研　究　報　告　書

「大規模ゲノム情報の安全な統合分析を実現する超高機能暗号」

研究タイプ：通常型
研究期間：　平成26年10月～平成30年3月
研 究 者：　縫田　光司

1．　研究のねらい

現代社会における情報技術や種々の科学技術の発達と普及に伴い、社会的・産業的な各種サービスにおいて「情報」として取り扱われる対象が広範なものとなってきている。そうした情報の中には、人々のプライバシーに関わる事項や個人・企業の知的財産のように、機微情報として慎重な取り扱いを要する種類の情報が含まれる傾向が強まっている。例えば、個人向けの遺伝子診断サービスにおいては、利用者は自身の遺伝子情報という個人特定能力が非常に強い情報を、診断サービスの提供者に渡すこととなる。また、ある病気の治療法を開発するために研究者がその病気の患者の遺伝子情報（これもまたプライバシー要素が極めて高い情報である）を参照する、といった状況も容易に想定される。遺伝子情報以外にも、いわゆるビッグデータ解析の対象として、個人の行動履歴や顔画像などのプライバシー情報を活用してサービスの最適化を図りたいという動向が産業界などで活発になってきている。

その一方で、公的機関や企業からの情報流出事故が後を絶たない。前述のような有益な機微情報の保有者側にとって、こうした情報流出の事例は、自身の持つデータをサービス提供者側に渡すことを躊躇わせる要因となる。そのこと自体は自然な反応と考えられるものの、結果として社会的・産業的に有益なデータの利活用を鈍らせることにもつながっている。

このような状況を、データ保有者とサービス提供者の双方に無理のない形で解決し得る技術として、データの詳細を秘匿した状態のまま必要な統計情報のみを算出する「秘密計算」という技術が知られている。その構成要素の一つに、データを暗号化したままの状態で元々のデータに演算処理を施せる「準同型暗号」という暗号技術がある。しかしながら従来技術は、効率的に動作可能な準同型暗号ではごく初歩的な演算処理しか行えず、逆に高度な演算処理が可能な準同型暗号は極めて低速である、というジレンマを抱えており、遺伝子情報のような大規模かつ高度な機密性が求められるデータへの応用は非現実的な状況である。この状況を打破するため、大規模データへ適用可能な効率性と実用的な演算を可能とする機能性を兼ね備えた安全な秘密計算に寄与する暗号技術を生み出すことが本研究の狙いである。

2．　研究成果

（1）概要

本研究の対象は、秘密計算技術の構成要素である準同型暗号と、それらを用いた秘密計算アルゴリズムに大別できる。本研究成果は多くの論文採録に加え、国外の招待講演や学会等での受賞という形でも高く評価されている（「主な研究成果リスト」その他の成果1～5）。

準同型暗号に関する研究では、暗号化状態のまま任意の演算処理が可能な完全準同型暗号について、従来のビット単位でのデータ暗号化から整数型データの直接的な暗号化への拡張に初めて成功した（「主な研究成果リスト」論文1）。また、既存の完全準同型暗号全てに

共通する効率低下要因である「ブートストラップ」操作を不要とする根本的に新しい構成原理を着想するとともに、従来の暗号分野では殆ど応用されてこなかった組合せ論的群論という数学の分野に現れる対象（非可換群）がその構成原理の実現に有効であることを見出し、安全かつ効率的な完全準同型暗号を実現する上で非可換群に求められる要件を整理した。そして、上記新構成原理の基盤となる組合せ論的群論に関する研究（「主な研究成果リスト」論文5）で得た知見に基づき、安全性に関する要件を満たすと期待される非可換群の具体的候補を選定した。現在、この非可換群を用いたプロトタイプ実装の作業中であり（本研究期間中の公開を目指している）、今後の継続研究で、安全性の詳細な解析および、効率性に関する要件も同時に満たす非可換群の具体的候補の探索を行う予定である。他にも、従来の準同型暗号では誰もが行えた暗号化状態での演算処理について、その実行権限を別途設定可能な方式を実現し、より多様な状況下での利用を可能とした（「主な研究成果リスト」論文4）。

