LETTER Special Section on Discrete Mathematics and Its Applications

On Weighted-Sum Orthogonal Latin Squares and Secret Sharing*

Koji NUIDA[†,††a)], ***Member and*** **Tomoko ADACHI**[†††], ***Nonmember***

SUMMARY Latin squares are a classical and well-studied topic of discrete mathematics, and recently Takeuti and Adachi (IACR ePrint, 2023) proposed $(2, n)$-threshold secret sharing based on mutually orthogonal Latin squares (MOLS). Hence efficient constructions of as large sets of MOLS as possible are also important from practical viewpoints. In this letter, we determine the maximum number of MOLS among a known class of Latin squares defined by weighted sums. We also mention some known property of Latin squares interpreted via the relation to secret sharing and a connection of Takeuti–Adachi's scheme to Shamir's secret sharing scheme.

key words: *Latin squares, upper bounds, secret sharing*

1. Introduction

A *Latin square* of size $v \times v$ (where $v \geq 2$) is a $v \times v$ square array of integers from 0 to $v - 1$ where each row/column consists of every integer in the range $[0, v-1]$ appearing only once. Latin squares are a classical well-studied topic in discrete mathematics. One of the famous and efficient constructions of Latin squares is one using weighted sums with fixed weights; here we call them *weighted-sum Latin squares*.

Recently, Takeuti and Adachi proposed in their preprint [10] a $(2, n)$-threshold secret sharing scheme based on mutually orthogonal Latin squares (MOLS). Secret sharing [5], [9] is a cryptographic technology to protect distributed data storage against both steals and deletion of data. By their result, efficient constructions of as large sets of MOLS as possible are important from not just theoretical but also practical viewpoints.

Let $M(v)$ and $M^{\mathrm{WS}}(v)$ denote, respectively, the maximum cardinalities of general MOLS and of MOLS consisting of weighted-sum Latin squares only (MOWSLS, in short) of size $v \times v$. A bound $M(v) \leq v - 1$ for MOLS is well-known. On the other hand, for MOWSLS, it is obvious that $M^{\mathrm{WS}}(v) \leq M(v)$, and values of $M^{\mathrm{WS}}(v)$ are evaluated for small v's by computer experiments in [7]. The main result of this letter is the following that fully determines the value of $M^{\mathrm{WS}}(v)$ for any $v \geq 2$ (see Sect. 3.1 for the proof):

Theorem 1. *Let p_0 be the smallest prime factor of $v \geq 2$. Then we have $M^{\mathrm{WS}}(v) = p_0 - 1$.*

Hence, the maximum cardinality $v - 1$ of MOLS is achievable by weighted-sum Latin squares when v is a prime; while considering composite v's instead of prime ones has no advantage in generating large sets of MOWSLS.

We also mention some known properties of Latin squares and secret sharing, in connection to Takeuti–Adachi's secret sharing scheme. First, we mention in Sect. 3.2 that the known bound $M(v) \leq v - 1$ is also deduced by applying a known lower bound for share sizes in secret sharing schemes to Takeuti–Adachi's scheme. Secondly, we point out in Sect. 4 that Takeuti–Adachi's scheme using MOWSLS can be interpreted as a variant of Shamir's (t, n)-threshold secret sharing with $t = 2$ (see Sect. 4.3 for details), and mention that the known protocols for converting shares of two secrets x, x' in Shamir's scheme into shares of $x + x'$ and of xx' [4] is extended to the case of Takeuti–Adachi's scheme. We note that instantiations of Latin squares for the use in Takeuti–Adachi's scheme different from weighted-sum ones are searched by computer experiments in [8]. It is a future research topic to establish similar share conversion protocols based on MOLS not of weighted-sum type.

