Hardware Random Number Generator Using Josephson Oscillation and SFQ Logic Circuits

doi: 10.1109/TASC.2020.2992248

Hardware Random Number Generator using Josephson Oscillation and SFQ Logic Circuits

Takeshi Onomi and Yoshinao Mizugaki

***Abstract*— A hardware random number generator using Josephson oscillation and a few single flux quantum (SFQ) logic gates is presented. The logic circuit of the random number generator consists of one toggle flip flop and one AND gate. A prototype random number generator is designed by logic cells based on a 2.5-kA/cm^2 Nb/AlOx/Nb integration process. The fundamental operation at a few hundred MHz of the random number sampling frequency is confirmed by numerical simulation when a DC/SFQ converter is used for generating trigger signals. An additional delay line using an overdamped Josephson transmission line is used for increasing the timing jitter to get random numbers. The delay line makes it possible for the random number generator to operate over 1 GHz. To confirm the fundamental operation of the circuit, a primitive SFQ random number generator is fabricated using the AIST standard process with 2.5-kA/cm^2 Nb/AlOx/Nb junctions and the standard logic cell library. A random number generation based on a low-speed functional test is successfully confirmed.**

***Index Terms*—Josephson oscillation, Random number generation, Single flux quantum logic circuits, Superconducting integrated circuits**

I. Introduction

RANDOM number generation is often required as important key ideas of data processing algorithms for scientific software simulations, statistical analysis, cryptography, and other situations or fields of research. Random number generation methods are classified roughly into two categories, which are based on software or hardware. Hardware random number generators (HRNGs) are preferable for applications of high-speed and large random number generations. There are two types of such HRNGs: a pseudorandom number generator and a true random number generator. The HRNG discussed in this paper is a true one, which is based on using some uncertain physical phenomena to get the source of random numbers.

We have alternatively proposed the stochastic logic using SFQ logic circuits for the computation of a neural network [1], [2]. Recently, stochastic-computing using adiabatic quantum-flux-parametron has also been proposed [3]. In the stochastic logic, a numeric value is converted to an occurrence probability of a pulse sequence. A HRNG is used for the generation of the stochastic pulse sequence. The usage of pseudorandom numbers generated by an m-sequence generator has been proposed in our previous concept. The independent random number generators must be installed for each bit of digital data to code the data to the stochastic pulse sequence. Therefore, if the bit length of digital data is large, the hardware cost of HRNGs is also large. HRNGs with low hardware cost are beneficial for the implementation of a large scale stochastic logic system.

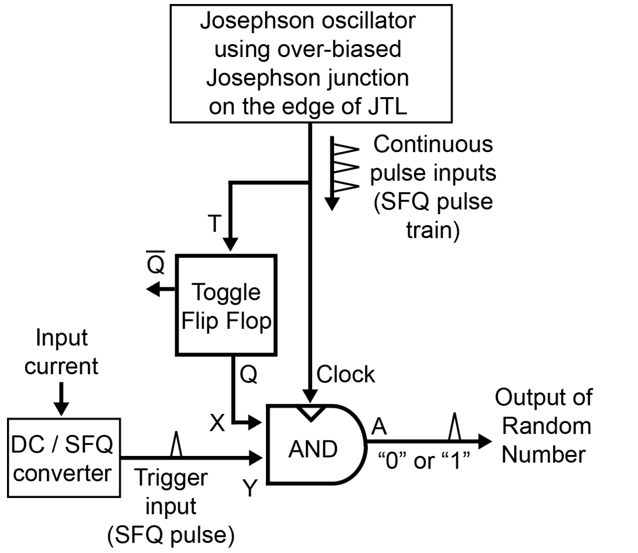
Josephson oscillator using over-biased Josephson junction on the edge of JTL
Continuous pulse inputs (SFQ pulse train)
T
$\overline{Q}$
Toggle Flip Flop
Q
Clock
Input current
DC / SFQ converter
X
Y
AND
A
"0" or "1"
Output of Random Number
Trigger input (SFQ pulse)

Fig. 1. Basic configuration of the SFQ HRNG circuit using Josephson oscillation. Each of logic cells is connected by Josephson transmission lines.

