Electronic Colloquium on Computational Complexity, Report No. 71 (2018)

Computational Two-Party Correlation

Iftach Haitner* Kobbi Nissim† Eran Omri‡ Ronen Shaltiel§ Jad Silbak§

April 5, 2018

Abstract

Let π be an efficient two-party protocol that given security parameter κ, both parties output single bits X_κ and Y_κ, respectively. We are interested in how (X_κ, Y_κ) "appears" to an efficient adversary that only views the transcript T_κ. We make the following contributions:

- We develop new tools to argue about this loose notion, and show (modulo some caveats) that for every such protocol π, there exists an efficient *simulator* such that the following holds: on input T_κ, the simulator outputs a pair (X'_κ, Y'_κ) such that $(X'_\kappa, Y'_\kappa, T_\kappa)$ is (somewhat) *computationally indistinguishable* from $(X_\kappa, Y_\kappa, T_\kappa)$.
- We use these tools to prove the following *dichotomy theorem*: every such protocol π is:
  - either *uncorrelated* — it is (somewhat) indistinguishable from an efficient protocol whose parties interact to produce T_κ, but then choose their outputs *independently* from some product distribution (that is determined in poly-time from T_κ),
  - or, the protocol implies a key-agreement protocol (for infinitely many κ).

  Uncorrelated protocols are completely uninteresting from a cryptographic viewpoint, as the correlation between outputs is uninteresting. Our dichotomy shows that every protocol is either completely uninteresting or implies key-agreement.
- We use the above dichotomy to make progress on open problems on minimal cryptographic assumptions required for differentially private mechanisms for the XOR function.
- A subsequent work of Haitner et al. uses the above dichotomy to makes progress on a long-standing open question regarding the complexity of fair two-party coin-flipping protocols.

We highlight the following two ideas regarding our technique:

- The simulator algorithm is obtained by a carefully designed "competition" between efficient algorithms attempting to forecast $((X_\kappa, Y_\kappa)|T_\kappa = t)$. The winner is used to simulate the outputs of the protocol. To the best of our knowledge, this idea has not been used before (at least in this context).
- Our key-agreement protocol uses the simulation to reduce to an information theoretic setup, and is in some sense non-black box.

*School of Computer Science, Tel Aviv University. E-mail: iftachh@cs.tau.ac.il. Member of the Israeli Center of Research Excellence in Algorithms (ICORE) and the Check Point Institute for Information Security. Research supported by ERC starting grant 638121.

†Department of Computer Science, Georgetown University. E-mail: kobbi.nissim@georgetown.edu. Research supported by NSF grant CNS-1565387.

‡Department of Computer Science, Ariel University. E-mail: omrier@ariel.ac.il. Research supported by ISF grants 544/13 and 152/17.

§Department of Computer Science. University of Haifa, E-mails: {ronen@cs.haifa.ac.il,jadsilbak@gmail.com}. Research supported by ISF grant 1628/17.

ISSN 1433-8092

1 Introduction

In this paper we discuss "computational correlation" of efficient single-bit output two-party protocols. We start with some notation for such protocols.

Two-party protocols with single bit output. We are interested in probabilistic polynomial-time (PPT), two-party, no-input, single-bit output protocols: the PPT parties receive a common input 1^κ (i.e., a security parameter), and each party outputs a single bit. For such protocols $\pi = (\mathsf{A}, \mathsf{B})$ we use the notation:

$$\pi(1^\kappa) = (\mathsf{A}, \mathsf{B})(1^\kappa) = (X_\kappa, Y_\kappa, T_\kappa).$$

where X_κ is the output of A, Y_κ is the output of B, and T_κ is the transcript of the protocol. Loosely speaking, we are interested in the correlation that an execution of $\pi(1^\kappa)$ generates between X_κ and Y_κ, when viewed from the point of view of a PPT algorithm that receives only the transcript T_κ as input. It is instructive to consider the following example:

Key-agreement protocols. These are PPT protocols with the following properties:

Secrecy. $\Pr[\mathsf{E}(T_\kappa) = X_\kappa] \leq \frac{1}{2} + s(\kappa)$ for every PPT algorithm (eavesdropper) E. (Here the standard choice for $s(\kappa)$ is a negligible function, but we will also consider versions where $s(\kappa) = s$ is a constant).

Agreement. $\Pr[X_\kappa = Y_\kappa] \geq \frac{1}{2} + a(\kappa)$. (Here the standard choice for $a(\kappa)$ is half minus a negligible function, but we will also consider versions where $a(\kappa) = a$ is a constant, and $a > s$).

The reader is referred to [13] for a survey on key-agreement protocols. We remark that by [13], a key-agreement protocol for constants s and a with $s < a^2/10$, implies a full-fledged key-agreement protocol (i.e., with the standard choices of agreement and secrecy).

Computational correlation. Loosely speaking, from the "point of view" of a PPT algorithm E that only sees the transcript t of a key-agreement protocol, the probability space $((X_\kappa, Y_\kappa)|T_\kappa = t)$ "should look like" (U, U), for U being a uniform bit (unknown to E). This in contrast to the view of an *unbounded* E: since for any protocol, and every transcript t, $((X_\kappa, Y_\kappa)|T_\kappa = t)$ is a product distribution.

An important contribution of this paper is developing tools to formalize the vague notion of "computational correlation" in a rigorous (and as we shall explain) useful way. Specifically, we show that (modulo some caveats and technicalities that we soon explain) for every single-bit output, two-party protocol, there exists a PPT algorithm (simulator) Sim such the the following holds: on input T_κ, Sim outputs two bits (simulated outputs) (X'_κ, Y'_κ) such that the simulated experiment $(X'_\kappa, Y'_\kappa, T_\kappa)$ is computationally indistinguishable from (real) experiment $(X_\kappa, Y_\kappa, T_\kappa)$.

The simulated experiment represents the "best understanding" that a PPT can obtain on the real experiment. We find it quite surprising that such a clean notion exists. One could have expected that different PPT's have "different views" or "different understanding" of the real execution, and it is impossible to come up with a *single* simulated distribution that represents the "collective understanding" of all PPT's. Loosely speaking, the above yields that such two-party protocols can be classified as follows:

- Protocols in which the simulated distribution $(X'_\kappa, Y'_\kappa, T_\kappa)$ has the property that (X'_κ, Y'_κ) are independent, conditioned on every fixing of T. We will call such protocols "uncorrelated".
- Protocols in which the simulated distribution $(X'_\kappa, Y'_\kappa, T)$ has the property that (X'_κ, Y'_κ) are correlated given T (at least for some fixings of T).

Uncorrelated protocols are cryptographically uninteresting. Uncorrelated protocols are uninteresting from a cryptographic viewpoint; whenever we have such a protocol π, we can imagine that the parties use the following alternative trivial protocol $\widehat{\pi} = (\widehat{\mathsf{A}}, \widehat{\mathsf{B}})$: party $\widehat{\mathsf{A}}$ samples a transcript T_κ (on his own) and sends T_κ to $\widehat{\mathsf{B}}$. Then each party samples its output (independently) by applying the simulator for π on T_κ.

As is often the case in simulation: for any PPT adversary E, if the adversary is able to perform some task (that is defined in terms of the original triplet $(X_\kappa, Y_\kappa, T_\kappa)$), then it achieves roughly the same success on the simulated triplet $(X'_\kappa, Y'_\kappa, T_\kappa)$. Specifically, if π is a key-agreement protocol, then $\widehat{\pi}$ is also a key-agreement protocol. The latter, however, is obviously false. This is because given T_κ, the adversary E can use the simulator to sample X'_κ with probability that is at least as large as $\Pr[X'_\kappa = Y'_\kappa]$. This means that in $\widehat{\pi}$ secrecy is less than agreement, ruling out any meaningful form of key-agreement.

Correlated protocols yield key-agreement. In this paper we prove that (again, modulo some caveats and technicalities that we soon explain) if a protocol is correlated, then it can be transformed into a key-agreement protocol. This can be interpreted as the following dichotomy theorem:

> Every PPT single-bit output two-party protocol is either uncorrelated (and is indistinguishable from a trivial and cryptographically uninteresting protocol), or it implies a key-agreement protocol.

We find this quite surprising. Intuitively, key-agreement protocols and trivial protocols represent two extremes in the spectrum of two-party protocols, and one may expect that there are many interesting intermediate types in between the two extremes.[1]

1.1 Our Results

1.1.1 Every two-party single bit output protocol has a simulator and a forecaster

We show that every protocol has a PPT *simulator* that, seeing only the transcript, produces a simulated distribution simulating the (real) output distribution of the protocol.

Theorem 1.1 (Existence of PPT simulators (informal))**.** *Let $\pi = (\mathsf{A}, \mathsf{B})$ be a* PPT *no-input, single-bit output two-party protocol. For every $\rho > 0$ there exists a* PPT Sim *such that when given $(1^\kappa, t)$, $\mathsf{Sim}(1^\kappa, t)$ outputs two bits, (x', y') such that: Let* $\text{REAL} = \{\text{REAL}_\kappa\}_{\kappa\in\mathbb{N}}$ *and* $\text{SML} = \{\text{SML}_\kappa\}_{\kappa\in\mathbb{N}}$

[1] One illuminating "intermediate setup" is "defective key-agreement protocols" in which the agreement and secrecy properties above hold, but with $a < s$ (namely, agreement is smaller than secrecy, and this is not a cryptographically meaningful key-agreement). Such protocols can be uncorrelated (and trivial), but they can also be correlated, and thus, by our result, imply key-agreement. As we shall explain, this approach yields several new results, as in some cases it was previously unknown whether key-agreement protocols are implied, but it is possible to show that the protocol is not uncorrelated.

be ensembles defined as follows: $\text{REAL}_\kappa = \pi(1^k) = (X_\kappa, Y_\kappa, T_\kappa)$ *and let* $\text{SML}_\kappa = (X'_\kappa, Y'_\kappa, T_\kappa)$ *for* $(X'_\kappa, Y'_\kappa) = \mathsf{Sim}(1^\kappa, T_\kappa)$. *For infinitely many* $\kappa \in \mathbb{N}$, REAL *cannot be distinguished from* SML *with advantage* ρ *by* PPT *algorithms.*

(A precise formal definition of computational indistinguishability with advantage ρ is given in Definition 2.1. Theorem 1.1 is formally stated in Section 3.) Theorem 1.1 comes with two caveats:

- The simulated ensemble SML is only guaranteed to resemble the real ensemble REAL on some infinite subset $\mathcal{I}$ of $\kappa \in \mathbb{N}$.
- For $\kappa \in \mathcal{I}$, REAL and SML are only weakly indistinguishable as ρ is not negligible.

We do not know whether the theorem can be proven without these caveats. We mention that most the machinery that we develop (with one notable exception) can be used towards proving a version without the caveats. As we will demonstrate, in some cases, the caveats do not affect applications, and we can prove clean results using the theorem.

Forecasters. In applications, it will be useful to assume that the simulators work in the following specific fashion: there is a "forecaster algorithm" F which on input t, generates a description of the probability space $((X'_\kappa, Y'_\kappa)|T_\kappa = t)$. For technical reasons, it is helpful to think of the forecaster F as a deterministic poly-time algorithm that receives its random coin r, as an additional input. Given input $(1^\kappa, t, r)$ the forecaster outputs three numbers:

- p_{A} which is a "forecast" for $\Pr[X_\kappa = 1|T_\kappa = t]$.
- $p_{\mathsf{B}|0}$ which is a "forecast" for $\Pr[Y_\kappa = 1|T_\kappa = t, X_\kappa = 0]$.
- $p_{\mathsf{B}|1}$ which is a "forecast" for $\Pr[Y_\kappa = 1|T_\kappa = t, X_\kappa = 1]$.

All that is left for the simulator is to sample according to this forecast. For $0 \leq p \leq 1$, we will use the notation U_p to denote the distribution of a biased coin that is one with probability p. We can now restate Theorem 1.1 in the following more general form:

Theorem 1.2 (Existence of PPT forecasters, informal)**.** *Let* $\pi = (\mathsf{A}, \mathsf{B})$ *be a* PPT *no-input, single-bit output two-party protocol. For every* $\rho > 0$ *there exists a deterministic poly-time machine* F *that on input* $(1^\kappa, t, r)$ *outputs three numbers* $p_{\mathsf{A}}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1} \in [0, 1]$ *such that the following holds: let* R_κ *be a uniform polynomially long string (intuitively* R *serves as the random coins of* F*), and let* $\text{REAL} = \left\{\text{REAL}_\kappa = (\pi(1^k), R_\kappa) = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa)\right\}$ *and* $\text{SML} = \{\text{SML}_\kappa = (X'_\kappa, Y'_\kappa, T_\kappa, R_\kappa)\}$ *be the distribution ensembles obtained by:*

- $(p_{\mathsf{A}}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1}) = \mathsf{F}(1^\kappa, T_\kappa, R_\kappa)$.
- $X'_\kappa \leftarrow U_{p_{\mathsf{A}}}$ *and* $Y'_\kappa \leftarrow U_{p_{\mathsf{B}|X'_\kappa}}$.

Then for infinitely many $\kappa \in \mathbb{N}$, REAL *cannot be distinguished from* SML *with advantage* ρ *by* PPT *algorithms.*

(Theorem 1.2 is formally stated in Section 3.)

Theorem 1.1 and Theorem 1.2 may be of independent interest, and we believe that they will find more applications. This is because the simulator induces a *single* distribution that is computationally indistinguishable (albeit only with advantage $\rho = o(1)$) from the real output distribution of the protocol. Moreover, in the simulated distribution $(X'_\kappa, Y'_\kappa, T_\kappa)$ (sampled using the forecaster) the variables (X'_κ, Y'_κ) have *information theoretic uncertainty* conditioned on $\{T_\kappa = t\}$. This enables us to use tools and techniques from information theory on the simulated distribution, and obtain results about the computational security of the original protocol (and protocols that we construct from it). Indeed, we use this approach in our applications.

We believe that a helpful analogy is the notion of *computational entropy*: which in some cases, given a distribution X assigns a distribution X' that is computationally indistinguishable from X and has *information theoretic uncertainty*.

We remark that Theorem 1.2 can be derived from Theorem 1.1 directly (without using specific properties of the proof). Nevertheless, we find the formulation of Theorem 1.2 illuminating, and useful. Specifically, our applications exploit the existence of forecasters (and not just of simulators). Moreover, the forecasting terminology is also the one we use for the dichotomy theorem below.

1.1.2 A Dichotomy of Single-bit Output Two-Party Protocols

We now give a precise definition of uncorrelated protocols. For that purpose we introduce the following notion of a "decorrelator". Loosely speaking, a decorrelator is a forecaster that forecasts that (X_κ, Y_κ) are independent conditioned on T. Once again, for technical reasons, it is helpful to think of a decorrelator as a deterministic poly-time algorithm that receives its random coin r, as an additional input.

Definition 1.3 (ρ-decorrelator, and ρ-uncorrelated protocols, informal)**.** *A deterministic poly-time algorithm* $\mathsf{Decor}(t, r)$ *is a* ρ-*decorrelator for protocol* $\pi = (\mathsf{A}, \mathsf{B})$ *if the following holds: let* $\text{REAL} = \{\text{REAL}_\kappa\}_{\kappa\in\mathbb{N}}$ *and* $\text{UCR} = \{\text{UCR}_\kappa\}_{\kappa\in\mathbb{N}}$ *be ensembles defined as follows:* $\text{REAL}_\kappa = (\pi(1^k); R_\kappa) = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa)$ *where* R_κ *is a uniformly chosen independent polynomially long string (that intuitively serves as the random coins of* Decor*). Let* $\text{UCR}_\kappa = (X'_\kappa, Y'_\kappa, T_\kappa, R_\kappa)$ *where* $(p_\mathsf{A}, p_\mathsf{B}) = \mathsf{Decor}(T_\kappa, R_\kappa)$*, and (independently sampled)* $X'_\kappa \leftarrow U_{p_\mathsf{A}}$ *and* $Y'_\kappa \leftarrow U_{p_\mathsf{B}}$*. It is required that for infinitely many* $\kappa \in \mathbb{N}$*,* REAL *cannot be distinguished from* UCR *with advantage* ρ *by* PPT *algorithms.*
A protocol π *is* ρ-*uncorrelated if it has a* ρ*-decorrelator.*

(Definition 1.3 is formally in Section 3.) Loosely speaking, the fact that the randomness R_κ appears in the two experiments, prevents the decorrelator from using R_κ to correlate between X'_κ and Y'_κ. In the definition the latter should appear independent, even after seeing R_κ.

We observe that ρ-uncorrelated protocols are uninteresting from a cryptographic viewpoint in the following sense (that is made precise in Section 3):

- A ρ-uncorrelated protocol cannot be a key-agreement protocol for $s < a - 2\rho$.
- If a "black-box construction" that makes ℓ invocations to a ρ-uncorrelated protocol, yields a key-agreement protocol with $s < a - 3 \cdot \ell \cdot \rho$, then the black-box construction itself can be used to give a key-agreement (with the standard choices of secrecy and agreement) that does not use the original protocol. This means that a ρ-uncorrelated protocol cannot be converted into an "interesting" protocol by a black-box construction that invokes it few times.

Loosely speaking, both properties follow because an uncorrelated protocol is somewhat indistinguishable from one in which one party samples (T_κ, R_κ) on his own, sends them to the other party, and each of the parties runs $\mathsf{Decor}(T_\kappa, R_\kappa)$ and samples its output independently (party A samples $X \leftarrow U_{p_\mathsf{A}}$, and party B samples $Y \leftarrow U_{p_\mathsf{B}}$). The latter protocol can be easily attacked, and by indistinguishability, this attack also succeeds on the original protocol.
We prove the following classification theorem:

Theorem 1.4 (Dichotomy theorem, informal)**.** *Let $\pi = (\mathsf{A}, \mathsf{B})$ be a* PPT *no-input, single-bit output two-party protocol. Then at least one of the following hold:*

- *π can be transformed into a key-agreement protocol (for infinitely many $\kappa \in \mathbb{N}$).*
- *For every constant $\rho > 0$, π is ρ-uncorrelated (for infinitely many $\kappa \in \mathbb{N}$).*

(Theorem 1.4 is formally stated in Section 3). The fact that we have statements on "infinitely many κ's" is unavoidable: it could be the case that on even κ, the protocol is a key agreement, and on odd κ, the protocol is trivial and performs no interaction.[2]

Once again, a caveat is the fact that we only get the result for $\rho = o(1)$ and not for negligible ρ (as is the standard in computational indistinguishability). It is an interesting open problem to extend our results to small ρ.

We demonstrate the usefulness of Theorem 1.4 below. It is important to emphasize that the caveats in Theorem 1.4 (and specifically, the limitation on ρ) do not matter for some of our suggested applications.

1.1.3 Perspective: Comparison to Impagliazzo and Luby Dichotomy Theorem

A celebrated result of Impagliazzo and Luby [14] is that distributional one-way functions imply one-way functions. This can be loosely stated this way:

Theorem 1.5 (Impagliazzo and Luby [14], informal)**.** *Let P be a poly-time algorithm, then at least one of the following holds:*

- *P can be transformed into a* one-way function*.*
- *P has a* PPT inverter *(for infinitely many $\kappa \in \mathbb{N}$).*

  Namely, for every constant c, there exists a PPT $\mathsf{Inverter}$*, such that for infinitely many $\kappa \in \mathbb{N}$ the following holds: let $X_\kappa \leftarrow U_\kappa$ and $T_\kappa = \mathsf{P}(X_\kappa)$. It holds that (X_κ, T_κ) is $(\rho = \kappa^{-c})$-close to (X'_κ, T_κ), for $X'_\kappa = \mathsf{Inverter}(T_\kappa)$.*

This theorem is celebrated for (at least) two reasons: first, it gives a dichotomy of poly-time algorithms (ruling out intermediate cases). Second, it gives a methodology to show that cryptographic primitives imply one-way functions: it is sufficient to show that the primitive has a component that cannot be inverted.

