Efficient Constructions of Non-interactive Secure Multiparty Computation from Pairwise Independent Hashing

Satoshi Obana[1][a] and Maki Yoshida[2][b]
[1]*Hosei University, Tokyo, Japan*
[2]*NICT, Tokyo, Japan*

Keywords: Secure Multiparty Computation, Non-interactive, Information Theoretical Security, Communication Complexity, Pairwise Independent Hash Functions.

Abstract: An important issue of secure multi-party computation (MPC) is to improve the efficiency of communication. Non-interactive MPC (NIMPC) introduced by Beimel et al. in Crypto 2014 completely avoids interaction in the information theoretical setting by allowing a correlated randomness setup where the parties get *correlated* random strings beforehand and *locally* compute their messages sent to an external output server. Existing studies have been devoted to constructing NIMPC with small communication complexity, and many NIMPC have been presented so far. In this paper, we present a new generic construction of NIMPC for arbitrary functions from a class of functions called indicator functions. We employ pairwise independent hash functions to construct the proposed NIMPC, which results in smallest communication complexity compared to the existing generic constructions. We further present a concrete construction of NIMPC for the set of indicator functions with smallest communication complexity known so far. The construction also employs pairwise independent hash functions. It will be of independent interest to see how pairwise independent hash functions helps in constructing NIMPC.

1 INTRODUCTION

Since the seminal paper by Yao (Yao, 1982), secure multiparty computation (MPC for short) have been a central topic in the area of cryptographic research. The work is followed by a large number of literatures (Ben-Or et al., 1988; Chaum et al., 1988; Data et al., 2014; Hirt and Tschudi, 2013), and some of efficient implementations even possess a potential to deal with real-world application. Though, such efficient implementations are attractive, they demand high speed network connection (i.e., 10Gbps network) among parties for achieving high-throughput computation, and do not work well in poor network environment.

Beimel *et al.* have introduced a novel type of MPC called non-interactive multiparty computation (NIMPC for short). In NIMPC for a function $f : \mathcal{X}_1 \times \cdots \times \mathcal{X}_n \to \{0,1\}^L$, each party P_i receives correlated randomness r_i, and outputs m_i computed from r_i and a private input x_i so that $f(x_1,..,x_n)$ is computed only from $m_1, m_2, \ldots, m_n$. The notable feature of NIMPC is that it completely gets rid of interaction among parties since the message m_i is locally computed by P_i. The security model presented by Beimel *et al.* guarantees information-theoretic security against honest-but-curious adversaries. More precisely, it guarantees any set of corrupted parties learns nothing about inputs of uncorrupted parties and the function they aim to evaluate other than the information inferred from their inputs and output. Beimel *et al.* also showed NIMPC for various classes of functions. In particular, they showed that NIMPC for *arbitrary* functions is possible by showing an exact construction of an NIMPC for arbitrary functions. Though, since the communication complexity of their NIMPC is very large (exponential in the input length), their construction is valuable only in the sense it shows the possibility of realizing NIMPC for arbitrary functions.

Since the seminal work by Beimel *et al.*, the theory of NIMPC has been further developed by literatures (Yoshida and Obana, 2016; Obana and Yoshida, 2016; Halevi et al., 2016; Halevi et al., 2017; Agarwal et al., 2019). In Eurocrypt 2019, Agarwal *et al.* present elegant construction of NIMPC for arbitrary functions (Agarwal et al., 2019). In their con-

[a] https://orcid.org/0000-0003-4795-4779
[b] https://orcid.org/0000-0002-1267-0058

Obana, S. and Yoshida, M.
Efficient Constructions of Non-interactive Secure Multiparty Computation from Pairwise Independent Hashing.
DOI: 10.5220/0009819203220329
In *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020) - SECRYPT*, pages 322-329
ISBN: 978-989-758-446-6

Table 1: The communication complexity of n-player NIMPC protocols for arbitrary functions $h : \mathcal{X} \to \{0,1\}^L$ where $d \leq |\mathcal{X}_i|$, and δ_{ind} is the communication complexity of NIMPC for the set of indicator functions.

	The communication complexity
Construction in (Agarwal et al., 2019)	$\lceil \log_2 d \rceil + L \cdot |\mathcal{X}|$
Construction in (Beimel et al., 2014)	$\delta_{\mathrm{ind}} \cdot L \cdot |\mathcal{X}|$
Construction in (Obana and Yoshida, 2016)	$(\delta_{\mathrm{ind}} + L \cdot \lceil \log_2 (d+1) \rceil) \cdot |\mathcal{X}|$
Our construction (generic)	$(\delta_{\mathrm{ind}} + \max(2L, L + \lceil \log_2 d \rceil)) \cdot |\mathcal{X}|$
Our construction (concrete)	$(4 \cdot \lceil \log_2 d \rceil \cdot n + \max(2L, L + \lceil \log_2 d \rceil)) \cdot |\mathcal{X}|$

Table 2: The communication complexity of n-player NIMPC protocols for the set of indicator functions.

	The communication complexity
Construction in (Beimel et al., 2014)	$d^2 \cdot n$
Construction in (Yoshida and Obana, 2016)	$\lceil \log_2 (d+1) \rceil^2 \cdot n$
Our construction	$4 \cdot \lceil \log_2 d \rceil \cdot n$

struction, the correlated randomness r_i consists of additively shared output table of the target function f where input and output are masked with random values, and the message m_i consists of masked output table of $f(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_n)$, together with the masked value of a_i. Such direct construction is very efficient in the sense that the communication complexity of the scheme is as small as $\lceil \log_2 d \rceil + L \cdot |\mathcal{X}|$ where $d = \max_{i \in [n]}\{|\mathcal{X}_i|\}$ and $\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$. The communication complexity of their NIMPC is close to the lower bound on the communication complexity shown by Yoshida and Obana in (Yoshida and Obana, 2016), though, there is still a gap between the lower bound and the most efficient scheme known so far.

