

Position-Based Cryptography and Multiparty Communication Complexity

Joshua Brody¹, Stefan Dziembowski², Sebastian Faust³, and Krzysztof Pietrzak⁴

¹ Swarthmore College, brody@cs.swarthmore.edu

² University of Warsaw, s.dziembowski@crypto.edu.pl*

³ Ruhr University Bochum and TU Darmstadt, sebastian.faust@rub.de **

⁴ IST Austria, pietrzak@ist.ac.at***

Abstract. *Position based cryptography (PBC)*, proposed in the seminal work of Chandran, Goyal, Moriarty, and Ostrovsky (SIAM J. Computing, 2014), aims at constructing cryptographic schemes in which the identity of the user is his geographic position. Chandran et al. construct PBC schemes for *secure positioning* and *position-based key agreement* in the *bounded-storage model* (Maurer, J. Cryptology, 1992). Apart from bounded memory, their security proofs need a strong additional restriction on the power of the adversary: he cannot compute *joint* functions of his inputs. Removing this assumption is left as an open problem.

We show that an answer to this question would resolve a long standing open problem in multiparty communication complexity: finding a function that is hard to compute with low communication complexity in the simultaneous message model, but easy to compute in the fully adaptive model.

On a more positive side: we also show some implications in the other direction, i.e.: we prove that lower bounds on the communication complexity of certain multiparty problems imply existence of PBC primitives. Using this result we then show two attractive ways to “bypass” our hardness result: the first uses the random oracle model, the second weakens the *locality* requirement in the bounded-storage model to *online computability*. The random oracle construction is arguably one of the simplest proposed so far in this area. Our results indicate that constructing improved provably secure protocols for PBC requires a better understanding of multiparty communication complexity. This is yet another example where *negative* results in one area (in our case: lower bounds in multiparty communication complexity) can be used to construct secure cryptographic schemes.

* Supported by the ERC starting grant CNTM-207908 and by the FNP *Team* grant 2016/1/4.

** Supported by the Emmy Noether Program FA 1320/1-1 of the German Research Foundation (DFG).

*** Supported by the European Research Council, ERC consolidator grant (682815 - TOCNeT).

1 Introduction

The standard way to identify participants in cryptographic protocols is to check their knowledge of some secret data (like a password or a key), to verify some biometric information, or the possession of some hardware tokens. A new intriguing idea, known under the name of *position-based cryptography (PBC)* [16] is to construct algorithms in which the participating parties are identified by *their geographic position*. For example, consider the setting where we want to grant access to a server only to the personnel within some military base. A position-based system could be used to give access to every user that is physically located within the base, but deny it to everybody outside. There are many other examples one can think of where position-based authentication would be useful. Say, a protocol for sending confidential documents to everyone who is present in some conference room, granting WiFi access to people within some building, or checking if a food delivery was indeed ordered from some physical address. Of course, such protocols can be combined with other means of authentication, and hence they can also serve for providing an additional layer of security. See [16] for more on potential applications of this concept.

PBC protocols are typically based on the physical characteristics of wireless communication channels; concretely, they are based on the fact that electronic signals are traveling at the speed of light, denoted c (and hence traveling from point \hat{A} to \hat{B} takes time $\|\hat{A}\hat{B}\|/c$, where $\|\cdot\|$ denotes the length of the segment $\hat{A}\hat{B}$). Thus, if a *verifier* \mathcal{V} sends a message at time T and receives a reply from a *prover* \mathcal{P} within time T' , the verifier can be sure that this reply was sent by a machine that is positioned at distance no more than $c \cdot (T' - T)/2$. A natural idea would be to exploit this fact, and use some standard trilateration techniques (like the one used in the GPS system) by having a group of verifiers $\mathcal{V}_1, \dots, \mathcal{V}_n$ positioned in space and letting them jointly verify the distance from the prover. Unfortunately, as shown by Chandran et al. [16], the problem of designing PBC protocols is harder than it may seem at the first sight. In fact, they show that in the so-called *vanilla model* (i.e. without any additional assumptions), PBC is impossible: There exists an adversarial strategy which places devices around some point \hat{A} , and these devices can jointly convince the verifiers in any PBC protocol that they are at point \hat{A} , thus breaking the scheme. One way to get around this would be to restrict the number of adversary's devices (as the number of devices required in their attack is as large as the number of the verifiers used in the protocol). This however is not very realistic, as deploying several adversarial devices is usually easy in practice, since modern wireless devices are cheap and small.

Chandran et al. is use Maurer's bounded-storage model (BSM) [26], studied in a number of papers, including [3,11,19,36,25,27], the bounded-*retrieval* model (BRM) is a closely related variant of the BSM [17,13,20]. In this model, it is assumed that the users of cryptographic protocols have short time access to a long random string X that is so large that it cannot be stored by the adversary in its entirety. The only thing that the adversary can do is to compute and store some function adv on X (where $|\text{adv}(X)| \leq \xi|X|$, for a constant $0 \leq \xi \ll 1$). On

the other hand, the honest parties of a protocol should be only required to access small parts of X in order to complete the protocol. The way this model is used in [16] is as follows: it is assumed that there is a group of *verifiers* \mathcal{V}_i positioned in space. Suppose that a *prover* \mathcal{P} claims to be at some position $\hat{\mathcal{P}}$. Each of the verifiers broadcasts a long string X_i in such a way that all the X_i 's arrive at $\hat{\mathcal{P}}$ at the same time T . When this happens, the prover computes some function f on the X_i 's, and takes some actions that depend on the computed value (e.g. sends the computed value back to the verifiers in order to prove that he is in point $\hat{\mathcal{P}}$). The function f should be very efficiently computable. In particular, to compute it one should only have to access a small fraction of the X_i 's [16].

In this model Chandran et al. construct a *positioning protocol*, where a prover convinces the verifiers that he is physically at some point $\hat{\mathcal{P}}$. In practice a protocol like this is not very useful as a standalone primitive, since it comes with no guarantee that any future communication will be happening with the machine that is indeed in $\hat{\mathcal{P}}$ (due to man-in-the-middle attacks). Chandran et al. also construct a more advanced primitive, called a *position-based key-agreement protocol*. Here the final output of the honest parties is a key K which is not known to a potential adversary. Both the positioning and the position-based key agreement protocols have a very simple structure (see Sect. 2.3). Namely, in case of the positioning protocol the prover just sends back $f(X_1, \dots, X_n)$ to the verifiers (who check if this value is correct and was received at the right time). For the position-based key agreement the prover simply lets the agreed key K be equal to $f(X_1, \dots, X_n)$. Such protocols are called *one-round*, and are very attractive because of their simplicity. They will also be the focus of this paper.

The proof in [16] requires one additional restriction on the power of the adversary, namely, it is assumed (see [16], page 1294, Sect. 1.2) that whenever an adversarial device receives strings X_{i_1}, \dots, X_{i_a} at the same time, it cannot compute an arbitrary joint function adv on X_{i_1}, \dots, X_{i_a} (with short output). Instead, it can only compute several (adaptively chosen) functions on each X_{i_j} independently (the same restriction applies to the honest parties). Removing this assumption is left as an “important open problem” in [16] and studying this open question is the main topic of this work. We show deep connections between the problem of constructing positioning and position-based key agreement protocols in the *unrestricted BSM* model (i.e. without restrictions on the adv function except of a bound on its output size), and the area of *multiparty communication complexity*. Before describing our contribution in more detail (in Sect. 1.2) let us provide a short introduction to this area (more formal definitions are given in Sect. 2.2, and for a more comprehensive introduction see [24])

1.1 Multiparty communication complexity

In a typical communication complexity problem, there are k players, denoted $\text{PLR}_1, \dots, \text{PLR}_k$. There are also k inputs $x_1, \dots, x_k \in \{0, 1\}^n$, and the players must communicate to compute some function $f(x_1, \dots, x_k)$ of the inputs. The *communication cost* of a protocol is measured as the worst-case maximal number

of bits communicated, taken over all possible inputs and all choices for the random string.

In the multiplayer setting (when $k > 2$) there are two different models for how the input is shared. In the number-in-hand (NIH) model, each player PLR_i sees the i th input x_i . In the number-on-the-forehead (NOF) model, each PLR_i sees all inputs *except* x_i . One can imagine in an NOF protocol that all players meet in a room, and PLR_i has x_i written on her forehead. In this way, players can see all inputs *except* what is written on their foreheads. When $k = 2$, the NIH and NOF models are one and the same, but for $k > 2$, they are quite different. In particular, communication in the NOF model becomes intuitively very easy, because so much information is shared. This makes proving NOF communication lower bounds *harder*. In this paper, we focus on NOF communication complexity.

It is particularly interesting to understand what role *interaction* plays in communication complexity. In an arbitrary (“fully adaptive”) protocol, players are allowed to speak back and forth, and messages are broadcast. It is also interesting to consider a more restrictive model, where each player sends a single message to a referee, who does not see the inputs, and must compute $f(x_1, \dots, x_k)$ only from the messages sent by the players. This restricted model of communication is called the Simultaneous Messages (SM) model. Occasionally, the communication complexity of problems can be the same in the SM and interactive model, but for other problems, allowing interactive communication can even lead to an exponential decrease in the communication complexity. The NOF communication model was invented thirty years ago in [15], who also gave as an application lower bounds for branching programs.

Position based cryptography was partly inspired by the area called *secure positioning* [8,33,37,12]. More recently there was work towards constructing PBC protocols based on other “physical” assumptions, such as quantum channels [10,35,14]⁵ (see also [9] and the webpage [34]) or noisy channels [21].

1.2 Our contribution

We show that constructing a one-round positioning protocol in the unrestricted BSM gives a construction of a function π with linear SM complexity (in the NOF model). If we additionally require that the computation on the prover is *local* (i.e. he only needs to look at small parts of the input), then π has low complexity in the fully adaptive model. Finding a function with such properties is a longstanding open problem in communication complexity, and therefore this result can be viewed as a “negative” answer to the question posted in [16].