Our Theorem 1.4 can be viewed as an analogous theorem for *two-party protocols*: either a protocol π implies *key-agreement* or it has a PPT *decorrelator*. Analogously, Theorem 1.4 gives a

[2] However, the fact that we have "for infinitely many κ" in the two items, and not just in one, is an artifact of our proof technique, and it is natural to ask whether the result can be improved to have such a statement in only one of the items (as in the case of the Theorem of Impagliazzo and Luby [14] that we mention in the next section).

dichotomy of two-party protocols, and in order to show that a protocol implies key-agreement, it is now sufficient to show that it is not uncorrelated. We will present applications of this methodology in Section 1.2.

We remark that many of the applications of the Impagliazzo and Luby [14] classification do not require that ρ is small, and would have worked just the same for constant ρ.[3] Analogously, the fact that ρ is not very small in our theorem is often unimportant in applications.

1.2 Consequences of our Dichotomy Theorem

We demonstrate the usefulness of our result by showing that it can be used to answers some open problems regarding differentially private protocols and coin flipping protocols (even with the caveats above). We now elaborate on these results.

1.2.1 Application to Differentially Private XOR

In a symmetric differentially private computation, the parties wish to compute a joint function of their inputs while keeping their inputs somewhat private. This is somewhat different from the classical client-server setting commonly address in the differentially privacy literature, where the the server, holding the data, answers the client's question while keeping the the date somewhat private. We show that the existence of a symmetric differential private protocol for computing Boolean XOR that achieves non-trivial accuracy, implies the existence of a key-agreement protocol.

We now consider protocols in which the two parties receive inputs $x, y \in \{0,1\}$ and each outputs a bit. A two-party protocol $\pi = (\mathsf{A}, \mathsf{B})$ for computing the XOR functionally is α-*correct*, if

$$\Pr\left[(\mathsf{A}(X), \mathsf{B}(Y)) = (X \oplus Y, X \oplus Y)\right] \geq \frac{1}{2} + \alpha$$

Such a protocol is (computationally) ε-*differentially private*, if for every x and efficient distinguisher D

$$\frac{\Pr\left[\mathsf{D}(\mathrm{view}^{\mathsf{A}}_{\pi}(x,0)) = 1\right]}{\Pr\left[\mathsf{D}(\mathrm{view}^{\mathsf{A}}_{\pi}(x,1)) = 1\right]} \in e^{\pm\varepsilon}$$

letting $\mathrm{view}^{\mathsf{A}}_{\pi}(x,y)$ being A's view in a random execution of $(\mathsf{A}(x), \mathsf{B}(y))$;[4] namely, the input of B remains somewhat private from the point of view of A. And the same should hold for the privacy of A.

The protocol has perfect *agreement*, if the parties' output is always the same (though might be different from the XOR). The results below are all stated with respect to such perfect agreement protocols, though the lower bound (including ours) allows disagreement in the magnitude of the differential privacy parameter ε.

Theorem 1.6. *[Differentially private XOR to key agreement, informal]*

[3] Loosely speaking, this happens whenever we have a cryptographic primitive where security can be amplified. For such protocols, a weaker version of [14] yields that either the primitive implies one-way functions or it has a PPT ρ-inverter for some constant $\rho > 0$. Then, using security amplification we obtain a more secure target primitive, such that an adversary that breaks the target primitive with small success $\rho' = \kappa^{-c}$ can be transformed into one that breaks the original protocol with large success $\rho > 0$.

[4] A more general definition allows also an additive error term. We address this definition in our formal theorem in Section 6.

For any $\varepsilon \in [0,1]$, the existence of $21\varepsilon^2$-correct ε-differentially private protocol for computing XOR, implies the existence of an infinitely-often secure key-agreement protocol.

(Theorem 1.6 is formally stated in Section 6). The above dependency between ε and α is tight since a $\Theta(\varepsilon^2)$-correct, ε-differential private, protocol for computing XOR can be constructed (with information theoretic security) using the so-called *randomized response* approach Warner [20]. It improves, in the (ε, α) dependency aspect, upon Goyal et al. [7] who showed that, for some constant $c > 0$, a $c\varepsilon$-correct ε-differentially private XOR implies oblivious transfer, and upon Goyal et al. [6] who showed that $c\varepsilon^2$-correct ε-differentially XOR implies one-way functions.

Theorem 1.6 extends for a weaker notion of differentially private in which the privacy is only guaranteed to hold against an *external* observer (assuming that the protocol's transcript explicitly states the parties common output). For such protocols, key agreement is a sufficient assumption.[5] Finally, we mention that since we use Theorem 1.4, the reduction we use to prove Theorem 1.6 is non black box in the adversary.

1.2.2 Application to Fair Coin Flipping

In a follow-up work, Haitner, Makriyannis, and Omri [11] used Theorem 1.4 to facilitate the attack of Beimel et al. [2] for two-party coin-flipping protocols, and proved that key-agreement is a necessary assumption for *two-party* r-round coin-flipping protocol of bias smaller than $1/\sqrt{r}$ (as long as r is independent of the security parameter). This partially answers a long-standing open question asking whether the existence of such two-party fair-coin flipping implies public-key cryptography. Previous to Haitner et al. [11] result, it was not even known that such protocols cannot be constructed in the random oracle model [4, 5].

1.3 Our Technique

1.3.1 A Competition of Forecasters

In this section we explain the high level idea behind the proof of Theorem 1.2. Our goal is to understand "how X_κ and Y_κ are distributed from the point of view of a PPT algorithm that receives T_κ as input". For this purpose, we set up a competition between all PPT forecasters. We will use the winner in this competition as our forecaster.

Given a transcript t, a participant forecaster is required to output three numbers $p_{\mathsf{A}}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1} \in [0,1]$. For every forecaster F and every $\kappa \in \mathbb{N}$, we associate a *price* $\mathsf{price}_\kappa(\mathsf{F})$. The minimal price is obtained by a forecaster that outputs $p_{\mathsf{A}} = \Pr[X_\kappa = 1 | T_\kappa = t]$ and $p_{\mathsf{B}|b} = \Pr[Y_\kappa = 1 | T_\kappa = t, X_\kappa = b]$. Note however, that a PPT forecaster might not be able to compute these quantities.

Existence of optimal forecasters. We will not give a precise definition of the price function in this overview. At this point, we observe that for every choice of price function where prices are in $[0,1]$, this competition has winners, in the following sense: we say that F is μ-optimal, if there exists an infinite subset $\mathcal{I} \subseteq \mathbb{N}$ such that $\mathsf{price}_\kappa(\mathsf{F}) \leq \mathsf{price}_\kappa(\mathsf{F}') + \mu$ for every other PPT F' and sufficiently large $\kappa \in \mathcal{I}$. This intuitively says that F cannot be significantly improved on the subset $\mathcal{I}$. We claim that for every constant $\mu > 0$ there exists a μ-optimal forecaster.

[5] One sends its *encrypted* input to the other party, who in turn computes the XOR of both inputs and publishes a noisy version (e.g., flipped with probability $\frac{1}{2} - \varepsilon$) of the outcome.

This follows as we can imagine the following iterative process: we start with some forecaster F and $\mathcal{I} = \mathbb{N}$. At each step, either F cannot be improved by μ, on infinitely many $\kappa \in \mathcal{I}$ (which means that F is μ-optimal), or else, there exists an infinite $\mathcal{I}' \subseteq \mathcal{I}$, and a forecaster F' that improves F by μ in $\mathcal{I}'$. In that case we set $\mathcal{I} = \mathcal{I}'$, $\mathsf{F} = \mathsf{F}'$ and continue. It is clear that at every iteration we improve the price by μ, and this can happen only $1/\mu$ times, this process shows the existence of a μ-optimal forecaster.[6]

Indistinguishability for optimal forecasters Let F be a μ-optimal forecaster, we can use F to produce a forecasted distribution (as in Theorem 1.2). Namely, given $t \leftarrow T_\kappa$, we apply $\mathsf{F}(t)$ to compute $p_{\mathsf{A}}(t), p_{\mathsf{B}|0}(t), p_{\mathsf{B}|1}(t)$, and use these forecasts to produce a distribution (X'_κ, Y'_κ) by sampling $X'_\kappa \leftarrow U_{p_{\mathsf{A}}(t)}$ and $Y'_\kappa \leftarrow U_{p_{\mathsf{B}|X'_\kappa}(t)}$. This can indeed be done in poly-time (and in this informal discussion we omit the additional random input r).

We show that if a PPT D distinguishes $(X_\kappa, Y_\kappa, T_\kappa)$ from $(X'_\kappa, Y'_\kappa, T_\kappa)$, then D can be used to construct an improved PPT F' whose $\mathsf{price}_\kappa(\mathsf{F}')$ is smaller than $\mathsf{price}_\kappa(\mathsf{F})$ by some function of the distinguishing advantage ρ. This is a contradiction to the μ-optimality of F if ρ is sufficiently large.

At the risk of getting too technical, let us try to explain how this argument works. The reader can skip to Section 1.3.2 that does not depend on the next paragraph.

It is helpful to note that $(X'_\kappa, Y'_\kappa, T_\kappa)$ can be seen as $(X'_\kappa, g(X'_\kappa), T_\kappa)$ where g is a probabilistic function. It is helpful to consider the hybrid distribution $H = (X_\kappa, g(X_\kappa), T_\kappa)$. Using a hybrid argument, we have that one of the following happens:

- D distinguishes $(X'_\kappa, g(X'_\kappa), T_\kappa)$ from $H = (X_\kappa, g(X_\kappa), T_\kappa)$. This induces a D' that distinguishes $(X'_\kappa, T_\kappa) = (U_{p_{\mathsf{A}}(T_\kappa)}, T_\kappa)$ from (X_κ, T_κ)
- D can distinguishes $(X_\kappa, Y_\kappa, T_\kappa)$ from $H = (X_\kappa, g(X_\kappa), T_\kappa)$. This gives that there exists $b \in \{0,1\}$, and a D' such that D' distinguishes $((Y_\kappa, T_\kappa)|X_\kappa = b)$ from $((Y'_\kappa, T_\kappa)|X_\kappa = b) = ((U_{p_{\mathsf{B}|b}(T_\kappa)}, T_\kappa)|X_\kappa = b)$.

We have made progress, in that in both cases we have reduced the number of variables from three to two, while obtaining a distinguisher D' that distinguishes between a "real distribution" and a "forecasted distribution". Let's assume without loss of generality that the first case happens. Note that D' obtains no distinguishing advantage on t if $\mathsf{D}'(t,0) = \mathsf{D}'(t,1)$.

Assume without loss of generality that D' is more likely to answer one on the real distribution than on the forecasted distribution. This intuitively means that on average, given a $t \leftarrow T_\kappa$, by trying out $\mathsf{D}'(t,0)$ and $\mathsf{D}'(t,1)$ we can figure out what "D' thinks" is more likely to be the bit of the forecasted distribution, and improve the forecast of F. Specifically,

- If $\mathsf{D}'(t,0) = \mathsf{D}'(t,1)$ then D does not gain on t, and we won't modify the forecast if F on t.
- If $\mathsf{D}'(t,1) = 1$ and $\mathsf{D}'(t,0) = 0$ then "D' thinks" that F's forecast for $\Pr[X_\kappa = 1|T_\kappa = t]$ was too low, and it makes sense to increase it.

[6] A drawback of the argument above is that it only works for constant $\mu > 0$. The distinguishing parameter ρ, will be selected to be say $\mu^{1/10}$, and this is why we only get the result in Theorem 1.1, Theorem 1.2 and Theorem 1.4 for constant $\rho > 0$. Consequently, if we could guarantee the existence of an optimal forecaster for smaller μ, we will immediately improve our results. Another drawback is that this argument only works on some infinite subset $\mathcal{I} \subseteq \mathbb{N}$ and this is the reason we get "for infinitely many κ" in our theorems. The remainder of our machinery does not require these caveats.

- If $\mathsf{D}'(t,0)=1$ and $\mathsf{D}'(t,1)=0$ then "D' thinks" that F's forecast for $\Pr[X_\kappa=1|T_\kappa=t]$ was too high, and it makes sense to decrease it.

By using this rationale, we can guarantee that the modified forecast (which can be computed in poly-time) improves upon F's forecast (at least on average $t \leftarrow T_\kappa$). We choose the price function carefully, so that this translates to a significant reduction in price, contradicting F's μ-optimality.

1.3.2 Using the Forecaster to Prove the Dichotomy

In this section we explain how to prove Theorem 1.4 given Theorem 1.2. Given a protocol π, we consider the optimal forecaster F from Theorem 1.2 (which is F from the previous section). We will once again oversimplify and ignore the random coin string r. Recall that on input $t \leftarrow T_\kappa$, F computes three numbers $p_{\mathsf{A}}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1}$, and induces a forecasted distribution $(X'_\kappa, Y'_\kappa, T_\kappa)$ that is ρ-indistinguishable from $\pi(1^\kappa)=(X_\kappa, Y_\kappa, T_\kappa)$, and furthermore, that $\Pr[X'_\kappa=1|T_\kappa=t]=p_{\mathsf{A}}$, and $\Pr[Y'_\kappa=1|X'_\kappa=b]=p_{\mathsf{B}|b}$.

Note that if for every possible transcript T_κ it holds that $\mathsf{F}(T_\kappa)$ produces $p_{\mathsf{B}|0}=p_{\mathsf{B}|1}$, then by setting $\mathsf{Decor}(T_\kappa)=(p_{\mathsf{A}}, p_{\mathsf{B}|0})$ we obtain a ρ-decorrelator. Increasing ρ slightly, this also extends to the case where with high probability over $t \leftarrow T_\kappa$, $p_{\mathsf{B}|0}$ is "not far" from $p_{\mathsf{B}|1}$.

If the condition above does not hold, we will want to use F to convert π into a key-agreement π'. We can use the forecaster as follows (and in fact this methodology seems quite general):

- When using π as a component in π', we can imagine that the output distribution of π is the forecasted distribution. More precisely, we are allowed to work in the following "information theoretic setting": party A receives X'_κ, party B receives Y'_κ and the adversary receives T_κ. Note that X'_κ and Y'_κ have *information theoretic uncertainty* given T_κ, and so we can now apply techniques and protocols from the information theoretic world. Information theoretic security in the latter setup translates into computational security in the original setup (with an additive loss of ρ).

- Consequently, we can use information theoretic methods to construct key-agreement to construct π' from the "simulation of" π. This then translates into computational security (with a constant loss ρ in security). By using security amplification for key agreement [13], we can amplify this security to give key-agreement with standard choices of secrecy and agreement. (This demonstrates that the fact that ρ cannot be made negligible, is not a problem, and we can get computational security with respect to negligible functions).[7]

- Moreover, when we work in the information theoretic setup, the honest parties are allowed to run the forecaster (that runs in polynomial time). This is in some sense "non-black-box" as the parties gain access to specific properties of the probability space $(X'_\kappa, Y'_\kappa, T_\kappa)$ by applying the forecaster on T_κ and can use its outputs $p_{\mathsf{A}}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1}$ when constructing information theoretic key-agreement.

[7] Continuing the analogy to computational entropy, this approach can be thought of as analogous to the constructions of Håstad et al. [12] and following work [9, 18] of pseudorandom generators from one-way functions. Indeed, a key idea in these works is that of "computational entropy" which given a distribution X (with low real entropy) presents an indistinguishable distribution X' (with a lot of entropy). This allows the construction to apply "information theoretic tools" (e.g., randomness extractors) on X and argue that the result is pseudorandom, by imagining that the information theoretic tools are applied on X'. Continuing this analogy, it is often the case that "pulling the result back" to the computational realm, suffers a significant loss in security, and computational amplification of security is performed to obtain stronger final results.

The one-sided von-Neumann protocol. The information theoretic setup described above can be thought of as follows: whenever the two parties invoke the protocol π, we can imagine that A receives variable X'_κ, B receives variable Y'_κ and the eavesdropper receives T_κ. Moreover, A, B can use F to compute all probabilities in the probability space $((X'_\kappa, Y'_\kappa)|T_\kappa = t)$. We now explain how to construct a key-agreement protocol.

- The two parties receive X'_κ and Y'_κ by running π, they also receive the transcript T_κ.
- The two parties use F to compute $\mathsf{F}(T_\kappa) = (p_\mathsf{A}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1})$. Party A samples an independent random variable $X''_\kappa \leftarrow U_{p_\mathsf{A}}$ (that is, an independent variable that is distributed like X'_κ).
- The two parties can use the von-Neumann trick [19] to obtain a shared random coin as follows: A informs B whether $X'_\kappa = X''_\kappa$.
  - If $X'_\kappa = X''_\kappa$, the parties output independent uniform bits.
  - If $X'_\kappa \neq X''_\kappa$, party A outputs X'_κ and party B outputs Y'_κ.

For every $t \in \mathrm{Supp}(T_\kappa)$, $\Pr[X'_\kappa = 1, X''_\kappa = 0|T_\kappa = t] = \Pr[X'_\kappa = 0, X''_\kappa = 1|T_\kappa = t]$, and consequently:

$$\Pr[X'_\kappa = 1|T_\kappa = t, X'_\kappa \neq X''_\kappa] = \tfrac{1}{2}.$$

This means that this information theoretic key-agreement protocol has perfect secrecy. Recall that we are assuming that X'_κ and Y'_κ are correlated conditioned on some fixings of $t \leftarrow T_\kappa$. This translates into the agreement property. (In the actual proof, we need a slightly more complicated protocol which also relies on $p_{\mathsf{B}|0}, p_{\mathsf{B}|1}$ to guarantee agreement, rather than just correlation).

Thus, this protocol is an information theoretic key agreement with secrecy $s = 0$ and agreement $a > 0$. By controlling the parameters, the gap between agreement and secrecy can be made significantly larger than ρ so that we can implement our overall plan.

1.4 Related Work

Characterization of two-party computations. The most relevant result is the classification of two-party protocols in the random oracle model (ROM) given in Haitner, Omri, and Zarosim [10]. In this model, the parties and the adversary are given an oracle access to a common random function, that they can query a limited number of times. This model is typically used to analyzed the security of cryptographic protocols in an idealistic model, and to prove impossibility results for such protocols. In particular, an impossibility result in this model, yields that the security of protocol in consideration cannot be based in a black-box way on one-way functions or collision resistant hash functions.

In their seminal work, [15] proved that a key-agreement protocol cannot be constructed in the random oracle model. That is, they show that for any query efficient protocol (i.e., polynomial query complexity) in the ROM, there exists a query efficient eavesdropper that finds the common key. Haitner et al. [10], using techniques developed by Barak and Mahmoody [1], and showed that for any no-input two-party random oracle protocol there exists a query efficient mapping into a *no oracle* protocol such that the distribution of the transcript and parties output are essentially the same. Since in the non-input setting the parties output are always uncorrelated (as far as no input protocol are concerned), the existence of such efficient mapping also tell us that interesting correlation cannot exits in the random oracle model. Our main result capturing the minimal

assumption for (output) correlation in actual protocol (rather than the hypothetical random oracle, model) is in a sense the non black-box version of the above characterization.

Other relevant results are amplifications of weak primitives into a full-fledge ones, and in particular that of key-agreement [13] and obvious transfer [8, 21, 3]. Such results aims to classify the different functionalities into groups of equivalent expression power, and many of them are achieved via the study of information-theoretic two-party correlation (also known as, channels): each party, including the observer, is given random variable from a predetermined distribution, and their goal is to use them to achieve a cryptographic task (i.e., key agreement). Our result demonstrates that going solely through the above information theoretic paradigm, is sometimes a too limited approach.

Minimal assumptions for differentially private symmetric computation. An accuracy parameter α is *trivial* with respect to a given functionality f and differential privacy parameter ε, if a protocol computing f with such accuracy and privacy exists information theoretically (i.e., with no computational assumptions). The accuracy parameter is called *optimal*, if it matches the bound achieved in the client-server model. [17] have shown that for the inner product and hamming distance functionality, there is a gap between the trivial and optimal accuracy parameters (with respect to some ε). [10] showed that the same holds also when a random oracle is available to the parties, implying that non-trivial protocols (achieving non-trivial accuracy) for computing these functionalities cannot be black-box reduced to one-way functions. [6] initiated the study of Boolean functions, showing a gap between the optimal and trivial accuracy for the XOR or the AND functionalities, and that non-trivial protocols imply one-way functions. [16] have shown that optimal protocols for computing the XOR or AND, cannot be black-box reduced to key agreement. Finally, [7] have shown that optimal protocols for computing the XOR imply oblivious transfer.