To deepen understanding of theory and practice of NIMPC, it is important to clarify to what extent we can construct a scheme with the communication complexity close to the lower bound. To answer the question, we must try various approaches to construct efficient NIMPCs. One of major and prominent approaches is *generic construction*. Generic construction of NIMPC is methodology to construct complex classes of function (e.g., arbitrary functions) based on simple classes of function. All the generic constructions known so far employ *indicator* function as a simple class of function, where indicator function $h_a(x) : \mathcal{X} \to \{0,1\}$ equals 1 if and only if the input x is identical to a. There is line of research that tries to construct an efficient NIMPC with small communication complexity based on NIMPC for the set of indicator functions (Beimel et al., 2014; Yoshida and Obana, 2016; Obana and Yoshida, 2016).

The contribution of the paper is twofold. First, we presents an efficient generic construction of NIMPC for arbitrary functions based on any NIMPC for the set of indicator functions. Second, we presents an efficient construction of NIMPC for the set of indicator functions. Combining the first and the second contributions, we obtain a concrete construction of NIMPC for arbitrary functions with the smallest communication complexity compared to existing generic constructions of NIMPC for arbitrary functions. Tables 1 and 2 summarize the communication complexity of existing NIMPC for arbitrary functions with L-bit output, and that of existing NIMPC for the set of indicator functions, respectively.

We see that the proposed NIMPC for the set of indicator function is the most efficient one, and the proposed generic construction is most efficient among generic constructions based on NIMPC for the set of indicator functions. Let δ_{ind} be the communication complexity of underlying NIMPC for set of indicator functions, and let $\log_2 d = L$ for simplicity. Then the communication complexity of the proposed NIMPC for arbitrary functions is $(\delta_{\mathrm{ind}} + 2L) \cdot |\mathcal{X}|$ while that of (Obana and Yoshida, 2016) is $(\delta_{\mathrm{ind}} + L^2) \cdot |\mathcal{X}|$. Compared to the most efficient NIMPC presented in (Agarwal et al., 2019), proposed NIMPC is less efficient, though, the overhead is not so large. Again, let $\lceil \log_2 d \rceil = L$ for the sake of simplicity, then the communication complexity of the proposed NIMPC for arbitrary functions becomes $L \cdot (4n+2) \cdot |\mathcal{X}|$, which is about $4n+2$ times larger than that of (Agarwal et al., 2019).

2 PRELIMINARIES

For an integer n, let $[n]$ be the set $\{1, 2, \ldots, n\}$. For a set $\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$ and $T \subseteq [n]$, we denote $\mathcal{X}_T \triangleq \prod_{i \in T} \mathcal{X}_i$. For $x \in \mathcal{X}$, we denote by x_T the restriction of x to $\mathcal{X}_T$, and for a function $h : \mathcal{X} \to \Omega$, a subset $T \subseteq [n]$, its complement $\overline{T} \subseteq [n]$, and $x_{\overline{T}} \in \mathcal{X}_{\overline{T}}$, we denote by $h|_{\overline{T}, x_{\overline{T}}} : \mathcal{X} \to \Omega$ the function h where the inputs of $\overline{T}$ are fixed to $x_{\overline{T}}$. For a set S, let $|S|$ denote its size (i.e., cardinality of S).

An NIMPC protocol for a family of functions $\mathcal{H}$ is defined by three algorithms: (1) a randomness generation function GEN, which given a description of a function $h \in \mathcal{H}$ generates n correlated random inputs $R_1, \ldots, R_n$, (2) a local encoding function ENC_i $(1 \leq i \leq n)$, which takes an input x_i and a random input R_i and outputs a message, and (3) a decoding algorithm DEC that reconstructs $h(x_1, \ldots, x_n)$ from the n messages. The formal definition given in (Beimel et al., 2014) is given as follows.

Definition 1 (Syntax and Correctness). *Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$, $\mathcal{R}_1$, ..., $\mathcal{R}_n$, $\mathcal{M}_1, \ldots, \mathcal{M}_n$ and Ω be finite domains. Let $X \triangleq \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$ and let $\mathcal{H}$ be a family of functions $h : \mathcal{X} \to \Omega$. A non-interactive secure multi-party computation (NIMPC) protocol for $\mathcal{H}$ is a triplet $\Pi = (\mathsf{GEN}, \mathsf{ENC}, \mathsf{DEC})$ where*

$\mathsf{GEN} : \mathcal{H} \to \mathcal{R}_1 \times \cdots \times \mathcal{R}_n$ is a random function,

ENC is an n-tuple deterministic functions $(\mathsf{ENC}_1, \ldots, \mathsf{ENC}_n)$, where $\mathsf{ENC}_i : \mathcal{X}_i \times \mathcal{R}_i \to \mathcal{M}_i$,

$\mathsf{DEC} : \mathcal{M}_1 \times \cdots \times \mathcal{M}_n \to \Omega$ is a deterministic function satisfying the following correctness requirement: for any $x = (x_1, \ldots, x_n) \in \mathcal{X}$ and $h \in \mathcal{H}$,

$$\Pr[R = (R_1, \ldots, R_n) \leftarrow \mathsf{GEN}(h) : \mathsf{DEC}(\mathsf{ENC}(x, R)) = h(x)] = 1, \quad (1)$$

where $\mathsf{ENC}(x, R) \triangleq (\mathsf{ENC}_1(x_1, R_1), \ldots, \mathsf{ENC}_n(x_n, R_n))$.

The communication complexity of NIMPC Π is defined to be the maximum value of $\log_2 |\mathcal{R}_1|, \ldots, \log_2 |\mathcal{R}_n|, \log_2 |\mathcal{M}_1|, \ldots, \log_2 |\mathcal{M}_n|$.

We next show the definition of robustness for NIMPC (Beimel et al., 2014), which states that a coalition can only learn the information they should. In the above setting, a coalition T can repeatedly encode any inputs for T and decode h with the new encoded inputs and the original encoded inputs of $\overline{T}$. Thus, the following robustness requires that they learn no other information than the information obtained from oracle access to $h|_{\overline{T}, x_{\overline{T}}}$.

