| \leq 8$.

Now assume that $|S| = 8$. Then equality holds above, so every point of $\{0,1\}^4 \setminus S$ is adjacent to four points of $S$. In particular, $\Delta(\{0,1\}^4 \setminus S) \geq 2$. Thus $\{0,1\}^4$ is partitioned into two sets of size 8, with $\Delta(S) \geq 2$ and $\Delta(\{0,1\}^4 \setminus S) \geq 2$. Since every edge of $\{0,1\}^4$ joins an even-weight vector and an odd-weight vector, membership in $S$ alternates with parity along every edge. Therefore $S$ is exactly one parity class. If necessary, flipping one coordinate maps the odd-parity class to the even-parity class, which is $S_1$. ◀

**Proof of Proposition 17.** Let $S := \mathrm{supp}(P)$. By Lemma 19, $\Delta(S) \geq 2$, no coordinate is constant on $S$, and no two coordinates are identical or complementary on $S$. By Lemma 20, $|S| \geq 4$. By Lemma 25, $|S| \neq 7$. By Lemma 26, $|S| \leq 8$. Thus $|S| \in \{4, 5, 6, 8\}$. If $|S| = 4$, apply Lemma 22. If $|S| = 5$, apply Lemma 23. If $|S| = 6$, apply Lemma 24. If $|S| = 8$, apply Lemma 26. ◀

## 5 Securely Sampling Non-Reducible Simple* 4-Party Boolean Distributions

To complete the proof of Theorem 1, it remains to show that all non-reducible simple* 4-party boolean distributions are securely samplable. By Proposition 17 and Lemma 16, it suffices to consider simple* distributions whose support is one of the 5 admissible supports $S_1, S_2, S_3, S_4, S_5$.

The argument in this section has three parts. First, we show that any "product-form distribution" is statistically securely samplable, provided its support admits a "semi-secure membership-test"; both these notions are defined below and the result is stated as Lemma 29. Next, as stated in Lemma 30, we show that each of the five admissible supports admits a semi-secure membership-test because each is additively representable. Finally, we show that every simple* distribution supported on one of the five admissible supports is a product-form distribution; this is stated in Lemma 31.

We present the above definitions and the statements of these three lemmas below.

▶ **Definition 27** (Product-form distribution). *A distribution $P$ on $\mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ is said to be a* product-form distribution *if there exist a nonempty set $S \subseteq \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ and weight functions $w_i : \mathcal{X}_i \to \mathbb{R}^+$ such that $supp(P) = S$ and, for every $x \in S$,*

$$P(x_1, \ldots, x_n) = \frac{1}{Z} \prod_{i=1}^{n} w_i(x_i) \tag{6}$$

*where $Z := \sum_{(x_1,\ldots,x_n)\in S} \prod_{i=1}^{n} w_i(x_i)$ is a normalization factor.*

▶ **Definition 28** (Semi-secure Membership-Test). *An $n$-party protocol $\Pi$ is said to be a* semi-secure membership-test *for a set $S \subseteq \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ if, on running $\Pi$ with inputs $x_i \in \mathcal{X}_i$ to each party, all parties learn whether $(x_1, \ldots, x_n) \in S$, and further, for all $C \subseteq [n]$, the joint views of the parties in $C$ are identically distributed on executions of $\Pi$ with inputs $x, x' \in S$ such that $x_C = x'_C$.*

Note that above, there is no privacy guarantee for inputs not in $S$.

We prove the following three lemmas in Sections 5.1–5.3.

▶ **Lemma 29.** *Let $P$ be an $n$-party product-form distribution with support $S \subseteq \mathcal{X}_1 \times \ldots \mathcal{X}_n$. Also, suppose there exists a semi-secure membership-test for $S$. Then $P$ is securely samplable.*

*More precisely, for any $\epsilon > 0$, there is an $\epsilon$-secure sampling protocol for $P$ that invokes the membership-test $O(\log 1/\epsilon)$ times.*

▶ **Lemma 30** (Admissible Supports have Semi-Secure Membership-tests). *Each of the supports $S_1, \ldots, S_5$ admits a semi-secure membership test.*

▶ **Lemma 31** (Non-Reducible Simple* Distributions are Product-Form). *Let $P$ be a 4-party simple$^*$ boolean distribution whose support is one of $S_1, \ldots, S_5$. Then $P$ is a product-form distribution.*

Combining Lemmas 29–31 with Proposition 17 and Lemma 16, we directly obtain the following, which is then used to complete the proof of Theorem 1.

