2025年度共同利用研究報告書

2026年04月21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	2025a044		
1.研究計画題目	Hypercubesを用いた秘密分散法				
2.新規・継続	継続				
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	2025年09月08日(月曜日)～2025年09月11日(木曜日)				
	2026年02月24日(火曜日)～2026年02月27日(金曜日)				
8.キーワード	秘密分散法、Hypercubes				
9.参加者人数	2人				

10.本研究で得られた成果の概要

秘密分散法は, 暗号プロトコルである. ディーラーと呼ばれる管理者が一つの秘密情報を持ち, その秘密情報からシェアと呼ばれる分散情報を作成し, 多数の参加者にシェアを分配し, 条件を満たす参加者がシェアを持ち寄れば秘密情報を復元できる. 秘密情報を復元できる参加者の集合を, アクセス集合と呼ぶ.アクセス集合でない参加者の集合の中で, 秘密情報に関する情報をまったく得ることのできない参加者の集合を, 非アクセス集合という.

(t,w)しきい値法は, 参加者w人のうち, 任意のt人が集まればアクセス集合になり, (t-1)人以下では非アクセス集合になるので,パーフェクトセキュリティとなる. これに対し, アクセス構造秘密分散法は,秘密情報に関する一部の情報が漏洩する.

互いに直交するラテン方陣の組をMOLS (Mutually Orthogonal Latin Squares)と呼ぶ. MOLSから直交配列を作ることができ, (2, n)しきい値法が構成できる. 一昨年度(2023年度)の共同研究では, ある種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, Nuida and Adachi (2024)で発表した.

ラテン方陣をd次元に拡張したものを, Hypercubeと呼ぶ. タイプj (j=1, 2 ..., d-1)のHypercubeを, (d,j)-cubeと表記する. Lu and Adachi(2020) は, MOLSの3次元への拡張として, ある種の互いに直交する位数q=p^2の(3,2)-cubesの組の構成法を与えた. 昨年度(2024年度)の共同研究では, より一般的に位数q=p^hの(k, k-1)-cubesの組の構成法を与えた.

ラテン方陣を用いた秘密分散法に, Cooper等(1994)のアクセス構造秘密分散法がある. 本研究では, この手法にHypercubeを適用し, 漏洩率を定め, 特別な形のHypercubeを用いたアクセス構造秘密分散法での漏洩の特徴について調べた.

暗号プロトコルの安全性の観点から, しきい値法のようにパーフェクトセキュリティとなるものが望ましい.アクセス構造秘密分散法では 秘密情報に関する情報が漏洩してしまうので,その漏洩の性質を利用することが求められる.

IMI 共同利用
「Hypercubes を用いた秘密分散法」
報告書

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

暗号プロトコルの一つに, 秘密分散法がある. 秘密分散法は, 1979 年に, Shamir[11] と Blakley [3] により, 別々に提案された. ディーラーと呼ばれる管理者が一つの秘密情報を持ち, その秘密情報からシェアまたはシャドウと呼ばれる分散情報を作成し, 多数の参加者にシェアを分配し, 条件を満たす参加者がシェアを持ち寄れば秘密情報を復元できる.

秘密情報を復元できる参加者の集合を, アクセス集合と呼ぶ. アクセス集合でない参加者の集合の中で, 秘密情報に関する情報をまったく得ることのできない参加者の集合を, 非アクセス集合という. すなわち, 非アクセス集合では, 秘密情報に関する情報がまったく漏洩しない.

秘密情報を復元する参加者の集まりの条件が, 参加者の人数のみであり, この人数がしきい値になってる秘密分散法を, しきい値法と呼ぶ. w 人の参加者のうち, 任意の t 人が集まればアクセス集合になり, $(t-1)$ 人以下では非アクセス集合になる秘密分散法を, (t, w) しきい値法と呼ぶ. (t, w) しきい値法では, w 人の参加者のうち, 任意の t 人が集まれば秘密情報が復元でき, $(t-1)$ 人以下の集まりでは秘密情報に関する情報がまったく漏洩しないという, パーフェクトセキュリティとなる.

しきい値法ではない一般の秘密分散法は, アクセス構造や一般アクセス構造と呼ばれる. アクセス構造の秘密分散法は, パーフェクトセキュリティではない場合が多く, アクセス集合でもなく, 非アクセス集合でもない, というような参加者の集合が存在する. このような参加者集合では, 秘密情報に関する一部の情報が漏洩する. このようなものとして, ランプ型の秘密分散法がある. ([7], [2]).

ラテン方陣の autotopism の性質を利用して, Sones, et. al (2016) [13] は (w, w) しきい値法を提案した. ラテン方陣ではないが, 強さ t の直交配列からは (t, w) しきい値法が構成できる.([5, 12]).

互いに直交するラテン方陣の組を MOLS (Mutually Orthogonal Latin Squares) と呼ぶ. MOLS から直交配列を作ることができ, $(2, w)$ しきい値

法が構成できる．一昨年度 (2023 年度) の共同研究では, ある種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 [10] で発表している．

ラテン方陣は 2 次元であるが, これを d 次元に拡張したものを, Hypercube と呼ぶ. Hypercube には, タイプと呼ばれる指標がある ([8]). タイプ j $(j = 1, 2..., d-1)$ の d 次元 Hypercube を, (d, j)-cube と表記する．Lu and Adachi(2020) [9] は, MOLS の 3 次元への拡張として, ある種の互いに直交する Hypercubes の組で, 位数 $q = p^2$(素数 p の 2 乗) の (3,2)-cubes の組の構成法を与えた．昨年度 (2024 年度) の共同研究では, より一般的に位数 $q = p^h$(素数 p の h 乗) の $(k, k-1)$-cubes の組の構成法を与えた．

ラテン方陣を用いた秘密分散法には, Cooper et. al. (1994) [4] のアクセス構造秘密分散法がある．足立等 (2024) [1] は, ラテン方陣の秘密情報がどの程度漏洩しているのかを実験的に調べた．本研究では, この手法に Hypercube を適用した場合について, 漏洩率を定め, 特別な形の Hypercube を用いたアクセス構造秘密分散法での漏洩の特徴について調べた.