Definition 2 (Robustness). *For a subset $T \subseteq [n]$, we say that an NIMPC protocol Π for $\mathcal{H}$ is T-*robust *if there exists a randomized function Sim_T (a "simulator") such that, for every $h \in \mathcal{H}$ and $x_{\overline{T}} \in \mathcal{X}_{\overline{T}}$, we have $Sim_T(h|_{\overline{T}, x_{\overline{T}}}) \equiv (M_{\overline{T}}, R_T)$, where R and M are the joint randomness and messages defined by $R \leftarrow \mathsf{GEN}(h)$ and $M_i \leftarrow \mathsf{ENC}_i(x_i, R_i)$.*

*For an integer $0 \leq t \leq n$, we say that Π is t-*robust *if it is T-robust for every $T \subseteq [n]$ of size $|T| \leq t$. We say that Π is* fully robust *(or simply refer to Π as an NIMPC for $\mathcal{H}$) if Π is n-robust. Finally, given a concrete function $h : \mathcal{X} \to \Omega$, we say that Π is a (t-robust) NIMPC protocol for h if it is a (t-robust) NIMPC for $\mathcal{H} = \{h\}$.*

As the same simulator Sim_T is used for every $h \in \mathcal{H}$ and the simulator has only access to $h|_{\overline{T}, x_{\overline{T}}}$, NIMPC hides both h and the inputs of $\overline{T}$. An NIMPC protocol is 0-robust if it is $\emptyset$-robust. In this case, the only requirement is that the messages $(M_1, \ldots, M_n)$ reveal $h(x)$ and nothing else.

An NIMPC protocol is also described in the language of protocols in (Beimel et al., 2014). Such a protocol involves n players $P_1, \ldots, P_n$, each holding an input $x_i \in \mathcal{X}_i$, and an external "output server," a player P_0 with no input. The protocol may have an additional input, a function $h \in \mathcal{H}$.

Definition 3 (Protocol Description). *For an NIMPC protocol Π for $\mathcal{H}$, let $\mathrm{P}(\Pi)$ denote the protocol that may have an additional input, a function $h \in \mathcal{H}$, and proceeds as follows.*

Protocol $\mathrm{P}(\Pi)(h)$

Offline Preprocessing. *Each player P_i, $1 \leq i \leq n$, receives the random input $R_i \triangleq \mathsf{GEN}(h)_i \in \mathcal{R}_i$.*

Online Messages. *On input R_i, each player P_i, $1 \leq i \leq n$, sends the message $M_i \triangleq \mathsf{ENC}_i(x_i, R_i) \in \mathcal{M}_i$ to P_0.*

Output. *P_0 computes and outputs $\mathsf{DEC}(M_1, \ldots, M_n)$.*

Informally, the relevant properties of protocol $\mathrm{P}(\Pi)$ are given as follows:

- For any $h \in \mathcal{H}$ and $x \in \mathcal{X}$, the output server P_0 outputs, with probability 1, the value $h(x_1, \ldots, x_n)$.
- Fix $T \subseteq [n]$. Then, Π is T-robust if in $\mathrm{P}(\Pi)$ the set of players $\{P_i\}_{i \in T} \cup \{P_0\}$ can simulate their view of the protocol (i.e., the random inputs $\{R_i\}_{i \in T}$ and the messages $\{M_i\}_{i \in \overline{T}}$) given oracle access to the function h restricted by the other inputs (i.e., $h|_{\overline{T}, x_{\overline{T}}}$).
- Π is 0-robust if and only if in $\mathrm{P}(\Pi)$ the output server P_0 learns nothing but $h(x_1, \ldots, x_n)$.

A lower bound on the communication complexity for any finite set of functions including the set of arbitrary functions was derived in (Yoshida and Obana, 2016). The result states that the communication complexity cannot be smaller than the logarithm of the size of the target class.

Proposition 1 (Lower Bound). *Fix finite domains $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and Ω. Let $\mathcal{X} \triangleq \mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{H}$ a set of functions $h : \mathcal{X} \to \Omega$. Then, any fully robust NIMPC protocol Π for $\mathcal{H}$ satisfies $\sum_{i=1}^{n} \log |\mathcal{R}_i| \geq \log |\mathcal{H}|$, and $\sum_{i=1}^{n} \log |\mathcal{M}_i| \geq \log |\Omega|$.*

Proposition 2 (Lower Bound). *Fix finite domains $\mathcal{X}_1, \ldots, \mathcal{X}_n$. Let $\mathcal{X} \triangleq \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$ and $\mathcal{H}_{\text{all}}^L$ the set of all functions $h : \mathcal{X} \to \{0,1\}^L$. Any NIMPC protocol Π for $\mathcal{H}_{\text{all}}^L$ satisfies $\sum_{i=1}^n \log|\mathcal{R}_i| \geq L \cdot |\mathcal{X}|$, and $\sum_{i=1}^n \log|\mathcal{M}_i| \geq L$.*

Here, we give definitions of indicator functions (Beimel et al., 2014), and generalized indicator functions (Obana and Yoshida, 2016) which are important classes of functions for our proposed construction.

Definition 4 (Indicator Functions). *Let $\mathcal{X}$ be a finite domain. For n-tuple $a = (a_1, \ldots, a_n) \in \mathcal{X}$, let $h_a : \mathcal{X} \to \{0,1\}$ be the function defined by $h_a(a) = 1$, and $h_a(x) = 0$ for all $a \neq x \in \mathcal{X}$. Let $h_0 : \mathcal{X} \to \{0,1\}$ be the function that is identically zero on $\mathcal{X}$. Let $\mathcal{H}_{\text{ind}} \triangleq \{h_a\}_{a \in \mathcal{X}} \cup \{h_0\}$ be the set of all indicator functions together with h_0.*

Definition 5 (Generalized Indicator Func.). *Let L be a positive integer $L > 0$. For $v \in \{0,1\}^L \setminus \{0^L\}$ and $a = (a_1, \ldots, a_n) \in \mathcal{X}$, we define the generalized indicator function $h_{a,v}$ as follows.*

$$h_{a,v}(x) = \begin{cases} v & \text{if } x = a \\ 0^L & \text{otherwise} \end{cases}$$

Let $h_0^L : \mathcal{X} \to \{0,1\}^L$ be the function that is identically 0^L on $\mathcal{X}$. We define the family of functions $\mathcal{H}_{ind}^L = \{h_{a,v}\}_{a \in \mathcal{X}, v \in \{0,1\}^L \setminus \{0^L\}} \cup \{h_0\}$.

