Channels of Small Log-Ratio Leakage and Characterization of Two-Party Differentially Private Computation

Iftach Haitner*† Noam Mazor* Ronen Shaltiel‡ Jad Silbak*

May 29, 2019

Abstract

Consider a PPT two-party protocol $\Pi = (\mathsf{A}, \mathsf{B})$ in which the parties get no private inputs and obtain outputs $O^{\mathsf{A}}, O^{\mathsf{B}} \in \{0,1\}$, and let V^{A} and V^{B} denote the parties' individual views. Protocol Π has α-*agreement* if $\Pr[O^{\mathsf{A}} = O^{\mathsf{B}}] = \frac{1}{2} + \alpha$. The *leakage* of Π is the amount of information a party obtains about the event $\{O^{\mathsf{A}} = O^{\mathsf{B}}\}$; that is, the *leakage* ϵ is the maximum, over $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$, of the distance between $V^{\mathsf{P}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}}$ and $V^{\mathsf{P}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}$. Typically, this distance is measured in *statistical distance*, or, in the computational setting, in *computational indistinguishability*. For this choice, Wullschleger [TCC '09] showed that if $\epsilon \ll \alpha$ then the protocol can be transformed into an OT protocol.

We consider measuring the protocol leakage by the *log-ratio distance* (which was popularized by its use in the differential privacy framework). The log-ratio distance between X, Y over domain Ω is the minimal $\epsilon \geq 0$ for which, for every $v \in \Omega$, $\log \frac{\Pr[X=v]}{\Pr[Y=v]} \in [-\epsilon, \epsilon]$. In the computational setting, we use computational indistinguishability from having log-ratio distance ϵ. We show that a protocol with (noticeable) accuracy $\alpha \in \Omega(\epsilon^2)$ can be transformed into an OT protocol (note that this allows $\epsilon \gg \alpha$). We complete the picture, in this respect, showing that a protocol with $\alpha \in o(\epsilon^2)$ does not necessarily imply OT. Our results hold for both the information theoretic and the computational settings, and can be viewed as a "fine grained" approach to "weak OT amplification".

We then use the above result to *fully* characterize the complexity of differentially private two-party computation for the XOR function, answering the open question put by Goyal, Khurana, Mironov, Pandey, and Sahai [ICALP '16] and Haitner, Nissim, Omri, Shaltiel, and Silbak [FOCS '18]. Specifically, we show that for any (noticeable) $\alpha \in \Omega(\epsilon^2)$, a two-party protocol that computes the XOR function with α-accuracy and ϵ-differential privacy can be transformed into an OT protocol. This improves upon Goyal et al. that only handle $\alpha \in \Omega(\epsilon)$, and upon Haitner et al. who showed that such a protocol implies (infinitely-often) key agreement (and not OT). Our characterization is tight since OT does not follow from protocols in which $\alpha \in o(\epsilon^2)$, and extends to functions (over many bits) that "contain" an "embedded copy" of the XOR function.

Keywords: oblivious transfer; differential privacy; hardness amplification.

*School of Computer Science, Tel Aviv University. Emails: iftachh@cs.tau.ac.il,noammaz@gmail.com,jadsilbak@gmail.com.
Research supported by ERC starting grant 638121.
†Member of the Check Point Institute for Information Security.

‡Department of Computer Science. University of Haifa, Email: {ronen@cs.haifa.ac.il}. Research supported by ISF grant 1628/17.

1 Introduction

Oblivious transfer (OT), introduced by Rabin [41], is one of the most fundamental primitives in cryptography and a complete primitive for secure multi-party computation [47, 13]. Oblivious transfer protocols are known to exist assuming (several types of) *families of trapdoor permutations* [11, 17], *learning with errors* [39], *decisional Diffie-Hellman* [37, 1] and *quadratic residuosity* [29]. While in some of the constructions of OT in the literature, the construction immediately yields a full-fledged OT, in others it only yields a "weak" form of OT, that is later "amplified" into a full-fledged one.

In this paper we introduce a new notion for a "weak form of OT", and show how to amplify this "weak OT" into full-fledged OT. This notion is more "fine grained" than some previously suggested notions, which allows us to obtain OT in scenarios that could not be handled by previous works. Our approach is suitable for the computational and for the information theoretic settings (i.e., the dishonest parties are assumed to be computationally bounded or not).

1.1 Our Results

We start with presenting our results in the information theoretic setting, and then move to the computation one.

1.1.1 The Information Theoretic Setting

The information theoretic analogue of a two-party protocol between parties A and B, is a "channel": namely, a quadruple of random variables $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$, with the interpretation that when "activating" (or "calling") the channel C, party $\mathrm{P} \in \{\mathsf{A}, \mathsf{B}\}$ receives his "output" O^{P} and his "view" V^{P}. In other words, "activating a channel" is analogous to running a two-party protocol with fresh randomness. (We assume that the view V^{P} contains the output O^{P}).

Log-ratio leakage (channels). We are interested in the special case where the channel $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ has Boolean outputs (i.e., $O^{\mathsf{A}}, O^{\mathsf{B}} \in \{0, 1\}$), and assume for simplicity that the channel is *balanced*, meaning that for both $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$, O^{P} is uniformly distributed. Such channels are parameterized by their *agreement* and *leakage*:

- A channel C has α-*agreement* if $\Pr[O^{\mathsf{A}} = O^{\mathsf{B}}] = \frac{1}{2} + \alpha$. (Without loss of generality, $\alpha \geq 0$, as otherwise one of the parties can flip his output).
- The *leakage* of party B in C is the distance between the distributions $V^{\mathsf{A}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}}$ and $V^{\mathsf{A}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}$. (Note that these two distributions are well defined if $\alpha \in [0, \frac{1}{2})$). The leakage of party A is defined in an analogous way, and the leakage of C is the maximum of the two leakages.

This approach (with somewhat different notation) was taken by past work [45, 44], using *statistical distance* as the distance measure.

Loosely speaking, leakage measures how well can a party distinguish the case $\{O^{\mathsf{A}} = O^{\mathsf{B}}\}$ from the case $\{O^{\mathsf{A}} \neq O^{\mathsf{B}}\}$. As each party knows his output, this can be thought of as the "amount of information" on the input of one party that *leaks* to the other party.[1]

[1] We remark that one should be careful with this intuition. Consider a "binary symmetric channel": a channel in which $V^{\mathsf{A}} = O^{\mathsf{A}}$ and $V^{\mathsf{B}} = O^{\mathsf{B}}$ (i.e., the parties receive no additional view except their outputs), O^{A} is uniformly

We will measure leakage using a *different distance measure*, which we refer to as "log-ratio distance".

Definition 1.1 (Log-Ratio distance)**.** *Two numbers $p_0, p_1 \in [0,1]$ satisfy $p_0 \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} p_1$ if for both $b \in \{0,1\}$: $p_b \leq e^{\epsilon} \cdot p_{1-b} + \delta$. Two distributions D_0, D_1 over the same domain Ω, are (ϵ,δ)-*log-ratio-close *(denoted $D_0 \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} D_1$) if for every $A \subseteq \Omega$:*

$$\Pr[D_0 \in A] \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} \Pr[D_1 \in A].$$

We use the notation $D_0 \overset{\mathrm{S}}{\approx}_{\delta} D_1$ to say that the *statistical distance* between D_0 and D_1 is at most δ. Log-ratio distance is a generalization of statistical distance as $\overset{\mathrm{S}}{\approx}_{\delta}$ is the same as $\overset{\mathrm{R}}{\approx}_{0,\delta}$. This measure of distance was popularized by its use in the *differential privacy* framework [9] (that we discuss in Section 1.1.3).

Loosely speaking, log-ratio distance considers the "log-ratio function" $L_{D_0||D_1}(x) := \log \frac{\Pr[D_0=x]}{\Pr[D_1=x]}$, and the two distribution are (ϵ,δ)-log-ratio-close if this function is in the interval $[-\epsilon,\epsilon]$ with probability $1-\delta$. As such, it can be seen as a "cousin" of *relative entropy* (also known as, *Kullback–Leibler (KL) divergence*) that measures the expectation of the log-ratio function.

Note that for $\epsilon \in [0,1]$, $D_0 \overset{\mathrm{R}}{\approx}_{\epsilon,0} D_1$ implies $D_0 \overset{\mathrm{R}}{\approx}_{0,2\epsilon} D_1$, but the converse is not true, and the condition $(D_0 \overset{\mathrm{R}}{\approx}_{\epsilon,0} D_1)$ gives tighter handle on the distance between independent samples of distributions (as we explain in detail in Section 2.1).

We use the log-ratio distance to measure leakage in channels. This leads to the following definition (in which we substitute "log-ratio distance" as a distance measure).

Definition 1.2 (Log-ratio leakage, channels, informal)**.** *A channel $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ has* log-ratio leakage (ϵ,δ)*,* denoted (ϵ,δ)-leakage *if for both $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$:*

$$V^{\mathsf{P}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}} \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} V^{\mathsf{P}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}.$$

This definition is related (and inspired by) the *differential privacy* framework [9]. In the terminology of differential privacy, this can be restated as follows: let E be the indicator variable for the event $\{O^{\mathsf{A}} = O^{\mathsf{B}}\}$. For both $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$, the "mechanism" V^{P} is (ϵ,δ)-differentially private with regards to the "secret"/"database" E.

Channels of small log-ratio leakage imply OT. Wullschleger [45] considered channels with small leakage (measured by statistical distance). Using our terminology, he showed for $\alpha \in [0,\frac{1}{2})$ and $\epsilon \in [0,1]$ with ϵ "sufficiently smaller than" α^2, a channel with α-agreement and $(0,\epsilon)$-leakage yields OT. This can be interpreted as saying that if the leakage ϵ is sufficiently *smaller* than the agreement α, then the channel yields OT. We prove the following "fine grained" amplification result, which is restated with precise notation in Theorem 4.2.

Theorem 1.3 (Channels of small log-ratio leakage imply OT, infromal)**.** *There exists a constants $c_1 > 0$ such that the following holds for every ϵ,δ,α with $c_1 \cdot \epsilon^2 \leq \alpha < 1/8$ and $\delta \leq \epsilon^2$: a channel C that has α-agreement and* (ϵ,δ)-leakage *yields OT (of statistical security).*

distributed, and $O^{\mathsf{B}} = O^{\mathsf{A}} \oplus U_p$ (where U_p is an independent biased coin which is one with probability p). The leakage of this channel is zero, for every choice of p, whereas each party can predict the output of the other party with probability $1-p$ by using his own output as a prediction.

For simplicity, let us focus on Theorem 1.3 in the case that $\delta = 0$. Two distributions that are $(\epsilon, 0)$-log-ratio close, may have statistical distance ϵ, and so, a channel with $(\epsilon, 0)$-leakage, can only be assumed to have $(0, \epsilon)$-leakage (when measuring leakage in statistical distance). Nevertheless, in contrast to [45], Theorem 1.3 allows the leakage parameter ϵ to be *larger* than the agreement parameter α.[2]

The above can be interpreted as saying that when the leakage is "well behaved" (that is the δ parameter in log-ratio distance is sufficiently small), OT can be obtained even from a channel whose leakage ϵ is *much larger* than the agreement α. This property will be the key for our applications in Section 1.1.3.

Triviality of channels with large leakage. We now observe that the relationship between ϵ and α in Theorem 1.3 is best possible (up to constants). Namely, a channel with agreement that is asymptotically smaller than the one allowed in Theorem 1.3 does not necessarily yield OT.

Theorem 1.4 (Triviality of channels with large leakage, informal)**.** *There exists a constant $c_2 > 0$, such that the following holds for for every $\epsilon > 0$: there exists a two-party protocol (with no inputs) that when it ends, party $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ outputs O^{P} and sees view V^{P}, and the induced channel $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ has $(c_2 \cdot \epsilon^2)$-agreement and $(\epsilon, 0)$-leakage.*

Together, the two theorems say that our characterization of "weak-OT" using agreement α and $(\epsilon, 0)$-log-ratio leakage has a "threshold behavior" at $\alpha \approx \epsilon^2$: if $\alpha \geq c_1 \cdot \epsilon^2$ then the channel yields OT, and if $\alpha \leq c_2 \cdot \epsilon^2$ then such a channel can be simulated by a two-party protocol with no inputs (and thus cannot yield OT with information theoretic security). The proof of Theorem 1.4 uses a variant of the well-known randomized response approach of Warner [42].

1.1.2 The Computational Setting

We consider a no-input, Boolean output, two-party protocol $\Pi = (\mathsf{A}, \mathsf{B})$. Namely, both parties receive a security parameter 1^κ as a common input, get no private input, and both output one bit. We denote the output of party P by O^{P}_κ, and its view by V^{P}_κ. In other words, an instantiation of $\Pi(1^\kappa)$ can be thought of as inducing a channel $C_\kappa = ((V^{\mathsf{A}}_\kappa, O^{\mathsf{A}}_\kappa), (V^{\mathsf{B}}_\kappa, O^{\mathsf{B}}_\kappa))$. Similar to the information theoretic setting, protocol Π has α-agreement if for every $\kappa \in \mathbb{N}$: $\Pr\left[O^{\mathsf{A}}_\kappa = O^{\mathsf{B}}_\kappa\right] = 1/2 + \alpha(\kappa)$.

Log-ratio leakage (protocols). We extend the definition of log-ratio leakage to the computational setting (where adversaries are PPT machines). We will use the simulation paradigm to extend the information theoretic definition to the computational setting.

Definition 1.5 (Log-ratio leakage, protocols, informal)**.** *A two-party no-input Boolean output protocol $\Pi = (\mathsf{A}, \mathsf{B})$ has* Comp-log-ratio leakage (ϵ, δ)*,* denoted (ϵ, δ)-comp-leakage*, if there exists an "ideal channel" ensemble $\widetilde{C} = \left\{\widetilde{C}_\kappa = ((V^{\tilde{\mathsf{A}}}_\kappa, O^{\tilde{\mathsf{A}}}_\kappa), (V^{\tilde{\mathsf{B}}}_\kappa, O^{\tilde{\mathsf{B}}}_\kappa))\right\}_{\kappa \in \mathbb{N}}$ such that the following holds:*

[2] To make this more concrete, consider the following channel $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$: $O^{\mathsf{A}} \leftarrow U_{1/2}$, $O^{\mathsf{B}} \leftarrow O^{\mathsf{A}} \oplus U_{1/2-\alpha}$, $V^{\mathsf{A}} \leftarrow O^{\mathsf{B}} \oplus U_{1/2-\epsilon}$, $V^{\mathsf{B}} \leftarrow O^{\mathsf{A}} \oplus U_{1/2-\epsilon}$ (where U_p denotes a biased coin which is one with probability p, and the three "noise variables" are independent). This channel is balanced, has α-agreement, and $(O(\epsilon), 0)$-leakage. However, if we were to measure leakage using statistical distance, then we would report that it has $(0, O(\epsilon))$-leakage. We are assuming that $\epsilon > \alpha$, and it will be critical that leakage is measured by log-ratio distance, as we do not know how to amplify leakage that is measured by statistical distance in this range.

- *For every* $\kappa \in \mathbb{N}$*: the channel* $\widetilde{C}_\kappa$ *has* $(\epsilon(\kappa), \delta(\kappa))$*-leakage.*
- *For every* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$*: the ensembles* $\left\{V_\kappa^{\mathsf{P}}, O_\kappa^{\mathsf{A}}, O_\kappa^{\mathsf{B}}\right\}_{\kappa\in\mathbb{N}}$ *and* $\left\{V_\kappa^{\widetilde{\mathsf{P}}}, O_\kappa^{\widetilde{\mathsf{A}}}, O_\kappa^{\widetilde{\mathsf{B}}}\right\}_{\kappa\in\mathbb{N}}$ *are* computationally indistinguishable.[3]

Protocols of small log-ratio leakage imply OT. We prove the following computational analogue of Theorem 1.3 (the next Theorem is restated with precise notation in Theorem 4.25).

Theorem 1.6 (Amplification of protocols with small log-ratio leakage, informal)**.** *There exists a constant* $c_1 > 0$ *such that the following holds for every function* ϵ, δ, α *with* $c_1 \cdot \epsilon(\kappa)^2 \leq \alpha(\kappa) < 1/8$*,* $\delta(\kappa) \leq \epsilon(\kappa)^2$ *and* $1/\alpha(\kappa) \in \text{poly}(\kappa)$*: a* PPT *protocol that has* α*-agreement and* (ϵ, δ)-comp-leakage *yields OT (of computational security).*

Triviality of protocols with large leakage. An immediate corollary of Theorem 1.4 is the relationship between ϵ and α in Theorem 1.6 is best possible (up to constants).

Corollary 1.7 (Triviality of protocols with large leakage, informal)**.** *There exists a constant* $c_2 > 0$*, such that the following holds for for every function* ϵ *with* $\epsilon(\kappa) > 0$*: there exists a* PPT *protocol that has* $(c_2 \cdot \epsilon^2)$*-agreement and* $(\epsilon, 0)$*-leakage.*

1.1.3 Application: Characterization of Two-Party Differentially Private Computation.

We use our results to characterize the complexity of differentially private two-party computation for the XOR function, answering the open question put by [16, 22]. The framework of differential privacy typically studies a "one-party" setup, where a "curator" wants to answer statistical queries on a database without compromising the privacy of individual users whose information is recorded as rows in the database [9]. In this paper, we are interested in *two-party* differentially-private computation (defined in [36]). This setting is closely related to the setting of secure function evaluation: the parties A and B have private inputs x and y, and wish to compute some functionality $f(x, y)$ without compromising the privacy of their inputs. In secure function evaluation, this intuitively means that parties do not learn any information about the other party's input, that cannot be inferred from their own inputs and outputs. This guarantee is sometimes very weak: For example, for the XOR function $f(x, y) = x \oplus y$, secure function evaluation completely reveals the inputs of the parties (as a party that knows x and $f(x, y)$ can infer y). Differentially private two-party computation aims to give some nontrivial security even in such cases (at the cost of compromising the *accuracy* of the outputs).

Definition 1.8 (Differentially private computation [36])**.** *A* PPT *two-party protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *over input domain* $\{0,1\}^n \times \{0,1\}^n$ *is* ϵ*-DP, if for every* PPT *nonuniform machines* B^* *and* D*, and every* $x, x' \in \{0,1\}^n$ *with* $\text{Ham}(x, x') = 1$*: let* $V_\kappa^{\mathsf{B}^*}(x)$ *be the view of* B^* *in a random execution of* $(\mathsf{A}(x), \mathsf{B}^*)(1^\kappa)$*), then*

$$\Pr\left[\mathsf{D}(V_\kappa^{\mathsf{B}^*}(x)) = 1\right] \leq e^{\epsilon(\kappa)} \cdot \Pr\left[\mathsf{D}(V_\kappa^{\mathsf{B}^*}(x')) = 1\right] + \text{neg}(\kappa),$$

[3] In the technical section, we consider computational indistinguishability by both *uniform* and *nonuniform* PPT machines. We ignore this issue in the introduction.

and the same hold for the secrecy of B.

Such a protocol is semi-honest ϵ-DP*, if the above is only guaranteed for semi-honest adversaries (i.e., for* $\mathsf{B}^* = \mathsf{B}$*).*

In this paper, we are interested in functionalities f, in which outputs are single bits (as in the case of the XOR function). In this special case, the accuracy of a protocol can be measured as follows:

Definition 1.9 (accuracy)**.** *A* PPT *two-party protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *over input domain* $\{0,1\}^n \times \{0,1\}^n$ *with outputs* $O^{\mathsf{A}}(x,y), O^{\mathsf{B}}(x,y) \in \{0,1\}$ *has* perfect agreement *if for every* $x, y \in \{0,1\}^n \times \{0,1\}^n$*, and every* $\kappa \in \mathbb{N}$*, in a random execution of the protocol* $(\mathsf{A}(x), \mathsf{B}(y))(1^\kappa)$*, it holds that* $\Pr[O^{\mathsf{A}}(x,y) = O^{\mathsf{B}}(x,y)] = 1$.

The protocol implements a functionality f *over input domain* $\{0,1\}^n \times \{0,1\}^n$ *with* α-accuracy*, if for* $\kappa \in \mathbb{N}$*, every* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$*, and every* $x, y \in \{0,1\}^n \times \{0,1\}^n$*, in a random execution of the protocol* $(\mathsf{A}(x), \mathsf{B}(y))(1^\kappa)$*, it holds that* $\Pr[O^{\mathsf{P}}(x,y) = f^{\mathsf{P}}(x,y)] = \frac{1}{2} + \alpha(\kappa)$.

A natural question is what assumptions are needed for two-party differentially private computation achieving a certain level of accuracy/privacy (for various functionalities). A sequence of works showed that for certain tasks, achieving high accuracy requires one-way functions [3, 5, 35, 15]; some cannot even be instantiated in the random-oracle model [21]; and some cannot be black-box reduced to key agreement [30]. See Section 1.2 for more details on these results. In this work we fully answer the above question for the XOR function.

