Detection of Cheaters in Non-interactive Polynomial Evaluation

Maki Yoshida[1] and Satoshi Obana[2]

[1] Osaka University, Japan
[2] Hosei University, Japan

Abstract. In this paper, we consider both theoretical and practical aspects of robust NI-PE (non-interactive polynomial evaluation with detection of cheaters). First, we give a necessary condition of adversary structures for which perfectly robust NI-PE with small communication complexity exists. More precisely, we show that for any positive integers n, m and $d > 1$, an n-player access structure $\mathcal{U}$, and an n-player adversary structure $\mathcal{T}$, there exists a $\mathcal{U}$-participating NI-PE scheme for m-variate polynomials over a finite field $\mathbb{F}$ with $\mathcal{T}$-private inputs such that

1. perfectly robust (i.e., successful cheating probability $\epsilon = 0$),
2. any polynomial of degree d can be evaluated,
3. the total size of shares of the output for some participating set is $o(m) \times \log |\mathbb{F}|$,

only if $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$, meaning that no $d+1$ sets in $\mathcal{T}$ cover any set in $\mathcal{U}$.
Second, we give constructions of perfectly robust NI-PE schemes against threshold adversary and general adversary, respectively. All the proposed schemes ensure perfect robustness against Q_{d+1} adversary, and computability of arbitrary polynomial of degree d.
Third, we show that efficient robust NI-PE schemes against general adversary can be constructed by allowing cheaters very small chance of successful cheating. Namely, we construct two robust NI-PE schemes with $\epsilon = 1/|\mathbb{F}|$ and the total size for shares of the output is only three times larger compared to the perfectly robust NI-PE scheme against threshold adversary.

1 Introduction

Secure multiparty computation (MPC for short) enables multiple players to cooperatively compute arbitrary function without revealing its inputs. Because of its importance in cryptography, there have been presented various type of MPCs based on various techniques so far. Among them, the technique utilizing multiplicative property of certain secret sharing schemes is one of the best-known paradigm to construct MPC. While MPC possesses such an attracting property that any function can be computed with it, efficiency of the entire protocol is rather low since it requires a large number of interactions among players to complete the protocol.

On the other hand, non-interactive polynomial evaluation (NI-PE for short) allows multiple players to *locally* convert (i.e., without interaction) shares of the inputs of a multivariate polynomial over a finite field $\mathbb{F}$ into additive shares of its output. It is shown in [1] that NI-PE for a polynomial of degree d can be constructed from a d-multiplicative secret sharing scheme (d-MSS for short). Here, d-MSS is a special type of secret sharing scheme which allows us to locally convert shares of d different secrets into an additive sharing of their product. Efficiency of NI-PE are pretty high since no interaction is required among players. The price we must pay for such high efficiency is restriction on the class of polynomials that NI-PE can computes. Namely, in [1], Barkol et al. clarify a necessary and sufficient condition of adversary structures with which d-MSS can be constructed. The result shows that for any positive integers n, d, and a n-player adversary structure $\mathcal{T}$, there exists a d-MSS $\mathcal{T}$-private secret sharing if and only if $\mathcal{T}$ is of type Q_d meaning that no d sets in $\mathcal{T}$ cover the entire set of players.

In the real-world scenario with multiple users, we cannot always assume users are trusted. To deal with untrusted users, many cryptographic primitives (such as MPC, secret sharing scheme [3, 4]) provide cheating prevention functionality. However, surprisingly, no d-MSS or NI-PE known so far possesses functionality for cheating prevention, which motivates us to consider cheating prevention in NI-PE.

The main contribution of the paper is the following. First, we give a necessary condition of adversary structures for which perfectly robust NI-PE with small communication complexity exists (Theorem 2). More precisely, we show that for any positive integers m, n, and $d > 1$, an n-player access structure $\mathcal{U}$, and an n-player adversary structure $\mathcal{T}$, there exists a $\mathcal{U}$-participating NI-PE scheme for m-variate polynomials with $\mathcal{T}$-private inputs such that

1. perfectly robust (i.e., successful cheating probability $\epsilon = 0$),
2. any polynomial of degree d can be evaluated,
3. the total size of shares of the output for some participating set is $o(m) \times \log |\mathbb{F}|$ (i.e., $\min_{P \in \mathcal{U}} |P| \times \log |\mathcal{V}| = o(m) \times \log |\mathbb{F}|$),

only if $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$, meaning that any $d+1$ sets in $\mathcal{T}$ cannot cover any set in $\mathcal{U}$.

It will be of interest to compare the above result to a necessary condition of adversary structures for *non-robust* NI-PE (i.e., Theorem 3). The conditions imposed in both theorems are identical except that Theorem 2 requires perfect robustness. However, necessary conditions on adversary structures derived from both theorems are completely different (i.e., non-robust NI-PE requires Q_d, whereas perfectly robust NI-PE requires stronger restriction Q_{d+1} as a necessary condition of adversary structure).

The second contribution is to give constructions of perfectly robust NI-PE schemes against threshold adversary and general adversary, respectively. All the proposed schemes ensure perfect robustness against Q_{d+1} adversary, and computability of arbitrary polynomial of degree d. However, efficiency of the total size of shares of the output are not ideal in all schemes. In particular, the schemes against general adversary are quite inefficient and considered to be impractical.

However, interestingly, we show that quite efficient robust NI-PE schemes against general adversary can be constructed by allowing cheaters very small chance of successful cheating. Namely, we construct two robust NI-PE schemes with $\epsilon = 1/|\mathbb{F}|$ based on the robust secret sharing scheme in [4]. The total size for shares of the output is only three times larger compared to the perfectly robust NI-PE scheme against threshold adversary, which is the third contribution of the paper.

The rest of the paper is organized as follows. In Section 2, we first recall the definition of multiplicative secret sharing and some results presented in [1]. The definition for the robustness of NI-PE against cheaters is also given in this section. In Section 3, we give a necessary condition of adversary structures for which perfectly robust NI-PE schemes with small communication complexity exist. In Section 4, we present constructions of perfectly robust NI-PE schemes against threshold and general adversary, respectively. In Section 5, we present two efficient constructions obtained by relaxing the robustness requirement. Concluding remarks and future works are given in Section 6.

2 Preliminaries

2.1 Secret Sharing

For a positive integer n, let $[n]$ denote the set $\{1, 2, \ldots, n\}$. A secret sharing scheme involves a dealer and n players $P_1, \ldots, P_n$, and specifies a randomized mapping from the secret s to an n-tuple of shares $(s_1, \ldots, s_n)$, where the share s_i is given to player P_i. We assume that the secret is taken from a finite field $\mathbb{F}$. We also assume that all shares s_i are taken from a finite share domain $\mathcal{S}$. Let $\mathcal{D}$ denote a discrete probability distribution from which the dealer's randomness is chosen. To share a secret $s \in \mathbb{F}$, the dealer chooses a random element $r \in \mathcal{D}$ and applies a sharing function $\mathsf{SHARE} : \mathbb{F} \times \mathcal{D} \to \mathcal{S}^n$ to compute $\mathsf{SHARE}(s, r) = (s_1, \ldots, s_n)$. For $T \subseteq [n]$, let $\mathsf{SHARE}(s, r)_T$ denote the restriction of $\mathsf{SHARE}(s, r)$ to its T-entries.

Definition 1. *(Adversary structure) An n-player adversary structure is a collection of sets $\mathcal{T} \subseteq 2^{[n]}$ that is closed under subsets: that is, if $T \in \mathcal{T}$ and $T' \subseteq T$, then $T' \in \mathcal{T}$. Let $\hat{\mathcal{T}}$ be the collection of maximal sets in $\mathcal{T}$.*

Definition 2. *(Access structure) An n-player access structure is a collection of sets $\mathcal{U} \subseteq 2^{[n]}$ that is closed under supersets (a.k.a. monotone): that is, if $P \in \mathcal{U}$ and $P' \supseteq P$, then $P' \in \mathcal{U}$. Let $\hat{\mathcal{U}}$ be the collection of minimal sets in $\mathcal{U}$.*

We extend the type-Q_d property of adversary structures to a relation between adversary structures and access structures, which is used for our characterization.

