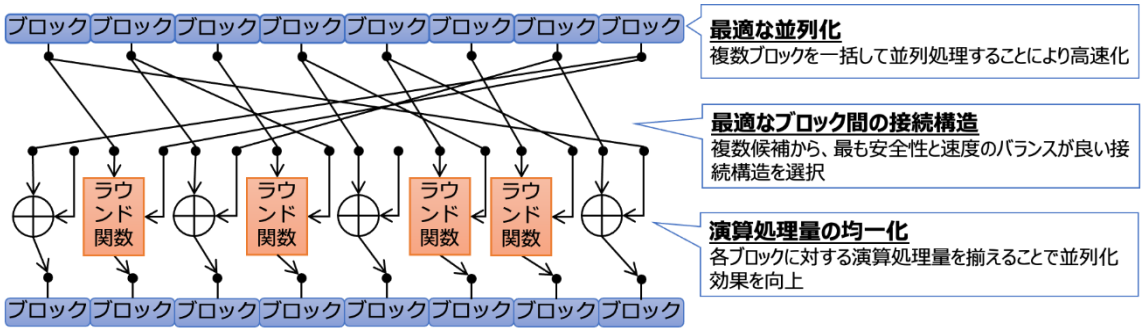
KDDI Research　兵庫県立大学 UNIVERSITY OF HYOGO

世界最速 Beyond 5G/6G に向けた超高速暗号アルゴリズム「Rocca」を開発

~256 ビット暗号で初めて（注１）100Gbps 超の処理性能を実現~

兵庫県立大学大学院 情報科学研究科の五十部孝典 准教授の研究グループと株式会社 KDDI 総合研究所（本社：埼玉県ふじみ野市、代表取締役所長：中村 元、以下「KDDI 総合研究所」）は、Beyond 5G/6G 時代に求められる処理性能と安全性を備えた新しい共通鍵暗号アルゴリズム「Rocca」を開発しました。「Rocca」は 256 ビットの鍵長に対応する認証付きストリーム暗号で、処理速度として世界最速（注１）となる 138Gbps を達成しました。



図：Rocca の処理イメージ

【背景】
Beyond 5G/6G では 100Gbps 超の通信速度を目標に研究開発が進められています。大容量映像伝送などの超高速通信が求められるサービスを実現するには、同様の処理性能を持つ暗号アルゴリズムが必要になります。

Beyond 5G/6G 時代に求められる共通鍵暗号技術の要件として、
- 通信速度のボトルネックとならない 100Gbps 超の処理速度を実現する
- 量子計算機による解読への耐性を持たせるため、256 ビットの鍵長をサポートする

・暗号化と認証機能を統合しデータが改ざんされていないことも保証可能なアルゴリズム（認証付き暗号）とする

の 3 点があり、これらを満たす暗号アルゴリズムとして「Rocca」を開発しました。

【今回の成果】

開発した認証付き暗号アルゴリズム「Rocca」は、PC やスマートフォンの CPU で高速に処理可能な演算（AES-NI（注２）を含む）を主な構成要素とし、それらを効率よく並列処理することで高速性を実現しています。加えて、十分な安全性が確保できる構造に配置することで、高速性と安全性を両立しました。米国標準暗号アルゴリズムとして広く使用されている AES との速度比較において、AES が AES-NI を利用しない場合で 100 倍以上、AES が AES-NI を利用した場合でも約 4.5 倍の高速化を達成しました。また、256 ビットの鍵長に対応する認証付き暗号アルゴリズムとして初めて 100Gbps を超える 138Gbps の処理性能を実現しており、これはソフトウェア実装された 256 ビットの鍵長に対応した認証付き暗号の計測結果として世界最速です。

■AES との性能比較

	AES-256-GCM (AES-NI なし)	AES-256-GCM (AES-NI あり)	Rocca （AES-NI あり）
処理速度(注 3)	0.9Gbps	31Gbps	138Gbps

【今後の展望】

今後、アルゴリズムのさらなる高速化に取り組むとともに、外部機関とも連携した詳細な安全性評価を実施していきます。将来の実用化に向け、スマートフォン上での動作など実際の利用を想定した環境での性能評価についても取り組んでいきます。

今回の成果は、暗号のソフトウェア実装に関する最高峰の国際会議 28th annual Fast Software Encryption conference （FSE2022）に採録されました。2022 年 3 月に発表予定です。

なお、本研究開発の一部は、総務省の「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の成果です。

<兵庫県立大学大学院 情報科学研究科の取り組み>

あらゆるものがネットワークに繋がる IoT（Internet of Things）やビッグデータ時代において、情報やプライバシーをいかに保護するのかは社会的に大きな課題です。本研究科では、情報セキュリティに関して、理論面と実践面の両面からアプローチすることで、高度なサイバーセキュリティ人材の育成を目指しています。また、実産業・実社会で脅威となっているセキュリティの課題に対して、体系だった計算機科学的アプローチで解決に取り組んでいます。

<KDDI 総合研究所の取り組み>

KDDI と KDDI 総合研究所は、2030 年を見据えた次世代社会構想「KDDI Accelerate　5.0」（https://www.kddi-research.jp/kddi_accelerate5_0/）を策定し、その具体化に向け、イノベーションを生むためのエコシステムの醸成に必要と考えられる「将来像」と「テクノロジー」の両面について Beyond 5G/6G ホワイトペーパー（https://www.kddi-research.jp/tech/whitepaper_b5g_6g/）にまとめました。両社は新たなライフスタイルの実現を目指し、7 つのテクノロジーとそれらが密接に連携するオーケストレーション技術の研究開発を推進します。今回の成果は 7 つのテクノロジーの中の「セキュリティ」に該当します。

【発表詳細】

国際会議: 28th annual Fast Software Encryption conference (FSE 2022)

論文タイトル: Rocca: An Efficient AES-based Encryption Scheme for Beyond 5G

著者: 阪本　光星(兵庫県立大学), リュウ　フカン(兵庫県立大学), 仲野　有登 (KDDI 総合研究所), 清本 晋作 (KDDI 総合研究所), 五十部　孝典 (兵庫県立大学)

【本件に関する一般の方からのお問い合わせ先】

兵庫県立大学大学院 情報科学研究科　准教授　五十部 孝典 (いそべたかのり)

E-Mail: takanori.isobe@ai.u-hyogo.ac.jp

（注1） ソフトウェア実装された 256 ビットの鍵長に対応する認証付き暗号アルゴリズムとして。Intel® Core™ i7-1068NG7 での計測結果。（2021 年 11 月 9 日時点、KDDI 総合研究所調べ）

（注2） Advanced Encryption Standard New Instructions の略で、AES の処理を高速に実行可能な命令セット。

（注3） Intel® Core™ i7-1068NG7 での計測結果。AES は OpenSSL の実装を利用して計測。Rocca も同様に Open SSL に組み込み計測を実施。