Flaws in a Verifiably Multiplicative Secret Sharing Scheme from ICITS 2017

Maki Yoshida[1] and Satoshi Obana[2]

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

Abstract. In this paper, we point out flaws in an existing verifiably multiplicative secret sharing (VMSS) scheme. Namely, we show that a scheme proposed by Yoshida and Obana presented at ICITS 2017 is insecure against an adversary who corrupts a single player. We then show that in the model of ICITS 2017 which restricts the decoder additive, the error-free verification is impossible. We further show that by allowing a general class of decoders which include a linear one, the scheme is error-free.

1 Introduction

A secret sharing (SS) scheme is a method of sharing a secret among a set of n players so that some predefined authorized subsets of the players are able to recover the secret. The notion of *threshold* SS was introduced by Shamir [8] and Blakley [5] independently where the cardinality of any authorized set is larger than a given threshold. Later, Ito et al. [7] generalized this notion to a setting where the authorized subsets are an arbitrary family of subsets of the players, called *access structures*.

SS is now used as a central building block in many cryptographic and distributed applications such as unconditionally secure multiparty computation (MPC) [4, 6, 1, 2]. In addition, for natural application to unconditionally secure MPC [4, 6], the *multiplicative* property of SS is essential.

Motivated by open problems in the area of MPC such as unconditionally secure MPC with minimal interaction, Barkol et al. [3] introduced *d-multiplicative* SS and studied the type of access structures for which such secret sharing schemes exist. A secret sharing scheme is *d-multiplicative* if the scheme allows the players to multiply shared d (rather than two) secrets by *locally* converting their shares into an *additive* sharing of the product. That is, the decoder is *additive* in the sense that it computes the output as the sum of elements in $\mathbb{F}$. They proved that d-multiplicative schemes exist if and only if no d unauthorized sets of players cover the whole set of players (type Q_d).

To improve the usefulness of d-multiplicative SS (MSS) in the context of MPC in the presence of malicious adversaries, Yoshida and Obana [9] introduced *verifiably d-multiplicative* SS, which keeps the additive property of decoding, and studied the type of access structures for which such secret sharing schemes exist.

Specifically, in [9], a scheme against the access structures of type Q_{d+1} and one against the access structures of type Q_d are presented.

In this paper, we show that the former scheme proposed in [9], constructed against the access structures of type Q_{d+1}, is insecure. Namely, we showed that an adversary corrupting a single player can forge a proof for any incorrect value that is always accepted. We then show that in the model of ICITS 2017 which restricts the decoder additive, the error-free verification is impossible. We then show that by allowing a general class of decoders which include a linear one, the scheme is error-free.

The rest of the paper is organized as follows. In Section 2, we briefly review the definitions of secret sharing in [3, 9]. In Section 3, we present an attack against the scheme given in [9]. In Section 4, we discuss some (im)possibilities on error-free verifiably multiplicative secret sharing. In Section 5, we summarize our work.

2 Preliminaries

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. It is assumed that the secret is taken from a finite field $\mathbb{F}$. It is also assumed 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.

In contrast to traditional secret sharing specifying a collection of authorized player sets, the complementary notion of an *adversary structure*, specifying a collection of *unauthorized* sets, is used for convenience in [3, 9].

Definition 1 (Adversary structure [3]). *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 $\mathcal{T}$ (namely those that are not contained in any other set from $\mathcal{T}$).*

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

Definition 3 ($\mathcal{T}$-Private secret sharing [3]). *Let $\mathcal{T}$ be an n-player adversary structure. A secret sharing scheme is said to be $\mathcal{T}$-private if every pair of secret $s, s' \in \mathbb{F}$ and every $T \in \mathcal{T}$, 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 secret sharing scheme is said to be t-private if $\mathcal{T} = \{T \subseteq [n] \mid |T| \leq t\}$.*

The multiplicative property requires each player to locally generate an additive sharing of the product of d secrets. In addition, the decoder is additive in the sense that it computes the output as the sum of elements in $\mathbb{F}$. We refer to such an MSS scheme as an *additive* MSS.

