Demonstration of 30 Gbit/s Generation of Superconductive True Random Number Generator

Tatsuro Sugiura, Yuki Yamanashi, Nobuyuki Yoshikawa *Member IEEE*.

***Abstract*— True random number generators, which output truly random numbers by extracting entropy from physical phenomena such as thermal and electronic noises, are widely used in the field of the cryptographic communication systems. We have been developing a superconductive true random number generator that can generate truly random number sequences, impossible to be predicted, by utilizing the high-speed operation and high-sensitivity of superconductive integrated circuits. In this study, we have calculated the dependences of correlation of output random bits on the generation rate. Statistical tests have been performed on the basis of the NIST statistical test suite in order to evaluate the quality of the randomness of sequences generated by the superconductive true random number generator at high generation rate. We have generated a random number sequence consisting of 3.2 M-bit at the generation rate of 30 Gbit/s using the superconductive true random number generator, fabricated by the ISTEC-SRL 2.5 kA/cm^2 Nb standard process. The generated random number sequences passed 13 kinds of the statistical tests in the NIST statistical test suit, although the 3 tests were not performed because of the shortage of the generated random numbers. The result sufficiently proves that a superconductive true random number generator can generate a high quality of random numbers that can be used for practical cryptographic applications, at a generation rate of up to 30 Gbit/s.**

***Index Terms*—Random number generation, Superconducting integrated circuits, Josephson junctions, Comparators.**

I. Introduction

RANDOM numbers form the essential foundation for simulations, such as statistic science, finance, and natural phenomena, or cryptographic technology in secure communication systems. Most random numbers used in applications are pseudo-random, which are generated by using certain mathematical algorithms. Though pseudo-random number generators (PRNGs) have a high generation rate thanks to advancements in computer technology, PRNGs are not suitable for the generation of cryptographic keys, which is one of the very important application of random number generators. Cryptographic keys are needed to be generated by truly random bits because pseudo-random number sequences are predictable because they are generated using computational algorithm. For this reason, true random number generators (TRNGs), which generate truly random number sequences by extracting entropy from physical random phenomena such as thermal and electronic noises [1], chaos in lasers [2], and radioactivity [3], have been developed in order to enhance the security of cryptographic communication systems [4-7]. Among these natural sources, thermal noise in resisters is the most used as the source of randomness. The generation rate of the random numbers of conventional TRNGs, which employ noise in semiconductor circuits, are limited to be much smaller than that of PRNGs because the amplitude of thermal noises is much smaller than the logic levels of the semiconductor circuits and the amplification process of noise is required. The amplification process restricts the generation rate of conventional TRNGs to less than 10 Mbps. This generation speed is insufficient for practical communication systems.

We have been developing a small-sized, high-speed TRNG using superconducting integrated circuits [8]. The proposed circuit uses the thermal noise in a single-flux-quantum (SFQ) circuit. In the SFQ circuit, signals are expressed by small voltage pulse of hundreds of micro-volts; therefore, there is no need to amplify the thermal noise to obtain the randomness, and a high-speed operation of the TRNG, tens of gigahertz, can be expected [9]. In this paper, we have calculated the correlation of output random number sequence to evaluate the maximum generating rate of the superconductive TRNG. Statistical test of the random number sequence, generated by the superconductive TRNG at 30 Gbit/s, have been performed on the basis of the NIST statistical test suite to evaluate the quality of randomness of the generated random number sequences.

II. Superconductive True Random Number Generator

A superconductive true random number generator consists of an SFQ balanced comparator and a current source [8]. Fig. 1

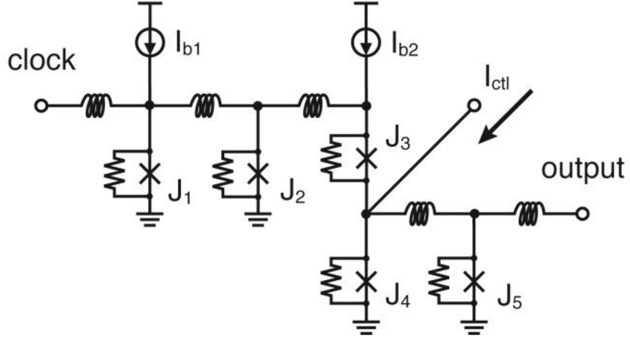

Fig. 1 Equivalent circuit of the superconductive true random number generator. Critical currents of all JJs are 216 μA, and shunt resistors are 1.73Ω. I_{b1} = 300 μA, I_{b2} = 167 μA.