暗号プロトコルの安全性の観点から, しきい値法のようにパーフェクトセキュリティとなるものが望ましい. アクセス構造秘密分散法では秘密情報に関する情報が漏洩してしまうので, [2] のように, その漏洩の性質を利用することが求められる.

参考文献

[1] 足立智子, 西川峻平, 中村紅葉, ラテン方陣を秘密情報とする部分的漏洩に関する一考察, 信学技報, 123(149), IT2024-7, 31-36, 2024.

[2] Ahmad Akmal Aminuddin, 藤沢, 匡哉, ランプ型秘密分散の部分情報漏洩の性質を利用した低通信量で実現できる安全な情報共有法の検討, コンピュータセキュリティシンポジウム *2025* 論文集, 5G1-4, 1953-1960, 2025-10-20.

[3] G. R. Blakley, Safeguarding cryptographic keys, *AFIPS Conference Proceedings.*, 48 (1979), pp.313-317.

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

[5] E. Dawson, E. S. Mahmoodian, and A. Rahilly, Orthogonal arrays and ordered threshold schemes, *Australian. J. Comb.*, 8(1993), 27-44.

[6] A. S. Hedayat, M. J. A. Sloane and John Stufken, *Orthogonal Arrays: Theory and Applications.*, Springer, 1999

[7] 岩本貢, 山本博資, 一般アクセス構造に対する強い秘密保護特性をもつランプ型秘密分散法, 第 *27* 回情報理論とその応用シンポジウム *(SITA2004)* 予稿集, 2004

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

[9] X. N. Lu and T. Adachi, On Dimensionlly Orthogonal Diagonal Hypercubes, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E103-A, no. 10, pp. 1211–1217, Oct. 2020.

[10] K. Nuida and T. Adachi, On Weighted-Sum Orthogonal Latin Squares and Secret Sharing, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E107-A, no. 9, pp. 1492–1495, Sep. 2024.

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

[12] D. R. Stinson, Combinatorial Designs and Cryptography, Revisited, *50 years of Comb., Graph Theory, and Computing*, Ed. F. Chung et al., CRC Press, 2020, pp. 335-357.

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

Hypercubesを用いた秘密分散法

整理番号	2025a044
種別	女性研究者活躍支援研究-短期研究員
研究計画題目	Hypercubesを用いた秘密分散法
研究代表者	足立 智子（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）
研究実施期間	2025年9月8日(月) ～2025年9月11日(木) 2026年2月24日(火) ～2026年2月27日(金)
研究分野のキーワード	秘密分散法、Hypercubes
目的と期待される成果	暗号の一手法に秘密分散法があり、Shamir(1979)の(k,n)しきい値法が有名である。 Dawson等 (1993)は直交配列を用いた秘密分散法を提案したが、暗号として有用な直交配列を作ることは難しい。互いに直交するラテン方陣の組をMOLS (Mutually Orthogonal Latin Squares)と呼び、直交配列になる。申請者は論文[5]で、暗号として扱いやすい形の特殊なMOLSの特性を調べ、パラメータの上限を与えた。この研究結果は、2023年度IMI共同利用研究(女性研究者活躍支援研究-短期研究員)「ラテン方陣を用いた暗号理論」(2023a016)のサポートを受けたものである。 ラテン方陣(2次元)を高次元にする際の場合分けとして、タイプと呼ばれる指標がある。高次元(k次元)の超立方体は、タイプj(j=1,2,…,k-1)があり、(k,j)-cubeと呼ばれる。論文[3]で、MOLS(2次元)の3次元への拡張として、互いに直交する位数q=p^2(素数pの2乗)の(3,2)-cubeの組の構成法を与えた。申請者は、これをより一般的に、位数q=p^h(素数pのh乗)の(k,k-1)-cubeの組の構成法を与え、2025年3月学会発表(縫田教授と共同研究)し、論文投稿の準備中である。この研究結果は、2024年度IMI共同利用研究(女性研究者活躍支援研究-短期研究員)「直交配列を用いた秘密分散法」(2024a041)のサポートをの助成を受けたものである。 MOLS(2次元)の高次元化として、上ではタイプが等しいラテン超立方体の組を考えたが、本研究では、タイプが異なるラテン超立方体の組を考える。 研究アイデアとして、Rawat等(2018)のMSD符号の構成法を基に、小行列がヴァンデルモンド型になるようなような行列を作る。これをEither(2012)の結果と組み合わせれば、異なるタイプが混在するk次元のラテン超立方体で互いに直交する組が構成できるだろう。この組により構成できる秘密分散法は(3,n)しきい値になり、完全秘匿を持つ。 期待できる成果として、セキュリティ面で安全な秘密分散法が構成できる。
組織委員(研究集会) 参加者(短期共同利用)	足立　智子（静岡理工科大学・教授） 顧　玉杰（九州大学　システム情報科学研究院 情報学部門・准教授）