Consider the functionality $f_\alpha(x,y)$ which outputs $x \oplus y \oplus U_{1/2-\alpha}$ (where $U_{1/2-\alpha}$ is an independent biased coin which is one with probability $1/2 - \alpha$). Assuming OT, there exists a two-party protocol that securely implement f_α, and this protocol is ϵ-DP, for $\epsilon = \Theta(\alpha)$. This is the best possible differential privacy that can be achieved for accuracy α. On the other extreme, an $\Theta(\epsilon^2)$-accurate, ϵ-differential private, protocol for computing XOR can be constructed (with information theoretic security) using the so-called *randomized response* approach of Warner [42], as shown in [15]. Thus, it is natural to ask whether OT *follows* from α-accurate, ϵ-DP computation of XOR, for intermediate choices of $\epsilon^2 \ll \alpha \ll \epsilon$. In this paper, we completely resolve this problem and prove that OT is implied for any intermediate $\epsilon^2 \ll \alpha \ll \epsilon$.

Differentially private XOR to OT, a tight characterization.

Theorem 1.10. *[Differentially private XOR to OT, informal] There exists a constant* $c_1 > 0$ *such that the following holds for every functions* ϵ, α *with* $\alpha \geq c_1 \cdot \epsilon^2$ *such that* $1/\alpha \in$ poly*: the existence of a perfect agreement,* α*-accurate, semi-honest* ϵ*-DP* PPT *protocol for computing XOR implies OT (of computational security).*

The above improves upon Goyal et al. [16], who gave a positive answer if the accuracy α is the best possible: if $\alpha \geq c \cdot \epsilon$ for a constant c. It also improves (in the implication) upon Haitner et al. [22], who showed that $c \cdot \epsilon^2$-correct ϵ-DP XOR implies (infinitely-often) key agreement. Finally, our result allows ϵ and α to be function of the security parameter (and furthermore, allow α and ϵ to be polynomially small in the security parameter) whereas previous reductions [16, 22] only hold for constant values of ϵ and α. Our characterization is tight as OT does not follow from protocols with $\alpha \in o(\epsilon^2)$.

Theorem 1.11 (Triviality of differentially private XOR with large leakage. Folklore, see [15])**.** *There exists a constant $c_2 > 0$ such that for every functions ϵ there exists a* PPT *protocol for computing XOR with information-theoretic ϵ-DP, perfect agreement and accuracy $c_2 \cdot \epsilon^2$.* [4]

Perspective. Most of the work in differentially private mechanisms/protocols is in the information theoretic setting (using the addition of random noise). There are, however, examples where using computational definitions of differential privacy together with cryptographic assumptions, yield significantly improved accuracy and privacy compared to those that can be achieved in the information theoretic setting (e.g., the inner product and the Hamming distance functionalities [35], see more references in the related work section below). Understanding the minimal assumptions required in this setting is a fundamental open problem. In this paper, we completely resolve this problem for the special case of the XOR function. We stress that the XOR function is the canonical example of a function $f(x, y)$ where the security guarantee given by secure function evaluation is very weak. More precisely, for $f(x, y) = x \oplus y$, the security guaranteed by secure function evaluation is meaningless, and the protocol in which both parties reveal their private inputs is considered secure. Differential privacy can be used to provide a meaningful definition of security in such cases, and we believe that the tools that we developed for the XOR function, can be useful to argue about the minimal assumptions required for other functionalities. As a first step, we provide a condition under which our approach applies to other functionalities $g : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

Extending the result to any function that is not monotone under relabeling. We can use our results on the XOR function to achieve OT from differentially private, and sufficiently accurate computation of a wide class of functions that are not "monotone under relabeling". A function $g : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is monotone under relabeling if there exist two bijective functions $\sigma_x, \sigma_y : [2^n] \to \{0,1\}^n$ such that for every $x \in \{0,1\}^n$ and $i \leq j \in [2^n]$:

$$g(x, \sigma_y(i)) \leq g(x, \sigma_y(j)),$$

and, for every $y \in \{0,1\}^n$ and $i \leq j \in [2^n]$:

$$g(\sigma_x(i), y) \leq g(\sigma_x(j), y).$$

We observe that every function g that is not monotone under relabeling has an "embedded XOR", meaning that there exist $x_0, x_1, y_0, y_1 \in \{0,1\}^n$ such that for every $b, c \in \{0,1\}$, $g(x_b, y_c) = b \oplus c$. This gives that a two-party protocol that computes g can be used to give a two-party protocol that computes XOR (with some losses in privacy) and these yield OT by our earlier results. Precise details are given in Section 5.

1.2 Related Work

Information-theoretic OT. Oblivious transfer protocols are also widely studies in their information theoretic forms [40, 7, 6, 38, 43]. In this form, and OT is simply a pair of jointly distributed random variable $(V_{\mathsf{A}}, V_{\mathsf{B}})$ (a "channel"). A pair of unbounded parties (A, B), having access to independent samples from this pair (from each sample $(v_{\mathsf{A}}, v_{\mathsf{B}})$, party P gets the value v_{P}). Interestingly, in the information theoretic form, we do have a "simple" notion of weak OT,

[4] The protocol is the randomized response one, and the proof is very similar to that of Theorem 1.4 (see Section 4).

that is complete: such pair can either be used to construct full-fledged (information theoretically secure) OT, or is trivial—there exists a protocol that generates these views. Unfortunately, these reductions are inherently inefficient: the parties wait till an event that might be of arbitrary small probability to occur, and thus, at least not in the most general form, cannot be translated into the computational setting.

Hardness amplification. Amplifying the security of weak primitives into "fully secure" ones is an important paradigm in cryptography as well as other key fields in heretical computer science. Most notable such works in cryptography are amplification of one-way functions [46, 14, 19], key-agreement protocols [26], and interactive arguments [24, 18]. Among the above, amplification of key-agreement protocols (KA) is the most similar to the OT amplification we consider in this paper. In particular, we do have a "simple" (non distributional) notion of weak KA [26]. This is done by reduction to the information theoretic notion of key-agreements. What enable this reduction to go through, is that unlike the case of information theoretic OT, the amplification of information theoretic KA are efficient, since they only use the designated output of the (weak) KA (and not the parties' view).

Minimal assumptions for differentially private symmetric computation. An accuracy parameter α is *trivial* with respect to a given functionality f and differential privacy parameter ϵ, if a protocol computing f with such accuracy and privacy exists information theoretically (i.e., with no computational assumptions). The accuracy parameter is called *optimal*, if it matches the bound achieved in the client-server model. Gaps between the trivial and optimal accuracy parameters have been shown in the multiparty case for count queries [3, 5] and in the two-party case for inner product and Hamming distance functionalities [35]. [21] showed that the same holds also when a random oracle is available to the parties, implying that non-trivial protocols (achieving non-trivial accuracy) for computing these functionalities cannot be black-box reduced to one-way functions. [15] initiated the study of Boolean functions, showing a gap between the optimal and trivial accuracy for the XOR or the AND functionalities, and that non-trivial protocols imply one-way functions. [28] showed that non-interactive randomised response is optimal among all the information theoretic protocols. [30] have shown that optimal protocols for computing the XOR or AND, cannot be black-box reduced to key agreement. [16] have shown that optimal protocols for computing the XOR imply oblivious transfer.
Very recently, [22] showed that a non-trivial protocol for computing XOR (i.e., accuracy better than ϵ^2) implies infinite often key-agreement protocols. Their reduction, however, only holds for constant value of ϵ, and is non black box. Finally, [2, 23] gave criteria, that proved the necessity of OT for a computationally secure function evaluation, for a select class functions.

Paper Organization

Due to space limitations, some of the technical details appear in the appendices. In Section 2 we give an overview of the main ideas used in the proof. In Section 3 we give some preliminaries and state some earlier work that we use. In Section 4 we give our amplification results, that convert protocols with small log-ratio leakage into OT. In Section 5 we prove our results on two-party differentially private computation of the XOR function, and on functions that are not monotone under relabeling.

2 Our Technique

In this section we give a high level overview of our main ideas and technique.

2.1 Usefulness of Log-Ratio Distance

Recall that the *leakage* we considered is measured using *log-ratio distance*, and not *statistical distance*. We survey some advantages of log-ratio distance over statistical distance.

As is common in "hardness amplification", our construction will apply the original channel/protocol many times (using fresh randomness). Given a distribution X, let X^ℓ denote the distribution of ℓ independent samples from X. A natural question is how does the distance between X^ℓ and Y^ℓ relate to the distance between X and Y. For concreteness, assume that $\mathrm{SD}(X,Y) = \epsilon$ (where SD denotes statistical distance) and that we are interested in taking $\ell = c/\epsilon^2$ repetitions where $c > 0$ is a very small constant. Consider the following two examples (in the following we use U_p to denote a coin which is one with probability p):

- $X_1 = U_0$ and $Y_1 = U_\epsilon$. In this case, $\mathrm{SD}(X_1^\ell, Y_1^\ell) = 1 - (1-\epsilon)^\ell \approx 1 - e^{-c/\epsilon}$ which approaches one for small ϵ.
- $X_2 = U_{1/2}$ and $Y_2 = U_{1/2+\epsilon}$, in this case $\mathrm{SD}(X_2^\ell, Y_2^\ell) = \eta$, where $\eta \approx \sqrt{c}$ is a small constant that is independent of ϵ, and can be made as small as we want by decreasing c.

There is a large gap in the behavior of the two examples. In the first, the distance is very close to one, while in the second it is very close to zero. This means that when we estimate $\mathrm{SD}(X^\ell, Y^\ell)$ in terms of $\mathrm{SD}(X,Y)$, we have to take a *pessimistic* bound corresponding to the first example, which is far from the truth in case our distributions behave like in the second example.

Loosely speaking, log-ratio distance provides a "fine grained" view that distinguishes the above two cases. Note that $X_2 \overset{\mathrm{R}}{\approx}_{O(\epsilon),0} Y_2$, whereas there is no finite c for which $X_1 \overset{\mathrm{R}}{\approx}_{c,0} Y_1$. For X, Y such that $X \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} Y$ for $\delta = 0$ (or more generally, for $\delta \ll \epsilon$) we get the behavior of the second example under repetitions, yielding a better control on the resulting statistical distance. More precisely, it is not hard to show that if $X \overset{\mathrm{R}}{\approx}_\epsilon Y$ then for $\ell = c/\epsilon^2$ it holds that $X^\ell \overset{\mathrm{S}}{\approx}_{O(\sqrt{c \cdot ln(1/c)})} Y^\ell$.[5] A more precise statement and proof are given in Theorem 3.5.[6]

[5] Let us explain the intuition behind the above phenomenon. The maximum value of both $L_{X||Y}(s) = \log \frac{\Pr[X=s]}{\Pr[Y=s]}$ and $L_{Y||X}(s) = \log \frac{\Pr[Y=s]}{\Pr[X=s]}$, is at most ϵ. The relative entropy (also known as, KL divergence) $D(X||Y)$ measures the expectation of $L_{X||Y}(s)$ according to $s \leftarrow X$, and is therefore smaller than ϵ. But in fact it is easy to show that both $D(X||Y)$ and $D(Y||X)$ are bounded by $\epsilon \cdot (e^\epsilon - 1)$ which is approximately ϵ^2 for small ϵ. It follows that $D(X^\ell||Y^\ell) = \ell \cdot D(X||Y) \approx \ell\epsilon^2 = c$. In other words, the expectation of $L_{X^\ell||Y^\ell} = D(X^\ell||Y^\ell) = c$. The random variable $L_{X^\ell||Y^\ell}$ can be seen as the sum of ℓ independent copies of $L_{X||Y}$, and we know that each of these variables lies in the interval $[-\epsilon, \epsilon]$. By a standard Hoeffding bound it follows that the probability that $L_{X||Y}$ deviates from the expectation c, by say some quantity η is at most $e^{-\Omega(\frac{\eta^2}{\ell\epsilon^2})} = e^{-\Omega(\eta^2/c)}$ and this means that we can choose η to be roughly $\sqrt{c \cdot \ln(1/c)}$ and obtain that the probability of deviation is bounded by η. Overall, this gives that $X^\ell \overset{\mathrm{R}}{\approx} \eta + c, \eta Y^\ell$, meaning that except for an η fraction of the space, the ratio is bounded by $\eta + c$, and therefore, the statistical distance is also bounded by $O(\eta + c) = O(\sqrt{c \cdot \ln(1/c)})$.

[6] This phenomenon is the rationale behind the differential privacy boosting result of [8], and can be derived from the proof in that paper. In our setting, however, the proof is straightforward as outlined here, and shown in the proof of Theorem 3.5.

2.2 The Amplification Protocol

In this section we give a high level overview of the proof of Theorem 1.3. The starting point is a channel $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ that has α-agreement, and (ϵ, δ)-leakage. (A good example to keep in mind is the channel from Footnote 2). For simplicity of exposition, let us assume that $\delta = 0$ (the same proof will go through if δ is sufficiently small). Our goal is to obtain OT if $\alpha \geq c_1 \cdot \epsilon^2$ for some constant c_1, which we will choose to be sufficiently large.

Wullschleger [45] showed that a balanced channel with α'-agreement, and $(0, \epsilon')$-leakage (that is ϵ' leakage in statistical distance) implies OT if $\epsilon' \leq c_{\mathsf{Wul}} \cdot (\alpha')^2$ for some constant $c_{\mathsf{Wul}} > 0$. Thus, we are looking for a protocol, that starts with a channel that has $(\epsilon, 0)$-leakage and α-agreement, where ϵ is *larger* than α, and produces a channel with $(0, \epsilon')$-leakage, and α'-agreement where ϵ' is *smaller* than α'. We will use the following protocol achieving $\alpha' \geq 1/5$ and an arbitrarily small constant $\epsilon' > 0$.[7]

Protocol 2.1 ($\Delta_\ell^C = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}})$, amplification of log-ratio leakage)**.**

Channel: $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$.

Prameter: Number of samples ℓ.

Operation: Do until the protocol produces output:

1. *The parties activate the channel* C *for* ℓ *times. Let* $\overline{O}^{\mathsf{A}}$ *and* $\overline{O}^{\mathsf{B}}$ *be the* (ℓ*-bit) outputs.*
2. $\widetilde{\mathsf{A}}$ *sends the (unordered) set* $\mathcal{S} = \{\overline{O}^{\mathsf{A}}, \overline{O}^{\mathsf{A}} \oplus 1^\ell\}$ *to* $\widetilde{\mathsf{B}}$.
3. $\widetilde{\mathsf{B}}$ *informs* $\widetilde{\mathsf{A}}$ *whether* $\overline{O}^{\mathsf{B}} \in \mathcal{S}$.

   If positive, party $\widetilde{\mathsf{A}}$ *outputs zero if* $\overline{O}^{\mathsf{A}}$ *is the (lex.) smallest element in* $\mathcal{S}$*, and one otherwise. Party* $\widetilde{\mathsf{B}}$ *does the same with respect to* $\overline{O}^{\mathsf{B}}$*. (And the protocol halts.)*

Let $\Delta = \Delta_\ell^C$ for $\ell = 1/4\alpha$. We first observe that Δ halts in a given iteration iff the event $E = \left\{\overline{O}^{\mathsf{A}} \oplus \overline{O}^{\mathsf{B}} \in \{0^\ell, 1^\ell\}\right\}$ occurs. Note that $\Pr[E] \geq 2^{-\ell}$, and thus the expected running time of Δ is $O(2^\ell) = 2^{O(1/\alpha)}$.

We also observe that the outputs of the two parties agree, iff in the final (halting) iteration it holds that $\overline{O}^{\mathsf{A}} = \overline{O}^{\mathsf{B}}$. Thus, the agreement of Δ is given by:

$$\Pr[\overline{O}^{\mathsf{A}} = \overline{O}^{\mathsf{B}} | E] = \frac{(\frac{1}{2}+\alpha)^\ell}{(\frac{1}{2}+\alpha)^\ell + (\frac{1}{2}-\alpha)^\ell} = \left(1 + \left(\frac{\frac{1}{2}-\alpha}{\frac{1}{2}+\alpha}\right)^\ell\right)^{-1}$$
$$\approx \frac{1}{1+e^{-4\alpha\ell}} \geq \frac{1}{1+e^{-1}} \geq \tfrac{1}{2} + \alpha',$$

for $\alpha' \geq 1/5$.

In order to understand the leakage of Δ, we examine the views of the parties in the *final* iteration of Δ (it is clear that the views of the previous iteration yields no information). Let us denote these part of a view v by $\mathrm{final}(v)$. We are interested in understanding the log-ratio distance

[7] Similar protocols were used in the context of key-agreement amplification [4, 34].

between final$(V^{\widetilde{\mathsf{A}}}|_{O^{\tilde{\mathsf{A}}}=O^{\tilde{\mathsf{B}}}})$ and final$(V^{\widetilde{\mathsf{A}}}|_{O^{\tilde{\mathsf{A}}}\neq O^{\tilde{\mathsf{B}}}})$. Observe that final$(V^{\widetilde{\mathsf{A}}}|_{O^{\tilde{\mathsf{A}}}=O^{\tilde{\mathsf{B}}}})$ is a (deterministic) function of ℓ independent samples from $V^{\mathsf{A}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}}$ (i.e., the function that appends $\{\overline{O}^{\mathsf{A}}, \overline{O}^{\mathsf{A}} \oplus 1^{\ell}\}$ to the view), and final$(V^{\widetilde{\mathsf{A}}}|_{O^{\tilde{\mathsf{A}}}\neq O^{\tilde{\mathsf{B}}}})$ is the *same* deterministic function of ℓ independent samples from $V^{\mathsf{A}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}$. Thus, by data processing, it suffices to bound the distance of ℓ independent samples from $V^{\mathsf{A}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}}$ from ℓ independent samples from $V^{\mathsf{A}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}$. By assumption, C has $(\epsilon, 0)$-leakage, which means that

$$V^{\mathsf{A}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}} \overset{\mathrm{R}}{\approx}_{\epsilon,0} V^{\mathsf{A}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}.$$

In the previous section we showed that by choosing a sufficiently small constant $c > 0$ and taking $\ell = c/\epsilon^2$ repetitions of a pair of distributions with $(\epsilon, 0)$-log ratio distance, we obtain two distributions with statistical distance that is an arbitrary small constant $\epsilon' > 0$. Here we consider $\ell = 1/(4\alpha) = 1/(4c_1 \cdot \epsilon^2)$ repetitions, and therefore

$$\text{final}(V^{\widetilde{\mathsf{A}}}|_{O^{\tilde{\mathsf{A}}}=O^{\tilde{\mathsf{B}}}}) \overset{\mathrm{S}}{\approx}_{\epsilon'} \text{final}(V^{\widetilde{\mathsf{A}}}|_{O^{\tilde{\mathsf{A}}}\neq O^{\tilde{\mathsf{B}}}}).$$

By picking c_1 to be sufficiently large, we can obtain that the leakage in Δ is $\epsilon' \leq c_{\mathsf{Wul}} \cdot (\alpha')^2$ as required.

2.2.1 Efficient Amplification

The (expected) running time of Δ_ℓ is $2^{O(\ell)}$ that for the above choice of $\ell = \Theta(1/\alpha)$ equals $2^{O(1/\alpha)}$. To be useful in a setting when the running time is limited, e.g., in the computational setting, this dependency restricts us to "large" values of α. Fortunately, Protocol 2.1 can be modified so that its (expected) running time is only polynomial in $1/\alpha$.

Intuitively, rather than making ℓ invocations of C at once, and hope that the tuple of invocations happens to be *useful*: $\overline{O}^{\mathsf{A}} \oplus \overline{O}^{\mathsf{B}} \in \{0^\ell, 1^\ell\}$, the efficient protocol combines smaller tuples of useful invocations, i.e., $\overline{O}^{\mathsf{A}} \oplus \overline{O}^{\mathsf{B}} \in \left\{0^{\ell'}, 1^{\ell'}\right\}$, for some $\ell' < \ell$, into a useful tuple of ℓ invocations. The advantage is that failing to generate the smaller useful tuples, only "wastes" ℓ' invocations of C. By recursively sampling the ℓ' tuples via the same approach, we get a protocol whose expected running time is $O(\ell^2)$ (rather than $2^{O(\ell)}$).

The actual protocol implements the above intuition in the following way: on parameter d, protocol Λ_d mimics the interaction of the inefficient protocol Δ_{2^d} (i.e., the inefficient protocols with sample parameter 2^d). It does so by using Δ_2 to combines the outputs of two of execution of Λ_{d-1}. Effectively, this call to Δ_2 combines the two 2^{d-1} useful tuples produced by Λ_{d-1}, into a single 2^d useful tuple.

Let $\Lambda_0^C = C$, and recursively define Λ_d, for $d > 0$, as follows:

Protocol 2.2 ($\Lambda_d^C = (\widehat{\mathsf{A}}, \widehat{\mathsf{B}})$, efficient amplification of log-ratio leakage)**.**

Channel: C.

Prameter: log number of sample d.

Operation: The parties interact in $\Delta_2^{(\Lambda_{d-1}^C)}$.

By induction, the expected running time of Λ_d^C is 4^d. A more careful analysis yields that the view of Λ_d^C can be *simulated* by the view of $\Delta_{2^d}^C$. Indeed, there are exactly 2^d useful invocations

of C in an execution of Λ_d^C: invocations whose value was not ignored by the parties, and their distribution is exactly the same as the 2^d useful invocations of C in $\Delta_{2^d}^C$. Hence, using Λ_d^C with $d = \log 1/4\alpha$, we get a protocol whose expected running time is polynomial in $1/\alpha$ and guarantees the same level of agreement and security as of $\Delta_{1/4\alpha}$.

