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　４ 年　 ６ 月 １４ 日現在

機関番号：１３９０１
研究種目：研究活動スタート支援
研究期間：2020～2021
課題番号：２０Ｋ２２４１２

研究課題名（和文）Research on Intrinsic Mechanism of True Random Number Generation for Absolutely Secure Communications by Using Half Flux Quantum Circuit

研究課題名（英文）Research on Intrinsic Mechanism of True Random Number Generation for Absolutely Secure Communications by Using Half Flux Quantum Circuit

研究代表者

李　峰（Li, Feng）

名古屋大学・工学研究科・研究員

研究者番号：００８８８３８１

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：本研究では、SFIS（Nb / NiPd / Al-AlOx / Nb）π-JJの特性を温度依存性で特性評価しました。 固有のπ位相シフトそれでも10mKの段階で維持でき、臨界電流密度はわずかに増加するだけです。 HFQTFFの正しい動作は最大6.7 GHzで測定され、SFQ/DC変換を備えたシャントされていない従来のシングルフラックス量子（SFQ）回路π-JJに基づくと、4Kで実証されました。これらの結果は、10mKでの量子ゆらぎで動作するHFQ回路のTRNG、または量子ビットの制御および読み出し回路のデモンストレーションの基礎を築きました。

研究成果の学術的意義や社会的意義
This research develope a new fabrication process for crygenic logical circuit, whose power consumption is extremely low, and can be used as the control or readout circuits of Qubits. The proposed TRNG operating with quantum fluctuation is an important element for future highly secure systems.

研究成果の概要（英文）： To demonstrate a true random number generator (TRNG) based on quantum fluctuation,an novel Half-flux-quantum (HFQ) balanced comparater composed of π-π-π SQUIDs was proposed as TRNG. The nominal critical current of π-π-π SQUIDs can be reduced to 100 nA, which means the HFQ circuit can operate in the quantum regime at 10 mK stage.
In this study,the properties of SFIS (Nb/NiPd/Al-AlOx/Nb)π-JJs were characterized with temperature dependence. The intrinsic π phase shift can still be mentained at 10 mK stage and the critical current density is only slightly increased, which is important for HFQ circuits. The correct operation of HFQ TFF was measured up to 6.7 GHz and the un-shunted conventional single-flux-quantum (SFQ) circuits with SFQ/DC converts based on π-JJs were demonstrate at 4 K. These result set the foundation for demonstration of a HFQ circuit based TRNG that operating with quantum fluctuation or the control and readout circuits for Qubit at 10 mK.

研究分野：Superconducting electronics

キーワード：Half-flux-quantum　balanced comparator　π-π-π SQUIDs　quantum fluctuation　random number generator　superconducting circuits

１．研究開始当初の背景

Random number is an important ingredient in science, art, statistics, cryptography and gambling. Different applications require different level of randomness. At present, we can easily generate a series of pseudorandom number with an algorithm, however, if others know the seed of your algorithm, these numbers will lose their randomness. To provide completely safety in cryptography, true random number generators (TRNGs) will be demanded. So far, conventional TRNG can be realized by various classical physical phenomena such as shot noise, spin reversal and laser chaos. Quantum random number generators (QRNGs) based quantum phenomenon also have been developed, like photon counting and phase noise. However, it is still an unsolved question whether the quantum phenomenon is more random than the classical (e.g., thermal) one. A device or circuit that can operate both in the classical and quantum regime can shed light on the understanding of the randomness of quantum and thermal fluctuation.

Until now, a Single Flux Quantum (SFQ) based RNG operating with thermal noise has been demonstrated, whose bit energy ($\sim I_c\Phi_0$) is determined by the critical current I_c of Josephson junction [1]. However, further decreasing of the critical current of Josephson junction is limited by the present available fabrication process while a RNG operating near the quantum limit has an extremely low energy fluctuation ($h/2\pi \approx 10^{-34}$ Js, in which h is the Plank's constant) during the circuit operation. The newly proposed Half Flux Quantum (HFQ) circuits, consisting of 0-π superconducting quantum interference devices (SQUIDs), is expected as a promising candidate for demonstration of QRNG [2]. As an energy efficient digital circuits, HFQ circuits are also expected to be monolithically fabricated with quantum circuits as the control or readout circuits of Qubits in the future [3]. Due to an intrinsic π phase shift in 0-π SQUID, the nominal critical current $I_{nominal}$ of SQUID is much smaller than that of single JJ even with the same process as SFQ circuits. In the initial propose, HFQ circuits are composed of 0-π SQUIDs, however, it's intractable to realize a symmetric 0-JJ and π-JJ in a loop. Alternative 0-0-π SQUIDs have been adopted to demonstrate HFQ circuits, in which Nb/PdNi/Nb (SFS) π-JJ was fabricated after 0-JJs and act as a negative phase shifter [4]. However, the post-fabrication of π-JJ will affect the property of 0-JJ in this hybrid process and the critical current of 0-JJ cannot be decrease to sub-microamp with present process.

