Exploring the Limits of Common Coins Using Frontier Analysis of Protocols

Hemanta K. Maji[1,⋆], Pichayoot Ouppaphan[1,⋆⋆], Manoj Prabhakaran[1,⋆], and Mike Rosulek[2]

[1] Department of Computer Science, University of Illinois, Urbana-Champaign. {hmaji2,pouppap2,mmp}@uiuc.edu.
[2] Department of Computer Science, University of Montana. mikero@cs.umt.edu.

Abstract. In 2-party secure computation, access to common, trusted randomness is a fundamental primitive. It is widely employed in the setting of computationally bounded players (under various complexity assumptions) to great advantage. In this work we seek to understand the power of trusted randomness, primarily in the computationally unbounded (or information theoretic) setting. We show that a source of common randomness does not add any additional power for secure evaluation of deterministic functions, even when one of the parties has arbitrary influence over the distribution of the common randomness. Further, common randomness helps only in a trivial sense for realizing randomized functions too (namely, it only allows for sampling from publicly fixed distributions), if UC security is required.

To obtain these impossibility results, we employ a recently developed protocol analysis technique, which we call the *frontier analysis*. This involves analyzing carefully defined "frontiers" in a weighted tree induced by the protocol's execution (or executions, with various inputs), and establishing various properties regarding one or more such frontiers. We demonstrate the versatility of this technique by employing carefully chosen frontiers to derive the different results. To analyze randomized functionalities we introduce a frontier argument that involves a geometric analysis of the space of probability distributions.

Finally, we relate our results to computational intractability questions. We give an equivalent formulation of the "cryptomania assumption" (that there is a semi-honest or standalone secure oblivious transfer protocol) in terms of UC-secure reduction among randomized functionalities. Also, we provide an *unconditional result* on the uselessness of common randomness, even in the computationally bounded setting.

Our results make significant progress towards understanding the exact power of shared randomness in cryptography. To the best of our knowledge, our results are the first to comprehensively characterize the power of large classes of randomized functionalities.

⋆ Partially supported by NSF grants CNS 07-47027 and CNS 07-16626.
⋆⋆ Supported by NSF grant CNS 0851957 for undergraduate research.

1 Introduction

In this work, we consider a fundamental question: *How cryptographically useful is a trusted source of public coins?*

While there are several instances in cryptography where a common random string or a trusted source of public coins is very useful (e.g. [3,5]), we show severe limitations to its usefulness[3] in secure two-party computation, without — and sometimes even with — computational intractability assumptions. In contrast, it is well known that more general correlated private random variables can be extremely powerful [2]. Given that for semi-honest security common randomness is useless (as one of the parties could sample and broadcast it), it is not surprising that it should turn out to be not as powerful as general correlated random variables. However, despite its fundamental nature, the exact power of common randomness has not yet been characterized. Here, we provide tight characterizations of what can be achieved with a source of common randomness, in various settings of 2-party computation. We show:

- For two-party secure function evaluation (SFE) of *deterministic* functions, being given a source of common randomness is useless, irrespective of any computational complexity assumptions, when considering security in the standalone setting.[4]
- Clearly a source of common randomness can be useful for realizing *randomized* functionalities. However, in the case of UC security, we show that a source of common coins can be useful only in a trivial sense (unless restricted to the computationally bounded setting, and intractability assumptions are employed). We show that any UC-secure protocol that uses common coins for evaluating a randomized function can be replaced by a protocol of the following simple form: one of the parties announces a probability distribution, based deterministically on its input, and then the two parties sample an outcome from this distribution using freshly sampled common coins. We call the resulting functionality a *publicly-selectable source.*
- We relate computational intractability assumptions to secure reductions among randomized functionalities, giving evidence that common randomness is useful only under strong computational assumptions. In particular we show that common randomness can be used to UC-securely realize a symmetric functionality with bi-directional influence (i.e., the output is influenced by both the parties' inputs) if and only if there exists a semi-honest secure protocol for oblivious transfer.

These results are actually proven for a class of sources more general than coin tossing, namely *selectable sources* – that let one of the parties (secretly) specify

[3] We say that a source of common randomness is useless in realizing some 2-party functionality $\mathcal{F}$ if either $\mathcal{F}$ could be realized without using the given source or $\mathcal{F}$ cannot be realized even given the source. Note that we consider only the feasibility question and not any efficiency issues.

[4] In the case of UC security, it follows from the results in [17] that a source of common randomness is useless except in Cryptomania, where it is a complete functionality.

which among a set of distributions should be used by the source. We highlight two aspects of these results:

Non-blackbox analysis of protocols. In deriving the impossibility results our analysis crucially relies on the communication and information structure of protocols. We build on the "frontier analysis" paradigm in [8,16,17], but significantly extend its power, among other things, to enable analyzing protocols for arbitrary randomized functionalities, and protocols using randomized functionalities.

These results (and hence proofs) are necessarily of a *non-relativizing* nature — if the protocol has access to another trusted functionality (more sophisticated than common randomness), the impossibility results no longer hold. Specifics about the common randomness functionality are (and must be) used in our proofs. Such low-level analysis of protocols, we believe, is crucial to understanding the power and complexity of multi-party computation primitives.

Understanding randomized functionalities. Secure evaluation of *randomized* functions has in general been a poorly understood area. In particular, to date it remains open to characterize which randomized functions can be securely realized even against computationally unbounded passive (honest-but-curious) adversaries — a problem that was solved for deterministic functions twenty years ago [1,14]. Much of the study of randomized functionalities has been focused on in-depth understanding of the simplest such functionality — namely generating shared fair coins (e.g., see [7,11,8,19] and references therein). Our results provide significant insight into *other* randomized functionalities as well, and their connections to computational intractability assumptions. In particular, our results involve two interesting classes of randomized functionalities, namely *selectable sources* and *publicly-selectable sources*.

1.1 Overview

Frontier analysis. The bulk of our results take the form of statements of cryptographic impossibility. That is, we show that a protocol for a given cryptographic task is impossible (or else implies a certain computational primitive like one-way functions). Such impossibility results have been a core challenge in cryptography. In this work, we present a powerful battery of techniques that we use to analyze 2-party protocols, which we broadly call "frontier analysis."

The basic outline of a frontier analysis is as follows. We first interpret a protocol as a tree of possible transcripts, with weights corresponding to the probability that the protocol assigns to each message, based on the parties' inputs. Within this tree, we identify "frontiers", which are simply a collection of nodes (partial transcripts) that form a cut and an independent set. Intuitively, these frontiers correspond to points in the protocol when some condition is satisfied for the first time, where the condition in question depends on the kind of analysis needed: for example, the first place the transcript leaks "significant" information about a party's input, or the first place that common coins have made a "significant" influence on the protocol's output.

Impossibility proofs using frontier analysis proceed by showing that frontiers of certain kind exist, often showing that multiple frontiers must be encountered in a specific order, and then showing that an adversary can effect an attack by exploiting the properties of these frontiers. Appendix A contains a high level discussion on frontier analysis as a tool for protocol analysis.

Common coins are not useful in SFE protocols. We show that against computationally unbounded adversaries (more precisely, against adversaries that can break one-way functions), any 2-party deterministic SFE (in which both parties receive the same output) functionality that can be securely realized given a trusted coin-tossing functionality can in fact be securely realized without it. This is most interesting for the standalone setting, because if one-way functions do exist then a standalone-secure coin-tossing protocols exist, so again access to a trusted coin-tossing functionality is redundant.[5]

We start off by showing that there is no secure protocol for evaluating boolean XOR given a coin-tossing functionality. In many ways these functionalities have similar "complexity" (in particular, neither is complete, and both are trivial to realize against passive adversaries), so establishing a qualitative separation between them is interesting in itself. In a protocol for XOR, either party may be the first to reveal information about their input, and the two parties can even gradually reveal more and more information about their input in an interleaved fashion. We define a frontier corresponding to the first point at which some party has revealed "significant" information about its input. Then we define an attack that can be carried out when the protocol crosses this frontier. Since a large class of SFE functionalities can be used to securely realize XOR, the impossibility extends to these functionalities as well.

We then use the combinatorial characterizations of Symmetric Secure Function Evaluation (SSFE) functionalities (obtained using frontier analysis) from [16] to extend the result to arbitrary SSFE functionalities (instead of just XOR). Further, using an extension of a result in [12], we extend this to arbitrary SFE functionalities by associating a symmetric SFE with every general SFE that has a secure protocol using a source of common randomness.

For randomized SFE, common coins help only in a trivial sense. We show that common coins are useful in constructing UC-secure protocols for randomized SFE functionalities only for the class of publicly-selectable sources (Theorem 2). For this result, we exploit the versatility of the frontier analysis and also employ a geometric analysis of the space of effective probability distributions.

The frontier analysis is carried out for an SSFE functionality, and then the result is extended to general SFE functionality separately. For a randomized

[5] A recent result in [17] gives a sharp result for the case of UC security: the coin-tossing functionality is useful in realizing further deterministic SFE functionalities if and only if there exists a semi-honest oblivious transfer protocol. However neither the result nor the approach in [17] extends to the standalone setting. Also, our result is applicable to not just symmetric functionalities and coin-tossing, but extends to general SFE functionalities and all selectable sources.

SSFE functionality, for each pair of inputs, the output is specified by a distribution (over a finite output alphabet). This distribution can be represented as a vector in d-dimensional real space where d is the size of the output alphabet. By considering all possible inputs, we obtain a set of points in this space as legitimate output distributions. But since the parties can choose their input according to any distribution they wish, the entire convex hull of these points is the set of legitimate output distributions. Note that the vertices of this polytope correspond to the output distributions for various specific input choices.

In analyzing a protocol for such a functionality, we define *two* very different frontiers: one intuitively captures the last point in the protocol where the parties' inputs have any noticeable influence over the output distribution. The other intuitively captures the first point where the common coins have had a non-trivial influence on the output distribution.

Defining these frontiers is a delicate task, but once they are defined, we can show that, for the protocol to be UC-secure, the two frontiers must be encountered in the order listed above. Thus there is always a point within the protocol where the parties' inputs have stopped influencing the output, yet the public coins have not yet started influencing the output in a non-trivial way. At this point, we can show that the output distribution is uniquely determined, and that the subsequent coins are simply used to sample from this publicly-chosen distribution.

Then, on each node in the first frontier the conditional output distribution is still within the polytope. On the other hand, since the input influence has ceased at this point, for any fixed input, its output distribution must be determined by this frontier: i.e., it must be a convex combination of the conditional output distributions at the nodes on the frontier. That is, the output distribution for this input is a convex combination of conditional output distributions which are all themselves within the polytope. Now, (without loss of generality, as it turns out) we can consider inputs whose output distributions are vertices of the polytope. Then, *for all nodes in the frontier* the conditional output distribution must coincide with the final distribution itself. Thus on reaching this frontier in the protocol, the output distribution is revealed (as a deterministic function of the inputs) and the rest of the protocol simply samples from this distribution.

Finally, we extend this result also to general SFE (instead of just symmetric SFE) functionalities, in the same way as for deterministic functionalities.

Selectable sources. Selectable sources are an interesting class of randomized functionalities with an intermediate level of complexity: they can be more complex than a (fixed) source of common randomness, yet they are simple enough that we can show that they are as useless as common randomness when it comes to securely realizing deterministic functionalities. The extension is observed by following the analysis for the case of the source of common randomness, and identifying the properties that it relies on. We do not know at this point whether these are exactly all the functionalities which are useless for realizing SFE functionalities, but based on our understanding so far, we conjecture that they are.

Connections to Computational Intractability. Finally, we relate our results to computational intractability questions. The attacks based on frontier analysis can often be extended to the computationally bounded setting, if one-way functions do not exist (as was pointed out in [17]). We show that this is indeed the case for our attacks. In fact, our first application of such an extension is to obtain an *unconditional* result about the uselessness of selectable sources in realizing deterministic secure function evaluation with standalone security. For this we use the fact that if one-way functions do not exist we can attack any given protocol, whereas if one-way functions do exist then we can realize any selectable source functionality (with standalone security) and then again they are useless.

