配布先：総務省記者クラブ、テレコム記者会、情報通信記者会、文部科学記者会、
立川市政記者クラブ

平成25年1月15日
独立行政法人情報通信研究機構
国立大学法人電気通信大学
株式会社東芝

M2M 向け暗号・認証 IC チップの安全性を実証

～「チップの指紋」[*1]を利用し、安全性を保ちながら実装コストを削減 ～

独立行政法人情報通信研究機構（以下「NICT」、理事長：宮原 秀夫）は、国立大学法人電気通信大学（学長：梶谷 誠）、株式会社東芝（代表執行役社長：佐々木 則夫）と共同で、暗号・認証に用いる秘密情報を物理的攻撃[*2]から保護する専用記憶回路を持たない機器において秘密情報を秘匿管理する技術について、統計学的評価に必要な大規模の実証システムを構築し、その安全性を世界で初めて[*3]実証しました。

今後、環境条件を考慮しながら機器の動作範囲を広げる研究開発を重ねることで、各機器を低コストで製造しなければならない M2M（Machine-to-Machine）通信[*4]やサイバーフィジカルシステム[*5]などにおいても、安全な暗号・認証が実現可能となります。

【背景】

現代の情報システムには、情報セキュリティの観点から様々な暗号技術が用いられています。従来、IC チップを用いて暗号・認証を行うためには、それらの機能を実現する暗号演算回路と共に、認証に必要な秘密情報を漏えいから守る回路を実装する必要がありました。この秘密情報を守る回路は、様々な物理的攻撃を考慮する必要があるため、これまで IC カードなどの製造コストを押し上げる要因となっていました。

特に、近年活発となっている M2M と呼ばれる機器間の通信では、機器のコストが PC に比べて非常に低価格であることが求められています。このような機器に対して安全な暗号・認証技術を実装することは、IC チップのコスト及び物理的な実装規模（半導体の数）の制約により困難でした。そこで、より低コストで暗号・認証機能を実装することのできる IC チップの実現技術の確立と、その安全性の実証が求められていました。

【今回の成果】

今回、我々は、個々の IC チップの物理的特性の違いである「チップの指紋」[*1]を同一の評価環境に 2 種類実装し、「チップの指紋」[*1]を利用して秘密情報を秘匿管理する技術“PMKG-RT”[*6]の実証を行いました。これまで、この技術については統計学的評価に十分な数の IC チップを用いた実証が行われたことはありませんでしたが、今回、統計学的に意味のある規模の IC チップ数を用いた大規模実験を行い、統計学的にその安全性を世界で初めて[*3]実証しました。

本成果により、M2M、センサーネットワーク、サイバーフィジカルシステムなど、各機器を低コストで製造しなければならない場面においても、安全なシステムを構築できることが期待されます。

本実証における評価環境

【今後の展望】

今後、さらに、温度や湿度など幅広い物理的条件を変化させた場合の安全性を評価するための実証実験を行い、機器の動作範囲を広げる研究開発を実施してまいります。

なお、本成果について、平成 25 年 1 月 22 日（火）～25 日（金）に、京都で開催される「2013 年暗号と情報セキュリティシンポジウム（SCIS2013）」で発表します<http://www.iwsec.org/scis/2013/index.html>。

以 上

＜ 本件に関する 問い合わせ先 ＞
NICT ネットワークセキュリティ研究所セキュリティアーキテクチャ研究室 松尾 真一郎 Tel: 042-327-5782, E-mail: smatsuo@nict.go.jp
国立大学法人電気通信大学 大学院情報理工学研究科 﨑山 一男 Tel: 042-443-5767, E-mail: sakiyama@uec.ac.jp

＜ 取材依頼及び広報 問い合わせ先 ＞
NICT 広報部 報道担当 廣田 幸子 Tel: 042-327-6923, E-mail: publicity@nict.go.jp
国立大学法人電気通信大学 広報担当 井田、和田 Tel: 042-443-5019, E-mail: kouhou-k@office.uec.ac.jp
株式会社東芝 広報室広報担当 槻本、古宮、福岡 Tel: 03-3457-2100

＜用語 解説＞

***1 「チップの指紋」**
製造時の環境要因により生じるチップ固有の物理的特性。同一の設計であっても、正常に動作する範囲内でチップ固有の物理的特性が変動する。

***2 物理的攻撃**
物理的なICチップの電力消費、処理時間及び回路上の情報を取得することにより、暗号・認証に必要な秘密情報を取得しようとする攻撃

***3 世界で初めて**
同一の評価環境に2種類の「チップの指紋」[*1]を実装し、「チップの指紋」[*1]を利用して秘密情報を秘匿管理する技術“PMKG-RT”[*6]の安全性評価を行う実証実験において（2013年1月15日現在）

***4 M2M（Machine-to-Machine）通信**
人間による意図的操作を介さずに、ネットワーク上につながれた電子機器が相互に情報交換を自動的に行う通信システム

***5 サイバーフィジカルシステム**
実世界の様々な情報をセンサなどにより、ネットワーク上の計算リソースと組み合わせ、より高度な社会を実現するシステム

***6 “PMKG-RT”**（Pattern Matching Key Generation with RoTation）
電気通信大学と東芝が共同開発した、「IC チップの指紋」を利用して秘密情報を秘匿管理する技術。IC チップの固有値（指紋）と秘密情報の演算結果を秘匿することなく、低コストで管理し、演算結果とICチップの固有値から秘密情報を復元して利用する技術

