検証可能な乗法秘密分散の効率向上

吉田 真紀[1]　尾花 賢[2]

概要：d-乗法秘密分散 (Multiplicative Secret Sharing，以下 MSS) とは，Barkol-Ishai-Weinreb (Journal of Cryptology，2010) が提案した秘密分散であり，情報理論的に安全な秘密分散の性質に加え各プレーヤが任意の d 個の秘密のシェアからそれらの乗算結果の加法的シェアを直接計算できる．著者らはこれまでに，乗算結果の正しさを検証可能な乗法秘密分散 (Verifiably MSS，以下 d-VMSS) を導入し，d-VMSS が存在するための必要十分条件を示し，効率的な構成法を示した (IEEE Transactions on Information Theory, 2019)．d-VMSS とは d-MSS の性質に加え乗算結果の正しさを示す証明の加法的シェアも計算でき，従来法では証明が有限体の要素二つであった．本稿では，証明を有限体の要素一つに最小化する構成法を提案する．そのために，MSS および VMSS における復元が加法であることに着目し，乗法に限定して準同型な関数 (multiplicative-only homomorphic function, 以下 MHF) を導入し，証明の構成に利用した．さらに，任意の有限体で利用でき，検証効率が良く，かつ実装が容易な MHF の具体例も示す．

キーワード：秘密分散，乗法，検証可能，乗法限定準同型

Efficiency Improvement in Verifiably Multiplicative Secret Sharing

Maki Yoshida[1]　Satoshi Obana[2]

Abstract: A d-multiplicative secret sharing (d-MSS) scheme [Barkol-Ishai-Weinreb, Journal of Cryptology, 2010] allows the players to multiply d shared secrets without recovering the secrets by converting their shares locally into an additive sharing of the product. We have introduced the notion of verifiably multiplicative SS, VMSS for short, proved a necessary and sufficient condition for VMSS to exist, and presented an efficient construction [IEEE Transactions on Information Theory, 2019]. In the previous construction, the overhead of verifiability, called a proof, is two field elements. This paper presents a more efficient construction of VMSS with a smaller proof size and a smaller share size than the previous schemes. Our main technical contribution is to formalize *multiplicative-only* homomorphic functions (MHFs) and use an MHF for generating a proof. In addition, we present a concrete instance of MHF that can be used for any finite field with highly efficient verification and easy implementation. Our technique also works for multi-party computation to guarantee robustness and improve efficiency.

Keywords: Secret sharing, multiplication, verifiability, somewhat homomorphic

1. はじめに

背景. d-乗法秘密分散 (Multiplicative Secret Sharing, 以下 MSS) とは，Barkol-Ishai-Weinreb が [1] (Journal of Cryptology，2010) で提案した秘密分散であり，情報理論的に安全な秘密分散の性質に加え，各プレーヤが任意の d 個の秘密のシェアからそれらの乗算結果のシェアを，他プレーヤとの通信無しでローカルに計算できる．このとき，秘密は有限体の要素一つであり，乗算結果のシェアも有限体の要素一つ，乗算結果は加法のみで復元できる．さらに，d-強乗法秘密分散 (Strongly MSS) とは，任意の攻撃者集合を排除しても d-乗法性を失なわない秘密分散である．

Barkol らは [1] で，d-MSS および d-Strongly MSS が存

[1] 情報通信研究機構, 東京都小金井市貫井北町 4-2-1, NICT, 4-2-1 Nukuikitamachi, Koganei, Tokyo, Japan
[2] 法政大学, 東京都小金井市梶野町 3-7-2, Hosei University, 3-7-2 Kajinocho, Koganei, Tokyo, Japan

表 1 従来の d-乗法秘密分散との比較．方式が耐性をもつ攻撃者構造 $\mathcal{T}$ については，type あるいは結託しきい値 t を示す．なお，$\hat{\mathcal{T}}$ は $\mathcal{T}$ の極大集合の族を表す．攻撃者構造の type は Q の添字が小さいほど耐性が高いことを表す．シェアと証明のサイズは，それぞれ $\mathbb{F}$ の要素数で数える．検証処理は，$\mathbb{F}$ 上の演算と等号判定からなるため，計算複雑度をそれらで数える．文献 [1] で乗算結果の正しさを検証するためには，全攻撃者集合に対して残りのプレーヤで乗算結果を復元し等号判定することになる．そこで，[1] の方式の証明は全ての復元結果とし，検証処理は等号判定とみなす．文献 [21] の方式と提案方式の検証誤り率は $\epsilon = 1/(|\mathbb{F}| - 1)$ で揃えている．$\epsilon = 0$ となる VMSS が存在しないことは [21] で証明されている．

