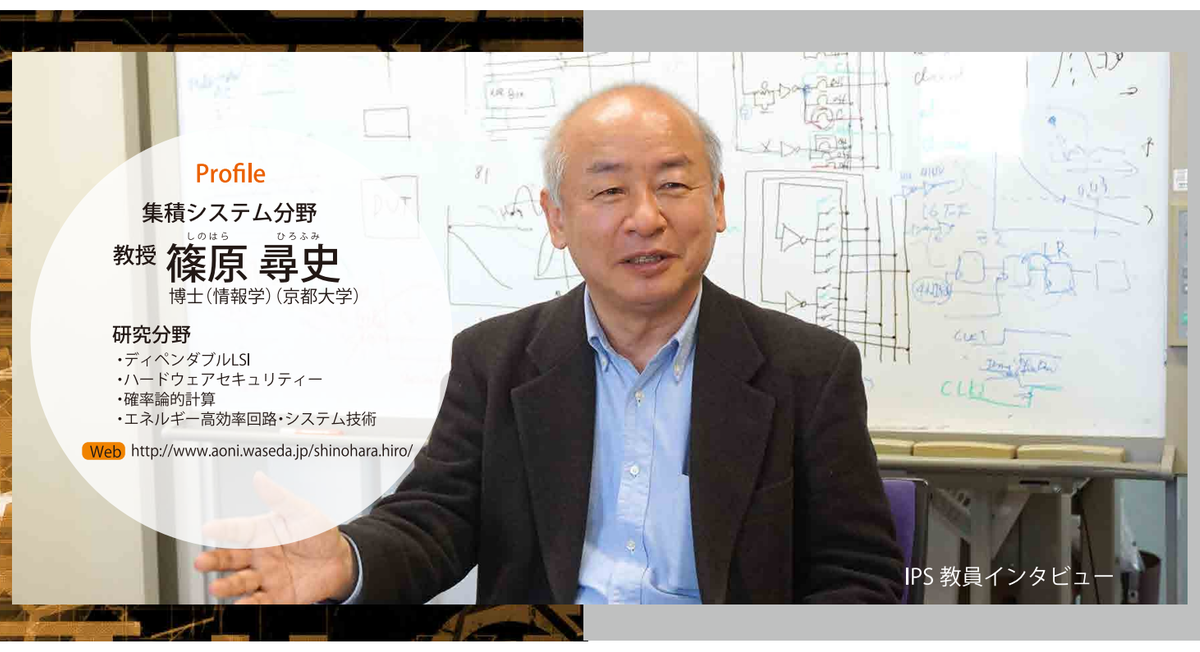


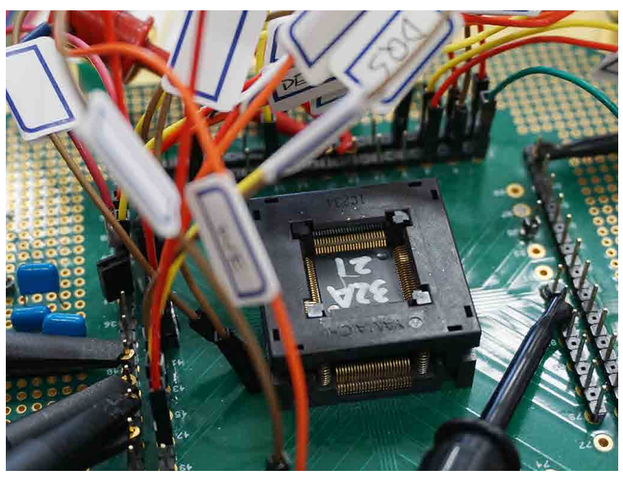
IPS 教員インタビュー

IoT社会の発展を支える「世界一」の乱数発生技術

サイバー攻撃などによる情報漏洩問題が深刻化する近年、より厳重な認証システムによる高度なセキュリティ対策が求められている。特に、様々なモノをネットワークでつなぐIoT環境が、あらゆる業界・業種に拡大するであろうこれからの時代、認証技術の高度化は、"待ったなし"のテーマの1つと言えるだろう。情報生産システム研究科の篠原尋史教授は、認証技術の根幹を成す「乱数(暗号キー)発生技術」の高度化に専門的に取り組むオーソリティだ。

