

On perfectly secure 2PC in the OT-hybrid model

Anat Paskin-Cherniavsky*

August 6, 2018

Abstract

We initiate the study of perfect (rather than merely statistical) reductions among cryptographic primitives. For simplicity, we focus on finite functionalities.

In addition to the obvious theoretical appeal of the question towards better understanding secure computation, perfect, as opposed to statistical reductions may be useful for designing MPC protocols with high concrete efficiency, achieved by eliminating the dependence on a security parameter.

1-out-of-2 bit-OT (dubbed OT) was shown to be complete for statistically secure 2PC for all functionalities [Kil88, IPS08]. Existing protocols in the OT-hybrid model only offer statistically secure with abort (efficient) protocols (requiring no further computational assumptions) for all 2PC functionalities. Disregarding efficiency requirements, all 2PC functionalities have protocols with full statistical security in this setting.

As opposed to the statistical setting, it is not known whether OT is complete for perfectly secure 2PC. Furthermore, only a few sporadic examples of functionalities that have such protocols are known. On the negative side we have somewhat better understanding as implied, for instance, by the literature on fairness (for statistical security in the OT hybrid model).

Quite surprisingly [IKOPS11] demonstrate that all client-server functionalities can be efficiently reduced to OT with statistical full security (no abort) in only one round.

Motivated by this relative “ease” of client-server functionalities for statistically secure 2PC in the OT-hybrid model, we study perfect reductions to OT for this class of functions. We prove that for many client-server functions of the form $f : X \times Y \rightarrow \{0, 1\}$, where server domain size $|Y|$ is larger than client domain size $|X|$, have a perfect reduction to OT. More precisely, a $g(|X|, |Y|) = \Omega(1)$ -fraction of functions are perfectly reducible to OT. This fraction grows roughly as $1 - \exp(-|X| - |Y|)$. Furthermore, our reduction is 1-round using an oracle to secure evaluation of OT^l (as in [IKOPS11]). More generally, for $f : X \times Y \rightarrow Z$, $\Omega(1)$ of the functions with $|Y| > |X|(|Z| - 1)$ are perfectly reducible to OT in 1 round.

Our work leaves many open questions. The main open the question of whether all finite client-server functionalities are perfectly reducible to OT (not necessarily in one round). Another open question is whether any 2PC functionalities in the OT-hybrid model require strictly more than 1 round.

1 Introduction

We revisit the question of what are the simplest idealized functionalities required for perfectly secure 2PC - either of all, or at least “interesting” classes of functionalities. As 1-out-of-2-bit-OT is complete for several useful security notions, in this work we focus on 1-out-of-2-bit-OT as a candidate. While the setting of statistical security is quite well understood, the question of perfect security of 2PC in the OT hybrid model is wide open.

Briefly, in the OT-hybrid model, in addition to sending messages among themselves, the parties are allowed to make (any number of) calls to an idealized secure implementation of 1-out-of-2-bit-OT. More precisely, we assume that in every round, one party either sends a message over the channel connecting the parties, or makes a call to an ideal OT functionality 1-out-of-2-bit- OT^l where $l \geq 1$ is some number. The same party plays the sender of the OT call.

That is, here we assume a somewhat larger set of ideal functionalities available to us $\mathcal{OT} = \{1\text{-out-of-2-bit-OT}^l\}_{l \geq 1}$, where in each round, the parties are allowed to make a call to some $g \in \mathcal{OT}$. In 1-out-of-2-bit- OT^l the parties submit all inputs simultaneously, and the receiver receives all outputs simultaneously. In particular, she may not choose some of the inputs based on

*Department of Computer Science, Ariel University. E-mail: anatpc@ariel.ac.il

outputs of other OT calls. In this work, and when discussing efficient protocols from the literature, we focus on finite functionalities, so the complexity is measured in terms of a security parameter 1^k (where the simulation error is $\epsilon = \text{neg}(k)$). Let us briefly review some key results on statistically secure protocols in the OT-hybrid model.

Statistically secure 2PC in the OT-hybrid model. In the subsequent discussion we consider the more standard setting where protocols are efficient, unless stated otherwise. Even inefficiently, statistically secure computation is known to be impossible in the plain model even against semi-honest adversaries for some simple functions such as AND and OR [1]. Here even a simulation error of, say, $1/3$ is not achievable. Among the functionalities that are efficiently semi-honestly computable even with perfect security, some are not computable with statistical security against malicious parties in the plain model.

In particular, Cleve [2] has demonstrated that even the simple functionality of coin tossing where both parties output the same random bit, is not efficiently computable with statistical security. This impossibility extends to the OT-hybrid model.

As a consequence, the 2PC literature (more generally, MPC without honest majority) has settled on a weaker notion of security with abort where the ideal world adversary A has the extra power allowing it to learn the output $f_A(x, y)$ first, and then decide whether to instruct the TP to send the honest party B its output $f_B(x, y)$ or to send it \perp (abort). General purpose 2PC protocols that are statistically secure with abort for any 2PC functionality have been developed starting with [3] in the computational setting, followed by [4], that only assumes an OT oracle (while [3] relies on additional cryptographic primitives, [4] demonstrates how to implement these and many other cryptographic primitives using OT).

A more recent alternative relaxation of statistical security [5] allows for a polynomial error $\text{poly}(k^{-1})$, while requiring the parties are still efficient. In [5], it is proved that all 2PC functionalities are computable with statistical security in the OT hybrid model according to this notion. They refer to this notion as $1/p$ -security.

Round complexity of fully statistically secure protocols in the OT-hybrid model. Arguably, one of the most important measures of efficiency of MPC protocols is their round complexity. On the OT-hybrid model, the results of [5] can be interpreted as statistically secure protocols in the OT hybrid model in the setting where efficiency is not required. In particular, their round complexity may be exponential in k .

Also, quite surprisingly, it turns out that many 2-party functionalities can be evaluated with full statistical security with round complexity $\text{poly}(k)$ (in fact, even $\text{polylog}(k)$) as discovered in the seminal work [6], which rekindled interest in statistical 2PC with full security (in the OT hybrid model) - also referred as security with *fairness*¹. It was followed by several, [7, 8] to mention a few. In particular [8] completes the characterization of symmetric boolean functions (where both parties receive the same output).

However, all (general) protocols from this line of work require round complexity of $\omega_k(1)$. In [9], a 1-round protocol is presented for *client-server* functionalities, where only the client learns an output. The protocol has a single round, and makes a single call to an 1-out-of-2-bit-OT^l oracle (it does not even use the channel connecting the parties). Furthermore, the protocol's computational and communication complexity are efficient in k . So, while all 2PC functionalities can be evaluated with statistical security in the OT hybrid model (possibly inefficiently), there are provable gaps in their round complexity.

For instance, Cleve's impossibility result, and [6]'s result for functions with a so called *embedded xor*, in fact prove that certain functionalities including coin-tossing require round complexity of $\omega_k(1)$. This puts coin tossing much higher in the round complexity hierarchy than all client-server functionalities which have protocols with round complexity of 1 (on the other hand, round complexity $\text{exp}(k)$ suffices for all functionalities).

On the other hand, functionalities computable with perfect full security by definition have round complexity of $O_k(1)$.

Perfectly secure 2PC in the OT-hybrid model. As we see from the brief survey above, the statistical setting is qualitatively understood (for unbounded parties), and even the round

¹Technically, fairness is not precisely equivalent to full security.

complexity of protocols is partially understood, much less is known in the perfect setting. The ultimate goal of this work is to understand which functionalities can be evaluated with perfect security in the OT hybrid model. We are interested both in full perfect security, and in perfect security with abort.

On the positive side, we are aware of only a handful of perfect reductions to 1-out-of-2-bit-OT. One is from string-OT [10], and one from 1-out-of-2-bit-TO [11], which is the same as 1-out-of-2-bit-OT where the roles of the parties are reversed. The first one sends no bits over the point to point channel, and their result can in fact be extended to 1-out-of- t l -string-OT for any parameter t, l . It only uses the 1-out-of-2-bit-OT ^{l} oracle. The latter requires only a single bit of additional communication over the channel connecting the parties. Let us get back for a moment to the broader question of identifying simple classes of functionalities \mathcal{F} which allow for perfectly secure 2PC in the \mathcal{F} -hybrid model for interesting (more complicated than \mathcal{F}) classes of functionalities. In [12], the authors show that all client-server functionalities can be efficiently evaluated in a hybrid model where \mathcal{F} consists of all randomized 2-party functionalities that receive no inputs (in their terminology - in the preprocessing model).

Much more is known on the negative side. Even for the more liberal setting of security with perfect abort, it has been shown that even in the preprocessing model, some simple functionalities such as $f(x_1, x_2) = (x_1 \oplus x_2, x_1 \oplus x_2)$ may not be securely evaluated [12].² This implies that 1-out-of-2-bit-OT ^{l} does not allow for perfectly secure with abort 2PC of this functionality either. The reason is that 1-out-of-2-bit-OT ^{l} is a client-server functionality, and as shown in [12], it is perfectly computable in the preprocessing model (with full security). Thus, having a secure with abort protocol in the OT-hybrid model, would imply a protocol in the preprocessing model, with the same notion of security.