Definition 3. *(Adversary structure of type Q_d for access structure) Let n, d be positive integers, $\mathcal{T} \subseteq 2^{[n]}$ be an n-player adversary structure, and $\mathcal{U} \subseteq 2^{[n]}$ be an n-player access structure. We say that $\mathcal{T}$ is of type Q_d for $\mathcal{U}$ if for every d sets $T_1, \ldots, T_d \in \mathcal{T}$ and every set $P \in \mathcal{U}$, we have $T_1 \cup \cdots \cup T_d \subset P$ (that is, no d sets in $\mathcal{T}$ cover any set in $\mathcal{U}$).*

Remark: The definition of type Q_d in [1] is the special case $\mathcal{U} = \{[n]\}$.

We recall the privacy property defined in [1].

Definition 4. *($\mathcal{T}$/t-private secret sharing) A secret sharing scheme is said to be $\mathcal{T}$-private if for every pair of secrets $s, s' \in \mathbb{F}$ and every set $T \in \mathcal{T}$, the random variables $\mathsf{SHARE}(s, r)_T$ and $\mathsf{SHARE}(s', r)_T$ induced by a random choice of $r \in \mathcal{D}$ are identically distributed. A $\mathcal{T}$-private scheme is said to be t-private if $\mathcal{T}$ consists of all the subsets of $[n]$ whose cardinality is at most t.*

We extend the multiplication property in order to allow a subset of players to execute multiplication.

Definition 5. *($\mathcal{U}$/u-Participating d-multiplicative secret sharing) Let n, d, u be positive integers. Let $\mathcal{U}$ be an n-player access structure. An n-player secret sharing scheme is said to be $\mathcal{U}$-participating d-multiplicative, $(\mathcal{U}, d)$-multiplicative in short, if it satisfies the following $(\mathcal{U}, d)$-multiplication property: For $s^{(j)} \in \mathbb{F}$ and $r^{(j)} \in \mathcal{D}$ with $1 \leq j \leq d$, let $(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$. There is a function $\mathsf{MULT} : \mathcal{U} \times [n] \times \mathcal{S}^d \to \mathbb{F}$ such that for all possible $s^{(j)}$ and $r^{(j)}$ as above and any $P \in \mathcal{U}$, $\sum_{i \in P} \mathsf{MULT}(P, i, s_i^{(1)}, \ldots, s_i^{(d)}) = \prod_{j=1}^{d} s^{(j)}$. A $(\mathcal{U}, d)$-multiplicative scheme is said to be (u, d)-multiplicative if $\mathcal{U}$ consists of all the subsets of $[n]$ whose cardinality is at least u.*

Remark: The definition of d-multiplicative property in [1] is the special case $\mathcal{U} = \{[n]\}$, i.e., $u = n$. The extension of d-multiplicative property is used for showing a general construction of NI-PE schemes.

For $(\mathcal{U}, d)$-multiplicative $\mathcal{T}$-private secret sharing, we can rederive the corresponding theorem and lemma of its characterization.

Theorem 1. *(Theorem 4.6 in [1]) For any positive integers n, d, an n-player access structure $\mathcal{U}$, and an n-player adversary structure $\mathcal{T}$, there exists a $(\mathcal{U}, d)$-multiplicative $\mathcal{T}$-private secret sharing scheme if and only if $\mathcal{T}$ is of type Q_d for $\mathcal{U}$.*

The proof is essentially the same as that in [1] and given in Appendix A). Note that the $\mathcal{T}$-private CNF scheme proposed by Itoh et al. in [7] is given as an example of d-multiplicative schemes in [1], and is shown to be $(\mathcal{U}, d)$-multiplicative in this paper.

Definition 6. *(Definition 2.4 in [1], Evaluating a polynomial on shares) Let $p \in \mathbb{F}[x_1, \ldots x_m]$ be an m-variate polynomial over $\mathbb{F}$ that can be written as the sum of degree-d monomials of the form $\alpha \cdot x_{i_1} \cdot x_{i_2} \cdots x_{i_d}$. That is,*

$$p(x_1, \ldots, x_m) = \sum_{J=(j_1,\ldots,j_d)\in[m]^d} \alpha_J \prod_{l=1}^{d} x_{j_l}.$$

Let $s^{(j)} \in \mathbb{F}$ with $j \in [m]$ be secrets and $s_i^{(j)}$ with $i \in [n]$ be shares of $s^{(j)}$ for player P_i obtained by using a $(\mathcal{U}, d)$-multiplicative secret sharing scheme. Define a function $p_i : \mathcal{U} \times \mathcal{S}^m \to \mathbb{F}$ by

$$p_i(P, s_i^{(1)}, \ldots, s_i^{(m)}) = \sum_{J=(j_1,\ldots,j_d)\in[m]^d} \alpha_J \cdot \mathsf{MULT}(P, i, s_i^{(j_1)}, \ldots, s_i^{(j_d)}). \tag{1}$$

For a general polynomial p' of total degree (at most) d, let p be the polynomial such that each monomial of degree $d' < d$ of p' is converted into an equivalent monomial of degree d by padding the monomial with $d - d'$ copies of a dummy variable x_0, whose corresponding secret is set to 1 and the shares of this secret will always be set to $\mathsf{SHARE}(1, r_0)$, where r_0 is some fixed element in the support of $\mathcal{D}$.

From Definition 6, it straightforwardly follows that the $(\mathcal{U}, d)$-multiplicative property can be used for non-interactively evaluating multivariate d polynomials.

Lemma 1. *(Lemma 2.5 in [1]) Let $p \in \mathbb{F}[x_1, \ldots x_m]$ be an m-variate degree d polynomial over $\mathbb{F}$ and $\mathcal{U} \subseteq 2^{[n]}$ be an n-player access structure. Suppose that the vector of secrets $\boldsymbol{s} = (s^{(1)}, \ldots, s^{(m)}) \in \mathbb{F}^m$ was coordinate-wise secret shared using a $(\mathcal{U}, d)$-multiplicative secret sharing scheme, such that for every $j \in [m]$, the shares corresponding to $s^{(j)}$ are $(s_1^{(j)}, \ldots, s_n^{(j)}) \in \mathcal{S}^n$. Then, it holds that for any $P \in \mathcal{U}$,*

$$p(\boldsymbol{s}) = \sum_{i\in P} p_i(P, s_i^{(1)}, \ldots, s_i^{(m)}).$$

2.2 Robust Non-interactive Evaluation of Polynomials

We define an NI-PE scheme that involves a dealer and n players $P_1, \ldots, P_n$ as follows: Let $\mathcal{U}$ be an n-player access structure. A $\mathcal{U}$-participating NI-PE scheme for an m-variate polynomial $p \in \mathbb{F}[x_1, \ldots, x_m]$ specifies a sharing function SHARE, n evaluating functions EVAL_i with $i \in [n]$, and a verification function VER.

As defined in Section 2.1, the sharing function SHARE is a random mapping from the secret $s \in \mathbb{F}$ to an n-tuple of shares $(s_1, \ldots, s_n) \in \mathcal{S}^n$, where the share s_i is given to player P_i. Let $\boldsymbol{s} = (s^{(1)}, \ldots, s^{(m)})$ be the input to p and $(s_1^{(j)}, \ldots, s_n^{(j)})$ an n-tuple of shares of $s^{(j)}$ with $j \in [m]$.

Each evaluating function EVAL_i with $i \in [n]$ is a mapping from a participating set $P \in \mathcal{U}$ with $i \in P$ and m shares $\boldsymbol{s}_i = (s_i^{(1)}, \ldots, s_i^{(m)}) \in \mathcal{S}^m$ to a share of the output v_i that is taken from a finite domain $\mathcal{V}$.

The verification function VER is a mapping from a participating set $P \in \mathcal{U}$ and $|P|$ shares $\{v_i | i \in P\}$ to the output that takes a value in $\mathbb{F}$ or $\perp$ where $\perp$ means that cheating exists.

