From Private Simultaneous Messages to Zero-Information Arthur-Merlin Protocols and Back

Benny Applebaum(✉) and Pavel Raykov

School of Electrical Engineering, Tel-Aviv University, Tel Aviv, Israel
{bennyap,pavelraykov}@post.tau.ac.il

Abstract. Göös, Pitassi and Watson (ITCS, 2015) have recently introduced the notion of *Zero-Information Arthur-Merlin Protocols* (ZAM). In this model, which can be viewed as a private version of the standard Arthur-Merlin communication complexity game, Alice and Bob are holding a pair of inputs x and y respectively, and Merlin, the prover, attempts to convince them that some public function f evaluates to 1 on (x, y). In addition to standard completeness and soundness, Göös et al., require a "zero-knowledge" property which asserts that on each yes-input, the distribution of Merlin's proof leaks no information about the inputs (x, y) to an external observer.

In this paper, we relate this new notion to the well-studied model of *Private Simultaneous Messages* (PSM) that was originally suggested by Feige, Naor and Kilian (STOC, 1994). Roughly speaking, we show that the randomness complexity of ZAM corresponds to the communication complexity of PSM, and that the communication complexity of ZAM corresponds to the randomness complexity of PSM. This relation works in both directions where different variants of PSM are being used. Consequently, we derive better upper-bounds on the communication-complexity of ZAM for arbitrary functions. As a secondary contribution, we reveal new connections between different variants of PSM protocols which we believe to be of independent interest.

1 Introduction

In this paper we reveal an intimate connection between two seemingly unrelated models for non-interactive information-theoretic secure computation. We begin with some background.

Research supported by the European Union's Horizon 2020 Programme (ERC-StG-2014-2020) under grant agreement No. 639813 ERC-CLC, ISF grant 1155/11, GIF grant 1152/2011, and the Check Point Institute for Information Security. This work was done in part while the first author was visiting the Simons Institute for the Theory of Computing, supported by the Simons Foundation and by the DIMACS/Simons Collaboration in Cryptography through NSF grant CNS-1523467.

E. Kushilevitz and T. Malkin (Eds.): TCC 2016-A, Part II, LNCS 9563, pp. 65–82, 2016.
DOI: 10.1007/978-3-662-49099-0_3

1.1 Zero-Information Unambiguous Arthur-Merlin Communication Protocols

Consider a pair of computationally-unbounded (randomized) parties, Alice and Bob, each holding an n-bit input, x and y respectively, to some public function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. In our first model, a third party, Merlin, wishes to convince Alice and Bob that their joint input is mapped to 1 (i.e., (x, y) is in the language $f^{-1}(1)$). Merlin gets to see the parties' inputs (x, y) and their private randomness r_A and r_B, and is allowed to send a single message ("proof") p to both parties. Then, each party decides whether to accept the proof based on its input and its private randomness. We say that the protocol accepts p if both parties accept it. The protocol is required to satisfy natural properties of (perfect) completeness and soundness. Namely, if $(x, y) \in f^{-1}(1)$ then there is always a proof $p = p(x, y, r_A, r_B)$ that is accepted by both parties, whereas if $(x, y) \in f^{-1}(0)$ then, with probability $1 - \delta$ (over the coins of Alice and Bob), no such proof exists. As usual in communication-complexity games the goal is to minimize the communication complexity of the protocol, namely the length of the proof p.

This model, which is well studied in the communication complexity literature [BFS86,Kla03,Kla10], is viewed as the communication complexity analogue of AM protocols [BM88]. Recently, Göös et al. [GPW15] suggested a variant of this model which requires an additional "zero-knowledge" property defined as follows: For any 1-input $(x, y) \in f^{-1}(1)$, the proof sent by the honest prover provides no information on the inputs (x, y) to an external viewer. Formally, the random variable $p_{x,y} = p(x, y, r_A, r_B)$ induced by a random choice of r_A and r_B should be distributed according to some universal distribution D which is independent of the specific 1-input (x, y). Moreover, an additional *Unambiguity* property is required: any 1-input $(x, y) \in f^{-1}(1)$ and any pair of strings (r_A, r_B) uniquely determine a single accepting proof $p(x, y, r_A, r_B)$.

This modified version of AM protocols (denoted by ZAM) was originally presented in attempt to explain the lack of explicit nontrivial lower bounds for the communication required by AM protocols. Indeed, Göös et al., showed that any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ admits a ZAM protocol with at most exponential communication complexity of $O(2^n)$. Since the transcript of a ZAM protocol carries no information on the inputs, the mere existence of such protocols forms a "barrier" against "information complexity" based arguments. This suggests that, at least in their standard form, such arguments cannot be used to prove lower bounds against AM protocols (even with Unambiguous completeness).

Regardless of the original motivation, one may view the ZAM model as a simple and natural information-theoretic analogue of (non-interactive) zero-knowledge proofs where instead of restricting the computational power of the verifier, we split it between two non-communicating parties (just like AM communication games are derived from the computational-complexity notion of AM protocols). As cryptographers, it is therefore natural to ask:

> How does the ZAM model relate to other more standard models of information-theoretic secure computation?

As we will later see, answering this question also allows us to make some (modest) progress in understanding the communication complexity of ZAM protocols.

1.2 Private Simultaneous Message Protocols

Another, much older, notion of information-theoretically secure communication game was suggested by Feige et al. [FKN94]. As in the previous model, there are three (computationally-unbounded) parties: Alice, Bob and a Referee. Here too, an input (x, y) to a public function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is split between Alice and Bob, which, in addition, share a common random string c. Alice (resp., Bob) should send to the referee a single message a (resp., b) such that the transcript (a, b) reveals $f(x, y)$ but nothing else. That is, we require two properties: (Correctness) There exists a decoder algorithm Dec which recovers $f(x, y)$ from (a, b) with high probability; and (Privacy) There exists a simulator Sim which, given the value $f(x, y)$, samples the joint distribution of the transcript (a, b) up to some small deviation error. (See Sect. 4 for formal definitions.)

Following [IK97], we refer to such a protocol as a private simultaneous messages (PSM) protocol. A PSM protocol for f can be alternatively viewed as a special type of *randomized encoding* of f [IK00, AIK04], where the output of f is encoded by the output of a randomized function $F((x, y), c)$ such that F can be written as $F((x, y), c) = (F_1(x, c), F_2(y, c))$. This is referred to as a "2-decomposable" encoding in [Ish13].

1.3 ZAM vs. PSM

Our goal will be to relate ZAM protocols to PSM protocols. Since the latter object is well studied and strongly "connected" to other information-theoretic notions (cf. [BIKK14]), such a connection will allow us to place the new ZAM in our well-explored world of information-theoretic cryptography.