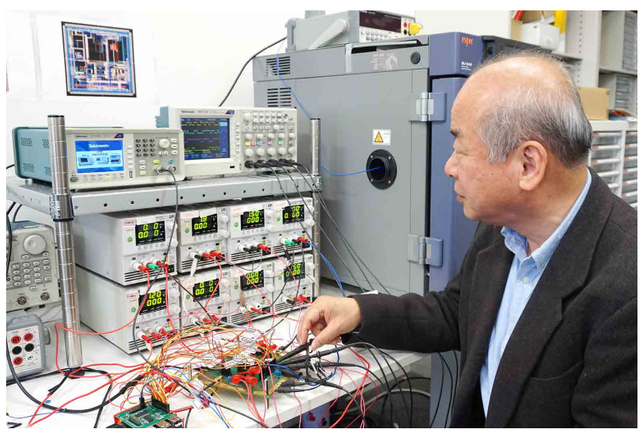
「乱数」技術の高度化で、より厳重な認証システムを

スマホやノートPCのセキュリティに、生体認証を選択している人は多いだろう。個人の"固有情報"である指紋や顔認証は安全性が高く、起動ごとにPINやパスワードを入力する手間も省くことができる。
「指紋は、1人ひとりランダムに異なる形状を持つという点で『乱数』の一種。生涯変わらないことから『静的乱数』だと言えます。集積回路の分野でも、個体ごとのバラつきを利用して静的な乱数を発生させる『PUF(複製不能関数)』という技術があります」。篠原研究室では、この『PUF』をIoTにおける個体認証に利用する技術を研究している。とは言え、簡単にはいかない。個体ごとのバラつきが生じる原因は、半導体製造時に注入する不純物原子由来の"ゆらぎ"なので、複製することはできない。ただし、その"ゆらぎ"が小さいと、「熱雑音」による1/1000V程度の微細な電圧変動にも影響を受け、乱数発生時のビットエラーが生じやすいという問題点があるからだ。
一方、PUFの場合はビットエラーの原因となる熱雑音を、逆に乱数の予測不能さを増すために活用し、動的な乱数を発生するのが『TRNG(真乱数発生回路)』という技術。「ランダムに発生する電圧変化を増幅して1か0かの電圧を得るので、PUFがチップ固有の乱数を発生するのに対し、TRNGはサイコロを振るように、毎回異なる乱数を発生させられます」。



「種(シード)」からアルゴリズムによって発生させる疑似乱数は、シードが攻撃者に読み取られてしまうと、乱数まで読み取られるという弱点がある。TRNGの物理現象はそのような心配がないので、より厳重な認証セキュリティシステムが構築できるわけだが、この方式にも、製造時の個体差や電源・電圧の変動などにより、データの偏りが生じるという問題点がある。
「現実には、集積回路ごとのバラつきと熱雑音とは混在して発生するので、それを分離してPUF側・TRNG側それぞれの乱数を得るための、ある種の『フィルター』が必要です。PUF・TRNGそれぞれの問題点を解決しなければならないのはもちろんですが『フィルター』に相当する回路の設計が一番の工夫しどころなのです」。

