On the Communication Complexity of Key-Agreement Protocols

Iftach Haitner*† Noam Mazor†‡ Rotem Oshman § Omer Reingold ¶
Amir Yehudayoff ‖

February 15, 2018

Abstract

Key-agreement protocols whose security is proven in the *random oracle model* are an important alternative to the more common public-key based key-agreement protocols. In the random oracle model, the parties and the eavesdropper have access to a shared random function (an "oracle"), but they are limited in the number of queries they can make to it. Unfortunately, as shown by Impagliazzo and Rudich [STOC '89] and Barak and Mahmoody [Crypto '09], such protocols can only guarantee limited secrecy: the key of any ℓ-query protocol can be revealed by an $O(\ell^2)$-query adversary. This quadratic gap between the query complexity of the honest parties and the eavesdropper matches the gap obtained by the *Merkle's Puzzles* protocol of Merkle [CACM '78].

In this work we tackle a new aspect of key-agreement protocols in the random oracle model: their *communication complexity*. In Merkle's Puzzles, to obtain secrecy against an eavesdropper that makes roughly ℓ^2 queries, the honest parties need to exchange $\Omega(\ell)$ bits. We show that for protocols with certain natural properties, ones that Merkle's Puzzle has, such high communication is unavoidable. Specifically, this is the case if the honest parties' queries are uniformly random, or alternatively if the protocol uses non-adaptive queries and has only two rounds. Our proof for the first setting uses a novel reduction from random-oracle protocols to the *set-disjointness* problem in two-party communication complexity, which is known to have high communication cost. For the second setting we prove the lower bound directly, using information-theoretic arguments.

Understanding the communication complexity of protocols whose security is proven in the random-oracle model is an important question in the study of practical protocols. Our results and proof techniques are a first step in this direction.

Keywords: key agreement; random oracle; communication complexity; Merkle puzzles

*The Blavatnik school of computer science,, Tel Aviv University. E-mail: iftachh@cs.tau.ac.il. Member of the Check Point Institute for Information Security.

†Supported by ERC starting grant 638121.

‡The Blavatnik school of computer science, Tel Aviv University. E-mail: noammaz@gmail.com.

§The Blavatnik school of computer science, Tel Aviv University. E-mail: rotem.oshman@gmail.com. Supported by the Israeli Centers of Research Excellence program 4/11 and BSF grant 2014256.

¶Computer Science Department, Stanford University. E-mail: reingold@stanford.edu. Supported by NSF grant CCF-1763311.

‖Department of Mathematics, Technion-Israel Institute of Technology. E-mail: amir.yehudayoff@gmail.com. Supported by ISF grant 1162/15.

1 Introduction

In a key-agreement protocol (Diffie and Hellman [5]), two parties communicating over an insecure channel want to securely agree on a shared secret key, so that an eavesdropper observing their communication cannot find the key. There are numerous candidate constructions of key-agreement schemes, e.g., [16, 14, 1, 11], based on assumptions implying that public-key encryption schemes exist. A fundamental open question is whether we can design key-agreement protocols based on the security of symmetric primitives, e.g., *private-key* encryption; the security of such primitives is believed to be more robust.

A first step in this direction was made by Merkle [12], presenting a key-agreement scheme called *Merkle's Puzzles*, which has some level of security in the *random oracle model*: the parties and the eavesdropper have limited access to a *random* function (an "oracle"). In Merkle's Puzzles, the honest parties make ℓ queries, for an arbitrary parameter $\ell \in \mathbb{N}$, and the key remains secure as long as the eavesdropper makes $o(\ell^2)$ oracle queries. While the quadratic gap between the ℓ-query honest parties and the ℓ^2-query eavesdropper achieved by Merkle's Puzzles might not seem like much, if the honest parties are willing to work hard enough (take large ℓ) and only need the secrecy of the key to hold for limited time, this limited gap might yield a good enough advantage.

It turns out that in the random oracle model it is not possible to achieve a better-than-quadratic gap: Barak and Mahmoody [2] (following Impagliazzo and Rudich [9]) showed that Merkle's Puzzles have optimal secrecy, as the security of any protocol where the honest parties make $O(\ell)$ queries can be broken by an adversary that makes $O(\ell^2)$ queries, and can guess the secret key with high success probability. Thus, the trade-off between the number of queries and security is completely characterized in the random oracle model.

In this work we consider another crucial aspect of any distributed protocol: *communication*. In many distributed systems, communication between the parties is the most energy and time-consuming part of the computation, dwarfing even computation-expensive local tasks (e.g., in [4], experiments show that a wireless network running Kerberos spends 95% of its energy consumption on communication and only 5% on local computation). In such settings, even a key-agreement protocol that uses a small number of queries cannot be considered *truly* efficient if it has high communication requirements. In Merkle's Puzzles, for example, the players need to send $\Theta(\ell)$ bits (the answers to all their queries).

In this work we initiate the study of communication-efficient protocols in the random oracle model. We show that under some restrictions on the protocol, the high communication incurred by Merkle's Puzzles is unavoidable: in order to achieve security against an adversary that can ask $\Theta(\ell^2)$ queries, the two parties must exchange $\Omega(\ell)$ bits of communication. Specifically, we show that the bound above holds for protocols where the parties' queries are *uniformly random subsets*, and the bound also holds for any non-adaptive protocol that uses only two rounds of communication. (These are both properties of Merkle's Puzzles: there, the parties use uniformly random queries and send one message each.) It is our hope that our work will initiate further interest in the communication cost of cryptography in the random oracle model.

A key-agreement protocol is measured by two parameters: its *agreement guarantee*, which is the probability that the honest parties output the same key, and its *secrecy guarantee*, the probability that an eavesdropper guesses the common key. To simplify the discussion, we focus below on protocols whose agreement guarantee is larger by some constant compared to their secrecy guarantee. Our results generalize to any arbitrary trade-off between the protocol's communication cost and the eavesdropper's query complexity.

Uniform-query protocols. An oracle protocol has *uniform queries*, if the parties' oracle queries are chosen independently and uniformly from a predetermined set. We give the following lower bound on the communication complexity of such protocols.

Theorem 1.1 (lower bound on uniform-inputs protocols, informal)**.** *Any ℓ-uniform-query key-agreement protocol achieving non-trivial secrecy against $o(\ell^2)$-query adversaries, has communication complexity $\Omega(\ell)$.*

Theorem 1.1 is proved by a novel reduction to *set-disjointness* — a problem in communication complexity known to require high communication complexity, a reduction we believe to be of independent interest. See more details in Section 1.1.1.

Two-message non-adaptive protocols. An oracle protocol has *non-adaptive* queries, if the distribution of queries the parties make is fixed in advance — it is determined (arbitrarily) before the parties communicate with each other and independently of the oracle's answers. We give the following lower bound on the communication complexity of such protocols.

Theorem 1.2 (lower bound on two-message non-adaptive protocols, informal)**.** *Any two-message ℓ-query non-adaptive key-agreement protocol of non-trivial secrecy against $o(\ell^2)$-query adversaries has communication complexity $\Omega(\ell)$.*

We prove the above bound by presenting an $o(\ell^2)$-query eavesdropper that prevents the parties from exploiting the correlation induced by their random oracle calls, by asking all joint (i.e., intersecting) queries that the parties "understand" to be such. This is very different from the eavesdropper used by Barak and Mahmoody [2], and by Impagliazzo and Rudich [9]: their eavesdropper, by making $\Theta(\ell^2)$ queries, has high probability of finding *all* joint queries. Finding the right definition for what it means to "learn" that a given query is in the intersection, and constructing a low query-complexity eavesdropper that manages to ask all such queries, is the main difficulty in our proof. See more details in Section 1.1.2.

1.1 Our Technique

We give some high-level description of the techniques used for proving our two lower bounds (Theorems 1.1 and 1.2).

1.1.1 Uniform-Query Protocols

The lower bound for uniform-query key-agreement protocols is proved via a reduction to *set-disjointness* — two parties receive sets from a predetermined distribution, and have to decide (by communicating) whether their sets intersect. We emphasize that the parties trying to solve the set-disjointness problem have no oracle, but are allowed to use joint (public) randomness. Set-disjointness was proved to require high communication complexity: for any $\ell \in \mathbb{N}$ there exists "hard" distribution over subsets of $[\ell]$, such that in order to solve disjointness over this distribution (even only with high probability), the parties have to exchange $\Theta(\ell)$ bits of communication. We show how to transform an ℓ-uniform-query key-agreement protocol of non-trivial secrecy against $o(\ell^2)$-query adversaries, to a protocol for solving set-disjointness over a hard distribution. This yields an $\Theta(\ell)$ bound on the communication complexity of the key-agreement protocol. More details below.

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be an ℓ-uniform-query key-agreement protocol. We assume for simplicity that the key-length is one (i.e., a bit), that Π has perfect agreement (parties always agree) and that an $o(\ell^2)$-query cannot guess the key with probability larger than $3/4$. We use Π to build two (no-oracle) protocols $\Lambda_{\mathsf{Com}} = (\mathsf{A}_{\mathsf{Com}}, \mathsf{B}_{\mathsf{Com}})$ and $\Lambda_{\mathsf{Dist}} = (\mathsf{A}_{\mathsf{Dist}}, \mathsf{B}_{\mathsf{Dist}})$, with the same communication complexity as of Π, such that at least one of them can be used to solve set-disjointness well over an hard distribution.

In protocol Λ_{Com}, the parties interact in a random execution of Π using public (common) randomness to emulate the random oracle: the common random string is interpreted as the description of a random function. Since the joint distribution of the transcript and outputs induced by a random execution of Λ_{Com} equals to that induced by a random execution Π, protocol Λ_{Com} has perfect agreement. Furthermore, an adversary seeing only the protocol transcript, cannot guess the common key with probability better than $3/4$. Indeed, such an adversary is equivalent to an adversary that is trying to guess the key in a random execution of Π without using the oracle.

In the second protocol Λ_{Dist}, the parties also interact in a random execution of Π, but use their *private* randomness to emulate the random oracle. In other words, each party uses a *different* function as the random oracle. The joint distribution of the transcript and outputs induced by a random execution of Λ_{Dist}, might be very far from the distribution induced by of Π. Yet, note that conditioned that the queries are disjoint, it is easy to see that the two distributions are the same. In particular, the perfect agreement of Π yields that the parties of Λ_{Dist} output the same key under this conditioning. A second observation is that since the parties of Λ_{Dist} use no common (public) randomness, their view is in a product distribution given the transcript. Hence, there exist an adversary E that seeing only the transcript, finds the key with same probability that the parties output the same value. Combining the above observations yields that one of the following must holds:

Agreement gap: The agreement probability Λ_{Dist} is at most $7/8$ (comparing to one in Λ_{Com}), or

Secrecy gap: the probability that E guesses $\mathsf{A}_{\mathsf{Dist}}$'s output in Λ_{Dist} is at least $7/8$ (comparing to $3/4$ in Λ_{Com}).

We start by describing the set-disjointness protocol assuming an accuracy gap exists, and later explain how to address the case of secrecy gap.

Agreement gap. Recall that Λ_{Dist} has perfect agreement if the parties' queries do not intersect, and that, by assumption, its overall agreement is at most $7/8$. Assume for simplicity that the inaccuracy of Λ_{Dist} holds for every non zero intersection size. That is, the agreement probability of Λ_{Dist} conditioned that the sets intersect with c queries is at most $7/8$, for every $c \in \mathbb{N}$. We exploit the gap between the imperfect agreement of Λ_{Dist} when the parties' inputs do not intersect, to its perfect agreement when they do, to build a protocol for solving set-disjointness over any distribution.[1]

The set-disjointness protocol $\Lambda_{\mathsf{Set}} = (\mathsf{A}_{\mathsf{Set}}, \mathsf{B}_{\mathsf{Set}})$ is defined as follows: first, each party permutes its input set using a permutation defined by the common public randomness. The parties then interact in Λ_{Dist}, with each party using the permuted value of its private input as its uniform queries. At the end of the execution, party $\mathsf{A}_{\mathsf{Set}}$ sends its output to $\mathsf{B}_{\mathsf{Set}}$, who outputs 1 if the received value is equal to its own output.

[1]The agreement gap might only exist for some values of c. We handle this complication using specific properties of a known hard distribution for set-disjointness. See Section 3.

If the parties' input sets are disjoint, the permuted input sets are disjoint as well (the parties permute their input sets using the same permutation defined by the public randomness) . Thus, the parties' outputs are equal with probability one. On the other hand, if the input sets do intersect, the permuted input sets are random sets in the domain of the same intersection size. Thus the parties' output are equal with probability at most 7/8.

It follows that $\mathsf{B}_{\mathsf{Set}}$ outputs 1 with probability one if the parties' input sets are disjoint, and with probability at most 7/8 otherwise. Since the latter hold for *any* input, the above protocol solves set-disjointness with error "too low" over hard distributions, and thus must have high communication complexity.

Secrecy gap. We convert Λ_{Com} and Λ_{Dist} into a pair of protocols with agreement gap, and then continue as above. Consider protocol $\Lambda'_{\mathsf{Dist}} = (\mathsf{A}'_{\mathsf{Dist}}, \mathsf{B}'_{\mathsf{Dist}})$ in which the parties acts as in Λ_{Dist}, but at the end of the execution $\mathsf{B}'_{\mathsf{Dist}}$ executes E on the transcript and outputs its output. Protocol Λ'_{Com} is defined analogously with respect to Λ_{Com}. By assumption, E guesses $\mathsf{A}_{\mathsf{Dist}}$'s output in Λ_{Dist} with probability at least 7/8, and guesses $\mathsf{A}_{\mathsf{Com}}$'s output in Λ_{Com} with probability at most 3/4. Hence, Λ'_{Dist} has agreement at least 7/8, and Λ'_{Com} has agreement at most 3/4. Namely, there is an agreement gap between Λ'_{Dist} and Λ'_{Com}, and we can apply a simple variant of the reduction described above to solve set-disjointness.

1.1.2 Two-Message Non-Adaptive Protocols

Consider an oracle key-agreement protocol $\Pi = (\mathsf{A}, \mathsf{B})$. We show that to produce a shared key, the parties of Π must transfer information about the *intersection* between their queries. Moreover, the queries and their intersection need to be "unpredictable" (have high min-entropy) given the transcript, otherwise an eavesdropper can make the same queries and neutralize the honest parties' advantage. Since A does not know in advance her intersection with B's queries, if she sends a short message, she will not convey much information about the intersection; and similarly for B's message. More formally, if each query as probability at most δ of being asked by B, and A's message has C bits, then B learns no more than δC bits of information about the intersection, and this argument can be carried to B's return message as well. However, what should we do about queries with probability higher than δ of being asked?

To guarantee that all queries have low prior probability of being asked by one of the players (or viewed another way — to "neutralize" queries that are too predictable) we use a variant of the eavesdropper of Barak and Mahmoody [2]. The eavesdropper in their work finds and queries all the "heavy queries" — queries that were asked with probability at least δ given the eavesdropper's view (the messages it has seen and the queries it has asked). In our proof, we set the "heavy query" threshold δ to $\Theta(1/C)$ instead of $1/\ell$, where C is the communication complexity of the protocol. Intuitively, this is because we only care about queries *the players have talked to each other about*, not queries they asked but did not communicate to the other player.[2] The eavesdropper asks all the heavy queries at the beginning of every communication round, and at the end of the protocol, it outputs the key it believes B would output, given the messages the eavesdropper observed between the players and the queries it asked. We prove that the eavesdropper generates a total of only $\Theta(C\ell)$ queries, and breaks the secrecy of the protocol.

[2]This is an over-simplification, since a player's message can contain partial information about queries, e.g., XORs of subsets of queries and so on.

Note that when $C \ll \ell$, an eavesdropper that asks only $\Theta(C\ell)$ queries stands no chance of finding all the intersection queries shared by the parties. For example, if A and B each ask ℓ random queries, but *do not communicate with each other at all* ($C = 0$), then our eavesdropper is not allowed to make any queries ($C \cdot \ell = 0$), and in particular, even though with high probability A and B's queries intersect, the eavesdropper will not find an intersection query. This is a key difference from the proof of [2, 9], whose eavesdropper with high probability asks all the intersection queries. Nevertheless, we show that unless the parties can *learn* that a given query is in their intersection, this query is not useful to them.

We assume without loss of generality that the secret key is the first bit of one of B's queries (we show that any protocol can be transformed into a protocol that has this property, without harming consistency or security). The technical key to the proof is to bound the dependence between B's queries and A's view: this dependence exactly captures the players' "advantage" over the eavesdropper. In particular, if the players can figure out an intersection query, they create a lot of dependence that is hidden from the eavesdropper. We show that this does not happen, except with small probability. Thus, the players have very small advantage over the eavesdropper, and when at the end of the protocol the eavesdropper guesses B's key, it has roughly the same chance of agreeing with A's key as B does.

The proof formalizes the intuition that any dependence between B's queries and A's view (or vice-versa) is "created through" the intersection of their queries. We then show that (1) A's message does not convey much information about the intersection, and hence, (2) B's message also does not convey much information about the intersection.

The argument for (1) uses fairly standard ideas from information theory: when we consider n random variables $\mathrm{X}_1, \ldots, \mathrm{X}_n$ and a function $\mathrm{M}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$, and choose an index $i \in [n]$ with some distribution that has high min-entropy, then $\mathrm{I}(\mathrm{M}; \mathrm{X}_i)$ is small. In our case, we choose not one index but possibly several (as the intersection can be large), so the argument needs to be generalized somewhat.[3]

The second message is a different story, because with some small probability, A's first message revealed too much information about the intersection. (The mutual information $\mathrm{I}(\mathrm{M}; \mathrm{X}_i)$ is, after all, an *expectation* over messages.) If the players managed to establish such dependence, then the eavesdropper no longer stands any chance of breaking the protocol's secrecy. To deal with this low-probability event, we switch to using statistical distance instead of mutual information. Mutual information is unbounded, so even low-probability events can cost too much in expectation; statistical distance on the other hand is bounded by one.

