（革新）様式 1-4-2 (2022-1)

令和６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　兵庫県立大学〈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年度から令和６年度までの総額 218 百万円（令和６年度 85 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	1	1
外部発表等	研究論文	16	5
	その他研究発表	19	8
	標準化提案・採択	2	1
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	1	1

（７）具体的な実施内容と最終成果

研究開発項目１：

昨年度までに開発したAreionとGleeokに対して安全性評価を実施した。暗号の設計を効率よく実施するために、設計数理ソルバーを用いた厳密な安全性が可能な評価ツールの作成を行った。具体的は、共通鍵暗号に対して最も強力な技術である差分攻撃を評価するため差分特性確率を導出するツールの作成をSATを用いて実施した。結果として、ブロック暗号Orthrosに対してのclustering effect, Piccoloに対しての最大差分特性確率の厳密な導出に成功した。また、既存の低遅延暗号PRINCEやQARMAに関しては、未知の差分特性の導出に成功した。Areionのベースになっていた AESの評価ではトップ会議ASIACRYPT 2024に採択された。これらの成果は、Areionや Gleeokが最先端の高い安全性技術により設計されたことを示し、これらの暗号の安全性に関する信頼をより強固にさせることに繋がった。

さらに、これまでの設計技術と安全性評価技術をベースとして暗号演算が超高速でかつ超低消費電力であるAETHER開発を開発した。この成果はトップ会議CHES 2025に採録されている。AreionやGleeokは標準化の観点で知財はとらなかったが、この技術に関しては主にデータセンター等で閉じて使用されることをターゲットとしているため、特許出願済みである。

研究開発項目２：

FHE（完全準同型暗号）向けの暗号の多くは、低い乗算深度を達成するため、ランダム化されたコンポーネントを採用し、少ないラウンド数で効率的に動作するように設計されている。しかし、こうした暗号の多くは過剰設計となっており、乱数やランダム化されたコンポーネントを過度に使用することで、平文の暗号化や準同型復号の性能に悪影響を及ぼしている。この課題を解決するため、新たな設計「PASTAv2」を提案した。PASTAv2では、第一ラウンドの線形層

のみランダム化されるというシンプルなアプローチを採用した。この新しい設計の安全性を保証するために、厳密な暗号解析を行っていた。特に、PASTAv2 は平文の暗号化において、最新のFHE向けの暗号PASTAと比較して２倍の速度を実現し、準同型復号においてもPASTAよりも約30%高速に動作している。

大きな有限体上で定義されるMPC/FHE/ZK向けの暗号を解析するために、複数の新たな技術を開発した。まず、MPC向けの暗号であるLowMC、Biscuit、RAIN、AIMに対しては、新しい代数攻撃を用いて効率的な鍵回復攻撃を提案し、その成果を FSE 2024 およびASIACRYPT2024で発表した。また、ZK向けのハッシュ関数Tip5とMonolithに関しては、大きな素数体上でのsplit-and-lookup S-boxの差分特性を効率的に解析するアルゴリズムを開発し、これを用いてこれらのハッシュ関数に対する最良の衝突攻撃を示した（FSE 2025）。

研究開発項目３：

- Internet Draft
  - 低遅延暗号Areionに関する仕様 Ultra-Low Latency Cryptography Areion
  - 低遅延暗号AreionをIPsecプロトコルで利用可能するための仕様 Ultra-Low Latency Cryptography Areion for IPsec

- OSS
  - リファレンス実装版Areion / low-latency-crypto-areion
  - OpenSSL版Areion / areion-openssl
  - リファレンス実装版Areion（ハッシュ関数） /（2025年３月末公開予定）
  - ARM NEON版 /（2025年３月末公開予定）
  - QUIC版Areion /（2025年３月末公開予定）
  - Rust版Areion /（2025年３月末公開予定）

標準化団体であるIETFにおいて低遅延暗号Areionに関するInternet Draftを執筆し、IETFの特徴である「仕様と実装」の両輪で進めていくことに注目を行い、IETF で開催されるHakachon インベントに参画することで、IETF 以外の様々な標準化団体に参加している層に対して、Areionの特徴や強みを周知するためにIETF会合毎にテーマを設定（例：低遅延性、モバイル環境での性能など）して、参加者に訴求できるように標準化を推進した。また、このHackathon で開発した実装物は OSS として公開することで興味を持ってくれた参加者が利用できるような環境の整備にも力を入れて活動を行った。

上記にあるような仕様検討と実装を両輪でやっていることで、地に足のついた議論ができるため、IETFに参加しているキーパーソンたちと情報交換や議論を行うことができ、その結果として、低遅延性を必要としているゲーム業界へのパスや日本国産暗号が必要な暗号利用のユースケース（IPsec）の実現など、IETFでの標準化だけではなく、社会実装に欠かせないアルゴリズムの利用実績を作るための仕込み活動も順調に進捗している。

