特集論文

IoT機器のLSI個体差を利用したセキュリティ技術

鈴木大輔*

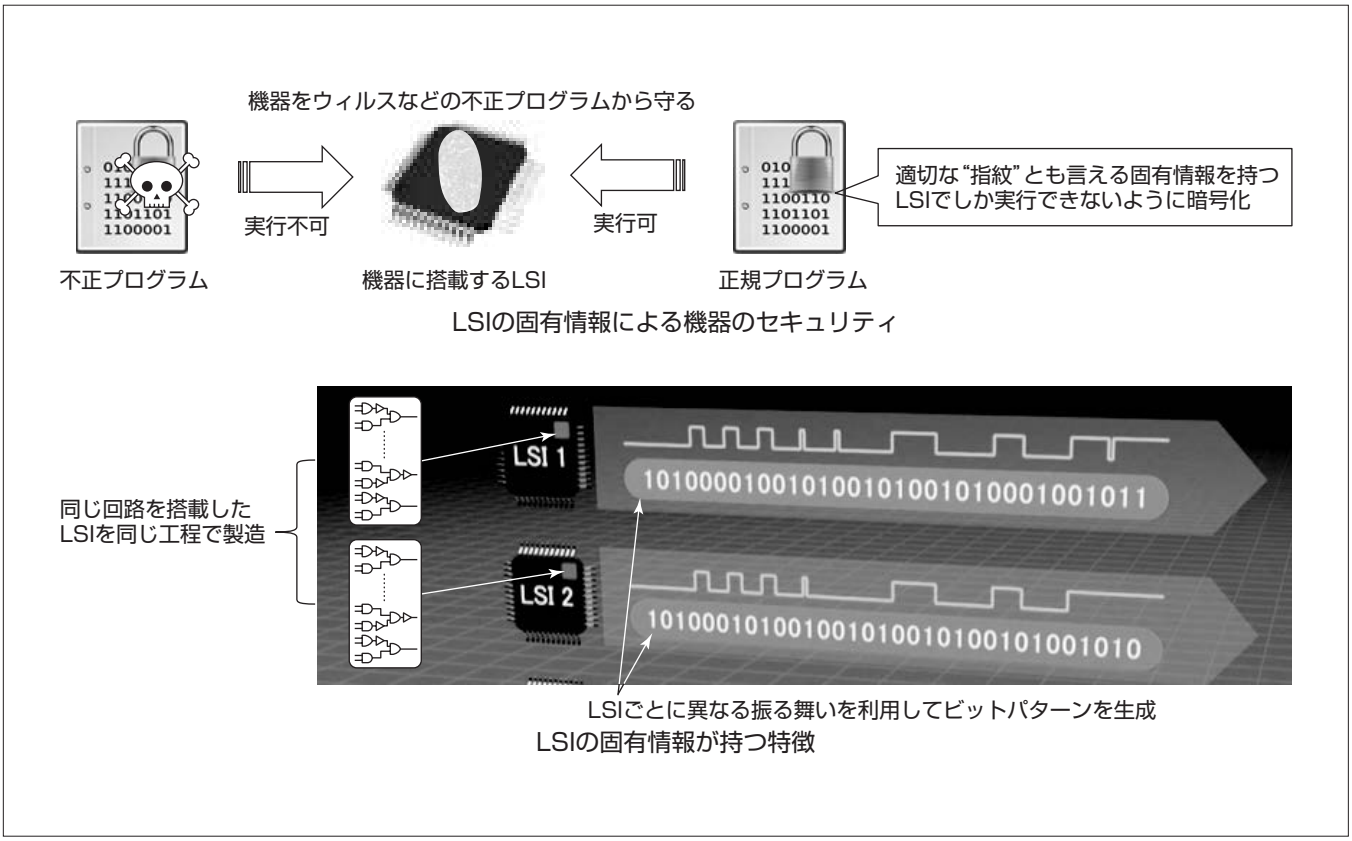
Security Technology by Using Individual Differences of LSIs for IoT Devices

Daisuke Suzuki

要　旨

パソコンなどの情報通信機器だけでなく，あらゆる機器がインターネットを介してつながるIoT（Internet of Things）の普及が本格化して，新しいサービスが次々と生まれる時代が到来している。一方で，これまでつながることを想定していなかった機器には，セキュリティ上の脅威への対策が求められている。特に，IoTが想定するサービスでは自動車を含めた様々なシステムがつながって自動化／無人化されていくため，セキュリティ事故は情報資産にとどまらず直接人命等に関わる可能性がある。現在，IoT機器は多くのセキュリティ課題を持つことで知られているが，その多くは暗号技術など既存のセキュリティ技術で解決することができる。

