PAPER *Special Section on Frontiers of Superconductive Electronics*

Statistical Evaluation of a Superconductive Physical Random Number Generator

Tatsuro SUGIURA[†], ***Nonmember***, **Yuki YAMANASHI**[††a)], ***and*** **Nobuyuki YOSHIKAWA**[†], ***Members***

SUMMARY A physical random number generator, which generates truly random number trains by using the randomness of physical phenomena, is widely used in the field of cryptographic applications. We have developed an ultra high-speed superconductive physical random number generator that can generate random numbers at a frequency of more than 10 GHz by utilizing the high-speed operation and high-sensitivity of superconductive integrated circuits. In this study, we have statistically evaluated the quality of the random number trains generated by the superconductive physical random number generator. The performances of the statistical tests were based on a test method provided by National Institute of Standards and Technology (NIST). These statistical tests comprised several fundamental tests that were performed to evaluate the random number trains for their utilization in practical cryptographic applications. We have generated 230 random number trains consisting of 20,000-bits by using the superconductive physical random number generator fabricated by the SRL 2.5 kA/cm^2 Nb standard process. The generated random number trains passed all the fundamental statistical tests. This result indicates that the superconductive random number generator can be sufficiently utilized in practical applications.

key words: *single-flux-quantum circuit, random number, Josephson junction, comparator*

1. Introduction

A random number generator is one of the most important devices for secure communication systems. For example, in the case of Secure Socket Layer (SSL) protocol, a secure communication protocol widely used today, the cryptographic key is generated on the basis of the random number sequences [1]. At present, pseudo-random numbers, i.e., numbers generated by computers, are used in SSL. A large number of pseudo-random numbers have been developed so far [2], [3]. However, pseudo-random numbers are not suitable for the generation of cryptographic keys because a considerable amount of computer resources are required to implement effective pseudo-random number generation algorithms. Another major disadvantage is that the random number sequences can be predicted as they are generated using computational algorithm.

Physical random number generators have been developed in order to enhance the security of cryptographic communication systems [4]–[8]. These physical random number generators can generate truly random numbers by extracting entropy from natural physical phenomena such as thermal noise in atmosphere and nuclear fission. Since these physical phenomena are random in nature, physical random number generators can ensure the security of cryptographic communication systems.

Conventional physical random number generators, which employ semiconductors, generally use the thermal noise in their circuits as the source of randomness. Because the amplitude of thermal noise is much lower than the logic levels of the semiconductor circuit, amplification of noise is required. The amplification process restricts the generation speed of conventional physical random number generators to less than 10 Mbps [5]. This generation speed is insufficient for practical communication systems.

We have been developing a small-sized, ultra-high-speed physical random number generator using Josephson integrated circuits [9]. The proposed circuit uses the thermal noise in a single-flux-quantum (SFQ) circuit. The SFQ circuit provides a signal voltage of the order of hundreds of microvolts; therefore, there is no need to amplify the thermal noise, and a high-speed operation of tens of gigahertz can be expected [10]. We developed a prototype of the superconductive physical random number generator and statistically evaluated the randomness of the generated random number sequences.

2. Superconductive Physical Random Number Generator

A superconductive physical random number generator consists of an SFQ comparator and a current source. Figure 1

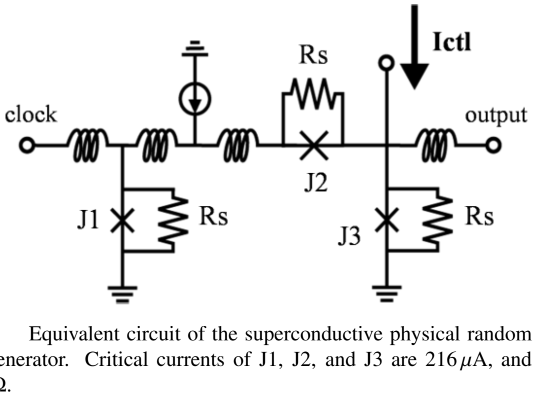


Fig. 1 Equivalent circuit of the superconductive physical random number generator. Critical currents of J1, J2, and J3 are 216 μA, and Rs = 1.73 Ω.

Manuscript received July 27, 2009.
Manuscript revised November 6, 2009.