Observe that ZAM and PSM share some syntactic similarities (illustrated in Fig. 1). In both cases, the input is shared between Alice and Bob and the third party holds no input. Furthermore, in both cases the communication pattern consists of a single message. On the other side, in ZAM the third party (Merlin) attempts to convince Alice and Bob that the joint input is mapped to 1, and so the communication goes from Merlin to Alice/Bob who generate the output (accept/reject). In contrast, in a PSM protocol, the messages are sent in the other direction: from Alice and Bob to the third party (the Referee) who ends up with the output. In addition, the privacy guarantee looks somewhat different. For ZAM, privacy is defined with respect to an external observer and only over 1-inputs, whereas soundness is defined with respect to the parties (Alice and Bob) who hold the input (x, y). (Indeed, an external observer cannot even tell whether the joint input (x, y) is a 0-input.) Accordingly, in the ZAM model, correctness and privacy are essentially two different concerns that involve different parties. In contrast, for PSM protocols privacy should hold with respect to the view of the receiver who should still be able to decode.

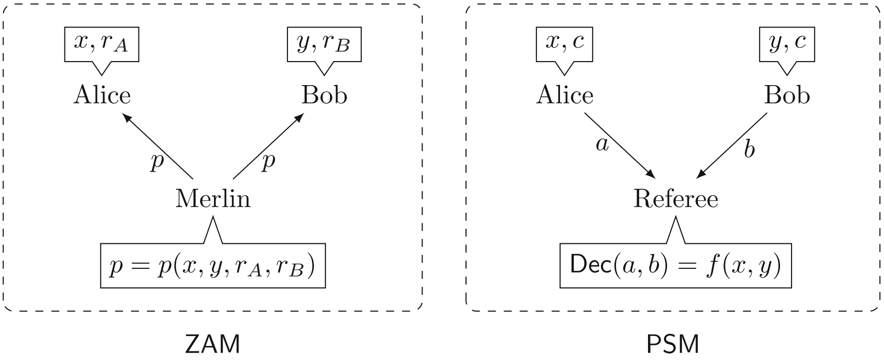

Fig. 1. Flow of messages

These differences seem to point to non-trivial gaps between these two notions. The picture becomes even more confusing when looking at existing constructions. On one hand, the general ZAM constructions presented by [GPW15, Theorem 6] (which use a reduction to Disjointness) seem more elementary than the simplest PSM protocols of [FKN94]. On the other hand, there are ZAM constructions which share common ingredients with existing PSM protocols. Concretely, the branching-program (BP) representation of the underlying function have been used both in the context of PSM [FKN94,IK97] and in the context of ZAM [GPW15, Theorem 1]. (It should be mentioned that there is a quadratic gap between the complexity of the two constructions.) Finally, both in ZAM and in PSM, it is known that any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ admits a protocol with exponential complexity, but the best known lower-bound is only linear in n. Overall, it is not clear whether these relations are coincidental or point to a deeper connection.[1]

2 Our Results

We prove that ZAM protocols and PSM protocols are intimately related. Roughly speaking, we will show that the *inverse* of ZAM is PSM and vice versa. Therefore, the randomness complexity of ZAM essentially corresponds to the communication complexity of PSM and the communication complexity of ZAM essentially corresponds to the randomness complexity of PSM. This relation works in both directions where different variants of PSM are being used. We proceed with a formal statement of our results. See Fig. 2 for an overview of our transformations.

[1] The authors of [GPW15] seem to suggest that there is no formal connection between the two models. Indeed, they explicitly mention PSM as "a different model of private two-party computation, [...] where the best upper and lower bounds are also exponential and linear."

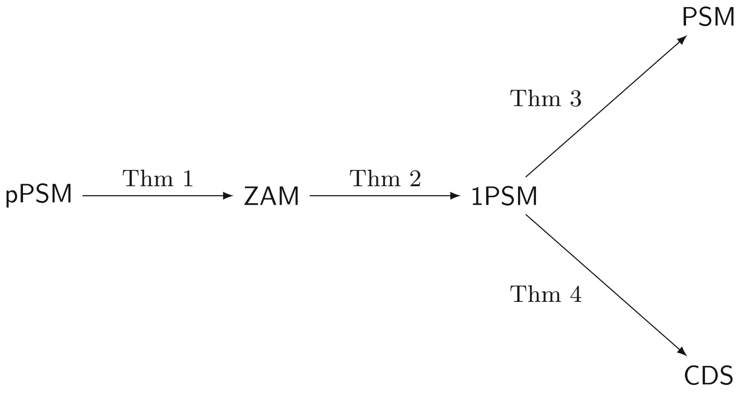

Fig. 2. Overview of the constructions

2.1 From Perfect PSM to ZAM

We begin by showing that a special form of *perfect* PSM protocols (referred to pPSM) yields ZAM protocols.

Theorem 1. *Let f be a function with a* pPSM*protocol that has communication complexity t and randomness complexity s. Then f has a $1/2$-sound* ZAM *scheme with randomness complexity of t and communication complexity of $s+1$.*

A pPSM protocol is a PSM in which both correctness and privacy are required to be errorless (perfect), and, in addition, the encoding should satisfy some regularity properties.[2]

To prove the theorem, we use the combinatorial properties of the perfect encoding to define a new function $g(x, y, p) = (g_1(x, p), g_2(y, p))$ which, when restricted to a 1-input (x, y), forms a bijection from the randomness space to the output space, and when (x, y) is a 0-input the restricted function $g(x, y, \cdot)$ covers only half of the range. Given such a function, it is not hard to design a ZAM: Alice (resp., Bob) samples a random point r_A in the range of g_1 (resp., r_B in the range of g_2), and accepts a proof $p = (p_1, p_2)$ if p_1 is a preimage of r_A under g_1 (resp. p_2 is a preimage of r_B under g_2). It is not hard to verify that the protocol satisfies Unambiguous completeness, 1/2-soundness and zero-information. (See Sect. 5.)

Although the notion of pPSM looks strong, we note that all known general PSM protocols are perfect. (See full version for details.) By plugging in the best known protocol from [BIKK14], we derive the following corollary.

[2] Essentially, the range of $F = (F_1, F_2)$ can be partitioned into two equal sets S_0 and S_1 and for every input (x, y) the function $F_{x,y}(c)$ that maps the randomness c to the transcript (a, b) forms a bijection from the randomness space to the set $S_{f(x)}$. In the context of randomized encoding, this notion was originally referred to as *perfect randomized encoding* [AIK04]. See Sect. 4 for formal definitions.

