Superconductive Random Number Generator Using Thermal Noises in SFQ Circuits

Y. Yamanashi and N. Yoshikawa *Member IEEE*

***Abstract*—A novel high-speed physical random number generator using the superconductive single-flux-quantum (SFQ) circuits and thermal noises in the circuit has been proposed. The proposed physical random number generator is similar to an SFQ balanced comparator. Thermal noises in shunt resisters are used to obtain random outputs. Because of the high-sensitivity of SFQ circuits, the true random numbers can be generated without amplification of the noises at high clock frequency. Generation of the true random numbers at the frequency of several tens GHz can be realized by using the proposed circuit. Moreover, the circuit scale of the proposed circuit is very small and the generation frequency of the random number generator can be easily enhanced by parallelizing the circuits. We have designed and tested the superconductive physical random number generator using the 2.5 kA/cm^2 Nb standard process and evaluated the quality of the generated random number train. We have examined a 2^{20}-bit random number train generated at a low frequency and no periodicity is observed. We believe that the superconductive physical random number generator can be applied to cryptographic applications for more secure information processing.**

***Index Terms*—Josephson junction, Random number, Thermal noise, Single flux quantum circuit**

I. INTRODUCTION

DEMANDS for the information security have increased with developments of information processing technologies. For the applications of the cryptographic security, a high-quality random numbers with no periodicity and no correlation between each bit are required, i.e., more secure communication is thought to be realized by using a true random number train for cryptographic key distribution. The physical random number generators using the randomness of physical phenomena such as thermal noises in resisters are used to obtain the true random number train. Several physical random number generators using semiconductor integrated circuits have been developed [1], [2]. However, the generation frequency of the random number remains less than 10 MHz because the magnitude of the noises is too small for the semiconductor circuit. So the amplification process is required additionally.

In the field of superconductive digital circuits [3], high-speed pseudo-random number generators have been developed [4]-[7]. The pseudo-random number generator is realized by the combination of the appropriate flip-flops. The generation frequency of the random number is 50 GHz, and the pseudo-random number generator has been experimentally used to measure the error rate of superconductive digital circuits [8]. However, the pseudo-random number generator cannot be applied to cryptographic applications because the bit can be predicted from the history of the generated random number train.

Manuscript received 19 August 2008.

Y. Yamanashi and N. Yoshikawa are with Yokohama National University, Yokohama 240-8501, Japan (e-mail: yamanasi@ynu.ac.jp).

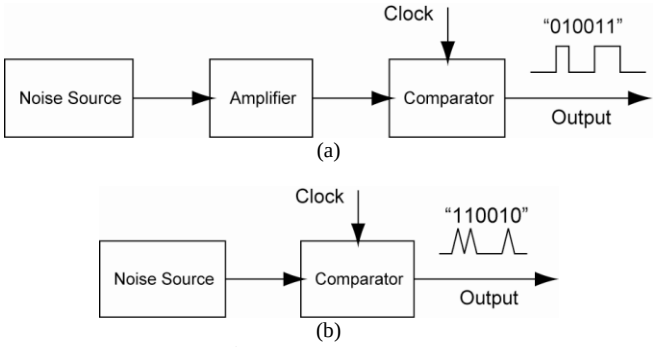

Fig. 1. Block diagrams of (a) an existent semiconductor physical random number generator and (b) a proposed superconductive physical random number generator.

In this study, we have proposed a superconductive physical random number generator which can generate the true random number trains at an extremely high frequency. A true random number train is generated by using the superconductive physical random number generator, and we have evaluated the quality of the random number train.