▶ **Lemma 32.** *Every non-reducible simple$^*$ 4-party boolean distribution is securely samplable.*

**Proof.** Let $P$ be such a distribution. Then by Proposition 17 and Lemma 16, it can be relabeled to a simple$^*$ boolean distribution $P'$ whose support is one of the admissible supports $S_1, S_2, S_3, S_4, S_5$. Then, by Lemmas 30 and 31, $P'$ satisfies the requirements of Lemma 29, and hence is securely samplable. By Lemma 16, so is $P$. ◀

**Proof of Theorem 1.** Let $P$ be a simple$^*$ 4-party boolean distribution. If $P$ is reducible, then by Lemma 14, it is securely samplable. On the other hand if $P$ is non-reducible, by Lemma 32, it is securely samplable. Thus every simple$^*$ 4-party boolean distribution is securely samplable. The converse holds by Lemma 8. ◀

In the rest of this section, we prove Lemmas 29–31.

## 5.1 Secure Sampling via Rejection Sampling

A distribution in product-form is amenable to being sampled using a rejection sampling procedure:

**Rejection Sampling Step.** Given a distribution $P_{\mathrm{X}}$ in product-form with support $S \subseteq \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ and weight functions $w_i : \mathcal{X}_i \to \mathbb{R}^+$.

- **Independent Sampling:** For $i = 1$ to $n$, independently sample $X_i$ such that $\Pr[X_i = x] = w_i(x)/Z_i$, where $Z_i = \sum_{x \in \mathcal{X}_i} w_i(x)$.
- **Accept or Reject:** If the values sampled $(x_1, \ldots, x_n)$ are such that $(x_1, \ldots, x_n) \in S$, output it, else output $\perp$.

Note that the probability of accepting is $\sum_{(x_1,\ldots,x_n)\in S} \prod_{i=1}^{n} \frac{w_i(x_i)}{Z_i} = \frac{Z}{\prod_i Z_i}$.

It is easy to see that conditioned on accepting, the output is distributed according to $P_{\mathrm{X}}$.[3] Now consider a process that repeats the rejection sampling step at most $k$ times until a step accepts; if it accepts, then we output the sample in that step, and if it rejects in all $k$ steps, then we output a sample from $P_{\mathrm{X}}$. (Later, we shall implement this procedure using a protocol.)

The output of this entire process is also distributed as $P_{\mathrm{X}}$. Further, the probability of this procedure requiring the final direct sampling step is $(1 - \frac{Z}{\prod_i Z_i})^k$. Note that $0 < Z \leq \prod_i Z_i$ (as follows from the definition of a product-form distribution), and hence this probability decreases exponentially with $k$.

**Proof of Lemma 29.** Let the weight functions associated with the product-form distribution $P$ be $w_i : \mathcal{X}_i \to \mathbb{R}^+$, for $i = 1$ to $n$. Also, let $Z = \sum_{(x_1,\ldots,x_n)\in S} \prod_{i=1}^{n} w_i(x_i)$ and $Z_i = \sum_{x_i \in \mathcal{X}_i} w_i(x_i)$.

Our protocol is to use the rejection procedure above, for some number of iterations $k$ (to be specified below), with the rejection step implemented using a membership-test. If the final direct sampling step is required (because all $k$ iterations of the rejection sampling step rejected), this will be carried out by a fixed party.