Manuscript received 3 August 2010.

T. Sugiura, Y. Yamanashi, and N. Yoshikawa are with Department of Electrical and Computer Engineering, Yokohama National University, Yokohama 240-8501, Japan. (e-mail: yamanasi@ynu.ac.jp).

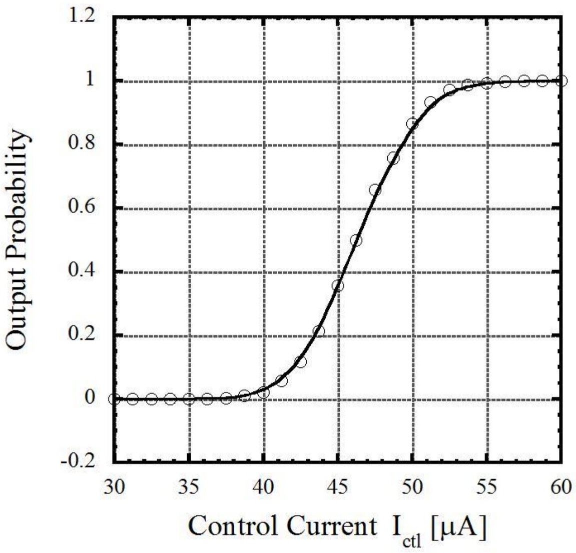

Fig. 2 Numerically simulated output characteristics of the SFQ balanced comparator. The bias voltage is designed value, 2.5 mV. The width of gray zone is estimated to be 11.7 μA.

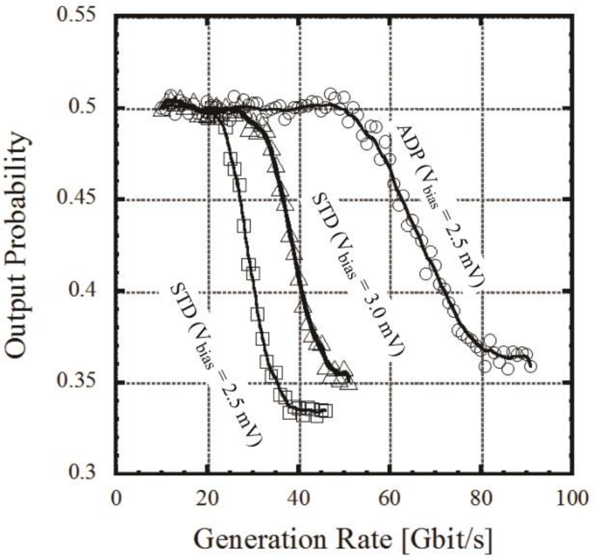

Fig .3 Dependences of output probabilities on the generation rates of random numbers. STD and ADP represent the SRL 2.5 kA/cm^2 standard process [12] and 10 kA/cm^2 advanced process, respectively.

shows an equivalent circuit of the superconductive TRNG. All Josephson junctions are resistively shunted to adjust the McCumber parameters of junctions to ~1. Either J_3 or J_4 switches depending on the I_{ctl} value. In an ideal environment, where noise is absent, the Josephson junction J_4 always switches if the control current I_{ctl} is larger than a certain threshold current value. However, a finite gray zone, where the output probability is obtained in the range from 0 to 1, exists because of the thermal noises and quantum fluctuation in the circuits [10]. The dependence of the output probability of the SFQ balanced comparator on the control current as obtained by numerical simulation is shown in fig. 2. The characteristics shown in fig. 2 was calculated by the circuit simulator JSIM_N [11] which can take the thermal noises in circuits into account, and the operation temperature of 4.2 K was assumed. And the parameters of Josephson junction for the Superconductivity Research Laboratory (SRL) 2.5-kA/cm^2 Nb standard fabrication process [12] were used. As shown in fig. 2, the output probability of the SFQ balanced comparator can be controlled by adjusting the supplied control current I_{ctl}. We can obtain truly random numbers by adjusting the control current at the operating point where that the output probability becomes to be 0.5 and inputting high frequency clock.

