Characterizing Optimal Security and Round-Complexity for Secure OR Evaluation

Amisha Jhanji* Hemanta K. Maji† Raphael Arkady Meyer‡

January 30, 2017

Abstract

Secure multi-party computation allows mutually distrusting parties to compute securely over their private data. However, even in the semi-honest two-party setting, most interesting functions cannot be computed securely in the information-theoretic plain model. Intuitively, the objective of accurately evaluating the output of such functions is inherently inimical to the privacy concerns of the parties. Securely evaluating OR of the input bits of two parties is the simplest example, and this result captures the essence of the hardness in securely evaluating most functions.

This work studies the interplay between accuracy and privacy of secure 2-party function evaluation in the information-theoretic plain model. We provide an optimal accuracy versus privacy tradeoff for computing $\mathsf{OR}(x, y)$, where x and y are, respectively, the private input bits of Alice and Bob. In particular, we construct a round-optimal two-party protocol for OR that has maximum semi-honest security in the information-theoretic plain model. Prior results exhibit only weak tradeoffs that are far from the optimal. We generalize our techniques to obtain a tight accuracy-versus-privacy tradeoff characterization for a stronger notion of security, namely differentially-private semi-honest security.

The technical heart of our result is a new technique to derive inequalities for distributions of transcripts generated by protocols. This approach reduces the domain of the optimization problem from an unbounded number of transcripts to a constant size while preserving the optimal solution to the original problem. We believe that these techniques for analyzing protocols in the information-theoretic plain model will be of independent interest.

*Department of Computer Science, Purdue University. ajhanji@purdue.edu.
†Department of Computer Science, Purdue University. hmaji@purdue.edu.
‡Department of Computer Science, Purdue University. meyer219@purdue.edu.

Contents

1 Introduction

Secure multi-party computation [Yao82, GMW87] allows mutually distrusting parties to compute securely over their private data. In the 2-party secure function evaluation setting, Alice has private input x, and Bob has private input y, and they are interested in computing $z = f(x, y)$, where f is a deterministic function. A secure protocol to compute f ensures that, at the end of the protocol, Alice does not find any information about Bob's private input y that is not already revealed by her input-output pair (x, z). The protocol provides an analogous security guarantee for Alice's private input x. Even against semi-honest parties, i.e., parties follow the protocol honestly but are curious to find additional information about the other party's input, most interesting functions cannot be securely computed in the information-theoretic plain model [Dol82, Kil88, IL89, Kus89, Bea89, MPR09, KMQR09].[1]

A key insight underlying these hardness results is that it is impossible to securely compute the OR of Alice and Bob's private input bits. In turn, any function that has an embedded OR-minor[2] cannot be securely computed; hence, the pivotal nature of the hardness of securely computing OR.

Intuitively, a secure OR evaluation protocol needs to ensure the following guarantees.

- **Accuracy**: When Alice and Bob run the protocol with their respective private inputs x and y, they agree on an output z' at the end of the protocol. If for all pairs of input bits (x, y) the probability that $z' \neq \mathsf{OR}(x, y)$ is at most ε, then the protocol is $(1 - \varepsilon)$-accurate.

- **Privacy**: When Alice has input $x = 0$, the output $z = \mathsf{OR}(x, y) = y$ reveals Bob's private input bit. So, for $x = 0$, no additional non-trivial constraint is imposed on the protocol. However, when Alice has input $x = 1$, the output $z = \mathsf{OR}(x, y) = 1$ irrespective of Bob's private input bit. For $x = 1$, therefore, the protocol has to ensure that Alice cannot predict Bob's private input bit y. If Alice has an advantage at most ε in predicting Bob's private input bit, then the protocol is $(1 - \varepsilon)$-private. Analogously, the protocol ensures the privacy of Alice's private input bit x when Bob has input $y = 1$.

A secure protocol for OR is $(1 - \varepsilon)$-accurate and $(1 - \varepsilon)$-private, where ε is a negligible function in the statistical security parameter.

Simultaneously ensuring accuracy and privacy in secure OR evaluation is impossible in the information-theoretic plain model. However, the precise characterization of this tradeoff is not known. Towards improving the understanding of this fundamental problem, our work explores the following problem.

"What is the optimal accuracy versus privacy tradeoff for secure OR *evaluation?"*

Prior works provided rough estimates of this tradeoff. The emphasis of our work is to develop technical tools that assist in tightly characterizing this tradeoff. We believe that these techniques for analyzing protocols in the information-theoretic plain model will be of independent interest.

1.1 Model

In this work, we consider 2-party secure OR evaluation against semi-honest adversaries in the information-theoretic plain model. We use the standard definition of *simulation-based security*,

[1] In the information-theoretic plain model, parties have unbounded computational power and they communicate over secure channels to each other.

[2] A function f has an embedded OR-minor if there are Alice inputs x_0, x_1, Bob inputs y_0, y_1, and outputs z_0, z_1 such that $f(x_i, y_j) = z_{(i \vee j)}$.

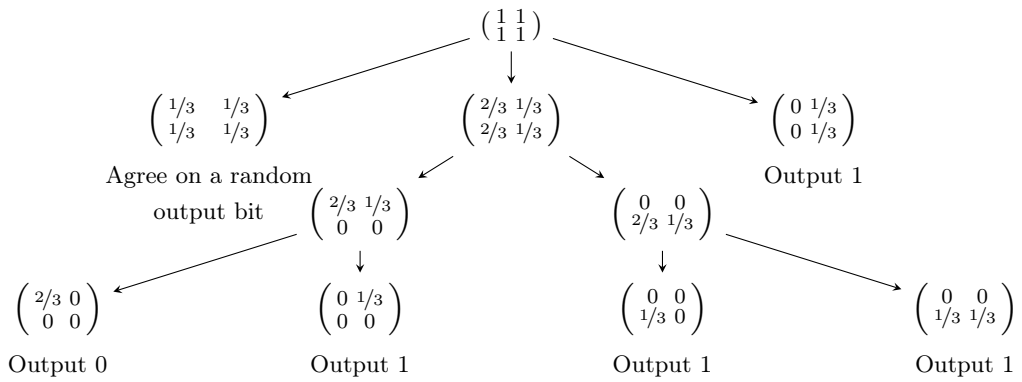


Figure 1: A 3-round semi-honest secure protocol π^* for OR that is $(1 - 1/6)$-simulation secure. The figure provides the probability distribution of the partial transcripts. For $x, y \in \{0, 1\}$, the (x, y)-th entry of a matrix corresponding to a node in the tree represents the probability of generating that node (the partial transcript) when Alice and Bob have respective private inputs x and y, respectively.

à la [Can00], that unifies the notions of accuracy and privacy. For all environments, if the statistical distance between the distributions of its view in the real and the ideal world is at most ε, then the protocol is $(1-\varepsilon)$-simulation secure. If the environment does not corrupt any party, then simulation security of a protocol is identical to its accuracy. Moreover, if the environment corrupts a party and sets its private input to 1, the simulation security of the protocol is identical to the input privacy of the other party. This work, we emphasize, uses a worst-case notion of security, i.e. we consider security against all possible environments. In particular, $(1 - \varepsilon)$-simulation security is identical to simultaneously satisfying $(1 - \varepsilon)$-accuracy and $(1 - \varepsilon)$-privacy.

Differential-privacy Restriction. For a parameter $\Theta > 1$, a 2-party protocol is Θ-*differentially private* [GMPS13] if the probability of generating any transcript can multiplicatively increase or decreases by a factor of at most Θ when one of the parties changes its private input.

1.2 Our Results

Our characterizations of accuracy and privacy tradeoff hold even against parties and simulators with unbounded computational power. On the other hand, our constructions admit efficient protocols and simulators.

Our first hardness result proves the following.

Theorem 1 (Upper-bound on Semi-honest Security)**.** *Let π be a 2-party secure* OR *evaluation protocol. Then, the protocol π is at most $(1-1/6)$-simulation secure against semi-honest adversaries. Further, there exists a 3-round protocol*[3] *π^* that is $(1 - 1/6)$-simulation secure.*

In fact, we show that ε-privacy error entails at least $(1/2 - 2\varepsilon)$-accuracy error in evaluating OR (see Lemma 1). Theorem 1 implies that any protocol for secure evaluation of an f that has an OR-minor incurs at least $1/6$ simulation error. Figure 1 presents the protocol π^*, and the following result implies its round optimality.

[3] In a 3-round protocol, one party sends the first message, the other party sends the second message, and, finally, the party who sent the first message sends the third message.

Theorem 2 (Round Optimality). *Let π be a 2-round secure* OR *evaluation protocol against semi-honest adversaries. If π has at most two rounds, then it is at most $(1 - 1/4)$-simulation secure.*

This result implies a constant gap in the maximum attainable security vis-à-vis 2-round and 3-round protocols, and there exists a 2-round protocol that achieves $(1 - 1/4)$-simulation security.

To demonstrate the power of the techniques introduced in our work, we characterize the maximum security achievable by OR evaluation protocols that are simultaneously semi-honest secure and Θ-differentially private.

Theorem 3 (Upper-Bound on Semi-honest DP Security). *For $\Theta > 1$, let ρ be a 2-party secure* OR *evaluation protocol that is also Θ-differentially private. Then, the protocol ρ is at most $(1 - (\Theta+2)/6(\Theta+1))$-simulation secure. Further, there exists a 3-round protocol ρ^* that is $(1 - (\Theta+2)/6(\Theta+1))$-simulation secure.*

As expected, for $\Theta \to \infty$, the guarantees of Theorem 3 and Theorem 1 coincide. We also show the round optimality of the construction ρ^*. If $\Theta \geqslant 4$, then any 2-round protocol is at most $(1 - 1/4)$-simulation secure. Note that, for large enough Θ, this result in independent of Θ.

1.3 Prior Results

Studies on the interplay between accuracy and (various notions of) security for realizing functionalities go beyond the information-theoretic plain model. For instance, computational hardness results for security notions like fairness [Cle86, GHKL08] and concurrent composition [CLOS02, Lin03] have been studied. In the context of secure function evaluation, several works [Dol82, Kil88, IL89, Kus89, Bea89, MPR09, KMQR09] have shown the impossibility of securely computing any function with an embedded OR-minor in the information-theoretic plain model.

Kushilevitz [Kus89] and Beaver [Bea89] independently proved that any two-party function evaluation that is not *decomposable* cannot have a perfectly secure protocol against semi-honest adversaries. Any function with an embedded OR-minor is not decomposable. Maji et al. [MPR09] showed that the characterization of Kushilevitz and Beaver extends to statistically secure protocols as well. They also proved that for every 2-party secure function evaluation f that is not decomposable there exists a constant $c_f > 0$ such that any semi-honest secure protocol for f is at most $(1 - c_f)$-simulation secure. In their work, for $f = \mathsf{OR}$, the constant $c_{\mathsf{OR}} \approx 0.0011$. As indicated by our results, the prior bound on simulation security was significantly far from the optimal.