In the next section, we will presents a generic construction of NIMPC for arbitrary set of functions. We employ pairwise independent hash functions to construct NIMPC for the set of generalized indicator functions. We note that pairwise independent hash function plays an important role in constructing various cryptographic protocols.

Definition 6. *A family of functions $\mathsf{G} = \{\mathsf{g} \mid \mathsf{g} : X \to Y\}$ is* pairwise independent *if the following two conditions hold when $\mathsf{g} \in \mathsf{G}$ is a function chosen uniformly at random from G:*

1. *For any $x \in X$, the random variable $\mathsf{g}(x)$ is uniformly distributed in Y.*
2. *For any distinct $x_1, x_2 \in X$, the random variables $\mathsf{g}(x_1)$ and $\mathsf{g}(x_2)$ are independent.*

When the function g is chosen uniformly at random from G, we can guarantee $\mathsf{g}(x)$ does not reveal any information about x. Further, the value $\mathsf{g}(x)$ does not reveal any information about the value $\mathsf{g}(x')$ such that $x' \neq x$. These properties of pairwise independent hash family help us in constructing NIMPC.

The following proposition gives a well-known fact about pairwise independent hash functions (e.g., (Vadhan, 2012)).

Proposition 3. *For every positive integer n, m, there is an family of pairwise independent functions $\mathsf{G}_{n,m} = \{\mathsf{g} : \{0,1\}^n \to \{0,1\}^m\}$ where a random function function from $\mathsf{G}_{n,m}$ can be selected using $\max(m,n) + m$ random bits.*

Let $\mathsf{G}_{n,m,\geq}$ and $\mathsf{G}_{n,m,<}$ be function families defined as follows where $\|$ denotes concatenation of bit strings, and $\phi_{n,m} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ denotes any surjective linear mapping:

$$\mathsf{G}_{n,m,\geq} = \left\{ \mathsf{g}'_{a,b} \,\middle|\, \begin{array}{c} \mathsf{g}'_{a,b}(x) = a \cdot (0^{m-n} \| x) + b, \\ a, b \in \mathbb{F}_{2^n} \end{array} \right\}$$

$$\mathsf{G}_{n,m,<} = \left\{ \mathsf{g}''_{a,b} \,\middle|\, \begin{array}{c} \mathsf{g}''_{a,b}(x) = \phi_{n,m}(a \cdot x) + b, \\ a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m} \end{array} \right\}$$

Then pairwise independent function family is constructed as follows

$$\mathsf{G}_{n,m} = \begin{cases} \mathsf{G}_{n,m,\geq} & \text{if } m \geq n \\ \mathsf{G}_{n,m,<} & \text{if } m < n \end{cases}$$

We note that any function in $\mathsf{G}_{n,m}$ can be described by $\max(m,n) + m$ bits (i.e., (a,b)) which we call *description* of the function $\mathsf{g}_{a,b}$, and denote it by $\mathsf{desc}(\mathsf{g}_{a,b})$. We also note some pairwise independent function families (including $\mathsf{G}_{n,m}$ described above) possess such an extra property that $\mathsf{desc}(\mathsf{g})$ can be sampled efficiently even when an output of $\mathsf{g}(a)$ is fixed to some value b for a single input a. We will use such function family in our constructions.

3 PROPOSED CONSTRUCTION

In this section, we presents NIMPC for $\mathcal{H}_{\text{all}}^L$, arbitrary functions with L-bit output from any NIMPC for $\mathcal{H}_{\text{ind}}$. The communication complexity of the proposed construction is $(\delta_{\text{ind}} + \max(2L, L + \lceil \log_2 d \rceil)) \cdot |\mathcal{X}|$ where δ_{ind} denotes the communication complexity of underlying NIMPC for $\mathcal{H}_{\text{ind}}$.

3.1 Overview of the Protocol

Historically, there two different approaches to construct NIMPC for arbitrary functions from NIMPC for the set of indicator functions. The first approach adopted in (Beimel et al., 2014; Yoshida and Obana, 2016) makes use of the fact that every function $h : \mathcal{X} \to \{0,1\}$ can be expressed as the sum of indicator functions $h = \sum_{a \in \mathcal{X}, h(a)=1} h_a$. They construct NIMPC for arbitrary function $h : \mathcal{X} \to \{0,1\}$ by $|\mathcal{X}|$ independent invocation of NIMPC for $\mathcal{H}_{\text{ind}}$, and realize NIMPC for $\mathcal{H}_{\text{ind}}^L$ by L independent invocation of NIMPC for $\mathcal{H}_{\text{ind}}$. Let δ_{ind} be the communication complexity of underlying NIMPC for indicator function. Then the communication complexity of resulting NIMPC for arbitrary functions is $\delta_{\text{ind}} \cdot L \cdot |\mathcal{X}|$.

In (Obana and Yoshida, 2016), Obana and Yoshida present the second approach to construct NIMPC for arbitrary functions. While the first approach separately compute each output bit, the second approach simultaneously computes all output bits. The key idea of the second approach is to introduce *generalized* indicator functions $h_{a,v}(x)$ outputting $v \in \{0,1\}^L$ if $x = a$ holds, and otherwise 0^L. Their construction is based on the observation that arbitrary function $h : \mathcal{X} \to \{0,1\}^L$ is represented by the sum of $h_{a,v} \in \mathcal{H}^L_{\text{ind}}$ (i.e., $h = \sum_{a \in \mathcal{X}, h(a) \neq 0^L} h_{a,h(a)}$), and use the fact to construct NIMPC for $\mathcal{H}^L_{\text{all}}$. The generic construction of (Obana and Yoshida, 2016) reduces the communication complexity to $\frac{\delta_{\text{ind}} \cdot L}{\delta_{\text{ind}} + L \cdot \lceil \log_2 |\mathcal{X}| \rceil}$ times smaller than that of the first approach.