II. EXPERIMENTAL

The proposed physical random number generator consists of a noise source and an SFQ comparator. This is similar to the existent physical random number generator using semiconductor integrated circuits. Fig. 1 shows the comparison of an existent semiconductor physical random number generator and the proposed superconductive physical random number generator. In the existent semiconductor physical random number generator, thermal carrier injection and ejection in local traps are used as noise sources to obtain the large thermal noises compared to the thermal currents in the resisters [1], [2]. However, the noises have to be amplified to generate the true random number generator because the voltage level of the noises is much smaller than the logic level of the semiconductor circuits even if such large noises are used. On the contrary, thermal noises in the circuits can be directly used in the superconductive physical random number generator because the superconductive circuits have ultra

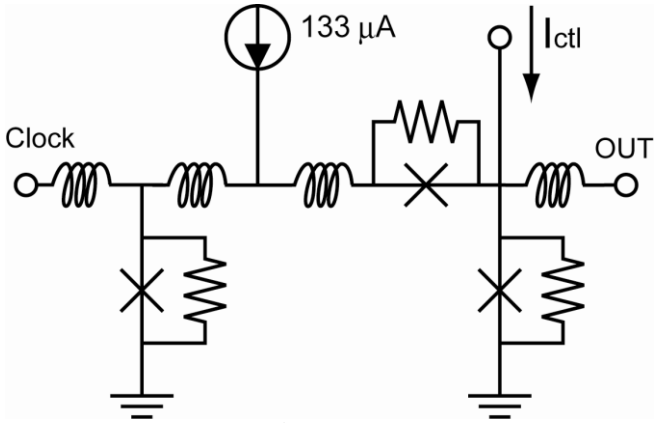

Fig. 2. An equivalent circuit of the SFQ balanced comparator used in the superconductive physical random number generator. All inductances are 2.52 pH. Critical current and shunt resisters of all Josephson junctions are 216 μA and 1.73 Ω, respectively.

high-sensitivity.

The proposed superconductive physical random number generator consists of a noise source and an SFQ comparator as shown in Fig 1 (b). Fig. 2 shows an equivalent circuit of the SFQ comparator used in the superconductive physical random number generator. All Josephson junction are resistively shunted to adjust the Stewart-McCumber parameters of junctions to be ~1. This comparator is similar to an SFQ balanced comparator. Identically, the output is exactly determined by the control current injected into the middle of the two Josephson junctions composing the comparator. The SFQ comparator has been well studied theoretically and experimentally [9], [10]. A gray zone, which has finite output probability $0<P(I_{ctl})<1$, exists for a finite range of the control current because of thermal or quantum fluctuations. At 4.2 K, the main sources of the fluctuation are thermal currents in shunt resisters.

The output probability can be controlled by adjusting the control current supplied to the SFQ comparator. In the superconductive physical random number generator, the control current is adjusted so that the output probability may set to be 0.5. At this biasing point, we do not find any correlation between each bit because the thermal currents in resisters are white noises and thus high-quality true random numbers can be obtained. Furthermore, the frequency of the random number generation is expected to be several tens GHz because the time width of SFQ pulses is very short.

The main part of the proposed superconductive physical random number generator is composed of only a few Josephson junctions as shown in Fig. 2. Therefore, the generation frequency of the random number can be easily enhanced by parallelizing the random number generators. Furthermore, an SFQ circuit using high-temperature superconductor (HTS) [11], which is difficult to apply to large-scale circuits, are expected to be utilized because of the small circuit scale and the operating principle.

We have designed the superconductive physical random number generator using the SRL 2.5 kA/cm^2 Nb standard process [12]. Fig. 3 shows the microphotograph of the

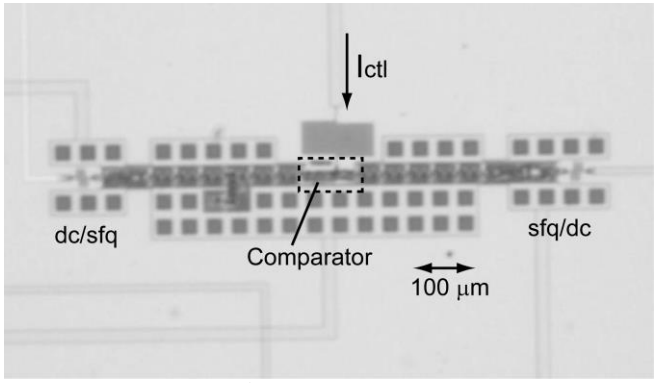

Fig. 3. Microphotograph of the superconductive physical random number generator.