IoT機器に対して暗号技術を利用してセキュリティ対策を行う際に課題となる鍵管理の問題を解決する技術では，LSI（Large Scale Integration）の製造段階で生じる個体差からLSIの“指紋”とも言える固有情報をビットパターンとして生成することができる。生成された固有情報は回路が動作した瞬間だけ現れるため，LSIを分解・解析されても固有情報が漏れることはない。また，製造段階で生じる個体差から固有情報を生成しているため，回路が複写されても固有情報は複写されないという2つの特長を持つ。この固有情報を，機器で管理したい鍵の保護に利用することで，暗号技術を安心して利用できる。また，この技術を応用した機器認証やLSIの動作環境に関する異常検出が可能となる。



IoT機器への不正プログラム混入防止

不正プログラムの混入防止は，正規プログラムとLSIを暗号技術によって紐（ひも）づけることで実現できる。その際，LSIの指紋とも言える固有情報を利用する。この固有情報は，機器やLSIを分解・解析されても盗み取られないセキュリティを達成している。また，実装が容易なので小規模の回路で実装でき，コストの厳しい組み込み機器に最適である。

*情報技術総合研究所（博士（工学））

1. まえがき

IoTという言葉とともに，これまでネットワークに接続されていない機器がつながることで新しい機能やサービスを実現しようとする動きが活発化している。一般に，IoTのアーキテクチャは，機器(デバイス)，ゲートウェイ，クラウド(サーバ)の3つの構成要素で表現される。このIoTのアーキテクチャでのセキュリティは，それぞれの層で様々な視点から議論されている。例えば，ゲートウェイでは多様な通信プロトコルに対応した暗号化通信，クラウドでは集めた情報のプライバシー保護などが挙げられる。

本稿では，より多くの課題を抱えるIoT機器のセキュリティに焦点を当てる。

2. IoT機器のセキュリティ課題

ヒューレット・パッカード社が行ったIoT機器に対するセキュリティ調査[(1)]で，多くの機器がセキュリティ対策を実施していないことが示された。これら課題の多くは，暗号技術を含む既存の技術で解決することができる。例えば，機器内でのパスワード管理は，暗号アルゴリズムで平文での管理を避けることができる。ファームウェアの更新は暗号化とデジタル署名でリバースエンジニアリングや悪意ある改ざんから守ることが可能であり，通信路の保護についても同様である。典型的な例として，**図1**にゲートウェイと通信する機器に対してゲートウェイが認証を行うケースを示す。**図1**はISO/IEC(International Electrotechnical Commission)9798-2をベースとした単純な認証プロトコルで機器を認証するフローを表している。ゲートウェイと機器が認証鍵を事前に共有している点がポイントであり，認証鍵を持たない機器は接続させないという機能を実現できる。

暗号技術を利用する際の課題として，鍵管理の問題が挙げられる。暗号を含むセキュリティプロトコルをセキュアに利用する前提として，秘密情報である鍵情報は安全に管理される必要があり，**図1**の例では認証鍵を盗まれないようにどのように管理できるかという問題である。一方で，実施可能な管理方法は機器の構成や実装に依存するため，場合によっては秘密情報を奪取されるリスクが残る。

そこで，機器の最小構成要素であるLSI内で安全に鍵を管理するための技術として“グリッチPUF(Physically Unclonable Function)”と呼ぶ技術を開発した。この技術では，LSIの製造段階で生じる個体差からLSIの“指紋”とも言える固有の情報を生成することができる。この情報は，LSIを分解・解析されても盗まれることはないため，装置の鍵管理の安全性を飛躍的に向上させることができる。さらに，IoTのセキュリティとして不可欠な機器の認証に用いる乱数生成や暗号化などの機能や，LSIの動作環境の異常を検出する機能をグリッチPUFの応用で実現した。

