Focus on the News

IoT向けメッセージ認証技術LightMACがISO標準に採択

NTTは，ルーベンカトリック大学およびデンマーク工科大学と共同で，農業分野やヘルスケア分野およびスマートハウスなどにおける小型機器向けのメッセージ認証技術「LightMAC」を開発して標準化を推進してきました．このたび，LightMACが軽量暗号技術に関する国際標準規格ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission）29192-6に採録され出版されました．本技術をIoTシステムの小型機器であるセンサや制御装置に適用することにより，例えば農業分野における栽培管理や収穫予測などを実現するIoTプラットフォーム全体の安全性を向上させたり，またスマートハウス全体のセキュリティを堅牢にしたりすることができます．

■背　景

IoT機器がインターネットに接続されることで利便性が向上する一方で，IoT機器のなりすましによるセキュリティリスクが増大します．IoTシステムを安全に運用するには，機器を制御する命令や，その判断の材料となるセンサ情報が改ざんされていないことが特に重要です．そこでNTTは，軽量暗号技術の1つとして，制御信号やセンサデータが改ざんされていないことを保証するメッセージ認証技術の開発に取り組んできました．軽量暗号技術とは，従来の暗号技術に比べ，メモリやCPUなどの情報処理リソースが限られた環境により適している暗号アルゴリズムのことです．

■LightMACの特長

従来のメッセージ認証技術では，ブロック長の短い軽量ブロック暗号を利用した場合，大きなデータを処理すると安全性が低下してしまうという課題がありました．LightMACは，ブロック暗号に対して独特の繰り返し方法を用いることにより，この課題を解決しました．これによりLightMACは既存の軽量ブロック暗号の実装を有効活用しつつ必要な安全性を確保することができます．

◆問い合わせ先
NTTサービスイノベーション総合研究所
企画広報担当
TEL　046-859-2032　　E-mail　randd-ml@hco.ntt.co.jp
URL　https://www.ntt.co.jp/news2019/1910/191004a.html

暗号の基礎研究では国際標準化と国際コラボレーションが重要

研究者紹介

安田　幹
NTTセキュアプラットフォーム研究所　データセキュリティプロジェクト　セキュリティ基盤研究グループ

私は入社して以来，共通鍵暗号技術の研究開発に携わってきました．共通鍵暗号技術が達成する機能には，大きく「暗号」と「認証」の2つがあります．今回の技術は後者の「認証」にあたるもので，省リソース環境においても，データが改ざんされていないか，データは正しい相手が作成したものか，安全性レベルを落とさずに検証することができます．今後，IoT機器の爆発的な増加が見込まれる中，今回の標準規格化をきっかけに本技術が普及し，安心・安全なネットワークとなっていくことを期待しています．暗号の基礎研究では，良いアルゴリズムを開発しただけでは，世の中で広く使ってもらえるようにはなりません．コンテストで勝利したり，国際標準に採録されたりすることが必要です．これらの活動はアルゴリズムを開発した研究者本人が行うことが多く，基礎研究とはまた違った面白さがあります．

また，暗号アルゴリズムの研究開発もグローバル化が進み，国際的なコラボレーションが不可欠になってきました．本アルゴリズムもベルギーのルーベンカトリック大学とデンマーク工科大学との共同開発によるものです．私がルーベンカトリック大学に留学し，そのときに出会った大学院生が，その後にNTT研究所にインターンとして来日し，彼の滞在期間中に本アルゴリズムが開発されました．このような共同研究の形態がどんどん増えつつあり，NTT研究所における暗号の基礎研究は，ますます活気付いています．今後も次々に新しい暗号アルゴリズムを世に出していき，安心・安全な社会の実現に貢献したいと考えています．