Paper Organization

Standard notions and definitions are given in Section 2. In Section 3 we formally define simulators, forecasters, decorelators, and uncorrelated protocols, and state there our main results. The existence of forecasters for every single-bit output two-party protocol whose forecasted distribution is indistinguishable from the real one, is proven in Section 4. The reduction from correlated protocols to key agreement is proven in Section 5. Finally in Section 6, we give the reduction from differentially private protocols for computing XOR to key-agreement protocols.

Acknowledgement

We are very grateful to Omer Reingold and Guy Rothblum for very useful discussions.

2 Preliminaries

2.1 Notations

We use calligraphic letters to denote sets, uppercase for random variables, lowercase for values, boldface for vectors, and sans-serif (e.g., A) for algorithms (i.e., Turing Machines). We let $\mathbb{1}_{\mathcal{S}}$ denote the charectristic function of the set $\mathcal{S}$. For $n \in \mathbb{N}$, let $[n] = \{1, \cdots, n\}$. Let poly denote the set of all positive polynomials and let PPT denote a probabilistic algorithm that runs in *strictly*

polynomial time. A function $\nu\colon \mathbb{N} \mapsto [0,1]$ is *negligible*, denoted $\nu(\kappa) = \mathrm{neg}(\kappa)$, if $\nu(\kappa) < 1/p(\kappa)$ for every $p \in \mathrm{poly}$ and large enough κ. Given an algorithm D getting input of the form $1^{\mathbb{N}} \times \{0,1\}^*$, we let $\mathsf{D}_\kappa(t)$ denote $\mathsf{D}(1^\kappa, t)$.

Distributions and random variables. For $0 \leq p < 1$, let U_p denote the distribution of a biased coin which is one with probability p. Given jointly distributed random variables X, Y and $x \in \mathcal{X}$, let $Y|_{X=x}$ denote the distribution of Y induced by the conditioning $X = x$ (set arbitrarily if $\Pr[X = x] = 0$). The *statistical distance* between two random variables X and Y over a finite set $\mathcal{U}$, denoted $\mathrm{SD}(X,Y)$, is defined as $\frac{1}{2} \cdot \sum_{u \in \mathcal{U}} |\Pr[X = u] - \Pr[Y = u]|$.

Computational indistinguishability (and infinitely-often variant). We first need the following variance of computational indistinguishability where the distinguishing advantage ρ is a parameter. We also discuss infinitely often indistinguishability.

Definition 2.1 (Computational indistinguishability with a parameter ρ)**.** *For a function $\rho : \mathbb{N} \to \mathbb{R}$, two distribution ensembles $X = \{X_\kappa\}_{\kappa \in \mathbb{N}}$, $Y = \{Y_\kappa\}_{\kappa \in \mathbb{N}}$ are ρ-*indistinguishable*, denoted $X \overset{\mathrm{C}}{\approx}_\rho Y$, if for every* PPTM D*, for every sufficiently large $\kappa \in \mathbb{N}$,*

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

We omit 1^κ when the secrecy parameter κ is clear from the context.

*For an infinite set $\mathcal{I} \subseteq \mathbb{N}$, the two ensembles X and Y are ρ-*indistinguishable in $\mathcal{I}$*, denoted $X \overset{\mathrm{C}}{\approx}_{\rho,\mathcal{I}} Y$, if the condition above holds when replacing the condition "for every sufficiently large $\kappa \in \mathbb{N}$" with "for every sufficiently large $\kappa \in \mathcal{I}$". We say that X and Y are* io-ρ-indistinguishable*, if there exists an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that X and Y are ρ-indistinguishable in $\mathcal{I}$.*

2.2 Protocols

Let $\pi = (\mathsf{A}, \mathsf{B})$ be a two-party protocol. Protocol π is PPT if both A and B ruining time is polynomial in their input length. We denote by $(\mathsf{A}(x), \mathsf{B}(y))(z)$ a random execution of π with private inputs x and y, and common input z, and sometimes abuse notation and refer to $(\mathsf{A}(x), \mathsf{B}(y))(z)$ as the parties' output in this execution.

We will mainly focus on no-input two-party protocol single-bit PPT output protocol: the two PPT parties only input is the common security parameter, given in unary, and at the end of the protocol each party output a single bit. Throughout, we assume without loss of generality that the transcript contains 1^κ as the first message.

Let $\pi = (\mathsf{A}, \mathsf{B})$ be such two-party protocol single-bit. For $\kappa \in \mathbb{N}$, let π_κ be protocol π with the common security parameter fixed (i.e., hardwired) to 1^κ. Protocol π has transcript length $m(\cdot)$, if the transcript of π_κ is of length at most $m(\kappa)$. We will assume without loss of generality that the protocol of consideration have fixed transcript length per security parameter. For $\kappa \in \mathbb{N}$, let $(X^\pi_\kappa, Y^\pi_\kappa, T^\pi_\kappa)$ denote the A and B outputs respectively, and the execution transcript, in a random execution of π_κ. We sometimes denote this triplet of random variables by $\pi(1^\kappa)$.

2.2.1 Key-Agreement Protocols (and Infinitely Often Variant)

We focus on single bit key agreement protocols.

Definition 2.2 (Key-agreement protocols)**.** *A* PPT *single-bit output two-party protocol* $\pi = (\mathsf{A}, \mathsf{B})$ *is a secure* key-agreement *with respect to a set* $\mathcal{I} \subseteq \mathbb{N}$*, if the following hold for* κ*'s in* $\mathcal{I}$*.*

Agreement. $\Pr[X_\kappa^\pi = Y_\kappa^\pi] \geq 1 - \mathrm{neg}(\kappa)$.

Secrecy. *For every* PPT E *it holds that* $\Pr[\mathsf{E}(T_\kappa^\pi) = X_\kappa^\pi] \leq 1/2 + \mathrm{neg}(\kappa)$.

Definition 2.3 (Key-agreement protocols)**.** *Let* $s, a : \mathbb{N} \mapsto \mathbb{R}$ *be functions. A* PPT *single-bit output two-party protocol* $\pi = (\mathsf{A}, \mathsf{B})$ *is an* (s, a)-key agreement *if the following two conditions hold.*

Agreement. $\Pr[X_\kappa^\pi = Y_\kappa^\pi] \geq 1/2 + a(\kappa)$ *for sufficiently large* $\kappa \in \mathbb{N}$*.*

Secrecy. *For every* PPTM E*:* $\Pr[\mathsf{E}(T_\kappa^\pi) = X_\kappa^\pi] \leq 1/2 + s(\kappa)$ *for sufficiently large* $\kappa \in \mathbb{N}$*.*

If we omit (s, a) *then we mean that the key-agreement has standard choices for secrecy and agreement, namely it is a* $(\mathrm{neg}(\kappa), 1/2 - \mathrm{neg}(\kappa))$*-key agreement.*

Protocol π *is an* (s, a)-key agreement in an infinite set $\mathcal{I} \subseteq \mathbb{N}$*, if the security and agreement conditions hold when replacing* $\mathbb{N}$ *above with* $\mathcal{I}$*. The protocol is an* io-(s, a)-key agreement *if there exits an infinite set* $\mathcal{I} \subseteq \mathbb{N}$ *for which the protocol is an* (s, a)*-key agreement in* $\mathcal{I}$*.*

We make use of the following amplification result that readily follow from Holenstein [13, Corollary 7.8.].

Theorem 2.4 (Key-agreement amplification, [13])**.** *Let* $s, a \colon \mathbb{N} \mapsto \mathbb{R}$ *be poly-time computable functions such that* $s(\kappa) < a(\kappa)^2/10$ *for sufficiently large* $\kappa \in \mathbb{N}$*. Then there is a reduction converting an* (s, a)*-key agreement protocol in an infinite set* $\mathcal{I}$ *into a (fully fledged) key-agreement in* $\mathcal{I}$*. The reduction is fully black-box and oblivious to* $\mathcal{I}$*.*

3 Classification of Boolean Two-Party Protocols

In this section we formally define simulator, forecasters, decorelators and uncorrelated protocols discussed in Section 1, and formally state the main results of this paper. Throughout this section we focus on no-input, single-bit output, two-party protocols.

3.1 Simulators and Forecasters

The results of this section holds for *any* no-input, single-bit output two-party protocols, even inefficient ones.

3.1.1 Simulators

Recall that a simulator seeing the protocol transcript, outputs a pair of bits that looks indistinguishable from the parties' real outputs, from the point of view of an efficient distinguisher that sees only the protocol's transcript. We now define this concept precisely, and state our results.

Definition 3.1 (Simulator)**.** *A* simulator *is a* PPT *algorithm that on input in* $(1^\kappa, t) \in 1^* \times \{0,1\}^*$ *outputs two bits.*

We associate the following two distribution ensembles with a two-party protocol and a simulator.

Definition 3.2 (Real and simulated distributions)**.** *Let $\pi = (\mathsf{A}, \mathsf{B})$ be a single-bit output two-party protocol, and let Sim be a simulator. We define the real and simulated distribution ensembles REAL^{π} and $\text{SML}^{\pi,\mathsf{Sim}}$ as follows. For $\kappa \in \mathbb{N}$, let X_κ, Y_κ and T_κ be the parties' outputs and protocol transcript in a random execution of π_κ. Then*

Real: $\text{REAL}^{\pi}_{\kappa} = (X_\kappa, Y_\kappa, T_\kappa)$.

Simulated: $\text{SML}^{\pi,\mathsf{Sim}}_{\kappa} = (\mathsf{Sim}_\kappa(T_\kappa), T_\kappa)$.

(Recall that $\mathsf{Sim}_\kappa(t)$ denotes the output of Sim on input $(1^\kappa, t)$.)

The following theorem states that every single-bit output two-party protocol (even inefficient one) has a simulator.

Theorem 3.3 (Existence of simulators)**.** *For every single-bit output, two-party protocol π, $\rho > 0$ and infinite set $\mathcal{I} \subseteq \mathbb{N}$, there exist a simulator Sim and an infinite set $\mathcal{I}' \subseteq \mathcal{I}$ such that*

$$\text{REAL}^{\pi} \overset{\text{C}}{\approx}_{\rho,\mathcal{I}'} \text{SML}^{\pi,\mathsf{Sim}}.$$

Theorem 3.3 is an immediate corollary of the existence of forecasters theorem given below.

3.1.2 Forecasters

A forecaster seeing the protocol transcript, outputs a *description* of a two bits distribution, that looks indistinguishable from the parties' real outputs, from the point of view of an an efficient distinguisher that sees only the protocol's transcript. Thus, a forecaster is a specific method for constructing simulators: the resulting simulator outputs the two bits according the the distribution described by the forecaster.

Definition 3.4 (Forecasters)**.** *A forecaster F is a* PPTM *that on input $(1^\kappa, t) \in 1^* \times \{0,1\}^*$, outputs a triplet in $[0,1]^3$. We use $\mathsf{F}(1^\kappa, t; r)$ to denote the instantiation of $\mathsf{F}(1^\kappa, t)$ when using the string r as random coins.*[8]

We associate the following two distribution ensembles with a two-party protocol and a forecasters. To define these distributions, we associate triplets in $[0,1]^3$ with distribution over $\{0,1\}^2$ in the following way.

Notation 3.5. *For $p = (p_{\mathsf{A}}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1}) \in [0,1]^3$, let U_p denote the random variable over $\{0,1\}^2$ defined by $\Pr[U_p = (x,y)] = \Pr[U_{p_{\mathsf{A}}} = x] \cdot \Pr\left[U_{p_{\mathsf{B}|x}} = y\right]$. For $p = (p_{\mathsf{A}}, p_{\mathsf{B}}) \in [0,1]^2$, let U_p denote the random variable $U_{(p_{\mathsf{A}}, p_{\mathsf{B}}, p_{\mathsf{B}})}$.*

With this notation, the variable $U_p = (X', Y')$ is composed of two random variables such that $\Pr[X' = 1] = p_{\mathsf{A}}$ and for $b \in \{0,1\}$, $\Pr[Y' = 1 | X' = b] = p_{\mathsf{B}|b}$. In particular, if $p_{\mathsf{B}|0} = p_{\mathsf{B}|1}$ then (X', Y') are independent.

Definition 3.6 (Real and forecasted distributions)**.** *Let $\pi = (\mathsf{A}, \mathsf{B})$ be a single-bit output two-party protocol and let F be a forecaster. We define the real and forecasted distribution ensembles $\text{REAL}^{\pi,\mathsf{F}}$ and $\text{FST}^{\pi,\mathsf{F}}$ as follows. For $\kappa \in \mathbb{N}$, let X_κ, Y_κ and T_κ be the parties' outputs and protocol transcript in a random execution of π_κ, and let R_κ be a uniform and independent string whose length is the (maximal) number of coins used by F_κ. Then,*

[8] Since we only care about PPT algorithms, we will implicitly assume that the number of coins used by them on a given security parameter is efficiently computable.

Real: $\text{REAL}_\kappa^{\pi,\mathsf{F}} = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa)$.

Forecasted: $\text{FST}_\kappa^{\pi,\mathsf{F}} = (U_p, T_\kappa, R_\kappa)$ *for* $p = \mathsf{F}_\kappa(T_\kappa; R_\kappa) = (p_\mathsf{A}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1})$.

(Recall that $\mathsf{F}_\kappa(t;r)$ denotes the output of F on input $(1^\kappa, t)$ when using randomness r.)

The computational distance between the real and forecasted distribution measures how well the forecaster realizes the real distribution, in the eyes of a computationally bounded distinguisher.

Definition 3.7 (Forecaster indistinguishability)**.** *A forecaster* F *is* $(\rho, \mathcal{I})$-indistinguishable*, for* $\rho > 0$ *and infinite subset* $\mathcal{I} \subseteq \mathbb{N}$*, with respect to protocol* π*, if*

$$\text{REAL}^{\pi,\mathsf{F}} \overset{\text{C}}{\approx}_{\rho,\mathcal{I}} \text{FST}^{\pi,\mathsf{F}}.$$

That is, for sufficiently large $\kappa \in \mathcal{I}$, the forecasted and real distributions are ρ indistinguishable for poly-time distinguishers.

The following theorem states that every single-bit output two-party protocol (even inefficient one) has a forecaster.

Theorem 3.8 (Existence of forecasters)**.** *For every single-bit output two-party protocol* π*,* $\rho > 0$ *and infinite set* $\mathcal{I} \subseteq \mathbb{N}$*, there exist a forecaster* F *and an infinite set* $\mathcal{I}' \subseteq \mathcal{I}$*, such that* F *is* $(\rho, \mathcal{I}')$-indistinguishable *with respect to* π*.*

Theorem 3.8 is proven in Section 4 (appears there as Theorem 4.15). The existence of simulators immediately follows by the above theorem.

Proof of Theorem 3.3. Let F be the forecaster for π guaranteed by Theorem 3.8. Given a transcript of the protocol, the simulator runs F on this transcript, and outputs two bits according the distribution described by its output. □

Correlated protocols and key agreement. We measure the correlation of a forecaster with respect to a given distribution ensemble, as the "conditional correlation distance" of $\text{FST}^{\pi,\mathsf{F}}$. That is, the expectation over T, of the statistical distance of $\text{FST}^{\pi,\mathsf{F}}$ from a distribution in which the two outputs are a product.

We use the following notation to define the product distribution naturally induced by an arbitrary distribution over $\{0,1\}^2$.

Notation 3.9. *For triplet* $p = (p_\mathsf{A}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1}) \in [0,1]^3$*, let* $\mathsf{prod}(p) = (p_\mathsf{A}, (1-p_\mathsf{A}) \cdot p_{\mathsf{B}|0} + p_\mathsf{A} \cdot p_{\mathsf{B}|1})$.

That is, $U_{\mathsf{prod}(p)}$ is the product of marginals distribution of U_p. We now define the product of a forecasted distribution in the natural way.

Definition 3.10 (The product of a forecasted distribution)**.** *For a single-bit output two-party protocol* π *and forecaster* F*, we defined the* product forecasted distribution $\text{PFST}^{\pi,\mathsf{F}}$ of F with respect to π *by* $\text{PFST}_\kappa^{\pi,\mathsf{F}} = (U_{\mathsf{prod}(\mathsf{F}(T_\kappa;R_\kappa))}, T_\kappa, R_\kappa)$*, where* T_κ *and* R_κ *are as in Definition 3.6.*

The correlation of a forecaster with respect to a given distribution ensemble, is just the expected statistical distance between the forecasted distribution and its product.

Definition 3.11 (Correlated forecasters)**.** *A forecaster* F *is* $(\eta, \mathcal{I})$-correlated *with respect to two-party protocol* π*, for* $\eta > 0$ *and* $\mathcal{I} \subseteq \mathbb{N}$*, if for every* $\kappa \in \mathcal{I}$*,*

$$\mathrm{SD}(\mathrm{FST}_\kappa^{\pi,\mathsf{F}}, \mathrm{PFST}_\kappa^{\pi,\mathsf{F}}) \geq \eta$$

The following fact is immediate.

Proposition 3.12 (Indistinguishability plus low correlation implies closeness to product)**.** *Let* π *be a two-party protocol and* F *be a forecaster. Assume* F *is* $(\rho, \mathcal{I})$*-indistinguishable with respect to* π *for some* $\rho > 0$ *and infinite set* $\mathcal{I} \subseteq \mathbb{N}$ *and that for* $\eta > 0$ *there exists no infinite subset* $\mathcal{I}' \subseteq \mathcal{I}$ *for which* F *is* $(\eta, \mathcal{I}')$*-correlated with respect to* π*. Then*

$$\mathrm{REAL}^{\pi,\mathsf{F}} \overset{\mathrm{C}}{\approx}_{\rho+\eta,\mathcal{I}} \mathrm{PFST}^{\pi,\mathsf{F}}.$$

Sufficiently correlated protocols (i.e., have correlated and indistinguishable forecasters) are important since they can be used to construct key-agreement protocols.

Theorem 3.13 (Key-agreement from correlated protocols)**.** *Let* π *be a* PPT *two-party single-bit output protocol and let* F *be a forecaster. Assume there exist an infinite set* $\mathcal{I} \subseteq \mathbb{N}$*,* $\rho > 0$ *and* $\eta > 30\sqrt{\rho}$ *such that* F *is* $(\rho, \mathcal{I})$*-indistinguishable and* $(\eta, \mathcal{I})$*-correlated with respect to* π*. Then there exists a key-agreement protocol in* $\mathcal{I}$*.*

We prove Theorem 3.13 in Section 5.

3.2 Decorelators and the Dichotomy Theorem

In the introduction we explained the concept of decorrelators and uncorrelated protocols, in informal Definition 1.3. We now repeat the definition using more precise language.

Definition 3.14 (Decorelators)**.** *A* decorelator Decor *is a* PPTM *that on input* $(1^\kappa, t) \in 1^* \times \{0,1\}^*$*, outputs two numbers in* $[0,1]$*. We use* $\mathsf{Decor}(1^\kappa, t; r)$ *to denote the instantiation of* $\mathsf{Decor}(1^\kappa, t)$ *when using the string* r *as random coins.*

We associate the following two distribution ensembles with a two-party protocol and a decorelator.

Definition 3.15 (Real and uncorrelated distributions)**.** *Let* $\pi = (\mathsf{A}, \mathsf{B})$ *be a single-bit output two-party protocol, and let* Decor *be a decorelator. We define the* real and uncorrelated distribution ensembles $\mathrm{REAL}^{\pi,\mathsf{Decor}}$ *and* $\mathrm{UCR}^{\pi,\mathsf{Decor}}$ *as follows. For* $\kappa \in \mathbb{N}$*, let* X_κ*,* Y_κ *and* T_κ *be the parties' outputs and protocol transcript in a random execution of* π_κ*, and let* R_κ *be a uniform and independent string whose length is the (maximal) number of coins used by* Decor_κ *(see Footnote 8). Then,*

Real: $\mathrm{REAL}_\kappa^{\pi,\mathsf{Decor}} = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa)$.

