2024年度共同利用研究報告書

2024年12月26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	2024a015	
1.研究計画題目	秘匿同時通信とカードベース暗号に関する研究			
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	2024年09月24日(火曜日)～2024年10月04日(金曜日)			
8.キーワード	秘密計算、秘匿同時通信、カードベース暗号			
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、複数人の参加者がそれぞれ秘密の入力を持つとき、各参加者の入力自体は他の参加者に隠したまま、全員の入力についてのある関数の値を計算する暗号技術である。本研究のテーマは、秘匿同時通信（PSM）とカードベース暗号である。申請者は、2022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PSMプロトコルの通信量の下界証明手法（埋め込み手法）およびカードプロトコルからPSMプロトコルの変換手法（カード・PSM変換）を提案し、2023年度のプロジェクト研究『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』においてカード・PSM変換の応用として間接ストレージアクセス関数に対する効率的なPSMプロトコルを提案した。本年度の一つ目の研究成果は、一様分解というカードベース暗号と有限群論に関するものである。本年度の二つ目の研究成果は、3変数ブール関数のPSMプロトコルの通信量下界に関するものである。

報告書は 2028 年 4 月に公開予定