

小型・低消費電力の物理乱数発生装置を開発！

ライセンス契約を受けていただき 本発明の実用化を目指していただける企業様を求めます。

従来の真の乱数生成器(TRNG)に比較して、自律的にバラツキの影響を相殺し、安定動作させる回路構成によって、小型・1/10以下の低消費電力化を実現しました。

◆背景

乱数生成器は、プロセッサ、セキュアな鍵の生成、識別番号(ID)の生成、モンテカルロシミュレーションなどに幅広く使われています。真の乱数生成器(TRNG: True Random Number Generator)は自然に存在する予測不可能な現象に基づいて値を生成するため、ソフトウェア乱数生成器に比較して物理攻撃に強いことが知られています。しかしながら、TRNG内で熱雑音の物理現象をデジタル値に変換する過程においてランダム性が乱れる現象が発生し、またTRNGに使われる部品の経年劣化、温度変化に伴う特性変化に対しても対策をとる必要があります。

さらに従来のTRNGは、出力を監視し、フィードバックし、複雑な後処理回路の付加してバラツキを抑えるために、大面積で消費電力が大きくなっています。

◆発明概要と利点

本発明は、2つのインバータ回路を含み、乱数データを出力可能なラッチ回路と、自律的にバラツキの影響を相殺し安定動作させる回路と、を備えた、物理乱数発生装置です。

➤ 自律的にバラツキの影響を相殺し安定した動作を実現（図1）

単体回路における1の確率は0.5を中心に分布します。

➤ 消費電力の大幅低減が可能（図2）

従来のTRNG（Latch w/cal.）と比べ、本発明（TRNG strong Arm Larch）では、消費電力で1/10以下となります。

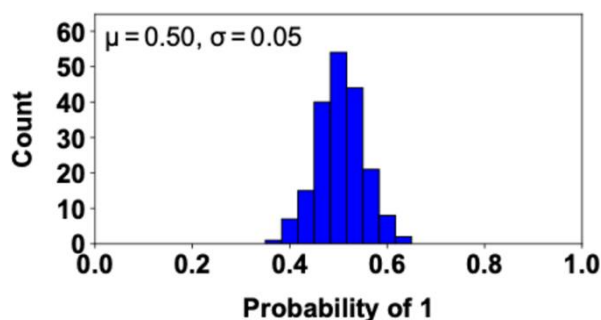


図1 単体回路における1の確率分布

図1 単体回路における1の確率分布

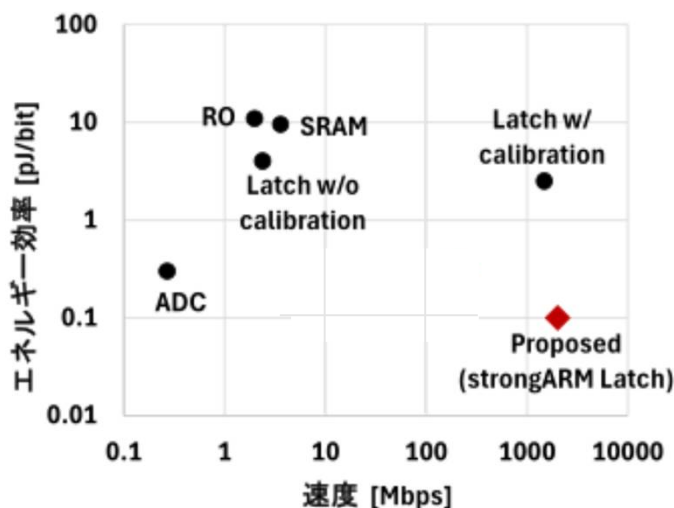


図2 従来のTRNGと本発明のTRNGとの比較

◆研究段階

- ・ CMOS試作にて回路動作確認済

◆適応分野

- ・ AI、通信等乱数発生回路が必要な装置

◆希望の連携形態

- ・ 実施許諾契約
 - ・ オプション契約
(技術検討のためのF/S)
- ※本発明は京都大学から特許出願中です。

◆お問い合わせ先

京都大学産学連携担当株式会社 TLO 京都

〒606-8501
京都市左京区吉田本町京都大学
成長戦略本部内
(075)753-9150
licensing_ku@tlo-kyoto.co.jp