To evaluate the maximum generation rate of the superconductive TRNG, we have calculated dependences of the output probability and autocorrelation between neighboring two bits on the generation rate of random numbers. To enhance the generation rate of the superconductive TRNG, employment of the high-J_C fabrication process is very effective because the operating frequency of the superconductive circuit is proportional to the square root of the critical current density (J_C) of the Josephson junction. And increasing of the bias voltage supplied to the circuit is also effective. Therefore we have simulated the superconductive TRNG assuming the circuits implemented by the Superconductivity Research Laboratory (SRL) 2.5-kA/cm^2 Nb standard fabrication process (STP) [12] and 10-kA/cm^2 Nb advanced fabrication process (ADP) [13], and different dc bias voltages.

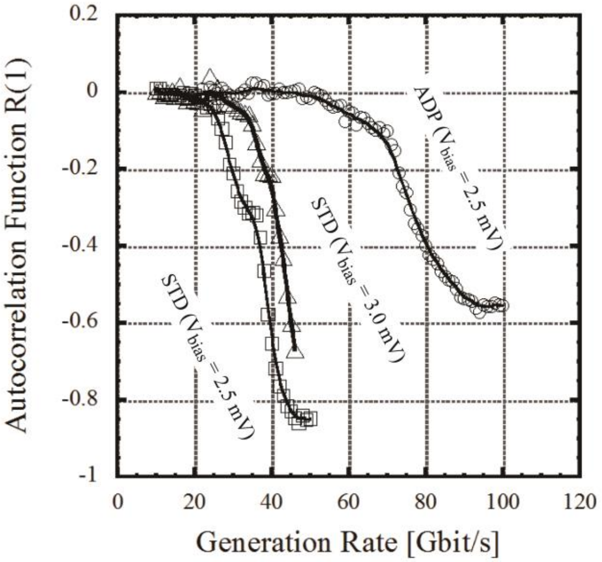

Fig. 4 Dependences of autocorrelation function R(1) on generation rates of random numbers.

We have calculated the output probabilities using simulated output 10-kbit random number sequences. Fig.3 shows the simulated output probabilities of superconductive TRNG. The control current I_{ctl} value was adjusted to obtain an output probability of 0.5 at a generation rate of 10 Gbit/s. From the simulation results, we observed that the superconductive TRNG operated at the speed of a maximum of 20 Gbit/s for the standard bias voltage, 2.5 mV, of a designed circuit, 30 Gbit/s for 3.0 mV, and 50 Gbit/s using 10-kA/cm^2 ADP.

We have calculated the correlation of the random output sequences on the basis of the circuit simulation. Fig. 4 shows the dependences of generated random number sequence's autocorrelation function $R(1)$ on generation rates. The

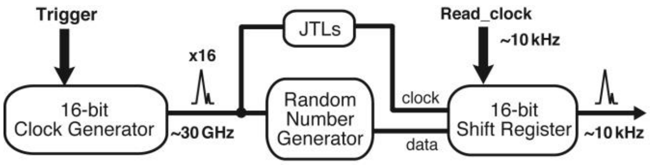

Fig. 5 Block diagram of on-chip high-speed testing system. A clock generator generates 16 SFQ pulses at 30 GHz whenever the trigger signal is input. The outputted random number sequence is stored in the 16-bit shift register, and is read out with low-frequency read clocks. There Josephson transmission line (JTL) stages are inserted to clock line to adjust the timing of clock inputs to the shift registers to prevent the operation errors of shift register.

.

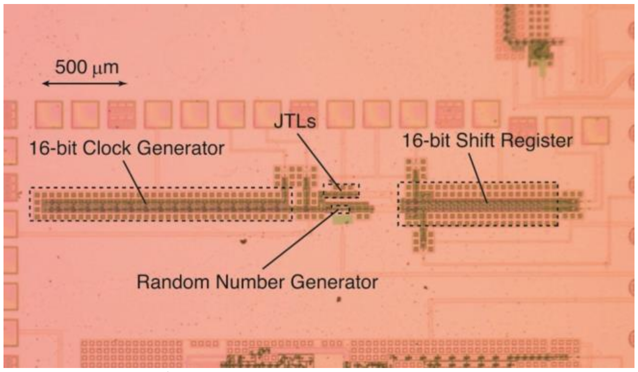

Fig.6 Micrograph of the superconductive true random number generator in on-chip high-speed testing system. This system includes a clock generator and a 16-bit shift register.