In the proposed construction, we adopt the same approach as in (Obana and Yoshida, 2016), that is, starting from an NIMPC for the set of indicator function, we construct an NIMPC for the set of generalized indicator function, which is used to construct NIMPC for the set of arbitrary function. The main difference between our construction and that in (Obana and Yoshida, 2016) is in the building block to construct an NIMPC for the set of generalized indicator functions. The construction in (Obana and Yoshida, 2016) employs binary vectors to extend the range of indicator function. On the other hands, we employ pairwise independent hash functions to extend the range, which results in NIMPC for arbitrary functions with smaller communication complexity.

3.2 NIMPC $\mathcal{H}_{\text{ind}} \Rightarrow$ NIMPC $\mathcal{H}^L_{\text{ind}}$

Here, we will give a generic construction of NIMPC for $\mathcal{H}^L_{\text{ind}}$ from any NIMPC for $\mathcal{H}_{\text{ind}}$. The basic idea behind the proposed generic construction is as follows. We will use an NIMPC $\Pi_{\text{ind}} = (\mathsf{GEN}', \mathsf{ENC}', \mathsf{DEC}')$ for $\mathcal{H}_{\text{ind}}$ to check whether the function $h \in \mathcal{H}^L_{\text{ind}}$ outputs non-zero value with the input $(x_1, \ldots, x_n) \in \mathcal{X}$. To obtain the actual output value (i.e., $h(x_1, \ldots, x_n)$), we employ functions g_i from pairwise independent hash family $\mathsf{G}_i : \mathcal{X}_i \to \mathbb{F}_{2^L}$ for $i \in [n]$. Functions $\mathsf{g}_i \in \mathsf{G}_i$ are chosen in such a way that $\sum_{i=1}^n \mathsf{g}_i(x_i) = h(x_1, \ldots, x_n)$ holds if the input $(x_1, \ldots, x_n)$ is identical to the input with which DEC' outputs 1.

Let $\Pi_{\text{ind}} = (\mathsf{GEN}', \mathsf{ENC}', \mathsf{DEC}')$ be any NIMPC for $\mathcal{H}_{\text{ind}}$. Then the concrete description of the proposed construction of NIMPC for $\mathcal{H}^L_{\text{ind}}$, denoted by $\Pi_{\text{gind}} = (\mathsf{GEN}, \mathsf{ENC}, \mathsf{DEC})$, is given as follows. For $i \in [n]$, let g_i be an element of pairwise independent hash family $\mathsf{G}_i : \mathcal{X}_i \to \{0,1\}^L$.

Fix a function $h \in \mathcal{H}^L_{\text{ind}}$ that we want to compute.

Offline Preprocessing. First, define a function $h' \in \mathcal{H}_{\text{ind}}$ as follows,

$$h' = \begin{cases} h_0 & \text{if } h = h^L_0 \\ h_a & \text{otherwise } \left(\text{i.e., } {}^{\exists a \in \mathcal{X}, v \in \{0,1\}^L \setminus \{0^L\}}_{\text{s.t. } h = h_{a,v}}\right) \end{cases}$$

and let $R' = (R'_1, \ldots, R'_n) \leftarrow \mathsf{GEN}(h')$. Next, if $h = h^L_0$ then choose n random functions $\mathsf{g}_i \in \mathsf{G}_i$. If $h = h_{a,v}$ for some $a = (a_1, \ldots, a_n) \in \mathcal{X}$ and $v \in \{0,1\}^L \setminus \{0^L\}$, choose $n-1$ functions g_i uniformly and randomly from G_i for $i \in [n-1]$ and choose a function $\mathsf{g}_n \in \mathsf{G}_n$ such that $\sum_{i=1}^n \mathsf{g}_i(a_i) = v$ holds, which can be done by choosing g_n from the function family $\{\mathsf{g}_n \mid \mathsf{g}_n \in \mathsf{G}_n, \mathsf{g}_n(a_n) = v - \sum_{i=1}^{n-1} \mathsf{g}(a_i)\}$ uniformly and randomly. Define $\mathsf{GEN}(h) \triangleq R = (R_1, \ldots, R_n)$ where $R_i = (R'_i, \mathsf{desc}(\mathsf{g}_i))$

Online Messages. For $R_i = (R'_i, \mathsf{desc}_i)$ and an input x_i, we first evaluate $(M'_1, \ldots, M'_n) \leftarrow \mathsf{ENC}(x, R')$. Next, we evaluate $v_i = \mathsf{g}_i(x_i)$ where g_i is an element of G_i described by desc_i. Finally, let $\mathsf{ENC}(x, R) \triangleq (M_1, \ldots, M_n)$ where $M_i = (M'_i, v_i)$.

Output $h(x_1, \ldots, x_n)$. $\mathsf{DEC}(M_1, \ldots, M_n) = \sum_{i=1}^n v_i$ if $\mathsf{DEC}(M'_1, \ldots, M'_n) = 1$ holds. Otherwise $\mathsf{DEC}(M_1, \ldots, M_n) = 0^L$.

Theorem 1. *Fix finite domains $\mathcal{X}_1, \ldots, \mathcal{X}_n$, and let $\mathcal{X} \triangleq \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$. If there exists a robust NIMPC for $\mathcal{H}_{ind} : \mathcal{X} \to \{0,1\}$ with communication complexity δ_{ind}, then there is an NIMPC protocol for $\mathcal{H}^L_{ind}$ with the communication complexity $\delta_{ind} + \max(2L, L + \lceil \log_2 d \rceil)$.*

Proof: First, we will show the correctness. Let $M_i = (M'_i, v_i)$. It holds that $\sum_{i=1}^n v_i = \sum_{i=1}^n \mathsf{g}_i(x_i)$. If $h = h_{a,v}$, then $\mathsf{DEC}'(M'_1, \ldots, M'_n) = 1$ holds if and only if $a = x$. In this case $\sum_{i=1}^n v_i = \sum_{i=1}^n \mathsf{g}_i(a_i) = v$ holds. This means $\mathsf{DEC}(M_1, \ldots, M_n) = v$ if and only if $x = a$. If $h = h_0$, then $\mathsf{DEC}(M'_1, \ldots, M'_n) = 1$ never happens because of the correctness of the underlying NIMPC for $\mathcal{H}_{\text{ind}}$. This means $\mathsf{DEC}(M_1, \ldots, M_n) = 0^L$ holds for any $x \in \mathcal{X}$.