Statistical distance is less convenient to work with (e.g., it is not additive), so our argument for the second message is more complex. It involves "pretending" that B learned *nothing* about the intersection, proving that in this case his message also does not reveal much about the intersection, and then switching back to the real distribution, where B knows a little about the intersection, and accounting for the difference.

The reason we could not continue this argument to any number of rounds is that perversely, after the second round, the eavesdropper's own queries may create dependence between the queries of the two parties.[4] This means that, even though we bounded the dependence created by the

[3] For the reader familiar with Shearer's inequality — we prove a Shearer-like statement for mutual information.

[4] For instance, A can send the answer to her first query, and B can reply with his first query, followed by the XOR of the answers to his first two queries. In this case, the view of A is independent from the queries of B; however, after the eavesdropper asks B's first query, she learns whether or not B's second query is equal to A's first query. This creates dependence between the honest parties' views, when we condition on the eavesdropper's view.

messages in the first two rounds, when the eavesdropper asks the heavy queries after the second round, its own queries can increase the dependence and violate our bound.

1.2 Related Work

Impagliazzo and Rudich [9] showed that the key of any ℓ-query key-agreement protocol in the random-oracle model can be revealed by an $O(\ell^6)$ query eavesdropper. Barak and Mahmoody [2] have improved upon the above presenting an $O(\ell^2)$ query eavesdropper for this task, yielding that Merkle Puzzles is optimal in this respect. Haitner, Omri, and Zarosim [6] used the machinery of [2], to show that any no-input ℓ-query random oracle protocol, can be mapped into an "equivalent" no-oracle protocol, using an $O(\ell^2)$-query mapping, yielding that a no input task that is impassible to achieve information theoretical, cannot be computed securely in the random-oracle model against $O(\ell^2)$-query adversaries. The focus of the above works is on no-input random oracle protocols. Finding limitation on the usefulness of random oracles for with-input protocols seems to be a more difficult question, Chor and Kushilevitz [3], and Mahmoody et al. [10] made some progress in this direction. Finally, Haitner, Hoch, Reingold, and Segev [7] gave lower bounds on the communication complexity of statistically hiding commitments and single-server private information retrieval in a weaker oracle model that captures the hardness of one-way functions/permutation more closely.

Paper Organization

Formal definitions and notation used throughout the paper are given in Section 2. The bound for uniform-query protocols is formally stated and proved in Section 3, and the bound for two-message non-adaptive protocols is stated and proved in Section 4.

2 Preliminaries

2.1 Notations

We use calligraphic letters to denote sets, uppercase for random variables and lowercase for values. For $m \in \mathbb{N}$, let $[m] = \{1, \ldots, m\}$. For a random variable X, let $x \xleftarrow{R} \mathrm{X}$ to denote that x is chosen according to X. Similarly, for a set S let $s \xleftarrow{R} \mathsf{S}$ to denote that s is chosen according to the uniform distribution over S. The support of the distribution D, denoted $\mathrm{Supp}(D)$, is defined as $\{u \in \mathcal{U} : \Pr_D[u] > 0\}$. The statistical distance between two distributions P and Q over a finite set $\mathcal{U}$, denoted $\mathrm{SD}(P, Q)$, is defined as $\frac{1}{2}\sum_{u\in\mathcal{U}} |\Pr_P[u] - \Pr_Q[u]|$, which is equal to $\max_{\mathcal{S}\subset\mathcal{U}}(\Pr_P[\mathcal{S}] - \Pr_Q[\mathcal{S}])$.

For a vector $\mathbf{X} = X_1, ..., X_n$ and an index $i \in [n]$, let $X_{<i}$ denote the vector $X_1, ..., X_{i-1}$ and $X_{\le i}$ denote the vector $X_1, ..., X_i$. For a set of indexes $T = \{i_1, \ldots, i_k\} \subseteq [n]$ such that $i_1 < i_2 < \cdots < i_k$, let X_T denote the vector $X_{i_1}, \ldots, X_{i_k}$. Similarly, $X_{T,<i}$ denotes the vector $X_{T\cap\{1,\ldots,i-1\}}$. For a function f, let $f(\mathbf{X}) = (f(X_1), ..., f(X_n))$.

For random variables A and B we use $\mathrm{A}|_{\mathrm{B}=b}$ to denote te distribution of A condition on the event $\mathrm{B} = b$.

2.2 Interactive Protocols

A two-party protocol $\Pi = (\mathsf{A}, \mathsf{B})$ is a pair of probabilistic interactive Turing machines. The communication between the Turing machines A and B is carried out in rounds, where in each round

one of the parties is active and the other party is idle. In the j-th round of the protocol, the currently active party P acts according to its partial view, writing some value on its output tape, and then sending a message to the other party (i.e., writing the message on the common tape). The communication transcript (henceforth, the transcript) of a given execution of the protocol $\Pi = (\mathsf{A}, \mathsf{B})$, is the list of messages m exchanged between the parties in an execution of the protocol, where $m_{1,\ldots,j}$ denotes the first j messages in m. A view of a party contains its input, its random tape and the messages exchanged by the parties during the execution. Specifically, A's view is a tuple $v_{\mathsf{A}} = (i_{\mathsf{A}}, r_{\mathsf{A}}, m)$, where i_{A} is A's input, r_{A} are A's random coins, and m is the transcript of the execution. Let out^{A} denote the output of A in the end of the protocol, and out^{B} B's output. Notice that given a protocol, the transcript and the outputs are deterministic function of the joint view $(i_{\mathsf{A}}, r_{\mathsf{A}}, i_{\mathsf{B}}, r_{\mathsf{B}})$. For a joint view v, let $\mathsf{trans}(v)$, $\text{out}^{\mathsf{A}}(v)$ and $\text{out}^{\mathsf{B}}(v)$ be the transcript of the protocol and the parties' outputs determined by v. For a distribution D we denote the distribution over the parties' joint view in a random execution of Π, with inputs drawn from D by $\Pi(D)$.

A protocol Π has r rounds, if for every possible random tapes for the parties, the number of rounds is exactly r. The Communication Complexity of a protocol Π, denote as $\text{CC}(\Pi)$ is the length of the transcript of the protocol in the worst case.

2.3 Oracle-Aided Protocols

An oracle-aided two-party protocol $\Pi = (\mathsf{A}, \mathsf{B})$ is a pair of interactive Turing machines, where each party has an additional tape called the oracle tape; the Turing machine can make a query to the oracle by writing a string q on its tape. It then receives a string *ans* (denoting the answer for this query) on the oracle tape. An oracle-aided protocol is ℓ-queries protocol if each party makes at most ℓ queries during each run of the protocol. In a *non-adaptive* oracle-aided protocol, the parties choose their queries before the protocol starts and before querying the oracle. A *uniform query* oracle-aided protocol, is a non-adaptive protocol in which the parties queries are chosen uniformly form a predetermined set.

2.4 Key-Agreement Protocols

Since we are giving lower bounds, we focus on single bit protocols.

Definition 2.1 (key-agreement protocol)**.** *Let $0 \leq \gamma$, $\alpha \leq 1$ and $q \in N$. A two-party boolean output protocol $\Pi = (\mathsf{A}, \mathsf{B})$ is a (q, α, γ)-key-agreement relative to a function family $\mathcal{F}$, if the following hold:*

Accuracy: Π has $(1-\alpha)$-accuracy. *For every $f \in \mathcal{F}$:*

$$\Pr_{v \xleftarrow{R} \Pi^f}\left[\text{out}^{\mathsf{A}}(v) = \text{out}^{\mathsf{B}}(v)\right] \geq 1 - \alpha.$$

Secrecy: Π has (q, γ)-secrecy. *For every q-query oracle-aided algorithm E:*

$$\Pr_{f \xleftarrow{R} \mathcal{F}, v \xleftarrow{R} \Pi^f}\left[\mathsf{E}^f(\mathsf{trans}(v)) = \text{out}^{\mathsf{A}}(v)\right] \leq \gamma.$$

If $\mathcal{F}$ is a trivial function family (e.g., $\mathcal{F}$ only contains only the identity function), then all correlation between the parties' view is implied by the transcript. Hence, an adversary that on a given transcript τ samples a random view for A that is consistent with τ, and outputs whatever A

would upon this view, agrees with B with the same probability as does A. This simple argument yields the following fact.

Fact 2.2. *For every $0 \leq \alpha \leq 1$ and $0 \leq \gamma < 1 - \alpha$, there exists no (q, α, γ)-key-agreement protocol relative to the trivial family.*

2.5 Entropy and Information

The Shannon Entropy of a random variable A is defined as $\mathrm{H}(\mathrm{A}) = \sum_{a \in \mathrm{Supp}(\mathrm{A})} \Pr_{\mathrm{A}}[a] \log \frac{1}{\Pr_{\mathrm{A}}[a]}$. The conditional Entropy of a random variable A given B is defined as $\mathrm{H}(\mathrm{A}|\mathrm{B}) = E_{b \xleftarrow{\mathrm{R}} \mathrm{B}}[H(\mathrm{A}|\mathrm{B} = b)]$. The following fact is called the chain rule of Shannon Entropy:

Fact 2.3 (Chain rule for entropy)**.** *For a random variable $\boldsymbol{A} = \mathrm{A}_1, ..., \mathrm{A}_n$ the following holds:*

$$\mathrm{H}(\mathrm{A}_1, ..., \mathrm{A}_n) = \sum_{i=1}^{n} \mathrm{H}(\mathrm{A}_i|\mathrm{A}_1, ...\mathrm{A}_{i-1}).$$

The mutual information between two random variables A and B is defined as $\mathrm{I}(\mathrm{A};\mathrm{B}) = \mathrm{H}(\mathrm{A}) - \mathrm{H}(\mathrm{A}|\mathrm{B})$. The mutual information is known to be symmetric, and the following facts are known:

Fact 2.4 (Chain rule for information)**.** *For a random variables $\boldsymbol{A} = \mathrm{A}_1, ..., \mathrm{A}_n$ and* B*,*

$$\mathrm{I}(\mathrm{A};\mathrm{B}) = \sum_{i=1}^{n} \mathrm{I}(\mathrm{A}_i;\mathrm{B}|\mathrm{A}_1, ..., \mathrm{A}_{i-1}).$$

Fact 2.5. *For every random variables* A *and* B*, $0 \leq \mathrm{I}(\mathrm{A};\mathrm{B}) \leq \mathrm{H}(\mathrm{A}) \leq |\mathrm{A}|$.*

Fact 2.6. *Let* $\mathrm{A}, \mathrm{B}, \mathrm{C}$ *be random variables.*

- *If* A *is independent of* C*, Then* $\mathrm{I}(\mathrm{A};\mathrm{B}) \geq \mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{C})$.
- *If condition on* B*,* A *is independent of* C*, Then* $\mathrm{I}(\mathrm{A};\mathrm{B}) \leq \mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{C})$.

Fact 2.7 (Data processing inequality)**.** *Let* A, B *be random variables, and f a function. Then:* $\mathrm{I}(f(\mathrm{A});\mathrm{B}) \leq \mathrm{I}(\mathrm{A};\mathrm{B})$ *and* $\mathrm{H}(f(\mathrm{A})) \leq \mathrm{H}(\mathrm{A})$.

Lastly, a connection between mutual information and statistical distance is known:

Fact 2.8 (Pinsker's inequality)**.**

$$\mathrm{SD}\left((\mathrm{A}, \mathrm{B}), (\mathrm{A} \times \mathrm{B})\right) \leq 2\sqrt{\mathrm{I}(\mathrm{A};\mathrm{B})}.$$

We will also use the next general lemmas in our proof:

Lemma 2.9. *For every random variables* $\mathrm{A}, \mathrm{B}, \mathrm{C}$ *and* D *it holds that*

$$-\mathrm{I}(\mathrm{A};\mathrm{D}|\mathrm{C}) \leq \mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{C},\mathrm{D}) - \mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{C}) \leq \mathrm{I}(\mathrm{A};\mathrm{D}|\mathrm{C},\mathrm{B})$$

.

Proof.

$$\begin{aligned}
&\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{C},\mathrm{D}) - I(\mathrm{A};\mathrm{B}|\mathrm{C}) \\
&\qquad = \mathrm{H}(\mathrm{A}|\mathrm{C},\mathrm{D}) - \mathrm{H}(\mathrm{A}|\mathrm{B},\mathrm{C},\mathrm{D}) - [\mathrm{H}(\mathrm{A}|\mathrm{C}) - \mathrm{H}(\mathrm{A}|\mathrm{B},\mathrm{C})] \\
&\qquad = \mathrm{H}(\mathrm{A}|\mathrm{C},\mathrm{D}) - \mathrm{H}(\mathrm{A}|\mathrm{C}) - [\mathrm{H}(\mathrm{A}|\mathrm{B},\mathrm{C},\mathrm{D}) - \mathrm{H}(\mathrm{A}|\mathrm{B},\mathrm{C})] \\
&\qquad = \mathrm{I}(\mathrm{A};\mathrm{D}|\mathrm{C},\mathrm{B}) - \mathrm{I}(\mathrm{A};\mathrm{D}|\mathrm{C})
\end{aligned}$$

The inequalities hold by the fact that mutual information is always positive. □

The next two lemmas are useful in bounding information by using Bernoulli random variables:

Lemma 2.10. *Let* J *be a Bernoulli random variable, s.t.* $\Pr[\mathrm{J}=1] \leq 1/2$. *Then*

$$\mathrm{H}(\mathrm{J}) \leq \Pr[\mathrm{J}=1]\,(\log \frac{1}{\Pr[\mathrm{J}=1]} + 4).$$

Proof.

$$\begin{aligned}
\mathrm{H}(\mathrm{J}) &= \Pr[\mathrm{J}=1] \log \frac{1}{\Pr[\mathrm{J}=1]} + \Pr[\mathrm{J}=0] \log \frac{1}{\Pr[\mathrm{J}=0]} \\
&\leq \Pr[\mathrm{J}=1] \log \frac{1}{\Pr[\mathrm{J}=1]} + \log \frac{1}{1-\Pr[\mathrm{J}=1]}
\end{aligned}$$

Let $f(x) = log\frac{1}{1-x} - 4x$. We need to show that $f(x) \leq 0$ for all $0 \leq x \leq 1/2$. $f(0) = 0$, therefore it is enough to show that $f'(x) \leq 0$.

$$\begin{aligned}
f'(x) =& \frac{1}{\ln 2}\frac{1}{1-x} - 4 \\
&\leq 2\frac{1}{1-x} - 4 \leq 4 - 4 = 0 \qquad (0 \leq x \leq 1/2)
\end{aligned}$$

□

Lemma 2.11. *Let* $\mathrm{A},\mathrm{B},\mathrm{M}$ *and for each* $m \in M$ E_m *be random variables. Let* J_m *be the indicator for the event* $\mathrm{M}=m$, *then*

$$\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{M},\mathrm{E}_M) \leq \sum_{m\in M} \big[I(\mathrm{A};\mathrm{B}|\mathrm{E}_m) + I(\mathrm{J}_m;\mathrm{B}|\mathrm{E}_m,\mathrm{A})\big].$$

Proof.

$$\begin{aligned}
\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{M},\mathrm{E}_M) &= \sum_{m\in\mathrm{M}} \Pr\left[\mathrm{M}=m\right]\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{M}=m,\mathrm{E}_m) \\
&= \sum_{m\in\mathrm{M}} \Pr\left[\mathrm{J}_m=1\right]\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{J}_m=1,\mathrm{E}_m) \\
&\leq \sum_{m\in\mathrm{M}} \left[\Pr\left[\mathrm{J}_m=1\right]\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{J}_m=1,\mathrm{E}_m) + \Pr\left[\mathrm{J}_m=0\right]\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{J}_m=0,\mathrm{E}_m)\right] \\
&\qquad\qquad \text{(Because I is non-negative)} \\
&= \sum_{m\in\mathrm{M}} \mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{J}_m,\mathrm{E}_m) \\
&\leq \sum_{m\in\mathrm{M}} \mathrm{I}(\mathrm{A},\mathrm{J}_m;\mathrm{B}|\mathrm{E}_m) && \text{(Chain rule)} \\
&= \sum_{m\in\mathrm{M}} \left[\mathrm{I}(\mathrm{A};\mathrm{B}|\mathrm{E}_m) + \mathrm{I}(\mathrm{J}_m;\mathrm{B}|\mathrm{E}_m,\mathrm{A})\right] && \text{(Chain rule)}
\end{aligned}$$

□

2.5.1 Some Useful Facts

Fact 2.12 (Data processing inequality for statistical distance)**.** *Let* A,B *be random variables, and* f *a function. Then:* $\mathrm{SD}(f(\mathrm{A}),f(\mathrm{B})) \leq \mathrm{SD}(\mathrm{A},\mathrm{B})$.

Fact 2.13. *Let* $\mathrm{A},\mathrm{B},\mathrm{C}$ *be random variables. Then:* $\mathrm{SD}((\mathrm{A},\mathrm{B}),(\mathrm{A},\mathrm{C})) = \mathrm{E}_{a\overset{R}{\leftarrow}\mathrm{A}}\left[\mathrm{SD}(\mathrm{B}|_{\mathrm{A}=a},\mathrm{C}|_{\mathrm{A}=a})\right]$.

Fact 2.14. *Let* $\mathrm{A},\mathrm{B},\mathrm{C}$ *be random variables. Then:* $\mathrm{SD}((\mathrm{A}\times\mathrm{B}),(\mathrm{A}\times\mathrm{C})) = \mathrm{SD}(\mathrm{B},\mathrm{C})$.

