（革新）様式 1-4-2 (2022-1)

令和５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年度から令和５年度までの総額 134 百万円（令和５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	0	0
外部発表等	研究論文	10	9
	その他研究発表	11	9
	標準化提案・採択	1	1
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	12	12

（７）具体的な実施内容と成果

- 研究開発項目１：

昨年度初期設計したS/W用の低遅延暗号の安全性評価を、外部の研究者（NEC, NICT）とともに実施した。安全性評価では、ハッシュ関数と認証暗号として利用した場合の安全性評価を実施した。ハッシュ関数としては、差分攻撃をベースにした衝突攻撃、中間一致攻撃をベースにした原像復元攻撃の安全性評価を実施し、十分に安全であることを評価した。また、認証暗号に関しては、関数自体が擬似ランダム置換と識別不可能なことを統計的偏りの有無で評価した。具体的には、数理ソルバーであるSATやMILPを用いて、差分攻撃、線形攻撃、積分攻撃、不能差分攻撃等の攻撃を網羅的に探索し、統計的偏りがないことを示した。これらの結果と、設計方針、実装評価を加えて、Areionという名前のアルゴリズムで暗号実装分野のトップ会議CHESに採録され、10月に発表を実施した[外部発表-論文20]。実装性能に関しては、世界標準のハッシュ関数SHA-2と比較しても３倍上高速であり、認証暗号としても256 bit認証暗号としては、IntelやARMの環境で世界最速を達成した。さらに同様の設計思想をベースにしたブロック暗号Ghidleも設計し、国際会議ACISで発表した[外部発表-論文8]

昨年度作成したハードウェア用の低遅延暗号に関して、スイス工科大学ローザンヌ校のSubhadeep Banik博士とAndrea Caforio博士とともにハードウェア評価を実施した。1cycleで暗号結果が返ってくるUnrolled実装をターゲットと、その実装方法で暗号化に必要なクリティカルパスと回路規模を最小化することを目標とした。ハードウェア実装結果を見ながら、暗号の構成要素の再検討や安全性評価実施し、暗号の低遅延目的での最適化を実施した。結果として、量子計算機に対しても安全性を有し、かつサブナノクラスの低遅延性能を有する暗号の設計を行うことができた。これらの結果と、設計方針、実装評価を加えて、Gleeokiという名前のアルゴリズムで暗号実装分野のトップ会議CHESに採録された。

- 研究開発項目２：

  F_(2^n)に定義される FHE フレンドリー共通鍵暗号 Chaghri に対して、coefficient grouping という斬新かつ効率的な代数度評価技術を開発し、世界で初めて Chaghri を破った。この技術を用いて、Chaghri の線形層の脆弱性を理論的解釈することが可能になった。この成果が暗号分野のトップ国際会議 EUROCRYPT 2023 に採録された。しかし、この技術は複雑な線形層に対して効率が悪い。これを解決するために、新しい理論を築き上げ、coefficient grouping 技術の応用範囲更に広げた。具体的には、coefficient grouping 技術を更に改良し、如何に F_(2^n)に定義される SPN 構造をベースにして、安全かつ高速な FHE フレンドリー共通鍵暗号を設計するのかを明らかにした。それに、NIST の耐量子暗号標準プロジェクトの候補暗号 AIMer に対して、新しい代数攻撃を提案し、完全に破ることができた。この論文が共通鍵暗号分野のトップ国際会議 FSE2024 に採録された。

- 研究開発項目３：

  研究開発項目 3-a）標準化団体および OSS の継続調査で実施した標準化団体および OSS の調査結果を踏まえて、低遅延が必要とされているプロトコルのターゲットとして、QUIC プロトコルを設定した。このプロトコルでは、プロトコルとして低遅延性が必要とされているにも関わらず、利用されている暗号アルゴリズムが従来の AES や ChaCha20-Poly1305 であるという課題がある。そこに注目し、暗号機能部分に対して Areion を利用可能とするために Areion のリファレンス実装を公開した。また、その Areion を QUIC プロトコルで利用可能とするために、TLS ハンドシェイク機能で Areion を動作させるために OpenSSL ベースのライブラリである quictls ライブラリに対して、暗号レイヤおよび TLS プロトコル機能部分に Areion に関する機能追加するための修正を実施した。 その結果として、２つの OSS を開発および公開することができた。