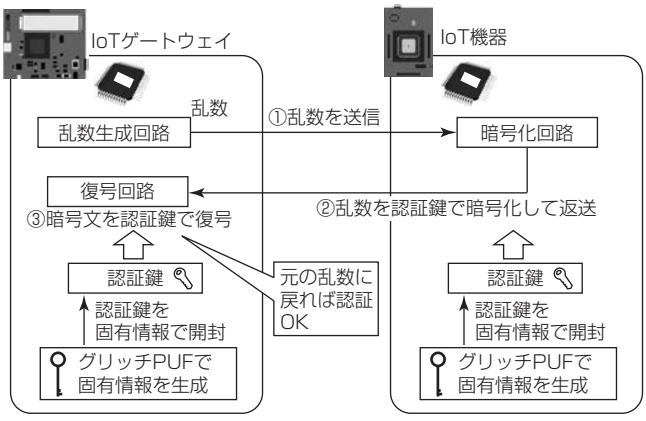


図1．暗号技術を用いた機器認証

3. IoTを支えるセキュリティ技術

3.1 グリッチPUF

PUFはLSIに代表される個々の人工物が持つ物理的な特徴量に応じて，与えられた入力に対して出力を返すように設計されたセキュリティモジュールの総称である。その人工物が持つ製造ばらつきを特徴量に利用することで，同じ特徴量の人工物の複製が困難である根拠としている。論理回路を構成する各ゲートの遅延ばらつきを特徴量として，その入出力信号間の遅延関係から発生するグリッチと呼ばれる現象を利用したPUFの構成法“グリッチPUF”を開発した[(2)]。

次に，**図2**に示す簡単な論理回路でその原理を述べる。**図2**のような複数の入力信号に対してANDやXORなどの論理演算を行う回路では，各信号の遅延差によってグリッチと呼ばれる信号の過渡遷移が発生する。**図2**で入力信号(x_1，x_2，x_3)が全て0から1に変化する場合，x_1，x_2の信号変化の時間差でまずXORゲートの出力に凸状のグリッ

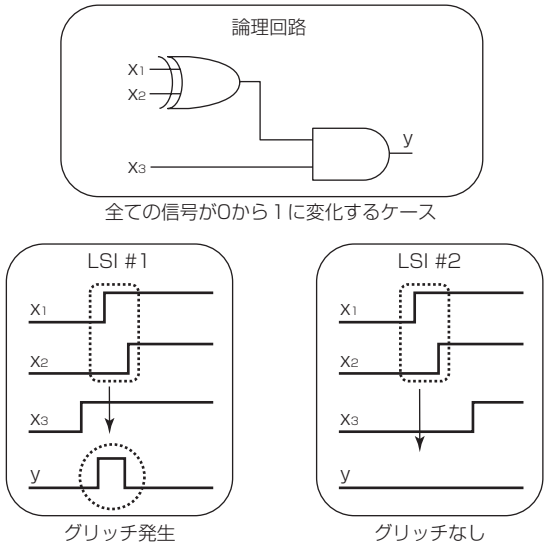


図2．遅延の違いによるグリッチの有無

チが発生する。次に，x_3の変化がこのグリッチよりも早くANDゲートに到達すれば，グリッチはANDゲートの出力に伝播(でんぱ)する。逆に，x_3の変化がこのグリッチよりも遅くANDゲートに到達すれば，グリッチはANDゲートの出力には伝播しない。すなわち，遅延の違いでグリッチの有無が異なる。この現象を利用して，**図2**よりも複雑な回路のグリッチを用いてLSIごとに固有の情報を生成する。**図3**に固有情報を生成するフローを示す。**図3**に示すように，各LSIに実装された同じ回路に信号を入力して，その際に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のビットを与える処理を行う。さらに，入力する信号を変えて繰り返しビットに変換して長いビット列から成る固有情報を生成する。

グリッチPUFで生成される固有情報は次の2つの特長を持つ。1つ目は，回路が動作した瞬間だけ固有情報が現れるためLSIを分解・解析されても固有情報が漏れない。2つ目は，製造段階で生じる個体差から固有情報を生成しているため，回路を複写されても固有情報は複写されない。この2つの特長は，グリッチPUFで生成される固有情報がセキュリティ上強固な秘密情報であることを意味する。

3.2 鍵 生 成

グリッチPUFを含め，PUFで生成される固有情報は生成ごとに完全一致しない想定で設計される。これは，人工物が持つ製造ばらつきのようなわずかな特徴量を利用するため，現象の再現性を必ずしも保証できないためである。一方で，このようにノイズを含む情報から安定的に一意のビットパターンを生成する方法は古くから研究されており，その代表例であるFuzzy Commitment[3]の動作を**図4**に示す。

PUFで生成する情報をWとして，生成ごとに完全一致せず誤りが発生する状態を(W＋E)と表現する。Fuzzy Commitmentの初期生成では，生成したWに乱数を符号化したデータCを排他的論理和して補助データSとして外部に記憶する。再生成時は，初期生成の情報と比較して誤りを含む(W＋E)と外部に記憶したSを排他的論理和して，その結果に対して誤り訂正の復号を行う。これによって，初期生成時に符号化したデータCが復元される。Cが復元されたことで補助データSからWを抽出することができるため，同一の秘密情報が生成可能となる。なお，補助データSからWを復元できない安全性の根拠は，符号化に用いた乱数の分だけのあいまいさをSが持つためである。

