様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １５ 日現在

機関番号：３２６８９
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ０４２０１

研究課題名（和文）暗号レスでIoT認証を軽量にするストロングPUFの研究

研究課題名（英文）Study of a Strong FUF for Light Weight Authentication without Cryptography

研究代表者
篠原　尋史（Shinohara, Hirofumi）

早稲田大学・理工学術院（情報生産システム研究科・センター）・特任教授

研究者番号：５０５３１８１０

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：モノの認証の低エネルギー化・高速化を目的に、ストロングPUFを研究開発した。研究代表者ら提案のSPN構造を基に、レスポンス累積、ブレンディング、追加ラウンド等の技術を導入するとともに、レスポンスビット幅を従来の1ビットから5ビット、100ビットと拡張していった。
試作チップ実測の結果、機械学習耐性は世界最高の40百万CRP学習耐性、10億ビット学習耐性を実証した。消費エネルギー2.17pJ/bit、スループット3.7bit/cycleは従来のストロングPUFを大きく上回った。ホットキャリア注入による安定化を行い、ストロングPUFで初となるエラーゼロ(エラー率<2E-8)を達成した。

研究成果の学術的意義や社会的意義
ストロングPUFはそれ自体で実質無尽蔵のレスポンスを生成できることから認証などのセキュリティ応用が期待されていたが、機械学習攻撃耐性が低いこととビットエラー率が高いことが大きな壁となっていた。本研究ではその両方を解決したことと、レスポンス出力を従来の1ビットから一気に100ビットまで広めることに成功した点に、高い学術的意義がある。
本研究成果により、暗号を必要としない低消費エネルギーで高速なIoTに適した認証の可能性が示された。セキュリティ向上に寄与する社会的意義は大きい。

研究成果の概要（英文）：Strong PUFs are researched for low energy consumption and fast authentication of connected things. Based on the SPN architecture proposed by a group of primary researchor of this project, techniques of response accumulation, blending, additional rounds are newly developed. And response bit width is extended from conventional 1bit to 5bit and as large as 100bit.
Experimental results demonstrated world record machine learning attack resiliency of 40million CRP learning and 1billion bit learning. Energy consumption of 2.17pJ/bit and throughput of 3.7bit/cycle far exceeded those of previous works. To solve bit error problem, hot carrier injection stabilization has been applied. And zero-bit error (error rate<2E-8) was fist achieved as a strong PUF.

研究分野：集積回路、ハードウェアセキュリティ

キーワード：ストロングPUF　機械学習攻撃　モデリング攻撃　ビットエラー率　認証　ハードウェアセキュリティ

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

１．研究開始当初の背景

モノが直接ネットワークにつながる IoT では、人の関与の少なさから新たなセキュリティ上の脅威が生まれる。これに対抗する信頼の礎（Root of Trust）として PUF が注目されている。PUF は複製不能なチップ固有の固定乱数(指紋に相当)を生成することから、暗号鍵の安全な生成やモノの認証に用いられる。認証ではサーバからの質問（チャレンジ C）に対する端末の応答（レスポンス R）が正しければ成功となる。C と R のペア（以下 CRP）は使い捨てなので多数の CRP を消費する。従来 PUF（ストロングに対してウィーク PUF と呼ばれる）を用いた認証では暗号処理が必要で、そこに低エネルギー化や高速応答の限界があった。

ストロング PUF に分類される PUF は､それ自身で実質無尽蔵のチップ固有 CRP を生成し、暗号処理無しに認証が可能なことから、この限界を破る潜在能力がある。しかし、a)機械学習攻撃耐性が低い b)ビットエラー率が高い、といった課題があった。また、機械学習攻撃耐性を高めるために、1bit だけのレスポンス R を得るのに複雑な内部構造が必要だったので、 c)消費エネルギーが大きくてスループットが低い欠点があり、性能面でウィーク PUF と暗号の組み合わせの限界を超えることが出来なかった。

