（革新）様式 1-4-2 (2022-1)

令和４年度研究開発成果概要書

採 択 番 号　　05801
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

（1）研究開発の目的

2021 年４月に NICT が発行した Beyond 5G(B5G)のホワイトペーパーでも言及されている通り、B5G の世界では、「超高速・大容量」「超低遅延」「超多数同時接続」の更なる高度化が求められる。そのため、プライバシー情報、個人情報、センシティブデータ等を保護する暗号技術にも従来の 5G の世界と比較し，大幅な高速化・低遅延化が求められる。安全性に関しては、B5G においては量子コンピュータができた場合の安全性も必要であり、鍵のサイズは 256 bit 以上が求められる。具体的には、NICT の開発対象のリストでも言及されている通り、B5G の世界では，サブナノ級のパフォーマンスを持つ低遅延暗号が必要となっており、既存の 5G 標準である AES-256 では B5G で要求されるパフォーマンスを達成することができない。よって、「256 bit セキュリティを持つサブナノ級の低遅延暗号アルゴリズム」は学術的にも未解決問題であり、解決可能な既存技術はない。

本研究では、センシング機器向けの「リアルタイム暗号化技術」の開発を行う。具体的には、量子計算機による攻撃にも耐性のある 256 bit セキュリティを有し、ハードウェアにおいてサブナノ級超低遅延暗号を開発する。この技術をセンシング機器に組み込みことで、フィジカル空間で取得したアナログデータを、超低遅延でサイバー空間に転送可能となり、サイバー空間とフィジカル空間で安全でかつシームレスなデータ連携が可能となる。暗号化したままで統計処理や機械学習が可能なマルチパーティ計算や完全準同型暗号等とのハイブリッド利用可能な技術に拡張することで、超多数接続においてもプライバシーの保護が可能とする。これにより、エッジコンピューティングによるリアルタイムでかつ安全な分析・解析が実現できる。

暗号の開発から実際の利用までには、第三者による数年間の安全性評価期間が必要であるため、7-10 年の時間を要するため、設計開発段階から技術普及のために、「標準化」と「知財化」を戦略的に進め、2030 年までに B5G でのアプリケーションで利用可能にする。

（2）研究開発期間

令和４年度から令和６年度（3 年間）

（3）受託者

兵庫県公立大学法人〈代表研究者〉
GMOサイバーセキュリティｂｙイエラエ株式会社

（4）研究開発予算（契約額）

令和４年度 50 百万円
※百万円未満切り上げ

（5）研究開発項目と担当

研究開発項目１　超低遅延暗号の開発

研究開発項目 1-a）　超低遅延暗号の初期アルゴリズム設計（兵庫県立大学）
研究開発項目 1-b）　超低遅延暗号の安全性評価（兵庫県立大学）
研究開発項目 1-c）　超低遅延暗号の実装評価
（兵庫県立大学/GMOサイバーセキュリティｂｙイエラエ株式会社）
研究開発項目 1-d）　超低遅延暗号の最終仕様決定（兵庫県立大学）

研究開発項目２　プライバシー保護技術への拡張

研究開発項目２-a）プライバシー保護技術フレンドリ暗号の安全性評価技術確立
（兵庫県立大学）

研究開発項目２-b）プライバシー保護技術フレンドリ暗号の設計
（兵庫県立大学/GMOサイバーセキュリティｂｙイエラエ株式会社）

研究開発項目３　研究成果展開

研究開発項目３-a）標準化団体およびOSSの調査
（GMOサイバーセキュリティｂｙイエラエ株式会社）

研究開発項目３-b）標準化団体およびOSSの継続調査および活動（その１）
（GMOサイバーセキュリティｂｙイエラエ株式会社）

研究開発項目３-c）標準化団体およびOSSの継続調査および活動（その２）
（GMOサイバーセキュリティｂｙイエラエ株式会社）

（６）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表等	研究論文	1	1
	その他研究発表	2	2
	標準化提案・採択	0	0
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	0	0