The view of the adversary consists of an integer $t$ (the number of iterations of the rejection sampling step that are rejected in the protocol), a view of the membership test in the first $t$ iterations, and the view in the final iteration (either an accepting iteration of the rejection sampling step, or a direct sampling step). We argue that this entire view can be perfectly or $\epsilon$-statistically simulated (depending on whether the party designated for direct sampling is corrupt or not). The integer $t$ is distributed according to a fixed geometric distribution and can be simulated. Given $t$, to simulate the view of the first $t$ iterations, we faithfully simulate the protocol for all parties conditioned on their inputs not being in $S$; each of these executions is independent of the others and independent of $t$ itself. For the final iteration, if $t < k$, then we simulate the view of the adversary as follows: the $x_i$ sampled by each corrupt party is set to be exactly the ideal output given to the simulator; and, the view of the corrupt parties in the membership test is sampled from the fixed distribution of views when inputs are in the set. In the case $t = k$, there are two possibilities. If the party designated for direct sampling is not corrupt, the view simply consists of the outputs $x_i$ sent to each corrupt party; however, if the designated party is corrupt, the simulation fails.

This simulation is perfect when the designated party is not corrupt. In case it is corrupt, we note that conditioned on $t < k$ (in both simulation and real execution), the simulation is perfect; so the statistical difference between the simulated view and the real view is at

[3] Probability of the procedure outputting $(x_1, \ldots, x_n) \in S$ is $\frac{\prod_i w_i(x_i)}{\prod_i Z_i}$, and the probability of accepting is $\frac{Z}{\prod_i Z_i}$. The conditional probability is their ratio, which is the desired probability $\frac{\prod_i w_i(x_i)}{Z}$.

most the probability that $t = k$, which corresponds to all $k$ iterations of rejection sampling rejecting. This, as discussed earlier, has probability $\alpha^k$ where $\alpha = 1 - \frac{Z}{\prod_i Z_i} < 1$. To make this simulation error at most $\epsilon$, we set $k \geq \log(1/\epsilon)/\log(1/\alpha) = O(\log(1/\epsilon))$ (since $\alpha$ is a constant that depends only on the given distribution $P$). ◀

## 5.2 Semi-Secure Membership-Test for Admissible Supports

To prove Lemma 30, we rely on the following observation.

▶ **Lemma 33** (Semi-secure membership-test protocol for an additively representable set)**.** *Let $S \subseteq \mathcal{X}_1 \times \ldots \times \mathcal{X}_n$ be additively representable (Definition 2). Then $S$ admits a semi-secure membership test.*

**Proof.** Since $S$ is additively representable, there is a finite abelian group $G$, maps $\mu_i : \mathcal{X}_i \to G$ and an element $g \in G$ such that

$$S = \Big\{ x \in \mathcal{X}_1 \times \ldots \times \mathcal{X}_n : \sum_{i=1}^{n} \mu_i(x_i) = g \Big\}.$$

The semi-secure membership test proceeds as follows: Each party with input $x_i$ locally computes $\mu_i(x_i) \in G$. A standard perfectly secure protocol for addition in $G$ allows the parties to compute the sum $\sum_{i=1}^{n} \mu_i(x_i)$. They output 1 if and only if the revealed sum equals $g$. If the input lies in $S$, then the revealed sum is always $g$, and so on such inputs the protocol reveals nothing beyond membership in $S$. No security is required when the input lies outside $S$. ◀

Now to prove that the admissible supports in Equation (5) have semi-secure membership tests, we can show that they are additively representable. We do this below.

**Proof of Lemma 30.** Each of the five admissible supports is additively representable. In particular,

$$\begin{aligned}
S_1 &= \{x \in \{0,1\}^4 : \ x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 2\},\\
S_2 &= \{x \in \{0,1\}^4 : \ x_1 - x_2 - x_3 + x_4 \equiv 0 \pmod 6\},\\
S_3 &= \{x \in \{0,1\}^4 : \ x_1 + x_2 + x_3 - x_4 \equiv 0 \pmod 3\},\\
S_4 &= \{x \in \{0,1\}^4 : \ x_1 + x_2 + x_3 - x_4 \equiv 0 \pmod 6\},\\
S_5 &= \{x \in \{0,1\}^4 : \ 4x_1 + x_2 + x_3 - x_4 \equiv 0 \pmod 6\}.
\end{aligned}$$

A direct check on the 16 points of $\{0,1\}^4$ shows that each displayed congruence holds exactly on the corresponding support. Note that each equation corresponds to an additive representation where multiplying by a coefficient $c$ corresponds to the local map $\mu(0) = 0, \mu(1) = c$, and the modular addition corresponds to addition in an abelian group. Therefore each $S_i$ is additively representable, and the conclusion follows from Lemma 33. ◀

## 5.3 Proof of Lemma 31: Case Analysis of Admissible Supports

We shall invoke the following observation in the arguments below.

▶ **Lemma 34** (The $K_{2,2}$ constraint)**.** *If $P_{\mathrm{U,V}}$ is a simple two-party distribution over $\mathcal{U} \times \mathcal{V}$ such that there exist $u_0, u_1 \in \mathcal{U}$ and $v_0, v_1 \in \mathcal{V}$ with $P_{\mathrm{U,V}}(u_i, v_j) > 0$ for all $i, j \in \{0,1\}$ (i.e., the biclique $\{u_0, u_1\} \times \{v_0, v_1\}$ is a subgraph of the support graph), then*

$$P_{\mathrm{U,V}}(u_0, v_0) P_{\mathrm{U,V}}(u_1, v_1) = P_{\mathrm{U,V}}(u_0, v_1) P_{\mathrm{U,V}}(u_1, v_0). \tag{7}$$

**Proof.** Since $P_{\mathrm{U,V}}(u_i, v_j) > 0$, we have $P_{\mathrm{U,V}}(u_i, v_j) = w_1(u_i)w_2(v_j)$ for some weight functions $w_1, w_2$ as required in Equation (3). Then the LHS and RHS of Equation (7) are both $\prod_{i=0}^{1} w_1(u_i)w_2(v_i)$. ◀

▶ **Lemma 35** (Support $S_1$). *If $P$ is a simple$^*$ 4-party boolean distribution with $supp(P) = S_1$, then it is a product-form distribution.*

**Proof.** Recall that $S_1 = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$. Note that for all the three subsets up to complement $J \subset [4]$ with $|J| = 2$, namely, $\{1,2\}, \{1,3\}$ and $\{1,4\}$, the support graph $B_J^{S_1}$ has two $K_{2,2}$ components, one of them defined on $\{00, 11\} \times \{00, 11\}$ and the other one defined on $\{01, 10\} \times \{01, 10\}$. Applying Lemma 34 to the components in $B_{\{1,2\}}^{S_1}$ gives

$$P(0000)P(1111) = P(0011)P(1100), \quad P(0101)P(1010) = P(0110)P(1001).$$

Symmetrically (since the support is symmetric along coordinates $2, 3$ and $4$), for $B_{\{1,3\}}^{S_1}$ and $B_{\{1,4\}}^{S_1}$, we have

$$P(0000)P(1111) = P(0101)P(1010), \quad P(0011)P(1100) = P(0110)P(1001), \text{ and}$$
$$P(0000)P(1111) = P(0110)P(1001), \quad P(0011)P(1100) = P(0101)P(1010)$$

respectively. Now, if $P$ is simple$^*$, then every one of these equalities must hold, and hence we have the following:

$$P(0000)P(1111) = P(0011)P(1100) = P(0101)P(1010) = P(0110)P(1001). \tag{8}$$

For brevity, let $a := P(0000)$, $b := P(1100)$, $c := P(0011)$, $d := P(1010)$, $e := P(0101)$, $f := P(1001)$, $g := P(0110)$ and $h := P(1111)$. Then

$$ah = bc = de = fg. \tag{9}$$

Define weights $\omega_i$ as follows: $\omega_1 := \sqrt{\frac{bd}{ag}}$, $\omega_2 := \frac{b}{a\,\omega_1}$, $\omega_3 := \frac{d}{a\,\omega_1}$, $\omega_4 := \frac{f}{a\,\omega_1}$. Then, the following can be verified directly (from the definition of $\omega_i$ for $b, d, f$, and using Equation (9) as well for the rest): $b = a\,\omega_1\omega_2$, $c = a\,\omega_3\omega_4$, $d = a\,\omega_1\omega_3$, $e = a\,\omega_2\omega_4$, $f = a\,\omega_1\omega_4$, $g = a\,\omega_2\omega_3$, $h = a\,\omega_1\omega_2\omega_3\omega_4$. That is, we have for each $x \in S_1$, $P(x) = a\prod_{i=1}^{4}\omega_i^{x_i}$. Defining functions $w_i : \{0,1\} \to \mathbb{R}^+$ as $w_i(\alpha) = \omega_i^{\alpha}$, and noting that $\sum_{x\in S_1} P(x) = 1$, we can see that (6) holds. ◀

