戦略的創造研究推進事業　CREST
研究領域「ビッグデータ統合利活用のための
次世代基盤技術の創出・体系化」
研究課題「ビッグデータ統合利用のための
セキュアなコンテンツ共有・流通基盤の構築」

研究終了報告書

研究期間　2015年10月～2021年3月
（新型コロナウイルス感染症の影響を受け2021年9月まで延長）

研究代表者：山名早人
（学校法人　早稲田大学理工学術院、
教授）

§1 研究実施の概要

(1)実施概要

本研究では、情報漏洩から重要なデータを守るための基盤技術の構築を目指した。従来の「匿名化」や「通信時の暗号化」から脱却し、通信時、計算時、保存時の全ての場面において常に暗号化した状態(完全準同型暗号(FHE)を採用)でデータを扱える基盤を(1)法的検討、(2)暗号面からの高速化、(3)アーキテクチャ面からの高速化、(4)クラウドプラットフォームの構築、(5)実証実験の 5 つ項目で実施した。成果は、広く公開し普及を図るためにオープンソースとして公開(合計 13 本のプログラム(内 2 本をコロナ延長期間中に追加))した。

法的検討においては、流通暗号化データの法的な扱いを明確にするため後藤グループが中心となり、一般財団法人情報法制研究所や他の研究者等と連携し、個人情報保護法における暗号化データの扱いに対し提言を行った。結果、個人情報保護法改正案(2020)では、「仮名加工情報(暗号化を含む)」が新設され、暗号化された情報の流通の前進に貢献した。

暗号化されたコンテンツ共有・流通基盤構築における問題は、FHE では計算が 100 億倍遅くなり実用に耐えないことである。本研究では、HElib(IBM が公開する FHE ライブラリ)からの 1,000 倍の高速化を目標にした。後藤グループによる理論面からの高速化と、山名グループと山口グループによるアーキテクチャ面からの高速化の両面から実現し、理論面から 26 倍、ミドルウェア面から 112 倍、両方を同時利用した場合、約 2,900 倍の高速化を達成した。

理論面からは、新暗号システム FHE4FX/FHE4FL の提案により、従来不可能であった固定・浮動小数点用の準同型暗号を実現した。さらにサブリング準同型暗号方式を提案し、一暗号文中に複数の平文を無駄なく配置することにより HElib 比で 26 倍の高速化を達成した。

コンピュータアーキあテクチャ面からの高速化では、まず、ミドルウェアとしての高速化として、(1)メモリアロケーション最適化による高速化(4.72 倍)、(2)ブートストラップ回数(暗号文中のノイズリダクション処理)削減による高速化(2.67 倍)、(3)ブートストラップ及びリニアライズ最適化問題の解法高速化(30～40%最適化時間短縮)、(4)属性ベース暗号のリボーク処理高速化(3.7 倍)、(5)非対話型秘匿数値比較手法による高速化(2.7 倍)、(6)FHE 演算を対象としたタスクスケジューリング手法(2.75 倍)、(7)FHE 関数の表検索置き換えによる高速化(表の1エントリに対し 3.4μ 秒で実行)、(8)ファイル格納位置制御による高速化(1.2 倍)を行った。これらの内、(1)(2)(5)(6)(8)は同時適用可能であり、併せて 112 倍の高速化となる。また、(7)の適用により、あらゆるFHE関数の固定時間での実行を可能とした。コロナ延長期間中において、(9)準同型 trace 型演算の高速化及び Intel AVX512 命令の適用を行い、未適用時に比較し 2.7 倍の高速化を可能とした。

次に、主要アプリケーションを対象とした高速化では、(1)頻出パターンマイニング高速化(430 倍)、(2)検索高速化(100 倍)、(3)外部委託秘匿共通集合濃度計算(100 データ時 5 分)、(4)外部委託秘匿和集合計算(50 データ×2 拠点時 103 秒)、(5)地理情報(POI)推薦(100POI 時 28 秒)、(6)推論処理(ナイーブベイズ分類器)(4クラス分類時 0.252 秒)、(7)推論処理(CNN 分類器)(CIFAR-10 で 77.55%の精度達成)、(8)電力網における異常検知(10 分間隔での異常検知実現)を行った。

クラウドプラットフォームの構築は、小口グループを中心に山名グループが協力し実証実験を想定したクラウドプラットフォームを構築した。Apriori 方式の秘匿データマイニングでは、マスタ・ワーカー処理での高速化(6.7 倍/8 ワーカ時)、FP-Growth 方式では、クライアント側処理高速化(1.57 倍)を行った。また、クライアントの能力が低い場合に備え、キースイッチングを用い、クライアント側での暗号化時間削減を行った。最後に FHE で多用される FFT 高速化を FFT オフロードエンジンにより実現(6.9 倍)した。

実証実験は、ライフログデータによる実証実験(新谷グループ)と医薬品副作用解析による実証実験(野口グループ)の2つである。コロナ延長期間中において、のべ 1 万 1,120 人日分のライフログデータによる実証実験を行い、暗号化されたデータに対して、秘匿アイテムセットマイニングにより生活パターンが抽出できることを確認した。これは、クラウドから利用者のパーソナル情報を守ることを主眼とした実験である。また、これらのデータのうち公開の承諾が得

られた 30 名の実験参加者の、のべ 4,200 人日分のデータを公開した(http://home.hol.is.uec.ac.jp/shintani/crestdataset/)。医薬品副作用解析による実証実験では、3 薬局グループと協力し実証実験を行った。シミュレーション結果では、99.8%のクエリに対して 60 秒以内での応答を確認し、(薬局では対面での医薬品提供であるため)実用上十分な時間であることを確認し、患者のプライバシーを守ることができる。コロナ延長期間中においては、4 店舗で実証実験を行った。本成果により、本事業終了後も2薬局との間での共同研究と実証実験の継続につなげることができた。

(2)顕著な成果

＜優れた基礎研究としての成果＞
1. サブリング準同型暗号方式の提案
概要:
「セキュアなコンテンツ共有・流通基盤」を実現するためには、完全準同型暗号により暗号化したまま各種アルゴリズムを効率的に実行することが要となる。理論面からの高速化として、新しい暗号方式であるサブリング準同型暗号方式を提案しライブラリとして公開した。従来、一つの暗号文に複数の平文を格納する場合、実際には使われない無駄領域が生じていた。これに対し本提案では、一つの暗号文に平文を無駄なく格納し、暗号化、復号、加算および乗算といった演算処理を一括して並列実行できるようにすることで、HELib 方式に比べ 26 倍の高速化(最も時間を要する除法での比較)を達成した。

2. 完全準同型暗号を高速処理するミドルウェアライブラリの公開
概要:
完全準同型暗号を高速処理する基礎技術として 6 ライブラリの公開を行った。(1)FHE 特有のメモリアクセスを高速化するメモリアロケータ 2 種、(2)任意 FHE 関数の表検索による高速化、(3)FHE 用粗粒度タスクスケジューラ、(4)非対話型秘匿数値比較、(5)ディスクアクセス制御(ブロック制御)による高速化の 6 ライブラリである。FHE の高速化用ミドルウェアとしてのまとまったライブラリ公開は世界でも類をみず、完全準同型暗号の高速化に欠かせないライブラリとなることが期待される。なお、(1)及び(5)は、FHE に限定することなく、同様の特徴を持つ一般アプリケーションに対しても適用可能である。コロナ延長期間中において、さらに 1 ライブラリの公開を行った。公開したライブラリは、(6)Boostrapping 及び Relinearization ソルバーである。

3. 完全準同型暗号によるアプリケーションライブラリの公開
概要:
完全準同型暗号の適用例として 4 ライブラリの公開を行った。(1)FHE による外部委託秘匿共通集合濃度計算、(2)FHE による地理情報(POI)推薦、(3)FHE による推論処理(ナイーブベイズ分類器)、(4)FHE による推論処理(CNN 分類器)の 4 ライブラリである。FHE を様々なアプリケーションに適用するためには、それぞれの分野において定石となる「モデル」が重要であり、こうした主要アプリケーションの実装公開の意義は大きい。また、複数の実装例の公開は、世界でも類をみない。コロナ延長期間中において、さらに 1 ライブラリの公開を行った。公開したライブラリは、(5) プライバシー保護医薬品副作用検索である。

＜科学技術イノベーションに大きく寄与する成果＞
1. 改正個人情報保護法への匿名加工情報の概念導入への貢献
概要:
2017 年施行の改正個人情報保護法では、匿名加工情報という概念が導入されたが、個人の特定を防ぐために情報の多くを消去する必要があった。本研究開発では、「暗号化によって個人情報を保護する」というという考え方を提言として出し、これは一般財団法人情報法制研究

所からの提言その他からの提言とも相まって、個人情報保護法改正案において「暗号化された情報を仮名加工情報として取り扱う」こととなった。これにより、規制が大幅に緩和され、個人情報の利活用促進に貢献した。

2. 表検索を用いた任意の FHE 関数の高速実行
概要:
完全準同型暗号(FHE)では、ビット演算でなければ実現できない関数が多数存在し、これが平文演算に比較しての大きなボトルネックである。これに対し、予め関数への入力と出力の関係を表として持ち、この表に対する検索(実際の入力が予め用意されている入力値に一致しない場合は近傍の値を採用)に置き換えることで、FHE 任意関数を高速実行できる仕組みを構築した。入力として複数の引数をとることができ、1 入力 82 万エントリを持つ表の場合で 3 秒、2 入力 4096×4096 エントリを持つ表の場合は 72 秒(Intel Core i7 8700 利用時)で任意の関数を実行できる。高速化手法として適用範囲が大きい手法であり、FHE での実現が困難な関数の構築が容易となるだけでなく、複雑な関数であるほど高速化が可能となる。

3. 医薬品副作用解析システムの構築
概要:
JAPIC が公開している全副作用情報(公開情報)と薬局から投入される副作用情報(FHE により暗号化済)をもとに、薬局からの暗号化されたクエリ(患者の投薬、副作用情報)に対して、副作用に関連する医薬品を提示するシステムを構築した。コロナ延長期間中においては、4 店舗で実証実験を行い、患者のパーソナル情報を秘匿しつつサービスを行うことができることを確認した。本成果により、本事業終了後も2薬局との間での共同研究と実証実験の継続につなげることができた。

＜代表的な論文＞
1. Seiko Arita, Shota Nakasato, "Fully Homomorphic Encryption For Point Numbers," Proc. of INSCRYPT 2016, Beijing, China, pp.253-270, 2016.
概要:本論文では、固定小数点を実現する初めての完全準同型暗号となる FHE4FX を提案している。FHE4FX は FV 方式(Ring-LWE 格子暗号に基づいた完全準同型暗号)に基づいている。FHE4FX は、2 つの暗号化されたデータの大小関係の判定結果としての 1bit(0 もしくは 1)を復号化することなく計算することを可能としている。さらに、FHE4FX が持つ大小関係の判定を利用することにより、浮動小数点を扱うことができ、これを FHE4FL として提案している。(被引用数 24)

2. Arita S., Handa S., "Subring Homomorphic Encryption," Kim H., Kim DC. (eds) Information Security and Cryptology - ICISC 2017, Lecture Notes in Computer Science, vol. 10779, Springer, pp.112-136, 2017.
概要:準同型暗号の実用化にあたっては、多くの平文を一つの暗号文に格納し、暗号化、復号、加算および乗算といった演算処理を一括して並列実行することが重要である。本論文では、データマイニング等で多用される整数演算を対象として、一括並列処理を無駄なく実行できる独自の準同型暗号方式として、サブリング準同型暗号方式を提案した。これによって、HELib 方式に比べ、2～23 倍の高速化(演算の種類により高速化率は異なる)を達成した。(被引用数 5)

3. Ruixiao Li, Yu Ishimaki, Hayato Yamana, "Privacy Preserving Calculation in Cloud using Fully Homomorphic Encryption with Table Lookup," Proc. of the 5th IEEE International Conference on Big Data Analytics (ICBDA2020), pp.315-322, 2020.
概要:本論文は、完全準同型暗号(FHE)で暗号化された入力をもとに任意の関数を表検索によって実行することにより、任意の FHE 計算を高速化する手法を提案している。関数

の引数の数は任意である。これにより、対数や平方根など、完全準同型暗号での演算が困難（ビット演算に落とした計算は可能が長時間を要する）な場合も、一定時間での出力が可能となる。引数 1 で表サイズ 164 万エントリ時、5.5 秒、引数 2 で表サイズ 6,710 万(各引数 8,192)エントリ時 187 秒で出力ができることを確認した。（被引用数 1）

4. Yu Ishimaki, Hayato Yamana, “Faster Homomorphic Trace-Type Function Evaluation,” IEEE Access, vol. 9, pp. 53061-53077, 2021.　※コロナ延長時の成果

概要：本論文は、準同型暗号（HE）（完全準同型暗号を含む)において標準的に用いられるベクトル要素間での準同型 trace 型演算の高速化を提案した。準同型 trace 型演算では、要素のローテーションと加算が頻繁に用いられる。ローテーションした要素とローテーションしていない要素間での計算においては、key-switching と呼ばれる特殊操作が必要であり計算量が大きい。これを loop-unrolling を用いることで高速化を行い、従来手法よりも 1.32～2.12 倍高速に動作することを示した。（被引用数 0）

§2 研究実施体制

(1)研究チームの体制について

① 山名グループ
・研究代表者:山名早人 (学校法人早稲田大学 理工学術院基幹理工学部情報理工学科、教授)
研究項目
・暗号ライブラリ構築(コンピュータアーキテクチャ面からの高速化)
・クラウドプラットフォーム構築

② 後藤グループ
・主たる共同研究者:後藤厚宏 (学校法人岩崎学園 情報セキュリティ大学院大学情報セキュリティ研究科、教授)
研究項目
・法的検討・ガイドライン策定
・暗号ライブラリ構築(暗号理論面からの高速化)

③ 小口グループ
・主たる共同研究者:小口正人 (国立大学法人お茶の水女子大学 基幹研究院、教授)
研究項目
・クラウドプラットフォーム構築

④ 山口グループ
・主たる共同研究者:山口実靖 (学校法人工学院大学 情報学部情報通信工学科、准教授)
研究項目
・暗号ライブラリ構築(I/O 面からの高速化)

⑤ 新谷グループ
・主たる共同研究者:新谷隆彦 (国立大学法人電気通信大学 大学院情報理工学研究科、准教授)
研究項目
・実証実験(ライフログデータ取得・解析システム構築及びライフログ実証実験)

⑥ 野口グループ
・主たる共同研究者:野口 保 (学校法人明治薬科大学 薬学部薬学教育研究センター数理科学部門、教授)
研究項目
・実証実験(医薬品副作用解析システム構築及び医薬品副作用実証実験)

(2)国内外の研究者や産業界等との連携によるネットワーク形成の状況について

- 海外連携
  - (山名G)米国ミズーリ工科大学 Sajal K. Das教授、米国ヴァンダービルト大学Abhishek Dubey講師、米国西ミシガン大学のShameek Bhattacharjee講師
    秘密計算によるパワーグリッドのスマートメーターデータへの侵入・改ざん防止について協業した。

- （山名G）米国ニュージャージー工科大学　Andrew　Sohn准教授
  各種FHEタスクの委託計算を行うサービスを粗粒度タスクレベルで並列化し高速化処理を行う研究を進めてた。

- （山名G、小口G）米国ニュージャージー工科大学サイバーセキュリティセンター所長　Kurt　Rohloff教授
  連携し、同センターが開発したFHEライブラリであるPALISADE上での本研究成果の展開を進めている。また、Kurt教授を中心に進められている世界的なFHE標準化についても協力を行った。

- （山口G）米国フロリダ大学　Jose　A.B.　Fortes教授
  連携し、ハードディスク上でのデータ配置の最適化手法の高度化を進めた。

- （山口G）米国テキサス　A&M大学　Jian　Tao教授
  シミュレーションプラットフォームSimHubに関する研究での連携を進めた。

- （山名G）米国IBMワトソン研究所　Shai　Halevi氏、Craig　B.　Gentry氏（現：Algorand（アルゴランド）社へ転職）
  2017年1月に訪問し、FHEの高速化、応用先について議論を行い、協力関係にある。ただし、2019年のAlgorand社への転職後は連携ができなかった。2019年、当時のIBMワトソン研究所Cryptographic　Researchチーム内の多くの研究者（ManagerのTal　Rabin氏を含む）がAlgorand社へ転職した。

- （小口 G）米国テンプル大学　Krishna Kant 教授
  2017 年 6 月の日米ワークショップで大規模災害時のネットワークにおけるデータ共有の安定性に関するテーマで連携を始めて以降、2018 年 5 月には東京で開催された Smart Cyberinfrastructure for Transnational Science (CENTRA 3) において Kant 教授が共同研究の成果を報告、また同年 9 月には米国 Philadelphia のテンプル大学を訪問し議論を行うなど共同研究を進めた。

- （山名 G）秘密計算で第一線の研究者が進捗を発表する WAHC での協力関係
  ニュージャージー工科大学、マイクロソフト、IBM 等、FHE ライブラリを公開している拠点を中心に運営されている Workshop on Encrypted Computing & Applied Homomorphic Cryptography において、2017 年～2020 年、プログラム委員として協力を行った。

- （後藤 G、山名 G、小口 G、山口 G、新谷 G、野口 G）マイクロソフトリサーチ　Kim Laine 主管研究員
  シンポジウムを連携して実施し今後の協力関係を構築した。
  ※コロナ延長時の成果

- 国内連携
  - （後藤G）一般財団法人情報法制研究所
    「研究を目的とした個人データの取扱い」について、連携し検討を行った。

  - （後藤G）高木浩光（産業技術総合研究所情報技術研究部門主任研究員）、宍戸常寿（東京大学教授）、鈴木正朝（新潟大学教授）、曽我部真裕（京都大学教授）

法的検討・ガイドライン策定に関して意見交換及び連携を行い、その成果をパブリック・コメント提出等によって随時、公開した。

- （後藤 G）穴田啓晃（長崎県立大学情報システム学部情報セキュリティ学科准教授）
  属性ベースの暗号技術について連携を行っている。その成果を国際論文誌 Theoretical Computer Science, Elsevier に投稿予定である。

- （山名G）奈良先端科学技術大学院大学　安本慶一教授、大阪大学　山口弘純准教授
  秘密計算によるスマートモビリティ各種応用について協業を行った。

- （山名G）田中紀子（東京都健康長寿医療センター　健康データ科学研究室　室長）
  連携し医療データ保全において完全準同型暗号の利用の検討を進めた。

- （野口G）龍生堂薬局（大久保店、多摩センター店、アイランド店）、マロン薬局、日生薬局
  医薬品副作用に関する実証実験において協力を行った。

- （野口G）ハロー薬局、弥生薬局、いろり薬局
  医薬品副作用に関する実証実験について説明を行った。コロナ延長期間中において、ハロー薬局での実証実験を開始した。ただし、残りの2薬局については非常事態宣言に伴う行動制限のため、実証実験の開始に至らなかった。