2023年度共同利用研究報告書

2024年02月29日

所属・職名 静岡理工科大学情報学部コンピュータシステム学科・教授
足立 智子

		整理番号	2023a016	
1.研究計画題目	ラテン方陣を用いた暗号理論			
2.新規・継続	新規			
3.種別	女性研究者活躍支援研究			
4.種目	短期研究員			
5.開催方法	対面開催			
6.研究代表者	氏名	足立 智子		
	所属部局名	静岡理工科大学情報学部コンピュータシステム学科	職名	教授
7.研究実施期間	2023年09月04日(月曜日)～2023年09月12日(火曜日)			
8.キーワード	ラテン方陣, 準群, 秘密分散法			
9.参加者人数	5人			

10.本研究で得られた成果の概要

本研究で得られた成果をまとめ、2023年9月下旬に下記論文を投稿したところ、2023年12月に採択された(2023/12/19web早期公開, 印刷中)。

K. Nuida and T. Adachi, On Weighted-Sum Orthogonal Latin Squares and Secret Sharing, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences

IMI 共同利用　報告書
「ラテン方陣を用いた暗号理論」

静岡理工科大学情報学部コンピュータシステム学科
足立智子

1. 概要

v を $v \geq 2$ の整数とする. 位数 v のラテン方陣 (Latin square) とは, 大きさ $v \times v$ の方陣に v 種類のシンボルを入れ, どの縦の列，横の行にもすべてのシンボルがちょうど 1 個ずつ出現するように配置したものである. 二つのラテン方陣を重ね合わせたとき, シンボルの順序対が方陣内ですべて異なるとき, この二つのラテン方陣は直交しているという. 互いに直交するラテン方陣の組を, MOLS(Mutually Orthogonal Latin Squares) と呼ぶ.

暗号理論の中で, 秘密分散法と呼ばれる一つの秘密情報を複数人で管理する仕組みがある. 秘密分散法の中で最も有名なものは, Shamir のしきい値 [7] である. k, n を $k \leq n$ の正整数とする. (k, n) しきい値法とは, n 人の参加者に, シェア (またはシャドウ) と呼ばれる分散情報を配布し, n 人の内, 任意の k 人が集まれば秘密情報の値を計算できるが, $k-1$ 人以下ではどのような参加者の集合からも秘密情報は求められない, という仕組みである. 秘密分散法の秘密計算については, [1, 2, 3] などの研究がある.

ラテン方陣を用いた秘密分散は, Cooper 等 [4], Stones 等 [8], Takeuti and Adachi[9] などがある. Cooper 等の手法はしきい値法ではないが, Stones 等 [8] の手法はラテン方陣の作用素を用いた (n, n) しきい値法であり, Takeuti and Adachi[9] の手法は MOLS を用いた $(2, n)$ しきい値法である.

本共同研究では, あるタイプのラテン方陣に関する MOLS の特徴を調べ, その個数に関する定理を得た. さらに, このラテン方陣の特徴による, 秘密分散法における秘密計算についても言及した. これらの結果は, Nuida and Adachi [6] で発表している.

2. Weighted-Sum Latin Square の特徴と秘密分散法

本稿では, 位数 v(大きさ $v \times v$) の方陣のシンボルは整数のみとし, 法 v で合同として計算する. また, 方陣の一番上の行を第 0 行とし, 方陣の一

番左の列を第 0 列とする.

定義 2.1 整数 a, b を $0 \leq a, b \leq v-1$ とする. 大きさ $v \times v$ の方陣において, 第 x 行第 y 列のシンボルを, $a \cdot x + b \mod v$ とする. このような方陣を位数 v の *Weighted-Sum Square* と呼び, $L_{a,b}$ と表記する.

命題 2.1 *a, v が互いに素かつ b, v が互いに素の場合に, Weighted-Sum Square $L_{a,b}$ はラテン方陣となり, また, その場合に限る. このとき, $L_{a,b}$ を Weighted-Sum Latin Square と呼ぶ.*

方陣 L の行と列を転置したものを L^T と表記する. 定義より $(L_{a,b})^T = L_{b,a}$ がすぐにわかる. ラテン方陣 L が L^T と直交であるとき, L は self-transpose-orthogonal であるという.

v を素因子の集合を $P = P(v)$ と表記する. Weighted-Sum Latin Square $L = L_{a,b}$ に対して, 次を定義する.

$$\lambda[p] = \lambda_L[p] = \lambda_{a,b}[p] := \frac{b}{a} \bmod p \in (\mathbb{F}_p)^\times \text{ for any } p \in P(v) \ ,$$
$$\lambda = \lambda_L = \lambda_{a,b} := (\lambda_{a,b}[p])_{p \in P(v)} \ .$$

定理 2.1 *二つの Weighted-Sum Latin Square $L_1 = L_{a_1,b_1}$, $L_2 = L_{a_2,b_2}$ に対して, L_1 と L_2 が直交する必要十分条件は, 各 $p \in P(v)$ について $\lambda_{L_1}[p] \neq \lambda_{L_2}[p]$ が成り立つことである.*

Weighted-Sum Latin Square のみで構成される MOLS を MOWSLS (Mutually Orthogonal Weighted-Sum Orthogonal Latin Squares) と呼ぶ. 位数 v の MOLS となるようなラテン方陣の個数を $M(v)$, MOWSLS の場合を $M^{WS}(v)$ と表記する. 一般的に $M(v) \leq v-1$ であり, v が素数のとき等号が成立することは知られている. 本共同研究では, MOWSLS について次の結果を得た.

定理 2.2 *$v(\geq 2)$ の最小素因子を p_0 とする. このとき, $M^{WS}(v) = p_0 - 1$ が成り立つ.*

秘密分散法の秘密計算については, [1, 2, 3] などの研究があり, Shamir のしきい値法についてに関しては [5] の結果がある. 本共同研究で得た MOWSLS の特徴により, MOWSLS を用いた秘密分散法における秘密計算に関して, [5] の結果を別視点から捉えることができた.

参考文献

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

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

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

[4] J. Cooper, D. Donovan, and J. Seberry (1994); Secret sharing schemes arising from Latin squares, *Bulletin of the Institute of Combinatorics and its Applications*, Vol. 12, pp. 33–43.

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

[6] K. Nuida and T. Adachi (2023); On Weighted-Sum Orthogonal Latin Squares and Secret Sharing, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, in printed : 2023.12.19. (Web 早期公開) DOI : 10.1587/transfun.2023DML0002

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

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

[9] I. Takeuti and T. Adachi, Secret Sharing Scheme with Parfect Concealment, IACR Cryptology ePrint Archive, report 2023/333,