Corollary 1. *Every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a* ZAM *with communication complexity and randomness complexity of $O(2^{n/2})$.*

Previously, the best known upper-bound for the ZAM complexity of a general function f was $O(2^n)$ [GPW15]. Using known constructions of BP-based pPSM, we can also re-prove the fact that ZAM complexity is at most polynomial in the size of the BP that computes f. (Though, our polynomial is worse than the one achieved by [GPW15].)

2.2 From ZAM to One-Sided PSM

We move on to study the converse relation. Namely, whether ZAM can be used to derive PSM. For this, we consider a relexation of PSM in which privacy should hold only with respect to 1-inputs. In the randomized encoding literature, this notion is referred to as *semi-private randomized encoding* [AIK04,AIK15]. In the context of PSM protocols we refer to this variant as 1PSM.

Theorem 2. *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function with a δ-complete* ZAM *protocol that has communication complexity ℓ and randomness complexity m. Then, for all $k \in \mathbb{N}$, the following hold:*

1. *f has $(2^{2n}\delta^k)$-correct and 0-private* 1PSM *with communication complexity of km and $2km$ bits of shared randomness.*
2. *f has $(2^{2n}\delta^k + 2^{-\ell k})$-correct and $(2^{-\ell k})$-private* 1PSM *with communication complexity of km and $2\ell k$ bits of shared randomness.*

In particular, if the underlying ZAM protocol has a constant error (e.g., $\delta = 1/2$), we can get a 1PSM with an exponential small error of $\exp(-\Omega(n))$ at the expense of a linear overhead in the complexity, i.e., communication complexity and randomness complexity of $O(nm)$ and $O(\ell n)$, respectively.

Both parts of the theorem are proven by "inverting" the ZAM scheme. That is, as a common randomness Alice and Bob will take a proof p sampled according to the ZAM's accepting distribution. Since each proof forms a rectangle, Alice and Bob can locally sample a random point (r_A, r_B) from p's rectangle (Alice samples r_A and Bob samples r_B). The 1PSM's encoding functions output the sampled point (r_A, r_B). We show that if (x, y) is a 1-input then (r_A, r_B) is distributed uniformly, while in the case of the 0-input the sampled point belongs to some specific set Z that covers only a small fraction of the point space. Therefore, the 1PSM's decoder outputs 0 if the sampled point is in Z and 1, otherwise.

The difference between the two parts of Theorem 2 lies in the way that the common randomness is sampled. In the first part we sample p according to the exact ZAM's accepting distribution, whereas in the second part we compromise on imperfect sampling. This allows us to reduce the length of the shared randomness in 1PSM at the expense of introducing the sampling error in privacy and correctness. The proof of the theorem appears in Sect. 6.

2.3 From 1PSM to PSM and CDS

Theorem 2 shows that a ZAM protocol with low randomness complexity implies communication-efficient 1PSM protocol. However, the latter object is not well-studied and one may suspect that, for one-sided privacy, such low-communication 1PSM protocols may be easily achievable. The following theorem shows that this is unlikely by relating the worst-case communication complexity of 1PSM to the worst-case communication complexity of general PSM (here "worst case" ranges over all functions of given input length).

Theorem 3. *Assume that for all n, each function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$has a $\delta(n)$-correct $\varepsilon(n)$-private* 1PSM *protocol with communication complexity $t(n)$and randomness complexity $s(n)$.Then, each f has a $[\delta(n) + \delta(t(n))]$-correct $\max(\varepsilon(n), \delta(n) + \varepsilon(t(n)))$-private* PSM *protocol with communication complexity $t(t(n))$ and randomness complexity $s(n) + s(t(n))$. In particular, if every such f has a* 1PSM *with polynomial communication and randomness, and negligible privacy and correctness errors, then every f has a* PSM *with polynomial communication and randomness, and negligible privacy and correctness errors.*

The existence of a PSM for an arbitrary function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ with polynomial communication and randomness and negligible privacy and correctness errors is considered to be an important open question in information-theoretic cryptography, and so constructing 1PSM with such parameters would be considered to be a major breakthrough. Together with Theorem 2, we conclude that it will be highly non-trivial to discover randomness-efficient ZAM protocols for general functions.

Finally, we observe that 1PSM protocols yield (almost) directly protocols for *Conditional Disclosure of Secrets* (CDS) [GIKM00]. In this model, Alice holds an input x and Bob holds an input y, and, in addition, both parties hold a common secret bit s. The referee, Carol, holds both x and y, but it does not know the secret s. Similarly to the PSM case, Alice and Bob use shared randomness to compute the messages m_1 and m_2 that are sent to Carol. The CDS requires that Carol can recover s from (m_1, m_2) iff $f(x, y) = 1$. Moving to the complement $\overline{f} = 1 - f$ of f, one can view the CDS model as a variant of 1PSM, in which the privacy leakage in case of 0-inputs is full, i.e., given the messages sent by Alice and Bob, one can recover their input (x, y). Indeed, it is not hard to prove the following observation (whose proof is deferred to the full version).

Theorem 4. *Let f be a function with a δ-complete and ε-private* 1PSM *that has communication complexity t and randomness complexity s. Then, the function $\overline{f} = 1 - f$ has a δ-complete and ε-private* CDS *scheme with communication complexity t and randomness complexity s.*

In the full version we also describe a direct transformation from ZAM to CDS which does not suffer from the overhead introduced in Theorem 2. We note that CDS protocols have recently found applications in Attribute-Based Encryption (see [GKW15]).

3 Preliminaries

For an integer $n \in \mathbb{N}$, let $[n] = \{1, \ldots, n\}$. The complement of a bit b is denoted by $\bar{b} = 1 - b$. For a set S, we let S^k be the set of all possible k-tuples with entries in S, and for a distribution D, we let D^k be the probability distribution over k-tuples such that each tuple's element is drawn according to D. We let $s \leftarrow_R S$ denote an element that is sampled uniformly at random from the finite set S. The uniform distribution over n-bit strings is denoted by U_n. For a boolean function $f : S \to \{0, 1\}$, we say that $x \in S$ is 0-input if $f(x) = 0$, and is 1-input if $f(x) = 1$. A subset R of a product set $A \times B$ is a *rectangle* if $R = A' \times B'$ for some $A' \subseteq X$ and $B' \subseteq Y$.

The statistical distance between two random variables, X and Y, denoted by $\Delta(X; Y)$ is defined by $\Delta(X; Y) := \frac{1}{2} \sum_z |\Pr[X = z] - \Pr[Y = z]|$. We will also use statistical distance for probability distributions, where for a probability distribution D the value $\Pr[D = z]$ is defined to be $D(z)$.