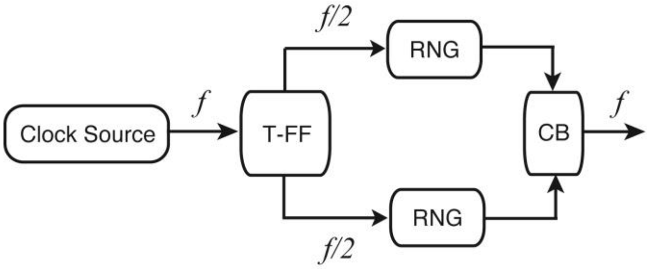

Fig.7 Block diagram of the parallelized superconductive TRNG. In dividing clock signals using toggle flip-flop and operating two RNGs, generation rate is obtained as twice on the whole.

autocorrelation function between neighboring bits $R(1)$ is calculated as

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

where $x(i)$ is a generated random number sequence, where the output bit “0” is encoded to “-1”, and N is the length of random number sequence. In this simulation, control current I_{ctl} value is adjusted to obtain an output probability of 0.5 at each generation rates.

Simulation results indicate that the output random number sequences are correlated and are not regarded as true random number sequences as the generation rate is increased. And we can obtain higher generation rate by increasing the dc bias voltage. If we apply the bias voltage of 3.0 mV to the superconductive TRNG implemented by the SRL 2.5 kA/cm^2 Nb standard process, the maximum generation rate of the superconductive TRNG is about 30 GHz. It can be predicted that the generation rate of superconductive TRNG can be increased more than twice by using 10-kA/cm^2 Nb advanced process.

TABLE 1 RESULTS OF NIST STATISTICAL TEST SUITE

Statistical Test	p-value	Result
Frequency: Monobit	0.122325	Success
Block Frequency	0.739918	Success
Cumulative Sums-Forward	0.035174	Success
Cumulative Sums-Reverse	0.122325	Success
Runs	0.017912	Success
Spectral DFT	0.911413	Success
Non-Overlapping Templates	0.066882	Success
Overlapping Templates	0.035174	Success
Universal	----	----
Approximate Entropy	0.739918	Success
Random Excursions	----	----
Random Excursions Variant	----	----
Linear Complexity	0.213309	Success
Serial	0.739918	Success

III. Implementation Results And Discussion

The superconductive TRNG was designed and implemented with on-chip high-speed testing system as shown in fig. 5 using the 2.5 kA/cm^2 Nb standard process. A clock generator generates 16 periodic SFQ pulses at 30 GHz whenever a trigger signal is input. The outputted random number sequence is stored in the 16-bit shift register, and is read out with low-frequency read clocks. This test system contains 523 Josephson junctions. Fig.6 shows the micrograph of the superconductive with a clock generator and 16-bit shift register.

We have generated 3.2 Mbit random number sequences at the generation rate of 30 Gbit/s. Because it takes a long time to record the 3.2 Mbit outputs using our experimental setup, we used automated current-control system to keep the control current I_{ctl} to the optimal value during measurements [14]. The dc bias voltage supplied to the superconductive TRNG was 3.0 mV.

The quality of randomness of the generated random number sequence has been statistically evaluated. The standard statistical tests, the monobit test, the porker test, the runs test, and the long runs test of the NIST FIPS 140-2 [15] had been performed. These tests use a single bit stream of 20,000 consecutive bits, so extracted 3.2 Mbit sequence is divided into 160 sequences and consists of 20 kbit. All the recorded 160 random number sequences passed these four statistical tests. The maximum autocorrelation function R(1) of among every 20 kbit random number sequences was 0.0218, the minimum was -0.0212, and the average was 0.0028. These results are in good agreements with the simulated autocorrelation function shown in fig. 4.

We also evaluated random number sequences using NIST Special Publication 800-22, a statistical test suite for random and pseudo-random number generators for cryptographic applications [16], which is the state-of-the-art test suite for random number generators. The NIST test suite consists of 16 statistical tests. In each test, p-value which is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested [16], is calculated and the test is passed if the p-value is larger than 0.01.

Although three tests were not performed due to the shortage of bits of random number sequence, the generated random number sequence passed other 13 tests as shown in table 1. This means that the random numbers generated at the generation rate of 30 Gbit/s by the implemented superconductive TRNG can be sufficiently used practical cryptographic applications.