We also generalize a result in [17] to the setting of randomized functionalities. There it was shown that if any non-trivial deterministic functionality is UC-securely realizable using access to common randomness, then there exists an oblivious transfer protocol secure against semi-honest adversaries. We generalize common randomness to any selectable source, and also generalize non-trivial deterministic functionalities to randomized SSFE functionalities with both parties' inputs having an influence on the output.

Related Results. Frontier analysis is possibly implicit in previous works on proving impossibility or lower bounds for protocols. For instance, the analysis in [8] very well fits our notion of what frontier analysis is. The analysis of protocols in [6,1,14] also have some elements of a frontier analysis, but of a rudimentary form which was sufficient for analysis of perfect security. In [16] frontier analysis was explicitly introduced and used to prove several protocol impossibility results and characterizations. [13] also presented similar results and used somewhat similar techniques (but relied on analyzing the protocol by rounds, instead of frontiers, and suffered limitations on the round complexity of the protocols for which the impossibility could be shown).

2 Preliminaries

We say that a function $\nu : \mathbb{N} \to \mathbb{R}$ is *negligible* if for every polynomial p, $\nu(k) < 1/p(k)$ for sufficiently large k. If $\mathcal{D}, \mathcal{D}'$ are discrete probability distributions with support S, we write $\mathrm{SD}(\mathcal{D}, \mathcal{D}')$ to denote the statistical distance of the distributions, defined as $\mathrm{SD}(\mathcal{D}, \mathcal{D}') = \frac{1}{2} \sum_{s \in S} |\mathcal{D}(s) - \mathcal{D}'(s)|$.

Security. We use standard conventions and terminology for the security of protocols for multi-party computation tasks. A protocol is secure if for every adversary in the real world (in which parties execute a protocol), there is an adversary, or *simulator*, in the ideal world (in which the task is carried out on behalf of the parties by a trusted third party called a *functionality*) that achieves the same effect. A *semi-honest* or *passive* adversary is one which is not allowed to deviate from the protocol. *Standalone* security is achieved if the simulator is allowed to rewind the adversary; *Universally composable (UC)* security [4] is achieved if the simulation is straight-line (i.e., never rewinds the adversary). In this work,

we exclusively consider *static* adversaries, who do not adaptively corrupt honest parties during the execution of a protocol.

The *plain model* is a real world in which protocols only have access to a simple communication channel; a *hybrid model* is a real world in which protocols can additionally use a particular trusted functionality. While hybrid worlds are usually considered only for UC security, we also use the terminology in the setting of standalone security. We note that protocols for *non-reactive* functionalities (i.e., those which receive input from all parties, then give output, and then stop responding) do securely compose even in the standalone security setting.

2.1 Functionalities

We focus on classifying several important subclasses of functionalities.

Secure function evaluation (SFE). A 2-party secure function evaluation (SFE) functionality is specified by two functions $f_1 : X \times Y \to Z$ and $f_2 : X \times Y \to Z$, where X and Y are finite sets. The functionality waits for input $x \in X$ from Alice and $y \in Y$ from Bob, then delivers $f_1(x, y)$ and $f_2(x, y)$ to them, respectively. There is no fairness guarantee: if a party is corrupt, it can obtain its own output first and decide whether the output should be delivered to the other party.

If $f_1 = f_2$ are identical we call it a *symmetric* SFE (or SSFE) functionality. SSFE functionalities are the most fundamental, and have been studied since Yao first introduced the concept of multi-party computation [21]. We can specify an SSFE function by simply giving its function table, where the rows correspond to an input of Alice, and columns correspond to an input of Bob. For instance, the XOR functionality has function table $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$.

Randomized functionalities. A randomized SFE functionality is specified by functions $f_1, f_2 : X \times Y \times R \to Z$. The functionality takes inputs $x \in X$ from Alice, $y \in Y$ from Bob, uniformly samples $r \in R$ and outputs $f_1(x, y, r)$ and $f_2(x, y, r)$ to Alice and Bob, respectively. An important example is the common randomness functionality, denoted by $\mathcal{F}_{\mathsf{coin}}$ (with $X = Y = \{0\}$, $R = \{0, 1\}$, and $f_1(x, y, r) = f_2(x, y, r) = r$). Note that for a given pair of inputs, the outputs to Alice and Bob could be correlated as the same value r is used in both.

We identify two important subclasses of randomized SSFE functionalities:

Selectable sources: One in which one party's input does not affect the output. That is, functions which can be written as $f(x, y, r) = h(x, r)$ for some function h. Note that for different values of x, the function's output distribution may be arbitrary.

Publicly-selectable sources: Those functions which can be written as $f(x, y, r) = (g(x), h(g(x), r))$, for some functions g and h. In this case, the function's output distribution for different values of x must be either identical (when $g(x) = g(x')$) or have disjoint supports (when $g(x) \neq g(x')$, which is included in the function's output). Intuitively, the function's output determines the identity of the random distribution $h(g(x), \cdot)$ that was used.

In these two classes of functionalities, only one party can influence the output, so we say they have *uni-directional influence*. If there exists inputs x, x', x'' for Alice and y, y', y'' for Bob so that $f(x, y') \not\equiv f(x, y'')$, and $f(x', y) \not\equiv f(x'', y)$, then both parties can potentially influence the output, and we say that the functionality has *bi-directional influence*.

Isomorphism. $\mathcal{F}$ and $\mathcal{G}$ are isomorphic[6] if either functionality can be UC-securely realized using the other functionality by a protocol that is "local" in the following sense: to realize $\mathcal{F}$ given $\mathcal{G}$ (say), each party maps its input (possibly probabilistically) to inputs for the functionality $\mathcal{G}$, calls $\mathcal{G}$ once with that input and, based on their private input, the output obtained from $\mathcal{G}$, and possibly private random coins, locally computes the final output, without any other communication. It is easy to see that isomorphism is an equivalence relation.

Usefulness of a source. We say that a source of common randomness $\mathcal{G}$ is **useless** in realizing a 2-party functionality $\mathcal{F}$ if either $\mathcal{F}$ could be securely realized in the plain model (i.e., without using $\mathcal{G}$) or $\mathcal{F}$ cannot be securely realized even in the $\mathcal{G}$-hybrid model. Note that we consider only the feasibility question and not any efficiency issues.

2.2 Frontier Analysis

Protocols and transcript trees. We view a 2-party protocol as a weighted tree of possible transcripts. The leaves of the tree correspond to completed transcripts, on which both parties give output. The tree's internal nodes alternate between "Alice" and "Bob" nodes, corresponding to points in the protocol (identified by partial transcripts) at which Alice and Bob send messages, respectively. Given a party's private input and the transcript so far (i.e., a node in the tree), the protocol assigns probabilities to the outgoing edges (i.e., possible next messages). In some settings we also consider nodes corresponding to invocations of ideal functionalities (like $\mathcal{F}_{\mathsf{coin}}$), when appropriate. For these the protocol tree assigns probabilities to the outputs of the functionality (the corresponding "messages" included in the transcripts for these steps) according to the probabilities of parties' inputs and the functionality's internal randomness. An execution of the protocol corresponds to a traversal from root to leaf in the tree.

Probabilities and frontiers. We write $\Pr[v|x, y]$ for the probability that the protocol visits node v (equivalently, generates a transcript with v as a prefix) when executed honestly on inputs x and y. Suppose $\pi_A(x, vb)$ is the probability that when Alice executes the protocol honestly with input x and the transcript so far is v, her next message is b. Similarly, we define a probability π_B for Bob. Then (assuming Alice speaks first in the protocol):

$$\Pr[v|x, y] = \pi_A(x, v_1)\pi_B(y, v_1v_2)\cdots = \left[\prod_{i \text{ odd}} \pi_A(x, v_1 \cdots v_i)\right]\left[\prod_{i \text{ even}} \pi_B(y, v_1 \cdots v_i)\right]$$

[6] The definition given here is a generalization for randomized functionalities of the definition from [16].

If we define $\alpha(v, x)$ and $\beta(v, y)$ to be the two parenthesized quantities (equivalently, the product of weights from Alice nodes and Bob nodes in the transcript tree, respectively), then we have $\Pr[v|x, y] = \alpha(v, x)\beta(v, y)$. Thus, in a plain protocol, the two parties make independent contributions to the probability of each transcript. In fact, even if the protocol is allowed to use a selectable source, this property still holds (see Section 4). This property of protocols is crucially used in all frontier analysis in this work.

When S is a set of independent nodes in the transcript tree (prefix-free partial transcripts), we define $\Pr[S|x, y] = \sum_{v \in S} \Pr[v|x, y]$, as all the probabilities in the summation are for mutually exclusive events. If $\Pr[F|x, y] = 1$, then we call F a *frontier.* Equivalently, a frontier is a maximal independent set in the transcript tree. In general, a frontier represents a point in the protocol where a certain event happens, usually defined in terms of the probabilities α and β.

3 Handling General SFE Functionalities

Frontier analysis is most naturally applied to protocols realizing SSFE functionalities — that is, functionalities which give the same output to both parties. So we derive our results for such functionalities. However, we can then extend our characterizations to apply to SFE functionalities with unrestricted outputs using the following lemma, proven in Appendix F:

Lemma 1. *Suppose $\mathcal{H}$ is a functionality that has a passive-secure protocol in the plain model. If $\mathcal{H}$ is useful in UC- or standalone-securely realizing a (possibly randomized) SFE functionality $\mathcal{F}$, then there exists a* **symmetric** *SFE functionality $\mathcal{F}^*$ such that $\mathcal{F}^*$ is isomorphic to $\mathcal{F}$, and $\mathcal{H}$ is useful in (respectively, UC- or standalone-) securely realizing $\mathcal{F}^*$.*

Here, being useful or not is in the sense of the definition given in Section 2.1.

Proving Lemma 1 essentially involves relating SSFE and SFE functionalities. As it turns out, relating symmetric and unrestricted functionalities is most convenient in the setting of passive security. In that setting, we associate with every SFE functionality $\mathcal{F}$ a symmetric functionality which is simply the maximal "common information" provided to the two parties by $\mathcal{F}$. (See proof of Lemma 11 for a combinatorial description of this function.) Following [12] it is not hard to show that if an SFE functionality $\mathcal{G}$ is not isomorphic to its (symmetric-output) common information functionality then $\mathcal{G}$ must be complete in the passive security setting.

To apply this result, however, we must be careful in relating passive security and active security. It is not necessarily the case that an actively secure protocol implies a passively secure protocol (since in the passive security setting, the security reduction must map passively corrupt adversaries to passively corrupt simulators). In Lemma 10 we show that every SFE functionality is isomorphic to a functionality that is "deviation-revealing" [20]. Such functionalities have the property that active-secure protocols imply passive-secure protocols. Using these two results, we are able to transition from active to passive security, and then argue about generalized vs. symmetric output.

4 Selectable Sources are Useless for Deterministic SFE

In this section we will show that any selectable source is useless for securely realizing any deterministic SFE functionality against computationally unbounded adversaries. In particular this shows that $\mathcal{F}_{\mathsf{coin}}$ is useless for realizing any deterministic SFE functionality.

Theorem 1. *Suppose $\mathcal{F}$ is a 2-party deterministic SFE and $\mathcal{G}$ is a selectable source. Then $\mathcal{F}$ has a standalone-secure (resp. UC-secure) protocol in the $\mathcal{G}$-hybrid model against computationally unbounded adversaries if and only if $\mathcal{F}$ has a standalone-secure (resp. UC-secure) protocol in the plain model.*

To give an overview of our techniques, we present the result for the special case of $\mathcal{F} = \mathcal{F}_{\mathsf{xor}}$ and $\mathcal{G} = \mathcal{F}_{\mathsf{coin}}$. Then we describe the modifications necessary to consider arbitrary $\mathcal{F}$ and arbitrary selectable source $\mathcal{G}$, respectively.

