

## 東北大学、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

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。

### 【開発背景】

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）。

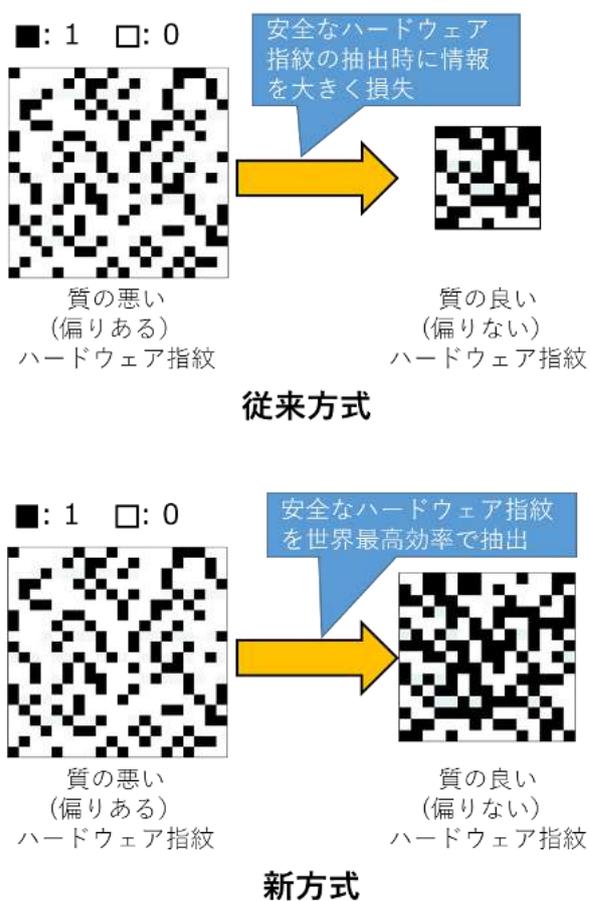


図 1：開発した新方式の概要（効率的にハードウェア指紋の生成が可能に）

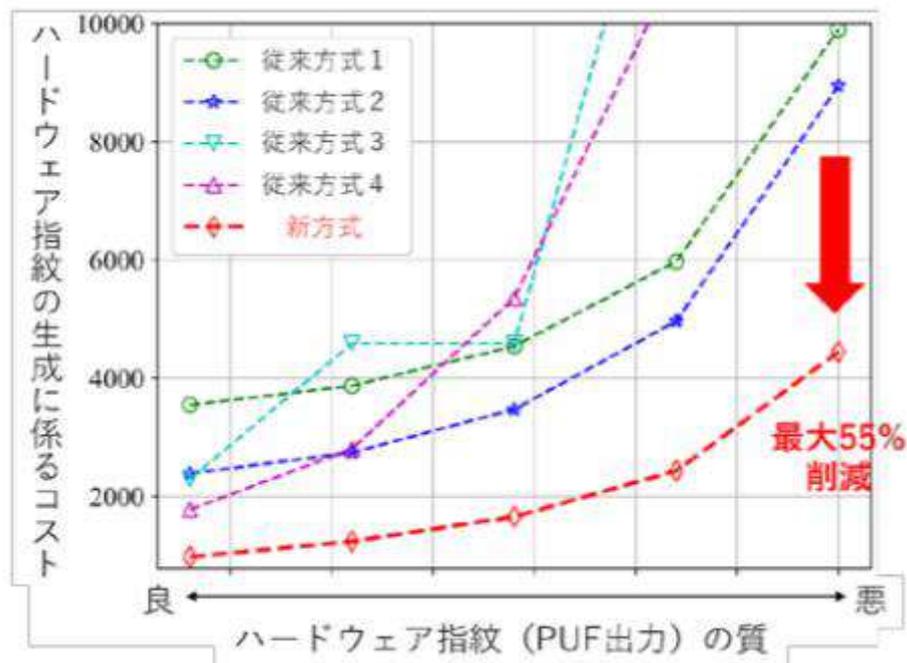


図 2：新方式の効果（従来方式の適用が困難な場合でも安全な認証が可能）

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み込みシステムに関する国際会議）で発表された。これからは、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。

### 論文情報

タイトル: Rejection Sampling Schemes for Extracting Uniform Distribution from Biased PUFs,

雑誌: IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2020, Issue 4, pp. 86-128, August 2020.

DOI: 10.13154/tches.v2020.i4.86-128

### 研究成果発表資料

<https://www.tohoku.ac.jp/japanese/2020/09/press20200917-02-hardware.html>

編訳 JST 客観日本編集部