2. Notations and Definitions

Throughout the letter, v denotes a fixed integer with $v \geq 2$. Let $[i, j] := \{i, i+1, \ldots, j\}$ for integers $i \leq j$. For $a, n \in \mathbb{Z}$ with $n \geq 1$, let $a \bmod n$ denote the remainder of a modulo n, taken from the range $0 \leq a \bmod n \leq n - 1$, which is also regarded as an element of $\mathbb{Z}/n\mathbb{Z}$.

Let $L = (L[x, y])_{x,y}$ be an $v \times v$ array of integers $L[x, y] \in [0, v-1]$, with row index x and column index y running over $[0, v-1]$. We say that L is a *Latin square* (of size $v \times v$) if for each row and each column, the entries of L are all different (or equivalently, every number in $[0, v-1]$ appears at least once).

Definition 2. We say that two Latin squares L_1 and L_2 are *orthogonal*, denoted here by $L_1 \perp L_2$, if the v^2 pairs $(L_1[x, y], L_2[x, y]) \in [0, v-1]^2$ are all different (or equivalently, every pair from $[0, v-1]^2$ appears at least once).

Manuscript received September 12, 2023.
Manuscript revised December 6, 2023.
Manuscript publicized December 19, 2023.

[†] Institute of Mathematics for Industry (IMI), Kyushu University, Fukuoka-shi, 819-0395 Japan.
[††] National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, 135-0064 Japan.
[†††] Department of Computer Science, Shizuoka Institute of Science and Technology, Fukuroi-shi, 437-8555 Japan.

[*] This work was supported by JSPS KAKENHI Grant Numbers JP19H01109 and JP22K11906, Japan. This work was supported by Institute of Mathematics for Industry, Joint Usage/Research Center in Kyushu University (FY2023 Short-term Visiting Researcher "Cryptography using Latin squares" (2023a016)).

a) E-mail: nuida@imi.kyushu-u.ac.jp

DOI: 10.1587/transfun.2023DML0002

The following definition and proposition (which is well-known; proved here for the sake of completeness) are for a famous and efficient construction of Latin squares.

Definition 3. For $a, b \in [0, v-1]$, we define an $v \times v$ array $L^{a,b}$, which we call *weighted-sum array*, by

$$L^{a,b}[x, y] := a \cdot x + b \cdot y \bmod v \text{ for } x, y \in [0, v-1] \ .$$

Proposition 4. *A weighted-sum array $L^{a,b}$ is a Latin square if and only if* $\gcd(a, v) = 1$ *and* $\gcd(b, v) = 1$. *When this is satisfied, we call the $L^{a,b}$* weighted-sum Latin square.

Proof. This follows by observing that for each $c \in \{a, b\}$, the values $c \cdot z \bmod v$ for $z \in [0, v-1]$ are all different if and only if $c \in (\mathbb{Z}/v\mathbb{Z})^\times$, i.e., $\gcd(c, v) = 1$. □

Due to this property, in what follows we focus on the case where $\gcd(a, v) = 1$ and $\gcd(b, v) = 1$.

We also consider the following kind of Latin squares. Here L^{T} denotes the transpose of a Latin square L, i.e., $L^{\mathrm{T}}[x, y] = L[y, x]$. Note that $(L^{a,b})^{\mathrm{T}} = L^{b,a}$.

Definition 5. We say that a Latin square L is *self-transpose-orthogonal* if $L \perp L^{\mathrm{T}}$.

3. On Upper Bounds for Mutually Orthogonal Sets

A sequence of Latin squares $L_1, \dots, L_\ell$ satisfying that $L_i \perp L_j$ for any $i \neq j$ is called *mutually orthogonal Latin squares* (MOLS). We abbreviate *mutually orthogonal weighted-sum Latin squares* (i.e., every L_i is a weighted-sum Latin square) as MOWSLS. We discuss about the maximum values of ℓ for MOLS and MOWSLS, denoted by $M(v)$ and $M^{\mathrm{WS}}(v)$.

3.1 The Case of Weighted-Sum Latin Squares

Let $P = P(v)$ denote the set of all prime factors of v. Then the condition stated in Proposition 4 is equivalent to that $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$ for every $p \in P(v)$.

For a weighted-sum Latin square $L = L^{a,b}$, we define

$$\lambda[p] = \lambda_L[p] = \lambda_{a,b}[p] := \frac{b}{a} \bmod p \in (\mathbb{F}_p)^\times$$

for any $p \in P(v)$, and define

$$\lambda = \lambda_L = \lambda_{a,b} := (\lambda_{a,b}[p])_{p \in P(v)} \ .$$

Note that for any tuple $\eta = (\eta_p)_{p \in P(v)} \in \prod_{p \in P(v)} (\mathbb{F}_p)^\times$, there is a weighted-sum Latin square L with $\lambda_L = \eta$; take an integer $b \in [0, v-1]$ satisfying $\eta_p = b \bmod p$ for every $p \in P(v)$ by using Chinese Remainder Theorem (note that now $\gcd(b, v) = 1$) and set $a := 1$. The following is the key property to prove our main result:

Theorem 6. *For two weighted-sum Latin squares $L_1 = L^{a_1,b_1}$ and $L_2 = L^{a_2,b_2}$, we have $L_1 \perp L_2$ if and only if $\lambda_{L_1}[p] \neq \lambda_{L_2}[p]$ for every $p \in P(v)$.*

Proof. First, we suppose that the latter condition does not hold, i.e., $\lambda_{L_1}[p] = \lambda_{L_2}[p]$ for some $p \in P(v)$, and show that $L_1 \not\perp L_2$. Fix an integer $\eta \in [0, v-1]$ with $\lambda_{L_1}[p] = \lambda_{L_2}[p] = \eta \bmod p$. Then for each $\mu \in \{1, 2\}$, we have

$$\eta \cdot a_\mu \equiv b_\mu \pmod{p} \ ,$$

therefore, by putting $v' := v/p \in \mathbb{Z}$, we have

$$\eta v' \cdot a_\mu \equiv v' \cdot b_\mu \pmod{v} \ .$$

Note that $1 \leq v' \leq v - 1$. Now we have

$$\begin{aligned} L_\mu[0, v'] - L_\mu[\eta v' \bmod v, 0] &\equiv v' \cdot b_\mu - \eta v' \cdot a_\mu \\ &\equiv 0 \pmod{v} \ , \end{aligned}$$

therefore

$$\begin{aligned} &(L_1[0, v'], L_2[0, v']) \\ &= (L_1[\eta v' \bmod v, 0], L_2[\eta v' \bmod v, 0]) \ . \end{aligned}$$

This implies that $L_1 \not\perp L_2$, as desired.

Now the remaining task is to show that the latter condition in the statement is not satisfied if $L_1 \not\perp L_2$. By the assumption, we have $(L_1[x, y], L_2[x, y]) = (L_1[u, w], L_2[u, w])$ for some different pair of indices $(x, y) \neq (u, w)$. Then for each $\mu \in \{1, 2\}$, we have

$$a_\mu \cdot x + b_\mu \cdot y \equiv a_\mu \cdot u + b_\mu \cdot w \pmod{v} \ .$$

Put $\Delta_a := x - u$ and $\Delta_b := w - y$, which are independent of μ. Then we have

$$a_\mu \cdot \Delta_a \equiv b_\mu \cdot \Delta_b \pmod{v} \ . \tag{1}$$

This and the property $\gcd(a_\mu, v) = \gcd(b_\mu, v) = 1$ imply

$$\begin{aligned} d := \gcd(\Delta_a, v) &= \gcd(a_\mu \cdot \Delta_a, v) \\ &= \gcd(b_\mu \cdot \Delta_b, v) = \gcd(\Delta_b, v) \end{aligned}$$

which is also independent of μ. Put $\Delta'_a := \Delta_a / d \in \mathbb{Z}$ and $\Delta'_b := \Delta_b / d \in \mathbb{Z}$. Then both Δ'_a and Δ'_b are coprime to $v' := v/d$. Now by Eq. (1), we have

$$a_\mu \cdot \Delta'_a \equiv b_\mu \cdot \Delta'_b \pmod{v'} \ ,$$

therefore (by noticing that both Δ'_b and a_μ are invertible modulo v') we have

$$\frac{b_\mu}{a_\mu} \equiv \frac{\Delta'_a}{\Delta'_b} \pmod{v'} \ .$$

The right-hand side is independent of μ, therefore we have

$$\frac{b_1}{a_1} \equiv \frac{b_2}{a_2} \pmod{v'} \ .$$

Moreover, the assumption $(x, y) \neq (u, w)$ implies that at least one of Δ_a and Δ_b is not a multiple of v, therefore we have $d < v$. This implies that $v' > 1$, and by taking any prime factor p of v', we have $p \in P(v)$ and

$$\frac{b_1}{a_1} \equiv \frac{b_2}{a_2} \pmod{p} \ ,$$

i.e., $\lambda_{L_1}[p] = \lambda_{L_2}[p]$. Hence the latter condition in the statement does not hold, as desired. □

By Theorem 6, members of any MOWSLS must have different values of $\lambda[p_0] \in (\mathbb{F}_{p_0})^\times$ where $p_0 := \min P(v)$, therefore $M^{\mathrm{WS}}(v) \le |(\mathbb{F}_{p_0})^\times| = p_0 - 1$; while $L^{1,b}$ for $b \in [1, p_0 - 1]$ form MOWSLS with cardinality $p_0 - 1$. This proves Theorem 1 in the introduction.

Theorem 6 also yields the following corollary:

Corollary 7. *Let $L = L^{a,b}$ be a weighted-sum Latin square. Then all the following conditions are equivalent:*

1. *L is self-transpose-orthogonal.*
2. *$\lambda_L[p] \ne \pm 1$ in $\mathbb{F}_p$ for every $p \in P(v)$.*
3. *$\gcd(a+b, v) = 1$ and $\gcd(a-b, v) = 1$.*

Proof. By Theorem 6, we have $L^{a,b} \perp L^{b,a}$ if and only if $\lambda_L[p] \ne \lambda_L[p]^{-1}$, i.e., $\lambda_L[p] \ne \pm 1$ in $\mathbb{F}_p$, for every $p \in P(v)$. This is also equivalent to that $b^2 \not\equiv a^2 \pmod{p}$, i.e., $a^2 - b^2 = (a+b)(a-b) \not\equiv 0 \pmod{p}$, for every $p \in P(v)$. The last condition means that $\gcd(a \pm b, p) = 1$ for every $p \in P(v)$, which is equivalent to $\gcd(a \pm b, v) = 1$. □

By this result, when we restrict MOWSLS further to self-transpose-orthogonal ones, two values ±1 are excluded from the values of $\lambda[p]$, therefore the maximum cardinality decreases to $p_0 - 3$ (such a set does not exist when $p_0 \le 3$).

3.2 The General Case

Takeuti and Adachi [10] proposed the following construction of a (perfectly secure) (t,n)-threshold secret sharing ((t,n)-SS, in short) scheme with parameter $t = 2$, which uses $n-1$ MOLS $L_1, \ldots, L_{n-1}$ of size $v \times v$ as public parameters:

Share Generation Given a secret $x \in [0, v-1]$ to be shared, the algorithm chooses $y \in [0, v-1]$ uniformly at random, and computes $z_i := L_i[x,y]$ for each $i \in [1, n-1]$. Then z_i is the share of x for party P_i, and y is the share of x for party P_n.

Secret Reconstruction When a pair of shares z_i and y from parties P_i ($i \ne n$) and P_n is given, the algorithm outputs the unique index x' with $L_i[x', y] = z_i$. When a pair of shares z_i and z_j from parties P_i and P_j ($i, j \ne n$) is given, the algorithm determines the unique pair of indices (x', y') with $(L_i[x', y'], L_j[x', y']) = (z_i, z_j)$ and outputs x'.