方式	攻撃者構造 (タイプ/結託しきい値)	秘密のシェア ($\mathbb{F}$ の要素数)	証明 ($\mathbb{F}$ の要素数)	検証 (演算・等号判定回数)
文献 [1]: Shamir-based	$t < \frac{n}{d+1}$	1	${}_nC_t$	加: 0, 乗: 0, 等: $O(n^t)$
文献 [1]: CNF-based (Theorem A.2)	type Q_{d+1}	${}_{n-1}C_t$	$\lvert\hat{\mathcal{T}}\rvert$	加: 0, 乗: 0, 等: $O(\lvert\hat{\mathcal{T}}\rvert)$
文献 [21]: Shamir-based (Lemma 1)	$t < \frac{n}{d}$	3	2	加: 0, 乗: 1, 等: 1
文献 [21]: CNF-based (Lemma 1)	type Q_d	$3 \times {}_{n-1}C_t$	2	加: 0, 乗: 1, 等: 1
提案方式: Shamir-based (定理 4)	$t < \frac{n}{d}$	2	1	加: 0, 乗: 1, 等: 1
提案方式: CNF-based (定理 4)	type Q_d	$2 \times {}_{n-1}C_t$	1	加: 0, 乗: 1, 等: 1

在するための必要十分条件を示し，Shamir の秘密分散 [17] と Ito-Saito-Nishizeki の CNF 秘密分散 [14] が MSS かつ Strongly MSS であることを示した．秘密のシェアから乗算結果のシェアへの変換は，適切なシェアの組み合わせに対する有限体上の乗法と加法を適用すればよく，現在の計算機環境で実装が容易である．これらが d-MSS および d-Strongly MSS となる条件は，攻撃者構造がそれぞれ type Q_d および Q_{d+1} であり，しきい値型の場合はプレーヤ数 n に対して結託しきい値 t が $t < n/d$ および $t < n/(d+1)$ を満たせばよい．

d-MSS および d-Strongly MSS の応用先は Multi-party computation (MPC) [2], [4], [6], [9] に加え zero-knowledge proofs や two-party computation など [10], [12], [13]， 多岐にわたる．例えば MPC への応用においては，乗法を適用する秘密の数 d を増やすことで MPC のラウンド数を減らすことができ [1]，強乗法性から active adversary に対する robustness が保証できる [6]．そのためには結託耐性 t を下げるか，総プレーヤ数 n を多ければ良い．このような設定は近年では不自然ではなく，実際に Hazay らが Asiacrypt 2017 [11] で，Tor network [7] ($n \geq 6000$) や Border Gateway Protocol ($n \geq 1000$) を例に挙げ，プレーヤ数が大きく (large-scale scenario) かつ honest players が占める割合が 10〜30%と小さい (small minority) 設定を対象としている．

このように従来の d-MSS および d-Strongly MSS [1] は，現在の計算機環境で実装が容易で近年の応用先の多様化に対応しているが，大きな課題が一つある．それは，乗算結果の正しさの検証で全攻撃者集合に対する復元処理が必要なことである．これにより，結託しきい値 t に対して計算コストが $O(n^t)$ と指数的に増加し，n が大きい場合には極めて効率が悪い．

従来の課題に対して著者らはこれまでに [21] (IEEE Transactions on Information, 2019) で，乗算結果の正しさを検証可能な秘密分散 (Verifiably MSS，以下 VMSS) を導入し，d-VMSS が存在するための必要十分条件が d-MSS と同じであることを示し，効率的な構成法を示した．d-VMSS とは，d-MSS の性質に加え，乗算結果の正しさを示す証明のシェアも他プレーヤとの通信無しでローカルに計算でき，加法のみで証明を復元できる．文献 [21] で提案した構成法では，乗算結果の証明が有限体の要素二つであり，証明の検証に要する計算コストは乗法一回，等号判定一回と極めて効率的である．なお，証明を構成する要素の一つは乱数，もう一つは乗算結果と乱数から求まる認証子であり，各プレーヤはシェアの計算においてそれらの値を知ることはない．

従来の d-VMSS [21] では秘密の分布への前提が無いため，証明のランダム性確保のため乱数は必要であり，有限体の要素一つは最良と考えられる．そこで生じる自然な疑問は，秘密の分布に何らかの前提をおくことで，証明から乱数を除き，有限体の要素一つまで減らすことができるかというものである．

本研究の貢献． 本研究では min-entropy が高い秘密を対象とし，証明が有限体の要素一つの VMSS を実現する (表 1 参照)．証明の検証に要する計算コストは乗法一回，等号判定一回であり，従来の d-VMSS [21] と同じである．シェアの加法性から証明の非線形性は必要であり，検証における乗法一回は最良と考えられる．具体的な貢献は以下の通りである．

- 乗法限定準同型関数 (Multiplicative-only Homomorphic Function, 以下 MHF) の導入：MSS および VMSS における復元の加法性に着目し，乗法に限定して準同型な関数 MHF を導入した．従来，加法的な攻撃を検

出可能にする符号 Algebraic Manipulation Detection Codes [5] はあったが，そこに乗法準同型性を含めたものは著者が知る限り無い．また，準同型性で演算が制約されることは，fully/somewhat homomorphic encryption のように，一般に機能面で短所となる．それに対して本研究では，演算を限定することを機能面の長所にする点で独創的である．

