Extended Abstracts of the 2010 International Conference on Solid State Devices and Materials, Tokyo, 2010, pp1128-1129

F-7-2(Invited)

Spin dice: Random Number Generator using Current-Induced Magnetization Switching in MgO-MTJs

Akio Fukushima, Takayuki Seki, Kay Yakushiji, Hitoshi Kubota,
Shinji Yuasa and Koji Ando

Spintronics Research Center, Advanced Industrial Science and Technology (AIST)
Phone: 029-861-5572, E-mail: akio.fukushima@aist.go.jp
AIST Tsukuba Central 2, Tsukuba, Ibaraki 305-8568, Japan

1. Introduction

We propose a new application of a spintronics device; a physical random number generator[1]. Random numbers are generated by the probabilistic characteristic of spin transfer switching[2] in MgO-barrier magnetic tunnel junctions (MgO-MTJs)[3]. Because each switching event is independent, the generated random numbers have intrinsic unpredictability.

Recently, security of digital information has become much more important. Random numbers are widely used in encrypting data. Pseudo random numbers are mostly used for such purposes because of their convenience. However, unpredictability of pseudo random numbers is strongly preferred from the security point of view.

On the other hand, physical random numbers have an advantage in unpredictability. Thus, new kinds of high-speed physical random number generators have been proposed recently based on the thermal fluctuation of electrons in semiconductors[4], intensity fluctuation in the interference of light[5], or flux fluctuation in superconducting devices[6]. Nevertheless, these generators have a disadvantage in that they require extra equipment to convert physical phenomena into random numbers. In actual applications, the random number generator is required to be fast, compact, and have the possibility of being integrated.

We demonstrated a random number generator, called *spin dice*, using spin transfer switching in MgO-MTJs. The MgO-MTJs were repeatedly switched near the critical current, and the switching results were converted to binary numbers. We fabricated *spin dice* as a one-board circuit with a microprocessor and a USB interface, which can generate random numbers at 500 kbit/sec.

2. Experiments

An MTJ is a magneto-resistive device that has two magnetic layers, and its resistance changes depending on the magnetic configuration of the two magnetic layers. These layers have two stable configurations, parallel and anti-parallel. The parallel configuration results in low resistance and the anti-parallel high resistance. These two resistance values can be assigned to binary data “0” and “1”. This feature is applied to memory cells in magnetic random access memory (MRAM).

As the size of the MTJ decreases to less than several hundred nm, magnetization can be switched using a current. The current produces spin-transfer torque, which causes the switching. This switching is very fast; less than 1 nsec[7]. We can switch the two resistance states by applying a current pulse sequence.

When the width of a current pulse is longer than the attempt time (~1 nsec), the switching probability is dominated by the thermal activation[8]. The switching probability is proportional to the current amplitude near the critical current for the switching. In other words, we can directly control the switching probability by the current amplitude.

We used conventional MgO-MTJs with a 2 nm-thick CoFeB free layer, where the junction size was 70 × 200 nm. The resistance-area product value was about 3 Ω μm^2, and the magnetic resistance (MR) ratio was about 110%. The resistance changed between 220 and 465 Ω. The critical current for switching was about 1 mA.

A circuit diagram of the *spin dice* and the operation sequence are shown in Fig. 1. The circuit consists of an MgO-MTJ, a pulse generation circuit, a comparator, and a feedback circuit. The pulses are generated using analog switches then the pulse voltages (V_{reset}, V_{set}) are converted to the pulse currents using a resistor. The comparator determines the state of the MTJ, where V_{th} is set to the middle

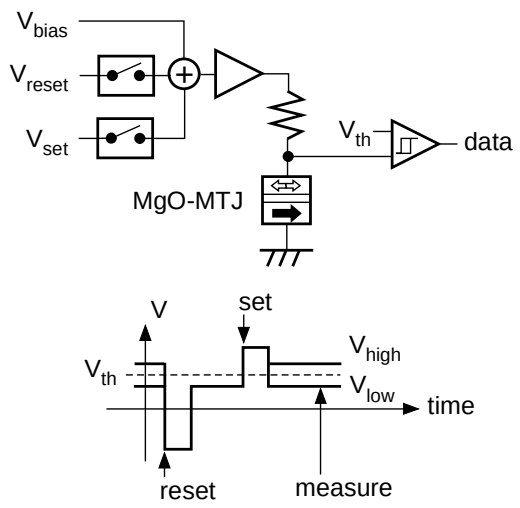

Fig. 1 Circuit diagram of *spin dice* and operation sequence for random number generation.