On the other hand, the following lower bound for the size of share spaces of (t,n)-SS schemes is known (it is known as an unpublished work by J. Kilian and N. Nisan, 1990; see e.g., the fourth paragraph of Sect. 1.2.3 of [3]):

Proposition 8. *For $i \in [1,n]$, let $\mathcal{S}_i$ be the set of possible shares for i-th party in a (t,n)-SS scheme with $2 \le t \le n-1$. Then $\sum_{i=1}^{n} \log_2 |\mathcal{S}_i| / n \ge \log_2(n - t + 2)$.*

By applying Proposition 8 to Takeuti–Adachi's $(2,n)$-SS scheme where $\mathcal{S}_i = [0, v-1]$, it follows that $\log_2 v \ge \log_2 n$, i.e., $v \ge n$. Then, any MOLS of cardinality $M(v)$ gives a $(2,n)$-SS scheme with $n = M(v) + 1$ and therefore satisfies that $M(v) + 1 \le v$. This yields a known upper bound $M(v) \le v - 1$ mentioned in the introduction.

4. Relation to Secure Multiparty Computation

In the research area of secure multiparty computation (MPC) in cryptography, several methods of computing shares of the addition/multiplication of two secrets from given shares of each secret in various secret sharing schemes have been proposed in the literature, e.g., [1], [2], [4]. Here we describe such a method for Takeuti–Adachi's $(2,n)$-SS scheme in Sect. 3.2 with $n \ge 3$ when using MOWSLS where v is a prime and the set $[0, v-1]$ is identified with $\mathbb{F}_v = \mathbb{Z}/v\mathbb{Z}$. Then we explain a relation to Shamir's secret sharing [9].

Let $(z_1, \ldots, z_{n-1}, y)$ and $(z'_1, \ldots, z'_{n-1}, y')$ be tuples of shares of secrets x and x', respectively.

4.1 Computing the Addition

By the construction of shares, we have

$$z_i = a_i \cdot x + b_i \cdot y \text{ and } z'_i = a_i \cdot x' + b_i \cdot y' \tag{2}$$

for each $i \in [1, n-1]$ (where the equalities are considered in $\mathbb{F}_v$). Therefore we have

$$z_i + z'_i = a_i \cdot (x + x') + b_i \cdot (y + y') \ .$$

This means that $(z_1 + z'_1, \ldots, z_{n-1} + z'_{n-1}, y + y')$, which can be obtained by local addition of each party's shares, forms a tuple of shares for secret $x + x'$.

4.2 Computing the Multiplication

First, for any $i \in [1, n-1]$, from Eq. (2), we have

$$z_i z'_i = {a_i}^2 \cdot xx' + a_i b_i \cdot (xy' + x'y) + {b_i}^2 \cdot yy' \ . \tag{3}$$

Note that the same relation also holds for $i = n$ when we put $z_n := y$, $z'_n := y'$, $a_n := 0$, and $b_n := 1$.

Lemma 9. *In the setting above, for any three distinct indices $i, j, k \in \{1, \ldots, n\}$, we have*

$$\begin{pmatrix} {a_i}^2 & {a_j}^2 & {a_k}^2 \\ a_i b_i & a_j b_j & a_k b_k \\ {b_i}^2 & {b_j}^2 & {b_k}^2 \end{pmatrix} \begin{pmatrix} C_{i;j,k} \\ C_{j;k,i} \\ C_{k;i,j} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \ , \tag{4}$$

where, for distinct indices $\alpha, \beta, \gamma \in [1, n]$,

$$C_{\alpha;\beta,\gamma} := \frac{b_\beta b_\gamma}{(a_\alpha b_\beta - a_\beta b_\alpha)(a_\alpha b_\gamma - a_\gamma b_\alpha)} \in \mathbb{F}_v \ . \tag{5}$$