The case of $\mathcal{F}_{\mathsf{xor}}$ and $\mathcal{F}_{\mathsf{coin}}$. This special case illustrates our new frontier-based attack. It is well-known that there is no standalone-secure (or UC-secure) protocol for $\mathcal{F}_{\mathsf{xor}}$ in the plain model (cf. the complete characterization of [13,16]). Also note that standalone security is a special case of UC security. Thus it suffices to show the following:

Lemma 2. *There is no standalone-secure protocol for $\mathcal{F}_{\mathsf{xor}}$ using $\mathcal{F}_{\mathsf{coin}}$, against computationally unbounded adversaries.*

Proof (Sketch). The full proof is given in Appendix B.1. The main novelty in this proof (compared to the techniques in [16]) is the nature of the frontier we consider, in a semi-honest protocol. For semi-honest security, $\mathcal{F}_{\mathsf{xor}}$ does not have a canonical order for *what information* must be revealed by the two parties. This thwarts the analysis in [16], which depends on defining frontiers corresponding to what information is revealed in what order. Nevertheless we show that using a frontier parameterized by a threshold μ on (an appropriately defined notion of) *how much information* is revealed about a party's input, one can devise an attack on purported protocol for $\mathcal{F}_{\mathsf{xor}}$ in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model.

For simplicity, first assume that we are given a protocol π for $\mathcal{F}_{\mathsf{xor}}$ in the *plain* model (i.e., let us ignore $\mathcal{F}_{\mathsf{coin}}$ for the moment). Let α and β be defined as in Section 2. Then for every node v in the transcript tree of π, define

$$\delta_A(v, x, x') = \frac{|\alpha(v, x) - \alpha(v, x')|}{\alpha(v, x) + \alpha(v, x')} \qquad \text{and} \qquad \delta_B(v, y, y') = \frac{|\beta(v, y) - \beta(v, y')|}{\beta(v, y) + \beta(v, y')}.$$

δ_A and δ_B are well-defined after we exclude any nodes that have $\alpha(v, x) = \alpha(v, x') = 0$ or $\beta(v, y) = \beta(v, y') = 0$. Intuitively, $\delta_A(v, x, x')$ and $\delta_B(v, y, y')$ measure how much the transcript reveals about the distinction between x and x', or y and y', respectively. A δ value of 0 means that the partial transcript v is independent of the choice between the two inputs; a value of 1 means that the transcript v is only consistent with one of the two inputs.

Then given a parameter μ, we define a frontier F as follows:

$$F = \left\{ v \;\middle|\; \begin{array}{c} \max\{\delta_A(v,0,1), \delta_B(v,0,1)\} \geq \mu \\ \text{and no proper prefix of } v \text{ also satisfies this condition} \end{array} \right\}$$

Intuitively, F is the first place at which one of the parties has revealed "significant" information about its input, where significance is measured by μ.

Now we sketch an attack based on this frontier. (The actual proof and calculations in Appendix B.1 follow a slightly different argument, but using the same frontier). Suppose by symmetry that on an honest execution, the protocol assigns the majority of the weight on F to transcripts v satisfying $\delta_B(v,0,1) \geq \mu$. Then, intuitively, Alice can launch an attack as follows. She runs the protocol honestly (say, with input 0) until reaching F. Then at F, the transcript is correlated with Bob's input enough so that Alice can guess Bob's input with bias roughly $\mu/2$. On the other hand, since $\delta_A(v,0,1) < \mu$ with good probability at this point of the protocol, both values for Alice's input are somewhat likely explanations for the transcript seen so far. Therefore if Alice changes her input at this point (by sampling a state consistent with the current transcript and the new input), the outcome of the protocol will change with all but negligible probability, thanks to the correctness guarantee of the protocol. Thus, Alice can significantly correlate her *effective* input with Bob's, so that Bob's output is biased significantly towards 1 (when Bob picks his input at random). But this is a behavior that is not possible in an ideal-world interaction with $\mathcal{F}_{\mathsf{xor}}$, so it constitutes a violation of the security of π.

The only difference when attacking a protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model is that the common coins also influence the probabilities of partial transcripts. One may consider the probability of a partial transcript v (which includes outputs of $\mathcal{F}_{\mathsf{coin}}$) as a product of $\alpha(v,x)$, $\beta(v,y)$, and a contribution $\gamma(v)$ from the combined calls to $\mathcal{F}_{\mathsf{coin}}$. However, $\gamma(v)$ does not depend on x or y, so we can absorb its contribution into (arbitrarily) $\alpha(v,x)$ and the analysis remains valid.[7]

Uselessness of $\mathcal{F}_{\mathsf{coin}}$ for any SFE $\mathcal{F}$. First we consider the case when $\mathcal{F}$ is a *symmetric* SFE functionality. We use the characterization of SSFE functionalities with standalone-secure protocols from [16] to show that if an SSFE functionality $\mathcal{F}$ has no standalone-secure protocol in the plain model, then either there is a standalone-secure protocol for $\mathcal{F}_{\mathsf{xor}}$ in the $\mathcal{F}$-hybrid model, or else there is a frontier-based attack that violates standalone security of every purported protocol for $\mathcal{F}$ in the plain model.

In the first case, Lemma 2 demonstrates that $\mathcal{F}$ can have no standalone-secure protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid world. In the second case, we observe that

[7] Note that α and β are defined only in terms of honest behavior by the parties, so that every call to $\mathcal{F}_{\mathsf{coin}}$ delivers its output to both parties in our analysis and associated attack. (Only corrupt parties can prevent output delivery in a functionality with no output fairness guarantee.) Thus our attacks neither rely on fairness nor crucially exploit unfairness in the source of common coins; the adversaries we construct will always choose to deliver the outputs of the setup functionality.

the frontier-based attacks go through unaltered even if the protocols are allowed access to $\mathcal{F}_{\mathsf{coin}}$. This is because the frontier attack merely relies on the fact that in a protocol, given a transcript prefix v, the next message depends only on one of Alice and Bob's inputs. However, this is true even if the protocol has access to $\mathcal{F}_{\mathsf{coin}}$— the bits from $\mathcal{F}_{\mathsf{coin}}$ being independent of both parties' inputs.

This allows us to conclude that in either case, there can be no protocol for $\mathcal{F}$ in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model, giving us the following lemma (see Appendix B.2 for more details).

Lemma 3. *If $\mathcal{F}$ is a 2-party deterministic SSFE that has no standalone-secure (resp. UC-secure) protocol against unbounded adversaries in the plain model, then $\mathcal{F}$ has no standalone-secure (resp. UC-secure) protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model.*

Replacing $\mathcal{G}$ with an arbitrary selectable source. Our analysis goes through with minimal modification when $\mathcal{F}_{\mathsf{coin}}$ is replaced by an arbitrary selectable source. Recall that in a selectable source functionality $\mathcal{G}$, only one party can influence the output at a time (depending on which "direction" $\mathcal{G}$ is used in). When $\mathcal{G}$ is used such that only Alice influences the output, the influence on the transcript's probability can be collected into the term $\alpha(v, x)$. Similarly, when only Bob can influence the output of $\mathcal{G}$, the influence can be collected into the term $\beta(v, y)$. Therefore, we can still write $\Pr[v|x, y] = \alpha(v, x)\beta(v, y)$ for appropriate α and β. Each invocation of $\mathcal{G}$ is an atomic event with respect to the frontiers and to the adversary's changes in behavior in our our attacks.

Extending to general SFE functionalities. Finally, we prove Theorem 1, using Lemma 1. Note that a selectable source has a passive secure protocol (Alice samples an output and gives it to Bob). Thus if there exists any SFE functionality $\mathcal{F}$ for which some selectable source is useful in (UC- or standalone-) securely realizing, then by Lemma 1 selectable source is useful in (UC- or standalone-) securely realizing some SSFE functionality as well, contradicting Lemma 3.

5 Coins are useless for Randomized SFE

In this section, we characterize the set of randomized SFE functionalities that can be reduced to $\mathcal{F}_{\mathsf{coin}}$.

Since $\mathcal{F}_{\mathsf{coin}}$ itself is not securely realizable (in the UC or standalone model) against computationally unbounded adversaries, common randomness clearly allow more functionalities to be securely realized. In particular common randomness can be used to generate a shared sample from a publicly agreed-upon distribution. However, we show that this is essentially the only use of common randomness, when UC security is required . (When standalone security is considered, we give examples of randomized SSFE for which $\mathcal{F}_{\mathsf{coin}}$ is useful in a more non-trivial way in the full version [15].) More precisely,

Theorem 2. *A randomized SFE functionality $\mathcal{F}$ has a UC-secure protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model if and only if $\mathcal{F}$ is isomorphic to the SSFE functionality $\mathcal{F}^*$ with output function $\mathcal{F}^*$ such that $\mathcal{F}^*(x, y, r) = (h(x), r)$, where h is a deterministic function.*

Note that a secure protocol for $\mathcal{F}^*(x, y, r)$ above is simple: Alice sends $h(x)$ to Bob, and then they obtain uniformly random coins r from $\mathcal{F}_{\mathsf{coin}}$. Thus, any UC secure protocol for f which uses $\mathcal{F}_{\mathsf{coin}}$ can be replaced by one of the following form: (1) one party sends a function of its input to the other party; (2) both parties access $\mathcal{F}_{\mathsf{coin}}$ to obtain coins r; (3) both parties carry out local computation to produce their outputs.

Given Lemma 1, it is enough to establish our characterization for the special case of *symmetric* SFE functionalities (for which we shall denote the common output by $f(x, y, r)$).

The first step in proving Theorem 2 for SSFE is to show that only one party's input can have influence on the outcome of the other party.

Lemma 4. *If $\mathcal{F}$ is a 2-party randomized SSFE functionality with a UC-secure protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model, then $\mathcal{F}(x, y)$ is distributed as $\mathcal{F}'(x)$ (or $\mathcal{F}'(y)$), where $\mathcal{F}'$ is some randomized function of one input.*

If $\mathcal{F}$ does not have the form $\mathcal{F}'(x)$ or $\mathcal{F}'(y)$, we call it an SSFE functionality with *bidirectional influence*. Using Lemma 9, we show that if a bidirectional influence SSFE $\mathcal{F}$ has a UC-secure protocol in the $\mathcal{F}_{\mathsf{coin}}$ hybrid then there exists a semi-honest protocol for OT. However, this is not possible against computationally unbounded adversaries and hence, $\mathcal{F}$ can not have bidirectional influence.

Frontiers of influence. Suppose we are given a protocol π for f in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model, with simulation error ϵ. Without loss of generality, we assume that the last step of π is to toss a random coin which is included in the output.[8] First, define $\mathcal{O}_v^x$ to be the output distribution of the protocol when executed honestly on (Alice) input x, *starting from partial transcript* v. We use this to define our first frontier:

$$G = \left\{ v \;\middle|\; \begin{array}{c} \forall x', x'' : \mathrm{SD}\left(\mathcal{O}_v^{x'}, \mathcal{O}_v^{x''}\right) < \sqrt{\epsilon} \\ \text{and no ancestor of } v \text{ satisfies the same condition} \end{array} \right\}$$

Intuitively, G represents the point at which Alice's input has first exhausted any "significant" influence on the final output distribution — her input can no longer change the output distribution by more than $\sqrt{\epsilon}$. Next, note that the only way to induce an output distribution in the ideal world is to choose an input

[8] To see that this is without loss of generality, define a randomized SSFE f' which on input x, outputs $f(x)$ as well as a random bit. Then define π' to be the protocol which runs π and in the last step uses $\mathcal{F}_{\mathsf{coin}}$ to toss a coin which is included in the output. It is easy to see that if π is a secure protocol for f, then π' is a secure protocol for f', so proving the insecurity of π' establishes the insecurity of π.

x according to some distribution $\mathcal{D}$ and then send x to f, yielding the output distribution $\{f(x)\}_{x \leftarrow \mathcal{D}}$. Let $\mathcal{S}$ be the space of all possible output distributions that can be induced in this way.[9] We use this to define a collection of frontiers, one for each value of x.

$$F_x = \{v \mid \mathrm{SD}(\mathcal{O}_v^x, \mathcal{S}) > \sqrt{\epsilon} \text{ and no ancestor of } v \text{ satisfies the same condition}\}$$

Intuitively F_x represents the first time that randomness has had a "significantly" non-trivial influence on the output when Alice's input is x. Here, the influence of randomness in the protocol is considered non-trivial if the protocol has reached a point such that the conditional output distribution induced by the protocol starting from that point cannot be achieved by Alice in the ideal world.