Finally, since the circuit area is very small and simple, the generation rate can be easily improved by parallelizing a circuit. Fig. 7 shows a block diagram of the parallelized superconductive TRNGs. Since a toggle flip-flop (T-FF) divides the frequency of the clock by 2, a superconductive TRNG operates at the rate of half input frequency. And by using the confluence buffer (CB), the generation rate of the random numbers can be reached to double maximum generation rate of the superconductive TRNG. We have already confirmed the correct operation of this system at the generation rate of 100 Gbit/s by circuit simulations assuming the 10-kA/cm^2 Nb advanced process. By adopting this circuit structure, the generation rate of random numbers above 100 Gbit/s, which is four orders of magnitude higher than that of the conventional semiconductor TRNG, is possible.

IV. Conclusion

We have numerically and experimentally evaluated the quality of random output sequence generated by the superconductive TRNG. We have estimated the maximum generation rate of the superconductive TRNG by calculating correlation of output random number sequences based on results of circuit simulation. We have designed a prototype of the superconductive true random number generator with on-chip high-speed measurement system. We have generated the 3.2 Mbit random number sequence at the generation rate of 30 Gbit/s. We have statistically evaluated the random number sequences generated by the superconductive TRNG on the basis of the FIPS 140-2 tests and the NIST statistical test suite. The generated random numbers passed 13 statistical tests of the test suite defined by NIST for cryptographic applications. These test results prove that a superconductive true random number generator can generate high quality of random number sequences at the frequency of 30 Gbit/s. And the generation rate of the superconductive TRNG can be increased to 100 Gbit/s by parallelizing a circuit fabricated using the SRL-ISTEC 10-kA/cm^2 advanced process.

Acknowledgment

National Institute of Advanced Industrial Science and Technology (AIST) partially contributed to the circuit fabrication. This research is financially supported by MEXT's program “Promotion of Environmental Improvement for Independence of Young Researchers.”

References

[1] C. S. Petrie and J. A. Connelly, “A noise-based IC random number generator for applications in cryptography,” *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, pp. 615-621, 2000.

[2] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura and D. Peter, “Fast physical random bit generation with chaotic semiconductor lasers,” *Nature Photonics*, vol. 2, no. 12, pp. 728-732, 2008.

[3] Y. Yoshizawa, H. Kimura, H. Inoue, K. Fujita, M. Toyama and O. Miyatake, “Physical random numbers generated by radioactivity,” *Journal of the Society of Computational Statics*, vol. 12, no. 1, pp. 67-81, 1999.

[4] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto and S. Fujita, “1200μm^2 Physical Random-Number Generators Based on SiN MOSFET for Secure Smart-Card Application,” *IEEE International Solid-State Circuits Conference Digest of Technical Papers*, pp. 414-624, 2008.

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

[6] C. Tokunaga, D. Blaauw and T. Mudge, “True Random Number Generator with a Metastability-Based Quality Control,” *IEEE International Solid-State Circuit Conference Digest of Technical Papers*, pp. 404-405, 2007.

[7] R. Brederlow, R. Prakash, C. Paulus and R. Thewes, “A Low-power True Random Number Generator Using Random Telegraph Noise of Single Oxide-Traps,” *IEEE International Solid-State Circuit Conference Digest of Technical Papers*, pp. 1666-1675, 2006.

[8] Y. Yamanashi and N. Yoshikawa, “Superconductive Random Number Generator Using Thermal Noises in SFQ Circuits,” *IEEE Trans. Appl. Supercond.*, vol. 19, pp. 630-633, 2009.

[9] K. K. Likharev and V. K. Semonov, “RSFQ Logic/Memory Family: A New Josephson-Junction Technology for Sub-Terahertz-Clock-Frequency Digital Systems,” *IEEE Trans. Appl. Supercond.*, vol. 1, pp. 3-28, 1991.

[10] 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, 1995.

[11] J. Satchell, “Stochastic Simulation of SFQ Logic,” *IEEE Trans. Appl. Supercond.*, vol. 7, pp. 3315-3318, 1997.

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

[13] S. Nagasawa, K. Hinode, T. Satoh, H. Akaike, Y. Kitagawa and M. Hidaka, “Development of advanced Nb process for SFQ circuits,” *Physica C: Supercond.*, vol. 412-414, part. 2, pp. 1429-1436, 2004.

[14] T. Sugiura, Y. Yamanashi and N. Yoshikawa, “Statistical Evaluation of a Superconductive Physical Random Number Generator,” *IEICE Trans. Electron.*, vol. E93-C, no. 4, 2010.

[15] NIST, “Security requirements for cryptographic modules,” Federal Information Processing Standards Publication 140-2, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[16] NIST, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” Special Publication 800-22 Rev. 1, 2008. http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800- 22rev1.pdf