Proof. Let A denote the 3×3 matrix in Eq. (4). By dividing each column of A by ${b_i}^2$, ${b_j}^2$, and ${b_k}^2$, respectively, we obtain a Vandermonde-type matrix

$$\begin{pmatrix} (a_i/b_i)^2 & (a_j/b_j)^2 & (a_k/b_k)^2 \\ a_i/b_i & a_j/b_j & a_k/b_k \\ 1 & 1 & 1 \end{pmatrix} \ .$$

Therefore we have

$$\frac{\det(A)}{{b_i}^2{b_j}^2{b_k}^2} = \left(\frac{a_i}{b_i} - \frac{a_j}{b_j}\right)\left(\frac{a_i}{b_i} - \frac{a_k}{b_k}\right)\left(\frac{a_j}{b_j} - \frac{a_k}{b_k}\right)$$

which is non-zero by the orthogonality of Latin squares and Theorem 6. Hence

$$\det(A) = (a_i b_j - a_j b_i)(a_i b_k - a_k b_i)(a_j b_k - a_k b_j) \ .$$

Now Cramer's rule to solve the system of linear equations (4) yields the values of $C_{i;j,k}$, $C_{j;k,i}$, and $C_{k;i,j}$ as follows:

$$\begin{aligned}
C_{i;j,k} &= \det(A)^{-1} \det \begin{pmatrix} a_j b_j & a_k b_k \\ {b_j}^2 & {b_k}^2 \end{pmatrix} \\
&= \det(A)^{-1} b_j b_k (a_j b_k - a_k b_j) \ , \\
C_{j;k,i} &= -\det(A)^{-1} \det \begin{pmatrix} a_i b_i & a_k b_k \\ {b_i}^2 & {b_k}^2 \end{pmatrix} \\
&= -\det(A)^{-1} b_k b_i (a_i b_k - a_k b_i) \ , \\
C_{k;i,j} &= \det(A)^{-1} \det \begin{pmatrix} a_i b_i & a_j b_j \\ {b_i}^2 & {b_j}^2 \end{pmatrix} \\
&= \det(A)^{-1} b_i b_j (a_i b_j - a_j b_i) \ .
\end{aligned}$$

They are equal to the values as in Eq. (5). □

Now we obtain the following protocol for multiplication of shared secrets, where $i_0, i_1, i_2 \in [1, n]$ are any three distinct and publicly known indices:

1. For each $\mu \in \{0, 1, 2\}$, party P_{i_μ} sets $(\alpha, \beta, \gamma) := (i_\mu, i_{\mu+1 \bmod 3}, i_{\mu+2 \bmod 3})$, and computes
$$X_\mu := \begin{cases} C_{\alpha;\beta,\gamma} \cdot z_{i_\mu} z'_{i_\mu} & \text{if } i_\mu \neq n \ , \\ C_{\alpha;\beta,\gamma} \cdot y y' & \text{if } i_\mu = n \ , \end{cases}$$
where the coefficient $C_{\alpha;\beta,\gamma}$ is as defined in Lemma 9 (with $a_n := 0$ and $b_n := 1$). Then P_{i_μ} generates shares $Z_1^{\langle \mu \rangle}, \dots, Z_{n-1}^{\langle \mu \rangle}, Y^{\langle \mu \rangle}$ of X_μ (by the same $(2, n)$-SS scheme), and sends $Z_\ell^{\langle \mu \rangle}$ to party P_k for $k \in [1, n-1]$ and $Y^{\langle \mu \rangle}$ to party P_n.
2. Each party generates a new share by adding the three shares received in the previous step.

