2022年度共同利用研究報告書

2022年12月07日

所属・職名 茨城大学理工学研究科・助教

品川 和雅

	整理番号	2022a006

1.研究計画題目	秘密計算方式の最小構成に関する研究			
2.新規・継続	新規			
3.種別	プロジェクト研究			
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	品川 和雅		
	所属 部局名	茨城大学理工学研究科	職名	助教
7.研究実施期間	2022年09月05日(月曜日)～2022年09月16日(金曜日)			
8.キーワード	秘密計算，秘匿同時メッセージ			
9.参加者人数	2人			

10.本研究で得られた成果の概要

秘匿同時通信（PSM）とは、情報理論的安全な秘密計算の一種であり、共有乱数かつ1ラウンド通信という特徴を持つものである。PSMプロトコルの研究において、通信量の上界及び下界を求めることは重要な問題である。一般の関数の場合、通信量の既存の上界は入力長について指数的である一方で、既存の下界は入力長について線形的であり、その指数的なギャップを埋めることは未解決問題である。本研究では、具体的な関数に対して通信量の上界と下界を与えた。下界に関しては、PSMプロトコルを抽象単体複体とみなすことによる組合せ論的手法を提案し、これによって、AND関数、Equality関数、多数決関数、大小比較関数、有限群/環上の積演算に対して、通信量の下界が得られる。特に、3ビットEquality関数、3ビット多数決関数、2ビット入力1ビット出力の任意関数、有限群上の積演算に対しては、最適な通信量のプロトコルを構成/特定できた。本成果は、国内最大級の暗号理論の会議である、暗号と情報セキュリティシンポジウム（SCIS2023）において発表予定である。また、国際学会および英語論文誌への投稿も計画中である。

報告書は 2024 年 4 月に公開予定