２．研究の目的

本研究は、ウィーク PUF と暗号の組み合わせによる性能限界を突破することが可能なストロング PUF による解決策を提供することにより、IoT セキュリティ向上に貢献することを目的とする。そのために、上記 a)に対しては世界最高レベルの 40 百万 CRP 学習でもレスポンス R が予測されない攻撃耐性を実現し、b)に対してはストロング PUF としては初めてエラーゼロ（10^6 評価でエラーゼロ；BER<1x10^{-6}）を達成する。そしてその上で、性能面でも AES 暗号を凌駕することを目標とする。更に研究期間中に、暗号解析に要攻撃への耐性強化も a)に関連した目標に追加した。

３．研究の方法

本研究の提案時（2020 年）に準備として進めていた、SRAM PUF（ウィーク PUF）を要素として用いた SPN（Substitution Permutation Network）アーキテクチャによるストロング PUF [1]をベースラインとして、これを改善する方法で研究を行った。改善の方向は、a)については演算履歴を出力に反映することとフィードバック回数を増すことで効率よく内部処理の複雑度を増すことを行った。これにより機械学習や暗号解析を困難にするとともに、レスポンス R のランダム性を理想乱数発生器レベルに高めた。b)については HCI (Hot Carrier Injection) の選択的注入によるミスマッチが強化の効率を高めた。また、セル間ばらつきによって一部のセルでは注入されるホットキャリア数が少ないことが分かったので、トランジスタサイズ拡大によるばらつき削減を行った。前記 a)の方法は c)については悪化する方向である。それにもかかわらず消費エネルギーとスループットを改善するために、レスポンス出力 R のビット幅を、従来は 1bit だけだったものを複数 bit に拡張する戦略を取った。最終的には 100bit 幅レスポンスを一括出力し、なおかつ攻撃耐性は劣化しないアーキテクチャを開発した。これにより、100bit レスポンス認証するには従来は 100 回の CRP のやり取りが必要だったものが 1 回で済むようになり、レスポンス 1bit あたりの消費エネルギーやスループットは飛躍的に改善した。

４．研究成果

(1) レスポンス幅 5bit のストロング PUF [2]

出力ビット幅拡張の第一段階として、チャレンジ入力 100bit、レスポンス出力 5bit のストロング PUF を 130nm CMOS プロセスで設計し、試作・評価した。全体構成を図 1 に示す。太線枠で囲んだ LUT（Look Up Table）は 5 個の 32 ワード x 7bit 構成 SRAM PUF（合計 1120bit）からなり､それを灰色の下地部分でループを回して SPN アーキテクチャを形成する。特徴は次の 4 点。①は 5bit 幅並列レスポンス。②は RA（Response Accumulation）でラウンドの度に出力を

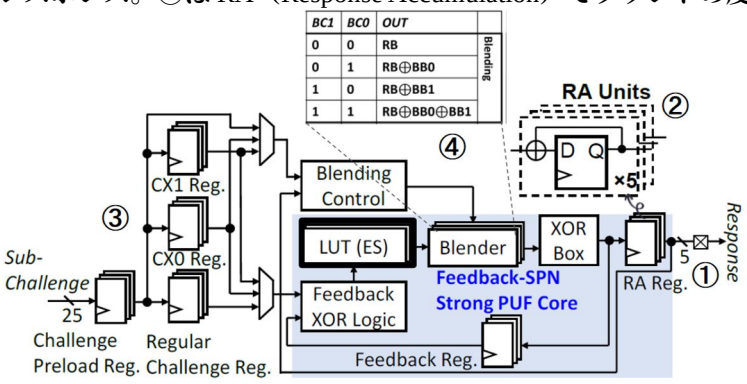

図 1. レスポンス幅 5bit の SPN 構成ストロング PUF

累積加算することでラウンド履歴を出力に反映させた。25bit のサブチャレンジによるラウンドを 4 回繰り返して 100bit チャレンジに対するレスポンスを得ているが、③では追加の 25bit チャレンジを 2 組（CX0, CX1）発生してラウンドを 2 個追加した。これにより処理の複雑度が増すとともに、5bit 出力が 2^5(=32)通り全て均等に現れるようになってランダム性が増した。④は暗号解析攻撃対策として追加したもので、7bit の LUT 出力を互いに XOR するなどブレンドして 5bit にしている。ブレンド方法を RA の中間履歴や次ラウンドのチャレンジを基に決めることで、攻撃者が LUT を一つのモデルとして暗号解析できないようにしている。