- 検証効率が良く実装が容易な MHF の具体的構成法：MHF の関数族を示し，具体的な関数三つ $f(x) = x^2, x^3, x^{-1}$ が MHF であることの証明を示した．他の関数についても同様に証明でき，いずれの関数を VMSS の構成に利用しても証明が有限体の要素一つ，かつ検証に必要な演算は乗法と等号判定であり現在の計算機で実装が容易である．さらに，具体例の一つは任意の有限体に利用可能であり，かつ検証に要する演算が乗法一回，等号判定一回と最小化され，汎用性と効率性の観点で望ましい．なお，上述の三つの関数は秘密分散の cheater detection に利用されているが [8], [15], [16]，関数族として一般化はされておらず，統合的な観点での攻撃耐性と効率の評価は本研究が初である．
- MHF を利用した d-VMSS の一般的構成法：d-MSS と MHF から d-VMSS を構成する手法を提案した．すなわち，d-MSS で独立に分散された d 個の秘密の乗算結果 m に対して MHF f を適用した結果 $\sigma = f(m)$ を証明とし，各プレーヤは秘密のシェアのみから m の加法的シェアに加え σ の加法的シェアも計算する．同様の関数が利用された秘密分散および MPC の手法は一般にはそのまま利用できない．なぜならば，d-VMSS では秘密分散と異なり各秘密の分散時点で f の適用対象の m も適用結果 σ も決まっておらず，さらに MPC とも異なり他プレーヤと情報交換しないためである．(逆に，d-VMSS の手法を秘密分散および MPC に適用した効率改善は可能である．本研究の手法の具体的な応用は今後の課題である．) 提案法では関数の乗法準同型性を生かし，秘密 s のシェアに $f(s)$ のシェアを含め，d-乗法性から乗算結果のシェアだけでなく証明のシェアも計算する．結果として，証明のサイズだけでなく秘密のシェアサイズも削減できた．具体的には，従来の d-VMSS [21] の秘密のシェアサイズは d-MSS の三倍だったが，提案法の秘密のシェアサイズは d-MSS の二倍である．

2. 準備

2.1 秘密分散と攻撃者構造

文献 [1] の秘密分散の定義を示す．

正整数 $n > 0$ に対して，$[n] = \{1, \ldots, n\}$ とする．秘密分散では，ディーラと n 人のプレイヤ $P_1, \ldots, P_n$ が参加し，ディーラは秘密 s をシェアの n 項組 $(s_1, \ldots, s_n)$ に分散し，シェア s_i をプレーヤ P_i に与える．

秘密は有限体 $\mathbb{F}$ の要素とし，シェアのドメインを $\mathcal{S}$，ディーラが選ぶ乱数 r の確率分布を $\mathcal{D}$ とする．

秘密 $s \in \mathbb{F}$ を分散するために，ディーラは乱数 $r \in \mathcal{D}$ を選択し，シェア関数 $\mathsf{SHARE} : \mathbb{F} \times \mathcal{D} \to \mathcal{S}^n$ を適用し，$\mathsf{SHARE}(s, r) = (s_1, \ldots, s_n)$ を計算する．プレーヤ集合 $T \subseteq [n]$ に対して，$\mathsf{SHARE}(s, r)_T$ は $\mathsf{SHARE}(s, r)$ の項目を T の要素に限定した $|T|$-項組とする．

定義 1 (t-Private Secret Sharing [1])．秘密分散 SHARE が t-秘匿 *(t-private)* とは，任意のプレーヤ集合 $T \subseteq [n]$ *($|T| = t$)* と任意の秘密の組 $s, s' \in \mathbb{F}$ に対して，ディーラの乱数 r が確率分布 $\mathcal{D}$ に従うとき，$\mathsf{SHARE}(s, r)_T$, $\mathsf{SHARE}(s', r)_T$ の確率分布が同じであること．

一般化においては，攻撃者集合の族である攻撃者構造が着目される．

定義 2 (Adversary Structure [1])．$n > 0$ を正整数とする．n プレーヤの攻撃者構造 *(adversary structure)* とは部分集合で閉じた集合族 $\mathcal{T} \subseteq 2^{[n]}$ である．すなわち，もし $T \in \mathcal{T}$ かつ $T' \subseteq T$ ならば，$T' \in \mathcal{T}$ である．また，$\hat{\mathcal{T}}$ は $\mathcal{T}$ に含まれる極大集合の族とする *(*任意の $\hat{\mathcal{T}}$ の要素は他の $\hat{\mathcal{T}}$ の要素に含まれない*)*.