秘密計算アルゴリズムに関しては、生命情報学分野の研究者らと連携して実応用を想定した研究を行った。特に、遺伝子配列などの文字列データベースに対する検索文字列の最長部分一致検索という複雑かつ実用度の高い検索アルゴリズムの効率的な秘密計算化に初めて成功した。本成果は生命情報学分野において学会での受賞やトップ論文誌への採録（「主な研究成果リスト」論文2）など高い評価を受けた。他にも、従来の秘密計算では一般に参加者の入力サイズ（データベースの項目数など）の完全な秘匿が要件に含められていなかったが、本研究では入力サイズをも秘匿できる秘密計算技術の基礎理論を構築し（「主な研究成果リスト」論文3）、より高い安全性を持つ秘密計算技術の実現への端緒を開いた。

（2）詳細

研究テーマ1「完全準同型暗号の効率化および構成原理の抜本的刷新」

秘密計算技術の構成要素の一つである準同型暗号のうち、暗号化状態のまま元データに任意の演算処理を施せる「完全準同型暗号」の効率化に関する研究を行った。完全準同型暗号は 2009 年に最初の具体的構成法が提案されて以降多くの研究が進められてきたが、データをビット単位に分解しての暗号化にしか対応できておらず、整数型のデータを一度に暗号化できる通常の暗号技術と比べて非効率的という問題があった。本研究では、整数型のデータ（より正確には、素数を法とする整数剰余）を一度に暗号化できる完全準同型暗号を初めて構成し、より多様なデータ型の効率的な取り扱いを可能とした。本成果は暗号分野のトップ国際会議の一つ EUROCRYPT（2015 年）に採録された（「主な研究成果リスト」論文1）。

また、前段落の成果を含む既存の完全準同型暗号の構成法では、安全性実現のために暗号文に「ノイズ」と呼ばれる項を付加する必要がある。そして、元データへの演算処理用の操作を暗号文に施すごとにノイズ項が拡大していき、そのまま演算処理を繰り返すと暗号文が壊れて復号が不可能となってしまう。既存の構成法では、暗号文が壊れる前にノイズ項を縮小させる「ブートストラップ」と呼ばれる特殊な操作を行う必要があり、このブートストラップ操作が極めて非効率的という大きな問題を抱えていた。そこで本研究では、この問題を根本的に解決するための、ブートストラップ操作に頼らない全く新しい完全準同型暗号の構成原理の確立を目指して研究を行った。本研究により、従来の構成法とは異なる組合せ論的群論という数学理論に立脚した新たな完全準同型暗号の構成原理を着想し、それに基づく安全で効率

的な完全準同型暗号の具体化に必要となる群構造の要件を整理することができた。

さらに本研究では、上記の構成原理の基盤となる組合せ論的群論の研究も行い(「主な研究成果リスト」論文5)、本研究の遂行に有益な専門的知見を蓄積してきた。その知見を基に、上記の構成原理の要件に合致する具体的な群の候補の探索を行い、安全性の実現に必要と目される要件を満たす群の候補を見出した。本報告書作成時点において、この群を用いた準同型暗号のプロトタイプ実装を作成中である(本研究期間中の公開を目標としている)。ただし、残念ながら現時点での群の候補は効率性の実現に必要と目される要件は満たせていないことから、今後の継続研究では要件の全てを満たす群の探索に取り組む予定である。なお、このように未完成の研究状況であるにもかかわらず、本研究で提唱した新たな構成原理は、これまでに国外での複数の研究集会から講演の招待を受ける(「主な研究成果リスト」その他の成果1, 2)など、当該分野において既に注目されている。

研究テーマ2「秘密計算技術の効率化と多機能化の両立」

秘密計算については、非現実的に大きい計算コストを掛ければあらゆる計算を秘密計算化できることと、足し算のような極めて単純な計算に限定すれば効率的な秘密計算が可能であることが暗号分野において既知であった。本研究では、「計算の種類の多彩さ」と「計算の効率性の高さ」という上記二つの利点を兼ね備えた秘密計算技術の研究を行った。

主な成果として、文字列データベースに対する検索文字列の最長部分一致検索という、従来例よりも複雑かつ実用度の高い検索条件に関して、生命情報学分野の研究者らとの連携により、検索アルゴリズムの効率的な秘密計算化に初めて成功した。より詳しくは、「再帰的紛失通信」と名付けた新しい暗号理論的な手法を考案しそれを用いることで、当該条件での検索手順を足し算操作の組み合わせへと還元する方法を考案し、暗号化状態のまま高速な足し算操作が可能な準同型暗号による実装を行うことで当該アルゴリズムの秘密計算化を行った。さらに、開発したアルゴリズムを遺伝子配列情報に関連する既存のデータセットへ適用して計算機実験を行い、実利用に近い条件下で実用に耐え得る性能の実現を確認した。本成果は生命情報学分野で高く評価され、国内学会発表での受賞(「主な研究成果リスト」その他の成果3)後、生命情報学分野のトップ論文誌 Bioinformatics 誌に採録された(「主な研究成果リスト」論文2)。なお、その後、上記アルゴリズムに更なる効率化を施した改良版アルゴリズムを国内学会にて発表し賞を受けている(「主な研究成果リスト」その他の成果5)。

上記の成果以外にも、化合物データベースに対する類似度検索の効率的な秘密計算化の研究成果も生命情報学分野において発表した(BMC Bioinformatics 誌、2015 年)。これらの成果により、本研究の狙いである効率性と実用的機能性を兼ね備えた秘密計算技術の実現に向けて大きく寄与することができたものと考える。なお、本成果をはじめとする秘密計算技術の研究により所属機関の内部表彰を受けている(「主な研究成果リスト」その他の成果4)。

研究テーマ3「準同型暗号および秘密計算技術の安全性評価と安全性向上」

上記研究テーマ2と関連して、秘密計算技術およびその構成要素技術である準同型暗号の安全性評価と安全性向上に関する研究も行った。主な成果の一つとして、従来の秘密計算技術においては各参加者の入力情報(例えば、データベース保有者のデータベースや検索利用

者の検索文字列など）のサイズ（データベース項目数など）を公開情報として扱わざるを得なかったところ、入力情報のサイズをも秘匿可能な多者間秘密計算に関する基礎理論を提案し（「主な研究成果リスト」論文3）、従来よりもさらに高い安全性を持つ秘密計算技術の実現への端緒を開いた。また、従来の準同型暗号においては、暗号化状態での元データに対する演算処理を誰もが行えるため、本来の意図とは異なる演算処理を攻撃者に実行され得るという潜在的な問題点が存在していたところ、暗号文の復号権限とは別に暗号化状態での演算処理の権限をも管理可能な準同型暗号を実現し、上記の問題点の解消に貢献した（「主な研究成果リスト」論文4）。他にも、ある種の準同型暗号の安全性の根拠となっている暗号学的仮定（素因数分解の計算困難性）に関する安全性検証（国際会議 CT-RSA、2015 年）などの研究成果も得た。これらの研究成果と上記研究テーマ1，2の研究成果の融合による秘密計算技術の安全性のさらなる向上は今後の継続研究における研究課題とする予定である。

3. 今後の展開

本研究内容のうち、完全準同型暗号の新たな構成原理の確立については、残念ながら本研究期間での完全な問題解決には至らなかったものの、部分的な解を与えることはできた。特に、本研究によって見出した暗号分野と数学分野（組合せ論的群論）との新たな関連は、本研究の対象である完全準同型暗号に留まらず、暗号分野全体に新たな潮流を引き起こす可能性を秘めていると考えている。今後の継続研究においては、前述した完全準同型暗号の新たな構成原理の確立を完成させるための研究に加えて、本研究で見出した暗号分野と数学分野の新たな関連の可能性を多角的に開拓するための研究にも注力する予定である。

また、秘密計算アルゴリズムの研究については、本研究で得た知見を活かして既に企業との共同研究へ参画する予定となっている。それに加えて、約1年前に始まった秘密計算アルゴリズムの実用化を主題とした JST CREST 研究プロジェクトの一員にもなっている。このような企業との共同研究や JST CREST 研究プロジェクトなど実応用を見据えた研究プロジェクトに本研究で得た知見を還元することで、本研究成果の社会展開へとつなげていきたいと考えている。

4. 評価

（1）自己評価

（研究者）

完全準同型暗号と数学分野（組合せ論的群論）の新たな関連について、研究構想時点で想像していたよりも多角的かつ深い関連性を見出すことができ、純粋に理論的な面白さと数学の他分野への応用可能性という両方の観点から、今後の暗号分野・数学分野双方の発展の礎として大きな成果を上げられたと考えている。その一方で、プログラミング等の実装分野の経験の浅さなどの要因で、考案した新構成原理のプロトタイプ実装作業が予定よりも遅れていることは否めず、この点は反省材料と考えている。また、効率的かつ高機能な秘密計算アルゴリズムの開発については、暗号分野内での評価に留まらず、より応用の現場に近い生命情報学分野においても複数の受賞やトップ論文誌採録など極めて高い評価を得たことから、研究成果の今後の学術的・実用的な展開について有望な感触を得ている。