  また、標準化活動については、IETF117（7 月）に参加を行い、インターネット標準化での低遅延が必要とされているシチュエーションの調査や技術動向を把握するために WG/RG への参加、ロビー活動を実施した。IETF117 において Hackathon に参加し、Areion の OpenSSL(quictls)実装を行なったことを報告し、TLS プロトコルで Areion が利用できることを報告した。その効果として、インターネットで活躍しているキーパーソンから低遅延暗号に対するフィードバックとして、既存暗号アルゴリズムとの比較観点や認証技術における適用の可能性等の遅延を得ることができた。現地でのヒアリング等において低遅延性が必要となる eSports などで活用されている通信プロトコルである WebRTC も有望なターゲットとして台頭してきたため、Areion 対応するための調査検討を行なった。

  そして、7 月会合の結果等を踏まえて、IETF118(11 月)に向けて、前回の IETF117 Hackathon で宣言したとおり、Areion に関する Internet Draft (I-D) の初版(00 版)を執筆/公開を標準化提案として実施した。この I-D に対しては加筆する方向で計画しており、暗号化機能やハッシュ関数機能を執筆するかどうかを検討しながら I-D の更新作業を実施する想定である。なお、近年の暗号技術に関する標準化における著作権等について、自由に利用可能なことが条件で与えられることが判明したため、本研究開発でどのように知財について取り扱うか検討する必要があることが判明した。

  11 月開催の IETF118 では、IETF117 に引き続き、インターネットプロトコルでの低遅延性に関するニーズや暗号技術に関する技術動向を調査するために WG/RG への参加およびロビー活動の実施を行った。Hackathon に参加し、Areion 対応の WebRTC の開発を進め、参加者に対して Areion に関する報告の実施を行った。

  さらに、2024 年３月開催の IETF119 にも参加を行い、現地に参加しているキーパーソンや Areion の浸透のための活動を実施した。IETF119 における Hackathon に

も参加を行い、今回は Areion が暗号化機能およびハッシュの機能の両方を備えることから、Areion に興味のあるメンバーが二つの機能を利用可能なようにハッシュの機能を OpenSSL の中で利用可能とする対応を行なった。活動の成果を Hackathon の中で発表を行い、それにより他の参加者から Areion に関する適用ユースケースや特徴などの質問があった。

今年度、IETF117～IETF119 にて毎回オンサイトで参加し、プレゼンテーションを行なったことで他の参加者に対しての認知度の向上や Areion 自身の理解度を高めたことで、参加者の中での興味度が上がっている効果が出てきていると考える。

（8）今後の研究開発計画

- 研究開発項目１：

  令和 5 年度までに設計したソフトウェア用低遅延暗号 Areion とハードウェア低遅延暗号 Gleeok の安全性評価や実装評価を実施する。具体的には、外部の研究者と共同で実施することで設計段階では評価できない特性等について検討する。これらを踏まえ、最終的な仕様を決定する。また、知財についても、これらの周辺技術や拡張技術についても２件申請予定である。

- 研究開発項目２：

  完全準同型暗号方式 BFV や BGV に向けの共通鍵暗号がいくつか提案されてきた。その中に性能が一番高いのは CHES 2023 で提案された Pasta というストリーム暗号である。来年度の目標として、Pasta をベースにして、最少のランダム層を持つ安全かつ高速な BFV/BGV 向けの新しい暗号アルゴリズムを開発する。具体的には、Pasta に複数のランダム線形層が使われているが、全部の線形層をランダムにする必要があるかとうか未だに研究されていない。この問題に対して、安全にランダム層の数を減らす暗号設計方法を見つけて、更に Pasta のプレーン暗号化及び準同型暗号化性能を向上させる。

- 研究開発項目３：

  今後は、超低遅延暗号の研究開発の成果として考案された Areion をインターネット等で興味を持ったエンジニア等が気軽に利用できる環境（リファレンス実装、メジャーな OSS へのパッチ）の拡充を更に推進していく。また、IETF での標準化仕様である RFC のように誰もが参照できる公式な仕様化を目指して、適切なタイミングで標準化提案中の Internet Draft の更新を行なっていく。さらに、低遅延性が必要となりそうなセキュリティプロトコルに対して、Areion を適用する場合の仕様についても、IETF への標準化提案として Internet-Draft を執筆/公開予定である。

  また、本プロジェクトの成果展開、普及を視野に、本研究開発において考案した暗号技術について、GMO サイバーセキュリティ by イエラエ社の技術ブログでの情報発信や情報セキュリティ関連の組織が実施しているセミナー等への登壇により、本研究開発が課題としている技術課題やその解決策としてのこの活動での成果を幅広く発信していく。

  また、本活動で実装/公開した OSS について、OSS コミュニティに移管できるようアプローチを行い、その OSS コミュニティが存在している限り永続的な保守管理が行われるよう活動を行う。

  上記の活動以外のアプローチとして、クローズドな製品などへの採用なども視野に入れながら実社会で利用できるよう活動を継続する。