IEICE TRANS. ELECTRON., VOL.E105–C, NO.6 JUNE 2022

BRIEF PAPER *Special Section on Progress & Trend of Superconductor-based Computers*

Evaluation of a True Random Number Generator Utilizing Timing Jitters in RSFQ Logic Circuits

Kenta SATO[†a)], **Naonori SEGA**[†], ***Student Members***, **Yuta SOMEI**[†], **Hiroshi SHIMADA**[†], ***Nonmembers***, **Takeshi ONOMI**[††], ***and*** **Yoshinao MIZUGAKI**[†b)], ***Members***

SUMMARY We experimentally evaluated random number sequences generated by a superconducting hardware random number generator composed of a Josephson-junction oscillator, a rapid-single-flux-quantum (RSFQ) toggle flip-flop (TFF), and an RSFQ AND gate. Test circuits were fabricated using a 10 kA/cm^2 Nb/AlO$_x$/Nb integration process. Measurements were conducted in a liquid helium bath. The random numbers were generated for a trigger frequency of 500 kHz under the oscillating Josephson-junction at 29 GHz. 26 random number sequences of 20 kb length were evaluated for bias voltages between 2.0 and 2.7 mV. The NIST FIPS PUBS 140-2 tests were used for the evaluation. 100% pass rates were confirmed at the bias voltages of 2.5 and 2.6 mV. We found that the Monobit test limited the pass rates. As numerical simulations suggested, a detailed evaluation for the probability of obtaining "1" demonstrated the monotonical dependence on the bias voltage.

key words: *Single-flux-quantum logic circuit, hardware random number generator, Nb integration*

1. Introduction

Single-flux-quantum (SFQ) digital circuitry is a superconductive technology [1]–[4] realizing high-speed operation (i.e., up to subterahertz for Nb/Al$_x$/Nb integrated circuits) with low power consumption (i.e., four orders of magnitude less than that of CMOS circuits) [5], [6]. A number of journal papers/technical reports on SFQ-based digital circuits demonstrating these features, such as [7]–[9], have been published.

In addition to digital computing elements, random number generators are another application of SFQ circuits [10], [11]. Random number sequences are used in various fields such as statistical analysis, simulations of natural phenomena, wireless communication, and cryptographic communication. There are two ways to generate random numbers: utilizing a mathematical algorithm and a random physical phenomenon. Random numbers generated by a mathematical algorithm are pseudo random. Although they are periodical and thus predictable, they are widely used for long periods to ensure practical unpredictability. A lot of SFQ-based pseudo-random number generators have been proposed and operated [10], [12]–[15]. On the other hand, random numbers that a physical phenomenon (i.e., thermal noise, atom collapse, and chaotic dynamics) generates is truly random, resulting in ideal nonperiodicity and unpredictability. Due to their generation methods, true random numbers are generated only by hardware random number generators (HRNGs). HRNGs composed of SFQ-based circuits were demonstrated in which thermal noises were utilized [11], [16].

We recently proposed an oscillation-based HRNG in which timing jitters in SFQ digital circuits were employed [17]. The oscillation-based HRNG was composed of a few logic gates and the Josephson oscillator using the Josephson relationship between the voltage and oscillation frequency. Due to its simple configuration, the oscillation-based HRNG was realized in SFQ circuitry with low hardware costs and technical difficulty. We designed and fabricated test circuits using the digital cell library (referred to as "CONNECT" [18]) and the 2.5 kA/cm^2 Nb/AlO$_x$/Nb integration process (STP2) [19] of the National Institute of Advanced Industrial Science and Technology (AIST), and confirmed that random numbers generated by a test circuit satisfied all criteria of the NIST FIPS PUBS 140-2 (hereafter, referred to as FIPS 140-2) tests [20]. However, our test at that time was conducted only for one biasing condition.

In this paper, we refer to our oscillation-based HRNG as an "SFQ oscillation-based HRNG," of which the abbreviation is "SO-HRNG." We transfer the design of the original SO-HRNG from STP2 to the 10 kA/cm^2 Nb/AlO$_x$/Nb integration process (HSTP) of AIST [21]. Higher random number generation rates are expected using SFQ circuitry with larger critical current densities even though we do not attempt high-speed random number generation in this paper. Test circuits fabricated using the HSTP are evaluated through the FIPS 140-2 tests with various biasing conditions. The dependence of the random number quality on the biasing conditions is discussed.