（７）具体的な実施内容と成果

研究開発項目１　超低遅延暗号の研究開発

A)　低遅延暗号の安全性評価技術の確立

B)　低遅延暗号の初期デザイン設計

A)安全で効率的な暗号の設計のためには、厳密な安全性評価が不可欠である。共通鍵暗号の場合には、差分、線形攻撃などあらゆる攻撃技術に対する安全性を保障する必要ある。しかしながら、さまざまな設計案に対して一つ一つ手作業ですべての安全性を評価することは非効率であり、現実的に不可能である。そこで、安全性評価を効率的にするため、数理ソルバーであるSAT solverやMILP solverを用いた汎用的な安全性評価ツールの開発を実施した。具体的には、差分、線形、不能差分、積分攻撃の４つの代表的な攻撃に対する安全性評価ツールを作成した。結果の有用性を示すため、既存の低遅延暗号Orthros, PRINCE, QARMAに対して適用し、未知の特性を発見することに成功した。Orthrosに対しては、新しい差分と積分特性を発見し、その解析結果は現在国際会議に採録された。PRINCE, QARMAに対する解析は国際論文誌に投稿した。

B)低遅延暗号の設計のため、全体構成と内部関数の初期設計の検討を実施した。全体構成としては、複数の関数を並列で実行し、最後にXORで連結する複数ブランチ構造を当初の予定通り採用する予定である。内部関数に関しては、安全性と低遅延性能の観点で優れている線型層と非線形層と呼ばれる関数を設計とした。(A)の評価ツールにより、安全性と実装性能の高い非線形層を発見した。また線形関数についても、さまざまなパラメータでの評価を実施し、初期の設計案が完成した。ハードウェアの実装評価も簡易的に行い、このアプローチでサブナノクラスの低遅延性能が達成可能であることを確認した。

研究開発項目２　プライバシー保護の拡張

A)　MPC/FHE フレンドリー共通鍵暗号に対する解析技術の開発

B)　FHE 関連技術の調査

A)EUROCRYPT 2015 で提案された MPC/FHE フレンドリー暗号 LowMC の一番の特徴は、非線形関数演算を内部状態全体ではなく、部分的に実施する部分非線形層の利用である。しかし、この部分非線形層の技術的解析はまだ不十分であり、どうのようにこの構造の特徴を利用してより効率的な解析技術を開発するのは重要な課題である。この問題に対して、部分非線形層に専用の代数解析技術を開発し、既存の LowMC に対する安全性評価を大幅に改良した。この結果はすでに国際会議 ASIACRYPT 2022 に採録された。また、ACM CCS 2022 で提案された FHE フレンドリー暗号 Chaghri に対して、大きい有限体に対する新しい代数度評価技術を用いて、致命的な脆弱性を発見し、安全性に大きな問題があること明らかにした。この結果は国際会議に投稿した。

B)FHE フレンドリー暗号の特徴は復号化の AND 演算の深さが少ないほど性能が高い特徴がある。このような暗号を設計するために、まずは FHE に関する設計、解析技術をより深くする理解する必要がある。特に、多数の FHE 方式が存在しているため、どうような構成に対して専用の共通鍵暗号を設計するのは重要な課題だと考え、FHE 技術に対しての体系統的な研究調査を進めた。

研究開発項目３　研究成果展開

A) 標準化団体に対する調査

B) OSS コミュニティに対する調査

A)インターネットプロトコルが標準化されている IETF において、通信としての低遅延が必要とされているか、低遅延暗号が活用されるユースケースとしてどのようなものが注目されているかを 2022 年 11 月に開催された IETF115 に現地参加することで各 WG での発表だけではなく、さまざまなセッションに参加してロビー活動を行った。