定義 3 ($\mathcal{T}$-Private Secret Sharing [1])．$n > 0$ を正整数，$\mathcal{T}$ を n プレーヤの攻撃者構造とする．秘密分散方式が $\mathcal{T}$-秘匿 *($\mathcal{T}$-private)* とは，任意の秘密の組 $s, s' \in \mathbb{F}$，任意の攻撃者集合 $T \in \mathcal{T}$ に対して，ディーラの乱数 r が確率分布 $\mathcal{D}$ に従うとき，$\mathsf{SHARE}(s, r)_T, \mathsf{SHARE}(s', r)_T$ の確率分布が同じであること．

例 1 (4-Player Adversary Structure of Type Q_2)．*4* プレーヤの攻撃者構造の例 $\mathcal{T}$ を示す．

$$\mathcal{T} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{3, 4\}\}.$$

$\mathcal{T}$ の極大集合 $\hat{\mathcal{T}}$ は $\{\{1\}, \{2\}, \{3, 4\}\}$ である．ここで，$\mathcal{T}$ の任意の *2* 集合 $T_1, T_2 \in \mathcal{T}$ の和 $T_1 \cup T_2$ は P にはならないため，$\mathcal{T}$ は *type* Q_2 である． □

2.2 乗法秘密分散

文献 [1] の乗法秘密分散 (Multiplicative Secret Sharing, 以下 MSS) の定義を示す．

定義 4 (d-Multiplicative Secret Sharing [1])．秘密分散方式が d-乗法 *(d-multiplicative)* とは，以下の d-乗法性 *(d-multiplicative property)* の要件を満たすことである*:* $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$ を d 個の秘密とし，$r^{(1)}, \ldots, r^{(d)} \in \mathcal{D}$ を $\mathcal{D}$ の台 *(support)* の d 個の要素とする．各 j $(1 \le j \le d)$ に対して，$(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$ とする．要件は乗法関数 $\mathsf{MULT} : [n] \times \mathcal{S}^d \to \mathbb{F}$ が存在し，任意の $s^{(j)}, r^{(j)}$ に対して，$\sum_{i=1}^{n} \mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)}) = \prod_{j=1}^{d} s^{(j)}$ を満たすこと．d-乗法な秘密分散 *(Multiplicative Secret Sharing)*

を，以下 d-*MSS* と表す．

Barkol ら [1] の主要な成果は，d-MSS の特徴付けである．

定理 1 (Theorem 4.6 [1])．任意の正整数 n, d，任意の n プレーヤの攻撃者構造 $\mathcal{T}$ に対して，$\mathcal{T}$ が *type* Q_d である場合かつその場合に限り，d-乗法かつ $\mathcal{T}$-秘匿の秘密分散が存在する．

2.3 検証可能な乗法秘密分散

文献 [21] の検証可能な乗法秘密分散 (Verifiably MSS, 以下 VMSS) の定義を示す．ここで，検証可能性に関する攻撃者構造は，秘匿に関する攻撃者構造と同じである．乗法結果の加法的シェアである $\mathbb{F}$ の要素に加えて，乗算結果の正しさを示す証明の加法的シェアとして，$\mathbb{F}$ の c 項組 ($c > 0$ に対する $\mathbb{F}^c$ の要素) が得られる．ここで，c 項組 $a = (a_1, \ldots, a_c)$ と $b = (b_1, \ldots, b_c)$ の加算は，各要素の加算で定義される．すなわち，$a + b = (a_1 + b_1, \ldots, a_c + b_c)$．

定 義 5 ((ϵ, d)-Verifiably Multiplicative Secret Sharing [21])．$c > 0$ を正整数とする．$\mathcal{T}$-秘匿な秘密分散方式が (ϵ, d)-検証可能乗法とは，d-乗法であり，以下を満たす *2* つの関数 $\mathsf{PROOF} : [n] \times \mathcal{S}^d \to \mathbb{F}^c$ と $\mathsf{VER} : \mathbb{F} \times \mathbb{F}^c \to \{1, 0\}$ が存在することである．

正当性*:* 任意の $s^{(j)} \in \mathbb{F}$, $r^{(j)} \in \mathcal{D}$ *(*$1 \le j \le d$*)* に対し，$(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$, $m = \sum_{i=1}^{n} \mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)})$, $\sigma = \sum_{i=1}^{n} \mathsf{PROOF}(i, s_i^{(1)}, \ldots, s_i^{(d)})$ としたとき，$\mathsf{VER}(m, \sigma) = 1$ が成立する．

検証可能性*:* 攻撃者が任意の攻撃者集合 $T \in \mathcal{T}$ の任意の加法的シェアを改ざんし，正しくない値を乗法結果として受理させる確率 *(*以下，検出誤り確率*)* は高々 ϵ である．厳密には，d 個の秘密 $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$, 攻撃者集合 $T \in \mathcal{T}$, 対話的攻撃者 Adv に対して以下のゲームを定義する．

$Exp(s^{(1)}, \ldots, s^{(d)}, T, \mathsf{Adv})$*:*

(1) 各 j *(*$1 \le j \le d$*)* に対して, $r^{(j)} \leftarrow \mathcal{D}$ を選択し，$(s_1^{(j)}, \ldots, s_n^{(j)}) = \mathsf{SHARE}(s^{(j)}, r^{(j)})$ を計算する．

(2) $\{(s_i^{(1)}, \ldots, s_i^{(d)}) | i \in T\}$ を Adv に与える．

(3) Adv は $m'_i \in \mathbb{F}$, $\sigma'_i \in \mathbb{F}^c$ *(*$i \in T$*)* を出力する *(*攻撃者集合に含まれるプレーヤ $i \in T$ の改ざんした加法的シェア*)*．各 $i \notin T$ に対して, $m'_i = \mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)})$, $\sigma'_i = \mathsf{PROOF}(i, s_i^{(1)}, \ldots, s_i^{(d)})$ とする *(*攻撃者集合に含まれないプレーヤの正しい加法的シェア*)*.