For differential privacy, Goyal et al. [GMPS13] characterized tight accuracy and security tradeoffs for OR and XOR functions. They constructed differentially private protocols that achieved the optimal bounds for accuracy and security. We emphasize that protocols that are differentially private can have abysmal semi-honest security. So, their results do not entail meaningful bounds for semi-honest secure OR evaluation.

2 Preliminaries

In this section, we assume that the sample space is $\Omega = [n] := \{1, \ldots, n\}$. We express any probability distribution over the sample space Ω by an equivalent vector in $\mathbb{R}^n$. In particular, the vector $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{R}^n$, such that $a_i \geqslant 0$, for all $i \in \Omega$, and $\sum_{i \in \Omega} a_i = 1$, represents the probability distribution that samples $i \in \Omega$ with probability a_i, for all $i \in \Omega$.

Definition 1 (Cross-Product Rule). *A four-tuple of probability distribution $\mathbf{a}, \mathbf{b}, \mathbf{c}$, and $\mathbf{d}$ satisfy the* cross-product rule *if, for all $i \in \Omega$, the distributions satisfy*

$$a_i \cdot d_i = b_i \cdot c_i$$

Definition 2 (Cross-section)**.** *For a four-tuple of distributions* $\mathbf{a}, \mathbf{b}, \mathbf{c}$, *and* $\mathbf{d}$, *their* cross-section *at* $i \in \Omega$, *is represented by the tuple* a_i, b_i, c_i, *and* d_i.

Given a four-tuple of probabilities $\mathbf{a}, \mathbf{b}, \mathbf{c}$, and $\mathbf{d}$ that satisfy the cross-product rule, we pictorially represent them as $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$ and their i-th cross-section as $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$.

Definition 3 (Statistical Distance)**.** *For two probability distributions* $\mathbf{a}$ *and* $\mathbf{b}$ *over the sample space* Ω, *their* statistical distance *is represented by*

$$\mathrm{SD}(\mathbf{a}, \mathbf{b}) := \frac{1}{2} \sum_{i \in \Omega} |a_i - b_i|$$

The contribution *at* $i \in \Omega$ *refers to the quantity* $|a_i - b_i|$.

If two distributions $\mathbf{a}$ and $\mathbf{b}$ have $\mathrm{SD}(\mathbf{a}, \mathbf{b}) = \varepsilon$ then the advantage of predicting whether a sample was drawn from $\mathbf{a}$ or $\mathbf{b}$ is at most $\varepsilon/2$.

For $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$, we are interested in four statistical distances (1) $\varepsilon_1 = \mathrm{SD}(\mathbf{a}, \mathbf{b})$, (2) $\varepsilon_2 = \mathrm{SD}(\mathbf{a}, \mathbf{c})$, (3) $\varepsilon_3 = \mathrm{SD}(\mathbf{c}, \mathbf{d})$, and (4) $\varepsilon_4 = \mathrm{SD}(\mathbf{b}, \mathbf{d})$. We say that $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ are the *statistical distances corresponding to* $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$. Two four-tuple of distributions $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & a \end{smallmatrix}\right)$ re *SD-equivalent* if the statistical distances corresponding to them are identical. Figure 2 summarizes these concepts pictorially.

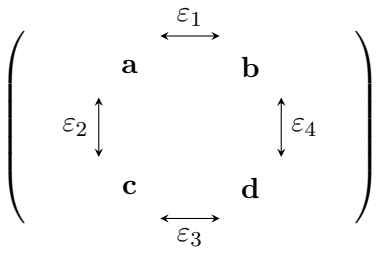


Figure 2: A pictorial summary of the concepts.

3 Relation of Semi-honest Security and Statistical Distances

Let π be a 2-party secure OR evaluation protocol. Let $\mathbb{T}(x, y)$ represent the transcript distribution of π when parties have private inputs bits x and y, respectively. Consider the four-tuple of probabilities $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$, where $\mathbf{a} = \mathbb{T}(0,0)$, $\mathbf{b} = \mathbb{T}(0,1)$, $\mathbf{c} = \mathbb{T}(1,0)$, and $\mathbf{d} = \mathbb{T}(1,1)$. Let $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ be the statistical distances corresponding to $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$.

Claim 1. *If protocol* π *is* $(1 - \varepsilon)$*-simulation secure against semi-honest adversaries, then the following inequalities hold.*

- $\varepsilon \geqslant 1/2 - \varepsilon_1/2$ *and* $\varepsilon \geqslant 1/2 - \varepsilon_2/2$
- $\varepsilon \geqslant \varepsilon_3/2$ *and* $\varepsilon \geqslant \varepsilon_4/2$.

Proof. Consider the case when the environment does not corrupt any party. We can, without loss of generality, assume that the party who sends the last message also sends the output.[4] This implies

[4] This assumption only reduces the accuracy error of a protocol.

that the output of the protocol is a deterministic function of the transcript. Note that $\mathbf{a}$ is the distribution of transcripts when the actual output $z = \mathsf{OR}(x, y) = 0$, and $\mathbf{b}$ is the distribution of transcript when the actual output $z = \mathsf{OR}(x, y) = 1$. Therefore, the output of the protocol can agree with the actual output z with probability at most $1/2 + \varepsilon_1/2$. That is, the accuracy error is at least $1/2 - \varepsilon_1/2$. So, we have $\varepsilon \geqslant 1/2 - \varepsilon_1/2$. Similarly, we also have $\varepsilon \geqslant 1/2 - \varepsilon_2/2$.

Consider the case when the environment corrupts Alice and sets her private input bit $x = 1$. In this case, $z = 1$. Let $\mathsf{Sim}_A(x, z)$ be the distribution of transcripts generated by Alice's simulator. We know that $\mathrm{SD}(\mathbf{c}, \mathbf{d}) = \varepsilon_3$. So, by triangle inequality, $\mathrm{SD}(\mathbf{c}, \mathsf{Sim}_A(x, z)) \geqslant \varepsilon_3/2$ or $\mathrm{SD}(\mathsf{Sim}_A(x, z), \mathbf{d}) \geqslant \varepsilon_3/2$. Therefore, the simulation error $\varepsilon \geqslant \varepsilon_3/2$. Similarly, by considering an environment that corrupts Bob and sets his private input bit $y = 1$, we get $\varepsilon \geqslant \varepsilon_4/2$. □

Claim 1, therefore, reduces the objective of minimizing the simulation error ε to minimizing the $\max\{1/2 - \varepsilon_1/2, 1/2 - \varepsilon_2/2, \varepsilon_3/2, \varepsilon_4/2\}$.

4 Limits on Semi-honest Security

Consider the four-tuple of probabilities $\left(\begin{smallmatrix}\mathbf{a} & \mathbf{b}\\ \mathbf{c} & \mathbf{d}\end{smallmatrix}\right)$, where $\mathbf{a}$ =$\mathbb{T}$ (0,0), $\mathbf{b}$ =$\mathbb{T}$ (0,1), $\mathbf{c}$ =$\mathbb{T}$ (1,0), and $\mathbf{d}$ =$\mathbb{T}$ (1,1).

Claim 2. *The four-tuple of probabilities* $\left(\begin{smallmatrix}\mathbf{a} & \mathbf{b}\\ \mathbf{c} & \mathbf{d}\end{smallmatrix}\right)$ *satisfy the cross-product rule.*

Claim 2 is a fairly standard result. We include a proof outline. In any protocol, the message m sent by a party P in a round is solely determined by the view V_P of the party. In the information-theoretic plain model, this implies the Markov chain $V_{\overline{P}} \to V_P \to m$, where $V_{\overline{P}}$ is the view of the other party. This property entails the cross-product rule.

Claim 1 indicates that to minimize the simulation error ε, one should minimize ε_3 and ε_4, while simultaneously increasing ε_1 and ε_2. Since $\mathbf{a}, \mathbf{b}, \mathbf{c}$, and $\mathbf{d}$ satisfy the cross-product rule (by Claim 2), there are limits to this optimization. Lemma 1 tightly characterizes this tradeoff between accuracy and privacy error.

Lemma 1 (Technical Result: Semi-honest)**.** *Let* $\mathbf{a}, \mathbf{b}, \mathbf{c}$, *and* $\mathbf{d}$ *be a four-tuple of probabilities that satisfy the cross-product rule. Let* $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ *be the statistical distances corresponding to* $\left(\begin{smallmatrix}\mathbf{a} & \mathbf{b}\\ \mathbf{c} & \mathbf{d}\end{smallmatrix}\right)$. *For all* $\varepsilon_3, \varepsilon_4$, *we have*

$$\varepsilon_1, \varepsilon_2 \leqslant \min\{\varepsilon_3 + \varepsilon_4, 1\}$$

Furthermore, for all $\varepsilon_3, \varepsilon_4$, *there exists a protocol whose transcript distribution achieves* $\varepsilon_1 = \varepsilon_2 = \min\{\varepsilon_3 + \varepsilon_4, 1\}$, *and it produces 6 distinct transcripts.*

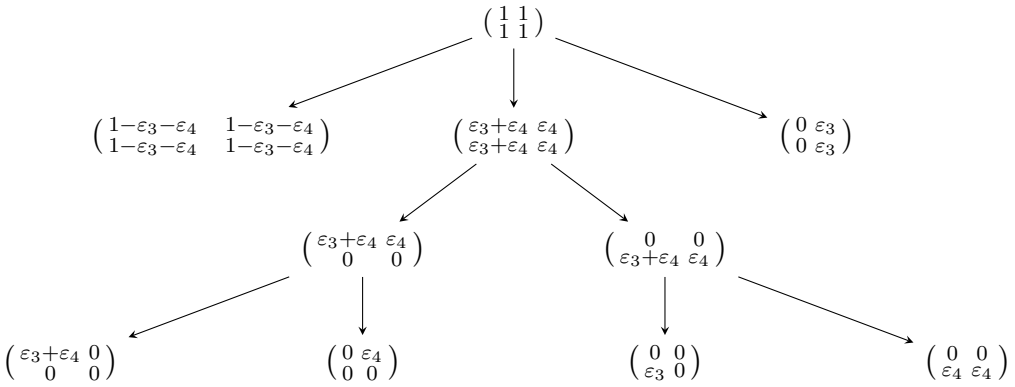
First, we remark that, for every fixing of ε_3 and ε_4, there is one distribution that *simultaneously* achieves the maximum possible ε_1 and ε_2. Figure 3 provides these distributions for both $\varepsilon_3 + \varepsilon_4 \leqslant 1$ and $\varepsilon_3 + \varepsilon_4 > 1$.

Intuitively, Lemma 1 states that if ε_3 and ε_4 are small, i.e. the protocol has low privacy error, then ε_1 and ε_2 are also small, i.e. the protocol has high accuracy error. Note that Claim 1 and Lemma 1 directly yields Theorem 1, by substituting $\varepsilon_1 = \varepsilon_2 = 2/3$ and $\varepsilon_3 = \varepsilon_4 = 1/3$.

