

2024年度共同利用研究報告書

2025年05月12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	2024a041
1.研究計画題目	直交配列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	2024年09月09日(月曜日)～2024年09月13日(金曜日)	
	2025年03月10日(月曜日)～2025年03月12日(水曜日)	
8.キーワード	ラテン方陣, 直交配列, 秘密分散法	
9.参加者人数	3人	

10.本研究で得られた成果の概要

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. 本研究では, 直交配列を用いた秘密分散法について扱う.

正整数 q に対して, 大きさ $q \times q$ の方陣(正方形)に, q 種類のシンボル(文字や数字)を, どの横の行も縦の列も異なるシンボルになるように配置したものを, 位数 q のラテン方陣という. 互いに直交するラテン方陣の組を MOLS (Mutually Orthogonal Latin Squares) と呼ぶ. 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. 昨年度(2023年度)の共同研究では, 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 で発表している.

ラテン方陣は2次元であるが, これを k 次元にし, 互いに直交する組を考えて直交配列を作ると, (k, n) しきい値法を構成できる. 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 ($j=1, 2, \dots, k-1$) があり, (k, j) -cube と呼ばれる. Lu and Adachi(2020)は, 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. 本研究では, より一般的に位数 $q=p^h$ (素数 p の h 乗) の $(k, k-1)$ -cube の組の構成法を与えた.

報告書は2028年4月に公開予定