To share the inputs, the dealer coordinate-wise shares $\boldsymbol{s}$ by using SHARE. To evaluate an m-variate polynomial p by a subset of players $P \in \mathcal{U}$, each player P_i with $i \in P$ locally computes $v_i = \mathsf{EVAL}_i(P, \boldsymbol{s}_i)$ and publishes it. Then, P_i locally detects cheating by computing $\mathsf{VER}(P, \{v_i | i \in P\})$ and obtains $v = p(\boldsymbol{s})$ if cheating does not exist. That is, for any vector of secrets $\boldsymbol{s} = (s^{(1)}, \ldots, s^{(m)}) \in \mathbb{F}^m$, any vector of choices $\boldsymbol{r} = (r^{(1)}, \ldots, r^{(m)}) \in \mathcal{D}^m$, and any $P \in \mathcal{U}$,

$$\mathsf{VER}(P, \{\mathsf{EVAL}_i(P, \boldsymbol{s}_i) | i \in P\}) = p(\boldsymbol{s}),$$

where $\boldsymbol{s}_i = (s_i^{(1)}, \ldots, s_i^{(m)})$ and $(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$.

We define a private property of shared inputs.

Definition 7. *($\mathcal{T}$/t-Private inputs of NI-PE) Let $\mathcal{T}$ be an n-player adversary structure and t a positive integer. An NI-PE scheme $(\mathsf{SHARE}, \{\mathsf{EVAL}_i\}_{i \in [n]}, \mathsf{VER})$ is said to have $\mathcal{T}$/t-private inputs if SHARE is $\mathcal{T}$/t-private.*

From Theorem 1 and Lemma 1, we can easily derive a sufficient condition for a $\mathcal{U}$-participating NI-PE scheme for m-variate polynomials of degree d with $\mathcal{T}$-private inputs to exist.

Corollary 1. *Let d be a positive integer larger than one (i.e., $d > 1$). Let n, m be positive integers. For an n-player access structure $\mathcal{U}$ and an n-player adversary structure $\mathcal{T}$, there exists a $\mathcal{U}$-participating NI-PE scheme for m-variate polynomials with $\mathcal{T}$-private inputs such that*

1. *any polynomial of degree d can be evaluated,*
2. *$\mathcal{V} = \mathbb{F}$ and the total size of shares of the output for a participating set $P \in \mathcal{U}$ is $|P| \times \log |\mathbb{F}|$,*

if $\mathcal{T}$ is of type Q_d for $\mathcal{U}$.

We turn to define the unconditional robustness of a $\mathcal{U}$-participating NI-PE scheme with $\mathcal{T}$-private inputs. We consider the following scenario: For $P \in \hat{\mathcal{U}}$ and $T \in \hat{\mathcal{T}}$ with $P \cap T \neq \emptyset$, the players in P try to evaluate a m-variate polynomial $p \in \mathbb{F}[x_1, \ldots, x_m]$ on inputs $\boldsymbol{s} = (s^{(1)}, \ldots, s^{(m)})$ while the players in $T \in \hat{\mathcal{T}}$, who somehow know the value of output $v = p(\boldsymbol{s})$ (known as CDV model [3]/robust secret sharing [4]), forge their shares $\boldsymbol{v}_T = \{v_i | i \in T \cap P\}$ in order to deceive $P \setminus T$. That is, the players in T (cheaters) try to find a set of false shares $\boldsymbol{v}_T^* = \{v_i^* | i \in T \cap P\}$ such that a false value $v^* \neq v$ is evaluated from the shares $\boldsymbol{v}_T^* \cup \{v_i | i \in P \setminus T\}$. In this case, we say that the players in $P \setminus T$ are cheated by the false shares $\boldsymbol{v}_T^*$. We measure the unconditional robustness by the probability of cheating.

Definition 8. *(Probability of cheating) Let $\mathcal{T}$ be an n-player access structure and $\mathcal{U}$ an n-player adversary structure. Let $T \in \hat{\mathcal{T}}$ and $P \in \hat{\mathcal{U}}$ with $P \cap T \neq \emptyset$. The probability that the players in T (cheaters) deceives the players $P \setminus T$ (honest players), denoted by $\mathrm{PC}(P,T)$, is defined as*

$$E_{\boldsymbol{v}_T,v}(\max_{\boldsymbol{v}_T^*} \Pr(P \setminus T \text{ are cheated by } \boldsymbol{v}_T^* \mid T \text{ have } \boldsymbol{v}_T, \text{ the output is } v)).$$

Definition 9. *(Robust non-interactive polynomial-evaluation) Let n be a positive integer, $\mathcal{U} \subseteq 2^{[n]}$ an n-player access structure, $\mathcal{T} \subseteq 2^{[n]}$ an n-player adversary structure, and ϵ a positive real number. A $\mathcal{U}$-participating NI-PE scheme with $\mathcal{T}$-private inputs is said to be ϵ-robust if $\mathrm{PC}(P,T) \leq \epsilon$ for any $P \in \mathcal{U}$ and any $T \in \mathcal{T}$. An NI-PE scheme is said to be perfectly robust if $\epsilon = 0$.*

3 Necessary Condition for Perfectly Robust NI-PE Schemes

We characterize perfectly robust NI-PE schemes with small communication complexity.

Theorem 2. *Let d be a positive integer larger than one (i.e., $d > 1$). Let n, m be positive integers. For an n-player access structure $\mathcal{U}$ and an n-player adversary structure $\mathcal{T}$, there exists a $\mathcal{U}$-participating NI-PE scheme for m-variate polynomials with $\mathcal{T}$-private inputs such that*

1. *perfectly robust (i.e., $\epsilon = 0$),*
2. *any polynomial of degree d can be evaluated,*
3. *the total size of shares of the output for some participating set is $o(m) \times \log|\mathbb{F}|$ (i.e., $\min_{P \in \mathcal{U}} |P| \times \log|\mathcal{V}| = o(m) \times \log|\mathbb{F}|$),*

only if $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$.

To make the requirement for the perfect robustness clear, we also show a characterization of an NI-PE schemes for which the robustness is not required. From the following theorem, we can see that the requirement for the perfect robustness is a stronger restriction on $\mathcal{T}$.

Theorem 3. *Let d be a positive integer larger than one (i.e., $d > 1$). Let n, m be positive integers. For an n-player access structure $\mathcal{U}$ and an n-player adversary structure $\mathcal{T}$, there exists a $\mathcal{U}$-participating NI-PE scheme for m-variate polynomials with $\mathcal{T}$-private inputs such that*

1. *any polynomial of degree d can be evaluated,*
2. *the total size of shares of the output for some participating set is $o(m) \times \log|\mathbb{F}|$ (i.e., $\min_{P \in \mathcal{U}} |P| \times \log|\mathcal{V}| = o(m) \times \log|\mathbb{F}|$),*

only if $\mathcal{T}$ is of type Q_d for $\mathcal{U}$.

The proof is essentially the same as that for the "only-if" part of Theorem 1 and omitted in this paper.

Our main result is the impossibility result for the simplest case, which is used for proving Theorem 2.

Lemma 2. *Let u be a positive integer larger than two (i.e., $u > 2$). Let m be a positive integer. There is no u-player u-participating NI-PE scheme for m-variate polynomials with 1-private inputs that satisfies the following three conditions:*

1. *perfectly robust (i.e.,* $\epsilon = 0$*),*
2. *any polynomial of degree* $u-1$ *can be evaluated,*
3. *the total size of shares of the output for* u *players is* $o(m) \times \log|\mathbb{F}|$ *(i.e.,* $u \times \log|\mathcal{V}| = o(m) \times \log|\mathbb{F}|$*).*

In this case, the requirement for the perfect robustness is a smaller degree of polynomials (in [1], the impossibility for the degree u is proved).