(4) $m' = \sum_{i=1}^{n} m'_i$, $\sigma' = \sum_{i=1}^{n} \sigma'_i$ を計算する．

(5) もし $m' \neq s^{(1)} \cdots s^{(d)}$ かつ $\mathsf{VER}(m', \sigma') = 1$ ならば, 1 を出力し，そうでなければ *0* を出力する．

要件は，任意の d 個の秘密 $s^{(1)}, \ldots, s^{(d)} \in \mathbb{F}$, 任意の攻撃者集合 $T \in \mathcal{T}$, 無限の計算能力を有する任意の攻撃者 Adv に対して，

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

文献 [21] の主要な成果は，(ϵ, d)-VMSS の特徴付けと，高効率な一般的構成法である．まず，結託耐性を type Q_d からおとすことなく誤り率 $\epsilon = 0$ を達成することは不可能である．

定理 2 (Theorem 1 [21])．任意の正整数 n, d, 任意の n プレーヤの攻撃者構造 $\mathcal{T}$ に対して，$\mathcal{T}$-秘匿かつ $(0, d)$-検証可能乗法秘密分散は存在しない．

誤り率 $\epsilon > 0$ を許せば，VMSS が存在する．

定理 3 (Theorem 2 [21])．任意の数 $0 < \epsilon < 1$, 任意の正整数 n, d, 任意の n プレーヤの攻撃者構造 $\mathcal{T}$ に対して，$\mathcal{T}$ が *type* Q_d である場合かつその場合に限り，$\mathcal{T}$-秘匿かつ (ϵ, d)-検証可能乗法秘密分散が存在する．

文献 [19] の Lemma 1 には，d-MSS から (ϵ, d)-VMSS への一般的構成法が示されており，証明は $\mathbb{F}$ の拡大体 $\mathbb{F}^E$ の要素二つ，$E = \frac{\log \epsilon^{-1}}{\log |\mathbb{F}|}$ である．

3. 効率の向上

3.1 乗法限定準同型関数

乗算結果の正しさを効率的に検証可能にするため，乗法限定準同型関数を概念を導入する．これは，秘密分散における秘密 s の復元結果の正しさの検証に用いられる認証子 s^2 [8], s^3 [16], s^{-1} [15] の一般化として捉えることができる (後述の補題 1〜 3 参照)．

定 義 6 (Multiplicative-only Homomorphic Function, MHF)．$\mathbb{F}$ を有限体とする．このとき，以下の二つの条件を満たす関数 $f : \mathbb{F} \to \mathbb{F}$ を col-乗法限定準同型という．

(1) 任意の $m, m' \in \mathbb{F}$ に対し $f(m) \cdot f(m') = f(m \cdot m')$.

(2) 任意の $\delta \in \mathbb{F} \setminus \{0\}$ と，任意の $\Delta \in \mathbb{F}$ に対し

$$|\{m \in \mathbb{F} \mid f(m + \delta) = f(m) + \Delta\}| \le \mathsf{col}\,.$$

次に，定義 4 の MHF の存在についていくつかの結果を示す．本稿では，有限体 $\mathbb{F}$ 上の関数族 $f(x) = x^i$ を考える．具体例として，$f(x) = x^2, x^3$, および $f(x) = x^{q-2}$ ($x \neq 0$ では x^{-1} であり，$x = 0$ では 0) が MHF であることの証明を示す．

補題 1. $\mathbb{F}$ を標数が奇素数である有限体とする．このとき関数 $f(x) = x^2$ は $\mathsf{col} = 1$ の乗法限定準同型である．

証明. 任意の $m, m' \in \mathbb{F}$ に対し $f(m) \cdot f(m') = m^2 \cdot m'^2 = (m \cdot m')^2 = f(m \cdot m')$ が成立するため f が性質 (1) を満足することが示された．次に f が性質 (2) を満足すること，つまり任意の $\delta \in \mathbb{F} \setminus \{0\}$ と任意 $\Delta \in \mathbb{F}$ に対し，次式を満たす m が一つ存在することを示す．

$$(m + \delta)^2 = m^2 + \Delta$$

上式は m の一次式 $2\delta \cdot m = \Delta - \delta^2$ と等価であり，体上の一次式はちょうど一つの解を有することから $\mathsf{col} = 1$ の

性質 (2)，すなわち，

$$|\{m \in \mathbb{F} \mid f(m+\delta) = f(m) + \Delta\}| = 1,$$

が示された． □

なお，体の標数が 2 の時，$(m+\delta)^2 = m^2 + \Delta$ は (係数 2 の項が 0 となるため) $\delta^2 = \Delta$ と等価となる．したがって，$\Delta = \delta^2$ を満たすように Δ を選ぶと，体の全ての元に対して $(m+\delta)^2 = m^2 + \Delta$ が成立するため，$|\{m \mid f(m+\delta) = f(m) + \delta^2\}| = |\mathbb{F}|$ となってしまう．これは，関数 $f(x) = x^2$ が標数 2 の体を秘密の要素とする VMSS の構成に利用できないことを意味している．