Definition 4 **(d-Multiplicative secret sharing [3]).** *We call a secret sharing scheme d-multiplicative if it satisfies the following d-multiplicative property. Let* $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$ *be d secrets, and* $r^{(1)}, \ldots, r^{(d)} \in \mathcal{D}$ *be d elements in the support of* $\mathcal{D}$. *For* $1 \leq j \leq d$, *let* $(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$. *We require the existence of a function* $\mathsf{MULT} : [n] \times \mathcal{S}^d \to \mathbb{F}$ *such that for all possible* $s^{(j)}$ *and* $r^{(j)}$ *as above,* $\sum_{i=1}^{n} \mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)}) = \prod_{j=1}^{d} s^{(j)}$.

The verifiable multiplication further requires each player to locally generate an additive sharing of not only the product of d secrets but also a proof that the value is indeed correct [9]. That is, the decoder remains additive and we refer to such an VMSS scheme as an *additive* VMSS.

Definition 5 **((ϵ, d)-Verifiably multiplicative secret sharing (VMSS) [9]).** *Let c be a positive integer. A* $\mathcal{T}$*-private secret sharing scheme is said to be* (ϵ, d)*-verifiably multiplicative if it is d-multiplicative and there are two functions* $\mathsf{PROOF} : [n] \times \mathcal{S}^d \to \mathbb{F}^c$ *and* $\mathsf{VER} : \mathbb{F} \times \mathbb{F}^c \to \{1, 0\}$ *that satisfy the following properties.*

– **Correctness:** *For* $s^{(j)} \in \mathbb{F}$ *and* $r^{(j)} \in \mathcal{D}$ *with* $1 \leq j \leq d$, *let* $(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$, $m = \sum_{i=1}^{n} \mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)})$, *and* $\sigma = \sum_{i=1}^{n} \mathsf{PROOF}(i, s_i^{(1)}, \ldots, s_i^{(d)})$. *Then,* $\mathsf{VER}(m, \sigma) = 1$.
– **Verifiability:** *An adversary that modifies any additive shares for any* $T \in \mathcal{T}$ *can cause a wrong value to be accepted with probability at most* ϵ. *More formally, the experiment* $Exp(s^{(1)}, \ldots, s^{(d)}, T, \mathsf{Adv})$ *with d secrets* $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$, *unauthorized set* $T \in \mathcal{T}$, *and interactive adversary* Adv *is defined.*
  $Exp(s^{(1)}, \ldots, s^{(d)}, T, \mathsf{Adv})$:
  1. *For each j with* $1 \leq j \leq d$, *sample* $r^{(j)} \leftarrow \mathcal{D}$ *and generate* $(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$.
  2. *Give* $\{(s_i^{(1)}, \ldots, s_i^{(d)}) | i \in T\}$ *to* Adv.
  3. Adv *outputs modified additive shares* $m'_i \in \mathbb{F}$ *and* $\sigma'_i \in \mathbb{F}^c$ *with* $i \in T$. *For* $i \notin T$, *we define* $m'_i = \mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)})$ *and* $\sigma'_i = \mathsf{PROOF}(i, s_i^{(1)}, \ldots, s_i^{(d)})$.
  4. *Compute* $m' = \sum_{i=1}^{n} m'_i$ *and* $\sigma' = \sum_{i=1}^{n} \sigma'_i$.
  5. *If* $m' \neq s^{(1)} \cdots s^{(d)}$ *and* $\mathsf{VER}(m', \sigma') = 1$, *then output 1 else 0.*

  Then, it is required that for any d secrets $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$, *any unauthorized set* $T \in \mathcal{T}$, *and any unbounded adversary* Adv,

$$\Pr[Exp(s^{(1)}, \ldots, s^{(d)}, T, \mathsf{Adv}) = 1] \leq \epsilon.$$

3 An Attack against a Scheme in [9]

In this section, we present an attack against the scheme presented by Yoshida and Obana in the proof of Theorem 2 of [9]. The scheme is designed to ensure the $(0, d)$-verifiably multiplicative property against any adversary structure $\mathcal{T}$ of type Q_{d+1}.

The scheme is based on the CNF scheme proposed by Ito et al. [7] as follows: for every set of malicious players $T \in \hat{\mathcal{T}}$, generates additive shares of the product among the other players $[n] \setminus T$ and check the equality of all recovered values. Specifically, the target scheme is constructed as follows.

The Target Scheme in [9]:

- SHARE of the CNF scheme: to share a given secret s, for $T \in \hat{\mathcal{T}}$, r_T is randomly chosen from $\mathbb{F}$ subject to the restriction that $\sum_{T \in \hat{\mathcal{T}}} r_T = s$. Each share s_i is the set $\{r_T | i \notin T\}$.
- MULT is given in [3] and omitted here.
- PROOF: The subsets in $\hat{\mathcal{T}}$ is numbered from 1 to $|\hat{\mathcal{T}}|$. Let $s^{(1)}, \ldots, s^{(d)}$ be secrets. For $1 \leq j \leq d$, let $r_T^{(j)}$ with $T \in \hat{\mathcal{T}}$ denote the additive parts of $s^{(j)}$. The product $s^{(1)} \cdots s^{(d)} = (\sum_{T \in \hat{\mathcal{T}}} r_T^{(1)}) \cdots (\sum_{T \in \hat{\mathcal{T}}} r_T^{(d)})$ is written as the sum of the $|\hat{\mathcal{T}}|^d$ monomials of the form $r_{T_{j_1}}^{(1)} \cdots r_{T_{j_d}}^{(d)}$. For each $T_l \in \hat{\mathcal{T}}$, we partition the monomials into $n - |T_l|$ disjoint sets $X_{l,i}$ such that $i \in [n] \setminus T_l$ and all monomials in set $X_{l,i}$ is obtained from s_i. The possibility of partition follows from the fact that every monomial as above can be assigned to a set $X_{l,i}$ such that $i \notin T_{j_1} \cup \cdots \cup T_{j_d} \cup T_l$. The existence of such i follows from the assumption that $\mathcal{T}$ is of type Q_{d+1}. For each $1 \leq i \leq n$, $\mathsf{PROOF}(i, \cdot)$ outputs $\sigma_i = (\sigma_{i,1}, \ldots, \sigma_{i,|\hat{\mathcal{T}}|}) \in \mathbb{F}^{|\hat{\mathcal{T}}|}$ where $\sigma_{i,l}$ is the sum of the monomials in $X_{l,i}$ if $i \notin T_l$, and otherwise 0. If all players follow the scheme, then $\sigma = \sum \sigma_i$ is the vector with all components being $s^{(1)} \cdots s^{(d)}$.
- $\mathsf{VER}(m, \sigma) = 1$ if and only if $\sigma = (m, \ldots, m)$ holds.

Any set of malicious players is contained by some $T \in \hat{\mathcal{T}}$. In [9], it is claimed that the value recovered from shares for $[n] \setminus T$ would be correct, and the equality of all recovered values could guarantee that the error-probability is zero. However, from the restriction of the *additive* VMSS, the above technique does not work because the adversary Adv corrupting any T can modifies all values recovered from shares so that VER outputs 1 with probability $\epsilon = 1$.

An Attack against the Scheme: Without loss of generality, we can assume the player P_1 is corrupted, i.e., $1 \in T$. In Step 3 of *Exp*,

- Adv randomly generates $\Delta \neq 0 \in \mathbb{F}$.
- For $i \in T$, Adv generates $m_i = \mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)})$ and $\sigma_i = \mathsf{PROOF}(i, s_i^{(1)}, \ldots, s_i^{(d)})$.
- For $i \in T$, Adv defines $m'_i = m_i + \Delta$ and $\sigma'_i = \sigma_i + (\Delta, \ldots, \Delta)$ if $i = 1$, and otherwise $m'_i = m_i$ and $\sigma'_i = \sigma_i$.

– Adv outputs $m'_i \in \mathbb{F}$ and $\sigma'_i \in \mathbb{F}^c$ with $i \in T$.

From the correctness of the CNF scheme, it holds that $m' = s^{(1)} \cdots s^{(d)} + \Delta$ and $\sigma' = (m', \ldots, m')$. Thus, for $m' \neq s^{(1)} \cdots s^{(d)} + \Delta$, it holds that $\mathsf{VER}(m', \sigma') = 1$. Thus, for any d secrets $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$, any unauthorized set $T \in \mathcal{T}$, and any unbounded adversary Adv,

$$\Pr[Exp(s^{(1)}, \ldots, s^{(d)}, T, \mathsf{Adv}) = 1] = 1.$$

It is obvious that the above attack works even if T is a singleton. Thus, the scheme is not verifiably multiplicative against any adversary structure $\mathcal{T}$ not only of type Q_{d+1} but also of any type as long as $\mathcal{T}$ contains a non-empty set.

4 (Im)possibilities of Error-free VMSS

In a similar way to the attack in the previous section, we can prove that there is no $(0, d)$-verifiably multiplicative scheme by showing an adversary who corrupts a single player and causes an positive error probability $\epsilon = 1/|\mathbb{F}|^c > 0$ for any *additive* VMSS scheme.

Thus, to achieve $\epsilon = 0$, we need to allow a more general class of decoders. In fact, the scheme in [9] can be a $(0, d)$-verifiably multiplicative secret sharing scheme if we use more general decoders such as a selective decoder which removes all l-th elements of σ_i with $i \in T_l$ and computes the sum of the remaining values, and a linear decoder which uses a $(c+1) \times n$ matrix $D = [d_{l,i}]_{0 \le l \le c, 1 \le i \le n} \in \mathbb{F}^{(c+1) \times n}$ by $d_{0,i} = 1$ with $1 \le i \le n$ and $d_{l,i} = 0$ if $i \in T_l$ and otherwise $d_{l,i} = 0$. The value of $d_{l,i}$ specifies which players' shares should be added. Let M be the $n \times (c+1)$ matrix of which i-th row is (m_i, σ_i). The decoder computes $(m, \sigma) = D \times M$. We note that these two decoders can be used for the motivating applications of both verifiably and standard multiplicative secret sharing in [3, 9].

5 Conclusion

In this paper, we have pointed out flaws in an existing verifiably multiplicative secret sharing (VMSS) scheme. Namely, we have shown that a scheme proposed by Yoshida and Obana presented at ICITS 2017 is insecure even against an adversary who corrupts a single player. Then, we have shown that in the model of ICITS 2017 which restricts the decoder additive, the error-free verification is impossible. In addition, we have shown that the above scheme can be error-free by allowing a general class of decoders which include a linear one.

References

1. T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara, "High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority," *23rd ACM Conference on Computer and Communications Security (ACM CCS 2016)*, pp. 805–817, 2016.

2. T. Araki, A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein, "Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier," *38th IEEE Symposium on Security and Privacy (S&P 2017)* pp. 843–862, 2017.
3. O. Barkol, Y. Ishai, and E. Weinreb, "On d-Multiplicative Secret Sharing," *Journal of Cryptology*, vol. 23, no. 4, pp. 580–593, 2010.
4. M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation," *The 20th Annual ACM Symposium on Theory of Computing, STOC '88*, pp. 1–10, 1988.
5. G.R. Blakley, "Safeguarding Cryptographic Keys," *AFIPS 1979 Nat. Comput. Conf.*, vol. 48, pp. 313–317, 1979.
6. D. Chaum, C. Crèpeau, and I. Damgård, "Multiparty Unconditionally Secure Protocols," *The 20th Annual ACM Symposium on Theory of Computing, STOC '88*, pp. 11–19, 1988.
7. M. Ito, 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. M. Yoshida and S. Obana, "Verifiably Multiplicative Secret Sharing," *The 10th International Conference on Information Theoretic Security ICITS2017, in Lecture Notes in Comput. Sci.*, vol. 10681, pp. 73–82, 2017.