On a more positive side: we show some implications in the other direction. Namely, we prove that any function that has high communication complexity in the so-called “one-round almost SM model” (see Sect. 2.2 for the definition) can be transformed into a secure positioning protocol. The assumed hardness has to hold in a strong, randomized sense, i.e., the probability that any “adaptive SM” protocol computes the output correctly has to be negligible. Fortunately, we show

⁵ Note that [35] uses the random oracle model, that we use in this work (in Sect. 4.1).

a function that satisfies this requirement. Our function uses a hash function as a building block, and the security proof models this hash function as a random oracle (hence, our construction does not contradict the negative result mentioned above). The resulting positioning protocol is very simple: essentially, one verifier sends a long string X , the other verifiers send much shorter strings Z_i , and the output is the sub-string of X on the positions determined by the hash of the concatenated Z_i 's.

We also construct positioning and position-based key agreement schemes from any function that has high complexity in the “fully adaptive SM model” (see Sect. 2.2). For our construction to work we need to assume even stronger hardness: the output of the function has to be “close to uniform” (in the sense of “statistical distance”, see Sect. 2 for the definition). We show that the so-called “generalized inner product” function has this property. The resulting protocol does *not* have the “locality” property, i.e., the prover in the protocol needs to read its entire input. The good news is that this computation is very simple, can be performed very efficiently in an “online” fashion, and hence it may still be possible to implement it in practice.

2 Preliminaries

Let A and B be random variables distributed over set \mathcal{A} . The *statistical distance between A and B* is defined as $\Delta(A; B) := \frac{1}{2} \sum_{a \in \mathcal{A}} |\mathbb{P}(A = a) - \mathbb{P}(B = a)|$. The *statistical distance of A from uniformity* is defined as $d(A) := \Delta(A; U_{\mathcal{A}})$, where $U_{\mathcal{A}}$ has uniform distribution over \mathcal{A} . The statistical distance of A from uniformity *conditioned on B* is defined as $d(A | B) = \Delta((A, B); (U_{\mathcal{A}}, B))$ (where $U_{\mathcal{A}}$ is uniform and independent from B). The *min-entropy* of a random variable W is defined as $\mathbb{H}_{\infty}(W) := -\log_2(\max_w \mathbb{P}[W = w])$. We will use the following fact that can be viewed as a chain-rule for the statistical distance from uniformity (see, e.g., [19], Lemma 3).

Lemma 1. *For any random variables X_1, \dots, X_n , and Y we have that*

$$d(X_1, \dots, X_n | Y) \leq \sum_{i=1}^n d(X_i | X_1, \dots, X_{i-1}, Y).$$

We also have the following (see, e.g., [19], Lemma 1).

Lemma 2. *For every random variables X and Y taking values from \mathcal{X} and \mathcal{Y} (respectively) we have that $\max_{\alpha: \mathcal{Y} \rightarrow \mathcal{X}} (\mathbb{P}(X = \alpha(Y))) \leq d(X | Y) + 1/|\mathcal{X}|$. Moreover, if $\mathcal{X} = \{0, 1\}$, then $2 \max_{\alpha: \mathcal{Y} \rightarrow \mathcal{X}} (\mathbb{P}(X = \alpha(Y))) - 1 = d(X | Y)$.*

2.1 Guessing bits from “compressed” information

The following machinery will be needed in Sect. 4.1. Consider the following natural question. Suppose $X \leftarrow \{0, 1\}^n$ is chosen uniformly at random. Let $\text{compress} : \{0, 1\}^n \rightarrow \{0, 1\}^{\beta n}$ be any function that “compresses” X , i.e., such

that $\beta < 1$. Let us ask what is the maximal probability that given $\text{compress}(X)$ one can compute the substring consisting of t random positions in X ? More precisely, let $\text{guess} : \{1, \dots, n\}^t \times \{0, 1\}^{\beta n} \rightarrow \{0, 1\}^t$ be any function that tries to “predict” these bits. We ask what is the maximal (over compress and guess) probability that $\text{guess}(R, \text{compress}(X)) = (X[R_1], \dots, X[R_t])$, where $R = (R_1, \dots, R_t) \leftarrow \{1, \dots, n\}^t$ is random. This question was first answered by Nisan and Zuckerman [29]. In what follows, we use the presentation from [16] (which, in turn, is partly based on [36]). The following lemma can be derived from the discussion in Sect. 4.3 (page 1306) of [16].

Lemma 3 ([29,36,16]). *Take any $\beta < 1$. For every t take n such that $n > t$. Then for every $\text{compress} : \{0, 1\}^n \rightarrow \{0, 1\}^{\beta n}$ and $\text{guess} : \{1, \dots, n\}^t \times \{0, 1\}^{\beta n} \rightarrow \{0, 1\}^t$ and a uniformly random $X \leftarrow \{0, 1\}^n$ and $R = (R_1, \dots, R_t) \leftarrow \{1, \dots, n\}^t$ we have that*

$$\mathbb{P}(\text{guess}(R, \text{compress}(X)) = (X[R_1], \dots, X[R_t])) \leq \text{negl}(t).$$

Proof. Simple inspection of the argument in Sect. 4.3 of [16]. Observe that EG in [16] is defined as $\text{EG}(X, R) := (X[Z_1], \dots, X[Z_t])$. The argument in [16] uses parameters β and δ in, where β is defined as the “adversarial storage rate“ (and is the same parameter as in our notation), and the δ is such that the min-entropy rate of X is $\beta + \delta$. Since in our case X is uniform, thus we can simply set $\delta := (1 - \beta)$. Observe that $\delta > 0$. In [16] the authors use a security parameter κ and require that $t \geq (2/\delta)\kappa$. We can however also treat t as the security parameter, and then set $\kappa := t\delta/2$. In [16] it is shown that the probability p of guessing $\text{EG}(X, R)$ correctly is negligible in κ . Therefore it is also negligible in t (as δ is a positive constant). \square

If \mathcal{A} is a finite set, then $A \leftarrow \mathcal{A}$ denotes the fact that A is sampled uniformly at random from \mathcal{A} . For a natural q the symbol $\text{GF}(q)$ denotes the Galois field of order q . The “||” symbol denotes the concatenation of strings, and for $X = (X_1, \dots, X_n) \in \mathcal{X}^n$ (for some set \mathcal{X}) and $i, j \in \{1, \dots, n\}$ (such that $i \leq j$) by writing $X[i]$ we mean X_i , and by $X[i, \dots, j]$ we mean (X_i, \dots, X_j) . We will use the *random oracle model* (ROM) [7].

2.2 Multiparty communication complexity

A brief introduction to the multiparty complexity was already given in Sect. 1.1. We now introduce more formally the concrete computation models that are used later in this paper. A *protocol* is a tuple $\text{PROT} := (\text{PLR}_1, \dots, \text{PLR}_k, \text{REF})$ of players (modeled as Turing machines) that interact with each other. We assume that the protocol is in the *public coins* model, i.e., the players have access to some common source of randomness. The *input of the protocol* is a tuple $(x_1, \dots, x_k) \in \mathcal{X}_1 \times \dots \times \mathcal{X}_k$ (where \mathcal{X}_i ’s are some sets). Informally speaking, the goal of the players is to jointly compute some function $f : \mathcal{X}_1 \times \dots \times \mathcal{X}_k \rightarrow \mathcal{Y}$ (where \mathcal{Y} is some set). The models that are considered in the literature differ in terms of what access the players have to the input, and how can they communicate.

The player REF is called the *referee* and typically takes no input. In the number-on-the-forehead (NOF) model each PLR_i sees all inputs *except* x_i . We also impose some restrictions on the communication between the parties. We say that *the protocol* PROT *operates in fully adaptive simultaneous message (SM) model* if the parties communicate as follows.

1. Every player PLR_i (for $i = 1$ to k) receives input $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_k$ (where each $x_i \in \mathcal{X}_i$), and the referee REF receives no input.
2. The computation is structured in some number of rounds. In the j th round the following happens:
 - For $i = 1, \dots, k$ every player PLR_i (for $i = 1, \dots, k$) broadcasts some value w_i^j , which is a function of his input variables and the messages broadcast by other players in the previous rounds.
3. Finally, REF computes the output of the protocol, denoted $\text{PROT}(x_1, \dots, x_k)$, that is a function of the values w_i^j that were broadcast by the PLR_i 's during the computation.

We say that the protocol operates in *one-round SM model* if the number of rounds in Step 2 above is 1 (in the literature this has also been called simply the “SM model”). The *one-round almost SM model* [31] is the same as the one-round SM model, except that one of the players, PLR_k , say, is the referee (and hence there is no need to specify REF separately, and we can write $\text{PROT} = (\text{PLR}_1, \dots, \text{PLR}_k)$). Compared to the one-round SM model the only difference is in Step 3, that in case of the one-round almost SM model becomes:

- 3'**. PLR_k computes the output of the protocol, denoted $\text{PROT}(x_1, \dots, x_k)$, that is a function of his own input (x_1, \dots, x_{k-1}) and the values w_i^j that were broadcast by the PLR_i 's during the computation.

Observe that in case of the one-round almost SM model we can assume that the message w_k^1 (sent by PLR_k) is empty, since the only receiver of this message is PLR_k himself.

For a protocol PROT the maximal *total* length of the w_i^j 's (where the maximum is taken over all $(x_1, \dots, x_k) \in \mathcal{X}_1 \times \dots \times \mathcal{X}_k$) is called the *communication cost* of PROT . The communication complexity of a function f is the minimum communication cost of any protocol computing f .

As explained above, we are mostly interested in the average-case complexity of the multiparty protocols.

Definition 1. *We say that a function $f : \mathcal{X}_1 \times \dots \times \mathcal{X}_k \rightarrow \mathcal{Y}$ is (s, ε) -hard in the one-round SM model (or the fully adaptive model) if for every protocol PROT whose communication complexity is at most s , and that operates in the one-round SM model (or the fully adaptive model, respectively), the probability that PROT computes f correctly is at most ε , i.e.,*

$$\mathbb{P}(\text{PROT}(X_1, \dots, X_k) = f(X_1, \dots, X_k)) \leq \varepsilon, \quad (1)$$

where the probability is taken over $(X_1, \dots, X_k) \leftarrow \mathcal{X}_1 \times \dots \times \mathcal{X}_k$ and the public randomness available to the players (the probability in Eq. (1) is called the correctness probability).

Observe that the adversary can always achieve $\epsilon = 1/|\mathcal{Y}|$. As we will be interested in protocols where ϵ is negligible, we will usually use \mathcal{Y} 's that are of size exponential in the security parameter t (e.g., $\mathcal{Y} = \{0, 1\}^t$). We will also use a stronger notion of hardness that informally speaking requires that the information about $f(X_1, \dots, X_k)$ obtained by a referee in a multiparty protocol with communication complexity s is small.

Definition 2. *We say that a function $f : \mathcal{X}_1 \times \dots \times \mathcal{X}_k \rightarrow \mathcal{Y}$ is (s, ϵ) -strongly-hard in the one-round SM model (or the fully adaptive model) if for every protocol PROT whose communication complexity is at most s , and that operates in the one-round SM model (or the fully adaptive model, respectively) we have that*

$$d\left(f(X_1, \dots, X_k) \mid \{W_1^j, \dots, W_k^j\}_{j=1}^t\right) \leq \epsilon, \quad (2)$$

where the experiment in (2) consists of sampling $(X_1, \dots, X_k) \leftarrow \mathcal{X}_1 \times \dots \times \mathcal{X}_k$ and the public randomness of the players, and each W_i^j is the message broadcast by PLR_i in the j th round.

To see why the notion defined in Def. 1 is at least as strong as the one from Def. 2, observe that, by Lemma 2, Eq. (2) implies that

$$\mathbb{P}(\text{PROT}(X_1, \dots, X_k) = f(X_1, \dots, X_k)) \leq 1/|\mathcal{Y}| + \epsilon$$

(see Eq. (1)), which is small for large \mathcal{Y} (and small ϵ).

2.3 Secure Positioning and the Position-Based Key Agreement

In this section we describe in details the model that was already informally discussed in Sect. 1 (for the full formal definition see [16]). A *secure positioning protocol in D dimensions* is a tuple $\Pi = (\mathcal{V}_1, \dots, \mathcal{V}_{D+1}, \mathcal{P})$, where the \mathcal{V}_i 's are the *verifiers* positioned in a D -dimensional space (and not lying on one $(D-1)$ -dimensional hyperspace) and a \mathcal{P} is a *prover*, positioned within the polytope determined by the verifiers. The protocol will be attacked by a set of adversaries $\{\mathcal{A}_1, \dots, \mathcal{A}_t\}$, each \mathcal{A}_i positioned in place $\hat{\mathcal{A}}_i$. The \mathcal{V}_i 's, \mathcal{A}_i 's, and \mathcal{P} are modeled as randomized Turing machines. We also assume that the \mathcal{A}_i 's have access to the common public randomness.

We assume that all the machines are equipped with perfect clocks and that their computation takes no time. Each machine is aware of its own position in space (more formally: it gets it as an auxiliary input). The position of each verifier \mathcal{V}_i is denoted by $\hat{\mathcal{V}}_i$. The verifiers also get as input a position $\hat{\mathcal{P}}$ where the prover “claims to be”. Their goal is to check if he indeed is in this position. The decision (yes/no) of the verifiers is communicated at the end of the protocol by one of them (\mathcal{V}_1 , say).

The only messages that are sent are of a broadcast type (i.e. there are no directional antennas). A message sent by a machine positioned in point U arrives to a machine in point U' in time $\|UU'\|/c$, where c is the speed of light. We assume that the adversary cannot block or delay the messages sent between the

honest participants. It is clear that such an assumption is unavoidable, as, by blocking all the messages, the adversary can always prevent any protocol from succeeding. The communication links between the verifiers are secure (secret and authenticated), which can be achieved by standard cryptographic techniques.

As already highlighted in Sect. 1, the important difference between our model and the one of [16] is that we assume that if in some moment T several messages $X_{i_1}, \dots, X_{i_\ell}$ meet at point $\widehat{\mathcal{A}}_i$, then \mathcal{A}_i can compute any joint function adv_i^T of $(X_{i_1}, \dots, X_{i_\ell})$. Let A_i^T be the result of this computation, and let A be the random variable denoting the concatenation of all the A_i^T . We require that $|A| \leq s$, where s is called the *retrieval bound*. Informally speaking, the adversary can either broadcast A_i^T or store it in his memory, but to keep the model as simple as possible we will make no distinction between these two cases. Namely, we assume that (1) each adversary always broadcasts every value immediately after he computed it, and (2) each adversary stores every message broadcast by any adversary.⁶ Hence a value of a function adv_i^T can depend on all the adversarial messages received by \mathcal{A}_i at or before time T (including the messages sent by \mathcal{A}_i himself in time T).

We assume that several adversaries can be put in one place in space, but for simplicity we require that the adversaries that are in the same place do not broadcast messages at the same time (clearly, this assumption can be made without loss of generality, as such adversaries can be “simulated” by one).

We also assume that every adversary computes (and broadcasts) a value only once. Note that this also does not affect the generality of the model, as we do not put any restrictions on the number of adversaries, and moreover, several adversaries can be put in the same point in space. Therefore an adversary that computes m values (in different moments in time), can be “simulated” by m adversaries placed in the same point. We say that Π is an (s, ρ) -secure positioning protocol if the following two conditions hold:

correctness: If the prover \mathcal{P} is placed in the claimed position $\widehat{\mathcal{P}} \in \mathcal{G}$ then \mathcal{V}_1 produces as output “yes”,

security: For any set of adversaries $\{\mathcal{A}_1, \dots, \mathcal{A}_t\}$ with retrieval bound s (such that no adversary or honest prover is in position $\widehat{\mathcal{P}}$), the verifier \mathcal{V}_1 produces as output “yes” with probability at most ρ . (If \mathcal{V}_1 produced “yes” then we say that the adversaries *broke the scheme*.)

Following [16], we also consider a stronger type of protocols called the *position-based key agreement*. In such a protocol the goal of the prover and the verifiers is to agree on a key $K \in \{0, 1\}^m$. More formally, at the end of the execution the prover produces as output $K_{\mathcal{P}}$, and one of the verifiers, \mathcal{V}_1 (say) produces $K_{\mathcal{V}}$. We say that Π is an (s, ρ) -secure position-based key agreement protocol in D dimensions if the following two conditions hold (assuming the prover \mathcal{P} is placed in the claimed position $\widehat{\mathcal{P}} \in \mathcal{G}$):

⁶ Observe that these assumptions can be made without loss of generality, as storing the computed values does not affect the retrieval bound.

correctness: The agreed keys are identical, i.e., $K_{\mathcal{P}} = K_{\mathcal{V}}$.

security: For any set of adversaries $\{\mathcal{A}_1, \dots, \mathcal{A}_t\}$ with retrieval bound s (such that no adversary is in position $\widehat{\mathcal{P}}$) we have that $d(K_{\mathcal{P}} | A) \leq \rho$ (recall that A is the random variable denoting all the information computed by the adversaries).⁷

For reasons explained in the introduction we are interested in protocols that have the following simple structure (let T be some moment in time):

1. Each \mathcal{V}_i sends a message $X_i \leftarrow \mathcal{X}_i$ (where \mathcal{X}_i is some set) to \mathcal{P} in time $T - \|\widehat{\mathcal{V}}_i \widehat{\mathcal{P}}\|/c$ (in this way all X_i 's arrive to \mathcal{P} in time T).
2. \mathcal{P} computes $Y = \pi(X_1, \dots, X_{D+1})$ (for some function $\pi : \mathcal{X}_1 \times \dots \times \mathcal{X}_{D+1} \rightarrow \mathcal{Y}$) and
 - **in case of the positioning protocols:** \mathcal{P} broadcasts Y ,
 - **in case of the key-agreement protocols:** \mathcal{P} sets $K_{\mathcal{P}} = Y$.
3. In the last step the verifiers compute $\pi(X_1, \dots, X_{D+1})$ in some way (e.g., they may simply send to one verifier all the inputs and let him compute the output). The details of this computation depend on the function that they compute. In many cases there also exist techniques that allow to save on the communication and space complexities of this procedure, e.g., each X_i can be generated pseudorandomly from some seed S_i , in which case it is enough that the verifiers store and send to each other only the S_i 's. We write more about it when we consider the concrete implementations in Sect. 4.
 - **in case of the positioning protocols:** each \mathcal{V}_i accepts the proof only if y that he received is indeed equal to $\pi(X_1, \dots, X_{D+1})$ and it arrived to him in time $T + \|\widehat{\mathcal{V}}_i \widehat{\mathcal{P}}\|/c$,
 - **in case of the key-agreement protocols:** the verifier \mathcal{V}_1 produces $K_{\mathcal{V}} = \pi(X_1, \dots, X_{D+1})$ as the agreed key.

A protocol of this type will be called a *one-round protocol parametrized by π* . We say that a protocol is *for positions in the set $\mathcal{W} \subseteq \mathbb{R}^D$* if it works only if $\widehat{\mathcal{P}} \in \mathcal{W}$ (note, however, that we do *not* restrict the set of positions where the adversary can be placed). Let us also comment on the assumption that X_i is sampled uniformly from some set. This is done mostly for the sake of simplicity, and to keep our model consistent with the one in Sect. 2.2. We could also have a more general definition where the X_i 's would come from some more general class of distributions, e.g., the distributions with high min-entropy (as is done in [16]). For the equivalence results shown in Sect. 3 to hold, we would need to extend the hardness definitions in Sect. 2.2 to cover also the case when the X_i 's are not uniform, but this can be done in a straightforward way. Also our constructions can be easily generalized to cover the case when the inputs come from a high-min entropy source (this generalization will be described in the full version of this paper).

⁷ In [16] the security of a key agreement is defined using the “indistinguishability” paradigm (cf. Def. 2.2 in [16]): no adversary, after learning A , should be able to distinguish $K_{\mathcal{P}}$ from a uniformly random key, with advantage larger than ρ . It is easy to see that these definitions are equivalent.

It is natural to ask how do these two primitives relate to each other. Obviously, every (s, ρ) -secure position-based key agreement protocol can be converted into an (s, ρ') -secure positioning protocol with $\rho' = 2^{-|K|} + \rho$ in the following way: let the prover send $K_{\mathcal{P}}$ to \mathcal{V}_1 , and let \mathcal{V}_1 output “yes” only if $K_{\mathcal{P}} = K_{\mathcal{V}}$. It easily follows from Lemma 2 that if \mathcal{P} is not in the position $\tilde{\mathcal{P}}$ then the probability that he can guess $K_{\mathcal{P}}$ is at most ρ' .

On the other hand, it is also possible to convert every secure (s, ρ) -secure positioning protocol (for some negligible ρ) into an (s, ρ') -secure position-based key agreement protocol (for negligible ρ'), at a cost of introducing computational assumptions. Concretely, public-key encryption and non-malleable commitments, we refer to [16] (Section 6, page 1311) for further details.

2.4 Prover’s efficiency

The function π needs to be computed also by the prover \mathcal{P} , and it is important to choose π such that this computation can be done efficiently. Note that the advantage of \mathcal{P} over the adversaries is that he has simultaneous access to all the π ’s inputs X_1, \dots, X_{D+1} . Since the X_i ’s are very long, we would ideally like to be able to compute π by looking only on some small parts of the inputs (polylogarithmic in $|X|$, say). This property, called *locality*, was stated as an explicit requirement in [16]. It is also common in the previous papers on the bounded-storage model [26,3,20,18]. One of our constructions in this paper (see Sect. 4.2) does not have this property (the one in Sect. 4.1 has it). Instead it has the property of being *online computable* which means that π reads its input by just processing its input online in small memory. We remark that in some cases such algorithms may actually be easier to implement than some of the locally computable ones (think of a locally computable algorithm that is required to access many bits on its input that are located far away).

3 The reductions

In this section we show strong connections between the two areas described in Sect. 2. We start (Sect. 3.1) with showing that a construction of a positioning protocol immediately gives a construction of a function with a high one-round SM complexity. Note that this means that a similar implication holds for position-based key agreement (since, as explained in Sect. 2.3, position-based key agreement is a stronger primitive than secure positioning). Then, in Sect. 3.2, we show an implication in the opposite direction, namely, we prove that every function with high one-round almost SM complexity gives rise to a secure positioning protocol, and every function with high fully adaptive SM complexity gives rise to a secure position-based key agreement protocol.

From an application point of view, the results in Sect. 3.1 are “negative”, as they show that in order to construct secure positioning protocols (and the position-based key agreement protocols) we need to show multiparty functions that have high communication complexity, which seems to be non-trivial, especially if the

locality is required (see end of Sect. 3.1 for a discussion on this). On the other hand, the results from Sect. 3.2 can be viewed as “positive”, since they provide a way to construct secure positioning (and position-based key agreement) protocols. Notice that these positive results yield a constructive use of lower bounds in communication complexity. We instantiate these constructions with concrete protocols in Sect. 4.

3.1 Secure positioning in the BRM implies lower bounds for SM complexity

We now show that existence of a one-round protocol for secure positioning implies lower bounds for the multiparty communication complexity. Note that, as described in Sect. 2.3, the secure positioning protocols are a weaker primitive than the position-based key agreement protocols, and a similar implication also holds for the position-based key agreement. To keep the exposition simple we address only the case when the verifiers are placed on vertices of a regular D -dimensional simplex, but it should be clear that our argument can be easily extended to more general cases. The statement of the lemma assumes that $D = 2$ or $D = 3$. This is because, obviously, the case of $D > 3$ has no practical relevance, and for $D = 1$ the function π has only two arguments, so, as described in the introduction, it makes little sense to talk about the NOF complexity. Recall that a regular 2-dimensional simplex is an equilateral triangle, and a regular 3-dimensional simplex is a regular tetrahedron. We now have the following theorem.

Theorem 1. *Suppose Π is an (s, ρ) -secure one-round positioning protocol in D dimensions (for $D = 2$ or $D = 3$) parametrized by $\pi : \mathcal{X}_1 \times \dots \times \mathcal{X}_{D+1} \rightarrow \mathcal{Y}$ with verifiers positioned on vertices of a regular D -dimensional simplex. Then π is (s, ρ) -hard in the 1-round SM model.*

Proof. Let a denote the length of the edge of the simplex, or, in other words, the distance between any pair of verifiers. For the sake of contradiction suppose π can be computed in a one-round SM model by a protocol $\text{PROT} = (\text{PLR}_1, \dots, \text{PLR}_{D+1}, \text{REF})$ with communication complexity s and correctness probability $\rho' > \rho$. For every $\text{PLR}_j \in \{\text{PLR}_1, \dots, \text{PLR}_{D+1}\}$ let $\text{Msg}_j = \text{Msg}_j(X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_{D+1})$ denote the message computed by PLR_j , and let $\text{Ref}(\text{Msg}_1, \dots, \text{Msg}_{D+1})$ be the value computed by the referee REF (equal to $\pi(X_1, \dots, X_{D+1})$ with probability ρ'). We now show a set of adversaries $\mathcal{A}_1, \dots, \mathcal{A}_{D+1}, \mathcal{B}_1, \dots, \mathcal{B}_{D+1}$ with retrieval bound s that break Π with probability ρ' (and none of them is positioned in position $\hat{\mathcal{P}}$).

We assume that position $\hat{\mathcal{P}}$ is the center of mass of the simplex determined by the verifiers. Hence, $\hat{\mathcal{P}}$ is in the same distance to all the verifiers, and therefore all the messages X_i are sent in the same moment $U = T - \|\hat{\mathcal{P}}\hat{\mathcal{V}}_1\|/c$, where (as it can be easily verified using basic geometric arguments) $\|\hat{\mathcal{P}}\hat{\mathcal{V}}_1\|$ is equal to $a\sqrt{3}/3$ (if $D = 2$) and is equal to $a\sqrt{6}/4$ (if $D = 3$). This situation is depicted on Fig. 1 for the case $D = 2$.

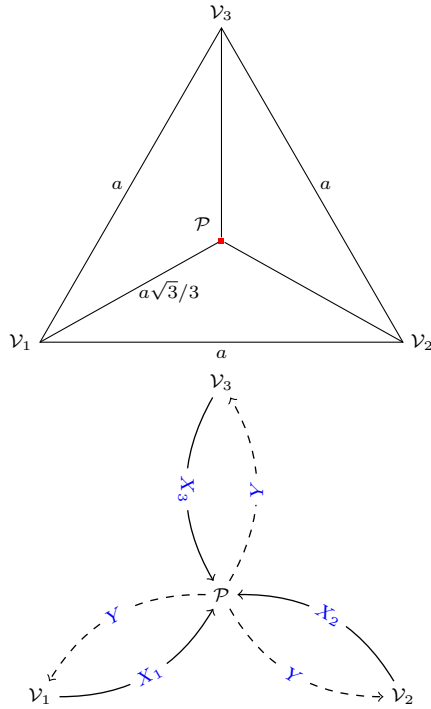


Fig. 1. On the left: the configuration of the prover and the verifiers for in the two-dimensional case. On the right: the execution of the positioning protocol in this configuration. The dashed lines indicate the messages sent back by the prover. Note that the X_i 's and Y are broadcast (there are no directional antennas in our model), and the lines are only indicating the communication that matters for the protocol.

Obviously, all the verifiers expect to receive the answer from the prover in time $T + \|\widehat{\mathcal{P}}\widehat{\mathcal{V}}_1\|/c = U + 2\|\widehat{\mathcal{P}}\widehat{\mathcal{V}}_1\|/c$. The adversaries $\mathcal{A}_1, \dots, \mathcal{A}_{D+1}, \mathcal{B}_1, \dots, \mathcal{B}_{D+1}$ behave in the following way (see Fig. 2).

- Each \mathcal{A}_j is positioned in point $\widehat{\mathcal{A}}_j$ defined as follows: $\widehat{\mathcal{A}}_j$ is the center of mass of the facet determined by the points $\widehat{\mathcal{V}}_1, \dots, \widehat{\mathcal{V}}_{j-1}, \widehat{\mathcal{V}}_{j+1}, \dots, \widehat{\mathcal{V}}_{D+1}$. This facet is either a line segment — in case $D = 2$, or an equilateral triangle — in case $D = 3$. From the regularity of this facet we get that the messages $X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_{D+1}$ (sent by the verifiers $\mathcal{V}_1, \dots, \mathcal{V}_{j-1}, \mathcal{V}_{j+1}, \dots, \mathcal{V}_{D+1}$) arrive to point $\widehat{\mathcal{A}}_j$ in the same moment. In the moment when they arrive there, the adversary \mathcal{A}_j computes $W_j = \text{Msg}_j(X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_{D+1})$ and broadcasts the result. This happens in time $U + \|\widehat{\mathcal{A}}_j\widehat{\mathcal{V}}_i\|/c$.
- Each \mathcal{B}_i is positioned in point $\widehat{\mathcal{V}}_i$.⁸ He does the following:

⁸ The reader may object that it is not realistic to assume that an adversary is positioned at zero distance from a verifier. At the end of the proof we argue that \mathcal{B}_i can actually

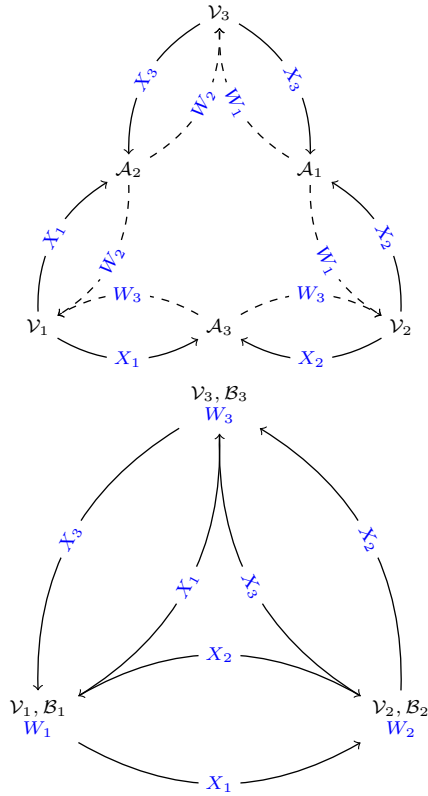


Fig. 2. On the left: the actions of the \mathcal{A}_i 's, on the right: the actions of the \mathcal{B}_i 's (recall that each W_i is a function of all the X_j 's except of X_i).

- When the messages $X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_{D+1}$ arrive to him (observe that, from the regularity of the simplex, they all arrive in the same moment $T' = U + a/c$) he computes $W_i := \text{Msg}_i(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_{D+1})$ and stores the result.
- He also stores each message W_j broadcast by \mathcal{A}_j (for $j \in \{1, \dots, i-1, i+1, \dots, D+1\}$) when it arrives to him. This happens in time $T'' = U + \|\widehat{\mathcal{A}}_j \widehat{\mathcal{V}}_i\|/c + \|\widehat{\mathcal{A}}_j \widehat{\mathcal{B}}_i\|/c$ (where $\widehat{\mathcal{B}}_i$ is the position of \mathcal{B}_i , which is equal to $\widehat{\mathcal{V}}_i$). Hence T'' is equal to $U + 2\|\widehat{\mathcal{A}}_j \widehat{\mathcal{V}}_i\|/c$.
Additionally since $\|\widehat{\mathcal{A}}_j \widehat{\mathcal{B}}_i\|$ is nonnegative, it follows that $\|\widehat{\mathcal{A}}_j \widehat{\mathcal{V}}_i\| + \|\widehat{\mathcal{A}}_j \widehat{\mathcal{B}}_i\| \geq \|\widehat{\mathcal{A}}_j \widehat{\mathcal{V}}_i\| = a$, and therefore $T'' \geq T'$.
- After the two steps above are completed (which happens in time $\max(T', T'') = T''$) the adversary \mathcal{B}_i knows all W_1, \dots, W_{D+1} and he can simply

be put at some place far from any verifier. We decided to assume that \mathcal{B}_i is positioned exactly in point $\widehat{\mathcal{V}}_i$ to keep the exposition simple.

compute the output Y as $\text{Ref}(W_1, \dots, W_{D+1})$, and pass it \mathcal{V}_i (which takes zero time, since \mathcal{B}_i is positioned exactly in $\widehat{\mathcal{V}}_i$). Moreover, he can do it exactly in time $U + 2\|\widehat{\mathcal{P}}\widehat{\mathcal{V}}_1\|/c$ when \mathcal{V}_i expects to receive y . This is possible, because (as we show below)

$$T'' < U + 2\|\widehat{\mathcal{P}}\widehat{\mathcal{V}}_1\|/c. \quad (3)$$

We now show (3). Let us start with case $D = 2$. Since in this case each facet of the simplex is a line segment of length a , hence $\|\widehat{\mathcal{A}}_j\widehat{\mathcal{V}}_i\| = a/2$. Therefore (3) becomes

$$U + a/c < U + 2a\sqrt{3}/(3c), \quad (4)$$

which holds because $1 < 2\sqrt{3}/3$. In case $D = 3$ each facet is a regular triangle with edge of length a . Thus $\|\widehat{\mathcal{A}}_j\widehat{\mathcal{V}}_i\| = \sqrt{3}/3$, and therefore (3) becomes

$$U + 2a\sqrt{3}/(3c) < U + 2a\sqrt{6}/(4c), \quad (5)$$

which holds because $2\sqrt{3}/3 < 2\sqrt{6}/4$. Clearly the adversaries constructed this way compute function π correctly with exactly the same probability σ' as the SM protocol computes it. It remains to calculate how much communication was generated by the adversaries. Observe that each Msg_j is computed by each \mathcal{A}_j and \mathcal{B}_j , respectively. Each \mathcal{B}_j can compute the final answer by storing Msg_j and receiving $\{\text{Msg}_i\}_{i \neq j}$, hence the total amount of retrieved information is $\sum_{i=1}^{D+1} \text{Msg}_i = s$. This finishes the proof.

Finally, note that both inequalities (4) and (5) are sharp, and the differences between the left hand sides and the right hand sides are non-negligible. This means that \mathcal{B}_i has to wait some noticeable amount of time before he sends y to the verifier \mathcal{V}_i . Hence, it is also ok to place \mathcal{B}_i in some position $\widehat{\mathcal{B}}_i$ further away from \mathcal{V}_i (as long as the $\widehat{\mathcal{B}}_i$ is in equal distance to the remaining verifiers). \square

Recall that according to the standard definitions (see Sect. 2.4) we want function π to be locally computable, which means that it should be possible to compute it by looking only at a polylogarithmic number of bits of its input (X_1, \dots, X_{D+1}) . It is easy to see that such an algorithm is trivial to implement by a multiparty protocol that has polylogarithmic communication complexity in the fully adaptive settings. On the other hand, function π , by Theorem 1, needs to have a linear complexity in the one-round SM model. Since finding such functions is an open problem we view this result as an indication why showing one-round positioning protocols in the unrestricted BSM model is hard. The reader may object that typically the communication complexity literature is more focused on deterministic functions that compute one bit, while here we consider randomized functions (with small correctness probability) with multi-bit output. This is not a problem for the following reasons: (1) it is easy to see that a lower bound on the communication complexity of our multi-bit output randomized function also implies a lower bound on a single-bit output functions (since there has to be at least one bit of output that is hard to guess with good probability), and (2) randomized lower bounds imply the deterministic ones.

3.2 Lower bounds for SM complexity imply results for PBC

In this section we show implications in the other direction than in Sect. 3.1, i.e., we show how to build positioning and position-based key agreement protocols from functions that have high communication complexity. Unlike in case of Sect. 3.1 we consider these two cases separately (the first one in Theorem 2), and the second one in Theorem 3. Although in principle the second construction would suffice for showing the general implication (as the key agreement is a stronger primitive than the positioning), such a separation makes sense, since the requirements for the communication complexity that we need in Theorem 2 are weaker (and hence Theorem 2 does not directly follow from Theorem 3). Also the conditions on the position of the prover \mathcal{P} are more restrictive in Theorem 3. First, we need the following geometric fact (see [16]).

Lemma 4. *Suppose $D \in \{2, 3\}$. Consider pairwise distinct points $\hat{\mathcal{V}}_1, \dots, \hat{\mathcal{V}}_{D+1}$ positioned in a D -dimensional space, and let $\hat{\mathcal{P}}$ be any point within the D -dimensional simplex S whose vertices are in points $\hat{\mathcal{V}}_1, \dots, \hat{\mathcal{V}}_{D+1}$. Then, for any point $\hat{\mathcal{A}} \neq \hat{\mathcal{P}}$ there exists i such that $\|\hat{\mathcal{V}}_i \hat{\mathcal{A}}\| > \|\hat{\mathcal{V}}_i \hat{\mathcal{P}}\|$.*

We now have the following.

Theorem 2. *Suppose $D \in \{2, 3\}$. Let $\pi : \mathcal{X}_1 \times \dots \times \mathcal{X}_{D+1} \rightarrow \mathcal{Y}$ be an (s, ρ) -hard function in the one-round almost SM model. Let Π be a one-round positioning protocol parametrized by π . Then Π is (s, ρ) -secure for positions within the D -dimensional simplex whose vertices are the positions of the verifiers $\hat{\mathcal{V}}_1, \dots, \hat{\mathcal{V}}_{D+1}$.*

Moreover, something slightly stronger holds, namely the protocol Π is secure even if only \mathcal{V}_k (i.e.: the arbiter in the almost adaptive NOF protocol) receives the message from the prover.

Proof. We say that an adversary \mathcal{A}_i *directly computes* on some X_j if he produces his output exactly when X_j passes through $\hat{\mathcal{A}}_i$. We also recursively define a partial order *dependence* relation “ \preceq ” among the verifiers and the adversaries as follows:

- $\mathcal{V}_i \preceq \mathcal{A}_j$ if the value broadcast by \mathcal{V}_i reaches \mathcal{A}_j not later than when \mathcal{A}_j produces his output. More precisely let T_i be the time when \mathcal{V}_i broadcast X_i and let T_j be the time when \mathcal{A}_j computes his function, then $\mathcal{V}_i \preceq \mathcal{A}_j$ if $\|\hat{\mathcal{A}}_j \hat{\mathcal{V}}_i\|/c \leq T_j - T_i$.
- analogously $\mathcal{A}_i \preceq \mathcal{A}_j$ if the value computed by \mathcal{A}_i reaches \mathcal{A}_j not later than when \mathcal{A}_j produces his output.

(Clearly the dependence relation is a partial order.) Set $k := D + 1$. Let \mathcal{P} be the prover, and $\mathcal{V}_1, \dots, \mathcal{V}_{D+1}$ be the verifiers. Assume the position $\hat{\mathcal{P}}$ of \mathcal{P} is within the D -dimensional simplex whose vertices are the positions of the verifiers $\hat{\mathcal{V}}_1, \dots, \hat{\mathcal{V}}_{D+1}$. For the sake of contradiction assume that Π can be broken by adversaries with retrieval bound s with probability $\rho' > \rho$. This means that one of the adversaries is able to send to the verifier \mathcal{V}_k a message Y equal to

$\pi(X_1, \dots, X_k)$ with probability ρ' (assuming $(X_1, \dots, X_k) \leftarrow \mathcal{X}_1 \times \dots \times \mathcal{X}_k$), and this message arrived to \mathcal{V}_k in time $T + \|\widehat{\mathcal{V}}_k \widehat{\mathcal{P}}\|/c$, where T is the time where all the X_i 's arrive to point $\widehat{\mathcal{P}}$. We now show a one-round almost adaptive protocol for computing π with probability ρ' and communication complexity s . The protocol works as follows.

Let Adv^1 be the set of all adversaries \mathcal{A}_i that depend on some proper subset of verifiers. Our protocol (in the first round) computes all \mathcal{A}_i 's such that $\mathcal{A}_i \in Adv^1$. This can clearly be done since each such \mathcal{A}_i is a function of some proper subset of the input variables X_ℓ .

Let Adv^2 be the set of all the remaining adversaries. Take any $\mathcal{A}_i \in Adv^2$. We know that \mathcal{A}_i depends on *all* the verifiers (as otherwise it would be in Adv^1). Let $\widehat{\mathcal{A}}_i$ be the position of this adversary. By Lemma 4 it has to be the case that for some $\widehat{\mathcal{V}}_j$ we have

$$\|\widehat{\mathcal{V}}_j \widehat{\mathcal{A}}_i\| > \|\widehat{\mathcal{V}}_j \widehat{\mathcal{P}}\|. \quad (6)$$

Any \mathcal{A}_i which depends on $\widehat{\mathcal{V}}_j$ must produce its output after receiving X_j . Therefore (6) implies that the time T_i when \mathcal{A}_i produces its output is such that

$$T_i > T. \quad (7)$$

Consider some $\mathcal{A}_i \in Adv^2$ that is positioned *further* away from \mathcal{V}_k than \mathcal{P} . By (7) the output of such \mathcal{A}_i will not reach \mathcal{V}_k before time $T + \|\widehat{\mathcal{V}}_k \widehat{\mathcal{P}}\|/c$, and hence it is irrelevant for the protocol.