２．研究の目的

In this research, TRNGs based on HFQ balanced comparator will be demonstrated to classify the randomness superiority of classical and quantum mechanism. By changing the circuits parameters, HFQ balanced comparators will operate with quantum and thermal fluctuations. A new and simple HFQ circuits fabrication process based on superconductor/ferromagnet/insulator/superconductor (SFIS) π-JJs will be developed to eliminate the post-process effect in 0-0-π SQUID. The demonstration of HFQ TRNG will help to establish the HFQ circuits design methodology, develop a HFQ circuits parameter optimization procedure and set up a digital measurement environment at mK stage.

３．研究の方法

Task1. Establishing HFQ circuits fabrication process.

Real HFQ circuits can be fabricate with 0-0-π or π-π-π SQUIDs, in which one π-JJ acts as a negative phase shifter and the others are used as switching elements. In this research, we plan to fabricate π-JJ with Nb/NiPd/Al-AlO_x/Nb (SFIS) structure, because it has a much larger characteristic voltage V_c ($\sim I_cR_n$) than SFS junction and can be used as phase shifter and switching junction simultaneously. Additional, SFIS π-JJs have overdamped characteristic, un-shunted HFQ circuits can be realize. This fabrication process is quite simple, only four Nb films will be required. The critical current of π-JJ will be tuned by the oxidation

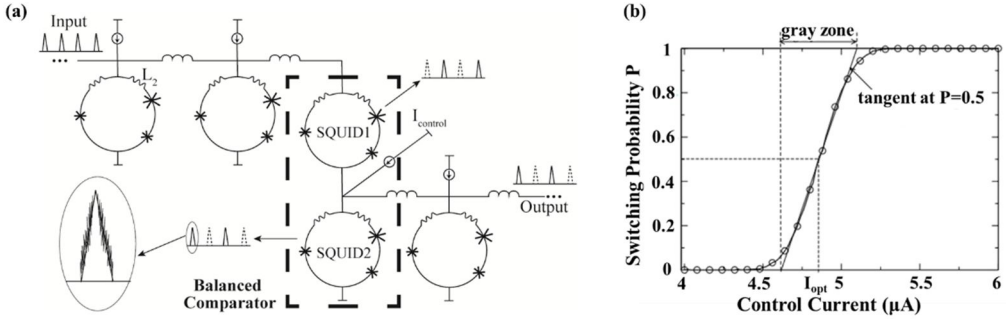

Fig. 1(a) TRNG based on HFQ balanced comparator. (b) gray zone of balanced comparator

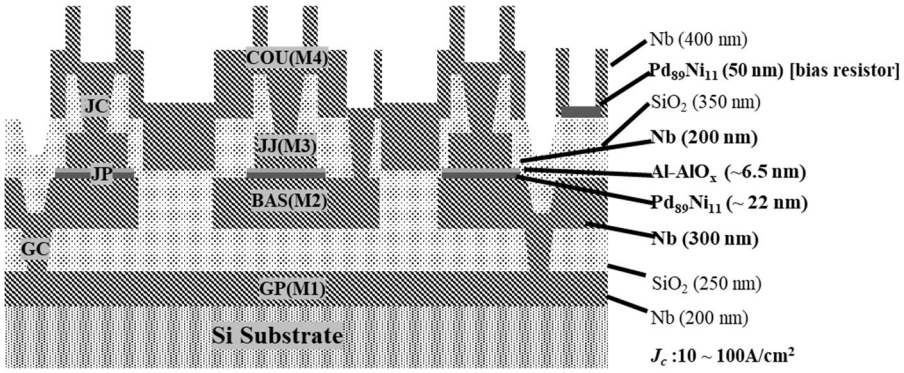

Fig. 2 SFIS fabrication process

time and pressure of Al-AlOx layer. The bias resistors will be formed with an additional NiPd layer.

Task2. Characterization of π-π-π SQUID at 4.2 K and 10 mK.

At first, the properties of SFIS junction will be characterized at 4.2 K. By measuring the modulation pattens of π-π and π-π-π SQUIDs, we can easily know the intrinsic phase state of our SFIS junctions. Since temperature can also leads to the phase transition of SFIS junction, the temperature (10 mK~ 4.2 K) dependence of I_c of SFIS junction should also be measured and make sure SFIS junctions are still in π state at 10 mK. In the dilution refrigerator, shielded DC cables, magnetic field shield, low pass and Eccosorb filters are adopted to minimum the effect of external noise or fields during the measurement.

Task3. HFQ circuits design and optimization.

In HFQ circuits, HFQ signal is transferred as half flux quantum and can be stored in the inductor of a superconducting loop. $LI_{nominal} \sim \Phi_0/2$ ($\Phi_0 \sim 2.067\times10^{-15}$ Wb) is an important requirement in a storage loop, in which L is the inductance between two π-π-π SQUIDs. The π-π-π SQUIDs of HFQ balanced comparators that work at 4.2 K or 10 mK have different nominal critical current $I_{nominal}$. For example, the RNG operating in the quantum regime has a $I_{nominal} \sim 100$ nA, and very large inductance (~ nH) will be required to maintain the correct operation. Superconducting meander line or ground plane perforation should be adopted to increase the sheet inductance of Nb film. An HFQ circuits optimization program is required to increase the circuits operating margins. As shown in Fig. 1(a), HFQ balanced comparator is two π-π-π SQUIDs connected in series. To generate a random number, HFQ comparator will connect to DC/HFQ and HFQ/DC converters through HFQ Josephson transmission line (JTL, parallel connected π-π-π SQUIDs in HFQ circuit). Taking the thermal or quantum fluctuation into consideration, the switching property of the balanced comparator show a gray zone as shown in the Fig.1 (b), in which SQUID1 and SQUID2 switch stochastically. If a control current $I_{control}$ is applied to the balanced comparator, it can output a series of random numbers and act as a TRNG if the switching probability of SQUID2 is tuned around 50%.

4．研究成果

(1) HFQ circuits fabrication process development

We developed the new and simple superconducting digital circuits fabrication process as shown in Fig. 2, in which all the π-JJs were fabricated at the same time and shunt resistors are no longer needed due to the overdamped characteristic of SFIS junctions. The critical current density (J_c) of SFIS junction can be tuned between 10 ~100 A/cm^2. This SFIS process can be used to fabricate HFQ as well as SFQ circuits. Additionally, some specific superconducting annealing circuits can also be fabricated with this process.

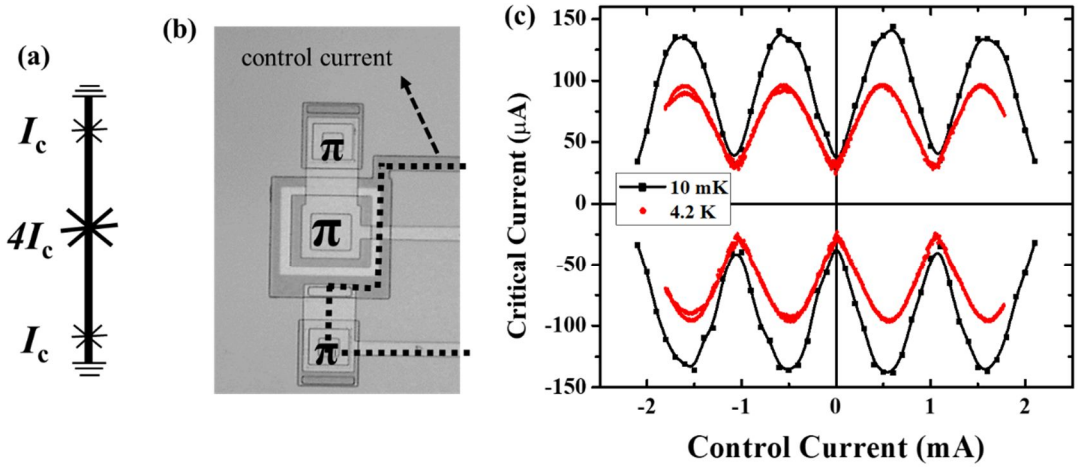

Fig. 3 (a) schematic and (b) photography of π-π-π SQUID.
(c) modulation patterns of π-π-π SQUID at 4 .2 K and 10 mK

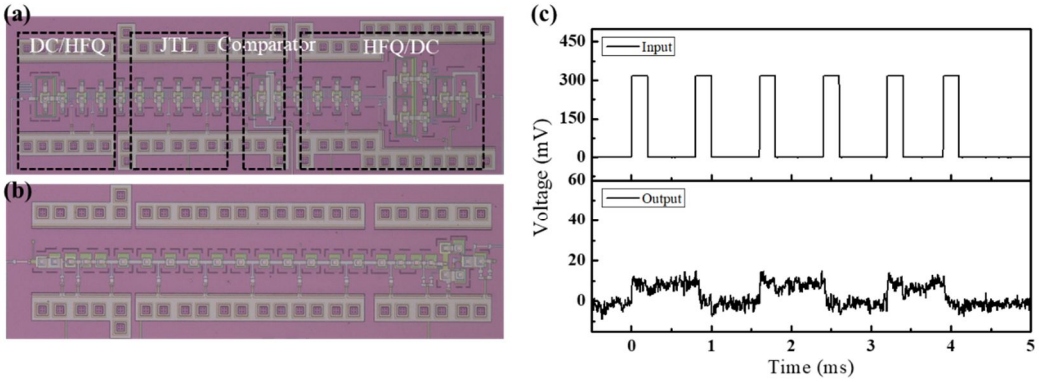

Fig. 4 (a) HFQ TRNG with DC/HFQ and HFQ/DC converters. (b) un-shunted SFQ circuit fabricated by SFIS process. (c) measurement of SFQ circuit

(2) π phase shift at 10 mK stage

SFIS junctions with different dimensions were characterized after amounted to a probe and dipped into liquid helium. By measuring the return current ($I_r = 4I_c/\pi\sqrt{\beta_c}$), we calculated the McCumber parameter β_c of SFIS junction is about 2. J_c and V_c are 25 A/cm^2 and 30 μV, respectively. I_c of SFIS junction increased gradually with decreasing of temperature. Figure 3(a) and (b) shows the schematic and picture of π-π-π SQUID, in which the middle large π-JJ (~ $4I_c$) is the negative π phase shifter while the upper and bottom small π-JJs (~ I_c) act as switching junctions. Usually, I_c of phase shifter should be as large as possible to eliminate the effect of its' kinetic inductance. Figure 3(c) shows the modulation patterns of π-π-π SQUID measured at 4.2 K and 10 mK by applying a control current as shown in Fig. 3(b). The minimum $I_{nominal}$ of π-π-π SQUID at origin indicates our SFIS junction can maintain its' intrinsic π phase shift in the temperature range of 4.2 K and 10 mK, which is essential for demonstration of HFQ TRNG operating with quantum and thermal fluctuations.

(3) π-JJs based HFQ and SFQ Circuits

To demonstrate a real RNG as shown in Fig .1(a), we connected it to DC/HFQ and HFQ/DC converters as shown in Fig .4(a) with DC input and output measurement. This circuit was simulated with PJsim, and inductance were extracted with InductEx. The HFQ balance comparator is in the middle of Fig. 4(a), we can adjust the circuits output probability and generate a random number train with quantum or thermal fluctuation. Unfortunately, we can't get the correct operation of this TRNG at present, the operating margin of HFQ/DC converter is only about ±5% even within the simulation. The HFQ optimization program is still under development. As the new process we developed, further optimization of the circuits parameters and fabrication process are required to measure a HFQ circuit at low frequency with DC output port. Meanwhile, we designed and fabricated a HFQ Toggle Flip-Flop (TFF) and measured with the average voltages at the input and output ports. The correct divide by two operation of HFQ TFF (not shown here) was measured up to 6.7 GHz at 4.2 K, indicating that HFQ signals can propagate and stored between π-π-π SQUIDs. We think it is feasible to demonstrate TRNGs with HFQ circuit if we can optimize operating margin of the output converter in the future.

Despite the narrow bias margin of HFQ/DC converter, we tried to design and fabricate the conventional SFQ circuit with π-JJs as shown in Fig. 4(b), because the SFQ/DC in our cell library has much wider operating margin. We measured the correct operations of SFQ circuit with DC/SFQ and SFQ/DC converters at 4.2 K as shown in Fig. 4(c). Since V_c of SFIS junction is about 30 μV, the output DC voltage is about 10 mV after amplified for 1000 times at room temperature. SFQ/DC converter can be used in HFQ circuits, however, an HFQ/SFQ converter is still required and limit the circuits operating margin. Anyway, a new research area, un-shunted SFQ circuits based on overdamped SFIS π-JJs has also been established according to this research. By incorporating the π phase shifter and eliminating the shunt resistor, much more compact SFQ circuits can be demonstrated with this SFIS process in the future.

References

[1] Tatsuro Sugiura, Yuki Yamanashi, Nobuyuki Yoshikawa, "Demonstration of 30 Gbit/s Generation of Superconductive True Random Number Generator" *IEEE Trans. Appl. Superconduct.* 21. 843-846 (2011)

[2] Tomohiro Kamiya, Masamitsu Tanaka, Kyosuke Sano, and Akira Fujimaki, "Energy/Space-Efficient Rapid Single-Flux-Quantum Circuits by Using π-Shifted Josephson Junctions" *IEICE TRANS. ELECTRON.* E101-C. 385 (2018)

[3] Feng Li, Yuto Takeshita, Daiki Hasegawa, Masamitsu Tanaka, Taro Yamashita, Akira Fujimaki, "Low-power High-speed Half-flux-quantum Circuits Driven by Low Bias Voltages" *Supercond. Sci. Technol.* 34, 025013 (2021)

[4] Daiki Hasegawa, Yuto Takeshita, Feng Li, Kyosuke Sano, Masamitsu Tanaka, Taro Yamashita, Akira Fujimaki, "Demonstration of interface circuits between half- and single- flux- quantum circuits" *IEEE Trans. Appl. Superconduct.* 31. 1-4 (2021)

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1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 Li Feng、Takeshita Yuto、Hasegawa Daiki、Tanaka Masamitsu、Yamashita Taro、Fujimaki Akira	４．巻 34
２．論文標題 Low-power high-speed half-flux-quantum circuits driven by low bias voltages	５．発行年 2021年
３．雑誌名 Superconductor Science and Technology	６．最初と最後の頁 025013～025013
掲載論文のDOI（デジタルオブジェクト識別子） 10.1088/1361-6668/abcaac	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6件（うち招待講演　2件／うち国際学会　4件）

１．発表者名 Feng Li, Yuto Takeshita, Daiki Hasegawa, Masamitsu Tanaka, Taro Yamashita, and Akira Fujimaki
２．発表標題 Demonstration of π-Junction-Based SQUIDs with Half-Flux-Quantum Modulation Periods for Energy-Efficient Circuits
３．学会等名 ASC2020（国際学会）
４．発表年 2020年

１．発表者名 Feng Li, Yuto Takeshita, Daiki Hasegawa, Masamitsu Tanaka, Taro Yamashita, and Akira Fujimaki
２．発表標題 Demonstration of Half-Flux-Quantum T-Flip Flops Made up with Only π Junctions
３．学会等名 EUCAS 2021（国際学会）
４．発表年 2021年

１．発表者名 Feng Li, Yuto Takeshita, Daiki Hasegawa, Masamitsu Tanaka, Taro Yamashita, and Akira Fujimaki
２．発表標題 Low-power Half-flux-quantum Circuits and the Fabrication Process Based on Ferromagnetic SFIS Josephson Junctions
３．学会等名 QCCC 2021（国際学会）
４．発表年 2021年

１．発表者名
Feng Li, Yuto Takeshita, Masayuki Higashi, Masamitsu Tanaka, Taro Yamashita, and Akira Fujimaki

２．発表標題
Half-flux-quantum Circuits Using π-shifted Ferromagnetic Junctions

３．学会等名
ISS 2021（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Feng Li, Yuto Takeshita, Masayuki Higashi, Masamitsu Tanaka, Taro Yamashita, and Akira Fujimaki

２．発表標題
Half-Flux-Quantum T-Flip Flops Based on π-π-π SQUIDs

３．学会等名
The 82nd JSAP Autumn Meeting

４．発表年
2021年

１．発表者名
Feng Li, Duong Pham, Yuto Takeshita, Masayuki Higashi, Masamitsu Tanaka, Taro Yamashita, and Akira Fujimaki

２．発表標題
π-π-π SQUIDs: The Switching Element of HFQ Circuits Operating at mK

３．学会等名
The 69nd JSAP Spring Meeting（招待講演）

４．発表年
2021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

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