4.1 Proof Outline of Lemma 1

The full proof of Lemma 1 is provided in Appendix A. The main contribution of this paper is the general technique that assists in obtaining such tight inequalities. We emphasize the salient features below. At a high level, our proof proceeds in three steps. Fix the values of ε_3 and ε_4.

Tight Protocol for $\varepsilon_3 + \varepsilon_4 \leqslant 1$



Tight Protocol for $\varepsilon_3 + \varepsilon_4 > 1$

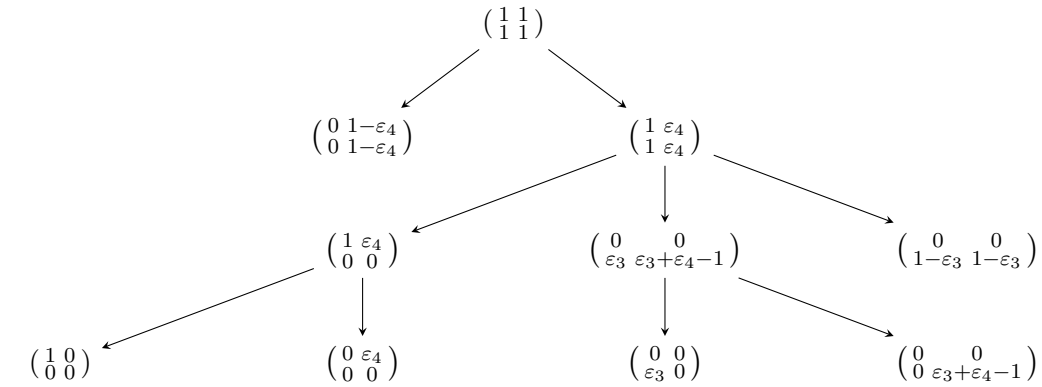


Figure 3: Three-round two-party protocols that have transcript distribution identical to the distribution that shows $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 + \varepsilon_4$. The top protocol is the for the case $\varepsilon_3 + \varepsilon_4 \leqslant 1$ and the bottom protocol is for the case $\varepsilon_3 + \varepsilon_4 > 1$.

1. **Reduction to Templates.** This step shows that the distributions $\mathbb{T}(x, y)$, for $x \in \{0,1\}$ and $y \in \{0,1\}$, that maximizes ε_1 or ε_2 has a *canonical form*. Let τ be any transcript generated by a protocol π that maximizes ε_1 or ε_2. Then the four-tuple of probabilities $\begin{pmatrix} \Pr[\mathbb{T}(0,0)=\tau] & \Pr[\mathbb{T}(0,1)=\tau] \\ \Pr[\mathbb{T}(1,0)=\tau] & \Pr[\mathbb{T}(1,1)=\tau] \end{pmatrix}$ can be partitioned into a *few* equivalence classes, namely the *templates*.

   For instance, in this particular case, there are nine different templates.

   (a) Type-0 Template. If there exists x such that the i-th cross-section is identical to $\left(\begin{smallmatrix} x & x \\ x & x \end{smallmatrix}\right)$

   (b) Type-2 Templates. If there exists x such that the i-th cross-section is identical to $\left(\begin{smallmatrix} x & x \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & x \\ 0 & x \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ x & x \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} x & 0 \\ x & 0 \end{smallmatrix}\right)$

   (c) Type-3 Templates. If there exists x such that the i-th cross-section is identical to $\left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ x & 0 \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} 0 & 0 \\ 0 & x \end{smallmatrix}\right)$

   Note that suboptimal four-tuple of distributions need not necessarily have template cross-sections.

2. **Reduction to a Constant Size Problem.** This step shows that if for every transcript τ the four-tuple $\begin{pmatrix} \Pr[\mathbb{T}(0,0)=\tau] & \Pr[\mathbb{T}(0,1)=\tau] \\ \Pr[\mathbb{T}(1,0)=\tau] & \Pr[\mathbb{T}(1,1)=\tau] \end{pmatrix}$ is a template then there exists a *constant-size protocol* that achieves identical ε_1, ε_2, ε_3, and ε_4. Intuitively, all cross-sections that have identical template can be merged into one cross-section. In particular, we show that there are optimal distributions that have at most nine possible transcripts.

3. **Obtaining the Maximum-achievable ε_1 and ε_2.** Finally, solving an appropriate constant-size *linear program* yields the optimal solution. In the linear program, we introduce one variable for each template. Next, linear constraints are set up to encode the fact that $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, and $\mathbf{d}$ are probability distributions with fixed ε_3 and ε_4. Under these constraints, we maximize ε_1 and ε_2 to obtain their respective upper-bounds.

The proof of our technical result (Lemma 3) that considers differentially private semi-honest protocols particularly highlights the potential of this approach.

4.2 Round Optimality

Lemma 2 (Technical Result: Semi-honest Round Optimality)**.** *Let π be a 2-party* OR *evaluation protocol with at most 2-rounds, where Alice sends the first message. Let $\mathbb{T}(x, y)$, for $x, y \in \{0,1\}$, represent the transcript distribution of the protocol π when Alice and Bob have private inputs x and y, respectively. Let $\mathbf{a} = \mathbb{T}(0,0)$, $\mathbf{b} = \mathbb{T}(0,1)$, $\mathbf{c} = \mathbb{T}(1,0)$, and $\mathbf{d} = \mathbb{T}(1,1)$ and $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ be the statistical distances corresponding to $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$. For all $\varepsilon_3, \varepsilon_4$, we have*

$$\varepsilon_2 = \varepsilon_4 \text{ and } \varepsilon_1 \leqslant \varepsilon_3 + \varepsilon_4$$

Intuitively, the message in the first round by Alice divulges information about her private input bit x that is independent of Bob's private input bit y. The second message by Bob cannot reveal any additional information about x. Therefore, we have $\varepsilon_2 = \varepsilon_4$. Lemma 1 already yields $\varepsilon_1 \leqslant \varepsilon_3 + \varepsilon_4$. The proof of this lemma is provided in Appendix B and the tight protocol is presented in Figure 5.

Lemma 2 directly yields Theorem 2, by substituting $\varepsilon_3 = \varepsilon_4 = 1/2$, and there exists a 2-round protocol that achieves the maximum possible simulation security for this case.

5 Differentially Private Semi-honest Security

Definition 4 (Θ-Close)**.** *For $\Theta > 1$, we say that the cross-section $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is Θ-close if the ratios $a/b, b/d, d/c, c/a \in [1/\Theta, \Theta]$.*

Similar to Lemma 1 we prove the following result for differentially-private semi-honest secure protocols.

Lemma 3 (Technical Result: Differentially Private Semi-honest)**.** *Let $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, and $\mathbf{d}$ be a four-tuple of probabilities that satisfy the cross-product rule. Let $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ be the statistical distances corresponding to $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$. Suppose there exists some $\Theta > 1$ such that every cross-section of $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$ is Θ-close. Suppose $\varepsilon_3/\varepsilon_4 \in [1/(\Theta+1), \Theta+1]$. Then we have:*

1. *If $(\varepsilon_3 + \varepsilon_4) + \varepsilon_3/\Theta \leqslant 1 - 1/\Theta$, then*

$$\varepsilon_1 \leqslant (\varepsilon_3 + \varepsilon_4) - \frac{2}{\Theta + 1}\varepsilon_4,$$

2. *If $(\varepsilon_3 + \varepsilon_4) + \varepsilon_4/\Theta \leqslant 1 - 1/\Theta$, then*

$$\varepsilon_2 \leqslant (\varepsilon_3 + \varepsilon_4) - \frac{2}{\Theta + 1}\varepsilon_3, \text{ and}$$

3. *If $\varepsilon_1 = \varepsilon_2$, $\varepsilon_3 = \varepsilon_4 = \varepsilon$ and $\varepsilon_3 + \varepsilon_4 \leqslant \frac{\Theta-1}{\Theta+1}$, then*

$$\varepsilon_1 = \varepsilon_2 \leqslant 2\varepsilon - \frac{3}{\Theta + 2}\varepsilon$$

Furthermore, for every $\varepsilon_3, \varepsilon_4$ and each of the inequality above, there exists a protocol whose transcript distribution achieves the equality, and it produces 6 distinct transcripts.

Recall that for Lemma 1 there is one protocol that simultaneously maximizes both ε_1 and ε_2. However, in the differentially private semi-honest security setting, optimizing ε_1 and ε_2 individually, and under the the restriction that $\varepsilon_1 = \varepsilon_2$ yields different upper bounds. The full proof of this lemma is provided in Appendix C and the tight protocol is provided in Figure 9.

Note that Claim 1 and Lemma 3 (part 3) directly yields Theorem 3, by setting $\varepsilon = (\Theta+2)/3(\Theta+1)$.

The proof outline is similar to that of Lemma 1. The nine templates used in this proof are $\left(\begin{smallmatrix} x & x \\ x & x \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} x & x \\ x/\Theta & x/\Theta \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} x & x/\Theta \\ x/\Theta & x/\Theta^2 \end{smallmatrix}\right)$ (with the corresponding rotations). To prove this lemma, we solve an appropriate 9-variable linear program, which is slightly more involved as compared to the corresponding one in Lemma 1.

We illustrate the solution space of the linear program in Figure 4, where $\varepsilon_3 = \varepsilon_4 = 1/3$ and $\Theta = 5$. We emphasize a subtlety. For every fixing of ε_3 and ε_4 the points P_1 is a 2-round protocol where Alice sends the first message, P_2 is a 2-round protocol where Bob sends the first message, and P_3 is a 3-round protocol that additionally constrains $\varepsilon_1 = \varepsilon_2$. But the choice of ε_3 and ε_4 that yields the optimally secure 3-round protocol is different from the choice of ε_3 and ε_4 that yields the optimally secure 2-round protocols.