In this paper, we propose a simple HRNG using an SFQ pulse sequence generated by Josephson oscillation and a few SFQ logic gates. A comparator-based high performance HRNG using SFQ circuits has been already proposed [4]. This type of HRNG requires severe control of its bias current to generate random numbers with equivalent ratios of "0" and "1". Our target is not such an extremely high-end HRNG with a generation speed of a several tens GHz, but a simple HRNG with low hardware costs and low technical difficulty. The operation principle of the proposed HRNG is based on a relatively high speed toggle signal generator compared with an acquisition speed of random numbers and the timing jitter of the trigger to acquire the random number. Such oscillator-based HRNGs using semiconductor circuits have been proposed [5],[6]. The randomness of this type of HRNG is mainly based

Manuscript receipt and acceptance dates will be inserted here. This research was supported by JSPS KAKENHI under Grant 18K11231. *(Corresponding author: Takeshi Onomi.)*

T. Onomi is with the Faculty of Engineering, Fukuoka Institute of Technology, Fukuoka, Fukuoka 8110295 Japan (e-mail: onomi@fit.ac.jp).

Y. Mizugaki is with the Department of Engineering Science, The University of Electro-Communications, Chofu, Tokyo 1828585 Japan (e-mail: y.mizugaki@uec.ac.jp).

Digital Object Identifier will be inserted here upon acceptance.

on the timing jitter of sampling signals. In the SFQ circuitry, it is relatively easy to design an oscillator and elements of the timing jitter.

II. Design of a Hardware Random Number Generator

A. Operation principle of the SFQ HRNG using Josephson oscillation

Fig. 1 shows the basic configuration of the SFQ HRNG circuit using Josephson oscillation. The logic circuit consists of one toggle flip flop (TFF) and one AND gate. The SFQ pulse sequence generated by Josephson oscillation is supplied to the input of the TFF and the clock input of the AND gate, of which the output (Q) of the TFF is connected to the input. The SFQ pulse sequence can be easily generated by suppling an injection current to the edge of the Josephson transmission line (JTL) [7]. The injection current makes the junction on the edge of JTL an over-biased state, i.e., a voltage state. The voltage V across the junction can be converted to the frequency f of the SFQ pulse sequence according to the Josephson voltage-frequency relation, $V = \Phi_0 f$, where Φ_0 is the flux quantum (2.07×10^{-15} Wb). The sequence signal is used for a state transition between two internal states, which are “0” or “1”, of the input of the AND gate connected to the TFF output. If a trigger input from the other pair of the AND gate input lines is supplied at a timing within the continuous transition, a signal of “0” or “1” in response to an internal state can be obtained. To get a random number from the output signal, any fluctuations of the trigger timing or the internal state transition must be introduced. We discuss in Sec. III that a timing jitter equal to or larger than the oscillation period of the oscillator may be required for generating random numbers. DC/SFQ converters [8] are often used as the method to introduce SFQ pulses into SFQ circuits. If a DC/SFQ converter is operated by a sine (or triangular) wave, some timing jitter of the SFQ generation occurs due to thermal noises of resistances in the circuit.

TABLE I
FIPS 140-2 TEST RESULTS OF NUMERICAL SIMULATIONS OF THE SFQ HRNG WITH TRIGGER SFQ PULSE INPUTS GENERATED BY A DC/SFQ CONVERTER.