Fact 2.15 (Hoeffding's inequality[8])**.** *Let* $\mathrm{A}_1,...,\mathrm{A}_n$ *be independent random variables s.t.* $\mathrm{A}_i\in[0,1]$ *and let* $\widehat{\mathrm{A}} = \frac{1}{n}\Sigma_{i=1}^n\mathrm{A}_i$*. It holds that:*

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

Fact 2.16 (Jensen's inequality)**.** *Let* f *be some convex function, and* $x_1,...,x_n$ *some numbers in* f*'s domain. And let* $w_1,...,w_n$ *be positive weights such that* $\Sigma w_i = 1$*. Then:*

$$f(\Sigma w_i x_i) \geq \Sigma w_i f(x_i).$$

The proofs for the next three lemmas are appear in Appendix B:

Lemma 2.17. *Let* A,B *and* C *be random variables. Then*

$$\mathop{\mathrm{E}}_{c\overset{R}{\leftarrow}\mathrm{C}}\left[\mathrm{SD}\left((\mathrm{A},\mathrm{B}|_{\mathrm{C}=c}),(\mathrm{A}|_{\mathrm{C}=c})\times(\mathrm{B}|_{\mathrm{C}=c})\right)\right] \leq 2\mathrm{SD}\left((\mathrm{A},\mathrm{C},\mathrm{B}),(\mathrm{A},\mathrm{C})\times(\mathrm{B})\right).$$

Lemma 2.18. *Let* A,B *and* M *be random variables. Then*

$$\mathrm{SD}\left((\mathrm{M},\mathrm{A}),(\mathrm{M}\times\mathrm{A})\right) \leq \mathop{\mathrm{E}}_{b\overset{R}{\leftarrow}\mathrm{B}}\left[\mathrm{SD}\left((\mathrm{M},\mathrm{A}|_{\mathrm{B}=b}),(\mathrm{M}|_{\mathrm{B}=b})\times(\mathrm{A}|_{\mathrm{B}=b})\right)\right] + \mathrm{SD}\left((\mathrm{A},\mathrm{B}),(\mathrm{A}\times\mathrm{B})\right).$$

Lemma 2.19. *Let* A, B *and* M *be random variables. Then*

$$\mathop{\mathrm{E}}_{m \xleftarrow{R} \mathrm{M}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{B}|_{\mathrm{M}=m}), ((\mathrm{A}|_{\mathrm{M}=m}) \times (\mathrm{B}|_{\mathrm{M}=m}))\right)\right] \leq 2 \mathop{\mathrm{E}}_{b \xleftarrow{R} \mathrm{B}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{M}|_{\mathrm{B}=b}), ((\mathrm{A}|_{\mathrm{B}=b}) \times (\mathrm{M}|_{\mathrm{B}=b}))\right)\right] + 2\mathrm{SD}\left((\mathrm{A}, \mathrm{B}), (\mathrm{A} \times \mathrm{B})\right).$$

For our proof we need only the following specific case of Lemma 2.19:

Corollary 2.20. *Let* A, B *and* M *be random variables, such that* $\mathrm{A} \perp \mathrm{B}$*. Then*

$$\mathop{\mathrm{E}}_{m \xleftarrow{R} \mathrm{M}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{B}|_{\mathrm{M}=m}), (\mathrm{A}|_{\mathrm{M}=m} \times \mathrm{B}|_{\mathrm{M}=m})\right)\right] \leq 2 \mathop{\mathrm{E}}_{b \xleftarrow{R} \mathrm{B}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{M}|_{\mathrm{B}=b}), (\mathrm{A}|_{\mathrm{B}=b} \times \mathrm{M}|_{\mathrm{B}=b})\right)\right].$$

3 Uniform-Query Protocols

In this section, we prove a lower bound on the communication complexity of *uniform-query* key-agreement protocols. Recall that an oracle-aided protocol has *uniform-queries*, if the queries made by the parties are uniformly chosen independently from an (a-priori fixed) domain. Our bound is that an ℓ-uniform-query protocol secure against ℓ^2-query eavesdropper, must have communication complexity $\Omega(\ell)$. It follows that the uniform-query protocol of Merkle [12] (i.e., Merkle puzzle) has optimal communication complexity (up to a log factor) for such protocols. We prove the bound by exhibiting a reduction from uniform-query key-agreement protocol to (no oracle) protocol for solving the *set-disjointness problem*.

Definition 3.1 (Set-disjointness)**.** *Protocol* $\Pi = (\mathsf{A}, \mathsf{B})$ solves set-disjointness with error ϵ over distribution D (with support $(\{0,1\}^*)^* \times (\{0,1\}^*)^*$)*, if*

$$\Pr_{\substack{(\mathcal{X},\mathcal{Y}) \xleftarrow{R} D \\ r_{\mathsf{A}} \xleftarrow{R} \{0,1\}^*, r_{\mathsf{B}} \xleftarrow{R} \{0,1\}^*, r_p \xleftarrow{R} \{0,1\}^*}} \left[(\mathsf{A}(\mathcal{X}; r_{\mathsf{A}}), \mathsf{B}(\mathcal{Y}; r_{\mathsf{B}}))(r_{\mathsf{P}}) = (\mathcal{X} \cap \mathcal{Y} = \emptyset \wedge \mathcal{X} \cap \mathcal{Y} = \emptyset)\right] \geq 1 - \varepsilon.$$

Namely, with save but probability ε over the instance in hand and their private and public randomness, the parties find outs whether their two input sets intersect. Our reduction is to solving set-disjointness over the distribution below, known to be hard for low complexity protocols.

Definition 3.2 (hard distribution for set-disjointness)**.** *For* $\ell \in \mathbb{N}$*, let* $\mathcal{Q}^0_\ell = \{\mathcal{X}, \mathcal{Y} \subset [\ell] \colon |\mathcal{X}| = |\mathcal{Y}| = \lfloor \ell/4 \rfloor \ , \ \mathcal{X} \cap \mathcal{Y} = \emptyset\}$ *and let* $\mathcal{Q}^1_\ell = \{\mathcal{X}, \mathcal{Y} \subset [\ell] \colon |\mathcal{X}| = |\mathcal{Y}| = \lfloor \ell/4 \rfloor, |\mathcal{X} \cap \mathcal{Y}| = 1\}$*. Let* D^0_ℓ *and* D^1_ℓ *be the uniform distribution over* $\mathcal{Q}^0_\ell$ *and* $\mathcal{Q}^1_\ell$ *respectively, and let* $D_\ell = \frac{3}{4} \cdot D^0_\ell + \frac{1}{4} \cdot D^1_\ell$*.*

Razborov [15] has shown that solving set-disjointness D_ℓ with small error require high communication complexity.

Theorem 3.3 (hardness of D_ℓ, [15])**.** *Exists* $\epsilon > 0$ *such that for every* $\ell \in \mathbb{N}$ *and a protocol* Π *that solves set-disjointness over* D_ℓ *with error* ϵ*, it holds that* $\mathrm{CC}(\Pi) \geq \Omega(\ell)$*.*

For a finite set $\mathcal{S}$, let $\mathcal{F}_{\mathcal{S}} = \{f : \mathcal{S} \mapsto \{0,1\}^*\}$ be the family of all functions from $\mathcal{S}$ to binary strings. Our reduction is stated in the following theorem.

Theorem 3.4 (from uniform-query key-agreement protocols to set-disjointness)**.** *Assume exists an ℓ-uniform-query $(0, \alpha, \gamma)$-key agreement protocol relative to $\mathcal{F}_{\mathcal{S}}$, for some set $\mathcal{S}$, of communication complexity c. Then there exists a protocol for solving set-disjointness over D_ℓ with ϵ error and communication complexity $\frac{2^{15} \cdot \ell^4 \cdot \log 1/\epsilon}{|\mathcal{S}|^2 (1-\alpha-\gamma)^4} \cdot c$.*

Note that the above theorem holds also for protocols that are only secure against eavesdropper without access to the oracle. Combining Theorems 3.3 and 3.4 yields the following bound on the communication complexity of uniform-query key-agreement protocols.

Theorem 3.5 (Main result for uniform-inputs protocols)**.** *For any ℓ-uniform-query (q, α, γ)-key agreement protocol Π relative to $\mathcal{F}_{\mathcal{S}}$, it holds that* $\mathrm{CC}(\Pi) \in \Omega((1-\alpha-\gamma)^4 q^2/\ell^3)$.

Proof. By Theorems 3.3 and 3.4, protocol Π has communication complexity $\Omega((1-\alpha-\gamma)^4 |\mathcal{S}|^2 / \ell^3)$. By Fact 2.2, an eavesdropper that queries all the elements in $\mathcal{S}$ can guess the key with probability $1-\alpha$. Since without loss of generality $1-\alpha > \gamma$, it must hold that $q < |\mathcal{S}|$. Hence, $\mathrm{CC}(\Pi) \in \Omega((1-\alpha-\gamma)^4 q^2/\ell^3)$. □

The rest of this section is devoted for proving Theorem 3.4. Assume there exists an ℓ-uniform-query $(0, \alpha, \gamma)$-key-agreement protocol $\Pi = (\mathsf{A}, \mathsf{B})$ relative to the function family $\mathcal{F}_{\mathcal{S}}$. We use Π to create a (no-oracle) protocol of about the same communication complexity that finds out the intersection size of parties inputs. We complete the proof showing that the latter protocol can be used to solve set-disjointness over the hard distribution D_ℓ.

Protocol Λ_{Com} below emulates protocol Π relative to the family $\mathcal{F}_{\mathcal{S}}$, in the communication complexity model (where no oracle is given). The parties of Λ_{Com} emulate of the random oracle using their shared public randomness interpreted as (description of a) function from the function family.

Protocol 3.6 ($\Lambda_{\mathsf{Com}} = (\mathsf{A}_{\mathsf{Com}}, \mathsf{B}_{\mathsf{Com}})$)**.**

$\mathsf{A}_{\mathsf{Com}}$*'s input: an ℓ-element set $\mathcal{X} \subseteq \mathcal{S}$.*

$\mathsf{B}_{\mathsf{Com}}$*'s input: an ℓ-element set $\mathcal{Y} \subseteq \mathcal{S}$.*

Public randomness: (description of a) function $f \in \mathcal{F}_{\mathcal{S}}$.

Operation:

$\mathsf{A}_{\mathsf{Com}}$ *and* $\mathsf{B}_{\mathsf{Com}}$ *interact in an execution* $(\mathsf{A}(\mathcal{X}, f(\mathcal{X})), \mathsf{B}(\mathcal{Y}, f(\mathcal{Y})))$ *of* Π*, taking the roles of* A *and* B *respectively:* $\mathsf{A}_{\mathsf{Com}}$ *acts as* A *with queries* $\mathcal{X}$ *and answers* $f(\mathcal{X})$*, and* $\mathsf{B}_{\mathsf{Com}}$ *as* B *with queries* $\mathcal{Y}$ *and answers* $f(\mathcal{Y})$*. At the end of the interaction,* $\mathsf{A}_{\mathsf{Com}}$ *and* $\mathsf{B}_{\mathsf{Com}}$ *output the outputs of* A *and* B *respectively.*

We compare the above protocol to a protocol that emulates a run of Π *without* using the shared oracle; each party sets the answers of the oracle using its *private* randomness, and acts accordingly.

The private-oracle emulation. In this protocol, each party sample a random function using private randomness. The parties then interact according to Λ_{Com}, while treating the private function as the shared oracle.

Protocol 3.7 ($\Lambda_{\mathsf{Dist}} = (\mathsf{A}_{\mathsf{Dist}}, \mathsf{B}_{\mathsf{Dist}})$)**.**

$\mathsf{A}_{\mathsf{Com}}$*'s input: an ℓ-element set $\mathcal{X} \subseteq \mathcal{S}$.*

$\mathsf{B}_{\mathsf{Com}}$*'s input: an* ℓ*-element set* $\mathcal{Y} \subseteq \mathcal{S}$*.*

Public randomness: none.

Operation:

1. $\mathsf{A}_{\mathsf{Dist}}$ *samples* $g \xleftarrow{R} \mathcal{F}_{\mathcal{S}}$*.*
2. $\mathsf{B}_{\mathsf{Dist}}$ *samples* $f \xleftarrow{R} \mathcal{F}_{\mathcal{S}}$*.*
3. $\mathsf{A}_{\mathsf{Dist}}$ *and* $\mathsf{B}_{\mathsf{Dist}}$ *interact in protocol* $(\mathsf{A}(\mathcal{X}, g(\mathcal{X})), \mathsf{B}(\mathcal{Y}, f(\mathcal{Y})))$ *taking the roles of* A *and* B *respectively:* $\mathsf{A}_{\mathsf{Dist}}$ *acts as* A *with queries* $\mathcal{X}$ *and answers* $g(\mathcal{X})$*, and* $\mathsf{B}_{\mathsf{Dist}}$ *as* B *with queries* $\mathcal{Y}$ *and answers* $f(\mathcal{Y})$*. At the end of the interaction,* $\mathsf{A}_{\mathsf{Dist}}$ *and* $\mathsf{B}_{\mathsf{Dist}}$ *output the outputs of* A *and* B *respectively.*

Let (X, Y) be distributed as the queries of parties A and B respectively in Π (that is, uniform sets in $\mathcal{S}$ of size ℓ), and recall that $\Lambda_{\mathsf{Dist}}(\mathrm{X}, \mathrm{Y})$ and $\Lambda_{\mathsf{Com}}(\mathrm{X}, \mathrm{Y})$ denote the parties' joint view in a random execution of Λ_{Dist} and Λ_{Com} respectively, with inputs drawn from (X, Y). We first show that $\Lambda_{\mathsf{Dist}}(\mathrm{X}, \mathrm{Y})$ is far from $\Lambda_{\mathsf{Com}}(\mathrm{X}, \mathrm{Y})$. Indeed, since Λ_{Dist} is a no-oracle protocol (and has no common randomness), Fact 2.2 yields that there is an algorithm E such that

$$\Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right] = \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Dist}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right] \tag{1}$$

In contrast, since Λ_{Com} is an emulation of the protocol Π with a random oracle, the secrecy of Π and the fact that E sees not the common randomness, yields that

$$\Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\right] = \Pr_{f \xleftarrow{R} F, v \xleftarrow{R} \Pi^f}\left[\mathsf{E}^f(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}}(v)\right] \leq \gamma \tag{2}$$

Finally, since the joint distribution of the outputs of the parties in Λ_{Com} is exactly as in Π, it holds that

$$\Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\right] = \Pr_{f \xleftarrow{R} F, v \xleftarrow{R} \Pi^f}\left[\mathrm{out}^{\mathsf{A}}(v) = \mathrm{out}^{\mathsf{B}}(v)\right] \geq 1 - \alpha \tag{3}$$

It follows that at least one of the two equations below holds:

Agreement gap: (4)

$$\Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\right] - \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Dist}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right] \geq (1 - \alpha - \gamma)/2$$

Secrecy gap: (5)

$$\Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right] - \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}}(v)\right] \geq (1 - \alpha - \gamma)/2$$

Namely, wither Λ_{Com} is significantly more accurate than Λ_{Dist}, or Λ_{Com} is significantly more secure than protocol Λ_{Dist} (or both). We claim that without loss of generality one can assume that Equation (4) holds (i.e., there is agreement gap). Assuming otherwise (i.e., Equation (5) holds), we

build a new protocol with inaccurate no-oracle emulation, and then continue the proof assuming Equation (4) holds.

Consider protocols $\Lambda'_{\mathsf{Com}} = (\mathsf{A}'_{\mathsf{Com}}, \mathsf{B}'_{\mathsf{Com}})$ and $\Lambda'_{\mathsf{Dist}} = (\mathsf{A}'_{\mathsf{Dist}}, \mathsf{B}'_{\mathsf{Dist}})$, in which the parties interact according to Λ_{Com} and Λ_{Dist} respectively, but parties $\mathsf{B}'_{\mathsf{Com}}$ and $\mathsf{B}'_{\mathsf{Dist}}$ output $\neg\mathsf{E}(\mathsf{trans})$. By the secrecy gap assumption,

$$\Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right] - \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\right] \geq (1-\alpha-\gamma)/2 \tag{6}$$

Hence,

$$\begin{aligned}
&\Pr_{v \xleftarrow{R} \Lambda'_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}'_{\mathsf{Com}}}(v) = \mathrm{out}^{\mathsf{A}'_{\mathsf{Com}}}(v)\right] - \Pr_{v \xleftarrow{R} \Lambda'_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}'_{\mathsf{Dist}}}(v) = \mathrm{out}^{\mathsf{A}'_{\mathsf{Dist}}}(v)\right] \\
&= (1 - \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}(v)\right]) - (1 - \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right]) \\
&= \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right] - \Pr_{v \xleftarrow{R} \Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathsf{E}(\mathsf{trans}(v)) = \mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\right] \geq (1-\alpha-\gamma)/2.
\end{aligned}$$

That is, protocol Λ'_{Dist} is less accurate than Λ'_{Com} by $(1-\alpha-\gamma)/2$. Namely, we are exactly in the same situation as if Equation (4) holds, but with respect to protocols Λ'_{Dist} and Λ'_{Com}. From hereafter, we assume for concreteness that Equation (4) holds with respect to the original protocols Λ_{Com} and Λ_{Dist}.

3.1 From Agreement Gap to Set Disjointness

Since, by assumption, Λ_{Dist} is less accurate than Λ_{Com} in (i.e., Equation (4) holds), it is less accurate for some specific intersection size; when the parties have *no* common query, Λ_{Dist} behaves just like Λ_{Com}, and thus Λ_{Dist} is (perfectly) accurate in this case. We exploit this observation to show that the accuracy difference between the protocols enables us to distinguish between disjoint inputs and intersecting inputs, yielding a protocol that solves set intersection over certain distributions.

For $z \in \{\mathsf{Com}, \mathsf{Dist}\}$ and a joint view $v = (\mathcal{X}, r_{\mathsf{A}}, \mathcal{Y}, r_{\mathsf{B}}, r_{\mathsf{P}}) \in \mathrm{Supp}(\Lambda_z)$, let $x(v) = \mathcal{X}$ and $y(v) = \mathcal{Y}$. For $i \in [\ell]$, let $\mathrm{Acc}_z(i)$ be the accuracy of Λ_z on inputs with intersection size i. Namely,

$$\mathrm{Acc}_z(i) := \Pr_{v \xleftarrow{R} \Lambda_z(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_z}(v) = \mathrm{out}^{\mathsf{A}_z}(v) \mid |x(v) \cap y(v)| = i\right].$$

Let $\mathrm{AccGap}(i)$ be the accuracy advantage of Λ_{Com} over Λ_{Dist} on inputs with intersection size i. That is,

$$\mathrm{AccGap}(i) := \mathrm{Acc}_{\mathsf{Com}}(i) - \mathrm{Acc}_{\mathsf{Dist}}(i)$$

A key observation is that for some intersection size, protocol Λ_{Com} is more accurate than Λ_{Dist}.