Lemma 4 (Technical Result: Differentially Private Semi-honest Round Optimal)**.** *For $\Theta > 1$, let ρ be a Θ-differentially private 2-party OR evaluation protocol with at most 2-rounds, where Alice sends the first message. Let $\mathbb{T}(x, y)$, for $x, y \in \{0, 1\}$, represent the transcript distribution of the protocol ρ when Alice and Bob has private inputs x and y, respectively. Let $\mathbf{a} = \mathbb{T}(0, 0)$, $\mathbf{b} = \mathbb{T}(0, 1)$,*

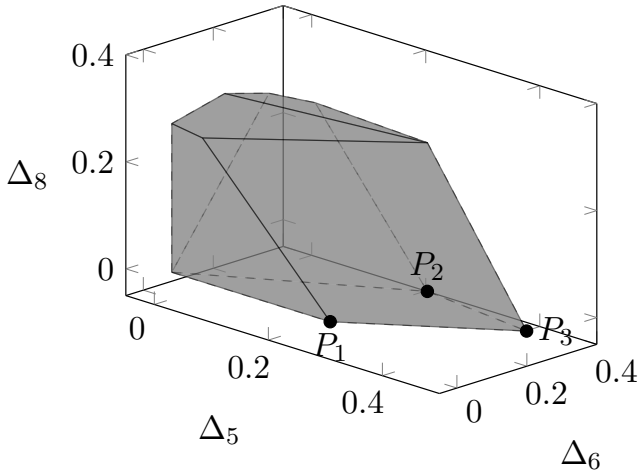


Figure 4: The convex polytope of all feasible solutions for $\varepsilon_3 = \varepsilon_4 = 1/3$ and $\Theta = 5$. The point P_1, P_2, and P_3 correspond to the solutions that achieve the equalities in part (1), (2), and (3) in Lemma 3. The variables are explained in Appendix C.1.

$\mathbf{c} = \mathbb{T}(1,0)$, *and* $\mathbf{d} = \mathbb{T}(1,1)$ *and* $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ *be the statistical distances corresponding to* $\left(\begin{smallmatrix}\mathbf{a} & \mathbf{b}\\ \mathbf{c} & \mathbf{d}\end{smallmatrix}\right)$. *Suppose* $\varepsilon_3/\varepsilon_4 \in [1/(\Theta+1), \Theta+1]$. *For all* $\varepsilon_3, \varepsilon_4$ *such that* $(\varepsilon_3+\varepsilon_4)+\varepsilon_3/\Theta \leqslant 1 - 1/\Theta$, *we have*

$$\varepsilon_2 = \varepsilon_4 \text{ and } \varepsilon_1 \leqslant (\varepsilon_3+\varepsilon_4) - \frac{2}{\Theta+1}\varepsilon_4$$

Note that this is identical to the bound obtained in Lemma 3 part 1. The full proof of this result is provided in Appendix D and the tight protocol is provided in Figure 8.

For $\Theta \geqslant 4$, the choice of $\varepsilon_3 = (\Theta-2)/2(\Theta+1)$ and $\varepsilon_4 = 1/2$ is a feasible solution, and this choice has simulation error at least $1/4$. Moreover, there exists a 2-round protocol that achieves $1/4$ simulation error. For $1 < \Theta < 4$, the simulation error of a two-round protocol is $3/2(\Theta+2)$.

6 Conclusions and Open Problems

The main technical contribution of our work is to express the transcript distributions of the "optimal solution" to a cryptographic problem as a convex linear combination of a few custom-designed templates. This step reduces the complexity of the problem to a constant size that can potentially be solved by brute force techniques. These techniques can serve as a stepping-stone to explore the optimal semi-honest secure protocols for any un-decomposable function [Kus89, Bea89]. Further, this technique is a potential approach for the long standing open problem of characterizing 2-party *randomized* secure function evaluations that can be semi-honest securely evaluated in the information-theoretic plain model.

Acknowledgements

The research effort is supported in part by an NSF CRII Award CNS–1566499 and an NSF SMALL Award CNS–1618822.

References

[Bea89] Donald Beaver. Perfect privacy for two-party protocols. In Joan Feigenbaum and Michael Merritt, editors, *Proceedings of DIMACS Workshop on Distributed Computing and Cryptography*, volume 2, pages 65–77. American Mathematical Society, 1989. 1, 3, 9

[Can00] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000. 2

[Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In Juris Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 364–369. ACM, 1986. 3

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In *34th Annual ACM Symposium on Theory of Computing*, pages 494–503, Montréal, Québec, Canada, May 19–21, 2002. ACM Press. 3

[Dol82] Danny Dolev. The byzantine generals strike again. *J. Algorithms*, 3(1):14–30, 1982. 1, 3

[GHKL08] S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete fairness in secure two-party computation. In Richard E. Ladner and Cynthia Dwork, editors, *40th Annual ACM Symposium on Theory of Computing*, pages 413–422, Victoria, British Columbia, Canada, May 17–20, 2008. ACM Press. 3

[GMPS13] Vipul Goyal, Ilya Mironov, Omkant Pandey, and Amit Sahai. Accuracy-privacy tradeoffs for two-party differentially private protocols. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 298–315, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany. 2, 3

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, NY, USA, May 25–27, 1987. ACM Press. 1

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th Annual Symposium on Foundations of Computer Science*, pages 230–235, Research Triangle Park, North Carolina, October 30 – November 1, 1989. IEEE Computer Society Press. 1, 3

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing*, pages 20–31, Chicago, IL, USA, May 2–4, 1988. ACM Press. 1, 3

[KMQR09] Robin Künzler, Jörn Müller-Quade, and Dominik Raub. Secure computability of functions in the IT setting with dishonest majority and applications to long-term security.

In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 238–255. Springer, Heidelberg, Germany, March 15–17, 2009. 1, 3

[Kus89] Eyal Kushilevitz. Privacy and communication complexity. In *30th Annual Symposium on Foundations of Computer Science*, pages 416–421, Research Triangle Park, North Carolina, October 30 – November 1, 1989. IEEE Computer Society Press. 1, 3, 9

[Lin03] Yehuda Lindell. Bounded-concurrent secure two-party computation without setup assumptions. In *35th Annual ACM Symposium on Theory of Computing*, pages 683–692, San Diego, CA, USA, June 9–11, 2003. ACM Press. 3

[MPR09] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In Omer Reingold, editor, *TCC 2009: 6th Theory of Cryptography Conference*, volume 5444 of *Lecture Notes in Computer Science*, pages 256–273. Springer, Heidelberg, Germany, March 15–17, 2009. 1, 3

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science*, pages 160–164, Chicago, Illinois, November 3–5, 1982. IEEE Computer Society Press. 1

A Proof of Lemma 1

In this section we prove the result for $\varepsilon_3 + \varepsilon_4 \leqslant 1$. To prove Lemma 1 it will be useful to introduce the following terminology. We identify nine special types of cross-sections that are formally defined below.

Type-0 Template. If there exists x such that the i-th cross-section is identical to $\left(\begin{smallmatrix} x & x \\ x & x \end{smallmatrix}\right)$ then we say that the i-th cross-section is a *type-0 template*.

Type-2 Templates. If there exists x such that the i-th cross-section is identical to $\left(\begin{smallmatrix} x & x \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & x \\ 0 & x \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ x & x \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} x & 0 \\ x & 0 \end{smallmatrix}\right)$ then we say that the i-th cross-section is a *type-2n*, *type-2e*, *type-2s*, or *type-2w* template, respectively. The letters refer to the cardinal direction associated with the nonzero elements.

Type-3 Templates. If there exists x such that the i-th cross-section is identical to $\left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ x & 0 \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} 0 & 0 \\ 0 & x \end{smallmatrix}\right)$ then we say that the i-th cross-section is a *type-3a*, *type-3b*, *type-3c*, or *type-3d* template, respectively.

Remark: The nine templates are defined based on the number of 0s in the cross-section. That is, all type-$k*$ templates have exactly k 0s in the cross-section, where $k \in \{0, 2, 3\}$.

First, we shall show the following claim.

Claim 3 (Reduction to Templates)**.** *Let* $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, *and* $\mathbf{d}$ *be a four-tuple of probabilities over the sample space* Ω *that satisfy the cross-product rule. Let* $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ *be the statistical distances corresponding to* $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$*. Then, there exists a four-tuple of probabilities* $\mathbf{a}'$, $\mathbf{b}'$, $\mathbf{c}'$, *and* $\mathbf{d}'$ *over the sample space* Ω' *such that:*

1. $(\varepsilon'_1, \varepsilon'_2, \varepsilon'_3, \varepsilon'_4)$ *are the statistical distances corresponding to* $\left(\begin{smallmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{smallmatrix}\right)$,
2. $\varepsilon'_3 = \varepsilon_3$, $\varepsilon'_4 = \varepsilon_4$,
3. $\varepsilon'_1 \geqslant \varepsilon_1$, $\varepsilon'_2 \geqslant \varepsilon_2$, *and*
4. *Each cross-section of* $\left(\begin{smallmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{smallmatrix}\right)$ *is a template.*

The proof of Claim 3 is provided in Appendix A.1.

Given Claim 3, it suffices to prove the inequality for four-tuple of distributions such that each of their cross-section is a template. Next, we shall show the following claim.

Claim 4 (Reduction of Templates to a Small Sample Space)**.** *Let* $\mathbf{a}', \mathbf{b}', \mathbf{c}'$, *and* $\mathbf{d}'$ *be a four-tuple of probabilities over the sample space* Ω' *such that, for each* $i \in \Omega'$*, the* i*-th cross-section of* $\left(\begin{smallmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{smallmatrix}\right)$ *is a template. Let* $(\varepsilon'_1, \varepsilon'_2, \varepsilon'_3, \varepsilon'_4)$ *be the statistical distances corresponding to* $\left(\begin{smallmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{smallmatrix}\right)$*. Then, there exists a four-tuple of probabilities* $\mathbf{a}'', \mathbf{b}'', \mathbf{c}''$, *and* $\mathbf{d}''$ *over the sample space* $\Omega'' = \{0, 2n, 2e, 2s, 2w, 3a, 3b, 3c, 3d\}$ *such that:*

1. $(\varepsilon''_1, \varepsilon''_2, \varepsilon''_3, \varepsilon''_4)$ *are the statistical distances corresponding to* $\left(\begin{smallmatrix} \mathbf{a}'' & \mathbf{b}'' \\ \mathbf{c}'' & \mathbf{d}'' \end{smallmatrix}\right)$,
2. $\varepsilon''_1 = \varepsilon'_1$, $\varepsilon''_2 = \varepsilon'_2$, $\varepsilon''_3 = \varepsilon'_3$, $\varepsilon''_4 = \varepsilon'_4$, *and*
3. *For every* $i \in \Omega''$*, the* i*-th cross-section of* $\left(\begin{smallmatrix} \mathbf{a}'' & \mathbf{b}'' \\ \mathbf{c}'' & \mathbf{d}'' \end{smallmatrix}\right)$ *is a type-*i *template.*

The proof of Claim 4 is provided in Appendix A.2.

