Exponential Correlated Randomness Is Necessary in Communication-Optimal Perfectly Secure Two-Party Computation

Keitaro Hiwatashi
The University of Tokyo, Japan
National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan

Koji Nuida
Kyushu University, Japan
National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan

Abstract

Secure two-party computation is a cryptographic technique that enables two parties to compute a function jointly while keeping each input secret. It is known that most functions cannot be realized by information-theoretically secure two-party computation, but any function can be realized in the correlated randomness (CR) model, where a trusted dealer distributes input-independent CR to the parties beforehand. In the CR model, three kinds of complexities are mainly considered; the size of CR, the number of rounds, and the communication complexity.

Ishai et al. (TCC 2013) showed that any function can be securely computed with optimal online communication cost, i.e., the number of rounds is one round and the communication complexity is the same as the input length, at the price of exponentially large CR. In this paper, we prove that exponentially large CR is necessary to achieve perfect security and online optimality for a general function and that the protocol by Ishai et al. is asymptotically optimal in terms of the size of CR. Furthermore, we also prove that exponentially large CR is still necessary even when we allow multiple rounds while keeping the optimality of communication complexity.

2012 ACM Subject Classification Security and privacy → Cryptography

Keywords and phrases Secure Computation, Correlated Randomness, Lower Bound

Digital Object Identifier 10.4230/LIPIcs.ITC.2023.18

Funding Supported by JST CREST Grant Number JPMJCR2113.
Keitaro Hiwatashi: This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)," which was supported by the Ministry of Internal Affairs and Communications, Japan. The author was also partially supported by JSPS KAKENHI Grant Number JP21J20186 and JP22KJ0546.
Koji Nuida: Supported by JSPS KAKENHI Grant Number JP19H01109, JP22K11906, and JST AIP Acceleration Research JPMJCR22U5.

1 Introduction

Secure multi-party computation (MPC) is a cryptographic technique that enables some parties to compute a function jointly while keeping each input secret. Secure multi-party computation has been extensively studied since Yao advocated it in the 1980s [25]. From a theoretical point of view, Kushilevitz [18] gave a complete characterization of a function class that can be realized by a two-party protocol perfectly secure against a semi-honest adversary, and Chor and Kushilevitz [7] gave a complete characterization of a boolean function that can be realized by a perfectly secure multi-party protocol in the dishonest-majority and semi-honest adversary setting. From their result, most functions (including even simple functions such as the AND function) cannot be securely realized by a multi-party protocol in the dishonest-majority setting. However, if we are allowed to use *correlated randomness* (CR, in short), any function can be securely realized. Indeed, by using additive secret sharing and Beaver Triple [2], we can securely compute any boolean circuits. For simplicity, we focus on the two-party case and consider a semi-honest adversary in this paper.

The CR model, also known as a preprocessing model, is a model where we are allowed to use CR, which is a randomness independent of an input of a function. In the CR model, a protocol is divided into two phases: the offline phase and the online phase. In the offline phase, CR is generated and distributed to the parties. In the online phase, the parties securely compute a function with their input and the CR distributed in the offline phase. In most cases, the online phase consists of lightweight computation and is fast enough, and therefore many recent works (e.g., [1, 5, 6, 9, 17]) adopted the CR model. Some papers (e.g., [1, 5, 6]) assume that a trusted dealer generates and distributes CR in the offline phase. In the CR model, three kinds of complexities are mainly considered: the size of CR, the number of rounds of the online phase, and the communication complexity of the online phase. By using Beaver Triple, we can construct a secure protocol for a boolean circuit C with $O(s)$-bit CR, $O(\mathrm{depth}(C))$ rounds, and $O(s)$-bit communication complexity, where s is the size of C and $\mathrm{depth}(C)$ is the depth of C. It is a major open problem whether it is possible to make the communication complexity sublinear in the circuit size.

Ishai et al. [16] partially solved the above open problem by developing a one-time truth table. In their protocol, the communication complexity is independent of the circuit size and is linear in the input length. Furthermore, their protocol using a one-time truth table achieves online optimality, i.e., the number of rounds is one round and the communication complexity is the same as the input length. However, the size of CR of their protocol is exponential in the input length.[1] Indeed, their protocol needs $O(N^2)$-bit CR where N is the cardinality of their input domain (which is exponential in the input length). Beimel et al. [4], the full version of [3], reduced the size of CR to $O(N^{1/2})$ bits, at the price of increasing the number of rounds to two rounds and the communication complexity to $O(N^{1/2})$ bits. Although there might have to be some trade-off among the three kinds of complexities mentioned above, the quantitative property of such a trade-off has not been well investigated in the literature. For example, focusing on Ishai et al.'s protocol, it is even not known whether the size of CR can be reduced to $o(N^2)$ bits while keeping the single round and optimal communication complexity.

1.1 Our Contributions

In this paper, we show some trade-offs by giving lower bounds of the size of CR in *online-restricted* settings where online communication cost (i.e., the number of rounds and the communication complexity) is restricted. Here we assume "shared-output" setting that the outputs (y_0, y_1) by two parties satisfy that the function value is reconstructed by $y_0 + y_1$ where '+' is some additive group operation. We discuss this setting in Section 1.2.

More concretely, we give (exponential) lower bounds of the size of CR in two types of online-restricted settings: online-optimal setting and communication-optimal setting. As described above, "online-optimal" means that the number of rounds is one round and the communication

[1] It is still an open problem whether it is possible to make the communication complexity sublinear in the circuit size in the setting that the time complexity (and therefore the size of CR) is polynomial in the input length.

complexity is the same as the input length. On the other hand, "communication-optimal" means that we allow multiple rounds but the total size of messages sent by a party to the other party during the multiple rounds is still equal to the size of the input of the party.

Our results are summarized as follows, where N is the cardinality of the domain $\mathcal{X}$:

1. We prove that there exists a function $f\colon \mathcal{X} \times \mathcal{X} \to \{0,1\}^2$ such that any *online-optimal* perfectly secure two-party protocol for f needs CR of at least $(N-1)^2 = \Omega(N^2)$ bits.
2. We prove that there exists a function $f\colon \mathcal{X} \times \mathcal{X} \to \{0,1\}^2$ such that any *communication-optimal* perfectly secure two-party protocol for f needs CR of at least $N-1 = \Omega(N)$ bits.

The first result implies that the one-time truth table [16], which is an online-optimal secure two-party protocol with $O(N^2)$-bit CR, is asymptotically optimal among online-optimal ones for general functions in terms of the size of CR.

1.2 Shared-output vs. Plain-output

Some papers, including Ishai et al. [16] and Beimel et al. [4], considered the "plain-output" setting, in which both parties output the function value itself, not the share of the function value. The shared-output setting is more general in the sense that shared-output protocols can be converted into plain-output protocols by adding a reconstruction step. The protocols in both Ishai et al. [16] and Beimel et al. [4] contained shared-output protocols in the sense that their protocols can be divided into two steps: Both protocols (Fig.1 in [16] and Theorem D.1 in [4]) compute the share of the function value first, and then reconstruct the function value by exchanging the shares.

Furthermore, the shared-output setting is suitable for the situation where the protocol is used as a subprotocol in another MPC protocol since the shared output does not leak any information about the function value itself. Due to this composability, many recent MPC protocols (e.g., [1, 5, 6, 24]) adopt the shared-output setting.

1.3 Related Work

The prior work most relevant to our setting is a combination of [6] and [14]. In [6], Boyle et al. showed that distributed point functions (DPF) can be constructed from an online-optimal (shared-output) equality protocol. In more detail, they showed that given an online-optimal shared-output equality protocol with r-bit CR, a DPF scheme with $O(r)$-bit key size can be constructed[2]. On the other hand, as Gilboa et al. [14] mentioned, the key size of an information-theoretic DPF scheme is at least $2^{\Omega(\log N)} = N^{\Omega(1)}$ bits, where N corresponds to the cardinality of the domain of point functions. Combining it with the reduction by Boyle et al., it can be proved that the size of CR of an online-optimal protocol for the equality function $EQ\colon [N] \times [N] \to \{0,1\}$ is at least $N^{\Omega(1)}$ bits. To the best of our knowledge, this is the only prior result showing an exponential lower bound of the size of CR.

There are several results on the randomness complexity not on the size of CR (e.g., [13, 15, 19, 20, 21, 22, 23]). We note that they consider MPC in the plain model (not in the CR model) and with more than two parties. There are also several results on the communication complexity in multi-party computation (e.g., [8, 10, 11, 12]).

[2] Though they only considered the computational security, their reduction can be applied also in the information-theoretic setting.

1.4 Organization

We provide the notations used in this paper and the definitions of online- or communication-optimal secure two-party protocols in Section 2. We provide a technical overview in Section 3. In Section 4, we prove the lower bound in the online-optimal setting. We prove the lower bound in the communication-optimal setting in Section 5.

2 Preliminaries

2.1 Notations

For an integer N, let $[N]$ denote the set $\{0, 1, \ldots, N-1\}$. Let P_0 and P_1 be the parties participating in a two-party protocol. We use $\Delta^{k\times\ell}(i,j)$ to denote the $k \times \ell$ matrix for which the (i,j)-th element is 1 and the other elements are 0. We let $\mathbb{G}$ denote an Abelian group, $+$ denote the operation on $\mathbb{G}$, and 0 denote the identity element of $\mathbb{G}$. For a boolean value $b \in \{0,1\}$, let $\bar{b}$ be the negation of b. For a matrix M, $M[x,y]$ denotes the (x,y)-th element of M.