Claim 3.8. *$\exists d < \frac{4\ell^2}{|\mathcal{S}|(1-\alpha-\gamma)}$ such that $\mathrm{AccGap}(d) \geq (1-\alpha-\gamma)/4$.*

Proof. Let $t := \mathrm{E}_{(\mathcal{X},\mathcal{Y}) \xleftarrow{R} (\mathrm{X},\mathrm{Y})}[|\mathcal{X} \cap \mathcal{Y}|]$ be the expected intersection size. We show below that

$$\sum_{i=0}^{\lfloor 4t/(1-\alpha-\gamma)\rfloor} \Pr_{(\mathcal{X},\mathcal{Y}) \xleftarrow{R} (\mathrm{X},\mathrm{Y})}[|\mathcal{X} \cap \mathcal{Y}| = i] \cdot \mathrm{AccGap}(i) \geq (1-\alpha-\gamma)/4 \tag{7}$$

It will then follows that $\exists d \leq 4t/(1-\alpha-\gamma)$ such that $\mathrm{AccGap}(d) \geq (1-\alpha-\gamma)/4$. We conclude the proof by showing that $t = \ell^2/|\mathcal{S}|$, and therefore $d \leq 4\ell^2/|\mathcal{S}|(1-\alpha-\gamma)$. By linearity of expectation,

$$t = \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[|\mathcal{X}\cap\mathcal{Y}|] = \sum_{i=1}^{\ell} \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[\mathcal{X}_i \in \mathcal{Y}] = \ell^2/|\mathcal{S}|\,.$$

So it is left to prove Equation (19). We first show that the expected value of $\mathrm{AccGap}(i)$ is at least $(1-\alpha-\gamma)/2$.

$$\begin{aligned}
&\mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[\mathrm{AccGap}(|\mathcal{X}\cap\mathcal{Y}|)] \qquad (8)\\
&= \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[\Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v) \mid |x(v)\cap y(v)| = |\mathcal{X}\cap\mathcal{Y}|\right]\right]\\
&\quad - \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[\Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Dist}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v) \mid |x(v)\cap y(v)| = |\mathcal{X}\cap\mathcal{Y}|\right]\right]\\
&= \Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\right] - \Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Dist}}}(v) = \mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right]\\
&\geq (1-\alpha-\gamma)/2.
\end{aligned}$$

It follows that

$$\begin{aligned}
&\sum_{i=0}^{\lfloor 4t/(1-\alpha-\gamma)\rfloor} \Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[|\mathcal{X}\cap\mathcal{Y}| = i]\cdot\mathrm{AccGap}(i)\\
&= \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[\mathrm{AccGap}(|\mathcal{X}\cap\mathcal{Y}|)] - \sum_{i=\lfloor 4t/(1-\alpha-\gamma)\rfloor+1}^{\ell} \Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[|\mathcal{X}\cap\mathcal{Y}| = i]\cdot\mathrm{AccGap}(i)\\
&\geq (1-\alpha-\gamma)/2 - \sum_{i=\lfloor 4t/(1-\alpha-\gamma)\rfloor+1}^{\ell} \Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[|\mathcal{X}\cap\mathcal{Y}| = i]\cdot\mathrm{AccGap}(i) && \text{(Equation (20))}\\
&\geq (1-\alpha-\gamma)/2 - \sum_{i=\lfloor 4t/(1-\alpha-\gamma)\rfloor+1}^{\ell} \Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}[|\mathcal{X}\cap\mathcal{Y}| = i] && (\mathrm{AccGap}(i)\leq 1)\\
&\geq (1-\alpha-\gamma)/2 - \Pr_{\mathcal{X}\xleftarrow{\mathrm{R}}\mathrm{X},\mathcal{Y}\xleftarrow{\mathrm{R}}\mathrm{Y}}[|\mathcal{X}\cap\mathcal{Y}| \geq 4t/(1-\alpha-\gamma)]\\
&\geq (1-\alpha-\gamma)/4., && \text{(Markov inequality)}
\end{aligned}$$

and the the proof of the claim follows. □

In contrast to the above claim, if the inputs are *disjoint* then there is no agreement gap. That is, we have the following fact.

Claim 3.9. $\mathrm{AccGap}(0) = 0$.

Proof. It is clear that for $(\mathrm{F},\mathrm{G}) \xleftarrow{R} \mathcal{F}_{\mathcal{S}}^2$ and pair of sets $\mathcal{X} \subseteq \mathcal{S}, \mathcal{Y} \subseteq \mathcal{S}$ with $\mathcal{X} \cap \mathcal{Y} = \emptyset$, the distributions of $(\mathcal{X}, \mathcal{Y}, \mathrm{F}(\mathcal{X}), \mathrm{F}(\mathcal{Y}))$ and of $(\mathcal{X}, \mathcal{Y}, \mathrm{F}(\mathcal{X}), \mathrm{G}(\mathcal{Y}))$ are the same. It follows that the distribution $\Lambda_{\mathsf{Dist}}|_{x\cap y=\emptyset}$ is identical to that of $\Lambda_{\mathsf{Com}}|_{x\cap y=\emptyset}$, meaning that the protocols act the same. □

Combining Claims 3.8 and 3.9 yields there exists some constant $0 < c \leq d$ such that

$$\mathrm{AccGap}\,(c) - \mathrm{AccGap}\,(c-1) \geq \mathrm{AccGap}\,(d)\,/d \geq \frac{(1-\alpha-\gamma)^2 \cdot |\mathcal{S}|}{16\ell^2} \tag{9}$$

Hence,

$$\begin{aligned} \frac{(1-\alpha-\gamma)^2\,|\mathcal{S}|}{16\ell^2} &\leq \mathrm{AccGap}\,(c) - \mathrm{AccGap}\,(c-1) \\ &= (\mathrm{Acc}_{\mathsf{Com}}\,(c) - \mathrm{Acc}_{\mathsf{Dist}}\,(c)) - (\mathrm{Acc}_{\mathsf{Com}}\,(c-1) - \mathrm{Acc}_{\mathsf{Dist}}\,(c-1)) \\ &= \mathrm{Acc}_{\mathsf{Com}}\,(c) - \mathrm{Acc}_{\mathsf{Com}}\,(c-1) + \mathrm{Acc}_{\mathsf{Dist}}\,(c-1) - \mathrm{Acc}_{\mathsf{Dist}}\,(c). \end{aligned} \tag{10}$$

Therefore, either

$$\mathrm{Acc}_{\mathsf{Com}}\,(c) - \mathrm{Acc}_{\mathsf{Com}}\,(c-1) \geq \frac{(1-\alpha-\gamma)^2\,|\mathcal{S}|}{32\ell^2}, \tag{11}$$

or

$$\mathrm{Acc}_{\mathsf{Dist}}\,(c-1) - \mathrm{Acc}_{\mathsf{Dist}}\,(c) \geq \frac{(1-\alpha-\gamma)^2\,|\mathcal{S}|}{32\ell^2}. \tag{12}$$

Namely, at least, one of protocols Λ_{Com} and Λ_{Dist} can be used to distinguish between input of intersection of size c and input of $c-1$ with good probability. We conclude the proof showing how to use this ability to solve set-disjointness on the hard distribution D_ℓ.

The set intersection protocol. In the following we assume for concreteness that Equation (11) holds, where the proof assuming Equation (12) holds follows analogously by replacing Λ_{Com} with Λ_{Dist}. Consider the following protocol for solving set intersection (in the standard communication complexity model). For simplicity, we assume that ℓ is a multiple of 4, and that $\mathcal{S} = \{1, \ldots, |\mathcal{S}|\}$.

Protocol 3.10 ($\Lambda_{\mathsf{Set}} = (\mathsf{A}_{\mathsf{Set}}, \mathsf{B}_{\mathsf{Set}})$)**.**

Parameter: $k \in N$.

$\mathsf{A}_{\mathsf{Set}}$*'s input: an* $\ell/4$*-element set* $\mathcal{X} \subseteq [\ell]$.

$\mathsf{B}_{\mathsf{Set}}$*'s input: an* $\ell/4$*-element set* $\mathcal{Y} \subseteq [\ell]$.

Public randomness: (description of) k *permutations* $\sigma_1, ..., \sigma_n$ *over* $\mathcal{S}$.

Operation:

1. $\mathsf{A}_{\mathsf{Set}}$ *sets* $\mathcal{X}' = \mathcal{X} \cup \{\ell+1, \ell+2, ..., \ell+c-1\} \cup \{2\ell, 2\ell+1, ..., 3\ell-\ell/4-c+1\}$ *and* $\mathsf{B}_{\mathsf{Set}}$ *sets* $\mathcal{Y}' = \mathcal{Y} \cup \{\ell+1, \ell+2, ..., \ell+c-1\} \cup \{3\ell, 3\ell+1, ..., 4\ell-\ell/4-c+1\}$.

2. $\mathsf{A}_{\mathsf{Set}}$ *sets* $\mathsf{counter} = 0$.

3. *For* $j = 1$ *to* k*:*

   (a) $\mathsf{A}_{\mathsf{Set}}$ *and* $\mathsf{B}_{\mathsf{Set}}$ *interact in random execution of* $(\mathsf{A}_{\mathsf{Com}}(\sigma_j(\mathcal{X}')), \mathsf{B}_{\mathsf{Com}}(\sigma_j(\mathcal{Y}')))$*, with fresh randomness, taking the roles of* $\mathsf{A}_{\mathsf{Com}}$ *and* $\mathsf{B}_{\mathsf{Com}}$ *respectively. Let* $\mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}$ *and* $\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}$ *be the parties outputs in the execution.*

   (b) $\mathsf{B}_{\mathsf{Set}}$ *sends* $\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}$ *to* $\mathsf{A}_{\mathsf{Set}}$.

   (c) *If* $\mathrm{out}^{\mathsf{A}_{\mathsf{Com}}} = \mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}$, $\mathsf{A}_{\mathsf{Set}}$ *increases* $\mathsf{counter}$ *by one.*

4. $\mathsf{A}_{\mathsf{Set}}$ *informs* $\mathsf{B}_{\mathsf{Set}}$ *whether* $\mathsf{counter}/k > (\mathrm{Acc}_{\mathsf{Com}}(c) + \mathrm{Acc}_{\mathsf{Com}}(c-1))/2$. *If positive, both parties output zero; otherwise, they output one.*

In the following we analyze the success probability and communication complexity of protocol Λ_{Set} for $k = k^* := \frac{2^{13}\ell^4 \log 1/\epsilon}{|\mathcal{S}|^2(1-\alpha-\gamma)^4}$.

Success probability of Λ_{Set}. We show that for $k = k^*$ it holds that

$$\Pr_{\substack{(\mathcal{X},\mathcal{Y}) \xleftarrow{R} D_\ell \\ r_{\mathsf{A}} \xleftarrow{R} \{0,1\}^*, r_{\mathsf{B}} \xleftarrow{R} \{0,1\}^*, r_p \xleftarrow{R} \{0,1\}^*}} [(\mathsf{A}_{\mathsf{Set}}(\mathcal{X}; r_{\mathsf{A}}), \mathsf{B}_{\mathsf{Set}}(\mathcal{Y}; r_{\mathsf{B}}))(r_{\mathsf{P}}) = (\mathcal{X} \cap \mathcal{Y} = \emptyset, \mathcal{X} \cap \mathcal{Y} = \emptyset)] \geq 1 - \varepsilon \quad (13)$$

We prove that Equation (13) holds for any fixed $(\mathcal{X}, \mathcal{Y}) \in \mathrm{Supp}(D_\ell)$. Fix such a pair $(\mathcal{X}, \mathcal{Y})$, and assume without loss of generality that $|\mathcal{S}| > 3\ell/(1-\alpha-\gamma)$ (as otherwise the proof of Theorem 3.4 is immediate). By this assumption, it holds that $c \leq d \leq 3/4\ell$. By construction, the sets $\mathcal{X}'$ and $\mathcal{Y}'$ set by the parties in Step 1 of the protocol, are both of size ℓ. Since, by definition, $(\mathcal{X}, \mathcal{Y})$ have at most one shared element, it holds that

$$\left|\mathcal{X}' \cap \mathcal{Y}'\right| = \begin{cases} c & \mathcal{X} \cap \mathcal{Y} \neq \emptyset \\ c-1, & \text{otherwise.} \end{cases} \quad (14)$$

It follows that if $|\mathcal{X}' \cap \mathcal{Y}'| = c$ and $\mathsf{counter}/k > (\mathrm{Acc}_{\mathsf{Com}}(c) + \mathrm{Acc}_{\mathsf{Com}}(c-1))/2$, then the protocol outputs the right answer. Similarly, this is the case if $|\mathcal{X}' \cap \mathcal{Y}'| = c-1$ and $\mathsf{counter}/k < (\mathrm{Acc}_{\mathsf{Com}}(c) + \mathrm{Acc}_{\mathsf{Com}}(c-1))/2$. Given these observations concerning the protocol correctness, we conclude the proof by bounding the probability that $\mathsf{counter}/k$ is far from $\mathrm{Acc}_{\mathsf{Com}}(|\mathcal{X} \cap \mathcal{Y}|)$.

Claim 3.11. *Let* $\mathsf{Counter}$ *be the value of* $\mathsf{counter}$ *in a random execution of* Λ_{Set} *on inputs* $(\mathcal{X}, \mathcal{Y})$*. Then for every* $\epsilon > 0$*,* $\delta > 0$ *and* $k = \lceil \log(1/\epsilon)/2\delta^2 \rceil$*, it holds that*
$\Pr[\mathsf{Counter}/k - \mathrm{Acc}_{\mathsf{Com}}(|\mathcal{X}' \cap \mathcal{Y}'|) > \delta] < \epsilon$ *and* $\Pr[\mathrm{Acc}_{\mathsf{Com}}(|\mathcal{X}' \cap \mathcal{Y}'| - \mathsf{Counter}/k) > \delta] < \epsilon$.

Proof. Since the parties randomly permute their inputs, for every $j \in [k]$ it holds that $\sigma_j(\mathcal{X}')$ and $\sigma_j(\mathcal{Y}')$ are random sets drawn (independently of other iteration) from the distribution $(\mathrm{X}, \mathrm{Y})|_{|\mathrm{X} \cap \mathrm{Y}| = |\mathcal{X}' \cap \mathcal{Y}'|}$. Therefore, the probability of the parties to have the same output in each run of Π is exactly $\mathrm{Acc}_{\mathsf{Com}}(|\mathcal{X} \cap \mathcal{Y}|)$. The stated bound thus follows by by Hoffeding inequality (Fact 2.15). □

Let $\delta = \frac{(1-\alpha-\gamma)^2|\mathcal{S}|}{2^7\ell^2}$. By Equation (11), it holds that $\delta < (\mathrm{Acc}_{\mathsf{Com}}(c) - \mathrm{Acc}_{\mathsf{Com}}(c-1))/2$. Hence, Claim 3.11 yields that protocol Λ_{Set} error probability on the input pair $(\mathcal{X}, \mathcal{Y})$ for parameter $k = k^*$ is less than ϵ, and Equation (13) follows.

Communication complexity. In each iteration of protocol Λ_{Set}, the parties run protocol Λ_{Com} and send one additional bit. Since $\mathrm{CC}(\Lambda_{\mathsf{Com}}) = \mathrm{CC}(\Pi)$, for $k = k^*$ we get that

$$\mathrm{CC}(\Lambda_{\mathsf{Set}}) \leq k(\mathrm{CC}(\Lambda_{\mathsf{Com}}) + 1) + 1 \leq 4k \cdot \mathrm{CC}(\Pi) = \frac{2^{15}\ell^4 \log 1/\epsilon}{|\mathcal{S}|^2 (1-\alpha-\gamma)^4} \cdot \mathrm{CC}(\Pi) \tag{15}$$

Proving Theorem 3.4. The proof of Theorem 3.4 immediately follows that above observations.

Proof of Theorem 3.4. Fix $k = k^* = \frac{2^{13}\ell^4 \log 1/\epsilon}{|\mathcal{S}|^2(1-\alpha-\gamma)^4}$. Equation (13) yields that protocol Λ_{Set} solves set-disjointness over D_ℓ with error ϵ, and Equation (15) yields that $\mathrm{CC}(\Lambda_{\mathsf{Set}}) \leq \frac{2^{15}\ell^4 \log 1/\epsilon}{|\mathcal{S}|^2(1-\alpha-\gamma)^4} \cdot \mathrm{CC}(\Pi)$. □

4 Two-Messages Non-Adaptive Protocols

In this section we prove a lower bound on the communication complexity of any non-adaptive key agreement protocol that uses only two messages. We consider protocols with respect to the family $\mathcal{F}_n$ of all functions from $\{0,1\}^n$ to $\{0,1\}^n$.

Theorem 4.1 (Main theorem for two-message, non-adaptive protocols)**.** *For any $n \in \mathbb{N}$, the communication complexity of a two-message, non-adaptive, ℓ-query (q, α, γ)-key-agreement protocol relative to $\mathcal{F}_n$ is at least*

$$\frac{(1-\alpha-\gamma)^2 q}{50^2 \ell} - 6.$$

Fix a two-message, non-adaptive, ℓ-query protocol $\Pi = (\mathsf{A}, \mathsf{B})$. Each execution of the protocol specifies the following:

- X and Y, the queries made by A and B, respectively;
- $\mathrm{M}_1, \mathrm{M}_2$, the messages sent in the two rounds;
- $\mathrm{out}^{\mathsf{A}}$ and $\mathrm{out}^{\mathsf{B}}$, the outputs of the parties.

