Classical Construction of Latin Squares and Their Application to Modern Cryptography

Tomoko Adachi
Shizuoka Institute of Science and Technology

E-mail: adachi.tomoko@sist.ac.jp

1 Introduction

Let q be an integer and $q \geq 2$. A Latin square of order q is an $q \times q$ array in which q distinct symbols are arranged so that each symbol occurs in each row and column.

The reader knows the definition of a group. Latin squares are familiar as groups, but sets that are not groups can also be Latin squares.

In this paper, firstly, we summarize algebraic properties and group-like structure of Latin squares etc. Secondly, we introduce classical construction of Latin Squares, and discribe recent results on the properties of Latin squares generated from this method. Thirdly, we reseach the application of Latin squers to modern cryptography.

2 Group-like structure

A Latin square is equivalent to a quasigroup with a binary operator. That is, there exists a bijection between the set of all quasigroups of order q with binary operators and the set of all Latin squares with a size of $q \times q$. In this section, we describe about group-like structure of Latin square etc.

Let Ω be a finete set of order q. Let $*$ be a binary operator in Ω. We deal with a set $(\Omega, *)$.

Definition 2.1 (Totality)**.** If there exsits unique $c \in \Omega$ such that $a*b = c$ for any $a, b \in \Omega$, then the set $(\Omega, *)$ is said to be totality.

A set $(\Omega, *)$ satisfying totality is called groupoid. To do this, first, we need to define whether operation about $*$ are closed in a set Ω.

Definition 2.2 (Divisibility)**.** For any $a, b \in \Omega$, if there exsits unique $x \in \Omega$ such that $a * x = b$ and exsits unique $y \in \Omega$ such that $y * a = b$, then the set $(\Omega, *)$ is said to be divisibility.

A groupoind satisfying divisibility is called quasigroup.

Definition 2.3 (Identity)**.** For any $a \in \Omega$, if there exsits $e \in \Omega$ such that $a * e = e * a = a$, then the element e is said to be identity element, and the set $(\Omega, *)$ is said to have an identity element.

A quasigroup with an identity element is called a loop.

Definition 2.4 (Associativity)**.** If the equation $(a * b) * c = a * (b * c)$ holds for any $a, b, c \in \Omega$, that is, the associative low of $*$ holds in Ω, then the set $(\Omega, *)$ is said to be assobiativity.

A loop satisfying assobiativity is a group. As readers know, A set Ω that is closed under operation of $*$ is a semigroup if it satisfies the associative low. If a semigroup has an identity element, it becomes a monoid. A monoid becomes a group, if any element has an inverse. These are summarised in the following table 1:

Table 1: The summry of group-like structure

	Totality	Divisibility	Identity	Asoociativity
Groupoid	✓	-	-	-
Quasigroup	✓	✓	-	-
Loop	✓	✓	✓	-
Group	✓	✓	✓	✓
Monoid	✓	-	✓	✓
Semigroup	✓	-	-	✓

A Latin square is said to be reduced if, in its first row and column, the symbols occur in natural order. For example, the following Latin square L is reduced.

For example, let $\Omega = \{1, 2, 3, 4, 5\}$. If we consider a Latin square L as an multiplication table for a set $(\Omega, *)$, we get table 2. A multiplication table such as table 2 obtainedfrom Latin square L is called to be a bordered Latin square.

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix}$$

Table 2: Multiplication table (bordered Latin square)

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	4	5	1	2
4	4	5	1	2	3
5	5	1	2	3	4

The following theorems are known, and these are summarised in the table 3:

Theorem 2.5. ([11]) Evey multiplication table of a quasigroup is a Latin square and conversely, any bordered Latin square is the multiplication table of a quasigroup.

Theorem 2.6. ([11]) Every multiplication table of a loop is a reduced Latin square and conversely,, any bordered a reduced Latin square is the multiplication table of a loop.