Negative results for the full security setting are implied for a broad class of functions by negative results from the fairness literature, such as impossibility results in [8].

However, the state of affairs is that most 2PC functionalities known to be computable with fairness remain unclassified as to perfect security.

1.1 Our results

Motivated by the relative ease of client-server functionalities for statistical security in the OT-hybrid model (only requiring an single call to 1-out-of-2 l -string-OT for a suitable l), we start with client-server functionalities.

Question 1. Characterize the set of 2PC functionalities (not necessarily boolean) which are perfectly secure in the OT-hybrid model. As a starting point, can we characterize client-server functionalities ?

We make progress on the above question, and discover a broad class of 2PC functionalities computable with perfect security.

Theorem 1.1 (Informal). *Let $f : X \times Y \rightarrow Z$ be a deterministic finite client-server functionality. If the truth table of f is full dimensional (as defined in [7]), then f is computable with perfect security in the OT-hybrid model.*

Roughly, this class contains most functionalities for each pair X, Y where $|X|$ is much larger than $|Y|$. This class includes some useful functionalities such as set intersection, where the set domain for X is somewhat larger than that of $|Y|$. Another clean example is t -out-of- n -bit-OT, where t is somewhat small relatively to n (but does not need to equal 1, as for previous OT functionalities known to be perfectly reducible to OT).

We do not know whether all client-server functionalities are computable with perfect security, and leave it as an interesting open question.

Our Techniques. In a nutshell, we start with a variant of [9]’s protocol, which is statistically secure with abort. We rely on a special structure of the protocol, where the probability of \perp is independent of the input, up to negligible differences.³

²Observe efficiency is not an issue here, as any fixed-round protocol with perfect security (with or without abort) is anyhow efficient.

³In [9], they also put forward a protocol which is fully statistically secure, essentially by setting the server’s input to some default value instead of outputting \perp . For the purpose of making the protocol perfectly secure, we make a different choice for \perp .

To make the protocol perfectly secure against malicious clients, we modify the so called “watch-lists” used in [9] to include exactly k out of n virtual servers, rather than enlist each server with a certain probability. Then, to make it perfectly secure against malicious servers, we rely on geometric interpretation of security (as previously used in the fairness literature), and come up with a way to replace \perp in the ideal model simulating a corrupted server for functions of *full dimension*.

Roadmap. Section 2 includes preliminaries from geometry and algebra that will be useful for us, and some useful facts on 1-out-of-2-bit-OT. In section 3 we discuss our model and (partially) restate the standard security definition in geometric terms, which is crucial for the analysis of our main construction. In section 4 we state our main perfect protocol working for so called *full-dimensional* client-server functions. The appendices contain some additional results. In appendix A we restate a folklore result as a simple instance of a perfect protocol in our model, which in fact, does not require an OT oracle at all. In the appendices we briefly go over possible applications of our result for concretely efficient 2PC constructions, and mention some of the open questions left by the paper.

Acknowledgement. The author is very grateful to Yuval Ishai for suggesting this question, and for many helpful discussions.

2 Preliminaries

Convex Geometry. We will need the following geometric notion (eventually, the represent truth tables of 2PC functions).

Definition 2.1 (Affine dimension [7]). *For a set of vectors $V = \{v_1, \dots, v_t\} \subseteq \mathbb{R}^n$, we define their affine dimension $\mathcal{A}(V)$ as the dimension of the set $\{v_i - v_1\}_{i \geq 2}$.*

For a vector $v \in \mathbb{R}^m$, we let $|v|_1 = \sum_i |v_i|$ denote its ℓ_1 norm, and $|v|_\infty = \max_i |v_i|$ denote its ℓ_∞ norm. For a set of vectors $V = \{v_1, \dots, v_t\} \subseteq \mathbb{R}^n$, a linear combination $\sum_i \alpha_i v_i$ where $\sum_i \alpha_i = 1$ and $\forall i \alpha_i \geq 0$ is a convex combination of V . The convex hull of V , $\text{CH}(V) = \{u = \sum_i \alpha_i v_i \mid u \text{ is a convex combination of } V\}$.

Algebra. For a matrix $A \in \mathbb{F}^{n \times n}$, where \mathbb{F} is a field, let $|A|$ denote the determinant of A . $A^{i,j}$ denotes the (i, j) 'th co factor of A , which is the $(n-1) \times (n-1)$ matrix obtained by removing the i 'th row and j 'th column of A . It is well known that:

Fact 1. $A^{-1} = C$ where $|C_{i,j}| = |A_{i,j}|/|A|$ (Cramer's formula).

For a pair of matrices $M_1 \in \mathbb{F}^{n_1 \times m}$, $M_2 \in \mathbb{F}^{n_2 \times m}$, we denote by $[M_1 || M_2]$ the concatenation of M_2 below M_1 .

Oblivious Transfer (OT). The 1-out-of-2-bit-OT functionality is a client-server functionality, where the server inputs a pair (b_1, b_2) of bits, the client inputs an index $i \in \{0, 1\}$. The client outputs b_i , while the server outputs \perp . A generalization 1-out-of- t -bit-OT of 1-out-of-2-bit-OT lets the client pick one out of t bits b_1, b_2, \dots, b_t supplied by the server. In a further generalization 1-out-of- t h -string-OT the t bits are replaced by strings $s_1, \dots, s_t \in \{0, 1\}^h$, of which on input i the client learns s_i .

A perfect reduction from 1-out-of- t h -string-OT to 1-out-of-2-bit-OT was put forward in the elegant work of [10], which constitutes one of the few examples of perfect reductions to 1-out-of-2-bit-OT known so far.

Theorem 2.1. *[[10]] There exists a perfectly secure protocol as in Definition 3.1 of 1-out-of-2 h -string-OT with communication complexity $l \leq (t-1)5h$. We refer to it as the Π_{int} protocol.*

3 Our model

We consider secure evaluation of client-server (non interactive, deterministic) functionalities $f : X \times Y \rightarrow Z$ for finite domains X, Y, Z , where the client outputs $f(x, y)$ and the server outputs \perp

(has no output).⁴ We focus on finite functionalities f (that is X, Y, Z are finite, and independent of a security parameters k). Generally 2PC functionalities may be interactive and randomized. We refer 2PC functionalities which are non-interactive and deterministic as 2PC *functions*.

We consider secure evaluation of such f in the stand-alone setting, with unconditional security, against a non adaptive malicious adversary corrupting a single party. We work in an “enhanced” version of the OT-hybrid model where in every round a party either sends information over the point-to-point channel, or the parties make a call to a perfectly secure implementation of 1-out-of-2-bit-OT ^{l} for some number l that may depend on the round number (the client plays the receiver’s role in all the oracle calls), which is rather standard. We assume the order of speaking is fixed, and does not depend on the communication so far, the inputs, or the randomness.⁵ For client and server inputs $c \in \{0, 1\}^l$, $s = ((s_{1,1}, s_{1,2}), \dots, (s_{l,1}, s_{l,2}))$ to 1-out-of-2-bit-OT ^{l} , respectively, we let $s[c]$ denote $s_{1,c_1}, \dots, s_{l,c_l}$.

Our security notion is the standard simulation-based notion as in [13]. That is, we require statistical security against a malicious server or a malicious client, and perfect correctness if both parties behave honestly. We say a protocol is $\epsilon(k)$ -client correct if for any malicious server the simulation error is bounded from above by ϵ .

More specifically, fix a 2PC protocol in the OT-hybrid model, where the parties are dubbed “client” and “server” respectively. For any (non-uniform) adversary A corrupting the server in Π , and $x \in X, z \in \{0, 1\}^*$ define $Real_A^{\Pi, z, x} = (OUT_A(1^k, z)(x), View_A(1^k, z)(z))$ For an ideal-world adversary S controlling the server let $Ideal_S^{\Pi, z, x} = (OUT_S(1^k, z)(x), View_S(1^k, z)(z))$ We require that for any adversary A there exists a simulator S_A such that for all x, z

$$SD(Ideal_S^{\Pi, z, x}, Real_A^{\Pi, z, x}) = neg(k).$$

Here the ideal-world adversary may not abort the computation (that is, we require full security). Additionally, if A is polynomial-time, then so is S_A . The definition for security against a corrupted client is analogous.

We say that the protocol is $\epsilon(k)$ server-private if the simulation error against every malicious client is bounded by $\epsilon(k)$.

For simplicity, we do not concern ourselves with the efficiency of protocols or the simulator, and allow all parties to be unbounded. The adversaries we allow are also unbounded. In fact, our simulator can be made efficient for efficient (in k) adversaries, but this is a secondary issue, and is deferred to the full version.

If the simulator’s output joint with honest party’s output corresponding to (every) malicious adversary (server or client respectively) has distance $\leq \epsilon$ from the real world distributions, we say the protocol is ϵ -statistically secure. The protocol is statistically secure if $\epsilon(k)$ is negligible in k . If ϵ equals 0 for all adversaries, we say the protocol is perfectly secure against a malicious server (client).