補題 2. $\mathbb{F}$ を標数が 3 以外の有限体とする．このとき関数 $f(x) = x^3$ は $\mathsf{col} = 2$ の乗法限定準同型である．

証明. 任意の $m, m' \in \mathbb{F}$ に対し $f(m) \cdot f(m') = m^3 \cdot m'^3 = (m \cdot m')^3 = f(m \cdot m')$ が成立するため f が性質 (1) を満足することが示された．次に f が性質 (2) を満足すること，つまり任意の $\delta \in \mathbb{F} \setminus \{0\}$ と任意 $\Delta \in \mathbb{F}$ に対し，次式を満たす m が高々二つ存在することを示す．

$$(m+\delta)^3 = m^3 + \Delta$$

上式は m の二次式 $3\delta \cdot m^2 + 3\delta^2 \cdot m + \delta^3 - \Delta^3 = 0$ と等価であり，体上の二次式は高々二つの解を有することから，$\mathsf{col} = 2$ の性質 (2) が示された． □

補題 1 と同様の議論により，体の標数が 3 であるときは，$(m+\delta)^3 = m^3 + \Delta$ は $\delta^3 = \Delta$ と等価になるため，$\Delta = \delta^3$ を満たすように Δ を選ぶと，体の全ての元に対して $(m+\delta)^3 = m^3 + \Delta$ が成立する．これは，関数 $f(x) = x^3$ が標数 3 の体を秘密の要素とする VMSS の構成に利用できないことを意味している．

補題 3. $\mathbb{F}$ を有限体とする．このとき関数

$$f(x) = \begin{cases} x^{-1} & if\ x \neq 0 \\ 0 & if\ x = 0 \end{cases}$$

は，$\mathsf{col} = 4$ の乗法限定準同型である．

証明. 任意の $m, m' \in \mathbb{F} \setminus \{0\}$ に対し $f(m) \cdot f(m') = m^{-1} \cdot m'^{-1} = (m \cdot m')^{-1} = f(m \cdot m')$ が成立し，m, m' のいずれかが 0 のときは $f(m) \cdot f(m') = 0 = f(m \cdot m')$ が成立するため f が性質 (1) を満足することが示された．次に f が性質 (2) を満足することを示す．性質 (2) を示すには，次の三つのケースを考える必要がある．

ケース 1) $m \neq 0$ **かつ** $m + \delta \neq 0$ **の場合:** このとき性質 (2) は次式と等価となる．

$$(m+\delta)^{-1} = m^{-1} + \Delta$$

上式の両辺に $m(m+\delta)$ を乗じて整理すると，次式が得られる．

$$\Delta \cdot m^2 + \delta\Delta \cdot m + \delta = 0$$

体上の二次式は高々二つの解を有することから上式を満たす m は高々二つとなる．

ケース 2) $m = 0$ **かつ** $m + \delta \neq 0$ **の場合:** このとき性質 (2) は次式と等価となる．

$$(m+\delta)^{-1} = \Delta$$

上式は $\delta = \Delta^{-1}$ を満たすときのみ解 $m = 0$ を有する (それ以外の場合は解が $m \neq 0$ となるため，ケース 2 の条件を満たさない)．

ケース 3) $m \neq 0$ **かつ** $m + \delta = 0$ **の場合:** このとき性質 (2) は次式と等価となる．

$$0 = m^{-1} + \Delta$$

上式は $\delta = \Delta^{-1}$ を満たすときのみ解 $m = -\delta$ を有する (それ以外の場合は解が $m \neq -\delta$ となるため，ケース 3 の条件を満たさない)．

以上の 3 つのケースをまとめると，$\delta = \Delta^{-1}$ を満たす δ と Δ に対して，$f(m+\delta) = f(m) + \Delta$ は $m = 0, -\delta$ および $\Delta \cdot m^2 + \delta\Delta \cdot m + \delta = 0$ の解からなる高々 4 つの解を有し，$\delta = \Delta^{-1}$ を満たさない場合は，高々 2 つの解を有する．以上により性質 (2) が示された． □

上述のように，MHF $f(x) = x^i$ は i の値によって col が異なる．$i > 1$ の増加に伴い $\mathsf{col} = 1$ から増加し，途中で減少に転じて $i = q-2$ で $\mathsf{col} = 4$ になる．一般に，i を標数 p で割り切れない数にすると，$(x+\delta)^i = x^i + \Delta$ の x^{i-1} の項は残るため，$\mathsf{col} \leq i-1$ は保証できる．$i = q-2$ の場合，標数 $p = 2$ に対して i は p の倍数になるが，別アプローチの証明により $\mathsf{col} \leq 4$ が保証できる．また，本関数 f を d-VMSS を利用した場合の検証は，復元した乗算結果 m' に対して $f(m') = m'^i$ を計算し，復元した証明 σ' と等号判定をする．ただし，$i \geq q/2$ に対しては $m'^{q-i-1} \cdot \sigma'$ を計算し 1 (あるいは 0) との等号判定でも検証可能である．よって，$i = 2, q-2$ すなわち，補題 1 と 3 の f で乗法回数が最小の一回となる．補題 1 の $f(x) = x^2$ は利用可能な有限体が標数 2 以外に限定されるが，補題 3 の $f(x) = x^{q-2}$ ($x \neq 0$ では x^{-1} であり，$x = 0$ では 0) は任意の有限体に利用可能であり，汎用性が高い．