Uncorrelated: $\mathrm{UCR}_\kappa^{\pi,\mathsf{Decor}} = (U_{p_\mathsf{A}}, U_{p_\mathsf{B}}, T_\kappa, R_\kappa)_{(p_\mathsf{A},p_\mathsf{B})=\mathsf{Decor}_\kappa(T_\kappa;R_\kappa)}$.

(Recall that $\mathsf{Decor}_\kappa(t; r)$ denotes the output of Decor on input $(1^\kappa, t)$ when using randomness r.) *Uncorrelated protocols*, are those protocols for which the above distributions are computational close.

Definition 3.16 (Uncorrelated protocols)**.** *Let $\pi = (\mathsf{A}, \mathsf{B})$ be a single-bit output two-party protocol, let $\rho > 0$ and $\mathcal{I} \subseteq \mathbb{N}$. Decorelator* Decor *is a $(\rho, \mathcal{I})$-*decorelator for π, if

$$\text{REAL}^{\pi,\mathsf{Decor}} \overset{\text{C}}{\approx}_{\rho,\mathcal{I}} \text{UCR}^{\pi,\mathsf{Decor}}.$$

Protocol π is $(\rho, \mathcal{I})$-uncorrelated, if it has a $(\rho, \mathcal{I})$-decorelator. Protocol π is io-ρ-uncorrelated, if there exists an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that π is $(\rho, \mathcal{I})$-uncorrelated.

A few remarks are in order:

Remark 3.17 (The role of R_κ in the definition above)**.** *We choose to include the randomness R_κ in the experiments $\text{REAL}_\kappa^{\pi,\mathsf{Decor}}$ and $\text{UCR}_\kappa^{\pi,\mathsf{Decor}}$. Loosely speaking, the inclusion of R_κ in the experiments is done to prevent a scenario where* Decor *uses the randomness R_κ in order to correlate between P_A and P_B. More precisely, we observe that a weaker notion (in which the experiments do not include R_κ) is not interesting (as in such a notion key-agreement protocol can be uncorrelated).*

Indeed, consider a decorrelator that uses a uniform bit R_κ and produces $P_\mathsf{A} = P_\mathsf{B} = R_\kappa$. Note that $(X'_\kappa, Y'_\kappa, T_\kappa)$ are computationally indistinguishable from a triplet $(X_\kappa, Y_\kappa, T_\kappa)$ that is the real distribution of a key-agreement. The insistence that Decor *"reveals its randomness" R_κ in the two experiments, prevents these problems, as can be seen formally in Theorems 3.20 and 3.23 (stated in Section 3.2.1) which loosely say that uncorrelated protocols are not key-agreement and cannot be used to construct key-agreement.*

This is the formal statement of our main theorem (that restates Theorem 1.4 from Section 1).

Theorem 3.18 (Dichotomy of two-party protocols)**.** *For every* PPT *single-bit output two-party protocol, one of the following holds:*

- *For every constant $\rho > 0$ and every infinite $\mathcal{I} \subseteq \mathbb{N}$, there exists an infinite set $\mathcal{I}' \subseteq \mathcal{I}$ such that the protocol is ρ-uncorrelated in $\mathcal{I}'$.*
- *Exists a two-party io key-agreement protocol.*

The proof of Theorem 3.18 readily follow the observations stated in the previous subsection.

Proof. Let $\rho > 0$ and let π be a PPT single-bit output two-party protocol. Let $\rho' = (\rho/60)^2$. By Theorem 3.8 there exists a forecaster F that is $(\rho', \mathcal{I}')$-indistinguishable with respect to π, for an infinite set $\mathcal{I}' \subseteq \mathcal{I}$. If there exists an infinite subset $\mathcal{I}'' \subseteq \mathcal{I}'$ for which F is $(\rho/2, \mathcal{I}'')$-correlated with respect to π, then by Theorem 3.13, there exists a two-party io key-agreement protocol.

Otherwise, let $\mathsf{Decor}(1^\kappa, t; r) = \mathsf{prod}(\mathsf{F}(1^\kappa, t; r))$ for $\mathsf{prod}(p)$ being the product distribution defined by the marginal of the distribution defined by p (see Notation 3.9). Proposition 3.12 yields that Decor is a $(\rho' + \rho/2 < \rho, \mathcal{I}')$-decorelator for π. □

Remark 3.19. *Assuming io key-agreement does not exist, Theorem 3.18 says that for every $\rho > 0$, the protocol is io-ρ-uncorrelated. We emphasize that this means that for every $\rho > 0$ there exists an infinite $\mathcal{I}$ and a (poly-time) $(\rho, \mathcal{I})$-decorelator for π. For every $\rho > 0$, however, the polynomial that bounds the running time of the decorrelator might be different.*

3.2.1 Properties of Uncorrelated Protocols

In this section we list two properties of uncorrelated protocols (that were listed informally in the introduction). We show that:

- Uncorrelated protocols are not key-agreement.
- Uncorrelated protocols cannot be transformed into key-agreement (in some precise sense described below).

Theorem 3.20 (An uncorrelated protocol is not a key agreement)**.** *Let $\pi = (\mathsf{A}, \mathsf{B})$ be a* PPT *single-bit output two-party protocol. Let $\mathcal{I} \subseteq \mathbb{N}$ be an infinite set. If π is $(\rho, \mathcal{I})$-uncorrelated then for every numbers s, a such that $s > a + 2\rho$, π is not an (s, a)-key agreement in $\mathcal{I}$.*

Proof. Let Decor be a $(\rho, \mathcal{I})$-decorrelator for π, let $\kappa \in \mathcal{I}$ and consider the distributions from Definition 3.15.

- $\text{REAL}_\kappa^{\pi,\mathsf{Decor}} = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa)$.
- $\text{UCR}_\kappa^{\pi,\mathsf{Decor}} = (X'_\kappa, Y'_\kappa, T_\kappa, R_\kappa)$.

We will show that there exists a PPTM E such that for every $\kappa \in \mathcal{I}$,

$$\Pr[\mathsf{E}(T_\kappa) = X'_\kappa] \geq \Pr[X'_\kappa = Y'_\kappa].$$

As $\text{REAL}^{\pi,\mathsf{Decor}}$ and $\text{UCR}^{\pi,\mathsf{Decor}}$ are ρ-indistinguishable in $\mathcal{I}$, and E is PPTM, it follows that for every sufficiently large $\kappa \in \mathcal{I}$:

$$\Pr[\mathsf{E}(T_\kappa) = X_\kappa] \geq \Pr[X_\kappa = Y_\kappa] - 2\rho.$$

Which gives the required consequence that π is not an io-key-agreement with a gap larger than 2ρ between agreement and secrecy.

We now define the PPTM E. Given input $t \in \text{Supp}(T_\kappa)$, E samples a uniform string r and applies $\mathsf{Decor}_\kappa(t; r) = (p_\mathsf{A}, p_\mathsf{B})$. It then outputs "one" iff $p_\mathsf{A} \geq \frac{1}{2}$. Note that for fixed (t, r),

$$\Pr[\mathsf{E}(T_\kappa) = X'_\kappa | T_\kappa = t, R_\kappa = r] = \max(p_\mathsf{A}, 1 - p_\mathsf{A}).$$

On the other hand, note that:

$$\Pr[X'_\kappa = Y'_\kappa | T_\kappa = t, R_\kappa = r] = p_\mathsf{A} \cdot p_\mathsf{B} + (1 - p_\mathsf{A}) \cdot (1 - p_\mathsf{B}) \leq \max(p_\mathsf{A}, 1 - p_\mathsf{A}).$$

By averaging, we conclude that:

$$\Pr[\mathsf{E}(T_\kappa) = X'_\kappa] \geq \Pr[X'_\kappa = Y'_\kappa]$$

and the theorem follows. □

We want to show that uncorrelated protocols cannot be "transformed" into key-agreement. We will be interested in a scenario in which a "black-box" transformation invokes a ρ-uncorrelated protocol $\pi = (\mathsf{A}, \mathsf{B})$, ℓ times, in order to construct a target protocol $\overline{\pi} = (\overline{\mathsf{A}}, \overline{\mathsf{B}})$. We can consider three types of transformations (in increasing order of strength)

- Transformations in which $\overline{\pi}$ only requires the outputs of the invocations (we call these black-box).
- Transformations in which in addition to the outputs, also use the transcripts of the ℓ invocations (we call these proper).
- Transformations that in addition to the outputs, and transcripts also use the parties' views of the ℓ invocations (we call these general).

We will give a precise definition shortly.

Note that in an uncorrelated protocol, it could be the case that there is a "hidden key-agreement" where following the protocol, the views of the two parties allow them to agree on a secret key. For example, the parties may run a key-agreement protocol but decide that their "formal outputs" X, Y are constants, and keep the key hidden in their view. Therefore, we cannot expect to show limitations on general transformations.

We will be able to show limitations on proper transformations that transform ρ-uncorrelated protocols into key-agreement protocols. We will explain below that the transformation that constructs an io key-agreement from the original protocol in Theorem 3.18, is a proper transformation.

Our limitations will be of the form: If a proper transformation constructs key-agreement from some protocol, then one can construct key-agreement *without* using the original protocol.

The argument for the limitation works by simply noting that PPT parties cannot distinguish the real output distribution of π from a simulated distribution of π, and so we can replace the ℓ real executions by uninteresting ℓ simulations, and still obtain a key-agreement protocol (with reduced gap between agreement and secrecy by a factor of $O(\ell \cdot \rho)$). Thus, if some gap remains, we can construct a meaningful key-agreement without using the original protocol.

We now state this result formally. We start by formally defining proper transformations.

Definition 3.21 (Proper transformation)**.** *Let $\pi = (\mathsf{A}, \mathsf{B})$ be a* PPT *single-bit output two-party protocol. We say that a protocol $\overline{\pi}$ is constructed from $\pi = (\mathsf{A}, \mathsf{B})$ using a* proper transformation *in ℓ invocations, if it has the following form.*

Protocol 3.22 ($\overline{\pi} = (\overline{\mathsf{A}}, \overline{\mathsf{B}})$)**.**

Input: Security parameter 1^κ.

Operation:

1. *The parties $\overline{\mathsf{A}}$ and $\overline{\mathsf{B}}$ engage in ℓ invocations of $(\mathsf{A}, \mathsf{B})(1^\kappa)$, where $\overline{\mathsf{A}}$ plays the role of A, and $\overline{\mathsf{B}}$ play the role of B.*

   Let $x = (x^1, \ldots, x^\ell)$, $y = (y^1, \ldots, y^\ell)$ and $t = (t^1, \ldots, t^\ell)$, denote the parties outputs and transcripts in the above executions.

2. *The parties $\overline{\mathsf{A}}$ and $\overline{\mathsf{B}}$ engage in a random execution of $(\widehat{\mathsf{A}}(x), \widehat{\mathsf{B}}(y))(1^\kappa, t)$, where $\widehat{\pi} = (\widehat{\mathsf{A}}, \widehat{\mathsf{B}})$ is an* arbitrary PPT *protocol, $\overline{\mathsf{A}}$ plays the role of $\widehat{\mathsf{A}}$, and $\overline{\mathsf{B}}$ play the role of $\widehat{\mathsf{B}}$.*

   The parties output their outputs in the above execution.

The following theorem shows that if π is ρ-uncorrelated, and if it is used by a proper transformation to construct a key agreement protocol in $\ell < \frac{1}{3\rho}$ invocations, then it is possible to take the proper transformation, and use it to construct a weak key-agreement protocol (without using the original protocol). This can be interpreted as saying that in fact, it was the transformation that constructed the key agreement, and the original protocol is uninteresting.

Theorem 3.23. *Let $\mathcal{I} \subseteq \mathbb{N}$ be an infinite set and let π be a* PPT *single-bit output two-party protocol that is $(\rho, \mathcal{I})$-uncorrelated. Let $\overline{\pi}$ be a* PPT *single-bit output two-party protocol that is constructed from π using a proper transformation in ℓ invocations. If $\overline{\pi}$ is an (s, a)-key agreement in $\mathcal{I}$, then the following protocol is an $(s + \ell \cdot \rho, a - \ell \cdot \rho)$-key agreement in $\mathcal{I}$.*

Protocol 3.24 ($\widetilde{\pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}})$)**.**

Input: Security parameter 1^κ.

Operation:

1. $\widetilde{\mathsf{A}}$ *samples ℓ pairs (t^i, r^i) from (T^i_κ, R^i_κ): for every $i \in [\ell]$ it independently emulates $\pi(1^\kappa)$ (on its own), sets t^i to be the emulation transcript, and tosses an independent r^i.*
2. $\widetilde{\mathsf{A}}$ *sends $(t^1, r^1), \ldots, (t^\ell, r^\ell)$ to $\widetilde{\mathsf{B}}$.*
3. *For $i \in [\ell]$:*
   (a) *Both $\widetilde{\mathsf{A}}$ and $\widetilde{\mathsf{B}}$ invoke $\mathsf{Decor}_\kappa(t^i, r^i)$, for* Decor *being the guaranteed decorelator for π, and let $(p^i_{\mathsf{A}}, p^i_{\mathsf{B}})$ be the outputs.*
   (b) *Party A samples $(x')^i \leftarrow U_{p^i_{\mathsf{A}}}$ and B samples $(y')^i \leftarrow U_{p^i_{\mathsf{B}}}$.*
   (I.e., the two-parties perform the simulated experiment in the i'th coordinate.)

   Let $x' = ((x')^1, \ldots, (x')^\ell)$ and $y' = ((y')^1, \ldots, (y')^\ell)$
4. *The parties $\widetilde{\mathsf{A}}$ and $\widetilde{\mathsf{B}}$ engage in $(\widehat{\mathsf{A}}(x'), \widehat{\mathsf{B}}(y'))(1^\kappa, t)$, where $\widehat{\pi} = (\widehat{\mathsf{A}}, \widehat{\mathsf{B}})$ is the (arbitrary) protocol used in the definition of $\overline{\pi}$, $\widetilde{\mathsf{A}}$ plays the role of $\widehat{\mathsf{A}}$, and $\widetilde{\mathsf{B}}$ play the role of $\widehat{\mathsf{B}}$.*

   The parties output their outputs in the above execution.

Proof. Let $\overline{X}_\kappa$, $\overline{Y}_\kappa$ and $\overline{T}_\kappa$ be the parties outputs and protocol transcript, in a random execution of $\overline{\pi}(1^\kappa)$, and let $\overline{Z}_\kappa = (\overline{X}_\kappa, \overline{Y}_\kappa, \overline{T}_\kappa)$. Since $\overline{\pi}$ is an (s, a)-key-agreement in $\mathcal{I}$, for every sufficiently large $\kappa \in \mathcal{I}$,

$$\Pr[\overline{X}_\kappa = \overline{Y}_\kappa] \geq \tfrac{1}{2} + a(\kappa) \tag{1}$$

and for every PPT E, for every sufficiently large $\kappa \in \mathcal{I}$

$$\Pr[\mathsf{E}(\overline{T}_\kappa) = \overline{X}_\kappa] \leq \tfrac{1}{2} + s(\kappa) \tag{2}$$

Let $\widetilde{X}_\kappa$, $\widetilde{Y}_\kappa$ and $\widetilde{T}_\kappa$ be the parties outputs and protocol transcript, in a random execution of $\widetilde{\pi}(1^\kappa)$, and let $\widetilde{Z}_\kappa = (\widetilde{X}_\kappa, \widetilde{Y}_\kappa, \widetilde{T}_\kappa)$. We will argue that $\left\{\overline{Z}_\kappa\right\}_{\kappa \in \mathbb{N}}$ and $\left\{\widetilde{Z}_\kappa\right\}_{\kappa \in \mathbb{N}}$ are $(\ell \cdot \rho)$-indistinguishable in $\mathcal{I}$, meaning that the two inequalities above also hold (with an additive "error

factor" of $\ell \cdot \rho$) when replacing $\overline{Z}_\kappa$ with $\widetilde{Z}_\kappa$. This will mean that $\widetilde{\pi}$ is a $(s + \ell \cdot \rho, a - \ell \cdot \rho)$-key agreement in $\mathcal{I}$.

Indeed, note that the only difference between $\overline{\pi}$ and $\widetilde{\pi}$ is that in $\overline{\pi}$ the parties use ℓ invocations of the real experiment whereas in $\widetilde{\pi}$ they use ℓ-invocations of the simulated experiment. By the hybrid argument and the fact that all protocols are PPT, it indeed follows that the distribution ensembles of $\overline{\pi}$ and $\widetilde{\pi}$ are $(\ell \cdot \rho)$-indistinguishable in $\mathcal{I}$, as required. □

We remark that the io key-agreement achieved in Theorem 3.18 works by using a proper transformation that invokes the original protocol ℓ times (where ℓ is a constant) in order to construct an io-(s, a)-key-agreement with constant $s < a$ (that protocol is later amplified into an io key-agreement with the standard choices of agreement and secrecy). By Theorem 3.23, if the original protocol is ρ-uncorrelated for every $\rho > 0$, then the existence of such a transformation implies key-agreement (without relying on the original protocol).

4 Existence of Forecasters

In this section we prove Theorem 3.8, that guarantees the existence of a forecaster for any single-bit output two-party protocol. Recall that a forecaster seeing the protocol transcripts, outputs a description of the distribution that aims to be indistinguishable from the parties' output, given this transcript.

We start, Section 4.1, by considering the one-sided variant of such a creature that we call *one-sided forecasters*. Such one-sided forecasters try to describe the output of *one* of the parties, possibly when conditioning on the other party output. In Section 4.2 we use the machinery developed in Section 4.1 for showing the existence of an indistinguishable forecaster for the distribution of both parties. To make distinction between the one-sided and two-sided case clear, in this section we call the latter *two-sided forecasters*.

Rather than considering the distributions induced by protocols, we consider the more general settings of arbitrary distribution ensembles.

4.1 One-Sided Forecasters

Given a distribution $Z = (V, T)$ over $\{0,1\} \times \{0,1\}^*$, we are interested in how well an efficient algorithm forecasts the probability space $V|_{T=t}$ when given t as input. We call such an algorithm a one-sided forecaster.

Definition 4.1 (One-sided forecasters)**.** *A* one-sided forecaster *is a* PPT *algorithm that on input pair* $(1^\kappa, t) \in 1^* \times \{0,1\}^*$*, outputs a number in* $[0,1]$*.*

Recall, that we use the abbreviation $\mathsf{F}_\kappa(\cdot) = \mathsf{F}(1^\kappa, \cdot)$.

Real and forecasted distributions. We associate the following two distribution ensembles, with a one-sided forecaster and a distribution ensemble over $\{0,1\} \times \{0,1\}^*$.

Definition 4.2 (Real and forecasted distributions)**.** *For a one-sided forecaster* F *and an ensemble of finite distributions* $Z = \{Z_\kappa = (V_\kappa, T_\kappa)\}_{\kappa \in \mathbb{N}}$ *over* $\{0,1\} \times \{0,1\}^*$*, we define the real and forecasted distributions* $\text{REAL}^{Z,\mathsf{F}}$ *and* $\text{FST}^{Z,\mathsf{F}}$ *by*

Real: $\text{REAL}_\kappa^{Z,\mathsf{F}} = (V_\kappa, T_\kappa, R_\kappa)$.

Forecasted: $\text{FST}_\kappa^{Z,\mathsf{F}} = (U_{\mathsf{F}(T_\kappa;R_\kappa)}, T_\kappa, R_\kappa)$.

Where R_κ is a uniform and independent string whose length is the (maximal) number of coins used by F_κ,[9] *$\mathsf{F}_\kappa(t;r)$ denotes the output of F_κ on input t and randomness r, and U_p stand for the Boolean random variable taking the value one with probability p.*

Namely, $\text{REAL}^{Z,\mathsf{F}}$ is just Z concatenated with the randomness of the length used by F, where $\text{FST}^{Z,\mathsf{F}}$ is the distribution forecasted by F (given T and R as input).

Indistinguishability. The computational distance between the real and forecasted distribution measures how well the forecaster realizes the real distribution, in the eyes of a computationally bounded distinguisher.