We now show that in a secure protocol, Alice's input must completely exhaust its influence before the randomness from $\mathcal{F}_{\mathsf{coin}}$ can begin to influence the output distribution.

Lemma 5. *In the above setting, let $F_x < G$ denote the event that the protocol generates a transcript that encounters frontier F_x strictly before encountering frontier G. Then $\Pr[F_x < G|x]$ is negligible for all x.*

Proof (Sketch). The full proof is given in Appendix C.1. Consider a malicious Alice that runs π honestly on input x. Whenever this adversary encounters F_x strictly before G, it reports the resulting partial transcript to the environment. Being in the frontier F_x, this transcript intuitively represents an assertion by the adversary that it can realize an output distribution $\mathcal{O}_v^x$ that is impossible to effect in the ideal world (by continuing hereafter with input x). Being before G, the transcript also indicates an assertion by the adversary that it can still induce two "significantly" different output distributions (by continuing hereafter with one of the inputs from the condition in the definition of G). The environment can choose to challenge the adversary on any of these choices, and in the real world the adversary can always succeed. However, for any simulator in the ideal world, there must be some challenge for which the simulator must fail. Namely, if the simulator has already sent an input to ideal f at the time it makes its "assertion", then it cannot proceed to induce two significantly different output distributions on command — the output is already fixed. On the other hand, if the simulator has not sent an input to the ideal f, then it cannot proceed to realize an output distribution that is impossible in the ideal world.

Thus this adversary violates the security of f with success proportional to $\Pr[F_x < G|x]$, so we conclude that this probability must be negligible.

Using the previous two lemmas, we can now prove the special case of Theorem 2, restricted to SSFE functionalities:

Lemma 6. *A 2-party randomized SSFE functionality $\mathcal{F}$ has a UC-secure protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model against computationally unbounded adversaries if*

[9] Note that $\mathcal{S}$ is the space of convex combinations of $\{f(x) \mid x\}$, where here $f(x)$ denotes the discrete probability distribution itself, represented by a stochastic vector.

and only if $\mathcal{F}$ is isomorphic to the SSFE functionality $\mathcal{F}^*$ with output function f^* such that $f^*(x, y, r) = (h(x), r)$, where h is a deterministic function.

Proof. The complete proof is given in Appendix C.2. Lemma 5 shows that there is a frontier G that separates all of the influence of Alice's input (before G) from all of the influence of $\mathcal{F}_{\mathsf{coin}}$ (after G).

Our analysis relies on the *geometric interpretation of possible output distributions*. As before, let $\mathcal{S}$ denote the space of output distributions that can be realized in the ideal world by randomly choosing an input and sending it to f to obtain a sample of $f(x)$. $\mathcal{S}$ is the convex closure of a finite set of points $f(x)$. Call an input x *fundamental* if $f(x)$ is a corner on the convex hull of $\mathcal{S}$. Without loss of generality, we restrict our attention exclusively to fundamental inputs.[10]

Let x be a fundamental input. Since x affects the output of the protocol only negligibly after the transcript reaches G, we have that $f(x)$ is statistically close to a convex combination of $\{\mathcal{O}_v^x \mid v \in G\}$. An overwhelming weight of these distributions $\mathcal{O}_v^x$ are negligibly close (in statistical distance) to the space $\mathcal{S}$. By a geometric argument, since $f(x)$ is a *corner* in the space $\mathcal{S}$, we have that an overwhelming weight of $\mathcal{O}_v^x$ distributions are negligibly close to $f(x)$.

Thus, consider any two inputs x, x' such that $f(x) \not\equiv f(x')$. The statistical distance between these two distributions is a constant Δ. The above argument implies that x and x' must induce distributions over G that have statistical distance negligibly close to 1. In other words, executing the protocol until G unambiguously determines the distribution $f(x)$; after G, x has no more influence on the output. Then it is straight-forward to show that the following simple protocol is also secure for f: Alice sends a description of the distribution $f(x)$ to Bob (say, the lexicographically smallest x^* s.t. the distributions of $f(x)$ and $f(x^*)$ are identical). Both parties use $\mathcal{F}_{\mathsf{coin}}$ to generate random coins r and use them to compute a sample from the distribution $f(x)$. Then it is clear that f has the desired form — the output of this protocol is computed from a deterministic function of x along with independent coins.

On extending to selectable sources. Unlike our results in Section 4, Theorem 2 does **not** generalize to arbitrary selectable sources (instead of just $\mathcal{F}_{\mathsf{coin}}$). To see this, one can easily construct a selectable source f which is not of the form $f(x, y, r) = (h(x), r)$. Then trivially f has a UC-secure protocol using some selectable source (namely, itself), but f is not of the form required by Theorem 2.

Indeed, to prove Theorem 2, we made a crucial distinction between Alice's choice of input influencing the output distribution and $\mathcal{F}_{\mathsf{coin}}$ influencing the output distribution. This distinction is lost if $\mathcal{F}_{\mathsf{coin}}$ is replaced by a functionality in which Alice is allowed to influence the output.

On a common random string (CRS) vs. $\mathcal{F}_{\mathsf{coin}}$. A common random string (CRS) is a source of shared randomness in which all random bits are generated once and for all at the beginning of a protocol interaction, rather than as-needed, as

[10] Any non-fundamental input x is redundant in f and we can remove it to obtain an isomorphic functionality (see proof of Lemma 10).

with $\mathcal{F}_{\mathsf{coin}}$. Our proof of Theorem 2 states that the influence of the parties' inputs ends before the influence of the shared randomness begins. Since the influence of a CRS must happen at the start of a protocol, a CRS is useless for SSFEs except those of the form $f(x, y, r) = h(x)$ (no influence from shared randomness) or $f(x, y, r) = h(r)$ (no influence from parties' inputs), for a deterministic h.

6 Randomized Functionalities and Computational Intractability

Our results so far have been presented in the computationally unbounded setting. However, they do extend somewhat to the probabilistic polynomial time (PPT) setting (where all entities, including the adversary and the environment are PPT), and yield interesting connections with computational intractability assumptions. These results are similar in spirit to the connections established in [17], but unlike there, are applicable to randomized functionalities.

Firstly, in the case of deterministic SFE functionalities, we obtain the following unconditional result in the PPT setting (see Appendix E.1).

Theorem 3. *For every 2-party deterministic SFE $\mathcal{F}$ and selectable source $\mathcal{G}$, $\mathcal{F}$ has a standalone secure protocol in the $\mathcal{G}$-hybrid model in the PPT setting, if and only if $\mathcal{F}$ has a standalone secure protocol in the plain model in the PPT setting.*

Our other results for the PPT setting are conditional. An important observation in [17] was that, statements of the form "2-party functionality $\mathcal{F}$ has a UC-secure protocol in the $\mathcal{G}$-hybrid world (in the PPT setting)" are either known to be unconditionally true or false, or tend to be *equivalent* to the assumption that one-way functions exist, or the assumption that there is an oblivious transfer (OT) protocol secure against semi-honest adversaries. [17] study a large class of such statements for deterministic $\mathcal{F}$ and $\mathcal{G}$, and show that for every one of them the corresponding statement falls into one of the four classes listed above. An important problem left open is to understand whether the same pattern holds when considering *randomized* functionalities.

Our results suggest that this may be the case: the only intractability assumptions (other than being known to be unconditionally true or false) that arise among randomized functionalities still seem to be the existence of OWF and the existence of a semi-honest OT protocol. In particular we have the following two results :

Theorem 4. *Let $\mathcal{F}$ be any 2-party SFE functionality, possibly randomized. If one-way functions do not exist then $\mathcal{F}$ has a UC-secure protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model in the PPT setting, if and only if $\mathcal{F}$ is a publicly-selectable source.*

This is proven in Appendix E.1.

Theorem 5. *The following three statements are equivalent:*

1. *There exists a semi-honest OT protocol.*

2. $\exists$ *(possibly randomized) 2-party SSFE* $\mathcal{F}$ *with bidirectional influence :* $\mathcal{F}$ *is UC securely-realizable in* $\mathcal{F}_{\mathsf{coin}}$*-hybrid world.*
3. $\forall$ *(possibly randomized) 2-party SSFE* $\mathcal{F}$ *with bidirectional influence :* $\mathcal{F}$ *is UC securely-realizable in* $\mathcal{F}_{\mathsf{coin}}$*-hybrid world.*

The main task in proving the above is to show that (2) $\Rightarrow$ (1), which is carried out in Lemma 9. (1) $\Rightarrow$ (3) follows from a result proven in [9,18] on the completeness of $\mathcal{F}_{\mathsf{coin}}$. (3) $\Rightarrow$ (2) is trivial.

7 Conclusion and Future Work

Recently, [17] made a case for "cryptographic complexity theory," trying to understand the qualitative difference between different multiparty functionalities. However, the results there were confined to deterministic functionalities; the universe of randomized functionalities is vastly more complex, and is little understood. Among other things, this work initiates a systematic study of randomized functionalities, by proving the low-complexity nature of certain classes of randomized functionalities. In this work we do not consider randomized functionalities of higher levels of complexity, nor do we seek to classify all kinds of randomized functionalities. Nevertheless, we believe that our proof techniques — both for the computationally unbounded setting and for the PPT setting — will be useful in such a study. We leave this for future work.

References

1. D. Beaver. Perfect privacy for two-party protocols. In J. Feigenbaum and M. Merritt, editors, *Proceedings of DIMACS Workshop on Distributed Computing and Cryptography*, volume 2, pages 65–77. American Mathematical Society, 1989.
2. D. Beaver. Precomputing oblivious transfer. In D. Coppersmith, editor, *CRYPTO*, volume 963 of *Lecture Notes in Computer Science*, pages 97–109. Springer, 1995.
3. M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *STOC*, pages 103–112. ACM, 1988.
4. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. Electronic Colloquium on Computational Complexity (ECCC) TR01-016, 2001. Previous version "A unified framework for analyzing security of protocols" availabe at the ECCC archive TR01-016. Extended abstract in FOCS 2001.
5. R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable two-party computation. In *Proc. 34th STOC*, pages 494–503. ACM, 2002.
6. B. Chor and E. Kushilevitz. A zero-one law for boolean privacy (extended abstract). In *STOC*, pages 62–72. ACM, 1989.
7. R. Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In *STOC*, pages 364–369. ACM, 1986.
8. R. Cleve and R. Impagliazzo. Martingales, collective coin flipping and discrete control processes. Manuscript, 1993. http://www.cpsc.ucalgary.ca/~cleve/pubs/martingales.ps.
9. I. Damgård, J. B. Nielsen, and C. Orlandi. On the necessary and sufficient assumptions for UC computation. Cryptology ePrint Archive, Report 2009/247, 2009. http://eprint.iacr.org/.

10. O. Goldreich, S. Micali, and A. Wigderson. How to play ANY mental game. In ACM, editor, *Proc. 19th STOC*, pages 218–229. ACM, 1987. See [**?**, Chap. 7] for more details.
11. R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proc. 30th FOCS*, pages 230–235. IEEE, 1989.
12. J. Kilian. More general completeness theorems for secure two-party computation. In *Proc. 32th STOC*, pages 316–324. ACM, 2000.
13. R. Künzler, J. Müller-Quade, and D. Raub. Secure computability of functions in the it setting with dishonest majority and applications to long-term security. In O. Reingold, editor, *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 238–255. Springer, 2009.
14. E. Kushilevitz. Privacy and communication complexity. In *FOCS*, pages 416–421. IEEE, 1989.
15. H. K. Maji, P. Ouppaphan, M. Prabhakaran, and M. Rosulek. Exploring the limits of common coins using frontier analysis of protocols. In *TCC*, 2011. Full version at http://eprint.iacr.org/.
16. H. K. Maji, M. Prabhakaran, and M. Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In O. Reingold, editor, *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 256–273. Springer, 2009.
17. H. K. Maji, M. Prabhakaran, and M. Rosulek. Cryptographic complexity classes and computational intractability assumptions. In A. C.-C. Yao, editor, *ICS*, pages 266–289. Tsinghua University Press, 2010.
18. H. K. Maji, M. Prabhakaran, and M. Rosulek. A zero-one law for cryptographic complexity with respect to computational UC security. In T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 595–612. Springer, 2010.
19. T. Moran, M. Naor, and G. Segev. An optimally fair coin toss. In *TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 1–18. Springer, March 2009.
20. M. Prabhakaran and M. Rosulek. Cryptographic complexity of multi-party computation problems: Classifications and separations. In D. Wagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 262–279. Springer, 2008.
21. A. C. Yao. Protocols for secure computation. In *Proc. 23rd FOCS*, pages 160–164. IEEE, 1982.