また，本稿では MHF の定義域と値域を同じにしているが，異なる有限体として一般化し構成することも可能である．その具体的な構成は今後の課題とする．

3.2 一般的構成法

定理 4. $(\mathsf{SHARE}', \mathsf{MULT}')$ を $\mathcal{T}$-秘匿かつ d-乗法な秘密分散とし，$f : \mathbb{F} \to \mathbb{F}$ は col の乗法限定準同型関数と

する．$\mathcal{T}$-秘匿かつ $(p_{\mathsf{max}} \cdot \mathsf{col}, d)$-検証可能な乗法秘密分散 $(\mathsf{SHARE}, \mathsf{MULT}, \mathsf{PROOF}, \mathsf{VER})$ が存在し，$c = 1$ となる *(*証明は有限体の要素一つ*)*．ただし，p_{max} は d 個の秘密の積 $s_1 \cdots s_d$ により定義される確率変数 M に対し $p_{\mathsf{max}} = \max_{(s_1,\ldots,s_d)\in\mathbb{F}^d} \Pr[M = s_1 \cdots s_d]$ を満たす数とする．

証明．d-乗法秘密分散 $\mathsf{SHARE}' : \mathbb{F} \to \mathcal{S}$，$\mathsf{MULT}' : [n] \times \mathcal{S}^d \to \mathbb{F}$ と $f : \mathbb{F} \to \mathbb{F}$ を用いて，検証可能な乗法秘密分散の各アルゴリズムを次のように構成する．

SHARE の構成: $\mathsf{SHARE} : \mathbb{F} \times \mathcal{D}^2 \to \mathcal{S}^2$ を $\mathsf{SHARE}(s, (r_1, r_2)) = (\mathsf{SHARE}'(s, r_1), \mathsf{SHARE}'(f(s), r_2))$ によって定義する．

MULT と PROOF の構成: $s^{(1)}, \ldots, s^{(d)}$ を d 個の秘密とし，秘密 $s^{(j)}$ のプレーヤ i 向けのシェアを $s_i^{(j)} = (t_i^{(j)}, u_i^{(j)})$ とする．この時，MULT を $\mathsf{MULT}(i, s_i^{(1)}, \ldots, s_i^{(d)}) = \mathsf{MULT}'(i, t_i^{(1)}, \ldots, t_i^{(d)})$，$\mathsf{PROOF}$ を $\mathsf{PROOF}(i, s_i^{(1)}, \ldots, s_i^{(d)}) = \mathsf{MULT}'(i, u_i^{(1)}, \ldots, u_i^{(d)})$ によって定義する．

VER の構成: $m_i = \mathsf{MULT}(i, t_i^{(1)}, \ldots, t_i^{(d)})$，$\sigma_i = \mathsf{MULT}(i, t_i^{(1)}, \ldots, t_i^{(d)})$ に対して $m = \sum_{i=1}^n m_i$ および $\sigma = \sum_{i=1}^n \sigma_i$ を計算し，$\sigma = f(m)$ が成立すれば 1 を出力し，そうでない場合は 0 を出力する．

上述のように構成した $(\mathsf{SHARE}, \mathsf{MULT}, \mathsf{PROOF}, \mathsf{VER})$ が $\mathcal{T}$-秘匿かつ $(p_{\mathsf{max}} \cdot \mathsf{col}, d)$-検証可能乗法であることを示す．

$(\mathsf{SHARE}', \mathsf{MULT}')$ が $\mathcal{T}$-秘匿であることより，$(\mathsf{SHARE}, \mathsf{MULT}, \mathsf{PROOF}, \mathsf{VER})$ も $\mathcal{T}$-秘匿であることは自明であり，また，$(\mathsf{SHARE}', \mathsf{MULT}')$ が d-乗法であることより，$(\mathsf{SHARE}, \mathsf{MULT}, \mathsf{PROOF}, \mathsf{VER})$ も d-乗法であることも自明である．