We write $\Delta_{x_1 \leftarrow D_1, \ldots, x_k \leftarrow D_k}(F(x_1, \ldots, x_k); G(x_1, \ldots, x_k))$ to denote the statistical distance between two distributions obtained as a result of sampling x_i's from D_i's and applying the functions F and G to $(x_1, \ldots, x_k)$, respectively. We use the following facts about the statistical distance. For every distributions X and Y and a function F (possibly randomized), we have that $\Delta(F(X), F(Y)) \le \Delta(X, Y)$. In particular, for a boolean function F this implies that $\Pr[F(X) = 1] \le \Pr[F(Y) = 1] + \Delta(X; Y)$.

For a sequence of probability distributions $(D_1, \ldots, D_k)$ and a probability vector $W = (w_1, \ldots, w_k)$ we let $Z = \sum w_i D_i$ denote the "mixture distribution" obtained by sampling an index $i \in [k]$ according to W and then outputting an element $z \leftarrow D_i$.

Lemma 1. *For any distribution $Z = \sum w_i D_i$ and probability distribution S, it holds that*

$$\Delta(S; M) \le \sum_{i=1}^{k} w_i \, \Delta(S; D_i).$$

Proof. By the definition of statistical distance we can write $\Delta(S; Z)$ as

$$\begin{aligned}
\frac{1}{2} \sum_z \left| S(z) - \sum_{i=1}^{k} w_i D_i(z) \right| &= \frac{1}{2} \sum_z \left| \sum_{i=1}^{k} w_i (S(z) - D_i(z)) \right| \\
&\le \frac{1}{2} \sum_z \sum_{i=1}^{k} w_i \, |S(z) - D_i(z)| \\
&= \frac{1}{2} \sum_{i=1}^{k} w_i \sum_z |S(z) - D_i(z)| \\
&= \sum_{i=1}^{k} w_i \, \Delta(S; D_i).
\end{aligned}$$

□

4 Definitions

4.1 PSM-Based Models

Definition 1 (PSM, 1PSM, pPSM). *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a boolean function. We say that a pair of (possibly randomized[3]) encoding algorithms $F_1, F_2 : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^t$ are* PSM *for f if they satisfy the following properties:*

δ-Correctness: *There exists a deterministic algorithm* Dec*, called decoder, such that for every input (x, y) we have that*

$$\Pr_{c \leftarrow_R \{0,1\}^s}[\mathsf{Dec}(F_1(x,c), F_2(y,c)) \neq f(x,y)] \leq \delta.$$

ε-Privacy: *There exists a randomized algorithm (simulator)* Sim *such that for any input (x, y) it holds that*

$$\Delta_{c \leftarrow_R \{0,1\}^s}(\mathsf{Sim}(f(x,y)); (F_1(x,c), F_2(y,c))) \leq \varepsilon,$$

where we write $\Delta_{x_1 \leftarrow D_1, \dots, x_k \leftarrow D_k}(F(x_1, \dots, x_k); G(x_1, \dots, x_k))$ to denote the statistical distance between two distributions obtained as a result of sampling x_i's from D_i's and applying the functions F and G to $(x_1, \dots, x_k)$, respectively.

If privacy holds only on 1-inputs then the protocol is referred to as 1PSM*. A* pPSM *protocol is a* PSM *which satisfies 0-correctness, (standard) 0-privacy, and, in addition, satisfies the following properties:*

Balance: *There exists a 0-private (perfectly private) simulator* Sim *such that* $\mathsf{Sim}(U_1) \equiv U_{2t}$.

Stretch-Preservation: *We have that $1 + s = 2t$, i.e., the total output length equals to the randomness complexity plus a single bit.*[4]

The communication complexity of the PSM *(resp.,* 1PSM*,* pPSM*) protocol is defined as the encoding length t, and the randomness complexity of the protocol is defined as the length s of the common randomness.*

Remark 1 (pPSM– *combinatorial view).* One can also formulate the pPSM definition combinatorially [AIK04]: For f's b-input (x, y), let $F_{xy}(c)$ denote the joint output of the encoding $(F_1(x,c), F_2(y,c))$. Let $S_b := \{F_{xy}(c) \mid c \in \{0,1\}^s, (x,y) \in f^{-1}(b)\}$ and let $R = \{0,1\}^t \times \{0,1\}^t$ denote the joint range of (F_1, F_2). Then, (F_1, F_2) is a pPSM of f if and only if (1) The 0-image S_0 and the 1-image S_1 are disjoint; (2) The union of S_0 and S_1 equals to the range R; and (3) for

[3] In the original paper [FKN94], the functions F_1, F_2 are deterministic. We extend this model by allowing Alice and Bob to use local randomness that is assumed to be available freely.

[4] Intuitively, this bit carries the outcome of the function.

all (x, y) the function F_{xy} is a bijection on $S_{f(x,y)}$. One can also consider a case when F_1 and F_2 have arbitrary ranges, i.e., $F_i : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^{t_i}$. In this case we say that (F_1, F_2) is a pPSM of f if the above conditions hold with respect to the joint range $R = \{0,1\}^{t_1} \times \{0,1\}^{t_2}$.

4.2 ZAM

Definition 2 (ZAM). *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. We say that a pair of deterministic boolean functions $A, B : \{0,1\}^n \times \{0,1\}^m \times \{0,1\}^\ell \to \{0,1\}$ is a* ZAM *for f if it satisfies the following properties:*

Unambiguous Completeness: *For any 1-input (x, y) and any randomness $(r_A, r_B) \in \{0,1\}^m \times \{0,1\}^m$ there exists a unique $p \in \{0,1\}^\ell$ such that $A(x, r_A, p) = 1 = B(y, r_B, p)$.*

Zero Information: *There exists a distribution D on the proof space $\{0,1\}^\ell$ such that for any 1-input (x, y) we have that*

$$\forall p \in \{0,1\}^\ell \; D(p) = \Pr_{r_A, r_B \leftarrow_R \{0,1\}^m}[A(x, r_A, p) = 1 = B(y, r_B, p)].$$

The distribution D is called the accepting distribution.

δ-Soundness: *For any 0-input (x, y) it holds that*

$$\Pr_{r_A, r_B \leftarrow_R \{0,1\}^m}[\exists p \in \{0,1\}^\ell : A(x, r_A, p) = 1 = B(y, r_B, p)] \leq \delta.$$

The communication complexity (resp., randomness complexity) of the ZAM *protocol is defined as the length ℓ of the proof (resp., the length m of the local randomness).*

The Zero Information property asserts that for every accepting input (x, y) the distribution $D_{x,y}$, obtained by sampling r_A and r_B and outputting the (unique) proof p which is accepted by Alice and Bob, is identical to a single universal distribution D.

