「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」
平成27年度採択研究代表者

H29 年度
実績報告書

山名　早人

早稲田大学理工学術院
教授

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

§1. 研究実施体制

(1)「山名」グループ
① 研究代表者:山名　早人 （早稲田大学理工学術院基幹理工学部情報理工学科　教授）
② 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
① 主たる共同研究者:後藤　厚宏 （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）
② 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
① 主たる共同研究者:小口　正人 （お茶の水女子大学基幹研究院　教授）
② 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
① 主たる共同研究者:山口　実靖 （工学院大学情報学部情報通信工学科　准教授）
② 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
① 主たる共同研究者:新谷　隆彦 （電気通信大学大学院情報理工学研究科　准教授）
② 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)

(6)「野口」グループ

① 主たる共同研究者:野口　保　(明治薬科大学薬学部薬学教育研究センター　教授)

② 研究項目

・実証実験(医薬品副作用解析システム構築)

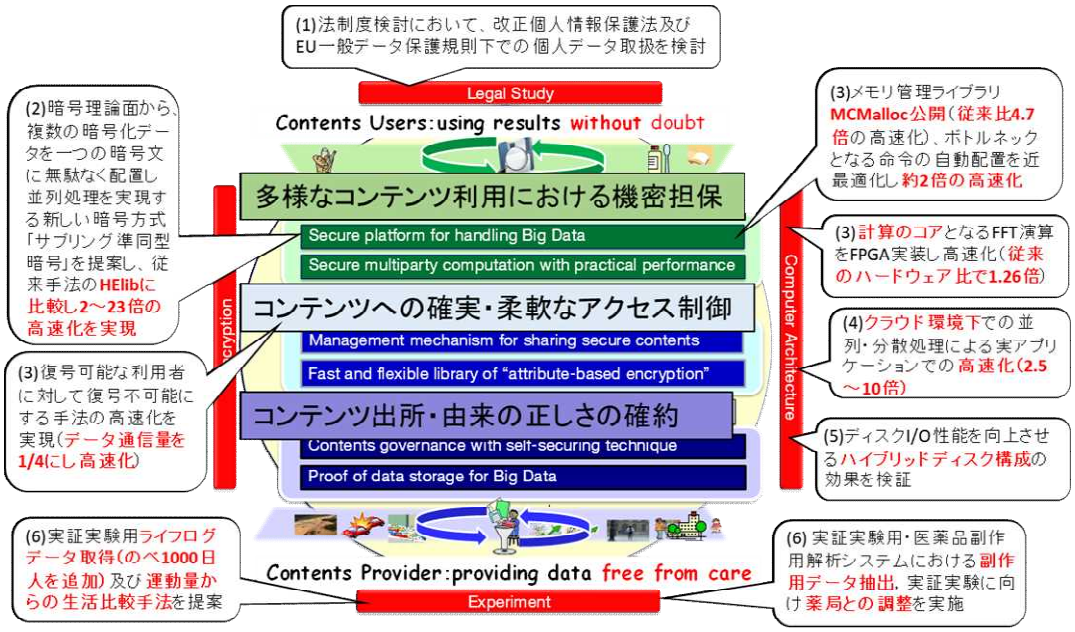
§2. 研究実施の概要

ビッグデータの利活用推進のためには、コンテンツ提供者が安心してデータを提供でき、コンテンツ利用者が信頼して結果を利用できる基盤が求められている。これに応えるため本研究では、「匿名化」や「通信時の暗号化」から脱却し、コンテンツを常に暗号化した状態で扱うことのできる基盤の構築を目指している。しかし、暗号化した状態で計算を実現するには膨大な時間が必要となるため実用化が困難である。これに対して本研究開発では、暗号理論とコンピュータアーキテクチャの両面で最適化を行うことにより、1,000 倍以上の高速化を行うことを目指している。

3 年目となる平成 29 年度は、個々の拠点(グループ)で進めてきた要素技術の統合調整を行いながら要素技術のさらなる改善を進めた。具体的には、各機能についてさらなる高速化とモジュール化を進め、一部については GitHub を通して公開を開始した。また、海外との連携を積極的に推進した。まず、CPS(サイバーフィジカル)分野への完全準同型暗号の応用を目指すためにミズーリ工科大学との連携を開始した。さらに、ニュージャージー工科大学を中心に世界規模で進められている完全準同型暗号 API 標準化活動への参加を開始した。なお、プロジェクト開始時に設定した中間評価時点までの 400 倍の高速化(HElib 比)は、昨年度末までに達成済である。

本年度の顕著な成果は、(a)暗号理論面からの新しい暗号プロトコル「サブリング準同型暗号方式」による高速化(演算の種類により 2～23 倍の高速化)[1]、(b)完全準同型暗号処理を高速化するためのメモリ管理ライブラリ MCMalloc の公開[2]、(c)並列分散処理改良による委託データマイニングの約 10 倍の高速化、ゲノムデータベース検索の約 2.5 倍の高速化[3]の実現である。

全体の成果は図に示す通り、(1)改正個人情報保護法、EU 一般データ保護規則下での個人データ取扱の検討、(2)新準同型型暗号「サブリング準同型暗号方式」の提案[1]、(3)完全準同型暗号向けメモリ管理ライブラリ公開[2]、ボトルネック命令の削減、属性ベース暗号高速化、(4)並列分散処理による高速化[3]、(5)I/O 高速化のためのハイブリッドディスク構成の検討、(6)データマイニング及び検索を内包するアプリケーションを対象とした実証実験準備である。



代表的な原著論文

[1] Arita S., Handa S., "Subring Homomorphic Encryption," In: Kim H., Kim DC. (eds) Information Security and Cryptology – ICISC 2017. ICISC 2017. Lecture Notes in Computer Science, Vol 10779. Springer, Cham, 2017.

[2] Akira Umayabara, Hayato YAMANA, "MCMalloc: A Scalable Memory Allocator for Multithreaded Applications on a Many-core Shared-Memory Machine," Proc. of IEEE Big Data 2017, 2017.

[3] Yuri Yamamoto, Masato Oguchi, "A Decentralized System of Genome Secret Search Implemented with Fully Homomorphic Encryption," Proc. of 2017 IEEE International Conference on Smart Computing (SMARTCOMP), 2017.