（開発 No.1504）

2015 年 2 月 5 日
三菱電機株式会社
立命館大学
独立行政法人 科学技術振興機構

LSIの個体差から指紋のような固有IDを生成し、組み込み機器の安心・安全に貢献

「IoT時代に向けたセキュリティー技術」を開発

三菱電機株式会社と立命館大学は、あらゆる機器がつながる IoT（Internet of Things：モノのインターネット）時代に向け、製造段階で生じる LSI（大規模集積回路）の個体差を利用して、機器の秘匿と認証を行うセキュリティー技術を開発しました。機器に搭載されるプログラムの保護や機器のなりすまし防止など、機器のネットワーク化に伴うセキュリティーリスクの低減に貢献します。

＜本技術適用の流れ＞

1. 同じ機能を持つ LSI の個体差を利用して固有 ID を生成する。
2. 生成した固有 ID で復号できるようにプログラムを暗号化し、機器に組み込む。
3. プログラムは固有 ID を再生成できる機器でのみ正常に作動する。固有 ID は LSI が動作する間しか生成されないので、ID の解析は難しく、安全に保管できる。

開発の特長

1. LSIの個体差を活用した独自のセキュリティー技術で、機器の安全性を向上

- 同じ機能を持つ LSI の製造段階で生じる個体差を活用し、LSI ごとに指紋のような固有 ID を生成する技術を開発
- 回路が動作する間しか固有 ID が現れないため、ID がチップのメモリー内部には残らず、ID の解析が困難
- プログラムを指定の LSI の固有 ID でしか復号できないように暗号化することで、その LSI を持つ機器でしか使えなくし、機器の安全性を確保
- 特定の固有 ID を持つ機器同士をつなげるように設定も可能

2. 小規模かつ特殊な製造プロセスが不要で様々な LSI に適用可能

- 固有 ID の生成、秘匿と認証に必要な暗号機能を小さな回路面積で内蔵できるため、個別実装に比べて回路の大きさを約 3 分の 1 に削減可能
- 複数の製造プロセスで本技術を適用した LSI の試作を実施し、安定的に ID の生成が可能※
- モジュール化により、一般的な LSI の設計フローで技術適用が可能

※：三菱電機と立命館大学の共同研究

本開発の一部は、独立行政法人 科学技術振興機構（JST）の戦略的創造研究推進事業（CREST）「ディペンダブル VLSI システムの基盤技術」（研究総括 浅井彰二郎）における研究課題「耐タンパディペンダブル VLSI システムの開発・評価」（研究代表者 立命館大学 理工学部 藤野毅教授）での成果です。

開発の概要

	実装形態	安全機能
今回	ID の生成、秘匿と認証に必要な暗号機能を小さな回路面積で LSI に内蔵可能	回路が動作する瞬間以外は ID が現れないため、ID の解析が困難
従来	電源の供給なしに記憶を保持するメモリーに、ID 情報を個別に書き込み	ID 情報がメモリー上に常に残留するため、チップを開封して内部を調べることで ID の解析が可能

今後の展開

2015 年度以降を目標に、本技術を三菱電機の製品に適用予定

開発の背景

ネットワークに接続される組み込み機器が増加する一方で、プログラムの解析・改ざんやデータの奪取、機器のなりすましなどの不正行為に対する対策がますます重要になっています。特に安全性が重要視される組み込み機器において、プログラムやデータの保護について抜けのない対策が必要です。一般的な対策として、機器に内蔵するメモリーに暗号処理を行った ID 情報を格納しますが、機器の電源を切っても ID 情報がメモリー上に残留するため、チップを開封して内部を調べることで ID の解析が可能になるという課題がありました。

当社は今回、同じ機能を持つ LSI の個体差を活用して指紋のような固有 ID を作り、復号時に鍵として用いる新たなセキュリティー技術を開発しました。

特長の詳細

1. LSI の個体差を活用した独自のセキュリティー技術で、機器の安全性を向上

LSI は内部の回路で定められた計算を行うため、同じ回路が入った LSI に同じ入力の計算をさせると同じ計算結果を出力します。しかし、計算結果に至る過程が個体ごとに異なり、この個体差を LSI の指紋に見立て、同じ回路を実装した LSI ごとに固有 ID を作り出すことに成功しました。

固有 ID は、回路を動かした時にしか現れないため、チップを開封して内部を調べても解析することができません。また、指定の LSI の固有 ID 情報でしか復号できないように暗号化されたプログラムやデータは、その LSI を持つ機器でしか使えなくなるため、機器の安全性を確保できます。また、特定の固有 ID を持つ機器同士をつなげるように設定することも可能になります。

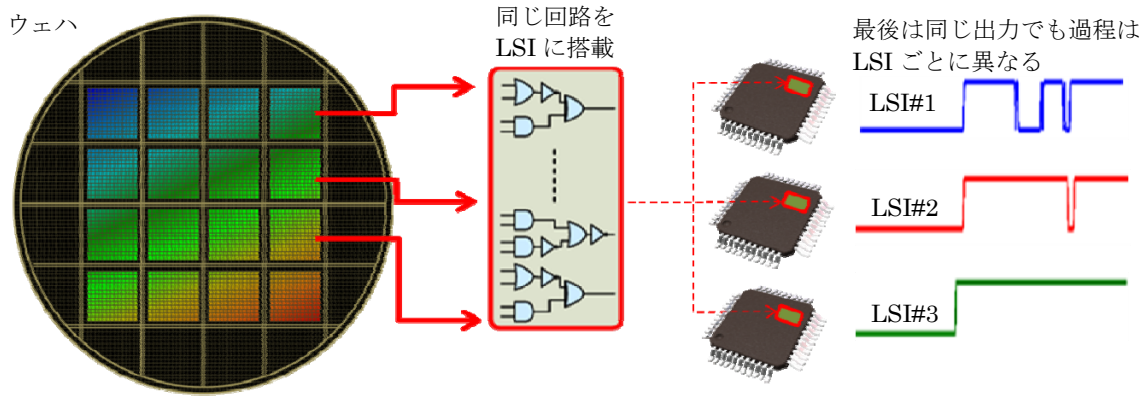

図 1　同じ回路が搭載された LSI に生じる個体差

【固有 ID の生成方法】

①信号を入力すると発生する電圧の上昇する回数を数え、その数が偶数個ならば 0、奇数個ならば 1 のビットを与える。

②入力する信号を変えて繰り返しビットに変換し、指紋のような固有 ID 情報を生成する。

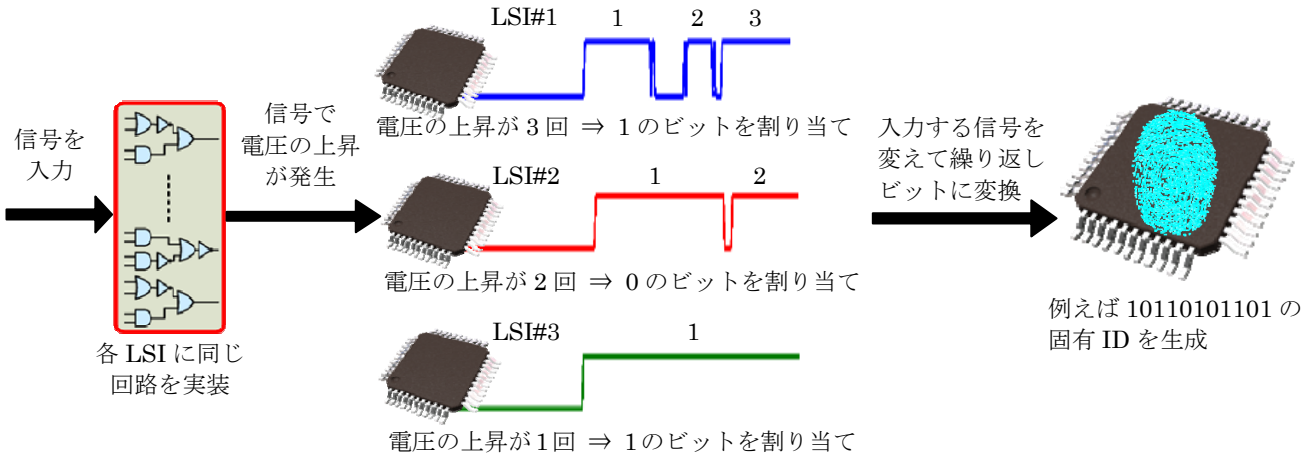

図 2　固有 ID の生成方法

2. 小規模かつ特殊な製造プロセスが不要で様々な LSI に適用可能

固有 ID の生成、秘匿と認証に必要な回路を一部共有化することで、それぞれを個別に実装したときと比べ、回路の大きさを約 3 分の 1 に削減しました。

また、立命館大学と共同で、複数の製造プロセスで本技術を適用した LSI を試作し、安定して固有 ID の生成が可能であることを確認しました。また、本方式はモジュール化することで、組み込むことが容易になり、一般的な LSI の設計フローに適用可能です。

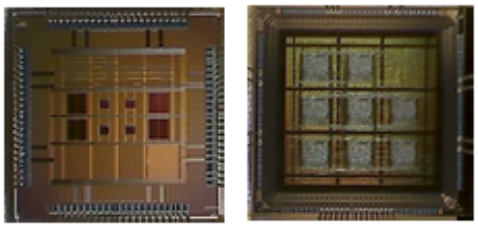

図 3　信号が変化する過程から指紋のような固有 ID を生成する試作 LSI
（左 65nm 2.1mm 角、右 180nm 2.5mm 角）

特許

国内5件　海外32件

お問い合わせ先

＜開発内容に関すること＞
【報道担当】
三菱電機株式会社 広報部
〒100-8310 東京都千代田区丸の内二丁目 7 番 3 号
TEL：03-3218-2359　FAX：03-3218-2431

【開発担当】
三菱電機株式会社　情報技術総合研究所　業務部
〒247-8501　神奈川県鎌倉市大船五丁目 1 番 1 号
FAX：0467-41-2142
http://www. MitsubishiElectric. co. jp/corporate/randd/inquiry/index_it. html

立命館大学 理工学部
教授　藤野 毅
〒525-8577 滋賀県草津市野路東 1 丁目 1 番 1 号
TEL：077-561-5150　FAX：077-561-2663
E-mail：fujino@se. ritsumei. ac. jp

＜JST 事業に関すること＞
松尾 浩司（マツオ コウジ）
科学技術振興機構 戦略研究推進部
〒102-0076 東京都千代田区五番町 7 K's 五番町ビル
TEL：03-3512-3526
FAX：03-3222-2064
E-mail：crest@jst. go. jp