東北大学
TOHOKU UNIVERSITY

Press Release

令和 2 年 9 月 17 日

報道機関　各位

東北大学電気通信研究所

ハードウェア“指紋”認証の新方式を開発

世界最高効率を達成、より多様な情報通信機器への搭載が可能に

【発表のポイント】

- ハードウェアの“指紋”（固有の乱数値を出力する機能）を用いてハードウェアの正当性を認証する新方式を開発。
- ハードウェア認証技術は、ハードウェアの流用や偽造、不正な改ざんを防ぐ技術として、近年重要性が高まっている。
- 開発した新方式では、質の悪い（安全性の低い）“指紋”であっても質の良い（安全性の高い）“指紋”に効率的に変換して認証する。これにより、多様な“指紋”への適用が可能となり、長期間の運用にも耐える認証を実現する。
- その上、世界最高の変換・認証効率により、従来比で半分以下のコストで実現できる。
- 上記特長から今後様々な情報通信機器の認証技術として広く利用が期待される。

【概要】

近年注目を集める「モノのインターネット（IoT）」など次世代のネットワーク・サービスでは、ハードウェアの不正な流用、偽造、改ざんによる脅威が危惧されている。東北大学電気通信研究所の本間尚文教授、上野嶺助教の研究グループは、こうした脅威に対抗するハードウェア認証技術として、ハードウェアの“指紋”（固有の乱数値を出力する機能）を利用した認証の新方式を開発した。

本技術により、多様な“指紋”の認証が可能となり、実現コストの大幅な削減（従来比半分以下）が達成されることから、これまで搭載が困難であった情報通信機器への利用拡大が期待される。

【問い合わせ先】
東北大学電気通信研究所
担当：助教　上野嶺、 教授　本間尚文
電話：022-217-5506
E-mail：ecsis-lab@riec.tohoku.ac.jp

研究

【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おり、そのような情報をサイバー攻撃から守る技術が不可欠となっている。特に、近年注目を集めるモノのインターネット（IoT: Internet of Things）やサイバーフィジカルシステム（CPS: Cyber-Physical System）などの次世代のネットワーク・サービスでは、無数の機器がネットワークに接続されることから、ハードウェアの流用や偽造、不正な改ざんを伴う悪意ある攻撃を防ぐため接続機器（ハードウェア）の真贋判定（認証）が強く求められている。しかし、IoT 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、それらの認証をいかに効率的に行うかが課題となっていた。加えて、近年増加している模造・偽造半導体チップの対策も課題となっていた。そうした課題を解決する有望な技術として、ハードウェアの指紋とも呼ばれる固有の乱数値を出力する機能（PUF: Physically Unclonable Function）*を利用したハードウェア認証がある。しかし、PUF は制御不能なハードウェアの微小な違いを利用することから一般に不安定・非効率であり、安定かつ効率的に PUF を使いこなす手法が必要とされていた。

【開発の経緯】

国立大学法人東北大学電気通信研究所環境調和型セキュア情報システム研究室（本間研究室）は、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、これまで搭載されていなかった小型機器・センサにもハードウェア認証技術を搭載するための技術開発を行ってきた。なお、今回の研究開発は、科学研究費補助金（No. 17H00729 および No. 20K19765）の研究開発の一環として行われた。

【開発した内容】

今回確立した PUF を用いたハードウェア認証技術では、棄却サンプリング**に基づく手法を用いることで、2 進数で表される PUF 出力の偏り（0 と 1 の割合）を効率的に解消することに成功した（図 1）。これにより PUF 出力の偏りに伴う安全性の低下を防ぎ、様々な PUF を安心して使用すること