Proof for Lemma 2. The basic idea is almost the same as that for the impossibility result on d-multiplicative secret sharing in [1]. The proof in [1] shows a method for u servers, holding a vector $\boldsymbol{y}$ of N field elements, to use any NI-PE scheme for degree-d polynomials (which can be constructed from a d-multiplicative secret sharing scheme) in order to communicate $\boldsymbol{y}$ to a client by sending him less than N field elements altogether. In this method, N is set to ${}_mC_d$ and $\boldsymbol{y}$ is encoded by a degree d polynomial. Every server sends ${}_mP_{u-1}$ field elements, each of which is an additive sharing of the outputs (i.e., $\mathcal{V} = \mathbb{F}$). Thus, the total number of field elements sent to the client is $u \times {}_mP_{u-1}$. If $d = u$, then the existence of an NI-PE scheme implies the contradiction that $u \times O(m^{u-1})$ field elements are enough to communicate $N = O(m^u)$ field elements. However, in the case $d = u-1$, there is no contradiction. So, we need a slight modification to show the impossibility for degree $u-1$. In our modified method, one server does not need to send any data while each of the other servers sends ${}_mP_{u-2}$ shares of the outputs. The total amount of sent data is $(u-1) \times {}_mP_{u-2} \times \log|\mathcal{V}| = o(m^{u-1}) \times \log|\mathbb{F}|$. For every inputs to be evaluated, one share of the output can be false. From the perfect robustness, the client can evaluate each output and reconstruct $\boldsymbol{y}$. Thus, even $d = u-1$ yields the desired contradiction.

To make the key point of our modification clear, we present the proof for the case $u = 3$. Suppose that there is a 3-player 3-participating NI-PE scheme for m-variate polynomials with 1-private inputs that satisfies the following three conditions:

1. perfectly robust, i.e., $\epsilon = 0$,
2. any polynomial of degree two can be evaluated,
3. the total size of shares of the output for three players is $o(m) \times \log|\mathbb{F}|$ (i.e., $3\log|\mathcal{V}| = o(m) \times \log|\mathbb{F}|$).

Let $N = {}_mC_2 = O(m^2)$. Let $I = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N\}$ be the set of all distinct length-m vectors over $\mathbb{F}$ which contain the value 1 in two positions and the value 0 elsewhere. Let h'_j and h''_j indicate the coordinates in which $\boldsymbol{u}_j$ is equal to 1. Define an m-variate degree two polynomial $p \in \mathbb{F}[x_1, \ldots, x_m]$ which encodes $\boldsymbol{y}$ so that $p(\boldsymbol{u}_j) = y_j$ by

$$p(x_1, \ldots, x_m) = \sum_{j=1}^{N} y_j \cdot x_{h'_j} \cdot x_{h''_j}.$$

From the above condition 2, the polynomial p can be evaluated on input vectors in I.

Let $(s_1^{(0)}, s_2^{(0)}, s_3^{(0)}) = \mathsf{SHARE}(0, r)$ for some $r \in \mathcal{D}$ (i.e., a valid secret sharing of the secret 0). Since SHARE is 1-private, there must exist two shares $s'_2, s'_3 \in \mathcal{S}$ such that $(s_1^{(0)}, s'_2, s'_3) = \mathsf{SHARE}(1, r')$ for some choice $r' \in \mathcal{D}$ (i.e., a valid secret sharing of 1). Similarly, there must exist two shares $s''_1, s''_3 \in \mathcal{S}$ such that $(s''_1, s_2^{(0)}, s''_3) = \mathsf{SHARE}(1, r'')$ for some choice $r'' \in \mathcal{D}$.

Let $Q_1 \subset \mathcal{S}^m$ be the set of all length-m vectors $\boldsymbol{q}_1$ that contain $m-1$ entries with the value $s_1^{(0)}$ and one entry with the value s''_1. Similarly, let $Q_2 \subset \mathcal{S}^m$ be the set of all length-m vectors $\boldsymbol{q}_2$

that contain $m-1$ entries with the value $s_2^{(0)}$ and one entry with the value s_2'. The cardinality of Q_i with $i \in \{1,2\}$ is m. In contrast, let $Q_3 \subset \mathcal{S}^m$ be the set of all length-m vectors $\boldsymbol{q}_3$ that contain $m-2$ entries with the value $s_3^{(0)}$, one entry that equals s_3', and one that equals to s_3''. The cardinality of Q_3 is $m(m-1)$. This difference of cardinality is the key point of our proof.

We can easily see that for any vector $\boldsymbol{u}_j \in I$ with $j \in [N]$, there are $\boldsymbol{q}_{i,j} \in Q_i$ with $i \in \{1,2,3\}$ which are valid coordinate-wise sharing of $\boldsymbol{u}_j$. Let $\boldsymbol{q}_{1,j} \in Q_1$ be the vector in which the h_j''-th entry is s_1'' (and all other entries are $s_1^{(0)}$). Let $\boldsymbol{q}_{2,j} \in Q_2$ be the vector in which the h_j'-th entry is s_2' (and all other entries are $s_2^{(0)}$). On the other hand, let $\boldsymbol{q}_{3,j} \in Q_3$ be the vector in which the h_j'-th entry is s_3' and the h_j''-th entry is s_3'' (and all other $m-2$ entries are $s_3^{(0)}$). Taking the h_j'-th entry and the h_j''-th entry of the three vectors, we get the shares $(s_1^{(0)}, s_2', s_3')$ and $(s_1'', s_2^{(0)}, s_3'')$, respectively, which are both valid secret sharings of 1. In the remaining entries, on the other hand, we get shares $(s_1^{(0)}, s_2^{(0)}, s_3^{(0)})$, which is a valid secret sharing of 0. Thus, the vectors $\boldsymbol{q}_{1,j}, \boldsymbol{q}_{2,j}, \boldsymbol{q}_{3,j}$ form share vectors of $\boldsymbol{u}_j$. Thus, letting $v_{i,j} = \mathsf{EVAL}_i([3], \boldsymbol{q}_{i,j})$ with $i \in [3]$, it holds that $\mathsf{VER}([3], \{v_{i,j} | i \in [3]\}) = p(\boldsymbol{u}_j)$.

To enable the client to reconstruct $\boldsymbol{y}$, the servers S_1 and S_2 send him $V_1 = \{\mathsf{EVAL}_1([3], \boldsymbol{q}_1) | \boldsymbol{q}_1 \in Q_1\}$ and $V_2 = \{\mathsf{EVAL}_2([3], \boldsymbol{q}_2) | \boldsymbol{q}_2 \in Q_2\}$, respectively. However, S_3 does not send any data. From the above condition 3, the total amount of sent data is $2m \times \log|\mathcal{V}| = o(m^2) \times \log|\mathbb{F}|$.

We show that the client can reconstruct $\boldsymbol{y} = (y_1, \ldots, y_N)$ from V_1 and V_2 as follows. For $j \in [N]$, let $v_{1,j} = \mathsf{EVAL}_1([3], \boldsymbol{q}_{1,j}) \in V_1$ and $v_{2,j} = \mathsf{EVAL}_2([3], \boldsymbol{q}_{2,j}) \in V_2$. To obtain $y_j = p(\boldsymbol{u}_j)$, for each element $v^* \in \mathcal{V}$, the client checks whether $\mathsf{VER}([3], \{v_{1,j}, v_{2,j}, v^*\}) = \perp$ or not. From the above condition 1 (the perfect robustness against one cheater), if $\mathsf{VER}([3], \{v_{1,j}, v_{2,j}, v\}) \neq \perp$, then the value is the output of p on $\boldsymbol{u}_j$, i.e., $p(\boldsymbol{u}_j)$.

We conclude that the servers can communicate any $\boldsymbol{y} \in \mathbb{F}^N$ to the client using shares of the output whose total size is $2m \times \log|\mathcal{V}| = o(m^2) \times \log|\mathbb{F}|$. Since $N = O(m^2)$, this is impossible for large m. Therefore, the initial assumption must be false.

For the case $u > 3$, $N = {}_mC_{u-1}$, I is the set of all distinct length-m vectors containing the value 1 in $u-1$ positions and the value 0 elsewhere, and $\boldsymbol{y}$ is encoded to a polynomial p of degree $u-1$. In this case, the total size of shares of the outputs sent by the servers $S_1, \ldots, S_{u-1}$ to the client is ${}_mP_{u-2} \times (u-1) \times \log|\mathcal{V}| = o(m^{u-1}) \times \log|\mathbb{F}|$, and since $N = O(m^{u-1})$, this yields the contradiction. □

We prove Theorem 2 by reduction. The reduction is essentially the same as the "only-if" part in Theorem 1.

