早稲田大学大学院情報生産システム研究科

博士論文審査結果報告書

論　文　題　目

Study on High Stability and Low Energy SRAM-Based Physically Unclonable Function for Hardware Security

申　請　者
Kunyang LIU

情報生産システム工学専攻
ディペンダブル情報システム研究

2021 年　4 月

モノのインターネット（Internet of Things 以下 IoT）の発展により、新たな情報セキュリティ課題が生まれている。IoT 端末は野外など様々な場所に設置されていて、ヒトの関与が限られているからである。モノである端末の個体認証や端末での秘密鍵の安全な生成と保管は、セキュリティシステムの重要な出発点である。物理的複製不可能関数（Physically Unclonable Function 以下 PUF）は、それらの実現手段として期待されていて、信頼の礎（Root of Trust）とも呼ばれる。PUF は、ランダムな素子ばらつきに基づいてチップ固有乱数を要求される度に生成するもので、ばらつきの基となる半導体中の不純物ゆらぎは複製できないこと、生成後は消えて観測が困難なことから、従来の不揮発メモリを用いた秘密鍵保管よりも安全である。

しかし、PUF には課題もある。最も重要なものはビットエラーの抑制である。素子ばらつきは通常 mV オーダーと微小なため、ランダムノイズ、電源電圧と温度の環境変動、長期エージング、などによって値が変化してしまう。これは暗号では許されない。また IoT 端末は電源リソースなどが限られているので、低エネルギーで省面積が求められる。更には、チップ内の秘密情報奪取を目的としたサイドチャネル攻撃に対しても、データを漏洩しない攻撃耐性はセキュリティ用途として不可欠である。

静的メモリ（Static Random Access Memory 以下 SRAM） を基本回路とする SRAM PUF は、面積が小さく差動で動作する特徴があり、数ある PUF 方式の中でも主要な方式である。差動構成によりデータの”0” ”1”にかかわらず電流が一定なため、代表的サイドチャネル攻撃である電力解析攻撃に高い耐性が本来備わっている。代表的な PUF 専業メーカである米国 Intrinsic ID 社も SRAM PUF を採用している。しかしビットエラー率が高く、これを低減するためには重いエラー訂正（Error Correction Code 以下 ECC）を用いる必要がある。これは IoT 端末に求められる低エネルギーや高速性を損ねている。近年ビットエラー率が比較的低い単安定型の PUF が提案されていて韓国三星電子が採用している(Y. Choi ら ISSCC 2020)が、差動構成ではなく、多重の ECC も必要である。別の方式として、ゲート酸化膜破壊を利用してビットエラーゼロを実現した PUF が報告されている(M-Y. Wu ら ISSCC2018, K-H Chuang ら A-SSCC2018)。しかしリバースエンジニアリングによりデータが漏洩する弱点があるため、これを PUF の範疇に含めない見方もある。

そこで、SRAM PUF の優れた特徴を維持しながらビットエラー率を低減して、ECC 負担を軽減あるいは無くすことが IoT 応用では求められる。

本論文はこのような課題、背景のもとに著者が行ってきた研究の成果を纏めたものである。SRAM PUF を基本方式として、新規なビットセルを二種類考案し、それぞれに適した二種類の後処理技術を提案している。第一のアプローチは純粋回路方式で、チップ内蔵のバイアス電圧発生回路を用いて潜在的不安定セルを検出し、そのセルをマスクする方法をとった。第二のアプローチは製造後に素子特性の調節を行うもので、ホットキャリア注入（Hot

Carrier Injection 以下 HCI）を意図的に導入してばらつきを拡大し、PUF の安定化を図った。どちらの研究も PUF チップを試作し、様々な環境変動やエージング加速の条件下で、数 100 万回から累積 1000 万回超に及ぶ測定を繰り返し、ビットエラーゼロの安定性を実証している、また電力解析攻撃に対する耐性の実証や、低消費エネルギー特性の評価も行っている。

本論文は 5 章から構成されている。以下、各章ごとにその内容の概略を述べ評価を加えることにする。

第 1 章"Background"では、IoT セキュリティの背景を、端末の認証を例に説明し、従来方法の問題点を明らかにし、それを解決する PUF を用いた認証方法を説明している。

第 2 章" Preliminaries"では、まず安定性、ユニーク性、ランダム性を評価するための PUF 特有の性能指標と、面積と消費エネルギーに関する性能指標を定義し、攻撃耐性について述べている。次に、先行研究による各種 PUF ならびに SRAM PUF について解説したうえで、安定な SRAM PUF の必要性を示している。そして、安定性を向上するための従来の後処理技術の特徴と課題を述べて、本研究の動機を明らかにしている。