「ムーアの法則」だけでない集積回路分野の進歩



最新の研究成果を実用化・製品化に結びつけるには、前述のようにPUF・TRNGそれぞれの課題解決と、信頼性の高い回路の設計とが重要なテーマだ。今後、IoT環境が一気に広がり、ネットワークに接続する端末機器数が急増すれば、機器同士の認証精度とセキュリティレベルとを、さらに高めねばならない。
特に近年、IoT機器を介して特定企業などのサーバに一斉攻撃をかけるタイプのサイバー犯罪が増えつつあるため、高度な機器認証システムが求められている。篠原教授が「工夫のしどころ」と考えているフィルターも、そのための研究の1つだ。
「ラッチ回路を用いた『ラッチ式PUF』『ラッチ式TRNG』を中心に研究を行っていますが、トランジスタ6個ほどしか使わないシンプルな回路だけで、もう何十年も研究・開発を続けています」「新しいアイデアを試すと新しい問題が出てきて、その問題を解く方法を試したら、また次の課題が出てくる。だからこそ、様々な工夫が活かせるクリエイティブな分野なのです」。
「ラッチ回路」は、キャッシュメモリ(SRAM)などに用いられているものだが、篠原研究室ではこれを乱数発生器として使い、ラッチ回路に"新しい価値"を与える研究を行っている。まさにクリエイティブな発想によるものだ。また、トランジスタの劣化要因として嫌われている「ホットキャリア注入(※)」を、敢えて意図的に発生させ、PUFのデータのビットエラーを解消する実験も行っている。このあたりも"工夫が活かせる部分"と言えるだろう。
回路の高性能化はもちろんだが、実用化するためには、外部からの影響を受けにくくするためのロバスト性向上、外部から不当に読み取られたり改変されたりしないようにする耐タンパー性の確保など、克服せねばならない課題は少なくない。
さらに、スマート農業や人体に装着する医療機器など、電源供給が難しい環境でのIoT機器に用いる場合、太陽光発電パネルや小型バッテリーなど、限られた電力でより長く安定稼働する省エネルギー性も必要だ。「だから、この分野の研究には、ちょっとした工夫を積み重ねたり、自然現象をじっくり観察したりするのが好きな学生が向いているかもしれませんね。オームの法則が理解できるレベルの基礎知識さえあれば、新しいやり方を考察できる研究ジャンルです」。

(※ 高電圧で運動エネルギーを得た電子が絶縁体(ゲート酸化膜)に飛び込み、トランジスタの特性を変化させる現象)

世界トップの「モデリング攻撃耐性」を実現

機器の認証には、乱数とそれを暗号化した符号をサーバ側と端末側とでやり取りする、「チャレンジレスポンス方式」が用いられている。この暗号キーにPUFの静的乱数を用いることで、機器を個別に認証することができる。
近年、「ストロングPUF」と呼ばれる、それ単体でほぼ無尽蔵のレスポンスを発生するPUFを用いて、IoT向けのセキュリティをより"簡便"に実装する研究が進んでいるのだが、皮肉なことに攻撃者側の技術も、セキュリティ強化を上回るスピードで進化を遂げている。機器とサーバのやり取りを傍受し、AI(機械学習)によって乱数発生のモデルを作る、「モデリング攻撃」が実用化する上での課題となっているのだ。
篠原研究室は、この攻撃に対する耐性を高める手法も研究しており、2000万回のやり取りをAIに機械学習されても破れないストロングPUFを作成。IEEE(アメリカに本部を置く国際的な電気・情報工学分野の学術研究団体)が2021年2月に開催した、半導体分野で最も権威ある国際固体回路会議で、「世界一のモデリング攻撃耐性」との評価を受けた。
「とは言え、これがゴールとは考えていません。何年も前から"間もなく終焉を迎えるだろう"と言われ続けてきた『ムーアの法則(※)』も、終焉を迎えるどころか現在も続いており、まだまだ伸びる余地があります。たとえそれが終わる時が来ても、集積回路の研究に終わりは無いのです」。素子数の増加・高密度化は進歩の一側面に過ぎず、様々な回路・システム技術、設計自動化技術、それらを基盤とする応用技術の発展が、私たちの社会を支えている。その一翼を担うのが、篠原教授が取り組む乱数発生技術の高度化なのである。

(※ ゴードン・ムーア(インテル創業者の1人)が1965年、『コスト最小の素子数は年率約2倍で増加してきた』と述べて集積回路の高密度化を予想したことから、この名が付いた。2021年現在でも約2年で2倍のペースで高密度化が進んでいる。)