Proof for the "only-if" part of Theorem 2. If $\mathcal{T}$ is not of type Q_{d+1} for $\mathcal{U}$, then there is a set $P \in \mathcal{U}$ which can be partitioned into $d+1$ disjoint subsets $T_1, \ldots, T_{d+1} \in \mathcal{T}$. Let $u = d+1 > 2$. We can construct an u-player u-participating NI-PE scheme for m-variate polynomials with 1-private inputs where each player P_i with $i \in [u]$ in the new scheme gets and generates the data of all players in T_i. This is in contradiction to Lemma 2. □

4 Constructions of Perfectly Robust Schemes

4.1 Construction against Threshold Adversary

We show that if we focus ourselves on threshold adversary, we can construct a very simple n-player u-participating NI-PE scheme for any m-variate polynomial with t-private inputs which satisfies the following properties:

1. perfectly robust (i.e., $\epsilon = 0$),
2. any polynomial of degree d can be evaluated,
3. $\mathcal{V} = \mathbb{F}$ and the total size of shares of the output for u players is $u \times \log|\mathbb{F}|$,

if $u > (d+1)t$ (i.e., $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$).

The complete description of the scheme is as follows. The sharing function is identical to Shamir's t-out-of-n threshold scheme. That is, shares $(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, (r_1^{(j)}, \ldots, r_t^{(j)}))$ are computed by $s_i^{(j)} = f^{(j)}(i)$ where $f^{(j)}(x) \in \mathbb{F}[x]$ is defined by $f^{(j)}(x) = s^{(j)} + \sum_{\ell=1}^{t} r^{(j)} \cdot x^{\ell}$. It is obvious that the scheme is t-private.

Let $p \in \mathbb{F}[x_1, \ldots, x_m]$ be any m-variate degree d polynomial, and $P \in \mathcal{U}$ be any subset of players satisfying $|P| > (d+1)t$. Then, on input $P \in \mathcal{U}$ and $\boldsymbol{s}_i = (s_i^{(1)}, \ldots, s_i^{(m)})$, the evaluating function EVAL_i computes $v_i = \mathsf{EVAL}_i(P, \boldsymbol{s}_i) = L(P,i) \cdot p(s_i^{(1)}, \ldots, s_i^{(m)})$ where $L(P,i)$ is defined by $L(p,i) = \prod_{\ell \in P \setminus \{i\}} \frac{-\ell}{i-\ell}$. That is, $\mathcal{V} = \mathbb{F}$.

Now, we show that the scheme is u-participating for any m-variate degree d polynomial (i.e., $\sum_{i \in P} \mathsf{EVAL}_i(P,i) = p(s^{(1)}, \ldots, s^{(m)})$ holds). Let $\hat{p}[x]$ be a polynomial defined by $\hat{p}(x) = p(f^{(1)}(x), \ldots, f^{(m)}(x))$. Since $\deg(p) = d$ and $\deg(f^{(j)}) \leq t$ hold, the degree of $\hat{p}$ satisfies $\deg(\hat{p}) \leq d \cdot t$. Therefore, $d \cdot t + 1$ or more points on $\hat{p}$ uniquely determine $\hat{p}$ using Lagrange interpolation. Furthermore, we can easily check that $(i, v_i/L(P,i))$ is a points on $\hat{p}$ since $v_i/L(P,i) = p(f^{(1)}(i), \ldots, f^{(m)}(i)) = \hat{p}(i)$ holds. Applying Lagrange interpolation to $|P| (> d \cdot t + 1)$ points $\{(i, v_i/L(P,i)) \mid i \in P\}$, we can reconstruct $\hat{p}(x)$ as follows:

$$\hat{p}(x) = \sum_{i \in P} \frac{v_i}{L(P,i)} \prod_{\ell \in P \setminus \{i\}} \frac{x - \ell}{i - \ell} \,. \tag{2}$$

Since $\hat{p}(0) = p(f^{(1)}(0), \ldots, f^{(m)}(0)) = p(s^{(1)}, \ldots, s^{(m)})$ holds, we have the following equation:

$$\begin{aligned} \hat{p}(0) &= \sum_{i \in P} \frac{v_i}{L(P,i)} \prod_{\ell \in P \setminus \{i\}} \frac{0 - \ell}{i - \ell} \;=\; \sum_{i \in P} \frac{v_i}{L(P,i)} \cdot L(P,i) \\ &= \sum_{i \in P} v_i \;=\; \sum_{i \in P} \mathsf{EVAL}_i(P,i) \;=\; p(s^{(1)}, \ldots, s^{(m)}) \,. \end{aligned}$$

Now, we show that the scheme is perfectly robust (i.e., $\epsilon = 0$). On input $P \in \mathcal{U}$ and $\{v_i \mid i \in P\}$, we define verification function VER of the proposed scheme as follows:

1. Compute $\hat{p}(x)$ according to eq. (2).
2. Output $\sum_{i \in P} \mathsf{EVAL}(P, \boldsymbol{s}_i)$ if $\deg(\hat{p}) \leq d \cdot t$ holds. Otherwise, output $\perp$.

It is easy to see that if there is no cheater, $\deg(\hat{p}) \leq d \cdot t$ holds with probability 1. Now we show that $\deg(\hat{p}) > d \cdot t$ holds with probability 1 if there is a player P_i submitting forged v_i^*. Without

loss of generality, we can assume $P_1, \ldots, P_t$ are cheaters who submit (possibly) forged shares $v_i^* = v_i + \delta_i$ (where at least one δ_i is non-zero) and try to fool honest players $P_{t+1}, \ldots, P_u$. Now we evaluate $\deg(\hat{p}')$ reconstructed from (possibly) forged $v_1^*, \ldots, v_t^*$ and unforged $v_{t+1}, \ldots, v_u$. Here, $\hat{p}'(x)$ reconstructed from $v_1^*, \ldots, v_{t+1}^*$ and $v_{t+1}, \ldots, v_u$ can be expressed by $\hat{p}'(x) = \hat{p}(x) + \hat{p}''(x)$ where $\hat{p}(x)$ is a polynomial of degree at most $d \cdot t$ reconstructed from $(1, v_1), \ldots, (u, v_u)$ and $\hat{p}''(x)$ is a polynomial reconstructed from $(1, \delta_1/L(P,1)), \ldots, (t, \delta_t/L(P,t)), (t+1, 0), (t+2, 0), \ldots, (u, 0)$. Since there are at least $u - t$ zeros in $p''(x)$ and $p''(x)$ cannot be the constant function $p''(x) = 0$, we see that $\deg(p'') \geq u - t \, (> (d+1)t - t = d \cdot t)$ holds with probability 1, which shows the perfect robustness (i.e., $\epsilon = 0$) of the scheme.

4.2 Construction against General Adversary

We show two constructions of a perfectly robust NI-PE schemes against general adversary with type Q_{d+1} structure: one is generic and the other is based on the CNF secret sharing scheme in [7]. In both schemes, for any set $P \in \mathcal{U}$, the total size of shares of the output is $|P| \times |\hat{\mathcal{T}}| \times \log |\mathbb{F}|$.

The generic construction is as follows. For an n-player adversary structure $\mathcal{T}$ which is of type Q_{d+1} for $\mathcal{U}$, let $\mathcal{U}'_T = \{P \setminus T | P \in \mathcal{U}\}$ for $T \in \mathcal{T}$. We use $\mathcal{U}'_T$-participating NI-PE schemes for m-variate degree d polynomials with $\mathcal{T}$-private inputs. The existence of such schemes follows from Corollary 1 because $\mathcal{T}$ is of type Q_d for any $\mathcal{U}'_T$. The sharing function in the new scheme is identical to that in the based scheme. When the players in a set $P \in \mathcal{U}$ evaluate an m-variate degree d polynomial p, for each $T \in \mathcal{T}$, the players in $P \setminus T$ executes the U'_T-participating NI-PE scheme. For some $T \in \mathcal{T}$, the players in $P' = P \setminus T$ are all honest and then the evaluated value is correct. Thus, if all evaluated values are the same, each player in P outputs the evaluated value, and otherwise outputs "$\perp$."

To show the concrete construction, we recall the CNF secret sharing scheme in [7].

Definition 10. *(CNF secret sharing) Let $\mathcal{T}$ be an n-player adversary structure. The $\mathcal{T}$-private CNF secret sharing scheme is defined by the following sharing algorithm. The dealer first additively breaks s into $|\hat{\mathcal{T}}|$ additive parts r_T with $T \in \hat{\mathcal{T}}$. The share of player P_i consists of all parts r_T such that $i \notin T$. That is, the parts r_T are chosen randomly from $\mathbb{F}$ subject to the restriction $\sum_{T \in \hat{\mathcal{T}}} r_T = s$.*

The concrete construction based on the CNF scheme is essentially the same as the generic construction. The sharing function of the proposed scheme is identical to the CNF scheme. Writing the k-th term $s^{(1)} \cdots s^{(d)}$ of an m-variate degree d polynomial p as the sum of the $|\hat{\mathcal{T}}|^d$ monomials of the form $r^{(1)}_{T_{k,1}} \cdots r^{(d)}_{T_{k,d}}$, for any $P \in \mathcal{U}$ and any $T \in \mathcal{T}$, the monomials can be partitioned into $|P \setminus T|$ sets $X_{P,T,k,i}$ with $i \in P \setminus T$ where all monomials in $X_{P,T,k,i}$ are known to P_i. This follows from the fact that every monomial as above can be assigned to a set $X_{P,T,k,i}$ such that $i \notin T \cup T_{k,1} \cup \cdots \cup T_{k,d}$ because $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$. Then, letting $\hat{p}_{P,T,i} \in \mathbb{F}$ denote the sum of all monomials in $\bigcup_k X_{P,T,k,i}$, the output of p is given by $\sum_{i \in P \setminus T} \hat{p}_{P,T,i}$. Thus, letting $\mathsf{EVAL}_i(P, \cdot)$ consist of $\hat{p}_{P,T,i}$ with $T \in \mathcal{T}$, $\mathsf{VER}(P, \cdot)$ can detect the existence of cheating by checking the consistency of the evaluated values $\sum_{i \in P \setminus T} \hat{p}_{P,T,i}$ for $T \in \mathcal{T}$. That is, the scheme is perfectly robust (i.e., $\epsilon = 0$).

5 Generic Constructions of $1/|\mathbb{F}|$-Robust Schemes

In this section, we give two efficient constructions of robust NI-PE schemes against general adversary with type Q_{d+1} structure with $\epsilon = 1/|\mathbb{F}|$. The sizes of share $|\mathcal{V}|$ of both schemes are as small as three field elements and are greatly reduced compared to the perfectly robust schemes against general adversary presented in the previous section. The proposed schemes are constructed based on the robust secret sharing scheme by Cabello, Padró and Sáez [4].

5.1 Construction for Any Degree d Polynomials

We show that by relaxing the robustness requirement so that $\epsilon > 0$ and using $(\mathcal{U}, d+1)$-multiplicative $\mathcal{T}$-private secret sharing scheme SHARE', for any $\mathcal{U}$ and $\mathcal{T}$, we can construct an efficient $\mathcal{U}$-participating NI-PE scheme for any m-variate polynomial with $\mathcal{T}$-private inputs which satisfies the following properties:

1. $\epsilon = 1/|\mathbb{F}|$,
2. any polynomial of degree d can be evaluated,
3. $\mathcal{V} = \mathbb{F}^3$ and the total size of shares of the output for a participating set P is $3 \times |P| \times \log |\mathbb{F}|$,

if $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$.

In the proposed scheme, one field element is additionally shared for each evaluation, independently of sharing secrets (but for the simplicity of description, we share the additional element when sharing a secret).

The overview of the scheme is as follows. To share a secret $s^{(j)} \in \mathbb{F}$, the dealer randomly chooses $r_1^{(j)}, r_2^{(j)} \in \mathcal{D}$ and $e^{(j)} \in \mathbb{F}$, and computes $\mathsf{SHARE}'(s^{(j)}, r_1^{(j)}) = (s_1^{(j)}, \ldots, s_n^{(j)})$ and $\mathsf{SHARE}'(e^{(j)}, r_2^{(j)}) = (e_1^{(j)}, \ldots, e_n^{(j)})$. The share of $s^{(j)}$ for each party P_i is $(s_i^{(j)}, e_i^{(j)})$. In the evaluation and verification phase by $P \in \mathcal{U}$, for any m-variate degree d polynomial p and shared secrets $\boldsymbol{s} = (s^{(1)}, \ldots, s^{(m)})$, they compute the values of $v = p(\boldsymbol{s})$, $v_e = e^{(i)}$ for some unused $e^{(i)}$, and $v_a = e^{(i)} \cdot p(\boldsymbol{s})$ by using the NI-PE scheme in Definition 6. The latter two values can be considered as the outputs of polynomials $p_e = x_e$ and $p_a = x_e \cdot p$ in $\mathbb{F}[x_1, \ldots, x_m, x_e]$, whose degree are 1 and $d+1$, respectively. Thus, from Lemma 1, we can see that the three values can be evaluated from the $(\mathcal{U}, d+1)$-multiplicative property. If $v \cdot v_e = v_a$, they take v as the correct value of the output, and otherwise, they are warned about the existence of cheaters.

Formally, we define the sharing function by $\mathsf{SHARE}(s, e, r_1, r_2) = ((s_1, e_1), \ldots, (s_n, e_n)) \in \mathcal{S}^{2n}$ where $(s_1, \ldots, s_n) = \mathsf{SHARE}'(s, r_1)$ and $(e_1, \ldots, e_n) = \mathsf{SHARE}'(e, r_2)$. Let $p_i, p_{e,i}, p_{a,i}$ be the functions defined in eq. (1) for p, p_e, p_a, respectively. Each evaluating function EVAL_i is defined by $\mathsf{EVAL}_i(P, \boldsymbol{s}_i) = (p_i(P, \boldsymbol{s}_i), p_{e,i}(P, \boldsymbol{s}_i), p_{a,i}(P, \boldsymbol{s}_i)) \in \mathbb{F}^3$ where $\boldsymbol{s}_i = ((s_i^{(1)}, e_i^{(1)}), \ldots, (s_i^{(m)}, e_i^{(m)}))$. On input P and $v_i = \mathsf{EVAL}_i(P, \boldsymbol{s}_i)$ with $i \in P$, VER outputs $\sum_{i \in P} p_i(P, \boldsymbol{s}_i)$ if $\sum_{i \in P} p_i(P, \boldsymbol{s}_i) \times \sum_{i \in P} p_{e,i}(P, \boldsymbol{s}_i) = \sum_{i \in P} p_{a,i}(P, \boldsymbol{s}_i)$ holds, and otherwise $\perp$.

We remark that the $(\mathcal{U}, d+1)$-multiplication property imposes no linearity requirement on the sharing function SHARE' itself while the resulting NI-PE scheme in Definition 6 has some type of linearity on the output. For example, given shares of $e^{(i)}$, the players can compute additive shares of $e^{(i)}$ by evaluating it as the output of polynomial $p_e = x_e$. Based on this linearity, we prove $1/|\mathbb{F}|$-robustness of the proposed NI-PE scheme.

Theorem 4. *Let d be a positive integer larger than one (i.e., $d > 1$). For any positive integers n, m, an n-player access structure $\mathcal{U}$ and an n-player adversary structure $\mathcal{T}$ such that $\mathcal{T}$ is of type*

Q_{d+1} for $\mathcal{U}$, the proposed NI-PE scheme is $1/|\mathbb{F}|$-robust for any m-variate degree d polynomial if SHARE' is $(\mathcal{U}, d+1)$-multiplicative (there exists MULT defined in Definition 5).