By Eq. (3) and the additive property of the shares explained in Sect. 4.1, the new share generated by the protocol is (by putting $z_n := y$ and $z'_n := y'$ as above) a share of

$$\begin{aligned}
& X_0 + X_1 + X_2 \\
&= \begin{pmatrix} xx' & xy' + x'y & yy' \end{pmatrix} \begin{pmatrix} {a_{i_0}}^2 & {a_{i_1}}^2 & {a_{i_2}}^2 \\ a_{i_0} b_{i_0} & a_{i_1} b_{i_1} & a_{i_2} b_{i_2} \\ {b_{i_0}}^2 & {b_{i_1}}^2 & {b_{i_2}}^2 \end{pmatrix} \begin{pmatrix} C_{i_0;i_1,i_2} \\ C_{i_1;i_2,i_0} \\ C_{i_2;i_0,i_1} \end{pmatrix} \\
&= \begin{pmatrix} xx' & xy' + x'y & yy' \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = xx'
\end{aligned}$$

as desired, where we used Lemma 9 at the second equality.

4.3 Relation to Shamir's Secret Sharing

In the case where $a_1 = \cdots = a_{n-1} = 1$, given a secret x and party P_n's share y of x, we consider a polynomial $f(T) := yT + x \in \mathbb{F}_v[T]$ of degree at most one. Then the share z_i of x for party P_i ($i \neq n$) is given by

$$z_i = a_i \cdot x + b_i \cdot y = y \cdot b_i + x = f(b_i) \ ,$$

and the share for party P_n is the coefficient y of $f(T)$ at the highest degree, while the secret is $x = f(0)$. This is the same situation as "the point at infinity" variant of Shamir's $(2, n)$-SS scheme described in Sect. 11.7 of [6]. On the other hand, for general $a_1, \dots, a_{n-1}$, by taking homogenization $f(T_1, T_0) = yT_1 + xT_0$ of $f(T)$, P_i's share z_i ($i \neq n$) is equal to $a_i \cdot x + b_i \cdot y = f(b_i, a_i)$ (corresponding to a non-infinity point $[b_i : a_i]$ in the projective line $\mathbb{P}_1(\mathbb{F}_v)$), and P_n's share y is also equal to $F(1, 0)$ (corresponding to the point at infinity $[1 : 0] \in \mathbb{P}_1(\mathbb{F}_v)$). Hence Takeuti–Adachi's $(2, n)$-SS scheme using MOWSLS and the protocols in Sects. 4.1 and 4.2 can be seen as a "homogeneous version" of Shamir's scheme and the corresponding MPC protocols [4].

Acknowledgements

The authors thank Reo Eriguchi for his information on Proposition 8 and on the variant of Shamir's scheme in [6].

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," Proc. ACM CCS 2016, pp.805–817, 2016.

[2] D. Beaver, "Efficient multiparty protocols using circuit randomization," Proc. CRYPTO 1991, pp.420–432, 1991.

[3] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. thesis, Technion - Israel Institute of Technology, 1996.

[4] M. Ben-Or, S. Goldwasser, A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," Proc. ACM STOC 1988, pp.1–10, 1988.

[5] G.R. Blakley, "Safeguarding cryptographic keys," Proc. 1979 International Workshop on Managing Requirements Knowledge (MARK 1979), pp.313–318, 1979.

[6] R. Cramer, I.B. Damgård, J.B. Nielsen, Secure Multiparty Computation and Secret Sharing, Cambridge University Press, 2015.

[7] K. Nakamura, S. Nishikawa, T. Adachi, "Mutually orthogonal Latin squares and computational complexity of the secret sharing scheme," IEICE Technical Report, IT2023-26, 2023 (in Japanese).

[8] K. Nakamura, S. Nishikawa, T. Adachi, "Search of Latin square for secret sharing scheme," Proc. FIT 2023, IEICE/IPSJ, no.4, pp.159–160, 2023 (in Japanese).

[9] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, pp.612–613, 1979.

[10] I. Takeuti and T. Adachi, "Secret sharing scheme with perfect concealment," IACR Cryptology ePrint Archive, report 2023/333, 2023. https://eprint.iacr.org/2023/333