Definition 4.3 (Forecaster indistinguishability)**.** *A one-sided forecaster F is $(\rho, \mathcal{I})$-*indistinguishable *with respect to an ensemble of finite distributions $Z = \{Z_\kappa = (V_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ over $\{0,1\} \times \{0,1\}^*$, for $\rho > 0$ and $\mathcal{I} \subseteq \mathbb{N}$, if*

$$\text{REAL}^{Z,\mathsf{F}} \overset{\text{C}}{\approx}_{\rho,\mathcal{I}} \text{FST}^{Z,\mathsf{F}}.$$

That is, for every sufficiently large $\kappa \in \mathcal{I}$, the forecasted and real distributions are ρ indistinguishable for efficient distinguishers. The following is our main result for one-sided forecasters.

Theorem 4.4 (Existence of indistinguishable one-sided forecaster)**.** *For every ensemble of finite distributions $Z = \{Z_\kappa = (V_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ over $\{0,1\} \times \{0,1\}^*$, $\rho > 0$ and infinite $\mathcal{I} \subseteq \mathbb{N}$, there exists a one-sided forecaster F and an infinite set $\mathcal{I}' \subseteq \mathcal{I}$, such that F is $(\rho, \mathcal{I}')$-*indistinguishable *for Z.*

The proof of Theorem 4.4 readily follow from its two-sided equivalent proven in the next section.

Price of one-sided forecasters. We associate a price function with a given ensemble of finite distributions of the above form and a one-sided forecasters. The function intuitively measures the quality of the forecaster (a smaller price corresponds to a better forecast).

Definition 4.5 (Price of a one-sided forecasters)**.** *For a one-sided forecaster F and an ensemble of finite distributions $Z = \{Z_\kappa = (V_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ over $\{0,1\} \times \{0,1\}^*$, we define, for $\kappa \in \mathbb{N}$, the price of F_κ with respect to Z_κ by*

$$\mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) = \text{E}\left[(\mathsf{F}_\kappa(T_\kappa) - V_\kappa)^2\right]$$

where the expectation is taken over the distribution Z_κ and the random coins of F_κ.

Note that the price function is set up so that the minimal price is achieved by a one-sided forecaster F that on input $t \in \text{Supp}(T_\kappa)$ outputs $q_t = \Pr[V_\kappa = 1 \mid T_\kappa = t]$. A key observations about one-sided forecasters is the connection between distinguishability and price improvement proven in the next section.

[9] Since we only care about PPTM forecasters, we implicitly assume that the number of coins used by the forecaster on $(1^\kappa, t \in \text{Supp}(T_\kappa))$ is efficiently computable.

4.1.1 Distinguishability to Price Improvement

Our main technical lemma for one-sided forecaster is that a distinguisher for such a forecaster can be used to get a forecaster with an improved price value.

Lemma 4.6 (Distinguishability imply improved forecaster)**.** *Let* F *be a one-sided forecaster and let* $Z = \{Z_\kappa = (V_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ *over* $\{0,1\} \times \{0,1\}^*$ *be an ensemble of finite distributions. Assume there exists a* PPTM D *and an infinite* $\mathcal{I} \subseteq \mathbb{N}$*, such that for every* $\kappa \in \mathcal{I}$*,*

$$\left|\Pr\left[\mathsf{D}_\kappa(\text{REAL}_\kappa^{Z,\mathsf{F}}) = 1\right] - \Pr\left[\mathsf{D}_\kappa(\text{FST}_\kappa^{Z,\mathsf{F}}) = 1\right]\right| > \rho \tag{3}$$

Then there exists a forecaster F' *and an infinite subset* $\mathcal{I}' \subseteq \mathcal{I}$*, such that for every* $\kappa \in \mathcal{I}'$*,*

$$\mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) - \mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) > \rho^2.$$

Proof. Assume there exists PPTM D and infinite $\mathcal{I}$ for which Equation (3) holds for every $\kappa \in \mathcal{I}$. Let m_κ be a bound on the number of coins used by D_κ on inputs drawn from $\text{REAL}_\kappa^{Z,\mathsf{F}}$ or $\text{FST}_\kappa^{Z,\mathsf{F}}$, and let R^{D} be an independent uniform string of length m_κ. We assume without loss of generality that for an infinite subset $\mathcal{I}' \subseteq \mathcal{I}$, for every $\kappa \in \mathcal{I}'$ it holds that

$$\Pr\left[\mathsf{D}_\kappa(\text{REAL}_\kappa^{Z,\mathsf{F}}; R_\kappa^{\mathsf{D}}) = 1\right] - \Pr\left[\mathsf{D}_\kappa(\text{FST}_\kappa^{Z,\mathsf{F}}; R_\kappa^{\mathsf{D}}) = 1\right] > \rho.$$

The following algorithm uses D for finding the subset of inputs to be changed for getting a better forecast.

Algorithm 4.7 ($\widehat{\mathsf{F}}_\gamma^{\mathsf{F},\mathsf{D}}$)**.**

Parameters: $\gamma > 0$.

Oracles: algorithms D *and* F.

Input: $(1^\kappa, t; r, r^{\mathsf{D}})$.

Operation:

1. *If* $\mathsf{D}_\kappa(1, t, r; r^{\mathsf{D}}) = 1$ *and* $\mathsf{D}_\kappa(0, t, r; r^{\mathsf{D}}) = 0$*, output* $\mathsf{F}_\kappa(t; r) + \gamma$.
2. *If* $\mathsf{D}_\kappa(0, t, r; r^{\mathsf{D}}) = 1$ *and* $\mathsf{D}_\kappa(1, t, r; r^{\mathsf{D}}) = 0$*, output* $\mathsf{F}_\kappa(t; r) - \gamma$.
3. *Else, output* $\mathsf{F}_\kappa(t; r)$.

Note that the output might not belong to $[0, 1]$.

Since D and F are PPTM, so is $\widehat{\mathsf{F}}_\gamma^{\mathsf{F},\mathsf{D}}$. The following claim states that for the right choice of γ, the above algorithm yields an improved forecasters.

Claim 4.8. *Let* $\gamma \in [0, \rho]$ *and let* $\widehat{\mathsf{F}} = \widehat{\mathsf{F}}_\gamma^{\mathsf{F},\mathsf{D}}$ *be according to Algorithm 4.7. Then* $\mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) - \mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa) > \gamma(2\rho - \gamma)$ *for every* $\kappa \in \mathcal{I}'$.

The proof of Claim 4.8 is given below, but we first use it to conclude the proof of the lemma. By taking $\gamma = \rho$, Claim 4.8 yields the desirable result that $\mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) - \mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa) > \rho^2$. Still, algorithm $\widehat{\mathsf{F}}$ may not be a valid forecaster, since it may output values outside of $[0, 1]$. Fortunately,

this is not an issue, since we can use it to define the following valid forecaster F' that preforms as well as $\widehat{\mathsf{F}}$. For $\kappa \in \mathbb{N}$, define

$$\mathsf{F}'_\kappa(t,r,r^{\mathsf{D}}) = \begin{cases} \widehat{\mathsf{F}}_\kappa(t,r,r^{\mathsf{D}}) & \text{if } \widehat{\mathsf{F}}_\kappa(t,r,r^{\mathsf{D}}) \in [0,1] \\ 1 & \text{if } \widehat{\mathsf{F}}_\kappa(t,r,r^{\mathsf{D}}) > 1 \\ 0 & \text{if } \widehat{\mathsf{F}}_\kappa(t,r,r^{\mathsf{D}}) < 0 \end{cases}$$

We claim that $\mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) \leq \mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa)$. This follows because in the definition of price, the term $|\mathsf{F}(T_\kappa) - V_\kappa|$ does not increase by making sure that the number forecasted by F, is in $[0,1]$, as done above. It follows that $\mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) \leq \mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa) < \mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) - \rho^2$, for every $\kappa \in \mathcal{I}'$, concluding the proof. □

Proof of Claim 4.8.

Proof of Claim 4.8. Fix $\kappa \in \mathcal{I}'$ and omit it when clear from the context. Let $T' = (T, R, R^{\mathsf{D}})$ and for $t' = (t, r, r^{\mathsf{D}}) \in \mathrm{Supp}(T')$ let $\mathsf{F}(t') = \mathsf{F}(t;r)$. Let $\mathcal{G}_{10} = \{t' \colon \mathsf{D}(0,t') = 1 \wedge \mathsf{D}(1,t') = 0\}$, $\mathcal{G}_{01} = \{\mathsf{D}(0,t') = 0 \wedge \mathsf{D}(1,t') = 1\}$, $\mathcal{G} = \mathcal{G}_{01} \cup \mathcal{G}_{10}$, and let $\overline{\mathcal{G}} = \mathrm{Supp}(T') \setminus \mathcal{G}$. For a given set $\mathcal{S}$ let $\mathbb{1}_{\mathcal{S}}(\cdot)$ denote the characteristic function of the set, that is, $\mathbb{1}_{\mathcal{S}}(t') = 1$ if $t' \in \mathcal{S}$ and $\mathbb{1}_{\mathcal{S}}(t') = 0$ otherwise.

We make the following observations (proven below) regarding the above sets

Claim 4.9. *The followings hold.*

- $\mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\overline{\mathcal{G}}}(T')\right] - \mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\overline{\mathcal{G}}}(T')\right] = 0.$
- $\mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] - \mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] = -2\gamma \cdot \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] - \gamma^2 \cdot \Pr\left[T' \in \mathcal{G}_{01}\right].$
- $\mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - \mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] = 2\gamma \cdot \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - \gamma^2 \cdot \Pr\left[T' \in \mathcal{G}_{10}\right].$

Claim 4.10. $\mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] > \rho.$

Given the above claims, we deduce that

$$\begin{aligned}
&\mathsf{price}(\mathsf{F}) - \mathsf{price}(\widehat{\mathsf{F}}) \\
&= \mathrm{E}\left[(\mathsf{F}(T') - V)^2\right] - \mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2\right] \\
&= \mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\overline{\mathcal{G}}}(T')\right] + \mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] + \mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] \\
&\quad - \mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\overline{\mathcal{G}}}(T')\right] - \mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] - \mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] \\
&= 2\gamma(\mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right]) - \gamma^2 \cdot \Pr\left[T' \in \mathcal{G}\right]. \\
&\geq 2\gamma\rho - \gamma^2 \\
&> 2\gamma(\rho - \gamma).
\end{aligned}$$

The third equality is by Claim 4.9, and the inequality is by Claim 4.10. □

Proof of Claim 4.9. The first item holds since by definition $\widehat{\mathsf{F}}(t') = \mathsf{F}(t')$ for every $t' \notin \mathcal{G}$. For the second item, since $\widehat{\mathsf{F}}(t') = \mathsf{F}(t') + \gamma$ for every $t' \in \mathcal{G}_{01}$, it holds that

$$\begin{aligned}
&\mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] \\
&= \mathrm{E}\left[(\mathsf{F}(T') + \gamma - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] \\
&= \mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] + 2\gamma \cdot \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] + \gamma^2 \cdot \Pr\left[T' \in \mathcal{G}_{01}\right].
\end{aligned}$$

For the third item, a similar calculation yields that

$$\begin{aligned}
&\mathrm{E}\left[(\widehat{\mathsf{F}}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] \\
&= \mathrm{E}\left[(\mathsf{F}(T') - V)^2 \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - 2\gamma \cdot \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] + \gamma^2 \cdot \Pr\left[T' \in \mathcal{G}_{10}\right].
\end{aligned}$$

□

Proof of Claim 4.10. Since $\mathsf{D}(1, t') = \mathsf{D}(0, t')$ for every $t' \notin \mathcal{G}$, it holds that $\mathrm{E}\left[\mathsf{D}(V, T') \cdot \mathbb{1}_{\overline{\mathcal{G}}}(T')\right] = \mathrm{E}\left[\mathsf{D}(U_{\mathsf{F}(T')}, T') \cdot \mathbb{1}_{\overline{\mathcal{G}}}(T')\right]$. Since, by assumption, $\mathrm{E}\left[\mathsf{D}(V, T')\right] - \mathrm{E}\left[\mathsf{D}(U_{\mathsf{F}(T')}, T')\right] > \rho$, we conclude that

$$\mathrm{E}\left[\mathsf{D}(V, T') \cdot \mathbb{1}_{\mathcal{G}}(T')\right] - \mathrm{E}\left[\mathsf{D}(U_{\mathsf{F}(T')}, T') \cdot \mathbb{1}_{\mathcal{G}}(T')\right] > \rho \tag{4}$$

By definition of $\mathcal{G}_{10}$,

$$\begin{aligned}
&\mathrm{E}\left[\mathsf{D}(V, T') \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - \mathrm{E}\left[\mathsf{D}(U_{\mathsf{F}(T')}, T') \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] \\
&= \Pr\left[(\mathsf{D}(V, T') \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')) = 1\right] - \Pr\left[(\mathsf{D}(U_{\mathsf{F}(T')}, T') \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')) = 1\right] \\
&= \Pr\left[\mathbb{1}_{\mathcal{G}_{10}}(T') = 1\right] - \mathrm{E}\left[V \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - (\Pr\left[\mathbb{1}_{\mathcal{G}_{10}}(T') = 1\right] - \mathrm{E}\left[U_{\mathsf{F}(T')} \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right]) \\
&= \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right],
\end{aligned} \tag{5}$$

and similarly

$$\mathrm{E}\left[\mathsf{D}(V, T') \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] - \mathrm{E}\left[\mathsf{D}(U_{\mathsf{F}(T')}, T') \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] = -\mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] \tag{6}$$

Since $\mathcal{G}_{01}$ and $\mathcal{G}_{10}$ are a partition of $\mathcal{G}$, we conclude that $\mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{10}}(T')\right] - \mathrm{E}\left[(\mathsf{F}(T') - V) \cdot \mathbb{1}_{\mathcal{G}_{01}}(T')\right] > \rho$. □

4.2 Two-Sided Forecasters

Given a distribution $Z = (X, Y, T)$ over $\{0,1\}^2 \times \{0,1\}^*$, we are interested in how well an efficient algorithm forecasts the probability space $(X, Y)|_{T=t}$, given t as input. We call such an algorithm a two-sided forecaster. Since the probability space $(X, Y)|_{T=t}$ is determined by three quantities:

- $\Pr[X = 1 \mid T = t]$,
- $\Pr[Y = 1 \mid T = t, X = 0]$ and
- $\Pr[Y = 1 \mid T = t, X = 1]$,

A two-sided forecaster F should output a triplet of numbers $(p_1, p_2, p_3) \in [0,1]^3$.

Definition 4.11 (Two-sided forecasters)**.** *A two-sided forecaster* F *is a* PPTM *that on input* $(1^\kappa, t) \in 1^* \times \{0,1\}^*$*, outputs a triplet in* $[0,1]^3$.

Real and forecasted distributions. Similarly to the one-sided case, we associate the following two distribution ensembles with a given ensemble of finite distributions (of the right form) and a two-sided forecaster. To define these distributions, we associate triplets in $[0,1]^3$ with distribution over $\{0,1\}^2$ in the following way.

Recall that in Section 3.1.2, we use Notation 3.5, restated below.

Notation 4.12. *For $p = (p_{\mathsf{A}}, p_{\mathsf{B}|0}, p_{\mathsf{B}|1}) \in [0,1]^3$, let U_p denote the random variable over $\{0,1\}^2$ defined by $\Pr[U_p = (x,y)] = \Pr[U_{p_{\mathsf{A}}} = x] \cdot \Pr\left[U_{p_{\mathsf{B}|x}} = y\right]$. For $p = (p_{\mathsf{A}}, p_{\mathsf{B}}) \in [0,1]^2$, let U_p denote the random variable $U_{(p_{\mathsf{A}}, p_{\mathsf{B}}, p_{\mathsf{B}})}$.*

Definition 4.13 (Real and forecasted distributions, two-sided case)**.** *For a two-sided forecaster F and an ensemble of finite distributions $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa \in \mathbb{N}}$ over $\{0,1\} \times \{0,1\} \times \{0,1\}^*$, we define the real and forecasted distributions $\text{REAL}^{Z,\mathsf{F}}$ and $\text{FST}^{Z,\mathsf{F}}$ by*

Real: $\text{REAL}^{Z,\mathsf{F}}_\kappa = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa)$.

Forecasted: $\text{FST}^{Z,\mathsf{F}}_\kappa = (U_{\mathsf{F}(T_\kappa; R_\kappa)}, T_\kappa, R_\kappa)$.

Where R_κ is a uniform and independent string whose length is the (maximal) number of coins used by F_κ,[10] *and $\mathsf{F}_\kappa(t;r)$ denotes the output of F_κ on input t and randomness r.*

Namely, $\text{REAL}^{Z,\mathsf{F}}$ is just Z concatenated with the randomness of the length used by F, where $\text{FST}^{Z,\mathsf{F}}$ is the distribution forecasted by F (given T and R as input).

Indistinguishability. Similarly to the one-sided case, the computational distance between the real and forecasted distribution, measures how well the forecaster realizes the real distribution, from the point of view of a computationally bounded distinguisher.

Definition 4.14 (Forecaster indistinguishability, two-sided case)**.** *A two-sided forecaster F is $(\rho, \mathcal{I})$-*indistinguishable*, for $\rho > 0$ and infinite subset $\mathcal{I} \subseteq \mathbb{N}$, with respect to an ensemble of finite distributions $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa \in \mathbb{N}}$ over $\{0,1\} \times \{0,1\} \times \{0,1\}^*$, if*

$$\text{REAL}^{Z,\mathsf{F}} \overset{\text{C}}{\approx}_{\rho,\mathcal{I}} \text{FST}^{Z,\mathsf{F}}.$$

That is, for sufficiently large $\kappa \in \mathcal{I}$, the forecasted and real distributions are ρ indistinguishable for poly-time distinguishers. In Section 4.2.1, we prove our main result for two-sided forecasters.

Theorem 4.15 (Existence of indistinguishable two-sided forecaster)**.** *For every ensemble of finite distributions $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa \in \mathbb{N}}$ over $\{0,1\} \times \{0,1\} \times \{0,1\}^*$, $\rho > 0$ and an infinite $\mathcal{I} \subseteq \mathbb{N}$, there exists a two-sided forecaster F and an infinite set $\mathcal{I}' \subseteq \mathcal{I}$, such that F is $(\rho, \mathcal{I}')$-indistinguishable with respect to Z.*

[10] As in the one-sided case, since we only care about PPTM's, we will implicitly assume that the number of coins used by them on a given security parameter is efficiently computable.

The price of two-sided forecasters. Similarly to the one-sided case, we associate a price function with a given ensemble of finite distributions of the above form and a two-sided forecaster, which intuitively measures the quality of the forecaster (a smaller price corresponds to a better forecast).

Notation 4.16. *Given a two-sided forecaster* F *and* $i \in \{1,2,3\}$*, we let* $\mathsf{F}^i(t) = \mathsf{F}(t)_i$*. Given an ensemble of finite distributions* $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ *over* $\{0,1\} \times \{0,1\} \times \{0,1\}^*$*, let* $Z^1 = \left\{Z^1_\kappa = (X_\kappa, T_\kappa)\right\}_{\kappa\in\mathbb{N}}$*,* $Z^2 = \left\{Z^2_\kappa = ((Y_\kappa, T_\kappa) \mid X_\kappa = 0)\right\}_{\kappa\in\mathbb{N}}$ *and* $Z^3 = \left\{Z^3_\kappa = ((Y_\kappa, T_\kappa) \mid X_\kappa = 1)\right\}_{\kappa\in\mathbb{N}}$*.*[11]

Namely, F^i is the one-sided forecaster induced by F for Z^i. The price of a two-sided forecaster with respect to an ensemble of finite distributions Z, is defined as the weighted sum of the price of its induced one-sided forecasters with respect to the relevant distributions.

