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 ２５ 日現在

機関番号：３７１１２
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１２３１

研究課題名（和文）超伝導単一磁束量子回路によるハードウェア乱数生成器とストカスティック演算への応用

研究課題名（英文）Hardware random number generator using superconducting single flux quantum circuits and the application of stochastic logic

研究代表者

小野美　武（Onomi, Takeshi）

福岡工業大学・工学部・准教授

研究者番号：７０３１２６７６

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究では、単一磁束量子回路によるストカスティック論理演算のためのハードウェア乱数生成器の提案と集積回路上での動作検証を行った。 ジョセフソン発振を利用した発振器ベースの真性乱数生成器の構成を新規に提案し、Nb/AlOx/Nbジョセフソン接合集積回路を利用した回路の設計・試作・測定を行い、実測での動作検証に成功した。同回路から生成される乱数列を検証し、品質の良い乱数列が得られることを確認した。さらに、提案した回路の安定性を向上させるための回路の改良を実施し、電源電圧変動に対する乱数品質の変動が少ない回路の提案と検証を実施した。

研究成果の学術的意義や社会的意義
超伝導体の単一磁束量子を情報担体とする回路を利用した、発振器ベースの独自のハードウェア乱数生成器を提案した。本回路は超伝導体を利用した集積回路で設計・試作が行われ、実験的に動作検証に成功した。この回路は人工神経回路網のハードウェア化を確率的なパルス信号で計算を行うストカスティック演算に応用するものを目指したものであり、将来の知的な情報処理システム実現への応用に対して学術的な意義があるものである。

研究成果の概要（英文）：A hardware random number generator for stochastic logic using superconducting single flux quantum circuits was proposed and demonstrated experimentally on an integrated circuit. A new true random number generator based on a signal generator using Josephson oscillation was proposed. The proposed random number generator was designed, fabricated and measured using Nb/AlOx/Nb Josephson junction integrated technology. The generator was demonstrated experimentally, and it was further confirmed that random numbers generated by this circuit have good qualities. Furthermore, improved design of the random number generator with less variation in random number quality with respect to changes in circuit bias voltage was also proposed and investigated.

研究分野：電気電子工学

キーワード：超伝導　単一磁束量子回路　乱数生成器　ストカスティック演算

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

単一磁束量子を情報担体とする回路（以下、SFQ 回路）は、100GHz を超える動作周波数で動作が見込まれる最も有望な回路である[1],[2]。現在の半導体回路の単純な高速化･高密度化では、電力消費に伴うチップ表面の熱放出が困難となることが予想され、半導体回路にとって代わり得る高速・低消費電力回路として最も大規模な回路が実現されているのが SFQ 回路である。SFQ 回路では信頼性の高い Nb/AlOx/Nb ジョセフソン接合を用いた回路により、数千個～数万個程度の接合を集積化した回路が実現されている。現在の超伝導回路集積化技術によって試作された回路はゲートレベルで 50～100GHz の動作周波数を持ち、パイプライン化した回路構成によるシステムレベルでは数 10GHz の動作周波数である。日本におけるこれらの集積回路は、産業技術総合研究所より提供される信頼性の高い集積化チップを用いて実現されており[3]、SFQ を利用したディジタル応用は高速・低消費電力性から次世代の情報処理技術として期待されている。

一方、近年 AI 技術に代表されるような、従来の計算機回路に基づくハードウェアやプログラム上で実装されることを意図したアルゴリズムとは異なる、生体が行っている情報処理機能を参考とした情報処理技術が進展してきている。そのような情報処理においては、ニューラルネットワークに代表されるような、確率的にあいまいな誤差を伴う信号でも正解または正解に近い解を導きだせる汎化能力を有している。このような信号の演算においては、必ずしも従来の計算機回路に基づく厳密な数値計算を必要としない場合も多い。そのような演算を実現する手法の一つにストカスティック論理演算[4]-[6]（信号のレベルを確率的なパルス頻度で表現して演算を行う）が挙げられる。ストカスティック論理表現を用いる最大の利点は、２入力の乗算を AND ゲート一つで実現することが可能となる点である。現状では半導体回路に比べて超伝導回路の集積度はそれほど高くないため、より少ない素子数で演算が可能となるストカスティック論理方式は超伝導回路にとって有効な手段である。