To prove robustness, fix a subset $T \subseteq [n]$ and $x_{\overline{T}} \in \mathcal{X}_{\overline{T}}$. The encodings $M_{\overline{T}}$ of $\overline{T}$ consist of $\{(M'_i, v_i)\}_{i \in \overline{T}}$. The randomness R_T consists of $\{(R'_i, \mathsf{desc}(\mathsf{g}_i))\}_{i \in T}$. Now we will construct a simulator Sim_T which queries $h|_{\overline{T}, x_{\overline{T}}}$ on all possible inputs in $\mathcal{X}_T$. First we will simulate $(R'_T, M'_{\overline{T}})$. Since $R' = \mathsf{GEN}'(h')$ and $M' = \mathsf{ENC}'(R', x)$ hold, and $\Pi_{\text{ind}} = (\mathsf{GEN}', \mathsf{ENC}', \mathsf{DEC}')$ is robust, it is possible to simulates $(R'_T, M'_{\overline{T}})$ if we can answer to a query to $h'|_{\overline{T}, x_{\overline{T}}}$, which is easily computed from $h|_{\overline{T}, x_{\overline{T}}}$ as follows.

$$h'|_{\overline{T},x_{\overline{T}}}(x_T) = \begin{cases} 0 & \text{if } h|_{\overline{T},x_{\overline{T}}}(x_T) = 0^L \\ 1 & \text{otherwise} \end{cases}$$

Next, we will simulate $\mathsf{desc}(g_i)$ for $i \in T$ and $v_i(= g_i(x_i))$ for $i \in \overline{T}$. If $h|_{\overline{T},x_{\overline{T}}} \equiv 0^L$, there are two possible cases. The first case is $h = h_0$. In this case $\mathsf{desc}(g_i)$ $(i \in T)$ and v_i $(i \in \overline{T})$ are uniformly and independently distributed since all g_i are uniformly and independently distributed. The second case to consider is $h = h_{a,v}$ for some a, v and $a_{\overline{T}} \neq x_{\overline{T}}$. In this case, g_i (and therefore $\mathsf{desc}(g_i)$) for $i \in [n]$ are uniformly and independently distributed under the constraint $\sum_{i\in[n]} g_i(a_i) = v$. In this case, from the properties of pairwise independent hash functions, g_i $(i \in T)$ and $v_i(= g_i(x_i))$ $(i \in \overline{T})$ are uniformly and independently distributed. From the above argument, we conclude that the $\mathsf{desc}(g_i)$ for $i \in T$ and v_i for $i \in \overline{T}$ are uniformly and independently distributed in both cases. Therefore, if $h|_{\overline{T},x_{\overline{T}}} \equiv 0$ then $\mathsf{desc}(g_i)$ $(i \in T)$ and $v_i(= g_i(x_i))$ are simulated simply by assigning uniformly distributed random strings to them. On the other hand, if $h|_{\overline{T},x_{\overline{T}}}(x_T) = v(\neq 0^L)$ holds for some $x_T \in \mathcal{X}_T$, then $\sum_{i\in[n]} g(a_i) = v$ holds. Let $\hat{i} \in \overline{T}$, then $\mathsf{desc}(g_i)$ $(i \in T)$ and $g_i(x_i)$ $(i \in \overline{T})$ are simulated by assigning uniform random strings to $\mathsf{desc}(g_i)$ $(i \in T)$ and v_i $(i \in \overline{T} \setminus \{\hat{i}\})$ and by assigning $v + (\sum_{i\in T} g_i(a_i)) + (\sum_{i\in\overline{T}\setminus\{\hat{i}\}} v_i)$ to $v_{\hat{i}}$.

Now, we will evaluate the communication complexity of the resulting NIMPC. Let δ_{ind} be the communication complexity of the underlying NIMPC for $\mathcal{H}_{\mathrm{ind}}$. The correlated randomness R_i is composed of R'_i and $L + \max(L, \lceil \log_2 d \rceil)$ binary string, whereas the encoding M_i is composed of M'_i and L-bit binary string. Therefore, the communication complexity is at most $\delta_{\mathrm{ind}} + \max(2L, L + \lceil \log_2 d \rceil)$. □

3.3 NIMPC $\mathcal{H}^L_{\mathrm{ind}} \Rightarrow$ NIMPC $\mathcal{H}^L_{\mathrm{all}}$

In this section, we present a generic construction of NIMPC for all L-bit boolean functions $\mathcal{H}^L_{\mathrm{all}}$ with input domain $\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$ from any NIMPC for $\mathcal{H}^L_{\mathrm{ind}}$ with the same input domain. The idea is to express any $h : \mathcal{X} \to \{0,1\}^L$ as a sum of generalized indicator functions $\mathcal{H}^L_{\mathrm{ind}}$ with L-bit output. The communication complexity of the resulting construction is much smaller than the existing constructions since a single invocation of the proposed NIMPC for $\mathcal{H}^L_{\mathrm{ind}}$ given in §3.2 is much more efficient than L invocation of the existing NIMPC for $\mathcal{H}_{\mathrm{ind}}$ for most L.

The detailed description of the compiler to construct $\mathcal{H}_{\mathrm{all}}$ from $\mathcal{H}^L_{\mathrm{ind}}$ is identical to that presented in (Obana and Yoshida, 2016). Let $\Pi^L_{\mathrm{ind}} = (\mathsf{GEN}', \mathsf{ENC}', \mathsf{DEC}')$ be any NIMPC for $\mathcal{H}^L_{\mathrm{ind}}$ and let $h : \mathcal{X} \to \{0,1\}^L$ that we want to compute. We construct a protocol $\mathrm{P}(\Pi)(h)$ for $\mathcal{H}_{\mathrm{all}}$, whose algorithms are denoted by $(\mathsf{GEN}, \mathsf{ENC}, \mathsf{DEC})$, as follows.