▶ **Lemma 36** (Support $S_2$). *If $P$ is a simple$^*$ 4-party boolean distribution with $supp(P) = S_2$, then it is a product-form distribution.*

**Proof.** Recall that $S_2 = \{0000, 0011, 0101, 1010, 1100, 1111\}$. For $J \in \{\{1,2\}, \{1,3\}\}$, the $K_{2,2}$ component of $B_J^{S_2}$ is on $\{00, 11\} \times \{00, 11\}$. For $B_{\{1,4\}}^{S_2}$, the $K_{2,2}$ component is over $\{01, 10\} \times \{01, 10\}$. Applying Lemma 34 gives, respectively,

$$P(0000)P(1111) = P(0011)P(1100),$$
$$P(0000)P(1111) = P(0101)P(1010),$$
$$P(0011)P(1100) = P(0101)P(1010).$$

If $P$ is simple$^*$, then the displayed equalities must hold, and hence we have

$$P(0000)P(1111) = P(0011)P(1100) = P(0101)P(1010). \tag{10}$$

Now let $a := P(0000)$, $b := P(0011)$, $c := P(0101)$, $d := P(1010)$, $e := P(1100)$, and $f := P(1111)$. Then $af = be = cd$. Set $\omega_1 := 1$, $\omega_2 := \frac{e}{a}$, $\omega_3 := \frac{d}{a}$, and $\omega_4 := \frac{c}{e}$. By construction, $a\,\omega_1\omega_2 = e$, $a\,\omega_1\omega_3 = d$, and $a\,\omega_2\omega_4 = c$. The remaining nontrivial values are $a\,\omega_3\omega_4 = \frac{cd}{e} = b$ and $a\,\omega_1\omega_2\omega_3\omega_4 = \frac{cd}{a} = f$, using $be = cd$ and $af = cd$. Thus $P(x) = a\prod_{i=1}^{4}\omega_i^{x_i}$ for every $x \in S_2$. With $w_i(\alpha) = \omega_i^{\alpha}$, and noting $\sum_{x\in S_2} P(x) = 1$ we get (6). ◀

For the remaining three supports, every distribution on the support already has the product form (6); no additional simple* constraints need to be imposed.

▶ **Lemma 37** (Supports $S_3, S_4, S_5$)**.** *If $P$ is a 4-party boolean distribution with supp$(P) = S_3, S_4$ or $S_5$, then $P$ is a product-form distribution.*

**Proof.** We shall denote the probabilities of the following elements: $a := P(0000), b := P(0011), c := P(0101), d := P(1001),$ and $e := P(1110)$ for all these supports.

**Case $S_3$.** Recall that $S_3 = \{0000, 0011, 0101, 1001, 1110\}$. Set $\omega_4 := \left(\frac{bcd}{ea^2}\right)^{1/3}$, $\omega_1 := \frac{d}{a\,\omega_4}$, $\omega_2 := \frac{c}{a\,\omega_4}$, and $\omega_3 := \frac{b}{a\,\omega_4}$. Then $a\,\omega_3\omega_4 = b$, $a\,\omega_2\omega_4 = c$, and $a\,\omega_1\omega_4 = d$ by construction, and $a\,\omega_1\omega_2\omega_3 = a \cdot \frac{d}{a\,\omega_4} \cdot \frac{c}{a\,\omega_4} \cdot \frac{b}{a\,\omega_4} = \frac{bcd}{a^2\omega_4^3} = e$. Thus $P(x) = a\prod_{i=1}^{4}\omega_i^{x_i}$ for every $x \in S_3$, and with $w_i(\alpha) = \omega_i^{\alpha}$, we get (6).