1-round protocols. In this work we further focus on 1-round protocols, where a single call to 1-out-of-2-bit-OT ^{l} is made by the parties. In this setting, security against malicious senders reduces to requiring that the client’s output distribution alone is consistent with some input distribution x^* over X , as the sender has no view and no output. For corrupted clients, we again consider only their view alone, as the sender has no output.

Definition 3.1 (1-round protocols in OT-hybrid model). *A protocol for evaluating $f : X \times Y \rightarrow Z$ are tuples $\Pi = (\Pi_Q, \Pi_R, \Pi_D)$ of randomized algorithms, where $\Pi_Q(x) : X \rightarrow \{0, 1\}^l$ generates client’s query c . $\Pi_R(x, c, v) : X \times \{0, 1\}^l \times \{0, 1\}^l \rightarrow Z$ generates client’s output based on x, c and OT reply v .⁶ $\Pi_D(y) : Y \rightarrow \{0, 1\}^{2l}$ is server’s generator of OT inputs. We refer to l as the communication complexity of Π .*

⁴All the definitions below readily generalize to randomized functionalities f , but we focus on deterministic f for simplicity.

⁵The point-to-point channel is not necessary in 1-round protocols where the client does not send messages to the server, as any messages sent to the client over this channel can be emulated by the OT channel.

⁶For some, but not all functions f , x is not required as an input to R , as $C_x \cup C_{x'} = \phi$ for all $x \neq x'$. It is not hard to prove that a sufficient condition on f for having $C_x \cup C_{x'} = \phi$ in all secure protocols for f is the existence of a 2×2 rectangle $\{y, y'\} \times \{x, x'\}$ in which 3 of the entries are identical, and the other entry differs from these three.

A protocol $\Pi = (\Pi_Q, \Pi_R, \Pi_D)$ as in Definition 3.1 with CC l operates in the 1-out-of-2-bit-OT^{*l*}-hybrid model as described above.⁷ That is, it is specified by a pair of randomized Turing machines $\Pi_C^?, \Pi_S^?$ with oracle access to an idealized functionality 1-out-of-2-bit-OT^{*l*} operating as follows

$\Pi_C^?(x; r)$: Let $c = \Pi_Q(x; r)$. Send c as input to the 1-out-of-2-bit-OT^{*l*} oracle, and let v denote the oracle's output. Output $\Pi_R(x, c, v; r)$.

$\Pi^?(y; r)$: Let $s = \Pi_D(y; r)$, and send it to the 1-out-of-2-bit-OT^{*l*} oracle.

Both algorithms Π_C, Π_S run in parallel, in a single round. We will usually use the notation $\Pi = (\Pi_Q, \Pi_R, \Pi_D)$ to denote protocols, while Π_C, Π_S are implicit.

The above definition defines the syntax of protocols we consider. In the following (this and following section) we discuss the security requirements we pose on our protocols.

We will usually state our protocols in a hybrid model where the parties have access to some l oracles 1-out-of- t_i h_i -string-OT in parallel, where l and (t_i, h_i) are numbers of our choice. This is potentially useful for optimizing the complexity of real-world, computationally secure protocols that are based on our construction, as OT extension allows to implement 1-out-of-2 h -string-OT using a sublinear (in k) number of calls to 1-out-of-2-bit-OT and some additional sublinear work, assuming a strong variant of PRG [14]. Also, this is wlog. in our perfectly secure setting and costs only linear time $O(tk)$ to convert into a perfect protocol in the 1-out-of-2-bit-OT-hybrid model by using the 1-round perfect reduction from Theorem 2.1.

From now on, all our definitions apply to 1-round protocols for client-server functionalities (in the OT hybrid), as we only consider this type of protocols.

Definition 3.2. *Here, we assume that f is defined on $f : X \times Y \rightarrow Z$, where $\perp \in Y, Z$ and $f(x, y) = \perp$ iff. $x = \perp$. We say a protocol Π as in Definition 3.1 evaluates f with ϵ -enhanced client correctness if it satisfies the same definition as ϵ -client correctness, with the following additional guarantee. For any (deterministic) server strategy S^* , there exists a distribution Y^* over Y such that for all x ,*

$$\Delta(\Pi_R(x, c \leftarrow \Pi_Q(x), S^*[c]), f(x, Y^*)) \leq \epsilon p_\perp$$

where $p_\perp = Pr_{Y^*}(\perp)$.⁸

The second notion is a relaxation of perfect client correctness.⁹

Definition 3.3. *Here we assume $\perp \in Y$. In the model with input-dependent client-security, we modify the ideal model to allow the simulator send a single value $y^* \in Y$ to the TP. It also gives the TP a predicate P such that the TP sends the client $f(x, y)$ if $P(x) = 0$, and $f(x, \perp)$ otherwise. We say a protocol Π as in Definition 3.1 evaluates f with perfect input-dependent security, if for any adversary, there exists a simulator with simulation error of 0.*

3.0.1 Restating security requirements geometrically.

We take a similar approach to that of [7] to representing (some of the) protocols' security requirements geometrically.

More specifically, for client correctness, we consider row distribution vectors achievable in the ideal model. That is, the region \tilde{P}_S denotes all achievable row distributions corresponding to possible ideal-world server strategies. This region simply corresponds to the convex hull of the rows of f 's truth table F .

To achieve security against a malicious server, we require that the region of real-world achievable row distributions P_S satisfies $P_S \subseteq \tilde{P}_S$. Properties 2,3 in the security definition are verified directly.

Geometric representation of client's output distributions. Fix a protocol $\Pi = (\Pi_Q, \Pi_R, \Pi_D)$ as in Definition 3.1 for evaluating a functionality $f : X \times Y \rightarrow Z$. For the sake of defining our output distributions we view the protocol as merely randomized mapping from $X \times Y$ to client outputs Z , and do not require it to securely evaluate f , or even correctly evaluate it if everyone behaves honestly.

⁷In particular, it first receives all inputs and only then returns all the outputs to the client. No rushing such as sending inputs to a certain OT instance after getting outputs from other OT instances is possible.

⁸This enhances the ϵ -client correctness requiring only a distance bound of ϵ , rather than ϵp_\perp .

⁹This is a relaxation as it allows for conditional abort. It also strengthens the definition in the sense that every deterministic server strategy induces a single effective input y , rather than a distribution.

Boolean functions. Fix $Z = \{0, 1\}$. For a given server's strategy $\Pi_D^*(x = y; r) = s^*$ for some fixed $s^* \in \{0, 1\}^{2^{|X|}}$, we consider the distributions of the client's output at the end of a protocol execution $\Pi^* = (\Pi_Q, \Pi_R, \Pi_D^*)$ (that is, a protocol resulting from Π when the server runs Π_D^* instead of Π_D). We denote this set of distributions by a vector $o \in \mathbb{R}^{|X|}$ indexed by $x \in [|X|]$. Here $o_x = p$ denotes the probability of the client outputting 1 on input x . That is,

$$o_x = \Pr_r[\Pi_Q(x; r) = c; \Pi_R(x, c, s^*[c]) = 1].$$

We refer to such a vector corresponding to some (possibly invalid) server's strategy s^* as a *geometric row distribution* for Π . We shall also consider geometric row distributions for the ideal model evaluating f , corresponding to server's input distributions $y \in Y$, referring to them as a row distribution for f . We omit Π, f whenever clear from the context.

Observe that the single number o_x uniquely encodes a distribution over the client's output set $\{0, 1\}$ on input x .¹¹ Similarly, we consider *geometric column distributions* for Π : for a given client's strategy $c^* \in \{0, 1\}^{|Y|}$ for its input to the OT oracle, we consider the corresponding *geometric column* distribution vector $o \in \{0, 1\}^{|Y|}$ indexed by $y \in [|Y|]$, where o_y is the probability of the client outputting 1 for server input y . That is:

$$o_y = \Pr_r[\Pi_R(x, c^*, \Pi_D(y; r)[c^*]) = 1].$$

General functions. Generalizing for larger $Z = \{0, 1, \dots, k-1\}$, a (geometric) row distribution $o \in \mathbb{R}^{(k-1)|X|}$, has entries labeled by pairs (x, i) where $x \in [|X|]$, $i \in Z \setminus \{0\}$, and $o_{(x,i)}$ denotes the probability of outputting i on input x . Thus, for every x, i we have $\sum_j o_{(x,j)} \leq 1$, and $o_{(x,i)} \geq 0$.¹² As in the case of $|Z| = 2$, this vector fully represents the client's output distribution for each input x . A similar extension can be made for (geometric) row distributions. For a given $x \in X$, let o_x denote the sub-vector $(o_{x,z})_{z \in [k-1]}$.

Truth tables. In the truth table F of f , we index rows by elements of Y and columns by elements of X . For $Z = \{0, 1\}$, the truth table representation we consider is just the standard one: a table where entry (y, x) equals $f(x, y)$. We use F_y to denote the row vector (X_x to denote the column) in F corresponding to y (x). We observe that each row F_y in this case is a geometric row distribution in the ideal model, where the server inputs y . We can interpret $F_{y,x}$ as $f(x, y) = p$, where p is the probability of outputting 1 (either $p = 0$ or $p = 1$).