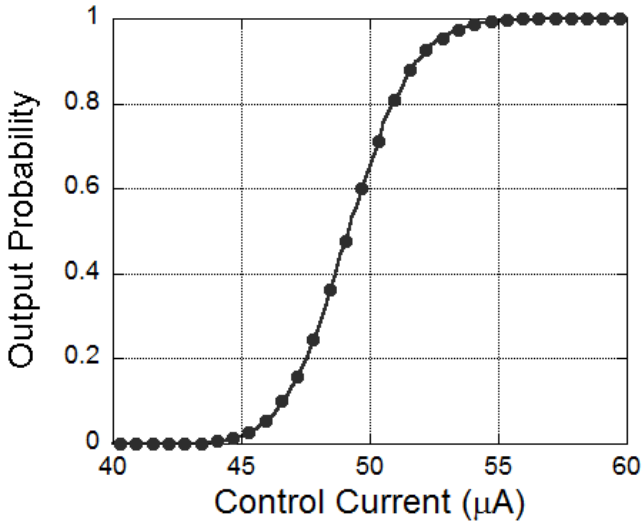

Fig. 4. Measured output probability of the SFQ comparator.

superconductive physical random number generator composed of the SFQ balanced comparator, a dc/sfq converter and an sfq/dc converter. The main part, an SFQ balanced comparator, is fabricated on 40 μm x 80 μm circuit area, which is indicated by dashed square in Fig. 3. The control current I_{ctl} is supplied via an on-chip 1 kΩ resister.

First, we have measured the output probability as a function of the control current by measuring the number of output signals when the SFQ pulses are input to the comparator 1000 times for each bias point at 4.2 K. We obtained the output probability of 50% by supplying the control current of 49.1 μA as shown in Fig. 4.

We have generated and recorded 2^{20}-bit random number train using the superconductive physical random number generator by applying the control current of 49.1 μA and inputting 2^{20}-bit SFQ signals at 4.2 K. The measurements were performed by a computer-controlled automated measurement system.

III. Results and Discussion

Fig. 5 shows the histogram of measured random numbers. In this result, random numbers are encoded from 0 to 7 by using neighboring 3 bits for clarity. The average value of the

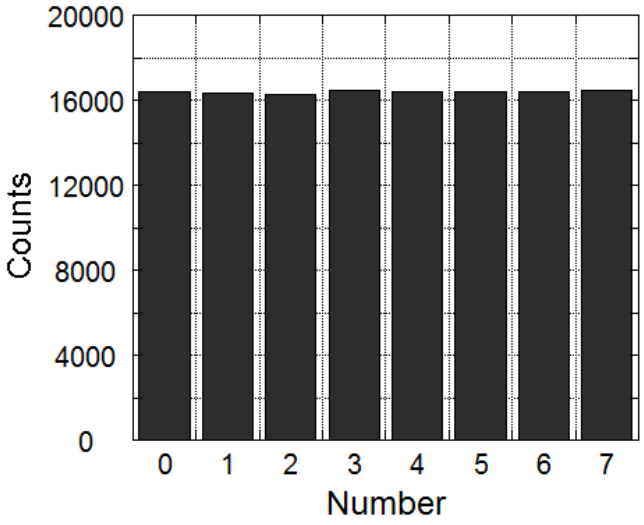

Fig. 5. Histogram of measured random numbers. Random numbers are encoded to 0-7 by using neighboring 3 bits. Maximum and minimum counts are 16440 and 16269, respectively.