2.2 Online-Optimal Protocols

▶ **Definition 1.** *An online-optimal secure two-party protocol for $f\colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ with correlated randomness $\mathcal{CR} \subseteq \mathcal{R}_0 \times \mathcal{R}_1$ consists of three algorithms* $(\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ *with following syntax:*

- Gen*:* Gen *outputs a correlated randomness $(r_0, r_1) \in \mathcal{CR} \subseteq \mathcal{R}_0 \times \mathcal{R}_1$ without taking any input.*
- Msg*: Taking party id $b \in \{0,1\}$, input $x \in \mathcal{X}_b$, and randomness $r \in \mathcal{R}_b$,* Msg *(deterministically) outputs a message $m \in \mathcal{M}_b$.*
- Eval*: Taking party id $b \in \{0,1\}$, input $x \in \mathcal{X}_b$, randomness $r \in \mathcal{R}_b$, and message $m \in \mathcal{M}_{\bar{b}}$,* Eval *(deterministically) outputs $g \in \mathbb{G}$.*

satisfying the following three requirements:

- *Optimality: For $b \in \{0,1\}$, the size of $\mathcal{M}_b$ is equal to the size of $\mathcal{X}_b$.*
- *Correctness: For all $(x_0, x_1) \in \mathcal{X}_0 \times \mathcal{X}_1$,*

$$\Pr\left[g_0 + g_1 = f(x_0, x_1) \;\middle|\; \begin{array}{c} (r_0, r_1) \leftarrow \mathsf{Gen}, \\ m_0 \leftarrow \mathsf{Msg}(0, x_0, r_0), \\ m_1 \leftarrow \mathsf{Msg}(1, x_1, r_1), \\ g_0 \leftarrow \mathsf{Eval}(0, x_0, r_0, m_1), \\ g_1 \leftarrow \mathsf{Eval}(1, x_1, r_1, m_0) \end{array} \right] = 1.$$

- *Security: For $b \in \{0,1\}$, the distribution of $\{(r_b, \mathsf{Msg}(\bar{b}, x, r_{\bar{b}}))\}_{(r_0,r_1)\leftarrow\mathsf{Gen}}$ is independent of $x \in \mathcal{X}_{\bar{b}}$.*

Without loss of generality, we assume that the randomness space is not redundant. That is, we assume that the probability $\Pr[(r_0, r_1) \leftarrow \mathsf{Gen}]$ is positive for all $(r_0, r_1) \in \mathcal{CR}$ and that for all $r_0 \in \mathcal{R}_0$ ($r_1 \in \mathcal{R}_1$, resp.), there exists $r_1 \in \mathcal{R}_1$ ($r_0 \in \mathcal{R}_0$, resp.) such that $(r_0, r_1) \in \mathcal{CR}$.

2.3 Communication-Optimal Protocols

▶ **Definition 2.** *A (T-round) communication-optimal secure two-party protocol for $f\colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ with correlated randomness $\mathcal{CR} \subseteq \mathcal{R}_0 \times \mathcal{R}_1$ consists of algorithms* $(\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ *with following syntax:*

- Gen*:* Gen *outputs a correlated randomness* $(r_0, r_1) \in \mathcal{CR} \subseteq \mathcal{R}_0 \times \mathcal{R}_1$ *without taking any input.*
- Msg*: Taking* $(x_0, r_0) \in \mathcal{X}_0 \times \mathcal{R}_0$ *and* $(x_1, r_1) \in \mathcal{X}_1 \times \mathcal{R}_1$, Msg *(deterministically) outputs messages* $(\mathrm{mes}_1, \dots, \mathrm{mes}_T) \in M^1 \times \cdots \times M^T$*. Here* mes_i *is a message sent to* $P_{i \bmod 2}$ *from* $P_{i+1 \bmod 2}$ *which is determined by* $P_{i+1 \bmod 2}$*'s input* $x_{i+1 \bmod 2}$*,* $P_{i+1 \bmod 2}$*'s randomness* $r_{i+1 \bmod 2}$ *and the messages* $(\mathrm{mes}_1, \dots, \mathrm{mes}_{i-1})$ *exchanged so far.*
- Eval*: Taking party id* $b \in \{0, 1\}$*, input* $x \in \mathcal{X}_b$*, randomness* $r \in \mathcal{R}_b$*, and messages* $(\mathrm{mes}_1, \dots, \mathrm{mes}_T)$ *exchanged so far,* Eval *(deterministically) outputs* $g \in \mathbb{G}$*.*

satisfying the following three requirements:

- *Optimality: For* $b \in \{0, 1\}$*, the size of the message space* $\mathcal{M}_b$ *is equal to that of the input space* $\mathcal{X}_b$*, where* $\mathcal{M}_0 = M^1 \times M^3 \times M^5 \times \cdots$ *and* $\mathcal{M}_1 = M^2 \times M^4 \times M^6 \times \cdots$*.*
- *Correctness: For all* $(x_0, x_1) \in \mathcal{X}_0 \times \mathcal{X}_1$*,*

$$\Pr\left[g_0 + g_1 = f(x_0, x_1) \;\middle|\; \begin{array}{c} (r_0, r_1) \leftarrow \mathsf{Gen}, \\ (\mathrm{mes}_1, \dots, \mathrm{mes}_T) \leftarrow \mathsf{Msg}(x_0, r_0, x_1, r_1), \\ g_b \leftarrow \mathsf{Eval}(b, x_b, r_b, (\mathrm{mes}_1, \dots, \mathrm{mes}_T)) \end{array} \right] = 1.$$

- *Security: For* $b \in \{0, 1\}$*, the distribution of* $\{(r_b, \mathsf{Msg}(x_0, r_0, x_1, r_1))\}_{(r_0, r_1) \leftarrow \mathsf{Gen}}$ *is independent of* $x_{\bar{b}} \in \mathcal{X}_{\bar{b}}$*.*

As an online-optimal secure two-party protocol, we assume that the randomness space is not redundant. In our definition, P_0 is the first party who sends a message. Note that a two-party protocol where P_1 is the first party who sends a message can be reduced to a protocol where P_0 is the first party who sends a message by letting the first message space M_1 be a singleton.

2.4 Non-Redundant Functions

Throughout this paper, we consider non-redundant functions in the following sense:

▶ **Definition 3.** *We say that a function* $f \colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ *is non-redundant for* P_0 *if* $f(x_0, \cdot) - f(x_0', \cdot) \colon \mathcal{X}_1 \to \mathbb{G}$ *is not constant for all* $x_0 \neq x_0' \in \mathcal{X}_0$*; a function* $f \colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ *is non-redundant for* P_1 *if* $f(\cdot, x_1) - f(\cdot, x_1') \colon \mathcal{X}_0 \to \mathbb{G}$ *is not constant for all* $x_1 \neq x_1' \in \mathcal{X}_1$*; and a function* $f \colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ *is non-redundant if* f *is non-redundant for* P_0 *and* P_1*.*

A two-party protocol for a redundant (i.e., not non-redundant) function f is reducible to a two-party protocol for a non-redundant function f' without any overhead. See Appendix A for more details.

3 Technical Overview

Similar research (e.g., [11, 12]) on the lower bounds for communication or randomness complexity mainly focuses on information entropy, e.g. the Shannon entropy. However, in such arguments, it is difficult to effectively handle the correctness requirement as a restraint condition, and thus the obtained bounds may not be tight in general. We consider this may be the main reason why strict bounds for our setting have not been obtained so far, and to overcome this issue, in this work, we instead directly utilize the algebraic aspect of the correctness requirement. This may require a more complicated argument than the entropy-based approach, but it would allow the correctness requirement to be fully utilized in the derivation of the tight lower bound. We provide a more detailed explanation of our approach in the following subsections.

3.1 The Case of Online-Optimal Setting

We give the $\Omega(N^2)$-bit lower bound for some function $f\colon [N] \times [N] \to \{0,1\}^2$ in two steps:

1. By the security, correctness and optimality requirements, we show that the following equation (hereinafter referred to as the *correctness equation*) holds: For all $(r_0, r_1) \in \mathcal{CR}$,
$$A_{0,r_0} + A_{1,r_1} = P_{0,r_0}^{\mathrm{T}} F P_{1,r_1}, \tag{1}$$
where A_{b,r_b} is an $N \times N$ matrix determined by r_b, P_{b,r_b} is an $N \times N$ permutation matrix determined by r_b, and F is an $N \times N$ matrix whose (i,j)-th element is equal to $f(i,j)$.
2. For some $r_0 \in \mathcal{R}_0$, we prove that the size of the set $\{A_{0,r_0} - A_{0,r'_0}\}_{r'_0 \in \mathcal{R}_0}$ is at least $2^{(N-1)^2}$. This implies that $\log|\mathcal{R}_0| \geq (N-1)^2$ and proves the $\Omega(N^2)$-bit lower bound.

Roughly speaking, each element of A_{b,r_b} corresponds to an output of Eval and P_{b,r_b} is a permutation matrix corresponding to Msg.

3.1.1 The First Step

The correctness equation Eq.(1) is deduced from the correctness requirement and the fact that $\mathsf{Msg}(b,\cdot,r_b)\colon \mathcal{X}_b \to \mathcal{M}_b$ is bijective for all $b \in \{0,1\}$ and $r_b \in \mathcal{R}_b$ (Lemma 6). First, we give an informal proof of the fact that Msg is bijective. Since the size of the domain $\mathcal{X}_b$ and the range $\mathcal{M}_b$ are the same, it is enough to prove that the function is injective. Without loss of generality, we set $b = 0$. Suppose on the contrary that there exist $x_0 \neq x'_0 \in \mathcal{X}_0$ such that $\mathsf{Msg}(0, x_0, r_0) = \mathsf{Msg}(0, x'_0, r_0) = m_0$. This assumption implies that for any input x_1 of P_1, P_1's output of Eval for the case of P_0's input being x_0 is the same as that for the case of x'_0. Therefore, from the correctness requirement, $f(x_0, x_1) - f(x'_0, x_1)$ is equal to $\mathsf{Eval}(0, x_0, r_0, m_1) - \mathsf{Eval}(0, x'_0, r_0, m_1)$ where m_1 is P_1's message with some $r_1 \in \mathcal{R}_1$ satisfying $(r_0, r_1) \in \mathcal{CR}$. The former depends on x_1 by the non-redundancy of f, while the latter can be computed solely by P_0, contradicting the security requirement that P_0 should not obtain any information on x_1.

Since $\mathsf{Msg}(b,\cdot,r_b)$ is bijective, the input of P_b can be determined by the correlated randomness r_b and the message m_b sent from P_b. Therefore, P_b's output of Eval can be computed from the messages (m_0, m_1) and the randomness r_b. Let A_{b,r_b} be an $N \times N$ matrix whose (m_0, m_1)-th element is equal to P_b's output of Eval when the messages and the randomness are (m_0, m_1) and r_b, respectively. From the correctness requirement, for all (m_0, m_1), $A_{0,r_0}[m_0, m_1] + A_{1,r_1}[m_0, m_1]$ is equal to the entry of the matrix F at the $\pi_{0,r_0}^{-1}(m_0)$-th row and the $\pi_{1,r_1}^{-1}(m_1)$-th column, where π_{b,r_b} denotes the bijection $\mathsf{Msg}(b,\cdot,r_b)$. This implies the correctness equation Eq.(1), where P_{0,r_0} and P_{1,r_1} are permutation matrices corresponding to π_{0,r_0}^{-1} and π_{1,r_1}^{-1}, respectively.

3.1.2 The Second Step

For simplicity, let F be $\Delta^{N\times N}(0,0)$, $\mathbb{G}$ be $\{0,1\}$ and the operation on $\mathbb{G}$ be XOR. Then, the right term of the correctness equation Eq.(1) is equal to $\Delta^{N\times N}(\mathsf{Msg}(0,0,r_0), \mathsf{Msg}(1,0,r_1))$. The notable point is that, given $r_0 \in \mathcal{R}_0$, we can choose the value of $\mathsf{Msg}(1,0,r_1)$ arbitrarily (Lemma 7). That is, for all $m_1 \in \mathcal{M}_1$, there exists $r_1 \in \mathcal{R}_1$ such that $(r_0, r_1) \in \mathcal{CR}$ and $\mathsf{Msg}(1,0,r_1) = m_1$ (otherwise, the fact that P_0 receives P_1's message m_1 would tell P_0 that P_1's input is not 0, contradicting the security).

Let $r_0 \in \mathcal{R}_0$ satisfy $\mathsf{Msg}(0,0,r_0) = 0$. From the property described above, for all $m_0 \in \mathcal{M}_0 \backslash \{0\}$ and $m_1 \in \mathcal{M}_1 \backslash \{0\}$, there exist $r_0', r_0'' \in \mathcal{R}_0$ and $r_1, r_1' \in \mathcal{R}_1$ such that $(r_0, r_1), (r_0', r_1), (r_0', r_1'), (r_0'', r_1') \in \mathcal{CR}$, $\mathsf{Msg}(1,0,r_1') = m_1$, $\mathsf{Msg}(0,0,r_0') = m_0$, $\mathsf{Msg}(1,0,r_1') = 0$, and $\mathsf{Msg}(0,0,r_0'') = 0$. Taking the sum of both sides of the four correctness equations, we have

$$A_{0,r_0} + A_{0,r_0''} = \Delta^{N\times N}(0,m_1) + \Delta^{N\times N}(m_0,m_1) + \Delta^{N\times N}(m_0,0) + \Delta^{N\times N}(0,0).$$

Note that $A + A = 0$ since the operation is XOR. This implies that the bottom right corner of $A_{0,r_0} + A_{0,r_0''}$ is equal to $\Delta^{(N-1)\times(N-1)}(m_0 - 1, m_1 - 1)$ (Theorem 9). Taking the sum of these equations with various values of m_0 and m_1, it follows that for all $M \in \{0,1\}^{(N-1)\times(N-1)}$, there exists $r_0' \in \mathcal{R}_0$ such that $\mathsf{Msg}(0,0,r_0') = 0$ and the bottom right corner of $A_{0,r_0} + A_{0,r_0'}$ is equal to M (Corollary 10). This implies that the size of $\{A_{0,r_0} + A_{0,r_0'}\}_{r_0' \in \mathcal{R}_0}$ is at least the size of $\{0,1\}^{(N-1)\times(N-1)}$, i.e., $2^{(N-1)^2}$ and this proves the $\Omega(N^2)$-bit lower bound.

3.2 The Case of Communication-Optimal Setting

The basic approach to proving the $\Omega(N)$-bit lower bound is the same as in the online-optimal setting. The main difference is that the message sent from one party at the second or later round may depend on the other party's input or randomness. Nevertheless, the situation is still similar due to the following facts:

1. The map $T_{r_0,r_1} \colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathcal{M}_0 \times \mathcal{M}_1$, which maps the pair of inputs to the transcript when the correlated randomness is (r_0, r_1), is bijective. (Lemma 13)
2. The input of P_b can be determined by the correlated randomness r_b and the transcript (m_0, m_1), and therefore, P_b's output of Eval can be computed from the transcript (m_0, m_1) and the randomness r_b. (Lemma 15)

From these facts, even in the present setting, the correctness equation (with a slight modification on the right side) holds: $A_{0,r_0} + A_{1,r_1} = T_{r_0,r_1} \circ F$, where $T_{r_0,r_1} \circ F$ is an $\mathcal{M}_0 \times \mathcal{M}_1$ matrix whose (m_0, m_1)-th element is equal to the $T^{-1}_{r_0,r_1}(m_0, m_1)$-th element of F.

Let F be $\Delta^{N\times N}(0,0)$. Unlike the online-optimal setting, now the right side of the correctness equation is equal to $\Delta^{N\times N}(T_{r_0,r_1}(0,0))$. A notable point is that each of the row and column entries of $T_{r_0,r_1}(0,0)$ depends on both r_0 and r_1, in contrast to the online-optimal setting where the row entry $\mathsf{Msg}(0,0,r_0)$ (resp. the column entry $\mathsf{Msg}(1,0,r_1)$) depends only on r_0 (resp. r_1). However, we can still somehow control the value of $T_{r_0,r_1}(0,0)$ (Lemma 12 and Lemma 14), and we can set the $(N-1) \times 1$ submatrix at the bottom left corner of $A_{0,r_0} + A_{0,r_0'}$ arbitrarily by varying r_0'. This proves the $\Omega(N)$-bit lower bound.

4 The Case of Online-Optimal Setting

In this section, we prove the optimality of Ishai et al.'s protocol [16] among online-optimal two-party protocols in terms of the size of CR for the "worst" function. In Section 4.1, we give a matrix representation of the three requirements for an online-optimal secure two-party protocol given in Section 2 (Theorem 8). In Section 4.2, we give a function whose domain is $[N] \times [N]$ such that any online-optimal two-party protocol for f needs $\Omega(N^2)$-bit CR.

4.1 Matrix Representation

Throughout this subsection, we let $(\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ denote an online-optimal secure two-party protocol for $f \colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ with correlated randomness $\mathcal{CR} \subseteq \mathcal{R}_0 \times \mathcal{R}_1$. For $b \in \{0,1\}$, $x \in \mathcal{X}_b$, and $m \in \mathcal{M}_b$, let $\mathcal{R}_{b,x,m} = \{r \in \mathcal{R}_b \mid \mathsf{Msg}(b,x,r) = m\}$.

First, we give four lemmas for the matrix representation:

▶ **Lemma 4.** *For all $b \in \{0,1\}$ and $x \in \mathcal{X}_b$, the following hold:*
- $\mathcal{R}_{b,x,m} \cap \mathcal{R}_{b,x,m'} = \varnothing$ *for all* $m \neq m' \in \mathcal{M}_b$.
- $\cup_{m \in \mathcal{M}_b} \mathcal{R}_{b,x,m} = \mathcal{R}_b$.

Proof. These two statements are deduced from the fact that r is in $\mathcal{R}_{b,x,m}$ if and only if m is equal to $\mathsf{Msg}(b,x,r)$. ◀

▶ **Lemma 5.** *For all $b \in \{0,1\}$ and $m \in \mathcal{M}_b$, the following hold:*
- $\mathcal{R}_{b,x,m} \cap \mathcal{R}_{b,x',m} = \varnothing$ *for all* $x \neq x' \in \mathcal{X}_b$.
- $\cup_{x \in \mathcal{X}_b} \mathcal{R}_{b,x,m} = \mathcal{R}_b$.

Proof. We fix $b = 0$ in this proof. In the case of $b = 1$, the statement can be proved similarly.

First, we prove the first statement. Suppose on the contrary that an $r \in \mathcal{R}_{0,x,m} \cap \mathcal{R}_{0,x',m}$ exists. By the non-redundancy of the randomness space, there is an $r' \in \mathcal{R}_1$ such that $(r,r') \in \mathcal{CR}$. Now it suffices to show that there exist $y, y' \in \mathcal{X}_1$ such that $y \neq y'$ and $\mathsf{Msg}(1,y',r'') \neq \mathsf{Msg}(1,y,r')$ for any $r'' \in \mathcal{R}_1$ with $(r,r'') \in \mathcal{CR}$; indeed, this implies that $(r, \mathsf{Msg}(1,y,r'))$ belongs to $\{(r^*, \mathsf{Msg}(1,y,r^{**}))\}_{(r^*,r^{**}) \in \mathcal{CR}}$ but not to $\{(r^*, \mathsf{Msg}(1,y',r^{**}))\}_{(r^*,r^{**}) \in \mathcal{CR}}$, which contradicts the security requirement. To show the claim, suppose on the contrary that for any $y, y' \in \mathcal{X}_1$ with $y \neq y'$, there is an $r'' \in \mathcal{R}_1$ such that $(r,r'') \in \mathcal{CR}$ and $\mathsf{Msg}(1,y',r'') = \mathsf{Msg}(1,y,r')$. From the correctness requirement, we have

$$\mathsf{Eval}(0,x,r,\mathsf{Msg}(1,y,r')) + \mathsf{Eval}(1,y,r',\mathsf{Msg}(0,x,r)) = f(x,y),$$
$$\mathsf{Eval}(0,x',r,\mathsf{Msg}(1,y,r')) + \mathsf{Eval}(1,y,r',\mathsf{Msg}(0,x,r)) = f(x',y)$$

(note that now $\mathsf{Msg}(0,x',r) = m = \mathsf{Msg}(0,x,r)$ by the choice of r), and therefore

$$\mathsf{Eval}(0,x,r,\mathsf{Msg}(1,y,r')) - \mathsf{Eval}(0,x',r,\mathsf{Msg}(1,y,r')) = f(x,y) - f(x',y). \tag{2}$$

By the same argument for (y',r'') instead of (y,r'), we also have

$$\mathsf{Eval}(0,x,r,\mathsf{Msg}(1,y',r'')) - \mathsf{Eval}(0,x',r,\mathsf{Msg}(1,y',r'')) = f(x,y') - f(x',y'). \tag{3}$$

By the choice of r'', the left-hand sides of Equations (2) and (3) are equal, therefore we have $f(x,y) - f(x',y) = f(x,y') - f(x',y')$. Since $y \neq y'$ were arbitrary, this implies that the function $f(x,\cdot) - f(x',\cdot)$ on $\mathcal{X}_1$ is constant, contradicting the non-redundancy of f. Hence, we have $\mathcal{R}_{0,x,m} \cap \mathcal{R}_{0,x',m} = \varnothing$.

Next, we prove the second statement. Suppose that $\cup_{x \in \mathcal{X}_0} \mathcal{R}_{0,x,m} \subsetneq \mathcal{R}_0$. Then, we have

$$\begin{aligned}\sum_{m \in \mathcal{M}_0} \sum_{x \in \mathcal{X}_0} |\mathcal{R}_{0,x,m}| &= \sum_{m \in \mathcal{M}_0} |\cup_{x \in \mathcal{X}_0} \mathcal{R}_{0,x,m}| \ (\because \text{the first statement}) \\ &< \sum_{m \in \mathcal{M}_0} |\mathcal{R}_0| = |\mathcal{M}_0| \cdot |\mathcal{R}_0|.\end{aligned}$$

From Lemma 4, we have

$$\sum_{x \in \mathcal{X}_0} \sum_{m \in \mathcal{M}_0} |\mathcal{R}_{0,x,m}| = \sum_{x \in \mathcal{X}_0} |\mathcal{R}_0| = |\mathcal{X}_0| \cdot |\mathcal{R}_0|.$$

This means that $|\mathcal{X}_0| \cdot |\mathcal{R}_0| < |\mathcal{M}_0| \cdot |\mathcal{R}_0|$ and contradicts the optimality requirement. Hence, we have $\cup_{x \in \mathcal{X}_0} \mathcal{R}_{0,x,m} = \mathcal{R}_0$. ◀

▶ **Lemma 6.** *For all $b \in \{0,1\}$ and $r \in \mathcal{R}_b$, $\mathsf{Msg}(b,\cdot,r)\colon \mathcal{X}_b \to \mathcal{M}_b$ is a bijection.*

Proof. From Lemma 5, $\mathsf{Msg}(b,\cdot,r)$ is an injection. Since $|\mathcal{X}_b| = |\mathcal{M}_b|$ from the optimality requirement, the injective function $\mathsf{Msg}(b,\cdot,r)$ is a bijection. ◀

▶ **Lemma 7.** *For all $b \in \{0,1\}$, $r_{\bar{b}} \in \mathcal{R}_{\bar{b}}$, and $(x_b, m_b) \in \mathcal{X}_b \times \mathcal{M}_b$, there exists $r_b \in \mathcal{R}_b$ such that $(r_0, r_1) \in \mathcal{CR}$ and $\mathsf{Msg}(b, x_b, r_b) = m_b$.*

Proof. We fix $b = 0$ in this proof. In the case of $b = 1$, the statement can be proved similarly.

Let $r_1 \in \mathcal{R}_1$ and $(x_0, m_0) \in \mathcal{X}_0 \times \mathcal{M}_0$. By the non-redundancy of the randomness space, there is an $r^* \in \mathcal{R}_0$ with $(r^*, r_1) \in \mathcal{CR}$. By Lemma 6, there exists an $x' \in \mathcal{X}_0$ such that $\mathsf{Msg}(0, x', r^*) = m_0$ and therefore $(r_1, m_0) \in \{(r', \mathsf{Msg}(0, x', r))\}_{(r,r')\in\mathcal{CR}}$. Since this set is independent of x' from the security requirement, we also have $(r_1, m_0) \in \{(r', \mathsf{Msg}(0, x_0, r))\}_{(r,r')\in\mathcal{CR}}$, therefore there is an $r_0 \in \mathcal{R}_0$ such that $(r_0, r_1) \in \mathcal{CR}$ and $\mathsf{Msg}(0, x_0, r_0) = m_0$. This proves the statement. ◀

Then, we give a matrix representation of the three requirements for an online-optimal secure two-party protocol:

▶ **Theorem 8.** *Given an online-optimal secure two-party protocol* $(\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ *for $f\colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ with correlated randomness $\mathcal{CR} \subseteq \mathcal{R}_0 \times \mathcal{R}_1$, let F be an $\mathcal{X}_0 \times \mathcal{X}_1$ matrix whose (x_0, x_1)-th element is $f(x_0, x_1)$. Then, for any $b \in \{0,1\}$ and $r \in \mathcal{R}_b$, there exist an $\mathcal{M}_0 \times \mathcal{M}_1$ matrix $A_{b,r}$ and an $\mathcal{X}_b \times \mathcal{M}_b$ permutation matrix $P_{b,r}$ such that*

- *for all $(r_0, r_1) \in \mathcal{CR}$, $A_{0,r_0} + A_{1,r_1} = P_{0,r_0}^{\mathrm{T}} F P_{1,r_1}$ holds;*
- *for all $r_{\bar{b}} \in \mathcal{R}_{\bar{b}}$ and $(x_b, m_b) \in \mathcal{X}_b \times \mathcal{M}_b$, there exists $r_b \in \mathcal{R}_b$ such that $(r_0, r_1) \in \mathcal{CR}$ and $P_{b,r_b}[x_b, m_b] = 1$.*

Note that, roughly speaking, the optimality requirement corresponds to $P_{b,r}$ being a permutation matrix, and the correctness and security requirements correspond to the first and the second conditions of the theorem, respectively.

