2023年度共同利用研究報告書

2023年12月25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	2023a009	
1.研究計画題目	物理的な秘密計算と非物理的な秘密計算の関係性の解明			
2.新規・継続	継続			
3.種別	若手・学生研究			
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	2023年09月19日(火曜日)～2023年09月29日(金曜日)			
8.キーワード	秘密計算、カードベース暗号、秘匿同時通信			
9.参加者人数	2人			

10.本研究で得られた成果の概要

秘密計算とは、複数人のプレイヤがそれぞれ秘密の入力情報を持っているとき、各プレイヤの入力情報自体は他のプレイヤに秘匿しつつ、全員の入力情報についてのある関数の値を計算することのできる暗号技術である。秘密計算は、プライバシー保護データマイニングや秘匿統計処理など多くの応用が知られているため、近年、研究開発が活発に行われている。本研究では、カードベース暗号と秘匿同時通信という二つの秘密計算モデルを対象とする。カードベース暗号とは、物理的なカード組を用いて秘密計算を実現する研究分野である。秘匿同時通信とは、複数のプレイヤと一人のレフリーとの間の秘密計算であり、プレイヤたちがレフリーに一度だけメッセージを送ることにより計算を行うものである。前年度のプロジェクト研究『秘密計算方式の最小構成に関する研究』においては、その部分的な研究成果として、カードベース暗号と秘匿同時通信の非自明な関係性を初めて示した。具体的には、有限時間カードベースプロトコルを秘匿同時通信プロトコルに一般的に変換する手法を提案した。本研究の目的は、カードベース暗号と秘匿同時通信の関係性について、さらなる解明を行うことである。

本研究の主な成果は、「カードベース暗号と語の組合せ論」と「秘匿同時通信プロトコルの通信量下界」である。どちらの成果も情報セキュリティシンポジウム（SCIS2024）において発表予定であり、前者は「カードベース暗号に現れる語の組合せ論」という題目で、後者は「3変数ブール関数に対するPSMプロトコルの通信量の上下界」という題目で発表する。また、前年度の成果に関する英語論文「Explicit Lower Bounds for Communication Complexity of PSM for Concrete Functions」は国際会議INDOCRYPT2023に採録された。

報告書は 2027 年 4 月に公開予定