[†] The authors are with the Department of Electrical and Computer Engineering, Yokohama National University, Yokohama-shi, 240-8501 Japan.
[††] The author is with Interdisciplinary Research Center, Yokohama National University, Yokohama-shi, 240-8501 Japan.
a) E-mail: yamanasi@ynu.ac.jp

DOI: 10.1587/transele.E93.C.453

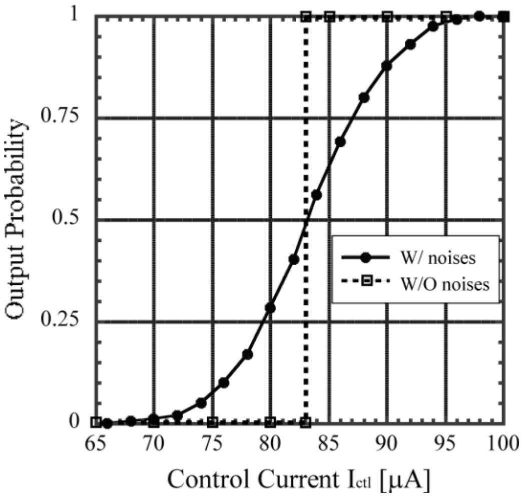


Fig. 2 Typical transition curve of the output probability of an SFQ comparator.

shows an equivalent circuit of the superconductive random number generator. All Josephson junctions are resistively shunted to adjust the McCumber parameters of junctions to ~1. In an ideal environment, where noise is absent, the Josephson junction *J*3 always switches if the control current *Ictl* 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 and quantum noises in the circuits [11]. The dependence of the output probability of the typical SFQ comparator on the control current as obtained by numerical simulation is shown in Fig. 2. The output probability of the SFQ comparator can be controlled by adjusting the supplied control current. We can obtain true random numbers by adjusting the control current such that the output probability is 0.5.

In order to estimate the maximum operating frequency of the superconductive physical random number generator, we performed a circuit simulation by Monte-Carlo analysis by considering the thermal noise [12]. The simulations were performed assuming the Superconductivity Research Laboratory (SRL) 2.5 kA/cm^2 Nb standard fabrication process [13], and the operation temperature was 4.2 K. Figure 3 shows the simulated results of the superconductive random number generator. The output signal, a datum "0" or "1," was obtained whenever the input clock was applied to the circuits. Therefore, the generation frequency for random numbers was equal to the frequency of the input clock. Figure 4 shows the simulated output probabilities of the superconductive physical random number generator. The control current I_{ctl} was adjusted to obtain an output probability of 0.5 for an input-clock frequency of 10 GHz. The dependence of the output probability of the superconductive physical random number generator on the input-clock frequency was studied by simulation. From the simulation results, we observed that the superconductive physical random number generator worked effectively at a generation frequency of up to 30 GHz for a bias voltage of 2.5 mV.

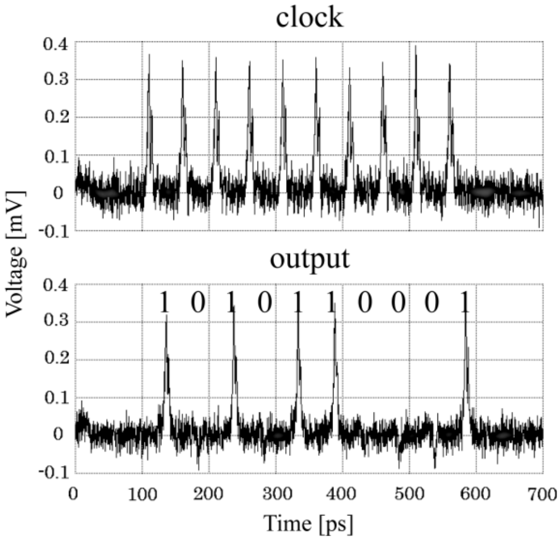


Fig. 3 An example of the simulated results of the superconductive physical random number generator. A random output sequence is obtained by inputting a periodical signal. The generation frequency for random numbers is 10 GHz. A random number train "1010110001" is obtained.

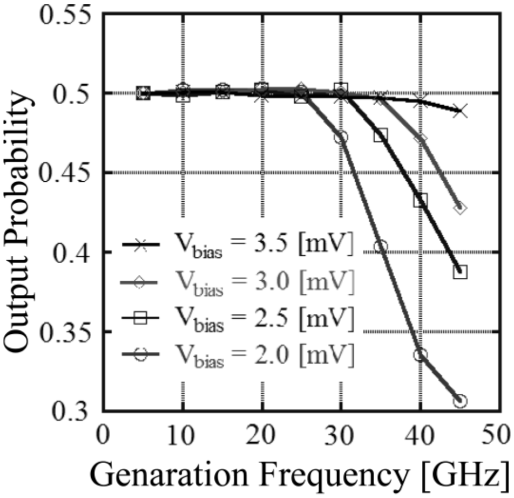


Fig. 4 Dependences of output probabilities on the generation frequencies for random numbers at various bias voltages. The standard bias voltage of the designed circuit is 2.5 mV.