上述の背景から、ポスト半導体集積回路としての SFQ 回路の優れた信号処理能力をあいまいな演算が適用可能なシステムに応用するための演算処理回路の動作実証を行うことは有意義なことと考えられる。

２．研究の目的

本研究では、SFQ論理演算回路による物理乱数生成器、およびその乱数生成器を用いたストカスティック論理演算回路の実験的な検証を、Nb/AlOx/Nbジョセフソン接合を用いた超伝導集積回路により行うことを目的としている。単一磁束量子（SFQ）回路はその高速・低消費電力性から信号処理回路への応用が期待されており、素子数の少ない回路で演算可能なストカスティック論理方式を利用することで、ソフトコンピューティングなどに適用可能なハードウェアコストの低い情報処理回路としての応用が期待される。ストカスティック論理演算に必要なハードウェアコストの低い乱数生成器の提案と開発を行い、ストカスティック演算への応用を目指す。

３．研究の方法

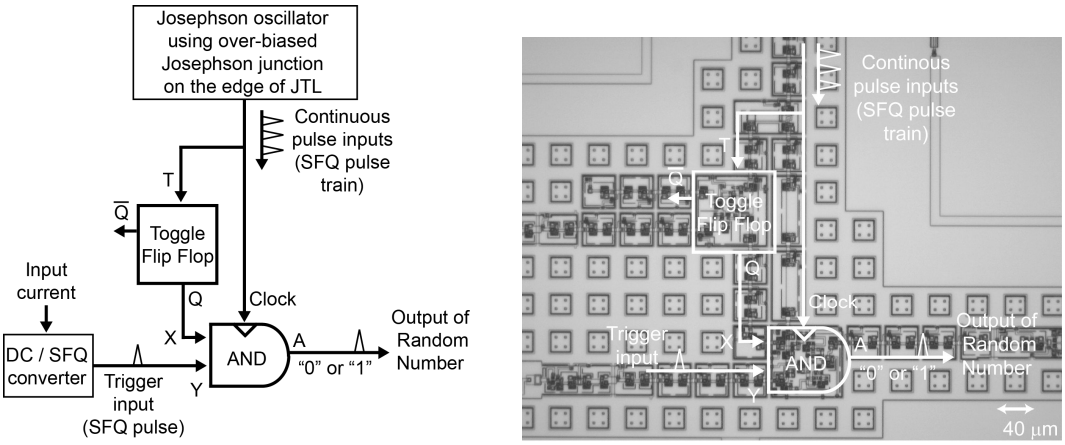
ストカスティック論理演算に必要なハードウェアコストの低い乱数生成器の提案と開発を、数値解析・設計・チップ試作・測定により行う。SFQ ディジタル回路としての同生成器の設計は比較的容易であるが、熱雑音による回路の揺らぎが乱数取得に有効に機能するかを、熱雑音を含む数値解析によって十分な検証を行う。特に、分周器入力の SFQ パルス列生成を行うジョセフソン発振器に加えるバイアス抵抗の熱雑音や、乱数取得トリガー入力ラインに存在する抵抗などの値を調整することで、どのような品質の乱数が取得できるかを探る。その後 CAD によるレイアウト設計を経て産業技術総合研究所のチップファンダリを利用した Nb/AlOx/Nb 集積回路によるチップを入手し、その乱数の評価を行う。

乱数生成器の安定性を乱数品質の検証から評価し、回路パラメータや電源電圧などに対するマージン向上の検討、および将来の高速化への性能向上に対しての検討も合わせて実施し、ストカスティック論理演算への適用を検討する。

４．研究成果

本研究では、ストカスティック論理演算のための SFQ 論理演算回路による物理乱数生成器の提案と検証を中心に、集積回路上での動作実証も含めて研究を行ってきた。以下にその成果を示す。

(1) 任意のディジタル値をストカスティックパルスコーディングするには一様乱数と入力値をコンパレーターで比較することにより行う。そのため、パルスコーディングには乱数生成器が必



(a) (b)

図 1. (a) ジョセフソン発振を利用した発振器ベースの真性乱数生成器の構成（それぞれのロジックセルはジョセフソン伝送線路により接続される）. (b) Nb/AlOx/Nb ジョセフソン接合集積回路による乱数生成器の集積化

要となるが、従来から提案してきた疑似乱数生成器よりハードウェアコストの低い独自の物理乱数生成器を提案・開発を行った。図 1 (a)に新しく提案を行った、ジョセフソン発振を利用した発振器ベースの真性乱数生成器の構成を示す。基本要素は、ジョセフソン伝送線路(JTL)端部の接合を発振源とした SFQ パルス列の発振回路（発振周波数は約 30～40 GHz）と、クロック信号毎に “0”, “1”の出力信号(Q) を繰り返す TFF、および回路の内部状態(X)と乱数を呼び出すためのトリガー信号(Y) の積をとる AND ゲートで構成される。AND ゲートの X 入力の内部状態は、クロック毎に “0,” “1” を繰り返すこととなり、トリガー信号 (Y) を任意のタイミングで入力すると乱数が取得される。

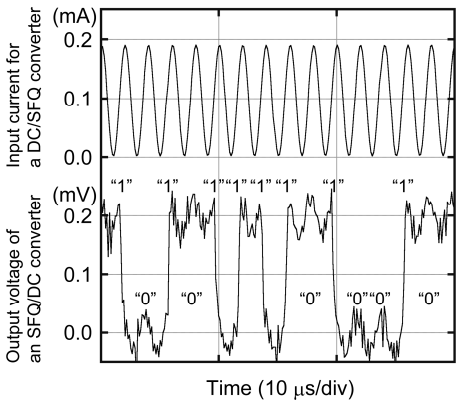


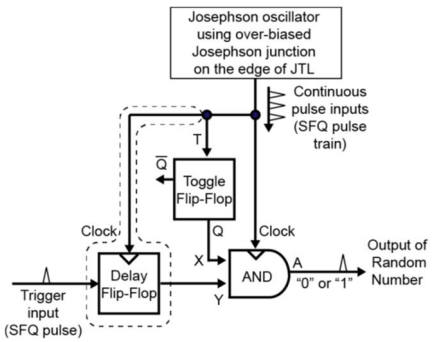
図 2. 集積化を行った乱数生成器の低温での測定結果（入力電流はトリガー信号を生成するための DC/SFQ コンバータへの電流を示し、正弦波の立ち上がりにおいて SFQ 信号を生成する。乱数の出力は SFQ/DC コンバータの出力として検出され、0.2 mV への電圧遷移時に SFQ 信号を検出している。）.

本回路の動作実証を行うため、産業技術総合研究所のチップファンダリを利用した Nb/AlOx/Nb 集積回路のレイアウト設計と集積化を行った。図 1(b)は集積回路の顕微鏡写真である。図 2 に液体ヘリウム下の低温での実測結果を示す。入力電流はトリガー信号を生成するための DC/SFQ コンバータへの電流を示し、正弦波の立ち上がりにおいて SFQ 信号を生成する。乱数の出力は SFQ/DC コンバータの出力として検出され、0 V から 0.2 mV へ、または 0.2 mV から 0 V への電圧遷移時に SFQ 信号を検出している。図中の出力電圧は入力のトリガー信号に対してランダムに遷移しており、乱数列が生成されていることが確認できる。このハードウェア乱数生成器から生成された乱数列を、2 万個を 1 セットとするバイナリ乱数列 25 セットに対して FIPS 140-2 の乱数検定[7]により評価し、検定をパスする乱数列が得られていることを確認した。 （発表論文 [8]）