**Case $S_4$.** Recall that $S_4 = \{0000, 0011, 0101, 1001\}$. Set $\omega_1 := \frac{d}{a}$, $\omega_2 := \frac{c}{a}$, $\omega_3 := \frac{b}{a}$, and $\omega_4 := 1$. Then $a\,\omega_3\omega_4 = b, a\,\omega_2\omega_4 = c,$ and $a\,\omega_1\omega_4 = d$, so $P(x) = a\prod_{i=1}^{4}\omega_i^{x_i}$ for every $x \in S_4$, and with $w_i(\alpha) = \omega_i^{\alpha}$, we get (6).

**Case $S_5$.** Recall that $S_5 = \{0000, 0011, 0101, 1110\}$. Set $\omega_1 := \frac{ae}{bc}$, $\omega_2 := \frac{c}{a}$, $\omega_3 := \frac{b}{a}$, and $\omega_4 := 1$. Then $a\,\omega_2\omega_4 = c$, $a\,\omega_3\omega_4 = b$, and $a\,\omega_1\omega_2\omega_3 = e$. Hence, $P(x) = a\prod_{i=1}^{4}\omega_i^{x_i}$ for every $x \in S_5$, and with $w_i(\alpha) = \omega_i^{\alpha}$, we get (6). ◀

**Proof of Lemma 31.** The proof follows immediately from Lemma 35, Lemma 36 and Lemma 37. ◀

## References


1 Saugata Basu, Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Geometry of secure two-party computation. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 1035–1044. IEEE, 2022. doi:10.1109/FOCS54457.2022.00101.

2 Saugata Basu, Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Solving linear inequalities over the space of convex sets & its applications to cryptography and hydrodynamics. In *66th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2025, Sydney, Australia, December 14-17, 2025*, pages 2369–2380. IEEE, 2025. doi:10.1109/FOCS63196.2025.00124.

3 Donald Beaver. Foundations of secure interactive computing. In *Advances in Cryptology — CRYPTO '91*, pages 377–391. Springer, 1991. doi:10.1007/3-540-46766-1_31.

4 Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1–10. ACM, 1988.

5 David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 11–19. ACM, 1988.

6 Benny Chor and Yuval Ishai. On privacy and partition arguments. *Inf. Comput.*, 167(1):2–9, 2001. doi:10.1006/inco.2000.3013.

7 Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC)*, pages 218–229. ACM, 1987. doi:10.1145/28395.28420.

8 Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 20–31. ACM, 1988. doi:10.1145/62212.62215.

9 Joe Kilian. More general completeness theorems for secure two-party computation. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 316–324. ACM, 2000. doi:10.1145/335305.335342.

10 Eyal Kushilevitz. Privacy and communication complexity. *SIAM Journal on Discrete Mathematics*, 5(2):273–284, 1992. Originally presented at FOCS 1989. doi:10.1137/0405021.

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

12 Manoj Prabhakaran and Vinod M. Prabhakaran. On secure multiparty sampling for more than two parties. In *2012 IEEE Information Theory Workshop, Lausanne, Switzerland, September 3-7, 2012*, pages 99–103. IEEE, 2012. doi:10.1109/ITW.2012.6404773.

13 Vinod M. Prabhakaran and Manoj M. Prabhakaran. Assisted common information with an application to secure two-party sampling. *IEEE Transactions on Information Theory*, 60(6):3413–3434, 2014. doi:10.1109/TIT.2014.2316011.


# A Beyond 4 Parties: A 6-Party Simple* Distribution without Additive Representation

In Section 5, our positive results for 4-party boolean simple* distributions relied on the fact that all 5 admissible supports are *additively representable* (Definition 2), which naturally enables a semi-secure membership test. A fundamental question is whether all boolean simple* supports have an additive representation.

In this appendix, we show that this is not the case. We present a 6-party simple* boolean support that is not additively representable, but the distribution uniformly distributed over the support is statistically securely samplable.