Where M_1 is a function (not necessarily deterministic) of X and F(X), and M_2 is a function of $\mathrm{Y}, \mathrm{F}(\mathrm{Y})$ and M_1. We define an eavesdropper $\mathrm{Eve} = \mathrm{Eve}_\delta$, where δ is a parameter we will specify later, and show that Eve violates the secrecy of Π if $\mathrm{CC}(\Pi)$ is too small. Loosely speaking, the eavesdropper, which is described below, queries all "heavy" queries and outputs what B would output given these queries.

Algorithm 4.2 (The eavesdropper Eve)**.**

Oracle: $f \in \mathcal{F}_n$.

Parameter: $\delta > 0$.

Operation: *Let $\boldsymbol{m} = m_1, m_2$ be the messages exchanged in the protocol.*

1. *Query f on all elements in $\mathcal{E}_0 \cup \mathcal{E}_1$ defined as*

$$\mathcal{E}_0 = \{q \in \{0,1\}^n : \Pr[q \in X \cup Y] \geq \delta\}.$$

and

$$\mathcal{E}_1 = \left\{q \in \{0,1\}^n : \Pr\left[q \in X \cup Y \;\middle|\; M_1 = m_1, \mathrm{F}|_{\mathcal{E}_0} = f|_{\mathcal{E}_0}\right] \geq \delta\right\}.$$

2. *Sample and output*

$$k \xleftarrow{R} \mathrm{out}^{\mathsf{B}}|_{\mathrm{M}_{\leq 2}=m_{\leq 2}, \mathrm{F}|_{\mathcal{E}_0\cup\mathcal{E}_1}=f|_{\mathcal{E}_0\cup\mathcal{E}_1}}.$$

It does not matter if Eve asks her queries *during* the protocol's run or *afterwards*. It is convenient to assume that Eve asks the queries $\mathcal{E}_{i-1}$ after observing $\mathrm{M}_{\leq i-1}$ and before the next message is sent. In particular, $\mathcal{E}_0$ denotes the queries that are heavy *before* the messages are sent. These queries are a function of Π itself.

4.1 Simplifying the Structure of the Protocol

For our lower bound it is convenient to assume that the protocol has two structural properties:

(1) There are no queries that a priori heavy, that is, $\mathcal{E}_0 = \emptyset$.

(2) The secret key chosen by the players is the first bit in B's last query; that is, if B's queries are $\mathrm{Y}_1, \ldots, \mathrm{Y}_s$, then the secret key is the first bit of Y_s.

We show that any key agreement protocol can be transformed into one that has these properties, with minor loss in the parameters.

Eliminating the a priori heavy queries. First we show that if $\mathcal{E}_0 \neq \emptyset$, we can *fix* the answers to $\mathcal{E}_0$ in advance, eliminating the need for the players and for Eve to ask these queries.

Lemma 4.3. *Let Π be any ℓ-query (q, α, γ)-key-agreement protocol. Then there is an ℓ-query $(q - |\mathcal{E}_0|, \alpha, \gamma)$-protocol Θ with the same communication complexity as Π, such that Θ has no queries that are heavy a priori, that is, for each $q \in \{0,1\}^n$, and for any oracle $f \in \mathcal{F}_n$,*

$$\Pr_{\theta^f}[q \in \mathrm{X} \cup \mathrm{Y}] \leq \delta.$$

Proof. For a mapping $R : \mathcal{E}_0 \to \{0,1\}^n$ representing the answers to the queries in $\mathcal{E}_0$, let

$$\mathcal{F}^R = \left\{f \in \mathcal{F}_n \;:\; f|_{\mathcal{E}_0} = R\right\}.$$

In words, it is the set of oracles whose answers on $\mathcal{E}_0$ agree with R.

We show that there is R so that the protocol $\Pi^{\mathcal{F}^R}$, where the answers to $\mathcal{E}_0$ are fixed to agree with R, is a $(q - |\mathcal{E}_0|, \alpha, \gamma)$-key agreement protocol. We then define Θ to be the simulation of $\Pi^{\mathcal{F}^R}$ where for each query in $\mathcal{E}_0$, instead of querying the oracle the players use the answer from R.

In Θ, the queries in $\mathcal{E}_0$ are never asked, so they are no longer heavy. Moreover, no new heavy queries are created, because the protocol is non-adaptive; the queries X, Y asked by the players do not change when we fix the answers in $\mathcal{E}_0$.

Now let us choose R. First, observe that consistency is maintained for *any* setting of R: for each $f \in \mathcal{F}_n$,

$$\Pr_{v \xleftarrow{R} \Pi^f}\left[\text{out}^{\mathsf{A}}(v) = \text{out}^{\mathsf{B}}(v)\right] \geq 1 - \alpha.$$

In particular this holds for $f \in \mathcal{F}^R$ for any R.

As for secrecy, assume for the sake of contradiction that there is no R under which Π is $(q - |\mathcal{E}_0|, \gamma)$-secure with respect to $\mathcal{F}^R$; that is, for each $R : \mathcal{E}_0 \to \{0,1\}^n$ there exists an attacker Eve_R that asks $q - |\mathcal{E}_0|$ queries such that

$$\Pr_{f \xleftarrow{R} \mathcal{F}^R, v \xleftarrow{R} \Pi^f}\left[\text{Eve}_R^f(trans(v)) = \text{out}^{\mathsf{A}}(v)\right] \geq \gamma.$$

Define an attacker Eve that breaks the original protocol Π as follows: First, Eve queries $\mathcal{E}_0$; let R be the answers she receives. Next, Eve simply runs Eve_R. We have:

$$\Pr_{\mathrm{f} \xleftarrow{R} \mathcal{F}_n, v \xleftarrow{R} \Pi^f}\left[\text{Eve}^f(trans(v)) = \text{out}^{\mathsf{A}}(v)\right] \geq \gamma.$$

This contradicts the secrecy of Π.

□

The key can be B's last query. Next we show that we can transform any protocol into one where the secret key is the first bit of B's last query.

Lemma 4.4. *Let Π be an ℓ-query (q, α, γ)-key-agreement protocol with two messages and communication complexity C. Then there is an $(\ell+1)$-query (q, α, γ)-protocol Θ with two messages and communication complexity $C+1$, in which the secret key is the first bit of $\mathrm{Y}_{\ell+1}$.*

Proof. In Θ, the players execute the original protocol Π, but with the following changes:

- In the beginning of the protocol, B asks one additional query $\mathrm{Y}_{\ell+1}$. This query is chosen uniformly at random and independently of his other queries (and is not used by Π).
- A then sends her message M_1 just as she would under Π, and B computes his message M_2 under Π, and the secret key out^{B} that he would output in Π.
- B sends A the message M_2, b, where $\mathrm{b} = \text{out}^{\mathsf{B}} \oplus (\mathrm{Y}_{\ell+1})_1$ is an additional bit B appends to the message.
- B outputs $(\mathrm{Y}_{\ell+1})_1$ as his secret key.
- A computes out^{A} as in Π, and outputs $\text{out}^{\mathsf{A}} \oplus \mathrm{b}$.

Whenever $\text{out}^{\mathsf{A}} = \text{out}^{\mathsf{B}}$, A's output agrees with B's. The consistency of the new protocol, therefore, is the same as Π's.

For secrecy, let F be the random oracle, and assume there is Eve^{F} that breaks the secrecy of Θ. Namely, Eve^{F} can guess the output of A with probability at least γ. Note that $(\mathrm{Y}_{\ell+1})_1$ is a uniform random bit independent of $\mathrm{M}_1, \mathrm{M}_2$ and F. Thus, we can think that in Θ, B chooses the value of $\text{out}^{\mathsf{B}} \oplus (\mathrm{Y}_{\ell+1})_1$ *after* M_2 was sent.

- Given a transcript M_1 and M_2, the eavesdropper $\widehat{\mathrm{Eve}}^{\mathrm{F}}$ chooses a uniform random bit b.
- $\widehat{\mathrm{Eve}}^{\mathrm{F}}$ runs $\mathrm{Eve}^{\mathrm{F}}(\mathrm{M}_1, \mathrm{M}_2, \mathrm{b})$. Let $\mathrm{out}^{\mathrm{Eve}}$ be $\mathrm{Eve}^{\mathrm{F}}$'s output.
- $\widehat{\mathrm{Eve}}^{\mathrm{F}}$ outputs $\mathrm{b} \oplus \mathrm{out}^{\mathrm{Eve}}$.

Since $\mathrm{M}_1, \mathrm{M}_2, \mathrm{b}$ are distributed exactly as in Θ, we have that $\widehat{\mathrm{Eve}}^{\mathrm{F}}$ breaks Π with the same probability $\mathrm{Eve}^{\mathrm{F}}$ does, and with the same number of queries. □

4.2 Proof of the Main Theorem

We are now ready to prove Theorem 4.1. Given a (q, α, γ)-protocol, we showed in the previous section that we can construct a $(q - |\mathcal{E}_0|, \alpha, \gamma)$-protocol with one extra query and one extra bit of communication, which has the two properties we need. Henceforth, we assume that the two structural properties hold.

The heart of the lower bound is the following lemma, which asserts that the eavesdropper Eve defined above is able to ask enough queries so that B has very little advantage over Eve when it comes to outputting a secret key shared with A.

Let Π^F_{Eve} denote the distribution of Eve's view under Π^F. Namely, it is the joint distribution of $(\mathrm{M}_1, \mathrm{M}_2, \mathrm{F}(\mathcal{E}_1))$. We use v_E to denote a view of Eve drawn from this distribution.

Lemma 4.5.

$$\mathop{\mathrm{E}}_{v_E \xleftarrow{R} \Pi^{\mathrm{F}}_{\mathrm{Eve}}} \left[\mathrm{SD}\left(\left(\mathrm{X}, \mathrm{F}(\mathrm{X}), \mathrm{Y}|_{v_E}\right), \left(\mathrm{X}, \mathrm{F}(\mathrm{X})|_{v_E}\right) \times \left(\mathrm{Y}|_{v_E}\right)\right)\right] \leq 25\sqrt{\delta(\mathrm{CC}(\Pi) + 5)}. \tag{16}$$

simplicity of notation, here and below we use $\mathrm{X}, \mathrm{F}(\mathrm{X}), \mathrm{Y}|_{v_E}$ to denote $\big(\mathrm{X}, \mathrm{F}(\mathrm{X}), \mathrm{Y}\big)|_{v_E}$ (we condition all the three random variables not just Y), and similarly in other cases. We prove Lemma 4.5 below, but let us first use it to prove Theorem 4.1.

Proof of Theorem 4.1. First, let us fix δ such that Eve does not ask more than q queries. Let[5] $\delta = 4\ell/q$. Since both A and B ask together at most 2ℓ queries,

$$2\ell \geq \mathop{\mathrm{E}}_{\Pi^{\mathrm{F}}} \left[|\mathrm{X} \cup \mathrm{Y}|\right] = \sum_{q \in \{0,1\}^n} \Pr_{\Pi^{\mathrm{F}}} \left[q \in \mathrm{X} \cup \mathrm{Y}\right].$$

Since every heavy-query contributes to the sum at least δ, the size[6] of $\mathcal{E}_0$ is at most $2\ell/\delta = q/2$. Similarly, for every m_1 and $f\big|_{\mathcal{E}_0}$,

$$2\ell \geq \sum_{q \in \{0,1\}^n} \Pr_{\Pi^{\mathrm{F}}} \left[q \in \mathrm{X} \cup \mathrm{Y} \mid \mathrm{M}_1 = m_1, \mathrm{F}\big|_{\mathcal{E}_0} = f\big|_{\mathcal{E}_0}\right].$$

So, the size of $\mathcal{E}_1$ is also at most $q/2$. Overall, Eve asks no more than q queries.

[5] In general, for an r-message protocol, we would set $\delta = 2r\ell/q$.

[6] Recall that we assumed that $\mathcal{E}_0 = \emptyset$. This assumption caused a loss in parameters, so here we need to bound the size of $\mathcal{E}_0$.

Now, recall that out^{B} is assumed to be the first bit of B's last query. In particular, out^{B} is a deterministic function of Y. From Equation (16) and Fact 2.12,

$$\mathop{\mathrm{E}}_{v_E \xleftarrow{\mathrm{R}} \Pi^{\mathrm{F}}_{\mathrm{Eve}}} \left[\mathrm{SD}\left(\left(\mathrm{X}, \mathrm{F}(\mathrm{X}), \text{out}^{\mathsf{B}}|_{v_E} \right), (\mathrm{X}, \mathrm{F}(\mathrm{X})|_{v_E}) \times \left(\text{out}^{\mathsf{B}}|_{v_E} \right) \right) \right] \leq 25\sqrt{\delta(\mathrm{CC}(\Pi)+5)}.$$

A's output is a function of her view $(\mathrm{X}, \mathrm{F}(\mathrm{X}), \mathrm{M}_1, \mathrm{M}_2)$, so conditioned on $v_E = (\mathrm{M}_1, \mathrm{M}_2, \mathrm{F}(\mathcal{E}_1))$, it is a function of $(\mathrm{X}, \mathrm{F}(\mathrm{X}))$. Using the data processing inequality again, we obtain

$$\mathop{\mathrm{E}}_{v_E \xleftarrow{\mathrm{R}} \Pi^{\mathrm{F}}_{\mathrm{Eve}}} \left[\mathrm{SD}\left(\left(\text{out}^{\mathsf{A}}, \text{out}^{\mathsf{B}}|_{v_E} \right), \left(\text{out}^{\mathsf{A}}|_{v_E} \right) \times \left(\text{out}^{\mathsf{B}}|_{v_E} \right) \right) \right] \leq 25\sqrt{\delta(\mathrm{CC}(\Pi)+5)}.$$

Eve samples her output $\text{out}^{\mathrm{Eve}}$ from $\text{out}^{\mathsf{B}}|v_E$. Therefore,

$$\begin{aligned} \Pr_{\Pi^{\mathrm{F}}}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathsf{B}}\right] - \Pr_{\Pi^{\mathrm{F}}}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathrm{Eve}}\right] &= \mathop{\mathrm{E}}_{v_E \xleftarrow{\mathrm{R}} \Pi^{\mathrm{F}}_{\mathrm{Eve}}} \left[\Pr_{\Pi^{\mathrm{F}}|v_E}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathsf{B}}\right] - \Pr_{\Pi^{\mathrm{F}}|v_E}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathrm{Eve}}\right] \right] \\ &\leq 25\sqrt{\delta(\mathrm{CC}(\Pi)+5)}. \end{aligned} \tag{17}$$

In words, Eve's probability of guessing A's output is close to B's when $\mathrm{CC}(\Pi)$ is small.

On the other hand, we know that Π is α-consistent and γ-secure, so Eve *cannot* have a success probability too close to B's: By the α-consistency of Π, we have $\Pr_{\Pi^{\mathrm{F}}}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathsf{B}}\right] \geq 1-\alpha$. By the γ-secrecy, we have $\Pr_{\Pi^{\mathrm{F}}}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathrm{Eve}}\right] \leq \gamma$. Together,

$$\Pr_{\Pi^{\mathrm{F}}}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathsf{B}}\right] - \Pr_{\Pi^{\mathrm{F}}}\left[\text{out}^{\mathsf{A}} = \text{out}^{\mathrm{Eve}}\right] \geq 1-\alpha-\gamma. \tag{18}$$

Combining (17) and (18) we see that we must have

$$\mathrm{CC}(\Pi) \geq \frac{(1-\alpha-\gamma)^2}{25^2\delta} - 5.$$

□

4.3 Proving Lemma 4.5

We prove Lemma 4.5 by considering each message separately. We start with an informal exposition of the proof. The advantage the players obtain over Eve is encapsulated by the difference between

- what A and B learn about the intersection $\mathrm{X} \cap \mathrm{Y}$ of their query sets given the transcript *and their queries* X or Y; and
- what Eve knows about the intersection $\mathrm{X} \cap \mathrm{Y}$ given the transcript and *her* queries $\mathrm{F}(\mathcal{E}_1)$.

To bound this advantage, we argue that

I. After the first message (A's message), all the knowledge that B has about A's queries X comes from her first message M_1. Any advantage he has over Eve comes from what he has learned about the intersection $\mathrm{X} \cap \mathrm{Y}$ of their query sets. Because M_1 is short, B cannot learn too much about this intersection. From his point of view, the posterior distribution of the intersection given M_1 remains close to the prior (which is known to Eve).

   To establish this part of the argument we use the language of mutual information.

II. Similarly, after the second message (B's message), all the knowledge that A has gained about B's queries Y comes from M_2 *and* what B already learned about the intersection $X \cap Y$ from M_1. In particular, there is a small probability that after seeing M_1, B has learned too much about the intersection, and can use this knowledge to communicate with A securely (as Eve does not know the intersection).

   To deal with this low-probability bad event, we need to switch to the language of statistical distance, and use Lemma 4.6 below.

The following technical lemma is useful in the analysis of the second message, as it allows to ignore the knowledge B gained about the intersection in the first message. This lemma can be useful in other contexts as well. Its proof appears in Appendix B.

Lemma 4.6. *Let* $A = A_1, \ldots, A_n$*, let* $T \subseteq [n]$ *and let* B *be random variables. Let* Z *be a random variable taking values in the set* $\mathcal{Z}$*, and let* $g : \mathcal{Z} \to \mathcal{P}([n])$ *be a function mapping the domain of* Z *to subsets of* $[n]$*. Let*

$$\epsilon = \mathop{\mathrm{E}}_{z \xleftarrow{R} Z}\left[\mathop{\mathrm{E}}_{t \xleftarrow{R} T|_z}\left[I(A_t; B|A_{g(z)}, z)\right]\right] \qquad \text{and} \qquad \delta = \mathop{\mathrm{E}}_{z \xleftarrow{R} Z}\left[SD\left((A, B, T|_z), (A, B|_z) \times (T|_z)\right)\right].$$

Then

$$\mathop{\mathrm{E}}_{z, a_{g(z)} \xleftarrow{R} Z, A_{g(z)}}\left[SD\left(\left(A_T, T, B|_{z, a_{g(z)}}\right), \left((A_T, T|_{z, a_{g(z)}}) \times B|_{z, a_{g(z)}}\right)\right)\right] \leq 2\sqrt{\epsilon} + 2\delta.$$

Analyzing the first message.