A Frontier Analysis

Our results are derived using a class of techniques that we refer to as the *frontier analysis* of protocols. A protocol can be represented by a (weighted) rooted binary tree, so that a path from the root represents the bits exchanged in an execution of the protocol. (The weight on an edge represents the probability that a party responds with a particular bit at a particular point in the protocol; these weights at each node are simply a function of the input of at most one party.) In our analyses we define frontiers on this tree where, typically, some information regarding the input or the eventual output becomes apparent in the protocol transcript (when both parties follow the protocol honestly). The specific frontiers we shall employ will be tailor-made for the problem at hand.

We briefly discuss why it seems that often such a detailed analysis of protocols is necessary. Some of the prior results that show impossibility of secure protocols [6,14,1] used somewhat similar but much simpler arguments. They are simpler in that (in the terminology of frontier analysis) they consider an individual node in the protocol tree at a time. However this limits their applicability to the setting of *perfect security* (as opposed to statistical security). Intuitively, the reason for this restriction is that protocols with super-logarithmic communication complexity are super-polynomial sized objects, and analyzing such a protocol locally (an individual node at a time) cannot demonstrate a statistically significant insecurity.

Another possible approach to protocol analysis[11] would be to reason about the protocol one round at a time. The idea will be to identify a round where some event occurs (like, in the case of simultaneous exchange of inputs, one party may have revealed some information about its input). Such an approach has a couple of drawbacks. Firstly, such impossibility results typically become weaker as the number of rounds in the protocol increases. leaving open the possibility that exponentially long protocols can in fact provide security (e.g., the results in [13]). Another issue is that in different possible evolutions of the protocol, events at the same round can offset each other's effect. Yet another serious problem is that "attacks" that one can demonstrate against a protocol often need to depend on specific sequences of events in history; however simply considering likelihood of various (easy to analyze) events at a round does not tell us about the correlation between events at various rounds. In short, a gross analysis that considers only the aggregate behavior of a protocol at each round is often limited in its ability to reason about arbitrary protocols and prove impossibility results.

B Proofs Relating to Theorem 1

B.1 Proof of Lemma 2

Lemma 2 states that there is no standalone-secure protocol for $\mathcal{F}_{\mathsf{xor}}$ in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model, against computationally unbounded adversaries.

Proof (Proof of Lemma 2). Suppose for contradiction π is a standalone-secure protocol for $\mathcal{F}_{\mathsf{xor}}$ in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model. Recall that in $\mathcal{F}_{\mathsf{xor}}$, Alice chooses an input $x \in \{0,1\}$, Bob chooses an input $y \in \{0,1\}$, and both parties learn $x \oplus y$. We will show an attack against π that violates the security guarantee of $\mathcal{F}_{\mathsf{xor}}$— specifically, we will show an attack whereby the honest party chooses its input at random, yet its output is significantly biased. This is indeed a violation of security since in the ideal world the corresponding output must be an unbiased bit.

Without loss of generality, assume that every other round of the protocol is an access to $\mathcal{F}_{\mathsf{coin}}$. We only use the property that the probability of each transcript

[11] We use the term protocol analysis to mean the analysis of arbitrary protocols, typically from the point of view of proving an impossibility. This must not be confused with analysis of specific protocols.

consists of independent probability contributions from Alice, Bob, and $\mathcal{F}_{\mathsf{coin}}$. Let $\epsilon = \epsilon(k)$ denote the security error (maximum deviation between ideal world and real world) of the protocol, thus ϵ is negligible in the security parameter k.

Define α and β as in Section 2, and let γ be the probability contribution from $\mathcal{F}_{\mathsf{coin}}$. Thus, for every partial transcript v we can express $\Pr[v|x,y] = \alpha(v,x)\beta(v,y)\gamma(v)$. Now, for every partial transcript v, define

$$\delta_A(v) = \frac{|\alpha(v,0) - \alpha(v,1)|}{\alpha(v,0) + \alpha(v,1)} \qquad \text{and} \qquad \delta_B(v) = \frac{|\beta(v,0) - \beta(v,1)|}{\beta(v,0) + \beta(v,1)}.$$

δ_A and δ_B are well-defined after we exclude any nodes that have $\alpha(v,0) = \alpha(v,1) = 0$ or $\beta(v,0) = \beta(v,1) = 0$. Intuitively, $\delta_A(v)$ and $\delta_B(v)$ measure how much Alice's or Bob's input affects the probability of reaching v, respectively. For instance, $\delta_A(v) = 0$ means that the partial transcript v contains no information about Alice's input (in fact, it is distributed independent of her input); $\delta_A(v) = 1$ means that the partial transcript v completely reveals Alice's input — it is uniquely determined by v.

Let $0 < \mu \leq 1$ be a fixed parameter to be defined later, and define the following sets:

$$F_A = \{v \mid \delta_A(v) \geq \mu \text{ and no proper prefix of } v \text{ satisfies } (\delta_A(v) \geq \mu \text{ or } \delta_B(v) \geq \mu)\}$$
$$F_B = \{v \mid \delta_B(v) \geq \mu \text{ and no proper prefix of } v \text{ satisfies } (\delta_A(v) \geq \mu \text{ or } \delta_B(v) \geq \mu)\}$$
$$F_C = \{v \mid v \text{ is a complete transcript and no proper prefix of } v \text{ satisfies } (\delta_A(v) \geq \mu \text{ or } \delta_B(v) \geq \mu)\}$$

It is easy to see that $F_A \cup F_B \cup F_C$ indeed constitute a complete frontier. Intuitively, F_A and F_B represent the first place where Alice or Bob has revealed "significant" information about their input, respectively, where the parameter μ measures the amount of significance. F_C represents the remaining transcripts needed to extend $F_A \cup F_B$ to a frontier.

First, we argue that F_C is only reached with negligible probability during honest executions of the protocol. Intuitively, the transcript must eventually reveal both parties inputs, since the transcript contains at least the output $x \oplus y$ and any two of $\{x, y, x \oplus y\}$ uniquely determine the third quantity. The following proposition is useful:

Proposition 1. *If $|p-q|/(p+q) < c$, then $\frac{p}{q}, \frac{q}{p} \in (\frac{1-c}{1+c}, \frac{1+c}{1-c})$.*

Thus, for any $v \in F_C$, we have $\alpha(v,0)/\alpha(v,1), \beta(v,0)/\beta(v,1) \in (\frac{1-\mu}{1+\mu}, \frac{1+\mu}{1-\mu})$. Since transcripts in F_C are complete transcripts, each one uniquely determines the output of the parties. Partition F_C into $F_C^{(0)}$ and $F_C^{(1)}$, where $F_C^{(b)}$ are the transcripts on which Alice outputs b. Note that by the correctness of the protocol, $\Pr[F_C^{(x \oplus y \oplus 1)}|x,y] \leq \epsilon$. Then

$$\begin{aligned}\Pr[F_C \mid x=0, y=0] &= \sum_{v \in F_C^{(1)}} \Pr[v|x=0,y=0] + \sum_{v \in F_C^{(0)}} \Pr[v|x=0,y=0] \\ &\leq \epsilon + \frac{1+\mu}{1-\mu} \sum_{v \in F_C^{(0)}} \Pr[v|x=1,y=0] \leq \frac{1+\mu}{1-\mu}\epsilon + \epsilon = \frac{2\epsilon}{1-\mu} = \text{negl}(k).\end{aligned}$$

Here we assume that μ is a constant independent of k. Similarly, $\Pr[F_C|x,y] \leq \mathrm{negl}(k)$ for all $x, y \in \{0,1\}$.

Now partition F_A and F_B respectively into the following sets:

$$F_{A0} = \{v \in F_A \mid \alpha(v,0) > \alpha(v,1)\} \qquad F_{B0} = \{v \in F_B \mid \beta(v,0) > \beta(v,1)\}$$
$$F_{A1} = \{v \in F_A \mid \alpha(v,1) > \alpha(v,0)\} \qquad F_{B1} = \{v \in F_B \mid \beta(v,1) > \beta(v,0)\}$$

Then $F_{A,x}$ is the point in the protocol at which the transcript is significantly biased towards Alice having input x; similarly for $F_{B,y}$.

By symmetry, suppose $\Pr[F_{B0} \mid x = 0, y = 0]$ is the maximum of the four values

$$\Big\{ \Pr[F_{A0} \mid x = 0, y = 0], \Pr[F_{A1} \mid x = 0, y = 0], \Pr[F_{B0} \mid x = 0, y = 0], \Pr[F_{B1} \mid x = 0, y = 0] \Big\}.$$

Then, since $\Pr[F_C \mid x = 0, y = 0] < \mathrm{negl}(k)$, we have $\Pr[F_{B0} \mid x = 0, y = 0] \geq \frac{1}{4} - \mathrm{negl}(k)$.

We now construct a strategy for a corrupt Alice that will bias Bob's output towards 1 when Bob is executing π on a randomly chosen bit y. Alice's strategy is to run the protocol honestly with input $x = 0$, until the transcript reaches a node v on frontier F. If $v \notin F_{B0}$, then she continues the execution honestly. Otherwise (i.e., $v \in F_{B0}$) she switches her input to 1 (by sampling a state consistent with the current transcript and the input 1) and continues the execution honestly with her new state.

Let OUT denote the output of Bob in the protocol, and let p' denote the probability in the interaction described above (honest Bob choosing a random input y, and Alice running the strategy described). It suffices to show that $\left|p'[\textsc{out} = 0] - \frac{1}{2}\right|$ is bounded by a positive constant.

We split the analysis into cases. Let F_{B0} denote the event that the transcript intersects the frontier F at a point in F_{B0}. Then

$$\begin{aligned} p'[\textsc{out} = 0] = \frac{1}{2}\Big[& p'[\textsc{out} = 0 \wedge F_{B0} \mid y = 0] + p'[\textsc{out} = 0 \wedge \overline{F_{B0}} \mid y = 0] \\ & + p'[\textsc{out} = 0 \wedge F_{B0} \mid y = 1] + p'[\textsc{out} = 0 \wedge \overline{F_{B0}} \mid y = 1] \Big] \end{aligned}$$

We bound each of these four quantities separately.

First, $p'[\textsc{out} = 0 \wedge F_{B0} \mid y = 0]$. Note that conditioning on event F_{B0}, Alice changes her input from $x = 0$ to $x = 1$. Intuitively, we should expect that the protocol will give output $0 \oplus 1 = 1$, not output 0. Formally:

$$\begin{aligned} p'[\textsc{out} = 0 \wedge F_{B0} \mid y = 0] &= \sum_{v \in F_{B0}} \Pr[\textsc{out} = 0 | v, x = 1, y = 0] \Pr[v | x = 0, y = 0] \\ &\leq \sum_{v \in F_{B0}} \Pr[\textsc{out} = 0 | v, x = 1, y = 0] \frac{1+\mu}{1-\mu} \Pr[v | x = 1, y = 0] \\ &\leq \frac{1+\mu}{1-\mu} \Pr[\textsc{out} = 0 | x = 1, y = 0] \leq \frac{1+\mu}{1-\mu}\, \epsilon = \mathrm{negl}(k) \end{aligned}$$

Note that Pr in these expressions denotes the probability over an entirely honest execution of the protocol.

Next, we consider $p'[\text{OUT} = 0 \wedge \overline{F_{B0}} \mid y = 0]$. Conditioning on event $\overline{F_{B0}}$, we have that malicious Alice will in fact run the protocol honestly on input $x = 0$ during the entire interaction. So by the properties of F_{B0}, we have:

$$p'[\text{OUT} = 0 \wedge \overline{F_{B0}} \mid y = 0] \leq \Pr[\overline{F_{B0}} \mid x = 0, y = 0] \leq 3/4 + \text{negl}(k)$$

Again, Pr only describes probabilities involving completely honest execution of the protocol.