（2）研究総括評価（本研究課題について、研究期間中に実施された、年2回の領域会議での評価フィードバックを踏まえつつ、以下の通り、事後評価を行った）。

（研究総括）

「完全準同型暗号」の効率化や構成原理の抜本的刷新を含む新たな暗号技術に対する数理的研究とその成果の実装を目指し，完全準同型暗号における整数型データの取り扱いの実現や文字列の最長部分一致検索アルゴリズムの効率的な秘密計算化などの著しい成果を挙げた．これらの成果に対しては，暗号分野のトップ国際会議・トップジャーナルに採録され，また国内での受賞や海外の国際研究集会からの招待講演など，国内外での評価も高い．

さきがけ研究を通じて，領域内の他の研究者，企業研究者，JST CREST などとの連携が広がった．文字列の最長部分一致検索アルゴリズムの効率的な秘密計算の研究では生命情報分野の研究者と連携し，実用に耐え得る性能を実現して，現場の研究者からの評価を得たことは，本領域の趣旨とよく合致する成果である．

本さきがけ研究は，完全準同型暗号の構成方法の根本的な革新によりその機能の格段の向上を目指す極めて挑戦的な研究計画であり，残念ながらその目標を研究期間内に完全に達成することはできなかったが，上記の優れた成果に加えて，組合せ論的群論を用いるという新たな発想とその予備的な研究も行われ，今後，さらに研究を継続することで，この大きな目標に到達できる可能性を見出したこと，さらには数学と暗号理論の新たな結びつきを開拓したことも評価される．今後は本研究の成果を踏まえてさらに研究を発展させ，これまでの研究成果の実装と共に，近い将来にこの大きな目標が実現されることを強く期待する．

5.　主な研究成果リスト

（1）論文（原著論文）発表

1. Koji Nuida, Kaoru Kurosawa, “(Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces”, in: Proceedings of EUROCRYPT 2015 (Part I) (2015), Springer Lecture Notes in Computer Science vol.9056, pp.537-555
2. Kana Shimizu, Koji Nuida, Gunnar Rätsch, “Efficient Privacy-Preserving String Search and an Application in Genomics”, Bioinformatics (2016) vol.32, no.11, pp.1652-1661
3. Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka, Eiji Okamoto, “Size-Hiding Computation for Multiple Parties”, in: Proceedings of ASIACRYPT 2016 (Part II) (2016), Springer Lecture Notes in Computer Science vol.10032, pp.937-966
4. Keita Emura, Goichiro Hanaoka, Koji Nuida, Go Ohtake, Takahiro Matsuda, Shota Yamada, “Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Cryptosystems”, Designs, Codes and Cryptography, in press
5. Robert B. Howlett, Bernhard Mühlherr, Koji Nuida, “Intrinsic Reflections and Strongly Rigid Coxeter Groups”, Proceedings of the London Mathematical Society, in press

（2）特許出願

研究期間累積件数：0件

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

1. [Invited Talk] Koji Nuida, “A Simple Framework for Noise-Free Construction of Fully Homomorphic Encryption from a Special Class of Non-Commutative Groups”, Conference on Mathematics of Cryptography, University of California, California, USA, September 1, 2015
2. [Invited Talk] Koji Nuida, “Towards Fully Homomorphic Encryption on Finite Simple Groups without Ciphertext Noise”, Colloquium Coding Theory and Cryptography, Brussels, Belgium, November 21, 2016
3.【受賞】生命医薬情報学連合大会 2015 年大会 最優秀口頭発表賞(題目:Efficient Privacy-Preserving Genomic Sequence Search), 清水 佳奈, 縫田 光司, Gunnar Rätsch, 2015 年 10 月 31 日
4.【受賞】平成 27 年度産総研理事長賞(研究)(題目:高機能暗号とデータベースの秘匿検索技術の開発), 花岡 悟一郎, 清水 佳奈, 縫田 光司, 照屋 唯紀, Attrapadung Nuttapong, 松田 隆宏, 浜田 道昭, 津田 宏治, 浅井 潔, 2016 年 4 月 1 日
5.【受賞】第 5 回生命医薬情報学連合大会 研究奨励賞(題目:Secure String Pattern Match Based on Wavelet Matrix), 須藤 弘貴, 神保 元脩, 縫田 光司, 清水 佳奈, 2016 年 10 月 1 日