第 3 章"EE SRAM PUF with 2-D Power Gating and V_{SS} Bias-Based Dark-Bit Detection Technique"では、Enhancement-Enhancement（以下 EE） SRAM PUF と回路技術による安定化手法を提案し、130nm CMOS 製造技術で試作したチップで実測評価を行っている。EE SRAM PUF ビットセルでは、低くない電源電圧で単安定から双安定に状態遷移する。これにより、標準条件でのビットエラー率を従来の 3.04%から 1/14 の 0.21%に低減することに SRAM PUF として初めて成功した。また n 型 MOS トランジスタだけで構成されるビットセル面積は $373F^2$（F は最小パターン寸法）と小さい。消費エネルギーは、独自の 2 次元パワーゲーティングで、それをしない場合と比べて 1/64 の 128fJ/bit に低減されている。

後処理技術として、オンチップの電圧発生回路を V_{SS} 電圧バイアスに適用して安定性を損ねる状況を意図的に作り出し、潜在的不安定ビットを検出する方法を提案した。室温試験だけで検出した潜在的不安定セルをマスクすることにより、電源電圧 0.8V と 1.4V, 温度-40℃と 120℃の 4 通りの最悪条件組み合わせのいずれでも 167 万回測定してエラー無し（ビットエラー率 5.99×10^{-7} 未満）を確認した。また、11 年相当の加速エージング試験でも、新たに発生した不安定セルは全て事前の V_{SS} 電圧バイアス試験で検出されていたことがわかり、手法の有効性が認められた。これは回路技術だけでビットエラーをゼロにした先駆的成果である。更に、サイドチャネル攻撃の主な一つである電力解析攻撃を試み、情報漏洩が無いことを確認している。

第 4 章"Hybrid SRAM PUF Using Hot Carrier Injection (HCI) Burn-in for Stability Reinforcement"では、ハイブリッド SRAM PUF と、ホットキ

ャリア注入 HCI による後処理を提案し、ここでも 130nm CMOS 製造技術で試作したチップで実測評価を行っている。ビットセルを EE SRAM と CMOS SRAM のハイブリッド型にすることにより、前者の高安定性と後者の低エネルギー性の両方の利点を兼ね備えている。0.5V の低電圧動作で、消費エネルギーを EE SRAM PUF の 1/61 の 2.07fJ/bit に低減した。この値は、それまでにビットエラーをゼロにした PUF の中では最も小さい。全 PUF の中でも最小のグループに入る。

後処理に用いた HCI 技術は、一対の n 型 MOS トランジスタの片方に選択的にキャリア注入してしきい値電圧 Vth のミスマッチを強化する方式である。ハイブリッド型セルは、この方式をトランジスタ追加なしに実現できる特徴がある。10 分間の HCI バーンインにより、電源電圧 0.5V と 0.7V、温度-40℃と 120℃の 4 通りの最悪条件組み合わせのいずれでも 256 万回測定してビットエラー無し（ビットエラー率 3.90×10^{-7} 未満）を確認した。また、最長 21 年に相当する加速エージング試験でも、累積 1331 万回に及ぶ測定でビットエラーは観測されていない。第 3 章の成果と比較すると、本後処理方式は素子特性の調節を伴うが、マスクによるビットセル損失は無く、マスクセルの番地を記憶する補助メモリも不要という利点がある。

第 5 章”Conclusion”では、本論文の研究成果を総括して結論を述べている。

以上が本研究の成果で、これを要約すると、本研究は SRAM PUF をベースとして、EE SRAM PUF とハイブリッド SRAM PUF の二種類のビットセルを考案し、一方には V_{SS} バイアスによる潜在的不安定セル検出とマスクと言う回路アプローチで、他方には HCI バーンインによるミスマッチ強化と言う素子特性アプローチで後処理を提案した。どちらもビットエラーを無くすことをテストチップで実証している。二種類のアプローチはそれぞれ特徴があり、用途に応じて使い分けることが出来る。また、サイドチャネル攻撃耐性があり、面積や消費エネルギーが低くて実用性も高い。これらの成果は IoT のセキュリティ向上に貢献するものと言える。よって本論文は博士（工学）の学位論文として価値あるものと認める

2021 年 4 月 8 日

審査員

主査　早稲田大学教授 博士(情報学)(京都大学)　篠原 尋史

早稲田大学教授 博士(工学) (筑波大学)　大澤 隆

早稲田大学准教授 博士(工学)(東京工業大学) 髙畑 清人