Following [GPW15], we sometimes refer to the proofs as "rectangles" because for each (x, y) a proof p naturally corresponds to a set of points $\{(r_A, r_B) : A(x, r_A, p) = 1 = B(y, r_B, p)\}$ which forms a rectangle in $\{0,1\}^m \times \{0,1\}^m$.

5 From pPSM to ZAM

In this section we construct a ZAM scheme from a pPSM protocol. By exploiting the combinatorial structure of pPSM, for each input (x, y) we construct a function h_{xy} that is a bijection if (x, y) is a 1-input and is two-to-one if (x, y) is a 0-input. In the constructed ZAM scheme Alice and Bob use their local randomness to sample a uniform point in h's range (Alice samples its x-coordinate r_A and Bob samples its y-coordinate r_B). Merlin's proof is the preimage p for the sampled point, i.e., a point p such that $h_{xy}(p) = (r_A, r_B)$. In order to accept the proof p, Alice and Bob verify that it is a preimage for the sampled point (r_A, r_B).

First, the constructed ZAM is unambiguously complete because h_{xy} is a bijection if (x, y) is a 1-input of f. Second, the constructed ZAM satisfies the zero-information property because the distribution of the accepted proofs is uniform. Third, the constructed ZAM is sound, because if (x, y) is a 0-input, then h_{xy} is two-to-one, implying that with probability at least 1/2 no preimage can be found.

Theorem 1. *Let f be a function with a* pPSM *protocol that has communication complexity t and randomness complexity s. Then f has a 1/2-sound* ZAM *scheme with randomness complexity of t and communication complexity of $s + 1$.*

Proof. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function with a pPSM $F_1, F_2 : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^t$. We show that there exists a 1/2-sound ZAM protocol for f with Alice's and Bob's local randomness spaces $\{0,1\}^m$ and proof space $\{0,1\}^\ell$, where $m = t$ and $\ell = 2t$.

First, we prove some auxiliary statement about pPSM. Let $g(x, y, c) := (F_1(x, c), F_2(y, c))$. For any (x, y), we define a new function $h_{xy} : \{0,1\}^s \times \{0,1\} \to \{0,1\}^t \times \{0,1\}^t$ as follows.

$$h_{xy}(c, b) := \begin{cases} g(x, y, c), \text{if}\, b = 0; \\ g(x_0, y_0, c), \text{if}\, b = 1\, (\text{where}\, (x_0, y_0)\, \text{is a canonical}\, 0 - \text{input for} f). \end{cases}$$

The function h satisfies the following useful properties as follows from the combinatorial view of pPSM (Remark 1).

Fact 1. *If (x, y) is a 1-input for f, then the function h_{xy} is a bijection. Otherwise, if (x, y) is a 0-input for f, then the image of the function h_{xy} covers exactly half of the range $\{0,1\}^t \times \{0,1\}^t$.*

We now describe a ZAM protocol for f in which the local randomness of Alice and Bob is sampled from $\{0,1\}^t$, and the proof space is $\{0,1\}^s \times \{0,1\}$. Recall that (F_1, F_2) is a pPSM and therefore $s + 1 = 2t$ and $\{0,1\}^s \times \{0,1\} = \{0,1\}^{2t}$. The ZAM's accepting functions A, B are defined as follows:

$$A(x, m_1, (c, b)) = \begin{cases} 1, \text{if}\, (m_1 = F_1(x, c)\, \text{and}\, b = 0)\, \text{or} \\ \quad (m_1 = F_1(x_0, c)\, \text{and}\, b = 1); \\ 0, \text{otherwise}. \end{cases}$$

$$B(y, m_2, (c, b)) = \begin{cases} 1, \text{if}\, (m_2 = F_2(y, c)\, \text{and}\, b = 0)\, \text{or} \\ \quad (m_2 = F_2(y_0, c)\, \text{and}\, b = 1); \\ 0, \text{otherwise}. \end{cases}$$

Observe that the following equivalence holds.

Claim. $\forall x, y, c, b, m_1, m_2 \ \Big[h_{xy}(c, b) = (m_1, m_2)\Big] \Leftrightarrow \Big[A(x, m_1, (c, b)) = 1 = B(y, m_2, (c, b))\Big]$.

Now we verify that A, B is ZAM for f:

Unambiguous Completeness: Consider any f's 1-input (x, y) and take any $(m_1, m_2) \in \{0,1\}^t \times \{0,1\}^t$. Since (x, y) is a 1-input for f, we have that h_{xy} is a bijection. This means that there exists a unique (c, b) such that $h_{xy}(c, b) = (m_1, m_2)$. By Claim 5, this proof (c, b) is the only proof which is accepted by both Alice and Bob when the randomness is set to m_1, m_2.

Zero Information: We show that the accepting distribution is uniform, i.e., for any 1-input (x, y) and for any $p \in \{0,1\}^s \times \{0,1\}$ it holds that

$$\Pr_{r_A, r_B \leftarrow_R \{0,1\}^t}[A(x, r_A, p) = 1 = B(y, r_B, p)] = 2^{-2t}.$$

Take any 1-input (x, y). Since (x, y) is a 1-input for f, we have that h_{xy} is a bijection. Hence, there exists a unique $(m_1^*, m_2^*) \in \{0,1\}^n \times \{0,1\}^n$ such that $h_{xy}(c, b) = (m_1^*, m_2^*)$. By Claim 5, this means that Alice and Bob accept only this (m_1^*, m_2^*). Hence, for all proofs p we have that

$$\Pr_{r_A, r_B \leftarrow_R \{0,1\}^t}[A(x, r_A, p) = 1 = B(y, r_B, p)] =$$
$$\Pr_{r_A, r_B \leftarrow_R \{0,1\}^t}[r_A = m_1^*, r_B = m_2^*] = 2^{-2t}.$$

1/2-Soundness: Fix some 0-input (x, y), and recall that the image H of h_{xy} covers exactly half of the range $\{0,1\}^t \times \{0,1\}^t$, i.e., $|H| = \left|\{0,1\}^t \times \{0,1\}^t\right|/2$. It follows that, with probability 1/2, the randomness of Alice and Bob (m_1, m_2) chosen randomly from $\{0,1\}^t \times \{0,1\}^t$ lands outside H. In this case, the set $h_{xy}^{-1}(m_1, m_2)$ is empty and so there is no proof (c, b) that will be accepted.

□

6 From ZAM to 1PSM

In this section we construct 1PSM protocols from a ZAM scheme and prove Theorem 2 (restated here for convenience).