Therefore what remains is to consider the adversaries $\mathcal{A}_i \in Adv^2$ that are *closer* to \mathcal{V}_k than \mathcal{P} . From (7) we have that the computation of such \mathcal{A}_i happens *after* X_k passed through \mathcal{A}_i , and therefore \mathcal{A}_i does not compute on X_k directly. Thus, every computation performed by the \mathcal{A}_i 's from Adv^2 (that are closer to \mathcal{V}_k than \mathcal{P}) can be performed if one knows the set X_1, \dots, X_{k-1} plus the outputs of the \mathcal{A}_j 's from Adv^1 . Hence, it can be done by PLR_k acting as a referee.

Since the SM protocol that we constructed simply simulates the adversaries \mathcal{A}_i by computing their outputs, its communication complexity is s . This completes the proof. \square

We now show Theorem 3 that is similar to Theorem 2, but it holds for position-based key agreement. Observe that for the lemma to hold we need a stronger assumption than in Theorem 2, namely that π is hard in the fully-adaptive SM model. Also, unlike in Theorem 2, we do not specify explicitly what geometric configurations of the verifiers and the prover are allowed. Instead, we simply say that they need to be such that the messages sent by the verifier (see Sect. 2.3) never “meet” at any place other than the position $\widehat{\mathcal{P}}$ of the prover. More precisely, we require that there does not exist time U and place $\widehat{\mathcal{Z}} \neq \widehat{\mathcal{P}}$ such that at time U all the X_i 's are in $\widehat{\mathcal{Z}}$. We refer the reader to [16], Sect. 7.3.1 as to what these valid configurations for the parties are. We now prove the following theorem.

Theorem 3. *Suppose $D \in \{2, 3\}$. Let $\pi : \mathcal{X}_1 \times \dots \times \mathcal{X}_{D+1} \rightarrow \mathcal{Y}$ be an (s, ρ) -strongly-hard function in the fully adaptive SM model. Let Π be a one-round*

key-agreement protocol in D dimensions parametrized by π . Then Π is a (s, ρ) -secure key-agreement protocol assuming all the messages sent by the verifiers never meet at any other place than the position $\widehat{\mathcal{P}}$ of the prover.

Proof. For the sake of contradiction suppose Π is not (s, ρ) -secure, i.e. there exists adversaries $\mathcal{A}_1, \dots, \mathcal{A}_t$, each positioned in $\widehat{\mathcal{A}}_1, \dots, \widehat{\mathcal{A}}_t$ (resp.), such that

$$d(\pi(X_1, \dots, X_{D+1}) \mid A) = \rho' > \rho, \quad (8)$$

where $X_1, \dots, X_{D+1} \leftarrow \mathcal{X}_1 \times \dots \times \mathcal{X}_{D+1}$ are the input variables, and A is a concatenation of the outputs A_i^T of the adv_i^T functions computed by the adversaries when the protocol Π is executed on input (X_1, \dots, X_{D+1}) . To finish the proof we show an NOF protocol with communication complexity s such that

$$d(\pi(X_1, \dots, X_{D+1}) \mid W) = \rho', \quad (9)$$

where W is a concatenation of the messages sent by the players when the NOF protocol is executed on variables (X_1, \dots, X_{D+1}) . Clearly, showing (9) will contradict the assumption that π is (s, ρ) -strongly-hard in the NOF model.

Let \preceq be the partial order from the proof of Lemma 2. The NOF protocol simply computes all the A_i^T starting least \mathcal{A}_i 's in the " \preceq " order, and maintaining the invariant that a given A_j^T can be computed only if the \mathcal{A}_ℓ 's that precede \mathcal{A}_j in this order were computed. By our assumption, its never the case that a \mathcal{A}_i computes directly on all the X_i 's. Therefore this computation can be performed by a (fully adaptive) NOF protocol. It is also easy to see that the output W of this protocol has identical distribution to A . This finishes the proof. \square

4 Concrete constructions

In this section we provide two concrete constructions of positioning and position-based key agreement protocols. This is done using the theory developed in Sect. 3.2, i.e., we first prove that some function π has high communication complexity, and then use this function to construct a position-based protocol. We start with a construction of a positioning protocol that has the "locality" property (see Sect. 2.4), and works in the random oracle model. Note, that using the techniques from [16], this positioning protocol can be transformed into a position-based key agreement, using the computational assumptions discussed in Sect. 2.3. Then, in Sect. 4.2, we show a construction of a position-based key agreement in the plain model (i.e. without a random oracle assumption). This second construction comes without the locality property, i.e., the prover has to read the entire random strings X_i that are sent to him by the verifiers. On the other hand, it has the *on-line-computability* property, i.e., the X_i 's need to be read only once in an on-line fashion, by an a machine with very small memory (see Sect. 2.4).

4.1 Protocols in the Random Oracle Model

As proven in Sect. 3.2 (see Theorem 2), to construct such a protocol it is enough to show a function $\pi : \mathcal{X}_1 \times \dots \times \mathcal{X}_k \rightarrow \mathcal{Y}$ whose one-round almost SM complexity is high. Let t be a security parameter. We assume that the parties have access to t random oracles containing functions $\{H_j : \{0, 1\}^* \rightarrow \{1, \dots, n\}\}_{j=1}^t$ (let \mathcal{H} denote this family of functions). The function π will depend on the functions in \mathcal{H} . Also every party will have access to the functions in \mathcal{H} . More concretely, let $\pi_{k,n}^{\mathcal{H},t} : (\{0, 1\}^t)^{k-1} \times \{0, 1\}^n \rightarrow \{0, 1\}^t$ be a function defined as: $\pi_{k,n}^{\mathcal{H},t}(Z_1, \dots, Z_{k-1}, X) := (X[H_1(Z)], \dots, X[H_t(Z)])$, where $Z = (Z_1 || \dots || Z_{k-1})$.

Our positioning protocol $\Pi_{D,n}^{\mathcal{H},t}$ in D dimensions (for $D \in \{2, 3\}$) is simply the one-round positioning protocol parametrized by $\pi_{D+1,n}^{\mathcal{H},t}$ (see Sect. 2.3). More concretely: it consists of $D+1$ verifiers $\mathcal{V}_1, \dots, \mathcal{V}_{D+1}$ (positioned in $\widehat{\mathcal{V}}_1, \dots, \widehat{\mathcal{V}}_{D+1}$, resp.). Each \mathcal{V}_i (for $i \leq D$) sends a random $Z_i \leftarrow \{0, 1\}^t$ in time $T - \|\widehat{\mathcal{V}}_i \widehat{\mathcal{P}}\|/c$ (where $\widehat{\mathcal{P}}$ is the claimed position of the prover), and \mathcal{V}_{D+1} sends a random $X \leftarrow \{0, 1\}^n$ (in time $T - \|\widehat{\mathcal{V}}_{D+1} \widehat{\mathcal{P}}\|/c$). All the messages arrive to \mathcal{P} in time T . Then, \mathcal{P} computes $X[H_1(Z)], \dots, X[H_t(Z)]$, and sends the result back to \mathcal{V}_{D+1} , who checks if the result is correct (at the end of this section we discuss how this check can be done very efficiently). The security of $\Pi_{D,n}^{\mathcal{H},t}$ follows directly from Theorem 3, and the following fact.

Lemma 5. *Consider an almost adaptive one-round SM protocol $\text{PLR}_1, \dots, \text{PLR}_k$ with PLR_k being the referee, and every player having random oracle access to the functions in \mathcal{H} . Let βn denote the total communication complexity of this protocol (where $n \in \mathbb{N}$ and $\beta < 1$ is some constant) and let q be the number of times the parties query the random oracles. Assume q is polynomial in t and n is any function of t such that $n \geq t$. Let Y denote the output of PLR_k . Then we have*

$$\mathbb{P}\left(Y = \pi_{k,n}^{\mathcal{H},t}(Z_1, \dots, Z_{k-1}, X)\right) \leq \text{negl}(t), \quad (10)$$

where negl denotes a negligible function, the probability in (10) is taken over random $X \leftarrow \{0, 1\}^n$, $(Z_1, \dots, Z_{k-1}) \leftarrow (\{0, 1\}^t)^{k-1}$, and the random choice of the functions on \mathcal{H} .

Proof. Suppose we have an almost adaptive one-round SM protocol $\text{PLR}_1, \dots, \text{PLR}_k$ (with PLR_k being the referee) such that the probability in (10) is non-negligible. Recall the guessing game from Sect. 2.1. We now show how to use $\text{PLR}_1, \dots, \text{PLR}_k$ to construct a pair of functions $\text{compress} : \{0, 1\}^n \rightarrow \{0, 1\}^{\beta n}$ and $\text{guess} : \{1, \dots, n\}^t \times \{0, 1\}^{\beta n} \rightarrow \{0, 1\}^t$ such that the probability that $\text{guess}(R, \text{compress}(X)) = (X[R_1], \dots, X[R_t])$ is non-negligible in t , where $X \leftarrow \{0, 1\}^n$ and $R = (R_1, \dots, R_t) \leftarrow \{1, \dots, n\}^t$. Since by Lemma 3 we know that this is impossible, we will obtain that the probability in (10) has to be negligible.

The functions compress and guess that we construct are randomized, i.e., they depend on some external fresh randomness. In particular, we will assume that the hash functions \mathcal{H} that the players have access to (via the random oracle) were sampled in advance. Of course, such sampling cannot be done efficiently

(since the set of all such functions is of exponential size), but this is ok, since our construction is anyway information-theoretic (note that Lemma 3 does not involve any complexity-theoretic assumptions). We will later argue why the assumption about the availability of external randomness can be done without loss of generality. First, however, let us present the definitions of the functions **compress** and **guess**.