Randomness Tests	Accepted range		Test results [a]	
	Pass low	*Pass high*	*Average score*	*Passed*
Monobit	9725	10275	9933	15/15
Porker	2.16	46.17	18.75	15/15
Runs 1	2315	2685	2457	15/15
Runs 2	1114	1386	1237	15/15
Runs 3	527	723	619	15/15
Runs 4	240	384	319	15/15
Runs 5	103	209	161	15/15
Runs 6+	103	209	162	15/15
Long Runs	1	26	13.9	15/15

[a] The results depend on 15 times simulations in total (5 times each at 301, 300, and 299MHz).

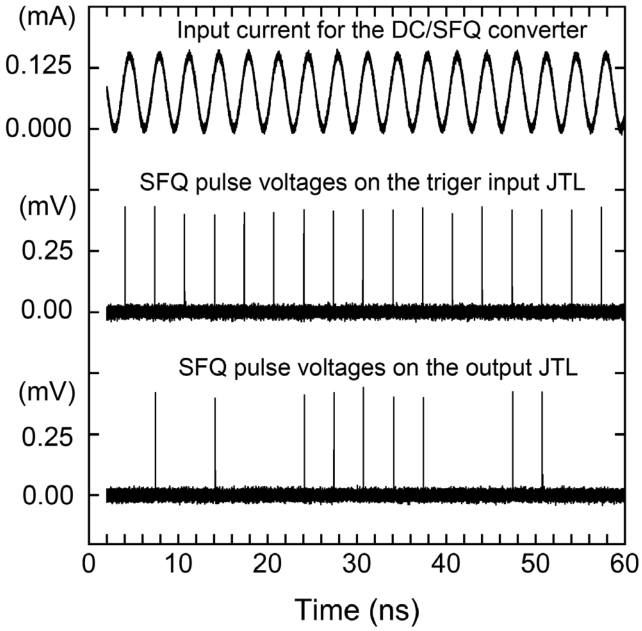

Fig. 2. An example of the dynamic simulation result of an SFQ HRNG circuit using Josephson oscillation. The upper line shows the input current for DC/SFQ converter of the trigger input to sample random numbers. The frequency of the sampling signal is 300 MHz. The middle line shows the SFQ pulse signals on the trigger input line. The lower lines shows the SFQ output signals as random numbers.

B. Design of the HRNG with a trigger input generated by a DC/SFQ converter

The SFQ circuits were designed using a cell library [9] based on the AIST standard process (STP2) [10] with 2.5-kA/cm^2 Nb/AlOx/Nb junctions. The designed HRNG was simulated by JSIM_N, which is a stochastic simulator that includes a thermal noise source [11]. In the dynamic simulations, SFQ pulse sequences with the frequency of 35.4 GHz were supplied by injection currents to the edge of the JTLs. The parameter of this frequency is not particularly optimized; there is room for further consideration because some thermal fluctuation of the frequency depending on the injection current is included [12]. The TFF and AND gate in the HRNG can operate at this frequency without difficulty.

III. Numerical Evaluations of the SFQ HRNG and Its Performance

Fig. 2 shows an example of the dynamic simulation result of the designed SFQ HRNG circuit. The upper trace is the input current for the DC/SFQ converter. The DC/SFQ converter of the input trigger line is supplied a 300-MHz sine wave current with DC offset, which is equal to the amplitude (0.075 mA). The SFQ pulses are generated at some currents near the value of 0.12 mA. The middle trace shows SFQ pulse voltages generated by the DC/SFQ converter. The generation timing of the SFQ pulses of 300 MHz has a fluctuation with a standard deviation of 14.7 ps estimated by numerical simulations. Because the standard deviation represents a one-sided

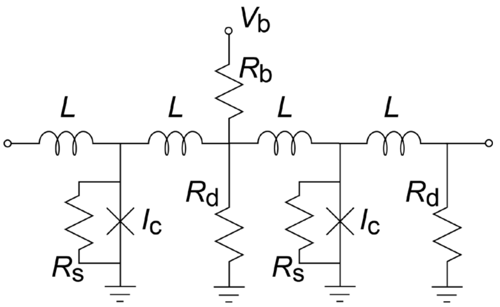

Fig. 3. One section of a delay line using an overdamped JTL to yield a timing jitter. The circuit parameters are $I_c = 0.108$ mA, $L = 4.41$ pH, $R_s = 0.53\ \Omega$, $R_d = 0.53\ \Omega$, $R_b = 24.3\ \Omega$, $V_b = 2.5$ mV.