Theorem 2. *Let $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ be a function with a δ-complete* ZAM *protocol that has communication complexity ℓ and randomness complexity m. Then, for all $k \in \mathbb{N}$, the following hold:*

1. *f has $(2^{2n}\delta^k)$-correct and 0-private* 1PSM *with communication complexity of km and $2km$ bits of shared randomness.*
2. *f has $(2^{2n}\delta^k + 2^{-\ell k})$-correct and $(2^{-\ell k})$-private* 1PSM *with communication complexity of km and $2\ell k$ bits of shared randomness.*

Proof. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function with a δ-sound ZAM protocol (A, B) with Alice's and Bob's local randomness spaces $\{0,1\}^m$ and the proof space $\{0,1\}^\ell$. Fix some integer k. We start by constructing the first $\mathsf{1PSM}$ protocol.

We first define some additional notation and prove auxiliary claims. For a pair of inputs (x, y) let

$$E_{xy} := \{(r_A, r_B) \in \{0,1\}^m \times \{0,1\}^m \mid \exists p : A(x, r_A, p) = 1 = B(y, r_B, p)\}$$

and $Z := \bigcup_{(x,y)\in f^{-1}(0)} E^k_{xy}$.

Claim. $|Z| \leq 2^{2n}(\delta 2^{2m})^k$.

Proof. By the soundness property of ZAM, we have that $|E_{xy}| \leq \delta 2^{2m}$ for any 0-input (x, y). Hence, each $|E^k_{xy}| \leq (\delta 2^{2m})^k$. We conclude that

$$|Z| = \left| \bigcup_{(x,y)\in f^{-1}(0)} E^k_{xy} \right| \leq \sum_{(x,y)\in f^{-1}(0)} |E^k_{xy}| \leq 2^{2n}(\delta 2^{2m})^k = \delta^k 2^{2n+2mk}.$$

□

Let $\mathcal{A}^x_p := \{r_A \in \{0,1\}^m \mid A(x, r_A, p) = 1\}$ and $\mathcal{B}^y_p := \{r_B \in \{0,1\}^m \mid B(y, r_B, p) = 1\}$.

Claim. Let D_{ACC} be the accepting distribution of ZAM. Then, for any 1-input (x, y) and $p \in \{0,1\}^\ell$ we have that $D_{\text{ACC}}(p) = 2^{-2m}|\mathcal{A}^x_p||\mathcal{B}^y_p|$.

Proof. By definition

$$D_{\text{ACC}}(p) = \frac{|\{(r_A, r_B) \in \{0,1\}^m \times \{0,1\}^m \mid A(x, r_A, p) = 1 = B(y, r_B, p)\}|}{|\{0,1\}^m| \cdot |\{0,1\}^m|}.$$

In order to derive the claim, it remains to notice that since every proof forms a "rectangle" [GPW15], we have that

$$\{(r_A, r_B) \in \{0,1\}^m \times \{0,1\}^m \mid A(x, r_A, p) = 1 = B(y, r_B, p)\} = \mathcal{A}^x_p \times \mathcal{B}^y_p.$$

□

We can now describe the encoding algorithms G_1 and G_2 and the decoder Dec. First, G_1 and G_2 use the shared randomness to sample a proof p according to the accepting distribution. Then G_1 and G_2 sample (private) randomness that can lead to the acceptance of p on their input (x, y), i.e., G_1 computes $a \leftarrow_R \mathcal{A}^x_p$ and G_2 computes $b \leftarrow_R \mathcal{B}^y_p$. We have that if $f(x, y) = 1$ then (a, b) is distributed uniformly, while if $f(x, y) = 0$ then (a, b) is sampled from the set Z. The task of the decoder is to verify whether it is likely that a point has been sampled from Z or uniformly. This is achieved by repeating the protocol k times. Below is the formal description of the algorithms G_1, G_2 and decoder.

- **Shared Randomness.** The common randomness $c \in \{0,1\}^{k \cdot 2m}$ is used for sampling k independent samples $(p_1, \dots, p_k)$ from D_{ACC}. (Each such sample can be obtained by sampling $r = (r_A, r_B) \leftarrow_R \{0,1\}^{2m}$ and outputting the unique proof p that corresponds to r and to some fixed 1-input (x_0, y_0).)
- **Encoders.** The encoder $G_1(x, c)$ outputs $(a_1, \dots, a_k) \leftarrow_R \mathcal{A}^x_{p_1} \times \cdots \times \mathcal{A}^x_{p_k}$ and the encoder G_2 outputs $(b_1, \dots, b_k) \leftarrow_R \mathcal{B}^y_{p_1} \times \cdots \times \mathcal{B}^x_{p_k}$.
- **Decoder.** $\mathsf{Dec}((a_1, \dots, a_k), (b_1, \dots, b_k))$
  If $((a_1, b_1), ..., (a_k, b_k)) \in Z$ then output 0, otherwise output 1.

Let us verify that the proposed protocol is a 1PSM for f.

$(2^{2n}\delta^k)$-Correctness. Since that the decoder never errs on 0-inputs, it suffices to analyze the probability that some 1-input (x, y) is incorrectly decoded to 0. Fix some 1-input (x, y). Below we will show that the message $\boldsymbol{s} = ((a_1, b_1), \dots, (a_k, b_k))$ generated by the encoders G_1 and G_2 is uniformly distributed over the set $(\{0,1\}^m \times \{0,1\}^m)^k$. Hence, the probability that $\boldsymbol{s}$ lands in Z (and decoded incorrectly to 0) is exactly $\frac{|Z|}{|(\{0,1\}^m \times \{0,1\}^m)^k|}$, which, by Claim 6, is upper-bounded by $2^{2n}\delta^k$.

It is left to show that $\boldsymbol{s}$ is uniformly distributed. To see this, consider the marginalization of (a_i, b_i)'s probability distribution: For a fixed (r_A, r_B) we have that

$$\Pr[(a_i, b_i) = (r_A, r_B)] = \sum_{p \in \{0,1\}^\ell} \Pr[(a_i, b_i) = (r_A, r_B) \mid p_i = p] \Pr[p_i = p].$$

Because of the unambiguous completeness property of ZAM, we have that there exists a single p^* such that $(r_A, r_B) \in \mathcal{A}^x_{p^*} \times \mathcal{B}^y_{p^*}$. Hence, all probabilities $\Pr[(a_i, b_i) = (r_A, r_B) \mid p_i = p]$ are zero, if $p \neq p^*$. This implies that

$$\Pr[(a_i, b_i) = (r_A, r_B)] = \Pr[(a_i, b_i) = (r_A, r_B) \mid p_i = p^*] \Pr[p_i = p^*].$$

We have that $\Pr[p_i = p] = D_{\text{ACC}}(p) = 2^{-2m}|\mathcal{A}^x_p||\mathcal{B}^y_p|$ (due to Claim 6), and $\Pr[(a_i, b_i) = (r_A, r_B) \mid p_i = p^*]$ is $\frac{1}{|\mathcal{A}^x_p| \cdot |\mathcal{B}^y_p|}$ by the construction of the encoding functions. Hence, $\Pr[(a_i, b_i) = (r_A, r_B)] = 2^{-2m}$. Because all pairs (a_i, b_i) are sampled independently, we get that the combined tuple $\boldsymbol{s} = ((a_1, b_1), \dots, (a_k, b_k))$ is sampled uniformly from $(\{0,1\}^m \times \{0,1\}^m)^k$, as required.