## A.1 The 6-Party Support $S_6$

Consider the 6-party boolean distribution uniformly distributed over the support $S_6 \subset \{0,1\}^6$, where $S_6 = \{000000, 101100, 110010, 010101, 001011, 111001, 100111\}$. One can verify that this distribution is simple* by checking every bipartite support graph across bipartitions.

▶ **Lemma 38.** *The support $S_6$ is not additively representable.*

**Proof.** Assume for contradiction that $S_6$ is additively representable. That is, there exist maps $\mu_i : \{0,1\} \to G$, where $G$ is some finite abelian group $G$, and a target element $g \in G$, such that $x \in S_6$ if and only if $\sum_{i=1}^{6} \mu_i(x_i) = g$.

Since $000000 \in S_6$, we have $\sum_{i=1}^{6} \mu_i(0) = g$. We can shift the maps without loss of generality by defining $\tilde{\mu}_i(x_i) = \mu_i(x_i) - \mu_i(0)$. This ensures that $\tilde{\mu}_i(0) = 0$ for all $i$, and the target natively becomes $\tilde{g} = 0$. Thus, $x \in S_6 \iff \sum_{i=1}^{6} \tilde{\mu}_i(x_i) = 0$.

Let $a_i = \tilde{\mu}_i(1) \in G$. The inclusion of the sequence of six non-zero points of $S_6$ yields the following additive relations in $G$:

$$a_1 + a_3 + a_4 = 0 \tag{11}$$
$$a_1 + a_2 + a_5 = 0 \tag{12}$$
$$a_2 + a_4 + a_6 = 0 \tag{13}$$
$$a_3 + a_5 + a_6 = 0 \tag{14}$$
$$a_1 + a_2 + a_3 + a_6 = 0 \tag{15}$$
$$a_1 + a_4 + a_5 + a_6 = 0 \tag{16}$$

Adding equations (11), (12), (13), and (14) and subtracting equations (15) and (16) yields:

$$\begin{aligned}&(a_1 + a_3 + a_4) + (a_1 + a_2 + a_5) + (a_2 + a_4 + a_6) + (a_3 + a_5 + a_6)\\ &- (a_1 + a_2 + a_3 + a_6) - (a_1 + a_4 + a_5 + a_6)\\ &= a_2 + a_3 + a_4 + a_5 = 0.\end{aligned}$$

This implies that the point 011110 is evaluated to 0, and thus must also belong to the set. However, $011110 \notin S_6$, which yields a contradiction. Consequently, $S_6$ is not additively representable over any finite abelian group. ◀

## A.2 Securely Sampling $S_6$

Let $m = 011110$ be the specific point that we saw in the proof of Lemma 38. Define the set $T_6 = S_6 \cup \{m\}$, resulting in

$$T_6 = \{000000, 101100, 110010, 010101, 001011, 111001, 100111, 011110\}.$$

Note that $T_6$ has an additive representation over the group $\mathbb{Z}_2^3$. By setting the target element $g = (0, 0, 0)$ and defining the maps $\mu_i : \{0, 1\} \to \mathbb{Z}_2^3$ such that $\mu_i(0) = (0, 0, 0)$ for all $i$ and the non-zero mappings are $\mu_1(1) = (1, 0, 0)$, $\mu_2(1) = (0, 1, 0)$, $\mu_3(1) = (1, 0, 1)$, $\mu_4(1) = (0, 0, 1)$, $\mu_5(1) = (1, 1, 0)$, and $\mu_6(1) = (0, 1, 1)$, the set $T_6$ is defined exactly by the single equation:

$$\sum_{i=1}^{6} \mu_i(x_i) = (0, 0, 0)$$

Because $T_6$ is additively representable, it admits a semi-secure membership test (by Lemma 34), and the uniform distribution supported on $T_6$ is securely samplable.

We construct the secure sampling protocol for uniform distribution over $S_6$ via the following protocol:

1. The 6 parties sample a joint outcome $\mathrm{X} = (\mathrm{X}_1, \ldots, \mathrm{X}_6)$ uniformly spanning $T_6$ enabled through a semi-secure membership test of $T_6$.
2. Let $d = \mathrm{X} \oplus m$. Note that $\mathrm{X} = m$ if and only if $d = 000000$. Every party $i$ samples an independent, uniformly random bit $r_i \in \{0, 1\}$, and computes $u_i = r_i d_i$.
3. The parties securely compute the sum $\beta = \bigoplus_{i=1}^{6} u_i$ over $\mathbb{Z}_2$ and reveal it via a standard secure summation protocol.
4. If $\beta = 1$, they accept X and terminate. Otherwise, they reject and repeat.