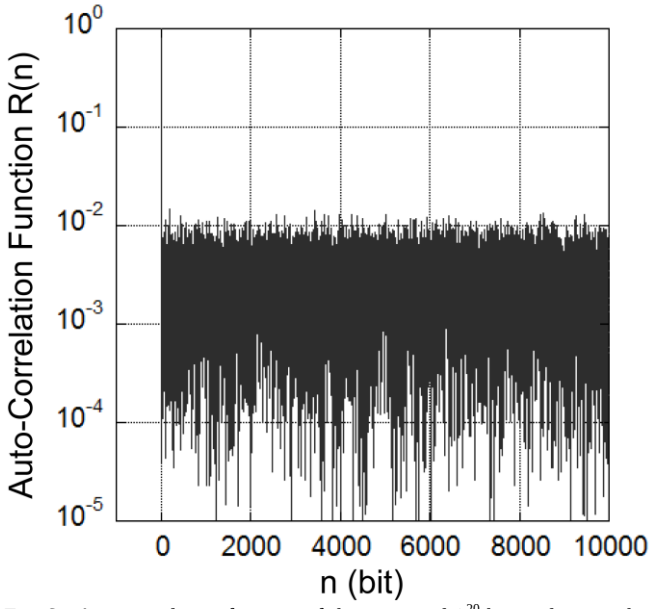

Fig. 6. Auto-correlation function of the generated 2^{20}-bit random number train. The auto-correlation function is normalized so that the maximum value, R(0), may be 1.

generated random number train is 3.504. This result means that the probability of the signal '1' being output is almost 50%.

To evaluate the quality of the generated random number train, we have calculated the auto-correlation function of the random number train, which corresponds to the correlation between each bit. The auto-correlation function *R(n)* is calculated as

$$R(n) = \frac{1}{N}\sum_{i=0}^{N-1} x(i)\cdot x(i+n), \qquad (1)$$

where x(i) represents the generated random number, and N is the length of the random number train. Fig. 6 shows the normalized auto-correlation function of the generated random number train. We cannot confirm the clear peaks of

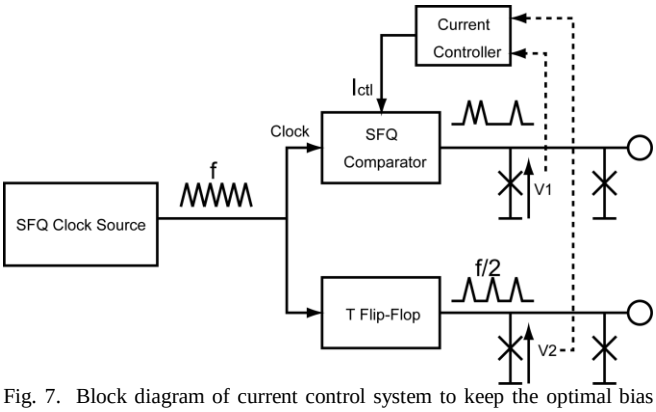

Fig. 7. Block diagram of current control system to keep the optimal bias point. The frequency of the SFQ pulse train input to the SFQ balanced comparator is f.

auto-correlation function except R(0), though Fig. 6 shows the region from R(0) to R(10000). This result means that the high-quality true random number train without correlation between each bit can be the generated by using the superconductive physical random number generator.

We have also performed a statistical test provided by NIST [13] to evaluate the quality of the random number train. We evaluate the randomness of the random number train by the frequency (monobit) test, which is the most fundamental statistical test and determines whether the number of ones and zeros in the random number train are approximately the same as would be expected for a true random sequence.

In the frequency test, the required probability that the output of '1' is obtained is from 48.625% to 51.375% to apply the random number train to the cryptographic applications [13]. In our experiments described above, the output probability is 50.11%. This value is generally better than results of semiconductor random number generator [2]. And the requirement is easily fulfilled by properly adjusting the supplied control current. This means the proposed superconductive random number generator can be sufficiently applied to the practical applications.

When the superconductive physical random number generator is in use practically, a precise adjustment of the control current is necessary because we can obtain the true random numbers at the bias point where the output probability of the comparator is around 50%.

The optimal bias point is thought to be shifted slightly as the input frequency changes. For the precise adjustment of the control current, we have devised a current control scheme. Fig. 7 shows a block diagram of the current control system. This system is composed of an SFQ clock source, a toggle flip-flop, the SFQ balanced comparator and a computer-based current controller, which adjusts the control current by a GPIB control. In this system, the SFQ clock source generates the SFQ pulse train, whose frequency is f. The current controller measures the average voltages of the two Josephson junctions, V1 and V2, and can apply the arbitrary value of the control current to the SFQ comparator. When the input frequency of the SFQ pulse train is f, V2 becomes $f\Phi_0/2$ because the T flip-flop divides the frequency of the SFQ pulse train by 2. In this case, V1 is adjusted by the control current because the V1 is proportional

to the output probability of the SFQ balanced comparator. When the output probability of the comparator is exactly 50 %, V1 becomes $f\Phi_0/2$. Therefore, by adjusting the control current so that V1 equals to V2, the bias point is kept to be optimal.