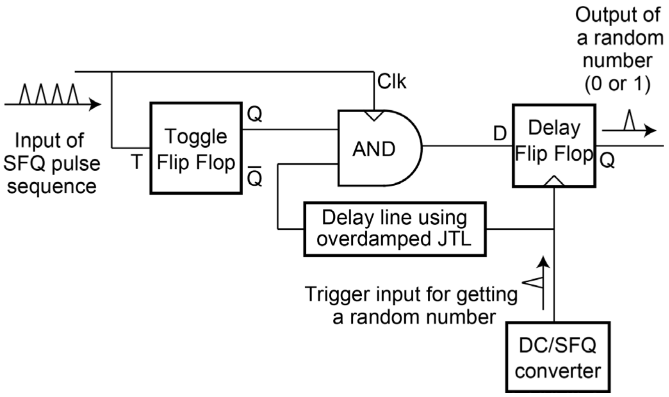

Fig. 4. SFQ HRNG circuit inserted a delay line using an overdamped JTL in order to increase the timing jitter of trigger input line. The delay line includes 20 sections of the overdamped JTL shown in Fig. 3.

TABLE II
FIPS 140-2 TEST RESULTS OF NUMERICAL SIMULATIONS OF THE SFQ HRNG ADDED DELAY LINE USING THE OVERDAMPED JTL

Randomness Tests	Accepted range		Test results [a]	
	Pass low	*Pass high*	*Average score*	*Passed*
Monobit	9725	10275	10005	15/15
Porker	2.16	46.17	17.14	15/15
Runs 1	2315	2685	2510	15/15
Runs 2	1114	1386	1271	15/15
Runs 3	527	723	617	15/15
Runs 4	240	384	310	15/15
Runs 5	103	209	154	15/15
Runs 6+	103	209	157	15/15
Long Runs	1	26	14.0	15/15

[a] The results depend on 15 times simulations in total (5 times each at 1001MHz, 1000MHz, and 999MHz).

variation from the mean, the timing jitter is twice the standard deviation. This timing jitter (29.4 ps) is slightly more than the oscillation period of the oscillator (28.2 ps). The lowest trace shows the output SFQ pulses as random numbers.

The random number bit sequences generated by the SFQ HRNG were evaluated by the statistical test of classical NIST FIPS PUBS140-2 [13]. This test suite can be executed for 20,000 bits of a random number sequence. Although there are currently stricter and newer test suites, a bit sequence including large numbers (at the Mb or Gb level) is required for such test suites. It is difficult for a dynamic circuit simulator to generate such a large random number bit sequence because it takes an inordinate processing time. We discuss the approximate operation performance of this proposed primitive HRNG. Table I shows the FIPS 140-2 test results of numerical simulations of the SFQ HRNG with a trigger SFQ pulse input generated by a DC/SFQ converter. The results depend on 15 times simulations in total (5 times each at 301, 300, and 299 MHz). Although there are few trial times because of the large processing time of the dynamic simulations, all tests were passed. Unfortunately, some tests were not passed near 400 MHz in similar tests. This may be because the timing jitter of the trigger input becomes smaller than the period of the signal from the Josephson oscillator. The standard deviation of the timing of the 400-MHz SFQ pulses is estimated by numerical simulations to be 11.7 ps. The standard deviation of the SFQ output timing of the DC/SFQ converter decreases as the frequency of the input current increases because the slope (sweep speed) of the input current is closely related to the timing jitter of the junction switching. From a qualitatively perspective, the quicker the input current passes through the vicinity of the threshold current, the more the timing jitter decreases, because the threshold has some fluctuation due to a thermal noise. To increase the frequency of sampling signals of random numbers, some other factors of the timing jitter may be needed.