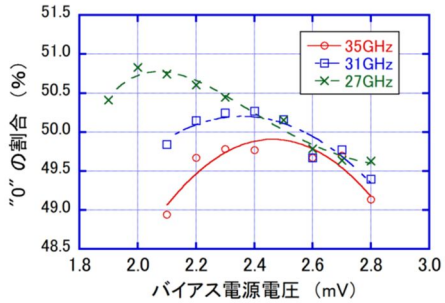
(2) 提案を行った発振器ベースの真性乱数生成器において、ジョセフソン接合の臨界電流密度 J_c を増加(J_c = 10 kA/cm²)させたプロセスによる試作と動作検証を行った。その結果、同プロセスによる回路においても乱数生成器の機能が実現され、将来の高速化への見通しが得られる結果となった。また、バイナリ乱数（“0”, “1”）の生成割合のバイアス電源依存性が評価され、電源電圧の変動により乱数生成割合が 50%から変動することが確認された。 （発表論文 [9]）

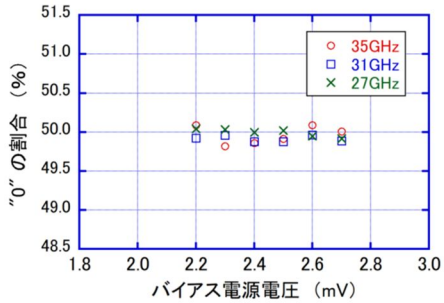
(3) バイナリ乱数生成割合がバイアス電源電圧により変動することを改善するため、乱数生成器の構成を改良した図 3(a)に示す回路の提案を行った。トリガー信号入力ラインに D フリップフロップを挿入することで、回路の内部クロックの一定タイミングでトリガーが入力するように変更したものである。図 3(b)は従来の回路の乱数生成割合のバイアス電源依存性を示したグ

ラフで、図 3(c)が改良後の回路の同依存性を数値解析により評価した結果である。この結果から、乱数の “0,” “1”の生成割合のバイアス依存性をほぼ無くすことが可能な構成を示すことができ、乱数品質の安定性向上に寄与する結果が得られた。　（学会発表 [10]）



(a)

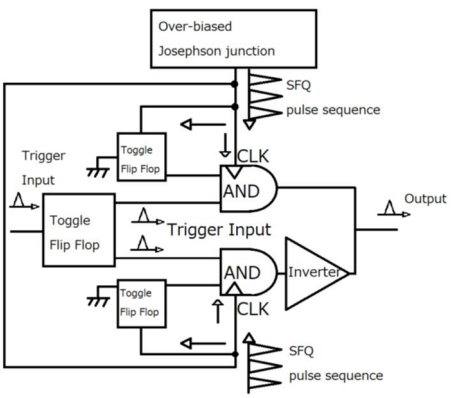


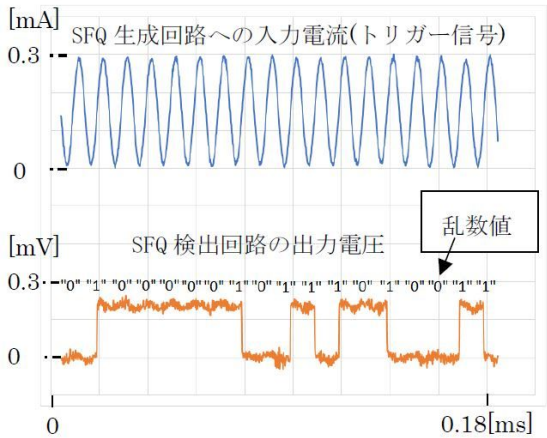


(b)　(c)

図 3.　(a) 乱数生成割合のバイアス電源電圧依存性を低下させるためのジョセフソン発振を利用した真性乱数生成器の構成. (b) 従来の回路構成による乱数生成割合のバイアス電源依存性の数値解析結果.　(c) 改良した回路構成による乱数生成割合のバイアス電源依存性の数値解析結果.