Next, we consider $p'[\text{OUT} = 0 \wedge F_{B0} \mid y = 1]$. This quantity includes the event that Bob has input $y = 1$ and yet the transcript intersected the frontier at F_{B0}. Intuitively, this event should not happen very often (and less and less, as μ is larger). By the properties of F_{B0}, we have that $\beta(v, 1)/\beta(v, 0) \leq \frac{1-\mu}{1+\mu}$ for every $v \in F_{B0}$. Thus:

$$\begin{aligned} p'[\text{OUT} = 0 \wedge F_{B0} \mid y = 1] &\leq \Pr[F_{B0} \mid x = 0, y = 1] = \sum_{v \in F_{B0}} \Pr[v | x = 0, y = 1] \\ &\leq \frac{1-\mu}{1+\mu} \sum_{v \in F_{B0}} \Pr[v | x = 0, y = 0] \leq \frac{1-\mu}{1+\mu}. \end{aligned}$$

Finally, we consider $p'[\text{OUT} = 0 \wedge \overline{F_{B0}} \mid y = 1]$. Conditioning on event $\overline{F_{B0}}$, we have that malicious Alice will in fact run the protocol honestly on input $x = 0$ during the entire interaction. So by the correctness of the protocol, we have:

$$p'[\text{OUT} = 0 \wedge \overline{F_{B0}} \mid y = 1] \leq \Pr[\text{OUT} = 0 \mid x = 0, y = 1] \leq \epsilon = \text{negl}(k).$$

Combining all of these inequalities, we finally have:

$$p'[\text{OUT} = 0] \leq \frac{1}{2}\left[\frac{3}{4} + \frac{1-\mu}{1+\mu} + \text{negl}(k)\right].$$

When μ is a fixed constant greater than $3/5$, we have that $p'[\text{OUT} = 0]$ is bounded away from $1/2$ by at least a constant, as desired.

B.2 $\mathcal{F}_{\mathsf{coin}}$ Useless for all SSFE Functionalities

To extend Lemma 2 to the case of all SSFE functionalities, we rely on results from [16] (some of which are also obtained using frontier analysis).

First, we give some needed definitions. We say a function $f : X \times Y \to Z$ is *decomposable* [14,1] if either:

- f is a constant function;
- there exists a partition $X = X_1 \cup X_2$, such that for all $y \in Y$, $x \in X_1$, $x' \in X_2$, we have $f(x, y) \neq f(x', y)$, and f is decomposable when restricted to both $X_1 \times Y$ and $X_2 \times Y$; or

– there exists a partition $Y = Y_1 \cup Y_2$, such that for all $x \in X$, $y \in Y_1$, $y' \in Y_2$, we have $f(x,y) \neq f(x,y')$, and f is decomposable when restricted to both $X \times Y_1$ and $X \times Y_2$

In [16], a special class of decomposable functions was considered. For our purposes, let us call a function f *uniquely decomposable* if f is decomposable and there is no protocol for $\mathcal{F}_{\mathsf{xor}}$ in the f-hybrid model.

Proof (Proof of Lemma 3). Suppose $\mathcal{F}$ is an SSFE that has no standalone-secure protocol against unbounded adversaries (in the plain model). This class of SSFE functionalities has a combinatorial characterization from [16]. From this characterization, there are three cases of $\mathcal{F}$ to consider:

(1) If $\mathcal{F}$ is decomposable but not uniquely decomposable, then we have that $\mathcal{F}_{\mathsf{xor}}$ has a standalone-secure protocol in the $\mathcal{F}$-hybrid model. Thus the attack of Lemma 2 shows that $\mathcal{F}$ cannot have a protocol in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model.

(2) If $\mathcal{F}$ is uniquely decomposable but yet has no standalone-secure protocol, then one of the frontier attacks of [16] applies. In particular, [16] shows that if the function evaluated is uniquely decomposable and has a certain other combinatorial property it has a standalone-secure protocol, but if it is uniquely decomposable but lacks this combinatorial property then any protocol allows either a passive (i.e., semi-honest) attack, or if not, an explicit active standalone attack.

(3) If $\mathcal{F}$ is not decomposable, then [16] shows that there is in fact a *passive* attack on any protocol for $\mathcal{F}$. This attack is also constructed using frontier analysis of a purported protocol.

The attacks mentioned in (2) and (3) can be carried out as long as the protocol has the property that for any transcript v, $\Pr[v|x,y] = \alpha(v,x)\beta(v,y)$ for some functions α, β. Since this is the case for protocols in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model, we can show that any purported protocol for $\mathcal{F}$ in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model can be attacked in a way that violates standalone security.

In the case of UC security, the case (2) above changes, and will have a larger set of functionalities. But again, in this case if there is no passive attack on a protocol, there is an explicit attack against UC security (or even concurrent security with two sessions [16]), which extends to protocols in the $\mathcal{F}_{\mathsf{coin}}$-hybrid model as well. Thus in the same way, the theorem holds with respect to UC security as well as standalone security. (In fact, a stronger result appears in [17], that even in the computationally bounded setting, $\mathcal{F}_{\mathsf{coin}}$ is useful for securely realizing deterministic SSFE functionalities in the UC setting only if there exists a semi-honest secure OT protocol.)

C Proofs Relating to Theorem 2

C.1 Proof of Lemma 5

We first observe that for complete transcripts (leaves) v, we have that $\mathcal{O}_v^{x'} \equiv \mathcal{O}_v^{x''}$ for all x', x''; thus G is indeed a frontier. Also, because of our normal form (last

step of π is a trusted coin toss that is included in the output), every complete transcript (leaf) v satisfies $\mathrm{SD}(\mathcal{O}_v^x, \mathcal{S}) = \Theta(1) > \sqrt{\epsilon}$, and so F_x is indeed a frontier.

We now prove Lemma 5, which says that $\Pr[F_x < G|x]$ is negligible for every x.

Proof (Proof of Lemma 5). Consider a particular adversary A which does the following when interacting with any environment of the appropriate form:

- Runs the protocol π honestly on input x until reaching frontier F_x. At that point, it gives the environment the value of the current partial transcript u, and pauses.
- After receiving x^* from the environment, A continues running the protocol honestly with input x^* (after back-sampling a random tape consistent with u and input x^*).

Let S denote the simulator for this adversary. If the simulator does not provide a sample $u \in F_x$ that is distributed statistically close to the real world adversary, then some environment of the required form can distinguish the real world from the ideal world. Thus, assume that the simulator S always generates u statistically close to the real world interaction A.

Consider the case where the simulator receives x^* from the environment before it has sent an input to the functionality f. Then consider the environment that sends $x^* = x$ in step 2. In this case, the real world adversary A will induce the distribution $\mathcal{O}_u^x$, which is an unsimulatable distribution by the definition of F_x. No matter how the simulator subsequently chooses its input to send to f, it will induce an output distribution for the honest party whose statistical distance from $\mathcal{O}_u^x$ is at least $\sqrt{\epsilon}$. Some environment of the required form can distinguish the two interactions, so we conclude that the simulator must send its input to f before step 2, except with negligible probability $\sqrt{\epsilon}$.

Thus without loss of generality assume that S sends an input to the ideal functionality f before receiving x^* from the environment, except with negligible probability. Then consider an environment that receives $u \in F_x$, and aborts if u has a prefix in G (i.e., if $F_x \not< G$). Otherwise, the environment chooses x^* uniformly from $\{x', x''\}$, where x' and x'' are such that $\mathrm{SD}\left(\mathcal{O}_u^{x'}, \mathcal{O}_u^{x''}\right) \geq \sqrt{\epsilon}$, by the definition of G. Now condition the entire interaction on the event that such an environment doesn't abort (whose probability of happening is negligibly close to $\Pr[F_x < G|x]$ in both the real and ideal interactions). Then in the ideal world, with probability at least $1/2$, the honest party's output from f will have statistical difference at least $\sqrt{\epsilon}$ from $\mathcal{O}_u^{x^*}$. But in the real world, the adversary always correctly induces the output distribution $\mathcal{O}_u^{x^*}$, so some environment of this form can distinguish the real and ideal worlds with probability $O(\Pr[F_x < G|x] \cdot \sqrt{\epsilon})$.

We conclude that $\Pr[F_x < G|x]$ must be at most $\sqrt{\epsilon}$, which is negligible.

C.2 Proof of Lemma 6

We follow the sketch in the main body in proving Lemma 6.

Proof (Proof of Lemma 6). For any fundamental input x, consider the probability distribution $f(x)$, which is a corner on the convex hull of $\mathcal{S}$. By the security of the protocol, $\mathcal{O}^x_r$ is within statistical distance ϵ of $f(x)$, where r is the root of the transcript tree (the empty transcript). We also have that $\mathcal{O}^x_r$ is equal to the convex combination $\sum_{v \in G} \Pr[v|x]\mathcal{O}^x_v$.

Let G^+ be the subset of G consisting of nodes v that have no ancestor in F_x. By Lemma 5, we have that $\Pr[G^+|x]$ is overwhelming. Thus $\mathcal{O}^x_r$ (and therefore $f(x)$) is negligibly close to the convex combination $\sum_{v \in G^+} \Pr[v|x]\mathcal{O}^x_v$.

By the definition of G^+, each of the distributions $\mathcal{O}^x_v$ in the above convex combination are negligibly close (within statistical distance ϵ_2) to the convex space $\mathcal{S}$. A straight-forward geometric argument shows that since $f(x)$ is a corner vertex in the convex space $\mathcal{S}$, and each of the $\mathcal{O}^x_v$ terms in the convex combination is negligibly close to the space $\mathcal{S}$, then there is a negligible quantity δ such that the probability of encountering $v \in G$ on input x such that $\mathrm{SD}(\mathcal{O}^x_v, f(x)) \leq \delta$ is overwhelming. That is, almost all of the weight that x places on frontier G is placed on nodes v that induce a distribution that is negligibly close to $f(x)$.

It then follows that for any x, x' such that $f(x) \not\equiv f(x')$, the two distributions $f(x)$ and $f(x')$ are distinct vertices on the convex hull of $\mathcal{S}$. Thus their statistical distance is a constant, and so x and x' induce distributions over G that have statistical distance negligibly close to 1.

Thus consider a simple protocol ρ of the following form: Given x, Alice determines (deterministically) a sampling circuit M_x that samples the distribution $f(x)$, and sends M_x to Bob. Both parties then obtain random coins r from $\mathcal{F}_{\mathsf{coin}}$, and evaluate $M_x(r)$ — a sample from $f(x)$.

We claim that π is as secure as ρ in the UC sense (that is, for every adversary attacking π, there is an adversary attacking ρ that achieves the same effect in all environments). The interesting case is when a corrupt Alice is attacking π. Then the corresponding simulator does the following. It interacts with Alice in π (playing the role of an honest Bob and honest $\mathcal{F}_{\mathsf{coin}}$), and pauses the interaction once the G frontier has been reached. Suppose that $v \in G$ is the π-transcript so far. At this point, from the arguments above, the simulator can identify Alice's distribution $f(x)$ with only negligible error. Then the simulator sends M_x in its ρ interaction. The simulator and honest Bob toss coins in their ρ interaction to sample $z \leftarrow M_x(r)$. By the properties of G, Alice can no longer significantly bias the outcome of protocol π — the remainder of the protocol's output depends almost entirely on the ideal coin tosses. Also, with overwhelming probability, $\mathcal{O}^x_v$ is negligibly close to $f(x)$, so the simulator can sample a set of simulated coin tosses (for the π interaction) which will result in z as the π protocol's output. It is straight-forward to see that the simulated interaction with Alice is indistinguishable from a real interaction.

Finally, we complete the proof of Theorem 2 by observing that f is indeed isomorphic to a function of the form $g(x, y) = (g'(x), r)$, since in ρ, both parties' outputs are a function of M_x (a deterministic function of x) and independent random coins r.