We attempted to introduce a delay line using an overdamped JTL, shown in Fig. 3, to yield such a timing jitter. Fig. 4 shows the SFQ HRNG circuit with an inserted delay line using the 20 sections of the overdamped JTL. The estimated average delay time and its standard deviation were estimated to be 2.40 ns and 15.9 ps, respectively, by numerical simulations. A delay flip flop, shown in Fig. 4, was inserted to match each timing of outputs. If the delay flip flop is not inserted, each timing of the output signals has fluctuations including timing jitters due to the JTL delay line. Table II shows

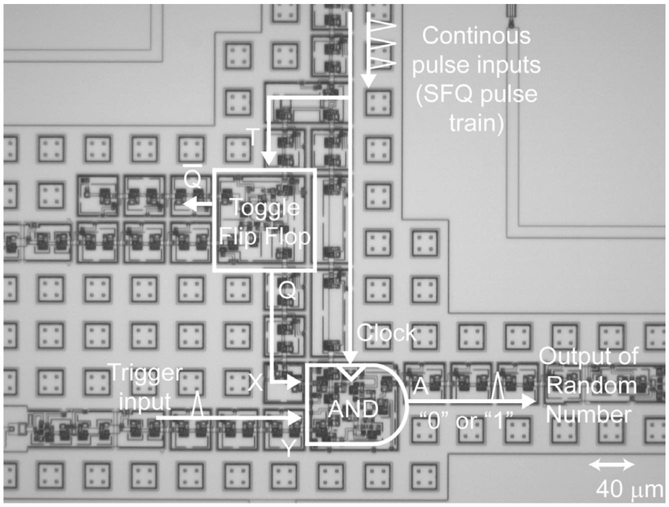

Fig. 5. Microphotograph of a fabricated SFQ HRNG circuit. The circuit configuration is based on the circuit shown in Fig. 1.

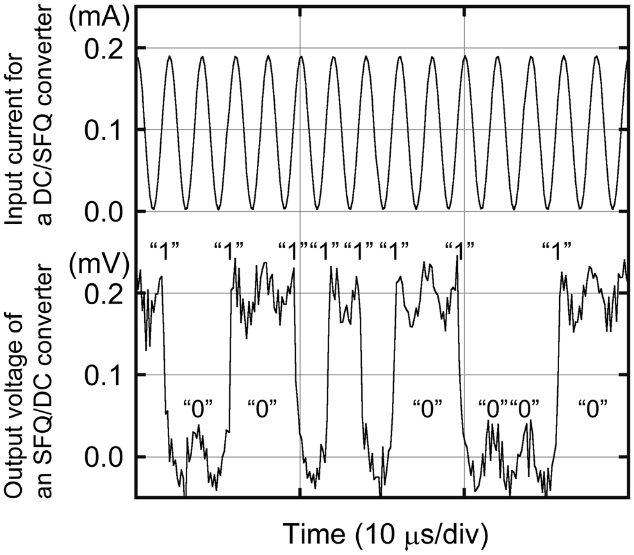

Fig. 6. Low-temperature measurement result of a SFQ HRNG circuit. The input current were supplied for a DC/SFQ converter to generate the trigger signals. The repetition frequency of the input trigger signals is 0.5 MHz. The outputs of random numbers were detected by the output voltage of an SFQ/DC converter.

the FIPS 140-2 test results of numerical simulations for this HRNG. The results depend on 15 times simulations in total (5 times each at 1001, 1000, and 999 MHz). The 15 times trial results confirmed that all tests were passed.

