平成２８年８月２２日

報道機関　各位

東北大学電気通信研究所
東北大学大学院情報科学研究科
日本電気株式会社中央研究所

AES 暗号処理にかかる消費エネルギーを半分以下に

IoT 機器向け高速・省電力暗号処理技術の開発に成功

【概要】

国立大学法人東北大学（総長：里見進）電気通信研究所の本間尚文教授、同大学院情報科学研究科の青木孝文教授、日本電気株式会社（代表取締役 執行役員社長 兼 CEO：新野隆）中央研究所の森岡澄夫博士らの研究グループは、ガロア体と呼ばれる数体系に基づく演算を圧縮する新手法を発見し、消費エネルギーをこれまでより 50%以上削減した世界最高効率の AES 暗号処理回路の開発に成功しました。今回の成果により、エネルギーの制約が大きい情報通信機器への暗号技術の搭載が促進され、モノのインターネット（IoT: Internet of Things）と呼ばれる次世代ネットワークの安全性を大きく高めることが期待されます。

本成果は，平成 28 年 8 月 19 日に米国サンタバーバラにて開催された国際暗号学会の国際会議（暗号ハードウェアと組込みシステムに関する国際会議）で発表されました。

問い合わせ先
東北大学　電気通信研究所
担当　本間　尚文
電話　022-217-5506
E-mail　homma@riec.tohoku.ac.jp

東北大学　大学院情報科学研究科
担当　上野　嶺
電話　022-795-7169
E-mail　ueno@aoki.ecei.tohoku.ac.jp

■ 開発の社会的背景 ■

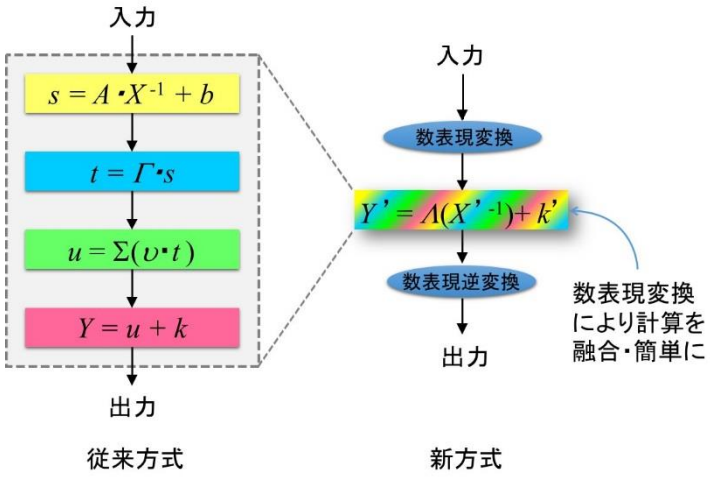
現在、個人情報や金融情報といった大切な情報が情報通信機器を通してインターネット上でやりとりされることが一般的となっていますが、そのような情報を守るため機器内部では暗号技術が利用されています。近年注目を集めているモノのインターネット（IoT: Internet of Things）などの次世代ネットワークでは、無数の機器がネットワークに接続されることが予想されるため、悪意ある攻撃を防ぐためそれらの接続機器にも暗号技術を搭載することが求められています。しかし、IoT の機器の中には、電池やバッテリーで駆動するエネルギー制約の大きい機器も多数含まれており、それらに消費エネルギーの大きい暗号処理をいかに実行させるかが課題となっていました。特に、国際標準暗号方式の一つである AES（Advanced Encryption Standard）は、世界で最も広く使われている暗号の一つであり、無線 LAN などでも使用されることから、AES 暗号処理を省エネルギーに設計することは実用上極めて重要とされていました。

■ 開発の経緯 ■

国立大学法人東北大学（以下、東北大学）と日本電気株式会社（以下、NEC）は、情報通信機器の安全性向上を目的として、2013 年から共同で研究開発に取り組んできました。特に、IoT に代表される次世代ネットワークにおける新たなサービスを安心して享受できるシステムの構築を目指し、これまで暗号機能が搭載されていなかった小型機器・センサにも暗号処理を搭載するための技術開発を行ってきました。なお、今回の研究開発は、科学研究費補助金「ガロア体算術演算に基づく VLSI データパスの形式的設計技術の開拓」(No. 25240006　研究代表：東北大学　本間尚文）の一環として行われたものです。

■ 研究の内容 ■

今回確立した設計技術では、AES 暗号アルゴリズムがガロア体と呼ばれる特殊な数体系に基づく計算として表現されることに着目しました。同研究グループは，入力の数表現を一旦別の数表現に変換することにより、その後の複数の演算を一度に計算でき、かつ、使用する回路素子を大幅に削減できることを見出しました。また、その後逆変換を行うことで、本来の出力を容易に得られることを確認しました。そこで、演算の前後に数表現変換と逆変換を挿入し、内部では変換した数表現を用いる演算方式を考案しました。さらに、新方式に基づく AES 暗号処理回路を設計・開発し、従来の世界最高の回路と比較して、半分以下（45%程度）のエネルギーで 1 回の暗号処理を行えることを確認しました。 開発した AES 暗号処理回路は、暗号化と復号の両方が実行可能であり、SSL や TLS といった世界標準の通信方式に最も適した構成となっています。



図：数表現変換による新しい暗号演算圧縮技術

■ 今後の予定 ■

今回開発した暗号処理技術を実際のシステムに搭載して実証実験を行うとともに他の暗号アルゴリズムへの応用を進める予定です。また、実用化に向けて、多様な攻撃に対する

耐性を考慮した構成を検討します。将来的には、当該暗号処理技術を通して、さまざまなIoT向け情報通信機器の安全性向上に貢献することを目指しています。

■ 発表論文 ■

Rei Ueno; Sumio Morioka; Naofumi Homma; Takafumi Aoki, “A High Throughput/Gate AES Hardware Architecture by Compressing Encryption and Decryption Datapaths - Toward Efficient CBC-Mode Implementation,” Conference on Cryptographic Hardware and Embedded Systems 2016.