Privacy for 1-inputs. As shown above, if (x, y) is a 1-input, then $\boldsymbol{s}$ is uniformly distributed over $(\{0,1\}^m \times \{0,1\}^m)^k$. Hence, the simulator for proving the privacy property of PSM can be defined as a uniform sampler from $(\{0,1\}^m \times \{0,1\}^m)^k$.

The Second Protocol. The second item of the theorem is proved by using the first protocol, except that the point $\boldsymbol{p} = (p_1, \ldots, p_k)$ is sampled from a different distribution D'. For a parameter t, the distribution D' is simply the distribution D^k_{ACC} discretized into $2^{-(\ell k+t)}$-size intervals. Such D' can be sampled using only $\ell k + t$ random bits. Moreover, for each point $\boldsymbol{p}$, the difference between $D^k_{\text{ACC}}(\boldsymbol{p})$ and $D'(\boldsymbol{p})$ is at most $2^{-(\ell k+t)}$. Since the support of D^k_{ACC} is of size at most $2^{\ell k}$, it follows that $\Delta(S(U_{\ell k+t}); D^k_{\text{ACC}}) \le 2^{-(\ell k+t)} \cdot 2^{\ell k} = 2^{-t}$. As a result, we introduce an additional error of 2^{-t} in both privacy and correctness. By setting t to ℓk, we derive the second 1PSM protocol. □

7 From 1PSM to PSM

In this section we show how to upgrade a 1PSM protocol into a PSM protocol. We assume that we have a way of constructing 1PSM for all functions. Our main idea is to reduce a construction of a PSM scheme for f to two 1PSM schemes. The first 1PSM scheme computes the function f, and the second 1PSM scheme computes the function $\overline{\mathsf{Dec}_f}$, i.e., the complement of the decoder Dec_f of the first scheme. We show how to combine the two schemes such that the first scheme protects the privacy of 1-inputs and the second scheme protects the privacy of 0-inputs.

Theorem 3. *Assume that for all n, each function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a $\delta(n)$-correct $\varepsilon(n)$-private* 1PSM *protocol with communication complexity $t(n)$ and randomness complexity $s(n)$. Then, each f has a $[\delta(n)+\delta(t(n))]$-correct $\max(\varepsilon(n), \delta(n) + \varepsilon(t(n))$-private* PSM *protocol with communication complexity $t(t(n))$ and randomness complexity $s(n) + s(t(n))$. In particular, if every such f has a* 1PSM *with polynomial communication and randomness, and negligible privacy and correctness errors, then every f has a* PSM *with polynomial communication and randomness, and negligible privacy and correctness errors.*

Proof. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Let $F_1, F_2 : \{0,1\}^n \times \{0,1\}^{s(n)} \to \{0,1\}^{t(n)}$ be a $\delta(n)$-correct and $\varepsilon(n)$-private on 1 inputs 1PSM for f with decoder Dec_f and simulator Sim_f. Define a function $g : \{0,1\}^{t(n)} \times \{0,1\}^{t(n)} \to \{0,1\}$ to be $1 - \mathsf{Dec}_f(m_1, m_2)$. Let $G_1, G_2 : \{0,1\}^{t(n)} \times \{0,1\}^{s(t(n))} \to \{0,1\}^{t(t(n))}$ be a $\delta(t(n))$-correct and $\varepsilon(t(n))$-private on 1 inputs 1PSM for g with decoder Dec_g and simulator Sim_g.

We construct a (standard) PSM for f as follows. Let $\{0,1\}^u = \{0,1\}^{s(n)} \times \{0,1\}^{s(t(n))}$ be the space of shared randomness, let $\{0,1\}^v = \{0,1\}^{t(t(n))}$ be the output space and define the encoding functions $H_1, H_2 : \{0,1\}^n \times \{0,1\}^u \to \{0,1\}^v$, by

$$H_1(x, (c, r)) = G_1(F_1(x, c), r) \quad \text{and} \quad H_2(y, (c, r)) = G_2(F_2(y, c), r).$$

We show that H_1, H_2 satisfy the security properties of PSM:

$\delta(n)+\delta(t(n))$-Correctness: On an input (e_1, e_2) define the decoding algorithm Dec to output $1-\mathsf{Dec}_g(e_1, e_2)$. The decoding algorithm Dec works correctly whenever both Dec_g and Dec_f succeed. Hence, the error probability for decoding can be bounded as follows:

$$\begin{aligned}
&\Pr_{(c,r)\leftarrow_R\{0,1\}^u}[\mathsf{Dec}(H_1(x,(c,r)),H_2(y,(c,r)))\neq f(x,y)]\\
&\quad= \Pr_{(c,r)\leftarrow_R\{0,1\}^u}[1-\mathsf{Dec}_g(G_1(F_1(x,c),r)),G_2(F_2(y,c),r)))\neq f(x,y)]\\
&\quad\leq \Pr_{c\leftarrow_R\{0,1\}^{s(n)}}[1-(1-(\mathsf{Dec}_f(F_1(x,c),F_2(y,c))))\neq f(x,y)]+\delta(t(n))\\
&\quad= \Pr_{c\leftarrow_R\{0,1\}^{s(n)}}[\mathsf{Dec}_f(F_1(x,c),F_2(y,c))\neq f(x,y)]+\delta(t(n))\\
&\quad\leq \delta(n)+\delta(t(n)).
\end{aligned}$$

ε-Privacy: We define the simulator Sim as follows: on 0-inputs it outputs Sim_g and on 1-inputs it computes $\mathsf{Sim}_f=(m_1,m_2)$, randomly samples r from $\{0,1\}^{s(t(n))}$, and outputs $(G_1(m_1,r),G_2(m_2,r))$. We verify that the simulator truthfully simulates the randomized encoding (H_1,H_2) with deviation error of at most ε.