Because of Claim 4, it suffices to prove the inequality only for four-tuple of distributions over $\Omega = \{0, 2n, 2e, 2s, 2w, 3a, 3b, 3c, 3d\}$ such that its i-th cross-section is type-i template, for $i \in \Omega$. Note that $\sum_i a_i = \sum_i b_i = 1$, so $\sum_i a_i - b_i = \sum_{a_i > b_i} (a_i - b_i) + \sum_{a_i < b_i} (a_i - b_i) = 0$. Therefore

$$\sum_{a_i > b_i} (a_i - b_i) = \sum_{a_i < b_i} (b_i - a_i)$$

Which allows us to conclude that

$$\varepsilon_1 = \mathrm{SD}\,(\mathbf{a}, \mathbf{b}) = \frac{1}{2} \sum_{i \in \Omega} |a_i - b_i| = \frac{1}{2} \sum_{b_i > a_i} 2(b_i - a_i) = \sum_{i \in \Omega \colon b_i > a_i} (b_i - a_i)$$

Of the nine templates, the only two that satisfy $b_i > a_i$ are: $\left(\begin{smallmatrix} 0 & x \\ 0 & x \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right)$. In these two templates $a_i = 0$. So, we have the following equation:

$$\varepsilon_1 = \sum_{i \in \Omega \colon b_i > a_i} (b_i - a_i) = \sum_{i \in \Omega \colon b_i > a_i} b_i$$

Since $b_i > a_i$ only allows for templates 2e and 1b, we can expand the summation above to a sum of sums over those two templates. In the template 2e, we have $d_i > c_i$ and in the template 1b, we have $b_i > d_i$. Then, we can relax the requirement that $b_i > a_i$ to transform the equation into an upper bound.

$$\begin{aligned} \varepsilon_1 &= \sum_{\substack{i \in \Omega \colon \\ \begin{smallmatrix} b_i > a_i \\ d_i > c_i \end{smallmatrix}}} (d_i - c_i) + \sum_{\substack{i \in \Omega \colon \\ \begin{smallmatrix} b_i > a_i \\ b_i > d_i \end{smallmatrix}}} (b_i - d_i) \\ &\leqslant \sum_{i \in \Omega \colon d_i > c_i} (d_i - c_i) + \sum_{i \in \Omega \colon b_i > d_i} (b_i - d_i) \\ &= \varepsilon_3 + \varepsilon_4 \end{aligned}$$

Equality holds if and only if the templates $\left(\begin{smallmatrix} 0 & 0 \\ 0 & x \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x & x \\ 0 & 0 \end{smallmatrix}\right)$ have 0 probability.

Analogously, we can prove that $\varepsilon_2 \leqslant \varepsilon_3 + \varepsilon_4$. Equality holds if and only if the templates $\left(\begin{smallmatrix} 0 & 0 \\ 0 & x \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x & 0 \\ x & 0 \end{smallmatrix}\right)$ have 0 probability.

Therefore, equality holds in both the inequalities if and only if $\left(\begin{smallmatrix} 0 & 0 \\ 0 & x \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} x & x \\ 0 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} x & 0 \\ x & 0 \end{smallmatrix}\right)$ have 0 probability. See the construction below Lemma 1 for a protocol transcript distribution that achieves equality for both these equations (the protocol is provided in Figure 3).

A.1 Proof of Claim 3

We begin by creating $\mathbf{a}' = \mathbf{a}$, $\mathbf{b}' = \mathbf{b}$, $\mathbf{c}' = \mathbf{c}$, and $\mathbf{d}' = \mathbf{d}$. For every cross-section that is not a template, we replace it by a set of four appropriately chosen templates such that the ε_3 and ε_4 remains same but both ε_1 and ε_2 do not decrease.

For each $i \in \Omega$ such that the i-th cross-section $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ of $\left(\begin{smallmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{smallmatrix}\right)$ is not a template. We consider the following exhaustive case analysis to modify $\mathbf{a}'$, $\mathbf{b}'$, $\mathbf{c}'$, and $\mathbf{d}'$.

Case 1: a_i is the minimum. If a_i is minimum then d_i is the maximum, since $a_i \cdot d_i = b_i \cdot c_i$. We can assume that $d_i > 0$, otherwise $a_i = b_i = c_i = d_i = 0$. Further, since $a_i \cdot d_i = b_i \cdot c_i$, we can re-write a_i, b_i, and c_i as follows:

$$\begin{aligned} a_i &= d_i - (d_i - b_i) - (d_i - c_i) + \frac{(d_i - b_i)(d_i - c_i)}{d_i} \\ b_i &= d_i - (d_i - b_i) \\ c_i &= d_i - (d_i - c_i) \end{aligned}$$

Consider the following exhaustive case analysis on the value of $d_i - (d_i - b_i) - (d_i - c_i)$.
Case 1.A: $d_i - (d_i - b_i) - (d_i - c_i) \geqslant 0$. We replace the cross-section $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ with the following four cross-sections.

$$\left(\begin{smallmatrix} d_i-(d_i-b_i)-(d_i-c_i) & d_i-(d_i-b_i)-(d_i-c_i) \\ d_i-(d_i-b_i)-(d_i-c_i) & d_i-(d_i-b_i)-(d_i-c_i) \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & d_i-c_i \\ 0 & d_i-c_i \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & 0 \\ d_i-b_i & d_i-b_i \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} \frac{(d_i-b_i)(d_i-c_i)}{d_i} & 0 \\ 0 & 0 \end{smallmatrix}\right)$$

Observe that each entry mentioned above in $\geqslant 0$ (because $d_i - b_i \geqslant 0$ and $d_i - c_i \geqslant 0$). Note that this replacement keeps ε_3 and ε_4 identical. And, ε_1 increases by

$$\begin{aligned} (d_i - c_i) + \frac{(d_i - b_i)(d_i - c_i)}{d_i} - (b_i - a_i) &= (d_i - c_i) + \frac{(d_i - b_i)(d_i - c_i)}{d_i} - (d_i - c_i) + \frac{(d_i - b_i)(d_i - c_i)}{d_i} \\ &= 2\frac{(d_i - b_i)(d_i - c_i)}{d_i} \geqslant 0 \end{aligned}$$

Similarly, ε_2 increases by

$$\begin{aligned} (d_i - b_i) + \frac{(d_i - b_i)(d_i - c_i)}{d_i} - (c_i - a_i) &= (d_i - b_i) + \frac{(d_i - b_i)(d_i - c_i)}{d_i} - (d_i - b_i) + \frac{(d_i - b_i)(d_i - c_i)}{d_i} \\ &= 2\frac{(d_i - b_i)(d_i - c_i)}{d_i} \geqslant 0 \end{aligned}$$

Case 1.B: $d_i - (d_i - b_i) - (d_i - c_i) < 0$. This is equivalent to $d_i > b_i + c_i$. We replace the cross-section $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ with the following four cross-sections.

$$\left(\begin{smallmatrix} 0 & b_i \\ 0 & b_i \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & 0 \\ c_i & c_i \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} a_i & 0 \\ 0 & 0 \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & 0 \\ 0 & d_i-b_i-c_i \end{smallmatrix}\right)$$

Observe that each entry mentioned above is $\geqslant 0$. Note that the replacement keeps ε_3 and ε_4 identical. And, ε_1 increases by $a_i + b_i - (b_i - a_i) = 2a_i \geqslant 0$. Similarly, ε_2 increases by $a_i + c_i - (c_i - a_i) = 2a_i \geqslant 0$.

Case 2: b_i is the minimum. We replace the cross-section $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ with the following four cross-sections.

$$\left(\begin{smallmatrix} b_i & b_i \\ b_i & b_i \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & 0 \\ d_i-b_i & d_i-b_i \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} a_i-b_i & 0 \\ 0 & 0 \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & 0 \\ c_i-d_i & 0 \end{smallmatrix}\right)$$

Observe that each entry mentioned above is $\geqslant 0$ (because if b_i is minimum then c_i is the maximum). Note that this replacement keeps ε_1, ε_3 and ε_4 identical. And, ε_2 increases by $(d_i - b_i) + (a_i - b_i) + (c_i - d_i) - (c_i - a_i) = 2(a_i - b_i) \geqslant 0$.

Case 3: c_i is the minimum. This case is analogous to the case when b_i is the minimum.

Case 4: d_i is the minimum. We replace the cross-section $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ with the following four cross-sections.

$$\left(\begin{smallmatrix} d_i & d_i \\ d_i & d_i \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} a_i-d_i & 0 \\ 0 & 0 \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & b_i-d_i \\ 0 & 0 \end{smallmatrix}\right) \qquad \left(\begin{smallmatrix} 0 & 0 \\ c_i-d_i & 0 \end{smallmatrix}\right)$$

Observe that each entry mentioned above is $\geqslant 0$ (because if d_i is the minimum then a_i is the maximum). Note that this replacement keep ε_3 and ε_4 identical. And, ε_1 increases by $(a_i - d_i) + (b_i - d_i) - (a_i - b_i) = 2(b_i - d_i) \geqslant 0$. And, ε_2 increases by $(a_i - d_i) + (c_i - d_i) - (a_i - c_i) = 2(c_i - d_i) \geqslant 0$.

For all replacement, the resultant four-tuple of distributions $\mathbf{a}'$, $\mathbf{b}'$, $\mathbf{c}'$, and $\mathbf{d}'$ satisfy the requirements of Claim 3.

A.2 Proof of Claim 4

Intuitively, we argue the following. Suppose there exists distinct i and j such that the i-th and the j-th cross-sections of $\left(\begin{smallmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{smallmatrix}\right)$ have type-k template, where $k \in \{0, 2n, 2e, 2s, 2w, 3a, 3b, 3c, 3d\}$. We can replace these two cross-sections by one cross-section of type-k that is the sum of these two cross-sections. This operation preserves their statistical distances. Repetitive application of this step provides us with the construction of $\mathbf{a}''$, $\mathbf{b}''$, $\mathbf{c}''$, and $\mathbf{d}''$ that satisfy Claim 4.

More formally, let $\mathbf{a}', \mathbf{b}', \mathbf{c}'$, and $\mathbf{d}'$ be distributions over the sample space $\Omega' = [n']$ such that for all $i \in \Omega'$, the cross section of $(\mathbf{a}', \mathbf{b}', \mathbf{c}', \mathbf{d}')$ at i both satisfies the cross-product rule and is a template.

If there exists i and j in Ω' such that the cross section of $(\mathbf{a}', \mathbf{b}', \mathbf{c}', \mathbf{d}')$ at i and j are of the same template type and rotation, then there exists $\Omega'' = [n' - 1]$ and $(\mathbf{a}'', \mathbf{b}'', \mathbf{c}'', \mathbf{d}'')$ that satisfies the cross product rule, only uses templates, and is also SD Equivalent to $(\mathbf{a}', \mathbf{b}', \mathbf{c}', \mathbf{d}')$.

We construct $\mathbf{a}'', \mathbf{b}'', \mathbf{c}''$, and $\mathbf{d}''$ by using the exact same cross sections from $\mathbf{a}', \mathbf{b}', \mathbf{c}'$, and $\mathbf{d}'$, but without indices i and j. We then insert one cross section, which is the sum of the cross sections at i and j. To show correctness, there are three fundamental cases to consider here, depending on the type of cross section $(\mathbf{a}'', \mathbf{b}'', \mathbf{c}'', \mathbf{d}'')$ has at index i.

Since each cross section has a single nonzero value, we can let k and l represent the nonzero values for the two cross sections at hand.