これらの技術が機械学習攻撃耐性の向上にどれだけ貢献したかを図 2 に示す。なお、ここでは LUT のハミング重み（HW: 1 を取る割合）を通常の 0.5 よりも意図的に小さくしてエントロピーを削減し、攻撃耐性を弱めた加速試験となっている。従来アーキテクチャから単純に出力を 5bit 幅に広げたのでは、赤矢印で示す通り◯から□へと攻撃による推定精度は向上して耐性が弱まるが、XOR BOX の追加（□）、RA の追加（◇）、追加チャレンジとブレンド（×）により次々と推定精度は下がり、最後には HW=0.1 でもあて推量と変わらない 50%精度にまで低下した。機械学習攻撃耐性の学習 CRP 数依存性を図 3 に示す。目標としていた 40 百万(4E7)CRP 学習でも、攻撃による推定精度はあて推量から有意な向上はなかった。1R=5bit を考慮すると学習 bit 数は 2 億 bit となり、従来比で一層大幅増となる。ビットエラー率は、図 4 に示すとおり、10 分間の HCI バーンインで、5 個の VT コーナ全てでエラーゼロ（<8E-5, <4E-7）を達成した。ストロング PUF エラーゼロを記録したのは初めてである。消費エネルギーは、図 5 に示す通り、0.4V で 2.17pJ/bit と準備していたベースラインの 20 分の 1 以下に削減した。これは 22nm CMOS による低消費エネルギーAES の 3.46pJ/bit (289Gbps/W) [3]をも凌ぐ。但し、5bit 生成に 8 サイクルを要しているので、スループットは 0.625bit/cycle と目標の 1bit/cycle に届いていない。