Proof. For $b \in \{0,1\}$, let E_{b,r_b} for $r_b \in \mathcal{R}_{r_b}$ be an $\mathcal{X}_b \times \mathcal{M}_{\bar{b}}$ matrix whose $(x_b, m_{\bar{b}})$-th element is equal to $\mathsf{Eval}(b, x_b, r_b, m_{\bar{b}})$. For $b \in \{0,1\}$, let P_{b,r_b} for $r_b \in \mathcal{R}_{r_b}$ be an $\mathcal{X}_b \times \mathcal{M}_b$ matrix whose $(x_b, \mathsf{Msg}(b, x_b, r_b))$-th element is 1 and other elements are 0. Since the $(x_b, x_{\bar{b}})$-th element of $E_{b,r_b} P_{\bar{b},r_{\bar{b}}}^{\mathrm{T}}$ is equal to $\mathsf{Eval}(b, x_b, r_b, \mathsf{Msg}(\bar{b}, x_{\bar{b}}, r_{\bar{b}}))$, the correctness requirement can be expressed by the following:

$$E_{0,r_0} P_{1,r_1}^{\mathrm{T}} + \left(E_{1,r_1} P_{0,r_0}^{\mathrm{T}}\right)^{\mathrm{T}} = F \tag{4}$$

for all $(r_0, r_1) \in \mathcal{CR}$. From Lemma 6, P_{b,r_b} is a permutation matrix and therefore P_{b,r_b}^{T} is its inverse. By multiplying P_{0,r_0}^{T} from the left (P_{1,r_1} from the right, resp.) to both sides of Equation (4), we have

$$P_{0,r_0}^{\mathrm{T}} E_{0,r_0} + E_{1,r_1}^{\mathrm{T}} P_{1,r_1} = P_{0,r_0}^{\mathrm{T}} F P_{1,r_1}. \tag{5}$$

Therefore, $(A_{0,r_0}, A_{1,r_1}) = (P_{0,r_0}^{\mathrm{T}} E_{0,r_0}, E_{1,r_1}^{\mathrm{T}} P_{1,r_1})$ satisfies the first condition of the statement.

The second condition of the statement is deduced from Lemma 7. ◀

4.2 Lower Bound

We prove the $\Omega(N^2)$-bit lower bound for the function $f\colon [N] \times [N] \to \{0,1\}^2$ defined as follows:

$$f(x_0, x_1) = \begin{cases} 11 & (x_0 = x_1 = 0) \\ 01 & (x_0 = x_1 \neq 0) \\ 00 & (\text{otherwise}). \end{cases}$$

That is, we prove that any online-optimal secure two-party protocol for f needs $\Omega(N^2)$-bit CR. Note that the operation '+' on $\{0,1\}^2$ is bitwise XOR here and that f is non-redundant.

In the rest of this section, we write $[N]$ instead of $\mathcal{X}_b$ and $\mathcal{M}_b$. Without loss of generality, we consider the lower bound for the size of P_0's CR (i.e., $\log|\mathcal{R}_0|$).

We use the notation A_{b,r_b} and P_{b,r_b} for representing $N \times N$ matrices whose existence is guaranteed by Theorem 8. Since the operation on $\{0,1\}^2$ is bitwise XOR, Equation (5) holds even if we focus on the first bit of each element of A_{b,r_b} and F. Therefore, we focus on the first bit and use the same notation A_{b,r_b} and F. Then we have $F = \Delta^{N\times N}(0,0)$ in the current setting.

First, we prove the following theorem:

▶ **Theorem 9.** *Suppose that $r_0 \in \mathcal{R}_0$ satisfies $\mathsf{Msg}(0,0,r_0) = 0$. Then, for all $i,j \in [N-1]$, there exists an $r'_0 \in \mathcal{R}_0$ such that*
- $\mathsf{Msg}(0,0,r'_0) = 0$,
- *the $(N-1)\times(N-1)$ submatrix in the bottom right corner of $A_{0,r_0} + A_{0,r'_0}$ is equal to $\Delta^{(N-1)\times(N-1)}(i,j)$.*

Proof. From the definition of P_{b,r_b} (see the proof of Theorem 8), the right term of Equation (5) is equal to $\Delta^{N\times N}(\mathsf{Msg}(0,0,r_0), \mathsf{Msg}(1,0,r_1))$. From Theorem 8, there exists an $r_1 \in \mathcal{R}_1$ such that $(r_0,r_1) \in \mathcal{CR}$ and $\mathsf{Msg}(1,0,r_1) = j+1$, and there exists $r''_0 \in \mathcal{R}_0$ such that $(r''_0, r_1) \in \mathcal{CR}$ and $\mathsf{Msg}(0,0,r''_0) = i+1$. From the property mentioned at the beginning, we have

$$A_{0,r_0} + A_{1,r_1} = \Delta^{N\times N}(0, j+1) \text{ and } A_{0,r''_0} + A_{1,r_1} = \Delta^{N\times N}(i+1, j+1),$$

and therefore

$$\begin{aligned} A_{0,r_0} + A_{0,r''_0} &= (A_{0,r_0} + A_{1,r_1}) + (A_{0,r''_0} + A_{1,r_1}) \\ &= \Delta^{N\times N}(0, j+1) + \Delta^{N\times N}(i+1, j+1). \end{aligned}$$

Similarly, there exist an $r'_1 \in \mathcal{R}_1$ and an $r'_0 \in R_0$ such that $(r''_0, r'_1) \in \mathcal{CR}$, $\mathsf{Msg}(1,0,r'_1) = 0$, $(r'_0, r'_1) \in \mathcal{CR}$, and $\mathsf{Msg}(0,0,r'_0) = 0$. Then, we have

$$A_{0,r''_0} + A_{1,r'_1} = \Delta^{N\times N}(i+1, 0) \text{ and } A_{0,r'_0} + A_{1,r'_1} = \Delta^{N\times N}(0,0),$$

and

$$A_{0,r''_0} + A_{0,r'_0} = (A_{0,r''_0} + A_{1,r'_1}) + (A_{0,r'_0} + A_{1,r'_1}) = \Delta^{N\times N}(i+1,0) + \Delta^{N\times N}(0,0).$$

Hence, we have

$$A_{0,r_0} + A_{0,r'_0} = \Delta^{N\times N}(0,j+1) + \Delta^{N\times N}(i+1,j+1) + \Delta^{N\times N}(i+1,0) + \Delta^{N\times N}(0,0).$$

Especially, the $(N-1)\times(N-1)$ submatrix in the bottom right corner of $A_{0,r_0} + A_{0,r'_0}$ is equal to $\Delta^{(N-1)\times(N-1)}(i,j)$. Therefore, r'_0 satisfies the condition of the statement. ◀

Using Theorem 9 sequentially, we have the following corollary:

▶ **Corollary 10.** *Suppose that $r_0 \in \mathcal{R}_0$ satisfies $\mathsf{Msg}(0,0,r_0) = 0$. Then, for all $M \in \{0,1\}^{(N-1)\times(N-1)}$, there exists an $r'_0 \in \mathcal{R}_0$ such that*
- $\mathsf{Msg}(0,0,r'_0) = 0$,
- *the $(N-1)\times(N-1)$ submatrix in the bottom right corner of $A_{0,r_0} + A_{0,r'_0}$ is equal to M.*

Proof. For $r \in \mathcal{R}_0$, we use the notation $A'_{0,r}$ for the $(N-1) \times (N-1)$ submatrix in the bottom right corner of $A_{0,r}$. Let I be the set of indices where the element of M is equal to 1, i.e., $I = \{(i,j) \in [N-1] \times [N-1] \mid M[i,j] = 1\}$. Let $M_k = \Delta^{(N-1)\times(N-1)}(i_k, j_k)$ for $k \geq 0$, where (i_k, j_k) is the k-th element of I (in some ordering). We define the sequence $r_{0,0}, r_{0,1}, \dots, r_{0,|I|}$ as follows:

- $r_{0,0} = r_0$.
- For $k \geq 1$, $r_{0,k}$ is an element of $\mathcal{R}_0$ such that $A'_{0,r_{0,k-1}} + A'_{0,r_{0,k}}$ is equal to M_{k-1} and $\mathsf{Msg}(0, 0, r_{0,k})$ is equal to 0. The existence of such $r_{0,k}$ is guaranteed by Theorem 9.

We have

$$A'_{0,r_{0,0}} + A'_{0,r_{0,|I|}} = \sum_{k=1}^{|I|} (A'_{0,r_{0,k-1}} + A'_{0,r_{0,k}}) = \sum_{k=1}^{|I|} M_{k-1} = M,$$

and therefore $r'_0 = r_{0,|I|}$ satisfies the condition of the statement. ◀

The lower bound of the size of P_0's CR is derived from Corollary 10:

▶ **Corollary 11.** *The size of CR delivered to P_0 is $\Omega(N^2)$ bits. More concretely, it is greater than or equal to $(N-1)^2$ bits.*

Proof. Let $r_0 \in \mathcal{R}_0$ satisfy $\mathsf{Msg}(0, 0, r_0) = 0$. (The existence of such r_0 is guaranteed by Lemma 7.) From Corollary 10, the following inequality holds:

$$\left| \{A_{0,r_0} + A_{0,r'_0}\}_{r'_0 \in \mathcal{R}_0} \right| \geq \left| \{0,1\}^{(N-1)\times(N-1)} \right|.$$

Since the left term of the above inequality is upper-bounded by $|\mathcal{R}_0|$, we have

$$|\mathcal{R}_0| \geq \left| \{0,1\}^{(N-1)\times(N-1)} \right| = 2^{(N-1)^2}.$$

Therefore, the size of P_0's CR is greater than or equal to $(N-1)^2$ bits. ◀

5 The Case of Communication-Optimal Setting

In this section, we prove the $\Omega(N)$-bit lower bound for the size of CR of a communication-optimal two-party protocol for the concrete function f given in Section 4.2.