We begin with the case where (x,y) is a 0-input for f. For any c, let L_c denote the distribution of the random variable $(G_1(F_1(x,c),r),G_2(F_2(y,c),r))$ where $r\leftarrow_R\{0,1\}^{s(t(n))}$. Let M denote the "mixture distribution" which is defined by first sampling $c\leftarrow_R\{0,1\}^{s(n)}$ and then outputting a random sample from L_c, that is, the distribution $M=\sum_{c\in\{0,1\}^{s(n)}}\Pr[U_{s(n)}=c]L_c$. Due to Lemma 1, we have that

$$\Delta(\mathsf{Sim}_g;M)\leq\sum_{c\in\{0,1\}^{s(n)}}\Pr[U_{s(n)}=c]\,\Delta(\mathsf{Sim}_g;L_c).$$

Let C denote a subset of $c\in\{0,1\}^{s(n)}$ such that $(F_1(x,c),F_2(y,c))$ is a 1-input for g. The set C satisfies the following two properties: (1) $\forall c\in C\,\Delta(\mathsf{Sim}_g;L_c)\leq\varepsilon(t(n))$ and (2) $|C|/2^{s(n)}\geq 1-\delta(n)$. The property (1) holds because G_1,G_2 is private on 1-inputs of g. The property (2) holds because Dec_f decodes correctly with the probability at least $1-\delta(n)$. After splitting the mixture sum in two, we have that

$$\begin{aligned}
\sum_{c\in\{0,1\}^{s(n)}}\Pr[U_{s(n)}=c]\,\Delta(\mathsf{Sim}_g;L_c) &=\sum_{c\in C}2^{-s(n)}\,\Delta(\mathsf{Sim}_g;L_c)\\
&\quad+\sum_{c\notin C}2^{-s(n)}\,\Delta(\mathsf{Sim}_g;L_c).
\end{aligned}$$

Because of the properties of C, we have that the first sum is upperbounded by $\varepsilon(t(n))$ and the second one is upperbounded by $\delta(n)$. This implies that $\Delta(\mathsf{Sim}_g;M)\leq\delta(n)+\varepsilon(t(n))$.

We move on to the case where (x, y) is a 1-input. Then

$$\underset{c \leftarrow_R \{0,1\}^{s(n)}}{\Delta} (\mathsf{Sim}_f \ ; \ (F_1(x, c), F_2(y, c))) \leq \varepsilon(n).$$

Consider the randomized procedure G which, given (m_1, m_2), samples $r \leftarrow_R \{0,1\}^{s(t(n))}$ and outputs the pair $(G_1(m_1, r), G_2(m_2, r))$. Applying G to the above distributions we get:

$$\underset{(c,r) \leftarrow_R \{0,1\}^u}{\Delta} (G(\mathsf{Sim}_f ; r); \ G(F_1(x, c), F_2(y, c); r)) \leq \varepsilon(n). \tag{1}$$

Recall that, for a random $r \leftarrow_R \{0,1\}^{s(t(n))}$, it holds that $G(\mathsf{Sim}_f ; r) \equiv \mathsf{Sim}(1)$, and for every r, $G(F_1(x, c), F_2(y, c); r) = (H_1(x, (c, r)), H_2(y, (c, r)))$. Hence, Eq. 1 can be written as

$$\underset{(c,r) \leftarrow_R \{0,1\}^u}{\Delta} (\mathsf{Sim}(1); \ (H_1(x, (c, r)), H_2(y, (c, r))))) \leq \varepsilon(n).$$

Since $\varepsilon(n) \leq \max(\varepsilon(n), \delta(n) + \varepsilon(t(n)))$, the theorem follows.

□

References

[AIK04] Applebaum, B., Ishai, Y., Kushilevitz, E.: Cryptography in NC^0. In: Proceedings of 45th Symposium on Foundations of Computer Science (FOCS 2004), pp. 166–175. IEEE Computer Society, Rome, Italy, 17–19 October 2004

[AIK15] Applebaum, B., Ishai, Y., Kushilevitz, E.: Minimizing locality of one-way functions via semi-private randomized encodings. Electron. Colloq. Comput. Complex. (ECCC) **22**, 45 (2015)

[BFS86] Babai, L., Frankl, P., Simon, J.: Complexity classes in communication complexity theory (preliminary version). In: 27th Annual Symposium on Foundations of Computer Science, pp. 337–347. IEEE Computer Society, Toronto, Canada, 27–29 October 1986

[BIKK14] Beimel, A., Ishai, Y., Kumaresan, R., Kushilevitz, E.: On the cryptographic complexity of the worst functions. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 317–342. Springer, Heidelberg (2014)

[BM88] Babai, L., Moran, S.: Arthur-merlin games: a randomized proof system, and a hierarchy of complexity classes. J. Comput. Syst. Sci. **36**(2), 254–276 (1988)

[FKN94] Feige, U., Kilian, J., Naor, M.: A minimal model for secure computation (extended abstract). In: Leighton, F.T., Goodrich, M.T. (eds.) Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, pp. 554–563. ACM, Montréal, Québec, Canada, 23–25 May 1994

[GIKM00] Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. J. Comput. Syst. Sci. **60**(3), 592–629 (2000)

[GKW15] Gay, R., Kerenidis, I., Wee, H.: Communication complexity of conditional disclosure of secrets and attribute-based encryption. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part II. LNCS, vol. 9216, pp. 485–502. Springer, Heidelberg (2015)

[GPW15] Göös, M., Pitassi, T., Watson, T.: Zero-information protocols and unambiguity in arthur-merlin communication. In: Roughgarden, T. (ed.) Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS 2015, pp. 113–122. ACM, Rehovot, Israel, 11–13 January 2015

[IK97] Ishai, Y., Kushilevitz, E.: Private simultaneous messages protocols with applications. In: Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems, pp. 174–183, June 1997

[IK00] Ishai, Y., Kushilevitz, E.: Randomizing polynomials: a new representation with applications to round-efficient secure computation. In: 41st Annual Symposium on Foundations of Computer Science, FOCS 2000, pp. 294–304. IEEE Computer Society, Redondo Beach, California, USA, 12–14 November 2000

[Ish13] Ishai, Y.: Randomization techniques for secure computation. In: Prabhakaran, M., Sahai, A., (eds.) Secure Multi-Party Computation, vol. 10 of Cryptology and Information Security Series, pp. 222–248. IOS Press (2013)

[Kla03] Klauck, H.: Rectangle size bounds and threshold covers in communication complexity. In: 18th Annual IEEE Conference on Computational Complexity (Complexity 2003), pp. 118–134. IEEE Computer Society, Aarhus, Denmark, 7–10 July 2003

[Kla10] Klauck, H.: A strong direct product theorem for disjointness. In: Schulman, L.J. (ed.) Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, pp. 77–86. ACM, Cambridge, Massachusetts, USA, 5–8 June 2010