Let us generalize this form to larger Z . We represent the truth table in "unary", where for each y, x we have $|Z| - 1$ columns $(x, z)_{z \in [|Z|-1]}$, and we set $F((x, z), y) = 1$ if $f(x, y) = z$, and $F((x, z), y) = 0$ otherwise (if $f(x, y) = 0$, all entries $F((x, z), y)$ will be 0).¹³ Again, each row F_y is a valid geometric row distribution in the ideal world (corresponding to a server input of y).

Definition 3.4 ([7]). *We say a function $f : X \times Y \rightarrow Z$ is full-dimensional if the affine dimension of the row set of its truth table F is the maximal possible - $(|Z| - 1)|X|$.*

Definition of security. As mentioned above, for client-server functionalities, the standard requirement of perfect stand-alone security in the 1-out-of-2-bit-OT^l-hybrid model can be restated as three separate requirements, all involving only the client's output distribution. For such functionalities and protocols Π as in Definition 3.1 the standard definition of perfect security against malicious parties is "almost" equivalent to the following definition. It would be fully equivalent if it required simulation of efficient (in k) adversaries is also efficient. Our protocols in fact satisfy the stronger definition, as we prove in the full version. We ignore efficiency issues altogether in this work for the sake of simplicity.

For simplicity, our security definition is stated without account for auxiliary information z that the adversary and simulator receive regarding the other party's input, required for sequential composition. It is easy to see that it in fact follows from our definition below.

In our security definition, security against malicious servers is stated in geometrical terms, which will be useful for use later.

¹⁰This notion naturally generalizes to randomized strategies, but we do not need this extent of generality here.

¹¹The vector o represents $|X|$ separate distributions, one for each client's input x . Nothing is implied about the correlation between client's outputs on different inputs for a given server's strategy s^* .

¹²The decision to exclude 0 is merely aesthetic, intended to remain consistent with standard binary truth tables.

¹³This is instead of having a single entry for each (x, y) with values in Z .

Definition 3.5 (Perfect security of protocols as in Definition 3.1). We say that a protocol Π as in Definition 3.1 for evaluating a client-server functionality $f : X \times Y \rightarrow Z$ as above is perfectly secure against a single malicious party if it satisfies:

1. *Client correctness:* For every server's strategy $s^* \in \{0,1\}^{2l}$, the corresponding row distribution o^* of f' is in $CH(\{F_y\}_{y \in Y})$, where the F_y 's are the rows of the truth table F of f .
2. *Server privacy:* For every client strategy c^* , there exists a simulator S such that for all y , $S(1^k)$ is distributed identically to $\Pi_D(y)$.
3. *Honest correctness:* Let $C_x = \text{support}(\Pi_Q(x))$, $S_y = \text{support}(\Pi_D(y))$. Then for all $c \in C_x$, $s \in S_y$, $\Pi_R(x, c, s[c]) = f(x, y)$.

Next we restate Definition 3.2 in geometrical terms.

Observation 1. Consider a protocol Π evaluating a function f as in Definition 3.2 with ϵ -enhanced client correctness. Then the following holds. For every server's strategy $s^* \in \{0,1\}^{2l}$, there exists an ideal world row distribution $o^* \in CH(\{F_y\}_{y \in Y})$ such that the real world row distribution o' corresponding to s^* satisfies

$$\Delta(o', o^*) \leq \epsilon(|Z| - 1)p_\perp$$

Here p_\perp is the coefficient of Y_\perp in o^* .¹⁴

4 A perfect protocol when F is full-dimensional

Due to the simple structure of 1-round protocols in the OT hybrid model, the first two security requirements are fully expressed as a single LP (linear program) [15, 16] specifying (Π_Q, Π_D, Π_R) . However, it is unclear how to incorporate the third requirement into the same program. Thus, we do not write an explicit LP searching for a specification of (Π_Q, Π_D, Π_R) . The resulting LP is not trivial to solve even for requirements 1,2 alone in 3.5. Instead, we take a similar road to that used in the fairness literature, which considers protocols with more general structure. We suggest a concrete protocol, and prove it is secure for a certain subclass of functions.

For every such function, we separately verify that each of conditions 1,2,3 in Definition 3.1. As in the fairness literature, we do use techniques related to solving LP's (analyzing the convex hull of a certain point set) only for proving condition 1 is satisfied by our protocol, but not for searching for a protocol.

Our starting point is a protocol as in Definition 3.1 (1-round protocol in the (1-out-of-2-bit-OT) ^{l} -hybrid model for some l) by [9][Section 3]. We denote this protocol by Π_{IKOPS} . It is stated for function with NC_0 circuits, but we restate it for general function (families), and bound its CC as a function of $|X|, |Y|, |Z|$ (which are assumed to be finite in our work).

The reason the protocol in [9] is restricted to NC_0 functionalities is for improving concrete efficiency, which is not a concern in our paper. Otherwise, their construction works for all functions, as summarized below.

Theorem 4.1. Let $f : X \times Y \rightarrow Z$ denote any (finite) client-server function. Then for all $\epsilon \geq 0$, Π_{IKOPS} evaluates f with ϵ -relaxed client correctness. Let h_i denote the smallest formula for evaluating the i 'th bit of $f(x, y)$, and let $h = \max_{i \leq \log(|Z|)} h_i$. Then, Π has communication complexity of $l = \log(|Z|)\tilde{O}(\log(|X|)(\log(\epsilon^{-1}) + h)^2) + \text{polylog}(\epsilon^{-1})$.

In a nutshell, in the $\Pi_{IKOPS11}$ protocol, reduces the evaluation of $f(x, y)$ to secure evaluation of a single instance of l parallel instances of OT 1-out-of-2 h -string-OT functionality for certain parameters h, l depending on f, ϵ . This is done using a decomposable randomized encodings of f [17]. Here we have $l = \log |X|$ - the input to i 'th OT instance is the bit x_i . The y is mapped to a string sequence $(s_{1,0}, s_{1,1}, \dots, s_{l,0}, s_{l,1})$ fed to the OT's in a certain manner.

Now, to securely evaluate the resulting functionality in the malicious setting, the OT is replaced by a COT (certified OT) functionality. The COT returns the client the output, and additionally reports whether the resulting string is consistent with some y and randomness r , as prescribed by reduction from $f(x, y)$ to the OT instances. Π_{COT} verifies that the OT input $s \in \{0,1\}^{2l}$ it feeds

¹⁴This is not exactly equivalent to enhanced ϵ -client correctness, as the parameters here are slightly worse, but this is all we need, and it simplifies the definition.

to the OT oracle is consistent with some y, r for the reduction. Along with s , the server feeds a representation of y, r as a witness that s is consistent. It gives client C_i the OT output along with a bit on whether it is consistent (with that witness y, r common for all indices) or not.

In the COT implementation, the server runs MPC in the head of an n' -party protocol Π for evaluating the (randomized) mapping from a pair (y, r) to a sequence s . More concretely, the protocol consists of a sender that privately sends n virtual servers its inputs y, r . There are also $2l$ clients who have no inputs, where client $C_{i,b}$ gets the output of the i 'th OT instance on input $x_i = b$. In Π , the virtual servers send messages to the clients in the last round of the protocol.

The COT client chooses the strings corresponding to the views seen by the virtual clients corresponding to its input x . Additionally, it asks for the entire view of each of the virtual servers with some small constant probability δ' . We observe that these so called *watchlists* (the client watches only a small fraction of the virtual server), along with the requests for client's views can be perfectly reduced in one round to 1-out-of-2-bit-OT oracles.

This MPC protocol Π is secure against malicious corruption of δn of the n parties. With high probability, the client will see $p/2n < \delta'n < \delta n$ of the views, catching cheating with high probability, but not learning anything besides $f(x, y)$. For a choice of δ' as above, the IKOPS protocol already happens to be statistically private against malicious clients.

There is however (small) non-zero probability of the client learning too much (in the worst case, $f(x, y)$ for all $x \in X$), by ending up watching too many of the virtual parties' view (potentially all of them).

Thus, Π_{IKOPS} is not perfectly server-private. In the following section, we slightly tweak Π_{IKOPS} , making watchlists deterministic, thereby making it perfectly server-private. In Section [?], using geometric techniques, we demonstrate how to make the protocol from Section 4.1 perfectly client correct. Here we critically rely on the fact that Π_{IKOPS} satisfies statistical enhanced client privacy, rather than just standard statistical client privacy.

4.1 Making Π_{IKOPS} perfectly server-private

4.1.1 Setting up deterministic watchlists

Recall the problem with client privacy was in the fact that the client may watch the internal state of too many servers, breaching security of the protocol Π , and thus of the entire construction. To solve this problem, we replace the probabilistic watchlist setup with a deterministic watchlist setup that allows the honest client to learn exactly $p_1 n$ of the views of its choice, while no client can learn more than $p_2 n$ of the values, where p_2 is not "much larger" than p_1 . We also allow the server to input \perp , in which case the client should output \perp . Formally let k_1, k_2, n, h where $n \geq k_2 > 2k_1$, and $h \geq 1$. We define $f_1 : k_1$ -out-of- n h -string-OT and $f_2 : k_2$ -out-of- n h -string-OT. We extend the f_i above into $f'_1 : X'_1 \times Y'_1 \rightarrow Z'_1, f'_2 : X'_2 \times Y_2 \rightarrow Z'_2$, so that $Z_i = Z_i \cup \{\perp\}, Y_i = Y_i \cup \{\perp\}$ so that $\forall x \in X_i, f_i(x, \perp) = \perp$.

Theorem 4.2 (a (k_1, k_2) -out-of- n h -string-OT protocol). *There exists a protocol Π as in Definition 3.1 for f'_1 with communication complexity l . Π satisfies:*

- Perfect honest correctness.
- Perfect client-correctness with input-dependent abort.
- Perfect server privacy relaxed to replace f'_1 with f'_2 (that is, malicious clients can be simulated by inputting additional, larger, sets beyond what is allowed by f_1).

Proof. We construct a protocol as required, we refer to as $\Pi_{\text{ramp-OT}}$.

Construction 1. *The parties perform n 1-out-of-2 nh -string-OT's in parallel (implemented via the 1-out-of-2-bit-OT ^{l} using parallel instances of Π_{int}).*

1. $\Pi_{\mathbf{D}}(\mathbf{y})$: *In the i 'th instance the sender samples n random strings $r_1, \dots, r_n \in \{0, 1\}^h$. Then, it secret-shares $r = (r_1, \dots, r_n)$ with a $(n - 2k_1)$ -out-of- n threshold using Shamir's secret sharing [18]. Let $s_1, \dots, s_n \in \{0, 1\}^{hn}$ denote the resulting shares. Output $s = (y_1 \oplus r_1, s_1, y_2, s_2, \dots, y_n \oplus r_n, s_n)$ (the y_i 's are padded accordingly).*
2. $\Pi_{\mathbf{Q}}(\mathbf{x} = \{\mathbf{x}_1, \dots, \mathbf{x}_{k_1}\})$: *Assume wlog. that all the x_i 's are distinct. Output $c = (c_1, \dots, c_n)$, where $c_i = 0$ iff. $i \in x = \{x_1, \dots, x_{k_1}\}$.*

3. $\Pi_{\mathbf{R}}(\mathbf{x}, \mathbf{c}, \mathbf{v} = (\mathbf{v}_1, \dots, \mathbf{v}_n))$: Here v_i is the string returned by the i 'th instance of Π_{int} . Let $w_i = \Pi_{int_R}(x, c_i, v_i)$ denote the output of the i 'th instance of Π_{int} . Use the w_i 's in $SR = [n] \setminus x$ to recover the secret vector r as follows:

- (a) If all subsets of size $n - 2k_1$ of SR agree on the same secret r , output $(w_i \oplus r_i)_{i \in x}$.
- (b) Otherwise, output \perp .

We now prove the protocol satisfies the required security guarantees. By construction, it is not hard to see that the protocol satisfies honest correctness. As for client correctness, we observe that for any server strategy r^* (input to OT oracle) there exists a value $y^* \in \{0, 1\}^{2nh}$ such that for every client's input x , either \perp or $y^*[x]$ is output (with probability 1), and the choice to abort or not depends on x . To see this, it suffices to observe the following

Observation 2. Fix some server strategy s . Then, for server strategy s , no two choices c_1, c_2 by the (honest) client yield corresponding reconstructed secret values $r_1 \neq r_2$ that are both non- \perp .

Assume the contrary, that for some server strategy $s = (s_{1,0}, s_{1,1}, \dots, s_{n,0}, s_{n,1})$ such c_1, c_2 exist. For any pair of sets SR_1, SR_2 of size k_1 , SR_1, SR_2 have at least $n - k_1 - k_1 = n - 2k_1$ coordinates in common. This set $B = SR_1 \cap SR_2$ can thus reconstruct the secret s . To lead to non- \perp output by Π_R , all reconstructing subsets of SR_1, SR_2 must agree with s (if not, the corresponding output is \perp).

Observation 3 implies that all sets SR leading to non- \perp values for some x lead to the reconstruction of the same value $r^* = s$ (if no such set exists, we fix r^* arbitrarily). Therefore, $y^* = (s_{1,0} \oplus r_1^*, \dots, s_{n,0} \oplus r_n^*)$ is as promised above. Now, clearly, for each x $y^*[x]$ or \perp is output (depending on the resulting SR_x). To see perfect server privacy holds, observe that if the client tries to learn a set S of at most k_2 of the 0-inputs, it can also reconstruct the secret mask r , and recover all values in S . It learns nothing about the other values, as it only learns one out of 2 'shares' in an additive sharing of these values (originating from r), this can be simulated by sending S in the ideal model. If it attempts to learn a set S of size $> k_2$, it learns nothing about r , as it does not have enough shares of it, so that it learns nothing about any of the server's inputs (its view consists of random field elements for the Shamir sharing, and random strings for each of the server inputs in S). Thus, its input can be simulated given any S (let us fix some S of size k_1) to be sent to the TP in the ideal model to simulate its view.

4.1.2 Upgrading Π_{IKOPS}

Let us recall and modify (a specific variant of) the original protocol Π_{IKOPS}^ϵ in more detail. In particular, we change the watchlists from picking each server with a certain probability p , to picking a random subset of size exactly pn .

Here we represent X, Y, Z as some $X = \{0, 1\}^{l_x}, Y = \{0, 1\}^{l_y}, Z = \{0, 1\}^{l_z}$.

Construction 2 ([9]). Fix f as above, and a security parameter $\epsilon > 0$. Then $\Pi_{IKOPS, f, \epsilon}^+$ is as follows.

1. Let $\kappa = O(\epsilon^{-1})$ for a suitable constant to be determined later. Let us encode input $x = (x_1, \dots, x_{l_x})$ via $Enc_I(x) = (x_{1,1}, \dots, x_{1,\kappa+1}, \dots, x_{l_x, \kappa+1})$, where each $x_{i,1}, \dots, x_{i,\kappa+1}$ is a random additive sharing of x_i . Let $h : X^{\kappa+1} \times Y \rightarrow Z$ be defined as $h(Enc_I(x), y) = f((\oplus_{i=1}^{\kappa+1} x_{1,i}, \dots, \oplus_{i=1}^{\kappa+1} x_{\kappa+1,i}), y)$.
2. Let (Enc_h, Dec_h) denote a decomposable PRE of a function $f'(x, y)$ related to f . For instance, we could separately encode each of the bits of $f(x, y)$ using the perfect formula-based encoding from [17]. The resulting encoding has monomials of degree at most 3, and degree 1 in x, y or combinations of the form $x_i y_j$, but for a fixed value of y , all these become degree-1 in x_i (with possibly r_j 's involved). Furthermore, each polynomial has a constant number of monomials, so it is easy to make the encoding (for any fixed y decomposable by introducing a constant overhead and more randomness r_s [1]). The complexity of this encoding is $(\kappa + |C|)^2$, where $|C|$ is the formula complexity of each bit of $f(x, y)$.
3. Consider a semi-honest protocol Π' for evaluating f where $c = Enc_I(x)$, and the server inputs s where $s_{i,b} = Enc_{h,i}(b, (y, r_s))$. The client then recovers $f(x, y)$ from $s[c] = s_{1,x_1}, \dots, s_{l_x, x_{l_x}}$ by applying Dec_h to $s[c]$. We denote $\alpha = (\kappa + 1)l_x$.

4. To evaluate the protocol Π' above, we reduce it to a COT (conditional OT) functionality, similar to that of [9]. The COT protocol receives (y, r) from the server, and evaluates the decomposable NC_0 encoding above to generate the $2l'_x$ purported output values $(v_{1,0}, v_{1,1}, \dots, v_{\alpha,0}, v_{\alpha,1}) = \text{Enc}_{h,1}(0, (y, r_s)), \dots, \text{Enc}_{h,\alpha}(1, (y, r_s))$. Each value is either the correct value $\text{Enc}_{h,i}(b, (y, r_s))$, or \perp in case the $v_{i,b}$ is not consistent with (y, r_s) . As in [9] the server performs MPC in the head of an MPC protocol Π_{HM} evaluating the COT functionality. The MPC participants are a sender with input (y, r_s) , 2α clients and some n virtual servers that perform the computation. The protocol proceeds by having the sender send messages to the virtual servers, the servers running Π_{HM} among themselves, and sending the corresponding outputs to the clients during a single round at the end, where each client receives a single message from the virtual servers, from which it recovers its output.

The protocol has the following security guarantees. It is perfectly correct against any adversary corrupting the sender and at most δn of the servers, and any number of the clients. Such protocols exist for all $\delta < 1/3$. Also, we will n to satisfy $2\lfloor \delta/3n \rfloor < \lfloor \delta n \rfloor$ (from now on we omit $\lfloor \cdot \rfloor$ for brevity). Let us fix $\delta = 1/4$, which imposes that $n > 12$.

If the sender is honest, Π_{HM} is perfectly private against semi-honest adversaries corrupting any subset of clients, and up to δn of the virtual servers. Consider [19] as such a protocol with CC linear in the size of the encoding circuit, which is an optimized variant of [19].