We give a matrix representation of the three requirements for a communication-optimal secure two-party protocol in Section 5.1 (Theorem 16). In Section 5.2, we prove that any communication-optimal two-party protocol for f given in Section 4.2 needs $\Omega(N)$-bit CR.

5.1 Matrix Representation

Throughout this subsection, we let $(\mathsf{Gen}, \mathsf{Msg}, \mathsf{Eval})$ denote a communication-optimal secure two-party protocol for $f \colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ with correlated randomness $\mathcal{CR} \subseteq \mathcal{R}_0 \times \mathcal{R}_1$. For $(r_0, r_1) \in \mathcal{R}_0 \times \mathcal{R}_1$, let $T_{r_0,r_1} \colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathcal{M}_0 \times \mathcal{M}_1$ be a function such that $T_{r_0,r_1}(x_0, x_1) = (m_0, m_1)$, where m_b is a message which P_b sends to $P_{\bar{b}}$ in the online phase whose input (CR, resp.) is (x_0, x_1) ((r_0, r_1), resp.). That is, m_0 is equal to $(\mathrm{mes}_1, \mathrm{mes}_3, \dots)$ and m_1 is equal to $(\mathrm{mes}_2, \mathrm{mes}_4, \dots)$, where $(\mathrm{mes}_1, \mathrm{mes}_2, \dots) = \mathsf{Msg}(x_0, r_0, x_1, r_1)$. Note that the message m_b which P_b sends to $P_{\bar{b}}$ is uniquely determined by $(x_b, r_b, m_{\bar{b}})$, where x_b is P_b's input, r_b is P_b's CR, and $m_{\bar{b}}$ is a message sent to P_b by $P_{\bar{b}}$. We define a function $g^b_{x_b,r_b} \colon \mathcal{M}_{\bar{b}} \to \mathcal{M}_b$ based on the above correspondence. Let $S^0_{x_0,r_0}$ be the set $\{(g^0_{x_0,r_0}(m_1), m_1)\}_{m_1 \in \mathcal{M}_1} \subseteq \mathcal{M}_0 \times \mathcal{M}_1$ and let $S^1_{x_1,r_1}$ be the set $\{(m_0, g^1_{x_1,r_1}(m_0))\}_{m_0 \in \mathcal{M}_0} \subseteq \mathcal{M}_0 \times \mathcal{M}_1$.

First, we give four lemmas for the matrix representation:

▶ **Lemma 12.** *$S^0_{x_0,r_0} \cap S^1_{x_1,r_1} = \{T_{r_0,r_1}(x_0,x_1)\}$ holds for all $(r_0,r_1) \in \mathcal{CR}$ and $(x_0,x_1) \in \mathcal{X}_0 \times \mathcal{X}_1$.*

Proof. Let $(m_0,m_1) := T_{r_0,r_1}(x_0,x_1)$. By the definition, $g^0_{x_0,r_0}(m_1) = m_0$ and $g^1_{x_1,r_1}(m_0) = m_1$, and therefore $(m_0,m_1) \in S^0_{x_0,r_0} \cap S^1_{x_1,r_1}$. Suppose on the contrary that there exists $(m'_0,m'_1) \in S^0_{x_0,r_0} \cap S^1_{x_1,r_1}$ such that $(m'_0,m'_1) \neq (m_0,m_1)$. Let t be the first round where the two transcripts determined by (m_0,m_1) and (m'_0,m'_1) differ and let P_b be the party who sends a message at t-th round. Since $g^b_{x_b,r_b}(m_{\bar{b}}) = m_b$ and $g^b_{x_b,r_b}(m'_{\bar{b}}) = m'_b$, the t-th messages msg_t and msg'_t in the transcripts (m_0,m_1) and (m'_0,m'_1) are determined by (x_b,r_b) and the $(t-1)$-th or earlier messages in the transcripts (m_0,m_1) and (m'_0,m'_1), respectively. Since the latter messages are equal by the minimality of t, we have $\mathrm{msg}_t = \mathrm{msg}'_t$, contradicting the choice of t. Therefore, there is no $(m'_0,m'_1) \in S^0_{x_0,r_0} \cap S^1_{x_1,r_1}$ such that $(m'_0,m'_1) \neq (m_0,m_1)$, and the statement holds. ◀

▶ **Lemma 13.** *For all $(r_0,r_1) \in \mathcal{CR}$, T_{r_0,r_1} is bijective.*

Proof. Since $|\mathcal{X}_0 \times \mathcal{X}_1| = |\mathcal{M}_0 \times \mathcal{M}_1|$ from the optimality requirement, it is enough to prove that T_{r_0,r_1} is injective. Suppose on the contrary that there exist $(x_0,x_1) \neq (x'_0,x'_1) \in \mathcal{X}_0 \times \mathcal{X}_1$ such that $T_{r_0,r_1}(x_0,x_1) = T_{r_0,r_1}(x'_0,x'_1) =: (m_0,m_1)$. We assume that $x_0 \neq x'_0$ in the proof; the other case $x_1 \neq x'_1$ is similar.

For any $x''_1 \in \mathcal{X}_1$, there exists an $r''_1 \in \mathcal{R}_1$ such that $(r_0,r''_1) \in \mathcal{CR}$ and $T_{r_0,r''_1}(x_0,x''_1) = (m_0,m_1)$, since we have $\{(r^*, T_{r^*,r^{**}}(x_0,x_1))\}_{(r^*,r^{**})\in\mathcal{CR}} = \{(r^*, T_{r^*,r^{**}}(x_0,x''_1))\}_{(r^*,r^{**})\in\mathcal{CR}}$ by the security requirement and the left-hand side contains $(r_0,(m_0,m_1))$. By Lemma 12, (m_0,m_1) belongs to all of $S^0_{x_0,r_0}$, $S^0_{x'_0,r_0}$, and $S^1_{x''_1,r''_1}$, therefore $T_{r_0,r''_1}(x_0,x''_1) = T_{r_0,r''_1}(x'_0,x''_1) = (m_0,m_1)$ by Lemma 12 again. Then, from the correctness requirement, we have

$$\mathsf{Eval}(0,x_0,r_0,(m_0,m_1)) + \mathsf{Eval}(1,x''_1,r''_1,(m_0,m_1)) = f(x_0,x''_1),$$
$$\mathsf{Eval}(0,x'_0,r_0,(m_0,m_1)) + \mathsf{Eval}(1,x''_1,r''_1,(m_0,m_1)) = f(x'_0,x''_1),$$

and therefore

$$\mathsf{Eval}(0,x_0,r_0,(m_0,m_1)) - \mathsf{Eval}(0,x'_0,r_0,(m_0,m_1)) = f(x_0,x''_1) - f(x'_0,x''_1). \tag{6}$$

Since x''_1 was arbitrary, it follows that the function $f(x_0,\cdot) - f(x'_0,\cdot)$ is constant on $\mathcal{X}_1$, contradicting the non-redundancy of f. Hence the statement holds. ◀

▶ **Lemma 14.** *For all $b \in \{0,1\}$, $r_b \in \mathcal{R}_b$, $x_{\bar{b}} \in X_{\bar{b}}$, and $(m_0,m_1) \in \mathcal{M}_0 \times \mathcal{M}_1$, there exists $r_{\bar{b}} \in \mathcal{R}_{\bar{b}}$ such that $(r_0,r_1) \in \mathcal{CR}$ and $(m_0,m_1) \in S^b_{x_{\bar{b}},r_{\bar{b}}}$.*

Proof. We prove the statement for the case of $b = 0$; the other case $b = 1$ is similar. By the non-redundancy of the randomness space, there is an $r'_1 \in \mathcal{R}_1$ such that $(r_0,r'_1) \in \mathcal{CR}$. By Lemma 13, there is $(x'_0,x'_1) \in \mathcal{X}_0 \times \mathcal{X}_1$ such that $(m_0,m_1) = T_{r_0,r'_1}(x'_0,x'_1)$. Therefore we have $(r_0,(m_0,m_1)) \in \{(r^*, T_{r^*,r^{**}}(x'_0,x'_1))\}_{(r^*,r^{**})\in\mathcal{CR}}$, while this set is equal to $\{(r^*, T_{r^*,r^{**}}(x'_0,x_1))\}_{(r^*,r^{**})\in\mathcal{CR}}$ by the security requirement. This implies that there is an $r_1 \in \mathcal{R}_1$ such that $(r_0,r_1) \in \mathcal{CR}$ and $T_{r_0,r_1}(x'_0,x_1) = (m_0,m_1)$, therefore $(m_0,m_1) \in S^1_{x_1,r_1}$ by Lemma 12. Hence the statement holds. ◀

▶ **Lemma 15.** *For all $(m_0,m_1) \in \mathcal{M}_0 \times \mathcal{M}_1$, $b \in \{0,1\}$, and $r_b \in \mathcal{R}_b$, there exists a unique $x_b \in \mathcal{X}_b$ such that $g^b_{x_b,r_b}(m_{\bar{b}}) = m_b$.*

Proof. We prove the statement for the case of $b = 0$; the other case $b = 1$ is similar. First, we prove the existence. By definition, $g^0_{x_0,r_0}(m_1) = m_0$ holds if and only if $(m_0, m_1) \in S^0_{x_0,r_0}$. Let $r_1 \in \mathcal{R}_1$ satisfy $(r_0, r_1) \in \mathcal{CR}$. From Lemma 13, there exists $(x_0, x_1) \in \mathcal{X}_0 \times \mathcal{X}_1$ such that $T_{r_0,r_1}(x_0, x_1) = (m_0, m_1)$. From Lemma 12, $S^0_{x_0,r_0}$ contains $T_{r_0,r_1}(x_0, x_1)$ and this proves the existence.

Then, we prove the uniqueness. Suppose on the contrary that there exist $x_0 \neq x'_0 \in \mathcal{X}_0$ such that $g^0_{x_0,r_0}(m_1) = g^0_{x'_0,r_0}(m_1) = m_0$ and therefore $S^0_{x_0,r_0}$ and $S^0_{x'_0,r_0}$ contain (m_0, m_1). From Lemma 14, for all $x_1 \in \mathcal{X}_1$, there exists $r_1 \in \mathcal{R}_1$ such that $(r_0, r_1) \in \mathcal{CR}$ and $(m_0, m_1) \in S^1_{x_1,r_1}$. Since $(m_0, m_1) \in S^0_{x_0,r_0} \cap S^1_{x_1,r_1}$ and $(m_0, m_1) \in S^0_{x'_0,r_0} \cap S^1_{x_1,r_1}$, we have $T_{r_0,r_1}(x_0, x_1) = T_{r_0,r_1}(x'_0, x_1) = (m_0, m_1)$ from Lemma 12. This contradicts the fact that T_{r_0,r_1} is bijective (Lemma 13). This proves the uniqueness. ◀

Then, we give a matrix representation of the three requirements for a communication-optimal secure two-party protocol:

▶ **Theorem 16.** *Given a communication-optimal secure two-party protocol* (Gen, Msg, Eval) *for $f\colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ with correlated randomness $CR \subseteq \mathcal{R}_0 \times \mathcal{R}_1$, let F be an $\mathcal{X}_0 \times \mathcal{X}_1$ matrix whose (x_0, x_1)-th element is $f(x_0, x_1)$. Then, for $b \in \{0, 1\}$ and $r_b \in \mathcal{R}_b$, there exist an $\mathcal{M}_0 \times \mathcal{M}_1$ matrix A_{b,r_b} and a bijection $T_{r_0,r_1}\colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathcal{M}_0 \times \mathcal{M}_1$ such that*
- *for all $(r_0, r_1) \in \mathcal{CR}$, $A_{0,r_0} + A_{1,r_1} = T_{r_0,r_1} \circ F$ holds;*
- *for all $b \in \{0, 1\}$, $r_b \in \mathcal{R}_b$, $x_{\bar{b}} \in \mathcal{X}_{\bar{b}}$ and $(m_0, m_1) \in \mathcal{M}_0 \times \mathcal{M}_1$, there exists $r_{\bar{b}} \in \mathcal{R}_{\bar{b}}$ such that $(r_0, r_1) \in \mathcal{CR}$ and $(m_0, m_1) \in S^{\bar{b}}_{x_{\bar{b}},r_{\bar{b}}}$.*

Here, $T_{r_0,r_1} \circ F$ is an $M_0 \times \mathcal{M}_1$ matrix whose (m_0, m_1)-th element is equal to $T^{-1}_{r_0,r_1}(m_0, m_1)$-th element of F.

Note that, roughly speaking, the optimality requirement corresponds to T_{r_0,r_1} being a bijection,the correctness requirement corresponds to the first condition of the theorem, and the security requirement corresponds to the second condition of the theorem.

Proof. $\mathsf{Eval}(b, x_b, r_b, (m_0, m_1))$ is determined by (m_0, m_1, r_b) since x_b is uniquely determined by (m_0, m_1, r_b) from Lemma 15. Let A_{b,r_b} be an $\mathcal{M}_0 \times \mathcal{M}_1$ matrix whose (m_0, m_1)-th element is equal to $\mathsf{Eval}(b, x_b, r_b, (m_0, m_1))$. Note that T_{r_0,r_1} is bijective from Lemma 13.

The first condition is deduced from the correctness requirement and the definition of A_{b,r_b} and T_{r_0,r_1}. The second condition is the same as Lemma 14. ◀

5.2 Lower Bound

We prove the $\Omega(N)$-bit lower bound for the function $f\colon [N] \times [N] \to \{0, 1\}^2$ defined in Section 4.2. That is, we prove that any communication-optimal secure two-party protocol for f needs $\Omega(N)$-bit CR.

In the rest of this section, we write $[N]$ instead of $\mathcal{X}_b$ and $\mathcal{M}_b$. We consider the lower bound for the size of P_0's CR (i.e., $\log |\mathcal{R}_0|$); the lower bound for the size of P_1's CR is similar. We use the notation A_{b,r_b} for representing $N \times N$ matrices whose existence is guaranteed by Theorem 16, and as in Section 4.2, we focus on the first bit and use the same notation A_{b,r_b} and F. Then we have $F = \Delta^{N\times N}(0, 0)$ in the current setting.

First, we prove the following theorem:

▶ **Theorem 17.** *Suppose that $r_0 \in \mathcal{R}_0$ satisfies $(0, 0) \in S^0_{0,r_0}$. Then, for all $i \in [N - 1]$, there exists $r'_0 \in \mathcal{R}_0$ such that*
- $(0, 0) \in S^0_{0,r'_0}$.
- *The $(N-1)\times 1$ submatrix at the bottom left corner of $A_{0,r_0}+A_{0,r'_0}$ is equal to $\Delta^{(N-1)\times 1}(i, 0)$.*

Proof. Let B_{b,r_b} be the $(N-1)\times 1$ submatrix at the bottom left corner of A_{b,r_b}. From the definition of the operation $\circ$, $T_{r_0,r_1}\circ F$ is equal to $\Delta^{N\times N}(T_{r_0,r_1}(0,0))$. From Theorem 16, there exists $r_1 \in \mathcal{R}_1$ such that $(r_0, r_1) \in \mathcal{CR}$ and $(i+1, 0) \in S^1_{0,r_1}$, and there exists $r''_0 \in \mathcal{R}_0$ such that $(r''_0, r_1) \in \mathcal{CR}$ and $(i+1, 0) \in S^0_{0,r''_0}$. Let $M := ([N]\times[N])\backslash\{(m, 0) \mid m = 1, \ldots, N-1\}$.

From the definition of S^0_{0,r_0} and the assumption that $(0, 0)$ belongs to S^0_{0,r_0}, $g^0_{0,r_0}(0) = 0$ and S^0_{0,r_0} is equal to $\{(0, 0)\}\cup\{(g^0_{0,r_0}(m), m)\}_{m=1,\ldots,N-1} \subseteq M$. Therefore, from Lemma 12, we have $T_{r_0,r_1}(0, 0) \in S^0_{0,r_0}\cap S^1_{1,r_1} \subseteq M$ and $B_{0,r_0} + B_{1,r_1}$ is the zero matrix. Also, $T_{r''_0,r_1}(0, 0) = (i + 1, 0)$ since $(i + 1, 0) \in S^0_{0,r''_0}\cap S^1_{0,r_1}$. Therefore, $B_{0,r''_0} + B_{1,r_1}$ is equal to $\Delta^{(N-1)\times 1}(i, 0)$ and we have

$$B_{0,r_0} + B_{0,r''_0} = (B_{0,r_0} + B_{1,r_1}) + (B_{0,r''_0} + B_{1,r_1}) = \Delta^{(N-1)\times 1}(i, 0).$$

Let $(m'_0, m'_1) \in S^0_{0,r''_0}\backslash\{(i, 0)\}$. Note that $(m'_0, m'_1) \in M$ since $S^0_{0,r''_0}\backslash\{(i, 0)\}$ is equal to $\{(g^0_{0,r''_0}(m), m)\}_{m=1,\ldots,N-1} \subseteq M$. From Theorem 16, there exists $r'_1 \in \mathcal{R}_1$ such that $(r''_0, r'_1) \in \mathcal{CR}$ and $(m'_0, m'_1) \in S^1_{0,r'_1}$, and there exists $r'_0 \in \mathcal{R}_0$ such that $(r'_0, r'_1) \in \mathcal{CR}$ and $(0, 0) \in S^0_{0,r'_0}$. From Lemma 12 and the fact that $(m'_0, m'_1) \in S^0_{0,r''_0}\cap S^1_{0,r'_1}$, we have $T_{r''_0,r'_1}(0, 0) = (m'_0, m'_1) \in M$ and $B_{0,r''_0} + B_{1,r'_1}$ is the zero matrix. Also, from the definition of S^0_{0,r'_0} and the fact that $(0, 0) \in S^0_{0,r'_0}$, S^0_{0,r'_0} is equal to $\{(0, 0)\} \cup \{(g^0_{0,r'_0}(m), m)\}_{m=1,\ldots,N-1} \subseteq M$. From Lemma 12, we have $T_{r'_0,r'_1}(0, 0) \in S^0_{0,r'_0}\cap S^1_{0,r'_1} \subseteq M$ and $B_{0,r'_0} + B_{1,r'_1}$ is the zero matrix. Therefore, $B_{0,r''_0} + B_{0,r'_0} = (B_{0,r''_0} + B_{1,r'_1}) + (B_{0,r'_0} + B_{1,r'_1})$ is the zero matrix.