従来であれば、標準化活動は長い時間を有する活動というのが一般的ではあるが、積極的にIETF HackathonにおいてAreionの発表や特徴を様々な切り口から訴求したことがこれらのような利用に向けた第一歩を踏み出せていると考える。

また、IETFでの標準化活動として、Internet Draftの執筆とOSSを実装し性能報告を行うことで、IETF以外の標準化団体であり6Gを検討している3GPPの参加者に認知されることとなり、Areionの性能について共有してよいか？という問い合わせが会合の会場で発生するなどの現地参加していることによる顔の見える標準化活動を体現できたものと考える。

（8）研究開発成果の展開・普及等に向けた計画・展望

2025年４月以降における現在公開中のInternet DraftやOSSに対しては適宜更新を行い、利用しようとする方に向けて情報発信を行う。

IETFに投稿しているAreionに関するInternet Draftを中心に、低遅延性を必要としているアプリケ

ーション（e-Sports）や日本国産暗号であることが重要となるユースケース（IPsec）での採用に向けて議論が進展している状況を前向きに捉えて、社会実装に向けて活動を行うための活動費用などの模索を行う。
定期的にステークホルダとのやり取りを継続して、実社会で低遅延暗号が利用されるような世界を実現に向けて邁進している。

学術的には、本プロジェクトで低遅延性能としてはソフトウェアとハードウェア用で世界最高性能の暗号の開発のために、新しい暗号の設計理論の構築をした。実際この論文発表の後に、いくつかの follow up work が論文発表されており、学術的な新しい方向性を切り拓いた。具体的には、同様の構造を用いた新しい暗号の設計や、これらの構造に対する安全性評価である。特に後者の安全性評価に関してはまだ未知な部分が多く、今後数年でも厳密な安全性を評価する研究が活発に行われることが予想される。そのため、5 年後には Areion や Gleeok の厳密な安全性評価が第三者を中心に実施され、その安全性の信頼がより高まっていることも予想される。また、技術の拡張の観点では、本プロジェクトで実施した高速・低消費電力暗号など新しい実装要求や機能に対する暗号技術への応用も期待される。
育成の観点でも本プロジェクトに参画した修士や博士課程の学生は、それぞれ企業の研究者や大学の教員として研究者としてのキャリアをスタートしている。そのため 5 年後には同様のプロジェクトで日本をリードする研究者として活躍していることが期待される。
Beyond 5G（6G）がもたらす想定市場規模は、主なユースケースを見てもある程度のボリュームを有するものとなると言われている。また、それぞれの市場成長に目を向けると Compound Annual Growth Rate（年平均成長率）の観点で市場を確認すると確実に成長する市場であることがわかる。

ユースケース	市場規模 (2023年)	市場規模 (2030年)	CAGR	CAGR予測期間
遠隔手術	64億1,000万米ドル	157億7,000万米ドル	11.90%	2024年-2031年
自動運転	1兆9,211億ドル	13兆6,324億ドル	32.3%	2023年-2030年
産業用IoT	766億米ドル	1,301億米ドル	6.50%	2021年-2030年

また、実用化状況については、Beyond 5G（6G）の実用化に関しては、過去の LTE（4G）や 5G を実現してきた実績を踏まえても着実に実用化に向けて計画的な準備および技術移行が実施されることが予想される。この時には 3GPP の方では 6G に関する標準化は完了している状況ではあるが、ユースケースに紐づくアプリケーションにおいて、現行暗号では実現できない低遅延性を必要とするような通信に関する要求や新たなインターネットプロトコル（例：SFrame 等）で安全な状態を実現するためのビルディングブロックとしての重要性が増加してくることが予想される。
今回、主に標準化を推進した Areion については、現在、IETF などで標準化されている共通鍵暗号が高スループットや軽量性を特徴としたアルゴリズムのみ提案されている状況であるため、我々が提案している低遅延暗号が世界に先駆けて標準化前の Draft を公開していることは大きな強みであると言え、検索エンジンのページランクの観点からも 1 ページ目に表示されるなど効果はあり、低遅延暗号といえば Areion というポジションを築けたと言える。また、低遅延性が必要とされる e-Sports（ゲーム）や日本国産暗号であることを必要とされる用途を中心にキーパーソンと密な連携を取っているため、5 年後くらいの将来において実社会で Areion が利用されていることが期待される。このように従来の暗号技術では実現できなかったような低遅延性という特徴を持った暗号技術が用途別に利用されるような高度な暗号技術が生まれていくことになると予想される。
この成果が、日本国内における国産暗号の研究開発および標準化活動を行うためのパイロットケースになることを願うばかりである。