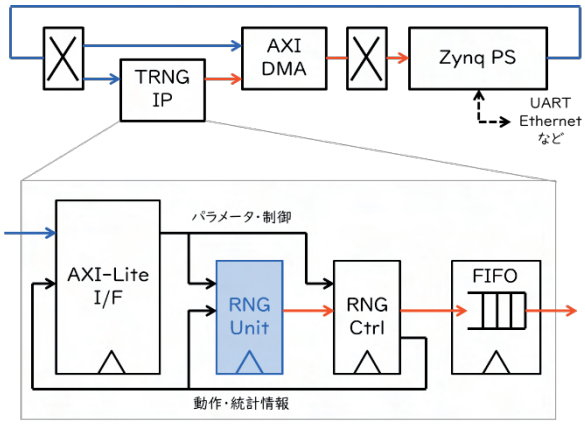
E26 FPGA向け真性乱数生成回路とその評価基盤

工学部・電気学科・准教授・藤枝　直輝
nfujieda@aitech.ac.jp

キーワード　FPGA、真性乱数、セキュリティ、ジッタ

概要



真性乱数生成回路(TRNG)は、予測不可能な物理現象から乱数を生成する回路で、暗号鍵の生成や認証プロトコルなどのセキュリティ応用に利用できます。本研究室では、FPGA (Field Programmable Gate Array)の回路素子を用いたTRNGの研究を進めています[1-2]。FPGAシステムの中にTRNGを組み込めば、部品点数・システムコストの削減が期待できます。

乱数の質を効率的に評価するには、大量の乱数を自動的かつ連続的に生成・評価する必要があります。こうした評価基盤構築のノウハウも豊富に持っています。これまでに、FPGA System-on-Chipを用いたPYNQというプラットフォームを対象に、複数のTRNGの方式に対応した評価基盤を構築しており、そのソースコードをGitHubで公開しています[3]。

セールスポイント

1．アルゴリズムで乱数を生成する場合と比べ、乱数値の予測が困難です。
2．FPGAの回路の一部としてTRNGを実装するため、外付けの部品が不要です。
3．対象のデバイスやボードに合わせた評価を速やかに始められます。

企業等での活用例、今後の展望等

1．FPGAを用いた組込みシステムのセキュリティ機能を強化できます。
2．動作環境や素子のばらつきに対する安定性向上について、研究を継続しています。

参考資料

[1] N. Fujieda, S. Takashima, “An MMCM-based high-speed true random number generator for Xilinx FPGA,” Intl. J. Netw. Comput., 11(2)154-171, 2021.
[2] N. Fujieda, “On the feasibility of TERO-based true random number generator on XIlinx FPGAs,” in FPL 2020, pp. 103-108, 2020.
[3] N. Fujieda, Versatile TRNG IP Core for Evaluation on PYNQ Platform, online, available at 〈https://github.com/nfproc/TRNG_IP〉.