IV. Conclusion

We have proposed a novel physical random number generator using superconductive SFQ circuits. Random bits can be obtained by utilizing the thermal current in the circuit. Because of high-sensitivity and high-speed operation of superconductive circuits, true random numbers can be generated at a high clock frequency without amplifying thermal noises. We have designed and measured the superconductive physical random number generators using the Nb standard process. We have examined the 2^{20}-bit random number train generated by the superconductive physical random number generator at 4.2 K. Measurement results indicate that we can obtain the high-quality true random number train by using the superconductive physical random number generator. And we have devised a bias control scheme to keep the optimal bias point for the practical applications.

References

[1] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A High-Speed Oscillator-Based Truly Random Number Source for Application on Smart Card IC," *IEEE Trans. Computers*, vol. 52, pp. 403-409, Apr.2003.

[2] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita, "1200μm^2 Physical Random-Number GeneratorsBased on SiN MOSFET for SECURE Smart-Card Application," in *Tech. Dig. IEEE Int. Solid-State Circuit Conf.*, San Francisco, CA, Feb. 2008.

[3] K. K. Likharev and V. K. Semenov, "RSFQ logic/memory family: A new Josephson-junction digital technology for sub-terahertz-clock-frequency digital systems," *IEEE Trans. Appl. Supercond.*, vol. 1, pp. 3–28, Mar. 1991.

[4] A. Y. Kidiyarova-Shevchenko, D. Y. Zinoviev, "RSFQ pseudo random generator and its possible applications," *IEEE Trans. Appl. Supercond.*, vol. 5, pp. 2820-2822, Jun. 1995.

[5] J. Kang, A. H. Worsham, and J. X. Przybysz, "4.6 GHz SFQ Shift Register and SFQ Pseudorandom Bit Sequence Generator," *IEEE Trans. Appl. Supercond.*, vol. 5, pp. 2827-2830, Jun. 1995.

[6] W. Kessel, F. I. Buchholz, M. I. Khabipov, R. Dolate, and J. Niemeyer, "Development of an Rapid-Single-Flux-Quantum Shift Register for Applications in RF Noise Power Metrology," *IEEE Trans. Instrumentation and Measurement*, vol. 46, pp. 477-481, 1997.

[7] X. Zhou, S. Xu, P. Rott, C. A. Mancini, and M. J. Feldman, "50 GHz RSFQ Pseudo-Random Number Generator Design," *IEEE Trans. Appl. Supercond.*, vol. 11, pp. 617-620, Jun. 2001.

[8] Q. P. Herr, A. D. Smith, and M. S. Wire, "High speed data link between digital superconductor chips," *Appl. Phys. Lett.*, vol. 80, pp. 3210–3212, Apr. 2002.

[9] T. V. Filippov, Y. A. Polyakov, V. K. Semenov, and K. K. Likharev, "Signal resolution of RSFQ comparators," *IEEE Trans. Appl. Supercond.*, vol. 5, pp. 2240-2243, Jun. 1995.

[10] V. K. Semenov, T. V. Filippov, Y. A. Polyakov, and K. K. Likharev, "SFQ balanced comparators at a finite sampling rate," *IEEE Trans. Appl. Supercond.*, vol. 7, pp. 3617-3621, Jun. 1997.

[11] D. L. Miller, J. X. Przybysz, and J. H. Kang, "Margins and yields of SFQ circuits in HTS materials," *IEEE Trans. Appl. Supercond.*, vol. 3, pp. 2728-2732, Mar. 1993.

[12] S. Nagasawa, Y. Hashimoto, H. Numata, and S. Tahara, "A 380 ps, 9.5 mW Josephson 4-kbit RAM operated at a high bit yield," *IEEE Trans. Appl. Supercond.*, vol. 5, pp. 2447–2452, Jan. 1995.

[13] NIST, "A Statistical Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," May 15, 2001, http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf