様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　５　月　３１　日現在

機関番号：　１２６０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2017
課題番号：　２６５４０００３

研究課題名（和文）効率的で有用性の高い準同型暗号の研究

研究課題名（英文）Study on Efficient and useful Homomorphic Encryption

研究代表者
國廣　昇（Kunihiro, Noboru）

東京大学・大学院新領域創成科学研究科・准教授

研究者番号：６０３４５４３６

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：本研究課題では，効率的で有用性の高い準同型暗号の提案，およびその実社会への応用を目指して研究を進めた．まず，準同型暗号を用いた関数評価を行う権限および復号結果を得る権限をデータ提供者がコントロールできる方式の提案を行った．このコントロールを実現するためにはオーバーヘッドが生じるが，実装によるオーバーヘッドがわずかであることを確認した．さらに，準同型演算実行の前処理として検索を行う処理を組み込むことにより，意図しない準同型演算を禁止させることができる方式の提案を行った．さらに，周辺研究として，部分空間メンバーシップ暗号，プライベート情報探索，検索可能暗号の提案も行った．

研究成果の概要（英文）：In this research project, we aimed to propose efficient and useful homomorphic encryption schemes and to apply them to real-world society. We first proposed an outsourced private function evaluation scheme with privacy policy enforcement with the help of homomorphic encryption. This scheme makes the data providers control the eligibility who can conduct the functional evaluation and obtain the decryption results. Implementation results show that the communication and computation overhead introduced by our privacy policy enforcement is very small. We also proposed a mis-operation resistant searchable encryption scheme, which enables the receivers to recognize a mis-operation happens in the evaluation phase. Furthermore, we also proposed subset space membership encryption, private information retrieval and searchable encryption as a sub-research project.

研究分野：　暗号理論

キーワード：　準同型暗号

１．研究開始当初の背景

(1)　研究の社会的背景

情報通信システムの発展とともに，大規模なデータを入手することが可能となっている．さらに，そのデータに潜む埋もれた情報を引き出すこともデータマイニングなどの機械学習理論の進展とともに，可能となっている．その一方で，計算機資源の効率化，コスト削減の要請により，計算を外部に委託することが多い．

大規模なデータ解析を行う際に，手元で保持している計算機で全ての解析が行われる状況では問題は生じないが，アウトソーシングなどにより，外部の専用の計算機群に計算を委託する方が，コスト的に安価であることが多い．しかしながら，その際，最も気をつけるべき事柄は，セキュリティおよびプライバシーである．センシティブな情報を扱う場合には，外部に委託した計算機に対しても情報を漏らすわけにはいかない．ここで，計算を任せたいが，その計算させたい情報自身や計算機結果は漏らしたくないという所に，困難が生じる．その困難に対する解決法として，実用的な環準同型暗号の実現が長年の宿願であった．

データを外部にアウトソーシングする際に重要となるのは，データの秘匿性が適切に守られているか？である．医療情報や個人の嗜好などセンシティブなデータの解析においては，この問題を軽視することができない．

(2) 研究の学術的背景

この問題を解決する手段として，和演算，積演算を暗号化したまま実現可能な環準同型暗号を用いる．既存研究の多くは，安全性を高く確保した上で，計算能力を優先するか？と演算時間を優先するか？のどちらかに過度に比重をおいた研究となっている．計算能力が高く，様々な計算を安全に行うことができるものの，演算時間が多く必要な方式か，逆に，高速に演算できるものの，計算能力が低い方式のどちらかであった．前者では，パラメタを大きく設定する必要があり，現実的な時間での計算が不可能であった．その一方で，後者では，可能な計算能力を抑える必要があった．本研究では，中間のアプローチを取る．どのような計算も可能である「完全」環準同型暗号ではなく，機械学習で用いるようなある程度高度な計算の実現を目的として，現実の問題に即して，計算能力を制限した環準同型暗号を想定し，現実時間で計算が終了する方式の提案を目指す．

現状において，現実的とは言えない環準同型暗号に対して，現実性を高める研究を行う．計算能力を抑えた上で，安全性と効率を両立させる方式の実現を目指す．計算の複雑度をあらかじめ制限し，その制限に特化した上で，現実の問題に適用可能な方式の提案を目指す点が独創的である．現実的なコストで環準同型暗号が実現できれば，その応用先は数多くある．ありとあらゆる機械学習の適用先での様々な複雑な計算を，個々のデータを秘匿したまま計算することが可能となる．

２．研究の目的

主たる研究目的は，効率と有用性を両立させた準同型暗号の開発である．効率性，有用性および安全性は，トレードオフの関係にあり，高いレベルで両立させることは困難である．従来の研究では，安全性を確保した上で，有用性は高いものの，効率的ではない方式，もしくは，その逆の両極端な提案が主であった．この研究課題では，意図的に，有用性を必要十分なレベルに設定することにより，高い安全性を保持したまま，効率を高めた方式の提案を目指す．全く新しい原理に基づく環準同型暗号の提案，もしくは，既存方式の原理に基づくものの，安全性，効率を両立させるパラメタ設定の考案を行う．

さらに，得られた成果を大規模なシステムへの適用につなげることも研究の目的とする．単に暗号方式，暗号プトロコルの提案にとどまらず，実社会への応用を視野においた上で，研究を進める．

３．研究の方法

本研究では，以下の２つのアプローチ

(1) 新しい原理に基づく環準同型暗号方式の探究，
(2) 既存方式の改良でありながらも，積極的に，対象の計算を現実の問題に制限した上で，適切なパラメタ設定を行う，

ことにより，効率を高めた環準同型暗号の開発を進める．研究開始直後は，よりチャレンジングな研究テーマである(1)の研究を行う．既存研究とは異なり，「完全」準同型暗号の実現はあえて狙わず，計算できる能力の上限を抑えることにより，安全で効率的な方式の実現を目指す．引き続き，新方式の提案を目指すとともに，既存方式の改良を積極的に行う．ただ単に，小手先の変更ではなく，網羅的なサーベイ，既存方式の抽象化，具体化を行い，可能な計算クラスを制限することにより，安全性を保持したまま効率を高める方式の開発を行い，徹底的な安全性，効率の評価を行う．

既存の環準同型暗号に関する研究では，安全性および実現する計算能力の高さを保証することに重点が置かれており，演算時間や必要となるメモリなどの実現可能性に関しては，それほど重要視されてこなかった．本研究課題では，行いたい秘匿計算に対して，まず，必要となる計算能力を担保した上で，効率的な環準同型暗号の構成を目指すところが特徴的である．より具体的には，安全性の解析を十分にしつつ，実用的な設定を探索することにより，安全性・効率性を両立させることに特徴がある．

個別の問題が与えられた時に，その問題に

応じて，そのつど，方式を定めることは現実的ではない．そのため，行う秘匿計算の適切な抽象化が必須である．抽象化の指標として，行う計算を論理回路で表現した時の論理ゲートの「深さ」がある．また，行いたい秘匿計算が，何らかの統計量であるならば，そのモーメントが指標となる．m 次のモーメント計算が必要な場合には，m-1 回の積演算で十分である．さらに，エントロピー関数の計算などの場合には，対数関数の計算が必要となる．論理回路では，正確な対数計算を実現することは不可能であるが，希望する近似精度を定めた上で，計算を行うことも可能となる．このように問題に則した適切な計算クラスを設定し，効率を高めることを目指す．

本研究では，可能となる計算能力を抑えることとの引き換えに，高い効率性，ひいては，実現可能性を手に入れることが最も特徴的な点である．従来の研究では，漸近的な性能評価が主流であった．これは，各パラメタの関係をこのように設定すれば（攻撃するには指数関数時間が必要であるという意味で）安全であり，理論上は（鍵生成，暗号化，復号，準同型演算が多項式時間で可能という意味で）効率的であるということを主張していることに対応する．しかしながら，漸近的な議論では，現実の状況を捉えきれておらず，各パラメタの設定に関しては，あまり知見を与えていないのが実情である．

これまでにも，プラバシー保護データマイニングの文脈で，実用に向けた研究が行われている．これらの研究は，主に，和の準同型性しか持たない Paillier 暗号，もしくは，無制限の和と１回までの積ができる BGN 暗号をもとにしている．そのため，計算できる対象が限定されていた．一般的な手法として，その問題を解決するために，計算を依頼する側との通信を行ない，依頼者側が，積に対応する計算をする形にしていることが多い．そのため，オンラインで計算をする必要があり，本来の目的であったコスト削減に寄与しないことが多い．そのため，本研究では，計算の依頼者は，オンラインでの計算に関与せず，全ての計算量的に重い計算は委託された側での計算機で行う方式のみを対象とする．

４．研究成果

(1) 準同型暗号に関する研究

準同型暗号に関して，研究を進め以下の成果を得た．暗号方式，暗号プロトコルの提案にとどまらず，実社会への展開も進めている．

(1-1) 遺伝子情報を用いた個別診断などのセンシティブな情報をもとに行われるサービスにおいて，プライバシーの保護が適切に行われることが重要である．そのため，遺伝子情報や臨床情報は，暗号化されて保持されなくてはならない．その一方で，診断に利用するためには，暗号化されたまま，何らかの関数評価をする必要がある．平成 27 年度は，データフローを適切に管理する手法を提案し，その手法に，準同型暗号を組み込むことにより，極めて安全性の高い関数評価手法の提案に成功した．データフローの管理においては，属性ベース暗号を用いて，評価する権限，復号する権限をデータ提供者が指定することができるという特徴を持つ．これにより，データ提供者が明確に自身のデータの権限をコントールすることが可能となる．評価できる関数としては，内積計算だけでなく，サポートベクターマシンによる分類，カイ二乗検定などが可能である．実際のデータを用い，実用的な時間で計算が終了することを確認している．また，データフローの管理には，オーバーヘッドが生じるが，関数評価部の検査時間と比較すると，そのオーバーヘッドは十分に小さいことを数値実験により確認した．この成果は，IEEE TrustCom2018 で採録されている．さらに，特許を出願し，実社会への展開も視野に入れている．

(1-2) プライバシーを保ったまま，何らかの計算をサーバーに行わせる場合，多くの場合，準同型暗号が用いられる．通常の準同型暗号の場合，準同型計算の入力として，任意の暗号文を取ることが可能である．そのため，意図的に，もしくは不可抗力として，本来の目的とは異なる形での暗号文同士の演算が可能である．平成 28 年度は，本来の目的とは異なる形での準同型計算が不可能な暗号方式の提案を行った．特に Mis-operation resistant searchable homomorphic encryption という概念を提案し，これを実現する暗号プロトコルの提案を行った．検索可能暗号の助けを借りることにより，正しいデータのみを集め，それに対して準同型演算を行うことにより，所望の機能を実現している．実際のデータとして，hidden keyword の独立性に対するカイ二乗検定を行い，現実的な時間で計算が完了することを確認している．この成果は，国内会議 CSS2016 で最優秀論文賞を受賞し，国際会議 AsiaCCS2017 でも発表を行っている．

(1-3)複数のクライアントが独自の鍵で暗号化を行うことができる Multi-Key 性を持ち，ID に基づく完全準同型暗号方式の提案を，平成 29 年度に行った．従来の研究では，部分的な実現しかされておらず，全てを成り立たせた初めての方式である．素朴な準同型暗号方式と比べて極めて高機能な方式であり，有用性が高い．

(1-4)補助情報付きの暗号学的自己双線形写像を導入し，識別不可性難読化を用いた上で，方式の提案を，平成 26 年度に行った．さらに，素因数分解仮定の元で，提案方式が安全であることを示した．提案した自己双線形写像を用いることにより，望ましい性質を持つ

多重線形写像の構成，複数人鍵共有，任意の回路に対する属性ベース暗号の構成などが可能となる．さらに，提案方式と同様のアイデアを用いることにより，準同型暗号の構成も行った．

(2) 準同型暗号の周辺技術（方式提案）に関する研究

準同型暗号を支える周辺技術として，暗号プロトコルの提案も行っている．以下の成果を得た．

(2-1) 部分空間メンバーシップ暗号は，内積述語暗号を拡張したものであり，より豊かな述語を表現することが可能であるという特性を持つ．さらに，Function privacy を持つという望ましい性質を持っている．平成 26 年度は，属性空間が小さい場合には，既存の論文中の主張に誤りがあり，所望の安全性を持たないことを明らかにした．ついで，内積述語暗号から，部分空間メンバーシップ暗号の構成法の一般化を行った．その結果，単純な拡張では，安全な方式を構成することができないことを示した．ついで，内部で用いる内積暗号の条件を緩め ，指数関数的な入力を持つ内積暗号を用いることにより，安全な方式の提案に成功している．

(2-2) 近似 GCD 問題という整数上での完全準同型暗号を構成する際に用いられる困難な問題に基づいて，private information retrieval (PIR)を構成した．実際の構成法は，van Dijk らの整数上での準同型暗号と類似している．平成 27 年度は，オフラインフェーズとして，事前計算を組み込むことにより，必要となるメモリ量は増加するものの，少ない通信量で実行するプロトコルの提案に成功した．この結果は，査読付き国際会議 SAC2015 で発表を行った．

(2-3) 平成 28 年度は，任意の系列に対して検索可能な検索可能暗号方式の提案を行った．従来の方式では，あらかじめ定めたキーワードに対してのみ検索が可能であるが，従来方式を改良することにより，任意の系列に対する検索が可能となっている．その際，従来方式と比較すると，オーバーヘッドが大きくなっており，状況に応じて，利用する方式を切り替えることが重要となる．

(3) 準同型暗号の周辺技術（安全性解析）に関する研究

準同型暗号を支える周辺技術として，暗号プロトコルの安全性解析も行っている．以下の成果を得た．

(3-1) 暗号化データベースにおいて，効率的に二分探索を行うために，順序保存型暗号が使われる．順序を保存する代償として，暗号自身は破られやすくなっている．平成 28 年度から継続的に研究を行い，従来よりも高い割合で，もとの情報の復元に成功する攻撃を提案している．従来の攻撃で用いられていた最適化問題を順序制約付きの問題に変更し，この問題を解く効率的なアルゴリズムを提案することにより実現している．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 9 件）

1. Noboru Kunihiro, Wen-Jie Lu, Takashi Nishide and Jun Sakuma, “Outsourced Private Function Evaluation with Privacy Policy Enforcement,” IEEE TrustCom2018 採録決定
2. Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka and Noboru Kunihiro, “Self-bilinear Map on Unknown Order Groups from Indistinguishability Obfuscation and Its Applications,” Algorithmica, 79 (4), pp.1286-1317,2017.
3. Keita Emura, Takuya Hayashi, Noboru Kunihiro and Jun Sakuma, “Mis-operation Resistant Searchable Homomorphic Encryption,” in Proc. of ASIA CCS'17, pp. 215--229, 2017.
4. Yoshinao Uchide and Noboru Kunihiro, “Searchable symmetric encryption capable of searching for an arbitrary string,” Security and Communication Networks, vol. 9, issue 12, pp. 1726--1736, 2016.

〔学会発表〕（計 13 件）

1. 近藤佑樹，勝又秀一，國廣昇，“標準的仮定に基づく Multi-key ID ベース完全準同型暗号の構成，” 1A1-4，SCIS2018，2018.
2. Sota Onozawa, Noboru Kunihiro, Masayuki Yoshino and Ken Naganuma, “Improving Inference Attacks on Order-Preserving Encrypted Databases,” Poster Presentation of IWSEC2017, 2017.

〔産業財産権〕

○出願状況（計 1 件）

名称：制御装置、統計解析装置、復号装置および送信装置
発明者：佐久間 淳、國廣 昇、津田 宏治、竹内 一郎、山田 芳司
権利者：同上
種類：特許
番号：特願 2016-566025
出願年月日：平成 27 年 11 月 1 日
国内外の別： 国内

６．研究組織

(1)研究代表者

國廣　昇　（KUNIHIRO, Noboru）
東京大学・大学院新領域創成科学研究科・
准教授
研究者番号：60345436