2.3 The Computational Case

So far, we considered information theoretic security. In order to prove Theorem 1.6 (that considers security against PPT adversaries) we note that Definition 1.5 (of computational leakage) is carefully set up to allow the argument of the previous section to be extended to the computational setting. Using the efficient protocol above, the reduction goes through as long as α is a noticeable function of the security parameter.

2.4 Two-Party Differentially Private XOR Implies OT

In this section we explain the main ideas that are used in the proof of Theorem 1.10. Our goal is to show that a perfect completeness, α-accurate, semi-honest ϵ-DP protocol for computing XOR, implies OT, if $\alpha \geq c \cdot \epsilon^2$ for a sufficiently large constant c. In order to prove this, we will show that such a protocol can be used to give a two-party protocol that has α-agreement and (computational) $(\epsilon, 0)$-leakage. Such a protocol yields OT by our earlier results.[8]

We remark that there are two natural definitions of "computational differential privacy" in the literature using either *computational indistinguishability* or *simulation* [36]. Definition 1.8 is using indistinguishability, while for our purposes, it is more natural to work with simulation (as using simulation enables us to "'switch back and forth" between the information theoretic setting and the computational setting). In general, these two definitions are not known to be equivalent. For functionalities like XOR, where the inputs of both parties are single bits, however, the two definitions are equivalent by the work of [36]. This means that when considering differential privacy of the XOR function, we can imagine that we are working in an information theoretic setting, in which there is a trusted party, that upon receiving the inputs x, y of the parties, provides party P, with its output O^{P} and view V^{P}. We will use the following protocol to obtain a "channel" with α-agreement and $(\epsilon, 0)$-leakage.

Protocol 2.3 (DP-XOR to channel)**.**

1. A *samples* $X \leftarrow \{0,1\}$ *and* B *samples* $Y \leftarrow \{0,1\}$.
2. *The parties apply the differentially private protocol for computing XOR, using inputs* X *and* Y *respectively, and receive outputs* $O_{DP}^{\mathsf{A}}, O_{DP}^{\mathsf{B}}$ *respectively.*
3. A *sends* $R \leftarrow \{0,1\}$ *to* B.
4. A *outputs* $O^{\mathsf{A}} = X \oplus R$ *and* B *outputs* $O_{DP}^{\mathsf{B}} \oplus Y \oplus R$.

[8] We believe that our results extend to the case of (ϵ, δ)-differential privacy, as long as $\delta = o(\epsilon^2)$, and then we obtain (ϵ, δ)-leakage, which is sufficient to yield OT. Proving this requires a careful examination of some of the previous work (which was stated for $\delta = 0$) and extending it to nonzero δ, as well as a more careful analysis on our part. We will not do this in this paper.

The intuition behind this protocol is that if $O^{\mathsf{B}}_{DP} = X \oplus Y$, then $O^{\mathsf{B}} = (X \oplus Y) \oplus Y \oplus R = X \oplus R = O^{\mathsf{A}}$. This means that the channel induced by this protocol inherits α-agreement from the α-accuracy of the original protocol. In Section 4 we show that this channel "inherits" log-ratio leakage of $(\epsilon, 0)$ from the fact that the original protocol is ϵ-DP.

3 Preliminaries

3.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables and functions, lowercase for values. For $a, b \in \mathbb{R}$, let $a \pm b$ stand for the interval $[a - b, a + b]$. For $n \in \mathbb{N}$, let $[n] = \{1, \ldots, n\}$ and $(n) = \{0, \ldots, n\}$. The Hamming distance between two strings $x, y \in \{0,1\}^n$, is defined by $\mathrm{Ham}(x, y) = \sum_{i \in [n]} x_i \neq y_i$. Let poly denote the set of all polynomials, let PPT stand for probabilistic polynomial time and PPTM denote a PPT TM (Turing machine) and let $\mathsf{ppt}^{\mathsf{NU}}$stands for a *non-uniform* PPTM. A function $\nu \colon \mathbb{N} \to [0,1]$ is *negligible*, denoted $\nu(n) = \mathrm{neg}(n)$, if $\nu(n) < 1/p(n)$ for every $p \in$ poly and large enough n.

3.2 Distributions and Random Variables

Given a distribution, or random variable, D, we write $x \leftarrow D$ to indicate that x is selected according to D. Given a finite set $\mathcal{S}$, let $s \leftarrow \mathcal{S}$ denote that s is selected according to the uniform distribution over $\mathcal{S}$. The support of D, denoted $\mathrm{Supp}(D)$, be defined as $\{u \in \mathcal{U} : D(u) > 0\}$. We will use the following distance measures.

Statistical distance.

Definition 3.1 (statistical distance)**.** *The* statistical distance *between two distributions P, Q over the same domain $\mathcal{U}$, (denote by $\mathrm{SD}(P,Q)$) is defined to be:*

$$SD(P,Q) = max_{\mathcal{A} \subseteq \mathcal{U}} |\Pr[P \in \mathcal{A}] - \Pr[Q \in \mathcal{A}]|.$$

*We say that P, Q are ϵ-*close *(denoted by $P \overset{\mathrm{S}}{\approx}_\epsilon Q$) if $\mathrm{SD}(P,Q) \leq \epsilon$.*

We use the following fact, proof given in the appendix.

Proposition 3.2. *Let $0 < \epsilon < \mu < 1$, and let (X,Y), $(\tilde{X}, \tilde{Y})$ be two pairs of random variables over the same domain $\mathcal{X} \times \mathcal{Y}$, such that $\mathrm{SD}((X,Y),(\tilde{X},\tilde{Y})) \leq \epsilon$. Let $E_0, E_1 \subseteq \mathcal{X} \times \mathcal{Y}$ be two sets such that for every $b \in \{0,1\}$, $\Pr[(X,Y) \in E_b] \geq \mu$. Then $\mathrm{SD}(\tilde{X}|_{\{(\tilde{X},\tilde{Y}) \in E_0\}}, \tilde{X}|_{\{(\tilde{X},\tilde{Y}) \in E_1\}}) \leq \mathrm{SD}(X|_{\{(X,Y) \in E_0\}}, X|_{\{(X,Y) \in E_1\}}) + 4\epsilon/\mu$.*

Log-Ratio distance. We will also be interested in the following natural notion of "log-ratio distance" which was popularized by the literature on differential privacy.

Definition 3.3 (Log-Ratio distance)**.** *Two numbers $p_0, p_1 \geq 0$ satisfy $p_0 \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} p_1$ if for both $b \in \{0,1\}$: $p_b \leq e^\epsilon \cdot p_{1-b} + \delta$. Two distributions P, Q over the same domain $\mathcal{U}$, are (ϵ, δ)-*log-ratio-close *(denoted $P \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} Q$) if for every $\mathcal{A} \subseteq \mathcal{U}$:*

$$\Pr[P \in \mathcal{A}] \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} \Pr[Q \in \mathcal{A}].$$

We let $\overset{\mathrm{R}}{\approx}_{\epsilon}$ *stands for* $\overset{\mathrm{R}}{\approx}_{\epsilon,0}$.

It is immediate that $D_0 \overset{\mathrm{S}}{\approx}_{\delta} D_1$ iff $D_0 \overset{\mathrm{R}}{\approx}_{0,\delta} D_1$, and that $D_0 \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} D_1$ implies $D_0 \overset{\mathrm{S}}{\approx}_{(e^{\epsilon}-1)+\delta} D_1$, and note that for $\epsilon \in [0,1]$, $e^{\epsilon}-1 = O(\epsilon)$. It is also immediate that the log-ratio distance respects data processing.

Fact 3.4. *Assume* $P \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} Q$*, then* $f(P) \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} f(Q)$ *for any (possibly randomized) function* f*.*

Log-Ratio distance under independent repetitions. As demonstrated by the framework of differential privacy, working with this notion of "relative distance" is often a very convenient distance measure between distributions, as it behaves nicely when considering independent executions. Specifically, let D^{ℓ} denote ℓ independent copies from D, the following follows:

Theorem 3.5 (Relative distance under independent repetitions)**.**
If $D_0 \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} D_1$ *then for every* $\ell \geq 1$*, and every* $\delta' \in (0,1)$

$$D_0^{\ell} \overset{\mathrm{R}}{\approx}_{(\eta(\epsilon,\ell,\delta'),\ell\delta+\delta')} D_1^{\ell},$$

where $\eta(\epsilon,\ell,\delta') = \ell \cdot \epsilon(e^{\epsilon}-1) + \epsilon \cdot \sqrt{2\ell \cdot \ln(1/\delta')}$.

We remark that Theorem 3.5 can also be derived by the (much more complex) result on "boosting differential privacy" [10]. However, it can be easily derived directly by a Hoeffding bound, as is done in the next two lemmata.

Lemma 3.6. *If* $D_0 \overset{\mathrm{R}}{\approx}_{\epsilon} D_1$ *then for each* $b \in \{0,1\}$, $\mathrm{E}_{x \leftarrow D_b}\left[\log \frac{\Pr_{D_b}[x]}{\Pr_{D_{1-b}}[x]}\right] \leq \epsilon(e^{\epsilon}-1)$.

The term $\mathrm{E}_{x \leftarrow D_b}\left[\log \frac{\Pr_{D_b}[x]}{\Pr_{D_{1-b}}[x]}\right]$ is also known as the KL-divergence between D_b and D_{1-b}, which is known to be non-negative for every two distribution D_0, D_1.

Proof.

$$\begin{aligned}
&\mathop{\mathrm{E}}_{x \leftarrow D_b}\left[\log \frac{\Pr_{D_b}[x]}{\Pr_{D_{1-b}}[x]}\right] \leq \mathop{\mathrm{E}}_{x \leftarrow D_b}\left[\log \frac{\Pr_{D_b}[x]}{\Pr_{D_{1-b}}[x]}\right] + \mathop{\mathrm{E}}_{x \leftarrow D_{1-b}}\left[\log \frac{\Pr_{D_{1-b}}[x]}{\Pr_{D_b}[x]}\right] \\
&= \sum_{x \in \mathcal{U}} \Pr_{D_b}[x]\left(\log \frac{\Pr_{D_b}[x]}{\Pr_{D_{1-b}}[x]} + \log \frac{\Pr_{D_{1-b}}[x]}{\Pr_{D_b}[x]}\right) + \sum_{x \in \mathcal{U}}\left(\Pr_{D_{1-b}}[x] - \Pr_{D_b}[x]\right) \log \frac{\Pr_{D_{1-b}}[x]}{\Pr_{D_b}[x]} \\
&= \sum_{x \in \mathcal{U}}\left(\Pr_{D_{1-b}}[x] - \Pr_{D_b}[x]\right) \log \frac{\Pr_{D_{1-b}}[x]}{\Pr_{D_b}[x]} \\
&\leq \epsilon \cdot \sum_{x \in \mathcal{U}}\left|\Pr_{D_{1-b}}[x] - \Pr_{D_b}[x]\right| \\
&\leq \epsilon \cdot \sum_{x \in \mathcal{U}}(e^{\epsilon}-1)\min\left(\Pr_{D_{1-b}}[x], \Pr_{D_b}[x]\right) \\
&= \epsilon \cdot (e^{\epsilon}-1)\sum_{x \in \mathcal{U}} \min\left(\Pr_{D_{1-b}}[x], \Pr_{D_b}[x]\right) \leq \epsilon \cdot (e^{\epsilon}-1).
\end{aligned}$$

Where the first inequality holds since KL-divergence is non-negative, and the second and third inequalities holds from the definition of Log-Ratio distance. □

Lemma 3.7. *If $D_0 \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} D_1$, then for each $b \in \{0,1\}$ there exist distributions D'_b such that $D'_b \overset{\mathrm{R}}{\approx}_{\epsilon} D_{1-b}$, and, $D'_b \overset{\mathrm{S}}{\approx}_{\delta} D_b$.*

Proof. Fix $b \in \{0,1\}$, and let $\mathcal{S}^+ \subseteq \mathcal{U}$ be the set of all x such that $\Pr_{D_b}[x] > e^{\epsilon} \cdot \Pr_{D_{1-b}}[x]$, and $\mathcal{S}^-$ be the set of all x with $\Pr_{D_b}[x] < e^{-\epsilon} \cdot \Pr_{D_{1-b}}[x]$. First, notice that

$$\Pr_{D_b}\left[\mathcal{S}^+\right] - e^{\epsilon} \cdot \Pr_{D_{1-b}}\left[\mathcal{S}^+\right] \leq \delta, \qquad e^{-\epsilon} \cdot \Pr_{D_{1-b}}\left[\mathcal{S}^-\right] - \Pr_{D_b}\left[\mathcal{S}^-\right] \leq \delta \tag{1}$$

Indeed, by the log-ration distance between D_0 and D_1, we get that $\Pr_{D_b}[\mathcal{S}^+] \leq e^{\epsilon} \cdot \Pr_{D_{1-b}}[\mathcal{S}^+] + \delta$, and $\Pr_{D_{1-b}}[\mathcal{S}^-] \leq e^{\epsilon} \cdot \Pr_{D_b}[\mathcal{S}^-] + \delta$.

In the following we assume for simplicity that $\Pr_{D_b}[\mathcal{S}^+] - e^{\epsilon} \cdot \Pr_{D_{1-b}}[\mathcal{S}^+] \geq e^{-\epsilon} \cdot \Pr_{D_{1-b}}[\mathcal{S}^-] - \Pr_{D_b}[\mathcal{S}^-]$, as the other case symmetrically follows.

In the following, it is shown how to modify D_b to construct D'_b. This is done by reducing the probability of every $x \in \mathcal{S}^+$, and increasing the probability of every $x \in \mathcal{S}^-$, to keep it inside the range $[e^{-\epsilon} \Pr_{D_{1-b}}[x], e^{\epsilon} \Pr_{D_{1-b}}[x]]$. To make sure that the resulting D'_b is a probability distribution ($\sum_x \Pr_{D'_b}[x] = 1$), the probability of other elements may have to be changed. For this purpose, consider the set $\mathcal{A} = \left\{x : \Pr_{D_{1-b}}[x] > \Pr_{D_b}[x]\right\}$. Notice that $\mathcal{S}^- \subseteq \mathcal{A}$, and it holds that

$$\begin{aligned} \Pr_{D_{1-b}}[\mathcal{A}] - \Pr_{D_b}[\mathcal{A}] &= \sum_{x \in \mathcal{A}} \Pr_{D_{1-b}}[x] - \Pr_{D_b}[x] \\ &= \sum_{x \notin \mathcal{A}} \Pr_{D_b}[x] - \Pr_{D_{1-b}}[x] \geq \Pr_{D_b}\left[\mathcal{S}^+\right] - e^{\epsilon} \cdot \Pr_{D_{1-b}}\left[\mathcal{S}^+\right] \end{aligned} \tag{2}$$

Where the second equality holds since $\sum_x \Pr_{D_b}[x] = \sum_x \Pr_{D_{1-b}}[x] = 1$.

We get that

$$\Pr_{D_{1-b}}[\mathcal{A}] - \Pr_{D_b}[\mathcal{A}] \geq \Pr_{D_b}\left[\mathcal{S}^+\right] - e^{\epsilon} \cdot \Pr_{D_{1-b}}\left[\mathcal{S}^+\right] \geq e^{-\epsilon} \cdot \Pr_{D_{1-b}}\left[\mathcal{S}^-\right] - \Pr_{D_b}\left[\mathcal{S}^-\right] \tag{3}$$

Thus, we can define D'_b as following:

- For every $x \in \mathcal{S}^+$, $\Pr_{D'_b}[x] = e^{\epsilon} \cdot \Pr_{D_{1-b}}[x]$.
- For every $x \notin \mathcal{A} \cup \mathcal{S}^+$, $\Pr_{D'_b}[x] = \Pr_{D_b}[x]$.
- For every $x \in \mathcal{A}$, $\max(\Pr_{D_b}[x], e^{-\epsilon} \cdot \Pr_{D_{1-b}}[x]) \leq \Pr_{D'_b}[x] \leq \Pr_{D_{1-b}}[x]$, such that $\sum_{x \in \mathcal{U}} \Pr_{D'_b}[x] = 1$.

It is clear from Equation (1) that $D'_b \overset{\mathrm{S}}{\approx}_{\delta} D_b$. Also, from definition it holds that for every x, $\Pr_{D'_b}[x] \overset{\mathrm{R}}{\approx}_{\epsilon} \Pr_{D_{1-b}}[x]$. □

Theorem 3.8 (Hoeffding bound [25])**.** *Let $A_1, ..., A_\ell$ be independent random variables s.t. $A_i \in [-c, c]$ and let $\widehat{A} = \Sigma_{i=1}^{\ell} A_i$. It holds that:*

$$\Pr\left[\widehat{A} - \mathrm{E}\left[\widehat{A}\right] \geq t\right] \leq e^{-t^2/2\ell c^2}.$$

Proof of Theorem 3.5. First, we show the proof for the case that $\delta = 0$. Later it is show how to use Lemma 3.7 in order to reduce the general case to this one.

For $\delta = 0$, fix $b \in \{0,1\}$, and let $\mathcal{A} \subseteq \mathcal{U}^\ell$ be some set. It suffice to show that $\Pr\left[D_b^\ell \in \mathcal{A}\right] \leq e^{\eta(\epsilon,\ell,\delta')} \cdot \Pr\left[D_{1-b}^\ell \in \mathcal{A}\right] + \delta'$.

Consider the set $\mathcal{S} := \left\{ y \mid \log \frac{D_b^\ell(y)}{D_{1-b}^\ell(y)} \geq \eta(\epsilon,\ell,\delta') \right\}$. It holds that:

$$\begin{aligned} \Pr\left[D_b^\ell \in \mathcal{A}\right] &= \Pr\left[D_b^\ell \in \mathcal{A} \setminus \mathcal{S}\right] + \Pr\left[D_b^\ell \in \mathcal{A} \cap \mathcal{S}\right] \\ &\leq e^{\eta(\epsilon,\ell,\delta')} \cdot \Pr\left[D_{1-b}^\ell \in \mathcal{A} \setminus \mathcal{S}\right] + \Pr\left[D_b^\ell \in \mathcal{A} \cap \mathcal{S}\right] \\ &\leq e^{\eta(\epsilon,\ell,\delta')} \cdot \Pr\left[D_{1-b}^\ell \in \mathcal{A}\right] + \Pr\left[D_b^\ell \in \mathcal{S}\right]. \end{aligned} \tag{4}$$

It therefore enough to show that $\Pr\left[D_b^\ell \in \mathcal{S}\right] \leq \delta'$. For this goal, consider the random variable $\widehat{A} = \log \frac{\Pr_{D_b^\ell}[X_1,\ldots,X_\ell]}{\Pr_{D_{1-b}^\ell}[X_1,\ldots,X_\ell]}$, where $X_1,\ldots,X_\ell$ are independent samples from D_b. Let $A_i := \log \frac{\Pr_{D_b}[X_i]}{\Pr_{D_{1-b}}[X_i]}$. Then it holds that $\widehat{A} = \sum_{i=1}^{\ell} A_i$, where for every i, $A_i \in [-\epsilon,\epsilon]$. By Lemma 3.6, it holds that for every i, $E[A_i] \leq \epsilon \cdot (e^\epsilon - 1)$. Therefore, by the Hoeffding bound,

$$\Pr\left[D_b^\ell \in \mathcal{S}\right] \leq \Pr\left[\widehat{A} \geq \ell \cdot \epsilon(e^\epsilon - 1) + \epsilon \cdot \sqrt{2\ell \cdot \ln(1/\delta')}\right] \leq e^{-(\epsilon \cdot \sqrt{2\ell \cdot \ln(1/\delta')})^2/2\ell\epsilon^2} = \delta'. \tag{5}$$

In the general case, for $\delta > 0$, let D'_b be the distribution promised in Lemma 3.7. By applying the above on D'_b, D_{1-b}, we get that for every set $\mathcal{A} \subseteq \mathcal{U}^\ell$, it holds that

$$\Pr_{D'^\ell_b}[\mathcal{A}] \leq e^{\eta(\epsilon,\ell,\delta')} \Pr_{D'^\ell_{1-b}}[\mathcal{A}] + \delta'. \tag{6}$$

Using the triangle inequality for statistical distance, it follows that:

$$\Pr_{D_b^\ell}[\mathcal{A}] \leq \Pr_{D'^\ell_b}[\mathcal{A}] + \ell\delta \leq e^{\eta(\epsilon,\ell,\delta')} \Pr_{D_{1-b}^\ell}[\mathcal{A}] + \delta' + \ell\delta. \tag{7}$$

□

Computational indistinguishability.