We designed and implemented a superconductive physical random number generator using the SRL 2.5 kA/cm^2 Nb standard process [13]. The SFQ comparator, which is the main component of the superconductive physical random number generator, was fabricated on a 40 μm × 80 μm circuit.

We also developed an automated current-control system to adjust the control current to realize a stable operation of the superconductive physical random number generator. Figure 5 shows the block diagram of the system. The output probability of the SFQ comparator changed because of the noises in the bias voltage, noises from room-temperature equipments, and a change in temperature. The control current supplied to the system automatically adjusts to an optimum bias point on the basis of the output probability of the

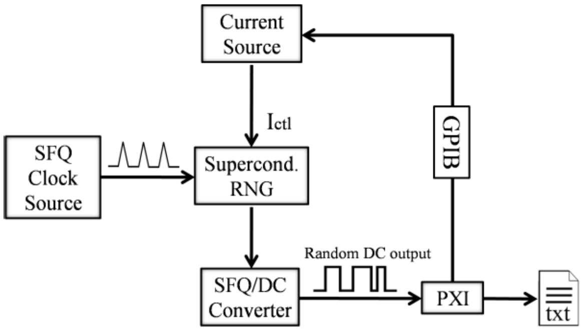


Fig. 5 Block diagram of the experimental setup.

circuit, which is monitored by a PXI system. In addition, this system can be used to record the output for a 20,000-bit random number train, and we can statistically evaluate the random number sequences. We have performed continuous tests for the superconductive random number generator using this setup.

3. Experimental and Statistical Tests

We have performed a low-speed test for the superconductive random number generator at 250 kHz and generated 230 random number trains consisting of 20,000-bit random numbers by using the automated measurement system. Figure 6 shows the experimental results of continuous tests on the superconductive physical random number generator. Since the automated current-control system worked, the output probability was maintained at approximately 0.5 during the measurement.

We have statistically evaluated the quality of the generated random number trains. The standard statistical tests — the monobit test, the porker test, the runs test, and the long runs test of the NIST FIPS 140-2 [14] — had been performed on the generated random number trains. At present, although these four tests have been deleted from the latest version of NIST FIPS140-2, they are often used as simple tests [15]. The four statistical tests of NIST FIPS 140-2 are provided below.

- The monobit (frequency) test
  The monobit test evaluates the probability of obtaining an output “1” in the random number sequences. In this test, the value of X is defined as the number of outputs of “1” in a 20-kbit stream. The required value of X is $9{,}725 < X < 10{,}275$.
- The poker test
  The random 20,000 stream is divided into 5,000 consecutive 4 bit segments. By counting and storing the number of occurrences of the 16 possible 4 bit values, $f(i)$ is defined as the number of each 4 bit value i, where $0 \leq i \leq 15$. X is determined as follows:

$$X = (16/5000) * \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000 \tag{1}$$

  The test is passed if $2.16 < X < 46.17$.

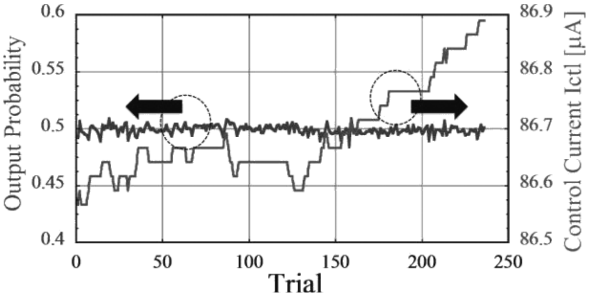


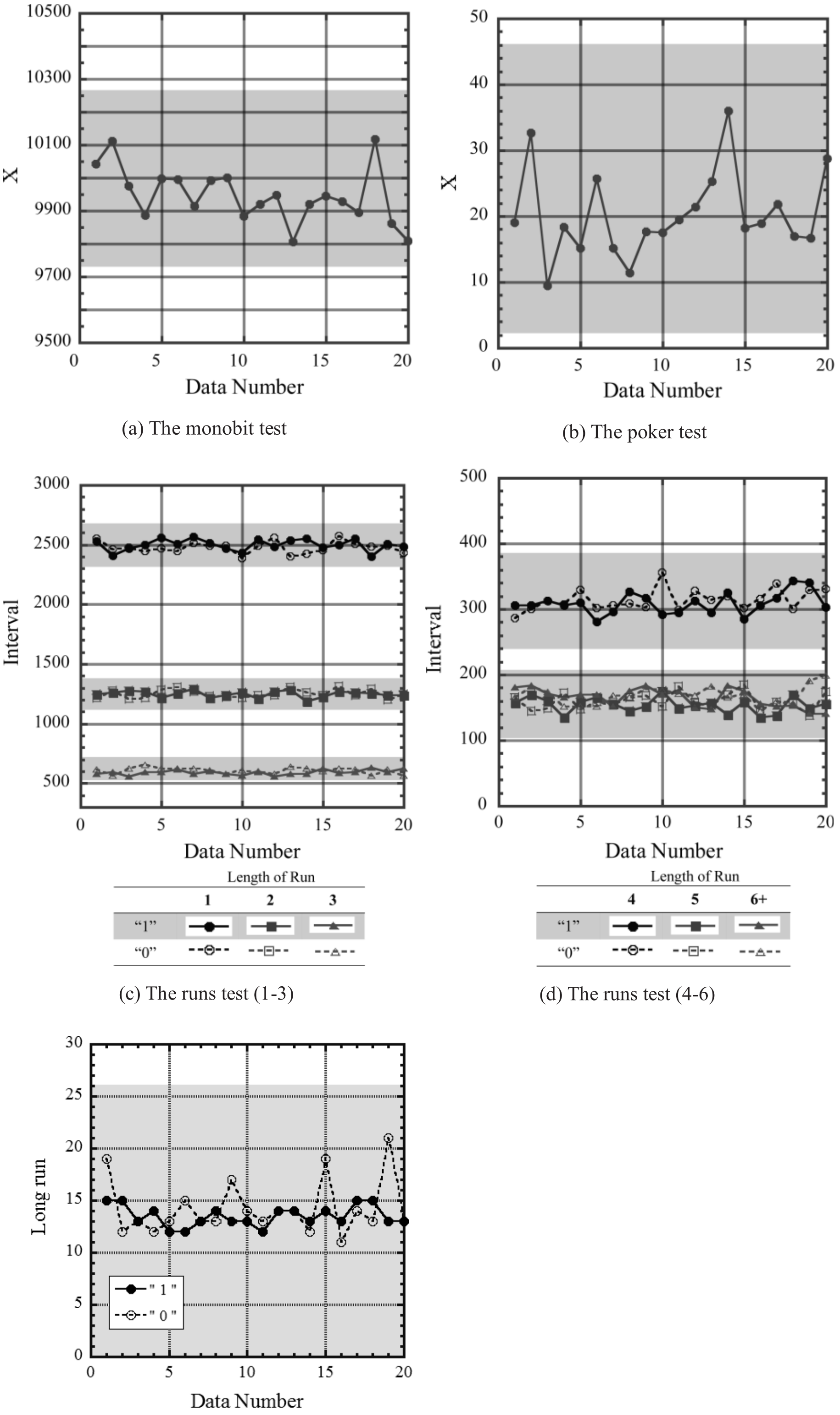
Fig. 6 Transitions of the measured output probability. One trial corresponds to a generation of 20-kbit random numbers.

Table 1 Requirements of the runs test.

Length of Run	Required Interval
1	2,315-2,685
2	1,114-1,386
3	527-723
4	240-384
5	103-209
6+	103-209

- The runs test
  A run is defined as a maximal sequence of consecutive bits in a sequence of either all ones or all zeros that are part of the 20,000-bit sample stream. The incidences of runs (for both consecutive zeros and consecutive ones) of all lengths (≥1) in the sample stream should be counted and stored. The test is passed if the runs (of lengths greater than 6) occur within the corresponding intervals, as specified in Table 1. This must hold true for both the zeros and ones (i.e., all 12 counts must lie in the specified interval). For the purposes of this test, runs of length greater than 6 are considered to have a length of 6.
- The long runs test
  A long run is defined as a run of length 26 or more (of either zeros or ones). In the case of the sample of 20,000 bits, the test is passed if there are no long runs.

All recorded random number trains passed these four statistical tests. The initially obtained statistical-test results of the 20 random number trains for each test are shown in Figs. 7(a)–(e) for clarify. These experimental results imply that the superconductive physical random number generator can be utilized in practical cryptographic applications. Additionally, a byte correlation plot (Fig. 8) of 8-Mbit random number sequences generated by the superconductive physical random number generator indicates a good quality of randomness.



(a) The monobit test

(b) The poker test

(c) The runs test (1-3)

(d) The runs test (4-6)

(e) The Long run test

Fig. 7 The results of NIST FIPS 140-2 tests. The colored regions indicate the ranges of the values required to pass the tests. The data number *n* refers to the *n*th measured random number sequence. The results of (a) the monobit test and (b) the poker test. (c) (d) Results of the runs test; runs for data "0" and data "1"are shown. (e) Results of the long run test.