5. The server runs Π' on (y, r_s) in his head, generating the views V_1, \dots, V_n of the virtual servers, and the purported messages $V_{1,0}, V_{1,1}, \dots, V_{2\alpha,1}$ received by each of the 2α clients from all n virtual parties.

Recall that in [9], on input $x' = \text{Enc}(x)$, the parties run parallel instances of 1-out-of-2-bit-OT $_h$ (for the proper value of h), where in the first α instances, instance i inputs $V_{i,0}, V_{i,1}$ are used by the server. The other set of parallel OT's is dedicated to watchlists. The client picks $\delta/3n$ of the views V_1, \dots, V_n . This is done using the $(\delta/3n, \delta n)$ -out-of- n h -string-OT protocol in $\Pi_{\text{ramp-OT}}$.¹⁵

The client sends $c = (x_1, \dots, x_\alpha)$ as its queries for the first part, we refer to as the “keys” part, and picks a random subset S of size $\delta/3n$ of $[n]$ as its input set for the watchlist part $\Pi_{\text{ramp-OT}}$. Given the replies of both parts: if $\Pi_{\text{ramp-OT}}$ outputs \perp , output \perp as well. Otherwise, it reconstructs the set $\{V_{s \in S}\}_S$ of virtual server views. It checks whether all the recovered V_i 's are consistent among them (comparing messages sent and received among viewed parties, and that they are consistent with their inputs and randomness). The client outputs \perp if an inconsistency among the watched views of the V_i 's was discovered. Otherwise, it checks whether any of the messages in some V_{i,x_i} seen by the client are inconsistent with the values sent in the watched V_j 's. Otherwise, it reconstructs $f(x, y) = h(\text{Enc}(x), y)$ from $(V_{i,x_1}, \dots, V_{i,x_\alpha})$.

Lemma 4.3. Fix some $\epsilon > 0$, and $f : X \times Y \rightarrow Z$. Then $\Pi_{IKOPS,f,\epsilon}^+$ in Construction 2 is perfectly correct for honest parties, and is perfectly server-private. It also satisfies enhanced ϵ -client correctness. Let us denote the complexity of the resulting protocol by $\ell(\epsilon, |X|, |Y|)$.

Proof Sketch. It easy to see that the protocol remains correct in face of honest parties. To prove perfect server privacy, fix some client strategy c^* . The first part (virtual client views) of the protocol only discloses at most one V_{i,b_i} for every $i \in [\alpha]$, by perfect server privacy of Π_{int} . Let x^* denote the input corresponding to the b_i 's learned (set x_i^* arbitrarily).

We run the simulator guaranteed by $\Pi_{\text{ramp-OT}}$ of the malicious client strategy c_2^* induced by c^* on $\Pi_{\text{ramp-OT}}$. Consider the client's induced strategy in $\Pi_{\text{ramp-OT}}$. The simulator sends some distribution M^* over $\{m \subseteq [n] \mid |c| \leq \delta n\}$. For m^* in $\text{support}(M^*)$, by perfect server privacy of Π_{HM} , the client learns exactly what follows from $h(x^*, y)$, as it learns at most δn of the virtual server's views. Like [9], we also use the fact that any value $v \in \{0, 1\}^\alpha$ corresponds to $\text{Enc}_I(x)$ for some x , so client's view can be perfectly simulated given $\text{Dec}_I(x^*)$.

Enhanced ϵ -client correctness holds similarly to the original construction. On a high level, the only new case that we need to address here is when $\Pi_{\text{ramp-OT}}$ makes the client output \perp .

In more detail, the simulator of the server acts as follows given the server's strategy s^* .

¹⁵As discussed above, the watchlist implementation is where we diverge from [9], everything so far is unmodified.

1. It runs the simulator for $\Pi_{\text{ramp-OT}}$ on s_2^* , the part of the server's input corresponding to the watchlist part of the protocol.
2. It picks a random subset T of size $\delta/3n$ of $[n]$. Let u_2 denote the server's effective input guaranteed by $\text{Sim}_{\text{ramp-OT}}$ for client inputs T for which the output is non- \perp .
 - (a) If the output is \perp for all T , send \perp as an input to the TP (of our 2-party protocol evaluating f).
 - (b) Otherwise, let u_2 denote the extracted server's input guaranteed to exist by the security definition of $\Pi_{\text{ramp-OT}}$. Consider the consistency graph G' among the virtual servers induced by u_2 , where an edge (A, B) exists between a pair of virtual servers A, B iff. their views do not match. That is, some message received by B (A) does not match the message sent by A (B) as determined by A 's (B) randomness and initial message from the sender.
 - i. If the minimal VC L of the consistency graph G' is of size $t > \delta/3n$, send \perp to the TP.
 - ii. Otherwise, $t < \delta/3n$. Pick a subset T of size $\delta/3n$ among the virtual servers. If there is an edge of G' inside T , send \perp to the TP. Otherwise, let u_1 denote the sender's input extracted for the "keys" part of the protocol - executing the α parallel instances of Π_{int} . Complete the graph G' into a graph G with all virtual clients and virtual servers (but not the sender). Add edges between V' and $V \setminus V'$ between client $A = (i, b)$ and server B iff. $u_1[i, b]$ is not consistent with B 's message to A according to u_2 . Let B_1 denote the set of client nodes that have a neighbor in T . Let $g = |B_1|$. If $g \geq \kappa + 1$ or $x_{i,j,0}, x_{i,j,1} \in B_1$ for some i, j send \perp to the TP. Otherwise, send the TP \perp with probability 2^{-g} , and (y, r_s) otherwise (with probability $1 - 2^{-g}$). Here (y, r_s) is obtained by extracting (y, r_s) according to the views of the sender and L , as appearing in u_2 . In particular, the sender's messages are taken from all virtual server's first messages as appearing in u_2 . In particular, send \perp if $(y, r_s) = \perp$ is extracted. ¹⁶

It remains to prove that the simulator indeed satisfies the client correctness requirement. Consider several cases.

1. Assume the server's input s to the second part is such that the client outputs \perp for all inputs $x \subseteq [n]$ of size $\delta/3n$. Then the client in the real world outputs \perp with probability 1. This is also the case in the simulation, leading to $\epsilon = 0$ simulation error.
2. Otherwise, let u_2 denote the server's input extracted by the simulator of $\Pi_{\text{ramp-OT}}$. This value is identical to the effective input in the real worlds (in fact, it is a single value, not even a general distribution).
 - (a) If the inconsistency graph induced by u_2 is of size $t > \delta/3n$, then the smallest maximum matching in the graph is of size at least $t/2$. Thus, by a simple analysis using Chernoff bounds (see [] for details), the client picks a set T of parties covering some edge in G' with probability $2^{-\Theta(n)}$. Thus, with probability at least $1 - 2^{-\kappa}$, we the client outputs \perp . This probability may also rise due to an event of outputting \perp for a certain choice of T due to $\Pi_{\text{ramp-OT}}$ leading to an output of \perp for that value of T . The simulator outputs \perp with probability $b_\perp = 1$. Thus the security requirement is satisfied in this case for a proper choice of κ .
 - (b) Otherwise, for fix some choice of T by the client in the watchlist part. If \perp is output due to $\Pi_{\text{ramp-OT}}$'s execution, then this is also the case when the simulator chooses T . Otherwise, extract the server's effective input \perp to the "keys" part of the protocol - it is

¹⁶Here a note on simulator efficiency is in order. In this work we do not require efficient simulation. In particular, we compute exact minimal VC, rather than approximate VC, for the sake of simplicity. Similarly to [] we could have, had we strived for efficient simulation. The part of extracting (y, r_s) is also efficient if Π_{HM} 's simulator is efficient. To be precise, the simulator is expected to receive the code of TM's rather than concrete views. The simulator assumes that the sender deterministically sends messages as in *all* virtual server's views, and the virtual servers in B have next-message functions consistent with the views in u_2 , and arbitrary otherwise. As the protocol is Π_{HM} perfectly correct in face of an adversary corrupting $\{\text{sender}\} \cup B$, the correct distribution (y, r_s) is always extracted.

also identically distributed to the effective input of the server to the first part (in fact, by structure of Π_{int} , this is also a single value). Consider the set B_1 of nodes in $V \setminus V'$ with neighbors in T .

- i. If $g \geq \kappa + 1$, consider the maximal subset $B'_1 \subseteq B_1$ where for every $\forall i \in [l_x], j \in [\kappa + 1] \forall b \in \{0, 1\} x_{i,j,b} \notin B'_1$. By the structure of Enc_h , at least a $(1 - 2\kappa^{-1})$ -fraction of B_1 is in B'_1 . This holds as for each i , we either keep all of the nodes in B_1 , or remove at most 2 out of at least $\kappa + 1$. For all $x \in X$, the probability that $E_h(x)$ has some $x_{i,j}$ value so that node $x_{i,j,x_{i,j}}$ is in B'_1 is $1 - 2^{-|B'_1|} \geq 1 - 2^{-\kappa/2}$. In this case the client outputs \perp . The probability of outputting \perp conditioned on choosing T by the simulator is 1.
- ii. Otherwise, $g \leq \kappa$. In this case, for all x , $B'_1 = B_1$ (where B_1, B'_1 are defined as above). Therefore, for all x , the probability of outputting \perp due to hitting an edge in $V \setminus V' \cup T$ is the same as for the simulator conditioned on choosing T . If the event of hitting an edge does not occur, the output induced by u_2 is always consistent with (y, r_s) extracted by the simulator conditioned on picking \perp (in particular, it may or may not equal \perp).

To summarize, for every input x , the extracted distribution on server inputs induces an output distribution that is at distance at most $2^{-\kappa} p_\perp$ from the real output distribution. More concretely, the difference stems only from case 2.b.ii. \blacksquare

4.2 Transforming Π_{IKOPS+} into a perfectly correct protocol

In this section we describe the first step of the construction. Here we rely on ideas from convex geometry that are somewhat similar to those of [7]. In particular, the geometric interpretation of ϵ -enhanced client correctness and the following notion of full-dimensional functions is central to our construction.

Lemma 4.4. *Let $\epsilon > 0$, and let Π denote a protocol as in Definition 3.1 for evaluating f with ϵ -enhanced client security, perfect server privacy, and perfect honest correctness. Then there exists a perfectly secure protocol as in Definition 3.1 for evaluating f with communication complexity $\ell(\epsilon, |X|, |Y|)$, where ℓ is as in Theorem 4.3.*

As a corollary from Lemma 4.4 and Theorem 4.3, we obtain our main result.

Theorem 4.5. *Let $f : X \times Y \rightarrow Z$ denote a full-dimensional function, and $g = |X|(|Z| - 1)$. Then there exists a protocol Π' as in Definition 3.1 evaluating f with perfect security against a malicious adversary in the 1-out-of-2-bit- OT^l -hybrid model for $l = \ell(1/10(g - 1)g!, |X|, |Z|) = \tilde{O}(h^2, \text{poly}(|X|, |Z|))$, where ℓ is the function in Theorem 4.3.*

Here $\text{poly}(|X|, |Z|)$ is a global polynomial, independent of f .

Proof sketch. We pick a sufficiently small $\epsilon > 0$, to be set later, and consider $\Pi_{IKOPS+,f,\epsilon}^+$. Fix some vector v in the convex hull of F 's (not F' 's) rows F_y , which is “far enough from the edges” of that polygon. By “far enough” we mean that adding up to $\pm \epsilon p_\perp$ in every coordinate results in a point which is still inside the polygon. Our protocol Π' proceeds as follows. Whenever $\Pi_{IKOPS+,f,\epsilon}^+$ outputs \perp as an output on input x , output a distribution consistent with v_x . Otherwise, output the value output by Π . Indeed, as $\Pi_{IKOPS+,f,\epsilon}^+$ satisfies ϵ -enhanced client correctness, its output distribution is of the form.

$$o^+ = \sum_i \alpha_i o_i + e_r \quad (1)$$

Here $\alpha_i o_i$ is a convex combination of the rows Y'_i of F' . The vector e_r is an error vector, $|e_r|_\infty \leq \epsilon \alpha_\perp$, where α_\perp is the coefficient of Y_\perp .¹⁷

Now, as in Π , an output of \perp on input x is replaced by v_x , o^+ in Equation 3 is replaced by

$$\tilde{o} = \sum_{i \in Y} \alpha_i Y_i + \alpha_\perp (v_x + \tilde{e}_r) \quad (2)$$

¹⁷In fact, for every x , $|e_x|_1 \leq \epsilon$, but using this stronger property would not improve our result.

where $|e_r|_\infty \leq \epsilon$. It remains to show that $d = v_x + \tilde{e}_r$ is in $\text{CH}(\{Y_y\}_{y \in [|Y|-1]})$ for the right choice of v, ϵ . This is the case as if $d = \beta_i Y_i$ is a convex combination of F 's rows, we get that

$$\tilde{o} = \sum_{i \in Y} \alpha_i Y_i + \alpha_\perp (\beta_i Y_i) = \sum_{i \in Y} (\alpha_i + \alpha_\perp \beta_i) Y_i$$

Since $\alpha_1, \alpha_\perp, \dots, \alpha_{|Y|}$, and (separately) the β_i 's are coefficients of a convex combination, thus constituting a valid ideal-world row distribution for f .

It remains to prove that there is a way to pick v, ϵ so that the resulting \tilde{o} satisfies the client correctness requirement. Since f is full-rank, let us pick a set of size $g = |X|(|Z| - 1) + 1$ of rows of F , $V = \{Y_1, \dots, Y_g\}$, such that the dimension of $\{\Delta_{i-1} = Y_i - Y_1\}_{i \geq 2}$ is $g - 1$. We will pick v as a convex combination

$$\sum_{i \leq g} \alpha_i Y_i$$

of the Y_i 's, which we determine in the following. As F has 0-1 entries we have

Observation 3. *Each Δ_j is has entries in the set $\{0, 1, -1\}$.*

Let us pick

$$v = 3/4 Y_1 + \sum_{2 \leq i \leq g} 1/4 (g-1) Y_i$$

Now, we adapt ϵ to this choice based on the following observation.

Claim 4.6. *Let $u \in \mathbb{R}^{g-1}$ be a vector with $|u|_\infty \leq \epsilon$. Then, in the representation $u = \sum_{i \leq g-1} \alpha_i \Delta_i$ (it exists and is unique as the Δ_i 's form a basis of \mathbb{R}^{g-1}), it must be the case that $|\alpha_i| \leq \epsilon \cdot g!$.*

To prove the claim we apply Fact 1 to $M = (\Delta_1 || \Delta_2 || \dots || \Delta_{g-1})$, and use Observation 3 to bound each $|M_{i,j}^{-1}|$ as $|C_{i,j}| \leq (g-1)!/1 = (g-1)!$. Now, the solution to $Mx = u$ is $M^{-1}u$, thus we get $|x|_\infty \leq (g-1)(g-1)! \epsilon \leq g! \epsilon$, as required (here $g-1$ is the length of u).

We can rewrite a convex combination of the Y_i 's as

$$\sum_{i \leq g} \alpha_i Y_i = Y_1 + \sum_{i \leq g-1} \alpha_{i+1} \Delta_i \tag{3}$$

where the α_i 's on the right hand side are non-negative integers summing to at most 1 (and move back and forth between the two representations). In particular, we have

$$v = Y_1 + 1/4 (g-1) \sum_{i \leq g-1} \Delta_i$$

Recall also that the resulting row distribution is $o' = (1 - \epsilon)v + e'$, where $|e'|_\infty \leq \epsilon$. Thus, we have $e' = \sum_{i \leq g-1} \alpha_i \Delta_i$, where $|\alpha_i| \leq g! \epsilon$.

Thus, we have

$$o' = (1 - \epsilon)v + e' = Y_1 + (1 - \epsilon)1/4 \sum_{i \leq g-1} \Delta_i + (e' - \epsilon Y_1)$$

Let us write $w = e' - \epsilon Y_1$. Clearly, $|w|_\infty \leq 2\epsilon$. Here $|\beta_i| \leq 2\epsilon$ for each i . Thus, from Claim 4.6 we have

$$o' = Y_1 + \sum_{i \leq g-1} ((1 - \epsilon)1/4 (g-1) + \beta_i) \Delta_i$$

where $|\beta_i| \leq 2g! \epsilon$. Thus (since $g \geq 2$), picking $\epsilon = 1/10(g-1)(g!)$, we obtain o' of the form presented in Equation 3, which falls in the required region (the coefficients of the Δ_i 's are all non-negative and sum to at most 1).

More precisely, let $f(x, y) : [n] \times [m] \leftarrow \{0, 1\}$ denote a function where F^T is of full dimension. Consider the protocol from [7] for evaluating this function with fairness (page 13 in the eprint version). Here $\text{RandOut}_2(y)$ is such that $X_{\text{Real}} = c$ is in $\text{CH}(X_1, \dots, X_l)$, where the X_i 's are the rows of F^T .

References

- [1] Benny Chor and Eyal Kushilevitz. A zero-one law for boolean privacy (extended abstract). In David S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA*, pages 62–72. ACM, 1989.
- [2] Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In Juris Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 364–369. ACM, 1986.
- [3] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.
- [4] Joe Kilian. Founding cryptography on oblivious transfer. In Simon [20], pages 20–31.
- [5] S. Dov Gordon and Jonathan Katz. Partial fairness in secure two-party computation. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 157–176. Springer, 2010.
- [6] S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete fairness in secure two-party computation. *IACR Cryptology ePrint Archive*, 2008:303, 2008.
- [7] Gilad Asharov. Towards characterizing complete fairness in secure two-party computation. In Yehuda Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, volume 8349 of *Lecture Notes in Computer Science*, pages 291–316. Springer, 2014. eprint version at <https://eprint.iacr.org/2014/098>.
- [8] Gilad Asharov, Amos Beimel, Nikolaos Makriyannis, and Eran Omri. Complete characterization of fairness in secure two-party computation of boolean functions. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, volume 9014 of *Lecture Notes in Computer Science*, pages 199–228. Springer, 2015.
- [9] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. Efficient non-interactive secure computation. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 406–425. Springer, 2011.
- [10] Gilles Brassard, Claude Crépeau, and Miklos Santha. Oblivious transfers and intersecting codes. *IACR Cryptology ePrint Archive*, 1996:10, 1996.
- [11] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232. Springer, 2006.
- [12] Amos Beimel, Ariel Gabizon, Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, and Anat Paskin-Cherniavsky. Non-interactive secure multiparty computation. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II*, volume 8617 of *Lecture Notes in Computer Science*, pages 387–404. Springer, 2014.
- [13] Ran Canetti. Security and composition of multiparty cryptographic protocols. *J. Cryptology*, 13(1):143–202, 2000.