Proof. From Lemma 1, it is obvious that if $\boldsymbol{v}_T^* = \boldsymbol{v}_T$, then the scheme enables the players in $P \in \mathcal{U}$ to compute the correct value of the output. In the following, we prove that the scheme is $1/|\mathbb{F}|$-robust, i.e., $\mathrm{PC}(P, T)$ is equal to $\epsilon = 1/|\mathbb{F}|$ for any $P \in \mathcal{U}$ and $T \in \mathcal{T}$. The cheaters in T know the value of $v = p(\boldsymbol{s})$ but they do not know the values of $e^{(i)} (= v_e)$ from the $\mathcal{T}$-privacy of SHARE'. For any $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}^3$, the cheaters in T can compute forged shares $\boldsymbol{v}_T^*$ so that in the evaluation phase, (v^*, v_e^*, v_a^*) is computed, where $v^* = v + \alpha_1, v_e^* = v_e + \alpha_2, v_a^* = v_a + \alpha_3$. They deceive the other honest players without detection if and only if $\alpha_1 \neq 0$ and $v^* \times v_e^* = v_a^*$, i.e., $v\alpha_2 + v_e\alpha_1 = \alpha_3$. For every choice of $(\alpha_1, \alpha_2, \alpha_3)$ with $\alpha_1 \neq 0$, there is unique $v_e = e^{(i)}$ satisfying the above equation. Thus, for any forged shares $\boldsymbol{v}_T^*$ used by the cheaters in T, $\Pr(P \setminus T$ is cheated by $\boldsymbol{v}_T^* | T$ have $\boldsymbol{v}_T$, the output is $v) = 1/|\mathbb{F}|$. Then, $\mathrm{PC}(P, T) = 1/|\mathbb{F}|$. □

5.2 Construction for a Subclass of Degree $d+1$ Polynomials

We also show that for any $\mathcal{U}$ and $\mathcal{T}$, we can construct an efficient $\mathcal{U}$-participating NI-PE scheme for any m-variate polynomial with $\mathcal{T}$-private inputs which satisfies the following properties:

1. $\epsilon = 1/|\mathbb{F}|$,
2. any polynomial of degree $d+1$ that is represented by $x_i \cdot \hat{p}_1 + \hat{p}_2$ for some variable x_i and m-variate degree (at most) d polynomials can be evaluated,
3. $\mathcal{V} = \mathbb{F}^3$ and the total size of shares of the output for a participating set P is $3 \times |P| \times \log |\mathbb{F}|$,

if $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$.

The scheme uses a $(\mathcal{U}, d+1)$-multiplicative secret sharing scheme SHARE' and shares two additional field elements for each secret where the additional data is one-time use.

The overview of the scheme is as follows. To share a secret $s^{(j)} \in \mathbb{F}$, the dealer randomly chooses $r_1^{(j)}, r_2^{(j)}, r_3^{(j)} \in \mathcal{D}$ and $e^{(j)} \in \mathbb{F}$ and computes $\mathsf{SHARE}'(s^{(j)}, r_1^{(j)}) = (s_1^{(j)}, \ldots, s_n^{(j)})$, $\mathsf{SHARE}'(e^{(j)}, r_2^{(j)}) = (e_1^{(j)}, \ldots, e_n^{(j)})$, and $\mathsf{SHARE}'(a^{(j)}, r_3^{(j)}) = (a_1^{(j)}, \ldots, a_n^{(j)})$ with $a^{(j)} = s^{(j)} \cdot e^{(j)}$. The share of $s^{(j)}$ for each player P_i is $(s_i^{(j)}, e_i^{(j)}, a_i^{(j)})$. In the evaluation and verification phase, for a given polynomial p represented as above and shared secrets $\boldsymbol{s} = (s^{(1)}, \ldots, s^{(m)})$, the players in $P \in \mathcal{U}$ compute the values of $v = p(\boldsymbol{s})$, $v_e = e^{(i)}$, and $v_a = a^{(i)} \cdot \hat{p}_1(\boldsymbol{s}) + e^{(i)} \cdot \hat{p}_2(\boldsymbol{s})$ by using the NI-PE scheme in Definition 6. The latter two values can be considered as the outputs of polynomials $p_e = x_e, p_a = x_a \cdot \hat{p}_1 + x_e \cdot \hat{p}_2 \in \mathbb{F}[x_1, \ldots, x_m, x_e, x_a]$, whose degree are 1 and $d+1$, respectively. Thus, from Lemma 1, we can see that the three values can be evaluated from the $(\mathcal{U}, d+1)$-multiplicative property. If $v \cdot v_e = v_a$, they take v as the correct value of the output, and otherwise, they are warned about the existence of cheaters.

We can define $(\mathsf{SHARE}, \{\mathsf{EVAL}_i\}_{i \in [n]}, \mathsf{VER})$ and prove the robustness in the same way as the construction for any degree d polynomials. Thus, the details and the proof are omitted here.

Theorem 5. *Let d be a positive integer larger than one (i.e., $d > 1$). For any positive integers n, m, an n-player access structure $\mathcal{U}$ and an n-player adversary structure $\mathcal{T}$ such that $\mathcal{T}$ is of type Q_{d+1} for $\mathcal{U}$, there is a $1/|\mathbb{F}|$-robust $\mathcal{U}$-participating NI-PE scheme for the class of m-variate degree $d+1$ polynomials that are represented as above.*

6 Conclusion

In this paper, we have considered both theoretical and practical aspects of robust NI-PE. First, we have given a necessary condition of adversary structures for which perfectly robust NI-PE with small communication complexity exists. Second, we have given constructions of perfectly robust NI-PE schemes against threshold adversary and general adversary, respectively. All the proposed schemes ensure perfect robustness against Q_{d+1} adversary, and computability of arbitrary polynomial of degree d. We have also given two practical robust NI-PE schemes against general adversary with $\epsilon = 1/|\mathbb{F}|$. We can confirm that these practical schemes dramatically reduce the communication complexity compared to that of perfectly robust NI-PE schemes against general adversary.

To find a necessary and sufficient condition of adversary structures for perfectly robust NI-PE scheme and efficient construction of perfectly robust NI-PE scheme against general adversary remains open problems.

References

1. O. Barkol, Y. Ishai, and E. Weinreb, "On d-Multiplicative Secret Sharing," *Journal of Cryptology*, Vol.23, No.4, pp.580–593, 2010.
2. G.R. Blakley, "Safeguarding Cryptographic Keys," *AFIPS 1979 Nat. Comput. Conf.*, vol. 48, pp. 313–317, 1979.
3. M. Carpentieri, A.De Santis, and U. Vaccaro, "Size of Shares and Probability of Cheating in Threshold Schemes," *Advances in Cryptology - EUROCRYPT1993 in Lecture Notes in Comput. Sci.*, vol. 765, pp. 118–125, 1994.
4. S. Cabello, C. Padró and G. Sáez, "Secret Sharing Schemes with Detection of Cheaters for a General Access structure," *Design, Codes and Cryptography*, vol. 25, no. 2, pp. 175–188, 2002.
5. R. Cramer, I. Damagård, and U. Maurer, "General Secure Multi-Party Computation from Any Linear Secret Sharing Scheme," *Advances in Cryptology - EUROCRYPT2000 in Lecture Notes in Comput. Sci.*, vol. 1807, pp. 316–335, 2000.
6. H. Chen, R. Cramer, R. de Haan, I. C. Pueyo, "Strongly Multiplicative Ramp Schemes from High Degree Rational Points on Curves," *Advances in Cryptology - EUROCRYPT2008 in Lecture Notes in Comput. Sci.*, vol. 4965, pp.451–470, 2008.
7. M. Itoh, A. Saito, and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure," *IEEE Global Telecommunications Conference, Globecom '87*, pp.99–102, 1987.
8. A. Shamir, "How to Share a Secret," *Comm. of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
9. Z. Zhang, M. Liu, Y.M. Chee, S. Ling, H. Wang, "Strongly Multiplicative and 3-Multiplicative Linear Secret Sharing Schemes," *Advances in Cryptology - ASIACRYPT 2008 in Lecture Notes in Comput. Sci.*, vol. 5350, pp. 19–36, 2008.
10. M. Liu, L. Xiao, Z. Zhang, "Multiplicative Linear Secret Sharing Schemes Based on Connectivity of Graphs," *IEEE Transactions on Information Theory* vol. 53, no. 11, pp. 3973–3978, 2007.

A Characterization of $(\mathcal{U}, d)$-MSS

A.1 Proof for the "Only-if" part of Theorem 1

First, we show the impossibility result for the simplest case.

Lemma 3. *Let u be a positive integer larger than one (i.e., $u > 1$). There is no u-player u-participating u-multiplicative secret sharing scheme that is 1-private.*

Proof for Lemma 3. Let N be a sufficiently large integer such that $N = {}_mC_u$ for some positive integer m. The proof shows a method for u servers, holding a vector $\boldsymbol{y}$ of N field elements, to use any a u-participating u-multiplicative secret sharing scheme in order to communicate $\boldsymbol{y}$ to a client by sending him less than N field elements altogether. In this method, $\boldsymbol{y}$ is encoded by a degree u polynomial. Every server sends ${}_mP_{u-1}$ field elements, each of which is an additive sharing of the outputs (i.e., an element of $\mathbb{F}$). Thus, the total number of field elements sent to the client is $u \times {}_mP_{u-1}$. The existence of the multiplicative scheme implies the contradiction that $u \times O(m^{u-1})$ field elements are enough to communicate $N = O(m^u)$ field elements, yielding a contradiction.

To make the key point of the proof clear, we present the proof for the case $u = 2$. Suppose that there is a 2-player 2-participating 2-multiplicative secret sharing scheme SHARE that is 1-private.

Let $N = {}_mC_2$. Let $I = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_N\}$ be the set of all distinct length-m vectors over $\mathbb{F}$ which contain the value 1 in two positions and the value 0 elsewhere. Let h'_j and h''_j indicate the coordinates in which $\boldsymbol{u}_j$ is equal to 1. Define an m-variate degree two polynomial $p \in \mathbb{F}[x_1, \ldots, x_m]$ which encodes $\boldsymbol{y}$ so that $p(\boldsymbol{u}_j) = y_j$ by

$$p(x_1, \ldots, x_m) = \sum_{j=1}^{N} y_j \cdot x_{h'_j} \cdot x_{h''_j}.$$

From Lemma 1, the polynomial p can be evaluated on input vectors in I.

Let $(s_1^{(0)}, s_2^{(0)}) = \mathsf{SHARE}(0, r)$ for some $r \in \mathcal{D}$ (i.e., a valid secret sharing of the secret 0). Since SHARE is 1-private, there must exist a share $s'_2 \in \mathcal{S}$ such that $(s_1^{(0)}, s'_2) = \mathsf{SHARE}(1, r')$ for some choice $r' \in \mathcal{D}$ (i.e., a valid secret sharing of 1). Similarly, there must exist a share $s''_1, s''_3 \in \mathcal{S}$ such that $(s''_1, s_2^{(0)}) = \mathsf{SHARE}(1, r'')$ for some choice $r'' \in \mathcal{D}$.

Let $Q_1 \subset \mathcal{S}^m$ be the set of all length-m vectors $\boldsymbol{q}_1$ that contain $m-1$ entries with the value $s_1^{(0)}$ and one entry with the value s''_1. Similarly, let $Q_2 \subset \mathcal{S}^m$ be the set of all length-m vectors $\boldsymbol{q}_2$ that contain $m-1$ entries with the value $s_2^{(0)}$ and one entry with the value s'_2. The cardinality of Q_i with $i \in \{1, 2\}$ is m.

We can easily see that for any vector $\boldsymbol{u}_j \in I$ with $j \in [N]$, there are $\boldsymbol{q}_{i,j} \in Q_i$ with $i \in \{1, 2\}$ which are valid coordinate-wise sharing of $\boldsymbol{u}_j$. Let $\boldsymbol{q}_{1,j} \in Q_1$ be the vector in which the h''_j-th entry is s''_1 (and all other entries are $s_1^{(0)}$). Let $\boldsymbol{q}_{2,j} \in Q_2$ be the vector in which the h'_j-th entry is s'_2 (and all other entries are $s_2^{(0)}$). Taking the h'_j-th entry and the h''_j-th entry of the three vectors, we get the shares $(s_1^{(0)}, s'_2)$ and $(s''_1, s_2^{(0)})$, respectively, which are both valid secret sharings of 1. In the remaining entries, on the other hand, the shares are $(s_1^{(0)}, s_2^{(0)})$, that is, a valid secret sharing of 0. Thus, the vectors $\boldsymbol{q}_{1,j}, \boldsymbol{q}_{2,j}$ form share vectors of $\boldsymbol{u}_j$. Thus, letting $v_{i,j} = p_i([2], \boldsymbol{q}_{i,j})$ with $i \in [2]$, it holds that $\sum_{i \in [2]} v_{i,j} = p(\boldsymbol{u}_j)$.

To enable the client to reconstruct $\boldsymbol{y}$, the servers S_1 and S_2 send him $V_1 = \{p_1([2], \boldsymbol{q}_1) | \boldsymbol{q}_1 \in Q_1\}$ and $V_2 = \{p_2([3], \boldsymbol{q}_2) | \boldsymbol{q}_2 \in Q_2\}$, respectively. Since each share of the output is an element in $\mathbb{F}$, the total amount of sent data is $2m \times \log |\mathbb{F}|$.

As described in the above, the client can reconstruct $\boldsymbol{y} = (y_1, \ldots, y_N)$ from V_1 and V_2. Thus, we can conclude that the servers can communicate any $\boldsymbol{y} \in \mathbb{F}^N$ to the client using shares of the output whose total size is $2m \times \log |\mathbb{F}|$. Since $N = m(m-1)/2$, this is impossible for $m > 5$. Therefore, the initial assumption must be false.

For the case $u > 2$, $N = {}_mC_u$, I is the set of all distinct length-m vectors containing the value 1 in u positions and the value 0 elsewhere, and $\boldsymbol{y}$ is encoded to a polynomial p of degree u. In this case, the total size of shares of the outputs sent by the servers $S_1, \ldots, S_u$ to the client is ${}_mP_{u-1} \times u \times \log|\mathcal{V}| = o(m^u) \times \log|\mathbb{F}|$, and since $N = O(m^u)$, this yields the contradiction. □

We prove the "only-if" part by reduction.

Proof for the "only-if" part of Theorem 1. If $\mathcal{T}$ is not of type Q_d for $\mathcal{U}$, then there is a set $P \in \mathcal{U}$ which can be partitioned into d disjoint subsets $T_1, \ldots, T_d \in \mathcal{T}$. We can construct an d-player d-participating d-multiplicative scheme that is 1-private where each player P_i with $i \in [d]$ in the new scheme gets the shares of all players in T_i. This is in contradiction to the above lemma. □

A.2 Proof for the "If" part of Theorem 1

We show that for any n-player adversary structure $\mathcal{T}$ and access structure $\mathcal{U}$ such that $\mathcal{T}$ is of type Q_d for $\mathcal{U}$, the $\mathcal{T}$-private CNF scheme is $(\mathcal{U}, d)$-multiplicative. For j with $1 \leq j \leq d$, let r_T^j with $T \in \mathcal{T}$ denote the additive parts of secret $s^{(j)}$. Writing the product $s^{(1)} \cdots s^{(d)}$ as the sum of the $|\hat{\mathcal{T}}|^d$ monomials of the form $r_{T_1}^{(1)} \cdots r_{T_d}^{(d)}$, for any $P \in \mathcal{U}$, the monomials can be partitioned into $|P|$ sets $X_{P,i}$ with $i \in P$ where all monomials in $X_{P,i}$ are known to P_i. This follows from the fact that every monomial as above can be assigned to a set $X_{P,i}$ such that $i \notin T_1 \cup \cdots \cup T_d$ because $\mathcal{T}$ is of type Q_d for $\mathcal{U}$. Then, letting $\mathsf{MULT}(P, i, \cdot)$ output the sum of all monomials in $X_{P,i}$, the $(\mathcal{U}, d)$-multiplicative property follows.