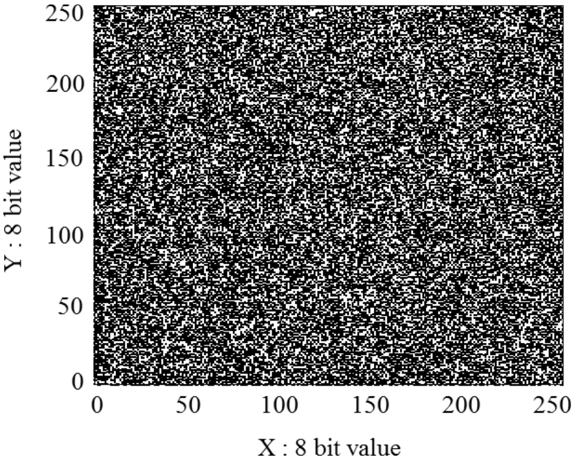


Fig. 8 Byte correlation plot of the 8 Mbit pattern.

4. Conclusion

We have designed and implemented a prototype of the superconductive physical random number generator. We developed a current-control system to ensure stable operation of the superconductive physical random number generator. The maximum generation frequency of random numbers is estimated to be 30 GHz through circuit simulations. We statistically evaluated the random number sequences generated by the superconductive physical random number generator. All generated random number sequences passed the FIPS 140-2 tests. This result indicates that the superconductive random number generator can be used for practical cryptographic applications.

References

[1] A.O. Freier and P.C. Kocher, "The SSL protocol — Version 3.0," IEFT, Internet Draft, 1996.

[2] Z. Gutterman, B. Pinkas, and T. Reinman, "Analysis of the linux RNG," IEEE Symposium on Security and Privacy, pp.371–385, 2006.

[3] M. Matsumoto and T. Nishimura, "Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator," ACM Trans. Modeling and Computer Simulations, vol.8, no.1, pp.3–30, 1998.

[4] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita, "1200 μm^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. Comput., vol.52, no.4, pp.403–409, 2003.

[6] 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.

[7] 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.

[8] C.S. Petrie and J.A. Connelly, "Noise-based IC random number generator for applications in cryptography," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.47, no.5, pp.615–621, 2000.

[9] 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, 2009.

[10] 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, no.1, pp.3–28, 1991.

[11] T.V. Filippov, Y.A. Polyakov, V.K. Semenov, and K.K. Likharev, "Signal resolution of RSFQ comparators," IEEE Trans. Appl. Supercond., vol.5, no.2, pp.2240–2243, 1995.

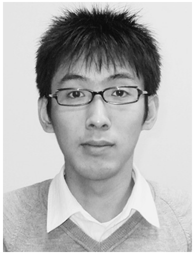
[12] Whiteley Research Inc., 456 Flora Vista Avenue, Sunnyvale, CA 94086. [Online]. Available: Homepage (http://www.srware.com/)

[13] 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, no.10, pp.2447–2452, 1995.

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

[15] M. Matsumoto, R. Ohba, S. Yasuda, K. Uchida, T. Tanamoto, and S. Fujita, "Non-stoichiometric Si$_x$N metal-oxide-semiconductor field-effect transistor for compact random number generator with 0.3 Mbit/s generation rate," Jpn. J. Appl. Phys., vol.47, pp.6191–6195, 2008.

Tatsuro Sugiura received the B.S. degree in electrical and computer engineering from Yokohama National University, in 2009. Since 2009, he has been with Graduate School of Engineering, Yokohama National University. He is a member of the Japan Society of Applied Physics.



Yuki Yamanashi received the B.S., M.E., and Ph.D. degrees in electrical and computer engineering from Yokohama National University, in 2003, 2005, and 2007, respectively. Since 2007, he has been with Interdisciplinary Research Center, Yokohama National University. His current research is on a novel application of superconductive circuits. He is a member of the Institute of Electrical and Electronics Engineering and the Japan Society of Applied Physics.

Nobuyuki Yoshikawa received the B.E., M.E., and Dr.Eng. degrees in electrical and computer engineering from Yokohama National University, Japan, in 1984, 1986, and 1989, respectively. Since 1989, he has been with the Department of Electrical and Computer Engineering, Yokohama National University, where he is currently a Professor. His research interests include superconductive devices and their applications to digital and analog circuits. He is also interested in single-electron-tunneling devices and quantum computing devices. Prof. Yoshikawa is a member of the Japan Society of Applied Physics, and the Institute of Electrical Engineering of Japan.