The function **compress** is defined as follows. First it samples $(Z_1, \dots, Z_{k-1}) \leftarrow (\{0, 1\}^t)^{k-1}$. Then, on input (X, R_1, \dots, R_{k-1}) it produces as output a tuple (V_1, \dots, V_{k-1}) , where each V_i is equal to the output of player PLR_i on input $(R_1, \dots, R_{i-1}, R_{i+1}, \dots, R_{k-1}, X)$ (recall that in this model the referee PLR_k does not produce any output in the first phase). Note that simulating the PLR_i 's may require replying to their random oracle queries. We reply to each such query using the hash functions \mathcal{H} that were sampled beforehand. Observe that $|(V_1, \dots, V_{k-1})| \leq \beta n$, and therefore **compress** can fit this output in the set $\{0, 1\}^{\beta n}$.

On input (R_1, \dots, R_t) and X the function **guess** does the following. It simulates the referee PLR_k on input (Z_1, \dots, Z_{k-1}) (which are the values that were already sampled by **compress**). It answers all the random oracle queries using \mathcal{H} , with one important exception. Namely, every query of a form $(Z_1 || \dots || Z_{k-1})$ to an oracle containing a hash function H_j (for $j = 1, \dots, t$) is answered with R_j .

Now, let \mathcal{E} denote the event that it never happened that any of the $\text{PLR}_1, \dots, \text{PLR}_{k-1}$ queried any of the random oracles on $(Z_1 || \dots || Z_{k-1})$. It is easy to see that we have the following:

$$\begin{aligned} & \mathbb{P} \left(Y = \pi_{k,n}^{\mathcal{H},t}(Z_1, \dots, Z_{k-1}, X) \mid \mathcal{E} \right) \\ &= \mathbb{P}(\text{guess}(R, \text{compress}(X)) = (X[R_1], \dots, X[R_t]) \mid \mathcal{E}). \end{aligned} \quad (11)$$

This is because if \mathcal{E} occurred then the functions **compress** and **guess** perfectly “emulated” the execution of $\text{PLR}_1, \dots, \text{PLR}_k$. Observe that here we use the assumption that the R_j 's are uniform, which implies that our answers to the “ $(Z_1 || \dots || Z_{k-1})$ ” queries are indistinguishable from the answers of the “real” random oracle. Of course, this would not be true if such a query was earlier asked by one of $\text{PLR}_1, \dots, \text{PLR}_{k-1}$, but this did not happen, since in (11) we condition on the event \mathcal{E} .

On the other hand, it is clear that $\mathbb{P}(-\mathcal{E}) \leq q/2^t$. This is because querying the oracle on “ $(Z_1 || \dots || Z_{k-1})$ ” requires the knowledge of all the Z_i 's, and every PLR_i (for $i = 1, \dots, k-1$) does not know one of them. Hence the probability that any PLR_i guesses “ $(Z_1 || \dots || Z_{k-1})$ ” in one query is 2^{-t} (remember that each of them is uniformly random on $\{0, 1\}^t$). Consequently, the probability that it guesses it in *at least one* of its q queries is at most $q/2^t$. Since we assumed that q is polynomial in t , thus we get that $\mathbb{P}(-\mathcal{E}) \leq \text{negl}(t)$. Combining it with (11) we obtain

$$\mathbb{P} \left(Y = \pi_{k,n}^{\mathcal{H},t}(Z_1, \dots, Z_{k-1}, X) \right) \quad (12)$$

$$\leq \mathbb{P}(\text{guess}(R, \text{compress}(X)) = (X[R_1], \dots, X[R_t])) + \text{negl}(t). \quad (13)$$

Thus, since we assumed that (12) is non-negligible, we obtain that the probability in (13) is non-negligible.

What remains is to describe how to “derandomize” the **compress** and **guess** functions that we constructed. This can be done via a very standard argument. Since the inequality (13) holds when the probability is computed *including* the internal randomness ρ of **compress** and **guess** thus there has to exist a concrete value ρ_0 such that (13) holds if we fix ρ to ρ_0 . We can therefore derandomize these functions by simply “hardwiring” these randomness into them. This finishes the proof. \square

Let us also discuss the nature of the $\pi_{k,n}^{\mathcal{H},t}$ function, focusing on the (simplest) case when $t = 1$, i.e., only one bit is produced as output. The reader familiar with the communication complexity literature may observe that this function is similar to so-called *shift function* [28], and more general notion called the *general addressing function (GAF)* [31,4]. The shift function is defined very similarly to $\pi_{k,n}^{\mathcal{H},1}$, except that the Z_i ’s take values in the \mathbb{Z}_n group, and H_1 is defined as $H(Z_1, \dots, Z_n) := X[Z_1 + \dots + Z_{k-1}]$ (in case of GAF we can also have groups other than \mathbb{Z}_n). Somewhat surprisingly it appears very hard to prove the lower bounds for the SM complexity in this model. The only known non-trivial lower bound in the shift function is $\Omega(n^{1/k})$ [28,31]. Moreover, sublinear upper bounds on this complexity are known [31,30,1,2]. The hardness of this problem can in some sense serve as a justification for the use of the random oracles in our construction. Theorem 3 and Lemma 5 together imply the following.

Corollary 1. *For any $\beta < 1$ and for $n > t$ the protocol $\Pi_{D,n}^{\mathcal{H},t}$ is a $(\beta n, \text{negl}(t))$ -secure positioning protocol for positions within the D -dimensional simplex whose vertices are the positions of the protocol’s verifiers.*

Let us also now mention that in a practical implementation one can let the verifiers choose the Z_i ’s in advance. Therefore \mathcal{V}_{D+1} can compute $H_i(Z_i)$ ’s and store only the $X[H_i(Z_i)]$ ’s. Thus, the storage requirements of this protocol are very low.

4.2 Protocols in the Plain Model

In this section we propose an alternative construction of positioning and key agreement protocols. The protocols presented in this section are online computable (see Sect. 2.4), and do not require the random oracle assumption. Let us first recall the definition of the generalized inner product function [5]. Let $\mathbb{F} = \text{GF}(2^m)$ be a finite field (for simplicity we restrict ourselves to the Galois fields of order 2^m , but our results can be generalized to arbitrary finite fields). For some natural parameters ℓ and k (such that $k \geq 2$) define the *generalized inner product (GIP)* function as $\text{GIP}_{\ell,k} : (\mathbb{F}^\ell)^k \rightarrow \mathbb{F}$ as $\text{GIP}_{\ell,k}^{\mathbb{F}}((x_1^1, \dots, x_\ell^1), \dots, (x_1^k, \dots, x_\ell^k)) = \sum_{i=1}^{\ell} \prod_{j=1}^k x_i^j$.

The positioning and the position-based key agreement protocols (in $D \in \{2, 3\}$ dimensions), denoted $\Gamma_{\ell,D,t}^{\text{pos}}$ and $\Gamma_{\ell,D,t}^{\text{ka}}$ (resp.), are simply the one-round

protocols parameterized by $\text{GIP}_{\ell, D+1}^{\mathbb{F}}$ (see Sect. 2.3), i.e., the verifiers $\mathcal{V}_1, \dots, \mathcal{V}_{D+1}$ broadcast random strings $X_i \leftarrow \mathbb{F}^\ell$, and the prover computes $\text{GIP}(X_1, \dots, X_{D+1})$, which he either keeps as the agreed key, or broadcasts back to the verifiers (depending on whether the protocol is for key agreement or for positioning). The verifiers compute $\text{GIP}(X_1, \dots, X_{D+1})$ and keep it as the agreed key (in the first case), or simply check if it is identical to what they got from the prover (in the second case). We now have the following lemma that states that GIP is hard in the fully adaptive model. Note that this lemma implies hardness in the almost adaptive one-round SM model (since this model is more restrictive), and hence, together with Theorems 2 and 3, implies security of the $\Gamma_{\ell, D, t}^{\text{pos}}$ and $\Gamma_{\ell, D, t}^{\text{ka}}$ protocols. The communication complexity of the GIP function has been studied in multiple papers [5,6,32,23,22], but up to our knowledge, not in the strong randomized settings that we need in this work. Our proof is a rather straightforward adaptation of the techniques from this prior work.

Lemma 6. *Suppose $\mathbb{F} = \text{GF}(2^m)$ (for any m such that $2^m \geq k^{1+\xi}$ for some $\xi > 0$). Then for every ℓ, k , the $\text{GIP}_{\ell, k}^{\mathbb{F}}$ function is (s, δ) -strongly hard in the fully adaptive model, for some $s = \Omega(m\ell/2^k)$ and $\delta = \text{negl}(\ell)$.*

Proof. Consider an arbitrary fully adaptive protocol $(\text{PLR}_1, \dots, \text{PLR}_k)$. Let s denote its communication complexity. Suppose that $\vec{X}^1, \dots, \vec{X}^k$ are sampled uniformly and independently, each from \mathbb{F}^ℓ . Let V denote the sequence of all the messages that were broadcast by the parties during the execution of the protocol on input $(\vec{X}^1, \dots, \vec{X}^k)$. Let $Y := \text{GIP}_{\ell, k}^{\mathbb{F}}(\vec{X}^1, \dots, \vec{X}^k)$. We will now treat $Y \in \text{GF}(2^m)$ as bit-strings of length m . We start with the following.

Claim. For any $i \in 1, \dots, m$ and $s = \Omega(m\ell/2^k)$ we have that

$$d(Y[i] \mid Y[1, \dots, i-1], V) \leq \text{negl}(\ell). \quad (14)$$

Proof (Proof of the Claim). We use the results of [5] which introduced the so-called *multiparty communication complexity with help*. More precisely, in [5] the authors consider protocols where the players can obtain an extra “help” from an external entity in a form of a function H that gets as input all the inputs of all the players, the only restriction being that the output of H has to be one bit shorter than the output of the computed function. Hence, in our case H is any function of a type $H : (\mathbb{F}^\ell)^k \rightarrow \{0, 1\}^{m-1}$. What they prove in their Lemma 3.3 can be translated to our notation as follows:

For any protocol whose communication complexity is at most

$$\log \left(\frac{1/2 - \epsilon}{\Gamma(f, \mathcal{C})} \right) \quad (15)$$

(we will comment on the “ $\Gamma(f, \mathcal{C})$ ” term in a moment) and for any $H : (\mathbb{F}^\ell)^k \rightarrow \{0, 1\}^{m-1}$ and any function α we have that

$$\mathbb{P} \left(\text{GIP}_{\ell, k}^{\mathbb{F}}(\vec{X}^1, \dots, \vec{X}^k) = \alpha(H(\vec{X}^1, \dots, \vec{X}^k), V) \right) \leq 1 - \epsilon. \quad (16)$$

(provided $2^m \geq k^{1+\xi}$ for some $\xi > 0$).

