2022年度共同利用研究報告書

2022年12月14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。

2022 年度共同利用研究報告書

応募枠	プロジェクト研究-短期研究員
研究計画題目	秘密計算方式の最小構成に関する研究
研究代表者氏名	品川 和雅
所属機関・部署・役職	茨城大学・理工学研究科・助教
研究実施期間	2022 年 9 月 5 日（月）～ 2022 年 9 月 16 日（金）

★目的

秘密計算とは、複数人の参加者がそれぞれ秘密の入力情報を保持していたとき、各自の入力情報自体は他の参加者に隠しつつ、全員の入力情報についてのある関数の値を計算するための暗号技術である。秘密計算は、電子オークション、電子投票、プライバシー保護データマイニングなど多くの応用が知られており、近年活発に研究が行われている分野である。秘密計算プロトコルの計算複雑性の代表的なものとして、通信ラウンド数、通信量、乱数長（乱数使用量）などがある。本研究の目的は、秘密計算プロトコルの構成について、最小のまたは最小に極めて近い計算複雑性を達成することである。ただし、それぞれの計算複雑性にはトレードオフの関係があるため、最小化する計算複雑性を固定する必要がある。そこで、通信ラウンド数を 1 ラウンドに制限した秘密計算プロトコル（秘匿同時通信）に注目する。秘匿同時通信は、共有乱数を用いることにより、通信ラウンド数 1 回（最小値）を達成するものであり、任意の関数を秘密計算できることが知られている。通信量（または乱数長）最小の秘匿同時通信プロトコルを構成できれば、それは通信ラウンド数最小の条件の下での、最小通信量（または最小乱数長）の構成を与えたことになる。最小構成を与えるためには、プロトコルの構成と同時に「それよりも小さい構成は実現不可能である」という不可能性を示す必要がある。一般的な実現不可能性を示すことは非常に難しいことが予想されるため、具体的な関数に対する実現不可能性を示す方針をとる。

成果１ 具体的な関数に対する秘匿同時通信プロトコルの通信量の上下界

★研究経過および得られた成果

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。

	構成/下界	条件	通信量	最適性
∘ AND関数 $x_1 \wedge \cdots \wedge x_n$				
Feige-Kilian-Naor (STOC 94)	構成	–	$\lvert M_1\rvert = \cdots = \lvert M_n\rvert = p$（$p > n$ は素数）	?
Data-Prabhakaran-Prabhakaran (CRYPTO 14)	下界	$n = 2$	$\lvert M_1\rvert \geq 3$ かつ $\lvert M_2\rvert \geq 3$	–
本研究	下界	$\lvert M_1\rvert = 3$	$\lvert M_i\rvert \geq 6$（$2 \leq i \leq n$）	–
∘ 3ビットEquality関数				
本研究	構成&下界	–	$\lvert M_1\rvert = \lvert M_2\rvert = \lvert M_3\rvert = 3$	✓
∘ 3ビット多数決関数				
本研究	構成&下界	–	$\lvert M_1\rvert = \lvert M_2\rvert = \lvert M_3\rvert = 4$	✓
∘ 3値大小比較関数				
Feige-Kilian-Naor (STOC 94)	構成	–	$\lvert M_1\rvert = \lvert M_2\rvert = 7$	?
本研究	下界	–	$\lvert M_1\rvert \geq 6$ または $\lvert M_2\rvert \geq 6$	–
∘ 有限群 G 上の積演算 $x_1 x_2 \cdots x_n$				
Feige-Kilian-Naor (STOC 94)	構成	–	$\lvert M_1\rvert = \cdots = \lvert M_n\rvert = \lvert G\rvert$	✓
本研究	下界	–	$\lvert M_i\rvert \geq \lvert G\rvert$	–
∘ 有限環 S 上の乗算 $x_1 \cdot x_2$				
本研究	構成	–	$\lvert M_1\rvert = \cdots = \lvert M_n\rvert = \lvert S\rvert^2$	?
本研究	下界	$S = \mathbb{Z}_m$	$\lvert M_i\rvert \geq \sum_{i=1}^{m} \gcd(i, m)$	–

表1 今回得られた成果と既存研究の比較

★国内/国際学会への投稿計画

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、「具体的な関数に対する秘匿同時通信プロトコルの通信量の上下界」というタイトルで発表予定である。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。（2022年12月7日現在）

成果２ 有限時間カードベースプロトコルから秘匿同時通信プロトコルへの変換

★研究経過および得られた成果

カードベース暗号とは、物理的なカード組を用いて暗号プロトコルを構成する研究分野である。一般に、暗号技術間の帰着関係を明らかにすることは重要な研究課題であるが、カードベースプロトコルを他の暗号技術へ変換するという類の研究はこれまでに全くなされていなかった。本研究では、有限時間カードベースプロトコルから秘匿同時通信プロトコルへの一般的変換を与えた。提案変換手法は、通常の二値カードだけでなく、上下カードや正多角形カードなども扱うことができる。変換先の秘匿同時通信プロトコルは、変換元のプロトコルと同じ関数を計算し、その通信量は(ntlog_2 q)ビットである。ここで、n はプレイヤー数、q はカードのシンボル数、t は変換元のプロトコルにおいて起こり得るターン操作の総数である。また、既存カードベースプロトコルに対する変換の具体例もいくつか与えた。

技術的には、カードベースプロトコルを根付き木として表現し、シャッフル（プロトコルで生じる乱択操作）の乱数を PSM プロトコルの共有乱数とすることにより変換を実現する。例えば、Four-card Trick と呼ばれている有名な AND プロトコルの根付き木は図 1 のように表せる。変換をする際に特に重要なのがターン操作（図 1 の v1, v2, v3）であり、これは一般的に分岐を持つという特徴がある。我々の変換のアイディアは、PSM プロトコルにおいては選ばれなかった方の分岐は乱数値でマスクをすることである。

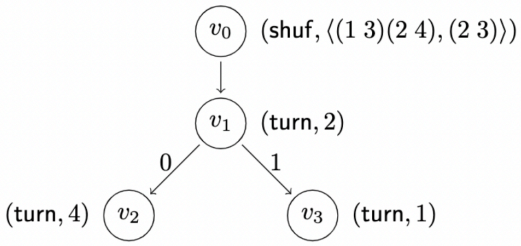

図 1 Four-card Trick の根付き木による表現

★国内/国際学会への投稿計画

本成果の一部はすでに ePrint で公開済みである。(Kazumasa Shinagawa, Koji Nuida, Single-shuffle Full-open Card-based Protocols Imply Private Simultaneous Messages Protocols, ePrint2022/1306, 2022.）また、成果 1 と同様に、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、「有限時間カードベースプロトコルから秘匿同時通信プロトコルへの一般的変換」というタイトルで発表予定である。また、こちらも成果 1 と同様に、国際学会および英語論文誌への投稿も計画中である。(2022 年 12 月 7 日現在)

秘密計算方式の最小構成に関する研究

整理番号	2022a006
種別	プロジェクト研究-短期研究員
研究計画題目	秘密計算方式の最小構成に関する研究
研究代表者	品川 和雅（茨城大学理工学研究科・助教）
研究実施期間	2022年9月5日(月) ～ 2022年9月16日(金)
研究分野のキーワード	秘密計算、秘匿同時通信
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。
組織委員(研究集会) 参加者(短期共同利用)	品川 和雅（茨城大学理工学研究科・助教）

報告書