2. Configuration of the SO-HRNG

Figure 1 shows a simplified configuration of the SO-HRNG [17]. The circuit consists of an over-biased Josephson junction, a toggle flip-flop (TFF), and an AND gate. The over-biased Josephson junction, which is in the voltage state by injecting DC current larger than the junction critical current, works as an oscillator generating SFQ pulses

Manuscript received July 28, 2021.
Manuscript revised October 11, 2021.
Manuscript publicized January 19, 2022.

[†]The authors are with The University of Electro-Communications, Chofu-shi, 182–8585 Japan.
[††]The author is with Fukuoka Institute of Technology, Fukuoka-shi, 811–0295 Japan.
a) E-mail: k-sato@w8-7f.ee.uec.ac.jp
b) E-mail: y.mizugaki@uec.ac.jp

DOI: 10.1587/transele.2021SES0001

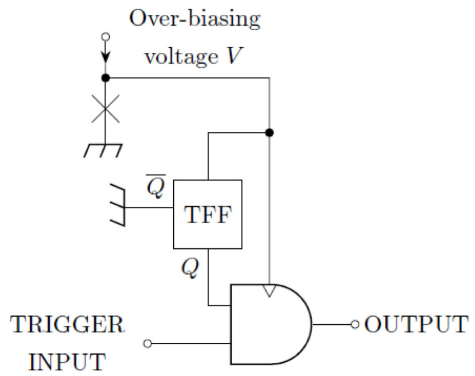

Fig. 1 Simplified block diagram of the SFQ oscillation-based HRNG (SO-HRNG)

with the repetition-frequency $f = V/\Phi_0$, where V and Φ_0 are the DC voltage across the junction and the quantity of an SFQ [22]. The high repetition-frequency SFQ pulses are transferred from the over-biased Josephson junction to the input terminal of the TFF and the clock terminal of the AND gate. Moreover, the TFF provides one SFQ pulse to a signal input terminal of the AND gate for every two input SFQ pulses. Then, the internal state of the AND gate switches between "0" and "1" at the oscillation frequency of the over-biased Josephson junction. Meanwhile, trigger SFQ pulses of low repetition-frequency are fed to another input terminal of the AND gate. If the internal state of the AND gate is "0" (or "1") at the timing of the trigger SFQ arrival, the output becomes "0" (or "1") for the subsequent clock signal. If there were no noise effects in the circuits, there should be synchronous operation of the high repetition-frequency SFQ pulses from the over-biased Josephson junction and the low-frequency SFQ pulses from the trigger terminal. However, thermal noise currents at finite temperatures must induce timing jitters in the trigger signal line, leading to a true random number output.

It should be noted that, the timing jitters should be larger than the oscillation period of the over-biased Josephson junction to generate true random numbers. Numerical simulation using "jsim_n" [23] for the SO-HRNG at 4.2 K with the parameters of the HSTP suggested that the trigger frequency reached no less than 400 MHz under the over-biased Josephson junction oscillating at 150 GHz.

3. Experiments

The SO-HRNG was designed using a digital cell library, the modified "CONNECT" library for the AIST HSTP. A DC-to-SFQ converter and an SFQ-to-DC converter were implemented for the SO-HRNG in addition to the over-biased Josephson junction, TFF, and AND gate shown in Fig. 1.

Test chips were fabricated using the AIST HSTP. Figure 2 shows a photomicrograph of a fabricated SO-HRNG.

In measurements, a test chip was cooled in a liquid helium bath. The trigger input was a sine wave fed from a function generator to a DC-to-SFQ converter via a 50 Ω resistor on the chip. The DC voltage across the over-biased Josephson junction was set to 60 μV, of which the corresponding oscillation frequency was 29 GHz. The output signal from the SFQ-to-DC converter was monitored and observed observed with a digital oscilloscope via a 40-dB preamplifier. We chose the trigger frequency as 500 kHz since the cut-off frequency of the preamplifier was 1 MHz.