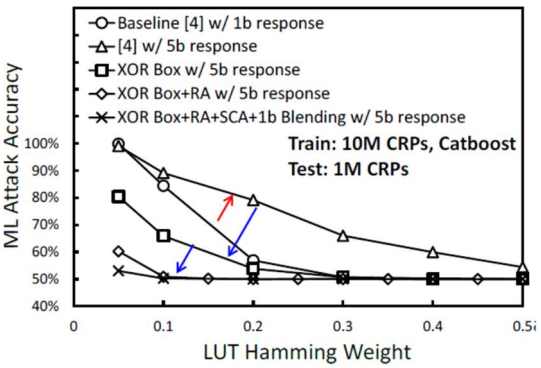

図 2. 機械学習攻撃耐性（加速試験）

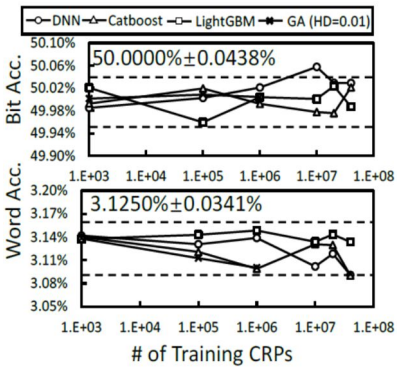

図 3.機械学習攻撃耐性（学習 CRP 数依存）

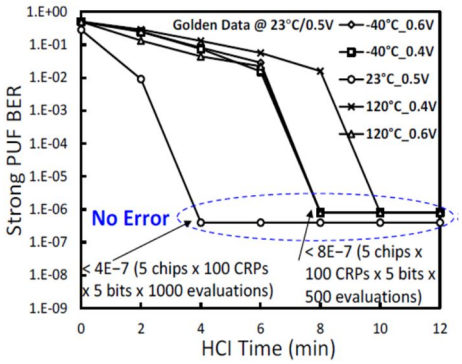

図 4.ビットエラー率特性

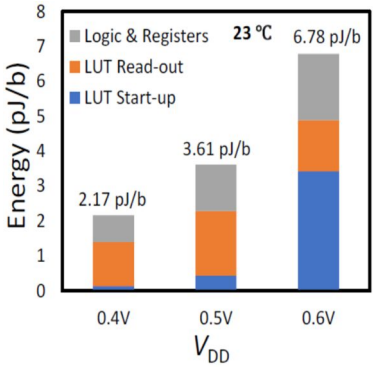

図 5.消費エネルギーの電圧依存性

(2) レスポンス幅 100bit のストロング PUF [4]

スループットの向上と一回の CRP のやり取りで認証が完結する実使用時の利便性の改善のため、次にレスポンス幅 100bit のストロング PUF を 130nm CMOS プロセスで設計し試作・評価した。全体の動作の流れと各要素の詳細を図 6 に示す。①の通り 100bit レスポンスで、ラウンド間はそれより多い 105bit データ幅としてラウンドを単位とする暗号解析攻撃を無意味としている。35bit 幅のサブラウンドへの攻撃には、②のラウンド内パーミュテーション（混ぜ返し）でサブラウンドを密結合にして対策した。前回の RA は、③の通りラウンドごとにビット位置をずらしながら累積加算することで、ビット位置間の結合を強くした。100bit 幅レスポンスで特に気を配ったのが、LUT 衝突である。LUT 衝突とは、チャレンジ入力が違っていても全ての LUT 出力が偶然同じになる現象で、これが発生すると本来ほとんど起きないはず（確率 2^{-100}）の 100bit レスポンスの一致が生じ、攻撃のヒントを与えてしまう。チャレンジが 1bit だけ変化した時（差分攻撃）が最も危険なので、それでも LUT 衝突が起きないようにした。具体的には④の通り

