令和4年度研究開発成果概要図（目標・成果と今後の研究計画）

採択番号：05801

1．研究課題・受託者・研究開発期間・研究開発予算

◆研究開発課題名：リアルタイム暗号技術とプライバシー保護への拡張
◆受託者　　：兵庫県公立大学法人、GMOサイバーセキュリティbyイエラエ株式会社
◆研究開発期間　令和4年度～令和6年度（3年間）
◆研究開発予算（契約額）　令和４年度50百万円

2．研究開発の目標

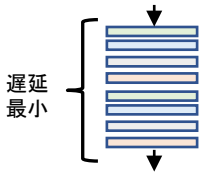
2025年度までに「256-bitセキュリティを持つサブナノ級低遅延暗号アルゴリズム」とその拡張であるプライバシー保護技術フレンドリ暗号を開発する。また、開発された各暗号アルゴリズムに対して世界中で利用できる環境の準備として標準化およびOSS化を行う。

3．研究開発の成果

研究開発目標

研究開発成果

研究開発項目１ 超低遅延暗号の研究開発



「リアルタイム暗号化」

サブナノ級低遅延暗号
-コア技術 ”低遅延ブロック暗号”

（数値目標: AES-256の1/4以下の0.3ns）

研究開発成果A：初期アルゴリズム設計
- 安全性と実装性能を兼ね備えた内部関数を設計し、初期設計案完成
  - ✓ サブナノ級の性能は達成可能であることを確認

研究開発成果B：暗号の自動評価ツールの作成
- 数理ソルバーを用いた差分、線形等の評価ツール開発
  - ✓ 既存の暗号に適用し未知の脆弱性発見

→研究論文1件採録、2件投稿中

研究開発項目2 プライバシー保護技術への拡張

「プライバシ保護技術」

プライバシ保護技術フレンドリ共通鍵暗号
-暗号化したままで演算可能・複数で秘匿計算
-プライバシー保護エッジコンピューティング）

（数値目標: AES-256の1.5倍以上の速度）

（2024年から開始予定だったが前倒しで開始）

研究開発成果：新しい代数的攻撃技術開発
- 部分非線形層に専用の代数解析技術を開発し、LowMCに適用
  - ✓ ASIACRYPTに研究論文1件発表
- 大きい有限体に対する新しい代数度評価技術、Chagriに適用
  - ✓ 安全性に問題があることを発見

→ 研究論文1件発表、1件投稿中

研究開発項目3 研究成果展開

研究成果展開：標準化団体に関する調査
- IETFにおける新規暗号アルゴリズムの提案可能性および低遅延/プライバシー保護技術が必要とされるユースケース

研究成果展開：OSSコミュニティに関する調査
- 利用実績の多いOSS選定および本研究開発の成果を入れ込むための既存OSSのI/F調査等を実施

標準化団体に関する調査
- IETF115に現地参加による調査/ロビー活動
  - ✓ 低遅延/プライバシー保護の需要が高いことが判明
  - ✓ 既存技術では低遅延を実現できないユースケースの発見

OSSコミュニティに関する調査
- IETF Hackathon等で利用されているOSSの調査
  - ✓ OpenSSLに対してパッチ実装し、アピール

4. 特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	標準化提案・採択	プレスリリース 報道	展示会	受賞・表彰
0 (0)	0 (0)	1 (1)	2 (2)	0 (0)	0 (0)	0 (0)	0 (0)

※成果数は累計件数、( )内は当該年度の件数です。

- **暗号分野の難関国際会議CT-RSAに採録**

低遅延暗号の安全性評価に関する論文が難関国際会議に採録

- **暗号分野のトップカンファレンスASIACRYPTで研究発表**

プライバシー保護技術の安全性評価に関する論文が国際暗号学会のフラッグシップ国際会議ASIACRYPT 2023に採録され、本プロジェクトの成果として2022年12月に発表

- **インターネットにおける標準化団体 IETF 115に参加**

IETF115に参加し、低遅延/プライバシー保護を実現する暗号技術に関する技術動向を把握した。標準化団体における暗号技術動向を以下の2件の講演を行った。

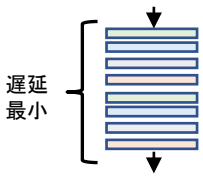
・ISOC Japan chapter IETF 115報告会

・日本ネットワークセキュリティ協会（JNSA） PKI相互運用WG IETF115報告会

5. 今後の研究開発計画

研究開発目標	研究開発計画

研究開発項目1 超低遅延暗号の研究開発



「リアルタイム暗号化」

サブナノ級低遅延暗号
–コア技術 ”低遅延ブロック暗号”

（数値目標: AES-256の1/4以下の0.3ns）

2022年度の成果	研究開発成果A：初期アルゴリズム設計 研究開発成果B：暗号の自動評価ツールの作成
2023年度の計画	• 初期設計アルゴリズムの安全性評価 ✓ 研究開発成果Bを用いた自己評価 ✓ 連携研究員を交えた第三者評価 • 初期設計アルゴリズムの性能評価 • 連携研究員とハードウェア実装評価 最終的なアルゴリズム開発（2023年度中）

研究開発項目2 プライバシー保護技術への拡張

「プライバシ保護技術」

プライバシ保護技術フレンドリ共通鍵暗号
–暗号化したままで演算可能・複数で秘匿計算
–プライバシー保護エッジコンピューティング）

（数値目標: AES-256の1.5倍以上の速度）

2022年度の成果	研究開発成果：新しい代数的攻撃技術開発
2023年度の計画	• 安全性を詳細に評価する技術の確立 ✓ 2022年度の解析技術を応用
2024年度の計画	• 実装性能と安全性を兼ね備えた暗号の設計 ✓ 2023年の評価技術を利用 • FHE/MPCと組み合わせて実装評価 最終的なアルゴリズム開発（2024年度中）

研究開発項目3 研究成果展開

研究成果展開：標準化団体に関する調査
- IETFにおける新規暗号アルゴリズムの提案可能性および低遅延/プライバシー保護技術が必要とされるユースケース

研究成果展開：OSSコミュニティに関する調査
- 利用実績の多いOSS選定および本研究開発の成果を入れ込むための既存OSSのI/F調査等を実施

2022年度の成果	研究開発成果：標準化/OSS化の下準備
2023年度の成果	• 標準化対象アルゴリズムの確定が近づいてきた段階でのInternet Draft執筆 • 実装対象アルゴリズムの確定が近づいてきた段階での実装
2024年度の成果	• 標準仕様およびOSSパッチに関するコミュニティからのコメントに対応することでブラッシュアップ