Case 1: Type One Template The following substitution visibly does not change any of the epsilon values and maintains the integrity of the probability distribution.

$$\left(\begin{smallmatrix} k & k \\ k & k \end{smallmatrix}\right) \left(\begin{smallmatrix} l & l \\ l & l \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} k+l & k+l \\ k+l & k+l \end{smallmatrix}\right)$$

Case 2: Type Two Template Like the case above, we can easily preserve the required properties.

$$\left(\begin{smallmatrix} k & k \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} l & l \\ 0 & 0 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} k+l & k+l \\ 0 & 0 \end{smallmatrix}\right)$$

Case 3: Type Three Template Again, simply writing out the cross sections shows the correctness of the substitution.

$$\left(\begin{smallmatrix} k & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} l & 0 \\ 0 & 0 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} k+l & 0 \\ 0 & 0 \end{smallmatrix}\right)$$

The rotations of the type two and three templates follow the same principles. Hence, all three possible templates and all rotations can be reduced from two cross sections to one without any impact on the ε-Distances. Thus, we provide a size $n' - 1$ probability distribution that upholds all required properties, completing the proof.

Iteratively applying this procedure, we reduce the number of cross-sections to 9.

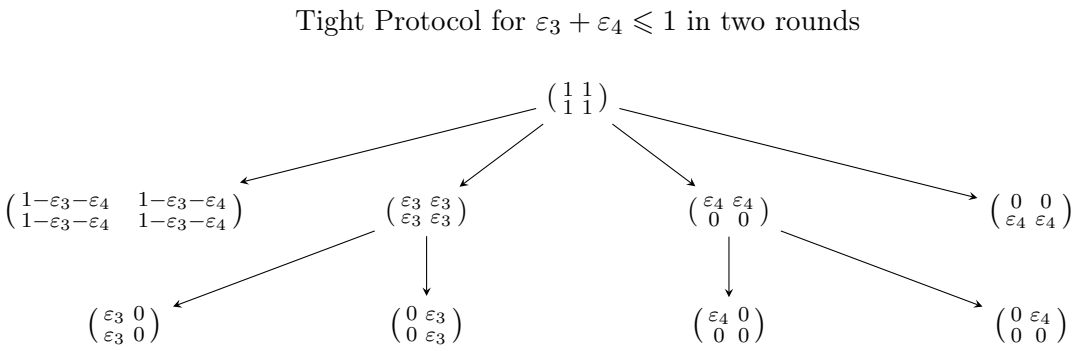


Figure 5: Two-round two-party protocol where Alice sends the first message such that $\varepsilon_2 = \varepsilon_4$ and $\varepsilon_1 = \varepsilon_3 + \varepsilon_4$.

B Proof of Lemma 2

In this section, we use the notion introduced in Appendix E. Note that we only need to prove that $\varepsilon_2 = \varepsilon_4$. We already know that $\varepsilon_1 \leqslant \varepsilon_3 + \varepsilon_4$ by Lemma 1.

Suppose Alice sends a message i in the first round. She sends i with probability p_i if her input is $x = 0$; otherwise, if her input is $x = 1$, she sends i with probability q_i.

Note that the four-tuple of probability corresponding to the empty transcript is $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.

The four tuple of probability corresponding to the partial transcript i is $\left(\begin{smallmatrix} p_i & p_i \\ q_i & q_i \end{smallmatrix}\right)$.

Conditioned on the first message being i, suppose Bob sends the message j with probability $p_{i,j}$ if his input is $y = 1$; otherwise, if his input is $y = 1$, he sends j with probability $q_{i,j}$.

Note that the four-tuple of probability corresponding to the complete transcript (i, j) is $\left(\begin{smallmatrix} p_i p_{i,j} & p_i q_{i,j} \\ q_i p_{i,j} & q_i q_{i,j} \end{smallmatrix}\right)$. Using the fact that, for every i, we have $\sum_j p_{i,j} = \sum_j q_{i,j} = 1$, consider the following manipulation.

$$\begin{aligned} \varepsilon_2 = \sum_{i,j} |p_i p_{i,j} - q_i p_{i,j}| &= \sum_i |p_i - q_i| \sum_j p_{i,j} \\ &= \sum_i |p_i - q_i| \\ &= \sum_i |p_i - q_i| \sum_j q_{i,j} \\ &= \sum_{i,j} |p_i q_{i,j} - q_i q_{i,j}| = \varepsilon_4 \end{aligned}$$

C Proof of Lemma 3

We identify 9 special types of cross-sections.

Type-0 Template. If there exists x such that the i-th template is identical to $\left(\begin{smallmatrix} x & x \\ x & x \end{smallmatrix}\right)$ then we say that the i-th cross-section is a *type-0 template*.

Type-2 Templates. If there exists x such that the i-th cross-section is identical to $\left(\begin{smallmatrix} x & x \\ x/\Theta & x/\Theta \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} x/\Theta & x \\ x/\Theta & x \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} x/\Theta & x/\Theta \\ x & x \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} x & x/\Theta \\ x & x/\Theta \end{smallmatrix}\right)$ then we say that the i-th cross-section is a *type-2n*, *type-2e*,

type-2s, or *type-2w* template respectively. The letters refer to the cardinal direction associated with the maximum elements.

Type-3 Templates. If there exists x such that the i-th cross-section is identical to $\begin{pmatrix} x & x/\Theta \\ x/\Theta & x/\Theta^2 \end{pmatrix}$, $\begin{pmatrix} x/\Theta & x \\ x/\Theta^2 & x/\Theta \end{pmatrix}$, $\begin{pmatrix} x/\Theta & x/\Theta^2 \\ x & x/\Theta \end{pmatrix}$, or $\begin{pmatrix} x/\Theta^2 & x/\Theta \\ x/\Theta & x \end{pmatrix}$ then we say that the i-th cross-section is a *type-3a*, *type-3b*, *type-3c*, or *type-3d* template respectively.

Claim 5 (Reduction to Templates)**.** *Let* $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, *and* $\mathbf{d}$ *be a four-tuple of probabilities over the sample space* Ω *that satisy the cross-product rule. Let* $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ *be the statistical distances corresponding to* $\mathbf{a}, \mathbf{b}, \mathbf{c}$, *and* $\mathbf{d}$*. Then, there exists a four-tuple of probabilities* $\mathbf{a}$*'*, $\mathbf{b}$*'*, $\mathbf{c}$*'*, *and* $\mathbf{d}$*' over the sample space* Ω' *such that:*

1. $(\varepsilon'_1, \varepsilon'_2, \varepsilon'_3, \varepsilon'_4)$ *are the statistical distances corresponding to* $\begin{pmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{pmatrix}$,
2. $\varepsilon'_i = \varepsilon_i$, *for all* $i \in \{1, 2, 3, 4\}$, *and*
3. *Each cross-section of* $\begin{pmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{pmatrix}$ *is a template.*

The proof of this claim is provided in Appendix C.2.

Given Claim 5, it suffices to prove the inequality for four-tuple of distributions such that each of their cross-section is a template. Next, we shall show the following claim.

Claim 6 (Reduction of Templates to a Small Sample Space)**.** *Let* $\mathbf{a}$*'*, $\mathbf{b}$*'*, $\mathbf{c}$*'*, *and* $\mathbf{d}$*' be a four-tuple of probabilities over the sample space* Ω' *such that, for each* $i \in \Omega'$*, the* i*-th cross-section of* $\begin{pmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{pmatrix}$ *is a template. Let* $(\varepsilon'_1, \varepsilon'_2, \varepsilon'_3, \varepsilon'_4)$ *be the statistical distances corresponding to* $\begin{pmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{pmatrix}$*. Then, there exists a four-tuple of probabilities* $\mathbf{a}$*"*, $\mathbf{b}$*"*, $\mathbf{c}$*"*, *and* $\mathbf{d}$*" over the sample space* $\Omega'' = \{0, 2n, 2e, 2s, 2w, 3a, 3b, 3c, 3d\}$ *such that:*

1. $(\varepsilon''_1, \varepsilon''_2, \varepsilon''_3, \varepsilon''_4)$ *are the statistical distances corresponding to* $\begin{pmatrix} \mathbf{a}'' & \mathbf{b}'' \\ \mathbf{c}'' & \mathbf{d}'' \end{pmatrix}$,
2. $\varepsilon''_i = \varepsilon'_i$, *for all* $i \in \{1, 2, 3, 4, \}$, *and*
3. *For all* $i \in \Omega''$*, the* i*-th cross-section of* $\begin{pmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{pmatrix}$ *is a type-*i *template.*

The proof of this claim is provided in Appendix C.3.

Because of Claim 6, it suffices to prove the inequality only for four-tuple of distributions over $\Omega = \{0, 2n, 2e, 2s, 2w, 3a, 3b, 3c, 3d\}$ such that its i-th cross-section is type-i template, for $i \in \Omega$. Unlike Lemma 1, obtaining a tight upper-bound on ε_1 and ε_2 is not trivial. So, we set up the linear program explicitly and analyze the optimal solution.

C.1 Setting the Linear Program

Given ε_3 and ε_4, we are interested in finding the maximum achievable ε_1 and ε_2. Due to Claim 5 and Claim 6 it suffices to consider a four-tuple of distributions $\begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{pmatrix}$ such that for each type of template there exists a unique cross-section corresponding to it. We plan to formulate this problem as a linear program and maximize ε_1.

For ease of presentation, without loss of generality, we assume that the sample space is $\Omega = \{0, \ldots, 8\}$. The 0-th cross-section corresponds to type-0 template. The 1-st, ..., 4-th cross-sections correspond to type-2n, ...,type-2w templates. The 5-th through 8-th cross-sections correspond to type-3a, ...,type-3d templates.

Let α_0 be the probability of type-0 template. Let $\alpha_1, \ldots, \alpha_4$ be the maximum probability entry in the type-2n, type-2e, type-2s, and types-2w template, respectively. For example, $\alpha_2 = b_2 = d_2$. Let $\alpha_5, \ldots, \alpha_8$ be the maximum probability entry in the type-3a, types-3b, types-3c, and types-3d templates, respectively.

Note that type-0 template makes no contributions to ε_1, ε_2, ε_3, and ε_4. Now consider the type-2n template. Note that the cross-section is $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha_1 & \alpha_1 \\ \alpha_1/\Theta & \alpha_1/\Theta \end{smallmatrix}\right)$. We consider four differences:

1. $b_1 - a_1 = 0$,
2. $d_1 - b_1 = -\alpha_1(1 - 1/\Theta) =: -\Delta_1$,
3. $c_1 - d_1 = 0$, and
4. $a_1 - d_1 = \alpha_1(1 - 1/\Theta) = \Delta_1$.

We pictorially represent these differences in the following figure. The arrows represent the fact that we subtract the variable at the "tail" of the arrow from the variable at the "head" of the arrow.