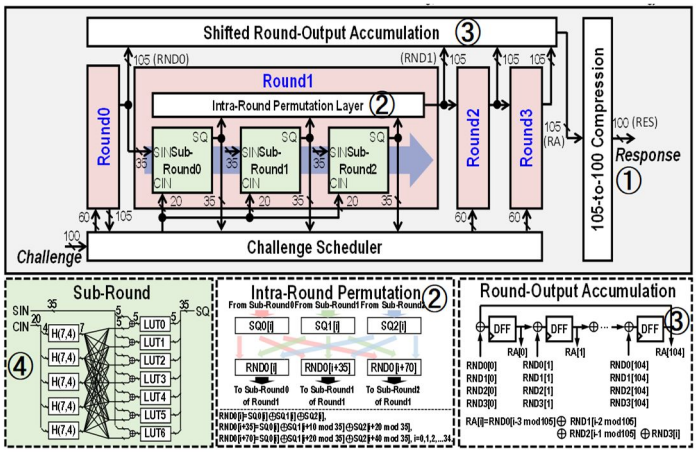

図 6. レスポンス幅 100bit の SPN ストロング PUF 全体フローと構成要素

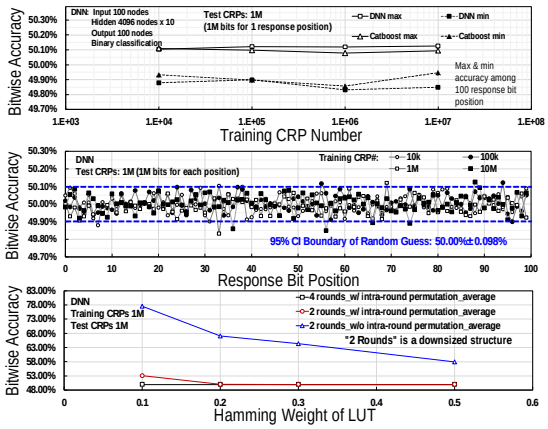

図 7. 機械学習攻撃耐性

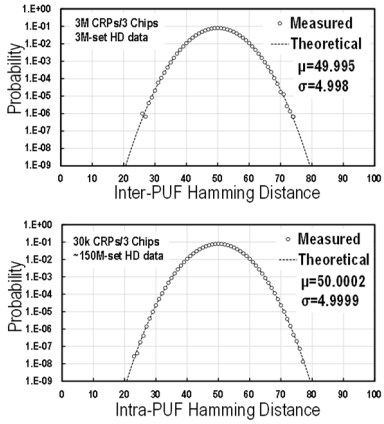

図 8 HD によるユニーク性評価

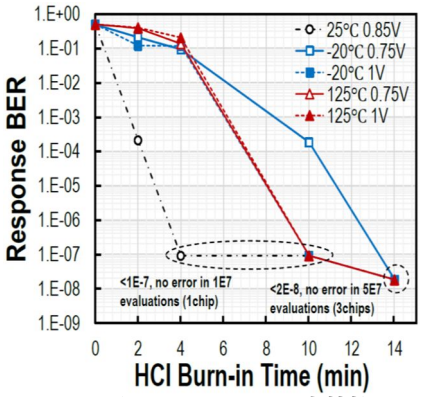

図 9 ビットエラー率特性

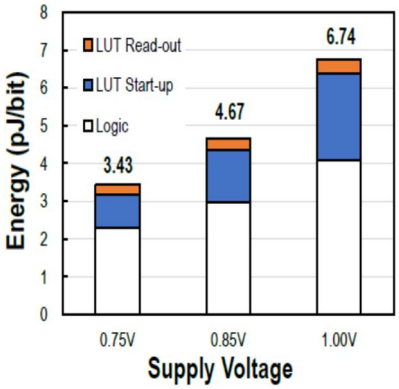

図 10.消費エネルギーの電圧依存性

ハミングコード H(7,4)を用いて 1bit 変化を 3bit 以上の変化に拡大し、追加サブラウンドを 7 回に増加した。これにより理論的 LUT 衝突確率は 2^{-123} 以下と問題ないレベルとなった。

機械学習攻撃耐性の評価結果を図 7 に示す。図 7 下段は、HW を小さくした加速試験でラウンド内パーミュテーションの効果を示したもので、合計 2 ラウンドの縮小版では、これ無しでは有意な精度で推論させる（青線）のが、有りでは HW=0.2 でも有意な精度が得られていない（赤線）。本来の 4 ラウンドでは HW=0.1（1 の確率が僅か 10%）で 50%から全く改善されていない。学習 CRP 数依存性とレスポンスビット位置依存性を図 7 上段と中段に示す。10 百万 CRP 学習下で、100bit レスポンスのどのビットをとっても有意な精度での推論は出来ていない。なお、CRP 数では前記の 40 百万 CRP より少ないが、ビット数で換算すると 10 億 bit 学習で、5 倍多い。

PUF チップ毎のユニーク性を図 8 上段のインターPUF HD に、PUF チップ内でチャレンジ毎のレスポンスのユニーク性を図下段のイントラ PUF HD に示している。どちらも±5σ の範囲まで測定値は統計論的理論的と一致している。ビットエラー率は図 9 に示す通り、14 分の HCI バーンイン時間で、5 個の VT コーナ全てでエラーゼロ（<2E-8）を達成した。消費エネルギーは図 10 に示す通り、0.75V で 3.43pJ/bit であった。これは前記レスポンス幅 5bit のものよりも大きいが、その要因は電源電圧が高いこととロジック部の占める割合が大きいことによる。スループットは、27 サイクルで 100bit 生成しているので 3.70bit/cycle であり、目標の 1bit/cycle を大きくクリアした。

(3) HCI バーンイン時間短縮 [5]