次に，検証可能性を証明する．$T \in \mathcal{T}$ とし，Exp のステップ 4 で計算された m' と σ' に対して $\delta = m - m'$，$\Delta = \sigma - \sigma'$ とする．攻撃者 Adv は任意の (δ, Δ) を選択し，Exp のステップ 3 で m'_i と σ'_i $(i \in T)$ を改ざんできる．関数 f の性質 (1) により，$\sigma = f(s^{(1)}) \cdots f(s^{(d)}) = f(s^{(1)} \cdots s^{(d)})$ が成立するため，検出誤りが発生するのは $\delta \neq 0$ にも関わらず，$m = s^{(1)} \cdots s^{(d)}$ に対して $\mathsf{VER}(m + \delta, f(m) + \Delta) = 1$ すなわち $f(m + \delta) = f(m) + \Delta$ が成立する場合である．この式が成立する確率の上界は次のように計算できる．

$$
\begin{aligned}
&\Pr[f(m+\delta) = f(m) + \Delta] \\
&= \sum_{m \in \{m | f(m+\delta) = f(m)+\Delta\}} \Pr[M = m] \\
&= |\{m | f(m+\delta) = f(m) + \Delta\}| \cdot \max_{m \in \mathbb{F}} \Pr[M = m] \\
&\leq p_{\mathsf{max}} \cdot \mathsf{col}
\end{aligned}
$$

したがって，方式が $(p_{\mathsf{max}} \cdot \mathsf{col}, d)$-検証可能乗法であることが示された． □

4. おわりに

本稿では，d-VMSS の効率向上を目的とし，乗法限定で準同型な関数 MHF を導入し，MHF の具体的な構成法を示し，min-entropy が高い秘密に対する d-VMSS を MHF と d-MSS から構成する手法を提案した．提案法は，従来よりも秘密のシェアサイズと証明のサイズが小さく，検証に要する計算コストの低さと結託耐性の高さ，現在の計算機環境における実装の容易さという従来の長所も兼ね備えている．今後の課題として，新たな MHF の提案や MHF の拡張，提案手法の MPC への応用が考えられる．

参考文献

[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] 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.

[3] G.R. Blakley, "Safeguarding Cryptographic Keys," *AFIPS 1979 Nat. Comput. Conf.*, vol. 48, pp. 313–317, 1979.

[4] 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.

[5] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs, "Detection of Algebraic Manipulation with Application to Robust Secret Sharing and Fuzzy Extractors," *Advances in Cryptology - EUROCRYPT2008 in Lecture Notes in Comput. Sci.*, vol. 4965, pp. 471–488, 2008.

[6] 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.

[7] R. Dingledine, N. Mathewson, and P.F. Syverson, "Tor: The Second-Generation Onion Router," *USENIX 2004*, pp. 303–320, 2004.

[8] M. Fitzi, J. Garay, S. Gollakota, C. Pandu Rangan, and K. Srinathan, "Round-Optimal and Efficient Verifiable Secret Sharing," *Third Theory of Cryptography Conference, TCC 2006 in Lecture Notes in Comput. Sci.*, vol. 3876, pp. 329–342, 2006.

[9] S. Goldwasser, S. Micali, and A. Wigderson, "How to Play Any Mental Game, or A Completeness Theorem for Protocols with an Honest Majority," *The 19th Annual ACM Symposium on Theory of Computing, STOC '87*, pp. 218–229, 1987.

[10] D. Harnik, Y. Ishai, E. Kushilevitz, and J.B. Nielsen, "OT-Combiners via Secure Computation," *Fifth Theory of Cryptography Conference, TCC 2008 in Lecture Notes in Comput. Sci.*, vol. 4948, pp. 393–411, 2008.

[11] C. Hazay, E. Orsini, P. Scholl, E. Soria-Vazquez, "Concretely Efficient Large-Scale MPC with Active Security (or, TinyKeys for TinyOT)," *Advances in Cryptology - ASIACRYPT 2017 in Lecture Notes in Comput. Sci.*, vol. 10624, Part III, pp. 86–117, 2017.

[12] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Zero-knowledge from Secure Multiparty Computation," *The 39th Annual ACM Symposium on Theory of Computing, STOC 2007*, pp.21–30, 2007.

[13] Y. Ishai, M. Prabhakaran, A. Sahai, "Founding Cryptography on Oblivious Transfer - Efficiently," *Advances in Cryptology - CRYPTO2008 in Lecture Notes in Comput. Sci.*, vol. 5157, pp. 572–591, 2008.

[14] M. Ito, A. Saito, and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure," *IEEE Global Telecommunications Conference, Globecom '87*, pp. 99–102, 1987.

[15] S. Obana and K. Tsuchida, "Cheating Detectable Secret Sharing Schemes Supporting an Arbitrary Finite Field," *The 9th International Workshop on Security, IWSEC 2014 in Lecture Notes in Comput. Sci.*, vol. 8639, pp. 88–97, 2014.

[16] W. Ogata and T. Araki, "Cheating Detectable Secret Sharing Schemes for Random Bit Strings," *IEICE Transactions*, 96-A(11), pp. 2230–2234, 2013.

[17] A. Shamir, "How to Share a Secret," *Comm. of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[18] A. C. Yao, "Protocols for Secure Computations," *The 23rd Annual Symposium on Foundations of Computer Science, FOCS '82*, pp. 160–164, 1982.

[19] 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.

[20] M. Yoshida and S. Obana, "Flaws in a Verifiably Multiplicative Secret Sharing Scheme from ICITS 2017," *Cryptology ePrint Archive, Report* 2018/083, 2018.

[21] M. Yoshida and S. Obana, "Verifiably Multiplicative Secret Sharing," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 3233–3245, 2019.