ECCC

On the Complexity of Two-Party Differential Privacy

Iftach Haitner[*][†]   Noam Mazor[*]   Jad Silbak[*]   Eliad Tsfadia[*]

August 17, 2021

Abstract

In *distributed* differential privacy, the parties perform analysis over their joint data while preserving the privacy for *both* datasets. Interestingly, for a few fundamental two-party functions such as *inner product* and *Hamming distance*, the accuracy of the distributed solution lags way behind what is achievable in the *client-server* setting. McGregor, Mironov, Pitassi, Reingold, Talwar, and Vadhan [FOCS '10] proved that this gap is inherent, showing upper bounds on the accuracy of (any) distributed solution for these functions. These limitations can be bypassed when settling for *computational* differential privacy, where the data is differentially private only in the eyes of a computationally bounded observer, using public-key cryptography primitives.

We prove that the use of public-key cryptography is *necessary* for bypassing the limitation of McGregor et al., showing that a non-trivial solution for the inner-product, or the Hamming distance, *implies* the existence of a key-agreement protocol. Our bound implies a combinatorial proof for the fact that non-Boolean inner product of independent (strong) *Santha-Vazirani* sources is a good condenser. We obtain our main result by showing that the inner-product of a (single, strong) SV source with a uniformly random seed is a good condenser, even when the seed and source are *dependent*.

Keywords: differential privacy; inner product; public-key cryptography.

Contents

1 Introduction

Differential privacy aims to enable statistical analyses of databases while protecting individual-level information. A common model for database access is the *client-server model*: a single server holds the entire database, performs a computation over it, and reveals the result. When the database contains sensitive information of individuals, the server should be restricted to only reveal the result of a differentially private function of the database. That is, a function that leaks very little information on any particular (single) individual from the database.

Definition 1.1 (Differential Privacy [10]). *A randomized function ("mechanism") f is (ε, δ)-differentially private, denote (ε, δ)-DP, if for any two databases x, x' that differ in one entry, and any event $\mathcal{T}$:*

$$\Pr[f(x) \in \mathcal{T}] \le e^{\varepsilon} \cdot \Pr[f(x') \in \mathcal{T}] + \delta.$$

For the sake of simplicity, in this section, we only focus on the case $\delta = 0$, called *pure* differential privacy.

In this work, we consider *distributed*, two-party, database access: each party holds a private database, and they interact to perform data analysis over the *joint* data. Such interaction is differentially private, for short, *two-party differential privacy* (Dwork and Nissim [7]), if the parties perform the analysis while protecting the differential privacy of *both* parts of the data. That is, each party's view of the protocol execution is a differentially private function of the other party's database (input).[1] Motivated by the works of Dwork and Nissim [7] and McGregor, Mironov, Pitassi, Reingold, Talwar, and Vadhan [27], we focus on performing natural statistical analysis of the joint database. Specifically, the databases $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are vectors in $\{-1, 1\}^n$ (e.g., each row x_i is one if i^{th} individual smokes or not, and each row y_i is one if it suffers from high blood pressure), and the desired functionality is to estimate their correlation (e.g., to estimate the correlation between smoking and high blood pressure). The parties do that by estimating the *inner product (also known as, scalar product)* of the two (private) databases, i.e., $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$.[2], or equivalently their *Hamming distance*, i.e., $\mathsf{Ham}(x, y) = |i : x_i = y_i|$. (Indeed, $\langle x, y \rangle = n - 2 \cdot \mathsf{Ham}(x, y)$ for every $x, y \in \{-1, 1\}^n$).

The simplest ε-DP protocol for estimating the inner product is based on "randomized response": roughly, the party that holds x, sends a randomized version $\hat{x}_i$ of each entry x_i (where $\hat{x}_i$ is set to x_i w.p. $(1 + \varepsilon)/2$ and to $-x_i$ otherwise), and the other party estimates the inner product based on $(\hat{x}_1, \ldots, \hat{x}_n)$ and $y = (y_1, \ldots, y_n)$. This protocol, however, induces an (expected) additive error of $\Omega(\sqrt{n}/\varepsilon)$ (with respect to the true value of $\langle x, y \rangle$). For comparison, in the standard client-server model where the server holds the entire database $w = (x, y)$, it is easy to achieve an accuracy of only $O(1/\varepsilon)$.[3] McGregor et al. [27] proved that the large gap between the randomized response protocol and what is achievable in the client-server model this gap is unavoidable. Specifically,

---

[1]More specifically, for a two-party protocol $\Pi = (\mathsf{A}, \mathsf{B})$, let $V^{\mathsf{P}}(x, y)$ denote the view of a party $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ in random execution of $\Pi(x, y)$. Then for every algorithm (distinguisher) D, input $x \in \{-1, 1\}^n$ and pair of inputs $y, y' \in \{-1, 1\}^n$ that differ in one entry, it should holds that $\Pr[\mathsf{D}(V^{\mathsf{A}}(x, y)) = 1] \le \Pr[\mathsf{D}(V^{\mathsf{A}}(x, y')) = 1] \cdot e^{\varepsilon} + \delta$. A similar constraint applies when considering the leakage from V^{B}. A formal definition appears in Section 3.7.

[2]Dwork and Nissim [7] reduced a central data-mining problem (detecting correlations between two binary attributes) to approximating the inner product between two binary vectors. ([7] considered databases over $\{0, 1\}^n$, but there is a simple reduction between the $\{-1, 1\}$ case we consider here and the $\{0, 1\}$ case.)

[3]The inner product over $\{-1, 1\}^n$ is a *sensitivity*-2 function (i.e., changing a single entry may only change the result by at most 2). Therefore, a server that holds both x and y can simply compute $\langle x, y \rangle$, and output a (privacy-preserving) noisy estimation of it by adding a Laplace noise with standard deviation $2/\varepsilon$.

they showed that any two-party ε-differentially private protocol for the inner product, must incur an additive error of $\Omega(\sqrt{n}/(e^{\varepsilon} \cdot \log n))$.[4]

Computational Differential Privacy (CDP). Motivated by the above limitations on multi-party differential privacy, Beimel, Nissim, and Omri [2] and Mironov, Pandey, Reingold, and Vadhan [28] considered protocols that only guarantee a computational analog of differential privacy. Roughly, instead of requiring that each party's view is a differentially private function of the other party's input, it is only required that the output of any *efficient* Boolean function over a party's view, is differentially private (see Section 3.4 for a formal definition, and see [28] for a broader discussion on computational differential privacy). With this relaxation, it is well known that assuming the existence of *oblivious transfer* protocol, any efficient single party (i.e., client-server) DP mechanism can be emulated by a multi-party CDP protocol (e.g., [2, 9]). Specifically, the parties just need to perform a *secure multi-party computation* for emulating the single-party mechanism. In particular, by emulating a (single-party) inner-product mechanism, we can obtain a multi-party CDP protocol that is very accurate.

The above separation between computational and information-theoretic differential privacy has spawned an interesting research direction for understanding the complexity of computational differential privacy. In particular, Vadhan [33] raised the following question:

Question 1.2 ([33]). *What is the minimal complexity assumption needed to construct a computational task that can be solved by a computationally differentially private protocol, but is impossible to solve by an information-theoretically differentially private protocol?*

Recent works have made progress on understanding this question for computing *Boolean* functions, for example, showing that differential private protocol for computing the XOR function with non-trivial accuracy requires the existence of oblivious transfer [21]. Much less progress was made, however, towards understanding the complexity of more natural statistical tasks (e.g., estimating the inner product). In this work, we make the first step towards filling this gap.

1.1 Our Results

1.1.1 Differentially Private Two-Party Inner Product

Our main result is that any (common output) computational differentially private protocol that estimates the inner product non-trivially, can be used to construct a key-agreement protocol.

Theorem 1.3 (Main result, informal). *An ε-CDP two-party protocol that, for some $\ell \geq \log n$, estimates the inner product over $\{-1, 1\}^n \times \{-1, 1\}^n$ up to an additive error ℓ with probability $c \cdot e^{c \cdot \varepsilon} \cdot \ell/\sqrt{n}$ (for some universal constant $c > 0$), can be used to construct a key-agreement protocol.*

Theorem 1.3 extends to (ε, δ)-CDP two-party protocols, for $\delta \leq 1/n^2$. Theorem 1.3 also extends to protocols whose accuracy guarantee only holds on average: over uniform inputs chosen by the parties, and it is tight (up to a constant) for this case: the trivial protocol that always outputs zero (which clearly cannot imply key-agreement) is with probability $\Theta(\ell/\sqrt{n})$ at distance at most

---

[4]McGregor et al. [27] proved it using a deterministic extraction approach, and showed that it can be extended to (ε, δ)-DP for $\delta = o(1/n)$. Using a different approach that explore connection between differentially private protocols and communication complexity, [27] also proved a slightly stronger lower bound of $\Omega(\sqrt{n})$ for ε-DP protocols for small enough constant ε. The latter, however, does not extend to the approximate DP case (i.e., when $\delta > 0$).

ℓ from the inner product of two uniform vectors over $\{-1, 1\}^n$. A high-level proof of Theorem 1.3 appears at Section 2.

Furthermore, Theorem 1.3 also extends to the information theoretic settings: an (information theoretic) DP protocol that accurately estimates the inner-product functionality, implies an information theoretically secure key agreement. Since the latter does not exist, it implies that such protocols do not exist either. Applying this result for $\varepsilon = O(1)$ and $\ell = \Theta(\sqrt{n})$, reproves (with slightly better parameters) the result of [27] regarding the in-existence of such protocols.[5]

Finally, Theorem 1.3 also holds for a weaker notion of CDP protocols, known as CDP *against external observer*: the (computational) privacy is guaranteed to hold only with respect to the transcript of the execution (and not necessarily with respect to the parties' view). Since the existence of a key-agreement protocol trivially implies a highly accurate CDP against external observer protocol for estimating the inner product,[6] Theorem 1.3 yields that the existence of such a non-trivial CDP protocol is *equivalent* to the existence of key-agreement protocols.

1.1.2 Condensers for Strong Santha-Vazirani Sources

An additional contribution of our work is a new result about condensing strong Santha-Vazirani (SV) sources [27]. A random variable $X = (X_1, \ldots, X_n)$ over $\{-1, 1\}^n$ is called an α-*strong SV source* if, for every i and every fixing x_{-i} of $X_{-i} = (X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$, it holds that

$$\frac{\Pr[X_i = 1 \mid X_{-i} = x_{-i}]}{\Pr[X_i = -1 \mid X_{-i} = x_{-i}]} \in [\alpha, 1/\alpha]$$

McGregor et al. [27] proved their main result mentioned above, by showing that the inner product is a good *two-source extractor* for (standard) SV sources.[7] Specifically, they proved that for any two independent SV sources X and Y, the inner product $\langle X, Y \rangle$ modulo $m = \Theta(\sqrt{n}/\log n)$ is statistically close to the uniform distribution over $\mathbb{Z}_m$. We observe that, to some extent, the converse direction also holds: for every two independent strong SV sources X, Y: the *nonexistence* of a DP-protocol for accurately estimating their inner product, implies that their inner product is a good two-source *condenser*. Assume otherwise, then there exists $z \in \mathbb{N}$ such that $\Pr[\langle X, Y \rangle = z]$ is large. Consider the two-party protocol (A, B) in which A draws a random sample from X, party B draws a random sample from Y, and both parties output z (regardless of their samples). By definition, this protocol is an accurate (information theoretic) DP-protocol for the inner-product functionality of the parties' samples.

Equipped with the above observation, we use Theorem 1.3 to deduce the following corollary:

Corollary 1.4 (Inner product is a good condenser for strong SV sources, informal)**.** *For any size n, independent, $e^{-\varepsilon}$-strong SV sources X and Y, it holds that* $\mathrm{H}_\infty(\langle X, Y \rangle) \geq \log(\sqrt{n}/(c \cdot e^{c \cdot \varepsilon} \cdot \log n))$ *(for some universal constant $c > 0$).*[8]

In most aspects Corollary 1.4 is weaker than the result of McGregor et al. [27]: it only states that the inner product is a good condenser (and not extractor), does not hold for (standard) SV sources,

---

[5]More specifically, McGregor et al. [27] proved that for any $\beta > 0$, there exists no ε-DP protocol that with probability β, estimates the inner product with additive error $O(\beta\sqrt{n}/(e^\varepsilon \cdot \log n))$. For $\varepsilon \in O(1)$ and $\beta \in \Omega(\log n/\sqrt{n})$, Theorem 1.3 improves the result of [27] by a $\log n$ factor.

[6]The parties can jointly emulate a single server functionality over an encrypted channel that they established.

[7]In a (standard) SV source [32], each bit is somewhat unpredictable given only the *previous* bits (but not necessary given *all* other bits, as in strong SV).

[8]A similar result holds for $\langle X, Y \rangle \mod c \cdot \sqrt{n}$, see Corollary 4.2

and only holds when both sources remain hidden (i.e., we did not prove "strong" condenser). On the upside, our condenser has an *efficient black-box reconstruction algorithm*: given an oracle-access to an algorithm that predicts the value of $\langle X, Y \rangle$ too well, the reconstruction algorithm violates the unpredictability guarantee of the sources. (The result of [27], proven via Fourier analysis, does not yield a reconstruction algorithm.)

In addition to Corollary 1.4, a key part for proving Theorem 1.3 is showing that the inner product of a (single) strong SV source with a uniformly random seed is a good condenser, even when the seed and the source are *dependent*.

Theorem 1.5 (informal). *Let $W = (X, Y)$ be an $e^{-\varepsilon}$-strong SV source, and let R be a uniformly random seed over $\{-1, 1\}^n$. Then conditioned on the values of R, $X_{R^+} := \{X_i\}_{R_i=1}$ and $Y_{R^-} := \{Y_i\}_{R_i=-1}$, it holds that $\mathrm{H}_\infty(\langle X \cdot Y, R \rangle) \geq \log\left(\frac{\sqrt{n}}{c \cdot e^{c \cdot \varepsilon} \cdot \log n}\right)$ for some universal constant $c > 0$, letting $\cdot$ stand for coordinate/element-wise product.*

We remark that when only conditioning on R and X_{R^+} (but not Y_{R^-}), the result of Theorem 1.5 is easy to prove: Y is a SV source conditioned on X, and thus by [27], $\langle X \cdot Y, R \rangle$ is a good extractor, conditioned on R and X (and thus a good condenser). The surprising part of Theorem 1.5 is that the result holds also when conditioning also on the *seed related* information (X_{R^+}, Y_{R^-}). Theorem 1.5 plays a critical role in the proof of our main result: in the key-agreement protocol we construct for proving Theorem 1.3, it is critical to expose these seed related values. We hope that such seed-related condensers will find further applications.

Computational Santha-Vazirani sources. Some of the above results extend to *computational* Santha-Vazirani sources: an ensemble of random variables $\left\{X^\kappa = (X_1^\kappa, \ldots, X_{n(\kappa)}^\kappa)\right\}_{\kappa \in \mathbb{N}}$ over $\{-1, 1\}^{n(\kappa)}$ is called a *computational α-strong SV source*, if for every PPT P, every $\kappa \in \mathbb{N}$ and every $i \in [n(\kappa)]$, it holds that

$$\frac{\Pr\left[\mathsf{P}(X_{-i}^\kappa) = X_i^\kappa\right]}{\Pr\left[\mathsf{P}(X_{-i}^\kappa) = -X_i^\kappa\right]} \in [\alpha(\kappa), 1/\alpha(\kappa)] \pm \mathrm{neg}(\kappa)$$

Namely, each entry X_i of X is somewhat unpredictable by a computationally bounded algorithm, even when all the other entries X_{-i} are known.

Computationally unpredictable sources have an important role in the study of cryptography, most notably in constructions of pseudorandom generators. For instance, *next-block pseudo-entropy* [17] quantifies the (average) hardness of efficiently predicting X_i from $X_{<i} = X_1, \ldots, X_{i-1}$. Next-block pseudo-entropy is a key ingredient in modern constructions of pseudorandom generators from one-way functions [17, 34], but the lack of efficient extraction tools for such sources prevents pushing the efficiency of these constructions even further.[9] In contrast, Theorem 1.5, which is proven via an efficient reconstruction algorithm, yields that the inner product is a good condenser for computational SV sources.[10] [11]

---

[9]Current technique apply a seeded extractor entry-by-entry, on the direct product of the source.

[10]The reconstruction algorithm of Dinur and Nissim [6] implies that it is hard to approximate the inner-product of computational SV source and an uniformly chosen vector. Their result, however, fails short (in terms of the approximation needed) to imply that the inner product is a good condenser for such sources.

[11]Like in the information theoretic case, the inner-product remains a good condenser also when conditioning on some seed related information.

Interestingly, we do not know whether Corollary 1.4 extends to computational SV sources (even if we require the sources to be efficiently samplable). In particular, trying to adjust the proof of Corollary 1.4 for the computational settings requires proving that there exists *no* pair of efficiently samplable computational SV sources such the the following protocol is a (weak) key agreement: each party samples from one of these sources, and then the parties interact, with these samples as private inputs, in the protocol we introduce for proving Theorem 1.3 (see Protocol 2.1).

1.2 Additional Related Work

Complexity of differentially private protocols. There are two natural approaches for defining computational differential privacy. The more relaxed and common one is the *indistinguishably-based* definition, which restricts the distinguishing event, $\mathcal{T}$ in Definition 1.1, to *computationally identified* events. The second approach is the *simulation*-based definition, which asserts that the output of the mechanism f is computationally close to that of an (information-theoretic) differentially private mechanism. Relations between these (and other) notions are given in [28]. We remind that our reduction from key-agreement to CDP holds even when assuming CDP against external observer, which is weaker than the notions consider in [28]. See Section 3.7 for the formal definition and comparison to the standard notions.

For the single-party case (i.e., the client-server model), computational and information-theoretic differential privacy seem closer in power. Indeed, Groce, Katz, and Yerukhimovich [15] showed that a wide range of CDP mechanisms can be converted into an (information-theoretic) DP mechanism. Bun, Chen, and Vadhan [3] showed that under (unnatural) cryptographic assumptions, there exists a (single-party) task that can be efficiently solved using CDP, but is infeasible (not impossible) for information-theoretic DP. Yet, the existence of a stronger separation (i.e., one that implies the impossibility for information-theoretic DP) remains open (in particular, under more standard cryptographic assumptions).

Another extreme (and very applicable) scenario is the *local model*, in which each of the, typically many, parties holds a single element. Usually, information-theoretic DP protocols for this model are based on randomized response. Indeed, Chan, Shi, and Song [5] proved that randomized-response is optimal for any counting functionality (and in particular, inner product). In contrast, local CDP protocols can emulate *any* efficient (single party) mechanism using secure multiparty computation (MPC), yielding a separation between the CDP and DP notions.

So the main challenge is understanding the complexity of CDP protocols in the two-party (or "few" party) case. Most works made progress on the Boolean case, where each party holds one (sensitive) bit, and the goal is to privately estimate a boolean function over the bits (e.g., the XOR). Goyal, Mironov, Pandey, and Sahai [13] demonstrated a constant gap between the maximal achievable accuracy in the client-server and distributed settings for any non-trivial boolean functionality, and showed that any CDP protocol that breaks this gap implies the existence of one-way functions. Goyal, Khurana, Mironov, Pandey, and Sahai [14] showed that the existence of an accurate enough CDP protocol for the XOR function implies the existence of an oblivious transfer protocol. Haitner, Nissim, Omri, Shaltiel, and Silbak [20] showed that any non-trivial ε-CDP two-party protocol for the XOR functionality, implies an (infinitely-often) key agreement protocol. Recently, Haitner, Mazor, Shaltiel, and Silbak [21] improved the results of [14, 20], showing that any non-trivial CDP two-party protocol for XOR implies oblivious transfer.

In contrast to the study of Boolean functionalities, understanding the complexity of CDP two-party protocols for more natural tasks (i.e., low-sensitivity many-bits functionalities, such as the

inner product) remains (almost) completely open. The only exception is the result of Haitner, Omri, and Zarosim [18], who applied their generic reduction on the impossibility result of Mironov et al. [28], to deduce that accurate CDP protocol for the inner product does not exist in the *random oracle model* (and thus such protocol cannot be constructed in a fully black-box way from a symmetric-key primitive).

Complexity of "secure" primitives. The above line of work is part of a more general research challenge of characterizing the complexity of "secure" primitives. That is, understanding which tasks can be carried out information-theoretically, which tasks are *equivalent* (require and can be based on) one-way functions, which tasks are equivalent to public-key cryptography, and so on. While the complexity of many such primitives was shown to be equivalent to one-way functions, e.g., pseudorandom generators, commitment schemes, digital signature, [24, 31, 16, 30, 26], much less is known outside the one-way functions world (the world we care about in this work). One exception is the recent work of Haitner, Makriyannis, and Omri [19], who uses the key-agreement dichotomy of [22] to show that the existence of non-trivial two-party fair coin-flipping protocols, implies the existence of (infinitely often secure) key-agreement protocols.

1.3 Open Questions

In this work, we make progress towards understanding the complexity of CDP protocols for estimating the inner-product functionality. The main challenge is to extend this understanding to other CDP distributed computations. For some functionalities, e.g., Hamming distance, we have a simple reduction to the inner-product functionality. But finding a more general characterization that captures more (or even all) functionalities, remains open.

Another important question is to determine the *minimal* complexity assumption required for constructing a non-trivial CDP for the inner-product functionality. In this work, we answer this question with respect to the weaker notion of CDP against external observer (showing that Key-agreement is necessary and sufficient). It is still open, however, whether oblivious transfer is the right answer for CDP protocols for the inner product, achieving the standard (stronger) notion of differential privacy (and doing the same for other functions as well).

1.4 Paper Organization

In Section 2, we give a high-level proof of Theorem 1.3. Notations, definitions and general statements used throughout the paper are given in Section 3. Our key-agreement protocol and its security proof (i.e., the proof of Theorem 1.3), and also the proof of Corollary 1.4, are given in Section 4. The proof given in Section 4 relies on technical tools that are proven in Sections 5 to 7. Theorem 1.5 is restated in Section 5 and proven in Appendix A, which also contains the other missing proofs.

2 Our Technique

In this section, we provide a rather elaborate description of our proof technique. In Section 2.1 we consider an easy variant of Theorem 1.3 where the protocol computes the inner-product very accurately. In Section 2.2, we discuss the much more challenging case of slightly accurate protocols.

2.1 Highly Accurate Protocols

We show how to construct a key-agreement protocol from an (external observer) ε-CDP protocol Γ (i.e., ε-differentially private against computationally bounded adversaries) that almost always computes the inner-product functionality with an additive error smaller than $\sqrt{n}$. That is,

$$\Pr\left[|\mathsf{Out} - \langle X, Y \rangle| \leq \sqrt{n}/c\right] \geq 1 - 1/n^4 \tag{1}$$

for large enough constant $c > 0$, where $(X, Y) \leftarrow (\{\text{-}1, 1\}^n)^2$, and Out is the common output of $\Gamma(X, Y)$ (part of the transcript). As noted by McGregor et al. [27], if Γ would have been ε-DP (i.e., against computationally *unbounded* adversaries), then conditioned on the (common) transcript T, it holds that X and Y are (independent) $e^{-\varepsilon}$-strong SV sources. McGregor et al. [27] proved that $\langle X, Y \rangle$, the (non boolean) inner product of X and Y, has min-entropy $\approx \log(\sqrt{n})$. By that, they concluded that the expected distance between Out (which is a function of T) and $\langle X, Y \rangle$, is $\sqrt{n}$, in contradiction to the accuracy of Γ.[12]

However, since we only assume that Γ is ε-CDP, it is no longer true that X and Y are $e^{-\varepsilon}$-Santha-Vazirani sources. Indeed, assuming the existence of oblivious transfer, there exists an accurate protocol Γ for which the inner product of X and Y has *tiny* min-entropy given T (i.e., $\log(1/\varepsilon)$). Yet, we prove, and this is our main technical contribution, that a randomized inner product of X and Y, i.e., $\langle X \cdot Y, R \rangle$, where $\cdot$ stands for coordinate-wise product and R is a random seed in $\{0, 1\}^n$, does have high-min-entropy in the *eyes of a computationally bounded observer*, which only sees the transcript T and the seed R. Not only that, the inner product remains hidden (i.e., have large min-entropy), even when some seed-related information about X and Y leaks to the observer. We exploit this observation to construct the following "weak" key-agreement protocol.

Protocol 2.1 $(\Pi = (\mathsf{A}, \mathsf{B}))$**.**

Parameter: 1^n.

Operation:

1. A *samples* $x \leftarrow \{\text{-}1, 1\}^n$, *and* B *samples* $y \leftarrow \{\text{-}1, 1\}^n$.

2. *The parties interact in* $\Gamma(x, y)$. *Let* out *be the common output.*

3. A *samples* $r \leftarrow \{0, 1\}^n$, *and sends* $(r, x_r = \{x_i \colon r_i = 1\})$ *to* B.

4. B *sends* $y_{-r} = \{y_i \colon r_i = 0\}$ *to* A.

5. A *(locally) outputs* $(\mathsf{out} - \langle x_{-r}, y_{-r} \rangle)$, *and* B *(locally) outputs* $\langle x_r, y_r \rangle$.

That is, A uses its knowledge of x_{-r}, and the estimation of $\langle x, y \rangle$ given by the execution of Γ, to estimate B's output ($\langle x_r, y_r \rangle$).

Let X^n, Y^n, Out^n and R^n, be the values of x, y, out and r in a random execution of $\Pi(1^n)$. Let T^n be the transcript of Γ in this execution, and let $\mathsf{Out}_\mathsf{A}^n, \mathsf{Out}_\mathsf{B}^n$ be the parties local output.

---

[12]Actually, the argument of [27] fails short of contradicting the accuracy stated in Equation (1), and only contradicts $\Pr[|\mathsf{Out} - \langle X, Y \rangle| \leq \sqrt{n}/\mathrm{polylog}(n)] \approx 1$.

Equation (1) immediately yields that

$$\text{Agreement:} \qquad \Pr\left[|\mathsf{Out}_\mathsf{A}^n - \mathsf{Out}_\mathsf{B}^n| < \sqrt{n}/c\right] \geq 1 - 1/n^4 \qquad (2)$$

The crux of the proof, and its most technical part, is showing that the computational differential privacy of Γ yields that no PPT E can estimate $\mathsf{Out}_\mathsf{B}^n$ "too well":

$$\text{Secrecy:} \qquad \Pr\left[\left|\mathsf{E}(1^n, X_R^n, Y_{-R}^n, T^n, R^n) - \langle X_R^n, Y_R^n\rangle\right| < \sqrt{n}/c\right] < 1 - 3/n^4 \qquad (3)$$

Combining Equations (2) and (3), yields that Π enjoys a gap between the "agreement" and "secrecy", of the parties' local output. With some technical work, such a gap can be amplified to get a full-fledged key-agreement protocol. Parts of this amplification part are described as an independent result in Section 7. For the sake of this section, however, we focus only on the proof of Equation (3).[13] Hereafter, we omit n when clear from the context.

Assume towards a contradiction that there exists a PPT E that violates Equation (3). That is

$$\Pr\left[\left|\mathsf{E}(X_R, Y_{-R}, T, R) - \langle X_R, Y_R\rangle\right| \leq \sqrt{n}/c\right] \geq 1 - 3/n^4 \qquad (4)$$

We will show that E violates the (external observer) computational differential privacy of Γ. In the following we assume for simplicity that E is deterministic, and let

$$\mathcal{G} = \left\{(x, y, t)\colon \Pr\left[\left|\mathsf{E}(x_R, y_{-R}, t, R) - \langle x_R, y_R\rangle\right| \leq \sqrt{n}/c\right] \geq 1 - 3/n^2\right\} \qquad (5)$$

I.e., the triplets for which E does well. Equation (4) yields that

$$\Pr[(X, Y, T) \in \mathcal{G}] \geq 1 - 1/n^2 \qquad (6)$$

As an easy warm-up, assume that for every good $(x, y, t) \in \mathcal{G}$ it holds that $\mathsf{E}(x_r, y_{-r}, t, r) = \langle x_r, y_r\rangle$ (for every $r \in \{0,1\}^n$). Then, for every $i \in [n]$ and $r \in \{0,1\}^n$ with $r_i = 1$, it holds that

$$\mathsf{E}(x_r, y_{-r}, t, r) - \langle x_{r\oplus e^i}, y_{r\oplus e^i}\rangle = \langle x_r, y_r\rangle - \langle x_{r\oplus e^i}, y_{r\oplus e^i}\rangle = x_i \cdot y_i$$

for $e^i := 0^{i-1}10^{n-i}$. That is, knowing x and $y_{-i}(:= y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n)$, but not y_i, suffices for learning y_i, which blatantly violates the the differential privacy of Γ. Doing such a reconstruction using the much weaker guarantee we have about E, is more challenging. Details below.

For a triplet $s = (x, y, t)$ and $i \in [n]$, let

$$\alpha_i^s := \underbrace{\mathrm{E}_{R|R_i=1}[\mathsf{E}(x_R, y_{-R}, t, R)]}_{\alpha_{i,\mathcal{Y}}^s} - \underbrace{\mathrm{E}_{R|R_i=0}[\mathsf{E}(x_R, y_{-R}, t, R)]}_{\alpha_{i,\mathcal{X}}^s} \qquad (7)$$

---

[13]It is instructive to note that if E has access only to (X_R, T, R) (and even to all of X, and not just X_R), then Equation (3) would have easily followed by the fact that the inner product, with a random seed, is a strong extractor for SV sources. Actually, the above argument requires that Γ is *simulation-based computational differential private*: $X, Y|T$ is computationally indistinguishable from $X', Y'|T$ for (X', Y', T) that is (information theoretic) differentially private. (A stronger notion of privacy that is not known to be implied by the notion we consider here.) What makes proving Equation (3) challenging, is that E has also access to Y_{-R}, an information that is *dependent* on the seed R. Arguing about the entropy of an extractor's output in the face of such "seed dependent" leakage is typically a non-trivial task.

Note that $\alpha_{i,\mathcal{Y}}^s$ can be computed *without* knowing y_i, and similarly $\alpha_{i,\mathcal{X}}^s$ can be computed *without* knowing x_i. Below we exploit this property for learning y_i, or learning x_i. We make the following key observation,[14] see proof sketch in Section 2.1.1. Let $\mathsf{sign}(v) = 1$ if $v > 0$, and -1 otherwise.

Claim 2.2 (Reconstruction from non-boolean Hadamard encoding). *For any $s \in \mathcal{G}$ it holds that* $\Pr_{i \leftarrow [n]}[\mathsf{sign}(\alpha_i^s) = x_i \cdot y_i] \geq 0.9$.

That is, by computing both $\alpha_{i,\mathcal{Y}}^s$ and $\alpha_{i,\mathcal{X}}^s$, one can reconstruct $x_i \cdot y_i$ for most i's. While for computing both of these values one has to know both x_i and y_i, we bootstrap the above for learning either x_i or y_i. Let $S = (X, Y, T)$. By Claim 2.2 and the assumption about the size of $\mathcal{G}$ (Equation (6)), for most $i \in [n]$ it holds that

$$\Pr[\mathsf{sign}(\alpha_i^S) = X_i \cdot Y_i] \geq 0.85 \tag{8}$$

For ease of notation, we assume that Equation (8) holds for $i = 1$, fix i to this value and omit it from the notation. For $w \in \{-1, 1\}^n$, let $\widehat{w} := (-w_1, w_2, \ldots, w_n)$ (i.e., first bit is flipped). As mentioned above, one cannot directly use Equation (8) for computing Y_1 from (X, Y_{-1}, T), since computing α^S requires knowing X_1. So rather, we use the fact that

$$\alpha_{\mathcal{Y}}^{x,y,t} = \alpha_{\mathcal{Y}}^{x,\widehat{y},t} \quad \text{and} \quad \alpha_{\mathcal{X}}^{x,y,t} = \alpha_{\mathcal{X}}^{\widehat{x},y,t}$$

for all (x, y, t), to make the following observation (proof sketch in Section 2.1.2).

Claim 2.3 (Inconsistent variant). $\min_{X' \in \{X, \widehat{X}\}, Y' \in \{Y, \widehat{Y}\}} \left\{ \Pr\left[\mathsf{sign}(\alpha^{X', Y', T}) = X_1' \cdot Y_1'\right] \right\} \leq 0.75$.

That is, not all variants of the first bit of X and Y are highly consistent with the prediction induced by α. Assume for concreteness that $\Pr\left[\mathsf{sign}(\alpha^{\widehat{X}, Y, T}) = \widehat{X}_1 \cdot Y_1\right] \leq 0.75$ (other cases are analogous), and consider the algorithm D that on input (x_{-1}, y, t) outputs one if $\mathsf{sign}(\alpha^{(1, x_{-1}), y, t}) = y_1$. Equation (8) yields that

$$\Pr[\mathsf{D}(X_{-1}, Y, T) = 1 \mid X_1 = 1] \geq \Pr[\mathsf{D}(X_{-1}, Y, T) = 1 \mid X_1 = 0] + 0.1.$$

Since $\alpha^{(1, x_{-1}), y, t}$ can be efficiently approximated from (X_{-1}, Y, T), given access to E, the above violates the assumed computational differential privacy of Γ (for small enough constant ε).[15]

2.1.1 Reconstruction from Non-Boolean Hadamard Code

We sketch the proof of Claim 2.2.

Proof sketch. Assume for simplicity that for any $s = (x, y, t) \in \mathcal{G}$:

$$|\mathsf{E}(x_r, y_{-r}, t, r) - \langle x_r, y_r \rangle| \leq \sqrt{n}/c \tag{9}$$

---

[14]For $w \in \{-1, 1\}^n$, consider the *Non-Boolean Hadamard encoding* defined by $C(w) := \{\langle w, r \rangle\}_{r \in \{0,1\}^n}$. Since $\langle x_r, y_r \rangle = \langle x \cdot y, r \rangle$, Claim 2.2 implies that given access to an approximation of $C(z)$ (as the one induced by E), it is possible to reconstruct most bits of w. While such reconstruction algorithms are known (cf., Dinur and Nissim [6]), for our purposes we critically exploit the very specific structure of the reconstruction value α_i^s. In particular, that it combines two estimations: one does not require knowing y_i, and the second does not require knowing x_i.

[15]We remark that our results hold for any $\varepsilon > 0$.

for *all* $r \in \{0,1\}^n$ (and not for $1 - 1/n^2$ fraction of the r's, as in the definition of $\mathcal{G}$).[16]

Fix $s = (x, y, t) \in \mathcal{G}$ and omit it when clear from the context, and let $\delta(r) := \mathsf{E}(x_r, y_{-r}, t, r) - \langle x_r, y_r \rangle$. A simple calculation yields that

$$\alpha_i = \mathrm{E}_{r \leftarrow \{0,1\}^n|_{r_i=1}}[\mathsf{E}(x_r, y_{-r}, t, r)] - \mathrm{E}_{r \leftarrow \{0,1\}^n|_{r_i=0}}[\mathsf{E}(x_r, y_{-r}, t, r)] \tag{10}$$

$$= \ldots = x_i \cdot y_i + \underbrace{\mathrm{E}_{R|_{R_i=1}}[\delta(R)] - \mathrm{E}_{R|_{R_i=0}}[\delta(R)]}_{\xi_i}.$$

It follows that if $|\xi_i| < 1$, then $\mathsf{sign}(\alpha_i) = x_i \cdot y_i$. Thus, for proving the claim it suffices to argue that ξ_i is smaller than 1 for .9 fraction of the i's. Let $\mathcal{I} := \{i \in [n] : \xi_i \geq 1\}$ and $\mathcal{I}' := \{i \in [n] : \xi_i \leq -1\}$. We conclude the proof showing that $\max\{|\mathcal{I}|, |\mathcal{I}'|\} \leq 0.05n$. Assume towards a contradiction that this is not the case, and specifically that $|\mathcal{I}| > 0.05n$ (the case $|\mathcal{I}'| > 0.05n$ is analogous). Let I be uniform over $\mathcal{I}$, and compute

$$|\mathrm{E}[\xi_I]| = \left| \mathrm{E}_{I, R|_{R_I=1}}[\delta(R)] - \mathrm{E}_{I, R|_{R_I=0}}[\delta(R)] \right| \tag{11}$$

$$\leq (\max_r\{\delta(r)\} - \min_r\{\delta(r)\}) \cdot \mathrm{SD}(\delta(R|_{R_I=1}), \delta(R|_{R_I=0}))$$

$$\leq (\sqrt{n}/c) \cdot \mathrm{SD}(\delta(R|_{R_I=1}), \delta(R|_{R_I=0})).$$

The second inequality is by Equation (9). A rather straightforward bound, see Proposition 3.28, yields that $\mathrm{SD}(R|_{R_I=0}, R|_{R_I=1}) \leq 1/\sqrt{|\mathcal{I}|}$, and thus, by the data-processing property of statistical distance:

$$\mathrm{SD}(\delta(R|_{R_I=0}), \delta(R|_{R_I=1})) \leq 1/\sqrt{|\mathcal{I}|} \tag{12}$$

Combining Equations (11) and (12), yields that

$$|\mathrm{E}[\xi_I]| \leq (\sqrt{n}/c) \cdot (1/\sqrt{|\mathcal{I}|}) \leq \sqrt{20}/c.$$

Thus, for large enough c, we obtain that $|\mathrm{E}[\xi_I]| < 1$, in contradiction to the fact that, by definition of $\mathcal{I}$, it holds that $|\mathrm{E}[\xi_I]| \geq 1$. $\qquad\square$

2.1.2 Proving Claim 2.3

We sketch the proof of Claim 2.3.

Proof sketch. By definition, for every (x, y, t) it holds that

$$\alpha_{\mathcal{Y}}^{x,y,t} = \alpha_{\mathcal{Y}}^{x,\widehat{y},t} \quad \text{and} \quad \alpha_{\mathcal{X}}^{x,y,t} = \alpha_{\mathcal{X}}^{\widehat{x},y,t}$$

Recalling that $\alpha^s := \alpha_{\mathcal{Y}}^s - \alpha_{\mathcal{X}}^s$, we conclude that

$$\alpha^{x,y,t} + \alpha^{\widehat{x},\widehat{y},t} = \alpha_{\mathcal{Y}}^{x,y,t} - \alpha_{\mathcal{X}}^{x,y,t} + \alpha_{\mathcal{Y}}^{\widehat{x},\widehat{y},t} - \alpha_{\mathcal{X}}^{\widehat{x},\widehat{y},t} \tag{13}$$

$$= \alpha_{\mathcal{Y}}^{x,\widehat{y},t} - \alpha_{\mathcal{X}}^{\widehat{x},y,t} + \alpha_{\mathcal{Y}}^{\widehat{x},y,t} - \alpha_{\mathcal{X}}^{x,\widehat{y},t}$$

$$= \alpha^{\widehat{x},y,t} + \alpha^{x,\widehat{y},t}.$$

---

[16]Note that the $1/n^2$ fraction of "bad" r's (for which Equation (9) does not hold) can only affect the α_i's by at most $\frac{2}{n^2} \cdot (\max_{r \in \{0,1\}^n}\{\mathsf{E}(x_r, y_{-r}, t, r)\} - \min_{r \in \{0,1\}^n}\{\mathsf{E}(x_r, y_{-r}, t, r)\})$. Therefore, since without loss of generality E always outputs an estimation in $[-n, n]$, the "bad" r's might only affect the following calculation by the insignificant additive term of $4/n$.

Assume towards contradiction that Claim 2.3 does not hold. That is,

$$\forall X' \in \left\{X, \widehat{X}\right\}, Y' \in \left\{Y, \widehat{Y}\right\} : \quad \Pr\left[\mathsf{sign}(\alpha^{X',Y',T}) = \mathsf{sign}(X'_1 \cdot Y'_1)\right] > 0.75 \tag{14}$$

We conclude that

$$\Pr\left[\mathsf{sign}(\alpha^{X,Y,T} + \alpha^{\widehat{X},\widehat{Y},T}) = \mathsf{sign}(X_1 \cdot Y_1)\right] \tag{15}$$
$$\geq \Pr\left[\mathsf{sign}(\alpha^{X,Y,T}) = \mathsf{sign}(X_1 \cdot Y_1) \wedge \mathsf{sign}(\alpha^{\widehat{X},\widehat{Y},T}) = \mathsf{sign}(\widehat{X}_1 \cdot \widehat{Y}_1)\right] > 0.5,$$

and

$$\Pr\left[\mathsf{sign}(\alpha^{\widehat{X},Y,T} + \alpha^{X,\widehat{Y},T}) = \mathsf{sign}(\widehat{X}_1 \cdot Y_1)\right] \tag{16}$$
$$\geq \Pr\left[\mathsf{sign}(\alpha^{\widehat{X},Y,T}) = \mathsf{sign}(\widehat{X}_1 \cdot Y_1) \wedge \mathsf{sign}(\alpha^{X,\widehat{Y},T}) = \mathsf{sign}(X_1 \cdot \widehat{Y}_1)\right] > 0.5.$$

Since $\mathsf{sign}(X_1 \cdot Y_1)$ and $\mathsf{sign}(\widehat{X}_1 \cdot Y_1)$ have opposite values, the above is in contradiction to Equation (13). $\qquad \square$

2.2 Slightly Accurate Protocols

Our result holds for differentially private protocols for computing the inner product, of much weaker accuracy than what we considered above. In particular, we can only assume that for some $\ell \in \mathbb{N}$ it holds that

$$\Pr[|\mathsf{Out} - \langle X, Y \rangle| < \ell] \geq c \cdot \ell/\sqrt{n} \tag{17}$$

for large enough constant $c > 0$. Namely, an accuracy which is only a constant factor away from the trivial bound. This weaker starting point translates into a few additional challenges comparing to the highly accurate protocols case discussed above. The first challenge (more details in Section 2.2.1) is that for such a weak accuracy, it is much harder to identify a noticeable fraction of *non-trivial triplets*: triplets (x, y, t) on which E (the estimator that violates the secrecy of Protocol 2.1) has non-trivial accuracy in computing $\langle x_r, y_r \rangle$. Furthermore, for violating differential privacy using similar means to those used in Section 2.1, it is not enough to prove that many such non-trivial triplets exist. Rather, it should be possible to identify them, while missing one of the entries of either x or of y.

A second challenge (more details in Section 2.2.2) is that the accuracy guarantee of such non-trivial triplets is $c \cdot \ell/\sqrt{n}$, and not close to 1 as assumed in Section 2.1. This requires us to use a much more sophisticated reconstruction algorithm than the one we use in Section 2.1 (i.e., $\mathsf{sign}(\alpha_i^s)$).

2.2.1 Identifying Good Triplets

We need to argue that even with respect to the weak accuracy of the inner-product protocol Γ stated in Equation (17), an estimator E that violates the secrecy of the key-agreement protocol Π (Protocol 2.1), has many non-trivial triplets. Our first step is to use a more sophisticated amplification reduction for Π, such that E has the following guarantee:

$$\Pr\left[\left|\mathsf{E}(1^n, X_R^n, Y_{-R}^n, T^n, R^n) - \langle X_R^n, Y_R^n \rangle\right| < \ell \ \mid \ |\mathsf{Out}_\mathsf{A}^n - \mathsf{Out}_\mathsf{B}^n| < \ell\right] \geq c \cdot \ell/\sqrt{n} \tag{18}$$

That is, E predicts the key non-trivially when conditioning on *agreement*. Assuming such E exists, the natural criterion for a triplet $(x, y, t = (\mathsf{Out}, \cdot))$ to be non-trivial, is that Out is close to $\langle x, y \rangle$ (which by definition implies that $\mathsf{Out}_\mathsf{A}^n - \mathsf{Out}_\mathsf{B}^n$ is small). But as mentioned above, to be a useful criterion we should be able to identify such a triplet while missing x_i (or y_i).[17] We overcome this problem by assuming the transcript contains an ε-DP estimation e of $\langle x, y \rangle$ with a small additive error, which allows making the above decision without knowing the missing coordinate. By composition of differential privacy, it follows that even with such an estimation, it is impossible to violate the privacy of the inner-product protocol Γ.[18] So the new candidates for non-trivial triplets are

$$\mathcal{G} = \{(x, y, t = (e, \mathrm{out}, \cdot)) \colon |\mathrm{out} - e| \leq \ell\}$$

Unfortunately, the set $\mathcal{G}$ is still not what we need: it might be that E does very well on a small fraction of $\mathcal{G}$, and very poorly elsewhere. Therefore, our next step is to identify those triplets $(x, y, t) \in \mathcal{G}$ for which E does well. Concretely, those for which

$$\beta_{x,y,t} := \Pr_R[|\mathsf{E}(1^n, x_R, y_{-R}, t, R) - \langle x_R, y_R \rangle| < \ell] \geq c \cdot \ell / 2\sqrt{n} \qquad (19)$$

A simple argument yields that the density of $\mathcal{G}' := \{(x, y, t) \in \mathcal{G} \colon \beta_{x,y,t} \geq c \cdot \ell / 2\sqrt{n}\}$ in $\mathcal{G}$ is at least $c \cdot \ell / 2\sqrt{n}$. But how can we identify the triplets of $\mathcal{G}'$, while missing a coordinate? The idea is to try an estimate $\beta_{x,y,t}$ without having, for instance, x_i. That is, using

$$\beta_{x,y,t}^i = \Pr_{R|R_1=0}[|\mathsf{E}(1^n, x_R, y_{-R}, t, R) - \langle x_R, y_R \rangle| < \ell] \qquad (20)$$

As mentioned in Footnote 17, using such estimate might cause the decision whether $(x, y, t) \in \mathcal{G}'$ to be strongly *dependent* on x_i, the bit that the estimator is missing. This is unfortunate, since our reconstruction algorithm is only guaranteed to reconstruct *most* entries, and the above estimator may use the reconstruction algorithm only on indexes that it fails to reconstruct. Luckily, it turns out that $\beta_{x,y,t}^i$ is "not too far" from the desired $\beta_{x,y,t}$ for all but at most $1/\sqrt{n}$ of the indexes. And when focusing on triplets in the (identifiable) set $\mathcal{G}$, a careful analysis yields that the above dependency is not too harmful. More details in Sections 4 and 5

2.2.2 Reconstructing Slightly Good Triplets

Our goal is to find an efficient algorithm D that given (x_{-i}, y) (or (x, y_{-i})) and t as input, and an oracle access to an estimator E that is slightly accurate on the triplet $s = (x, y, t)$, computes a (non-trivial) prediction of the missing element x_i (or of y_i). Similarly to the highly accurate protocols case, see Section 2.1, we would like to determine a set of values $\{\alpha_i^s\}_{i \in [n]}$ such that:

1. $\Pr_{i \leftarrow [n]}[\mathsf{sign}(\alpha_i^s) = x_i \cdot y_i]$ is sufficiently larger than $1/2$ (i.e., the analog of Claim 2.2), and

2. $\alpha_i^s = \alpha_{i,\mathcal{Y}}^s + \alpha_{i,\mathcal{X}}^s$, where $\alpha_{i,\mathcal{Y}}^s$ can be computed without knowing y_i, and $\alpha_{i,\mathcal{X}}^s$ can be computed without knowing x_i.[19]

---

[17]It is tempting to ignore the missing coordinate and to decide whether a triplet is non-trivial by comparing $\langle x_{-i}, y_{-i} \rangle$ to Out. It turns out, however, that taking this approach might create an over-fitting between the decision and the value of x_i, which might result in a very poor predictor. As we mention below, a similar approach is useful with respect to a more distinguished set of triplets.

[18]We remark that while it may be impossible to implement a protocol with such an accurate estimation, privacy still holds by composition.

[19]In Section 2.1, we defined $\alpha_i^s = \alpha_{i,\mathcal{Y}}^s - \alpha_{i,\mathcal{X}}^s$ (i.e., with minus instead of plus) since it was more suitable for the specific α_i^s that we considered there. In general, there is nothing special about the minus, and we can always switch between the cases by considering $(-\alpha_{i,\mathcal{X}}^s)$ as the part that is independent of x_i (rather than $\alpha_{i,\mathcal{X}}^s$).

12

In particular, we search for a function g such that

$$\alpha_i^s := \mathrm{E}_R\Big[g^{\mathsf{E}}(i,x,y,t,R)\Big] = \frac{1}{2}\Bigg(\underbrace{\mathrm{E}_{R|R_i=1}\Big[g^{\mathsf{E}}(i,x,y,t,R)\Big]}_{\alpha_{i,\mathcal{Y}}^s} + \underbrace{\mathrm{E}_{R|R_i=0}\Big[g^{\mathsf{E}}(i,x,y,t,R)\Big]}_{\alpha_{i,\mathcal{X}}^s}\Bigg) \qquad (21)$$

for $R \leftarrow \{0,1\}^n$, satisfy the above requirements.[20] [21]

For ease of notation, in the following we assume that the domain of the vector r sent in Protocol 2.1 is $\{-1,1\}^n$ (rather than $\{0,1\}^n$.) For such $r \in \{-1,1\}^n$, let $r^+ := \{i\colon r_i = 1\}$, and let $r^- := [n] \setminus r^+$. Recall, see Section 2.2.1, that without loss of generality, the transcript contains a part e that is an ε-DP estimation of $\langle x,y\rangle$. In the following we assume for simplicity that $|e - \langle x,y\rangle| \le \ell$ (and not only with high probability). Towards defining the desired function g^{E}, we define the following function f^{E}:

$$f^{\mathsf{E}}(i, x_{r^+}, y_{r^-}, t = (e,\cdot), r) := 2 \cdot \mathsf{E}(i, x_{r^+}, y_{r^-}, t, r) - e \qquad (22)$$

Since E is a good estimator of $\langle x_{r^+}, y_{r^+}\rangle$ (followed by Equation (19)), it holds that

$$\Pr_{r\leftarrow\{-1,1\}^n}\Big[\big|f^{\mathsf{E}}(1^n, x_{r^+}, y_{r^-}, t, r) - \langle x\cdot y, r\rangle\big| < 3\ell\Big] \ge c\cdot\ell/2\sqrt{n} \qquad (23)$$

That is, f estimates $\langle x\cdot y, r\rangle$ well. In the following, let

$$\delta_i^{\mathsf{E}}(x,y,t,r) := f^{\mathsf{E}}(x_{r^+}, y_{r^-}, t, r) - \langle x_{-i}\cdot y_{-i}, r_{-i}\rangle$$

Note that if f would have computed $\langle x\cdot y, r\rangle$ perfectly, then $\delta_i(x,y,t,r) = x_i y_i r_i$, and the function g defined by $g(i,x,y,t,r) := \delta_i(x,y,t,r)\cdot r_i$ would have satisfies Requirment 1 (it is clear, see below, that g also satisfies Requirment 2). While we do not have such a strong guarantee about f, we manage to prove that taking some additive offset of δ_i yields a good enough g. Specifically, for $k \in \mathbb{Z}$, consider the function g_k^{E} defined by

$$g_k^{\mathsf{E}}(i,x,y,t,r) := \begin{cases} (\delta_i^{\mathsf{E}}(x,y,t,r) - k)\cdot r_i & \delta_i^{\mathsf{E}}(x,y,t,r) \in \{k-1, k+1\} \\ 0 & \text{otherwise;} \end{cases} \qquad (24)$$

Namely, g_k^{E} checks whether $f(i, x_{r^+}, y_{r^-}, \cdot)$ might be off by exactly k in estimating $\langle x,y\rangle$. If positive, it assumes this is the case and predicts $x_i y_i$, accordingly. In all other cases, g_k^{E} takes no risks an

---

[20]In Section 2.1, we implicitly used $g^{\mathsf{E}}(i,x,y,t,r) = 2\cdot(-1)^{r_i+1}\cdot\mathsf{E}(x_r, y_{-r}, t, r)$ and, assuming that E is highly accurate, showed that it satisfies the above requirements. We do not know whether this g satisfies the above requirements with respect to slightly accurate E.

[21]A reconstruction method from a somewhat accurate estimator for the inner-product functionality was presented by Dinur and Nissim [6], who showed a method for revealing most of the entries of a vector z given an oracle access to an algorithm E that accurately estimates $\langle z,r\rangle$ for 0.51 fractions of of the r's. This method, however, can only be carried out *efficiently* with respect to E that is accurate on $1 - \Omega(1/n)$ fraction of the r's ([8]). Dwork et al. [11] improved over the above, presenting an efficient reconstruction estimator that does well for given access to an estimator that does well on 0.77 fraction of the r's. Both methods, however, are not suitable for estimators that are accurate for less than a constant fraction of the r's (as we are aiming for in Equation (19)). Furthermore, there is no clear way how to turn the reconstruction algorithms presented by these methods to satisfy the second requirement above.

outputs 0. Of course, even if the check is positive, it might be that $f(i, x_{r^+}, y_{r^-}, \cdot)$ is off by $k - 2$ or by $k + 2$, and in this case g_k is wrong.

Since $\delta_i^{\mathsf{E}}(x, y, t, r)$ can be computed without knowing y_i if $r_i = 1$, and without knowing x_i if $r_i = -1$, the function g_k^{E}, for each k, satisfies Requirment 2. We conclude the proof by arguing that for some k, the function g_k^{E} satisfies Requirment 1.[22] That is,

$$\mathrm{E}_{i \leftarrow [n], r \leftarrow \{-1, 1\}^n} \left[x_i \cdot y_i \cdot g_k^{\mathsf{E}}(i, x, y, t, r) \right] > 0 \tag{25}$$

Hereafter, we remove E from notation, remove x, y, t from the inputs of g_k and δ_i, and remove x_{r^+}, y_{r^-}, t from the inputs of f. We also let $z := x \cdot y$ (coordinate-wise product), and let R be uniformly distributed $\{-1, 1\}^n$. Let A_k be the event $\{f(R) = \langle z, R \rangle + k\}$, and let B_k^i be the event $\{f(R) = \langle z_{-i}, R_{-i} \rangle - z_i R_i + k\}$. In words, A_k is the event that f accurately computes $\langle z, R \rangle$ with offset k (i.e., g_k^{E} is correct), and B_k^i is the event that f is not off by k, but seems so when z_i is not given (i.e., g_k^{E} is wrong). By definition, $g_k(i, r) = z_i$ for $r \in A_k$ (i.e., r's with $f(r) = \langle z, r \rangle + k$), equals to $-z_i$ for $r \in B_k^i$, and equals to zero for all other r's. Therefore,

$$z_i \cdot \mathrm{E}_R[g_k(i, R)] = \Pr_R[A_k] - \Pr_R\left[B_k^i\right] \tag{26}$$

We next argue that $\Pr_R[A_k] - \mathrm{E}_{i \leftarrow [n]}\left[\Pr_R\left[B_k^i\right]\right] > 0$ for some k, yielding that g_k satisfies Equation (25). In the following, let $a_k := \Pr_R[A_k]$ and $b_k := \mathrm{E}_{i \leftarrow [n]}\left[\Pr_R\left[B_k^i\right]\right]$. We make the following key observation: for any $k \in \mathbb{Z}$ it holds that

$$\left| b_k - \frac{1}{2}(a_{k-2} + a_{k+2}) \right| \leq \mu, \text{ for } \mu \in O(1/n) \tag{27}$$

That is, the probability of the "bad" event B_k^i is essentially the average of the probabilities of the good events A_{k-2} and A_{k+2}.[23]

To conclude the argument, assume towards a contraction that all k's are "bad": a_k is not larger than b_k (otherwise we are done). Under this assumption, Equation (27) yields that for every k:

$$a_{k+2} \geq 2a_k - a_{k-2} - \mu \tag{28}$$

Let $k^* := \mathrm{argmax}_{k \in \mathbb{Z}}\{a_k\}$. Equation (23) yields that $a_{k^*} \geq \frac{c}{12\sqrt{n}}$. By Equation (28), we deduce that $a_{k^*+2} \geq \frac{c}{12\sqrt{n}} - \mu$, that $a_{k^*+4} \geq \frac{c}{12\sqrt{n}} - 2\mu$, and so forth. Hence, for large enough c, the sequence $\{a_{k^*}, a_{k^*+2}, \ldots\}$ contains many large values, whose sum is more than one, in contradiction to the fact that they denote probabilities of disjoint events. We conclude that at least one k is not bad, making g_k is the desired function. More details in Section 6.

---

[22]Actually, this k, whose value might depend on (x, y, t), has to be efficiently computable. We ignore this concern from this high-level description.

[23]Equation (27) is over simplified, and we refer to Section 6 for the actual statement and proof. But very intuitively, (a close variant of) Equation (27) holds since, by definition, the event B_k^i occurs if and only if: (1) A_{k+2} occurs and $z_i R_i = -1$, or (2) A_{k-2} occurs and $z_i R_i = 1$. For a uniformly chosen i, the probability of (1) is (roughly) $\in a_{k+2} \cdot (1/2 \pm O(1/\sqrt{n}))$, and the probability of (2) is (roughly) $\in a_{k-2} \cdot (1/2 \pm O(1/\sqrt{n}))$. Equation (27) now follows since "typically" $a_{k-2}, a_{k+2} \in \Theta(1/\sqrt{n})$.

3 Preliminaries

3.1 Notations

We use calligraphic letters to denote sets, uppercase for random variables, and lowercase for values and functions. Let poly stand the set of all polynomials. Let neg stand for a negligible function.

For $x \in \mathbb{R}$, let $\lfloor x \rfloor$ [resp., $\lceil x \rceil$] denote the closest integer which is smaller [resp., larger] than x, and let $\lfloor x \rceil$ denote the closes integer to x (rounding of x). For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$, and for $a < b \in \mathbb{Z}$ let $[[a, b]] := [a, b] \cap \mathbb{Z}$. Given a vector $v \in \Sigma^n$, let v_i denote its ith entry. For a set $\mathcal{I} \subseteq [n]$, let $v_\mathcal{I}$ be the *ordered sequence* $(v_i)_{i \in \mathcal{I}}$, let $v_{-\mathcal{I}} := v_{[n] \setminus \mathcal{I}}$, and let $v_{-i} := v_{-\{i\}}$ (i.e., $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$). For $v \in \{-1, 1\}^n$, let $v_{<i>} := (v_1, \ldots, v_{i-1}, -v_i, v_{i+1}, \ldots, v_n)$. For $r \in \{-1, 1\}^n$, let $r^+ := \{i \in [n]: r_i = 1\}$ and let $r^- := [n] \setminus r^+$. For two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, let $x \cdot y := (x_1 \cdot y_1, \ldots, x_n \cdot y_n)$, and let $\langle x, y \rangle := \sum_{i=1}^n x_i y_i$. The vectors x and y are *neighboring*, if they differ in exactly one entry. All logarithms considered here are in base 2.

3.2 Distributions and Random Variables

The support of a distribution P over a finite set $\mathcal{S}$ is defined by $\text{Supp}(P) := \{x \in \mathcal{S} : P(x) > 0\}$. For a (discrete) distribution D let $d \leftarrow D$ denote that d was sampled according to D. Similarly, for a set $\mathcal{S}$, let $x \leftarrow \mathcal{S}$ denote that x is drawn uniformly from $\mathcal{S}$. For a finite set $\mathcal{X}$ and a distribution C_X over $\mathcal{X}$, we use the capital letter X to denote the random variable that takes values in $\mathcal{X}$ and is sampled according to C_X. The statistical distance (also known as, variation distance) of two distributions P and Q over a discrete domain $\mathcal{X}$ is defined by $\text{SD}(P, Q) := \max_{\mathcal{S} \subseteq \mathcal{X}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2} \sum_{x \in \mathcal{S}} |P(x) - Q(x)|$.

Definition 3.1 (Strong Santha-Vazirani sources)**.** *The random variable X over $\{-1, 1\}^n$ is an α-*strong Santha-Vazirani source *(denoted α-strong* SV*) if for every $i \in [n]$ and $x_{-i} \in \{-1, 1\}^{n-1}$ it holds that:*

$$\alpha \leq \frac{\Pr[X_i = 1 \mid X_{-i} = x_{-i}]}{\Pr[X_i = -1 \mid X_{-i} = x_{-i}]} \leq 1/\alpha.$$

Computation Santha-Vazirani sources.

Definition 3.2 (Computational strong Santha-Vazirani sources)**.** *The random variable ensemble $X = \{X_\kappa\}_{\kappa \in \mathbb{N}}$ over $\{-1, 1\}^n$ is an $\alpha(\kappa)$-*strong computational Santha-Vazirani source *(denoted α-*strong CSV*) if for every* PPT *A, $i \in [n]$ and $x_{-i} \in \{-1, 1\}^{n-1}$, the following holds for every large enough κ:*

$$\alpha(\kappa) \leq \frac{\Pr[\mathsf{A}(1^\kappa, (X_\kappa)_{-i}) = (X_\kappa)_i \mid X_{-i} = x_{-i}]}{\Pr[\mathsf{A}(1^\kappa, (X_\kappa)_{-i}) = -(X_\kappa)_i \mid X_{-i} = x_{-i}]} \leq 1/\alpha(\kappa).$$

3.3 Algorithms

We consider both uniform and non-uniform algorithms (i.e., Turing machines). Let PPT stand for probabilistic polynomial time, and PPTM stand for PPT (uniform) algorithm. Oracle access to a deterministic algorithm, means access to its input/output function. When using oracle access to a randomized algorithm, the caller has to set random coins for the call. Oracle access to a distribution D is just an oracle access to a no-input randomized function, in which the output distributed according to D. A distribution ensemble $\mathcal{D} = \{D_n\}_{n \in \mathbb{N}}$ is called *efficiently samplable* if

there exists a PPTM A such that for every $n \in \mathbb{N}$, the output of $\mathsf{A}(1^n)$ is distributed according to D_n.

If the coins are not specified, it means that they are sampled uniformly at random. We denote an algorithm A with advice z, by A_z.

3.4 Two-Party Protocols

A two-party protocol $\Pi = (\mathsf{A}, \mathsf{B})$ is PPT if the running time of both parties is polynomial in their input length. We let $\Pi(x, y)(z)$ denote a random execution of Π on a common input z, and private inputs x, y. We assume without loss of generality that a protocol has a common output (part of its transcript).

Definition 3.3 ((α, γ)-Accurate protocol). *A two-party protocol Π with private inputs is (α, γ)-* accurate for the function f, *if for any inputs $x, y \in \{\text{-}1, 1\}^n$, $\Pr[|\mathrm{out}(T) - f(x, y)| \leq \alpha] \geq \gamma$, where T is the transcript of $\Pi(x, y)$ and $\mathrm{out}(T)$ is the designated common output.*

A two-party protocol Π that gets security parameter 1^κ as its common input is (α, γ)-accurate for f if $\Pi(\cdot, \cdot)(1^\kappa)$ is ($\alpha(\kappa), \gamma(\kappa)$)-accurate for f, for every $\kappa \in \mathbb{N}$.

Definition 3.4 (Oracle-aided protocols). *In a two-party protocol Π with oracle access to a* protocol Ψ, *denoted Π^Ψ, the parties make use of the next-message function of Ψ.[24] In a two-party protocol Π with oracle access to a* channel C_{XYT}, *denoted Π^C, the parties can jointly invoke C_{XYT} for several times. In each call, an independent triplet (x, y, t) is sampled according to C_{XYT}, one party gets x, the other gets y, and t is added to the transcript of the protocol.*

3.5 Differential Privacy

We use the following standard definition of (information theoretic) differential privacy, due to Dwork et al. [10]. For notational convenience, we focus on databases over $\{\text{-}1, 1\}$.

Definition 3.5 (Differentially private mechanisms). *A randomized function $f \colon \{\text{-}1, 1\}^n \mapsto \{0, 1\}^*$ is an n-size, (ε, δ)-differentially private mechanism (denoted (ε, δ)-DP) if for every neighboring $w, w' \in \{\text{-}1, 1\}^n$ and every function $g \colon \{0, 1\}^* \mapsto \{0, 1\}$, it holds that*

$$\Pr[g(f(w)) = 1] \leq \Pr\big[g(f(w')) = 1\big] \cdot e^\varepsilon + \delta.$$

If $\delta = 0$, we omit it from the notation.

The Laplace mechanism The most ubiquitous differential private mechanism is the so-called Laplace mechanism. For $\sigma \geq 0$, the *Laplace distribution with parameter σ, denoted* $\mathrm{Lap}(\sigma)$, is defined by the probability density function $p(z) = \frac{1}{2\sigma} \exp\left(-\frac{|z|}{\sigma}\right)$.

Fact 3.6. *Let $\varepsilon > 0$. If $X \leftarrow \mathrm{Lap}(1/\varepsilon)$ then for all $t > 0 \colon \quad \Pr[|X| > t/\varepsilon] \leq e^{-t}$.*

Definition 3.7 (Laplace mechanism for the inner-product functionality over $\{\text{-}1, 1\}^n \times \{\text{-}1, 1\}^n$). *For $\varepsilon > 0$, the mechanism IP_ε is defined by $\mathrm{IP}_\varepsilon(x, y) = \langle x, y \rangle + \lfloor w \rfloor$, where $w \leftarrow \mathrm{Lap}(2/\varepsilon)$.*

Theorem 3.8 ([10]). *For every $\varepsilon > 0$ it holds that IP_ε is ε-DP.[25]*

---

[24]The function that on a partial view of one of the parties, returns its next message.

[25]The original definition proposed by [10] did not round the value of the Laplace distribution. However, by the

3.5.1 Computational Differential Privacy

There are several ways for defining computational differential privacy (see Section 1.2). We use the most relaxed version due to Beimel et al. [2].

Definition 3.9 (Computational differentially private mechanisms)**.** *A randomized function ensemble* $f = \left\{ f_\kappa \colon \{\text{-}1,1\}^{n(\kappa)} \mapsto \{0,1\}^* \right\}$ *is an* n-size, (ε, δ)-computationally differentially private *(denoted* (ε, δ)-CDP*) if for every poly-size circuit family* $\{\mathsf{A}_\kappa\}_{\kappa \in \mathbb{N}}$*, the following holds for every large enough* κ *and every neighboring* $w, w' \in \{\text{-}1,1\}^{n(\kappa)}$*:*

$$\Pr[\mathsf{A}_\kappa(f_\kappa(w)) = 1] \leq \Pr\big[\mathsf{A}_\kappa(f_\kappa(w')) = 1\big] \cdot e^{\varepsilon(\kappa)} + \delta(\kappa).$$

If $\delta(\kappa) = \operatorname{neg}(\kappa)$*, we omit it from the notation.*

3.6 Channels

A channel is a distribution over triplets (X, Y, T), as defined below.

Definition 3.10 (Channels)**.** *A* channel C_{XYT} *of size* n *over alphabet* Σ *is a probability distribution over* $\Sigma^n \times \Sigma^n \times \{0,1\}^*$*. The ensemble* $C_{XYT} = \{C_{X_\kappa Y_\kappa T_\kappa}\}_{\kappa \in \mathbb{N}}$ *is an* n-size channel ensemble*, if for every* $\kappa \in \mathbb{N}$*,* $C_{X_\kappa Y_\kappa T_\kappa}$ *is an* $n(\kappa)$-size channel*. We denote a channel of size one by a* single-bit channel*.*

We refer to X *and* Y *as the* local outputs*, and to* T *as the* transcript*. A part of* T *is marked as the* designated (common) output*, denoted by* $\operatorname{out}(T)$*.*

Unless said otherwise, the channels we consider are over the alphabet $\Sigma = \{\text{-}1,1\}$. We naturally identify channels with the distribution that characterize their output.

Definition 3.11 (The channel of a protocol)**.** *For a no-input two-party protocol* $\Pi = (\mathsf{A}, \mathsf{B})$*, we associate the channel* C_Π*, defined by* $C_\Pi = C_{XYT}$*, where* X*,* Y *and* T *are the local output of* A*, the local output of* B *and the protocol's transcript (respectively), induced by the random execution of* Π*. The designated output of* C_Π *is set to the common output of* Π*, if such exists.*

For a two-party protocol Π *that gets a security parameter* 1^κ *as its (only, common) input, we associate the channel ensemble* $\left\{C_{\Pi(1^\kappa)}\right\}_{\kappa \in \mathbb{N}}$*.*

Definition 3.12 $((\alpha, \gamma)$-Accurate channel)**.** *Channel* C_{XYT} *is* (α, γ)-accurate *for the function* f*, if* $\Pr_{C_{XYT}}[|\operatorname{out}(T) - f(X,Y)| \leq \alpha] \geq \gamma$*. Channel ensemble* $C_{XYT} = \{C_{X_\kappa Y_\kappa T_\kappa}\}_{\kappa \in \mathbb{N}}$ *is* (α, γ)-accurate *for* f *if* $C_{X_\kappa Y_\kappa T_\kappa}$ *is* $(\alpha(\kappa), \gamma(\kappa))$-accurate *for* f*, for every* $\kappa \in \mathbb{N}$*.*

3.6.1 Differentially Private Channels

Differentially private channels are naturally defined as follows:

Definition 3.13 (Differentially private channels)**.** *An* n-size channel C_{XYT} *is* (ε, δ)-differentially private *(denoted* (ε, δ)-DP*) if there exists a* $2n$-size (ε, δ)-DP *mechanism* M *such that* $(X, Y, T) \equiv (X, Y, M(X, Y))$*.*

---

definition of differential privacy, any post-processing (function) applied on the output of the mechanism does not effect the DP property of the mechanism. Specifically, if f is an ε-DP mechanism, then for every function g, the mechanism $g(f(\cdot))$ is also ε-DP. Thus, by taking g to be the rounding function, $\mathrm{IP}_\varepsilon(x,y) = \lfloor \langle x,y \rangle + \gamma \rceil = \langle x,y \rangle + \lfloor \gamma \rceil$ is also ε-DP.

Definition 3.14 (Computational differentially private channels). *A channel ensemble $C_{XYT} = \{C_{X_\kappa Y_\kappa T_\kappa}\}_{\kappa \in \mathbb{N}}$ is (ε, δ)-computationally differentially private (denoted (ε, δ)-CDP) if there exists an (ε, δ)-CDP mechanism ensemble $M = \{M_\kappa\}_{\kappa \in \mathbb{N}}$ such that $(X_\kappa, Y_\kappa, T_\kappa) \equiv (X_\kappa, Y_\kappa, M_\kappa(X_\kappa, Y_\kappa))$ for every $\kappa \in \mathbb{N}$.*

We use the following properties of differentially private channels. We state the properties using efficient black-box reductions. Thus, they are applicable for both information-theoretic and computational differential privacy.

Composition.

Proposition 3.15 (Composition of differentially private channels.). *Let M_0 and M_1 be n-size mechanisms, and let $\widehat{M}$ be the mechanism by $\widehat{M}(w) := (M_0(w), M_1(w))$. If M_0 is ε_0-DP and M_1 is (ε_1, δ)-DP, then $\widehat{M}$ is $(\varepsilon_0 + \varepsilon_1, \delta)$-DP.*

Furthermore, the proof is black-box: there exists an oracle-aided poly-time algorithm $\widehat{f}$ such that for any algorithm f violating the $(\varepsilon_0 + \varepsilon_1, \delta)$-DP of $\widehat{M}$, there exists $a \in \{-1, 1\}^n$ such that either $\widehat{f}$, with advice a, violates the ε_0-DP of M_0, or it violates the (ε_1, δ)-DP of M_1.

Proof. Assume towards a contradiction that $\widehat{M}$ is not $(\varepsilon_0 + \varepsilon_1, \delta)$-DP. Then, by definition, there exists a function f, and neighboring $w, w' \in \{-1, 1\}^n$ such that,

$$\Pr\Big[f(\widehat{M}(w')) = 1\Big] > e^{\varepsilon_0 + \varepsilon_1} \cdot \Pr\Big[f(\widehat{M}(w)) = 1\Big] + \delta. \tag{29}$$

In the following, let $f_0(x) := f(M_0(w'), x)$ and $f_1(x) := f(x, M_1(w))$. Compute

$$\begin{aligned}
\Pr\Big[f(\widehat{M}(w')) = 1\Big] &= \Pr\big[f(M_0(w'), M_1(w')) = 1\big] \\
&= \Pr\big[f_0(M_1(w')) = 1\big] \\
&\leq e^{\varepsilon_1} \cdot \Pr[f_0(M_1(w)) = 1] + \delta \\
&= e^{\varepsilon_1} \cdot \Pr\big[f_1(M_0(w')) = 1\big] + \delta \\
&\leq e^{\varepsilon_0 + \varepsilon_1} \cdot \Pr[f_1(M_0(w)) = 1] + \delta \\
&= e^{\varepsilon_0 + \varepsilon_1} \cdot \Pr\Big[f(\widehat{M}(w)) = 1\Big] + \delta,
\end{aligned}$$

in contradiction to Equation (29). The two inequalities follow from the DP property of M_0 and M_1. Thus we get a contradiction. The black-box property holds by considering $\widehat{f}$ to be either f_0 (with advice w') or f_1 (with advice w). $\qquad\square$

Composing SV source with DP mechanism.

Proposition 3.16. *There exists a poly-time oracle-aided algorithm A such that the following holds. Let X be $e^{-\varepsilon_1}$-strong-SV source over $\{-1, 1\}^n$, let M be a (ε_2, δ)-DP mechanism, let $\varepsilon := \varepsilon_1 + \varepsilon_2$, and let D be an algorithm such that*

$$\Pr[\mathsf{D}(i, X, \mathsf{M}(X)) = 1] > e^\varepsilon \cdot \Pr[\mathsf{D}(i, X_{<i>}, \mathsf{M}(X)) = 1] + \delta.$$

Then there exists $z \in [n] \times \{-1, 1\}^n$, such that A^D with advice z, violates the (ε_2, δ)-DP of M.

Proof. Since X is strong-SV, for every $x \in \{-1, 1\}^n$ it holds that $\Pr[X = x] \leq e^{\varepsilon_1} \cdot \Pr[X_{<i>} = x]$. It follows that

$$
\begin{aligned}
\Pr[\mathsf{D}(i, X, \mathsf{M}(X_{<i>})) = 1] &= \Pr_{z \leftarrow X}[\mathsf{D}(i, z, \mathsf{M}(z_{<i>})) = 1] \\
&\leq e^{\varepsilon_1} \cdot \Pr_{z \leftarrow X_{<i>}}[\Pr[\mathsf{D}(i, z, \mathsf{M}(z_{<i>})) = 1]] \\
&= e^{\varepsilon_1} \cdot \Pr[\mathsf{D}(i, X_{<i>}, \mathsf{M}(X)) = 1].
\end{aligned}
$$

By combining it with the assumption on D, we obtain that

$$
\begin{aligned}
\Pr_{i \leftarrow [n]}[\mathsf{D}(i, X, \mathsf{M}(X)) = 1] &> e^{\varepsilon} \cdot \Pr[\mathsf{D}(i, X_{<i>}, \mathsf{M}(X)) = 1] + \delta \\
&\geq e^{\varepsilon_2} \cdot \Pr_{i \leftarrow [n]}[\mathsf{D}(i, X, \mathsf{M}(X_{<i>})) = 1] + \delta
\end{aligned}
$$

By an averaging argument, there exists $x \in \{-1, 1\}^n$ and $i \in [n]$ such that

$$
\Pr[\mathsf{D}(i, x, \mathsf{M}(x)) = 1] > e^{\varepsilon_2} \cdot \Pr[\mathsf{D}(i, x, \mathsf{M}(x_{<i>})) = 1] + \delta.
$$

Let A^D be the algorithm that given advice $z \in [n] \times \{-1, 1\}^n$ and input w, outputs $\mathsf{D}(z, w)$. It follows that A with advice (i, x) violates the (ε_2, δ)-DP of M, with respect to the neighboring $x, x_{<i>} \in \{-1, 1\}^n$. $\qquad\square$

3.7 Two-Party Differential Privacy

In this section we formally define distributed differential privacy mechanism (i.e., protocols).

Definition 3.17. *A two-party protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ *is* (ε, δ)-differentially private, *denoted* (ε, δ)-DP, *if the following holds for every algorithm* D*: let* $V^\mathsf{P}(x, y)(\kappa)$ *be the view of party* P *in a random execution of* $\Pi(x, y)(1^\kappa)$*. Then for every* $\kappa, n \in \mathbb{N}$*,* $x \in \{-1, 1\}^n$ *and neighboring* $y, y' \in \{-1, 1\}^n$*:*

$$
\Pr\Big[\mathsf{D}(V^\mathsf{A}(x, y)(\kappa)) = 1\Big] \leq \Pr\Big[\mathsf{D}(V^\mathsf{A}(x, y')(\kappa)) = 1\Big] \cdot e^{\varepsilon(\kappa)} + \delta(\kappa),
$$

and for every $y \in \{-1, 1\}^n$ *and neighboring* $x, x' \in \{-1, 1\}^n$*:*

$$
\Pr\Big[\mathsf{D}(V^\mathsf{B}(x, y)(\kappa)) = 1\Big] \leq \Pr\Big[\mathsf{D}(V^\mathsf{B}(x', y)(\kappa)) = 1\Big] \cdot e^{\varepsilon(\kappa)} + \delta(\kappa).
$$

Protocol Π *is* (ε, δ)-DP against external observer *if we limit the above* D *to see only the protocol transcript.*

Protocol Π *is* (ε, δ)-computational differentially private, *denoted* (ε, δ)-CDP, *if the above inequalities only hold for a non-uniform* PPT D *and large enough* κ*. We omit* $\delta = \mathrm{neg}(\kappa)$ *from the notation.*

Remark 3.18 (Comparison with simulation-based definition of computational differential privacy)**.** *An alternative stronger definition of computational differently privacy, known as simulation based computational differential privacy, stipulates that the distribution of each party's view is computationally indistinguishable from a distribution that preserves privacy in an information-theoretic setup. Definition 3.17 is* weaker *than the above, and thus proving lower bound on a protocol that achieves this weaker guarantee (as we do in this work) is a stronger bound.*

The randomized response protocol for IP. The randomized response method of [36] can be used in order to construct a protocol for the inner-product. This protocol achieves ε-DP and $(c_\varepsilon \sqrt{n}, 1/2)$-accuracy, for every $\varepsilon > 0$ and some constant c_ε (dependent on ε)[28].

Protocol 3.19 $(\Pi = (\mathsf{A}, \mathsf{B}))$.

Parameter: n, ε.

A*'s private input:* $x \leftarrow \{\text{-}1, 1\}^n$

B*'s private input:* $y \leftarrow \{\text{-}1, 1\}^n$

Operation:

1. *Let* $p := \frac{e^\epsilon}{e^\epsilon + 1} - \frac{1}{2}$. A *samples* $\hat{x}$, *a noise verson of* x: *for every* $i \in [n]$, A *sets* $\hat{x}_i$ *to be* x_i *with probability* $\frac{1}{2} + p$ *and* $-x_i$ *with probability* $\frac{1}{2} - p$, *independently.*

2. B *computes* $z := 1/(2p) \cdot \sum_{i=1}^{n} y_i \cdot \hat{x}_i + \mathrm{Lap}(1/(p \cdot \varepsilon))$ *and send* z *to* A.

3. *Both parties output* z.

Proposition 3.20. *Let* Π *be Protocol 3.19. For every* $\epsilon > 0$ *there exists a constant* c_ε *such that the following holds. For every* $n \in \mathbb{N}$, $\Pi_{n,\varepsilon}$ *is a* ε-DP *protocol with* $(c_\epsilon \sqrt{n}, 1/2)$-*accuracy for IP.*

3.8 Key Agreement

We start with defining the information-theoretic case.

Definition 3.21 (Key-agreement channel)**.** *The following properties are associate with a channel* $C = C_{XYT}$:

Agreement: C *has* α-agreement *if* $\Pr[X = Y] \geq \alpha$.

Leakage: C *has* δ-leakage *if* $\Pr[f(T) = X] \leq \delta$ for every *function (i.e., "eavesdropper")* f.

Equality-leakage: C *has* δ-equality-leakage *if* $\Pr[f(T) = X \mid X = Y] \leq \delta$ *for every function* f.

*A single-bit, α-agreement, δ-leakage channel is called an (α, δ)-*key agreement*. An α-agreement, δ-equality-leakage channel is called an (α, δ)-*key-agreement-with-equality-leakage*.*

Amplification. We use the following amplification result, implicit in [25], for key-agreement channels with equality-leakage.

Theorem 3.22 (Key-agreement amplification, implicit in [25])**.** *Let* $\alpha > \delta \in (0, 1]$ *be constants. There exists a* PPT, *oracle-aided, two-party protocol* Π *such that the following holds. Let* C *be a single-bit, (α, δ)-key-agreement with equality-leakage channel. Then the channel* $\widetilde{C}$ *induced by* $\Pi^C(1^\kappa)$ *is a single-bit, $(1 - 2^{-\kappa}, 1/2 + 2^{-\kappa})$-key agreement.*

Furthermore, the security proof is black-box: there exists an oracle-aided E *such that for every single-bit channel* C *with* δ-agreement, *and an algorithm* $\widetilde{\mathsf{E}}$ *violating the* $(1/2 + 2^{-\kappa} + \beta))$-leakage *of* $\widetilde{C}$ *for some* $\beta > 0$, *algorithm* $\mathsf{E}^{C,\widetilde{\mathsf{E}}}(\kappa, \beta)$ *runs in time* $\mathrm{poly}(\kappa, 1/\beta)$ *and violates the* δ-leakage *of* C.

Combiners. We use the following key-agreement "combiner".

Theorem 3.23 (Key-agreement combiner [23]). *There exists a* PPT*, oracle-aided, two-party protocol Π such that the following holds: let $\mathcal{C} = \{C_i\}_{i \in [\ell]}$ be a set of channels such that at least one of them is a single-bit $(3/4, 1/2 + \delta)$-key-agreement for some $\delta > 0$. Then the channel $\widetilde{C}$ induced by $\Pi^{\{C_i\}_{i \in [\ell]}}(1^\kappa, 1^\ell)$ is a single-bit $(1 - 2^{-\kappa}, 1/2 + \delta \cdot p(\kappa))$-key-agreement, for some universal $p \in \mathrm{poly}$.*

Furthermore, the security proof is black-box: there exists an oracle-aided PPT *E such that for every single-bit channel family $\mathcal{C} = \{C_i\}_{i \in [\ell]}$, every index $i \in [\ell]$ such that C_i has $3/4$-agreement, and every algorithm $\widetilde{\mathsf{E}}$ that violates the $(1/2 + \delta \cdot p(\kappa))$-security of $\widetilde{C}$, algorithm $\mathsf{E}^{\mathcal{C}, \widetilde{\mathsf{E}}}(1^\kappa, 1^\ell, i)$ violates the $(1/2 + \delta)$-security of C_i.*

3.8.1 Key-Agreement Protocols

We now define the computational notion for key-agreement protocols and channel ensembles.

Definition 3.24 (Computational key-agreement channels and protocols). *The following properties are associate with a channel ensemble $C = \{C_{X_\kappa Y_\kappa T_\kappa}\}_{\kappa \in \mathbb{N}}$*

Agreement: *C has α-*agreement *if $\Pr[X_\kappa = Y_\kappa] \geq \alpha(\kappa)$.*

Leakage: *C has δ-*leakage *$\Pr[\mathsf{F}(T_\kappa) = X_\kappa] \leq \delta(\kappa)$ for every* PPT *(i.e., "eavesdropper") F and a large enough $\kappa \in \mathbb{N}$.*

Equality-leakage: *C has δ-*equality-leakage *if $\Pr[f(T_\kappa) = X_\kappa \mid X_\kappa = Y_\kappa] \leq \delta(\kappa)$ for every* PPT *(i.e., "eavesdropper") F and a large enough $\kappa \in \mathbb{N}$.*

*A single-bit, α-agreement, δ-leakage channel is called an (α, δ)-*key *agreement. An α-agreement, δ-equality-leakage channel is called an (α, δ)-*key-agreement-with-equality-leakage*.*

*A two-party protocol $\Pi = (\mathsf{A}, \mathsf{B})$ is an (α, δ)-*key *agreement protocol, if its associate channel ensemble $\{C_{\Pi(1^\kappa)}\}_{\kappa \in \mathbb{N}}$ is an (α, δ)-key agreement channel ensemble.*

3.9 Basic Probability Bounds

Fact 3.25 (Hoeffding's Inequality). *Let $X_1, \ldots, X_n$ be independent random variables, each X_i is bounded by the interval $[a_i, b_i]$, and let $\bar{X} = \frac{1}{n} \cdot \sum_{i=1}^n X_i$. Then for every $t \geq 0$:*

$$\forall t \geq 0: \quad \Pr[\bar{X} - \mathrm{E}[\bar{X}] \geq t], \ \Pr[\bar{X} - \mathrm{E}[\bar{X}] \leq -t] \leq \exp\left(-\frac{2n^2 t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right)$$

The following propositions are proven in Appendices A.1.1 to A.1.3, respectively.

Proposition 3.26. *Let $n \in \mathbb{N}$ be larger than some universal constant, and let $X = |X_1 + \ldots + X_n|$, where the X_i's are i.i.d., each takes 1 w.p. $1/2$ and -1 otherwise. Then for event E, it holds that*

$$\Pr[E] \cdot \mathrm{E}[X \mid E] \leq 4\sqrt{n}$$

Proposition 3.27. *Let R be an uniform random variable over $\{0,1\}^n$, and E some event s.t. $\Pr_R[E] \geq 1/n$. Then for every $q > 0$ it holds that*

$$\Pr_{i \leftarrow [n]}\left[\exists b \in \{0,1\} \ s.t. \ \Pr_{R|_{R_i = b}}[E] \notin (1 \pm 2q) \cdot \Pr_R[E]\right] \leq \log n/(n \cdot q^2).$$

Proposition 3.28. *Let R be uniform random variable over $\{0,1\}^n$, and let I be uniform random variable over $\mathcal{I} \subseteq [n]$, independent of R. Then $SD(R|_{R_I = 1}, R|_{R_I = 0}) \leq 1/\sqrt{|\mathcal{I}|}$.*

21

4 Key Agreement from Differentially Private Inner Product

In this section we prove that differentially private protocols (and channels) that estimate the inner product "well", can be used to construct a key agreement protocol. We start, Section 4.1, with the information-theoretic case, in which the privacy holds information-theoretically (i.e., against unbounded observers). In Section 4.2, we extend the result to the computational case.

4.1 The Information-Theoretic Case

The starting point in the information-theoretic case is a differentially private channel (i.e., a triplet of random variables) that estimates the inner product well. For such channels, we prove the following result.

Theorem 4.1 (Key-agreement from differentially private channels estimating the inner product). *There exists an oracle-aided PPT protocol Λ and a universal constant $c > 0$ such that the following holds for every $\varepsilon_1, \varepsilon_2 > 0$: let C_{XYT} be an n-size, $(\varepsilon_1, 1/n^2)$-DP channel over $\{-1,1\}$, such that (X, Y) is an $e^{-\varepsilon_2}$-strong SV source over $\{-1,1\}^{2n}$, and let $\varepsilon := \varepsilon_1 + \varepsilon_2$. If C is an $(\mu, c \cdot e^{c \cdot \varepsilon} \cdot \mu/\sqrt{n})$-accurate channel for the inner-product functionality, for some $\mu \geq \log n$, then the channel induced by $\Lambda^C(1^\kappa)$ is $(1 - 2^{-\kappa}, 1/2 + 2^{-\kappa})$-key agreement.* [26] [27]

As mentioned in the introduction, Theorem 4.1 immediately yields that inner-product is a condenser for, independent, strong Santha-Vazirani sources.

Corollary 4.2 (Inner-product is a good condenser for strong SV sources, Corollary 1.4 restated). *There exist universal constants $c_1, c_2 > 0$ such that the following hold for every independent $e^{-\varepsilon}$-strong SV sources X and Y of size n.*

- $H_\infty(\langle X, Y \rangle) \geq \log(\sqrt{n}/e^{c_1 \varepsilon} c_1 \log n)$, *and*

- $H_\infty(\langle X, Y \rangle \bmod c_2 \sqrt{n}) \geq \log(\sqrt{n}/e^{c_1 \varepsilon} c_1 \log n)$.

Proof of Corollary 4.2. We only prove the second item (the proof of the first item follows by similar means). Let $\widetilde{\Pi}$ be the $1/2$-DP randomized-response protocol for the inner-product (Protocol 3.19) with accuracy $(c \cdot \sqrt{n}, 1/2)$ for some constants c, and assume towards contradiction that Corollary 4.2 does not hold. It follows that there exist two independent $e^{-\varepsilon}$-strong SV sources X and Y, and $z \in [[0, c\sqrt{n} - 1]]$, such that

$$\Pr\big[\langle X, Y \rangle \equiv z \bmod c\sqrt{n}\big] > e^{4\varepsilon} \cdot c' \cdot \log(n)/\sqrt{n} \tag{30}$$

Consider the following two-party protocol $\Pi = (A, B)$: A draws $x \leftarrow X$, B draws $y \leftarrow Y$, and the parties interact in $\widetilde{\Pi}(x, y)$ to get a common output $\widetilde{\text{out}}$. A then sends $s \leftarrow \{-1, 0, 1\}$ to B, and both parties output out $:= (\lfloor \widetilde{\text{out}}/c\sqrt{n} \rfloor + s)c\sqrt{n} + z$.

---

[26] Requiring that (X, Y) has "enough" of entropy is mandatory. For instance, perfectly accurate, perfect DP(i.e., $(0,0)$-DP) channels exist *unconditionally* for 0-entropy (i.e., fixed) (X, Y), or more generally, for X and Y that most of their coordinates are fixed.

[27] It seems provable that the $(\varepsilon_1, 1/n^2)$-DP can be improved to $(\varepsilon_1, O(1/n))$-DP. However, since it complicates the (already rather long) proof, we chose to prove the slightly weaker variant of this theorem, stated here.

Let $X, Y, S, \widetilde{\mathsf{Out}}$ and Out, be the values of $x, y, s, \widetilde{\mathsf{out}}$ and out, in a random execution of Π. It is not hard to verify that if $|\langle x, y\rangle - \widetilde{\mathsf{out}}| \leq c\sqrt{n}$, then $\lfloor \widetilde{\mathsf{out}}/c\sqrt{n} \rfloor = \lfloor \langle x, y\rangle/c\sqrt{n} \rfloor \pm 1$. Therefore, by the accuracy of $\widetilde{\Pi}$ (Proposition 3.20), for every x, y it holds that:

$$\Pr\left[\left\lceil \widetilde{\mathsf{Out}}/c\sqrt{n} \right\rceil + S = \lfloor \langle X, Y\rangle/c\sqrt{n} \rfloor \mid (X, Y) = (x, y)\right] \geq 1/6 \tag{31}$$

Note that for every x, y with $\langle x, y\rangle \equiv z \mod c\sqrt{n}$, it holds that $\langle x, y\rangle = \lfloor \langle x, y\rangle/c\sqrt{n} \rfloor \cdot c\sqrt{n} + z$. Hence, by Equations (30) and (31)

$$\Pr[\mathsf{Out} = \langle X, Y\rangle] \geq e^{4\varepsilon} \cdot c' \cdot \log(n)/6\sqrt{n}.$$

By definition, the channel C induced by Π is distributed according to $(X, Y, (\widetilde{T}, S))$, for $\widetilde{T}$ being the transcript of $\widetilde{\Pi}(X, Y)$. Since $\widetilde{\Pi}$ is $1/2$-DP, then so is C. Thus, by Theorem 4.1, assuming that the constant c' is large enough, there exists a channel C' that is $(1 - 2^{-\kappa}, 1/2 + 2^{-\kappa})$-key agreement. Such channels, however, do not exist unconditionally. $\qquad\square$

We prove Theorem 4.1 using the following transformation that utilizes a DP channel that estimates the inner-product functionality well, to create a key-agreement-with-equality-leakage protocol (over non-boolean domain).

Protocol 4.3 ($\Pi_{n,\ell}^C = (\mathsf{A}, \mathsf{B})$).

Oracle: n-size channel C_{XYT}.

Parameters: n, ℓ.

Operation:

1. *The parties (jointly) call the channel C_{XYT}.*

    Let x, y, and t, be the output of A and B, and the common transcript of this call, respectively.

2. *A samples $v \leftarrow [\ell]$ and $r \leftarrow \{-1, 1\}^n$, and sends (v, x_{r+}, r) to B.*

3. *B sends y_{r-} to A.*

4. *A sets $u_{\mathsf{A}} = \langle x_{r-}, y_{r-}\rangle$, and (locally) outputs $o_{\mathsf{A}} = \left\lfloor \frac{u_{\mathsf{A}} - v}{\ell} \right\rfloor \cdot \ell$.*

    B sets $u_{\mathsf{B}} = \mathsf{out}(t) - \langle x_{r+}, y_{r+}\rangle$, and (locally) outputs $o_{\mathsf{B}} = \left\lfloor \frac{u_{\mathsf{B}} - v}{\ell} \right\rfloor \cdot \ell$.

The following lemma, which is the main technical contribution of this section, states that for the right choice of parameters, the channel induced by Protocol 4.3 is a weak key agreement.

Lemma 4.4 (Main lemma, information theoretic case)**.** *There exists a constant $c > 0$ such that the following holds for every $\varepsilon_1, \varepsilon_2, \delta > 0$: let C_{XYT} be an n-size, $(\varepsilon_1, 1/n^2)$-DP channel over $\{-1, 1\}$, such that (X, Y) is $e^{-\varepsilon_2}$-strong SV over $\{-1, 1\}^{2n}$, and let $\varepsilon := \varepsilon_1 + \varepsilon_2$ and $\beta := c \cdot e^{c \cdot \varepsilon}$. If C_{XYT} is $(\mu, \beta \cdot \mu/\sqrt{n})$-accurate for the inner-product functionality, for some $\mu \geq \log n$, then there exists $\widehat{\ell} \geq \mu$ such that channel induced by $\Pi_{n, \widehat{\ell}}^C$ is a $(\alpha, \alpha/2^{15})$-key-agreement-with-equality-leakage, for $\alpha := (\beta \cdot \widehat{\ell})/(8\sqrt{n})$.*

Furthermore, the above is proved in a black-box way: *there exists an oracle-aided* PPT Dist *such that for any deterministic algorithm* E *that breaks the above stated equality-leakage of* $\Pi_{n,\widehat{\ell}}^C$, *there exists an advice string* $a \in \{\text{-}1,1\}^{3n}$ *such that* $\mathsf{Dist}^{C,\mathsf{E}}$, *with advice* a, *violates the* $(\varepsilon_1, 1/n^2)$-DP *property of* C.

We prove Lemma 4.4 below, but first use it for proving Theorem 4.1.

Proving Theorem 4.1. In addition to Lemma 4.4, we make use of the following key-agreement amplification theorem, proven in Section 7, that yields that for the correct value of $\widehat{\ell}$, the channel implied by $\Pi_{n,\widehat{\ell}}^C$ can be amplified into a full-fledged key agreement.

Theorem 4.5 (Key-agreement amplification). *There exists an oracle-aided two-party protocol* Φ *such that the following holds for every* $\alpha \in (0,1]$. *Let* C *be an* n-size, $(\alpha, \alpha/2^{15})$-key-agreement-with-equality-leakage channel. Then the channel $\widetilde{C}$ induced by $\Phi^C(\kappa, n, \alpha)$ is a single-bit, $(1 - 2^{-\kappa}, 1/2 + 2^{-\kappa})$-key agreement. The running time of $\Phi^C(\kappa, n, \alpha)$ is* $\text{poly}(\kappa, n, 1/\alpha)$.*

Furthermore, the security proof is black-box: there exists a PPT *oracle-aided* E *such that for every* n-size channel C with α-agreement, and every algorithm $\widetilde{\mathsf{E}}$ that violates the $(1/2 + 2^{-\kappa} + \beta)$-equality-leakage of $\widetilde{C}$, for some $\beta > 0$, algorithm $\mathsf{E}^{C,\widetilde{\mathsf{E}}}(\kappa, n, \alpha, \beta)$ violates the equality-leakage of C, and runs in time $\text{poly}(\kappa, n, 1/\alpha, 1/\beta)$*

Equipped with the above results, we are ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let Amp be the protocol guaranteed by Theorem 4.5. For $\ell \in [n]$, let $\widehat{C}_\ell$ be the channel induced by $\Pi_{n,\widehat{\ell}}^C$ (Protocol 4.3). Let c be the constant from Lemma 4.4, and let $\widetilde{C}_\ell$ be the channel induced by $\mathsf{Amp}^{\widehat{C}_\ell}(1^\kappa, \alpha_\ell)$ for $\alpha_\ell = (e^{c \cdot \varepsilon} \cdot c \cdot \ell)/(8\sqrt{n})$. By Lemma 4.4, there exists $\widehat{\ell} \in [n]$ such that $\widehat{C}_{\widehat{\ell}}$ is a $(\alpha_{\widehat{\ell}}, \alpha_{\widehat{\ell}}/2^{15})$-key-agreement-with-equality-leakage channel. Thus, Theorem 4.5 yields that $\widetilde{C}_{\widehat{\ell}}$ is a $(1 - 2^{-\kappa}, 1/2 + 2^{-\kappa})$-key-agreement channel. Using Theorem 3.23 to combine the channels $\left\{\widetilde{C}_\ell\right\}_{\ell \in [n]}$ into a single channel, yields the desired (full-fledged) key-agreement channel. □

The rest of this section is dedicated to proving Lemma 4.4.

Proving Lemma 4.4. In the following fix $\kappa \in \mathbb{N}$. For $\ell \in \mathbb{N}$, the following random variables are associated with a random execution of $\Pi_{n,\ell}^C(1^\kappa)$: let (X, Y, T) be the output of the call to C_{XYT} done by the parties, let R and V_ℓ be the value of r and v sent in the execution, let O_A and O_B, be the local outputs of A and B, respectively. Finally, let $\widehat{T}_\ell := (X_{R^+}, Y_{R^-}, T, R, V_\ell)$, and let $\widehat{C}_{O_\mathsf{A} O_\mathsf{B} \widehat{T}_\ell}$ denote the channel defined by the distribution of $(O_\mathsf{A}, O_\mathsf{B}, \widehat{T}_\ell)$. The proof of the lemma makes use of the main result of Section 5, stated below. (In the following recall that $z_{<i>} = (z_{<i}, -z_i, z_{>i})$, i.e., i^{th} bit is flipped.)

Theorem 4.6 (Estimation to Distinguishing). *There exist constants $c_1, c_2 > 0$ and a poly-time oracle-aided algorithm* Dist *such that the following holds: let $n \in \mathbb{N}$, $\varepsilon \geq 0$ and $\ell \geq \log n$, and let D be a distribution over $\{\text{-}1,1\}^n \times \{\text{-}1,1\}^n \times \Sigma^*$. Then for every function f such that*

$$\Pr_{\substack{(x,y,t) \leftarrow D \\ r \leftarrow \{\text{-}1,1\}^n}} [|f(r, x_{r^+}, y_{r^-}, t) - \langle x \cdot y, r \rangle| \leq \ell] \geq e^{c_1 \cdot \varepsilon} \cdot c_2 \cdot \ell/\sqrt{n},$$

it holds that

$$\Pr_{\substack{(x,y,t)\leftarrow D \\ i\leftarrow[2n]}}\left[\mathsf{Dist}^{D,f}(i,(x,y)_{<i>},t)=1\right] < e^{-\varepsilon}\cdot\Pr_{\substack{(x,y,t)\leftarrow D \\ i\leftarrow[2n]}}\left[\mathsf{Dist}^{D,f}(i,(x,y),t)=1\right]-1/n.$$

Informally, the existence of an adversary E that violates the equality-leakage of $\widehat{C}_{O_\mathsf{A}O_\mathsf{B}\widehat{T}_\ell}$ yields that there exists an algorithm f such that

$$\Pr\left[\left|f^\mathsf{E}(T,R)-\langle X\cdot Y,R\rangle\right|<3\ell \mid O_\mathsf{A}=O_\mathsf{B}\right] > e^{c_1\cdot\varepsilon}\cdot c_2\cdot\ell/\sqrt{n}.$$

Very superficially, the above should have allowed us to use Theorem 4.6 for violating the differential privacy of $D := (C \mid O_\mathsf{A} = O_\mathsf{B})$. The conditioning on the event $\{O_\mathsf{A} = O_\mathsf{B}\}$ in the definition of D, however, poses two problems: the first is that there is no guarantee that D is differentially private (even though C is), and thus the predictor guaranteed by Theorem 4.6 does not yield a contradiction. The second issue is that after the conditioning, the random variable R might no longer be uniform and independent of the other parts D (as required by Theorem 4.6). To overcome these challenges, we consider a *different* distribution that is (1) differentially private, and (2) we have a good inner-product estimator for (with independent and uniform R meeting the requirements in Theorem 4.6). See formal proof below.

Proof of Lemma 4.4. Let $\ell \geq \mu$ be such that there exists a (deterministic) adversary E that violates the equality-leakage of $\widehat{C}_{O_\mathsf{A}O_\mathsf{B}\widehat{T}_\ell}$. That is,

$$\Pr\left[\mathsf{E}(\widehat{T}_\ell)=O_\mathsf{A} \mid O_\mathsf{A}=O_\mathsf{B}\right] > \alpha/2^{15} = \frac{\beta\cdot\ell}{2^{18}\sqrt{n}} \tag{32}$$

Recall that $\widehat{T}_\ell = (X_{R^+}, Y_{R^-}, T, R, V_\ell)$. By the definition of $\Pi_{n,\ell}^C$, the event $\{O_\mathsf{A}=O_\mathsf{B}\}$ implies the designated output of the call to C is close to $\langle X, Y\rangle$. That is,

$$\{O_\mathsf{A}=O_\mathsf{B}\} \implies \{|\mathrm{out}(T)-\langle X,Y\rangle|<\ell\} \tag{33}$$

In addition, note that the event $\{|\mathrm{out}(T)-\langle X,Y\rangle|<\ell\}$ implies that $2\cdot(O_A+V_\ell)-\mathrm{out}(T)$ and $\langle X\cdot Y,R\rangle$ are at distance at most 3ℓ. Indeed,

$$
\begin{aligned}
|2\cdot(O_A+V_\ell)-\mathrm{out}(T)-\langle X\cdot Y,R\rangle| &= \left|2\cdot\left(\left\lfloor\frac{\langle X_{R^-},Y_{R^-}\rangle-V_\ell}{\ell}\right\rfloor\cdot\ell+V_\ell\right)-\mathrm{out}(T)-\langle X\cdot Y,R\rangle\right| \\
&\leq 2\ell+|2\cdot\langle X_{R^-},Y_{R^-}\rangle-\mathrm{out}(T)-\langle X\cdot Y,R\rangle| \\
&< 3\ell+|2\cdot\langle X_{R^-},Y_{R^-}\rangle-\langle X,Y\rangle-\langle X\cdot Y,R\rangle| \\
&= 3\ell.
\end{aligned}
$$

Therefore, by combining Equations (32) and (33), we obtain that $f^\mathsf{E}(\widehat{T}_\ell):=2(\mathsf{E}(\widehat{T}_\ell)+V_\ell)-\mathrm{out}(T)$ is an accurate estimation for $\langle X\cdot Y,R\rangle$. Specifically, for every such ℓ:

$$\Pr\left[\left|f^\mathsf{E}(\widehat{T}_\ell)-\langle X\cdot Y,R\rangle\right|<3\ell \mid O_\mathsf{A}=O_\mathsf{B}\right] > \frac{\beta\cdot\ell}{2^{18}\sqrt{n}} \tag{34}$$

Let $\mathrm{IP}_2(x,y) := \langle x,y\rangle+\lfloor w\rceil$ for $w \leftarrow \mathrm{Lap}(1)$, i.e., IP_2 is the Laplace mechanism defined at Theorem 3.8 and $\lfloor w\rceil$ being the rounding of w to its closes integer. Let Δ_{Lap} be the random variable, jointly distributed with $\widehat{C}$, defined by

$$\Delta_{\mathrm{Lap}} = |\mathrm{out}(T)-\mathrm{IP}_2(X,Y)| \tag{35}$$

We make use of the following key claim, proven below.

25

Claim 4.7. *There exists an integer $\widehat{\ell} \geq \mu$ and a constant $c > 0$ such that the following holds:*

1. $\Pr_{\widehat{C}_{O_\mathsf{A} O_\mathsf{B} \widehat{T}_{\widehat{\ell}}}}[O_\mathsf{A} = O_\mathsf{B}] \geq \beta \cdot \widehat{\ell}/8\sqrt{n}.$

2. For every function f such that $\Pr\left[\left| f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R \rangle \right| < 3\widehat{\ell} \mid O_\mathsf{A} = O_\mathsf{B} \right] > \frac{\beta \cdot \widehat{\ell}}{2^{18} \cdot \sqrt{n}}$, it holds that $\Pr\left[\left| f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R \rangle \right| < 3\widehat{\ell} \mid \Delta_{\mathrm{Lap}} < \widehat{\ell} \right] > \frac{\beta \cdot \widehat{\ell}}{10 \cdot 2^{22} \cdot \sqrt{n}}.$

3. $\Pr\left[\Delta_{\mathrm{Lap}} < \widehat{\ell} \right] \geq 2/n.$

Let $\widehat{\ell} \in \mathbb{N}$ be value guaranteed by Claim 4.7. Claim 4.7(1) yields that the channel $\widehat{C}_{O_\mathsf{A} O_\mathsf{B} \widehat{T}_{\widehat{\ell}}}$ has $(\beta \cdot \widehat{\ell}/8\sqrt{n})$-agreement. By Equation (34) and Claim 4.7(2), it holds that

$$\Pr\left[\left| f^\mathsf{E}(\widehat{T}_{\widehat{\ell}}) - \langle X \cdot Y, R \rangle \right| < 3\widehat{\ell} \mid \Delta_{\mathrm{Lap}} < \widehat{\ell} \right] > \frac{\beta \cdot \widehat{\ell}}{10 \cdot 2^{22} \cdot \sqrt{n}} \tag{36}$$

Consider the function $g = g^{f^\mathsf{E}}$ that on input (r, x_{r+}, y_{r-}, t): (1) samples $v \leftarrow [\widehat{\ell}]$, and (2) outputs $f^\mathsf{E}(x_{r+}, y_{r-}, t, r, v)$. Since conditioned on $\left\{ \Delta_{\mathrm{Lap}} < \widehat{\ell} \right\}$ the value of both R and V in $\widehat{T}_{\widehat{\ell}}$ are uniform and independent of all other parts of the transcript, Equation (36) yields that

$$\Pr_{r \leftarrow \{-1,1\}^n}\left[|g(r, X_{r+}, Y_{r-}, T) - \langle X \cdot Y, r \rangle| \leq 3\widehat{\ell} \mid \Delta_{\mathrm{Lap}} < \widehat{\ell} \right] > \frac{\beta \cdot \widehat{\ell}}{10 \cdot 2^{22} \cdot \sqrt{n}} \tag{37}$$

Let C_{Lap} be the channel $(X, Y, (T, P := \mathrm{IP}_2(X, Y)))$ and let D be the distribution $(C_{\mathrm{Lap}} \mid \Delta_{\mathrm{Lap}} < \widehat{\ell})$. Equation (37) yields that

$$\Pr_{\substack{(x,y,(t,p)) \leftarrow D \\ r \leftarrow \{-1,1\}^n}}\left[|g(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle| \leq 3\widehat{\ell} \right] > \frac{\beta \cdot \widehat{\ell}}{10 \cdot 2^{22} \cdot \sqrt{n}} \tag{38}$$

Hence, there exists a fixed value of $v \in [\widehat{\ell}]$ such that above holds with respect to g_v, the variant of g with v hardwired. Recall that $\beta = e^{c \cdot \varepsilon} \cdot c$. Taking $c \geq 3 \cdot e^{2 \cdot c_1} \cdot c_2 \cdot 10 \cdot 2^{22}$, yields that

$$\Pr_{\substack{(x,y,(t,p)) \leftarrow D \\ r \leftarrow \{-1,1\}^n}}\left[|g_v(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle| \leq 3\widehat{\ell} \right] > e^{c_1 \cdot (\varepsilon + 2)} \cdot c_2 \cdot (3\widehat{\ell})/\sqrt{n}.$$

Thus by Theorem 4.6, it holds that

$$\Pr_{\substack{(x,y,(t,p)) \leftarrow D \\ i \leftarrow [2n]}}\left[\mathsf{Dist}^{D, g_v}(i, (x,y)_{<i>}, t) = 1 \right] < e^{-(\varepsilon + 2)} \cdot \Pr_{\substack{(x,y,(t,p)) \leftarrow D \\ i \leftarrow [2n]}}\left[\mathsf{Dist}^{D, g_v}(i, (x,y), t) = 1 \right] - 1/n \tag{39}$$

for Dist being the poly-time algorithm guaranteed by Theorem 4.6. Let $\widetilde{\mathsf{Dist}}$ be the poly-time algorithm that given $(x, y, (t, p))$, outputs $\mathsf{Dist}(x, y, t)$ if $|p - \mathrm{out}(t)| < \widehat{\ell}$, and abort otherwise.

Claim 4.7(3 yields that $\widetilde{\mathsf{Dist}}$ does not abort with probability at least $2/n$. Furthermore, since the decision of $\widetilde{\mathsf{Dist}}$ whether to abort or not is a function of the transcript (t, p), it holds that

$$\Pr_{\substack{(x,y,(t,p))\leftarrow C_{\mathrm{Lap}} \\ i\leftarrow[2n]}} \left[\widetilde{\mathsf{Dist}}^{D,g_v}(i, (x,y)_{<i>}, (t,p)) = 1 \right] \tag{40}$$

$$< e^{-(\varepsilon+2)} \cdot \Pr_{\substack{(x,y,(t,p))\leftarrow C_{\mathrm{Lap}} \\ i\leftarrow[2n]}} \left[\widetilde{\mathsf{Dist}}^{D,g_v}(i, (x,y), (t,p)) = 1 \right] - 2/n^2.$$

Recall that $\varepsilon = \varepsilon_1 + \varepsilon_2$ and that (X, Y) is a strong $e^{-\varepsilon_2}$-SV source. Thus by combining Equation (40) and Proposition 3.16, we deduce that C_{Lap} is *not* $(\varepsilon_1 + 2, 1/n^2)$-DP. Specifically, there exists an advise $z = (i, (x, y)) \in [n] \times \{-1, 1\}^{2n}$ such that the oracle-aided algorithm $\mathsf{Dist}_z(t) := \widetilde{\mathsf{Dist}}^{D,g_v}(z, t)$ violates the $(\varepsilon_1 + 2, 1/n^2)$-DP of C_{Lap}.

By Claim 4.7(3), oracle access to C_{Lap} suffices for efficiently emulating (with negligible probability of failure) the distribution D. Hence, there exits a deterministic, poly-time algorithm, that uses only oracle access to C_{Lap} and g_v, for violating the $(\varepsilon_1 + 2, 1/n^2)$-DP of C_{Lap}.

Finally, since IP_2 is a 2-DP mechanism (see Theorem 3.8), by differential privacy composition (see Proposition 3.15) there exists a distinguisher with an advise $a \in \{-1, 1\}^n$ and an oracle access to C and Dist_z, that violates the $(\varepsilon_1, 1/n^2)$-DP of the (original) channel C. Putting it all together, we get an oracle-aided PPT that given oracle access to C and E, and the advice $(z, v, a) \in \{-1, 1\}^{3n}$, violates the $(\varepsilon_1, 1/n^2)$-DP of the channel C.

$\square$

4.1.1 Proving Claim 4.7

Let $\Delta := |\mathrm{out}(T) - \langle X, Y \rangle|$, let $\mathcal{A} := \left\{ a \in [n] : \Pr[\Delta < a] \geq \frac{a \cdot \beta}{\sqrt{n}} \right\}$, and let $a_{\max} := \max(\mathcal{A}) \leq \sqrt{n}$. We prove that Claim 4.7 holds for the choice:

$$\widehat{\ell} = 2 \cdot a_{\max} \tag{41}$$

Since, by the accuracy of the channel, it holds that $\mu \in \mathcal{A}$, we deduce that $\widehat{\ell} \geq \mu$.

We will make use of the following claims:

Claim 4.8. $\Pr[O_{\mathsf{A}} = O_{\mathsf{B}}] \geq \frac{1}{4} \cdot \Pr\left[\Delta < \widehat{\ell}\right]$.

Claim 4.9. *Let f be a function such that* $\Pr\left[\left|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R \rangle\right| < 3\widehat{\ell} \mid O_{\mathsf{A}} = O_{\mathsf{B}}\right] > \frac{\beta \cdot \widehat{\ell}}{2^{18} \cdot \sqrt{n}}$. *Then* $\Pr\left[\left|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R \rangle\right| < 3\widehat{\ell} \mid \Delta < \widehat{\ell}\right] > \frac{\beta \cdot \widehat{\ell}}{2^{20} \cdot \sqrt{n}}$.

Claim 4.10. $\frac{\Pr[\Delta < \widehat{\ell}]}{\Pr[\Delta_{\mathrm{Lap}} < \widehat{\ell}]} \geq 1/5$.

The proof Claims 4.8 to 4.10 is given below, but first we will use the above claims to prove Claim 4.7.

Proof of Claim 4.7. Since $\widehat{\ell} = 2 \cdot a_{\max}$, it holds that

$$\Pr\left[\Delta < \widehat{\ell}\right] \geq \Pr[\Delta < a_{\max}] \geq \frac{a_{\max} \cdot \beta}{\sqrt{n}} \geq \frac{\widehat{\ell} \cdot \beta}{2 \cdot \sqrt{n}} \tag{42}$$

Thus, by Equation (42) and Claim 4.8, we prove Item 1 in the claim statement. Recall that $\Delta = |\text{out}(T) - \langle X, Y \rangle|$ and that $\Delta_{\text{Lap}} = |\text{out}(T) - \langle X, Y \rangle - \Gamma|$, where $\Gamma = \lfloor W \rceil$ and W is sampled from $\text{Lap}(1)$. Note that

$$(\Delta_{\text{Lap}} | \{\Gamma = 0\}) \equiv \Delta \tag{43}$$

In addition, the definition of $\text{Lap}(1)$ readily yields that

$$\Pr[\Gamma = 0] = \Pr\left[|W| \leq \tfrac{1}{2}\right] \geq 1 - e^{-1/2} > \tfrac{1}{2} \tag{44}$$

The second inequality holds by Fact 3.6. It follow that

$$\Pr\left[\Delta_{\text{Lap}} < \widehat{\ell}\right] > \Pr\left[\Delta < \widehat{\ell} \mid \Gamma = 0\right] \cdot \Pr[\Gamma = 0] > \frac{a_{\max} \cdot \beta}{\sqrt{n}} \cdot \frac{1}{2} > \frac{2}{n},$$

which satisfies Item 3 in the claim. Finally, compute

$$\Pr\left[\left|f(\widehat{T_{\widehat{\ell}}}) = \langle X \cdot Y, R \rangle\right| < 3\widehat{\ell} \mid \Delta_{\text{Lap}} < \widehat{\ell}\right]$$

$$> \Pr\left[\left|f(\widehat{T_{\widehat{\ell}}}) = \langle X \cdot Y, R \rangle\right| < 3\widehat{\ell} \mid \Delta_{\text{Lap}} < \widehat{\ell}, \Gamma = 0\right] \cdot \Pr\left[\Gamma = 0 \mid \Delta_{\text{Lap}} < \widehat{\ell}\right]$$

$$= \Pr\left[\left|f(\widehat{T_{\widehat{\ell}}}) = \langle X \cdot Y, R \rangle\right| < 3\widehat{\ell} \mid \Delta < \widehat{\ell}\right] \cdot \frac{\Pr\left[\Delta_{\text{Lap}} < \widehat{\ell} \mid \Gamma = 0\right]\Pr[\Gamma = 0]}{\Pr\left[\Delta_{\text{Lap}} < \widehat{\ell}\right]}$$

$$= \Pr\left[\left|f(\widehat{T_{\widehat{\ell}}}) = \langle X \cdot Y, R \rangle\right| < 3\widehat{\ell} \mid \Delta < \widehat{\ell}\right] \cdot \frac{\Pr\left[\Delta < \widehat{\ell}\right]\Pr[\Gamma = 0]}{\Pr\left[\Delta_{\text{Lap}} < \widehat{\ell}\right]}$$

$$> \Pr\left[\left|f(\widehat{T_{\widehat{\ell}}}) = \langle X \cdot Y, R \rangle\right| < 3\widehat{\ell} \mid \Delta < \widehat{\ell}\right] \cdot \frac{1}{10}.$$

The first and third equalities follow from Equation (43) and the fact that the event $\{\Gamma = 0\}$ is independent from X, Y and $\widehat{T_{\widehat{\ell}}}$. The last inequality holds by Claim 4.10 and Equation (44). Combing the above inequality with Claim 4.9, proves Item 2 in Claim 4.7. $\qquad \square$

The remainder of this section is dedicated to proving Claims 4.8 to 4.10. We start by proving Claim 4.10.

Proving Claim 4.10.

Proof of Claim 4.10. Recall that $\Delta = |\text{out}(T) - \langle X, Y \rangle|$ and that $\Delta_{\text{Lap}} = |\text{out}(T) - \langle X, Y \rangle - \Gamma|$, where $\Gamma = \lfloor W \rceil$ and W is sampled from $\text{Lap}(1)$. It holds that

$$\Pr\left[\Delta_{\text{Lap}} < \widehat{\ell}\right] = \Pr\left[\Delta_{\text{Lap}} < \widehat{\ell}, \Delta < 2 \cdot \widehat{\ell}\right] + \Pr\left[\Delta_{\text{Lap}} < \widehat{\ell}, \Delta \geq 2 \cdot \widehat{\ell}\right] \tag{45}$$

$$\leq \Pr\left[\Delta < 2 \cdot \widehat{\ell}\right] + \Pr\left[|\Gamma| > \widehat{\ell}\right].$$

The inequality follows since the event $\left\{\Delta_{\text{Lap}} < \widehat{\ell}, \Delta \geq 2 \cdot \widehat{\ell}\right\}$ implies the event $\left\{|\Gamma| > \widehat{\ell}\right\}$. Since $\widehat{\ell} \geq \mu \geq \log(n)$, we deduce by Fact 3.6 that

$$\Pr\left[|\Gamma| > \widehat{\ell}\right] = \Pr\left[|\text{Lap}(1)| > \widehat{\ell}\right] \leq \frac{1}{n} \tag{46}$$

On the other hand, since we set $\widehat{\ell} = 2\max\left\{a \in [n] \colon \Pr[\Delta < a] \geq \frac{a \cdot \beta}{\sqrt{n}}\right\}$, it holds that

$$4/n < \Pr\left[\Delta < 2 \cdot \widehat{\ell}\right] < 4 \cdot \Pr\left[\Delta < \widehat{\ell}/2\right] \tag{47}$$

Combining Equations (45) to (47), we conclude that

$$\frac{\Pr\left[\Delta < \widehat{\ell}\right]}{\Pr\left[\Delta_{\mathrm{Lap}} < \widehat{\ell}\right]} \geq \frac{\Pr\left[\Delta < \widehat{\ell}\right]}{\Pr\left[\Delta < 2 \cdot \widehat{\ell}\right] + \Pr\left[|\Gamma| > \widehat{\ell}\right]} \geq \frac{\Pr\left[\Delta < \widehat{\ell}/2\right]}{4 \cdot \Pr\left[\Delta < \widehat{\ell}/2\right] + 1/n} \geq \frac{1}{5}.$$

$\square$

Proving Claims 4.8 and 4.9. We make use of the following claim.

Claim 4.11. $\Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \mid \Delta < \widehat{\ell}/2\right] \geq 1/2.$

Proof of Claim 4.11. Let $\overline{\Delta} := \mathrm{out}(T) - \langle X, Y \rangle$ and note that $\Delta = \left|\overline{\Delta}\right|$. Let $Z = \langle X_{R^-}, Y_{R^-} \rangle - V$, by construction it holds that

$$O_{\mathsf{A}} = \left\lfloor \frac{Z}{\widehat{\ell}} \right\rfloor \cdot \widehat{\ell} \qquad \text{and} \qquad O_{\mathsf{B}} = \left\lfloor \frac{\overline{\Delta} + Z}{\widehat{\ell}} \right\rfloor \cdot \widehat{\ell}, \tag{48}$$

Let $Z_{\mathsf{mod}} := (Z \mod \widehat{\ell})$. Since V is uniform over $[\widehat{\ell}]$ and independent from X and Y, and since $\left|\mathbb{Z} \cap [0, \widehat{\ell}/2)\right| = \left|\mathbb{Z} \cap [\widehat{\ell}/2, \widehat{\ell})\right| = \widehat{\ell}/2$ (holds since $\widehat{\ell}/2$ is an integer), we deduce that

$$\Pr\left[Z_{\mathsf{mod}} < \widehat{\ell}/2\right] = \Pr\left[Z_{\mathsf{mod}} \geq \widehat{\ell}/2\right] = \tfrac{1}{2} \tag{49}$$

Moreover, if $Z_{\mathsf{mod}} < \widehat{\ell}/2$ and $0 \leq \overline{\Delta} < \widehat{\ell}/2$, then $\left\lfloor \frac{Z}{\widehat{\ell}} \right\rfloor = \left\lfloor \frac{\overline{\Delta} + Z}{\widehat{\ell}} \right\rfloor$ (and $O_{\mathsf{A}} = O_{\mathsf{B}}$). Thus,

$$\Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \mid 0 \leq \overline{\Delta} < \widehat{\ell}/2\right] \tag{50}$$
$$\geq \Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \mid 0 \leq \overline{\Delta} < \widehat{\ell}/2, Z_{\mathsf{mod}} < \widehat{\ell}/2\right] \cdot \Pr\left[Z_{\mathsf{mod}} < \widehat{\ell}/2 \mid 0 \leq \overline{\Delta} < \widehat{\ell}/2\right]$$
$$= 1 \cdot \Pr\left[Z_{\mathsf{mod}} < \widehat{\ell}/2 \mid 0 \leq \overline{\Delta} < \widehat{\ell}/2\right]$$
$$= \Pr\left[Z_{\mathsf{mod}} < \widehat{\ell}/2\right]$$
$$= 1/2.$$

The penultimate equation holds since V is uniform over $[\widehat{\ell}]$ and independent of $\overline{\Delta}$. A similar argument yields that

$$\Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \mid \widehat{\ell}/2 \leq \overline{\Delta} < 0\right] \tag{51}$$
$$\geq \Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \mid \widehat{\ell}/2 \leq \overline{\Delta} < 0, Z_{\mathsf{mod}} \geq \widehat{\ell}/2\right] \cdot \Pr\left[Z_{\mathsf{mod}} \geq \widehat{\ell}/2 \mid \widehat{\ell}/2 \leq \overline{\Delta} < 0\right]$$
$$\geq \Pr\left[Z_{\mathsf{mod}} \geq \widehat{\ell}/2\right] = 1/2.$$

29

Combining Equations (50) and (51), yields that

$$\Pr\Big[O_\mathsf{A} = O_\mathsf{B} \mid \Delta < \widehat{\ell}/2\Big] \geq \Pr\Big[O_\mathsf{A} = O_\mathsf{B} \mid 0 \leq \overline{\Delta} < \widehat{\ell}/2\Big] \cdot \Pr\Big[0 \leq \overline{\Delta} < \widehat{\ell}/2 \mid \Delta < \widehat{\ell}/2\Big]$$
$$+ \Pr\Big[O_\mathsf{A} = O_\mathsf{B} \mid \widehat{\ell}/2 \leq \overline{\Delta} < 0\Big] \cdot \Pr\Big[\widehat{\ell}/2 \leq \overline{\Delta} < 0 \mid \Delta < \widehat{\ell}/2\Big]$$
$$\geq 1/2,$$

which concludes the proof of Claim 4.11. □

Proving Claim 4.8.

Proof of Claim 4.8. Recall that by definition a_max is the largest element in the set $\mathcal{A} = \left\{a \in [n]\colon \Pr[\Delta < a] \geq \frac{a \cdot \beta}{\sqrt{n}}\right\}$ and that $\widehat{\ell} = 2 \cdot a_\mathrm{max}$. Thus,

$$\Pr\Big[\Delta < \widehat{\ell}/2 \mid \Delta < \widehat{\ell}\Big] = \Pr[\Delta < a_\mathrm{max} \mid \Delta < 2 \cdot a_\mathrm{max}] \tag{52}$$
$$= \frac{\Pr[\Delta < a_\mathrm{max}]}{\Pr[\Delta < 2 \cdot a_\mathrm{max}]}$$
$$> 1/2.$$

The inequality holds since otherwise, we have that $\Pr[\Delta < a_\mathrm{max}] \leq 2 \cdot \Pr[\Delta < 2 \cdot a_\mathrm{max}]$ which (since $a_\mathrm{max} \in \mathcal{A}$) implies that $\widehat{\ell} = 2 \cdot a_\mathrm{max} \in \mathcal{A}$, contradicting the maximality of a_max.

By Equation (52) and Claim 4.11, it follows that:

$$\Pr[O_\mathsf{A} = O_\mathsf{B}] = \Pr\Big[O_\mathsf{A} = O_\mathsf{B} \mid \Delta < \widehat{\ell}\Big] \cdot \Pr\Big[\Delta < \widehat{\ell}\Big]$$
$$\geq \Pr\Big[O_\mathsf{A} = O_\mathsf{B} \mid \Delta < \widehat{\ell}/2\Big] \cdot \Pr\Big[\Delta < \widehat{\ell}/2 \mid \Delta < \widehat{\ell}\Big] \cdot \Pr\Big[\Delta < \widehat{\ell}\Big]$$
$$\geq \frac{1}{4} \cdot \Pr\Big[\Delta < \widehat{\ell}\Big].$$

□

Proving Claim 4.9.

Proof of Claim 4.9. The claim immediately holds by observing that:

$$\Pr\Big[\Big|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R\rangle\Big| < 3\widehat{\ell} \mid O_\mathsf{A} = O_\mathsf{B}\Big] \tag{53}$$
$$= \frac{1}{\Pr[O_\mathsf{A} = O_\mathsf{B}]} \cdot \Pr\Big[\Big|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R\rangle\Big| < 3\widehat{\ell} \wedge (O_\mathsf{A} = O_\mathsf{B})\Big]$$
$$= \frac{1}{\Pr[O_\mathsf{A} = O_\mathsf{B}]} \cdot \Pr\Big[\Big|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R\rangle\Big| < 3\widehat{\ell} \wedge (O_\mathsf{A} = O_\mathsf{B}) \wedge (\Delta < \widehat{\ell})\Big]$$
$$\leq \frac{1}{\Pr[O_\mathsf{A} = O_\mathsf{B}]} \cdot \Pr\Big[\Big|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R\rangle\Big| < 3\widehat{\ell} \wedge (\Delta < \widehat{\ell})\Big]$$
$$= \frac{\Pr\Big[\Delta < \widehat{\ell}\Big]}{\Pr[O_\mathsf{A} = O_\mathsf{B}]} \cdot \Pr\Big[\Big|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R\rangle\Big| < 3\widehat{\ell} \mid \Delta < \widehat{\ell}\Big]$$
$$\leq 4 \cdot \Pr\Big[\Big|f(\widehat{T}_{\widehat{\ell}}) = \langle X \cdot Y, R\rangle\Big| < 3\widehat{\ell} \mid \Delta < \widehat{\ell}\Big]. \tag{54}$$

The second equality holds by Equation (33), and the last one by Claim 4.8. □

4.2 The Computational Case

In this section we state and prove our results for the computational case: CDP (computational differential private) protocols that estimate the inner product well. For such protocols, we prove the following result.

Theorem 4.12 (Key-agreement from differentially private channels estimating the inner product, the computational case, restatement of Theorem 1.3)**.** *There exists an oracle-aided protocol Λ and a universal constant $c > 0$, such that the following holds for every protocol Ψ that is ε-CDP against external observer. If Ψ is $(\mu(\kappa), e^{c \cdot \varepsilon(\kappa)} \cdot c \cdot \mu(\kappa)/\sqrt{n(\kappa)})$-accurate for the inner-product functionality on inputs of length n, for some $\mu(\kappa) \geq \log n(\kappa)$, then Λ^{Ψ} is a (full fledged) key-agreement protocol.* [28] [29]

Theorem 4.12 is an immediate corollary of the following key lemma. Let Amp be the key-agreement amplifier guaranteed by Theorem 4.5, and let Comb be the key-agreement combiner guaranteed by Theorem 3.23. To avoid notational cluttering, in the following we omit κ when clear from the context.

Lemma 4.13 (Main lemma, the computational case)**.** *There exists a constant $c > 0$ such that the following holds: let $C = \{C_\kappa\}_{\kappa \in \mathbb{N}}$ be an n-size, ε-CDP channel ensemble, that is $(\mu, e^{c \cdot \varepsilon} \cdot c \cdot \mu/\sqrt{n})$-accurate for the inner-product functionality, for some $\mu \geq \log n$, and let Π be according to Protocol 4.3. Let $\Gamma_{n,\ell} := \Pi_{n,\ell}^{C_\kappa}$, let $\Gamma_{n,\ell}^{\mathsf{Amp}} := \mathsf{Amp}^{\Gamma_{n,\ell}}(\kappa, n, \alpha(\ell))$, for $\alpha(\ell) := (\beta \cdot \ell)/(8\sqrt{n})$, and let $\Gamma^{\mathsf{Comb}} := \mathsf{Comb}^{\left\{\Gamma_{n,\ell}^{\mathsf{Amp}}\right\}_{\ell \in [n]}}(1^\kappa, 1^n)$. Then Γ^{Comb} is a key-agreement protocol.*

We prove Lemma 4.13 by using (the "information theoretic") Lemma 4.4 to show that for the right choice of ℓ, protocol $\Gamma_{n,\ell} = \Pi_{n,\ell}^{C_\kappa}$ is a weak key-agreement protocol, and hence, procedure Amp turns it into a full-fledged key agreement $\Gamma_{n,\ell}^{\mathsf{Amp}}$. It follows that applying the above procedure for all $\ell \in [n]$, yields the set of protocols $\left\{\Gamma_{n,\ell}^{\mathsf{Amp}}\right\}_{\ell \in [n]}$ that *contains* a key-agreement protocol. Applying Comb on this set, yields the desired key-agreement protocol Γ^{Comb}. Lemma 4.13 is formally proved below, but we first use it for proving Theorem 4.12.

Proving Theorem 4.12. For using Lemma 4.13, we first convert protocol Ψ into a (no private input) protocol such that the CDP-channel it induces, accurately estimate the inner-product functionality. Such a transformation is simply the following protocol that invokes Ψ over uniform inputs, and each party locally outputs its input.

---

[28]The theorem extends to $(\varepsilon(\kappa), 1/n(\kappa)^2)$-CDP channels.

[29]The theorem extends accurate on *average* protocols: i.e., the probability of inaccuracy is small over uniformly chosen inputs.

Protocol 4.14 $(\widehat{\Psi} = (\widehat{\mathsf{A}}, \widehat{\mathsf{B}}))$**.**

Common input: 1^κ.

Operation:

1. $\widehat{\mathsf{A}}$ *samples* $x \leftarrow \{\text{-}1, 1\}^{n(\kappa)}$ *and* $\widehat{\mathsf{B}}$ *samples* $y \leftarrow \{\text{-}1, 1\}^{n(\kappa)}$.

2. *The parties interact in a random execution protocol* $\Psi(1^\kappa)$, *with* $\widehat{\mathsf{A}}$ *playing the role of* A *with private input* x, *and* $\widehat{\mathsf{B}}$ *playing the role of* B *with private input* y.

3. $\widehat{\mathsf{A}}$ *locally outputs* x *and* $\widehat{\mathsf{B}}$ *locally outputs* y.

Let $\widehat{C}$ be the channel ensemble induced by $\widehat{\Psi}$, letting its designated output (the function out) be the designated output of the embedded execution of Ψ. The following fact is immediate by definition.

Proposition 4.15. *The channel ensemble* $\widehat{C}$ *is* (ε, δ)-CDP, *and has the same accuracy for computing the inner product as protocol* Ψ *has.*

Proof of Theorem 4.12. Immediate by Lemma 4.13 and Proposition 4.15 $\qquad\qquad\square$

4.2.1 Proving Lemma 4.13

Proof of Lemma 4.13. Assume towards a contradiction that there exits PPT E that for infinity often $\kappa \in \mathbb{N}$ breaks the security of $\Gamma^{\mathsf{Comb}}(1^\kappa, 1^n)$ with probability $1/p(\kappa)$, for some $p \in \mathrm{poly}$. Fix such $\kappa \in \mathbb{N}$ and omit it from notation when clear from the context. The proof follows by the following steps:

1. Recall that $\Gamma^{\mathsf{Comb}} = \mathsf{Comb}^{\left\{\Gamma_\ell^{\mathsf{Amp}}\right\}_{\ell \in [n]}}(1^n)$, and let $\widehat{\mathsf{E}}$ be the PPTM (i.e., black-box reduction) guaranteed by Theorem 3.23. By the contradiction assumption, for every $\ell \in [n]$, $\widehat{E}(\ell) := \widehat{\mathsf{E}}^{\mathsf{E}, \left\{\Gamma_\ell^{\mathsf{Amp}}\right\}_{\ell \in [n]}}(1^n, \ell)$ violates the $1/p'(\kappa)$-secrecy of $\Gamma_\ell^{\mathsf{Amp}}$, for some $p' \in \mathrm{poly}$.

2. Recall that $\Gamma_\ell^{\mathsf{Amp}} = \mathsf{Amp}^{\Gamma_{n,\ell}}(n, \alpha(\ell))$, and let $\widetilde{\mathsf{E}}$ be the algorithm guaranteed by Theorem 4.5. By the above, for every $\ell \in [n]$, $\widetilde{E}(\ell) := \widetilde{\mathsf{E}}^{\widehat{\mathsf{E}}(\ell), \Gamma_\ell}(1^\kappa, 1/2p'(\kappa))$ runs in polynomial time, and violates the $\alpha(\ell)$-secrecy of $\Gamma_{n,\ell}$, for $\alpha(\ell) := (2^{c \cdot \varepsilon(\kappa)} \cdot c' \cdot \ell)/(8\sqrt{n})/15$.

3. For each $\ell \in [n]$, use polynomial number of sampling to find, with save but negligible failure probability, a random string r_ℓ such that $\widetilde{E}(\ell; r_\ell)$ violates the $\alpha(\ell)$-secrecy of $\Gamma_{n,\ell}$. Let E^* be deterministic algorithm that on input ℓ acts like $\widetilde{E}(\ell; r_\ell)$.

4. By Lemma 4.4, recalling that $\Gamma_{n,\ell} = \Pi_{n,\ell}^{C_\kappa}$, there exists a PPTM $\mathsf{A}^{\mathsf{E}^*}$ such the the following holds: there exits $\widehat{\ell} \in [n]$ and (advise) $a_\kappa \in \{\text{-}1, 1\}^{2n}$ such that $\mathsf{A}^{\mathsf{E}^*}(1^\kappa, \widehat{\ell}, a_\kappa)$ violates the $(\varepsilon, 1/n^2)$-DP of C_κ.

Since we assumed (toward contradiction) that the above holds for infinitely many κ'n, the algorithm that for every $\kappa \in \mathbb{N}$, gets $(\widehat{\ell}, a_\kappa)$ as non-uniform advice and runs $\mathsf{A}^{\mathsf{E}^*}(1^\kappa, \widehat{\ell}, a_\kappa)$, violates the assume ε-CDP of the ensemble C. This concludes the proof. $\qquad\qquad\square$

5 Condensing Santa-Vazirani Source using Source-Dependent Seed

In this section, we prove Theorem 4.6, restated below. Recall that for a string $z \in \{-1, 1\}^{2n}$ and an index $i \in [2n]$, we denote $z_{<i>} := (z_1, \ldots, z_{i-1}, -z_i, z_{i+1}, \ldots, z_{2n})$.

Theorem 5.1 (Estimation to Distinguishing). *[Restatement of Theorem 4.6] There exist constants $c_1, c_2 > 0$ and a poly-time oracle-aided algorithm Dist such that the following holds: let $n \in \mathbb{N}$, $\varepsilon \geq 0$ and $\ell \geq \log n$, and let D be a distribution over $\{-1, 1\}^n \times \{-1, 1\}^n \times \Sigma^*$. Then for every function f such that*

$$\Pr_{\substack{(x,y,t) \leftarrow D \\ r \leftarrow \{-1,1\}^n}} [|f(r, x_{r^+}, y_{r^-}, t) - \langle x \cdot y, r \rangle| \leq \ell] \geq e^{c_1 \cdot \varepsilon} \cdot c_2 \cdot \ell / \sqrt{n},$$

it holds that

$$\Pr_{\substack{(x,y,t) \leftarrow D \\ i \leftarrow [2n]}} \left[\mathsf{Dist}^{D,f}(i, (x, y)_{<i>}, t) = 1 \right] < e^{-\varepsilon} \cdot \Pr_{\substack{(x,y,t) \leftarrow D \\ i \leftarrow [2n]}} \left[\mathsf{Dist}^{D,f}(i, (x, y), t) = 1 \right] - 1/n.$$

That is, given an oracle to a function f that estimates the inner product $\langle x \cdot y, r \rangle$ well, Dist distinguishes, for most i's, between (x, y) and its variant in which the ith bit is flipped. Theorem 5.1 immediately yields the following corollary, proven in Appendix A.2.1.

Corollary 5.2 (Restatement of Theorem 1.5). *Let $\mathsf{C} \colon (\{-1, 1\}^n)^3 \mapsto \mathbb{Z}$ be defined by $\mathsf{C}(x, y, r) := \langle x \cdot y, r \rangle$. Then for every $\varepsilon > 0$ and any $e^{-\varepsilon}$-strong SV source (X, Y) over $(\{-1, 1\}^n)^2$ and $R \leftarrow \{-1, 1\}^n$, it holds that for every $0 \leq \delta \leq 1$:*

$$\Pr_{(x,y,r) \leftarrow (X,Y,R)} \left[\mathrm{H}_\infty(\mathsf{C}(X, Y, R)|_{(R, X_{R^+}, Y_{R^-}) = (r, x_{r^+}, y_{r^-})}) \geq \log\left(\frac{\delta \sqrt{n}}{c_2 \cdot e^{c_1 \varepsilon} \cdot \log n} \right) \right] \geq 1 - \delta,$$

where c is the constant from Theorem 5.1. [30][31]

Namely, the inner product is a good strong seeded condenser for such SV source, even when significant seed related information (i.e., X_{R^+}, Y_{R^-}) is leaked. Since clearly $\mathrm{H}_\infty(\mathsf{C}(X, Y, R)) \leq \log \sqrt{n} + O(1)$, the above result is tight up to $c_1 \varepsilon + \log \log n$ additive term. The rest of this section is devoted for proving Theorem 5.1. The proof uses the following key lemma (which in turn proven using the main result of Section 6).

Lemma 5.3. *There exist PPT algorithms A_1, A_2 and A_3, and $n_0 \in \mathbb{N}$ such that the following holds for every $n \geq n_0$, $\ell \in \mathbb{N}$ and $\varepsilon \geq 0$: let Q be a distribution over $\{-1, 1\}^n \times \{-1, 1\}^n \times \Sigma^*$ and let f be a function such that for every $(x, y, t) \in \mathrm{Supp}(Q)$:*

$$\Pr_{r \leftarrow \{-1,1\}^n} [|f(r, x_{r^+}, y_{r^-}, t) - \langle x \cdot y, r \rangle| < \ell] \geq \frac{1024 \cdot e^\varepsilon \cdot \ell}{\sqrt{n}}.$$

Then $\exists \mathsf{A} \in \{\mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3\}$ such that

---

[30] A similar statement holds for $\mathsf{C}(x, y, r) := \langle x \cdot y, r \rangle \mod \sqrt{n} \cdot \log n$.

[31] Since the proof is by black-box reduction, it automatically applies to computational strong SV sources.

1. $\Pr_{(x,y,t)\leftarrow Q, i\leftarrow[2n]}\left[\mathsf{A}^f(i,(x,y),t,\ell)=1\right] \geq e^{-\varepsilon}/16$, and

2. $\Pr_{(x,y,t)\leftarrow Q, i\leftarrow[2n]}\left[\mathsf{A}^f(i,(x,y)_{<i>},t,\ell)=1\right] \leq 1/2 \cdot e^{-\varepsilon} \cdot \Pr_{(x,y,t)\leftarrow Q, i\leftarrow[2n]}\left[\mathsf{A}^f(i,(x,y),t,\ell)=1\right]$.

That is, Lemma 5.3 essentially proves Theorem 5.1 for a distribution Q for which f is a good estimator of $\langle x \cdot y, R \rangle$ for *all* $(x, y, t) \leftarrow Q$. We prove Lemma 5.3 below, and use it to prove Theorem 5.1 in Section 5.2.

5.1 Proving Lemma 5.3

We prove Lemma 5.3 using the following theorem, proved in Section 6.

Definition 5.4 (Inner-product estimator). *Let $n, \ell \in \mathbb{N}$, let $\lambda > 0$ and let $z \in \{-1,1\}^n$. A function $f\colon \{-1,1\}^n \mapsto \mathbb{Z}$ is an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$ if*

$$\Pr_{r\leftarrow\{-1,1\}^n}[|f(r) - \langle z, r \rangle| < \ell] \geq \frac{\lambda\ell}{\sqrt{n}} \ .$$

Theorem 5.5. *There exists a PPTM P such that the following holds for large enough $n \in \mathbb{N}$: let $z \in \{-1,1\}^n$, let $\lambda \geq 64$, and let f be an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$. Then with probability at least $(1 - \frac{4096}{\lambda^2})$ over $j \leftarrow [n]$, it holds that*

$$z_j \cdot \mathrm{E}_{r\leftarrow\{-1,1\}^n}[\mathsf{P}(j, z_{-j}, r, f(r), \ell)] \geq \frac{\lambda}{8n^{1.5}} \ ,$$

where the expectation is also over the randomness of P.

Let ℓ, ε, Q and f be as in Lemma 5.3, and let P be PPTM guaranteed in Theorem 5.5. The following algorithm reconstructs the jth bit of $(x \cdot y)$, for $(x, y, t) \leftarrow Q$, given only oracle access to the function:

$$\mathsf{G}_{x,y,t}(j,r) := \mathsf{P}(j, (x \cdot y)_{-j}, f(r, x_{r^+}, y_{r^-}, t), \ell). \tag{55}$$

Algorithm 5.6 (The reconstruction algorithm Rec).

Oracle: $\mathsf{G}_{x,y,t}$.

Input: $j \in [n]$.

Operation:

1. *Sample uniform* $(r_1, ..., r_{n^4}) \leftarrow (\{-1,1\}^n)^{n^4}$, *let* $\mathcal{R} := \{r_i\}_{i\in[n^4]}$.

2. *For every* $r \in \mathcal{R}$, *let* $g_{x,y,t}(j,r) = \mathsf{G}_{x,y,t}(j,r)$.

3. *Return* $\mathsf{sign}(\mathrm{E}_{r\leftarrow\mathcal{R}}[g_{x,y,t}(j,r)])$.

We next prove that Rec has good success probability in reconstructing $(x \cdot y)_j$, for $i \leftarrow [n]$ and $(x, y, t) \leftarrow Q$.

Claim 5.7. *For large enough $n \in \mathbb{N}$, it holds that*

$$\Pr_{(x,y,t)\leftarrow Q, j\leftarrow [n]}\left[\mathsf{Rec}^{\mathsf{G}_{x,y,t}}(j) = x_j \cdot y_j\right] \geq 1 - e^{-2\varepsilon}/16.$$

Proof. We assume without loss of generality that $\varepsilon \leq \log n$ (otherwise the claim follows trivially). The proof is immediate by the Hoffeding bound, Theorem 5.5 and the observation that $f_{x,y,t}(r) := f(r, x_{r^+}, y_{r^-}, t)$ is an $(1024 \cdot e^\varepsilon, \ell)$-estimator of $\langle x \cdot y, \cdot \rangle$. $\square$

The next claim essentially yields that Rec distinguishes between (x, y) and $(x, y)_{<i>}$, for some $i \in [2n]$.

Claim 5.8. *For every $n \in \mathbb{N}$, at least one of the following holds:*

1. $\Pr_{(x,y,t)\leftarrow Q, j\leftarrow [n]}\left[\mathsf{Rec}^{\mathsf{G}_{x,y,t}}(j) = x_j \cdot y_j\right] \leq 3/4.$

2. $\Pr_{(x,y,t)\leftarrow Q, j\leftarrow [n]}\left[\mathsf{Rec}^{\mathsf{G}_{x_{<j>},y,t}}(j) = -x_j \cdot y_j\right] \leq 3/4.$

3. $\Pr_{(x,y,t)\leftarrow Q, j\leftarrow [n]}\left[\mathsf{Rec}^{\mathsf{G}_{x,y_{<j>},t}}(j) = -x_j \cdot y_j\right] \leq 3/4.$

4. $\Pr_{(x,y,t)\leftarrow Q, j\leftarrow [n]}\left[\mathsf{Rec}^{\mathsf{G}_{x_{<j>},y_{<j>},t}}(j) = x_j \cdot y_j\right] \leq 3/4.$

Proof. By definition of G (see Equation (55)), for every r with $r_j = 1$, it holds that

$$\mathsf{G}_{x,y,t}(j,r) \equiv \mathsf{G}_{x,y_{<j>},t}(j,r), \quad \text{and} \quad \mathsf{G}_{x_{<j>},y,t}(j,r) \equiv \mathsf{G}_{x_{<j>},y_{<j>},t}(j,r) \tag{56}$$

Similarly, for every r with $r_j = -1$, it holds that

$$\mathsf{G}_{x,y,t}(j,r) \equiv \mathsf{G}_{x_{<j>},y,t}(j,r), \quad \text{and} \quad \mathsf{G}_{x,y_{<j>},t}(j,r) \equiv \mathsf{G}_{x_{<j>},y_{<j>},t}(j,r) \tag{57}$$

Fix $(x, y, t) \in \mathrm{Supp}(Q)$, $j \in [n]$, and the randomness of Rec (including the part uses in the call to G). We prove that for at least one of the possible assignments to $(u, v) \in \{(x,y), (x_{<j>},y), (x, y_{<j>}), (x_{<j>}, y_{<j>})\}$, algorithm $\mathsf{Rec}^{\mathsf{G}_{u,v,t}}(j)$ fails to output the value of $u_j \cdot v_j$.

Let $\mathcal{R}$ be the value sampled by $\mathsf{Rec}(j)$, and for a pair (u, v) and $r \in \mathcal{R}$, let $g_{u,v,t}(j, r)$ be the value set by $\mathsf{Rec}(j)$ (all values with respect to the above fixing). Note that for a pair (u, v), it holds that

$$\mathrm{E}_{r\leftarrow\mathcal{R}}[g_{u,v,t}(j,r)] \tag{58}$$
$$= \Pr_{r\leftarrow\mathcal{R}}[r_j = -1] \cdot \mathrm{E}_{r\leftarrow\mathcal{R}|_{r_j=-1}}[g_{u,v,t}(j,r)] + \Pr_{r\leftarrow\mathcal{R}}[r_j = 1] \cdot \mathrm{E}_{r\leftarrow\mathcal{R}|_{r_j=1}}[g_{u,v,t}(j,r)].$$

Let

$$\alpha_{j,\mathcal{X}}^{u,v} := \Pr_{r\leftarrow\mathcal{R}}[r_j = -1] \cdot \mathrm{E}_{r\leftarrow\{-1,1\}^n|_{r_j=-1}}[g_{u,v,t}(j,r)], \quad \text{and}$$
$$\alpha_{j,\mathcal{Y}}^{u,v} := \Pr_{r\leftarrow\mathcal{R}}[r_j = 1] \cdot \mathrm{E}_{r\leftarrow\{-1,1\}^n|_{r_j=1}}[g_{u,v,t}(j,r)].$$

Equation (56) yields that

$$\alpha_{j,\mathcal{Y}}^{x,y} = \alpha_{j,\mathcal{Y}}^{x,y_{<j>}}, \quad \text{and} \quad \alpha_{j,\mathcal{Y}}^{x_{<j>},y} = \alpha_{j,\mathcal{Y}}^{x_{<j>},y_{<j>}} \tag{59}$$

35

Similarly, Equation (57) yields that

$$\alpha_{j,\mathcal{X}}^{x,y} = \alpha_{j,\mathcal{X}}^{x_{<j>},y}, \quad \text{and} \quad \alpha_{j,\mathcal{X}}^{x,y_{<j>}} = \alpha_{j,\mathcal{X}}^{x_{<j>},y_{<j>}} \tag{60}$$

Combining the above two equations, we get that

$$(\alpha_{j,\mathcal{X}}^{x,y} + \alpha_{j,\mathcal{Y}}^{x,y}) + (\alpha_{j,\mathcal{X}}^{x_{<j>},y_{<j>}} + \alpha_{j,\mathcal{Y}}^{x_{<j>},y_{<j>}}) = (\alpha_{j,\mathcal{X}}^{x_{<j>},y} + \alpha_{j,\mathcal{Y}}^{x_{<j>},y}) + (\alpha_{j,\mathcal{X}}^{x,y_{<j>}} + \alpha_{j,\mathcal{Y}}^{x,y_{<j>}}) \tag{61}$$

By definition, $\mathsf{Rec}^{\mathsf{G}_{u,v}}(j)$ outputs 1 iff $\alpha_{j,\mathcal{X}}^{u,v} + \alpha_{j,\mathcal{Y}}^{u,v} \geq 0$. Assume towards a contradiction that, for the fixed randomness above, for every $(u,v) \in \{(x,y),(x_{<j>},y),(x,y_{<j>}),(x_{<j>},y_{<j>})\}$ it holds that $\mathsf{Rec}^{\mathsf{G}_{u,v}}(j) = u_j \cdot v_j$. Assume for simplicity that $x_j \cdot y_j = 1$ (the case $x_j \cdot y_j = -1$ is symmetric). It follows that $(\alpha_{j,\mathcal{X}}^{x,y} + \alpha_{j,\mathcal{Y}}^{x,y}) + (\alpha_{j,\mathcal{X}}^{x_{<j>},y^y} + \alpha_{j,\mathcal{Y}}^{x_{<j>},y_{<j>}}) \geq 0$ and $(\alpha_{j,\mathcal{X}}^{x_{<j>},y} + \alpha_{j,\mathcal{Y}}^{x_{<j>},y}) + (\alpha_{j,\mathcal{X}}^{x,y_{<j>}} + \alpha_{j,\mathcal{Y}}^{x,y_{<j>}}) < 0$, in contradiction to Equation (61).

Since for every fixing of (x,y,t), j, and its randomness, Rec errs on at least one of the cases appearing in the claim statements, we conclude that for (at least) one of the cases, it errs with probability at least $1/4$, over a random choice of (x,y,t), j and its random coins. $\qquad \square$

Equipped with the above claim, we prove Lemma 5.3 with respect to algorithms $\mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3$, defined below using the following algorithm.

Algorithm 5.9 (The algorithm A).

Oracle: f.

Input: $i \in [2n], (x,y) \in \{-1,1\}^n \times \{-1,1\}^n, t \in \Sigma^*, \ell \in [n], \mathcal{I} \subseteq [2n]$.

Operation: If $i \notin \mathcal{I}$, output 0. Otherwise,

1. *Let* $j = \begin{cases} i & i \leq n \\ i - n & i > n \end{cases}$.

2. *Emulate* $\mathsf{Rec}^{\mathsf{G}_{x,y,t}}(j)$, *for* $\mathsf{G}_{x,y,t} := \mathsf{P}(j, (x \cdot y)_{-j}, f(r, x_{r^+}, y_{r^-}, t), \ell)$. *Let d be its output.*

3. *If $d \neq x_j \cdot y_j$, output 1. Otherwise, output 0.*

Let $j(i) := i$ if $i \leq n$ and $i - n$ otherwise, and let

- $\mathsf{A}_1(i, (u,v), t, \ell) := A(i, (u,v)_{<i>}, t, \ell, [n])$,

- $\mathsf{A}_2(i, (u,v), t, \ell) := A(i, (u,v)_{<i>}, t, \ell, [2n] \setminus [n])$, and

- $\mathsf{A}_3(i, (u,v), t, \ell) := A(i, (u_{<j(i)>}, v_{<j(i)>}), t, \ell, [n])$.

Proof of Lemma 5.3. Let $n_0 \in \mathbb{N}$ be large enough for Theorem 5.5. Let $n \geq n_0$, and let Q, f, ε and ℓ be as in Lemma 5.3. Claim 5.7 yields that

$$\Pr_{(x,y,t) \leftarrow Q, j \leftarrow [n]} \left[\mathsf{Rec}^{\mathsf{G}_{x,y,t}}(j) = x_j \cdot y_j \right] \geq 1 - e^{-2\varepsilon}/16 > 3/4.$$

Thus, Claim 5.8 yields that (at least) one of the following holds:

1. $\Pr_{(x,y,t)\leftarrow Q,j\leftarrow[n]}\left[\mathsf{Rec}^{\mathsf{G}_{x<j>,y,t}}(j) = -x_j \cdot y_j\right] \leq 3/4.$

2. $\Pr_{(x,y,t)\leftarrow Q,j\leftarrow[n]}\left[\mathsf{Rec}^{\mathsf{G}_{x,y<j>,t}}(j) = -x_j \cdot y_j\right] \leq 3/4.$

3. $\Pr_{(x,y,t)\leftarrow Q,j\leftarrow[n]}\left[\mathsf{Rec}^{\mathsf{G}_{x<j>,y<j>,t}}(j) = x_j \cdot y_j\right] \leq 3/4.$

The proof continues by case analysis:

Case 1: $\Pr_{(x,y,t)\leftarrow Q,j\leftarrow[n]}\left[\mathsf{Rec}^{\mathsf{G}_{x<j>,y,t}}(j) = -x_j \cdot y_j\right] < 1 - e^{-\varepsilon}/8$. In this case A_1 fulfills the requirements of the lemma. Indeed,

$$\Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n],a\leftarrow\mathsf{A}_1^f(j,(x,y)_{<i>},t,\ell)}[a = 1] = \Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n]}\left[i \in [n] \wedge \mathsf{Rec}^{\mathsf{G}_{x,y,t}}(i) \neq x_i \cdot y_i\right]$$
$$\leq e^{-2\varepsilon}/32,$$

and similarly,

$$\Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n],a\leftarrow\mathsf{A}_1^f(i,(x,y),t,\ell)}[a = 1] = \Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n]}\left[i \in [n] \wedge \mathsf{Rec}^{\mathsf{G}_{(x,y)_{<i>},t}}(i) \neq -x_i \cdot y_i\right]$$
$$\geq e^{-\varepsilon}/16.$$

Case 2: $\Pr_{(x,y,t)\leftarrow Q,j\leftarrow[n]}\left[\mathsf{Rec}^{\mathsf{G}_{x,y<j>,t}}(j) = -x_j \cdot y_j\right] < 1 - e^{-\varepsilon}/8$. This case is analogous to the previous one, taking A_2 instead of A_1.

Case 3: $\Pr_{(x,y,t)\leftarrow Q,j\leftarrow[n]}\left[\mathsf{Rec}^{\mathsf{G}_{x<j>,y<j>,t}}(j) = x_j \cdot y_j\right] \leq 3/4$. We show that assuming case 1 does not hold, A_3 fulfills the requirements of the lemma. Indeed

$$\Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n],a\leftarrow\mathsf{A}_3^f(i,(x,y)_{<i>},t,\ell)}[a = 1] = \Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n]}\left[i \in [n] \wedge \mathsf{Rec}^{\mathsf{G}_{x,y<i>,t}}(i) \neq -x_i \cdot y_i\right]$$
$$\leq e^{-\varepsilon}/16,$$

and similarly

$$\Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n],a\leftarrow\mathsf{A}_3^f(i,(x,y),t,\ell)}[a = 1] = \Pr_{(x,y,t)\leftarrow Q,i\leftarrow[2n]}\left[i \in [n] \wedge \mathsf{Rec}^{\mathsf{G}_{x<i>,y<i>,t}}(i) \neq x_i \cdot y_i\right]$$
$$\geq 1/8.$$

$\square$

5.2 Proving Theorem 5.1

In this section we use Lemma 5.3 for proving Theorem 5.1. Throughout this section, let n, ε, ℓ, D and f be as in Theorem 5.1, let $\mathsf{A}_1, \mathsf{A}_2$ and A_3 be the algorithms guaranteed by Lemma 5.3, let n_0 be the constant guaranteed by Lemma 5.3, let $m := e^{2\varepsilon} \cdot 1000$, let $c := 2^{30} \cdot n_0$, let $c_1 := 10$ and let $c_2 := c^3$.

We prove that the following algorithm, for the right choice of parameters, fulfills the requirements of Theorem 5.1.

Algorithm 5.10 (The distinguisher Dist).

Oracle: f.

Parameters: $\widehat{\ell}, \widehat{v}, d \in \{1, 2, 3\}$.

Input: $i \in [2n]$, $(x', y') \in \{-1, 1\}^{2n}$ and $t \in \Sigma^*$.

Operation:

1. *Let $(j, b) := \begin{cases} (i, -1) & i \leq n \\ (i - n, 1) & i > n \end{cases}$.*

2. *Sample uniform $(r_1, \ldots, r_{n^5}) \leftarrow (\{-1, 1\}^n)^{n^5}$, conditioned on $(r_k)_j = b$ for every $k \in [n^5]$. Let $\mathcal{R} := \{r_k\}_{k \in [n^5]}$, and let $q := \Pr_{r \leftarrow \mathcal{R}}\left[\left|f(r, x'_{r+}, y'_{r-}, t) - \langle (x' \cdot y')_{-j}, r_{-j} \rangle\right| \leq \widehat{\ell}\right]$.*

3. *If $q \leq \widehat{v}$, abort.*
   Else, output $\mathsf{A}_d^f(i, (x', y'), t, \widehat{\ell} + 1)$.

Recall that, given Dist aims to distinguish between (x, y) and $(x, y)_{<i>}$ (in which the ith bit is flipped). Dist starts by trying to figure out whether f is a good estimator of $\langle x \cdot y, r \rangle$, for a random r. Since Dist does not know the right value of $(x, y)_i$, it invokes f only on inputs that do not contain the missing bit $(x, y)_i$. If Dist finds out that f is a good estimator, it uses A_d for telling whether $(x', y')_i = (x, y)_i$. It easily follows from Lemma 5.3 that if for every $s = (x, y, t)$, Dist could have computed the success of f on (truly) random r, which requires knowing $(x, y)_i$, that is to compute

$$p_{\widehat{\ell}}^s := \Pr_{r \leftarrow \{-1, 1\}^n}\left[\left|f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle\right| \leq \widehat{\ell}\right], \tag{62}$$

then, for the right choice of d, it would have fulfilled the requirement of Theorem 5.1. The crux of our proof is showing that, for most i's, the difference between $p_{\widehat{\ell}}^s$ and the computed q is unlikely to affect Dist's answer. We do the latter by considering a second distinguisher $\widetilde{\mathsf{Dist}}$, an idealized variant of Dist that (miraculously) manages to computes a value that is in a sense in-between the value q computed by Dist and the above $p_{\widehat{\ell}}^s$, and used that instead of the value of q. Note that the value of q can be written as

$$q = \Pr_{r \leftarrow \mathcal{R}}\left[\left|f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle - b \cdot x_j \cdot y_j\right| \leq \widehat{\ell}\right] \tag{63}$$

where j and b are the functions of i computed by Dist. Hereafter, we use $j(i)$ and $b(i)$ as the values of j and b (respectively) for a given input i (i.e., $j(i) := i$ and $b(i) := -1$ if $i \leq n$ or $i - n$ and 1 otherwise). Algorithm $\widetilde{\mathsf{Dist}}$ manages to computes the value

$$q_{\widehat{\ell}, i}^s := \Pr_{r \leftarrow \{-1, 1\}^n}\left[\left|f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle - b(i) \cdot x_{j(i)} \cdot y_{j(i)}\right| \leq \widehat{\ell}\right] \tag{64}$$

I.e., r is chosen uniformly, without the restriction that $r_j = b$. (Note that, without knowing $(x, y)_i$, Dist cannot calculate $q_{\widehat{\ell}, i}^s$.) We start, Section 5.2.1, by proving that $\widetilde{\mathsf{Dist}}$ is a good distinguisher, and in Section 5.2.2 extend the proof to the real distinguisher Dist.

5.2.1 Analyzing the Idealized Distinguisher

In this section, we prove that Theorem 5.1 holds with respect to the idealized algorithm $\widetilde{\mathsf{Dist}}$. We start by making two observation regarding the probabilities p_ℓ^s considered above (i.e., the probability that f estimates the inner product on s with error at most $\widehat{\ell}$). In the following, recall that $[[a, b]] := [a, b] \cap \mathbb{Z}$. The first claims states that p_ℓ^s is large with high probability over $s \leftarrow D$.

Claim 5.11. $\Pr_{s \leftarrow D}[p_\ell^s \geq e^{c_1 \varepsilon} \cdot c_2 \ell / 2\sqrt{n}] \geq e^{c_1 \varepsilon} \cdot c_2 \ell / 2\sqrt{n}$.

Proof of Claim 5.11. Recall that,

$$\mathrm{E}_{s \leftarrow D}[p_\ell^s] = \Pr_{s \leftarrow D, r \leftarrow \{-1,1\}^n}[|f(r, x_r, y_{-r}, t) - \langle x \cdot y, r \rangle| \leq \ell] > e^{c_1 \varepsilon} c_2 \ell / \sqrt{n}. \tag{65}$$

Hence,

$$
\begin{aligned}
e^{c_1 \varepsilon} c_2 \ell / \sqrt{n} &< \mathrm{E}_{s \leftarrow D}[p_\ell^s] \\
&\leq \Pr_{s \leftarrow D}[p_\ell^s \geq e^{c_1 \varepsilon} c_2 \ell / 2\sqrt{n}] \cdot 1 + \Pr_{s \leftarrow D}[p_\ell^s < e^{c_1 \varepsilon} c_2 \ell / 2\sqrt{n}] \cdot e^{c_1 \varepsilon} c_2 \ell / 2\sqrt{n} \\
&\leq \Pr_{s \leftarrow D}[p_\ell^s \geq e^{c_1 \varepsilon} c_2 \ell / 2\sqrt{n}] + e^{c_1 \varepsilon} c_2 \ell / 2\sqrt{n}.
\end{aligned}
$$

$\square$

The second claim states that for the right value of $\widehat{\ell}$, the probability that $p_{\ell-1}^s$ is larger than the threshold $\widehat{v}$ is very close to the probability that $p_{\ell+1}^s$ is larger than this threshold.

Claim 5.12. *For every $\widehat{v} \leq e^{4\varepsilon} \cdot c_2 \ell / 2\sqrt{n}$ there exists $\widehat{\ell} \in [[\ell + 1, \ell + m \cdot \lceil \log n \rceil]]$ such that:*

$$\Pr_{s \leftarrow D}\left[p_{\ell-1}^s \geq \widehat{v}\right] \leq \Pr_{s \leftarrow D}\left[p_{\ell+1}^s \geq \widehat{v}\right] \leq (1 + 2/m) \cdot \Pr_{s \leftarrow D}\left[p_{\ell-1}^s \geq \widehat{v}\right].$$

Proof of Claim 5.12. Since $\widehat{v} \leq e^{4\varepsilon} c_2 \ell / 2\sqrt{n}$, Claim 5.11 yields that

$$\Pr_{s \leftarrow D}[p_\ell^s \geq \widehat{v}] \geq e^{4\varepsilon} c_2 \ell / 2\sqrt{n} \geq 1/\sqrt{n} \tag{66}$$

Assume toward contradiction that for every $\widehat{\ell} \in [[\ell + 1, \ell + m\lceil \log n \rceil]]$, it holds that

$$\Pr_{s \leftarrow D}\left[p_{\ell+1}^s > \widehat{v}\right] > (1 + 2/m) \cdot \Pr_{s \leftarrow D}\left[p_{\ell-1}^s \geq \widehat{v}\right] \tag{67}$$

But, it would have followed that

$$1 \geq \Pr_{s \leftarrow D}\left[p_{\ell+m\lceil \log n \rceil}^s > \widehat{v}\right] > (1 + 2/m)^{(m/2) \cdot \log n} \cdot \Pr_{s \leftarrow D}[p_\ell^s \geq \widehat{v}] \geq n \cdot (1/\sqrt{n}) > 1.$$

$\square$

We now prove that Theorem 5.1 holds with respect to the idealized algorithm $\widetilde{\mathsf{Dist}}$, formally stated in the following claim.

Claim 5.13 ($\widetilde{\mathsf{Dist}}$ is a good distinguisher)**.** *It holds that*

$$\Pr_{\substack{(x,y,t) \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^{D,f}(i, (x, y)_{<i>}, t) = 1\right] < 0.9 \cdot e^{-\varepsilon} \cdot \Pr_{\substack{(x,y,t) \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^{D,f}(i, (x, y), t) = 1\right] - 2/n.$$

Proof. Recall that n_0 be the constant guaranteed by Lemma 5.3, and that $c := 2^{30} \cdot n_0$, $c_1 := 10$ and $c_2 := c^3$. In addition, let $\widehat{v} \in [e^{4\varepsilon} c\ell/4\sqrt{n}, e^{4\varepsilon} c\ell/2\sqrt{n}]$, and let $\widehat{\ell}$ be the value guaranteed by Claim 5.12. We assume without loss of generality that $n \geq e^{4\varepsilon} c_2 > n_0$ and $\varepsilon \leq 1/20 \cdot \log n$ (otherwise, the proof holds trivially as $e^{c_1 \cdot \varepsilon} \cdot c_2 \cdot \ell/\sqrt{n} > 1$).

We start by upper bounding the probability that $\widetilde{\mathsf{Dist}}$ (with the above choice of $\widehat{v}$ and $\widehat{\ell}$) abort. By definition, it holds that $p^s_{\widehat{\ell}-1} \leq p^s_{\widehat{\ell}}$ for every $s \in \mathrm{Supp}(D)$. Moreover, by the triangle inequality,

$$q^s_{\widehat{\ell},i} \in [p^s_{\widehat{\ell}-1}, p^s_{\widehat{\ell}+1}] \tag{68}$$

for every $i \in [2n]$. By Claim 5.11, $\Pr_{s \leftarrow D}\left[p^s_{\widehat{\ell}-1} \geq \widehat{v}\right] \geq e^{c_1 \varepsilon} c_2 \ell/2\sqrt{n} \geq e^{4\varepsilon} c\ell/2\sqrt{n}$, and we conclude that

$$\begin{aligned}
\Pr_{s=(x,y,t)\leftarrow D, i\leftarrow[2n]}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right] &= \Pr_{s\leftarrow D, i\leftarrow[2n]}\left[q^s_{\widehat{\ell},i} \geq \widehat{v}\right] \\
&\geq \Pr_{s\leftarrow D}\left[p^s_{\widehat{\ell}-1} \geq \widehat{v}\right] \\
&\geq e^{4\varepsilon} c\ell/2\sqrt{n}.
\end{aligned} \tag{69}$$

The equality is by definition of $\widetilde{\mathsf{Dist}}$. We next want to use Lemma 5.3 in order to show that there exists $d \in \{1,2,3\}$ such that A_d is a good distinguisher for the distribution of (x,y,t) sampled from D conditioned on $\widetilde{\mathsf{Dist}}$ not aborting. In order to use the above lemma, we first need to show that i is close to be uniform when conditioning on no abort. That is, we argue that the value i is close to being independent of the decision taken by $\widetilde{\mathsf{Dist}}$ whether to abort or not. Let $\mathcal{B} = \left\{s\colon p^s_{\widehat{\ell}+1} \geq \widehat{v} \wedge p^s_{\widehat{\ell}-1} < \widehat{v}\right\}$. By Claim 5.12 and Equation (69),

$$\Pr_{s\leftarrow D}[s \in \mathcal{B}] \leq 2/m \cdot \Pr_{s\leftarrow D}\left[p^s_{\widehat{\ell}-1} \geq \widehat{v}\right] \leq 2/m \cdot \Pr_{\substack{s\leftarrow D \\ i\leftarrow[2n]}}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right] \tag{70}$$

Thus,

$$\Pr_{\substack{s=(x,y,t)\leftarrow D \\ i\leftarrow[2n]}}\left[s \in \mathcal{B} \mid \widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right] \leq 2/m \tag{71}$$

We next observe that for every $s = (x,y,t) \notin \mathcal{B}$, it holds that

$$i \leftarrow [2n]\big|_{\widetilde{\mathsf{Dist}}^f(i,(x,y)_{-i},t) \text{ not abort}} \equiv i \leftarrow [2n] \tag{72}$$

Indeed, let $s = (x,y,t) \notin \mathcal{B}$ be such that $\widetilde{\mathsf{Dist}}^f(i,(x,y)_{-i},t)$ does not abort for some $i \in [2n]$. By assumption, $q^s_{\widehat{\ell},i} \geq \widehat{v}$. Thus by Equation (68), $p^s_{\widehat{\ell}+1} \geq \widehat{v}$. Hence, by definition of $\mathcal{B}$, $p^s_{\widehat{\ell}-1} \geq \widehat{v}$. Therefore by Equation (68), $q^s_{\widehat{\ell},i'} \geq \widehat{v}$ for every i', and $\widetilde{\mathsf{Dist}}$ does not abort on every i.

We are left to show that the distribution of (x,y,t) in

$$((x,y,t), i \leftarrow D \times [n])\big|_{\widetilde{\mathsf{Dist}}^f(i,(x,y)_{-i},(x,y)_i,t) \text{ not abort} \wedge (x,y,t)\notin\mathcal{B}} \tag{73}$$

fulfills the requirements of Lemma 5.3. Let Q be the distribution of (x,y,t) in Equation (73), and notice that by Equation (72) we get that the distribution in Equation (73) is equal to $Q \times I$, where

I is the uniform distribution over $[2n]$. Note that by construction of $\widetilde{\mathsf{Dist}}$, the above distribution is independent from the value of $(x', y')_i$. Also by construction, $\widetilde{\mathsf{Dist}}^f(s, j)$ does not abort only if $q^s_{\widehat{\ell}, i} \geq \widehat{v}$. Thus, in this case we obtain by Equation (68) that $p^s_{\widehat{\ell}+1} \geq \widehat{v}$. The choice of c and the fact that $\widehat{\ell}+1 \leq 2m\ell$ yields that if $\widetilde{\mathsf{Dist}}^f(s, j)$ does not abort, then s satisfies the conditions of Lemma 5.3 with respect to length parameter $\ell' = \widehat{\ell} + 1$. Thus, by Lemma 5.3 there exists $d \in \{1, 2, 3\}$ such that

$$\Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f_d(i, (x, y), t, \ell') = 1\right] \geq e^{-\varepsilon}/16 \tag{74}$$

and,

$$\Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f_d(i, (x, y)_{<i>}, t, \ell') = 1\right] \leq 1/2 \cdot e^{-\varepsilon} \cdot \Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f_d(i, (x, y), t, \ell') = 1\right] \tag{75}$$

We now use the above observations above to conclude the claim. We first bound $\Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) = 1\right]$. Compute,

$$\Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) = 1\right] \tag{76}$$

$$\geq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) = 1 \ \wedge \ s \notin \mathcal{B}\right]$$

$$= \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort} \ \wedge \ s \notin \mathcal{B}\right] \cdot \Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f(i, (x, y), t, \ell') = 1\right]$$

$$\geq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort}\right](1 - 2/m) \cdot \Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f(i, (x, y), t, \ell') = 1\right].$$

The first equality holds by the construction of Q, and the last inequality by Equation (71). Similarly,

$$\Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y)_{<i>}, t) = 1\right] \tag{77}$$

$$\leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y)_{<i>}, t) \text{ not abort} \ \wedge \ s \notin \mathcal{B}\right] \cdot \Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f(i, (x, y)_{<i>}, t, \ell') = 1\right]$$

$$+ \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y)_{<i>}, t) \text{ not abort} \ \wedge \ s \in \mathcal{B}\right] \cdot 1$$

$$= \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort} \ \wedge \ s \notin \mathcal{B}\right] \cdot \Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f(i, (x, y)_{<i>}, t, \ell') = 1\right]$$

$$+ \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort} \ \wedge \ s \in \mathcal{B}\right] \cdot 1$$

$$\leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort}\right] \cdot \left(\Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}}\left[\mathsf{A}^f(i, (x, y)_{<i>}, t, \ell') = 1\right] + 2/m\right).$$

The equality holds by the observation that the decision to abort is independent of $(x', y')_i$, and the

last inequality by Equation (71). Combining Equations (75) to (77), yields

$$\Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y)_{<i>}, t) = 1 \right] \tag{78}$$

$$\leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \right] \cdot \left(\Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}} \left[\mathsf{A}^f(i, (x,y)_{<i>}, t, \ell') = 1 \right] + 2/m \right)$$

$$\leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \right] \cdot \left(1/2 \cdot e^{-\varepsilon} \cdot \Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}} \left[\mathsf{A}^f(i, (x,y), t, \ell') = 1 \right] + 2/m \right)$$

$$\leq e^{-\varepsilon}/2 \cdot (1 - 2/m)^{-1} \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) = 1 \right] + 2/m \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \right]$$

$$\leq 0.75 \cdot e^{-\varepsilon} \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) = 1 \right] + 2/m \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \right].$$

The first equation holds by Equation (77), the second by Equation (75), the third by Equation (76), and the last one since $m \geq 1000$.

We conclude the proof by showing that

$$2/m \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \right] < 0.1 \cdot e^{-\epsilon} \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) = 1 \right] - 2/n \tag{79}$$

which yields the theorem. Indeed,

$$\Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) = 1 \right] \tag{80}$$

$$\geq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \ \wedge \ s \notin \mathcal{B} \right] \cdot \Pr_{\substack{s \leftarrow Q \\ i \leftarrow [2n]}} \left[\mathsf{A}^f(i, (x,y), t, \ell') = 1 \right]$$

$$\geq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \ \wedge \ s \notin \mathcal{B} \right] \cdot e^{-\varepsilon}/16$$

$$\geq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \right] \cdot (1 - 2/m) \cdot e^{-\varepsilon}/16$$

$$> e^{-\varepsilon}/32 \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}} \left[\widetilde{\mathsf{Dist}}^f(i, (x,y), t) \text{ not abort} \right].$$

The first equation holds by the definition of Q, the second by Equation (74), the third by Equation (71), and the last inequality holds since $m > 4$. Equation (79) now follows since $n \geq c$, by the choice of m and Equation (69).

The above concludes the claim proof, apart from the fact that we need to find the right value of $\widehat{\ell}$ and d hardwired into distinguisher $\widetilde{\mathsf{Dist}}$. These values can be easily found, however, by trying all options of $(\widehat{\ell}, d) \in [n] \times [3]$. For each such pair, sample a polynomial number of samples from D, and by emulating $\widetilde{\mathsf{Dist}}$ on them, estimating the prediction probability up to $o(1/n)$ error (with overwhelming probability). Since there are only $O(n)$ possibilities for such value, the above can be done efficiently. □

5.2.2 Analyzing the Non-Idealized Distinguisher

In this section, we use the above observations to lower bound the distinguishing advantage of (the non-idealized) algorithm Dist, and thus proving Theorem 5.1. Recall that Dist uses the value of

$$q = \Pr_{r \leftarrow \mathcal{R}}\left[\left|f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r\rangle - b \cdot x_j \cdot y_j\right| \leq \widehat{\ell}\right], \tag{81}$$

rather than that of $q_{\ell,i}^s$, used by its idealized variant $\widetilde{\text{Dist}}$ considered above. For fixed $\widehat{\ell}$ and $s = (x, y, t)$, let $Q_{\widehat{\ell},i}^s$ be the value of q in a random execution $\text{Dist}^f(i, (x, y), t)$ (recall that Dist do not use $(x, y)_i$ in order to compute this value). In the following we assume $n \geq e^{4\varepsilon}c$, as otherwise the theorem follows trivially. The following two claims will be useful in the proof of Theorem 5.1.

The first claim shows that small values added to the value of $q_{\ell,i}^s$ are not likely to change the decision of Dist. In the following, let $c_\varepsilon := e^{4\varepsilon}c$ and $\alpha := \frac{\ell}{\sqrt{n}\cdot\log^3 n}$.

Claim 5.14. *There exists $\widehat{v} \in [c_\varepsilon\ell/4\sqrt{n}, c_\varepsilon\ell/2\sqrt{n}] \cap \{c_\varepsilon\ell/4\sqrt{n} + k \cdot \alpha \colon k \in \mathbb{N}\}$ such that for every $\widehat{\ell} \in [[\ell + 1, \ell + m \cdot \lceil\log n\rceil]]$ it holds that*

$$\Pr_{s \leftarrow D, i \leftarrow [2n]}\left[q_{\widehat{\ell},i}^s \in (\widehat{v} \pm \alpha)\right] \leq 1/(\sqrt{c_\varepsilon}\log n) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[q_{\widehat{\ell},i}^s \geq \widehat{v} + \alpha\right].$$

The proof of Claim 5.14 is similar to the one of Claim 5.12. For every fixing of $\widehat{\ell}$, it cannot holds for too many $\widehat{v}$ that $\Pr_{s \leftarrow D, i \leftarrow [2n]}\left[q_{\widehat{\ell},i}^s \in (\widehat{v} \pm \alpha)\right] > 1/(\sqrt{c_\varepsilon}\log n) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[q_{\widehat{\ell},i}^s \geq \widehat{v} + \alpha\right]$, as otherwise it holds that $\Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[q_{\widehat{\ell},i}^s \geq c_\varepsilon\ell/4\sqrt{n}\right] > 1$. By our choice of the range of $\widehat{v}$, $[c_\varepsilon\ell/4\sqrt{n}, c_\varepsilon\ell/2\sqrt{n}] \cap \{c_\varepsilon\ell/4\sqrt{n} + k \cdot \alpha \colon k \in \mathbb{N}\}$, to be large enough, we can show that at least one $\widehat{v}$ in this range is good for every $\widehat{\ell}$.

The next claim states that $Q_{\widehat{\ell},i}^s$ is not too far from $q_{\widehat{\ell},i}^s$.

Claim 5.15. *For every $s \in \text{Supp}(D)$, $\widehat{\ell} \in [[\ell + 1, \ell + m \cdot \lceil\log n\rceil]]$ and $\widehat{v} \leq c_\varepsilon\ell/2\sqrt{n}$, it holds that*

$$\Pr_{i \leftarrow [2n]}\left[\left(Q_{\widehat{\ell},i}^s \geq \widehat{v} \wedge q_{\widehat{\ell},i}^s < \widehat{v} - \alpha\right) \vee \left(Q_{\widehat{\ell},i}^s < \widehat{v} \wedge q_{\widehat{\ell},i}^s \geq \widehat{v} + \alpha\right)\right] \leq 2/\sqrt{n}.$$

Claim 5.15 follows by Proposition 3.27. Recall that

$$q_{\widehat{\ell},i}^s := \Pr_{r \leftarrow \{-1,1\}^n}\left[\left|f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r\rangle - b(i) \cdot x_{j(i)} \cdot y_{j(i)}\right| \leq \widehat{\ell}\right]$$

and that $Q_{\widehat{\ell},i}^s$ is an estimation of

$$\Pr_{r \leftarrow \{-1,1\}^n|_{r_{j(i)}=b(i)}}\left[\left|f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r\rangle - b(i) \cdot x_{j(i)} \cdot y_{j(i)}\right| \leq \widehat{\ell}\right].$$

Thus, the main difference between $Q_{\widehat{\ell},i}^s$ to $q_{\widehat{\ell},i}^s$ is the expectation that taken only over r's for which $r_{j(i)} = b(i)$. Using Proposition 3.27 it can be shown that for most values of i, $Q_{\widehat{\ell},i}^s$ and $q_{\widehat{\ell},i}^s$ are close. We prove Claims 5.14 and 5.15 below, but first we use them to prove Theorem 5.1.

Proving Theorem 5.1.

Proof of of Theorem 5.1. The proof goes by coupling Dist with its idealized variant $\widetilde{\mathsf{Dist}}$ considered above. Let $\widehat{v}$ be the value guaranteed by Claim 5.14, $\widehat{\ell}$ be the value guaranteed by Claim 5.12, and let $(X, Y, T) \leftarrow D$ and $I \leftarrow [2n]$. Let O and $\widetilde{O}$ be the output in of random executions of $\mathsf{Dist}(I, (X, Y), T)$ and $\widetilde{\mathsf{Dist}}(I, (X, Y), T)$ respectively, using the same random tape for both executions. We start with bounding the probability that $O \neq \widetilde{O}$. By construction, the event $O \neq \widetilde{O}$ implies that $Q_I^s \geq \widehat{v}$ and $q_I^s < \widehat{v}$, or $Q_I^s < \widehat{v}$ and $q_I^s \geq \widehat{v}$, omitting the subscript $\widehat{\ell}$ for clarity of the notation. Hence,

$$\Pr\left[O \neq \widetilde{O}\right] \leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\left(Q_{\widehat{\ell},i}^s \geq \widehat{v} \wedge q_{\widehat{\ell},i}^s < \widehat{v}\right) \vee \left(Q_{\widehat{\ell},i}^s < \widehat{v} \wedge q_{\widehat{\ell},i}^s \geq \widehat{v}\right)\right] \tag{82}$$

$$\leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\left(q_{\widehat{\ell},i}^s \in (\widehat{v} \pm \alpha)\right) \vee \left(Q_{\widehat{\ell},i}^s \geq \widehat{v} \wedge q_{\widehat{\ell},i}^s < \widehat{v} - \alpha\right) \vee \left(Q_{\widehat{\ell},i}^s < \widehat{v} \wedge q_{\widehat{\ell},i}^s \geq \widehat{v} + \alpha\right)\right]$$

$$\leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[q_{\widehat{\ell},i}^s \in (\widehat{v} \pm \alpha)\right] + \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\left(Q_{\widehat{\ell},i}^s \geq \widehat{v} \wedge q_{\widehat{\ell},i}^s < \widehat{v} - \alpha\right) \vee \left(Q_{\widehat{\ell},i}^s < \widehat{v} \wedge q_{\widehat{\ell},i}^s \geq \widehat{v} + \alpha\right)\right]$$

$$\leq 1/(\sqrt{c_\varepsilon}\log n) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[q_{\widehat{\ell},i}^s \geq \widehat{v} + \alpha\right] + 2/\sqrt{n}$$

Where the third inequality holds by the union bound and the last by Claims 5.14 and 5.15. By definition of $\widetilde{\mathsf{Dist}}$, it holds that,

$$\Pr_{s \leftarrow D, i \leftarrow [2n]}\left[q_{\widehat{\ell},i}^s \geq \widehat{v} + \alpha\right] \leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort}\right], \tag{83}$$

and by Equation (69)

$$2/\sqrt{n} \leq (4/c_\varepsilon \ell) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort}\right] \tag{84}$$

Combining the above with the assumption that $\ell \geq \log n$, we get that,

$$\Pr\left[O \neq \widetilde{O}\right] \leq 2/(\sqrt{c_\varepsilon}\log n) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort}\right] \tag{85}$$

We now use the above to bound the distinguishing advantage of Dist. By Equation (85) we immediately get that

$$\Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\mathsf{Dist}^f(i, (x, y), t) = 1\right] \tag{86}$$

$$\geq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) = 1\right] - 2/(\sqrt{c_\varepsilon}\log n) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort}\right]$$

Recall that by construction, the decision to call A_d is independent of $(x, y)_i$. Thus, using the same line of proof,

$$\Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\mathsf{Dist}^f(i, (x, y)_{<i>}, t) = 1\right] \tag{87}$$

$$\leq \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y)_{<i>}, t) = 1\right] + 2/(\sqrt{c_\varepsilon}\log n) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i, (x, y), t) \text{ not abort}\right]$$

Observe that by the choice of c and m it holds that $4/(\sqrt{c_\varepsilon}\log n) \le 1/m$. Combining the above with Equation (78), we get,

$$\Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\mathsf{Dist}^f(i,(x,y)_{<i>},t)=1\right] \tag{88}$$

$$\le 0.75 \cdot e^{-\varepsilon} \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\mathsf{Dist}^f(i,(x,y),t)=1\right] + (3/m) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right]$$

We conclude the proof by showing that

$$3/m \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right] \le 0.25 \cdot e^{-\varepsilon} \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\mathsf{Dist}^f(i,(x,y),t)=1\right] - 2/n. \tag{89}$$

Indeed,

$$3/m \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right] \tag{90}$$

$$< 0.15 \cdot e^{-\epsilon} \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t)=1\right] - 2/n$$

$$\le 0.15 \cdot e^{-\epsilon} \cdot (\Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\mathsf{Dist}^f(i,(x,y),t)=1\right] + 1/m \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right]) - 2/n,$$

where the first inequality holds by Equation (79), and the second by Equation (86) and since $2/(\sqrt{c_\varepsilon}\log n) \le 1/m$. The above implies that

$$(3/m - 0.15 \cdot e^{-\varepsilon}/m) \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [2n]}}\left[\widetilde{\mathsf{Dist}}^f(i,(x,y),t) \text{ not abort}\right] \tag{91}$$

$$\le 0.15 \cdot e^{-\epsilon} \cdot \Pr_{\substack{s \leftarrow D \\ i \leftarrow [n]}}\left[\mathsf{Dist}^f(i,(x,y),t)=1\right] - 2/n$$

which easily yields Equation (89) as $(3/m - 0.15 \cdot e^{-\varepsilon}/m) \ge 2/m$.

Similar to the ideal case, we need to find the right value of $\widehat{\ell},\widehat{v}$ and d hardwired into distinguisher Dist. As in the ideal case, these values can be found by trying all options of triplets $\widehat{\ell},\widehat{v},d$. For each such triplet, sample a polynomial number of samples from D, and by emulating Dist on them, estimating the prediction probability up to $o(1/n)$ error (with overwhelming probability). Since by Claim 5.14 $\widehat{v} \in [c_\varepsilon\ell/4\sqrt{n}, c_\varepsilon\ell/2\sqrt{n}] \cap \{c_\varepsilon\ell/4\sqrt{n} + k \cdot \alpha \colon k \in \mathbb{N}\}$, this can be done efficiently. $\qquad\square$

Proving Claim 5.14.

Proof of Claim 5.14. Recall that $m = e^{2\varepsilon} \cdot 1000$, $c = 2^{30} \cdot n_0$, $c_\varepsilon = e^{4\varepsilon} \cdot c$ and $\alpha = \frac{\ell}{\sqrt{n}\cdot\log^3 n}$, and let $d := \lfloor c_\varepsilon\ell/(4 \cdot \alpha \cdot \sqrt{n}) \rfloor$. By the choice d it holds that

$$d > 2\sqrt{c_\varepsilon} \cdot m \cdot \log^3 n \tag{92}$$

For every $\widehat{\ell} \in [[\ell+1, \ell+m\log n]]$, let $\mathcal{B}_{\widehat{\ell}}$ be the set of $v \in [d]$ such that

$$\Pr_{s \leftarrow D, i \leftarrow [2n]}\left[q_{\ell,i}^s \ge c_\varepsilon\ell/4\sqrt{n} + \alpha(v-1)\right] > (1 + 1/(\sqrt{c_\varepsilon}\log n))\Pr_{s \leftarrow D, i \leftarrow [2n]}\left[q_{\ell,i}^s \ge c_\varepsilon\ell/4\sqrt{n} + \alpha(v+1)\right].$$

We need to show that there exists $v \in [d]$ such that $v \notin \mathcal{B}_{\widehat{\ell}}$ for every $\widehat{\ell} \in [[\ell+1, \ell + m \log n]]$.

We start by showing that for every $\widehat{\ell} \in [[\ell+1, \ell + m \log n]]$, the size of $\mathcal{B}_{\widehat{\ell}}$ is at most $2\sqrt{c_\varepsilon} \log^2 n$. The claim now follows since $\left| \cup_{\widehat{\ell} \in [[\ell+1, \ell+m \log n]]} \mathcal{B}_{\widehat{\ell}} \right| \leq 2\sqrt{c_\varepsilon} \log^2 n \cdot m \log n < d$. To bound the size of $\mathcal{B}_{\widehat{\ell}}$ we use a similar argument to the proof of Claim 5.12.

To see the above, fix $\widehat{\ell} \in [[\ell+1, \ell+m \log n]]$. We start with showing that

$$\Pr_{s \leftarrow D, i \leftarrow [2n]} \left[q_{\widehat{\ell}, i}^s \geq c_\varepsilon \ell / 4\sqrt{n} + \alpha \cdot d \right] \geq 1/\sqrt{n} \tag{93}$$

To see this, notice that

$$e^{c_1 \varepsilon} \cdot c_2 \ell / 2\sqrt{n} \geq c_\varepsilon \ell / 2\sqrt{n} \geq c_\varepsilon \ell / 4\sqrt{n} + d\alpha. \tag{94}$$

and recall that by Equation (68) it holds that $q_{\widehat{\ell}, i}^s \in [p_{\widehat{\ell}-1}^s, p_{\widehat{\ell}+1}^s]$. Since $\widehat{\ell} \geq \ell+1$, the last implies that

$$q_{\widehat{\ell}, i}^s \geq p_{\widehat{\ell}-1}^s \geq p_\ell^s. \tag{95}$$

Lastly, by Claim 5.11 it holds that $\Pr_{s \leftarrow D}[p_\ell^s \geq e^{c_1 \varepsilon} \cdot c_2 \ell / 2\sqrt{n}] \geq e^{c_1 \varepsilon} \cdot c_2 \ell / 2\sqrt{n}$. Together with Equation (94), we get that,

$$\Pr_{s \leftarrow D} \left[p_\ell^s \geq c_\varepsilon \ell / 4\sqrt{n} + \alpha \cdot d \right] \geq c_\varepsilon \ell / 2\sqrt{n} \geq 1/\sqrt{n}. \tag{96}$$

Combining Equations (95) and (96) yields Equation (93).

Next, assume toward contradiction that $|\mathcal{B}_{\widehat{\ell}}| > 2\sqrt{c_\varepsilon} \log^2 n$. By monotonicity, for every $v \in [d]$ it holds that

$$\Pr_{s \leftarrow D, i \leftarrow [2n]} \left[q_{\widehat{\ell}, i}^s \geq c_\varepsilon \ell / 4\sqrt{n} + \alpha(v-1) \right] \geq \Pr_{s \leftarrow D, i \leftarrow [2n]} \left[q_{\widehat{\ell}, i}^s \geq c_\varepsilon \ell / 4\sqrt{n} + \alpha(v+1) \right], \tag{97}$$

and, by definition, for every $v \in \mathcal{B}_{\widehat{\ell}}$ it holds that,

$$\Pr_{s \leftarrow D, i \leftarrow [2n]} \left[q_{\widehat{\ell}, i}^s \geq c_\varepsilon \ell / 4\sqrt{n} + \alpha(v-1) \right] \tag{98}$$
$$\geq (1 + 1/(\sqrt{c_\varepsilon} \log n)) \Pr_{s \leftarrow D, i \leftarrow [2n]} \left[q_{\widehat{\ell}, i}^s \geq c_\varepsilon \ell / 4\sqrt{n} + \alpha(v+1) \right].$$

Combining Equations (97) and (98) together with Equation (93), we get,

$$\Pr_{s \leftarrow D, i \leftarrow [2n]} \left[q_{\widehat{\ell}, i}^s \geq c_\varepsilon \ell / 4\sqrt{n} \right]$$
$$\geq (1 + 1/(\sqrt{c_\varepsilon} \log n))^{|\mathcal{B}_{\widehat{\ell}}|/2} \Pr_{s \leftarrow D, i \leftarrow [2n]} \left[q_{\widehat{\ell}, i}^s \geq c_\varepsilon \ell / 4\sqrt{n} + \alpha d \right] \geq n \cdot 1/\sqrt{n} > 1,$$

which cannot holds. $\qquad \square$

Proving Claim 5.15. The proof of Claim 5.15 easily follows from the following claim.

Claim 5.16. *For every $s \in \mathrm{Supp}(D)$ and $\widehat{\ell} \in [[\ell+1, \ell+m \cdot \lceil \log n \rceil]]$, it holds that*

1. $\Pr_{i \leftarrow [2n]} \left[\left(Q_{\widehat{\ell}, i}^s \leq c_\varepsilon \ell / \sqrt{n} \right) \wedge \left(\left| Q_{\widehat{\ell}, i}^s - q_{\widehat{\ell}, i}^s \right| > \alpha \right) \right] < 1/\sqrt{n}$, *and*

46

2. $\Pr_{i \leftarrow [2n]} \left[\left(Q^s_{\widehat{\ell},i} \geq c_\varepsilon \ell / \sqrt{n} \right) \wedge \left(q^s_{\widehat{\ell},i} \leq c_\varepsilon \ell / 2\sqrt{n} \right) \right] < 1/\sqrt{n}$.

we prove Claim 5.16 next, but first we use it in order to prove Claim 5.15.

Proof of Claim 5.15. Let $s, \widehat{\ell}$ and $\widehat{v}$ as in Claim 5.15. Observe that since $\widehat{v} \leq c_\varepsilon \ell / 2\sqrt{n}$, it holds that

$$\Pr_{i \leftarrow [2n]} \left[\left(Q^s_{\widehat{\ell},i} \geq \widehat{v} \wedge q^s_{\widehat{\ell},i} < \widehat{v} - \alpha \right) \vee \left(Q^s_{\widehat{\ell},i} < \widehat{v} \wedge q^s_{\widehat{\ell},i} \geq \widehat{v} + \alpha \right) \right]$$

$$\leq \Pr_{i \leftarrow [2n]} \left[\left(\left| Q^s_{\widehat{\ell},i} - q^s_{\widehat{\ell},i} \right| > \alpha \right) \wedge \left(Q^s_{\widehat{\ell},i} \leq \widehat{v} \vee q^s_{\widehat{\ell},i} \leq \widehat{v} \right) \right]$$

$$\leq \Pr_{i \leftarrow [2n]} \left[\left(\left| Q^s_{\widehat{\ell},i} - q^s_{\widehat{\ell},i} \right| > \alpha \right) \wedge \left(Q^s_{\widehat{\ell},i} \leq c_\varepsilon \ell / 2\sqrt{n} \vee q^s_{\widehat{\ell},i} \leq c_\varepsilon \ell / 2\sqrt{n} \right) \right]$$

$$\leq \Pr_{i \leftarrow [2n]} \left[\left(Q^s_{\widehat{\ell},i} \leq c_\varepsilon \ell / \sqrt{n} \wedge \left| Q^s_{\widehat{\ell},i} - q^s_{\widehat{\ell},i} \right| > \alpha \right) \vee \left(Q^s_{\widehat{\ell},i} \geq c_\varepsilon \ell / \sqrt{n} \wedge q^s_{\widehat{\ell},i} \leq c_\varepsilon \ell / 2\sqrt{n} \right) \right]$$

$$\leq 2/\sqrt{n}$$

where the last inequality follows by Claim 5.16 and the union bound. $\square$

Proving Claim 5.16.

Proof of Claim 5.16. Fix $s = (x, y, t) \in \mathsf{Supp}(D)$ and $\widehat{\ell} \in [[\ell + 1, \ell + m \log n]]$. First, by definition of $\mathsf{Dist}(i, (x, y)_i, t)$, the expectation of $Q^s_{\widehat{\ell},i}$ (i.e., of value of q in a random execution) is

$$p_i := \Pr_{r \leftarrow \{-1,1\}^n |_{r_{j(i)} = b(i)}} \left[\left| f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle - b(i) \cdot x_{j(i)} \cdot y_{j(i)} \right| \leq \widehat{\ell} \right]$$

and thus, by applying the Hoffeding bound it holds that,

$$\Pr \left[\left| p_i - Q^s_{\widehat{\ell},i} \right| \geq 1/n^2 \right] \leq 1/n. \tag{99}$$

Next, recall that,

$$q^s_{\widehat{\ell},i} := \Pr_{r \leftarrow \{-1,1\}^n} \left[\left| f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle - b(i) \cdot x_{j(i)} \cdot y_{j(i)} \right| \leq \widehat{\ell} \right] \tag{100}$$

We next want to use Proposition 3.27 in order to show that p_i and $q^s_{\widehat{\ell},i}$ are close for most values of i. However, the event that $\left| f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle - b(i) \cdot x_{j(i)} \cdot y_{j(i)} \right| \leq \widehat{\ell}$ is by definition dependent in i. To overcame this, we observe that the only dependency of $q^s_{\widehat{\ell},i}$ on i is in the term $b(i) \cdot x_{j(i)} \cdot y_{j(i)}$ which can be only -1 or 1. For every $\sigma \in \{-1, 1\}$, we define

$$q_\sigma := \Pr_{r \leftarrow \{-1,1\}^n} \left[\left| f(r, x_{r+}, y_{r-}, t) - \langle x \cdot y, r \rangle - \sigma \right| \leq \widehat{\ell} \right] \tag{101}$$

It is easy to see that $q^s_{\widehat{\ell},i} \in \{q_1, q_{-1}\}$ for every $i \in [2n]$. Below we fix $\sigma \in \{-1, 1\}$ and denote by I_σ the distribution $i \leftarrow [2n]|_{b(i) \cdot x_{j(i)} \cdot y_{j(i)} = \sigma}$. In words, choose i uniformly from $[2n]$ under the condition that $b(i) \cdot x_{j(i)} \cdot y_{j(i)} = \sigma$. It is not hard to see that the distribution of $j(i)$ in this process is uniform over $[n]$.

Recall that we want to show that $Q^s_{\widehat{\ell},i}$ is not too far from $q^s_{\widehat{\ell},i}$ (with high probability over i). By Equation (99), $Q^s_{\widehat{\ell},i}$ is close to p_i and thus the heart of the proof is showing that p_i is close to q_σ for most i's. Indeed, by applying Proposition 3.27 we get that, if $q_\sigma \geq 1/n$ then,

$$\Pr_{i \leftarrow I_\sigma} \left[p_i \in (1 \pm 4n^{-1/4} \cdot \sqrt{\log n}) \cdot q_\sigma \right] \geq 1 - 1/(2\sqrt{n}). \tag{102}$$

We next show that $\Pr_{i \leftarrow I_\sigma}\left[\left(Q^s_{\hat{\ell},i} \leq c_\varepsilon \ell/\sqrt{n}\right) \wedge \left(\left|Q^s_{\hat{\ell},i} - q_\sigma\right| > \frac{\ell}{2\sqrt{n}\cdot\log^3 n}\right)\right] < 1/\sqrt{n}$, and,

$\Pr_{i \leftarrow I_\sigma}\left[\left(Q^s_{\hat{\ell},i} \geq c_\varepsilon \ell/\sqrt{n}\right) \wedge (q_\sigma \leq c_\varepsilon \ell/2\sqrt{n})\right] < 1/\sqrt{n}$. The claim will follow since the uniform distribution $i \leftarrow [2n]$ is a convex combination of I_1 and I_{-1}.

The proof is by splitting into cases:

1. $q_\sigma \leq 1/n$

2. $q_\sigma \in [1/n, 5c_\varepsilon \ell/\sqrt{n}]$

3. $q_\sigma \geq 5c_\varepsilon \ell/\sqrt{n}$

The case $q_\sigma \leq 1/n$. Assume the first case holds. Observe that, since for every j and b $\Pr_{r \leftarrow \{-1,1\}^n}[r_j = b] = 1/2$, it is true that $p_i \in [0, 2 \cdot q_\sigma]$. Thus, by Equation (99),

$$\Pr_{i \leftarrow I_\sigma}\left[Q^s_{\hat{\ell},i} \leq c_\varepsilon \ell/\sqrt{n} \wedge \left|Q^s_{\hat{\ell},i} - q_\sigma\right| > \frac{\ell}{2\sqrt{n} \cdot \log^3 n}\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[\left|Q^s_{\hat{\ell},i} - q_\sigma\right| > \frac{\ell}{2\sqrt{n} \cdot \log^3 n}\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[\left|Q^s_{\hat{\ell},i} - p_i\right| > 1/n^2\right]$$

$$\leq 1/n.$$

Similarly,

$$\Pr_{i \leftarrow I_\sigma}\left[Q^s_{\hat{\ell},i} \geq c_\varepsilon \ell/\sqrt{n} \wedge q_\sigma \leq c\ell/2\sqrt{n}\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[\left|Q^s_{\hat{\ell},i} - q_\sigma\right| > \frac{\ell}{2\sqrt{n} \cdot \log^3 n}\right]$$

$$\leq 1/n.$$

The case $q_\sigma \in [1/n, 5c_\varepsilon \ell/\sqrt{n}]$. For the second case, notice that by Equation (102) and the fact that $c_\varepsilon = c \cdot e^{4\varepsilon} \leq n^{1/4}/\log^4 n$,

$$\Pr_{i \leftarrow I_\sigma}\left[|q_\sigma - p_i| \leq \frac{\ell}{4\sqrt{n} \cdot \log^3 n}\right] = \Pr_{i \leftarrow I_\sigma}\left[|q_\sigma - p_i| \leq (1/(20c_\varepsilon \cdot \log^3 n))(5c_\varepsilon \ell/\sqrt{n})\right] \quad (103)$$

$$\geq \Pr_{i \leftarrow I_\sigma}\left[|q_\sigma - p_i| \leq (4n^{-1/4} \cdot \sqrt{\log n})(5c_\varepsilon \ell/\sqrt{n})\right]$$

$$\geq \Pr_{i \leftarrow I_\sigma}\left[p_i \in (1 \pm 4n^{-1/4} \cdot \sqrt{\log n}) \cdot q_\sigma\right]$$

$$\geq 1 - 1/(2\sqrt{n}).$$

Thus, we get,

$$\Pr_{i \leftarrow I_\sigma}\left[\left(Q_{\hat{\ell},i}^s \leq c_\varepsilon \ell/\sqrt{n}\right) \wedge \left(\left|Q_{\hat{\ell},i}^s - q_\sigma\right| > \frac{\ell}{2\sqrt{n} \cdot \log^3 n}\right)\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[\left|Q_{\hat{\ell},i}^s - q_\sigma\right| > \frac{\ell}{2\sqrt{n} \cdot \log^3 n}\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[\left|q_\sigma - p_i\right| > \frac{\ell}{4\sqrt{n} \cdot \log^3 n}\right] + \Pr_{i \leftarrow I_\sigma}\left[\left|Q_{\hat{\ell},i}^s - p_i\right| > 1/n^2\right]$$

$$\leq 1/\sqrt{n}.$$

And similarly,

$$\Pr_{i \leftarrow I_\sigma}\left[\left(Q_{\hat{\ell},i}^s \geq c_\varepsilon \ell/\sqrt{n}\right) \wedge \left(q_\sigma \leq c_\varepsilon \ell/2\sqrt{n}\right)\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[\left|Q_{\hat{\ell},i}^s - q_\sigma\right| > \frac{\ell}{2\sqrt{n} \cdot \log^3 n}\right]$$

$$\leq 1/\sqrt{n}.$$

The case $q_\sigma \geq 5c_\varepsilon \ell/\sqrt{n}$. Lastly, assume the third case. Notice that,

$$\Pr_{i \leftarrow I_\sigma}\left[Q_{\hat{\ell},i}^s \leq c_\varepsilon \ell/\sqrt{n} \wedge \left|Q_{\hat{\ell},i}^s - q_\sigma\right| > \frac{\ell}{2\sqrt{n} \cdot \log^3 n}\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[Q_{\hat{\ell},i}^s \leq c_\varepsilon \ell/\sqrt{n}\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[p_i \leq 2c_\varepsilon \ell/\sqrt{n}\right] + \Pr_{i \leftarrow I_\sigma}\left[\left|Q_{\hat{\ell},i}^s - p_i\right| > 1/n^2\right]$$

$$\leq \Pr_{i \leftarrow I_\sigma}\left[p_i \leq 1/2 \cdot q_\sigma\right] + 1/n$$

$$\leq 1/\sqrt{n}$$

Where the last inequality holds by Equation (102). □

6 Reconstruction from Non-Boolean Hadamard Code

In this section, we prove Theorem 5.5, restated below.

Definition 6.1 (Inner-product estimator, restatement of Definition 5.4)**.** *Let $n, \ell \in \mathbb{N}$, let $\lambda > 0$ and let $z \in \{-1, 1\}^n$. A function $f \colon \{-1, 1\}^n \mapsto \mathbb{Z}$ is an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$ if*

$$\Pr_{r \leftarrow \{-1,1\}^n}[|f(r) - \langle z, r \rangle| < \ell] \geq \frac{\lambda \ell}{\sqrt{n}} \ .$$

Theorem 6.2 (Restatement of Theorem 5.5)**.** *There exists a PPTM P such that the following holds for large enough $n \in \mathbb{N}$: let $z \in \{-1, 1\}^n$, let $\lambda \geq 64$, and let f be an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$. Then with probability at least $(1 - \frac{4096}{\lambda^2})$ over $i \leftarrow [n]$, it holds that*

$$z_i \cdot \mathrm{E}_{r \leftarrow \{-1,1\}^n}[\mathsf{P}(i, z_{-i}, r, f(r), \ell)] \geq \frac{\lambda}{8n^{1.5}} \ ,$$

where the expectation is also over the randomness of P.

49

That is, Theorem 6.2 guarantees the existence of an efficient predictor P, whose output given (i, z_{-i}) and a single sample from an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$, is positively correlated with z_i (for most i's). We remark that Theorem 6.2 is tight up to a constant factor: for small enough constant λ (e.g., $\lambda = 1/4$) and not too large ℓ (i.e., $\ell \ll \sqrt{n}$), the function $f(r) := 0$ is an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$ (Holds by standard properties of the binomial distribution). Clearly, it is impossible to predict any information about z_i from z_{-i} and such f.

The proof of Theorem 6.2 is an easy corollary of the following lemma.

Definition 6.3. *For $k \in \mathbb{Z}$, let*

$$g_k(i, z_{-i}, r, a) := \begin{cases} (a - \langle z_{-i}, r_{-i} \rangle - k) \cdot r_i & a - \langle z_{-i}, r_{-i} \rangle \in \{k - 1, k + 1\} \\ 0. & otherwise \end{cases},$$

For $f \colon \{\text{-}1, 1\}^n \mapsto \mathbb{Z}$, let

$$g_k^f(i, z_{-i}, r) := g_k(i, z_{-i}, r, f(r)).$$

Lemma 6.4. *There exists an efficiently samplable distribution ensemble $\mathcal{K} = \{\mathcal{K}_{n,\ell}\}_{n,\ell \in \mathbb{N}}$ such that the following holds for every $\lambda \geq 64$, $\ell \in \mathbb{N}$ and sufficiently large $n \in \mathbb{N}$: let f be a (λ, ℓ)-estimator of $\langle z, \cdot \rangle$ and let $\left\{ g_k^f \right\}_{k \in \mathbb{Z}}$ be according to Definition 6.3. Then for every $z \in \{\text{-}1, 1\}^n$*

$$\Pr_{i \leftarrow [n]} \left[z_i \cdot \mathrm{E}_{k \leftarrow \mathcal{K}_{n,\ell}, r \leftarrow \{\text{-}1,1\}^n} \left[g_k^f(i, z_{-i}, r) \right] \geq \frac{\lambda}{8n^{1.5}} \right] \geq 1 - 4096/\lambda^2.$$

We prove Lemma 6.4 below, but first use it for proving Theorem 6.2.

Proving Theorem 6.2. We prove Theorem 5.5 by applying Lemma 6.4 with respect to the following PPTM P. Let g_k be according to Definition 6.3, and let $\{\mathcal{K}_{n,\ell}\}$ is the distribution ensemble guaranteed by Lemma 6.4.

Algorithm 6.5 (P).

Inputs: $i \in [n]$, $z_{-i} \in \{\text{-}1, 1\}^{n-1}$, $r \in \{\text{-}1, 1\}^n$, $a \in \mathbb{Z}$ and $\ell \in [\lfloor \sqrt{n} \rfloor]$.

Operation:

1. *Sample $k \leftarrow \mathcal{K}_{n,\ell}$.*

2. *Output $g_k(i, z_{-i}, r, a)$.*

Proof of Theorem 6.2. Immediate by applying Lemma 6.4 on Algorithm 6.5 (note that for every r, $\mathrm{E}[\mathsf{P}(i, z_{-i}, r, f(r), \ell)] = \mathrm{E}_{k \leftarrow \mathcal{K}_{n,\ell}} \left[g_k^f(i, z_{-i}, r) \right]$). $\qquad \square$

6.1 Proving Lemma 6.4

The proof of the lemma is an easy corollary of the following claims, which we prove in Section 6.1.1. Let λ, n, ℓ be as in the lemma statement, let $f \colon \{-1, 1\}^n \mapsto \mathbb{Z}$, and let $\left\{ g_k^f \right\}_{k \in \mathbb{Z}}$ be according to Definition 6.3, and fix $z \in \{-1, 1\}^n$. We use the following notation: for $k \in \mathbb{Z}$, let $\mathcal{G}_k := \{ r \in \{-1, 1\}^n \colon f(r) = \langle z, r \rangle + k \}$, i.e., those r on which $f(r)$ is off by k. Let $p_k := \Pr_{r \leftarrow \{-1,1\}^n}[r \in \mathcal{G}_k]$ and let $q_k := p_k + p_{-k}$. For $i \in [n]$, let $\mathcal{B}_k^i := \{ r \in \{-1, 1\}^n \colon f(r) = \langle z_{-i}, r_{-i} \rangle - z_i r_i + k \}$, i.e., those r's that are not in $\mathcal{G}_k$, but to refute that one needs to know z_i. By definition, for every i and k, it holds that

$$
g_k^f(i, z_{-i}, r) = \begin{cases} z_i & r \in \mathcal{G}_k \\ -z_i & r \in \mathcal{B}_i^k \\ 0 & \text{o.w.} \end{cases} \tag{104}
$$

Fix an (arbitrary) set of indices $\mathcal{I} \subseteq [n]$, and let $\mu_k := \frac{1}{|\mathcal{I}|} \cdot p_k \cdot \mathrm{E}_{r \leftarrow \mathcal{G}_k}[\langle z_{\mathcal{I}}, r_{\mathcal{I}} \rangle] = p_k \cdot \mathrm{E}_{i \leftarrow \mathcal{I}, r \leftarrow \mathcal{G}_k}[z_i \cdot r_i]$, i.e., the (normalized) correlation between $z_{\mathcal{I}}$ and $\mathcal{G}_k$. The first claim expresses, for every fixed k, the accuracy of g_k^f over $i \leftarrow \mathcal{I}$, in terms of p_j's and μ_j's.

Claim 6.6. *For every $k \in \mathbb{Z}$, it holds that*

$$
\mathrm{E}_{i \leftarrow \mathcal{I}, r \leftarrow \{-1,1\}^n} \left[z_i \cdot g_k^f(i, z_{-i}, r) \right] = \frac{1}{2} \cdot \underbrace{(2p_k - p_{k+2} - p_{k-2} + \mu_{k+2} - \mu_{k-2})}_{\alpha_k}.
$$

The following claims gradually proves the existence of a distribution $\mathcal{K}_{n,\ell}$ over the values of k, such that the expected value of α_k is large. Towards this end, the next claim expresses the expected value of α_k for $k \leftarrow [[-(m+1), m+1]]$, as a function of the q_j's and μ_j's.

Claim 6.7. *For every $m \in \mathbb{N} \cup \{0\}$, it holds that*

$$
\mathrm{E}_{k \leftarrow [[-(m+1), m+1]]}[\alpha_k] = \underbrace{\frac{1}{(2m+3)} \left(q_m + q_{m+1} - q_{m+2} - q_{m+3} + \sum_{j=0}^{3} (\mu_{m+j} - \mu_{-(m+j)}) \right)}_{\beta_m}.
$$

The next claim lower-bounds the expected value of β_m (defined in Claim 6.7) with respect to the following distribution.

Definition 6.8 (The distribution $\mathcal{M}_{s,t}$). *For $s, t \in \mathbb{N}$ with $s < t$, let $\mathcal{M}_{s,t}$ be the distribution over $[[s, t-1]]$ defined by $\mathcal{M}_{s,t}(m) := \frac{2m+3}{(t-s)(t+s+2)}$. (I.e., $\mathcal{M}_{s,t} \propto 2m+3$.)*

Claim 6.9. *Assume the size of $\mathcal{I}$ is larger than a universal constant, then for every $s, t \in \mathbb{Z}$ with $0 \leq s \leq t - 3$, and $t \leq \sqrt{n}$, it holds that*

$$
\mathrm{E}_{m \leftarrow \mathcal{M}_{s,t}}[\beta_m] \geq \underbrace{\frac{1}{(t-s)(t+s+2)} \cdot \left(q_s - (q_t + 2q_{t+1} + q_{t+2}) - \frac{32}{\sqrt{|\mathcal{I}|}} \right)}_{\gamma_{s,t}}.
$$

Finally, assume f is a good estimator, the next claim lower-bounds the expected value of $\gamma_{s,t}$ (defined in Claim 6.9) with respect to the following distribution.

Definition 6.10 (The distribution $\mathcal{P}_{\mathcal{S},\mathcal{T}}$). *For finite $\mathcal{S}, \mathcal{T} \subseteq \mathbb{N} \cup \{0\}$ with $\max(\mathcal{S}) < \min(\mathcal{T})$, let $\mathcal{P}_{\mathcal{S},\mathcal{T}}$ be the distribution over $\mathcal{S} \times \mathcal{T}$ defined by $\mathcal{P}_{\mathcal{S},\mathcal{T}}(s,t) := \frac{(t-s)(t+s+2)}{\sum_{(s',t') \in \mathcal{S} \times \mathcal{T}}(t'-s')(t'+s'+2)}$ (i.e., $\mathcal{P}_{\mathcal{S},\mathcal{T}}(s,t) \propto (t-s)(t+s+2)$).*

Claim 6.11. *Assume f is an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$ and that $|\mathcal{I}| \geq 4096n/\lambda^2$. Let $\mathcal{S} := [[0, \ell-1]]$, $\mathcal{T} := [[\ell+2, \sqrt{n}]]$, and let $\mathcal{P}_{\mathcal{S},\mathcal{T}}$ be according to Definition 6.10. Then*

$$\mathrm{E}_{(s,t) \leftarrow \mathcal{P}_{\mathcal{S},\mathcal{T}}}[\gamma_{s,t}] \geq \lambda/4n^{1.5}.$$

Given the above claims, we are now ready to prove Lemma 6.4

Proof of Lemma 6.4. Let λ, n, ℓ, z, f and $\{g_k^f\}_{k \in \mathbb{Z}}$ be as in the lemma statement. Since f is an (λ, ℓ)-estimator of $\langle z, \cdot \rangle$, it holds that $\ell \leq \sqrt{n}/\lambda < \sqrt{n} - 2$. Let $\mathcal{S} := [[0, \ell-1]]$, let $\mathcal{T} := [[\ell+2, \sqrt{n}]]$, and let $\mathcal{K}_{n,\ell}$ be the output distribution of the following random process:

Algorithm 6.12 (The distribution $\mathcal{K}_{n,\ell}$).

1. *Sample $(s,t) \leftarrow \mathcal{P}_{\mathcal{S},\mathcal{T}}$. (See Definition 6.10 for the definition of $\mathcal{P}_{\mathcal{S},\mathcal{T}}$).*

2. *Sample $m \leftarrow \mathcal{M}_{s,t}$. (See Definition 6.8 for the definition of $\mathcal{M}_{s,t}$).*

3. *Output $k \leftarrow [[-(m+1), m+1]]$.*

It is clear that $\mathcal{K}_{n,\ell}$ is samplable in polynomial time (by an algorithm getting $(1^n, 1^\ell)$ as input). By Claims 6.6, 6.7, 6.9 and 6.11, for any set $\mathcal{I} \subseteq [n]$ of size $4096n/\lambda^2$, it holds that

$$\mathrm{E}_{k \leftarrow \mathcal{K}_{n,\ell}, \, i \leftarrow \mathcal{I}, \, r \leftarrow \{-1,1\}^n}\left[z_i \cdot g_k^f(i, z_{-i}, r)\right] = \frac{1}{2} \cdot \mathrm{E}_{(s,t) \leftarrow \mathcal{P}_{\mathcal{S},\mathcal{T}}, m \leftarrow \mathcal{M}_{s,t}, k \leftarrow [[-(m+1),m+1]]}[\alpha_k] \quad (105)$$

$$= \frac{1}{2} \cdot \mathrm{E}_{(s,t) \leftarrow \mathcal{P}_{\mathcal{S},\mathcal{T}}, m \leftarrow \mathcal{M}_{s,t}}[\beta_m]$$

$$\geq \frac{1}{2} \cdot \mathrm{E}_{(s,t) \leftarrow \mathcal{P}_{\mathcal{S},\mathcal{T}}}[\gamma_{s,t}]$$

$$\geq \frac{\lambda}{8n^{1.5}}.$$

The first equality holds by Claim 6.6, the second equality by Claim 6.7, the first inequality by Claim 6.9, and the last inequality by Claim 6.11. To conclude the proof, consider the set of "bad" indices:

$$\mathcal{I} := \left\{ i \in [n] \colon \mathrm{E}_{k \leftarrow \mathcal{K}_{n,\ell}, \, r \leftarrow \{-1,1\}^n}\left[z_i \cdot g_k^f(i, z_{-i}, r)\right] < \frac{\lambda}{8n^{1.5}} \right\}$$

Assume towards a contradiction that the lemma does not hold, and therefore $|\mathcal{I}| \geq 4096n/\lambda^2$. Equation (105) yields that $\mathrm{E}_{k \leftarrow \mathcal{K}_{n,\ell}, \, i \leftarrow \mathcal{I}, \, r \leftarrow \{-1,1\}^n}\left[z_i \cdot g_k^f(i, z_{-i}, r)\right] \geq \frac{\lambda}{8n^{1.5}}$, in a contradiction to the definition of $\mathcal{I}$. $\square$

6.1.1 Proving Claims 6.6, 6.7, 6.9 and 6.11

Proving Claim 6.6.

Proof of Claim 6.6. Equation (104) yields that for every $i \in [n]$ and $k \in \mathbb{Z}$,

$$
\begin{aligned}
&\mathrm{E}_{r \leftarrow \{-1,1\}^n}\left[z_i \cdot g_k^f(i, z_{-i}, r)\right] \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (106) \\
&= \mathrm{Pr}_{r \leftarrow \{-1,1\}^n}[r \in \mathcal{G}_k] \cdot \mathrm{E}_{r \leftarrow \mathcal{G}_k}[z_i \cdot z_i] + \mathrm{Pr}_{r \leftarrow \{-1,1\}^n}\left[r \in \mathcal{B}_k^i\right] \cdot \mathrm{E}_{r \leftarrow \mathcal{B}_k^i}[z_i \cdot (-z_i)] \\
&= p_k - \mathrm{Pr}_{r \leftarrow \{-1,1\}^n}\left[r \in \mathcal{B}_k^i\right].
\end{aligned}
$$

Note that $r \in \mathcal{B}_i^k$ if and only if: (1) $r \in \mathcal{G}_{k+2}$ and $z_i \cdot r_i = -1$, or (2) $r \in \mathcal{G}_{k-2}$ and $z_i \cdot r_i = 1$. Therefore, for every $k \in \mathbb{Z}$

$$
\begin{aligned}
&\mathrm{E}_{i \leftarrow \mathcal{I}}\left[\mathrm{Pr}_{r \leftarrow \{-1,1\}^n}\left[r \in \mathcal{B}_k^i\right]\right] \qquad\qquad\qquad\qquad\qquad\qquad\qquad (107) \\
&= p_{k+2} \cdot \mathrm{Pr}_{i \leftarrow \mathcal{I}, r \leftarrow \mathcal{G}_{k+2}}[z_i \cdot r_i = -1] + p_{k-2} \cdot \mathrm{Pr}_{i \leftarrow \mathcal{I}, r \leftarrow G^{k-2}}[z_i \cdot r_i = 1] \\
&= p_{k+2} \cdot \frac{1}{|\mathcal{I}|} \cdot \mathrm{E}_{r \leftarrow \mathcal{G}_{k+2}}[|\{i \in \mathcal{I} \colon z_i \cdot r_i = -1\}|] + p_{k-2} \cdot \frac{1}{|\mathcal{I}|} \cdot \mathrm{E}_{r \leftarrow \mathcal{G}_{k-2}}[|\{i \in \mathcal{I} \colon z_i \cdot r_i = 1\}|] \\
&= p_{k+2} \cdot \frac{1 - \frac{1}{|\mathcal{I}|} \cdot \mathrm{E}_{r \leftarrow \mathcal{G}_{k+2}}[\langle z_{\mathcal{I}}, r_{\mathcal{I}}\rangle]}{2} + p_{k-2} \cdot \frac{1 + \frac{1}{|\mathcal{I}|} \cdot \mathrm{E}_{r \leftarrow \mathcal{G}_{k-2}}[\langle z_{\mathcal{I}}, r_{\mathcal{I}}\rangle]}{2} \\
&= \frac{1}{2} \cdot (p_{k+2} + p_{k-2} - \mu_{k+2} + \mu_{k-2}).
\end{aligned}
$$

The penultimate equality holds since since $|\{i \in \mathcal{I} \colon z_i \cdot r_i = 1\}| = \frac{|\mathcal{I}| + \langle z_{\mathcal{I}}, r_{\mathcal{I}}\rangle}{2}$. The proof now follows by Equations (106) and (107). $\qquad\square$

Proving Claim 6.7.

Proof of Claim 6.7. Note that

$$
\begin{aligned}
\mathrm{E}_{k \leftarrow [[-(m+1), m+1]]}[\alpha_k] &= \mathrm{E}_{k \leftarrow [[-(m+1), m+1]]}[2p_k - p_{k+2} - p_{k-2} + \mu_{k+2} - \mu_{k-2}] \\
&= \frac{1}{2m+3} \sum_{k=-(m+1)}^{m+1} (2p_k - p_{k+2} - p_{k-2} + \mu_{k+2} - \mu_{k-2}).
\end{aligned}
$$

The proof of the claim now follows since

$$
\sum_{k=-(m+1)}^{m+1} (2p_k - p_{k+2} - p_{k-2}) = p_{-(m+1)} + p_{-m} + p_m + p_{m+1} - p_{-(m+3)} - p_{-(m+2)} - p_{m+2} - p_{m+3}
$$

$$
= q_m + q_{m+1} - q_{m+2} - q_{m+3},
$$

and since

$$
\sum_{k=-(m+1)}^{m+1} (\mu_{k+2} - \mu_{k-2}) = \sum_{j=0}^{3}(\mu_{m+j} - \mu_{-(m+j)}).
$$

$\qquad\square$

Proving Claim 6.9.

Proof of Claim 6.9. Let $\widetilde{\mu}_k := \frac{1}{|\mathcal{I}|} \cdot p_k \cdot \mathrm{E}_{r \leftarrow \mathcal{G}_k}[|\langle z_\mathcal{I}, r_\mathcal{I} \rangle|]$. Compute

$$
\mathrm{E}_{m \leftarrow \mathcal{M}_{s,t}}[\beta_m] \tag{108}
$$

$$
= \mathrm{E}_{m \leftarrow \mathcal{M}_{s,t}}\left[\frac{1}{2m+3}\left(q_m + q_{m+1} - q_{m+2} - q_{m+3} + \sum_{j=0}^{3}(\mu_{m+j} - \mu_{-(m+j)}) \right) \right]
$$

$$
= \frac{1}{(t-s)(t+s+2)} \cdot \sum_{m=s}^{t-1}\left(q_m + q_{m+1} - q_{m+2} - q_{m+3} + \sum_{j=0}^{3}(\mu_{m+j} - \mu_{-(m+j)}) \right)
$$

$$
= \frac{1}{(t-s)(t+s+2)} \cdot \left(q_s + 2q_{s+1} + q_{s+2} - q_t - 2q_{t+1} - q_{t+2} + \sum_{m=s}^{t-1}\sum_{j=0}^{3}(\mu_{m+j} - \mu_{-(m+j)}) \right)
$$

$$
\geq \frac{1}{(t-s)(t+s+2)} \cdot \left(q_s - (q_t + 2q_{t+1} + q_{t+2}) - 8 \cdot \sum_{m=-(s+3)}^{t+2} \widetilde{\mu}_m \right).
$$

The inequality holds since $q_j \geq 0$, for every j, and since $|\mu_j| \leq \widetilde{\mu}_j$. The third equality holds since

$$
\sum_{m=s}^{t-1}(q_m + q_{m+1} - q_{m+2} - q_{m+3}) = \sum_{m=s}^{t-1}(q_m - q_{m+2}) + \sum_{m=s}^{t-1}(q_{m+1} - q_{m+3})
$$

$$
= (q_s + q_{s+1} - q_t - q_{t+1}) + (q_{s+1} + q_{s+2} - q_{t+1} - q_{t+2})
$$

$$
= q_s + 2q_{s+1} + q_{s+2} - q_t - 2q_{t+1} - q_{t+2}.
$$

Let $\mathcal{G}' := \bigcup_{k=-(s+3)}^{t+2} \mathcal{G}_k$, and observe that

$$
\sum_{m=-(s+3)}^{t+2} \widetilde{\mu}_m = \frac{1}{|\mathcal{I}|} \cdot \Pr_{r \leftarrow \{-1,1\}^n}\left[r \in \mathcal{G}' \right] \cdot \mathrm{E}_{r \leftarrow \mathcal{G}'}[|\langle z_\mathcal{I}, r_\mathcal{I} \rangle|] \leq \frac{4}{\sqrt{|\mathcal{I}|}} \tag{109}
$$

The inequality holds by applying Proposition 3.26 over the event $\mathcal{G}'$, noting that $\langle z_\mathcal{I}, r_\mathcal{I} \rangle$, for $r \leftarrow \{-1,1\}^n$, is a sum of $|\mathcal{I}|$ uniform and independent random variables over $\{-1,1\}$.[32] $\qquad\square$

Proving Claim 6.11.

Proof of Claim 6.11. Recall that f is a (λ, ℓ)-estimator for $\lambda \geq 64$, and that $\mathcal{S} = [[0, \ell - 1]]$ and $\mathcal{T} = [[\ell + 2, \sqrt{n}]]$. Since $q_k = \Pr_{r \leftarrow \{-1,1\}^n}[f(r) - \langle z, r \rangle = k] + \Pr_{r \leftarrow \{-1,1\}^n}[f(r) - \langle z, r \rangle = -k]$, it holds that

$$
\mathrm{E}_{s \leftarrow \mathcal{S}}[q_s] = \frac{1}{|\mathcal{S}|} \cdot \sum_{s=0}^{\ell-1} q_s \geq \frac{1}{\ell} \cdot \Pr_{r \leftarrow \{-1,1\}^n}[|f(r) - \langle z, r \rangle| < \ell] \geq \lambda/\sqrt{n}. \tag{110}
$$

---

[32] The event $\mathcal{G}'$ is defined over a larger probability space that include also $r_{-\mathcal{I}}$. Yet, for every fixing of $r_{-\mathcal{I}}$, we can apply Proposition 3.26 over the event $\{r_\mathcal{I} : r \in \mathcal{G}'\}$.

On the other hand, since $q_k \leq 2$ for every k, it holds that

$$\mathrm{E}_{t \leftarrow \mathcal{T}}[q_t + 2q_{t+1} + q_{t+2}] = \frac{1}{|\mathcal{T}|} \cdot \sum_{t \in \mathcal{T}} (q_t + 2q_{t+1} + q_{t+2}) \leq \frac{1}{\sqrt{n} - \ell - 1} \cdot 8 \leq \frac{16}{\sqrt{n}} \leq \frac{\lambda}{4\sqrt{n}} \quad (111)$$

The first inequality holds since, by assumption, $\ell \leq \sqrt{n}/\lambda < \sqrt{n}/2 - 1$. Compute

$$\mathrm{E}_{(s,t) \leftarrow \mathcal{P}_{\mathcal{S},\mathcal{T}}}[\gamma_{s,t}] = \mathrm{E}_{(s,t) \leftarrow \mathcal{P}_{\mathcal{S},\mathcal{T}}} \left[\frac{1}{(t-s)(t+s+2)} \cdot \left(q_s - (q_t + 2q_{t+1} + q_{t+2}) - \frac{32}{\sqrt{|\mathcal{I}|}} \right) \right]$$

$$= \frac{1}{\sum_{(s,t) \in \mathcal{S} \times \mathcal{T}} (t-s)(t+s+2)} \cdot \sum_{(s,t) \in \mathcal{S} \times \mathcal{T}} \left(q_s - (q_t + 2q_{t+1} + q_{t+2}) - \frac{32}{\sqrt{|\mathcal{I}|}} \right)$$

$$= \frac{|\mathcal{S}||\mathcal{T}|}{\sum_{(s,t) \in \mathcal{S} \times \mathcal{T}} (t-s)(t+s+2)} \cdot \left(\mathrm{E}_{s \leftarrow \mathcal{S}}[q_s] - \mathrm{E}_{t \leftarrow \mathcal{T}}[q_t + 2q_{t+1} + q_{t+2}] - \frac{32}{\sqrt{|\mathcal{I}|}} \right)$$

$$\geq \frac{1}{\mathrm{E}_{(s,t) \leftarrow \mathcal{S} \times \mathcal{T}}[(t-s)(t+s+2)]} \cdot \left(\frac{\lambda}{\sqrt{n}} - \frac{\lambda}{4\sqrt{n}} - \frac{\lambda}{2\sqrt{n}} \right).$$

The last inequality holds follows by Equations (110) and (111), since, by assumption, $|\mathcal{I}| \geq 4096n/\lambda^2$. This concludes the proof since $\mathrm{E}_{(s,t) \leftarrow \mathcal{S} \times \mathcal{T}}[(t-s)(t+s+2)] \leq \mathrm{E}_{t \leftarrow \mathcal{T}}[t(t+2)] \leq n$. $\quad \square$

7 Key-Agreement Amplification over Large Alphabet

In this section we prove our amplification result for key-agreement protocol over large alphabet that we used in Section 4, restated below.

Theorem 7.1 (Key-agreement amplification over large alphabet, Theorem 4.5 restated). *There exists an oracle-aided two-party protocol Φ such that the following holds for every $\alpha \in (0,1]$. Let C be an n-size, $(\alpha, \alpha/2^{15})$-key-agreement-with-equality-leakage channel. Then the channel $\widetilde{C}$ induced by $\Phi^C(\kappa, n, \alpha)$ is a single-bit, $(1 - 2^{-\kappa}, 1/2 + 2^{-\kappa})$-key agreement. The running time of $\Phi^C(\kappa, n, \alpha)$ is $\mathrm{poly}(\kappa, n, 1/\alpha)$.*

Furthermore, the security proof is black-box: there exists a PPT oracle-aided E such that for every n-size channel C with α-agreement, and every algorithm $\widetilde{\mathsf{E}}$ that violates the $(1/2 + 2^{-\kappa} + \beta)$-equality-leakage of $\widetilde{C}$, for some $\beta > 0$, algorithm $\mathsf{E}^{C,\widetilde{\mathsf{E}}}(\kappa, n, \alpha, \beta)$ violates the equality-leakage of C, and runs in time $\mathrm{poly}(\kappa, n, 1/\alpha, 1/\beta)$

That is, given an n-size channel whose agreement is better than its equality-leakage, we construct a (single-bit) key-agreement channel. Our amplification protocol is stated below.

Protocol 7.2 ($\Pi_{\mathcal{H}}^{C} = (\mathsf{A}, \mathsf{B})$)**.**

Parameter: ensemble of function families $\mathcal{H} = \{\mathcal{H}_{n,m} = \{h \colon \{0,1\}^n \mapsto \{0,1\}^m\}\}_{n,m \in \mathbb{N}}$.

Inputs: $n, m \in \mathbb{N}$.

Oracle: an n-size channel C_{XYT}.

Operation:

1. *The parties (jointly) call C_{XYT}, where A gets x, B gets y and t is the common output.*

2. *A samples $h \leftarrow \mathcal{H}_{n,m}$, $r \in \{0,1\}^n$ and sends $(h, h(x), r)$ to B.*

3. *B informs A whether $h(y) = h(x)$.*
   If positive, A outputs $o_{\mathsf{A}} = \langle r, x \rangle \bmod 2$, and B outputs $o_{\mathsf{B}} = \langle r, y \rangle \bmod 2$.
   Otherwise, both parties aborts.

It is clear that if the function family ensemble $\mathcal{H}$ is efficient, i.e., sampling and evaluation time is polynomial in n and m, then so is $\Pi_{\mathcal{H}}^{C}$. For the security part, we prove that if $\mathcal{H}_{n,m}$ is pairwise independent, then the protocol is a single-bit (weakly) secure key agreement.

Definition 7.3 (Pairwise independent hash functions). *A function family $\mathcal{H} = \{h \colon \{0,1\}^n \to \{0,1\}^m\}$ is* pairwise independent *if for every $x_1 \neq x_2 \in \{0,1\}^n$ and $y_1, y_2 \in \{0,1\}^m$, it holds that $\Pr_{h \leftarrow \mathcal{H}}[h(x_1) = y_1 \wedge h(x_2) = y_2] = 2^{-2m}$.*

It is well-known. cf., [35], that efficient ensemble of pairwise independent hash functions exits. The crux of out proof for Theorem 7.1 is in the next lemma.

Lemma 7.4 (alphabet reduction). *Let $\alpha \in (0,1]$, let $m := \lceil \log(1/\alpha) \rceil + 8$, let C be an n-size channel, and let $\widehat{C}$ denote the channel induced by a random execution of $\Pi_{\mathcal{H}}^{C}(n,m)$ conditioned on non abort. If C is a $(\alpha, \alpha/2^{15})$-key agreement with equality-leakage, and $\mathcal{H}_{n,m}$ is pairwise independent, then $\widehat{C}$ is $(0.9, 0.8)$-key-agreement-with-equality-leakage.*

Furthermore, the security proof is black-box: there exists an oracle-aided E such that for every n-size channel C with α-agreement, and an algorithm $\widetilde{\mathsf{E}}$ violating the equality-leakage of $\widehat{C}$, algorithm $\mathsf{E}^{C, \widetilde{\mathsf{E}}}(n, m, \alpha, \cdot)$ violates the equality-leakage of C and runs in time $\mathrm{poly}(n, m, 1/\alpha)$.

We prove Lemma 7.4 below, but first use it for proving Theorem 7.1.

Proving Theorem 7.1.

Proof of Theorem 7.1. Let $\mathcal{H}$ be an efficient ensemble of pairwise independent hash families, and let $\Pi_{\mathcal{H}}$ be the oracle-aided protocol from Protocol 7.2. Let $\widehat{\Pi}$ be the protocol that given oracle access to an n-size channel C, and inputs κ, α, sets $m = \lceil \log(\lceil 1/\alpha \rceil) \rceil + 8$ and does the following: the parties repetitively interact in $\Pi_{\mathcal{H}}^{C}(n,m)$ until not abort, up to $5/\alpha$ fail attempts. The parties output their output in the no aborting execution of $\Pi_{\mathcal{H}}^{C}$, or 0 if all executions have aborted.

Let C' be the channel induced by a random execution of $\widehat{\Pi}$. By Lemma 7.4, if C has α-agreement, C' has agreement at least 0.9. Let B be the event that all attempts made by the parties

have failed. Then by construction of $\widehat{\Pi}$ and the agreement of C, it holds that

$$\Pr[B] \le (1 - \alpha)^{5/\alpha} \le e^{-5}$$

Assuming that C is also $\alpha/2^{15}$-secure with equality-leakage, then by Lemma 7.4 and the above bound on $\Pr[B]$, C' is $0.8 + e^{-5} < 0.81$-secure with equality-leakage. Hence, by applying known amplification for single-bit channels, in particular, applying Theorem 3.22 on C' with parameters $\alpha = 0.9$ and $\delta = 0.81$, and input 1^κ, we get the required key-agreement protocol Φ.

Finally, we note that since both Lemma 7.4 and theorem 3.22 have black-box security reductions, then so is the security of Φ. □

7.1 Proving Lemma 7.4

In this section we prove Lemma 7.4. We make use of a weak version of the Goldreich-Levin theorem [12].

Theorem 7.5 (Goldreich-Levin, [12]). *There exists an oracle-aided* PPT *algorithm* Dec *such that the following holds: for every* $n \in \mathbb{N}$, *algorithm* $\mathsf{D} : \{0,1\}^n \to \{0,1\}$, *and* $x \in \{0,1\}^n$ *that satisfy*

$$\Pr_{r \leftarrow \{0,1\}^n}[\mathsf{D}(r) = (\langle x, r \rangle \mod 2)] \ge 3/4 + 0.01,$$

it holds that $\Pr[\mathrm{Dec}^{\mathsf{D}} = x] \ge 0.99$.

In the rest of this section we prove Lemma 7.4. Let $\alpha, s, m, \mathcal{H}, \Pi_{\mathcal{H}}^C$ be as in Lemma 7.4. We associate the following random variables with a random execution of $\Pi_{\mathcal{H}}^C(n, m)$. Let (X, Y, T) be the output of the call to C_{XYT} done by the parties, let R and H be the value of r and h sent in the execution, and let $O_\mathsf{A}, O_\mathsf{B}$ be the local outputs of A and B, respectively. Let NoAbort be the event that the parties did not abort during the execution, and $T' := (T, H, H(X), R)$. Note that conditioned on NoAbort, T' fully describes the transcript of the protocol. Finally, let $\widehat{T} = (T, H, H(X))$ denote the prefix of T' (without the randomness R) such that $T' = (\widehat{T}, R)$.

We will make use of the following claims:

The first claim bounds the agreement probability under the event NoAbort.

Claim 7.6. $\Pr[O_\mathsf{A} = O_\mathsf{B} \mid \mathsf{NoAbort}] \ge \alpha/(\alpha + 2^{-m})$.

The second claim essentially bounds the leakage of the protocol. This is done with a reduction to the security of C.

Claim 7.7. *There exists an oracle-aided algorithm* E_{KA} *such that the following holds. For every algorithm* $\mathsf{D}\colon \mathrm{Supp}(T') \to \{0,1\}$ *such that* $\Pr[\mathsf{D}(T') = O_\mathsf{A} \mid O_\mathsf{A} = O_\mathsf{B}, \mathsf{NoAbort}] > 0.8$, *it holds that* $\Pr[\mathsf{E}_{KA}^{\mathsf{D}}(T) = X \mid X = Y] > \alpha \cdot 2^{-15}$.

We prove Claims 7.6 and 7.7 below, but first we use Claims 7.6 and 7.7 in order to prove Lemma 7.4, which is now follows immediately.

Proof of Lemma 7.4. Recall that

$$m = \lceil \log(1/\alpha) \rceil + 8 \tag{112}$$

57

Thus, by Claim 7.6 it follows that,

$$\Pr[O_\mathsf{A} = O_\mathsf{B} \mid \mathsf{NoAbort}] \geq \alpha/(\alpha + 2^{-m}) \geq 1/(1 + 2^{-8}) > 0.9.$$

By Claim 7.7 and the $\alpha \cdot 2^{-15}$-secrecy with equality-leakage of C, we get that $\widehat{C}$ is 0.8-secure with equality-leakage. Since Claim 7.7 is a reduction, the lemma holds. □

We now prove Claims 7.6 and 7.7.

Proving Claim 7.6. We start with the proof of Claim 7.6.

Proof of Claim 7.6. By construction we get that,

$$\Pr[O_\mathsf{A} = O_\mathsf{B}|\mathsf{NoAbort}] = \Pr[O_\mathsf{A} = O_\mathsf{B}|H(X) = H(Y)] \geq \Pr[X = Y|H(X) = H(Y)]. \qquad (113)$$

Let $\beta := \Pr[X = Y] \geq \alpha$, and note that since $\mathcal{H}$ is pairwise independent, it holds that for $\Pr[H(X) = H(Y) \mid X \neq Y] = 2^{-m}$. Thus, it holds that,

$$
\begin{aligned}
\Pr[X = Y|H(X) = H(Y)] &= \frac{\Pr[X = Y]}{\Pr[H(X) = H(Y)]} \qquad\qquad (114)\\
&= \frac{\Pr[X = Y]}{\Pr[X = Y] + \Pr[H(X) = H(Y), X \neq Y]}\\
&= \frac{\Pr[X = Y]}{\Pr[X = Y] + \Pr[X \neq Y] \cdot 2^{-m}}\\
&= \frac{\beta}{\beta + (1 - \beta) \cdot 2^{-m}}\\
&\geq \frac{\beta}{\beta + 2^{-m}}\\
&\geq \alpha/(\alpha + 2^{-m}),
\end{aligned}
$$

where the last inequality holds since $x/(x + 2^{-m})$ is a monotonic increasing function for $x \geq 0$. We conclude the claim by combining Equations (113) and (114). □

Proving Claim 7.7. To prove Claim 7.7, we will use the next two claims. The first claim will be useful in order to bound the probability of an adversary to guess X, after seeing (part of) the transcript of Protocol 7.2.

Claim 7.8. *There exists an oracle-aided* PPTM E *such that the following holds. For every algorithm* $\widehat{\mathsf{E}} : \mathrm{Supp}(\widehat{T}) \to \{0,1\}^n$ *such that* $\Pr\left[\widehat{\mathsf{E}}(\widehat{T}) = X|X = Y\right] \geq 2^m \cdot \alpha \cdot 2^{-15}$, *it holds that* $\Pr\left[\mathsf{E}^{\widehat{\mathsf{E}}}(1^n, 1^m, T) = X|X = Y\right] \geq \alpha \cdot 2^{-15}$

The second claim bounds the probability that $X \neq Y$ under the event that the parties agreed on the output.

Claim 7.9. $\Pr[X \neq Y|O_\mathsf{A} = O_\mathsf{B}, \mathsf{NoAbort}] < 2^{-m}/\alpha$.

Proof of Claim 7.9.

$$\begin{aligned}
\Pr[X \neq Y | O_\mathsf{A} = O_\mathsf{B}, \mathsf{NoAbort}] &= \Pr[X \neq Y | O_\mathsf{A} = O_\mathsf{B}, H(X) = H(Y)] \\
&\leq \frac{\Pr[O_\mathsf{A} = O_\mathsf{B}, H(X) = H(Y) | X \neq Y]}{\Pr[O_\mathsf{A} = O_\mathsf{B}, H(X) = H(Y)]} \\
&\leq \frac{2^{-m}}{\alpha},
\end{aligned}$$

where the last inequality holds since $\mathcal{H}$ is pairwise independent hash function, and $\Pr[O_\mathsf{A} = O_\mathsf{B}, H(X) = H(Y)] \geq \Pr[X = Y] = \alpha$. $\qquad\square$

We prove Claim 7.8 below, but first we use it in order to prove Claim 7.7.

Proof of Claim 7.7. Let D be as in Claim 7.7. That is,

$$\Pr\big[\mathsf{D}(T') = O_\mathsf{A} | \mathsf{NoAbort}, O_\mathsf{A} = O_\mathsf{B}\big] > 0.8 \tag{115}$$

Since the event $\{X = Y\}$ implies the event $\{\mathsf{NoAbort}, O_\mathsf{A} = O_\mathsf{B}\}$, it holds that,

$$\begin{aligned}
\Pr\big[\mathsf{D}(T') = O_\mathsf{A} | \mathsf{NoAbort}, O_\mathsf{A} = O_\mathsf{B}\big] &\leq \Pr\big[\mathsf{D}(T') = O_\mathsf{A} | X = Y\big] + \Pr[X \neq Y | \mathsf{NoAbort}, O_\mathsf{A} = O_\mathsf{B}] \\
&\leq \Pr\big[\mathsf{D}(T') = O_\mathsf{A} | X = Y\big] + 2^{-m}/\alpha,
\end{aligned}$$

where the second inequality holds by Claim 7.9. Thus, by our choice of m, we get that

$$\Pr\big[\mathsf{D}(T') = O_\mathsf{A} | X = Y\big] > 0.79 \tag{116}$$

Recall that $T' = (\widehat{T}, R)$. It follows by construction that conditioned on the event $\{X = Y\}$, the randomness R is uniform and independent of $\widehat{T}$. We now define the set of "good transcripts" $\mathcal{G}$ for the algorithm D:

$$\mathcal{G} = \left\{ \widehat{t} \in \mathrm{Supp}(\widehat{T}) \colon \Pr\big[\mathsf{D}(\widehat{t}, R) = O_\mathsf{A} | X = Y, \widehat{T} = \widehat{t}\big] \geq 3/4 + 0.01 \right\}.$$

We next show by an averaging argument over Equation (116) that $\Pr\big[\widehat{T} \in \mathcal{G} \mid X = Y\big] \geq 1/8$.

Indeed, assume for contradiction that $\Pr\big[\widehat{T} \in \mathcal{G} \mid X = Y\big] < 1/8$. Then

$$\begin{aligned}
\Pr\big[\mathsf{D}(T') = O_\mathsf{A} | X = Y\big] &= \Pr\big[\mathsf{D}(T') = O_\mathsf{A} | X = Y, \widehat{T} \in \mathcal{G}\big] \cdot \Pr\big[\widehat{T} \in \mathcal{G} | X = Y\big] \\
&\quad + \Pr\big[\mathsf{D}(T') = O_\mathsf{A} | X = Y, \widehat{T} \notin \mathcal{G}\big] \cdot \Pr\big[\widehat{T} \notin \mathcal{G} | X = Y\big] \\
&< 1 \cdot 1/8 + (3/4 + 0.01) \cdot (1 - 1/8) = 0.79.
\end{aligned}$$

Which is a contradiction to Equation (116).

Let Dec be the algorithm promised by Theorem 7.5, and for $\widehat{t} \in \mathrm{Supp}(\widehat{T})$, let $\mathsf{D}_{\widehat{t}}(r) := \mathsf{D}(\widehat{t}, r)$. It follows by Theorem 7.5 and the definition of $\mathcal{G}$ that,

$$\Pr\big[\mathrm{Dec}^{\mathsf{D}_{\widehat{T}^*}} = X | X = Y, \widehat{T}^* \in \mathcal{G}\big] \geq 0.99.$$

Combining the above, we get that,

$$\Pr\left[\mathrm{Dec}^{\mathsf{D}_{\widehat{T}}} = X | X = Y\right] \geq \Pr\left[\mathrm{Dec}^{\mathsf{D}_{\widehat{T}}} = X | X = Y, \widehat{T} \in \mathcal{G}\right] \cdot \Pr\left[\widehat{T} \in \mathcal{G} | X = Y\right] \qquad (117)$$

$$\geq 0.99 \cdot 1/8$$

$$\geq 0.1$$

$$> 2^m \cdot \alpha \cdot 2^{-15},$$

where the last inequality holds by the choise of m. Finally, let $\widehat{\mathsf{E}}^{\mathsf{D}}(\widehat{t}) := \mathrm{Dec}^{\mathsf{D}_{\widehat{t}}}$ and let E be the algorithm promised by Claim 7.8. By Equation (117) and Claim 7.8 we get that $\Pr\left[\mathsf{E}^{\widehat{\mathsf{E}}^{\mathsf{D}}}(1^n, 1^m, T) = X | X = Y\right] > \alpha \cdot 2^{-15}$. Thus the claim holds with respect to $\mathsf{E}_{KA}^{(\cdot)} := \mathsf{E}^{\widehat{\mathsf{E}}^{(\cdot)}}$. $\qquad\square$

Proving Claim 7.8. In order to prove Claim 7.8, consider the following algorithm.

Algorithm 7.10 ($\mathsf{E}^{\widehat{\mathsf{E}}}$).

Input: 1^n, 1^m, $t \in \mathrm{Supp}(T)$.

Oracle: An algorithm, $\widehat{\mathsf{E}} : \mathrm{Supp}(\widehat{T}) \to \{0,1\}^n$.

Operation:

  1. *Sample* $h \leftarrow \mathcal{H}_{n,m}$, $v \leftarrow \{0,1\}^m$

  2. *Output* $\widehat{\mathsf{E}}(t, h, v)$.

Proof of Claim 7.8. Let $\widehat{\mathsf{E}}$ be as in Claim 7.8. That is,

$$\Pr\left[\widehat{\mathsf{E}}(\widehat{T}) = X | X = Y\right] > 2^m \cdot \alpha/2^{15}. \qquad (118)$$

We show that the above inequality implies that the algorithm $\mathsf{E}_{n,m} := \mathsf{E}^{\widehat{\mathsf{E}}}(1^n, 1^m, \cdot)$ defined in *Algorithm* 7.10 fulfills the requirement of the claim. That is, we want to show that:

$$\Pr[\mathsf{E}(T) = X | X = Y] > \alpha/2^{15}. \qquad (119)$$

First note that by the construction, $\mathsf{E}_{n,m}(T) = \widehat{\mathsf{E}}(T, H, V)$ (where H and V are sampled independently at random) and recall that by definition $\widehat{T} = (T, H, H(X))$. Consequently, $\widehat{\mathsf{E}}(T, H, V)|_{V=H(X)} \equiv \widehat{\mathsf{E}}(\widehat{T})$ and $\Pr[H(X) = V | X = Y] = 2^{-m}$, and it follows that:

$$\Pr[\mathsf{E}_{n,m}(T) = X | X = Y] = \Pr\left[\widehat{\mathsf{E}}(T, H, V) = X | X = Y\right]$$

$$\geq \Pr\left[\widehat{\mathsf{E}}(T, H, V) = X | X = Y, H(X) = V\right] \cdot \Pr[H(X) = V | X = Y]$$

$$\geq \Pr\left[\widehat{\mathsf{E}}(\widehat{T}) = X | X = Y\right] \cdot 2^{-m},$$

$$> 2^m \cdot \alpha/2^{15} \cdot 2^{-m}$$

$$= \alpha/2^{15}.$$

Where the inequality follows by Equation (118). Thus Equation (119) holds. $\qquad\square$

Acknowledgment

We are grateful to Kobbi Nissim, Eran Omri and Ronen Shaltiel for very useful discussions.

References

[1] D. R. Barr and E. T. Sherrill. Mean and variance of truncated normal distributions. *The American Statistician*, 53(4):357–361, 1999. 63

[2] A. Beimel, K. Nissim, and E. Omri. Distributed private data analysis: Simultaneously solving how and what. In *Annual International Cryptology Conference (CRYPTO)*, pages 451–468, 2008. 2, 17

[3] M. Bun, Y.-H. Chen, and S. Vadhan. Separating computational and statistical differential privacy in the client-server model. In *Theory of Cryptography (TCC)*, pages 607–634, 2016. 5

[4] C. Calabro. *The exponential complexity of satisfiability problems*. PhD thesis, UC San Diego, 2009. 65

[5] T. H. Chan, E. Shi, and D. Song. Optimal lower bound for differentially private multi-party aggregation. In *European Symposium on Algorithms*, pages 277–288, 2012. 5

[6] I. Dinur and K. Nissim. Revealing information while preserving privacy. In *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 202–210, 2003. 4, 9, 13

[7] C. Dwork and K. Nissim. Privacy-preserving datamining on vertically partitioned databases. In *Annual International Cryptology Conference (CRYPTO)*, pages 528–544, 2004. 1

[8] C. Dwork and S. Yekhanin. New efficient attacks on statistical disclosure control mechanisms. In *Annual International Cryptology Conference (CRYPTO)*, pages 469—-480, 2008. 13

[9] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor. Our data, ourselves: Privacy via distributed noise generation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pages 486–503, 2006. 2

[10] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography (TCC)*, pages 265–284, 2006. 1, 16

[11] C. Dwork, F. McSherry, and K. Talwar. The price of privacy and the limits of lp decoding. In *Annual ACM Symposium on Theory of Computing (STOC)*, pages 85–94, 2007. 13

[12] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *Annual ACM Symposium on Theory of Computing (STOC)*, pages 25–32, 1989. 57

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

[14] V. Goyal, D. Khurana, I. Mironov, O. Pandey, and A. Sahai. Do distributed differentially-private protocols require oblivious transfer? In *Automata, Languages and Programming, 24th International Colloquium (ICALP)*, pages 29:1–29:15, 2016. 5

[15] A. Groce, J. Katz, and A. Yerukhimovich. Limits of computational differential privacy in the client/server setting. In *Theory of Cryptography (TCC)*, pages 417–431, 2011. 5

[16] I. Haitner, M. Nguyen, S. J. Ong, O. Reingold, and S. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM Journal on Computing*, 39(3):1153–1218, 2009. 6

[17] 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. Preliminary version in *STOC'10*. 4

[18] I. Haitner, E. Omri, and H. Zarosim. Limits on the usefulness of random oracles. *Journal of Cryptology*, 29(2):283–335, 2016. 6

[19] I. Haitner, N. Makriyannis, and E. Omri. On the complexity of fair coin flipping. In *Theory of Cryptography (TCC)*, pages 539–562, 2018. 6

[20] I. Haitner, K. Nissim, E. Omri, R. Shaltiel, and J. Silbak. Computational two-party correlation: A dichotomy for key-agreement protocols. In *Annual Symposium on Foundations of Computer Science (FOCS)*, pages 136–147, 2018. 5

[21] I. Haitner, N. Mazor, R. Shaltiel, and J. Silbak. Channels of small log-ratio leakage and characterization of two-party differentially private computation. In *Theory of Cryptography (TCC)*, pages 531–560, 2019. 2, 5

[22] I. Haitner, K. Nissim, E. Omri, R. Shaltiel, and J. Silbak. Computational two-party correlation: A dichotomy for key-agreement protocols. *SIAM Journal on Computing*, 49(6):1041–1082, 2020. 6

[23] D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen. On robust combiners for oblivious transfer and other primitives. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pages 96–113. Springer, 2005. 21

[24] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999. 6

[25] T. Holenstein. *Strengthening key agreement using hard-core sets*. PhD thesis, ETH Zurich, 2006. 20

[26] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989. 6

[27] A. McGregor, I. Mironov, T. Pitassi, O. Reingold, K. Talwar, and S. Vadhan. The limits of two-party differential privacy. In *Annual Symposium on Foundations of Computer Science (FOCS)*, pages 81–90, 2010. , 1, 2, 3, 4, 7

[28] I. Mironov, O. Pandey, O. Reingold, and S. Vadhan. Computational differential privacy. In *Annual International Cryptology Conference (CRYPTO)*, pages 126–142, 2009. 2, 5, 6, 20

[29] S. V. Nagaev. Some limit theorems for large deviations. *Theory of Probability & Its Applications*, 10(2):214–235, 1965. 63

[30] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991. 6

[31] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Annual ACM Symposium on Theory of Computing (STOC)*, pages 387–394, 1990. 6

[32] M. Santha and U. V. Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of computer and system sciences*, 33(1):75–87, 1986. 3

[33] S. Vadhan. The complexity of differential privacy. In *Tutorials on the Foundations of Cryptography*, pages 347–450. Springer, 2017. 2

[34] S. Vadhan and C. J. Zheng. Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In *Annual ACM Symposium on Theory of Computing (STOC)*, pages 817–836, 2012. 4

[35] S. P. Vadhan. Pseudorandomness. *Found. Trends Theor. Comput. Sci.*, 7(1-3):1–336, 2012. 56

[36] S. L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965. 20

A Missing Proofs

A.1 Missing Proofs from Section 3

A.1.1 Proving Proposition 3.26

In this section, we prove Proposition 3.26, restated below.

Proposition A.1. *Let $n \in \mathbb{N}$ be larger than some universal constant, and let $X = |X_1 + \ldots + X_n|$, where the X_i's are i.i.d., each takes 1 w.p. 1/2 and -1 otherwise. Then for event E, it holds that*

$$\Pr[E] \cdot \mathrm{E}[X \mid E] \leq 4\sqrt{n}$$

Throughout this section, we let $\mathcal{N}(0,1)$ be the standard normal distribution with probability density function $\phi(z) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{z^2}{2}\right)$, and we let S_n be the sum of n i.i.d. random variables, each takes 1 w.p. 1/2 and -1 otherwise. We use the following facts:

Fact A.2 ([1]). *Let $Z \leftarrow \mathcal{N}(0,1)$. Then for every $t \in \mathbb{R}$:*

$$\Pr[Z > t] \cdot \mathrm{E}[Z \mid Z > t] = \phi(t).$$

Fact A.3 (Nonuniform Berry-Esseen bound [29]). *Let $X \leftarrow S_n$, and let $Z \leftarrow \mathcal{N}(0,1)$. Then for every $t \in \mathbb{R}$:*

$$\Pr\left[X > t\sqrt{n}\right] - \Pr[Z > t] = O\left(\frac{1}{(1 + |t|^3)\sqrt{n}}\right)$$

Fact A.4. *For any random variable X over $\mathbb{R}^+$, it holds that*

$$\mathrm{E}[X] = \int_0^\infty \Pr[X > x]dx$$

The proof of Proposition 3.26 immediately follows by the following proposition.

Proposition A.5. *Let $n \in \mathbb{N}$ be larger than some universal constant, and let $X \leftarrow S_n$. Then for every $t > 0$:*

$$\Pr[X > t] \cdot \mathrm{E}[X \mid X > t] \leq 2\sqrt{n}$$

Proof. Compute

$$
\begin{aligned}
\Pr[X > t] \cdot \mathrm{E}[X \mid X > t] &= \Pr[X > t] \cdot \int_0^\infty \Pr[X > x \mid X > t]dx \\
&= \int_0^\infty \Pr[X > \max\{x, t\}]dx \\
&= t \cdot \Pr[X > t] + \int_t^\infty \Pr[X > x]dx \\
&\leq t \cdot \exp\left(-\frac{t^2}{2n}\right) + \sqrt{n} \cdot \int_{t/\sqrt{n}}^\infty \Pr\left[X > z\sqrt{n}\right]dz \\
&\leq e^{-1/2} \cdot \sqrt{n} + \sqrt{n} \cdot \int_{t/\sqrt{n}}^\infty \Pr[Z > z]dz + O(1) \\
&\leq e^{-1/2} \cdot \sqrt{n} + \frac{1}{2} \cdot \sqrt{n} \cdot \int_0^\infty \Pr[Z > z \mid Z > 0]dz + O(1) \\
&= e^{-1/2} \cdot \sqrt{n} + \frac{1}{2}\sqrt{n} \cdot \mathrm{E}[Z \mid Z > 0] + O(1) \\
&\leq 2\sqrt{n}.
\end{aligned}
$$

The first equality holds by Fact A.4. The first inequality holds by Hoeffding's inequality (Fact 3.25) along with the variable substitution $x = z\sqrt{n}$ in the integral. The second inequality holds by Fact A.3 along with the fact that $t \cdot \exp\left(-\frac{t^2}{2n}\right) \leq e^{-1/2} \cdot \sqrt{n}$ for every t. The third inequality holds since Z is symmetric around 0. The last equality holds by Fact A.4, and the last inequality holds by Fact A.2 which implies that $\mathrm{E}[Z \mid Z > 0] = 2\phi(0) = \sqrt{\frac{2}{\pi}}$. $\qquad\square$

A.1.2 Proving Proposition 3.27

In this section we prove Proposition 3.27, restated below.

Proposition A.6. *Let R be an uniform random variable over $\{0,1\}^n$, and E some event s.t. $\Pr_R[E] \geq 1/n$. Then for every $q > 0$ it holds that*

$$\Pr_{i \leftarrow [n]}\left[\exists b \in \{0,1\} \ s.t. \ \Pr_{R|_{R_i=b}}[E] \notin (1 \pm 2q) \cdot \Pr_R[E]\right] \leq \log n / (n \cdot q^2).$$

In the following, let H be the Entropy function. That is, for a random variable X, $H(X) = -\sum_{x \in \mathrm{Supp}(X)} \log(\Pr[X = x])$. We will use the following facts about H:

Fact A.7. *[Entropy upper bound, [4]] Let X be a random variable supported on $\{0,1\}$, and let $q \in [0,1]$. Assume $H(x) \geq 1 - q^2$. Then $\Pr[X = 1] \in [1/2 - q, 1/2 + q]$.*

Fact A.8. *Let $X = (X_1, \ldots, X_n)$ be a random variable. Then $H(X) \leq \sum_i H(X_i)$.*

Fact A.9. *Let X be a random variable and let E be an event. Then $H(X|E) \geq H(X) + \log(\Pr[E])$.*

Proof of Proposition 3.27. We first show that for every $q \in [0,1]$, it holds that

$$\Pr_{i \leftarrow [n]}\big[H(R_i|E) \geq 1 - q^2\big] \geq 1 - (\log n)/(n \cdot q^2). \tag{120}$$

To see this, let $\mathcal{B} = \big\{i : H(R_i|E) < 1 - q^2\big\}$. We want to show that $|\mathcal{B}| \leq (\log n)/q^2$. Indeed, assume toward contradiction this is not the case. Then

$$\sum_i H(R_i|E) < |\mathcal{B}| \cdot (1 - q^2) + (n - |B|) \cdot 1 = n - q^2 \cdot |\mathcal{B}| \leq n - \log n. \tag{121}$$

On the other hand, using Facts A.8 and A.9 we get that

$$\sum_i H(R_i|E) \geq H(R|E) \geq H(R) - \log(1/\Pr_R[E]) \geq n - \log n \tag{122}$$

which contradicts Equation (121), and thus Equation (120) holds.

Next, we show that for every $i \in [n]$ with $H(R_i|E) \geq 1 - q^2$ it holds that $\Pr[E \mid R_i = b] \in (1 \pm 2q)\Pr[E]$, which concludes the proof. Indeed, by Fact A.7, it holds that for every $b \in \{0,1\}$, $\Pr[R_i = b \mid E] \in 1/2 \pm q$. Applying Bayes rule, we get that

$$\Pr[E \mid R_i = b] = \frac{\Pr[E] \cdot \Pr[R_i = b \mid E]}{\Pr[R_i = b]} = 2\Pr[E] \cdot \Pr[R_i = b \mid E] \in (1 \pm 2q)\Pr[E]$$

as we wanted to show. $\qquad\square$

A.1.3 Proving Proposition 3.28

In this section we prove Proposition 3.28, restated below.

Proposition A.10. *Let R be uniform random variable over $\{0,1\}^n$, and let I be uniform random variable over $\mathcal{I} \subseteq [n]$, independent of R. Then $SD(R|_{R_I=1}, R|_{R_I=0}) \leq 1/\sqrt{|\mathcal{I}|}$.*

To prove Proposition 3.28, we will use the following simple lemma:

Lemma A.11. *Let X ba a random variable. Then $\mathrm{E}[|X - \mathrm{E}[X]|] \leq \sqrt{\mathrm{Var}(X)}$.*

Proof. Recall that $\mathrm{Var}(X) = \mathrm{E}\big[(X - \mathrm{E}[X])^2\big]$. So, by taking $Y := |X - \mathrm{E}[X]|$, it is enough to show that $\mathrm{E}[Y] \leq \sqrt{\mathrm{E}[Y^2]}$. Since Y is positive, the above is equivalent to $\mathrm{E}[Y]^2 \leq \mathrm{E}\big[Y^2\big]$. Recall that

$$0 \leq \mathrm{Var}(Y) = \mathrm{E}\big[Y^2\big] - \mathrm{E}[Y]^2$$

which ends the proof. $\qquad\square$

We are now ready to prove Proposition 3.28.

Proof of Proposition 3.28. For a vector $r \in \{0,1\}^n$, let $1(r) := \sum_{i \in \mathcal{I}} r_i$ be the number of 1's that r has in $\mathcal{I}$, and $0(r) := |\mathcal{I}| - 1(r)$ be the number of 0's that r has in $\mathcal{I}$. By definition of statistical distance,

$$
\begin{aligned}
SD(R|_{R_I=1}, R|_{R_I=0}) &= 1/2 \cdot \sum_{r \in \{0,1\}^n} |\Pr[R = r \mid R_I = 1] - \Pr[R = r \mid R_I = 0]| \\
&= 1/2 \cdot \sum_{r \in \{0,1\}^n} \left| \frac{\Pr[R = r, R_I = 1]}{\Pr[R_I = 1]} - \frac{\Pr[R = r, R_I = 0]}{\Pr[R_I = 0]} \right| \\
&= 1/2 \cdot \sum_{r \in \{0,1\}^n} 2^{-n} \cdot \left| \frac{\Pr[R_I = 1 \mid R = r]}{1/2} - \frac{\Pr[R_I = 0 \mid R = r]}{1/2} \right| \\
&= \sum_{r \in \{0,1\}^n} 2^{-n} \cdot |\Pr[R_I = 1 \mid R = r] - \Pr[R_I = 0 \mid R = r]| \\
&= \sum_{r \in \{0,1\}^n} \frac{2^{-n}}{|\mathcal{I}|} \cdot |1(r) - 0(r)| \\
&= \frac{2}{|\mathcal{I}|} \cdot \mathrm{E}_{r \leftarrow R}[|1(r) - |\mathcal{I}|/2|],
\end{aligned}
$$

where the last equality holds since $|1(r) - 0(r)| = 2 \cdot |1(r) - |\mathcal{I}|/2|$.

Notice that $\mathrm{E}[1(r)] = |\mathcal{I}|/2$ and $\mathrm{Var}(1(r)) = |\mathcal{I}|/4$. Thus, by Lemma A.11 we conclude that

$$
\begin{aligned}
SD(R|_{R_I=1}, R|_{R_I=0}) &\leq 2/|\mathcal{I}| \cdot \sqrt{|\mathcal{I}|/4} \\
&= 1/\sqrt{|\mathcal{I}|}.
\end{aligned}
$$

$\square$

A.2 Missing Proofs from Section 5

A.2.1 Proving Corollary 5.2

In this section we prove Corollary 5.2, restated below.

Corollary A.12. *Let* $\mathsf{C} \colon (\{-1,1\}^n)^3 \mapsto \mathbb{Z}$ *be defined by* $\mathsf{C}(x,y,r) := \langle x \cdot y, r \rangle$. *Then for every* $\varepsilon > 0$ *and any* $e^{-\varepsilon}$*-strong SV source* (X, Y) *over* $(\{-1,1\}^n)^2$ *and* $R \leftarrow \{-1,1\}^n$, *it holds that for every* $0 \leq \delta \leq 1$:

$$
\Pr_{(x,y,r) \leftarrow (X,Y,R)} \left[\mathrm{H}_\infty(\mathsf{C}(X,Y,R)|_{(R, X_{R^+}, Y_{R^-}) = (r, x_{r^+}, y_{r^-})}) \geq \log\left(\frac{\delta\sqrt{n}}{c_2 \cdot e^{c_1 \varepsilon} \cdot \log n} \right) \right] \geq 1 - \delta,
$$

where c *is the constant from Theorem 5.1.*

Proof. Let (X,Y), R, ε and δ be as in Corollary 5.2. Let c_1 and c_2 be as in Theorem 5.1, $\ell := \log n$, $t = \perp$, $D := (X, Y, \perp)$ and let f be the function defined by

$$
f(r, x_{r^+}, y_{r^-}, t) := \underset{c \in [n]}{\mathrm{argmax}}\{\Pr_{(x,y,r) \leftarrow (X,Y,R)}[\mathsf{C}(X,Y,R) = c \mid (R, X_{R^+}, Y_{R^-}) = (r, x_{r^+}, y_{r^-})]\}
$$

66

Let $Z = (R, X, Y)$ and $Z_r = (R, X_{R^+}, Y_{R^-})$. By Theorem 4.6 and Proposition 3.16, it holds that $\Pr_{(x,y,t) \leftarrow D, r \leftarrow \{-1,1\}^n}[f(r, x_{r^+}, y_{r^-}, t) = \mathsf{C}(x, y, r)] < e^{c_1 \varepsilon} \cdot c_2 \cdot \ell/\sqrt{n}$. Thus,

$$\mathrm{E}_{z_r \leftarrow Z_r}\left[\Pr_{z \leftarrow Z|Z_r = z_r}[f(r, x_{r^+}, y_{r^-}, t) = \mathsf{C}(x, y, r)]\right] < e^{c_1 \varepsilon} \cdot c_2 \cdot \ell/\sqrt{n}$$

By the Markov inequality, we get that

$$\Pr_{z_r \leftarrow Z_r}\left[\Pr_{z \leftarrow Z|Z_r = z_r}[f(r, x_{r^+}, y_{r^-}, t) = \mathsf{C}(x, y, r)] \geq 1/\delta \cdot e^{c_1 \varepsilon} \cdot c_2 \cdot \ell/\sqrt{n}\right] \leq \delta$$

and by the definition of f, it holds that

$$\Pr_{(r,x_{r^+},y_{r^-}) \leftarrow Z_r}\left[\max_{c \in [n]}\{\Pr_{(x,y,t) \leftarrow D, r \leftarrow \{-1,1\}^n}[\mathsf{C}(x, y, r) = c \mid r, x_{r^+}, y_{r^-}]\} \geq 1/\delta \cdot e^{c_1 \varepsilon} \cdot c_2 \cdot \ell/\sqrt{n}\right] \leq \delta$$

The last implies by the definition of min-entropy that

$$\Pr_{z_r \leftarrow Z_r}\left[\mathrm{H}_\infty(C(X, Y, R)|_{Z_r = z_r}) \leq \log\left(\frac{\delta\sqrt{n}}{c_2 \cdot e^{c_1 \varepsilon} \log n}\right)\right] \leq \delta$$

which ends the proof.

$\square$