Offline Preprocessing. Let $I \subseteq \mathcal{X}$ be the set of inputs $x \in \mathcal{X}$ such that $h(x) \neq 0^L$. For each $a \in I$, let $R^a = (R^a_1, \ldots, R^a_n) \leftarrow \mathsf{GEN}'(h_{a,v})$. For $a \in \mathcal{X} \setminus I$, let $R^a \leftarrow \mathsf{GEN}'(h_0)$. Then, choose random permutation π of $\mathcal{X}$ and let $R_{i,b} = R_i^{\pi(b)}$ for $i \in [n], b \in \mathcal{X}$. Define $\mathsf{GEN}(h) \triangleq R = (R_1, \ldots, R_n)$, where $R_i = \{R_{i,b}\}_{b\in\mathcal{X}}$.

Online Messages. For an input x_i, P_i computes $M_{i,b} \triangleq \mathsf{ENC}'_i(x_i, R_{i,b})$ for every $b \in \mathcal{X}$. Define $\mathsf{ENC}(x,R) \triangleq (M_1, \ldots, M_n)$ where $M_i = \{M_{i,b}\}_{b\in\mathcal{X}}$.

Output $h(x_1, \ldots, x_n)$. $\mathsf{DEC}(M_1, \ldots, M_n) = v$ if and only if there exists $b \in \mathcal{X}$ such that $\mathsf{DEC}'(M_{1,b}, \ldots, M_{n,b}) = v$. Otherwise $\mathsf{DEC}(M_1, \ldots, M_n) = 0^L$.

Theorem 2. *Fix finite domains $\mathcal{X}_1, \ldots, \mathcal{X}_n$, and let $\mathcal{X} \triangleq \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$. Let $\mathcal{H}_{all}$ be the set of all functions $h : \mathcal{X} \to \{0,1\}^L$. If there exists a robust NIMPC for $\mathcal{H}^L_{ind} : \mathcal{X} \to \{0,1\}^L$ with communication complexity δ_{gind}, then there is an NIMPC protocol for $\mathcal{H}_{all}$ with the communication complexity $\delta_{gind} \cdot |\mathcal{X}|$.*

The proof is almost identical to that of Theorem 2 of (Obana and Yoshida, 2016), and is omitted here.

By combining Theorem 1 and Theorem 2, we obtain the following corollary.

Corollary 1 *Fix finite domains $\mathcal{X}_1, \ldots, \mathcal{X}_n$, and let $\mathcal{X} \triangleq \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$. Let $\mathcal{H}_{all}$ be the set of all functions $h : \mathcal{X} \to \{0,1\}^L$. If there exists a robust NIMPC for $\mathcal{H}_{ind} : \mathcal{X} \to \{0,1\}$ with communication complexity δ_{ind}, then there is an NIMPC protocol for $\mathcal{H}_{all}$ with the communication complexity $(\delta_{ind} + \max(2L, L + \lceil \log_2 d \rceil)) \cdot |\mathcal{X}|$.*

4 EFFICIENT NIMPC for $\mathcal{H}_{\mathrm{ind}}$

In this section, we present a construction of NIMPC for $\mathcal{H}_{\mathrm{ind}}$, which results in $\mathcal{H}^L_{\mathrm{all}}$ via generic construction given in the previous section. As the generic construction to construct $\mathcal{H}^L_{\mathrm{ind}}$, we also employ pairwise independent hash family to construct $\mathcal{H}_{\mathrm{ind}}$. It should be noted that, if $d \geq 4$ (i.e., if the maximum bit length of input is larger then 1), the proposed construction of NIMPC for $\mathcal{H}_{\mathrm{ind}}$ offers smallest communication complexity known so far. Namely, the communication complexity of the proposed construction is $4 \cdot \lceil \log_2 d \rceil \cdot n$ whereas that of the best known construction (i.e., the construction in (Yoshida and Obana, 2016)) is $(\lceil \log_2 (d+1) \rceil)^2 \cdot n$.

The detailed description of the protocol is as follows. For $i \in [n]$, let ϕ_i be a one-to-one mapping from X_i to a finite field $\mathbb{F}$ with the order lager than $\max_i |X_i|$. Fix a function $h \in \mathcal{H}_{\text{ind}}$ that we want to compute.

The proposed NIMPC $\Pi_{\text{ind}}(h)$

Offline Preprocessing. If $h = h_0$, then choose $2n$ linearly independent random vectors $\{v_i, v_i'\}_{i\in[n]}$ in $\mathbb{F}^{2n}$. If $h = h_a$ for some $a = (a_1, \ldots, a_n) \in X$, then choose $2n$ random vectors $\{v_i, v_i'\}_{i\in[n]}$ in $\mathbb{F}^{2n}$ such that $\sum_{i=1}^{n}(v_i + \phi(a_i)v_i') = 0$, and there are no other linear relations other than $\sum_{i=1}^{n} c\cdot(v_i+\phi(a_i)v_i') = 0$ for $c \in \mathbb{F}$. Let $\mathsf{GEN}(h) = R = (R_1, \ldots, R_n)$, where $R_i = \{v_i, v_i'\}$.

Online Messages. For an input x_i, let $\mathsf{ENC}(x,R) = (M_1, \ldots, M_n)$ where $M_i = v_i + \phi_i(x_i)v_i'$.

Output $h(x_1, \ldots, x_n)$**.** $\mathsf{DEC}(M_1, \ldots, M_n) = 1$ if $\sum_{i=1}^{n} M_i = 0$.

Theorem 3 . *Fix finite domains $X_1, \ldots, X_n$ Then, there is an NIMPC protocol Π_{ind} for $\mathcal{H}_{\text{ind}}$ with the communication complexity $4\cdot\lceil\log_2 d\rceil\cdot n$.*

Proof: The correctness is obvious from the description of Offline preprocessing. Namely, $\sum_{i=1}^{n}(v_i + x_i'v_i') = 0$ never happen with $(x_1', \ldots, x_n') \neq (a_1, \ldots, a_n)$. In fact, $\sum_{i=1}^{n}(v_i + a_iv_i') = 0$ is the only possible solution since coefficient of v_i is fixed to 1. Moreover, $\sum_{i=1}^{n}(v_i + x_i'v_i') = 0$ never happen when $h = h_0$ since all v_i, v_i' are linearly independent in this case.