We start by proving that in expectation, the first message does not create too much dependence between the players' views:

Claim 4.7. *The following statements hold after seeing* A*'s message:*

1. A*'s view remain independent of* B*'s queries:* $I(X, F(X); Y|M_1) = 0$.
2. *The same holds conditioned on Eve's queries:* $I(X, F(X); Y|M_1, F(\mathcal{E}_1)) = 0$.
3. *Not much dependence is created between* B*'s view and* A*'s queries:* $I(Y, F(Y); X|M_1) \leq \delta|M_1|$.

Proof for Claim 4.7. The proof of the first item:

$$\begin{aligned} 0 \leq I(X, F(X); Y|M_1) &\leq I(X, F(X), M_1; Y) && \text{(Chain rule)} \\ &= I(X, F(X); Y) && \text{(Since } M_1 \text{ is a function of } X, F(X)) \\ &= 0. && \text{(Because } Y \perp (X, F(X))) \end{aligned}$$

The proof of the second item:

$$\begin{aligned} 0 \leq I(X, F(X); Y|M_1, F(\mathcal{E}_1)) &\leq I(X, F(X), M_1, F(\mathcal{E}_1); Y) && \text{(Chain rule)} \\ &= I(X, F(X), F(\mathcal{E}_1); Y) && \text{(Since } M_1 \text{ is a function of } X, F(X)) \\ &\leq I(X, F; Y) && \text{(Data processing)} \\ &= 0. && \text{(Because } Y \perp (X, F)) \end{aligned}$$

To prove the third item, we first show that all the "secret information" B has about X after seeing M_1 — that is, the dependence between his view and X given M_1 — comes from the intersection between A and B's sets.

Let $\mathrm{T} := \{i \,:\, \mathrm{X}_i \in \mathrm{Y}\}$ be the indexes of the intersection queries.

Claim 4.8. $\mathrm{I}(\mathrm{Y}, \mathrm{F}(\mathrm{Y}); \mathrm{X}|\mathrm{M}_1) \leq \mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{T}, \mathrm{X})$.

Proof.

$$\begin{aligned}
\mathrm{I}(\mathrm{Y}, \mathrm{F}(\mathrm{Y}); \mathrm{X}|\mathrm{M}_1) &= \mathrm{I}(\mathrm{Y}, \mathrm{F}(\mathrm{Y}); \mathrm{X}|\mathrm{M}_1) - \mathrm{I}(\mathrm{Y}, \mathrm{F}(\mathrm{Y}); \mathrm{X}) && \text{(Because } \mathrm{X} \perp (\mathrm{Y}, \mathrm{F}(\mathrm{Y}))\text{)} \\
&\leq \mathrm{I}(\mathrm{M}_1; \mathrm{Y}, \mathrm{F}(\mathrm{Y})|\mathrm{X}) && \text{(Lemma 2.9)} \\
&\leq \mathrm{I}(\mathrm{M}_1; \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T}), \mathrm{Y}, \mathrm{F}(\mathrm{Y})|\mathrm{X}) \\
&= \mathrm{I}(\mathrm{M}_1; \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{X}) + \mathrm{I}(\mathrm{M}_1; \mathrm{Y}, \mathrm{F}(\mathrm{Y})|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T})). && \text{(Chain rule)}
\end{aligned}$$

The second term is 0: because M_1 is a function of $\mathrm{X}, \mathrm{F}(\mathrm{X})$, we have

$$\begin{aligned}
&\mathrm{I}(\mathrm{M}_1; \mathrm{Y}, \mathrm{F}(\mathrm{Y})|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T})) \\
&\leq \mathrm{I}(\mathrm{F}(\mathrm{X}); \mathrm{Y}, \mathrm{F}(\mathrm{Y})|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T})) && \text{(Data processing)} \\
&= \mathrm{I}(\mathrm{F}(\mathrm{X}); \mathrm{Y}|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T})) + \mathrm{I}(\mathrm{F}(\mathrm{X}); \mathrm{F}(\mathrm{Y})|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T}), \mathrm{Y}) && \text{(Chain rule)} \\
&\leq \mathrm{I}(\mathrm{F}(\mathrm{X}), \mathrm{F}(\mathrm{X}_\mathrm{T}); \mathrm{Y}|\mathrm{X}, \mathrm{T}) + \mathrm{I}(\mathrm{F}(\mathrm{X}); \mathrm{F}(\mathrm{Y})|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T}), \mathrm{Y}) && \text{(Chain rule)} \\
&= 0 + \mathrm{I}(\mathrm{F}(\mathrm{X}); \mathrm{F}(\mathrm{Y})|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T}), \mathrm{Y}) && ((\mathrm{X}, \mathrm{Y}, \mathrm{T}) \perp \mathrm{F}) \\
&= \mathrm{I}(\mathrm{F}(\mathrm{X} \setminus \mathrm{X}_\mathrm{T}); \mathrm{F}(\mathrm{Y} \setminus \mathrm{X}_\mathrm{T})|\mathrm{X}, \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T}), \mathrm{Y}) \\
&= 0. && \text{(Since } F \text{ is a random function and } (\mathrm{X} \setminus \mathrm{X}_\mathrm{T}) \cap (\mathrm{Y} \setminus \mathrm{X}_\mathrm{T}) = \emptyset\text{)}
\end{aligned}$$

Bound the first term:

$$\begin{aligned}
&\mathrm{I}(\mathrm{M}_1; \mathrm{T}, \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{X}) \\
&= \mathrm{I}(\mathrm{M}_1; \mathrm{T}|\mathrm{X}) + \mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{T}, \mathrm{X}) && \text{(Chain rule)} \\
&\leq \mathrm{I}(\mathrm{M}_1; \mathrm{Y}|\mathrm{X}) + \mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{T}, \mathrm{X}) && \text{(Data processing: T is a function of Y given X)} \\
&= \mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{T}, \mathrm{X}). && (\mathrm{M}_1 \perp \mathrm{Y}|\mathrm{X})
\end{aligned}$$

□

Next, we bound the information M_1 conveys about $\mathrm{F}(\mathrm{X}_\mathrm{T})$, using the fact that every element in X is in the intersection only with small probability (less than δ). The proof of the claim is similar to the proof of Shearer's inequality.

Claim 4.9. $\mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{T}, \mathrm{X}) \leq \delta|\mathrm{M}_1|$.

Proof. Recall that we denote by $X_{t,<i}$ the restriction of X to coordinates in t that are less than i. Write

$$\begin{aligned}
&\mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T})|\mathrm{T}, \mathrm{X}) \\
&= \mathop{\mathrm{E}}_{x \xleftarrow{\mathrm{R}} \mathrm{X}} \left[\mathop{\mathrm{E}}_{t \xleftarrow{\mathrm{R}} \mathrm{T}|\mathrm{X}=x} [\mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_t)|\mathrm{T} = t, \mathrm{X} = x)] \right] \\
&= \mathop{\mathrm{E}}_{x \xleftarrow{\mathrm{R}} \mathrm{X}} \left[\mathop{\mathrm{E}}_{t \xleftarrow{\mathrm{R}} \mathrm{T}|\mathrm{X}=x} \left[\sum_{i \in t} \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i)|\mathrm{T} = t, \mathrm{X} = x, \mathrm{F}(X_{t,<i})) \right] \right]. && \text{(Chain rule)}
\end{aligned}$$

For fixed x, t, i, by the chain rule,

$$\begin{aligned}
&\mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i) | \mathrm{T} = t, \mathrm{X} = x, \mathrm{F}(X_{t,<i})) \\
&\leq \mathrm{I}(\mathrm{M}_1, \mathrm{F}(X_{\{1,\ldots,i-1\}\setminus t}); \mathrm{F}(X_i) | \mathrm{T} = t, \mathrm{X} = x, \mathrm{F}(X_{t,<i})) \\
&= \mathrm{I}(\mathrm{F}(X_{\{1,\ldots,i-1\}\setminus t}); \mathrm{F}(X_i) | \mathrm{T} = t, \mathrm{X} = x, \mathrm{F}(X_{t,<i})) + \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i) | \mathrm{T} = t, \mathrm{X} = x, \mathrm{F}(X_{<i})) \\
&= 0 + \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i) | \mathrm{T} = t, \mathrm{X} = x, \mathrm{F}(X_{<i})).
\end{aligned}$$

Conditioned on X, A's message M_1 and the oracle F are independent of B's queries Y and therefore also from the intersection T. Therefore,

$$\begin{aligned}
\mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T}) | \mathrm{T}, \mathrm{X}) &\leq \mathop{\mathrm{E}}_{x \xleftarrow{\mathrm{R}} \mathrm{X}} \left[\mathop{\mathrm{E}}_{t \xleftarrow{\mathrm{R}} \mathrm{T} | \mathrm{X} = x} \left[\sum_{i \in t} \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i) | \mathrm{T} = t, \mathrm{X} = x, \mathrm{F}(X_{<i})) \right] \right] \\
&= \mathop{\mathrm{E}}_{x \xleftarrow{\mathrm{R}} \mathrm{X}} \left[\mathop{\mathrm{E}}_{t \xleftarrow{\mathrm{R}} \mathrm{T} | \mathrm{X} = x} \left[\sum_{i \in t} \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i) | \mathrm{X} = x, \mathrm{F}(X_{<i})) \right] \right] \\
&= \mathop{\mathrm{E}}_{x \xleftarrow{\mathrm{R}} \mathrm{X}} \left[\sum_i \Pr[i \in T \mid \mathrm{X} = x] \, \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i) | \mathrm{X} = x, \mathrm{F}(X_{<i})) \right].
\end{aligned}$$

From the assumption that no queries are heavy a priori, $\Pr[i \in T \mid \mathrm{X} = x] \leq \delta$ for all i. Finally,

$$\begin{aligned}
\mathrm{I}(\mathrm{M}_1; \mathrm{F}(\mathrm{X}_\mathrm{T}) | \mathrm{T}, \mathrm{X}) &\leq \delta \sum_i \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X_i) | \mathrm{X}, \mathrm{F}(X_{<i})) \\
&= \delta \, \mathrm{I}(\mathrm{M}_1; \mathrm{F}(X) | \mathrm{X}) && \text{(Chain rule)} \\
&\leq \delta |M_1|. && \text{(Fact 2.5)}
\end{aligned}$$

□

The proof of the third item is complete. □

Analyzing the second message.

We now want to show that the second message also does not create much dependence between A and B's views. As with Claim 4.7 for the first message, we first want to show that all the dependence between A's view and B's queries comes from B's message, and that this dependence goes through the intersection between A and B's queries and what the players learn about the intersection from the transcript. This is done by the next claim. Let

$$\mathrm{T}_1 := \{ i \ : \ \mathrm{Y}_i \in \mathrm{X} \setminus \mathcal{E}_1 \}.$$

In words, it is the set of the indices of B's queries in the intersection that were not queried by Eve. Recall that $\Pi^{\mathrm{F}}_{\mathrm{Eve}}$ is the distribution of Eve's view, which includes $\mathrm{M}_1, \mathrm{M}_2$ and $\mathrm{F}(\mathcal{E}_1)$. Let $\mathrm{B}_E = (\mathrm{M}_1, \mathrm{Y}, \mathrm{F}(\mathrm{Y} \cap \mathcal{E}_1))$.

Claim 4.10.

$$\begin{aligned}
&\mathop{\mathrm{E}}_{v_E \xleftarrow{R} \Pi^{\mathrm{F}}_{\mathrm{Eve}}} \left[\mathrm{SD}\left((\mathrm{X}, \mathrm{F}(\mathrm{X}), \mathrm{Y}|_{v_E}), (\mathrm{X}, \mathrm{F}(\mathrm{X})|_{v_E}) \times (\mathrm{Y}|_{v_E}) \right) \right] \\
&\qquad \leq 4 \mathop{\mathrm{E}}_{b_E \xleftarrow{R} \mathrm{B}_E} \left[\mathrm{SD}\left((\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1}), \mathrm{M}_2|_{b_E}), (\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1})|_{b_E}) \times (\mathrm{M}_2|_{b_E}) \right) \right].
\end{aligned}$$

The proof for the claim appears in Appendix B.

Now we left to show that on average, B's message cannot convey too much information about the intersection queries and their answers, as we did in Claim 4.9 for the first message. Specifically, we want to bound

$$\mathop{\mathrm{E}}_{b_E \xleftarrow{R} \mathrm{B}_E} \left[\mathrm{SD}\left(\left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1}), \mathrm{M}_2|_{b_E}\right), \left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1})|_{b_E}\right) \times \left(\mathrm{M}_2|_{b_E}\right)\right)\right].$$

It would be easier if B knew *nothing* about the intersection (i.e. M_2 was independent of T_1 given M_1). But this is not the case, as B can learn some info from A's message. However, from Claim 4.7, we know that he does not learn a lot, and his message does not strongly depend on the intersection. Formally,

Claim 4.11.

$$\mathop{\mathrm{E}}_{b_E \xleftarrow{R} \mathrm{B}_E} \left[\mathrm{SD}\left(\left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1}), \mathrm{M}_2|_{b_E}\right), \left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1})|_{b_E}\right) \times \left(\mathrm{M}_2|_{b_E}\right)\right)\right] \leq 6\sqrt{\delta(|\mathrm{M}_1| + |\mathrm{M}_2| + 5)}.$$

The two claims above complete the proof of Lemma 4.5.

Proof. By definition of B_E,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{b_E \xleftarrow{R} \mathrm{B}_E} \mathrm{SD}\left(\left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1}), \mathrm{M}_2|_{b_E}\right), \left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1})|_{b_E}\right) \times \left(\mathrm{M}_2|_{b_E}\right)\right) \\
&\quad = \mathop{\mathrm{E}}_{b_E \xleftarrow{R} \mathrm{B}_E} \mathrm{SD}\Big(\left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1}), \mathrm{M}_2|_{m_1,y,f(e_1 \cap y)}\right), \\
&\qquad\qquad \left(\mathrm{T}_1, \mathrm{F}(\mathrm{Y}_{\mathrm{T}_1})|_{m_1,y,f(e_1 \cap y)}\right) \times \left(\mathrm{M}_2|_{m_1,y,f(e_1 \cap y)}\right)\Big).
\end{aligned}$$

By Lemma 4.6, it is enough to show:

(1) $\mathrm{E}_{m_1,y \xleftarrow{R} \mathrm{M}_1,\mathrm{Y}} \left[\mathrm{SD}\left(\left(\mathrm{F}(\mathrm{Y}), \mathrm{M}_2, \mathrm{T}_1|_{m_1,y}\right), \left(\mathrm{F}(\mathrm{Y}), \mathrm{M}_2|_{m_1,y}\right) \times \left(\mathrm{T}_1|_{m_1,y}\right)\right)\right] \leq 2\sqrt{\delta|\mathrm{M}_1|}.$

(2) $\mathrm{E}_{m_1,y \xleftarrow{R} \mathrm{M}_1,\mathrm{Y}} \left[\mathrm{E}_{t \xleftarrow{R} \mathrm{T}_1|m_1,y} \left[\mathrm{I}(\mathrm{F}(y_t); \mathrm{M}_2 | m_1, y, \mathrm{F}(e_1 \cap y))\right]\right] \leq \delta(|\mathrm{M}_1| + |\mathrm{M}_2| + 5).$

The proof of the first item is (which is similar to the analysis of the first message):

$$\begin{aligned}
&\mathop{\mathrm{E}}_{m_1,y \xleftarrow{R} \mathrm{M}_1,\mathrm{Y}} \left[\mathrm{SD}\left(\left(\mathrm{F}(\mathrm{Y}), \mathrm{M}_2, \mathrm{T}_1|_{m_1,y}\right), \left(\mathrm{F}(\mathrm{Y}), \mathrm{M}_2|_{m_1,y}\right) \times \left(\mathrm{T}_1|_{m_1,y}\right)\right)\right] \\
&\leq 2\sqrt{\mathrm{I}(\mathrm{F}(\mathrm{Y}), \mathrm{M}_2; \mathrm{T}_1 | \mathrm{M}_1, \mathrm{Y})} && \text{(Fact 2.8)} \\
&= 2\sqrt{\mathrm{I}(\mathrm{F}(\mathrm{Y}); \mathrm{T}_1 | \mathrm{M}_1, \mathrm{Y})} && (\mathrm{M}_2 \text{ is a function of } \mathrm{Y}, \mathrm{F}(\mathrm{Y}), \mathrm{M}_1) \\
&\leq 2\sqrt{\mathrm{I}(\mathrm{F}(\mathrm{Y}); \mathrm{X} | \mathrm{M}_1, \mathrm{Y})} && (\mathrm{T}_1 \text{ is a function of X, Y and } \mathrm{M}_1) \\
&\leq 2\sqrt{\mathrm{I}(\mathrm{Y}, \mathrm{F}(\mathrm{Y}); \mathrm{X} | \mathrm{M}_1)} && \text{(Chain rule)} \\
&\leq 2\sqrt{\delta|\mathrm{M}_1|}. && \text{(Claim 4.7)}
\end{aligned}$$

To bound the second item we use a similar argument to the proof of Claim 4.9. The proof is more complicated here, because when we condition on M_1 and on Eve's queries, the answers of the oracle F are no longer independent of each other (e.g., A could send the XOR of the answers to her queries). Nevertheless, because not much information was revealed about the oracle's answers, not much dependence is created between them. The proof consists of two steps. First, we show that this term is bounded by $\delta\,|\mathrm{M}_2|$, plus the dependency between the answers, created by the first message and Eve's queries (Claim 4.12). Next, we bound this dependency (Claim 4.13).

Claim 4.12.

$$\mathop{\mathrm{E}}_{m_1,y\xleftarrow{R}\mathrm{M}_1,\mathrm{Y}}\left[\mathop{\mathrm{E}}_{t\xleftarrow{R}\mathrm{T}_1|m_1,y}\left[\mathrm{I}(\mathrm{F}(y_t);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y))\right]\right]$$
$$\leq \delta|\mathrm{M}_2|+\delta\mathop{\mathrm{E}}_{y\xleftarrow{R}\mathrm{Y}}\left[\sum_i \mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|\mathrm{M}_1,y,\mathrm{F}(\mathcal{E}_1\cap y))\right].$$

The proof for Claim 4.12 is similar to the proof of Claim 4.9 and appears in Appendix B.