Definition 3.9 (Computational indistinguishability)**.** *Two distribution ensembles $X = \{X_\kappa\}_{\kappa\in\mathbb{N}}$, $Y = \{Y_\kappa\}_{\kappa\in\mathbb{N}}$ are* [resp., non-uniformly] computationally indistinguishable*, denoted $X \overset{\text{C}}{\approx} Y$ [resp., $X \overset{\text{nuC}}{\approx} Y$] if for every* PPT *[resp.,* $\mathsf{ppt}^{\mathsf{NU}}$*]* D*:*

$$|\Pr[\mathsf{D}(1^\kappa, X_\kappa) = 1] - \Pr[\mathsf{D}(1^\kappa, Y_\kappa) = 1]| \leq \text{neg}(\kappa).$$

3.3 Protocols

Let $\Pi = (\mathsf{A},\mathsf{B})$ be a two-party protocol. Protocol Π is PPT if both A and B running time is polynomial in their input length. We denote by $(\mathsf{A}(x_\mathsf{A}),\mathsf{B}(x_\mathsf{B}))(z)$ a random execution of Π with private inputs $(x_\mathsf{A}, y_\mathsf{A})$, and common input z. At the end of such an execution, party $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$ obtains his view $V^\mathsf{P}(x_\mathsf{A}, x_\mathsf{B}, z)$, which may also contain a "designated output" $O^\mathsf{P}(x_\mathsf{A}, x_\mathsf{B}, z)$ (if the protocol specifies such an output). A protocol has Boolean output, if each party outputs a bit.

3.4 Two-Output Functionalities and Channels

A two-output *functionality* is just a random function that outputs a tuple of two values in a predefined domain. In the following we omit the two-output term from the notation.

Channels. A *channel* is simply a no-input functionality with designated output bits. We naturally identify channels with the random variable characterizes their output.

Definition 3.10 (Channels)**.** *A* channel *is a no-input Boolean functionality whose output pair is of the from* $((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ *and for both* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$*,* O^{P} *is Boolean and determined by* V^{P}*. A channel has* agreement α *if* $\Pr\left[O^{\mathsf{A}} = O^{\mathsf{B}}\right] = \frac{1}{2} + \alpha$*. A channel ensemble* $\{C_\kappa\}_{\kappa\in\mathbb{N}}$ *has agreement* α *if* C_κ *has agreement* $\alpha(\kappa)$ *for every* κ*.*

It is convenient to view a channel as the experiment in which there are two parties A and B. Party A receives "output" O^{A} and "view" V^{A}, and party B receives "output" O^{B} and "view" V^{B}.

We identify a no-input Boolean output protocol with the channel "induced" by its semi-honest execution.

Definition 3.11 (The protocol's channel)**.** *For a no-input Boolean output protocol* Π*, we define the channel* $\mathrm{CHN}(\Pi)$ *by* $\mathrm{CHN}(\Pi) = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$*, for* V^{P} *and* O^{P} *being the view and output of party* P *in a random execution of* Π*. Similarly, for protocol* Π *whose only input is a security parameter, let* $\mathrm{CHN}(\Pi) = \{\mathrm{CHN}(\Pi)_\kappa = \mathrm{CHN}(\Pi(1^\kappa))\}_{\kappa\in\mathbb{N}}$*.*

All protocols we construct in this work are *oblivious*, in the sense that given oracle access to a channel, the parties only make use of the channel output (though the channel's view becomes part of the party view).[9]

3.5 Secure Computation

We use the standard notion of securely computing a functionality, cf., [12].

Definition 3.12 (Secure computation)**.** *A two-party protocol* securely computes a functionality f*, if it does so according to the real/ideal paradigm. We add the term perfectly/statistically/computationally/non-uniform computationally, if the the simulator output is perfect/statistical/computationally indistinguishable/ non-uniformly indistinguishable from the real distribution. The protocol have the above notions of security* against semi-honest adversaries*, if its security only guaranteed to holds against an adversary that follows the prescribed protocol. Finally, for the case of perfectly secure computation, we naturally apply the above notion also to the non-asymptotic case: the protocol with no security parameter perfectly compute a functionality* f*.*

A two-party protocol securely computes a functionality ensemble f in the g-hybrid model*, if it does so according to the above definition when the parties have access to a trusted party computing* g*. All the above adjectives naturally extend to this setting.*

[9] This is in accordance with definition of channels in the literature in which the view component of the channel is only accessible to the eavesdropper (and not to the honest parties using the channel).

3.6 Oblivious Transfer

The (one-out-of-two) oblivious transfer functionality is defined as follows.

Definition 3.13 (oblivious transfer functionality f_{OT})**.** *The oblivious transfer functionality over* $\{0,1\} \times (\{0,1\}^*)^2$ *is defined by* $f_{\mathrm{OT}}(i,(\sigma_0,\sigma_1)) = (\perp,\sigma_i)$.

A protocol is $*$ secure OT, for
$* \in$ {semi-honest statistically/computationally/computationally non-uniform}, if it compute the f_{OT} functionality with $*$ security.

3.7 Two-Party Differential Privacy

We consider differential privacy in the 2-party setting.

Definition 3.14 (Differentially private functionality)**.** *A functionality* f *over input domain* $\{0,1\}^n \times \{0,1\}^n$ *is* ϵ-DP*, if the following holds: let* $(V^{\mathsf{A}}_{x,y}, V^{\mathsf{B}}_{x,y}) = f(x,y)$*, then for every* x, x' *with* $\mathrm{Ham}(x,x') = 1$*,* $y \in \{0,1\}^n$ *and* $v \in \mathrm{Supp}(V^{\mathsf{B}}_{x,y})$*:*

$$\Pr\left[V^{\mathsf{B}}_{x,y} = v\right] \leq e^{\epsilon} \cdot \Pr\left[V^{\mathsf{B}}_{x',y} = v\right],$$

and the for every y, y' *with* $\mathrm{Ham}(y,y') = 1$*,* $x \in \{0,1\}^n$ *and* $v \in \mathrm{Supp}(V^{\mathsf{A}}_{x,y})$*:*

$$\Pr\left[V^{\mathsf{A}}_{x,y} = v\right] \leq e^{\epsilon} \cdot \Pr\left[V^{\mathsf{A}}_{x,y'} = v\right].$$

Note that the above definition is equivalence to asking that $V^{\mathsf{B}}_{x,y} \overset{\mathrm{R}}{\approx}_{\epsilon} V^{\mathsf{B}}_{x',y}$ for any x, x' with $\mathrm{Ham}(x,x') = 1$ and y, and analogously for the view of A, for $\overset{\mathrm{R}}{\approx}_{\epsilon}$ being the log-ratio according to Definition 3.3.

We also remark that a more general definition allows also an additive error δ in the above, making the functionality (ϵ,δ)-DP. However, for the sake simplicity, we focus on the simpler notion of ϵ-DP stated above.

Definition 3.15 (Differentially private computation)**.** *A* PPT *two-output protocol* $\Pi = (\mathsf{A},\mathsf{B})$ *over input domain* $\{0,1\}^n \times \{0,1\}^n$ *is* ϵ-IND-DP *if the following holds for every* $\mathsf{ppt}^{\mathsf{NU}}$ B^**,* D *and* $x, x' \in \{0,1\}^n$ *with* $\mathrm{Ham}(x,x') = 1$*: let* $V^{\mathsf{B}^*}_x$ *be the view of* B^* *in a random execution of* $(\mathsf{A}(x), \mathsf{B}^*)(1^\kappa)$*, then*

$$\Pr\left[\mathsf{D}(V^{\mathsf{B}^*}_x) = 1\right] \leq e^{\epsilon(\kappa)} \cdot \Pr\left[\mathsf{D}(V^{\mathsf{B}^*}_{x'}) = 1\right] + \mathrm{neg}(\kappa),$$

and the same hold for the secrecy of B.

Such a protocol is semi-honest ϵ-IND-DP*, if the above is only guaranteed to hold for semi-honest adversaries (i.e., for* $\mathsf{B}^* = \mathsf{B}$*).*

3.8 Passive Weak Binary Symmetric Channels

We rely on the work of Wullschleger [45] that shows that certain channels imply oblivious transfer. The following notion, adjusted to our formulation, of a "Passive weak binary symmetric channel" was studied in [45].

Definition 3.16 (Passive weak binary symmetric channels, WBSC, [45])**.** *An* $(\mu, \epsilon_0, \epsilon_1, p, q)$-WBSC *is a channel* $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ *such that the following holds:*

- *Correctness:* $\Pr\left[O^{\mathsf{A}} = 0\right] \in [\frac{1}{2} - \mu/2, \frac{1}{2} + \mu/2]$
  and for every $b_{\mathsf{A}} \in \{0,1\}$, $\Pr\left[O^{\mathsf{B}} \neq O^{\mathsf{A}} \mid O^{\mathsf{A}} = b_{\mathsf{A}}\right] \in [\epsilon_0, \epsilon_1]$.
- *Receiver security:* $(V^{\mathsf{A}}, O^{\mathsf{A}})|_{O^{\mathsf{B}}=O^{\mathsf{A}}} \overset{\mathrm{S}}{\approx}_p (V^{\mathsf{A}}, O^{\mathsf{A}})|_{O^{\mathsf{B}}\neq O^{\mathsf{A}}}$.[10]
- *Sender security: for every* $b_{\mathsf{B}} \in \{0,1\}$, $V^{\mathsf{B}}|_{O^{\mathsf{B}}=b_{\mathsf{B}},O^{\mathsf{A}}=0} \overset{\mathrm{S}}{\approx}_q V^{\mathsf{B}}|_{O^{\mathsf{B}}=b_{\mathsf{B}},O^{\mathsf{A}}=1}$.

The following was proven in [45].

Theorem 3.17 (WBSC implies oblivious transfer)**.** *There exist a protocol* Δ *such that the following holds. Let* $\epsilon, \epsilon_0 \in (0, 1/2), p \in (0,1)$ *be such that* $150(1-(1-p)^2) < (1 - \frac{2\epsilon^2}{\epsilon^2+(1-\epsilon)^2})^2$*, and* $\epsilon_0 \leq \epsilon$*. Let* C *be a* $(0, \epsilon_0, \epsilon_0, p, p)$-WBSC*. Then* $\Delta(1^\kappa, \epsilon)$ *is a semi-honest statistically secure OT in the* C*-hybrid model, and its running time is polynomial in* κ*,* $1/\epsilon$ *and* $1/(1-2\epsilon)$*. Furthermore, the parties in* Δ *only makes use of the output bits of the channel.*

Theorem 3.17 considers channels with $\mu = 0$, and $\epsilon_0 = \epsilon_1$. This is equivalent to saying that the channel is balanced (i.e., each of the output bits is uniform) and has α-agreement, for $\alpha = \frac{1}{2} - \epsilon_0$. When stated in this form, Theorem 3.17 says that such a channel implies OT if $p = O(\alpha^2)$, and in particular, it is required that $p < \alpha$.

3.8.1 Specialized Passive Weak Binary Symmetric Channels

We will be interested in a specific choice of parameters for passive WBSC's, and for this choice, it will be more convenient to work with the following stronger notion of a channel (that is easier to state and argue about, as security is defined in the same terms for both parties).

Definition 3.18 (Specialized passive weak binary symmetric channels)**.** *An* (ϵ_0, p)-SWBSC *is a channel* $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ *such that the following holds:*

- *Correctness:* $\Pr\left[O^{\mathsf{A}} = 0\right] = \frac{1}{2}$*, and for every* $b_{\mathsf{A}} \in \{0,1\}$,
  $\Pr\left[O^{\mathsf{B}} \neq O^{\mathsf{A}} \mid O^{\mathsf{A}} = b_{\mathsf{A}}\right] = \epsilon_0$.
- *Receiver security:* $V^{\mathsf{A}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}} \overset{\mathrm{S}}{\approx}_p V^{\mathsf{A}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}$.
- *Sender security:* $V^{\mathsf{B}}|_{O^{\mathsf{B}}=O^{\mathsf{A}}} \overset{\mathrm{S}}{\approx}_p V^{\mathsf{B}}|_{O^{\mathsf{B}}\neq O^{\mathsf{A}}}$.

Proposition 3.19. *An* (ϵ_0, p)-SWBSC *is a* $(0, \epsilon_0, \epsilon_0, 2p, 2p)$-WBSC.

The proof for Proposition 3.19 appears in Appendix A.

[10] In the requirement above, one can replace $(V^{\mathsf{A}}, O^{\mathsf{A}})$ with V^{A} (as by our conventions the latter determines the former). We remark that [45] does not use this convention, and this is why we explicitly include the random variable O^{A}.

3.9 Additional Inequalities

The following fact is proven in Appendix A.

Proposition 3.20. *The following holds for every $b \in (0, 1/2)$ and $\ell \in \mathbb{N}$ such that $b\ell < 1/4$.*

$$\frac{(1/2+b)^\ell}{(1/2+b)^\ell + (1/2-b)^\ell} \in [\tfrac{1}{2}(1+b\ell), \tfrac{1}{2}(1+3b\ell)].$$

4 Amplification of Channels with Small Log-Ratio Leakage

In this section we formally define log-ratio leakage and prove our amplification results. We start in Section 4.1 with the information theoretic setting, in which we restate and prove Theorem 1.3 and Theorem 1.4. In Section 4.2 we extend our result to the computational setting, restating and proving Theorem 1.6.

4.1 The Information Theoretic Setting

We start with a definition of log-ratio leakage (restating Definition 1.2 with more formal notation).

Definition 4.1 (Log-ratio leakage)**.** *A channel $((O^{\mathsf{A}}, V^{\mathsf{A}}), (O^{\mathsf{B}}, V^{\mathsf{B}}))$ has* (ϵ, δ)-leakage *if*

- *Receiver security:* $V^{\mathsf{A}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}} \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} V^{\mathsf{A}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}$.
- *Sender security:* $V^{\mathsf{B}}|_{O^{\mathsf{A}}=O^{\mathsf{B}}} \overset{\mathrm{R}}{\approx}_{\epsilon,\delta} V^{\mathsf{B}}|_{O^{\mathsf{A}}\neq O^{\mathsf{B}}}$.

The following theorem is a formal restatement of Theorem 1.3

Theorem 4.2 (Small log-ratio leakage implies OT)**.** *There exists an (oblivious)* PPT *protocol Δ and constant $c_1 > 0$ such that the following holds. Let $\epsilon, \delta \in [0, 1]$ be such that $\delta \leq \epsilon^2$, and let $\alpha \leq \alpha_{\max} < 1/8$ be such that $\alpha \geq \max\{c_1 \cdot \epsilon^2, \alpha_{\max}/2\}$. Then for any channel C with (ϵ, δ)-*leakage *and α-agreement, protocol $\Delta^C(1^\kappa, 1^{\lfloor 1/\alpha_{\max} \rfloor})$ is a semi-honest statistically secure OT in the C-hybrid model.*

Before proving Theorem 4.2, we first show that it is tight.

Theorem 4.3 (Triviality of channels with large leakage)**.** *There exists a constant $c_2 > 0$, such that for every $\epsilon > 0$ there is a two-party protocol (with no inputs) where at the end of the protocol, every party $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ has output O^{P} and view V^{P}. Moreover, the induced channel $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ has α-agreement,and $(\epsilon, 0)$-leakage, for $\alpha \geq c_2 \cdot \epsilon^2$.*

Together, the two theorems show that if $\alpha \geq c_1 \cdot \epsilon^2$ then the channel yields OT, and if $\alpha \leq c_2 \cdot \epsilon^2$ then such a channel can be simulated by a two-party protocol with no inputs (and thus cannot yield OT with information theoretic security).

Theorem 4.3 is proven in Section 4.1.4.

The proof of Theorem 4.2 is an immediate consequence of the following two lemmata.

Recall (Definition 3.11) that CHN(Π) denotes the channel induced by a random execution of the no-input, Boolean output protocol Π.

Lemma 4.4 (Gap amplification)**.** *There exists an (oblivious)* PPT *protocol* Δ *and constant* $c_1 > 0$ *such that the following holds. Let* $\epsilon, \delta, \alpha, \alpha_{\max}$ *be parameters satisfying requirements in Theorem 4.2 with respect to* c_1*. Let* C *be a channel with* (ϵ, δ)-leakage *and* α*-agreement, let* $\ell = 2^{(\lfloor \log 1/\alpha_{\max} \rfloor - 2)}$ *and let* $\widetilde{C} = \mathrm{CHN}(\Delta^C(1^\ell))$*. Then*

- $\widetilde{C}$ *has* $\widetilde{\alpha} \in [1/32, 3/8]$-agreement*.*
- *For any* $\delta' \in (0,1)$*:* $\widetilde{C}$ *has* $(\widetilde{\epsilon}, \widetilde{\delta})$-leakage *for* $\widetilde{\epsilon} = 2\ell\epsilon^2 + \epsilon\sqrt{2\ell \ln(1/\delta')}$ *and* $\widetilde{\delta} = \delta' + \ell\delta$*.*

Definition 4.5 (Bounded execution)**.** *Given Boolean output protocol* Π *and* $n \in \mathbb{N}$*, let* $\mathsf{bound}_n(\Pi)$ *be the variant of* Π *that if the protocol does not halt after* n *steps, it halts and the parties output uniform independent bits.*

Lemma 4.6 (Large Gap to OT)**.** *There exist an (oblivious)* PPT *protocol* Δ *and constants* $n, c > 0$ *such that the following holds: let* Π *be a protocol of expected running time at most* t *that induces a channel* C *with* $\alpha \in [1/32, 3/8]$*-agreement, and* (ϵ, δ)-leakage *for* $\epsilon, \delta \leq c$*.*

Then $\Delta^{C'}(1^\kappa)$ *is a semi-honest statistically secure OT in the* $C' = \mathrm{CHN}(\mathsf{bound}_{n \cdot t}(\Pi))$ *hybrid model.*

We prove the above two Lemmas in the following subsections, but first we will prove Theorem 4.2.

Proof of Theorem 4.2. Let $\ell = 2^{(\lfloor \log 1/\alpha_{\max} \rfloor - 2)}$. By Lemma 4.4, there exists an expected polynomially time protocol Λ such that $\Lambda^C(1^\ell)$ induces a channel $\widetilde{C}$ of $\widetilde{\alpha} \in [1/32, 3/8]$-agreement, and $(\widetilde{\epsilon}, \widetilde{\delta})$-leakage for $\widetilde{\epsilon} = 2\ell\epsilon^2 + \epsilon\sqrt{2\ell \ln(1/\delta')}$ and $\widetilde{\delta} = \delta' + \ell\delta$, for any $\delta' \in (0,1)$.

Let $t \in \mathrm{poly}$ be a polynomial that bounds the expected running time of Λ. By Lemma 4.6, there exist universal constants n, c and PPT protocol Δ, such that if

$$\widetilde{\epsilon} = 2\ell\epsilon^2 + \epsilon\sqrt{2\ell \ln(1/\delta')} \leq c \qquad \text{and} \qquad \widetilde{\delta} = \delta' + \ell\delta \leq c \tag{8}$$

then the protocol Γ, defined by $\Gamma^C(1^\kappa, 1^{\lfloor 1/\alpha_{\max} \rfloor}) = \Delta^{C'}(1^\kappa)$ for
$C' = \mathrm{CHN}(\mathsf{bound}_{n \cdot t(\ell)}(\Lambda^C(1^\ell)))$, is a semi-honest statistically secure OT. Hence, we conclude the proof noting that Equation (8) holds by setting $\delta' = \ell\delta$ and choosing c_1 (the constant in Theorem 4.2) to be sufficiently large.

□

Lemma 4.6 is proved in Section 4.1.3 using the amplification result of [45]. Toward proving Lemma 4.4, our main technical contribution, we start in Section 4.1.1 by presenting an inefficient protocol implementing the desired channel. In Section 4.1.2 we show how to bootstrap the the above protocol into an efficient one.

4.1.1 Inefficient Amplification

The following protocol implements the channel stated in Lemma 4.4, but its running time is *exponential* in $1/\alpha_{\max}$.

Protocol 4.7. *[Protocol* $\Delta^C = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}})$*]*

Oracle: channel $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$.

Input: 1^ℓ.

Operation: The parties repeat the following process until it produces outputs:

1. *The parties (jointly) call the channel C for ℓ times. Let $\overline{o}^{\mathsf{A}} = (o_1^{\mathsf{A}}, \ldots, o_\ell^{\mathsf{A}}), \overline{o}^{\mathsf{B}} = (o_1^{\mathsf{B}}, ..., o_\ell^{\mathsf{B}})$ be the outputs.*
2. *$\widetilde{\mathsf{A}}$ computes and sends $\mathcal{S} = \left\{\overline{o}^{\mathsf{A}}, 1^\ell \oplus \overline{o}^{\mathsf{A}}\right\}$ according to their lexical order to $\widetilde{\mathsf{B}}$.*
3. *$\widetilde{\mathsf{B}}$ inform $\widetilde{\mathsf{A}}$ whether $\overline{o}^{\mathsf{B}} \in \mathcal{S}$.*

   If positive, both parties output the index of their tuple in $\mathcal{S}$ (and the protocol ends).

We show that the channel induced by protocol $\Delta^C(1^\ell)$ satisfies all the requirement of Lemma 4.4 apart from its expected running time (which is exponential in ℓ).

Let $\widetilde{C} = \mathrm{CHN}(\Delta^C(\ell)) = ((V^{\widetilde{\mathsf{A}}}, O^{\widetilde{\mathsf{A}}}), (V^{\widetilde{\mathsf{B}}}, O^{\widetilde{\mathsf{B}}}))$. The following function outputs the calls to C made in the final iteration in $\widetilde{C}$.