D Usefulness of $\mathcal{F}_{\mathsf{coin}}$ for Randomized SSFE for Standalone Security

Standalone-secure protocols and corresponding functionalities can be constructed as follows: consider any tree with nodes corresponding to Alice, Bob and $\mathcal{F}_{\mathsf{coin}}$. Label all the leaves with distinct characters. Define a randomized SSFE in which Alice's input set X are the set of (deterministic) strategies she has in this protocol: a strategy is a function mapping each of her nodes in the tree to one of its children. Similarly, Bob's input set Y is the set of his strategies. Given $(x, y) \in X \times Y$, a distribution over the leaves of the protocol is determined, which defines our randomized SSFE functionality. It is easy to see that a protocol in which Alice and Bob traverse the above tree with strategies corresponding to their inputs, accessing $\mathcal{F}_{\mathsf{coin}}$ at the nodes marked as such, is a standalone secure realization of this functionality.

One can construct functionalities of the above kind which are *not realizable* using a protocol in which Alice and Bob first compute a deterministic function, and then sample from a source specified by the outcome of that computation (or vice versa). An example is $\boxed{\begin{matrix}(1,0,0,0) & (1,0,0,0)\\ (0,\frac{1}{2},\frac{1}{2},0) & (0,0,\frac{1}{2},\frac{1}{2})\end{matrix}}$ where the vectors indicate probability distribution over an output alphabet of size 4.

E Randomized Functionalities and Computational Intractability

E.1 Extending Frontier Analysis for PPT Adversaries

Our frontier-based analyses crucially rely on the fact that an adversary can calculate the nodes of a protocol frontier, and perform a simple calculation (in general, computing the sign associated with a δ_A or δ_B value) at that frontier in order to attack any supposedly secure protocol. However, since protocol trees may have superpolynomial description size, and the frontiers are defined in terms of global probabilities, it is not clear how to extend frontier-based attacks to the PPT setting. However, following [17], we can extend the attacks to a setting where one-way functions do not exist.

In [11], it is shown that the existence of one-way functions (OWF) is implied by the much weaker assumption that *distributionally one-way* functions exist. Thus if OWFs do not exist, then no function is distributionally one-way: In other words, for every efficient function f and polynomial p, there is an efficient algorithm that on input y samples close to uniformly (within $1/p$ statistical difference) from the preimage set $f^{-1}(y)$.

Under such an assumption, we can carry out all of the frontier analyses employed in Section 4. It suffices to show that a PPT adversary, given a partial transcript, can efficiently estimate values of the form $\hat{\delta}_A(u, x, x') = \alpha(u, x)/(\alpha(u, x) + \alpha(u, x'))$ or $\hat{\delta}_B(u, y, y') = \beta(u, y)/(\beta(u, y) + \beta(u, y'))$ within a sufficiently small

1/poly additive error.[12] Below, we show how this can be accomplished using a straight-forward sampling approach.

The error inherent in our sampling of these values induces an additional 1/poly error in the attacks that are demonstrated in the previous section. However, since all of these attacks resulted in a violation of the security guarantees with *constant* probability, they are resilient to these extra 1/poly errors incurred by sampling.

Estimating the frontier. We outline how to compute $\hat{\delta}_A(u, x_0, x_1) = \alpha(u, x_0)/(\alpha(u, x_0) + \alpha(u, x_1))$ within arbitrarily small 1/poly error in polynomial time, provided that no one-way functions exist.

Define the function $f(x, r_A, y, r_B, r_C, i) = (\tau, x)$, where τ is the first i bits of the transcript generated when the protocol is executed honestly with inputs (x, y), and Alice uses random tape r_A, Bob uses random tape r_B, and $\mathcal{F}_{\mathsf{coin}}$ generates random coins r_C.

Given x_0, x_1, we use the guarantee of no distributionally one-way functions to sample from $f^{-1}(u, x_0)$ and $f^{-1}(u, x_1)$. If both preimages are empty, then the protocol never generates u as a partial transcript on inputs x_0 or x_1. If only one is empty, then $\{\hat{\delta}_A(u, x_0, x_1), \hat{\delta}_A(u, x_1, x_0)\} = \{0, 1\}$.

Otherwise, assume that u is indeed a possible partial transcript for both x_0 and x_1 (i.e., the protocol assigns positive probability to u when Alice has either input x_0 or x_1). Our previous sampling of f^{-1} has yielded an input y^* such that u is a possible partial transcript when executing π on inputs (x_0, y^*). Thus u is also a possible partial transcript on inputs (x_1, y^*). Now define:

$$g(x, r_A, y, r_B, r_C, i) = \begin{cases} (\tau, y) & \text{if } x \in \{x_0, x_1\} \\ \perp & \text{otherwise} \end{cases}$$

We now sample n times from $g^{-1}(u, y^*)$. Let n_b be the number of times the sampled preimage included x_b as the first component. Then n_b/n is an estimate of $\hat{\delta}_A(u, x_b, x_{1-b})$. By setting n to be a sufficiently large polynomial in the security parameter, we can ensure that the estimate is within an additive factor $1/k^c$ of the actual value for any c, with high probability.

This argument implies that if one way functions do not exist, then the frontiers introduced in Lemma 2 and Lemma 3 can be identified in polynomial time, though at the expense of an additional 1/poly error which can be driven arbitrarily small. So, we can generalize the result in Lemma 3 as:

Lemma 7. *Let $\mathcal{F}$ be any deterministic SSFE and $\mathcal{G}$ be any selectable source. If one way functions do not exist then $\mathcal{F}$ has a standalone secure protocol in the $\mathcal{G}$-hybrid model if and only if $\mathcal{F}$ has a standalone secure protocol in the plain model.*

[12] Note that $\delta_A(u, x, x') = |\hat{\delta}_A(u, x, x') - \hat{\delta}_A(u, x', x)|$ and δ_B is similarly defined in terms of $\hat{\delta}_B$. All the frontiers considered in this section are defined in terms of δ_A and δ_B.

For the case of standalone security, we can derive an unconditional result:

Lemma 8. *For all deterministic SSFE $\mathcal{F}$, $\mathcal{F}$ has a standalone secure protocol in the $\mathcal{G}$-hybrid world if and only if $\mathcal{F}$ has a standalone secure protocol in the plain world, where $\mathcal{G}$ is a selectable source.*

Proof. If one-way functions do not exist, then the claim is true by Lemma 7. On the other hand, if one-way functions exist, then take any protocol for $\mathcal{F}$ in the $\mathcal{G}$-hybrid model. Since $\mathcal{G}$ is a selectable source, it has a simple semi-honest secure protocol ρ. Assuming the existence of one-way functions, we can apply the GMW compiler [10] on ρ to obtain a standalone secure protocol for $\mathcal{G}$. Composing it with the $\mathcal{G}$-hybrid protocol for $\mathcal{F}$, we obtain a standalone secure protocol for $\mathcal{F}$ in the plain model.

Finally, it is easy to see that Lemma 1 holds in the PPT setting as well, yielding Theorem 3 as a corollary of Lemma 8.

Proof of Theorem 4 For Theorem 2, the main subproblem needing to be solved to effect the frontier-based attack is the following: Let $\mathcal{F}$ be a selectable source and v be any partial transcript. Compute the output distribution $\mathcal{O}_v^x$ corresponding to the transcripts which have v as its prefix.

Suppose only Alice input has influence on the output of $\mathcal{F}$. Let $g(x, r_A, r_B, i)$ be the function which outputs the first i bits of the transcript and Alice input x, where r_A and r_B are local random tapes of Alice and Bob respectively. If one way functions do not exist, then we can sample from the set $g^{-1}(v, x)$ in polynomial time. Given a tuple (x, r_A, r_B, i) we run the complete protocol and note down the output it generates. Performing this sampling for a large number of times, we can obtain an estimate of $\mathcal{O}_v^x$ within 1/poly additive error for each output.

To perform the frontier-based attack of Theorem 2, we also need to compute the statistical distance $\mathrm{SD}(\mathcal{O}_v^x, \mathcal{S})$. Using the estimated value of O_v^x, we can compute it with an additive error of 1/poly in polynomial time, yielding Theorem 4.

E.2 Hardness of SSFE Functionalities with Bidirectional Influence

In this section we will show the following result:

Lemma 9. *Let $\mathcal{F}$ be a (possibly randomized) SSFE, with bidirectional influence. For any selectable source $\mathcal{G}$, $\mathcal{F}$ has a UC secure protocol in the $\mathcal{G}$-hybrid then there exists a semi-honest secure protocol for OT.*

This generalizes a result from [17] which considered the case of $\mathcal{G}$ being the $\mathcal{F}_{\mathsf{coin}}$ functionality and $\mathcal{F}$ being deterministic (with bidirectional influence). The proof uses techniques similar to the ones introduced in their paper. We will sketch the outline of the ideas of the major modifications and the interested reader is requested to refer to the original paper for explicit details.

Consider the following protocol $P_{A\to B}$: Suppose Alice has two inputs x_0, x_1 from her input domain of $\mathcal{F}$ and Bob has a choice bit b. There are two session S_0 and S_1. In session S_b, Bob runs the simulator for corrupt Alice and in session S_{1-b} Bob runs the protocol honestly. Bob aborts both sessions at a round which is uniformly chosen at random. The instance of $\mathcal{G}_A$ and $\mathcal{G}_B$ are realized by Alice and Bob, respectively, computing the output honestly and sending it to the other party. If in session S_b, Bob is unable to extract Alice's input x_b, then it asks Alice to send both her inputs; and Alice sends (x_0, x_1) to Bob.

There is a similar protocol where the roles of Alice and Bob are reversed, say $P_{B\to A}$. It has been shown in [17] that under certain guarantees, the protocols $P_{A\to B}$ and $P_{B\to A}$ can be amplified into semi-honest secure protocols for OT. We will show that if $\mathcal{F}$ has a UC secure protocol in the $\mathcal{G}$-hybrid then the conditions are satisfied for $P_{A\to B}$ or $P_{B\to A}$.

Since $\mathcal{F}$ is bidirectional, for every Alice input x and x' there exists a Bob input y such that the distributions $f(x, y)$ and $f(x', y)$ are different. Similarly, for every Bob input y and y' there exists an Alice input x such that the distributions $f(x, y)$ and $f(x, y')$ are different. Consider the case when Alice is semi-honest corrupt. Let t_A be the round where Alice can predict Bob's input with probability at least $\zeta = 1/n + c < 1$, where the size of Bob's input domain is n and c is a small constant. Suppose in round s_B, the simulator for corrupt Alice extracts her inputs and sends it to $\mathcal{F}$. The simulator extracts the correct input of Alice, otherwise there exists a Bob input which can distinguish the actual input of Alice from the input sent by the simulator. Since Bob input is chosen uniformly at random, the environment can distinguish these two case with constant probability. We claim that $t_A \geq s_B + 1$. Suppose s_B is a round where Alice sends a bit or they use $\mathcal{G}_A$. In this case, at this round, all inputs for Bob are equally likely and hence $t_A > s_B$. Otherwise, if s_B is a round where Bob sends a bit or they use $\mathcal{G}_B$, then the simulator could have alternatively extracted one round earlier. This reduces the problem to the previous case.

In particular, we can conclude that $E[t_A] \geq E[s_B] + 1$. Let u_A be the round where Alice in the real protocol can predict Bob's input with probability ζ. Security guarantee implies that the simulated view should not be significantly different from the real view. Hence we obtain that $|E[u_A] - E[t_A]| \leq \epsilon/\zeta = \epsilon'$. This implies that $E[u_A] \geq E[s_B] + (1 - \epsilon')$.

Similarly, we define the quantities s_A, t_B and u_B and conclude that $E[u_B] \geq E[s_A] + (1-\epsilon')$. These two inequalities imply that either $E[u_A] \geq E[s_A] + (1-\epsilon')$ or $E[u_B] \geq E[s_B] + (1-\epsilon')$. In other words, either the simulator for corrupt Bob extracts significantly before Alice has a good guess about Bob's input; or other way around. Using the algorithm mentioned earlier, this guarantee is sufficient to obtain a semi-honest secure protocol for OT [17].