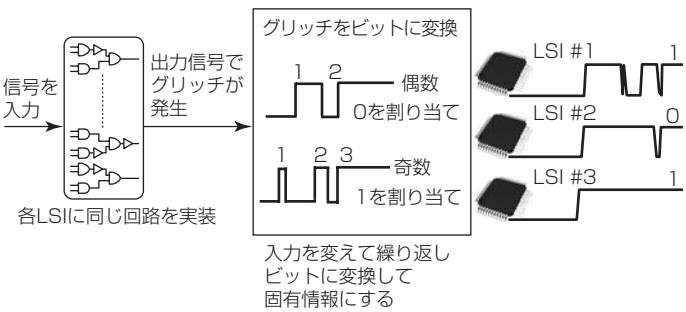


図3．グリッチPUFによる固有情報の生成

3.3 物理乱数生成及び暗号化・復号

グリッチPUFでグリッチを生成する回路の深さと生成される情報の関係を**図5**に示す。生成する回路が浅いと通過する論理ゲートが少なく，個体差が生まれない。一方，深すぎると生成する固有情報のエラーが増大して，**2．2節**で述べた誤り訂正の能力を超えるエラーが発生する。これは，固有情報を生成する立場からは望ましくない性質であるが，暗号プロトコルで不可欠な“乱数生成”としては有用な現象である。そこで，米国標準暗号であるAES(Advanced Encryption Standard)の暗号化・復号回路を基本回路として論理段数を調整する機能を追加することで，グリッチ