To prove the robustness, we describe a simulator Sim_T: the simulator queries $h|_{\overline{T},x_{\overline{T}}}$ on all possible inputs in X_T. If all answers are zero, this simulator generates random independent vectors v_i, v_i' (for $i \in T$) and m_i (for $i \in \overline{T}$). Otherwise, there is an $\hat{x_T} \in X_T$ such that $h|_{\overline{T},x_{\overline{T}}}(\hat{x_T}) = 1$, and the simulator outputs random vectors such that $\sum_{i\in\overline{T}} m_i + \sum_{i\in T}(v_i + \phi_i(\hat{x}_i)v_i') = 0$, and there are no other linear relations other than $\sum_{i=1}^{n} c\cdot(v_i + \phi(\hat{x}_i)v_i') = 0$ for $c \in \mathbb{F}$.

The communication complexity of the resulting protocol is $4\cdot\lceil\log_2 d\rceil\cdot n$ since R_i consists of $2\cdot 2n$ elements of finite field $\mathbb{F}$ with $|\mathbb{F}| \le d$. □

By combining Theorem 3 and Corollary 2, we obtain the following corollary.

Corollary 2 *Fix finite domains $X_1, \ldots, X_n$ with $|X_i| \le d$ for all $1 \le i \le n$ and let $X \triangleq X_1 \times \cdots \times X_n$. Then, there is an NIMPC protocol for $\mathcal{H}_{\text{all}} : X \to \{0,1\}^L$ with communication complexity at most $(4\cdot\lceil\log_2 d\rceil\cdot n + \max(2L, L+\lceil\log_2 d\rceil))\cdot|X|$.*

Let δ_{ind} be the communication complexity of underlying NIMPC for $\mathcal{H}_{\text{ind}}$, and suppose, for the sake of simplicity, $|X_i| = 2^L$ for any $i \in [n]$. Then the communication complexity of the proposed NIMPC for $\mathcal{H}_{\text{all}}^L$ becomes $(\delta_{\text{ind}} + 2L)|X|$, which is the most efficient construction among existing NIMPCs for arbitrary functions constructed based on NIMPC for the set of indicator functions since the best known communication complexity of such NIMPC is $(\delta_{\text{ind}} + L^2)|X|$.

5 CONCLUSION

In this paper, we have presented a novel generic construction of NIMPC for the set of arbitrary functions $\mathcal{H}_{\text{all}}^L$ from NIMPC for the set of indicator functions $\mathcal{H}_{\text{ind}}$. The communication complexity of the resulting scheme is the most efficient compared to that of NIMPC for arbitrary functions constructed based on NIMPC for the set of indicator functions. Further, we have presented an NIMPC for the set of indicator functions with the smallest communication complexity known so far. By combining the proposed generic construction and the proposed NIMPC for $\mathcal{H}_{\text{ind}}$, we have obtained a concrete NIMPC for arbitrary functions with the communication complexity $(4\cdot\lceil\log_2 d\rceil\cdot n + \max(2L, L+\lceil\log_2 d\rceil))\cdot|X|$. Compared to the most efficient NIMPC known so far (i.e., NIMPC presented in (Agarwal et al., 2019), the proposed NIMPC is less efficient, though, the gap is as small as $4n+2$.

Though the proposed construction is pretty efficient with respect to the communication complexity, there still remains a gap between the lower bound in (Yoshida and Obana, 2016) and our upper bound. Therefore, reducing the gap will be a challenging future work.

REFERENCES

Agarwal, N., Anand, S., and Prabhakaran, M. (2019). Uncovering algebraic structures in the mpc landscape. In *Advances in Cryptology – EUROCRYPT 2019 in Lecture Notes in Comput. Sci. 11477*, pages 381–406. Springer Verlag.

Beimel, A., Gabizon, A., Ishai, Y., Kushilevitz, E., Meldgaard, S., and Paskin-Cherniavsky, A. (2014). Non-interactive secure multiparty computation. In *Advances in Cryptology - CRYPTO2014 in Lecture Notes in Comput. Sci. 8617*, pages 387–404. Springer Verlag.

Ben-Or, M., Goldwasser, S., and Wigderson, A. (1988). Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *The 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 1–10. ACM Press.

Chaum, D., Crèpeau, C., and Damgård, I. (1988). Multi-party unconditionally secure protocols. In *The 20th*

Annual ACM Symposium on Theory of Computing (STOC '88), pages 11–19. ACM Press.

Data, D., Prabhakaran, M., and Prabhakaran, V. (2014). On the communication complexity of secure computation. In *Advances in Cryptology - CRYPTO2014 in Lecture Notes in Comput. Sci. 861*, pages 199–216. Springer Verlag.

Halevi, S., Ishai, Y., A. Jain, I. K., Sahai, A., , and Yogev, E. (2017). Non-interactive multiparty computation without correlated randomness. In *Advances in Cryptology - Asiacrypt 2017, Part III in Lecture Notes in Comput. Sci. 10626*, page 181–211. Springer Verlag.

Halevi, S., Ishai, Y., Jain, A., Kushilevitz, E., and .Rabin, T. (2016). Secure multiparty computation with general interaction patterns. In *the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 157—-168. ACM Press.

Hirt, M. and Tschudi, D. (2013). Efficient general-adversary multi-party computation. In *Advances in Cryptology - Asiacrypt 2013, Part II in Lecture Notes in Comput. Sci. 8270*, pages 181–200. Springer Verlag.

Obana, S. and Yoshida, M. (2016). An efficient construction of non-interactive secure multiparty computation. In *the 15th International Conference on Cryptology and Network Security, CANS2016, in Lecture Notes in Comput. Sci. 10052*, pages 604–614. Springer Verlag.

Vadhan, S. (2012). Pseudorandomness. In *Foundations and Trends in Theoretical Computer Science, vol. 7, no. 1–3*, pages 1–336.

Yao, A. C. (1982). Protocols for secure computations. In *The 23rd Annual Symposium on Foundations of Computer Science (FOCS '82)*, pages 160–164. IEEE.

Yoshida, M. and Obana, S. (2016). On the (in)efficiency of non-interactive secure multiparty computation. In *the 18th Annual International Conference on Information Security and Cryptology, ICISC2015, in Lecture Notes in Comput. Sci. 9558*, pages 185–93. Springer Verlag.