(4)　２つの乱数生成器を組み合わせ、全体での乱数発生の割合を50%に補償するためのジョセフソン発振を利用したSFQ 回路による相補型真性乱数生成器の提案を行い、同方式による乱数生成器の低温での動作検証を行った。図4(a)は相補型乱数生成器の構成であり、低温測定を行った結果が(b)である。乱数生成器としての動作が確認されたが、乱数出力を検出するSFQ/DCコンバータの不具合により、確率的にSFQ信号の一部が検出エラーとなっていることが確認され、乱数の生成割合が50%にはならなかったものの、電源電圧変化に対して乱数生成割合の変動が少ない、良好な結果が得られた。（学会発表 [11]）





(a)　(b)

図 4.　(a) ジョセフソン発振を利用した相補型真性乱数生成器の構成. (b) Nb/AlOx/Nb　ジョセフソン接合集積回路による同回路の測定結果の一例

以上の結果から、本方式による乱数生成器を利用することで、乱数生成に対するハードウェアコストの低いストカスティック論理演算への応用が期待される結果が得られた。

＜引用文献＞

[1] K. Nakajima, et. al., *IEEE Trans. Appl. Superconduct*., vol.1, no.1, pp.29-36, (1991)
[2] K. Likharev and V. Semonov, *IEEE Trans. Appl. Superconduct*., vol.1, no.1, pp.3-28, (1991)
[3] S. Nagasawa, et. al., *IEICE Trans. Electronics*, vol. E97-C, pp. 132-140, (2014)
[4] B. D. Brown, and H. C. Card, *IEEE Trans. Computaters*, vol. 50, no. 9, pp.891-905, (2001)
[5] S. Sato, et. al., *IEEE Trans. Neural Networks*, vol. 14, no. 5, pp.1122-1127, (2003)
[6]鬼沢直哉、他、電子情報通信学会基礎・境界ソサイエティ *Fundamental review*, vol. 11, no. 1, pp.28-39, (2017)
[7] NIST, “Security requirements for cryptographic modules,” FIPS pub. 140-2, May 2001.
[8] T. Onomi and Y. Mizugaki, *IEEE Trans. Appl. Superconduct*., vol.30, no.1, p. 1301305, (2020)
[9] K. Sato, N. Sega, Y. Somei, H. Shimada, T. Onomi, and Y. Mizugaki, *IEICE Transactions on Electronics*, vol. E105-C, pp. 296-299, (2022)
[10] 小野美武、2022 年電子情報通信学会総合大会、C-8-17,(2022)
[11] 小野美武、吉田渉悟，2023 年応用物理学会九州支部講演会、25Da-1，(2023)

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 K. Sato, N. Sega, Y. Somei, H. Shimada, T. Onomi, and Y. Mizugaki	４．巻 E105-C
２．論文標題 Evaluation of a True Random Number Generator Utilizing Timing Jitters in RSFQ Logic Circuits	５．発行年 2022年
３．雑誌名 IEICE Transactions on Electronics	６．最初と最後の頁 296-299
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transele.2021SES0001	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 －

１．著者名 Takeshi Onomi and Yoshinao Mizugaki	４．巻 30
２．論文標題 Hardware Random Number Generator Using Josephson Oscillation and SFQ Logic Circuits	５．発行年 2020年
３．雑誌名 IEEE Transactions on Applied Superconductivity	６．最初と最後の頁 1301305
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TASC.2020.2992248	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 －