F Proof of Lemma 1

We say that two SFE functionalities $\mathcal{F}$ and $\mathcal{G}$ are *isomorphic* if there is a *local* protocol for UC-securely realizing $\mathcal{F}$ in the $\mathcal{G}$-hybrid model, and vice-versa. By

local, we mean that the protocol (say, the protocol for $\mathcal{F}$ in the $\mathcal{G}$-hybrid model) makes only one call to the ideal functionality $\mathcal{G}$ and performs no other communication. Local protocols allow each party to do no more than locally "translate" both the input from the environment and the output from $\mathcal{G}$. This translation may be randomized, especially in the case that $\mathcal{F}$ and $\mathcal{G}$ are randomized.

We say that an input for Alice x is *redundant* in an SFE $\mathcal{F}$ if $\mathcal{F}$ is isomorphic to a variant $\mathcal{F}_{-x}$ of $\mathcal{F}$ that does not allow input x from Alice. In other words, the effect of x can be achieved by having Alice locally translate her inputs and outputs to/from $\mathcal{F}$, using only inputs other than x. In this definition of redundancy, the protocol for $\mathcal{F}_{-x}$ in the $\mathcal{F}$-hybrid model is always the dummy protocol; the simulator for corrupt Alice in the $\mathcal{F}$ protocol in the $\mathcal{F}_{-x}$-hybrid model is also the dummy simulation. The simulator for the $\mathcal{F}_{-x}$ protocol and Alice's protocol for $\mathcal{F}$ coincide, and they correspond to Alice's "translation" technique for obviating the input x. Bob's protocol is the dummy protocol without loss of generality.

[20] define a property of functionalities called *deviation-revealing*, which relates UC security to passive security. UC security considers only actively corrupt adversaries — as such, it does not require that passively corrupt adversaries (who receive inputs from the environment on which to follow the protocol) are mapped to passively corrupt simulators (i.e., a simulator that runs the dummy protocol with the functionality).

For the purposes of this result, we define deviation-revealing slightly more restrictively than [20], requiring a condition for standalone security as well. We say that a functionality $\mathcal{F}$ is *deviation-revealing* if every UC-secure *or standalone-secure* protocol for $\mathcal{F}$ in the $\mathcal{G}$-hybrid model is itself a passive-secure protocol for $\mathcal{F}$ in the $\mathcal{G}$-hybrid model. But if $\mathcal{F}$ is deviation-revealing, then without loss of generality the simulator for a passively corrupt adversary can be passively corrupt. The name "deviation-revealing" comes from the fact that the functionality's behavior would reveal to an environment whether a party is interacting with $\mathcal{F}$ using the dummy protocol or deviating from it.

Lemma 10. *For every SFE functionality $\mathcal{F}$ there is a deviation-revealing functionality $\mathcal{G}$ that is isomorphic to it.*

Proof. Given an SFE $\mathcal{F}$, we define $\mathcal{G}$ by iteratively removing redundant inputs in $\mathcal{F}$ (for both parties). We do not require that removing redundant inputs results in a unique $\mathcal{G}$. Clearly $\mathcal{G}$ and $\mathcal{F}$ are isomorphic, and it suffices to show that $\mathcal{G}$ is deviation-revealing.

Let π be any UC-secure or standalone-secure protocol for $\mathcal{G}$ in the $\mathcal{H}$-hybrid model. We must show that π is itself also passive-secure in the $\mathcal{H}$-hybrid model. Consider a passive adversary $\mathcal{A}$ for π — that is, the adversary receives inputs from the environment and executes π honestly on those inputs, but also outputs its entire view to the environment. Let $\mathcal{S}$ be the simulator for this adversary, and it suffices to show that $\mathcal{S}$ can be made to interact with $\mathcal{G}$ according to the dummy protocol without loss of generality.

Consider a class of environments that inspect only the inputs and outputs of the parties, and in particular ignore $\mathcal{A}$'s reported view of the protocol. By

the correctness of π, an interaction with $\mathcal{A}$ is indistinguishable from an interaction with $\mathcal{G}$ in which all parties run the dummy protocol, for this class of environments.

Suppose such an environment gives input x to $\mathcal{S}$, and condition on the event that its simulator $\mathcal{S}$ sends an input other than x to $\mathcal{G}$. This $\mathcal{S}$ is expected to also return the output from $\mathcal{G}$, since the original passive adversary returned the output from π. By the security of π, this interaction is indistinguishable from an interaction with ideal $\mathcal{G}$ in which all parties run the dummy protocol, for this class of environments. Thus $\mathcal{S}$ is effecting a *local protocol* which demonstrates that the input x is *redundant*. Since $\mathcal{G}$ contains no redundant inputs, we conclude that this event (environment provides x but $\mathcal{S}$ sends an input other than x) happens with only negligible probability. Without loss of generality, we can add a wrapper around $\mathcal{S}$ that aborts if $\mathcal{S}$ sends an input other than the one provided by the environment. This wrapped simulator is still a sound simulation and is a passive simulator.

Lemma 11. *For every SFE functionality $\mathcal{G}$ that has a passive secure protocol in the plain model, there is a symmetric functionality $\mathcal{G}'$ that is isomorphic to it.*

Proof. We define the symmetric functionality $\mathcal{G}'$ to be the "common information" that Alice and Bob get from $\mathcal{G}$. This is best described by representing $\mathcal{G}$ as a bipartite graph G: the set of nodes on the left are (x, a) for each possible input value x for Alice x and output value a for Alice; similarly, the set of nodes on the right are (y, b) for all possible inputs y and outputs b for Bob. There is a weighted edge between (x, a) and (y, b) with weight $\Pr[a, b|x, y]$, namely, the probability that Alice and Bob get outputs a and b when they send x and y as their respective inputs to $\mathcal{G}$. If this weight is 0, then we consider the edge to be absent. $\mathcal{G}'$ is defined as an SSFE functionality which takes x and y from the parties, samples the outcome (a, b) according to $\mathcal{G}$, and returns to both parties the *connected component* H containing the edge $((x, a), (y, b))$ in G. Observe that $\mathcal{G}'$ gives the same output to both parties.

It suffices to show that if $\mathcal{G}'$ and $\mathcal{G}$ are not isomorphic, then $\mathcal{G}$ cannot have a passive secure protocol in the plain model. For this we rely on a result by Kilian [12] to show that in this case $\mathcal{G}$ will actually be *complete* for passive security, and hence cannot have a passive secure protocol in the plain model (unless we impose computational restrictions and assume that there is such a protocol for oblivious transfer).

Due to the restriction of *local* protocols, we see that $\mathcal{G}$ and $\mathcal{G}'$ are isomorphic if and only if, given the connected component H and their respective inputs, Alice and Bob can *independently* sample outcomes that are jointly distributed as outcomes from $\mathcal{G}$. This is possible only when there is a labeling of every vertex $q(x, a)$ (or $q(y, b)$) so that $\Pr[a, b|x, y] = q(x, a)q(y, b) \Pr[H|x, y]$. By $\Pr(H|x, y)$, we mean the probability that $\mathcal{G}'$ outputs H on inputs x and y.

Now suppose no such labeling exists. Then we claim that $\mathcal{G}$ must be *complete* for passive security. We adapt an argument of Kilian, who proved an analogous

statement for a special class of (deterministic) "asymmetric" SFEs $\mathcal{G}$ (Theorem 1.3 in [12]).[13]

We consider two cases which exhaustively characterize the condition described above:

Case 1: Suppose there exists $(x_0, a_0), (y_0, b_0), (y_1, b_1)$ such that $\Pr[a_0, b_0|x_0, y_0] > \Pr[a_0, b_1|x_0, y_1] > 0$ (or vice-versa with the roles of Alice and Bob exchanged). Then there must be a value a_1 such that $\Pr[a_1, b_0|x_0, y_0] < \Pr[a_1, b_1|x_0, y_1]$

Then consider the following passive protocol using $\mathcal{G}$, where Bob has input m:

1. Bob chooses a random bit t. The parties evaluate $\mathcal{G}$ twice, on inputs (x_0, y_t) and (x_0, y_{1-t}).
2. If Bob did not receive output sequence (b_1, b_1) or Alice did not receive a sequence of outputs in the set $\{(a_0, a_1), (a_1, a_0), (a_0, a_0)\}$ then the parties repeat step 1.
3. Bob sends $M = m \oplus t$ to Alice. If Alice received (a_0, a_1), she guesses $\hat{t} = 0$; if Alice received (a_1, a_0), she guesses $\hat{t} = 1$; otherwise, she sets $\hat{t}$ randomly. Alice locally outputs $M \oplus \hat{t}$.

The analysis of this protocol closely follows that of [12] (Lemma 5.2). Briefly, Bob's choice t is uniformly distributed conditioned on Alice receiving (a_0, a_0). In this case, she receives no information about Bob's input m. Otherwise, Alice's guess of $\hat{t}$ is biased towards Bob's choice of t and she learns partial information about m. The protocol therefore gives a "noisy" variant of Rabin OT that can be refined using the techniques described in [12].

Case 2: Suppose Case 1 does not hold and that there exist $(x_0, a_0), (x_1, a_1), (y_0, b_0), (y_1, b_1)$ such that $\Pr[a_0, b_0|x_0, y_0] = 0$, yet each of $\Pr[a_0, b_1|x_0, y_1], \Pr[a_1, b_0|x_1, y_0], \Pr[a_1, b_1|x_1, y_1]$ are nonzero. Since Case 1 does not hold, then these latter three probabilities must in fact be equal. Then consider the following passive protocol using $\mathcal{G}$:

1. Alice chooses random bit s. Bob chooses random bit t. Alice sends x_s to $\mathcal{G}$ and Bob sends y_t to $\mathcal{G}$.
2. If Alice did not receive output a_s or Bob did not receive output b_t, then the parties repeat step 1.
3. Alice locally outputs s. Bob locally outputs t.

This protocol allows Alice and Bob to generate correlated pairs (s, t) that are *uniformly* distributed in $\{(0, 1), (1, 0), (1, 1)\}$. Using the techniques spelled out in [12], such correlated pairs can be used to implement a passively secure OT.

We can now prove Lemma 1:

Lemma 1 (restated). *Suppose $\mathcal{H}$ is a functionality that has a passive-secure protocol in the plain model. If $\mathcal{H}$ is useful in UC- or standalone-securely realizing a (possibly randomized) SFE functionality $\mathcal{F}$, then there exists a* **symmetric**

[13] Kilian does not state the result in terms of isomorphism or common information. But the combinatorial condition is identical to the above.

SFE functionality $\mathcal{F}^*$ such that $\mathcal{F}^*$ is isomorphic to $\mathcal{F}$, and $\mathcal{H}$ is useful in (respectively, UC- or standalone-) securely realizing $\mathcal{F}^*$.

Proof. First note that if $\mathcal{F}$ is isomorphic to $\mathcal{F}^*$, then $\mathcal{H}$ is useful in securely realizing $\mathcal{F}$ if and only if $\mathcal{H}$ is useful in securely realizing $\mathcal{F}^*$. (This is because, if there is a protocol for $\mathcal{F}$ in the $\mathcal{H}$-hybrid model there is one for $\mathcal{F}^*$, and if there is no protocol for $\mathcal{F}$ in the plain model, there is none for $\mathcal{F}^*$ either.) So it is enough to give an SSFE functionality that is isomorphic to $\mathcal{F}$.

If $\mathcal{H}$ is useful in UC-/standalone-securely realizing a randomized SFE functionality $\mathcal{F}$, then $\mathcal{F}$ has a (respectively, UC- or standalone-) secure protocol in the $\mathcal{H}$-hybrid model. Let $\mathcal{G}$ be the deviation-revealing functionality guaranteed by Lemma 10. Because $\mathcal{G}$ is isomorphic to $\mathcal{F}$, we have that $\mathcal{G}$ has a (respectively UC- or standalone-) secure protocol in the $\mathcal{H}$-hybrid protocol. Then, since $\mathcal{G}$ is deviation-revealing, the same protocol is also passively secure in the $\mathcal{H}$-hybrid model. By our assumption, $\mathcal{H}$ has a passive-secure protocol in the plain model; so by composing these two protocols we can obtain a passive secure protocol for $\mathcal{G}$ in the plain model. Now, by Lemma 11, there is an SSFE functionality $\mathcal{F}^*$ that is isomorphic to $\mathcal{G}$. Thus $\mathcal{F}^*$ is our desired SSFE that is isomorphic to $\mathcal{F}$.