- [14] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 433–442. ACM, 2008.
- [15] L. V. Kantorovich. Mathematical methods of organizing and planning production. *Management Science*, 6(4):366–422, 1960.
- [16] George B. Dantzig. Inductive proof of the simplex method. *IBM Journal of Research and Development*, 4(5):505–506, 1960.
- [17] Yuval Ishai and Eyal Kushilevitz. Perfect constant-round secure computation via perfect randomizing polynomials. In Peter Widmayer, Francisco Triguero Ruiz, Rafael Morales Bueno, Matthew Hennessy, Stephan Eidenbenz, and Ricardo Conejo, editors, *Automata, Languages and Programming, 29th International Colloquium, ICALP 2002, Malaga, Spain, July 8-13, 2002, Proceedings*, volume 2380 of *Lecture Notes in Computer Science*, pages 244–256. Springer, 2002.
- [18] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
- [19] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In Simon [20], pages 1–10.
- [20] Janos Simon, editor. *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*. ACM, 1988.
- [21] Yehuda Lindell and Benny Pinkas. Secure two-party computation via cut-and-choose oblivious transfer. *J. Cryptology*, 25(4):680–722, 2012.

A Warmup - $Y = \{0, 1\}$

As a warmup, we observe that for all finite Z all client-server functions $f : X \times Y \rightarrow Z$ where $Y = \{0, 1\}$ have a perfectly secure protocol in the OT hybrid model. In turn, this is a special case of a folklore construction for f 's where F has a column x_0 that *dominates* all other columns (recall that a column x dominates a column x' if for all $y \in Y$ $F(x, y) = F(x', y)$ implies that $F(x', y) = F(x, y)$). The protocol in fact does not use OT oracle, and is secure in the plain model.¹⁸

This trivial (set of) examples is the only type of functions we know of that is not fully covered by our main construction 4.5.

Theorem A.1. *Let $f : X \times Y \rightarrow Z$ be a client server functionality where F has a column x_0 that dominates all other columns. Then there exists a 1-round perfectly secure protocol for f in the plain model.*

Proof Sketch. Consider the following protocol. If all columns in F are constant, the client just outputs $f(x_0, y_1)$ where $y_1 \in Y$ is fixed arbitrarily without any communication. Otherwise, the server simply sends $o = f(x_0, y)$ to the client. The client recovers $f(x, y)$ from o : as column F^{x_0} dominates column F^x , $f(x, y)$ is uniquely determined by o .

The construction is private against malicious clients, as the client's view can be simulated by sending x_0 to the trusted party, where x_0 is an entry such that column x_0 in F has two distinct entries.

A malicious server's behavior can also be simulated, as it sends a message distributed over $\{f(x_0, y)\}_{y \in Y}$ according to some distribution (anything outside Y is interpreted as some default value). ■

Corollary A.2. *Let $f : X \times Y \rightarrow Z$ be a client server functionality where $Y = \{0, 1\}$. Then there exists a 1-round perfectly secure protocol in the plain model.*

¹⁸The protocol is 1-round, and in particular can be replaced by one as in Definition 3.1, since sending a message in $|Z|$ over a channel can be implemented via a call to 1-out-of-2-bit-OT $\log |Z|$ where the message to be sent is placed in both positions.

B Applications

As discussed in the intro, our protocol allows evaluating functions whose truth table are full-dimensional with computational (and communication) complexity which is independent of the security parameter to achieve 0 simulation error. For domains that the not very large, this may help achieving concretely efficient protocols. The focus of our work is mostly theoretical, so we did not try to optimize the concrete parameters, but it paves a way for designing protocols which may be competitive in efficiency (say, in CC) with the state of the art statistically or computationally secure protocols.

Observe that a large fraction of functions $f : X \times Y \rightarrow Z$ with $|Y| > |X|$ satisfy the requirements of Theorem 4.5. More concretely, analysis of row-rank of random functions with domains $|X|, |Y|, |Z|$ this fraction behaves as $1 - \exp(-(|Y| - |X|)(|Z| - 1))$ (see discussion in [7] for more details). For instance, at least $1 - 1.6 \cdot 10^{-6}$ of the functions with $|Y| = 31, |X| = 30, |Z| = 2$ can be computed with perfect security in the OT-hybrid model!

C Future work

In this work we initiate a systematic study of perfect security in the OT hybrid model. More concretely, we have focused on client-server functionalities. Although we have made some progress, many interesting questions remain wide open.

Client-server functionalities. A natural open question is to fully characterize the set of client-server functionalities that can be evaluated. One concrete question that is interesting to resolve is that of k -out-of- n -bit-OT for any $k \neq 1, n$. A perfect protocol for 2-out-of-3-bit-OT this functionality would be particularly useful for improving concrete efficiency of 2PC protocols - via constructing improved cut and choose OT [21]. Observe that k -out-of- n -bit-OT implies k -out-of- n' -bit-OT for all $n' \leq n$ (in our model). This holds via a simple perfect reduction from the latter to the former, where the sender pads its n inputs to n' , and the client only picks subsets of the first n bits.

A concrete approach. Trivially, if a 2PC functionality has a perfectly secure protocol in the OT hybrid model it is also securely computable with fairness. The other direction is not true. As follows from the $\omega_k(1)$ bound in [6] for symmetric functions with an embedded XOR, and the construction of [7] for all full dimensional functions (some of which have an embedded XOR), fairness does not imply perfect security.

The work of [7] puts forward a class of symmetric functions that have protocols which are statistically secure with fairness, for which our protocols do not work. The condition characterizing the functions that can be handled by his protocol is identical to ours.

Theorem C.1 (Informal [7]). *Every symmetric function $f(x, y)$ such that the truth table F of $f(x, y)$ is full-dimensional (when considering the set of rows of the matrix representing F), can be evaluated with full security.*

This is precisely the condition we impose, where the columns of F are labeled by X , and the rows are labeled by Y . However, if F^T rather than f is of full dimension, since f is symmetric, reversing the roles of the row player and the column player allows to securely compute $f'(y, x) = f(x, y)$, and thus compute $f(x, y)$. For client-server functionalities, this transpose is not possible, as the roles of the parties in the protocol are not symmetric.

This is interesting, since client-server functionalities are particularly easy to implement with (statistical) fairness, while symmetric functionalities are less so. However, even symmetric functionalities that are computable with full statistical security may not be computable with perfect security even in their client-server variant.

This provides guidance for candidate client-server functionalities with no perfect protocols to look at first.

Question 1.1 Consider $f(x, y)$ for which F is not full dimensional, but F^T is. Such functions have a protocol with full statistical security in the OT-hybrid model [7], but are not covered by our construction. Do all these function have a perfect protocol in the OT hybrid model?

Another interesting open question on perfect security refers to round complexity.

The round complexity of perfect 2PC. *Question 2. For (inefficient) statistical security it follows from the fairness literature that increasing round complexity helps to evaluate more functions (some examples for efficient 2PC are also known: combining [7, 6] to obtain certain functions with embedded xor). Does increasing round complexity beyond 1 allow to perfectly evaluate more functions? This relates to both client-server and other types of 2PC functionalities.*

Roughly, increasing round complexity in the fully secure statistical setting allows to decrease the simulation error of that protocol, by making it harder for a malicious party to guess what is the “right” time to abort. It is not apriori clear throughout which mechanism, if any, this could be useful for obtaining protocols with perfect full security.

A concrete approach One approach towards constructing multi-round protocols for possibly new functionalities, is modifying [7]’s GHKL-style protocols for general (possibly asymmetric) functions.

Here full dimension properties of f alone will not generally suffice, as for (symmetric) functionalities with an embedded xor every protocol with error $neg(k)$ requires $\omega_k(1)$ rounds [6] so perfect security is in fact impossible. Thus new techniques will be required if we are to find functionalities which can be perfectly computed, but in multiple rounds.

Security with abort. Although this notion is equivalent for client-server functionalities, it is natural to ask whether the full perfect security notion and perfect security with abort in the OT-hybrid model are equivalent for 2PC functionalities.

As we know, this is not the case for efficient statistical 2PC in the OT-hybrid model. It is also known that even perfect security with abort is not possible for certain 2PC functionalities.

Can we separate the two notions in the 2PC setting? As a first step, it would be interesting to understand whether client-server functionalities can be handled with security with abort (even before understanding the status of this class for perfect full security).