本研究ではビットエラーゼロのため、一貫して HCI バーンインによるミスマッチ拡大に取り組んできた。バーンイン時間 10 分や 14 分は、準備研究によるベースラインの 60 分から大幅に短縮されているが、一層短縮するための研究を行った。HCI バーンインによるミスマッチ拡大は図 11 に示す通り、元々正規分布に従うミスマッチ分布を、HCI の選択的注入により正の極性のものはより大な方向、負の極性のものはより小さな方向（負側）にシフトさせて、不安定な原点付近のセルを無くすことが基本的原理である。しかしシフトの大きさは一様でなく、ばらつきがあるために、原点付近に分布の Tail が残ってエラーの原因となっていた。

研究代表者らは統計分析から、シフト量の分布はガンマ分布（n 個の電荷による効果の分布）とポアッソン分布（注入電荷の個数 n の分布）の合成でモデル化されることを見出した[6]。この知見から、トランジスのゲート幅を大きくすると n の平均が大きくなり、平均に対する相対ばらつきは $\sqrt{n}$ に反比例して小さくなると考えた。基本サイズに対して 2 倍、4 倍で分布がどう変化するかを簡単な計算で示したものが図 12 である。赤破線の Tail 部分が小さくなっていくのが分かる。図 13 は 130nm CMOS による SRAM PUF ビットセルの実測値とモデル式でフィッティングしたものを、基本サイズと 4 倍サイズで比較している。エラーゼロに対するクライテリアを「ミスマッチ 20mV 以下の累積確率-5.4σ以下」としたとき、この実験では 18 分の HCI バーンインで、4 倍サイズでは満たしているが、基本サイズは満たしていない。基本サイズでは 46 分の HCI バーンインが必要と試算された。即ち約 1/3 のバーンイン時間短縮が予測できた。この成果を前記(1)(2)に当てはめると、単純計算では 3.9 分～5.5 分と見積もられる。

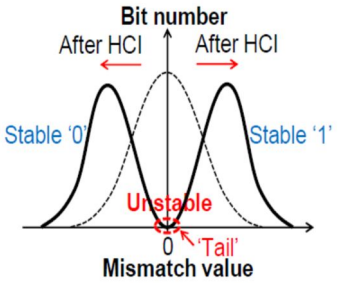

図 11.HCI によるミスマッチ拡大概念

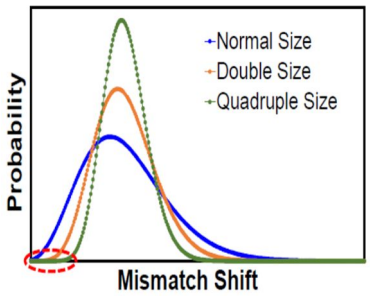

図 12.サイズ拡大の効果予想

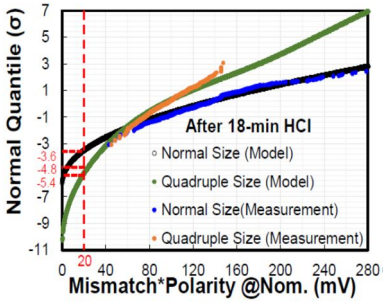

図 13. サイズ拡大の実測比較

(4) SPN アーキテクチャ改良検討

以上により当初設定していた目標と、追加の暗号解析対策を達成したが、スループットの一層の改善のための SPN アーキテクチャ改良を検討した。(2) ④で用いたハミングコード H(7,4)を 2bit 以上のエラー訂正能力を有するコードに置き換えるなどして、低い LUT 衝突確率を維持しながらラウンド数を減らすことで、サイクル当たりの生成ビット数を更に 2 倍以上高める見通しを得た。

参考文献

[1] Kunyang Liu, Zihan Fu, Gen Li, Hongliang Pu, Zhibo Guan, Xingyu Wang, Xinpeng Chen, and Hirofumi Shinohara, "A Modeling Attack Resilient Strong PUF with Feedback-SPN Structure Having <0.73 % Bit Error Rate through In-Cell Hot Carrier Injection Burn-in," IEEE 2021 ISSCC Digest of Technical Papers, pp. 502-503, Feb. 2021.

