2019 年 9 月 20 日
株式会社日立製作所
ルーベンカトリック大学

重要インフラを支える IoT システム向けに開発した メッセージ認証技術「Chaskey」が軽量暗号国際標準 ISO/IEC に採択

標準的に利用されている暗号化技術に比べ、少ないメモリで高速処理を実現

株式会社日立製作所(執行役社長兼 CEO:東原 敏昭／以下、日立)とルーベンカトリック大学(Katholieke Universiteit Leuven、学長: Luc Sels)が共同で開発した、センサーやコントローラーなどの小型 IoT 機器向けメッセージ認証技術「Chaskey」が、ISO(International Organization for Standardization、国際標準化機構)での最終承認を経て、このたび、軽量暗号国際標準規格 ISO/IEC*1 29192-6 として採択されました。標準化は国立研究開発法人産業技術総合研究所(理事長:中鉢 良治／以下、産総研)協力のもと行われました。Chaskey は標準的に利用されている暗号化技術よりも少ないメモリで高速処理を実現します。本規格により、重要インフラや車載システムを支える小型機器に基本的なセキュリティ機能の導入が容易となることから、システムの安全性が向上することが期待されます。

IoT 技術の発展により、さまざまな機器がインターネットに接続され、情報を得られることで利便性が向上する一方で、情報漏えい防止やプライバシー保護などのセキュリティ管理の必要性が一層高まってきています。ISO では、従来の暗号標準規格に加え、小型 IoT 機器向けに軽量暗号の規格 ISO/IEC 29192 の策定を進めており、日本でも軽量暗号技術の開発や標準化に向けた検討が行われています。 IoT システムを安全かつリアルタイムに運用するためには、機器を制御する命令や判断の材料となるセンサー情報が改ざんされていないことをスピーディに保証する必要がありますが、小型 IoT 機器は情報処理を行うメモリなどのリソースが少ないため、暗号処理の省メモリ性と高速性の両立が課題でした。そこで、日立とルーベンカトリック大学は、小型 IoT 機器のデータが改ざんされていないことを、標準的に利用されている暗号化技術に比べ、1/2～1/5 の少ないメモリで、2～7 倍の高速で保証することができる Chaskey を開発し、このたび、軽量暗号国際標準として採択されました。Chaskey の特長は以下の通りです。

1. 多様な CPU での高速性を実現するパラメータの選定技術

Chaskey では、CPU で実装されている基本命令のみでデータ変換を行う ARX 設計法*2 を採用しました。ARX 設計法を使う方式は、表参照を行わないためメモリ使用量が小さく、また、特定のレジスタ幅の CPU において高速性を発揮します。さらに、Chaskey では、小型 IoT 機器で使用されている 8～32 ビット CPU で高速な処理を実現するため、パラメータの選定に着目しました。ARX 設計法では、従来、適したパラメータの選定に時間がかかっていましたが、ルーベンカトリック大学が開発した評価ツールにより、短時間で適したパラメータを選定することができ、小型 IoT 機器で使用されている 8～32 ビット CPU でも、省メモリで高速な処理を実現することができました。

2. IoT データ処理に適した構成法の組み合わせ技術

IoT システムでは制御コマンドやセンサデータなど、小さいサイズのデータを高速に処理することが求められます。暗号処理では、事前に秘密鍵を展開する初期化処理が必要ですが、複数の IoT 機器が相互に通信するシステムでは、頻繁に初期化処理が発生し処理速度が低下する恐れがあります。Chaskey は初期化処理のコストを最小限に抑える Even-Mansour 構成法を採用することで、小さいサイズのデータでの高速処理を実現しました。また、Even-Mansour 構成法は本来ブロック暗号を作る方法ですが、さらにメッセージ認証機能を実現する用法(mode of operation)を開発し、その安全性を理論的に検証しました。

今後、日立とルーベンカトリック大学は、Chaskey をはじめとする暗号技術の製品への適用など、安全なネットワーク社会を実現する技術の研究に継続して取り組み、重要インフラのセキュリティを向上させることで、安全安心な社会の実現に貢献していきます。

*1 IEC (International Electrotechnical Commission): 国際電気標準会議

*2 ARX (Addition-Rotation-XORing)設計法: 多くの CPU で実装されている算術加算、(巡回)シフト演算、論理演算だけで処理を構成する設計法。

■照会先

株式会社日立製作所 研究開発グループ
問い合わせフォーム: https://www8.hitachi.co.jp/inquiry/hqrd/news/jp/form.jsp

以上