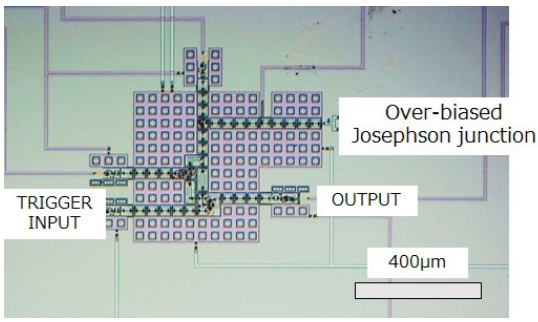

Fig. 2 Photomicrograph of a fabricated SO-HRNG.

Test sets defined in the FIPS 140-2 tests (Monobit, Poker, Runs 1–Runs 6+, and Long Runs) [20] were again used to evaluate the quality of random numbers generated by the SO-HRNG. Notably, the FIPS 140-2 testing has ended, and other improved tests such as NIST SP800-22 [24] and TestU01 [25] are now available. However, the other modern tests require 10–1000 Mb random numbers, which were beyond the capacity of the storage in the digital oscilloscope. The trigger frequency of 500 kHz was not high enough, either. Due to these limitations in our experimental setup, we chose the FIPS 140-2 tests for evaluation.

26 random number sequences of 20 kb length were acquired and evaluated for each biasing condition.

4. Results and Discussion

Figure 3 presents an example of the SO-HRNG operation. It should be noted that each high/low transition of the SFQ-to-DC converter represents an output of "1," while no transition at a rising edge of the trigger signal means "0". Therefore, Fig. 3 exhibits a bit sequence of "01101010010010111100," demonstrating a typical random number sequence.

Figure 4 displays the bias voltage dependence of the pass rate for the FIPS 140-2 tests. As a result, the pass rate became 100% at 2.5 and 2.6 mV, and the nominal bias voltage of the cell library was 2.5 mV. That is, 26 random number sequences of 20 kb length generated by the SO-HRNG at the biasing conditions of 2.5 and 2.6 mV satisfied all criteria of the FIPS 140-2 tests. As the biasing condition moves far from the nominal value, the pass rates gradually deteriorate below 2.5 and above 2.6 mV.

Furthermore, the pass rate for each test at each biasing condition is presented in Fig. 5. The pass rates for the Runs 1–Runs 6+ and Long Runs tests are 100% for the biasing conditions between 2.0 and 2.7 mV, whereas those for the Poker test reach 100% between 2.2 and 2.7 mV. Con-

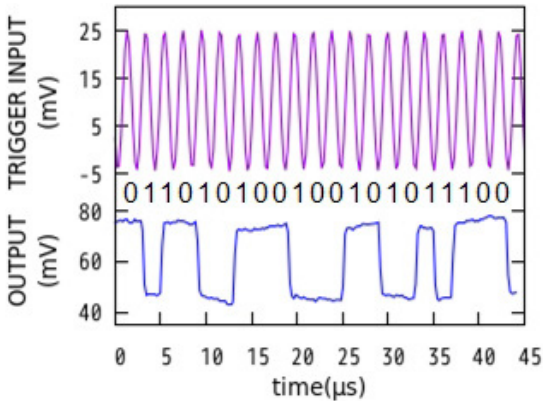

Fig. 3 Measured waveforms for SO-HRNG operation for the bias condition of 2.5 mV. The frequencies of the over-biased Josephson junctions and trigger signal were 29 GHz and 500 kHz, respectively. The trigger signal was fed to the DC-to-SFQ converter via a 50 Ω resistor on the chip, whereas the output signal from the SFQ-to-DC converter was amplified by a 40-dB preamplifier. The output offset of the preamplifier was approximately 45 mV.

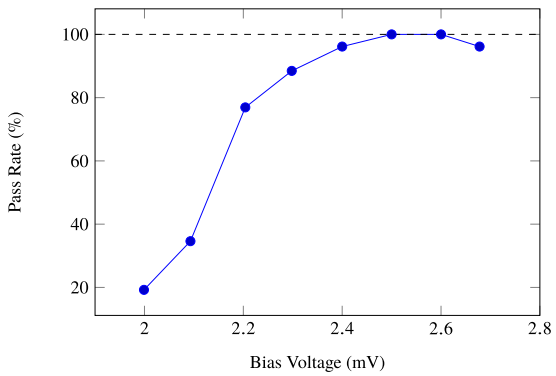

Fig. 4 Bias voltage dependence of the pass rates for the FIPS 140-2 tests.

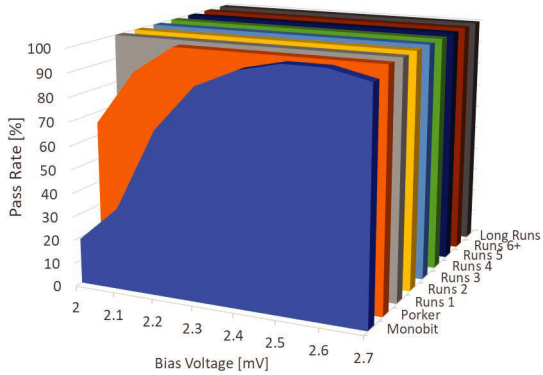

Fig. 5 Detailed results of the FIPS 140-2 tests. The pass rates for nine tests are plotted as functions of the bias voltage.

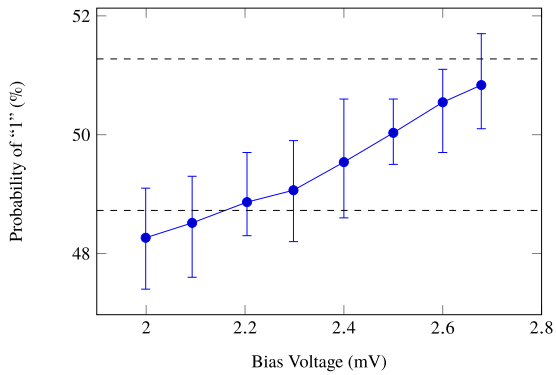

Fig. 6 Bias voltage dependence of the probability of getting "1". The average probabilities for each bias voltage are plotted with circles, whereas the bars represent the minimum and maximum probabilities among 26 sequences of 20 kb length. The Monobit test in the FIPS 140-2 requires the probabilities between 48.725 and 51.275%, of which dashed lines indicate edges.

versely, the Monobit test was 100% satisfied for the limited conditions of 2.5 and 2.6 mV. Additionally, the Monobit test checks if the number "1" in a 20 kb sequence falls into the range between 9,725 and 10,275. From Fig. 5, it is determined that the Monobit test is the most challenging test for the SO-HRNG.

Further evaluation for the Monobit test is shown in Fig. 6. Consequently, the probability of getting "1" was increased monotonically with increasing the bias voltage. Such bias dependence was in agreement with our numerically results [26], as discussed below. For the bias voltages of 2.5 and 2.6 mV, the "1" probabilities of all 26 random number sequences of 20 kb length satisfied the criteria (between 48.725 and 51.275%). For other biasing conditions, some random number sequences did not satisfy the Monobit requirements in the FIPS 140-2.

Numerical simulation in our previous work [26] figured out that the AND gate had different switching areas for the outputs of "0" and "1" and that they depended on the bias voltage. In the SO-HRNG shown in Fig. 1, the time duration ratio for the AND gate generating "1" and "0" should ideally be 50%:50% for two clock periods. However, the time duration ratio for the AND gate in the "CONNECT" library changes from 49.88%:50.12% to 50.05%:49.95% as the bias voltage increases from 2.2 to 2.7 mV. More specifically, numerical results signified that the ratio for the output of "1" increased as the bias voltage increased, consistent with the experimental results shown in Fig. 6. In order to improve the bias margin of the SO-HRNG in the future, the bias dependence of the AND gate should be addressed.

5. Conclusion

We experimentally evaluated random number sequences generated by the SO-HRNG. Test circuits were fabricated using the AIST HSTP (10 kA/cm^2). Measurements were conducted in a liquid helium bath. 26 random number sequences of 20 kb length were evaluated for bias voltages between 2.0 and 2.7 mV. The FIPS 140-2 tests were used for evaluation, where 100% pass rates were confirmed at bias voltages of 2.5 and 2.6 mV. We determined that the Monobit test limited the pass rates. Detailed evaluation for the probabilities of getting "1" showed the monotonical dependence on the bias voltage as numerical simulation had suggested.

The bias voltage dependence was likely to be attributed to the characteristics of the AND gate.

Acknowledgements

The authors thank the lab members in The University of Electro-Communications (UEC Tokyo) for their fruitful discussion and technical support. The circuits used in this work were fabricated using the Nb HSTP in the CRAVITY, AIST, Japan. This work was partly supported by JSPS Grant-in-Aid for Scientific Research JP17K04979 & JP20H02201 and by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Cadence Design Systems. The stable supply of liquid helium from the Co-ordinated Center for UEC Research Facilities, UEC Tokyo, Japan, is also acknowledged.

References

[1] K. Nakajima and Y. Onodera, "Logic design of Josephson network," J. Appl. Phys., vol.47, no.4, pp.1620–1627, April 1976. DOI: 10.1063/1.322782

[2] K. Nakajima and Y. Onodera, "Logic design of Josephson network. II," J. Appl. Phys., vol.49, no.5, pp.2958–2963, May 1978. DOI: 10.1063/1.325138

[3] O.A. Mukhanov, V.K. Semenov, and K.K. Likharev, "Ultimate performance of the RSFQ logic circuits," IEEE Trans. Magn., vol.MAG-23, no.2, pp.759–762, March 1987. DOI: 10.1109/TMAG.1987.1064951

[4] K.K. Likharev and V.K. Semenov, "RSFQ logic/memory family: A new Josephson-junction technology for sub-terahertz-clock-frequency digital systems," IEEE Trans. Appl. Supercond., vol.1, no.1, pp.3–28, March 1991. DOI: 10.1109/77.80745

[5] H. Hayakawa, N. Yoshikawa, S. Yorozu, and A. Fujimaki, "Superconducting Digital Electronics," IEEE, vol.92, no.10, pp.1549–1563, Sept. 2004. DOI: 10.1109/JPROC.2004.833658

[6] N.K. Katam, J. Kawa and M. Pedram, "Challenges and the status of superconducting single flux quantum technology," March 2019 Design, Automation & Test in Europe Conference & Exhibition, pp.1781–1787, Sept. 2019. DOI: 10.23919/DATE.2019.8747356

[7] M. Tanaka, F. Matsuzaki, T. Kondo, N. Nakajima, Y. Yamanashi, A. Fujimaki, H. Hayakawa, N. Yoshikawa, H. Terai, and S. Yorozu, "A single-flux-quantum logic prototype microprocessor," 2004 IEEE International Solid-State Circuits Conference (IEEE Cat. No.04CH37519), pp.298–529, Sept. 2004. DOI: 10.1109/ISSCC.2004.1332714

[8] Y. Yamanashi, T. Kainuma, N. Yoshikawa, I. Kataeva, H. Akaike, A. Fujimaki, M. Tanaka, N. Takagi, S. Nagasawa, M. Hidaka, "100 GHz demonstrations based on the single-flux-quantum cell library for the 10 kA/cm^2 Nb multi-layer process," IEICE Trans. electron., vol.E93-C, no.4, pp.440–444, April 2010. DOI: 10.1587/transele.E93.C.440

[9] I. Nagaoka, M. Tanaka, K. Inoue and A. Fujimaki, "A 48GHz 5.6mW gate-level-pipelined multiplier using single-flux quantum logic," 2019 IEEE International Solid- State Circuits Conference, pp.460–462, Feb. 2019. DOI:10.1109/ISSCC.2019.8662351

[10] J.H. Kang, J.X. Przybysz, S.S. Martinet, A.H. Worsham, D.L. Miller, J.D. McCambridge, "3.69 GHz single flux quantum pseudo-random bit sequence generator fabricated with Nb/AlO$_x$/Nb," IEEE Trans. Appl. Supercond., vol.7, no.2, pp.2673–2676, June 1997. DOI: 10.1109/77.621789

[11] Y. Yamanashi and N. Yoshikawa, "Superconductive Random Number Generator Using Thermal Noises in SFQ Circuits" IEEE Trans. Appl. Supercond., vol.19, no.3, pp.630–633, June 2009. DOI: 10.1109/TASC.2009.2019294

[12] A. Akahori, N. Takeuchi, N. Mori, Y. Suzuki, F. Furuta, A. Fujimaki, and H. Hayakawa, "Demonstration of 17 GHz operation of M-code generator based on SFQ with resettable latch," IEEE Trans. Appl. Supercond., vol.11, no.1, pp.521–524, March 2001. DOI: 10.1109/77.919397

[13] 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, no.1, pp.617–620, March 2001. DOI: 10.1109/77.919420

[14] T. Yamada, M. Maezawa, and C. Urano, "Design and test of component circuits of an integrated quantum voltage noise source for Johnson noise thermometry," Physica C, vol.518, pp.85–88, Nov. 2015. DOI: 10.1016/j.physc.2015.02.046

[15] Y. Mizugaki, Y. Mutoh, Y. Urai, K. Sawada, and T. Watanabe, "Three parallel generation of a 4-bit M-sequence using single-flux-quantum digital circuits," IEEE Trans. Appl. Supercond., vol.26, no.5, 1300504, Aug. 2016. DOI: 10.1109/TASC.2016.2536737

[16] T. Sugiura, Y. Yamanashi, N. Yoshikawa, "Demonstration of 30 Gbit/s generation of superconductive true random number generator," IEEE Trans. Appl. Supercond., vol.21, no.3, pp.843–846, Dec. 2010. DOI: 10.1109/TASC.2010.2092401

[17] T. Onomi and Y. Mizugaki, "Hardware random number generator using josephson oscillation and SFQ logic circuits" IEEE Trans. Appl. Supercond., vol.30, no.7, 1301305, Oct. 2020. DOI: 10.1109/TASC.2020.2992248

[18] S. Yorozu, Y. Kameda, H. Terai, A. Fujimaki, T. Yamada, and S. Tahara,"A single flux quantum standard logic cell library," Physica C, vol.378–381, pp.1471–1474, 2002. DOI: 10.1016/S0921-4534(02)01759-8

[19] S. Nagasawa, S. Hashimoto, Y. 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, no.2, pp.2447–2452, June, 1995. DOI: 10.1109/77.403086

[20] National Institute of Standards and Technology (NIST), "Security requirements for cryptographic modules," Federal Information Processing Standards Publication, Dec. 2002. DOI: 10.6028/NIST.FIPS.140-2

[21] N. Takeuchi, S. Nagasawa, F. China, T. Ando, M. Hidaka, Y. Yamanashi, and N. Yoshikawa, "Adiabatic quantum-flux-parametron cell library designed using a 10 kA cm^{-2} niobium fabrication process," Supercond. Sci. Technol., vol.30, no.3, Art. No. 035002, Jan. 2017. DOI: 10.1088/1361-6668/aa52f3

[22] P.I. Bunyk, A. Oliva, V.K. Semenov, M. Bhushan, K.K. Likharev, and J.E. Lukens, "High-speed single-flux-quantum circuit using planarized niobium-trilayer Josephson junction technology," Appl. Phys. Lett., vol.66, no.5, pp.646–648, Jan. 1995. DOI: 10.1063/1.114147

[23] E.S. Fang, "A josephson integrated circuit simulator (jsim) for superconductive electronics application," Extended Abstracts of 1989 Int. Conf. (The Japan Society of Appl. Phys., Tokyo, 1989), 1989.

[24] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, A. Heckert, D. Banks, J. Dray, and S. Vo, " A statistical test suite for random and pseudorandom number generators for cryptographic applications," Special Publication (NIST SP), National Institute of Standards, Sept. 2010. DOI: 10.6028/NIST.SP.800-22r1a

[25] P. L'Ecuyer, R. Simard, "TestU01: A C library for empirical testing of random number generators," ACM Trans. Mathematical Software, vol.33, no.4, Article No. 22, pp.1–40, Aug. 2007. DOI: 10.1145/1268776.1268777

[26] K. Koga and T. Onomi, "Relation between random number quality of superconducting random number generator based on single flux quantum generator and switching time of AND gate," JSAP Kyushu Chapter Annual Meeting 2020/The 5th Asian Applied Physics Conference (Asian-APC), 28Cp-18, on-line, Nov., 2020.