Table 3: The correspondence of set and Multiplication table

Set	Multiplication table
Quasigroup	Latin square
Loop	Reduced Latin square

3 Classical construction and their property

Much research has been done on the construction and properties of Latin squares. In this section. we introduce a long-known method for constructing Latin squares and present recent results on the properties of

Latin squares constructed from this method. We suggest that readers who wish to learn more about Latin squares refer to [11, 12, 16].

We define the following $qtimesq$ suare $L(a,b)$ for integers $a, b (a \neq b)$. Each entry of this square is calculated as a congruence modulo q.

$$L(a,b) = \begin{bmatrix} 0 & a & 2a & \cdots & (q-1)a \\ b & b+a & b+2a & \cdots & b+(q-1)a \\ 2b & 2b+a & 2b+2a & \cdots & 2b+(q-1)a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (q-1)b & (q-1)b+a & (q-1)b+2a & \cdots & (q-1)b+(q-1)a \end{bmatrix},$$

When $a, b, a+b, a-b$ are all relatively prime to q, $L(a,b)$ is a diagonal Latin square of order q. Here, a diagonal Latin square is meant a Latin square in which both diagonals contain distinct elements. This construction of Latin square is introduced in the proof of theorem 3.1

Theorem 3.1. ([12]) If q is odd and not a multiple of 3, then there is a diagonal Latin square of order q.

Let L_1 and L_2 be Latin squares of the same order, We say that L_1 and L_2 are orthogonal if, when superimposed, each of the possible q^2 ordered pairs occurs exactly once. Moreover, We say that a set $\{L_1, L_2, \cdots, L_t\}$ of $t \geq 2$ Latin squares of order q is orthogonal if any two distinct squares are orthogonal, that is if L_i is orthogonal to L_j whenver $i \neq j$. Such a set of orthogonal squares is said to be a set of mutually orthogonal Latin squares (MOLS).

For example, let $L_1 = L(1,2), L_2 = L(1,3), L_3 = L(2,1) = {}^tL_1, L_4 = L(3,1) = {}^tL_2$, where ${}^tL$ is the transpose of L. Then, the set $\{L_1, L_2, L_3, L_4\}$ is MOLS.

$$L_1 = L(1,2) = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 0 \\ 4 & 5 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 1 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}, L_2 = L(1,3) = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 1 \\ 4 & 5 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 0 \end{bmatrix},$$

For constructing mutually orthogonal Latin hyper cubes in higher dimensions, there are [9, 13].

Nuida and Adachi [14] called $L(a,b)$ a weighted-sum square, and investigated the properties of weighted-sum orthogonal Latin squares. We will describe their application to cryptograhy in the next section

4 Application to cryptography

A secret sharing scheme is one of the methods in cryptography, was independently proposed by Blakley and Shamir in 1979 [5, 15]. The most famous secret sharing scheme is a (t,w)-threshold scheme which was proposed by Shamir [15] in 1979. It is a method of sharing a secret value K among a finite set $\mathcal{P} = \{P_1, P_2, \cdots, P_w\}$ of w participants in such a way that any t participants can reconstruct K but no group of $t-1$ or fewer participants can reconstruct K. Each piece of information of K distributed to each participant is called *share* or a *shadow*.

Secret sharing schemes using Latin squares are Cooper's scheme [6] and Stones' scheme [17] and so on. [6, 1] is not a (t,w)-threshold scheme, but [17] is a (t,t)-threshold scheme. An extension concept of MOLS is an orthogonal array, and [8] is a (t,w)-threshold scheme using an orthogonal array. For an orthogonal array, we refer to [10].

Recently, Takeuti and Adachi proposed in their preprint [20] a $(2,w)$-threshold secret sharing scheme, which have made [8] easier to use by forcusing it for Latin squares. Nuida and Adachi [14] have taken a different approach to proving secret computation in [20] by using the features of $L(a,b)$ in previous section. This is the same situation as the point at infinity variant of $(2,w)$-threshold scheme of [15], which is described in section 11.7 of [7]

We suggest readers who wish to learn more about cryptography using combinatorial designs refer to [18, 19], and readers who wish to learn more about secure multiparty computation (MPC) in cryptography refer to [2, 3, 4].