Hence, $B_{0,r_0} + B_{0,r'_0} = (B_{0,r_0} + B_{0,r''_0}) + (B_{0,r''_0} + B_{0,r'_0})$ is equal to $\Delta^{(N-1)\times 1}(i, 0)$, and therefore r'_0 satisfies the conditions of the statement. ◀

Using Theorem 17 sequentially, we have the following corollary:

▶ **Corollary 18.** *Suppose that $r_0 \in \mathcal{R}_0$ satisfies $(0, 0) \in S^0_{0,r_0}$. Then, for all $M \in \{0, 1\}^{[N-1]\times[1]}$, there exists $r'_0 \in \mathcal{R}_0$ such that*

- $(0, 0) \in S^0_{0,r'_0}$.
- *The $(N-1) \times 1$ submatrix at the bottom left corner of $A_{0,r_0} + A_{0,r'_0}$ is equal to M.*

Proof. We can prove this corollary similarly to Corollary 10. ◀

The lower bound of the size of P_0's CR is derived from Corollary 18:

▶ **Corollary 19.** *The size of CR delivered to P_0 is $\Omega(N)$ bits. More concretely, it is greater than or equal to $N-1$ bits.*

Proof. We can prove this corollary similarly to Corollary 11. ◀

References

1 Nuttapong Attrapadung, Goichiro Hanaoaka, Takahiro Matsuda, Hiraku Morita, Kazuma Ohara, Jacob C. N. Schuldt, Tadanori Teruya, and Kazunari Tozawa. Oblivious linear group actions and applications. In *CCS'21*, pages 630–650. ACM, 2021. doi:10.1145/3460120.3484584.

2 Donald Beaver. Efficient multiparty protocols using circuit randomization. In *11th CRYPTO*, volume 576 of *LNCS*, pages 420–432. Springer, 1991. doi:10.1007/3-540-46766-1_34.

3 Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *11th TCC*, volume 8349 of *LNCS*, pages 317–342. Springer, 2014. doi:10.1007/978-3-642-54242-8_14.

4 Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions (full version of [3]). https://people.csail.mit.edu/ranjit/papers/BIKK.pdf, 2014.

5 Elette Boyle, Nishanth Chandran, Niv Gilboa, Divya Gupta, Yuval Ishai, Nishant Kumar, and Mayank Rathee. Function secret sharing for mixed-mode and fixed-point secure computation. In *40th EUROCRYPT*, volume 12697 of *LNCS*, pages 871–900. Springer, 2021. `doi:10.1007/978-3-030-77886-6_30`.

6 Elette Boyle, Niv Gilboa, and Yuval Ishai. Secure computation with preprocessing via function secret sharing. In *17th TCC*, volume 11891 of *LNCS*, pages 341–371. Springer, 2019. `doi:10.1007/978-3-030-36030-6_14`.

7 Benny Chor and Eyal Kushilevitz. A zero-one law for boolean privacy. In *21st STOC*, pages 62–72. ACM, 1989. `doi:10.1145/73007.73013`.

8 Geoffroy Couteau. A note on the communication complexity of multiparty computation in the correlated randomness model. In *38th EUROCRYPT*, volume 11477 of *LNCS*, pages 473–503. Springer, 2019. `doi:10.1007/978-3-030-17656-3_17`.

9 Ivan Damgård, Jesper Buus Nielsen, Michael Nielsen, and Samuel Ranellucci. The tinytable protocol for 2-party secure computation, or: Gate-scrambling revisited. In *37th CRYPTO*, volume 10401 of *LNCS*, pages 167–187. Springer, 2017. `doi:10.1007/978-3-319-63688-7_6`.

10 Ivan Damgård, Jesper Buus Nielsen, Antigoni Polychroniadou, and Michael Raskin. On the communication required for unconditionally secure multiplication. In *36th CRYPTO*, volume 9815 of *LNCS*, pages 459–488. Springer, 2016. `doi:10.1007/978-3-662-53008-5_16`.

11 Ivan Bjerre Damgård, Boyang Li, and Nikolaj Ignatieff Schwartzbach. More communication lower bounds for information-theoretic mpc. In *2nd ITC*, volume 199 of *LIPIcs*, pages 2:1–2:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. `doi:10.4230/LIPIcs.ITC.2021.2`.

12 Deepesh Data, Manoj M. Prabhakaran, and Vinod M. Prabhakaran. On the communication complexity of secure computation. In *34th CRYPTO*, volume 8617 of *LNCS*, pages 199–216. Springer, 2014. `doi:10.1007/978-3-662-44381-1_12`.

13 Anna Gál and Adi Rosén. Lower bounds on the amount of randomness in private computation. In *35th STOC*, pages 659–666. ACM, 2003. `doi:10.1145/780542.780638`.

14 Niv Gilboa and Yuval Ishai. Distributed point functions and their applications. In *33rd EUROCRYPT*, volume 8441 of *LNCS*, pages 640–658. Springer, 2014. `doi:10.1007/978-3-642-55220-5_35`.

15 Vipul Goyal, Yuval Ishai, and Yifan Song. Tight bounds on the randomness complexity of secure multiparty computation. In *42nd CRYPTO*, volume 13510 of *LNCS*, pages 483–513. Springer, 2022. `doi:10.1007/978-3-031-15985-5_17`.

16 Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, Claudio Orlandi, and Anat Paskin-Cherniavsky. On the power of correlated randomness in secure computation. In *10th TCC*, volume 7785 of *LNCS*, pages 600–620. Springer, 2013. `doi:10.1007/978-3-642-36594-2_34`.

17 Marcel Keller, Emmanuela Orsini, and Peter Scholl. Mascot: Faster malicious arithmetic secure computation with oblivious transfer. In *CCS'16*, pages 830–842. ACM, 2016. `doi:10.1145/2976749.2978357`.

18 Eyal Kushilevitz. Privacy and communication complexity. In *30th FOCS*, pages 416–421. IEEE Computer Society, 1989. `doi:10.1109/sfcs.1989.63512`.

19 Eyal Kushilevitz and Yishay Mansour. Randomness in private computations. In *15th PODC*, pages 181–190. ACM Press, 1996. `doi:10.1145/248052.248089`.

20 Eyal Kushilevitz, Rafail Ostrovsky, Emmanuel Prouff, Adi Rosén, Adrian Thillard, and Damien Vergnaud. Lower and upper bounds on the randomness complexity of private computations of and. In *17th TCC*, volume 11892 of *LNCS*, pages 386–406. Springer, 2019. `doi:10.1007/978-3-030-36033-7_15`.

21 Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Characterizing linear size circuits in terms of privacy. In *28th STOC*. ACM, 1996. `doi:10.1145/237814.238002`.

22 Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Amortizing randomness in private multiparty computations. In *17th PODC*, pages 81–90. ACM, 1998. `doi:10.1145/277697.277710`.

23 Eyal Kushilevitz and Adi Rosén. A randomness-rounds tradeoff in private computation. In *14th CRYPTO*, volume 839 of *LNCS*, pages 397–410. Springer, 1994. doi:10.1007/3-540-48658-5_36.

24 Arpita Patra, Thomas Schneider, Ajith Suresh, and Hossein Yalame. ABY2.0: improved mixed-protocol secure two-party computation. In *30th USENIX Security Symposium*, pages 2165–2182. USENIX Association, 2021. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/patra.

25 Andrew C.-C. Yao. How to generate and exchange secrets (extended abstract). In *27th FOCS*, pages 162–167. IEEE Computer Society, 1986. doi:10.1109/SFCS.1986.25.

A Reduction to Protocol for Non-Redundant Function

In this section, we reduce a protocol for $f\colon \mathcal{X}_0 \times \mathcal{X}_1 \to \mathbb{G}$ to a protocol for a non-redundant function f'. We define the binary relations '$\sim$' on $\mathcal{X}_0$ as follows: $x_0 \sim x_0'$ if and only if $f(x_0,\cdot) - f(x_0',\cdot)\colon \mathcal{X}_1 \to \mathbb{G}$ is constant. Note that   is an equivalence relation. Let $\mathcal{X}_0' \subseteq \mathcal{X}_0$ be a complete system of representatives, and let ϕ_0 be the natural sujection $\mathcal{X}_0 \to \mathcal{X}_0'$. By the definition, $f(x,\cdot) - f(\phi(x),\cdot)\colon \mathcal{X}_1 \to \mathbb{G}$ is constant and we denote $h_0(x)$ as the constant. Similarly, we define $\mathcal{X}_1'$, ϕ_1, and $h_1(x)$.

Let $f'\colon \mathcal{X}_0' \times \mathcal{X}_1' \to \mathbb{G}$ be a restriction of f. Note that f' is non-redundant. Then, we can construct a two-party protocol Π for f from a two-party protocol Π' for f' with the same CR size, the number of rounds, and the communication complexity: $\Pi(x_0, x_1)$ computes $(g_0, g_1) \leftarrow \Pi'(\phi_0(x_0), \phi(x_1))$ and outputs $(g_0 + h_0(x_0), g_1 + h_1(x_1))$. CR size, the number of rounds, and the communication complexity of Π is the same as Π' and the security, and Π is secure when Π' is secure.