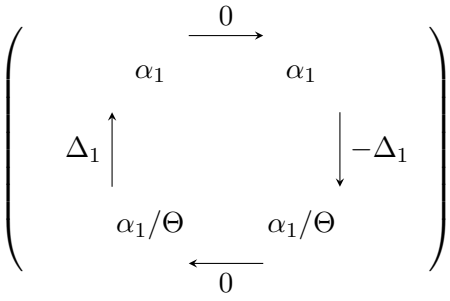


Figure 6: A pictorial summary of the variables.

Similarly, we define $\Delta_2 = \alpha_2(1 - 1/\Theta)$, $\Delta_3 = \alpha_3(1 - 1/\Theta)$, and $\Delta_4 = \alpha_4(1 - 1/\Theta)$.

Now, we consider the cross-section that is type-3a template. The four differences are:

1. $b_5 - a_5 = -\alpha_5(1 - 1/\Theta) =: -\Delta_5$,
2. $d_5 - b_5 = -\alpha_5(1 - 1/\Theta)/\Theta = -\Delta_5/\Theta$,
3. $c_5 - d_5 = \alpha_5(1 - 1/\Theta)/\Theta = \Delta_5/\Theta$, and
4. $a_5 - c_5 = \alpha_5(1 - 1/\Theta) = \Delta_5$.

For intuition, we elaborate the variables in the figure below.

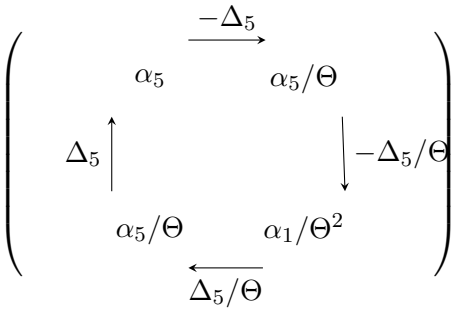


Figure 7: A pictorial summary of the variables.

Constraints of the Linear Program. For given ε_3 and ε_4, we have the following constraints:

1. The first constraint is
$$\sum_{i\in\Omega:\ b_i>a_i} b_i - a_i = \sum_{i\in\Omega:\ b_i<a_i} a_i - b_i$$
We formalize this constraint as follows.
$$\Delta_2 + \Delta_6 + \Delta_8/\Theta = \Delta_4 + \Delta_5 + \Delta_7/\Theta \tag{1}$$
This constraint also ensures that $a_1 + \cdots + a_8 = b_1 + \cdots + b_8$.

2. The second constraint is
$$\sum_{i\in\Omega:\ d_i>b_i} d_i - b_i = \sum_{i\in\Omega:\ d_i<b_i} b_i - d_i = \varepsilon_4$$
We formalize this constraint as follows.
$$\Delta_3 + \Delta_7/\Theta + \Delta_8 = \Delta_1 + \Delta_5/\Theta + \Delta_6 = \varepsilon_4 \tag{2}$$
This constraint also ensures that $b_1 + \cdots + b_8 = d_1 + \cdots + d_8$.

3. The third constraint is
$$\sum_{i\in\Omega:\ c_i>d_i} c_i - d_i = \sum_{i\in\Omega:\ c_i<d_i} d_i - c_i = \varepsilon_3$$
We formalize this constraint as follows.
$$\Delta_4 + \Delta_5/\Theta + \Delta_7 = \Delta_2 + \Delta_6/\Theta + \Delta_8 = \varepsilon_3 \tag{3}$$
This constraint also ensures that $d_1 + \cdots + d_8 = c_1 + \cdots + c_8$.

4. The fourth constraint is:
$$\sum_{i\in\Omega:\ a_i>c_i} a_i - c_i = \sum_{i\in\Omega:\ a_i<c_i} c_i - a_i$$
We formalize this constraint as follows.
$$\Delta_1 + \Delta_5 + \Delta_6/\Theta = \Delta_3 + \Delta_7 + \Delta_8/\Theta \tag{4}$$
This constraint also ensures that $c_1 + \cdots + c_8 = a_1 + \cdots + a_8$.

5. We need to also ensure that
$$\Delta_1, \ldots, \Delta_8 \geqslant 0 \tag{5}$$

6. Finally, we need to ensure that $a_0 \geqslant 0$. So, we have the following constraint.
$$a_1 + \cdots + a_8 = \left(\Delta_1 + \frac{\Delta_2}{\Theta} + \frac{\Delta_3}{\Theta} + \Delta_4 + \Delta_5 + \frac{\Delta_6}{\Theta} + \frac{\Delta_7}{\Theta} + \frac{\Delta_8}{\Theta^2}\right)\left(1 - \frac{1}{\Theta}\right)^{-1} \leqslant 1 \tag{6}$$

Objective. To maximize ε_1, we maximize $\Delta_2 + \Delta_6 + \Delta_8/\Theta$. And, to maximize ε_2, we maximize $\Delta_1 + \Delta_5 + \Delta_6/\Theta$.

Remarks. Before we move ahead, we want to highlight a few quick observations about this linear program.

1. The linear program has a solution
$$\Delta_1 = \varepsilon_4, \Delta_2 = \varepsilon_3, \Delta_3 = \varepsilon_4, \Delta_4 = \varepsilon_3, \Delta_5 = 0, \Delta_6 = 0, \Delta_7 = 0, \Delta_8 = 0$$
if $(\varepsilon_3 + \varepsilon_4)(1 + \Theta^{-1}) \leqslant (1 - \Theta^{-1})$.

2. It is straightforward to conclude that $\varepsilon_1, \varepsilon_2 \leqslant \varepsilon_3 + \varepsilon_4$ because $\varepsilon_1 = \Delta_2 + \Delta_6 + \Delta_8/\Theta \leqslant \Delta_2 + \Delta_6 + \Delta_8 \leqslant (\Delta_2 + \Delta_6/\Theta + \Delta_8) + (\Delta_1 + \Delta_5/\Theta + \Delta_6) = \varepsilon_3 + \varepsilon_4$. Analogously, we can conclude that $\varepsilon_2 \leqslant \varepsilon_3 + \varepsilon_4$.

Parametrized (Potential) Solution Space. The set of all solutions $(\Delta_1, \ldots, \Delta_8)$ under the constraints Equation 1 to Equation 4 is represented by the following set of points $(p_1, \ldots, p_8)$ such that:
$$\begin{aligned}
p_1 &= \varepsilon_4 - p_5/\Theta - p_6 \\
p_2 &= \varepsilon_3 - p_6/\Theta - p_8 \\
p_3 &= \varepsilon_4 - p_5/\Theta + p_6/\Theta - p_8(1 + 1/\Theta) \\
p_4 &= \varepsilon_3 - p_5(1 + 1/\Theta) + p_6 - p_8 \\
p_7 &= p_5 - p_6 + p_8
\end{aligned}$$

Note that all coordinates have been expressed as a function of p_5, p_6, and p_8. The first objective function translates to $\varepsilon_1 = \varepsilon_3 + (1 - 1/\Theta)(p_6 - p_8)$. And, the second objective function translates to $\varepsilon_2 = \varepsilon_4 + (1 - 1/\Theta)(p_5 - p_6)$.

C.1.1 Maximizing ε_1.

Under the constraint Equation 5, we want to maximize ε_1, that is, maximize $(p_6 - p_8)$. We consider three equations in particular:
$$\begin{aligned}
0 \leqslant \Delta_1 &= \varepsilon_4 - p_5/\Theta - p_6 \\
0 \leqslant \Delta_7 &= p_5 - p_6 + p_8 \\
0 \leqslant \Delta_8 &= p_8
\end{aligned}$$

Claim 7. *The quantity $(p_5 - p_8)$ is maximized if and only if $p_5 = p_6 = \Theta\varepsilon_4/(\Theta + 1)$ and $p_8 = 0$.*

Tight Protocol to maximize ε_1 and happens to have $\varepsilon_2 = \varepsilon_4$

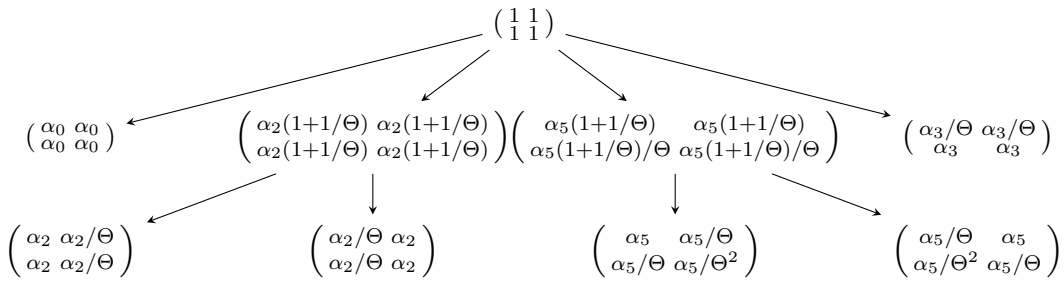


Figure 8: For $\Theta > 1$ and $(\varepsilon_3 + \varepsilon_4) + \varepsilon_3/\Theta \leqslant 1 - 1/\Theta$, a two-round protocol where Alice speaks first with $\varepsilon_2 = \varepsilon_4$ and $\varepsilon_1 = (\varepsilon_3 + \varepsilon_4) - \frac{2}{\Theta+1}\varepsilon_4$. In this solution we have $\alpha_2 = \alpha_4$ and $\alpha_5 = \alpha_6$.

Proof. Suppose $p_5 - p_6 + p_8 = \delta \geqslant 0$, that is: $p_5 = p_6 - p_8 + \delta$, for some non-negative δ. Next, we have $\varepsilon_4 - p_5/\Theta - p_6 = \delta' \geqslant 0$. Substituting, we get: $\Theta\varepsilon_4 - \Theta p_6 - \Theta\delta' = p_5 = p_6 - p_8 + \delta$. We solve for $p_6 = (\Theta\varepsilon_4 + p_8 - \Theta\delta' - \delta)/(\Theta + 1)$. Now, $(p_6 - p_8) = (\Theta\varepsilon_4 - \Theta p_8 - \Theta\delta' - \delta)/(\Theta + 1)$. Under the constraint $0 \leqslant \Delta_8 = p_8$, we note that $(p_6 - p_8)$ is maximized if and only if $\delta = \delta' = p_8 = 0$. □

For this assignment we have $(\Delta_1, \ldots, \Delta_8) =$

$$\left(0, \varepsilon_3 - \frac{\varepsilon_4}{\Theta+1}, \varepsilon_4, \varepsilon_3 - \frac{\varepsilon_4}{\Theta+1}, \frac{\Theta\varepsilon_4}{\Theta+1}, \frac{\Theta\varepsilon_4}{\Theta+1}, 0, 0\right)$$

This is a valid solution, because the following two reasons. First, all coordinates are non-negative because $\varepsilon_3/\varepsilon_4 \geqslant \frac{1}{\Theta+1}$. Finally, we have $a_0 \geqslant 0$ because

$$\begin{aligned}(a_1 + \cdots + a_8)\left(1 - \frac{1}{\Theta}\right) &= 0 + \left(\frac{\varepsilon_3}{\Theta} - \frac{\varepsilon_4}{\Theta(\Theta+1)}\right) + \frac{\varepsilon_4}{\Theta} + \left(\varepsilon_3 - \frac{\varepsilon_4}{\Theta+1}\right) + \frac{\Theta\varepsilon_4}{\Theta+1} + \frac{\varepsilon_4}{\Theta+1} + 0 + 0 \\ &= \varepsilon_3\left(1 + \frac{1}{\Theta}\right) + \varepsilon_4 \ \leqslant \left(1 - \frac{1}{\Theta}\right)\end{aligned}$$

And the maximized objective function is

$$\varepsilon_1^* = \varepsilon_3 + \frac{\Theta - 1}{\Theta + 1}\varepsilon_4 = (\varepsilon_3 + \varepsilon_4) - \frac{2}{\Theta+1}\varepsilon_4$$

C.1.2 Maximizing ε_2.

