2 つの断熱量子磁束パラメトロン乱数生成器を用いた多出力乱数生成器の評価

Evaluation of a multi-output random number generator using two adiabatic quantum flux parametron random number generators

横国大院理工 [1]，横国大 IAS[2]　○(M1) 羅文輝 [1]，竹内尚輝 [2]，陳オリビア [2]，吉川信行 [1,2]

Dept. of Electrical and Computer Eng., Yokohama Natl. Univ. [1], IAS, Yokohama Natl. Univ. [2]

°Wenhui Luo[1], Naoki Takeuchi[2], Olivia Chen[2], Nobuyuki Yoshikawa[1,2]

E-mail: luo-wenhui-dv@ynu.jp

従来の乱数生成器（RNG）はアルゴリズムを使用して擬似乱数を生成するのに対し、本研究では断熱量子磁束パラメトロン（Adiabatic Quantum-Flux-Parametron：AQFP）回路 [1] に熱ゆらぎに起因する確率的挙動を導入することで、真性乱数の生成を実現する。特に本発表では、2 つの AQFP-RNG を用いて複数の乱数列を生成する多出力 RNG を実証する。

Fig. 1 に示すように、多出力 RNG は、エントロピーソースである 2 つの AQFP-RNG と、2 つの乱数列から複数の乱数列を生成する XOR ゲートアレイで構成される。AQFP-RNG は、出力“1”または“0”の確率を制御するためにオフセット入力電流が印加された AQFP バッファチェーンである。2 つの AQFP-RNG によって生成される乱数列内及び乱数列間には相関がないため、2 つの乱数列を各出力ポートでタイミングをずらして XOR ゲートに入力することで、複数の乱数列を生成できる。AIST 10kA/cm^2 Nb 高速標準プロセス（HSTP）[2] を使用して多出力 RNG を設計および作製し、実験により生成された乱数の質を評価した。作製した 4 ビット RNG のチップ写真を Fig. 2 に示す。実験結果や、評価結果から得られた設計の優位性等については当日報告する。

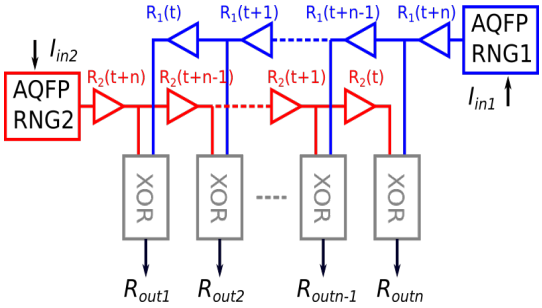

Fig. 1 RNG の概略図

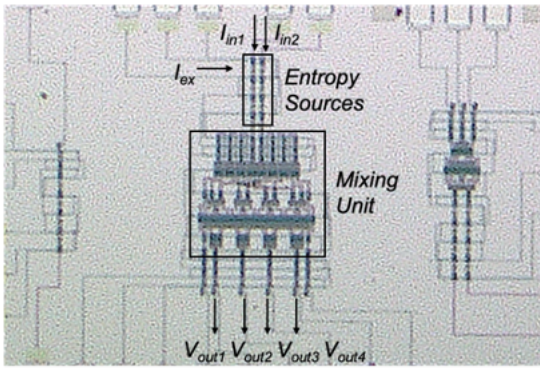

Fig. 2 チップ写真

謝辞

本研究に使用された回路は、産業技術総合研究所 (AIST) の超伝導クリーンルーム CRAVITY を用いて作成された。本研究は JSPS 科研費（No.18H01493，No.19H05614）の助成を受けたものである。

参考文献

[1] N. Takeuchi, D. Ozawa, Y. Yamanashi, and N. Yoshikawa. Supercond. Sci. Tech., vol. 26, no. 3, p. 035010, 2013.

[2] N. Takeuchi et al., Supercond. Sci. Technol., vol. 30, no. 3, p. 035002, Mar. 2017.