Claim 4.13.

$$\mathop{\mathrm{E}}_{y\xleftarrow{R}\mathrm{Y}}\left[\sum_i \mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|\mathrm{M}_1,y,\mathrm{F}(\mathcal{E}_1\cap y))\right]\leq|\mathrm{M}_1|+5.$$

Proof. For every $m\in\mathrm{Supp}(\mathrm{M}_1)$, let $\mathcal{E}(m)$ be the set of queries Eve asks after seeing the message m. By Lemma 2.11 (recall that J_m is the indicator for the event $\mathrm{M}=m$),

$$\mathop{\mathrm{E}}_{y\xleftarrow{R}\mathrm{Y}}\left[\sum_i \mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|\mathrm{M}_1,y,\mathrm{F}(\mathcal{E}_1\cap y))\right]$$
$$\leq \mathop{\mathrm{E}}_{y\xleftarrow{R}\mathrm{Y}}\left[\sum_i\sum_{m\in\mathrm{M}_1}\left[\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|y,\mathrm{F}(\mathcal{E}(m)\cap y))+\mathrm{I}(\mathrm{F}(y_i);\mathrm{J}_m|y,\mathrm{F}(\mathcal{E}(m)\cap y),\mathrm{F}(y_{<i}))\right]\right]$$
(Lemma 2.11)

For every m,y,i, by the structure of F, and since $\mathrm{F}(\mathcal{E}(m)\cap y)$ is a fixed set, we have $\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|y,\mathrm{F}(\mathcal{E}(m)\cap y))=0$. Thus,

$$\mathop{\mathrm{E}}_{y\xleftarrow{R}\mathrm{Y}}\left[\sum_i\sum_{m\in\mathrm{M}_1}\left[\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|y,\mathrm{F}(\mathcal{E}(m)\cap y))+\mathrm{I}(\mathrm{F}(y_i);\mathrm{J}_m|y,\mathrm{F}(\mathcal{E}(m)\cap y),\mathrm{F}(y_{<i}))\right]\right]$$
$$=\mathop{\mathrm{E}}_{y\xleftarrow{R}\mathrm{Y}}\left[\sum_i\sum_{m\in\mathrm{M}_1}\mathrm{I}(\mathrm{F}(y_i);\mathrm{J}_m|y,\mathrm{F}(\mathcal{E}(m)\cap y),\mathrm{F}(y_{<i}))\right]$$
$$=\mathop{\mathrm{E}}_{y\xleftarrow{R}\mathrm{Y}}\left[\sum_{m\in\mathrm{M}_1}\mathrm{I}(\mathrm{F}(y);\mathrm{J}_m|y,\mathrm{F}(\mathcal{E}(m)\cap y))\right]$$ (Chain rule)
$$\leq\sum_{m\in\mathrm{M}_1}\mathrm{H}(\mathrm{J}_m).$$ (Fact 2.5)

There is at most one m' such that $\Pr[\mathrm{M}_1=m']\geq 1/2$, hence,

$$\sum_{m\in\mathrm{M}_1}\mathrm{H}(\mathrm{J}_m)$$
$$\leq 1+\sum_{m\in\mathrm{M}_1}\Pr[\mathrm{M}_1=m](-\log(\Pr[\mathrm{M}_1=m])+4)$$ (Lemma 2.10)
$$=\mathrm{H}(\mathrm{M}_1)+5.$$

□

The proof of Claim 4.11 is complete. □

4.4 Remarks

Adaptive Protocols. While we believe that the eavesdropper Eve we defined above should allow us to prove lower bounds for every non-adaptive protocol, Eve will not work for adaptive protocol, even if she can choose the sets adaptively as well. Protocol 4.14 is an example of a one-message protocol with only $O(\log(\ell))$ communication, but without any heavy query (for every $\delta > 1/\ell$). Specifically, Eve will not make any query, and can not, therefore, break the protocol. Notice, however, that every one-message protocol can be broken trivially by simulating B, so this protocol is not secure.

Protocol 4.14.

Parameters: n, $\ell = 2^{n/2}$

Common functions: $f, g : \{0,1\}^n \to \{0,1\}^n$

1. A *choses a random string* $x \in \{0,1\}^n$ *and queries* $x, f(x), ..., f^{\ell-1}(x)$ *and* $g(f^{i-1}(x))$ *for a random index* $i \in [\ell]$.
2. B *choses a random string* $y \in \{0,1\}^n$ *and queries* $y, f(y), ..., f^{\ell-1}(y)$ *and* $g(y), ..., g(f^{\ell-1}(y))$.
3. A *sends* $M_1 = g(f^{i-1}(x))$ *to* B*, and outputs* $f^{i-1}(x)$.
4. *If there is* $j \in [\ell]$ *so that* $g(f^{j-1}(y)) = M_1$ *then* B *outputs* $f^{j-1}(y)$*. Otherwise,* B *aborts.*

.

Constant Rounds Protocols We failed to continue the proof for multi-message protocol. The main reason is that we were not able to deal with the dependency caused by Eve's queries. In two-message protocol, Eve's only asks queries after the first message, which depends only on A's view. We show here that conditioning on Eve's view in this case, cannot add too much dependency between A and B. However, in protocols with more messages, the queries of Eve depend on the view of both sides, and conditioning on Eve's view can potentially make the dependency more significant.

Acknowledgement

We thank Yuval Ishai for challenging us with this intriguing question, and Omer Rotem for very useful discussions.

References

[1] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *stoc29*, pages 284–293. See also ECCC TR96-065.

[2] 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 '09*, pages 374–390, 2009.

[3] B. Chor and E. Kushilevitz. A zero-one law for boolean privacy. *SIAM Journal on Discrete Mathematics*, 4(1):36–47, 1991.

[4] G. De Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira. On the energy cost of communication and cryptography in wireless sensor networks. In *Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,*, pages 580–585. IEEE, 2008.

[5] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[6] I. Haitner, E. Omri, and H. Zarosim. Limits on the usefulness of random oracles. Technical Report 2012/573, Cryptology ePrint Archive, 2012. http://eprint.iacr.org/2012/573.

[7] I. Haitner, J. J. Hoch, O. Reingold, and G. Segev. Finding collisions in interactive protocols - tight lower bounds on the round and communication complexities of statistically hiding commitments. *SIAM Journal on Computing*, 44(1):193–242, 2015. Preliminary version in *STOC'07*.

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

[9] 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] M. Mahmoody, H. K. Maji, and M. Prabhakaran. Limits of random oracles in secure computation. *arXiv preprint arXiv:1205.3554*, 2012.

[11] R. J. McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[12] R. C. Merkle. Secure communications over insecure channels. In *SIMMONS: Secure Communications and Asymmetric Cryptosystems*, 1982.

[13] R. C. Merkle. A digital signature based on a conventional encryption function. In *Advances in Cryptology – CRYPTO '87*, pages 369–378, 1987.

[14] M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical report, MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE, 1979.

[15] A. A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, 1992.

[16] R. L. Rivest, A. Shamir, and L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

A Merkle's Puzzles

For completeness, we briefly describe here the Merkle Puzzles protocol [13]. Let $\mathcal{S}$ be a set of size ℓ^2, and $\mathcal{F}_{\mathcal{S}} = \left\{ f : \mathcal{S} \mapsto \{0,1\}^{2\log|\mathcal{S}|} \right\}$ be the family of all functions from $\mathcal{S}$ to binary strings of length $2\log|\mathcal{S}|$.

Protocol A.1 (Merkle's Puzzles protocol $\Pi = (\mathsf{A}, \mathsf{B})$)**.**

Oracle: $f \in \mathcal{F}_{\mathcal{S}}$.

Operation:

1. A *samples uniformly and independently* ℓ *elements* $x_1, ..., x_\ell \in \mathcal{S}$*, and sets* $a_1 = f(x_1), ..., a_\ell = f(x_\ell)$.

   B *samples uniformly and independently* ℓ *elements* $y_1, ..., y_\ell \in \mathcal{S}$*, and set* $b_1 = f(y_1), ..., b_\ell = f(y_\ell)$.

2. A *sends* $a_1, ..., a_\ell$ *to* B.

3. B *looks for indices* $i, j \in [\ell]$ *with* $a_i = b_i$*. If no such indices exists, it aborts.*

4. B *sends* i *to* A.

5. A *outputs* x_i *and* B *outputs* y_j.

Since each party samples $\ell = \sqrt{|\mathcal{S}|}$ uniform random element from $\mathcal{S}$, by the birthday paradox they have a common element (i.e., collision) with constant probability. By construction, the parties out the same collision, if such exists. On the other hand, from an attacker point of view the collision is a random element of $\mathcal{S}$, and therefore she cannot find it with good probability without querying a constant fraction of the element of $\mathcal{S}$, namely by making $\Theta(\ell^2)$ queries.

Note that Merkle Puzzless non-adaptive, uniform-queries, two-message protocol with near linear communication, and therefore shows that our two lower bounds (Theorems 1.1 and 1.2) are tight.

B Missing Proofs

Proof of Lemma 2.17.

$$
\begin{aligned}
&\mathop{\mathrm{E}}_{c \xleftarrow{\mathrm{R}} \mathrm{C}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{B}|_{\mathrm{C}=c}), (\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}|_{\mathrm{C}=c}) \right) \right] \\
&\leq \mathop{\mathrm{E}}_{c \xleftarrow{\mathrm{R}} \mathrm{C}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{B}|_{\mathrm{C}=c}), (\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}) \right) + \mathrm{SD}\left((\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}), (\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}|_{\mathrm{C}=c}) \right) \right] \\
&\qquad\qquad \text{(Triangle inequality)} \\
&= \mathop{\mathrm{E}}_{c \xleftarrow{\mathrm{R}} \mathrm{C}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{B}|_{\mathrm{C}=c}), (\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}) \right) + \mathrm{SD}\left((\mathrm{B}), (\mathrm{B}|_{\mathrm{C}=c}) \right) \right] \qquad \text{(Fact 2.14)} \\
&\leq \mathop{\mathrm{E}}_{c \xleftarrow{\mathrm{R}} \mathrm{C}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{B}|_{\mathrm{C}=c}), (\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}) \right) + \mathrm{SD}\left((\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}), (\mathrm{A}, \mathrm{B}|_{\mathrm{C}=c}) \right) \right] \qquad \text{(Data procesing)} \\
&= 2 \mathop{\mathrm{E}}_{c \xleftarrow{\mathrm{R}} \mathrm{C}} \left[\mathrm{SD}\left((\mathrm{A}, \mathrm{B}|_{\mathrm{C}=c}), (\mathrm{A}|_{\mathrm{C}=c} \times \mathrm{B}) \right) \right] \\
&= 2\mathrm{SD}\left((\mathrm{A}, \mathrm{C}, \mathrm{B}), (\mathrm{A}, \mathrm{C}) \times (\mathrm{B}) \right)
\end{aligned}
$$

□

Proof of Lemma 2.18.

$$\begin{aligned}
&\mathrm{SD}\left((\mathrm{M}\times\mathrm{A}),(\mathrm{M},\mathrm{A})\right)\\
&\leq \mathrm{SD}\left((\mathrm{M},\mathrm{B})\times(\mathrm{A}),(\mathrm{M},\mathrm{B},\mathrm{A})\right) && \text{(Data processing)}\\
&= \mathop{\mathrm{E}}_{b\xleftarrow{\mathrm{R}}B}\left[\mathrm{SD}\left((\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}),(\mathrm{A},\mathrm{M}|_{\mathrm{B}=b})\right)\right] && \text{(Fact 2.13)}\\
&\leq \mathop{\mathrm{E}}_{b\xleftarrow{\mathrm{R}}B}\left[\mathrm{SD}\left((\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}),(\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}|_{\mathrm{B}=b})\right)+\mathrm{SD}\left((\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}|_{\mathrm{B}=b}),(\mathrm{A},\mathrm{M}|_{\mathrm{B}=b})\right)\right]\\
& && \text{(Triangle inequality)}\\
&= \mathop{\mathrm{E}}_{b\xleftarrow{\mathrm{R}}B}\left[\mathrm{SD}\left((\mathrm{A}),(\mathrm{A}|_{\mathrm{B}=b})\right)+\mathrm{SD}\left((\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}|_{\mathrm{B}=b}),(\mathrm{A},\mathrm{M}|_{\mathrm{B}=b})\right)\right] && \text{(Fact 2.14)}\\
&= \mathrm{SD}\left((\mathrm{A}\times\mathrm{B}),(\mathrm{A},\mathrm{B})\right)+\mathop{\mathrm{E}}_{b\xleftarrow{\mathrm{R}}\mathrm{B}}\mathrm{SD}\left((\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}|_{\mathrm{B}=b}),(\mathrm{A},\mathrm{M}|_{\mathrm{B}=b})\right) && \text{(Fact 2.13)}
\end{aligned}$$

□

Proof of Lemma 2.19.

$$\begin{aligned}
&\mathop{\mathrm{E}}_{m\xleftarrow{\mathrm{R}}\mathrm{M}}\left[\mathrm{SD}\left((\mathrm{A},\mathrm{B}|_{\mathrm{M}=m}),(\mathrm{A}|_{\mathrm{M}=m}\times\mathrm{B}|_{\mathrm{M}=m})\right)\right]\\
&= \mathop{\mathrm{E}}_{m,b\xleftarrow{\mathrm{R}}\mathrm{M},\mathrm{B}}\left[\left[\mathrm{SD}\left((\mathrm{A}|_{\mathrm{M}=m,\mathrm{B}=b}),(\mathrm{A}|_{\mathrm{M}=m})\right)\right]\right] && \text{(Fact 2.13)}\\
&\leq \mathop{\mathrm{E}}_{m,b\xleftarrow{\mathrm{R}}\mathrm{M},\mathrm{B}}\left[\mathrm{SD}\left((\mathrm{A}|_{\mathrm{M}=m,\mathrm{B}=b}),(\mathrm{A}|_{\mathrm{B}=b})\right)+\mathrm{SD}\left((\mathrm{A}|_{\mathrm{B}=b}),(\mathrm{A})\right)+\mathrm{SD}\left((\mathrm{A}),(\mathrm{A}|_{\mathrm{M}=m})\right)\right]\\
& && \text{(Triangle inequality)}\\
&= \mathop{\mathrm{E}}_{b\xleftarrow{\mathrm{R}}\mathrm{B}}\left[\left[\mathrm{SD}\left((\mathrm{A},\mathrm{M}|_{\mathrm{B}=b}),(\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}|_{\mathrm{B}=b})\right)\right]+\mathrm{SD}\left((\mathrm{A},\mathrm{B}),(\mathrm{B}\times\mathrm{A})\right)+\mathrm{SD}\left((\mathrm{M}\times\mathrm{A}),(\mathrm{A},\mathrm{M})\right)\right]\\
& && \text{(Fact 2.13)}\\
&\leq 2\mathop{\mathrm{E}}_{b\xleftarrow{\mathrm{R}}\mathrm{B}}\left[\mathrm{SD}\left((\mathrm{A},\mathrm{M}|_{\mathrm{B}=b}),(\mathrm{M}|_{\mathrm{B}=b}\times\mathrm{A}|_{\mathrm{B}=b})\right)\right]+2\mathrm{SD}\left((\mathrm{A},\mathrm{B}),(\mathrm{A}\times\mathrm{B})\right) && \text{(Lemma 2.18)}
\end{aligned}$$

□

Proof. Let $t := \mathrm{E}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[|\mathcal{X}\cap\mathcal{Y}|\right]$ be the expected intersection size. We show below that

$$\sum_{i=0}^{\lfloor 4t/(1-\alpha-\gamma)\rfloor}\Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[|\mathcal{X}\cap\mathcal{Y}|=i\right]\cdot\mathrm{AccGap}\left(i\right)\geq(1-\alpha-\gamma)/4 \tag{19}$$

It will then follows that $\exists d\leq 4t/(1-\alpha-\gamma)$ such that $\mathrm{AccGap}\left(d\right)\geq(1-\alpha-\gamma)/4$. We conclude the proof by showing that $t=\ell^2/\left|\mathcal{S}\right|$, and therefore $d\leq 4\ell^2/\left|\mathcal{S}\right|(1-\alpha-\gamma)$. By linearity of expectation,

$$t=\mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[|\mathcal{X}\cap\mathcal{Y}|\right]=\sum_{i=1}^{\ell}\mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[\mathcal{X}_i\in\mathcal{Y}\right]=\ell^2/\left|\mathcal{S}\right|.$$

So it is left to prove Equation (19). We first show that the expected value of $\mathrm{AccGap}\,(i)$ is at least $(1-\alpha-\gamma)/2$.

$$\begin{aligned}
&\mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{AccGap}\,(|\mathcal{X}\cap\mathcal{Y}|)\right] \qquad (20)\\
&= \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[\Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}(v)=\mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\mid |x(v)\cap y(v)|=|\mathcal{X}\cap\mathcal{Y}|\right]\right]\\
&\quad - \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[\Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Dist}}}(v)=\mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\mid |x(v)\cap y(v)|=|\mathcal{X}\cap\mathcal{Y}|\right]\right]\\
&= \Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Com}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Com}}}(v)=\mathrm{out}^{\mathsf{A}_{\mathsf{Com}}}(v)\right]-\Pr_{v\xleftarrow{\mathrm{R}}\Lambda_{\mathsf{Dist}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{out}^{\mathsf{B}_{\mathsf{Dist}}}(v)=\mathrm{out}^{\mathsf{A}_{\mathsf{Dist}}}(v)\right]\\
&\geq (1-\alpha-\gamma)/2.
\end{aligned}$$