Definition 4.17 (Price of a two-sided forecasters)**.** *The price of a two-sided forecaster with respect to an ensemble of finite distributions* $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ *over* $\{0,1\} \times \{0,1\} \times \{0,1\}^*$*, is defined for* $\kappa \in \mathbb{N}$ *by*

$$\mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) = \mathsf{price}_{Z^1_\kappa}(\mathsf{F}^1_\kappa) + \Pr\left[X_\kappa = 0\right] \cdot \mathsf{price}_{Z^2_\kappa}(\mathsf{F}^2_\kappa) + \Pr\left[X_\kappa = 1\right] \cdot \mathsf{price}_{Z^3_\kappa}(\mathsf{F}^3_\kappa)$$

for price *being the (one-sided) price function from Definition 4.5.*

The following relation between price and indistinguishability, proven in Section 4.2.2, is a main tool in the proof of Theorem 4.15.

Lemma 4.18 (Distinguishability to price improvement, two-sided case)**.** *Let* F *be a two-sided forecaster and let* $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ *be an ensemble of finite distributions over* $\{0,1\} \times \{0,1\} \times \{0,1\}^*$*. If there exists a* PPTM D *and infinite* $\mathcal{I} \subseteq \mathbb{N}$ *such that*

$$\left|\Pr\left[\mathsf{D}_\kappa(\mathrm{REAL}^{Z,\mathsf{F}}_\kappa) = 1\right] - \Pr\left[\mathsf{D}_\kappa(\mathrm{FST}^{Z,\mathsf{F}}_\kappa) = 1\right]\right| > \rho$$

for every $\kappa \in \mathcal{I}$*, then there exists an infinite subset* $\mathcal{I}' \subseteq \mathcal{I}$ *and a two-sided forecaster* F' *such that* $\mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) < \mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) - (\rho/3)^3$ *for every* $\kappa \in \mathcal{I}'$*.*

Optimal forecasters. Roughly speaking, an optimal forecaster with respect to distribution Z, has the lowest price among all other forecasters with respect to this distribution. The existence of such forecasters for any ensemble of finite distributions, is the corner stone for the proof of our main result.

Definition 4.19 (Optimal forecasters)**.** *A two-sided forecaster* F *is* $(\mu,\mathcal{I})$-optimal with respect to an ensemble of finite distributions $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ over $\{0,1\} \times \{0,1\} \times \{0,1\}^*$*, for* $\mu > 0$ *and infinite* $\mathcal{I} \subseteq \mathbb{N}$*, if for every two-sided forecaster* F' *and every sufficiently large* $\kappa \in \mathcal{I}$*,* $\mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) \leq \mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) + \mu$*.*

The following fact, proven in Section 4.2.3, is a main tool in the proof of Theorem 4.15.

[11] Following the convention we coin in Section 2.1, Z^2_κ [resp., Z^3_κ] is arbitrarily defined if $\Pr\left[X_\kappa = 0\right] = 0$ [resp., $\Pr\left[X_\kappa = 0\right] = 1$].

Lemma 4.20 (Existence of optimal forecaster)**.** *For every ensemble of finite distributions $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ over $\{0,1\}\times\{0,1\}\times\{0,1\}^*$, $\mu > 0$ and infinite $\mathcal{I} \subseteq \mathbb{N}$, there exists a two-sided forecaster F and an infinite set $\mathcal{I}' \subseteq \mathcal{I}$, such that F is $(\mu, \mathcal{I}')$-optimal with respect to Z.*

Remark 4.21. *We emphasize that the proof of Lemma 4.20 is what restricts us to constant distinguishability error in the main theorem. The rest of the proof goes through for any non-negligible error.*

4.2.1 Existence of Indistinguishable Forecaster

In this section we prove our main result for two-sided forecasters.

Theorem 4.22 (Existence of indistinguishable two-sided forecaster, restated)**.** *For every ensemble of finite distributions $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ over $\{0,1\}\times\{0,1\}\times\{0,1\}^*$, $\rho > 0$ and an infinite $\mathcal{I} \subseteq \mathbb{N}$, there exists a two-sided forecaster F and an infinite set $\mathcal{I}' \subseteq \mathcal{I}$, such that F is $(\rho, \mathcal{I}')$-indistinguishable with respect to Z.*

Proof. The proof follows by the existence of an optimal forecaster, and by the fact that a distinguisher can be used to improve a forecaster.

Let $\mu = (\rho/3)^3$. By Lemma 4.20 there exists an infinite subset $\mathcal{I}' \subseteq \mathcal{I}$ and a forecaster F that is $(\mu, \mathcal{I}')$-optimal with respect to Z. We now claim that F is also $(\rho, \mathcal{I}')$-indistinguishable with respect to Z, as desired.

Assume toward contradiction, that there exists an infinite subset $\mathcal{I}'' \subseteq \mathcal{I}'$ and a PPTM D such that $\left|\Pr\left[\mathsf{D}_\kappa(\text{REAL}_\kappa^{Z,\mathsf{F}}) = 1\right] - \Pr\left[\mathsf{D}_\kappa(\text{FST}_\kappa^{Z,\mathsf{F}}) = 1\right]\right| > \rho$, for every $\kappa \in \mathcal{I}''$. By Lemma 4.18 there exists an infinite subset $\hat{\mathcal{I}} \subseteq \mathcal{I}''$ and a forecaster $\widehat{\mathsf{F}}$ such that, $\mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) - \mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa) > (\rho/3)^3 = \mu$ for every $\kappa \in \hat{\mathcal{I}}$. Since $\hat{\mathcal{I}} \subseteq \mathcal{I}'$, this is contradiction to the fact that F is $(\mu, \mathcal{I}')$-optimal. □

4.2.2 Distinguishability to Price Improvement

In this section we prove the following lemma.

Lemma 4.23 (Distinguishability to price improvement, two-sided case, restated)**.** *Let F be a two-sided forecaster and let $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ be an ensemble of finite distributions over $\{0,1\}\times\{0,1\}\times\{0,1\}^*$. If there exists a PPTM D and infinite $\mathcal{I} \subseteq \mathbb{N}$ such that*

$$\left|\Pr\left[\mathsf{D}_\kappa(\text{REAL}_\kappa^{Z,\mathsf{F}}) = 1\right] - \Pr\left[\mathsf{D}_\kappa(\text{FST}_\kappa^{Z,\mathsf{F}}) = 1\right]\right| > \rho$$

for every $\kappa \in \mathcal{I}$, then there exists an infinite subset $\mathcal{I}' \subseteq \mathcal{I}$ and a two-sided forecaster F' such that $\mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) < \mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) - (\rho/3)^3$ for every $\kappa \in \mathcal{I}'$.

We use the following lemma, that allows us to reduce the proof of the above lemma to the single-sided case.

Lemma 4.24 (Two-sided distinguisher implies one-sided distinguisher)**.** *Let F be a two-sided forecaster, and let $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ be an ensemble of finite distributions over $\{0,1\}\times\{0,1\}\times\{0,1\}^*$. Let $\mathsf{F}^1, \mathsf{F}^2, \mathsf{F}^3$ and Z^1, Z^2, Z^3, be the one-sided forecasters and the ensembles of finite distributions defined according to Notation 4.16 with respect to F and Z. Assume there exists PPTM D and an infinite $\mathcal{I} \subseteq \mathbb{N}$, such that for every $\kappa \in \mathcal{I}$,*

$$\left|\Pr\left[\mathsf{D}_\kappa(\text{REAL}_\kappa^{Z,\mathsf{F}}) = 1\right] - \Pr\left[\mathsf{D}_\kappa(\text{FST}_\kappa^{Z,\mathsf{F}}) = 1\right]\right| > \rho$$

Then there exists a PPTM D' *and an infinite subset* $\mathcal{I}' \subseteq \mathcal{I}$ *such that one of the following hold:*

- *For every* $\kappa \in \mathcal{I}'$, $\left|\Pr\left[\mathsf{D}'_\kappa(\text{REAL}_\kappa^{Z^1,\mathsf{F}^1}) = 1\right] - \Pr\left[\mathsf{D}'_\kappa(\text{FST}_\kappa^{Z^1,\mathsf{F}^1}) = 1\right]\right| > \rho/3$.
- *There exists* $b \in \{0,1\}$*, such that for every* $\kappa \in \mathcal{I}'$,

$$\left|\Pr\left[\mathsf{D}'_\kappa(\text{REAL}_\kappa^{Z^{2+b},\mathsf{F}^{2+b}}) = 1\right] - \Pr\left[\mathsf{D}'_\kappa(\text{FST}_\kappa^{Z^{2+b},\mathsf{F}^{2+b}}) = 1\right]\right| \cdot \Pr[X = b] > \rho/3.$$

where the distributions $\text{REAL}^{Z^i,\mathsf{F}^i}$ *and* $\text{FST}^{Z^i,\mathsf{F}^i}$ *above, are the "one-sided" distributions according to Definition 4.2.*

Lemma 4.24 is proven below, but we first use it for proving Lemma 4.23.

Proof of Lemma 4.23 . By Lemma 4.24, there exists a PPTM D', an infinite set $\mathcal{I}' \subseteq \mathcal{I}$ and a fixed $i^* \in [3]$, such that for every $\kappa \in \mathcal{I}'$:

$$\left|\Pr\left[\mathsf{D}'_\kappa(\text{REAL}_\kappa^{Z^{i^*},\mathsf{F}^{i^*}}) = 1\right] - \Pr\left[\mathsf{D}'_\kappa(\text{FST}_\kappa^{Z^{i^*},\mathsf{F}^{i^*}}) = 1\right]\right| > \rho/3 \tag{7}$$

and if $i^* \in \{2,3\}$, then also

$$\Pr[X_\kappa = (i^* - 2)] > \rho/3 \tag{8}$$

By Lemma 4.6 and Equation (7), there exist a one-sided forecaster $\widehat{\mathsf{F}}$ and an infinite set $\widehat{\mathcal{I}} \subseteq \mathcal{I}'$, such that for every $\kappa \in \widehat{\mathcal{I}}$:

$$\mathsf{price}_{Z_\kappa^{i^*}}(\mathsf{F}_\kappa^{i^*}) - \mathsf{price}_{Z_\kappa^{i^*}}(\widehat{\mathsf{F}}_\kappa) > (\rho/3)^2 \tag{9}$$

Consider the two-sided forecaster F' resulting by replacing F^{i^*} with $\widehat{\mathsf{F}}$. That is, $\mathsf{F}'(t) = (\mathsf{F}'^1(t), \mathsf{F}'^2(t), \mathsf{F}'^3(t))$, for $\mathsf{F}'^i = \widehat{\mathsf{F}}$ for $i = i^*$, and $\mathsf{F}'^i = \mathsf{F}^i$ otherwise. The definition of the price function yields the following for every $\kappa \in \widehat{\mathcal{I}}$:

If $i^* = 1$, then

$$\mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) - \mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) = \mathsf{price}_{Z_\kappa^1}(\mathsf{F}_\kappa^1) - \mathsf{price}_{Z_\kappa^1}(\widehat{\mathsf{F}}_\kappa) > (\rho/3)^2$$

and if $i^* \in \{2,3\}$, then

$$\begin{aligned}\mathsf{price}_{Z_\kappa}(\mathsf{F}'_\kappa) - \mathsf{price}_{Z_\kappa}(\mathsf{F}_\kappa) &= \Pr[X_\kappa = (i^* - 2)] \cdot (\mathsf{price}_{Z_\kappa^{i^*}}(\mathsf{F}_\kappa^{i^*}) - \mathsf{price}_{Z_\kappa^{i^*}}(\widehat{\mathsf{F}}_\kappa)) \\ &> \Pr[X_\kappa = (i^* - 2)] \cdot (\rho/3)^2 \\ &\geq (\rho/3)^3,\end{aligned}$$

where the last inequality holds by Equation (8). This concludes the proof. □

Proof of Lemma 4.24.

Proof of Lemma 4.24. We use the following algorithm to define three different distinguishers, and then prove that at least one of them can serve as D'.

Algorithm 4.25 (A).

Input: Security parameter 1^κ *and* $(v,t,r) \in \{0,1\} \times \{0,1\}^* \times \{0,1\}^*$.

Operation: If $v = 0$, *output* $\mathsf{F}^2_\kappa(t,r)$, *else, output* $\mathsf{F}^3_\kappa(t,r)$.

By definition,

$$\text{FST}^{Z,\mathsf{F}}_\kappa = (X'_\kappa, U_{\mathsf{A}_\kappa(X'_\kappa,T_\kappa,R_\kappa)}, T_\kappa, R_\kappa) \tag{10}$$

for $X'_\kappa = U_{\mathsf{F}^1(T_\kappa;R_\kappa)}$. Let $\mathsf{D}^1_\kappa(v,t,r) = \mathsf{D}_\kappa(v, U_{\mathsf{A}_\kappa(v,t,r)}, t, r)$, $\mathsf{D}^2_\kappa(v,t,r) = \mathsf{D}_\kappa(0,v,t,r)$ and $\mathsf{D}^3_\kappa(v,t) = \mathsf{D}_\kappa(1,v,t,r)$. We conclude the proof using the following claim, proven below.

Claim 4.26. *Let* $\kappa \in \mathbb{N}$ *be such that* $\left|\Pr\left[\mathsf{D}_\kappa(\text{REAL}^{Z,\mathsf{F}}_\kappa) = 1\right] - \Pr\left[\mathsf{D}_\kappa(\text{FST}^{Z,\mathsf{F}}_\kappa) = 1\right]\right| > \rho$. *Then (at least) one of the following holds,*

1. $\left|\Pr\left[\mathsf{D}^1_\kappa(\text{REAL}^{Z^1,\mathsf{F}^1}_\kappa) = 1\right] - \Pr\left[\mathsf{D}^1_\kappa(\text{FST}^{Z^1,\mathsf{F}^1}_\kappa) = 1\right]\right| > \rho/3$,
2. $\left|\Pr\left[\mathsf{D}^2_\kappa(\text{REAL}^{Z^2,\mathsf{F}^2}_\kappa) = 1\right] - \Pr\left[\mathsf{D}^2_\kappa(\text{FST}^{Z^2,\mathsf{F}^2}_\kappa) = 1\right]\right| \cdot \Pr[X = 0] > \rho/3$, *or*
3. $\left|\Pr\left[\mathsf{D}^3_\kappa(\text{REAL}^{Z^3,\mathsf{F}^3}_\kappa) = 1\right] - \Pr\left[\mathsf{D}^3_\kappa(\text{FST}^{Z^3,\mathsf{F}^3}_\kappa) = 1\right]\right| \cdot \Pr[X = 1] > \rho/3$.

By Claim 4.26 and the Pigeonhole principle, there exists $i \in [3]$ and an infinite set $\mathcal{I}' \subseteq \mathcal{I}$, such that D^i satisfies the i$^{\text{th}}$ item in the claim for every $\kappa \in \mathcal{I}'$. Thus, the proof follows by taking $\mathsf{D}' = \mathsf{D}^i$. □

Proof of Claim 4.26.

Proof of Claim 4.26. Fix $\kappa \in \mathbb{N}$ that satisfies the condition of the claim, and omit it from the following text to avoid clutter. By definition,

$$\left|\Pr\left[\mathsf{D}((X,Y,T,R) = \text{REAL}^{Z,\mathsf{F}}) = 1\right] - \Pr\left[\mathsf{D}((X', U_{\mathsf{A}(X',T,R)}, T, R) = \text{FST}^{Z,\mathsf{F}}) = 1\right]\right| > \rho \tag{11}$$

Consider the hybrid distribution

$$H = (X, U_{\mathsf{A}(X,T,R)}, T, R)$$

resulting from replacing the "forecasted" X' in $\text{FST}^{Z,\mathsf{F}}$ with the "real" value X. By Equation (11),

$$\left|\Pr\left[\mathsf{D}(\text{REAL}^{Z,\mathsf{F}}) = 1\right] - \Pr[\mathsf{D}(H) = 1] + \Pr[\mathsf{D}(H) = 1] - \Pr\left[\mathsf{D}(\text{FST}^{Z,\mathsf{F}}) = 1\right]\right| > \rho$$

and thus either

$$\left|\Pr[\mathsf{D}(H) = 1] - \Pr\left[\mathsf{D}(\text{FST}^{Z,\mathsf{F}}) = 1\right]\right| > \rho/3, \text{ or} \tag{12}$$

$$\left|\Pr\left[\mathsf{D}(\text{REAL}^{Z,\mathsf{F}}) = 1\right] - \Pr[\mathsf{D}(H) = 1]\right| > 2\rho/3 \tag{13}$$

Suppose Equation (12) holds. By definition, $\mathsf{D}^1(X,T,R) = \mathsf{D}(H)$ and $\mathsf{D}^1(X',T,R) = \mathsf{D}(\text{FST}^{Z,\mathsf{F}})$. Thus, $\left|\Pr\left[\mathsf{D}^1(X,T,R)=1\right] - \Pr\left[\mathsf{D}^1(X',T,R)=1\right]\right| > \rho/3$, which concludes the proof since $(X',T,R) = \text{FST}^{Z^1,\mathsf{F}^1}$ and $(X,T,R) = \text{REAL}^{Z^1,\mathsf{F}^1}$.

Suppose now that Equation (13) holds. It follows that for some $b \in \{0,1\}$

$$\Pr[X=b] \cdot \left|\Pr[\mathsf{D}(b,Y,T,R)=1 \mid X=b] - \Pr\left[\mathsf{D}(b,U_{\mathsf{A}(b,T,R)},T,R)=1 \mid X=b\right]\right| > \rho/3 \quad (14)$$

Since, by definition,

$$(U_{\mathsf{A}(b,T,R)},T,R)|_{X=b} \equiv (U_{\mathsf{F}^{2+b}(T;R)},T,R)|_{X=b} \equiv \text{FST}^{Z^{2+b},\mathsf{F}^{2+b}} \quad (15)$$

and

$$(Y,T,R)|_{X=b} \equiv \text{REAL}^{Z^{2+b},\mathsf{F}^{2+b}} \quad (16)$$

It follows that $\Pr[X=b]\cdot\left|\Pr\left[\mathsf{D}^{2+b}(\text{REAL}^{Z^{2+b},\mathsf{F}^{2+b}})\right] - \Pr\left[\mathsf{D}^{2+b}(\text{FST}^{Z^{2+b},\mathsf{F}^{2+b}})\right]\right| > \rho/3$, concluding the proof. □

4.2.3 Existence of Optimal Forecasters

In this section we prove the following lemma.

Lemma 4.27 (Existence of optimal forecaster, restated)**.** *For every ensemble of finite distributions $Z = \{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)\}_{\kappa\in\mathbb{N}}$ over $\{0,1\}\times\{0,1\}\times\{0,1\}^*$, $\mu > 0$ and infinite $\mathcal{I} \subseteq \mathbb{N}$, there exists a two-sided forecaster F and an infinite set $\mathcal{I}' \subseteq \mathcal{I}$, such that F is $(\mu,\mathcal{I}')$-optimal with respect to Z.*

Proof. Let $\mathcal{F}$ denote the set of all forecasters. Consider the following iterative process:

Initialization: We start by picking some $\mathsf{F}^{(1)} \in \mathcal{F}$, and let $\mathcal{I}_1 = \mathcal{I}$, and $\nu_1 = 2$.

Step i: (start with Step 1)

1. At the beginning of step i we hold $\mathsf{F}^{(i)} \in \mathsf{F}$ and an infinite set $\mathcal{I}_i \subseteq \mathbb{N}$, such that $\mathsf{price}_{Z_\kappa}(\mathsf{F}^{(i)}_\kappa) \leq \nu_i$ for every $\kappa \in \mathcal{I}_i$. (Note that this holds trivially for $i=1$, because the price function of a forecaster is bounded from above by 2).
2. If exists $\widehat{\mathsf{F}} \in \mathcal{F}$ and an infinite subset $\mathcal{I}' \subseteq \mathcal{I}_i$, such that

   $$\mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa) < \mathsf{price}_{Z_\kappa}(\mathsf{F}^{(i)}_\kappa) - \mu,$$

   for every $\kappa \in \mathcal{I}'$, set $\mathsf{F}^{(i+1)} = \widehat{\mathsf{F}}$, $\nu_{i+1} = \nu_i - \mu$ and $\mathcal{I}_{i+1} = \mathcal{I}'$, and continue to step $i+1$. Note that we indeed have that for every $\kappa \in \mathcal{I}_{i+1}$,

   $$\mathsf{price}_{Z_\kappa}(\mathsf{F}^{(i+1)}_\kappa) < \mathsf{price}_{Z_\kappa}(\mathsf{F}^{(i)}_\kappa) - \mu \leq \nu_i - \mu = \nu_{i+1}.$$

   Therefore we meet the requirement at the beginning of step $i+1$.