＜以下、補足資料の用語解説＞

***7 耐タンパ性**
暗号・認証を行うICチップに対して物理的攻撃が行われたとしても、秘密情報を保護することができる性質

***8 物理的複製困難関数（PUF）**
Physically Unclonable Function。装置固有の物理的特性を利用して、同一の入力から装置固有の異なる出力を導く技術。バイオメトリクスに対比して、人工物メトリクスとも呼ばれる。

***9 バイオメトリクス認証**
指紋、静脈や虹彩など、一人一人で異なる特徴を持つ要素を利用して、人間の認証を行う技術

***10 SRAM**
広く使われている書換え可能な半導体メモリの一種で、電力供給がされている間のみ情報を記録可能なメモリ

***11 2線式回路**
均一となるように設計された2つの経路（配線）を利用して、同一の情報を伝達する回路

***12 Arbiter-PUF**
2線式回路製造時の環境要因に依存し、2つの配線容量（電気抵抗）が装置ごとにばらつくことを利用して、装置固有の出力を導く技術

***13 FPGA**（Field Programmable Gate Array）
論理回路の構成を製造後に設定することで、利用者が任意の論理機能を実装できる集積回路

***14 不揮発性メモリ**
電源が供給されない状態においても、書き込まれたデータを保持するように製造されたメモリ

***15 パターン照合**
2つの値の類似度を判定する方法。固有の機器でも試行ごとにPUFから出力される値には誤差が生じるため、あらかじめ定めた誤差を許容し、2つの値が同一の入力に対して固有の機器が出力した値であるかを判定する。

＜各機関の主な役割分担＞

○NICT: 安全性評価手法の構築、測定結果の分析及び100個のICチップを利用した評価環境の提供を実施

○**電気通信大学**: 評価環境の構築、秘密鍵を管理する方法の実装及び実験データの収集を実施

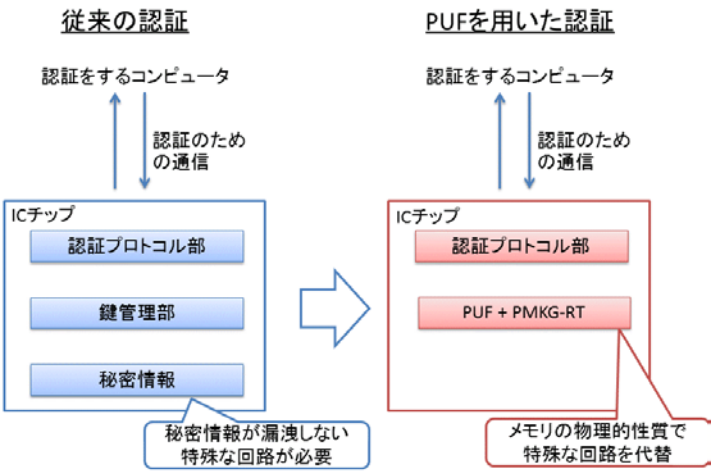
○**東芝**: 秘密情報を管理する方法の実装支援及び安全性評価支援を実施

補足資料

【暗号・認証技術の現状】

現代の情報システムでは秘密情報を扱う場面が非常に多くなっています。そのため、様々な暗号・認証技術を利用して情報セキュリティを十分に確保する必要があります。現在広く使われている暗号・認証技術の多くは、十分な演算処理能力を持つサーバやパソコンでの動作を想定して設計されています。

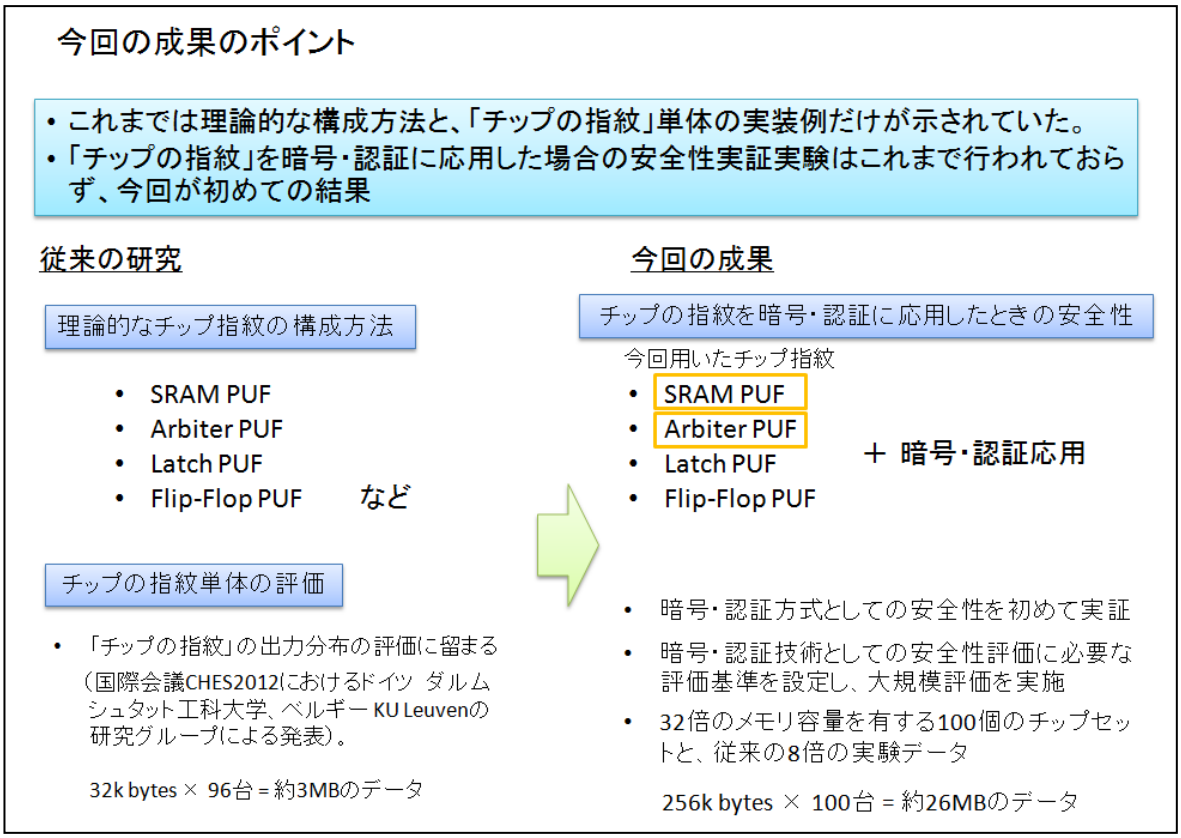
しかし、近年スマートメーターやセンサなど、サーバやパソコンに比べて処理能力の低い機器がネットワークに接続される、M2M やサイバーフィジカルシステムと呼ばれる通信形態が注目を浴び、新たなサービスが実現されています。このようなサービスでは、大量の機器が必要であることから、一つ一つの機器は安価に製造する必要があります。NICT、電気通信大学及び東芝は、このような機器においても十分な安全性を有する暗号・認証技術についての共同研究を行ってきました。



従来の認証と PUF を用いた認証の実装コストの違い

一般的に、暗号・認証技術をハードウェアで実現するためには、(1)暗号・認証のための演算を行う回路及び(2)暗号・認証に必要な秘密情報が漏えいしないように管理する回路(鍵管理部)が必要です。このうち、(2)鍵管理部は、様々な物理的な手段によって秘密情報を取得しようという攻撃に耐性を持たせる耐タンパ性[*7] が必要であり、現在広く使われている IC カード等で利用される IC チップにも、この回路が実装されています。一方で、この鍵管理部の設計・製造コストは、IC チップの製造コストを押し上げる要因となっており、個々の機器を大量かつ安価に製造しなければならないサービスの普及の妨げとなっていました。

近年、この鍵管理部をチップの物理的な個体差を用いて代替する「物理的複製困難関数(PUF)[*8]」という技術が登場しています。この技術は、個々人で異なる人間の指紋を利用してバイオメトリクス認証[*9] を実現するのと同様に、個々の IC チップの物理的特性を指紋のように利用して暗号・認証機能を実現します。PUF は、PUF として使用する IC チップの物理的特徴を取り出して複製することが困難であるため、これまで必要だった鍵管理部は不要となり、コスト面で大きなメリットがあります。一方で、IC チップの個体差が持つ安全性は、バイオメトリクス認証と同様に、統計学的に証明する必要があります。これまで、PUF は、理論的な構成方法の研究が中心であり、複数の PUF やその応用を実際の IC チップで実現した際の安全性を統計学的に有意な量のサンプルを用いて評価した例はありませんでした。