IV. Implementation of the Oscillator-based SFQ HRNG and Quality Evaluation of Random Numbers

A primitive oscillator-based SFQ HRNG was fabricated using the AIST standard process (STP2) with 2.5-kA/cm^2 Nb/AlOx/Nb junctions and the standard logic cell library mentioned in the previous section to confirm the basic circuit operations. Fig. 5 shows a microphotograph of a fabricated SFQ HRNG. The circuit configuration is as same as that shown in Fig. 1. The SFQ pulse sequence for the oscillation of the internal state transition of the AND gate was generated by supplying an injection current to an overdamped Josephson junction connected to the edge of the JTL. We used the overdamped junction to easily control the oscillation frequency as the change of the injection current. Trigger inputs were generated by a popular DC/SFQ converter. The output SFQ signals were measured using an SFQ/DC converter. The oscillation frequency of 30.9 GHz was used for the measurement because the global circuit parameter deviations existed on a fabricated circuit. (Both the critical current density of the Josephson junctions and the sheet resistance were about 7% smaller than each of the design values.)

Fig. 6 shows a measured low-speed test result of the SFQ HRNG circuit. The trigger SFQ signals for calling random numbers were generated at the rising slopes of the 0.5-MHz sine wave current for the DC/SFQ converter. However, the output signals as random numbers were measured by the SFQ/DC converter which detects SFQ pulses at the rising or falling edges of the pulse signals. The result shows a typical random number "10101111010010."

TABLE III
FIPS 140-2 test results of a measured SFQ HRNG

Randomness Tests	Accepted range		Test results	
	Pass low	*Pass high*	*Average score*	*Passed*
Monobit	9725	10275	9993	25/25
Porker	2.16	46.17	15.44	25/25
Runs 1	2315	2685	2498	25/25
Runs 2	1114	1386	1246	25/25
Runs 3	527	723	626	25/25
Runs 4	240	384	312	25/25
Runs 5	103	209	158	25/25
Runs 6+	103	209	157	25/25
Long Runs	1	26	13.5	25/25

To verify the quality of the random numbers, a long range data sequence was recorded on the memory of the oscilloscope that was used for the measurement shown in Fig. 6. We verified 25 data sets of bit sequences for the FIPS 140-2 test suite because the obtained data included 500 kbit of random numbers. Table III shows the FIPS 140-2 test results of the measured SFQ HRNG. All of the obtained data sets passed the test suite.

V. Conclusion

An oscillator-based HRNG using an SFQ pulse sequence generated by Josephson oscillation and SFQ logic circuits is proposed. The primitive HRNG is designed using an SFQ standard logic cell library based on the AIST standard process. The fundamental operation at 300 MHz of the random number sampling frequency is confirmed by numerical simulation when a DC/SFQ converter is used for generating trigger signals. An additional delay line using an overdamped JTL enables the HRNG to operate over 1GHz. A designed SFQ HRNG with a fundamental configuration was fabricated using the AIST standard process with 2.5-kA/cm^2 Nb/AlOx/Nb junctions. The generation of random numbers based on a low-speed functional test was successfully confirmed by a low-temperature measurement.

Acknowledgment

This research was partly supported by VLSI Design and Education Center (VDEC), the University of Tokyo, in collaboration with Cadence Design Systems, Inc. The circuits were fabricated in the clean room for analog-digital superconductivity (CRAVITY) of the National Institute of Advanced Industrial Science and Technology (AIST) with the standard process 2 (STP2). The authors thank Mr. K. Yamazaki and Mr. Y. Soumei for technical support during the low-temperature measurements.

References

[1] T. Kondo, M. Kobori, T. Onomi and K. Nakajima, “Design and Implementation of Stochastic Neurosystem Using SFQ Logic Circuits,” IEEE Trans. Appl. Superconduct., vol. 15, no. 2, June 2005, pp. 320–323.

[2] T. Onomi, T. Kondo, and K. Nakajima, “Implementation of High-Speed Single Flux-Quantum Up/Down Counter for the Neural Computation Using Stochastic Logic,” IEEE Trans. Appl. Superconduct., vol.19, no.3, June 2009, pp.626-629.

[3] R. Cai, A. Ren, O. Chen, N. Liu, C. Ding, X. Qian, J. Han, W. Luo, N. Yoshikawa, and Y.Wang, “A stochastic-computing based deep learning framework using adiabatic quantum-flux-parametron superconducting technology,” Proc. the 46th Int. Symp. Computer Architecture - ISCA ’19, June 2019, pp. 567–578.

[4] T. Sugiura, Y. Yamanashi, and N. Yoshikawa, “Demonstration of 30 Gbits/s Generation of Superconductive True Random Number Generator,” IEEE Trans. Appl. Superconduct., vol.21, no.3, June 2011, pp.843-846.

[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 a smart card IC, IEEE transactions on computers, vol. 52, no. 4, Apr. 2003, pp. 403–409.

[6] T. Amaki, M. Hashimoto and T. Onoye, “An oscillator-based true random number generator with jitter.” Proc. 2011 IEEE Int. Symp. Circuit and Systems, May 2011, pp. 725-728.

[7] P. I. Bunyk, A. Oliva, V. K. Semenov, M. Bhushan, K. K. Likharev, J. E. Lukens, M. B. Ketchen, and W. H. Mallison, “High-speed single-flux-quantum circuit using planarized niobium-trilayer Josephson junction technology,” Appl. Phys. Lett., vol. 66, no. 5, Jan. 1995, pp. 646-648.

[8] 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. Superconduct., vol. 1, no. 1, Mar. 1991, pp. 3–28.

[9] 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, Oct. 2002, pp. 1471-1474.

[10] S. Nagasawa, Y. Hashimoto, H. Numata, and S. Tahara, “A 380ps, 9.5mW Josephson 4-K bit RAM operated at a high bit yield,” IEEE Trans. Appl. Superconduct., vol. 5, no.2, Jun. 1995, pp. 2447–2452.

[11] J. Satchell, “Stochastic simulation of SFQ logic,” IEEE Trans. Appl. Superconduct., vol. 7, no. 2, June 1997, pp. 3315–3318.

[12] Y. Mizugaki, Y. Urai, and H. Shimada, “Thermally-fluctuated single-flux-quantum pulse intervals reflected in input-output characteristics of a double-flux-quantum amplifier,” Journal of Physics: Conf. Series, vol. 871, no. 012066, July 2017.

[13] NIST, “Security requirements for cryptographic modules,” FIPS pub. 140-2, May 2001.

Takeshi Onomi received the B.E., M.E., and Ph.D. degrees from Tohoku University, Sendai, Japan, in 1993, 1995, and 1998, respectively.

From 1999 to 2015, he was with the Research Institute of Electrical Communication, Tohoku University. Since 2015, he has been with the Faculty of Engineering, Fukuoka Institute of Technology, Fukuoka, Japan. His research interests are in Josephson computing devices and intelligent integrated systems.

Dr. Onomi is a member of the Institute of Electronics, Information and Communication Engineers of Japan, and the Japan Society of Applied Physics.

Yoshinao Mizugaki received the B.E., M.E., and Ph.D. degrees from Tohoku University, Sendai, Japan, in 1990, 1992, and 1995, respectively.

In 1995, he was a Research Fellow of the Japan Society for the Promotion of Science (JSPS) at Nagoya University for six months. From 1995 to 2002, he was a Research Associate at the Research Institute of Electrical Communication, Tohoku University, except for one year from 1999 to 2000, when he was a Visiting Researcher at Chalmers University of Technology, Gothenburg, Sweden. From 2002 to 2009, he was an Associate Professor at The University of Electro-Communications, Tokyo, Japan, where he has been a Professor since 2009. His research interests are in Josephson devices, single-electron devices, electronics using lipid bilayer membranes under water, and advanced integration systems.

Prof. Mizugaki is a member of the Japan Society of Applied Physics and the Institute of Electronics Information and Communication Engineers of Japan.