3. Otherwise, we have that for every $\widehat{\mathsf{F}} \in \mathcal{F}$, there are only finitely many $\kappa \in \mathcal{I}_i$, for which

$$\mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa) < \mathsf{price}_{Z_\kappa}(\mathsf{F}^{(i)}_\kappa) - \mu.$$

This means that for every sufficiently large $\kappa \in \mathcal{I}_i$,

$$\mathsf{price}_{Z_\kappa}(\widehat{\mathsf{F}}_\kappa) \geq \mathsf{price}_{Z_\kappa}(\mathsf{F}^{(i)}_\kappa) - \mu.$$

It follows that $\mathsf{F}^{(i)}$ is $(\mu, \mathcal{I}_i)$-optimal with respect to Z, and we obtain an optimal forecaster.

Noting that at every step i, if we continue to the next step, then $\nu_{i+1} \leq \nu_i - \mu$. However, at every step i, it is trivial that $\nu_i \leq 2$. This is because, the price of of a forecaster is bounded by 2. It follows that after at most $2/\mu$ iterations, we will obtain an infinite set $\mathcal{I}'$ and a forecaster F that is $(\mu, \mathcal{I}')$-optimal with respect to Z, as required. □

Remark 4.28 (on the generality of the above argument)**.** *It is instructive to note that we have used no specific properties of the price function or of the set $\mathcal{F}$ and the argument will work just the same for every choice of price function, and every class $\mathcal{F}$ of functions.*

5 Correlated Forecaster to Key Agreement

In this section we show how to use a protocol that has a correlated indistinguishable forecaster to construct a key-agreement protocol. The core of the reduction is a new information theoretic key-agreement protocol, that we can apply in the computational setting using an indistinguishable forecaster (recall that this approach is explained in the introduction).

5.1 Non-oblivious Key Agreement from Correlated Distributions

Key-agreement protocols in the information theoretic setting assume that two (honest) parties A and B, and an adversary (eavesdropper) E, receive (possibly correlated) random variables X, Y and T, respectively. The goal of the parties is to interact, so that their final outputs will be identical, and statistically close to a uniform distribution even conditioned on T and the transcript of their interaction. Note that in this setting, the honest parties do not see T. This is in contrast to the computational setting, where we imagine that T is the transcript of some earlier protocol, and is available to the honest parties.

We will now consider an information theoretic setting where honest parties A and B receive inputs X' and Y' respectively, and in addition they also receive T. The adversary E is unbounded, and receives (only) T. Loosely speaking, this setting corresponds to the following setup: a protocol π was run on input 1^κ generating transcript T, and the parties' outputs are X and Y respectively. We consider a simulation of that protocol (in the sense of Section 3) that produces a triplet (X', Y', T) that is somewhat indistinguishable from (X, Y, T). Indeed, in this information theoretic setting, A and B receive X' and Y' respectively, and also receive access to T. The adversary E receives T. There are several advantages in considering this scenario:

- (X', Y') has information theoretic uncertainty given T, and so we can work in an information theoretic setting where E is unbounded.

- The honest parties see T.
- Moreover, the honest parties have access to a (PPT) forecaster, which given t, allows them to compute all probabilities in the probability space $(X', Y')|_{T=t}$.

We now describe a key-agreement protocol in this setting. More precisely, in the protocol below, in addition to their inputs, parties are given access to a function $f : \{0,1\}^* \to [0,1]^3$ which on input t, produces a description of the probability space $(X', Y')|_{T=t}$. We will show that this protocol is a key-agreement that has perfect secrecy, and agreement that depends on the the "correlation distance" of the forecasted distribution. A precise statement appears below. Later, we will "pull back" this protocol to the computational world, using an indistinguishable forecaster.

Protocol 5.1 (Non-oblivious key-agreement protocol $\Phi^f = (\mathsf{A}, \mathsf{B})$)**.**

Common input $t \in \{0,1\}^*$.

A*'s private input:* $x \in \{0,1\}$.

B*'s private input:* $y \in \{0,1\}$.

Oracle: function $f\colon \{0,1\}^* \mapsto [0,1]^3$.

Operation:

1. *Both parties compute* $p = (p_1, p_2, p_3) = f(t)$.
2. A *samples* $x' \leftarrow U_{p_1}$*, and informs* B *whether* $x = x'$.
3. *If* $x \neq x'$*,*
   - A *outputs* x.
   - B *outputs* y *if* $p_3 > p_2$*, and* $(1-y)$ *otherwise.*

   Otherwise, each party outputs an independent uniform bit.

The following lemma relates the quality of the above protocol, as key agreement, to the "correlation" of its inputs distribution.

Recall, that $U_{p=(p_1,p_2,p_3)}$ is a random variable over $\{0,1\}^2$ distributed according to p (i.e., $\Pr[U_p = (x,y)] = \Pr[U_{p_1} = x] \cdot \Pr\left[U_{p_{x+2}} = y\right]$), and that, see Notation 3.9, $\mathsf{prod}(p)$ is the description of the product of U_p marginals (i.e., $\mathsf{prod}(p) = (p_1, (1-p_1)\cdot p_2 + p_1 \cdot p_3)$).

Lemma 5.2. *Let* $Z = (X, Y, T)$ *be a triplet distributed over* $\{0,1\} \times \{0,1\} \times \{0,1\}^*$*, and let* $f\colon \{0,1\}^* \mapsto \{0,1\}^3$ *be such that* $(X,Y)|_{f(T)=t} \equiv U_{f(t)}$ *for every* $t \in \mathrm{Supp}(T)$*. Let* $(\mathsf{A}, \mathsf{B}) = \Phi^f$ *be the protocol as specified in Protocol 5.1 and let* $\eta = \mathrm{SD}((X,Y,T), (U_{\mathsf{prod}(f(T))}, T))$*. Then*

Agreement: $\Pr[(\mathsf{A}(X), \mathsf{B}(Y))(T) = (b,b) \text{ for some } b \in \{0,1\}] = \frac{1}{2} + \eta/2$.

Secrecy: $\Pr[(\mathsf{A}(X), \mathsf{B}(Y))(T) = (1,\cdot) \mid T = t] = 1/2$*, for every* $t \in \mathrm{Supp}(T)$.

Proof. Let X' denote the value of x' sampled by $\mathsf{A}(X,T)$ (Step 2), and let $(O_\mathsf{A}, O_\mathsf{B}) = (\mathsf{A}(X), \mathsf{B}(Y))(T)$. We use the following claims, proven below.

Claim 5.3. $\Pr[O_{\mathsf{A}} = 1 \mid T = t] = 1/2$ *for every* $t \in \mathrm{Supp}(T)$.

Claim 5.4. $\Pr[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X = X'] = \Pr[X = X']/2$.

Claim 5.5. $\Pr[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X \neq X'] = \frac{1}{2}(\Pr[X \neq X'] + \eta)$.

The secrecy part immediately follows from Claim 5.3. For the agreement part, using Claims 5.4 and 5.5 we get that

$$\begin{aligned}\Pr[O_{\mathsf{A}} = O_{\mathsf{B}}] =& \Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X = X'\right] + \Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X \neq X'\right] \\ =& \tfrac{1}{2}(1 - \Pr\left[X \neq X'\right] + \Pr\left[X \neq X'\right] + \eta) \\ =& \tfrac{1}{2} + \eta/2.\end{aligned}$$

□

We now proceed to proving Claims 5.3 to 5.5.

Proof of Claim 5.3. Fix $t \in \mathrm{Supp}(T)$. Since A outputs a uniform bit if $X = X'$, it holds that

$$\Pr\left[O_{\mathsf{A}} = 1 \mid T = t, X = X'\right] = \tfrac{1}{2} \tag{17}$$

Hence, we can assume without loss of generality that $\Pr[X \neq X' \mid T = t] \neq 0$, as otherwise by the above equality we are done. Note that

$$\begin{aligned}\Pr\left[O_{\mathsf{A}} = 1 \mid T = t, X \neq X'\right] &= \Pr\left[X = 1 \mid T = t, X \neq X'\right] \\ &= \frac{\Pr[X = 1 \wedge X' = 0 \mid T = t]}{\Pr[X \neq X' \mid T = t]} \\ &= \frac{\Pr[X = 1 \wedge X' = 0 \mid T = t]}{2\Pr[X = 1 \wedge X' = 0 \mid T = t]} \\ &= \tfrac{1}{2},\end{aligned} \tag{18}$$

where the penultimate equality holds since $\Pr[X = 1 \wedge X' = 0 \mid T = t] = f(t)_1 \cdot (1 - f(t)_1) = \Pr[X = 0 \wedge X' = 1 \mid T = t]$. It follows that,

$$\begin{aligned}&\Pr[O_{\mathsf{A}} = 1 \mid T = t] \\ &= \Pr\left[X \neq X' \mid T = t,\right] \cdot \Pr\left[O_{\mathsf{A}} = 1 \mid T = t, X \neq X'\right] + \Pr\left[X = X' \mid T = t,\right] \cdot \Pr\left[O_{\mathsf{A}} = 1 \mid T = t, X = X'\right] \\ &= \Pr\left[X \neq X' \mid T = t,\right] \cdot \tfrac{1}{2} + \Pr\left[X = X' \mid T = t,\right] \cdot \tfrac{1}{2} = \tfrac{1}{2}.\end{aligned}$$

□

Proof of Claim 5.4. Holds since A outputs a uniform bit if $X = X'$. □

Proof of Claim 5.5. We will show that for every $t \in \mathrm{Supp}(T)$,

$$\Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X \neq X' \mid T = t\right] = f(t)_1 \cdot (1 - f(t)_1) \cdot (1 + |f(t)_2 - f(t)_3|) \tag{19}$$

We assume without loss of generality that $\Pr[X \neq X' \mid T = t] \neq 0$, as otherwise $f(t)_1 \in \{0, 1\}$ and the above equality trivially holds. Fix $t \in \mathrm{Supp}(T)$, and let $p = (p_1, p_2, p_3) = f(t)$, we want to calculate $\Pr[O_{\mathsf{A}} = O_{\mathsf{B}} \mid X \neq X', T = t]$. The proof continues according to whether $p_3 > p_2$.

Assuming $p_3 > p_2$, then $\Pr[O_{\mathsf{A}} = O_{\mathsf{B}} \mid X \neq X', T = t] = \Pr[X = Y \mid T = t, X \neq X']$. Thus

$$\begin{aligned}\Pr\left[X = Y \mid T = t, X \neq X'\right] =& \Pr\left[X = 1 \mid T = t, X \neq X'\right] \cdot \Pr[Y = 1 \mid T = t, X = 1] \\ &+ \Pr\left[X = 0 \mid T = t, X \neq X'\right] \cdot \Pr[Y = 0 \mid T = t, X = 0] \\ =& \tfrac{1}{2} \cdot \Pr[Y = 1 \mid T = t, X = 1] + \tfrac{1}{2} \cdot \Pr[Y = 0 \mid T = t, X = 0] \\ =& \tfrac{1}{2} \cdot p_3 + \tfrac{1}{2} \cdot (1 - p_2) \\ =& \tfrac{1}{2}(1 + (p_3 - p_2)).\end{aligned} \tag{20}$$

Assuming $p_3 \leq p_2$, then $\Pr[O_{\mathsf{A}} = O_{\mathsf{B}} \mid X \neq X', T = t] = \Pr[X \neq Y \mid T = t, X \neq X']$. Thus

$$\begin{aligned}\Pr\left[X \neq Y \mid T = t, X \neq X'\right] =& \Pr\left[X = 1 \mid T = t, X \neq X'\right] \cdot \Pr[Y = 0 \mid T = t, X = 1] \\ &+ \Pr\left[X = 0 \mid T = t, X \neq X'\right] \cdot \Pr[Y = 1 \mid T = t, X = 0] \\ =& \tfrac{1}{2} \cdot \Pr[Y = 0 \mid T = t, X = 1] + \tfrac{1}{2} \cdot \Pr[Y = 1 \mid T = t, X = 0] \\ =& \tfrac{1}{2} \cdot (1 - p_3) + \tfrac{1}{2} \cdot p_2 \\ =& \tfrac{1}{2}(1 + (p_2 - p_3)).\end{aligned} \tag{21}$$

Putting it together, $\Pr[O_{\mathsf{A}} = O_{\mathsf{B}} \mid T = t, X \neq X'] = \frac{1}{2}(1 + |p_2 - p_3|)$. Since, $\Pr[X \neq X' \mid T = t] = 2 \cdot p_1 \cdot (1 - p_1)$, it follows that

$$\Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X \neq X' \mid T = t\right] = p_1 \cdot (1 - p_1) \cdot (1 + |p_2 - p_3|) \tag{22}$$

We conclude that

$$\begin{aligned}\Pr\left[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X \neq X'\right] &= \mathrm{E}_{t \leftarrow T}\left[O_{\mathsf{A}} = O_{\mathsf{B}} \wedge X \neq X \mid T = t\right] \\ &= \mathrm{E}_{t \leftarrow T}\left[f(t)_1 \cdot (1 - f(t)_1) \cdot (1 + |f(t)_2 - f(t)_3|)\right] \\ &= \mathrm{E}_{t \leftarrow T}\left[f(t)_1 \cdot (1 - f(t)_1) + f(t)_1 \cdot (1 - f(t)_1) \cdot |f(t)_2 - f(t)_3|\right] \\ &= \mathrm{E}_{t \leftarrow T}\left[f(t)_1 \cdot (1 - f(t)_1)\right] + \mathrm{E}_{t \leftarrow T}\left[f(t)_1 \cdot (1 - f(t)_1) \cdot |f(t)_2 - f(t)_3|\right] \\ &= \tfrac{1}{2} \cdot \Pr\left[X \neq X'\right] + \mathrm{E}_{t \leftarrow T}\left[f(t)_1 \cdot (1 - f(t)_1) \cdot |f(t)_2 - f(t)_3|\right] \\ &= \tfrac{1}{2} \cdot \Pr\left[X \neq X'\right] + \eta/2.\end{aligned}$$

The second equality is by Equation (22) and the last one by Claim 5.6, given below. □

Claim 5.6. $\mathrm{E}_{t \leftarrow T}\left[(1 - f(t)_1) \cdot f(t)_1 \cdot |f(t)_2 - f(t)_3|\right] = \mu/2$.

Proof. Since $\eta = \mathrm{SD}((U_{f(T)}, T), (U_{\mathsf{prod}(f(T))}, T)) = \mathrm{E}_{t \leftarrow T}\left[\mathrm{SD}(U_{f(t)}, U_{\mathsf{prod}(f(t))})\right]$, it suffices to prove that

$$\mathrm{SD}(U_{f(t)}, U_{\mathsf{prod}(f(t))}) = 2 \cdot f(t)_1 \cdot (1 - f(t)_1) \cdot |f(t)_2 - f(t)_3| \tag{23}$$

for every $t \in \mathrm{Supp}(T)$.

Fix such t and let $p = (p_1, p_2, p_3) = f(t)$, let $q = p_1 p_3 + (1 - p_1)p_2$, let $(X_t, Y_t) = U_p$ and $(X'_t, Y'_t) = U_{\mathsf{prod}(p)}$. We assume without loss of generality that $p_1 \in (0, 1)$, as otherwise Equation (23) holds trivially. Compute

$$\begin{aligned}\mathrm{SD}((X_t, Y_t)|_{X_t=0}, (X'_t, Y'_t)|_{X'_t=0}) &= \mathrm{SD}((0, U_{p_2}, t), (0, U_q, t)) \\ &= |p_2 - q| \\ &= |p_2 - p_1 \cdot p_3 - (1 - p_1) \cdot p_2| \\ &= p_1 \cdot |p_2 - p_3|\,.\end{aligned} \tag{24}$$

And similarly,

$$\mathrm{SD}((X_t, Y_t)|_{X_t=1}, (X'_t, Y'_t)|_{X'_t=1}) = (1-p_1)\cdot|p_2-p_3| \tag{25}$$

Since $X_t \equiv X'_t$, we conclude that $\mathrm{SD}((X_t, Y_t), (X'_t, Y'_t)) = 2\cdot p_1\cdot(1-p_1)\cdot|p_2-p_3|$. □

5.2 Key Agreement from Correlated Protocols

In this section we invoke Protocol 5.1 on a distribution induced by a protocol outputs and transcript, using the forecaster for this distribution as the oracle f used by Protocol 5.1. The resulting protocol inherits the forecasted distribution indistinguishability and correlation, with small losses that depend on the indistinguishability parameter ρ.

Given a protocol π and a forecaster F for π, consider the following protocol

Protocol 5.7 (key agreement protocol $\Phi^{\mathsf{F},\pi,m} = (\mathsf{A},\mathsf{B})$)**.**

Parameters: security parameter 1^κ*.*

Oracles: forecaster F*, next message function of a two-party single output protocol* $\pi = (\widehat{\mathsf{A}},\widehat{\mathsf{B}})$ *and a function* $m\colon \mathbb{N}\mapsto\mathbb{N}$*.*

Operation:

1. *Parties interact in a random executions of* $\pi(1^\kappa)$*, with* A *and* B *taking the role of* $\widehat{\mathsf{A}}$ *and* $\widehat{\mathsf{B}}$*, respectively. Let* (x,y,t)*, be* A *and* B *local outputs and the protocol transcript.*
2. A *sample a uniform string* $r\leftarrow\{0,1\}^{m(\kappa)}$ *and sends it to* B*.*
3. *The parties* A *and* B *interact in* $(\widetilde{\mathsf{A}}(x),\widetilde{\mathsf{B}}(y))(1^\kappa,t,r)$*, for* $(\widetilde{\mathsf{A}},\widetilde{\mathsf{B}}) = \Phi^{\mathsf{F}}$ *being according to Protocol 5.1, and party* A *plays the role of* $\widetilde{\mathsf{A}}$*, and party* B *plays the role of* $\widetilde{\mathsf{B}}$*.*

   The parties output their outputs in the above execution.

Lemma 5.8 (Weak key-agreement protocol from correlated protocols)**.** *Let* π *be a* PPT *two-party single-bit output protocol, let* F *be a forecaster and let* $m\in$ poly *be a bound on number of coins used by* F *on transcripts of* $\pi(1^\kappa)$ *and let* $Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa)$ *be the distribution of the parties' output and protocol transcripts induce by a random execution of* $\pi(1^\kappa)$*. Let* $\mathcal{I}\subseteq\mathbb{N}$ *and* $\rho,\eta>0$ *be such that* F *is* $(\rho,\mathcal{I})$*-indistinguishable and* $(\eta,\mathcal{I})$*-correlated with respect to* $Z = \{Z_\kappa\}_{\kappa\in\mathbb{N}}$*, then protocol* $\Phi^{\mathsf{F},\pi,m}$*, defined in Protocol 5.7, is an* $(\rho,\eta/2-\rho)$*-key agreement-protocol in* $\mathcal{I}$*.*

Lemma 5.8 is proven below, but we first use it for proving the main result of this section.