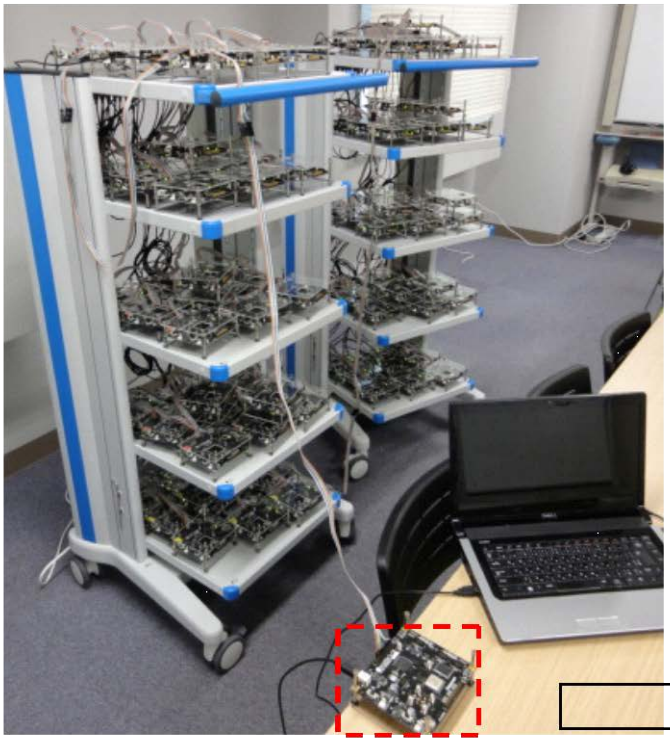
【今回の実証実験の内容】

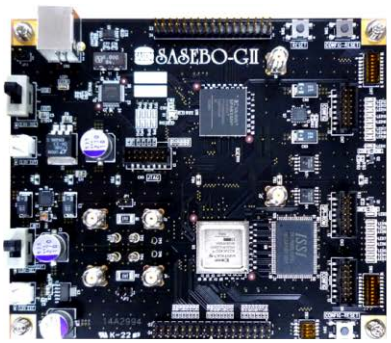
今回の研究成果は、NICT が保有する 100 台の IC チップ用の実験機器を用いて、一般的なメモリ用 IC である SRAM[*10] のみを利用する SRAM-PUF と、2 線式回路[*11] を実装した Arbiter-PUF[*12] に対して、世界で初めて統計学的に意味のある規模で、PUF を用いる鍵管理方式の安全性を実証したものになります。この結果、鍵管理部が存在しない IC チップでも、低コストで暗号・認証が実現できることが実証されました。

今回の実証実験では、NICT が所有する 100 台の実験機器に、電気通信大学と東芝が共同開発した鍵管理方式 PMKG-RT を実装し、安全に暗号鍵の生成・管理が行える制御パラメータを実験的に算出しました。今回は、PMKG-RT のコア技術である PUF 回路として、電力投入時のメモリ上のデータばらつきを利用する SRAM-PUF 及び FPGA[*13] 上に 2 線式回路を実装した Arbiter-PUF を利用しました。

PMKG-RT は、秘密情報を不揮発性メモリ[*14] に記憶しない代わりに、PUF を用いて暗号・認証時に必要となる鍵を一時的に生成します。実験では、SRAM-PUF と Arbiter-PUF のそれぞれについて、PUF を実装した異なる 100 台の機器に同一のデータを入力したときに、固有の機器でも試行ごとに PUF から出力される情報は誤差が生じて異なること及び出力に機器ごとの差異があることを確認しました。PMKG-RT は、初期設定において、鍵をランダムに選択し、PUF の出力を鍵の値だけ巡回シフトした値を、耐タンパ性を必要としない不揮発性メモリに記憶します。そして、PMKG-RT は、暗号・認証時に鍵が必要となる場面において、PUF の出力を 1 ビットずつ巡回シフトし、不揮発性メモリに記憶された値とのパターン照合[*15] に合格するシフト量を探索することで鍵を再現します。また、1回の巡回シフトとパターン照合により管理できる鍵はビット長が短いため、PMKG-RT は、巡回シフトとパターン照合を繰り返すことで、安全な暗号・認証を実現するための暗号鍵を管理します。今回は、PUF の出力を 256 ビットと定め、出力誤差の許容範囲を 10 ビット刻みで設定して実験を繰り返した結果、Arbiter-PUF を用いる場合は 30 から 40 ビット、SRAM-PUF を用いる場合では 50 から 70 ビットの出力誤差を許容し、PMKG-RT が機器固有の暗号鍵を正しく生成・管理できることを確認しました。

上記の結果より、SRAM-PUF や Arbiter-PUF を構成し、鍵管理を安全に行うために PUF を利用する方法（制御回路の設定）を導出し、暗号応用への実用性を示すことができました。





IC チップを再現した評価ボード

本実証における評価環境（IC チップ 100 個による並行処理）