▶ **Theorem 39.** *The uniform distribution over $S_6$ is statistically securely samplable using the protocol described above.*

**Proof.** First, we analyze the output distribution. In step 1, the protocol samples X uniformly from $T_6$. If $\mathrm{X} = m$, then $d = \mathrm{X} \oplus m = 000000$. This implies $u_i = 0$ for all $i \in \{1, \ldots, 6\}$, and the revealed sum is always $\beta = 0$, so the sample is rejected. If $\mathrm{X} \in S_6$, then $d \neq 000000$, and there is at least one coordinate $i$ where $d_i = 1$. Since $r_i$ is sampled uniformly and independently in step 2, the term $u_i = r_i d_i$ is uniformly and independently distributed over $\{0, 1\}$ for every such coordinate $i$. This makes $\beta$ uniformly distributed as well. Hence, every $\mathrm{X} \in S_6$ is accepted with probability exactly $1/2$. Conditioned on acceptance, the output is exactly the uniform distribution over $S_6$.

Next, we establish privacy. Fix a corrupt coalition $C \subset \{1, \ldots, 6\}$. We construct a simulator for the view of $C$. On a given output $\mathrm{X}_C$, the simulator generates the local random bits $r_C$ uniformly. It remains to simulate the transcript of the secure summation for the accepted condition $\beta = 1$.

Let $D = \{x \oplus m \mid x \in T_6\}$. Observe two properties of $D$:

1. $D$ is a linear space under bitwise XOR.
2. For any two distinct, non-zero vectors $d, e \in D$, their sets of non-zero coordinates intersect. That is, no two non-zero vectors in $D$ have disjoint supports.

In the real protocol, the honest parties' contribution to $\beta$ is $\bigoplus_{i \notin C} u_i = \bigoplus_{i \notin C} r_i d_i$. The secure summation transcript is perfectly simulatable from the corrupt inputs $u_C$ and the final sum $\beta = 1$, provided that the honest contribution to $\beta$ is uniformly random. This uniformity holds as long as $d_{C^c} \neq \mathbf{0}$ (meaning that there is at least one honest party $i \notin C$ with $d_i = 1$).

Suppose, for contradiction, that there exist two valid outcomes $x, y \in S_6$ corresponding to the same output $\mathrm{X}_C = x_C = y_C$ for the coalition, and it happens that $d = x \oplus m$ satisfies $d_{C^c} = \mathbf{0}$. This means $d$ is entirely supported on $C$. Let $e = y \oplus m$. Because $x_C = y_C$, the vector $d \oplus e = x \oplus y$ is zero on $C$, meaning it is entirely supported on $C^c$. By property 1, both $d$ and $d \oplus e$ are in $D$. Since their supports are disjoint, property 2 implies that one must be the zero vector. Since $x \in S_6$, it follows that $d \neq 000000$, and therefore $d \oplus e = 000000$, which implies $x = y$.

Therefore, for any given output $\mathrm{X}_C$ for the coalition, exactly one of two cases applies:

- $d_{C^c} \neq \mathbf{0}$ for all valid $x$ consistent with $\mathrm{X}_C$. In this case, the honest parties always supply an independent, uniform bit to $\beta$. The simulator simply sets $\beta = 1$ and perfectly simulates the secure sum transcript.
- $\mathrm{X}_C$ is consistent with exactly one outcome $x \in S_6$. In this case, the simulator knows the entire vector X, and can simulate the secure sum transcript by simulating the honest parties as well.

Furthermore, rejected iterations are independent and the view for such iterations can be simulated by simulating all parties conditional on $\beta = 0$. The statistical distance between the simulated view and the real view approaches zero exponentially with the number of rounds. This satisfies the security requirement. ◀