Definition 4.8 (Final calls)**.** *For $c \in \mathrm{Supp}(\widetilde{C})$ let $\mathrm{final}(c)$ denote the output of the ℓ calls to C made in the* final *iteration in c.*

We make the following observation about the final calls.

Claim 4.9. *The following holds for $((\cdot, \overline{O}^{\mathsf{A}}), (\cdot, \overline{O}^{\mathsf{B}})) = \mathrm{final}(\widetilde{C} = ((\cdot, O^{\widetilde{\mathsf{A}}}), (\cdot, O^{\widetilde{\mathsf{B}}})))$.*

- *$O^{\widetilde{\mathsf{A}}} = O^{\widetilde{\mathsf{B}}}$ iff $\overline{O}^{\mathsf{A}} = \overline{O}^{\mathsf{B}}$.*
- *Let $C^\ell = ((\cdot, (O^{\mathsf{A}})^\ell), (\cdot, (O^{\mathsf{B}})^\ell))$ be the random variable induced by taking ℓ copies of C and let E be the event that $(O^{\mathsf{B}})^\ell \in \left\{(O^{\mathsf{A}})^\ell, (O^{\mathsf{A}})^\ell \oplus 1^\ell\right\}$. Then $\mathrm{final}(\widetilde{C}) \equiv C^\ell|_E$.*

Proof. Immediate by construction. □

Agreement.

Claim 4.10 (Agreement)**.** $\Pr\left[O^{\widetilde{\mathsf{A}}} = O^{\widetilde{\mathsf{B}}}\right] \in [17/32, 7/8]$.

Proof. By Claim 4.9,

$$\begin{aligned}
\Pr\left[O^{\widetilde{\mathsf{A}}} = O^{\widetilde{\mathsf{B}}}\right] &= \frac{\Pr\left[(O^{\mathsf{A}})^\ell = (O^{\mathsf{B}})^\ell \mid E\right]}{\Pr\left[(O^{\mathsf{A}})^\ell = (O^{\mathsf{B}})^\ell \mid E\right] + \Pr\left[(O^{\mathsf{A}})^\ell \oplus (O^{\mathsf{B}})^\ell = 1^\ell \mid E\right]} \\
&= \frac{\Pr\left[(O^{\mathsf{A}})^\ell = (O^{\mathsf{B}})^\ell\right]}{\Pr\left[(O^{\mathsf{A}})^\ell = (O^{\mathsf{B}})^\ell\right] + \Pr\left[(O^{\mathsf{A}})^\ell \oplus (O^{\mathsf{B}})^\ell = 1^\ell\right]} \\
&= \frac{(1/2+\alpha)^\ell}{(1/2+\alpha)^\ell + (1/2-\alpha)^\ell}.
\end{aligned} \tag{9}$$

Since, $\ell = 2^{(\lfloor \log 1/\alpha_{\max} \rfloor - 2)}$ and $\alpha_{\max}/2 \le \alpha \le \alpha_{\max}$, we get that $1/4 \ge \ell \cdot \alpha \ge 1/16$. By Proposition 3.20,

$$\frac{(1/2+\alpha)^\ell}{(1/2+\alpha)^\ell + (1/2-\alpha)^\ell} \in [\tfrac{1}{2}(1+\alpha\ell), \tfrac{1}{2}(1+3\alpha\ell)] \tag{10}$$

Thus, $\Pr\left[O^{\widetilde{\mathsf{A}}} = O^{\widetilde{\mathsf{B}}}\right] \in [17/32, 7/8]$, which concludes the proof. □

Leakage.

Claim 4.11 (Leakage)**.** *$\widetilde{C}$ has $(\widetilde{\epsilon},\widetilde{\delta})$-leakage, where $\widetilde{\epsilon} = 2\ell\epsilon^2 + \epsilon\sqrt{2\ell\ln(1/\delta')}$ and $\widetilde{\delta} = \delta' + \ell\delta$ for every $\delta' \in (0,1)$.*

Proof. We need to prove that for both $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$:

$$V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}}=O^{\widetilde{\mathsf{B}}}} \overset{\mathrm{R}}{\approx}_{(\widetilde{\epsilon},\widetilde{\delta})} V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}}\neq O^{\widetilde{\mathsf{B}}}} \tag{11}$$

By assumption C has (ϵ,δ)-leakage. Thus, by Theorem 3.5,

$$(V^{\mathsf{P}})^{\ell}|_{(O^{\mathsf{A}})^{\ell}=(O^{\mathsf{B}})^{\ell}} \overset{\mathrm{R}}{\approx}_{(\widetilde{\epsilon},\widetilde{\delta})} (V^{\mathsf{P}})^{\ell}|_{(O^{\mathsf{A}})^{\ell}=(O^{\mathsf{B}})^{\ell}\oplus 1^{\ell}} \tag{12}$$

Let $((\overline{V}^{\mathsf{A}},\overline{O}^{\mathsf{A}}),(\overline{V}^{\mathsf{B}},\overline{O}^{\mathsf{B}}) = \mathrm{final}(\widetilde{C})$. By the above and Claim 4.9,

$$\overline{V}^{\mathsf{P}}|_{O^{\widetilde{\mathsf{A}}}=O^{\widetilde{\mathsf{B}}}} \overset{\mathrm{R}}{\approx}_{(\widetilde{\epsilon},\widetilde{\delta})} \overline{V}^{\mathsf{P}}|_{O^{\widetilde{\mathsf{A}}}\neq O^{\widetilde{\mathsf{B}}}} \tag{13}$$

Equation (11) now follows by a data processing argument: let f be the randomized function that on input $v \in \mathrm{Supp}(\overline{V}^{\mathsf{P}})$ outputs a random sample from $V^{\widetilde{\mathsf{P}}}|_{\overline{V}^{\mathsf{P}}=v}$. It easy to verify that $f(\overline{V}^{\mathsf{P}}|_{O^{\widetilde{\mathsf{A}}}=O^{\widetilde{\mathsf{B}}}}) = V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}}=O^{\widetilde{\mathsf{B}}}}$ and $f(\overline{V}^{\mathsf{P}}|_{O^{\widetilde{\mathsf{A}}}\neq O^{\widetilde{\mathsf{B}}}}) \equiv V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}}\neq O^{\widetilde{\mathsf{B}}}}$. Thus Equation (11) follows by Fact 3.4. □

4.1.2 Efficient Amplification

We will show how to make Protocol 4.7 protocol more efficient in terms of α. The resulting protocol will run in poly-time even if α is inverse polynomial. The efficient amplification protocol is defined as follows. Let Δ be the (inefficient) protocol from Protocol 4.7.

Protocol 4.12. *[Protocol $\Lambda^C = (\widehat{\mathsf{A}},\widehat{\mathsf{B}})$]*

Oracle: Channel C.

Prameter: Recursion depth d.

Operation: The parties interact in $\Delta^{\Lambda^C(d-1)}(2)$, letting $\Lambda^C(0) = C$.

We show that the channel induced by protocol $\Lambda^C(d)$ satisfies all the requirement of Lemma 4.4. But we first show that the expected running time of $\Lambda^C(d)$ is $O(4^d)$, and therefore, the protocol that on input 1^ℓ invoke $\Lambda^C(\log\ell)$, is PPT, as stated in Lemma 4.4.

Running time.

Claim 4.13 (Expected running time)**.** *Let C be a channel, the for any $d \in \mathbb{N}$ the expected running time of $\Lambda^C(d)$ is at most $O(4^d)$.*

We will use the following claim:

Claim 4.14. *For any channel C, $\Delta^C(2)$ makes in expectation at most 4 calls to C.*

Proof. Let C with a channel with agreement $\alpha \in [-1/2, 1/2]$. Let $\overline{O}^{\mathsf{A}} = (O_1^{\mathsf{A}}, O_2^{\mathsf{A}})$ and $\overline{O}^{\mathsf{B}} = (O_1^{\mathsf{B}}, O_2^{\mathsf{B}})$ denote the outputs of two invocations of C, respectively. By construction, $\Delta^C(2)$ concludes on the event $E = \left\{(O_1^{\mathsf{B}}, O_2^{\mathsf{B}}) \in \{\overline{O}^{\mathsf{A}}, 1^2 \oplus \overline{O}^{\mathsf{A}}\}\right\}$. It is clear that $\Pr[E] = (\frac{1}{2}+\alpha)^2 + (\frac{1}{2}-\alpha)^2 = \frac{1}{2} + \alpha^2 \geq \frac{1}{2}$. Thus, the expected number of invocations preformed by $\Delta^C(2)$ is bounded is 4. □

We now prove *Claim* 4.13 using the above claim.

Proof of Claim 4.13. For $d \in \mathbb{N}$, let $T(d)$ denote the expected runtime of $\Lambda^C(d)$. By Claim 4.14,

$$T(d) = 4 \cdot T(d-1) + O(1), \tag{14}$$

letting $T(0) = 1$. Thus, $T(d) \in O(4^d)$. □

Let $\widehat{C}_d = \mathrm{CHN}(\Lambda^C(d)) = ((V_d^{\widehat{\mathsf{A}}}, O_d^{\widehat{\mathsf{A}}}), ((V_d^{\widehat{\mathsf{B}}}, O_d^{\widehat{\mathsf{B}}}))$. The following function outputs the "important' calls of C made in $\widehat{C}_d$, the ones used to set the final outcome.

Let $\circ$ denote vectors concatenation.

Definition 4.15 (Important calls)**.** *For $d \in \mathbb{N}$ and $c \in \mathrm{Supp}(\widehat{C}_d)$, let $\mathrm{final}(c) = (c_0, c_1)$ be the two calls to $\Lambda^C(d-1)$ done in final execution of $\Delta^{\Lambda^C(d-1)}(2)$ in c. Define $\mathrm{important}(c) = \mathrm{important}(c_0) \circ \mathrm{important}(c_1)$, letting $\mathrm{important}(c) = c$ for $c \in \mathrm{Supp}(\widehat{C}_0)$.*

Similarly to the analysis of inefficient protocol, the crux is the following observation about the important calls.

Claim 4.16. *Let $d \in \mathbb{N}$ and set $\ell = 2^d$. The following holds for $((\cdot, \overline{O}^{\mathsf{A}}), (\cdot, \overline{O}^{\mathsf{B}})) = \mathrm{important}(\widehat{C}_d = ((\cdot, O^{\widehat{\mathsf{A}}}), (\cdot, O^{\widehat{\mathsf{B}}})))$.*

- *$O^{\widehat{\mathsf{A}}} = O^{\widehat{\mathsf{B}}}$ iff $\overline{O}^{\mathsf{A}} = \overline{O}^{\mathsf{B}}$.*
- *Let $C^\ell = ((\cdot, (O^{\mathsf{A}})^\ell), (\cdot, (O^{\mathsf{B}})^\ell))$ be the random variable induced by taking ℓ copies of C and let E be the event that $(O^{\mathsf{B}})^\ell \in \left\{(O^{\mathsf{A}})^\ell, (O^{\mathsf{A}})^\ell \oplus 1^\ell\right\}$. Then*

  $\mathrm{important}(\widehat{C}_d) \equiv C^\ell|_E$.

We prove Claim 4.16 below, but first use it for proving Lemma 4.4.

Agreement.

Claim 4.17 (Agreement)**.** $\Pr\left[O^{\widehat{\mathsf{A}}} = O^{\widehat{\mathsf{B}}}\right] \in [17/32, 7/8]$.

Proof. The proof follows by Claim 4.16, using the same lines as the proof that Claim 4.10 follows from Claim 4.9. □

Leakage.

Claim 4.18 (Leakage)**.** *$\widehat{C}$ has $(\widetilde{\epsilon}, \widetilde{\delta})$-leakage, where $\widetilde{\epsilon} = 2\ell\epsilon^2 + \epsilon\sqrt{2\ell\ln(1/\delta')}$ and $\widetilde{\delta} = \delta' + \ell\delta$ for every $\delta' \in (0,1)$.*

Proof. The proof follows by Claim 4.16 and a data processing argument, using similar lines to the proof that Claim 4.11 follows from Claim 4.9. □

Proving Lemma 4.4.

Proof of Lemma 4.4. Consider the protocol $\mathrm{T}^C(1^\ell) = \Lambda^C(\lfloor \log \ell \rfloor)$. The proof that T satisfies the requirements of Lemma 4.4 immediately follows by Claims 4.13, 4.17 and 4.18. □

Proving Claim 4.16.

Proof of Claim 4.16. First note that the first item in the claim immediately follows by construction. We now prove the second item.

Let $d \in \mathbb{N}$ and let $\ell = 2^d$. For $C^\ell = ((\cdot, (O^{\mathsf{A}})^\ell), (\cdot, (O^{\mathsf{B}})^\ell))$, let D_ℓ be the distribution of $C^\ell|_{\{(O^{\mathsf{B}})^\ell \in \{(O^{\mathsf{A}})^\ell, (O^{\mathsf{A}})^\ell \oplus 1^\ell\}\}}$. We need to prove that

$$\text{important}(\widehat{C}_d) \equiv D_\ell$$

We prove the claim by induction on d. The base case $d = 1$ follows by Claim 4.9.

Fix $d > 1$, for $j \in \{0, 1\}$, let $\widehat{C}_{d-1,j}$ be an invocations of the channel on input $d - 1$ and let $((\cdot, \overline{O}^{\mathsf{A}}_j), (\cdot, \overline{O}^{\mathsf{B}}_j)) = \text{important}(\widehat{C}_{d-1,j})$. By the induction hypothesis,

$$\text{important}(\widehat{C}_{d-1,j}) \equiv D_{\ell/2} \tag{15}$$

The key observation is that by construction, the event $\text{final}(\widehat{C}_d) = \widehat{C}_{d-1,0} \circ \widehat{C}_{d-1,1}$ occurs if and only if,

$$\overline{O}^{\mathsf{B}}_0 \circ \overline{O}^{\mathsf{B}}_1 \in \left\{ \overline{O}^{\mathsf{A}}_0 \circ \overline{O}^{\mathsf{A}}_1, 1^\ell \oplus \overline{O}^{\mathsf{A}}_0 \circ \overline{O}^{\mathsf{A}}_1 \right\} \tag{16}$$

Recall this means that,

$$\text{important}(\widehat{C}_d) = \left(\text{important}(\widehat{C}_{d-1,0}) \circ \text{important}(\widehat{C}_{d-1,1}) \right) |_{\overline{E}}$$

where $\overline{E} = \left\{ \overline{O}^{\mathsf{B}}_0 \circ \overline{O}^{\mathsf{B}}_1 \in \left\{ \overline{O}^{\mathsf{A}}_0 \circ \overline{O}^{\mathsf{A}}_1, 1^\ell \oplus \overline{O}^{\mathsf{A}}_0 \circ \overline{O}^{\mathsf{A}}_1 \right\} \right\}$. The above observations yields that $\text{important}(\widehat{C}_d) \equiv D_\ell$. □

4.1.3 From Channels with Large Gap to OT

Definition 4.19. *A channel* $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ *is* balanced *if* $\Pr\left[O^{\mathsf{A}} = 1\right] = \Pr\left[O^{\mathsf{B}} = 1\right] = \frac{1}{2}$.

We use the following claim.

Claim 4.20. *Let* $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ *be a balanced channel that has* $\alpha \in [\alpha_{\min}, \alpha_{\max}]$*-agreement and* (ϵ, δ)-leakage. *Then* C *is a* (ϵ_0, p)-SWBSC *for some* $\epsilon_0 \in [\frac{1}{2} - \alpha_{\max}, \frac{1}{2} - \alpha_{\min}]$*, and* $p = 2\epsilon + \delta$.

Proof. For every $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ we have that, $V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}} = O^{\widetilde{\mathsf{B}}}} \overset{\mathrm{R}}{\approx}_{(\epsilon,\delta)} V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}} \neq O^{\widetilde{\mathsf{B}}}}$, thus by definition it follows that, $V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}} = O^{\widetilde{\mathsf{B}}}} \overset{\mathrm{S}}{\approx}_{(2\epsilon+\delta)} V^{\widetilde{\mathsf{P}}}|_{O^{\widetilde{\mathsf{A}}} \neq O^{\widetilde{\mathsf{B}}}}$, and the claim holds. □

The following claim, states that a given a channel with bounded leakage and agreement we can construct a new protocol using the olds one, that has the same leakage and agreement, while having the additional property of being balanced.

Claim 4.21. *There exists a constant-time single oracle call protocol Δ such that for every channel C, the channel $\widetilde{C}$ induced by Δ^C is balanced and has the same agreement and leakage as of C.*

Protocol 4.22. *[Protocol $\Delta = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}})$]*

Oracle: Channel C.

Operation:

1. *The parties (jointly) call the channel C. Let o^{A} and o^{B} denote their output respectively.*
2. *$\widetilde{\mathsf{A}}$ sends $r \leftarrow \{0,1\}$ to $\widetilde{\mathsf{B}}$.*
3. *$\widetilde{\mathsf{A}}$ outputs $o^{\mathsf{A}} \oplus r$ and $\widetilde{\mathsf{B}}$ outputs $o^{\mathsf{B}} \oplus r$.*

Proof of Claim 4.21. Let $\widetilde{C} = \mathrm{CHN}(\Delta^C)$. By construction $\widetilde{C}$ is balanced and has α-agreement. Finally, by a data processing argument, $\widetilde{C}$ has the same leakage as C. □

Proving Lemma 4.6.

Proof of Lemma 4.6. Set $n = 10^8$, let $C = \mathrm{CHN}(\Pi)$, let $\Pi' = \mathsf{bound}_{n \cdot t}(\Pi)$ and let $C' = \mathrm{CHN}(\Pi')$. By Markov inequality,

$$C' \overset{\mathrm{S}}{\approx}_{1/n} C \tag{17}$$

By Claim 4.21, there exist a protocol Δ such that Δ^C is balanced and has the same leakage and agreement as C. Moreover, since Δ only uses one call to the channel C, by data processing argument,

$$\mathrm{CHN}(\Delta^{C'}) \overset{\mathrm{S}}{\approx}_{1/n} \mathrm{CHN}(\Delta^C) \tag{18}$$

By Claim 4.21, $\Delta^{C'}$ is also balanced. Claim 4.20 yields that Δ^C is a $(15/32, p)$-WBSC for $p = 2\epsilon + \delta$. Hence, using Proposition 3.2, we get that $\Delta^{C'}$ is $(\epsilon_0, \overline{p})$-WBSC, for $\epsilon_0 = \epsilon + 1/10^8$ and $\overline{p} = p + 4/10^7$.

In the following we use Theorem 3.17 to show that $\Delta^{C'}$ can be used to construct semi-honest statistically secure OT. To do this, we need to prove that

$$150(1 - (1-2\overline{p})^2) < (1 - \frac{2\epsilon_0^2}{\epsilon_0^2 + (1-\epsilon_0)^2})^2 \tag{19}$$

Indeed, since $(1 - 2\frac{\epsilon_0^2}{\epsilon_0^2 + (1-\epsilon_0)^2})^2 \geq 1/100$, for $\delta' = 1/10^7$ it holds that, for small enough c,

$$\begin{aligned} (1 - (1-2\overline{p})^2) \leq 4\overline{p} \leq 4p + 2/10^6 \leq 2\epsilon + \delta + 2/10^6 \\ \leq 3c + 2/10^6 \\ < 1/(150 \cdot 100). \end{aligned} \tag{20}$$

And therefore $\Delta^{C'}$ satisfies the requirement of Theorem 3.17. Let Γ be the protocol guaranteed in Theorem 3.17, and let $\widetilde{\Gamma}^{C'}(1^\kappa) = \Gamma^{\Delta^{C'}}(1^\kappa, 49/100)$. By Equation (19) and theorem 3.17, $\widetilde{\Gamma}^{C'}(1^\kappa)$ is statistically secure semi-honest OT. Since ϵ_0 is a bounded from 0 and 1/2 by constants, $\widetilde{\Gamma}$ running time in polynomial in κ. □

4.1.4 Triviality of Channels with Large Leakage

Proof of Theorem 4.3. Consider the following protocol:

Protocol 4.23. *[$\Pi = (\mathsf{A}, \mathsf{B})$]*

Parameter: ϵ.

Operation:

1. A *sends* $r \leftarrow \{0,1\}$ *to* B.
2. *Each party outputs* r *with probability* $1/2 + \epsilon$, *and* $1 - r$ *otherwise.*

Let $C = ((V^{\mathsf{A}}, O^{\mathsf{A}}), (V^{\mathsf{B}}, O^{\mathsf{B}}))$ be the channel induced by a random execution of Π. A simple calculation shows that C has agreement $1/2 + \Theta(\epsilon^2)$.

To see that Protocol 4.23 has $(\Theta(\epsilon), 0)$-leakage, note that the parties' views contain only their output bit and the bit r. Let R the value of the bit r in C and consider A's view (the proof for B's view is follows the same lines). For every $b, r \in \{0,1\}$, it holds that

$$\begin{aligned}
&\Pr\left[O^{\mathsf{A}} = b, R = r \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right] \\
&= \Pr\left[O^{\mathsf{A}} = O^{\mathsf{B}} \mid O^{\mathsf{A}} = b, R = r\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = b, R = r\right]}{\Pr\left[O^{\mathsf{A}} = O^{\mathsf{B}}\right]} \\
&= \Pr\left[O^{\mathsf{B}} = b \mid O^{\mathsf{A}} = b, R = r\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = b, R = r\right]}{\Pr\left[O^{\mathsf{A}} = O^{\mathsf{B}}\right]},
\end{aligned}$$

and,

$$\begin{aligned}
&\Pr\left[O^{\mathsf{A}} = b, R = r \mid O^{\mathsf{A}} \neq O^{\mathsf{B}}\right] \\
&= \Pr\left[O^{\mathsf{B}} = 1 - b \mid O^{\mathsf{A}} = b, R = r\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = b, R = r\right]}{\Pr\left[O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]}.
\end{aligned}$$

It follows that

$$\begin{aligned}
&\frac{\Pr\left[O^{\mathsf{A}} = b, R = r \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = b, R = r \mid O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]} \\
&= \frac{\Pr\left[O^{\mathsf{B}} = b \mid O^{\mathsf{A}} = b, R = r\right]}{\Pr\left[O^{\mathsf{B}} = 1 - b \mid O^{\mathsf{A}} = b, R = r\right]} \cdot \frac{\Pr\left[O^{\mathsf{A}} = O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]}
\end{aligned} \tag{21}$$

By construction, the terms $\Pr\left[O^{\mathsf{B}} = b \mid O^{\mathsf{A}} = b, R = r\right]$, $\Pr\left[O^{\mathsf{B}} = 1 - b \mid O^{\mathsf{A}} = b, R = r\right]$, $\Pr\left[O^{\mathsf{A}} = O^{\mathsf{B}}\right]$ and $\Pr\left[O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]$ are all in the range $[1/2+\epsilon, 1/2-\epsilon]$. Hence,

$$\frac{\Pr\left[O^{\mathsf{A}} = b, \widehat{B} = c \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = b, R = r \mid O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]} \in \left[\left(\frac{1/2 - \epsilon}{1/2 + \epsilon}\right)^2, \left(\frac{1/2 + \epsilon}{1/2 - \epsilon}\right)^2\right] \subseteq [e^{-\Theta(\epsilon)}, e^{\Theta(\epsilon)}].$$

□

4.2 The Computational Setting

In this section we extend Theorem 4.2 to the computational setting. We start by defining the computational analogue of log-ratio leakage. We give two such definition, for the uniform and non-uniform settings. As in similar computational analogue of information measures [26, 20], for the uniform version we need to give the uniform distinguisher the ability to sample from the distributions in consideration,

Definition 4.24 (Computational log-ratio leakage)**.** *A channel ensemble* $C = \left\{C_\kappa = ((V^{\mathsf{A}}_\kappa, O^{\mathsf{A}}_\kappa), (V^{\mathsf{B}}_\kappa, O^{\mathsf{B}}_\kappa))\right\}_{\kappa\in\mathbb{N}}$ *has* (ϵ,δ)-comp-leakage [resp., (ϵ,δ)-nu-comp-leakage] *if there exists a channel ensemble* $\widetilde{C} = \left\{\widetilde{C}_\kappa = ((V^{\tilde{\mathsf{A}}}_\kappa, O^{\tilde{\mathsf{A}}}_\kappa), (V^{\tilde{\mathsf{B}}}_\kappa, O^{\tilde{\mathsf{B}}}_\kappa))\right\}_{\kappa\in\mathbb{N}}$ *such that the following holds:*

- *For every* $\kappa\in\mathbb{N}$*: the channel* $\widetilde{C}_\kappa$ *has* $(\epsilon(\kappa),\delta(\kappa))$-leakage *(according to Definition 4.1).*
- *For every* $\mathsf{P}\in\{\mathsf{A},\mathsf{B}\}$ *and* PPT D*:*

$$\left|\Pr\left[\mathsf{D}^{C_\kappa,\widetilde{C}_\kappa}(1^\kappa, V^{\mathsf{P}}_\kappa, O^{\mathsf{A}}_\kappa, O^{\mathsf{B}}_\kappa)=1\right] - \Pr\left[\mathsf{D}^{C_\kappa,\widetilde{C}_\kappa}(1^\kappa, V^{\tilde{\mathsf{P}}}_\kappa, O^{\tilde{\mathsf{A}}}_\kappa, O^{\tilde{\mathsf{B}}}_\kappa)=1\right]\right| \le \mathrm{neg}(\kappa).$$

[resp., for every $\mathsf{P}\in\{\mathsf{A},\mathsf{B}\}$*:* $\{V^{\mathsf{P}}_\kappa, O^{\mathsf{A}}_\kappa, O^{\mathsf{B}}_\kappa\}_{\kappa\in\mathbb{N}} \overset{\text{nuC}}{\approx} \{V^{\tilde{\mathsf{P}}}_\kappa, O^{\tilde{\mathsf{A}}}_\kappa, O^{\tilde{\mathsf{B}}}_\kappa\}_{\kappa\in\mathbb{N}}$*]*

That is, the distinguisher D aiming to tell P's view in C from its view in $\widetilde{C}$ is equipped the ability to oracle access to C and $\widetilde{C}$. This ability is crucial when arguing about the leakage of many samples of such channels. We note that typically, the channel C in consideration is a one induced by an efficient protocol, and thus the oracle access to C given to D can be simulated efficiently.

Theorem 4.25 (Small computational log-ratio leakage implies OT)**.** *There exists constant* $c_1>0$ *such that the following holds. Let* ϵ,δ,α *be functions such that for every* $\kappa\in\mathbb{N}$*:* $\epsilon(\kappa),\delta(\kappa)\in[0,1]$*,* $1/8>\alpha(\kappa)\ge c_1\cdot\epsilon(\kappa)^2$ *and* $\delta(\kappa)\le\epsilon(\kappa)^2$ *and* $\alpha(\kappa)>1/p(\kappa)$ *for some* $p\in\mathrm{poly}$*. Let* C *be a channel ensemble that has* (ϵ,δ)-comp-leakage *[resp.,* (ϵ,δ)-nu-comp-leakage *] and* α-agreement*. Then in the* C*-hybrid model there exists a semi-honest [resp., non-uniform] computational OT.*

Theorem 4.25 yields the following result.

Corollary 4.26 (Protocols with small log-ration leakage implies OT)**.** *Let* ϵ,δ,α *be as in Theorem 4.25. Assume there exists a* PPT *protocol that induces a channel ensemble that has* α-agreement *and* (ϵ,δ)-comp-leakage *[resp.,* (ϵ,δ)-nu-comp-leakage *], then there exists a [resp., non-uniform] computational OT.*

Proof. We only prove the uniform security case, the non-uniform case follow analogously. By Theorem 4.25, the existence of the guaranteed protocol yields a semi-honest computational OT protocol Π. By [27], the existence of Π implies the existence of one-way functions. Finally, by [13], using one-way functions we can compile Π into an OT secure against arbitrary adversaries. □

Proof of Theorem 4.25. Let $\Delta=(\mathsf{A},\mathsf{B})$ be the protocol guaranteed by Theorem 4.2. Consider the following protocol.

Protocol 4.27. *[Protocol* $\widetilde{\Delta}=(\mathsf{A},\mathsf{B})$*]*

Oracle: channel C.

Parameter: security parameter 1^κ.

Operation:

1. A *samples $t(\kappa)$ independent instances from C_κ, and sends the average agreement $\widetilde{\alpha}$ to $\widetilde{\mathsf{B}}$. If $\widetilde{\alpha} < 1/p(\kappa)$, the two parties abort.*
2. *The parties interact in $\Delta^{C_\kappa}(1^\kappa, 1^\ell)$, for $\ell = \max(1, 2^{\lfloor \log(2/(3\cdot\alpha_{\max}))\rfloor - 2})$ (and output the same values as the parties in this interaction do).*

It is clear that $\widetilde{\Delta}^C$ runs in polynomial time. Let $\widetilde{A}_\kappa$ be the value of $\widetilde{\alpha}$ in a random execution of $\widetilde{\Delta}^C(1^\kappa)$. By Hoffeding bound,

$$\Pr\left[\widetilde{A}_\kappa \notin [\alpha - 1/3\alpha, \alpha + 1/3\alpha]\right] \leq \Pr\left[\widetilde{A}_\kappa \notin [\alpha - 1/3 \cdot p(\kappa), \alpha + 1/3 \cdot p(\kappa)]\right] \leq \mathrm{neg}(\kappa),$$

which implies that $\alpha \in [3/4 \cdot \widetilde{A}_\kappa, 3/2 \cdot \widetilde{A}_\kappa]$. The correctness of $\widetilde{\Delta}$ thus follows by Theorem 4.2.

We prove security only for the uniform security case, the non-uniform case follow analogously. Let $\widetilde{C}$ be the channel ensemble that realizes the (ϵ, δ)-comp-leakage of C. First note that the correctness of $\widetilde{C}$ is the same as C up to some negligible additive value, as otherwise it is easy to distinguish between C and $\widetilde{C}$. By the above observation about $\widetilde{A}_k$ and Theorem 4.2, it follows that $\widetilde{\Delta}^{\widetilde{C}}$ is a semi-honest secure OT in the $\widetilde{C}$-hybrid model. Assume there exists a distinguisher that violates the security of one of the parties in $\widetilde{\Delta}^C$, a simple hybrid argument yields that a distinguisher with the ability to sample from C and $\widetilde{C}$ can exploit the above security breach to violates the assumed indistinguishability of C and $\widetilde{C}$. □

5 Characterization of Channel for Distributed Differentially Private Computation

In this section we prove our results on 2-party differentially private computation. Our goal is to show that a sufficiently accurate 2-party differentially private computation of the XOR function implies OT. In Section 5.1.1 we consider differential privacy in an information theoretic setting. In Section 5.1.2 we consider the computational setting, giving formal definitions with which we restate and prove Theorem 1.10. Finally, in Section 5.2 we extend our result to functions over many bits that are not "monotone under relabeling".

Throughout, we use the following notions of agreement and accuracy for functionalities. Since we care about lower bounds, we only consider (a weaker) average-case variant of these notions.

Definition 5.1 (Accuracy and agreement, functionalities)**.** *Let $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}^n$ be a Boolean output functionality and let $(O^{\mathsf{A}}_{x,y}, O^{\mathsf{B}}_{x,y}) = f(x,y)$. We say that f has* average agreement *α if $\Pr_{x,y \leftarrow \mathcal{X},\mathcal{Y}}\left[O^{\mathsf{A}}_{x,y} = O^{\mathsf{B}}_{x,y}\right] = \frac{1}{2} + \alpha$. We say that f* computes a Boolean function *g* with average correctness *β, if $\Pr\left[O^{\mathsf{A}}_{x,y} = O^{\mathsf{B}}_{x,y} = g(x,y)\right] = \frac{1}{2} + \beta$.*

A non-Boolean output functionality f has agreement α if the Boolean functionality f', defined by $f'(x,y) = (o^{\mathsf{A}}_1, o^{\mathsf{B}}_1)$ for $(o^{\mathsf{A}}, o^{\mathsf{B}}) \leftarrow f(x,y)$, has agreement α. Similarly, f computes g with correctness β, if the functionality f' does.

Namely, a non-Boolean functionality f has certain agreement and correctness (with respect to Boolean function g) if this holds with respect to the first bits it outputs (i.e., its "designated output bits").

5.1 The XOR Functionality

5.1.1 The Information Theoretic Case

We prove the following characterization of differential private functionalities for computing XOR.

Theorem 5.2. *There exists a* PPT *protocol* Δ *and a constant* $c_1 > 0$ *such that the following holds. Let* $\epsilon, \beta \in [0,1]$ *be such that* $\beta \geq c_1 \cdot \epsilon^2$*. Let* $f = (f_{\mathsf{A}}, f_{\mathsf{B}})$ *be a functionality that is* ϵ*-DP, has perfect agreement and computes the XOR function with average correctness* β*. Then* $\Delta^f(1^\kappa, 1^{\lfloor 1/\beta \rfloor})$ *is a semi-honest statistically secure OT in the* f*-hybrid model. Furthermore, the parties in* Δ *only make use of the first bit of the outputs of* f*.*

We prove Theorem 5.2 by constructing in the f-hybrid model a balanced protocol that induced balanced channel with β-agreement and that has $(2\epsilon, 0)$-leakage.

Protocol 5.3 ($\Pi^f = (\mathsf{A}, \mathsf{B})$)**.**

Oracle: f*.*

Operation:

1. A *samples* $i_{\mathsf{A}} \leftarrow \{0,1\}$ *and* B *samples* $i_{\mathsf{B}} \leftarrow \{0,1\}$*.*
2. *The parties make a joint call to* $f(i_{\mathsf{A}}, i_{\mathsf{B}})$*. Let* out_{B} *be the first bit of the output given to* B*.*
3. A *sends* $r \leftarrow \{0,1\}$ *to* B*.*
4. *The parties output* $i_{\mathsf{A}} \oplus r$ *and* $\text{out}_{\mathsf{B}} \oplus i_{\mathsf{B}} \oplus r$*, respectively.*

The proof of Theorem 5.2 immediately follows be the next lemma and the tools we devolved in the previous section.

Lemma 5.4. *Let* β, ϵ *and* f *be as in Theorem 5.2, then in the* f*-hybrid model protocol* Π^f *induces a channel of* $(2\epsilon, 0)$-leakage *and* β-agreement*.*

We prove Lemma 5.4 below, but first use it for proving Theorem 5.2.

Proof of Theorem 5.2. The proof directly follows from Theorem 4.2 and Lemma 5.4. Note that, by differential privacy properties, β is bounded. Specifically, for sufficiently large c_1, $\beta \leq 1/8$. □

Let $C = ((O^{\mathsf{A}}, V^{\mathsf{A}}), (O^{\mathsf{B}}, V^{\mathsf{B}}))$ denote the channel induces by a random execution of Π^f. Lemma 5.4 is an immediate consequence of the following three claims.

Claim 5.5. $\Pr\left[O^{\mathsf{A}} = O^{\mathsf{B}}\right] = 1/2 + \beta$*.*

Proof. Follows by construction and the assumed accuracy of f. □

Claim 5.6. *For both* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$*:* $(V^{\mathsf{P}}, O^{\mathsf{P}}) \mid_{O^{\mathsf{A}} = O^{\mathsf{B}}} \overset{\text{R}}{\approx}_{2\epsilon} (V^{\mathsf{P}}, O^{\mathsf{P}}) \mid_{O^{\mathsf{A}} \neq O^{\mathsf{B}}}$*.*

We use the following claim that states that we have bounded leakage with respect to the outputs of protocol $\widetilde{\Pi}$.

Claim 5.7. *For every $a, b \in \{0,1\}$ it holds that,*

- $(V^{\mathsf{A}}, O^{\mathsf{A}}) \mid_{O^{\mathsf{B}}=b} \overset{\mathrm{R}}{\approx}_{\epsilon} (V^{\mathsf{A}}, O^{\mathsf{A}}) \mid_{O^{\mathsf{B}}=\bar{b}}$
- $(V^{\mathsf{B}}, O^{\mathsf{B}}) \mid_{O^{\mathsf{A}}=a} \overset{\mathrm{R}}{\approx}_{\epsilon} (V^{\mathsf{B}}, O^{\mathsf{B}}) \mid_{O^{\mathsf{A}}=\bar{a}}$

We now prove Claim 5.6 using the above claim. We prove for $\mathsf{P} = \mathsf{A}$, where the case $\mathsf{P} = \mathsf{B}$ follows analogously.

Proof of Claim 5.6. For $v \in \mathrm{Supp}(V^{\mathsf{A}})$ and $a \in \{0,1\}$, let $H^{v,a} = \left\{(V^{\mathsf{A}}, O^{\mathsf{A}}) = (v, a)\right\}$. We need to show that for every v, a:

$$\Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}=O^{\mathsf{B}}}\left[H^{v,a}\right] \overset{\mathrm{R}}{\approx}_{2\epsilon} \Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}\neq O^{\mathsf{B}}}\left[H^{v,a}\right] \tag{22}$$

Compute,

$$\begin{aligned}
\Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}=O^{\mathsf{B}}}\left[H^{v,a}\right] &= \Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}=O^{\mathsf{B}},O^{\mathsf{A}}=a}\left[H^{v,a}\right] \cdot \Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right] \\
&= \Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}=a,O^{\mathsf{B}}=a}\left[H^{v,a}\right] \cdot \Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right] \\
&= \Pr_{V^{\mathsf{A}}|O^{\mathsf{B}}=a}\left[H^{v,a}\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{B}} = a\right]}.
\end{aligned} \tag{23}$$

In the same way,

$$\Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}\neq O^{\mathsf{B}}}\left[H^{v,a}\right] = \Pr_{V^{\mathsf{A}}|O^{\mathsf{B}}=\bar{a}}\left[H^{v,a}\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{B}} = \bar{a}\right]} \tag{24}$$

By construction,

$$\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right] = \Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} \neq O^{\mathsf{B}}\right] = 1/2 \tag{25}$$

We conclude that

$$\begin{aligned}
\Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}=O^{\mathsf{B}}}\left[H^{v,a}\right] &= \Pr_{V^{\mathsf{A}}|O^{\mathsf{B}}=a}\left[H^{v,a}\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{B}} = a\right]} && \text{(by Equation (23))} \\
&\leq e^{\epsilon} \cdot \Pr_{V^{\mathsf{A}}|O^{\mathsf{B}}=\bar{a}}\left[H^{v,a}\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} = O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{B}} = a\right]} && \text{(by Claim 5.7)} \\
&= e^{\epsilon} \cdot \Pr_{V^{\mathsf{A}}|O^{\mathsf{B}}=\bar{a}}\left[H^{v,a}\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{B}} = a\right]} && \text{(by Equation (25))} \\
&\leq e^{2\epsilon} \cdot \Pr_{V^{\mathsf{A}}|O^{\mathsf{B}}=\bar{a}}\left[H^{v,a}\right] \cdot \frac{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{A}} \neq O^{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}} = a \mid O^{\mathsf{B}} = \bar{a}\right]} \\
&= e^{2\epsilon} \cdot \Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}\neq O^{\mathsf{B}}}\left[H^{v,a}\right]. && \text{(by Equation (24))}
\end{aligned}$$

The last inequality holds since by Claim 5.7, $\frac{\Pr\left[O^{\mathsf{A}}=a|O^{\mathsf{B}}=\bar{a}\right]}{\Pr\left[O^{\mathsf{A}}=a|O^{\mathsf{B}}=a\right]} \leq e^{\epsilon}$.

The proof that $\Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}=O^{\mathsf{B}}}\left[H^{v,a}\right] \geq e^{2\epsilon} \cdot \Pr_{V^{\mathsf{A}}|O^{\mathsf{A}}\neq O^{\mathsf{B}}}\left[H^{v,a}\right]$ is identical, thus the claim holds. □

Proving Claim 5.7.

Proof of Claim 5.7. We write $f = (f^{\mathsf{A}}, f^{\mathsf{B}})$. Let I^{A} and I^{B} be the values of the inputs of the parties, and let Out be the (common) values of the output $f^{\mathsf{P}}(I^{\mathsf{A}}, I^{\mathsf{B}})_1$ and the random bit r in V^{P} respectively. Fix $o \in \{0,1\}$ and $v \in \sup(V^{\mathsf{B}})$, and let b, r be the values of I^{B} and R according to v. Since R and I^{A} are uniform bits, the value of R is independent from I^{A}, and independent from $O^{\mathsf{A}} = I^{\mathsf{A}} \oplus R$ (separately). Thus,

$$\begin{aligned}
&\Pr\left[V^{\mathsf{B}} = v \mid O^{\mathsf{A}} = o\right] = \Pr\left[V^{\mathsf{B}} = v, I^{\mathsf{B}} = b, R = r \mid O^{\mathsf{A}} = o\right] \qquad (26)\\
&= \Pr\left[V^{\mathsf{B}} = v, I^{\mathsf{B}} = b \mid O^{\mathsf{A}} = o, R = r\right] \cdot \Pr\left[R = r \mid O^{\mathsf{A}} = o\right]\\
&= \Pr\left[V^{\mathsf{B}} = v, I^{\mathsf{B}} = b \mid I^{\mathsf{A}} = o \oplus r, R = r\right] \cdot \Pr\left[R = r \mid O^{\mathsf{A}} = o\right]\\
&= \Pr\left[V^{\mathsf{B}} = v, I^{\mathsf{B}} = b, R = r \mid I^{\mathsf{A}} = o \oplus r\right] \cdot \frac{\Pr\left[R = r \mid O^{\mathsf{A}} = o\right]}{\Pr\left[R = r \mid I^{\mathsf{A}} = o \oplus r\right]}\\
&= \Pr\left[V^{\mathsf{B}} = v, I^{\mathsf{B}} = b, R = r \mid I^{\mathsf{A}} = o \oplus r\right]\\
&= 1/2 \cdot \Pr\left[V^{\mathsf{B}} = v \mid I^{\mathsf{A}} = o \oplus r, I^{\mathsf{B}} = b\right].
\end{aligned}$$

Since Equation (26) holds for every $o \in \{0,1\}$, and since

$$1/2 \cdot \Pr\left[V^{\mathsf{B}} = v \mid I^{\mathsf{A}} = r, I^{\mathsf{B}} = b\right] \overset{\mathrm{R}}{\approx}_{\epsilon} 1/2 \cdot \Pr\left[V^{\mathsf{B}} = v \mid I^{\mathsf{A}} = \overline{r}, I^{\mathsf{B}} = b\right],$$

we conclude that $\Pr\left[V^{\mathsf{B}} = v \mid O^{\mathsf{A}} = 0\right] \overset{\mathrm{R}}{\approx}_{\epsilon} \Pr\left[V^{\mathsf{B}} = v \mid O^{\mathsf{A}} = 1\right]$.

The proof of the second item follows in by a similar argument. For every $o \in \{0,1\}$ and $v \in \sup(V^{\mathsf{A}})$, let a, r' be the values of I^{A} and $R \oplus \mathrm{Out}$ according to v respectively. Since the value of $R \oplus \mathrm{Out}$ is independent from I^{B}, and independent from O^{B} (separately), we conclude that

$$\begin{aligned}
&\Pr\left[V^{\mathsf{A}} = v \mid O^{\mathsf{B}} = o\right] = \Pr\left[V^{\mathsf{A}} = v, I^{\mathsf{A}} = a, R \oplus \mathrm{Out} = r' \mid O^{\mathsf{B}} = o\right]\\
&= \Pr\left[V^{\mathsf{A}} = v, I^{\mathsf{A}} = a \mid O^{\mathsf{B}} = o, R \oplus \mathrm{Out} = r'\right] \cdot \Pr\left[R \oplus \mathrm{Out} = r' \mid O^{\mathsf{B}} = o\right]\\
&= \Pr\left[V^{\mathsf{A}} = v, I^{\mathsf{A}} = a \mid I^{\mathsf{B}} = o \oplus r', R \oplus \mathrm{Out} = r'\right] \cdot \Pr\left[R \oplus \mathrm{Out} = r' \mid O^{\mathsf{B}} = o\right]\\
&= \Pr\left[V^{\mathsf{A}} = v, I^{\mathsf{A}} = a, R \oplus \mathrm{Out} = r' \mid I^{\mathsf{B}} = o \oplus r'\right] \cdot \frac{\Pr\left[R \oplus \mathrm{Out} = r' \mid O^{\mathsf{B}} = o\right]}{\Pr\left[R \oplus \mathrm{Out} = r' \mid I^{\mathsf{B}} = o \oplus r'\right]}\\
&= \Pr\left[V^{\mathsf{A}} = v, I^{\mathsf{A}} = a, R \oplus \mathrm{Out} = r' \mid I^{\mathsf{B}} = o \oplus r'\right]\\
&= 1/2 \cdot \Pr\left[V^{\mathsf{A}} = v \mid I^{\mathsf{B}} = o \oplus r', I^{\mathsf{A}} = a\right].
\end{aligned}$$

□

Proving Lemma 5.4.

Proof of Lemma 5.4. Let $C = (O^{\mathsf{A}}, O^{\mathsf{B}}, V^{\mathsf{A}}, V^{\mathsf{B}})$ denotes the channel induces by Π^f. Claim 5.5 yields that C has β-agreement, and Claim 5.6 yields that C has $(2\epsilon, 0)$-leakage. □

5.1.2 The Computational Case

In this section we restate and prove Theorem 1.10. We will use the following definition.

Definition 5.8 (Accuracy and agreement, protocols)**.** *Let* Π *be a Boolean output protocol and let* $(O^{\mathsf{A}}_{x,y}, O^{\mathsf{B}}_{x,y}) = \Pi(x,y)$*. We say that* Π *has* average agreement α *if,* $\Pr_{x,y\leftarrow\mathcal{X},\mathcal{Y}}\left[O^{\mathsf{A}}_{x,y} = O^{\mathsf{B}}_{x,y}\right] = \frac{1}{2}+\alpha$*. We say that* Π computes a Boolean function $g : \mathcal{X}\times\mathcal{Y} \to \{0,1\}^n$ with average correctness β*, if* $\Pr_{x,y\leftarrow\mathcal{X},\mathcal{Y}}\left[O^{\mathsf{A}}_{x,y} = O^{\mathsf{B}}_{x,y} = g(x,y)\right] = \frac{1}{2}+\beta$*. Similarly, we say that* Π computes g with worst-case correctness β*, if for every inputs* $x, y \in \mathcal{X}, \mathcal{Y}$*,* $\Pr\left[O^{\mathsf{A}}_{x,y} = O^{\mathsf{B}}_{x,y} = g(x,y)\right] \geq \frac{1}{2}+\beta$*.*

The following is a restatement of Theorem 1.10.

Theorem 5.9. *There exists a constant* $c > 0$ *such that the following holds. Let* ϵ, β *be functions such that for every* $\kappa \in \mathbb{N}$*:* $\epsilon(\kappa), \beta(\kappa) \in [0,1]$*,* $\beta(\kappa) \geq c\cdot\epsilon(\kappa)^2$ *and* $\beta(\kappa) \geq 1/p(\kappa)$ *for some* $p \in$ poly*. Assume there exist a* PPT *Boolean output protocol that is semi-honest* ϵ-IND-DP *and computes the XOR functionality with perfect agreement and average correctness at least* $\beta(\kappa)$*. Then there exists a computationally non-uniform secure OT.*

We make use of the following notion of simulation based computational differential privacy, in the spirit of [36].

Definition 5.10 (Simulation based computational differential privacy)**.** *A two-output functionality ensemble* $\left\{f_\kappa = (f^{\mathsf{A}}_\kappa, f^{\mathsf{B}}_\kappa)\right\}_{\kappa\in\mathbb{N}}$ *over input domain* $\{0,1\}^n \times \{0,1\}^n$ *is* ϵ-SIM-DP *if the there exists a functionality ensemble* $\left\{\tilde{f}_\kappa = (\tilde{f}^{\mathsf{A}}_\kappa, \tilde{f}^{\mathsf{B}}_\kappa)\right\}_{\kappa\in\mathbb{N}}$ *such that the following holds:*

- *For every* $\kappa \in \mathbb{N}$*: the functionality* $\tilde{f}_\kappa$ *is* $\epsilon(\kappa)$-DP *(according to Definition 3.14).*
- *For both* $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$ *and every* $x, y \in \{0,1\}^n$*:*

$$\left\{f^{\mathsf{P}}_\kappa(x,y)\right\}_{\kappa\in\mathbb{N}} \overset{\text{nuC}}{\approx} \left\{\tilde{f}^{\mathsf{P}}_\kappa(x,y)\right\}_{\kappa\in\mathbb{N}}$$

As Lemma 5.11 (give below) shows, for Boolean inputs, the above functionality (Definition 5.10) is closely related to the more standard ϵ-IND-DP (Definition 3.15).

The proof of Theorem 5.9 immediately follows by the next two lemmata.

Lemma 5.11. *For any* ϵ-IND-DP *protocol* $\Pi = (\mathsf{A},\mathsf{B})$*, the functionality ensemble* $\left\{f_\kappa = (f^{\mathsf{A}}_\kappa(x,y), f^{\mathsf{B}}_\kappa(x,y)\right\}_{\kappa\in\mathbb{N}}$ *defined by* $f_\kappa(x,y)$ *outputting the parties' views in a random execution of* $(\mathsf{A}(x),\mathsf{B}(y))(1^\kappa)$*, is* ϵ-SIM-DP*.*

Lemma 5.12. *Let* ϵ, β *be functions satisfying the requirements of Theorem 5.9. Let* f *be a functionality ensemble that is* ϵ-SIM-DP*, has perfect agreement and computes the XOR function with average correctness at least* $\beta(\kappa)$*. Then in the* f*-hybrid model there exists a semi-honest secure OT.*

Proving Theorem 5.9.

Proof of Theorem 5.9. Let Π be a protocol satisfying the requirements in Theorem 5.9, and let f be the functionality ensemble guaranteed by Lemma 5.11 for Π. By construction, f has perfect agreement and computes the XOR function with correctness β. Thus, the theorem proof follows by Lemma 5.12. □

Proving Lemma 5.11.

Proof of Lemma 5.11. Let $\mathsf{M}_x^{\mathsf{A}}(1^\kappa, y) = f_\kappa^{\mathsf{A}}(x,y)$ and $\mathsf{M}_y^{\mathsf{B}}(1^\kappa, x) = f_\kappa^{\mathsf{B}}(x,y)$. Fix $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$. Since Π is ϵ-IND-DP, it is clear that $\mathsf{M}_b^{\mathsf{P}}$ is ϵ-IND-DP mechanism for every $b \in \{0,1\}$. From [36], for every $b \in \{0,1\}$ there exists distributions ensembles $\left\{D_\kappa^{\mathsf{P},b,0}\right\}_{\kappa\in\mathbb{N}}, \left\{D_\kappa^{\mathsf{P},b,1}\right\}_{\kappa\in\mathbb{N}}$, such that

1. for every $\kappa \in \mathbb{N}$: $D_\kappa^{\mathsf{P},b,0} \overset{\mathrm{R}}{\approx}_\epsilon D_\kappa^{\mathsf{P},b,1}$, and
2. for every $c \in \{0,1\}$: $\left\{D_\kappa^{\mathsf{P},b,c}\right\}_{\kappa\in\mathbb{N}} \overset{\mathrm{nuC}}{\approx} \left\{\mathsf{M}_b^{\mathsf{P}}(1^\kappa, c)\right\}_{\kappa\in\mathbb{N}}$

Consider the functionality ensemble $\left\{\tilde{f}_\kappa\right\}_{\kappa\in\mathbb{N}}$ defined by $\tilde{f}_\kappa(x,y) = (\tilde{f}_\kappa^{\mathsf{A}}(x,y), \tilde{f}_\kappa^{\mathsf{B}}(x,y))$ outputting a random sample from $(D_\kappa^{\mathsf{A},x,y}, D_\kappa^{\mathsf{B},y,x})$. By definition, for every $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$ it holds that

$$\left\{\tilde{f}_\kappa^{\mathsf{P}}(x,y)\right\}_{\kappa\in\mathbb{N}} \overset{\mathrm{nuC}}{\approx} \left\{f_\kappa^{\mathsf{P}}(x,y)\right\}_{\kappa\in\mathbb{N}}.$$

Thus, $\tilde{f}$ realizes the ϵ-IND-DP functionality of f. □

Proving Lemma 5.12. The proof immediately follows by the next claim.

Claim 5.13. *Let $f = \left\{f_\kappa = (f_\kappa^{\mathsf{A}}, f_\kappa^{\mathsf{B}})\right\}_{\kappa\in\mathbb{N}}$ be a functionality ensemble that is ϵ-SIM-DP, and has perfect agreement. Then f is ϵ-SIM-DP with respect to a ϵ-DP functionality ensemble $\left\{\tilde{f}_\kappa = (\tilde{f}_\kappa^{\mathsf{A}}, \tilde{f}_\kappa^{\mathsf{B}})\right\}_{\kappa\in\mathbb{N}}$ that satisfies that for every $x, y \in \{0,1\}^n$:*

$$\left\{(v^{\mathsf{A}}, v_1^{\mathsf{B}})_{(v^{\mathsf{A}},v^{\mathsf{B}})\leftarrow f_\kappa(x,y)}\right\}_{\kappa\in\mathbb{N}} \overset{\mathrm{nuC}}{\approx} \left\{(v^{\mathsf{A}}, v_1^{\mathsf{B}})_{(v^{\mathsf{A}},v^{\mathsf{B}})\leftarrow \tilde{f}_\kappa(x,y)}\right\}_{\kappa\in\mathbb{N}}, \tag{27}$$

and the same holds for or the view of B.

That is, the above claim states that if a functionality is ϵ-SIM-DP and has perfect agreement, then the view of each party is indistinguishable from the view in an ϵ-DP functionality, even when adding the output of the other party.

Proof. The straightforward proof replaces an arbitrary functionality realizing the ϵ-SIM-DP of f with one that has (almost) perfect agreement.

By Lemma 5.11, there exists functionality ensemble $\widehat{f} = \left\{\widehat{f}_\kappa = (\widehat{f}_\kappa^{\mathsf{A}}, \widehat{f}_\kappa^{\mathsf{B}})\right\}_{\kappa\in\mathbb{N}}$ that realizes the ϵ-IND-DP of f. We show there exists a functionality ensemble $\left\{\tilde{f}_\kappa = (\tilde{f}_\kappa^{\mathsf{A}}, \tilde{f}_\kappa^{\mathsf{B}})\right\}_{\kappa\in\mathbb{N}}$ such that

1. $\tilde{f}_\kappa^{\mathsf{P}}(x,y)$ and $\widehat{f}_\kappa^{\mathsf{P}}(x,y)$ are the same for every $x, y \in \{0,1\}$, $\kappa \in \mathbb{N}$ and $\mathsf{P} \in \{\mathsf{A},\mathsf{B}\}$, and
2. $\Pr\left[\tilde{f}_\kappa^{\mathsf{A}}(x,y)_1 = \tilde{f}_\kappa^{\mathsf{B}}(x,y)_1\right] \geq 1 - \mathrm{neg}(\kappa)$.

Namely, $\tilde{f}$ also realizes the ϵ-IND-DP of f and has an almost perfect agreement. Since f has perfect agreement, $\tilde{f}$ satisfies Equation (27).

In the rest of the proof we construct the desired $\tilde{f}$. Since f has perfect agreement, and since $\widehat{f}^{\mathsf{P}}$ is computationally close to f^{P}, for every $x, y \in \{0,1\}$ it holds that

$$\left|\Pr\left[\widehat{f}^{\mathsf{A}}_{\kappa}(x,y)_1 = 1\right] - \Pr\left[\widehat{f}^{\mathsf{B}}_{\kappa}(x,y)_1 = 1\right]\right| \leq \mathrm{neg}(\kappa) \tag{28}$$

Therefore, for every $x, y \{0,1\}$ there exists ensembles of Boolean random variables pairs $\left\{(R^{\mathsf{A}}_{x,y,\kappa}, R^{\mathsf{B}}_{x,y,\kappa})\right\}_{\kappa\in\mathbb{N}}$ such that for any κ:

$$R^{\mathsf{P}}_{x,y,\kappa} \equiv \widehat{f}^{\mathsf{P}}_{\kappa}(x,y)_1 \tag{29}$$

and

$$\Pr\left[R^{\mathsf{A}}_{x,y,\kappa} = R^{\mathsf{B}}_{x,y,\kappa}\right] \geq 1 - \mathrm{neg}(\kappa) \tag{30}$$

For $r \in \{0,1\}$, define $\tilde{f}^{\mathsf{P}}_{\kappa}(x,y,r) := \widehat{f}^{\mathsf{P}}_{\kappa}(x,y)|_{\widehat{f}^{\mathsf{P}}_{\kappa}(x,y)=r}$, and let $\tilde{f}^{\mathsf{P}}_{\kappa}(x,y) = \tilde{f}^{\mathsf{P}}_{\kappa}(x,y,R^{\mathsf{P}}_{x,y,\kappa})$. By construction, the distributions $\tilde{f}^{\mathsf{P}}_{\kappa}(x,y)$ and $\widehat{f}^{\mathsf{P}}_{\kappa}(x,y)$ are the same and $\tilde{f}$ has almost perfect agreement. □

Proof of Lemma 5.12. The proof follows Theorem 5.2 and Claim 5.13, using a similar hybrid argument as in the proof of Theorem 4.25. □

5.2 Extension to Functions that are not Monotone under Relabeling

We now extend our results to a large class of functions: functions that are not "monotone under relabeling".

Definition 5.14 (Monotone under relabeling)**.** *A function $g\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is* monotone under relabeling *if there exists bijective functions $\sigma_x, \sigma_y : [2^n] \to \{0,1\}^n$ such that for every $x \in \{0,1\}^n$ and $i \leq j \in [2^n]$:*

$$g(x, \sigma_y(i)) \leq g(x, \sigma_y(j)),$$

and, for every $y \in \{0,1\}^n$ and $i \leq j \in [2^n]$:

$$g(\sigma_x(i), y) \leq g(\sigma_x(j), y).$$

Theorem 5.15. *There exists a constant $c > 0$ such that the following holds for every $n \in \mathbb{N}$. Let ϵ, β be functions such that for every $\kappa \in \mathbb{N}$: $\epsilon(\kappa), \beta(\kappa) \in [0,1]$, $1/2 \geq \beta(\kappa) \geq c \cdot n^2 \cdot \epsilon(\kappa)^2$ and $\beta(\kappa) \geq 1/p(\kappa)$ for some $p \in \mathrm{poly}$. Let Π be a PPT two-party protocol that is ϵ-IND-DP, and computes a function g over $\{0,1\}^n \times \{0,1\}^n$ that is not monotone under relabeling, with worst-case correctness at least $\beta(\kappa)$ and perfect agreement, then there exists a non-uniform computationally secure OT.*

We will show that every function that is not monotone under relabeling, has a copy of the XOR function that is "embedded" in it.

Definition 5.16 (Embedded XOR)**.** *A function* $g\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *has* embedded XOR *if there exists* $x_0, x_1 \in \{0,1\}^n$ *and* $y_0, y_1 \in \{0,1\}^n$ *such that for every* $b, c \in \{0,1\}$, $g(x_b, y_c) = b \oplus c$.

For example the Hamming distance function $\mathrm{Ham}(x,y)$ over $\{0,1\}^n \times \{0,1\}^n$ has an embedded XOR, by using the inputs $x_b = b \circ 0^{n-1}$ and $y_c = c \circ 0^{n-1}$.

It is clear that a function that is monotone under relabeling does not have an embedded XOR. In the following we show the opposite direction: every function g that is not monotone under relabeling has an embedded XOR. Moreover, we show that if Π is a ϵ-IND-DP protocol that computes function g with worst-case correctness β, then there exists a $n \cdot \epsilon$-IND-DP protocol $\widetilde{\Pi}$ that compute XOR with the same correctness. Theorem 5.15 then follows by Theorem 5.9.

Lemma 5.17. *A function that is not monotone under relabeling, has an embedded XOR.*

Proof. Let $g\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function that has no embedded XOR. We show that g is monotone under relabeling.

For input $x \in \{0,1\}^n$, let $Z_x = \{y \mid g(x,y) = 0\}$. We claim that for any x_0 and x_1 in $\{0,1\}$, it must hold that either $Z_{x_0} \subseteq Z_{x_1}$, or, $Z_{x_1} \subseteq Z_{x_0}$. Indeed, otherwise there is y_0, y_1 such that $y_0 \in Z_{x_0} \setminus Z_{x_1}$ and $y_1 \in Z_{x_1} \setminus Z_{x_0}$, and therefore, for $b, c \in \{0,1\}$, $g(x_b, y_c) = b \oplus c$.

Let $\sigma_x : [2^n] \to \{0,1\}^n$ be a bijective function such that for every $i \leq j$, $\left|Z_{\sigma_x(i)}\right| \geq \left|Z_{\sigma_x(j)}\right|$. Then it must hold that $Z_{\sigma_x(j)} \subseteq Z_{\sigma_x(i)}$, and therefore for every $y \in \{0,1\}^n$, $g(\sigma_x(i), y) \leq g(\sigma_x(j), y)$.

Repeating this argument to construct σ_y ends the proof. □

Lemma 5.18. *Let* ϵ *be a function with* $\epsilon(\kappa) \in [0,1]$ *and let* $\Pi = (\mathsf{A}, \mathsf{B})$ *be a* ϵ-IND-DP *protocol. Then for every* $x_0, x_1, y_0, y_1 \in \{0,1\}^n$*, the protocol* $\widetilde{\Pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}})$ *defined by* $(\widetilde{\mathsf{A}}(b), \widetilde{\mathsf{B}}(c))(1^\kappa) = (\mathsf{A}(x_b), \mathsf{B}(y_c))(1^\kappa)$ *is* $(n\epsilon)$-IND-DP.

Proof. For $x, y \in \{0,1\}^n$ and $\kappa \in \mathbb{N}$, let $V^{\mathsf{B}}_{x,y,\kappa}$ be the view of B in a random execution of $(\mathsf{A}(x), \mathsf{B}(y))(1^\kappa)$. Let D be a $\mathsf{ppt}^{\mathsf{NU}}$. Since Π is ϵ-IND-DP, for every $x, x' \in \{0,1\}^n$ with $\mathrm{Ham}(x,x') = 1$ it hold that

$$\Pr\left[\mathsf{D}(V^{\mathsf{B}}_{x,y,\kappa}, 1^\kappa) = 1\right] \leq e^{\epsilon(\kappa)} \cdot \Pr\left[\mathsf{D}(V^{\mathsf{B}}_{x',y,\kappa}, 1^\kappa) = 1\right] + \mathrm{neg}(\kappa) \tag{31}$$

A simple calculation (known as "singleton privacy implies group privacy") shows that for every $x, x' \in \{0,1\}^n$ with $\mathrm{Ham}(x,x') = d$:

$$\Pr\left[\mathsf{D}(V^{\mathsf{B}}_{x,y,\kappa}, 1^\kappa) = 1\right] \leq e^{d\cdot\epsilon(\kappa)} \cdot \Pr\left[\mathsf{D}(V^{\mathsf{B}}_{x',y,\kappa}, 1^\kappa) = 1\right] + \mathrm{neg}(\kappa).$$

The proof for A's privacy thus followed by the fact that for any $x_0, x_1 \in \{0,1\}^n$, the Hamming distance $\mathrm{Ham}(x,x')$ is at most n. The proof for the privacy of B follows similar lines. □

We remark that the loss incurred in Lemma 5.18 is sometimes unnecessary. For example, in the XOR-embedding of the Hamming distance function that we considered above, the distance between x_0 and x_1 (and also between y_0 and y_1) is only one, and therefore, no losses in privacy are incurred in this case, and Theorem 5.15 holds for $g(x,y) = \mathrm{Ham}(x,y)$ without the loss of n^2 factor, in the privacy.