References

[1] T. Adachi and X. N. Lu (2018); Magic cubes and secret sharing schemes, *Algebras, Logics, Languages and related areas, Publications of the Research Institute for Mathematical Sciences, Kyoto University,* Vol. 2096, pp. 115–118.

[2] T. Araki, J. Furukawa, Y. Lindell, A. Nof, K. Ohara (2016), “High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority”, in: Proceedings of ACM CCS 2016, pp.805–817.

[3] D. Beaver (1991), “Efficient Multiparty Protocols Using Circuit Randomization”, in: Proceedings of CRYPTO 1991, pp.420–432.

[4] M. Ben-Or, S. Goldwasser, A. Wigderson (1988), “Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation”, in: Proceedings of ACM STOC 1988, pp.1–10.

[5] G. R. Blakley (1979), “Safeguarding Cryptographic Keys”, in: Proceedings of 1979 International Workshop on Managing Requirements Knowledge (MARK 1979), pp.313–318.

[6] J. Cooper, D. Donovan, and J. Seberry (1994); Secret sharing schemes arising from latin squares, *Bull. Inst. Combin. Appl.*, Vol. 12 (1994), pp. 33–43.

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

[8] E. Dawson, E. S. Mahmoodian and A. Rahilly (1993); Orthogonal arrays and ordered threshold schemes, *Australasian Journal of Combinatorics*, Vol. 8 (1993), pp.27-44.

[9] J.T. Ethier and G.L. Mullen (2012); Strong forms of orthogonality for sets of hypercubes, *Discrete Math* , Vol.312, No.12, pp.2050–2061.

[10] A. S. Hedayat, N. J. A. Sloane and John Stufken (1999); *Orthogonal Arrays : Theory and Applications*, Springer-Verlag, New York, Inc.

[11] D. Keedwell and J. Dénes (2015); *Latin Squares and their applications, (second edition)*, North-Holland publications.

[12] C. F. Laywine and G. L. Mullen (1998); *Discrete Mathematics Using Latin Squares*, John Weiley & Sons, INC.

[13] X. N. Lu and T. Adachi (2020); On Dimensionally Orthogonal Diagonal Hypercubes, *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E103-A, No.10, pp.1211-1217.
DOI: 10.1587/transfun.2019DMP0009

[14] K. Nuida and T. Adachi (2024+); On Weighted-Sum Orthogonal Latin Squares and Secret Sharing, *IEICE TRANSACTIONS on Fundamentals of Electronics, Comunications and Computer Sciences*, in printing. early release on 2023.12.19.
DOI: 10.1587/transfun.2023DML0002

[15] A. Shamir (1979); How to share a secret, *Communications of the ACM*, Vol. 22, pp. 612–613.

[16] V. Shcherbacov (2017); *Elements of Quasigroup Theory and Applications*, Chapman and Hall/CRC.

[17] R. J. Sones, M. Su, X. Liu, G. Wang and S. Lin (2016); A Latin square autotopism secret sharing scheme, *Des. Codes Cryptogr.*, Vol. 80, pp. 635–650.

[18] D. R. Stinson (2005).: *Cryptography: Theory and Practice, Third Edition.* Chapman and Hall/CRC.

[19] D. R. Stinson (2020).: Combinatorial Designs and Cryptography, Revisited *50 Years of Combinatorics, Graph Theory, and Computing*, edited by F. Chung, R. Graham, F. Hoffman, L. Hogben, R. C. Mullin and D. B. West, Chaper 19, pp. 335–357. Chapman and Hall/CRC.

[20] I. Takeuti, T. Adachi, “Secret Sharing Scheme with Perfect Concealment”, IACR Cryptology ePrint Archive, report 2023/333, 2023.