[2] Kunyang Liu, Gen Li, Zihan Fu, Xuanzhen Wang, and Hirofumi Shinohara, "A 2.17-pJ/b 5b-Response Attack-Resistant Strong PUF with Enhanced Statistical Performance," IEEE, 48th European Solid-State Circuits Conference (ESSCIRC), pp513-516, Sept. 2022.

[3] Sanu Mathew, Sudhir Satpathy, Vikram Suresh, Ram K. Krishnamurthy, “Energy Efficient and Ultra Low Voltage Security Circuits for Nanoscale CMOS Technologies,” IEEE, 2017 CICC, April 2017.

[4] Kunyang Liu, Yichen Tang, Shufan Xu, Ruilin Zhang, and Hirofumi Shinohara, "A 100-Bit-Output Modeling Attack-Resistant SPN Strong PUF with Uniform and High-Randomness Response," Proc. 2023 IEEE Custom Integrated Circuits Conference (CICC), 30-3, April 2023.

[5] Shufan Xu, Kunyang Liu, Yichen Tang, Ruilin Zhang, and Hirofumi Shinohara, "Effect of Quadruple Size Transistor on SRAM Physically Unclonable Function Stabilized by Hot Carrier Injection," 2023 IEEE Int. Conf. Microelectronic Test Structures (ICMTS), 5-4, March 2023.

[6] Kunyang Liu, Yichen Tang, Shufan Xu, and Hirofumi Shinohara,"Vss-Bias-Based Measurement of Random Telegraph Noise in Hybrid SRAM PUF after Hot Carrier Injection Burn-In," 2023 IEEE Int. Conf. Microelectronic Test Structures (ICMTS), 2-3, March 2023.

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 Liu Kunyang、Chen Xinpeng、Pu Hongliang、Shinohara Hirofumi	４．巻 56
２．論文標題 A 0.5-V Hybrid SRAM Physically Unclonable Function Using Hot Carrier Injection Burn-In for Stability Reinforcement	５．発行年 2021年
３．雑誌名 IEEE Journal of Solid-State Circuits	６．最初と最後の頁 2193～2204
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSSC.2020.3035207	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Kunyang Liu, Yichen Tang, Shufan Xu, and Hirofumi Shinohara
２．発表標題 Vss-Bias-Based Measurement of Random Telegraph Noise in Hybrid SRAM PUF after Hot Carrier Injection Burn-In
３．学会等名 2023 IEEE Int. Conf. Microelectronic Test Structures (ICMTS)（国際学会）
４．発表年 2023年

１．発表者名 Shufan Xu, Kunyang Liu, Yichen Tang, Ruilin Zhang, and Hirofumi Shinohara
２．発表標題 Effect of Quadruple Size Transistor on SRAM Physically Unclonable Function Stabilized by Hot Carrier Injection
３．学会等名 2023 IEEE Int. Conf. Microelectronic Test Structures (ICMTS)（国際学会）
４．発表年 2023年

１．発表者名 Kunyang Liu, Gen Li, Zihan Fu, Xuanzhen Wang, and Hirofumi Shinohara
２．発表標題 A 2.17-pJ/b 5b-Response Attack-Resistant Strong PUF with Enhanced Statistical Performance
３．学会等名 IEEE, 48th Europian Solid state Circuits Conference (ESSCIRC)（国際学会）
４．発表年 2023年

１．発表者名 Kunyang Liu, Kiyoshi Takeuchi, and Hirofumi Shinohara
２．発表標題 Statistical Modeling of SRAM PUF Cell Mismatch Shift Distribution After Hot Carrier Injection Burn-In
３．学会等名 2022 IEEE International conference on Microelectronics Test Structures (ICMTS)（国際学会）
４．発表年 2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関