Theorem 5.9 (Key-agreement from correlated protocols, restated)**.** *Let* π *be a* PPT *two-party single-bit output protocol and let* F *be a forecaster. Assume there exist an infinite set* $\mathcal{I}\subseteq\mathbb{N}$*,* $\rho>0$ *and* $\eta>30\sqrt{\rho}$ *such that* F *is* $(\rho,\mathcal{I})$*-indistinguishable and* $(\eta,\mathcal{I})$*-correlated with respect to* π*. Then there exists a key-agreement protocol in* $\mathcal{I}$*.*

Proof. The proof directly follows from Lemma 5.8 and theorem 2.4. □

Proof of Lemma 5.8. Let $\Phi^{\mathsf{IT}} = (\mathsf{A}^{\mathsf{IT}}, \mathsf{B}^{\mathsf{IT}})$ be the protocol defined by $\Phi^{\mathsf{IT}}_\kappa = \Phi^{\mathsf{F}_\kappa}$, for Φ^{F} being according to Protocol 5.1. Let $\widetilde{Z} = \left\{\widetilde{Z}_\kappa = (\widetilde{X}_\kappa, \widetilde{Y}_\kappa, T_\kappa, R_\kappa) = \text{FST}^{\pi,\mathsf{F}}_\kappa\right\}_{\kappa\in\mathbb{N}}$ and let $Z = \left\{Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa) = \text{REAL}^{\pi,\mathsf{F}}_\kappa\right\}_{\kappa\in\mathbb{N}}$ be the real and forecasted distribution of F with respect to Z (see Definition 3.6). For $\kappa \in \mathcal{I}$, let $(\widetilde{O}^{\mathsf{A}}_\kappa, \widetilde{O}^{\mathsf{B}}_\kappa)$ denote the parties' output in a random execution of $(\mathsf{A}^{\mathsf{IT}}(\widetilde{X}_\kappa), \mathsf{B}^{\mathsf{IT}}(\widetilde{Y}_\kappa))(1^\kappa, T_\kappa, R_\kappa)$. By Lemma 5.2,

- $\Pr\left[\widetilde{O}^{\mathsf{A}}_\kappa = \widetilde{O}^{\mathsf{B}}_\kappa\right] \geq \frac{1}{2} + \eta/2$, and
- $\Pr\left[\mathsf{E}(T_\kappa, R_\kappa) = \widetilde{O}^{\mathsf{A}}_\kappa\right] = 1/2$ for every (even unbounded) algorithm E.

Now let $(O^{\mathsf{A}}_\kappa, O^{\mathsf{B}}_\kappa)$ denote the parties' output in a random execution of $(\mathsf{A}^{\mathsf{IT}}(X_\kappa), \mathsf{B}^{\mathsf{IT}}(Y_\kappa))(1^\kappa, T_\kappa, R_\kappa)$. Since Φ^{IT} can be computed efficiently (recall that F is PPT), and since, by definition, $Z \overset{\text{C}}{\approx}_{\rho,\mathcal{I}} \widetilde{Z}$, it follows that

- $\Pr\left[O^{\mathsf{A}}_\kappa = O^{\mathsf{A}}_\kappa\right] \geq \frac{1}{2} + \eta/2 - \rho$, for large enough $\kappa \in \mathcal{I}$, and
- For every PPT E it holds that $\Pr\left[\mathsf{E}(T_\kappa, R_\kappa) = O^{\mathsf{A}}_\kappa\right] \leq 1/2 + \rho$, for large enough $\kappa \in \mathcal{I}$.

Indeed, otherwise there exists a PPT algorithm E that distinguishes between the real and the forecasted distributions with advantage greater than ρ, contradicting the fact that F is a $(\rho, \mathcal{I})$-forecaster with respect to Z.

Let $\Phi^{\mathsf{COM}} = \Phi^{\mathsf{F},\pi,m}$ be the ("computational") protocol defined in Protocol 5.7. Noting that the transcript and outputs induced by a random execution of $\Phi^{\mathsf{COM}}(1^\kappa)$ are identical to that of $(\mathsf{A}^{\mathsf{IT}}(X_\kappa), \mathsf{B}^{\mathsf{IT}}(Y_\kappa))(1^\kappa, T_\kappa, R_\kappa)$, yields the proof. □

6 Non-Trivial Differentially Private XOR Implies Key Agreement

In this section we use our classification from Section 3, to prove that a non-trivial differentially private protocol for computing XOR, implies the existence of a key-agreement protocol. In Section 6.1 we extend the reduction for protocols whose privacy guarantee only assumed to hold against *external* observers.

Notation. We introduce some new notation to be used for with input protocols. Given a two-party protocol $\pi = (\mathsf{A}, \mathsf{B})$, $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ and $z \in \{0,1\}^*$, let $(\text{trans}_\pi(z), \text{out}^{\mathsf{P}}_\pi(z), \text{view}^{\mathsf{P}}_\pi(z))$, denote the transcript, P's output and P's view receptively, in a random execution of $\pi(z)$.

Differential privacy Since the focus of this result is on single bit input protocol, we only define differential privacy for such protocols. Also, since we are in the computational setting, we only define the notion for efficient distinguishers.

Definition 6.1 ((ε,δ)-differential privacy)**.** *A single-bit input two-party protocol $\pi = (\mathsf{A}, \mathsf{B})$ is* (ε,δ)-differentially private*, denoted* (ε,δ)- DP*, with respect to $\varepsilon, \delta \colon \mathbb{N} \mapsto \mathbb{R}^+$, if for any* PPT *distinguisher D and $x \in \{0,1\}$, for all but finitely many κ's it holds that*

$$\Pr\left[\mathsf{D}(\text{view}^{\mathsf{A}}_\pi(1^\kappa, x, 0)) = 1\right] \in e^{\pm\varepsilon(\kappa)} \cdot \Pr\left[\mathsf{D}(\text{view}^{\mathsf{A}}_\pi(1^\kappa, x, 1)) = 1\right] \pm \delta(\kappa)$$

and similarly for any $y \in \{0,1\}$*:*

$$\Pr\left[\mathsf{D}(\text{view}_\pi^{\mathsf{B}}(1^\kappa,0,y))=1\right] \in e^{\pm\varepsilon(\kappa)} \cdot \Pr\left[\mathsf{D}(\text{view}_\pi^{\mathsf{B}}(1^\kappa,1,y))=1\right] \pm \delta(\kappa)$$

Namely, an adversary seeing the view of one of the parties, cannot tell the other party's input too well.

Computing XOR.

Definition 6.2 (α-accurate XOR)**.** *Protocol* $\pi = (\mathsf{A},\mathsf{B})$ *is computing the XOR functionality in a* α-correct manner, denoted α-correct*, with respect to* $\alpha\colon \mathbb{N} \mapsto \mathbb{R}^+$*, if for any* $x,y \in \{0,1\}$ *it holds that* $\Pr\left[\text{out}_\pi^{\mathsf{A}}(1^\kappa,x,y) = \text{out}_\pi^{\mathsf{B}}(1^\kappa,x,y) = x \oplus y\right] \geq \frac{1}{2} + \alpha(\kappa)$.

Such protocols are symmetric*, if the parties always agree on the output (i.e.,* $\text{out}_\pi^{\mathsf{A}}(1^\kappa,x,y) = \text{out}_\pi^{\mathsf{B}}(1^\kappa,x,y)$*).*

We focus on symmetric protocols with constant α (independent of κ).

Our result.

Theorem 6.3. *Let* $\varepsilon \in [0,1]$*. Assume there exists a symmetric* $(21\varepsilon^2)$-correct*,* $(\varepsilon,\varepsilon^3)$-DP *protocol for computing XOR, then there exists an* io *key-agreement protocol.*

Proof. Let $\pi = (\mathsf{A},\mathsf{B})$ be an α-correct, (ε,δ)-DP protocol for computing XOR. We assume without loss of generality that π's transcript contain the security parameter, so we can omit it from the distinguisher list of inputs. Consider the following no-input protocol $\widehat{\pi}$.

Protocol 6.4 ($\widehat{\pi} = (\widehat{\mathsf{A}},\widehat{\mathsf{B}})$)**.**

Parameters: security parameter 1^κ*.*

Operation:

1. $\widehat{\mathsf{A}}$ *samples* $x \leftarrow \{0,1\}$ *and* $\widehat{\mathsf{B}}$ *samples* $y \leftarrow \{0,1\}$*.*
2. *The parties interact in* $(\mathsf{A}(x),\mathsf{B}(y))(1^\kappa)$*, with* $\widehat{\mathsf{A}}$ *and* $\widehat{\mathsf{B}}$ *taking the role of* A *and* B *respectively. Let* out *be the (common) output of this interaction.*
3. *If* $\text{out} = 0$*, the parties locally outputs* x *and* y *respectively.*

   Otherwise, the parties locally outputs x *and* $1-y$ *respectively.*

Since π is symmetric, its α correctness yields that

$$\Pr\left[\text{out}_{\widehat{\pi}}^{\widehat{\mathsf{A}}}(1^\kappa) = \text{out}_{\widehat{\pi}}^{\widehat{\mathsf{B}}}(1^\kappa)\right] \geq \frac{1}{2} + \alpha \tag{26}$$

Since π is symmetric and $(\varepsilon,\varepsilon^3)$-DP, the *output* of each party of $\widehat{\pi}$ is $(\varepsilon,\varepsilon^3)$ differential private from the other party. Namely, for any PPT distinguisher D and uniformly chosen bit X,

$$\Pr\left[\mathsf{D}(1^\kappa,\text{view}_{\widehat{\pi}}^{\widehat{\mathsf{A}}}(1^\kappa),\text{out}_{\widehat{\pi}}^{\widehat{\mathsf{B}}}(1^\kappa))=1\right] \in e^{\pm\varepsilon} \cdot \Pr\left[\mathsf{D}(1^\kappa,\text{view}_{\widehat{\pi}}^{\widehat{\mathsf{A}}}(1^\kappa),X)=1\right] \pm \delta \tag{27}$$

for all but finitely many κ's, and similarly for the output of $\widehat{\mathsf{A}}$.

Let $\rho = \varepsilon^3$. By Theorem 3.18, either $\widehat{\pi}$ can be used to construct an io key-agreement protocol, or it is io-ρ-uncorrelated. Since we would like to prove the former, we assume that the latter holds and derive a contradiction for the assumed combination of privacy and accuracy of π.

Since protocol π is io-ρ-uncorrelated, there exits a PPTM (decorelator) Decor that outputs a pair of numbers in $[0,1]$, and an infinite set $\mathcal{I} \subseteq \mathbb{N}$ such that the following holds: Let $Z = \left\{ Z_\kappa = (X_\kappa, Y_\kappa, T_\kappa, R_\kappa) = (\mathrm{out}^{\widehat{\mathsf{A}}}_{\widehat{\pi}}(1^\kappa), \mathrm{out}^{\widehat{\mathsf{B}}}_{\widehat{\pi}}(1^\kappa), \mathrm{trans}_{\widehat{\pi}}(1^\kappa), R_\kappa) \right\}_{\kappa\in\mathbb{N}}$, where R_κ is the uniform string whose length bounds the number of coins used by Decor on input $t \in \mathrm{Supp}(T_\kappa)$, and let $Z' = \left\{ Z'_\kappa = (U_p, T_\kappa, R_\kappa)_{p\leftarrow \mathsf{Decor}(T_\kappa;R_\kappa)} \right\}_{\kappa\in\mathbb{N}}$. It holds that,

$$Z \overset{\mathrm{C}}{\approx}_{\rho,\mathcal{I}} Z' \tag{28}$$

for $U_{p=(p_1,p_2)}$ being the output of two independent coins, first coin taking the value one with probability p_1, and the second with probability p_2. Namely, given the transcript and the decorator's coins, it is impossible to distinguish too well the parties' output from the pair of independent coins sample according to the predictor prediction.

We call a pair $(p_1,p_2) \in [0,1]^2$ *private*, if $p_1, p_2 \in \frac{1}{2} \pm 3\varepsilon$. Similarly, Decor is *private on* κ, denoted κ-$\mathsf{private}$, if

$$\Pr\left[\mathsf{Decor}(T_\kappa; R_\kappa) \text{ is private}\right] \geq 1 - \varepsilon^2 \tag{29}$$

We use the privacy of $\widehat{\pi}$ to derive the following fact.

Claim 6.5. Decor *is* κ-$\mathsf{private}$ *for all but finitely many* $\kappa \in \mathcal{I}$.

The proof of Claim 6.5 is given below, but we first use it to conclude the theorem's proof. Let $\kappa \in \mathcal{I}$ be such that Decor is κ-$\mathsf{private}$. It follows that

$$\Pr_{(p_1,p_2)\leftarrow\mathsf{Decor}(T_\kappa;R_\kappa)}\left[U_{p_1} = U_{p_2}\right] \leq \frac{1}{2} + 18\varepsilon^2 + \varepsilon^2 = \frac{1}{2} + 19\varepsilon^2$$

where U_p is a uniform coin that takes the value one with probability p. By Equation (28), for large enough $\kappa \in \mathcal{I}$ it holds that

$$\begin{aligned}\Pr\left[X_\kappa = Y_\kappa\right] &\leq \frac{1}{2} + 19\varepsilon^2 + \rho \\ &\leq \frac{1}{2} + 20\varepsilon^2 \\ &< \frac{1}{2} + \alpha,\end{aligned}$$

in contradiction to Equation (26). □

Proof of Claim 6.5. For $\kappa \in \mathcal{I}$ for which Decor is not κ-$\mathsf{private}$, assume without loss of generality that $\beta = \Pr\left[\mathsf{Decor}(T_\kappa; R_\kappa)_1 \geq \frac{1}{2} + 3\varepsilon\right] \geq \varepsilon^2$. Consider the distinguisher D that on input (p,x), outputs one if $p \geq \frac{1}{2} + 3\varepsilon$ and $x = 1$. By assumption

$$\Pr_{p\leftarrow\mathsf{Decor}(T_\kappa;R_\kappa)_1; x\leftarrow U_p}\left[\mathsf{D}(p,x) = 1\right] \geq \beta \cdot (\frac{1}{2} + 3\varepsilon) = \frac{\beta}{2} + 3\beta\varepsilon$$

Hence, Equation (28) yields that large enough $\kappa \in \mathcal{I}$,

$$\Pr_{p \leftarrow \mathsf{Decor}(T_\kappa; R_\kappa)_1; x \leftarrow X_\kappa}[\mathsf{D}(p, x) = 1] \geq \frac{\beta}{2} + 3\beta\varepsilon - \rho \geq \frac{\beta}{2} + 2\beta\varepsilon \tag{30}$$

Since,

$$\Pr_{p \leftarrow \mathsf{Decor}(T_\kappa; R_\kappa)_1; x \leftarrow U_{1/2}}[\mathsf{D}(p, x) = 1] = \beta/2, \tag{31}$$

we conclude that

$$\begin{aligned}
\Pr[\mathsf{D}(\mathsf{Decor}(T_\kappa; R_\kappa)_1, X_\kappa) = 1] &\geq \frac{\beta}{2} + 2\beta\varepsilon = \frac{\beta}{2}(1 + 2\varepsilon) + \beta\varepsilon \\
&> e^{\varepsilon} \cdot \frac{\beta}{2} + \beta\varepsilon \\
&= e^{\varepsilon} \cdot \Pr[\mathsf{D}(\mathsf{Decor}(T_\kappa; R_\kappa)_1, U) = 1] + \beta\varepsilon \\
&\geq e^{\varepsilon} \cdot \Pr[\mathsf{D}(\mathsf{Decor}(T_\kappa; R_\kappa)_1, U) = 1] + \varepsilon^3.
\end{aligned}$$

Namely, the algorithm that on input (t, x) samples an independent uniform string r, and returns $\mathsf{D}(\mathsf{Decor}(t; r)_1, x)$, contradicts the assumed differential privacy of π (see Equation (27)). □

6.1 External Differential Privacy

Our result extends to weaker notion of differential privacy, that only guarantee to hold against external observers.

Definition 6.6 ((ε, δ)-external differential privacy)**.** *A single-bit input two-party protocol $\pi = (\mathsf{A}, \mathsf{B})$ is (ε, δ)-*external differentially private*, denoted (ε, δ)-* EDP*, with respect to $\varepsilon, \delta \colon \mathbb{N} \mapsto \mathbb{R}^+$, if for any* PPT *distinguisher* D *and $x, y, y' \in \{0,1\}$, for all but finitely many κ's it holds that*

$$\Pr[\mathsf{D}(1^\kappa, \mathrm{trans}_\pi(1^\kappa, x, y)) = 1] \in e^{\pm\varepsilon(\kappa)} \cdot \Pr\left[\mathsf{D}(1^\kappa, \mathrm{trans}_\pi(1^\kappa, x, y')) = 1\right] \pm \delta(\kappa)$$

for all but finitely many κ's, and same for B*'s input.*

Namely, privacy is only required to hold against an external viewer that sees only the protocol transcript. Achieving external privacy is typically much simpler than the full-fledged notion of Definition 6.1. In particular, for functionalities such as the XOR described above, constructing such protocol only need to assume key-agreement, where we currently only know how to construct them assuming oblivious transfer require for the full-fledged notion.

A protocol has *explicit output* if the parties' common output appears explicitly in the transcript. For such protocols we have the following result.

Theorem 6.7. *Let $\varepsilon \in [0, 1]$. Assume there exists an explicit-output $(21\varepsilon^2)$-*correct*, $(\varepsilon, \varepsilon^3)$-*EDP *protocol for computing XOR, then there exists an* io *key-agreement protocol.*

Proof. Follows the same line as the proof of Theorem 6.7. □

References

[1] B. Barak and M. Mahmoody. Merkle puzzles are optimal - an $O(n^2)$-query attack on any key exchange from a random oracle. In *Advances in Cryptology – CRYPTO 2009*, pages 374–390, 2009. 10

[2] A. Beimel, I. Haitner, N. Makriyannis, and E. Omri. Tighter bounds on multi-party coin flipping via augmented weak martingales and differentially private sampling. Technical Report TR17-168, Electronic Colloquium on Computational Complexity, 2017. 7

[3] Crepeau and Kilian. Weakening security assumptions and oblivious transfer. In *Advances in Cryptology – CRYPTO '88*, 1988. 11

[4] D. Dachman-Soled, Y. Lindell, M. Mahmoody, and T. Malkin. On the black-box complexity of optimally-fair coin tossing. In *Proceedings of the 8th Theory of Cryptography Conference, TCC 2011*, volume 6597, pages 450–467, 2011. 7

[5] D. Dachman-Soled, M. Mahmoody, and T. Malkin. Can optimally-fair coin tossing be based on one-way functions? In Y. Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014*, volume 8349 of *Lecture Notes in Computer Science*, pages 217–239. Springer, 2014. 7

[6] V. Goyal, I. Mironov, O. Pandey, and A. Sahai. Accuracy-privacy tradeoffs for two-party differentially private protocols. In *Advances in Cryptology – CRYPTO 2013*, pages 298–315, 2013. 7, 11

[7] V. Goyal, D. Khurana, I. Mironov, O. Pandey, and A. Sahai. Do distributed differentially-private protocols require oblivious transfer? In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 55. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016. 7, 11

[8] I. Haitner. Implementing oblivious transfer using collection of dense trapdoor permutations. In *Proceedings of the First Theory of Cryptography Conference, TCC 2004*, pages 394–409, 2004. 11

[9] I. Haitner, O. Reingold, and S. Vadhan. Efficiency improvements in constructing pseudorandom generators from one-way functions. *SIAM Journal on Computing*, 42(3):1405–1430, 2013. Special Issue on *STOC '10*. 9

[10] I. Haitner, E. Omri, and H. Zarosim. Limits on the usefulness of random oracles. *Journal of Cryptology*, 29(2):283–335, 2016. 10, 11

[11] I. Haitner, N. Makriyannis, and E. Omri. On the complexity of fair coin flipping. Technical Report TR18-?, Electronic Colloquium on Computational Complexity, 2018. 1, 7

[12] 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. Preliminary versions in *STOC'89* and *STOC'90*. 9

[13] T. Holenstein. Strengthening key agreement using hard-core sets - PhD thesis, 2006. 1, 9, 11, 13

[14] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989. 5, 6

[15] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC)*, pages 44–61. ACM Press, 1989. 10

[16] D. Khurana, H. K. Maji, and A. Sahai. Black-box separations for differentially private protocols. In *Advances in Cryptology – ASIACRYPT 2014*, pages 386–405, 2014. 11

[17] A. McGregor, I. Mironov, T. Pitassi, O. Reingold, K. Talwar, and S. P. Vadhan. The limits of two-party differential privacy. *Electronic Colloquium on Computational Complexity (ECCC)*, page 106, 2011. Preliminary version in *FOCS'10*. 11

[18] S. Vadhan and C. J. Zheng. Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC)*, pages 817–836, 2012. 9

[19] J. von Neumann. Various techniques used in connection with random digits. *Applied Math Series*, 12:36–38, 1951. 10

[20] S. L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965. 7

[21] J. Wullschleger. Oblivious-transfer amplification. In *Advances in Cryptology – EUROCRYPT 2007*, pages 555–572, 2007. 11

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il