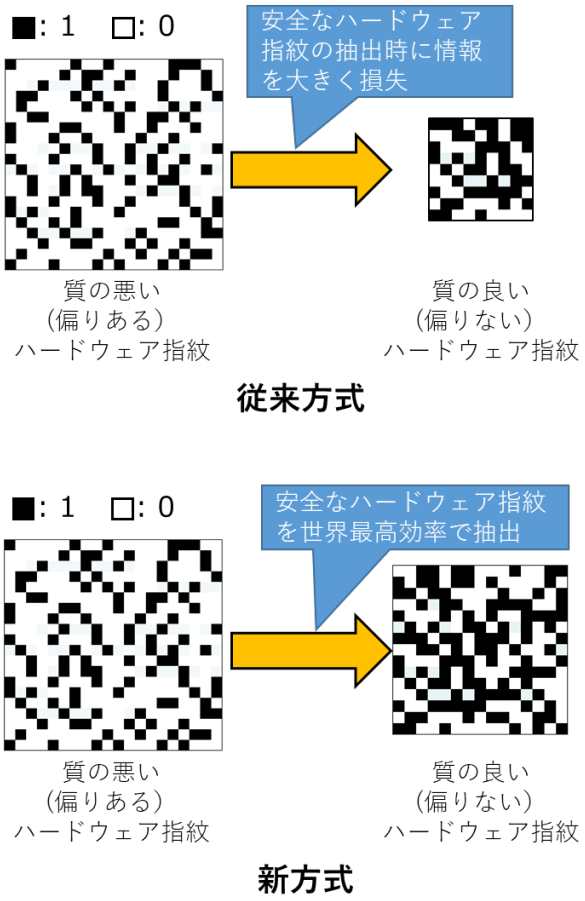

図 1：開発した新方式の概要（効率的にハードウェア指紋の生成が可能に）

が可能となった。また、従来手法と比べて実装コストをこれまでの半分以下（最大で 55%削減）に抑えることが可能となり、これまでハードウェア認証が搭載されていなかったセンサや超小型情報通信機器への適用が期待される（図 2）。

なお、本成果は、令和 2 年 9 月 16 日にオンラインで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 ）で発表された。

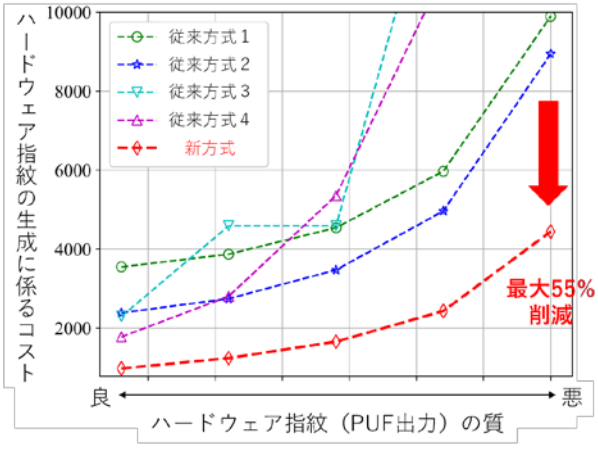

図 2：新方式の効果（従来方式の適用が困難な場合でも安全な認証が可能）

【今後の予定】

今回開発したハードウェア認証技術を実際のシステムに搭載して実証実験をさらに実施するとともに新規のデバイスへの応用を進める。将来的には、当該ハードウェア認証技術を通して、さまざまな IoT 向け情報通信機器およびそれらを用いたシステム全体の安全性向上に貢献することを目指している。

【発表論文】

Rei Ueno, Kohei Kazumori, and Naofumi Homma, “Rejection Sampling Schemes for Extracting Uniform Distribution from Biased PUFs,” IACR Transactions on Cryptographic Hardware and Embedded Systems, DOI: 10.13154/tches.v2020.i4.86-128, Vol. 2020, Issue 4, pp. 86–128, August 2020.

【用語解説】

*PUF：Physically Unclonable Function（物理複製困難関数）の略。半導体チップの物理的な個体差（ばらつき）を利用して、チップ固有の出力を得る回路技術。複製が困難なため半導体チップの個体認証技術として期待されており、一部は実用化されている。

**棄却サンプリング：ある想定した分布に従う乱数値を生成する（サンプリングする）方法。ここでは、0 と 1 が等確率で出現する乱数値を生成するために使用する。