It follows that

$$\begin{aligned}
&\sum_{i=0}^{\lfloor 4t/(1-\alpha-\gamma)\rfloor}\Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[|\mathcal{X}\cap\mathcal{Y}|=i\right]\cdot\mathrm{AccGap}\,(i)\\
&= \mathop{\mathrm{E}}_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[\mathrm{AccGap}\,(|\mathcal{X}\cap\mathcal{Y}|)\right]\\
&\quad - \sum_{i=\lfloor 4t/(1-\alpha-\gamma)\rfloor+1}^{\ell}\Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[|\mathcal{X}\cap\mathcal{Y}|=i\right]\cdot\mathrm{AccGap}\,(i)\\
&\geq (1-\alpha-\gamma)/2-\sum_{i=\lfloor 4t/(1-\alpha-\gamma)\rfloor+1}^{\ell}\Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[|\mathcal{X}\cap\mathcal{Y}|=i\right]\cdot\mathrm{AccGap}\,(i) && \text{(Equation (20))}\\
&\geq (1-\alpha-\gamma)/2-\sum_{i=\lfloor 4t/(1-\alpha-\gamma)\rfloor+1}^{\ell}\Pr_{(\mathcal{X},\mathcal{Y})\xleftarrow{\mathrm{R}}(\mathrm{X},\mathrm{Y})}\left[|\mathcal{X}\cap\mathcal{Y}|=i\right] && (\mathrm{AccGap}\,(i)\leq 1)\\
&\geq (1-\alpha-\gamma)/2-\Pr_{\mathcal{X}\xleftarrow{\mathrm{R}}\mathrm{X},\mathcal{Y}\xleftarrow{\mathrm{R}}\mathrm{Y}}\left[|\mathcal{X}\cap\mathcal{Y}|\geq 4t/(1-\alpha-\gamma)\right]\\
&\geq (1-\alpha-\gamma)/4., && \text{(Markov inequality)}
\end{aligned}$$

and the the proof of the claim follows. □

Proof of Lemma 4.6. For $z\in\mathrm{Z}$, let $(\mathrm{T}'|_z)$ be distributed as the marginal distribution of $(\mathrm{T}|_{Z=z})$. From the triangle inequality for statistical distance, we get:

$$\begin{aligned}
&\mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left(\mathrm{A}_{\mathrm{T}},\mathrm{T},\mathrm{B}|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}},\mathrm{T})|_{z,a_{g(z)}}\times\mathrm{B}|_{z,a_{g(z)}}\right)\right)\right]\\
&\leq \mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}},\mathrm{T},\mathrm{B})|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}',\mathrm{B})|_{z,a_{g(z)}}\right)\right)\right]\\
&\quad + \mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}',\mathrm{B})|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}')|_{z,a_{g(z)}}\times\mathrm{B}|_{z,a_{g(z)}}\right)\right)\right]\\
&\quad + \mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}')|_{z,a_{g(z)}}\times\mathrm{B}|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}},\mathrm{T})|_{z,a_{g(z)}}\times\mathrm{B}|_{z,a_{g(z)}}\right)\right)\right].
\end{aligned}$$

We bound each term above separately: the first term is bounded by δ, because by Fact 2.13 and the data processing inequality, we have

$$\begin{aligned}
&\mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}},\mathrm{T},\mathrm{B})|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}',\mathrm{B})|_{z,a_{g(z)}}\right)\right)\right]\\
&=\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z}}\left[\mathrm{SD}\left((\mathrm{A}_{\mathrm{T}},\mathrm{A}_{g(z)},\mathrm{T},\mathrm{B})|_z\right),\left(\mathrm{A}_{\mathrm{T}'},\mathrm{A}_{g(z)},\mathrm{T}',\mathrm{B})|_z\right)\right)\right]\\
&\le\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z}}\left[\mathrm{SD}\left(((\mathrm{A},\mathrm{T},\mathrm{B})|_z\right),\left((\mathrm{A},\mathrm{T}',\mathrm{B})|_z\right)\right)\right]\\
&=\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z}}\left[\mathrm{SD}\left((\mathrm{A},\mathrm{B},\mathrm{T}|_z\right),\left(\mathrm{A},\mathrm{B}|_z\right)\times\left(\mathrm{T}|_z\right)\right)]=\delta.
\end{aligned}$$

Similarly, the third term is also bounded by δ, as by data processing,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}')|_{z,a_{g(z)}}\times\mathrm{B}|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}},\mathrm{T})|_{z,a_{g(z)}}\times\mathrm{B}|_{z,a_{g(z)}}\right)\right)\right]\\
&=\mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}')|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}},\mathrm{T})|_{z,a_{g(z)}}\right)\right)\right]\\
&=\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}'},\mathrm{A}_{g(z)},\mathrm{T}')|_z\right),\left((\mathrm{A}_{\mathrm{T}},\mathrm{A}_{g(z)},\mathrm{T})|_z\right)\right)\right]\le\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z}}\left[\mathrm{SD}\left((\mathrm{A},\mathrm{B},\mathrm{T}|_z\right),\left(\mathrm{A},\mathrm{B}|_z\right)\times\left(\mathrm{T}|_z\right)\right)]=\delta.
\end{aligned}$$

Finally, for the second term, we can write

$$\begin{aligned}
&\mathop{\mathrm{E}}_{z,a_{g(z)}\xleftarrow{\mathrm{R}}\mathrm{Z},\mathrm{A}_{g(z)}}\left[\mathrm{SD}\left(\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}',\mathrm{B})|_{z,a_{g(z)}}\right),\left((\mathrm{A}_{\mathrm{T}'},\mathrm{T}')|_{z,a_{g(z)}}\times\mathrm{B}|_{a_{g(z)},z}\right)\right)\right]\\
&=\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z},a_g(z)\xleftarrow{\mathrm{R}}\mathrm{A}_g(z)}\left[\mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}|_z}\left[\mathrm{SD}\left(\left(\mathrm{A}_t,\mathrm{B}|_{a_{g(z)},z}\right),\left(\mathrm{A}_t|_{a_{g(z)},z}\right)\times\left(\mathrm{B}|_{a_{g(z)},z}\right)\right)\right]\right] && \text{(Fact 2.13)}\\
&\le\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z},a_g(z)\xleftarrow{\mathrm{R}}\mathrm{A}_g(z)}\left[\mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}|_z}\left[2\sqrt{\mathrm{I}(\mathrm{A}_t;\mathrm{B}|z,a_g(z))}\right]\right] && \text{(Fact 2.8)}\\
&\le 2\sqrt{\mathop{\mathrm{E}}_{z\xleftarrow{\mathrm{R}}\mathrm{Z}}\left[\mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}T|_z}\left[\mathrm{I}(\mathrm{A}_t;\mathrm{B}|z,\mathrm{A}_{g(z)})\right]\right]} && \text{(Fact 2.16)}\\
&=2\sqrt{\epsilon}.
\end{aligned}$$

□

Proof of Claim 4.10. From Claim 4.7 and Corollary 2.20 we get that:

$$\begin{aligned}
&\mathop{\mathrm{E}}_{v_E\xleftarrow{\mathrm{R}}\Pi^{\mathrm{F}}_{\mathrm{Eve}}}\left[\mathrm{SD}\left((\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{Y}|_{v_E}\right),\left(\mathrm{X},\mathrm{F}(\mathrm{X})|_{v_E}\right)\times\left(\mathrm{Y}|_{v_E}\right)\right)\right]\\
&\le 2\mathop{\mathrm{E}}_{m_1,f(e_1),y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{F}(\mathcal{E}_1),\mathrm{Y}}\mathrm{SD}(\left(\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{m_1,f(e_1),y}\right),\\
&\qquad\qquad\left(\mathrm{X},\mathrm{F}(\mathrm{X})|_{m_1,f(e_1),y}\right)\times\left(\mathrm{M}_2|_{m_1,f(e_1),y}\right)\big)).
\end{aligned}$$

For every $b_E = (y, m_1, f(e_1 \cap y))$,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{f(e_1)\xleftarrow{\mathrm{R}}\mathrm{F}(e_1)|_{\mathrm{B}_E=b_E}} \mathrm{SD}\left(\left(\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{b_E,f(e_1)}\right),\left((\mathrm{X},\mathrm{F}(\mathrm{X})\times\mathrm{M}_2)|_{b_E,f(e_1)}\right)\right)\\
&\leq 2\mathrm{SD}\left((\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{F}(e_1),\mathrm{M}_2|_{b_E}),(\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{F}(e_1)|_{b_E}\times\mathrm{M}_2|_{b_E})\right) && \text{(Lemma 2.17)}\\
&= 2\mathop{\mathrm{E}}_{x,f(x)\xleftarrow{\mathrm{R}}\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{F}(e_1),\mathrm{M}_2|_{b_E,x,f(x)}\right),\left(\mathrm{F}(e_1)|_{b_E,x,f(x)}\times\mathrm{M}_2|_{b_E}\right)\right)\right] && \text{(Fact 2.13)}
\end{aligned}$$

Alice's message M_1 is only a function of $\mathrm{X},\mathrm{F}(\mathrm{X})$, and Eve's queries $\mathcal{E}_1$ are a function of M_1. Thus, since F is a random function, $\mathrm{F}(\mathcal{E}_1 \setminus \mathrm{Y})$ is independent from $\mathrm{F}(\mathrm{Y} \setminus \mathcal{E}_1)$ conditioned on $\mathrm{M}_1,\mathrm{Y},\mathrm{F}(\mathcal{E}_1\cap\mathrm{Y}),\mathrm{X},\mathrm{F}(\mathrm{X})$. Next, because M_2 is a function of M_1,Y and $\mathrm{F}(\mathrm{Y})$, we have that M_2 is independent from $\mathrm{F}(\mathcal{E}_1 \setminus \mathrm{Y})$ under the same conditioning.

We get that the distribution $(\mathrm{F}(e_1),\mathrm{M}_2|_{b_E,x,f(x))}$ is equal to

$$\mathrm{F}(e_1)|_{b_E,x,f(x)}\times\mathrm{M}_2|_{b_E,x,f(x)},$$

and therefore,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{x,f(x)\xleftarrow{\mathrm{R}}\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{F}(e_1),\mathrm{M}_2|_{b_E,x,f(x)}\right),\left(\mathrm{F}(e_1)|_{b_E,x,f(x)}\times\mathrm{M}_2|_{b_E}\right)\right)\right]\\
&= \mathop{\mathrm{E}}_{x,f(x)\xleftarrow{\mathrm{R}}\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{F}(e_1)|_{b_E,x,f(x)}\times\mathrm{M}_2|_{b_E,x,f(x)}\right),\left(\mathrm{F}(e_1)|_{b_E,x,f(x)}\times\mathrm{M}_2|_{b_E}\right)\right)\right]\\
&= \mathop{\mathrm{E}}_{x,f(x)\xleftarrow{\mathrm{R}}\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{M}_2|_{b_E,x,f(x)}\right),\left(\mathrm{M}_2|_{b_E}\right)\right)\right] && \text{(Fact 2.14)}\\
&= \mathrm{SD}\left((\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{b_E}),((\mathrm{X},\mathrm{F}(\mathrm{X})\times\mathrm{M}_2)|_{b_E})\right). && \text{(Fact 2.13)}
\end{aligned}$$

Now we can show all the dependence comes from the intersection. Since T_1 is a function of Y, X and $\mathcal{E}_1$, and $\mathcal{E}_1$ is a function of M_1, we get that

$$\begin{aligned}
&\mathrm{SD}\left((\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{b_E}),((\mathrm{X},\mathrm{F}(\mathrm{X})\times\mathrm{M}_2)|_{b_E})\right)\\
&= \mathrm{SD}\left((\mathrm{X},\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1}),\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{b_E}),(\mathrm{X},\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1}),\mathrm{F}(\mathrm{X})|_{b_E}\times\mathrm{M}_2|_{b_E})\right)\\
&= \mathop{\mathrm{E}}_{t,f(y_t)\xleftarrow{\mathrm{R}}\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{b_E,t,f(y_t)}\right),\left(\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E,t,f(y_t)}\times\mathrm{M}_2|_{b_E}\right)\right)\right] && \text{(Fact 2.13)}
\end{aligned}$$

Again, M_2 is a function of $\mathrm{Y},\mathrm{F}(\mathrm{Y})$ and M_1, and $\mathrm{X},\mathrm{F}(\mathrm{X})$ are independent from $\mathrm{F}(\mathrm{Y})$ conditioned on $\mathrm{M}_1,\mathrm{Y},\mathrm{F}(\mathcal{E}\cap\mathrm{Y}),\mathrm{T}_1,\mathrm{F}(\mathrm{Y}_{\mathrm{T}_1})$. Thus, the distribution $(\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{b_E,t,f(y_t))}$ is equal to

$$\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E,t,f(y_t)}\times\mathrm{M}_2|_{b_E,t,f(y_t)},$$

and we get:

$$\begin{aligned}
&\mathop{\mathrm{E}}_{t,f(y_t)\xleftarrow{\mathrm{R}}\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{X},\mathrm{F}(\mathrm{X}),\mathrm{M}_2|_{b_E,t,f(y_t)}\right),\left(\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E,t,f(y_t)}\times\mathrm{M}_2|_{b_E}\right)\right)\right]\\
&= \mathop{\mathrm{E}}_{t,f(y_t)\xleftarrow{\mathrm{R}}\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E,t,f(y_t)}\times\mathrm{M}_2|_{b_E,t,f(y_t)}\right),\left(\mathrm{X},\mathrm{F}(\mathrm{X})|_{b_E,t,f(y_t)}\times\mathrm{M}_2|_{b_E}\right)\right)\right]\\
&= \mathop{\mathrm{E}}_{t,f(y_t)\xleftarrow{\mathrm{R}}\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1})|_{b_E}}\left[\mathrm{SD}\left(\left(\mathrm{M}_2|_{b_E,t,f(y_t)}\right),\left(\mathrm{M}_2|_{b_E}\right)\right)\right] && \text{(Fact 2.14)}\\
&= \mathrm{SD}\left((\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1}),\mathrm{M}_2|_{b_E}),((\mathrm{T}_1,\mathrm{F}(y_{\mathrm{T}_1})\times\mathrm{M}_2)|_{b_E})\right). && \text{(Fact 2.13)}
\end{aligned}$$

To conclude the proof, we take the expectation over B_E, and the claim follows by the monotonicity of expectation. □

Proof of Claim 4.12.

$$
\begin{aligned}
&\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\ \mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}_1|_{m_1,y}}\left[\mathrm{I}(\mathrm{F}(y_t);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y))\right]\\
&=\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\ \mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}_1|_{m_1,y}}\left[\sum_{i\in t}\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{t,<i}))\right] && \text{(Chain rule)}\\
&=\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\ \mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}_1|_{m_1,y}}\left[\sum_{i\in t}\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{<i}))\right]\\
&\qquad+\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\ \mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}_1|_{m_1,y}}\left[\sum_{i\in t}\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{t,<i}))\right.\\
&\qquad\left.-\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{<i}))\right]\\
&\le\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\ \mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}_1|_{m_1,y}}\left[\sum_{i\in t}\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{<i}))\right]\\
&\qquad+\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\ \mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}_1|_{m_1,y}}\left[\sum_{i\in t}\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|m_1,y,\mathrm{F}(e_1\cap y))\right] && \text{(Lemma 2.9)}\\
&=\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\ \mathop{\mathrm{E}}_{t\xleftarrow{\mathrm{R}}\mathrm{T}_1|_{m_1,y}}\sum_{i\in t}\left[\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{<i}))\right.\\
&\qquad\left.+\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|m_1,y,\mathrm{F}(e_1\cap y))\right]\\
&=\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}}\sum_{i\in[\ell]}\Pr\left[i\in\mathrm{T}_1|m_1,y\right]\left[\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{<i}))\right.\\
&\qquad\left.+\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|m_1,y,\mathrm{F}(e_1\cap y))\right]
\end{aligned}
$$

Since we excluded the heavy queries $\mathcal{E}_1$ from T_1, and y_i is some fixed query, and since X is independent from Y conditioned on M_1 we have

$$\Pr\left[i\in\mathrm{T}_1|m_1,y\right]=\Pr\left[y_i\in(\mathrm{X}\setminus\mathcal{E}_1)|m_1,y\right]\le\Pr\left[y_i\in(\mathrm{X}\setminus\mathcal{E}_1)|m_1\right]\le\Pr\left[y_i\in((\mathrm{X}\cup\mathrm{Y})\setminus\mathcal{E}_1)|m_1\right]\le\delta.$$

Therefore,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}} \sum_{i\in[\ell]} \Pr\left[i\in \mathrm{T}_1|_{m_1,y}\right]\Big[\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{<i}))\\
&\qquad\qquad +\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|m_1,y,\mathrm{F}(e_1\cap y))\Big]\\
&\le \mathop{\mathrm{E}}_{m_1,y\xleftarrow{\mathrm{R}}\mathrm{M}_1,\mathrm{Y}} \sum_{i} \delta\Big[\mathrm{I}(\mathrm{F}(y_i);\mathrm{M}_2|m_1,y,\mathrm{F}(e_1\cap y),\mathrm{F}(y_{<i}))\\
&\qquad\qquad +\mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|m_1,y,\mathrm{F}(e_1\cap y))\Big]\\
&\le \delta \mathop{\mathrm{E}}_{y\xleftarrow{\mathrm{R}}\mathrm{Y}}\Big[\mathrm{I}(\mathrm{F}(y);\mathrm{M}_2|\mathrm{M}_1,y,\mathrm{F}(\mathcal{E}_1\cap y))\\
&\qquad\qquad +\sum_i \mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|\mathrm{M}_1,y,\mathrm{F}(\mathcal{E}_1\cap y))\Big] && \text{(Chain rule)}\\
&\le \delta \mathop{\mathrm{E}}_{y\xleftarrow{\mathrm{R}}\mathrm{Y}}\Big[|\mathrm{M}_2|+\sum_i \mathrm{I}(\mathrm{F}(y_i);\mathrm{F}(y_{<i})|\mathrm{M}_1,y,\mathrm{F}(\mathcal{E}_1\cap y))\Big] && \text{(Fact 2.5)}
\end{aligned}$$

□