得られた大きなものをサマリーとして示す。Satellite 通信での利用において低遅延を実現するために QUIC プロトコルを用いる提案が行われていたが、QUIC で利用されている暗号技術が現行暗号である AES や ChaCha20-Poly1305 であり、低遅延という観点から低遅延を実現する上でボトルネックになる可能性があり、今後の通信において低遅延を実現しようとする際に重大な課題になると考えられる。今回の研究課題として実現しようとしている超低遅延な暗号技術の付加価値があることを確認できた。また、IETF115 に参加して得られた暗号技術の動向について、ISOC Japan Chapter および JNSA PKI 相互運用 WG が開催する勉強会において、登壇することで、新しい暗号技術に対する意見交換を行った。

2023 年３月に横浜で開催される IETF116 にて、QUIC プロトコルで利用されている暗号技術の超低遅延化というアプローチで成果が妥当かどうかを IETF Security Area のキーパーソンなどにヒアリングを行った。

B)OSS コミュニティへの投稿する事前準備として、新しい暗号技術を考案した際にどのようにコミュニティに訴求するかを調査・検討を行った。活動としては、IETF115 で開催された IETF Hackathon の参加者たちがどのような OSS を用いて開発しているなどの調査を行った。また、利用できる環境を増やすという観点から標準化仕様と OSS が両輪となっているので相互影響を与えられるよう IETF Hackathon での活動が可能かどうかという観点でも当該会議を参加・調査した。その結果として、IETF Hackathon に参加することで、多くの技術者たちに低遅延暗号についてアピールすることができる可能性があることがわかった。研究開発項目 1 および 2 の進捗を踏まえて、Hackathon での活動を行いながら OSS 化に向けた開発を行う準備を行った。2022 年度末までには暗号ライブラリとして広く利用されている OpenSSL へのインターフェイス等について調査を行った。

（8）今後の研究開発計画

研究開発項目１　超低遅延暗号の研究開発

研究開発項目 1 に関しては、本年度当初の計画どおり、低遅延暗号アルゴリズムの初期設計を実施した。来年度は、連携研究員とともに、初期設計暗号の安全性評価やハードウェア評価を実施する。暗号の安全性評価では、設計者以外の第三者の目線を入れることを目的に、連携研究員とともに詳細な解析を実施する。これらの安全性と実装評価を通して、さらに安全性を向上させ、かつ遅延の削減可能な方式のアイデアを得る。その後に、これらの知見をもとに、兵庫県立大学で初期アルゴリズムのアップデートを行い、最終仕様を決定し、令和 5 年度中に国際会議に投稿する予定である。また実装技術の知財に関しても検討し推進する。

研究開発項目２　プライバシー保護の拡張

研究開発項目２では、MPC や FHE などのプライバシー保護技術フレンドリー暗号」の実現のため、耐量子低遅延暗号の設計理論を拡張し、AND gate の数と深さの最小化が可能な新しい暗号の設計理論を構築する。既存の暗号設計では、同じラウンド関数を繰り返すことで高い安全性を達成しているが、安全性向上に直接寄与していない AND 演算が多く回路に含まれる。本研究では、通常の繰り返し構造ではなく、ラウンド毎に AND の数や配置が異なる関数を設計することで、ANDgate を効率的に用いる構造を設計する。具体的には、ラウンド間の関係性を考慮し、AND 演算の影響をラウンド毎に厳密に評価することで、安全性達成のために必要な AND gate の最小化を行う。

研究開発項目３　研究成果展開

研究開発項目３に関しては、研究開発項目 1 および研究開発項目２の研究成果が確定した際に、スムーズに IETF での Internet Draft の執筆や実装が行えるよう、事前に行える開発/実行環境の構築や研究成果の展開先の技術動向や課題感について調査・検討を行い、順調に準備は進捗している。

研究開発項目 1 および研究開発項目２の研究成果が確定後には、IETF での Hackathon 参加を行い能動的な研究成果展開に向けたアピールおよびフィードバックを得るための実装や仕様執筆を行う。IETF には OSS コミュニティの重鎮も多数参加しているため、技術の素晴らしさを説くだけではなく、どのような恩恵があるのかという利用者視点での展開を行う。