〔学会発表〕　計13件（うち招待講演　1件／うち国際学会　2件）

１．発表者名 小野美武、吉田渉悟
２．発表標題 ジョセフソン発振を利用した相補型物理乱数生成器の動作検証
３．学会等名 2023年応用物理学会九州支部講演会
４．発表年 2023年

１．発表者名 Y. Mizugaki, K. Sato, H. Shimada, and T. Onomi
２．発表標題 Random Number Generation Utilizing Timing Jitters of Single-Flux-Quantum Propagation
３．学会等名 Proceedings of 2023 Photonics & Electromagnetics Research Symposium（国際学会）
４．発表年 2023年

１．発表者名
吉田 渉悟、 小野美 武

２．発表標題
ジョセフソン発振を利用した相補型物理乱数生成器の集積回路設計

３．学会等名
2022 年応用物理学会九州支部学術講演会

４．発表年
2022年

１．発表者名
小野美 武

２．発表標題
ジョセフソン発振を利用した発振器ベースの乱数生成器への発振周期揺らぎ機構の導入

３．学会等名
電子情報通信学会超伝導エレクトロニクス研究会

４．発表年
2023年

１．発表者名
古賀仁誌、横山聡、小野美武

２．発表標題
超伝導物理乱数生成器に用いる AND ゲートの回路パラメータの最適化

３．学会等名
2021 年応用物理学会九州支部学術講演会

４．発表年
2021年

１．発表者名
吉田渉悟、小野美武

２．発表標題
ジョセフソン発振を利用した相補型物理乱数生成器の設計

３．学会等名
2021 年応用物理学会九州支部学術講演会

４．発表年
2021年

１．発表者名
小野美武

２．発表標題
ジョセフソン発振を利用したＳＦＱ真性乱数生成器におけるバイナリ乱数生成割合のバイアス電源電圧依存性の低減化

３．学会等名
2022年電子情報通信学会総合大会

４．発表年
2022年

１．発表者名
古賀仁誌、小野美武

２．発表標題
単一磁束量子発振器に基づく超伝導乱数生成器の乱数品質とAND ゲートのスイッチング時間の関係

３．学会等名
2020年応用物理学会九州支部学術講演会

４．発表年
2020年

１．発表者名
小野美武

２．発表標題
単一磁束量子回路による発振パルスサンプリング型真性乱数生成器の開発

３．学会等名
電子情報通信学会超伝導エレクトロニクス研究会、共催：東北大学電気通信研究所共同プロジェクト「量子検出のための高Q値マイクロ波共振器に関する研究」研究会（招待講演）

４．発表年
2020年

１．発表者名
Takeshi Onomi

２．発表標題
Design of a Hardware Random Number Generator using Josephson Oscillation and SFQ Logic Circuits

３．学会等名
The 17th IEEE International Superconductive Electronics Conference 2019（国際学会）

４．発表年
2019年

１．発表者名
小野美 武、水柿 義直

２．発表標題
SFQ パルス発振器に基づくSFQ 乱数生成器の試作

３．学会等名
2019年電子情報通信学会エレクトロニクスソサエティ大会

４．発表年
2019年

１．発表者名
小野美 武

２．発表標題
単一磁束量子発振器に基づく超伝導乱数生成器の乱数品質の検証

３．学会等名
2019年応用物理学会九州支部学術講演会

４．発表年
2019年

１．発表者名
小野美　武

２．発表標題
結合SQUIDs ゲートを利用したシュミットトリガー回路による弛張発振器の発振周波数と回路パラメータの関係

３．学会等名
2018年応用物理学会九州支部学術講演会

４．発表年
2018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
研究協力者	水柿　義直 (Mizugaki Yoshinao)		

6．研究組織（つづき）

	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
研究協力者	古賀　仁誌 (Koga Hitoshi)		
研究協力者	吉田　渉悟 (Yoshida Shogo)		

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