This is a symmetric problem and $\varepsilon_2^* = (\varepsilon_3 + \varepsilon_4) - \frac{2}{\Theta+1}\varepsilon_3$. We can use the following parameters: $p_5 = \Theta\varepsilon_3/(\Theta + 1)$, $p_6 = 0$, and $p_8 = 0$. This yields $(\Delta_1, \ldots, \Delta_8) =$

$$\left(\varepsilon_4 - \frac{\varepsilon_3}{\Theta+1}, \varepsilon_3, \varepsilon_4 - \frac{\varepsilon_3}{\Theta+1}, 0, \frac{\Theta\varepsilon_3}{\Theta+1}, 0, \frac{\Theta\varepsilon_3}{\Theta+1}, 0\right)$$

This is a valid solution because $\varepsilon_4/\varepsilon_3 \geqslant \frac{1}{\Theta+1}$. Further, $a_0 \geqslant 0$ because

$$(a_1 + \cdots + a_8)\left(1 - \frac{1}{\Theta}\right) = \varepsilon_4\left(1 + \frac{1}{\Theta}\right) + \varepsilon_3 \ \leqslant \left(1 - \frac{1}{\Theta}\right)$$

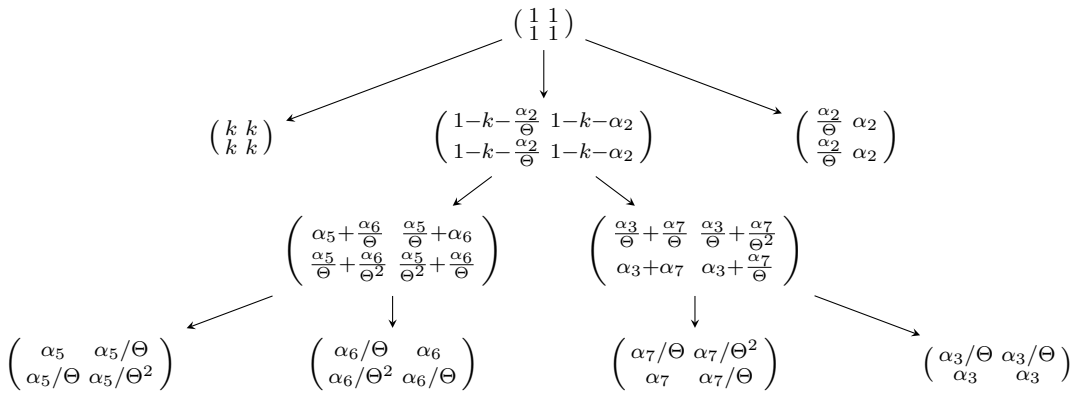


Figure 9: For $\varepsilon_3 + \varepsilon_4 \leqslant 1 - \frac{2}{\Theta+1}$ and $\varepsilon_3 = \varepsilon_4 = \varepsilon$, a three-round protocol that maximizes ε_1 under the constraint that $\varepsilon_1 = \varepsilon_2$.

C.1.3 Maximizing Subject to $\varepsilon_1 = \varepsilon_2$ and $\varepsilon_3 = \varepsilon_4 = \varepsilon$.

Under this case, we can maximize $\varepsilon_1^* = \varepsilon_2^*$ for $p_5 = \frac{2\Theta}{\Theta+2}\varepsilon$, $p_6 = \frac{\Theta}{\Theta+2}\varepsilon$, and $p_8 = 0$. The solution $(\Delta_1, \ldots, \Delta_8)$ is:

$$\left(0, \frac{\Theta+1}{\Theta+2}\varepsilon, \frac{\Theta+1}{\Theta+2}\varepsilon, 0, \frac{2\Theta}{\Theta+2}\varepsilon, \frac{\Theta}{\Theta+2}\varepsilon, \frac{\Theta}{\Theta+2}\varepsilon, 0\right)$$

This achieves $\varepsilon_1^* = \varepsilon_2^* = 2\varepsilon - \frac{3}{\Theta+2}\varepsilon$. We have:

$$(a_1 + \cdots + a_8)\left(1 - \frac{1}{\Theta}\right) = 2\frac{(\Theta+1)^2}{\Theta(\Theta+2)}\varepsilon = 2\varepsilon\left(1 + \frac{1}{\Theta(\Theta+2)}\right) \leqslant \left(1 - \frac{1}{\Theta}\right)$$

C.2 Proof of Claim 5

In this section, we use α, β as parameter that are in the range $(1, \Theta)$. We prove Claim 5 by performing the following exhausting case analysis.

Case 1. Suppose we have a cross-section $\begin{pmatrix} x & x \\ x/\alpha & x/\alpha \end{pmatrix}$. We will write this cross-section as a linear combination of type-0 and type-2n templates.

$$\begin{pmatrix} x & x \\ x/\alpha & x/\alpha \end{pmatrix} = \begin{pmatrix} y & y \\ y & y \end{pmatrix} + \begin{pmatrix} z & z \\ z/\Theta & z/\Theta \end{pmatrix}$$

The constraints are:

$$y + z = x$$
$$y + z/\Theta = x/\alpha$$

This has positive solutions $y = \frac{x(1/\alpha - 1/\Theta)}{1-1/\Theta}$ and $z = \frac{x(1-1/\alpha)}{1-1/\Theta}$, because $\alpha \in (1, \Theta)$.

Case 2. Suppose we have a cross-section $\begin{pmatrix} x & x/\Theta \\ x/\alpha & x/\alpha\Theta \end{pmatrix}$. We will write this cross-section as a linear combination of type-2w and type-3a templates.

$$\begin{pmatrix} x & x/\Theta \\ x/\alpha & x/\alpha\Theta \end{pmatrix} = \begin{pmatrix} y & y/\Theta \\ y & y/\Theta \end{pmatrix} + \begin{pmatrix} z & z/\Theta \\ z/\Theta & z/\Theta^2 \end{pmatrix}$$

The constraints are:

$$y + z = x$$
$$y + z/\Theta = x/\alpha$$

And, similar to the previous case, positive solutions for y and z are guaranteed.

Case 3. Suppose we have a cross-section $\begin{pmatrix} x & x/\beta \\ x/\alpha & x/\alpha\beta \end{pmatrix}$. We will write this cross-section as a linear combination of Case 1 cross-section and Case 2 cross-section.

$$\begin{pmatrix} x & x/\beta \\ x/\alpha & x/\alpha\beta \end{pmatrix} = \begin{pmatrix} y & y/\beta \\ y & y/\beta \end{pmatrix} + \begin{pmatrix} z & z/\beta \\ z/\Theta & z/\beta\Theta \end{pmatrix}$$

Again, the constraints are:

$$y + z = x$$
$$y + z/\Theta = x/\alpha$$

And, similar to the previous cases, positive solutions for y and z are guaranteed. The two cross-sections produced are already covered in Case 1 and 2.

Note of SD-contributions. Note that the convex linear combinations preserve the SD-contributions in each case. Hence, we get the desired result.

C.3 Proof of Claim 6

Similar to Claim 4, we simply collapse all the cross-sections of type $i \in \Omega''$ of $\begin{pmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{pmatrix}$ into one cross-section. It is easy to see that it preserves the total statistical distances contributions of all cross-sections that are type-i template in $\begin{pmatrix} \mathbf{a}' & \mathbf{b}' \\ \mathbf{c}' & \mathbf{d}' \end{pmatrix}$. Iterating this process for every $i \in \Omega''$, we get our result.

D Proof of Lemma 4

We alredy know by Lemma 3 part 1 that the solution that maximizes ε_1 without any restriction on the round complexity of the protocol already has $\varepsilon_2 = \varepsilon_4$ (which is a property of two-round protocols where Alice sends the first message) and admits a two-round protocol as demonstrated in Figure 8. Therefore, restricted to two-round protocols and $\varepsilon_2 = \varepsilon_4$ the optimal solution coincides with the solution of Lemma 3 part 1.

E Tree Representation of a Protocol

For completeness, in this section, we provide details of how a protocol can be equivalently represented by a tree with probability matrices associated with each of the nodes in the tree. Note that partial transcripts of a protocol π naturally define a tree $\mathbb{T}_\pi$. The internal nodes of the tree represent partial

transcripts and the leaves represent the full transcripts of the protocol. In this presentation, we restrict to the case where both parties participating in π has two possible private inputs each, say $\{0,1\}$. By $\pi(x,y)$ we represent the protocol where parties have private input x and y, respectively.

For every node $v \in \mathbb{T}_\pi$, we associate a 2×2 matrix $M(v)$. The (i,j)-th entry of $M(v)$, i.e., $M(v)_{i,j}$, represents the probability that the (partial) transcript v is generated by $\pi(i,j)$. These probabilities satisfy the following properties:

1. Let r be the root of $\mathbb{T}_\pi$. Then $M(r) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. For any internal node v, let $\mathsf{child}(v)$ be the set of all its children. Then, $M(v) = \sum_{w \in \mathsf{child}(v)} M(w)$.

2. Let v be an internal node where Alice sends the next message. Then, for any $w \in \mathsf{child}(v)$, there exists p, q such that $M(w) = \left(\begin{smallmatrix} p & 0 \\ 0 & q \end{smallmatrix}\right) \cdot M(v)$. Similarly, if v be an internal node where Bob sends the next message. Then, for any $w \in \mathsf{child}(v)$, there exists $p, q \geqslant 0$ such that $M(w) = M(v) \cdot \left(\begin{smallmatrix} p & 0 \\ 0 & q \end{smallmatrix}\right)$.

Interestingly, if a tree $\mathbb{T}$ is provided with associate $M(v)$, for $v \in \mathbb{T}$, that satisfies the above mentioned constraints then there exists a protocol π that generates it.