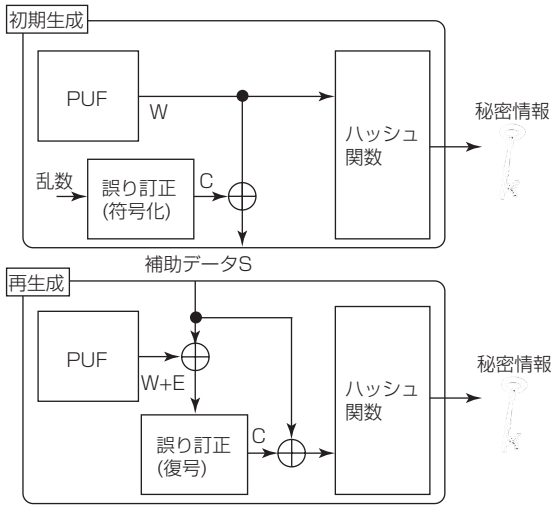


図4．Fuzzy CommitmentでのPUFによる鍵生成

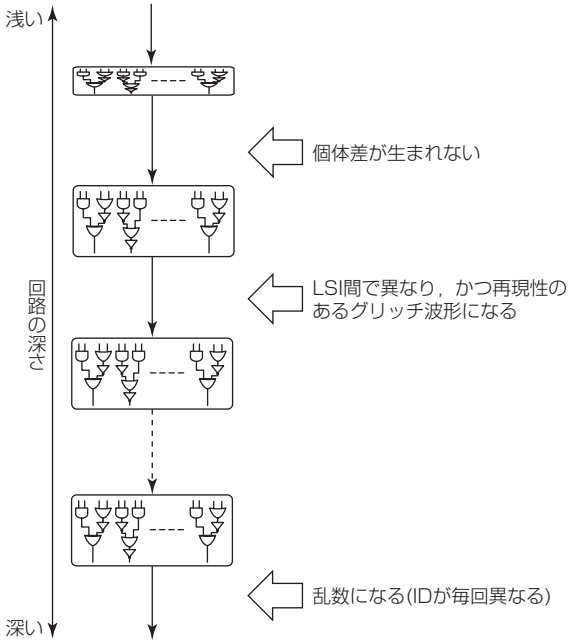


図5．グリッチとランダムロジックの関係

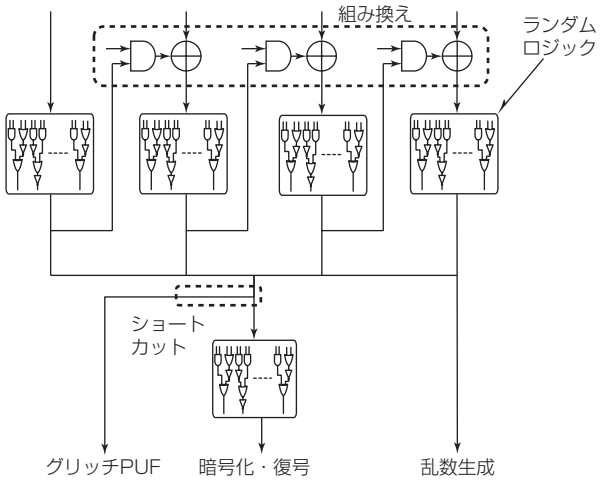


図6．回路の共有化

PUFの固有情報生成と乱数生成を統合する回路を開発した[4]。**図6**のように回路を暗号化・復号回路，グリッチPUF，乱数生成で共有することで，それぞれの機能を独立に実装するケースと比較して回路の大きさを約3分の1に削減することができ，3つの機能を約15Kゲートの論理回路で実装できる。

図6の点線の枠で示される回路や配線は，グリッチPUFの固有情報生成と乱数生成のために追加した部分である。それ以外はAESの処理として必要な回路であり，追加分は非常に単純な回路であることが分かる。

暗号化・復号，グリッチPUF及び乱数生成による固有情報生成の3つの機能がそろうことで，**図1**に示した機器認証をセキュアに効率よく実現できる。図から分かるように，機器認証には暗号化・復号と乱数生成の機能が必要となる。また，認証鍵をグリッチPUFの固有情報で暗号化して保護し，認証時だけ復号して利用することで，安全な鍵管理が可能となる。

3.4　LSIの動作環境の異常検出

暗号技術だけでは防げないIoT機器に対する脅威として，悪意あるデバイスの取付けによるセンサへの攻撃[5]や，共振を利用したセンサの誤動作を誘発する攻撃[6]などが挙げられる。このような攻撃を防ぐ手段の候補として，PUFを利用したLSIの動作環境の異常検出を提案している[7]。先に述べたとおり，グリッチPUFを含めたPUFで生成される固有情報は生成ごとに完全一致しない想定で設計されるが，一般に温度や電圧変化などによってその誤りが増大する。鍵生成をするのであれば，LSIが許容する動作範囲では，その誤り率をFuzzy Commitmentで用いる誤り訂正符号の訂正能力内に抑える必要がある。逆に言えば，誤り率の急激な増大からLSIの動作環境の変化を検出できる。**図7**にその基本原理を示す。グリッチPUFが生成する固有情報の誤り率を定期的に監視することで，LSIの動作環境の異常を検出する。この方式の最大の特長は，非常に短時間での環境変化も検出できる点であり，およそ100nsで発生する瞬間的な電圧ドロップも検出することができる。

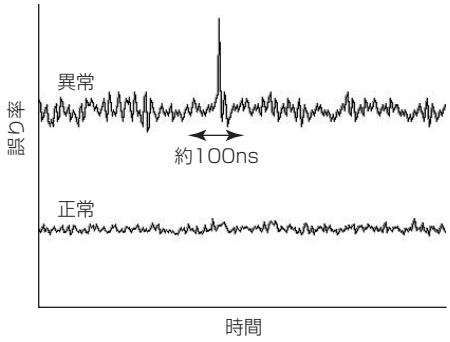


図7．グリッチPUFによるLSIの動作環境の異常検出

4. むすび

IoT機器のセキュリティ課題の解決には，暗号技術が不可欠である。本稿では，暗号を利用する上で課題となる鍵管理を解決する技術として“グリッチPUF”及びその応用技術について述べた。この技術は，機器の最小構成要素であるLSIにセキュリティ脅威を封じ込めるための技術である。今後は，事業化に向けて，上位アプリケーションとの連携やセンサなどの低コストデバイスへの適用などについて取り組んでいく。

参考文献

(1) Hewllet Packard Enterprise：Internet of Things Research Study（2015）
http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en, 2014.
(2) Suzuki，D.，et al.：The Glitch PUF：A New Delay-PUF Architecture Exploiting Glitch Shapes，CHES 2010，366～382（2010）
(3) Juels，A.，et al.：A Fuzzy Commitment Scheme，Proc. the 6th ACM Conference on Computer and Communications Security，28～36（1999）
(4) Shimizu，K.，et al.：Unified Coprocessor Architecture for Secure Key Storage and Challenge-Response Authentication，IEICE Transactions，E97-A，No.1，264～274（2014）
(5) Shoukry，Y.，et al.：Non-invasive Spoofing Attacks for Anti-lock Braking Systems，CHES 2013，55～72（2015）
(6) Son，Y.，et al.：Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors，USENIX Security Symposium 2015，881～896（2015）
(7) Shimizu，K.，et al.：PUF as a Sensor，IEEE GCCE 2015（2015）