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 Low Energy True Random Number Generator with Latch-based Core and von Neumann-based Post-Processing for Hardware Security

申　請　者
Ruilin ZHANG

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

2022 年　5 月

モノのインターネット IoT では、端末デバイスへの人の関与の少なさ等から、端末自身が情報セキュリティ機能を持つことが重要となる。真乱数発生回路 True Random Number Generator (以下 TRNG)は情報セキュリティを基盤から支えるハードウェアセキュリティの主要な要素で、熱雑音などの物理現象を乱数の源とするため、周期性が無く予測が困難なことから、アルゴリズムに基づく疑似乱数発生器よりも高いセキュリティが期待出来る。

TRNG に対する要求は、暗号に用いる高品質な乱数性だけでなく、IoT 端末に適した低エネルギー特性が重要となる。また、電源電圧や温度の環境条件の変化、攻撃者による人為的攻撃などに対しても乱数性が損なわれない幅広い耐性が求められる。

一般に TRNG は、物理現象からランダムな生の乱数列を生成する TRNG コアと、生乱数から高品質な乱数を抽出する後処理の二つの部分から構成される。本研究はこの両方を対象としていて、全体として低エネルギーで幅広い耐性を持つ TRNG を得ることを目的としている。

後処理では von Neumann の方法が簡易で低エネルギーな手法として知られているが、抽出効率が高々25%、つまり 2bit の生乱数から 1bit の高品質乱数が最大 50%の確率でしか抽出できない、という課題があった。この対策として、von Neumann 法を繰り返す逐次 von Neumann 法と、N-bit(N は 3 以上の整数) を一括処理する N-bit von Neumann 法、の理論が報告されている。 N-bit von Neumann は、抽出効率が N と伴に向上することと、低エネルギーに有利な 1/N 分周動作が出来る利点がある。しかし、抽出効率の理論値と現実値にギャップが有る、論理の複雑さが N の指数関数で増すといった欠点があるため、回路実装では逐次 von Neumann 法が先行していた。

一方、TRNG コアで採用したラッチ方式は、他のリング発振器方式などと比べて、乱数生成のためのデータ遷移が一度きりなので低消費電力化に有利な利点がある反面、ラッチを構成するインバータ対の製造ばらつきによるミスマッチに敏感で、出力データが 1 または 0 に固定しやすい欠点がある。このため従来のラッチ形 TRNG は、複雑なフィードバック制御、もしくは 256 個ものラッチの排他的論理和が必要で、利点が活かせれていなかった。

以上の考察に基づいて、本論文は上記の欠点を克服し、原理的長所を活かした N-bit von Neumann 後処理とラッチ形 TRNG コアを提案している。

後処理では、ウェイティングストラテジーという新アルゴリズムで抽出効率の理論と現実のギャップを埋め、階層アーキテクチャと入力シンボルに基づくコード設定を考案して、論理の複雑さを低減している。

TRNG コアでは、ミスマッチ自己補償と乱雑さの源である雑音電圧の強化に関する二個の新規技術で、ラッチ形でありながらフィードバック制御無しに安定した生乱数生成に成功した、技術の基本原理は、前者がラッチの初期状態をメタ安定点に誘導する、後者が減衰発振における共振現象を利用するというもので、コンセプトから独創的である。

このラッチ形 TRNG コアと 8bit von Neumann 後処理 VN_8W からなる TRNG を 130nm CMOS で設計、試作(大学外部に委託)し、PVT(Process, Voltage, Temperature)ばらつき、エージング、人為的攻撃に対しても乱数性の耐性を実証している。また、低エネルギー特性の実測評価も行っている。

本論文は五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。

第一章"Background"では、IoT 時代のハードウェアセキュリティを述べたうえで、その中での真乱数発生回路 TRNG の位置づけと適用事例、基本構成、低エネルギー化の動向について概説している。

第二章"Preliminaries"では、本論文の準備として、まずここで用いた(1)乱数性評価指標、(2)NIST SP800-22 と同 SP800-90B による標準的乱数テスト、(3)耐性評価のための PVT ばらつき、長期信頼性加速係数、電源ノイズ注入による攻撃方法、(4)面積とエネルギーに関する性能指標を説明している。

次に、先行研究による各種の後処理方式と本研究で採用した N-bit von Neumann の位置づけ、各種の TRNG コアと本研究で使用したラッチ形 TRNG コアの位置づけ示している。そして本研究の主たる課題が、後処理では現実的抽出効率の改善と論理の複雑さ低減にあることを、TRNG コアではラッチ回路のミスマッチ低減と雑音強化にあることを、それぞれ明らかにしている。

第三章"VN_N based Post-Processing Technique Having High Extraction Efficiency and Low Energy"では、高抽出効率かつ低消費エネルギーな N-bit von Neumann 後処理を実現するため、アルゴリズム、アーキテクチャ、論理の各レベルで改善をしている。アルゴリズムレベルでは、高品質乱数抽出にウェイティングストラテジーと呼ぶ過程を加えて現実の抽出効率を向上した。例えば 4bit ではウェイティングストラテジーを適用することで抽出効率は 40.63%から 46.88%に改善した。これは 6bit でそれを適用しない 41.67%よりも高い。小さな N 値で高い抽出効率が得られるので、2 の N 乗で増える複雑さの軽減にも効果がある。論理レベルでは、入力シンボルに基づくコード設定を提案して、論理が約 2/8 に簡略化されることを示している(4bit の場合)。アーキテクチャレベルでは、入力 Hamming Weight に基づく階層アーキテクチャにより、複雑さを約 4.5 分の 1 に低減した(8bit の場合)。

これらを総合して、8bit で 62.21%の高い抽出効率の VN_8W を設計した。N_bit 方式の利点を生かして、エネルギー低減に効果的な 1/8 分周動作も行った。130nm CMOS による実測結果では、0.45V で 0.18pJ/bit の低エネルギーを実証した。これは同時に設計した先行研究(V. Roˇzic´ら IEEE HOST 2016)に基づく逐次 von Neumann よりも 20%以上のエネルギー削減である。

第四章" Latch-Based True Random Number Generator Featuring Mismatch Compensation and Random Noise Enhancement"では、ラッチ形 TRNG コアとそれに後処理を加えた TRNG 全体について述べている。まず

TRNG コアにおいて、ミスマッチ自己補償の基本原理であるラッチ初期状態のメタ安定点への誘導とその回路、雑音強化の基本原理である減衰発振における共振現象とその回路を提案する。回路シミュレーション結果では、前者では補償用ゲート容量を付加することでミスマッチの 66.3%が補償させることを、後者ではインバータのイコライズ回路に抵抗挿入して減衰振動モードに設定することで雑音電圧が約 3 倍強化されることを示している。このように雑音対ミスマッチ比を大きくすることで、フィードバック制御することなく、4 個のラッチから成る TRNG コアだけで 6σ の製造ばらつき耐性を持つことが実測で示された。これは先行研究(N. Torii ら EURASIP Journal of Information Security 2016)の 256 個の 1/64 である。

次に、このラッチ形 TRNG コアと VN_8W 後処理を組み合わせた TRNG を 130nm CMOS で設計、試作し、特性を検証した。電源電圧範囲 0.3V から 1V、温度範囲-20℃から 100℃の広い環境範囲や電源ノイズ注入攻撃下においても、標準的な乱数テスト NIST SP800-22 と同 SP800-90B に合格することを実証している。また、11 年に相当するエージング加速試験でもエントロピー劣化はほとんどないことを示した。高品質乱数 1bit あたりの消費エネルギーは 0.3V で 0.186pJ/bit と、世界最小級である。

本章の最後には、本研究の主眼ではなかったがスループット特性についても考察を加えて、IoT に限らない広い応用分野への準備としている。

第五章”Conclusions”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 TRNG の低エネルギー化と耐性の強化を目的として、後処理と TRNG コアの両方に解決策を提案し 130nm CMOS で実機評価した。後処理では、N-bit von Neumann にアルゴリズム、アーキテクチャ、論理の各レベルからアプローチし、62.21%の高抽出効率と 0.18pJ/bit(0.45V)の低エネルギーを達成した。ラッチ形 TRNG コアでは、ラッチ初期状態の誘導によるミスマッチ自己補償と、減衰発振における共振現象を利用した雑音強化により、安定な乱数生成に成功した。両者を組み合わせた TRNG の消費エネルギーは 0.186pJ/bit(0.3V)と小さくて、エネルギー制約の強い IoT 端末に適している。また、PVT ばらつきやエージング、更には電源ノイズ注入攻撃にも幅広い耐性があり、実用性が高い。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

2022 年 5 月 12 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(学術) (神戸大学) 吉増 敏彦

早稲田大学教授 博士(工学) (筑波大学) 大澤　隆