Above $\Gamma(f, \mathcal{C})$ is a value called *the strong discrepancy of f in \mathcal{C}* (for this discussion it is irrelevant what \mathcal{C} is). Moreover, as inspection of the proof of Corollary 4.12 [5] shows we have that

$$\log(1/\Gamma(f, \mathcal{C})) \geq \Omega(m\ell/2^k). \quad (17)$$

Now, set $\epsilon := 1/2 - \sqrt{\Gamma(f, \mathcal{C})}$. It is easy to see that (15) now becomes equal to

$$\log(1/\sqrt{\Gamma(f, \mathcal{C})}) \geq \Omega(m\ell/2^k).$$

This also implies that $\epsilon - 1/2$ is negligible in ℓ . Moreover, by Lemma 2, we have that

$$d(\text{GIP}_{\ell, k}^{\mathbb{F}}(\vec{X}^1, \dots, \vec{X}^k) \mid H(\vec{X}^1, \dots, \vec{X}^k), V) \leq 2(1 - \epsilon) - 1 \leq \text{negl}(\ell), \quad (18)$$

Now set $H(\vec{X}^1, \dots, \vec{X}^k) := (Y[1, \dots, i-1], Y[i+1], \dots, Y[m])$. Then, (18) becomes

$$\begin{aligned} \text{negl}(\ell) &\geq d(Y \mid Y[1, \dots, i-1], Y[i+1], \dots, Y[m], V) \\ &\geq d(Y[i] \mid Y[1, \dots, i-1], V), \end{aligned} \quad (19)$$

where (19) follows from Lemma 2. Hence (14) is proven.

To finish the proof of Lemma 6 we just apply the chain-rule for the statistical distance (Lemma 1), obtaining

$$d(Y \mid V) \leq m \cdot \text{negl}(\ell) = \text{negl}(\ell).$$

We therefore obtain that for any protocol with the communication complexity $\Omega(m\ell/2^k)$ we have $d(\text{GIP}_{\ell, k}^{\mathbb{F}}(\vec{X}^1, \dots, \vec{X}^k) \mid V) \leq \text{negl}(\ell)$, and the lemma is proven. \square

Now, combining Lemma 6 with Theorems 2 and 3 we obtain the following.

Corollary 2. *For $D \in \{2, 3\}$ and for k, m , and ℓ as in Lemma 6, we have that $\Gamma_{\ell, D, t}^{\text{pos}}$ is one-round $(\Omega(m\ell), \text{negl}(\ell))$ -secure positioning protocol in D dimensions for positions inside of a simplex determined by the verifiers, and $\Gamma_{\ell, D, t}^{\text{ka}}$ is a one-round $(\Omega(m\ell), \text{negl}(\ell))$ -secure key agreement protocol in D dimensions for positions such that the messages sent by the verifiers never meet at any other position than the one claimed by the prover (see [16], Sect. 7.3.1).*

Since the generalized inner product is a multi-source extractor, the reader might be tempted to think that our construction works when $\text{GIP}^{\ell, k}$ is replaced with any k -source extractor. We note that this is not the case, as the generalized inner product has additional properties, that multi-source extractors do not have. Namely the multi-source extractors require that their inputs are fully independent (conditioned on adversary's information), which is not the case for GIP.

4.3 Practical considerations for the GIP-based protocol

Note that, unlike in the case of protocol $\Pi_{D,n}^{\mathcal{H},t}$ (see remark after Corollary 1), there is no simple trick to avoid the need for the verifiers to store large amounts of data (the X_i 's), as long as we want the protocols to be information-theoretically secure. However, if we move to the “computational world” we can simply let the X_i 's be generated pseudorandomly: for $i = 1, \dots, D + 1$ sample a short random seed S_i , and let $X_i := \text{prg}(S_i)$, where prg is a pseudorandom generator. In this case, the verifiers need to store only the S_i 's. Also, instead of sending the X_i 's (via a private channel) to each other, they can just send the S_i .

References

1. Andris Ambainis. Upper bounds on multiparty communication complexity of shifts. In Claude Puech and Rüdiger Reischuk, editors, *STACS 96, 13th Annual Symposium on Theoretical Aspects of Computer Science, Grenoble, France, February 22-24, 1996, Proceedings*, volume 1046 of *Lecture Notes in Computer Science*, pages 631–642. Springer, 1996.
2. Andris Ambainis and Satyanarayana V. Lokam. Improved upper bounds on the simultaneous messages complexity of the generalized addressing function. In Gaston H. Gonnet, Daniel Panario, and Alfredo Viola, editors, *LATIN 2000: Theoretical Informatics, 4th Latin American Symposium, Punta del Este, Uruguay, April 10-14, 2000, Proceedings*, volume 1776 of *Lecture Notes in Computer Science*, pages 207–216. Springer, 2000.
3. Yonatan Aumann and Michael O. Rabin. Information theoretically secure communication in the limited storage space model. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 65–79, Santa Barbara, CA, USA, August 15–19, 1999. Springer, Heidelberg, Germany.
4. László Babai, Anna Gál, Peter G. Kimmel, and Satyanarayana V. Lokam. Communication complexity of simultaneous messages. *SIAM J. Comput.*, 33(1):137–166, January 2004.
5. László Babai, Thomas P. Hayes, and Peter G. Kimmel. The cost of the missing bit: Communication complexity with help. *Combinatorica*, 21(4):455–488, 2001.
6. László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Comput. Syst. Sci.*, 45(2):204–232, 1992.
7. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73, Fairfax, Virginia, USA, November 3–5, 1993. ACM Press.
8. Stefan Brands and David Chaum. Distance-bounding protocols (extended abstract). In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 344–359, Lofthus, Norway, May 23–27, 1994. Springer, Heidelberg, Germany.
9. G. Brassard. Quantum information: The conundrum of secure positioning. *Nature*, 479:307–308, November 2011.
10. Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014.

11. Christian Cachin and Ueli M. Maurer. Unconditional security against memory-bounded adversaries. In Burton S. Kaliski Jr., editor, *CRYPTO'97*, volume 1294 of *LNCS*, pages 292–306, Santa Barbara, CA, USA, August 17–21, 1997. Springer, Heidelberg, Germany.
12. S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1917–1928 vol. 3, March 2005.
13. David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard J. Lipton, and Shabsi Walfish. Intrusion-resilient key exchange in the bounded retrieval model. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 479–498, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Heidelberg, Germany.
14. Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Phys. Rev. A*, 92:052304, Nov 2015.
15. Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In *Proc. 15th Annual ACM Symposium on the Theory of Computing*, pages 94–99, 1983.
16. Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position-based cryptography. *SIAM Journal on Computing*, 43(4):1291–1341, 2014.
17. Stefan Dziembowski. Intrusion-resilience via the bounded-storage model. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 207–224, New York, NY, USA, March 4–7, 2006. Springer, Heidelberg, Germany.
18. Stefan Dziembowski and Ueli M. Maurer. Tight security proofs for the bounded-storage model. In *34th ACM STOC*, pages 341–350, Montréal, Québec, Canada, May 19–21, 2002. ACM Press.
19. Stefan Dziembowski and Ueli M. Maurer. Optimal randomizer efficiency in the bounded-storage model. *Journal of Cryptology*, 17(1):5–26, January 2004.
20. Stefan Dziembowski and Krzysztof Pietrzak. Intrusion-resilient secret sharing. In *48th FOCS*, pages 227–237, Providence, USA, October 20–23, 2007. IEEE Computer Society Press.
21. Stefan Dziembowski and Maciej Zdanowicz. Position-based cryptography from noisy channels. In David Pointcheval and Damien Vergnaud, editors, *AFRICACRYPT 14*, volume 8469 of *LNCS*, pages 300–317, Marrakesh, Morocco, May 28–30, 2014. Springer, Heidelberg, Germany.
22. Jeff Ford and Anna Gál. Hadamard tensors and lower bounds on multiparty communication complexity. *Computational Complexity*, 22(3):595–622, 2013.
23. Fan Chung Graham. Quasi-random hypergraphs revisited. *Random Struct. Algorithms*, 40(1):39–48, 2012.
24. Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, Cambridge, 1997.
25. Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology*, 17(1):27–42, January 2004.
26. Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.
27. Tal Moran, Ronen Shaltiel, and Amnon Ta-Shma. Non-interactive timestamping in the bounded-storage model. *Journal of Cryptology*, 22(2):189–226, April 2009.
28. Noam Nisan and Avi Wigderson. Rounds in communication complexity revisited. In *23rd ACM STOC*, pages 419–429, New Orleans, Louisiana, USA, May 6–8, 1991. ACM Press.

29. Noam Nisan and David Zuckerman. Randomness is linear in space. *J. Comput. Syst. Sci.*, 52(1):43–52, February 1996.
30. Pavel Pudlák. Unexpected upper bounds on the complexity of some communication games. In Serge Abiteboul and Eli Shamir, editors, *Automata, Languages and Programming, 21st International Colloquium, ICALP94, Jerusalem, Israel, July 11-14, 1994, Proceedings*, volume 820 of *Lecture Notes in Computer Science*, pages 1–10. Springer, 1994.
31. Pavel Pudlák, Vojtech Rödl, and Jiří Sgall. Boolean circuits, tensor ranks, and communication complexity. *SIAM Journal on Computing*, 26(3):605–633, 1997.
32. Ran Raz. The bns-chung criterion for multi-party communication complexity. *Computational Complexity*, 9(2):113–122, 2000.
33. Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *Proceedings of the 2Nd ACM Workshop on Wireless Security, WiSe '03*, pages 1–10, New York, NY, USA, 2003. ACM.
34. Christian Schaffner. Position-based quantum cryptography. webpage <http://homepages.cwi.nl/~schaffne/positionbasedqcrypto.php>, accessed on Feb 17, 2016.
35. Dominique Unruh. Quantum position verification in the random oracle model. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 1–18, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.
36. Salil P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, January 2004.
37. Adnan Vora and Mikhail Nesterenko. Secure location verification using radio broadcast. In *Proceedings of the 8th International Conference on Principles of Distributed Systems, OPODIS'04*, pages 369–383, Berlin, Heidelberg, 2005. Springer-Verlag.