Proving Theorem 5.15. We now ready to prove Theorem 5.15.

Proof of Theorem 5.15. Let Π be a protocol that satisfies the requirements of Theorem 5.15 with respect to a function g that is not monotone under relabeling. By Lemma 5.17, there exist $x_0, x_1, y_0, y_1 \in \{0,1\}^n$ such that for every $b, c \in \{0,1\}$, $g(x_b, y_c) = b \oplus c$. Therefore, the protocol defined by $(\widetilde{\mathsf{A}}(b), \widetilde{\mathsf{B}}(c))(1^\kappa) := (\mathsf{A}(x_b), \mathsf{B}(y_c))(1^\kappa)$ computes the XOR functionality with average correctness at least $\beta(\kappa)$, and by Lemma 5.18 this protocol is $(n\epsilon)$-IND-DP. Thus, the theorem follows by Theorem 5.9. □

References

[1] B. Aiello, Y. Ishai, and O. Reingold. Priced oblivious transfer: How to sell digital goods. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 119–135. Springer, 2001. 1

[2] A. Beimel, T. Malkin, and S. Micali. The all-or-nothing nature of two-party secure computation. In *Annual International Cryptology Conference*, pages 80–97. Springer, 1999. 7

[3] A. Beimel, K. Nissim, and E. Omri. Distributed private data analysis: Simultaneously solving how and what. In *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, pages 451–468, 2008. 5, 7

[4] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995. 9

[5] T. H. Chan, E. Shi, and D. Song. Optimal lower bound for differentially private multi-party aggregation. In *Algorithms - ESA 2012 - 20th Annual European Symposium, Ljubljana, Slovenia, September 10-12, 2012. Proceedings*, pages 277–288, 2012. 5, 7

[6] C. Crépeau. Efficient cryptographic protocols based on noisy channels. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 306–317. Springer, 1997. 6

[7] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *Foundations of Computer Science, 1988., 29th Annual Symposium on*, pages 42–52. IEEE, 1988. 6

[8] C. Dwork and G. N. Rothblum. Concentrated differential privacy. *arXiv preprint arXiv:1603.01887*, 2016. 8

[9] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006*, pages 265–284, 2006. 2, 4

[10] C. Dwork, G. N. Rothblum, and S. Vadhan. Boosting and differential privacy. In *Proceedings of the 51st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 51–60, 2010. 13

[11] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985. 1

[12] O. Goldreich. *Foundations of Cryptography – Volume 2: Basic Applications*. Cambridge University Press, 2004. 16

[13] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *stoc19*, pages 218–229, 1987. 1, 27

[14] O. Goldreich, H. Krawczyk, and M. Luby. On the existence of pseudorandom generators. *SIAM Journal on Computing*, 22(6):1163–1175, 1993. 7

[15] V. Goyal, I. Mironov, O. Pandey, and A. Sahai. Accuracy-privacy tradeoffs for two-party differentially private protocols. In *Advances in Cryptology – CRYPTO '13*, pages 298–315, 2013. 5, 6, 7

[16] V. Goyal, D. Khurana, I. Mironov, O. Pandey, and A. Sahai. Do distributed differentially-private protocols require oblivious transfer? In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 55. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016. , 4, 5, 7

[17] I. Haitner. Implementing oblivious transfer using collection of dense trapdoor permutations. In *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004*, pages 394–409, 2004. 1

[18] I. Haitner. A parallel repetition theorem for any interactive argument. *SIAM J. Comput.*, 42 (6):2487–2501, 2013. 7

[19] I. Haitner, D. Harnik, and O. Reingold. On the power of the randomized iterate. *SIAM J. Comput.*, 40(6):1486–1528, 2011. 7

[20] I. Haitner, O. Reingold, and S. Vadhan. Efficiency improvements in constructing pseudorandom generators from one-way functions. *SIAM Journal on Computing*, 42(3):1405–1430, 2013. Special Issue on *STOC '10*. 27

[21] I. Haitner, E. Omri, and H. Zarosim. Limits on the usefulness of random oracles. *Journal of Cryptology*, 29(2):283–335, 2016. 5, 7

[22] I. Haitner, K. Nissim, E. Omri, R. Shaltiel, and J. Silbak. Computational two-party correlation. In *Proceedings of the 59th Annual Symposium on Foundations of Computer Science (FOCS)*, 2018. , 4, 5, 7

[23] D. Harnik, M. Naor, O. Reingold, and A. Rosen. Completeness in two-party secure computation: A computational view. *Journal of Cryptology*, 19(4):521–552, 2006. 7

[24] J. Håstad, R. Pass, K. Pietrzak, and D. Wikström. An efficient parallel repetition theorem. In *Theory of Cryptography, Seventh Theory of Cryptography Conference, TCC 2010*, 2010. 7

[25] W. Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58:13–30, 1963. 14

[26] T. Holenstein. Pseudorandom generators from one-way functions: A simple construction for any hardness. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006*, 2006. 7, 27

[27] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989. 27

[28] P. Kairouz, S. Oh, and P. Viswanath. Differentially private multi-party computation: Optimality of non-interactive randomized response. *arXiv preprint arXiv:1407.1546*, 2014. 7

[29] Y. T. Kalai. Smooth projective hashing and two-message oblivious transfer. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 78–95. Springer, 2005. 1

[30] D. Khurana, H. K. Maji, and A. Sahai. Black-box separations for differentially private protocols. In *Advances in Cryptology – ASIACRYPT 2014*, pages 386–405, 2014. 5, 7

[31] J. Kilian. A general completeness theorem for two party games. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 553–560. ACM, 1991.

[32] J. Kilian. More general completeness theorems for secure two-party computation. In *STOC*, pages 316–324. Citeseer, 2000.

[33] E. Kushelvitz. Privacy and communication complexity. *SIAM Journal on Discrete Mathematics*, 5(2):273–284, 1992.

[34] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE transactions on information theory*, 39(3):733–742, 1993. 9

[35] A. McGregor, I. Mironov, T. Pitassi, O. Reingold, K. Talwar, and S. P. Vadhan. The limits of two-party differential privacy. *Electronic Colloquium on Computational Complexity (ECCC)*, page 106, 2011. Preliminary version in *FOCS'10*. 5, 6, 7

[36] I. Mironov, O. Pandey, O. Reingold, and S. P. Vadhan. Computational differential privacy. In *Advances in Cryptology – CRYPTO '09*, pages 126–142, 2009. 4, 11, 32, 33

[37] M. Naor and B. Pinkas. Efficient oblivious transfer protocols. In *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*, pages 448–457. Society for Industrial and Applied Mathematics, 2001. 1

[38] A. C. Nascimento and A. Winter. On the oblivious-transfer capacity of noisy resources. *IEEE Transactions on Information Theory*, 54(6):2572–2581, 2008. 6

[39] C. Peikert, V. Vaikuntanathan, and B. Waters. A framework for efficient and composable oblivious transfer. In *Annual international cryptology conference*, pages 554–571. Springer, 2008. 1

[40] V. M. Prabhakaran and M. M. Prabhakaran. Assisted common information with an application to secure two-party sampling. *IEEE Transactions on Information Theory*, 60(6):3413–3434, 2014. 6

[41] M. O. Rabin. How to exchange secrets by oblivious transfer. TR-81, Harvard, 1981. 1

[42] S. L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965. 3, 5

[43] S. Wolf and J. Wultschleger. Zero-error information and applications in cryptography. In *Information Theory Workshop, 2004. IEEE*, pages 1–6. IEEE, 2004. 6

[44] J. Wullschleger. *Oblivious-Transfer Amplification*. PhD thesis, ETH Zurich, 2008. 1

[45] J. Wullschleger. Oblivious transfer from weak noisy channels. In *Theory of Cryptography Conference*, pages 332–349. Springer, 2009. , 1, 2, 3, 9, 17, 18, 20

[46] A. C. Yao. Protocols for secure computations. In *Proceedings of the 23th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 160–164, 1982. 7

[47] A. C. Yao. How to generate and exchange secrets. In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 162–167. IEEE Computer Society, 1986. 1

A Missing Proofs

Proving Proposition 3.2

Proposition A.1 (Proposition 3.2, recited)**.** *Let* $0 < \epsilon < \mu < 1$*, and let* (X,Y)*,* $(\tilde{X},\tilde{Y})$ *be two pairs of random variables over the same domain* $\mathcal{X} \times \mathcal{Y}$*, such that* $\mathrm{SD}((X,Y),(\tilde{X},\tilde{Y})) \leq \epsilon$*. Let* $E_0, E_1 \subseteq \mathcal{X} \times \mathcal{Y}$ *be two sets such that for every* $b \in \{0,1\}$*,* $\Pr[(X,Y) \in E_b] \geq \mu$*. Then* $\mathrm{SD}(\tilde{X}|_{\{(\tilde{X},\tilde{Y})\in E_0\}}, \tilde{X}|_{\{(\tilde{X},\tilde{Y})\in E_1\}}) \leq \mathrm{SD}(X|_{\{(X,Y)\in E_0\}}, X|_{\{(X,Y)\in E_1\}}) + 4\epsilon/\mu$.

Proof. In the following we show that for every $b \in \{0,1\}$,
$\mathrm{SD}(\tilde{X}|_{\{(\tilde{X},\tilde{Y})\in E_b\}}, X|_{\{(X,Y)\in E_b\}}) \leq 2\epsilon/\mu$. The proof then follows using the triangle inequality.

Note that, by data processing,
$\mathrm{SD}(\tilde{X}|_{\{(\tilde{X},\tilde{Y})\in E_b\}}, X|_{\{(X,Y)\in E_b\}}) \leq \mathrm{SD}((\tilde{X},\tilde{Y})|_{\{(\tilde{X},\tilde{Y})\in E_b\}}, (X,Y)|_{\{(X,Y)\in E_b\}})$

For every set $\mathcal{A} \subseteq \mathcal{X} \times \mathcal{Y}$, and $b \in \{0,1\}$, we want to bound
$\Pr[(X,Y) \in \mathcal{A} \mid (X,Y) \in E_b] - \Pr\left[(\tilde{X},\tilde{Y}) \in \mathcal{A} \mid (\tilde{X},\tilde{Y}) \in E_b\right]$.

It holds that,

$$\begin{aligned}
&\Pr\left[(X,Y)\in\mathcal{A}\mid(X,Y)\in E_b\right]-\Pr\left[(\tilde{X},\tilde{Y})\in\mathcal{A}\mid(\tilde{X},\tilde{Y})\in E_b\right] \qquad (32)\\
&=\frac{\Pr\left[(X,Y)\in\mathcal{A}\cap E_b\right]}{\Pr\left[(X,Y)\in E_b\right]}-\frac{\Pr\left[(\tilde{X},\tilde{Y})\in\mathcal{A}\cap E_b\right]}{\Pr\left[(\tilde{X},\tilde{Y})\in E_b\right]}\\
&\leq\frac{\Pr\left[(X,Y)\in\mathcal{A}\cap E_b\right]}{\Pr\left[(X,Y)\in E_b\right]}-\frac{\Pr\left[(X,Y)\in\mathcal{A}\cap E_b\right]-\epsilon}{\Pr\left[(X,Y)\in E_b\right]+\epsilon}\\
&=\frac{\epsilon\cdot\Pr\left[(X,Y)\in\mathcal{A}\cap E_b\right]+\epsilon\cdot\Pr\left[(X,Y)\in E_b\right]}{\Pr\left[(X,Y)\in E_b\right]\left(\Pr\left[(X,Y)\in E_b\right]+\epsilon\right)}\\
&\leq\frac{2\epsilon\cdot\Pr\left[(X,Y)\in E_b\right]}{\left(\Pr\left[(X,Y)\in E_b\right]\right)^2}\\
&\leq\frac{2\epsilon}{\mu}
\end{aligned}$$

Where the last equality follows because $\frac{A}{B}-\frac{A-\epsilon}{B+\epsilon}=\frac{\epsilon(A+B)}{B(B+\epsilon)}$. Since Equation (32) holds for every set $\mathcal{A}\subseteq\mathcal{X}\times\mathcal{Y}$, we get that
$(X,Y)|_{\{(X,Y)\in E_b\}}\overset{\mathrm{S}}{\approx}_{2\epsilon/\mu}(X,Y)|_{\left\{(\tilde{X},\tilde{Y})\in E_b\right\}}$, for every $b\in\{0,1\}$. □

Proving Proposition 3.19

Proposition A.2 (Proposition 3.19, recited)**.** *An* (ϵ_0,p)-SWBSC *is a* $(0,\epsilon_0,\epsilon_0,2p,2p)$-WBSC.

Proof. The correctness and the receiver security properties hold from the definition.

For sender security, first notice that for every b_{B}, we get from the symmetry of SWBSC that:

$$\Pr\left[O^{\mathsf{B}}=b_{\mathsf{B}}\mid O^{\mathsf{A}}=O^{\mathsf{B}}\right]=\frac{\Pr\left[O^{\mathsf{A}}=O^{\mathsf{B}}\mid O^{\mathsf{B}}=b_{\mathsf{B}}\right]\Pr\left[O^{\mathsf{B}}=b_{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}}=O^{\mathsf{B}}\right]}=1/2,$$

and

$$\Pr\left[O^{\mathsf{B}}=b_{\mathsf{B}}\mid O^{\mathsf{A}}\neq O^{\mathsf{B}}\right]=\frac{\Pr\left[O^{\mathsf{A}}\neq O^{\mathsf{B}}\mid O^{\mathsf{B}}=b_{\mathsf{B}}\right]\Pr\left[O^{\mathsf{B}}=b_{\mathsf{B}}\right]}{\Pr\left[O^{\mathsf{A}}\neq O^{\mathsf{B}}\right]}=1/2$$

Now, assume for contradiction that, for some $b\in\{0,1\}$, a distinguisher D_b breaks the sender security in the WBSC definition. That is,
$\Pr\left[\mathsf{D}_b(V^{\mathsf{B}})=1|O^{\mathsf{B}}=b,O^{\mathsf{A}}=0\right]-\Pr\left[\mathsf{D}_b(V^{\mathsf{B}})=1|O^{\mathsf{B}}=b,O^{\mathsf{A}}=1\right]>2p$. Then, we can construct a distinguisher that breaks the specialized sender security: Let D_{1-b} be an algorithm such that $\Pr\left[\mathsf{D}_{1-b}(V^{\mathsf{B}})=1|O^{\mathsf{B}}=1-b,O^{\mathsf{A}}=0\right]-\Pr\left[\mathsf{D}_{1-b}(V^{\mathsf{B}})=1|O^{\mathsf{B}}=1-b,O^{\mathsf{A}}=1\right]\geq 0$, and consider the following algorithm:

Algorithm A.3 (D')**.**

Input: $(v,y)\in\mathrm{Supp}(V^{\mathsf{B}},O^{\mathsf{B}})$.

Operation: Output $\mathsf{D}_y(v)$.

It holds that:

$$\begin{aligned}
p \geq & \Pr\left[\mathsf{D}'(V^{\mathsf{B}}, O^{\mathsf{B}}) = 1 | O^{\mathsf{A}} = O^{\mathsf{B}}\right] - \Pr\left[\mathsf{D}'(V^{\mathsf{B}}, O^{\mathsf{B}}) = 1 | O^{\mathsf{A}} \neq O^{\mathsf{B}}\right] \\
= & 1/2 \cdot [\Pr\left[\mathsf{D}'(V^{\mathsf{B}}, 0) = 1 | O^{\mathsf{A}} = O^{\mathsf{B}}, O^{\mathsf{B}} = 0\right] - \Pr\left[\mathsf{D}'(V^{\mathsf{B}}, 0) = 1 | O^{\mathsf{A}} \neq O^{\mathsf{B}}, O^{\mathsf{B}} = 0\right]] \\
& + 1/2 \cdot [\Pr\left[\mathsf{D}'(V^{\mathsf{B}}, 1) = 1 | O^{\mathsf{A}} = O^{\mathsf{B}}, O^{\mathsf{B}} = 1\right] - \Pr\left[\mathsf{D}'(V^{\mathsf{B}}, 1) = 1 | O^{\mathsf{A}} \neq O^{\mathsf{B}}, O^{\mathsf{B}} = 1\right]] \\
= & 1/2 \cdot [\Pr\left[\mathsf{D}_0(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} = O^{\mathsf{B}}, O^{\mathsf{B}} = 0\right] - \Pr\left[\mathsf{D}_0(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} \neq O^{\mathsf{B}}, O^{\mathsf{B}} = 0\right]] \\
& + 1/2 \cdot [\Pr\left[\mathsf{D}_1(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} = O^{\mathsf{B}}, O^{\mathsf{B}} = 1\right] - \Pr\left[\mathsf{D}_1(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} \neq O^{\mathsf{B}}, O^{\mathsf{B}} = 1\right]] \\
= & 1/2 \cdot [\Pr\left[\mathsf{D}_0(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} = 0, O^{\mathsf{B}} = 0\right] - \Pr\left[\mathsf{D}_0(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} = 1, O^{\mathsf{B}} = 0\right]] \\
& + 1/2 \cdot [\Pr\left[\mathsf{D}_1(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} = 0, O^{\mathsf{B}} = 1\right] - \Pr\left[\mathsf{D}_1(V^{\mathsf{B}}) = 1 | O^{\mathsf{A}} = 1, O^{\mathsf{B}} = 1\right]] \\
> & p.
\end{aligned}$$

□

Proving Proposition 3.20

Proposition A.4 (Proposition 3.20, recited)**.** *The following holds for every $b \in (0, 1/2)$ and $\ell \in \mathbb{N}$ such that $b\ell < 1/4$.*

$$\frac{(1/2+b)^\ell}{(1/2+b)^\ell + (1/2-b)^\ell} \in [\tfrac{1}{2}(1+b\ell), \tfrac{1}{2}(1+3b\ell)].$$

Proof. We start with the lower bound,

$$\begin{aligned}
\frac{(1/2+b)^\ell}{(1/2+b)^\ell+(1/2-b)^\ell} &= \frac{(1+2b)^\ell}{(1+2b)^\ell+(1-2b)^\ell} \\
&= \frac{\sum_{i=0}^{\ell}\binom{\ell}{i}(2b)^i}{2\sum_{i=0}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}}. \\
&= \frac{\sum_{i=0}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}+\sum_{i=0}^{\lfloor (\ell-1)/2\rfloor}\binom{\ell}{2i+1}(2b)^{2i+1}}{2\sum_{i=0}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}} \\
&= 1/2+\frac{\sum_{i=0}^{\lfloor (\ell-1)/2\rfloor}\binom{\ell}{2i+1}(2b)^{2i+1}}{2\sum_{i=0}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}} \\
&= 1/2+\frac{2b\ell}{2\sum_{i=0}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}}+\frac{\sum_{i=1}^{\lfloor (\ell-1)/2\rfloor}\binom{\ell}{2i+1}(2b)^{2i+1}}{2\sum_{i=0}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}} \\
&= 1/2+\frac{b\ell}{1+\sum_{i=1}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}}+\frac{\sum_{i=1}^{\lfloor (\ell-1)/2\rfloor}\binom{\ell}{2i+1}(2b)^{2i+1}}{2+2\sum_{i=1}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}} \\
&\geq 1/2+\frac{b\ell}{\sum_{i=0}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}} \\
&= 1/2+\frac{b\ell}{1+\sum_{i=1}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}} \\
&\geq 1/2+\frac{b\ell}{1+\sum_{i=1}^{\lfloor \ell/2\rfloor}(2b\ell)^{2i}} \\
&\geq 1/2+b\ell/2 = \tfrac{1}{2}(1+b\ell)
\end{aligned}$$

Finally a similar calculation yields the following upper bound,

$$\begin{aligned}
\frac{(1/2+b)^\ell}{(1/2+b)^\ell+(1/2-b)^\ell} &\leq 1/2+b\ell+\frac{\sum_{i=1}^{\lfloor (\ell-1)/2\rfloor}\binom{\ell}{2i+1}(2b)^{2i+1}}{2+2\sum_{i=1}^{\lfloor \ell/2\rfloor}\binom{\ell}{2i}(2b)^{2i}} \\
&\leq 1/2+b\ell+\frac{\sum_{i=1}^{\lfloor (\ell-1)/2\rfloor}(2b\ell)^{2i+1}}{2} \\
&\leq \tfrac{1}{2}(1+3b\ell)
\end{aligned}$$

□