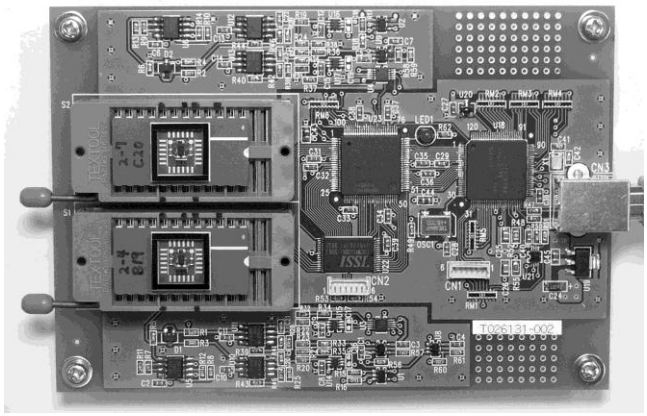

Fig. 2 Photograph of *spin dice*. Two pulse drive circuits are placed at upper and bottom parts. In middle are two MgO-MTJs, microprocessor with USB interface, FPGA, and SRAM.

of V_{high} and V_{low}. The feedback circuit (not shown in the figure) adjusts the set current to a switching probability of 50%. First, a large current pulse (reset pulse) is applied to initialize the magnetization state with a probability of 100%. Then a current pulse near the critical current (set pulse) is applied, and the state of the MTJ is measured. The switching results, success or failure, are converted to binary random numbers. V_{bias} is a bias voltage of 0.2 V, which is needed for measuring resistance.

Figure 2 shows a photograph of *spin dice*. The board has two sets of the MgO-MTJ and circuit. The MTJs are mounted in the dual-inline package (DIP) of 24 pins, and the board has a USB interface for connecting a host computer. The two sets of MTJs are indispensable for exclusive-or (XOR) operation. The board is operated at a current pulse width of 500 ns, and the generation speed of random numbers is up to 500 kbit/sec.

3. Results and discussion

We generated more than 1 Tbits of random numbers from the same MgO-MTJs. The resistance and MR ratio did not changed during operation. The average probability of the random numbers was obtained in a packet of 200,000 cycles of the reset-set sequence. The average probabilities fluctuated randomly in spite of the feedback operation. We consider this as mainly due to temperature fluctuation. To improve equiprobability of random numbers, we used XOR operation, which is commonly used in the field of information science.

Figure 3 shows a time chart of the averaged probabilities of the random numbers generated by MTJ-1 and MTJ-2, and that after XOR operation. The variance of the random numbers after XOR operation decreased to one fifth that by MTJ-1 and MTJ-2. The distribution of XOR data agrees well with the ideal binominal distribution.

Furthermore, we checked the randomness of 400 Gbits

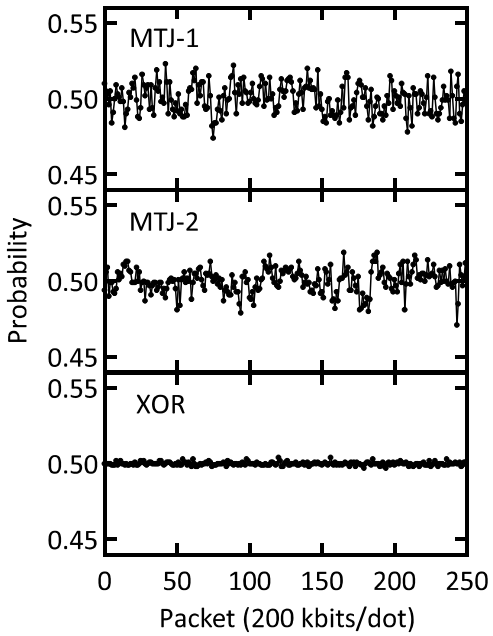

Fig. 3 Average probabilities of packet of 200-kbit random numbers. Bottom is probabilities after XOR operation of above two data sets.

of random numbers after XOR operation using the statistic test suite for randomness (NIST SP 800-22), and found those random numbers passed the test reasonably.

4. Conclusion

We fabricated *spin dice*: a physical random number generator using spin transfer switching in MgO-MTJs. Random numbers are generated from the probabilistic switching induced by the spin-transfer torque. This is a new type of random number generator in which probability is directly controlled by the current.

Because the structure of *spin dice* is identical to that of MRAM, it would be easy to integrate a number of MTJs in parallel for higher speed operation. The intrinsic unpredictability of *spin dice* will be useful for encrypting data.

Acknowledgements

This study was supported by the New Energy and Industrial Technology Development Organization (NEDO).

References

[1] A. Fukushima *et al.*, 52nd MMM Conference, DE-11, Tampa, USA (2007); Intermag 2008, GD-12, Madrid, Spain (2008).
[2] J. C. Slonczewski, J. Magn. Magn Mater. **159**, L1 (1996).
[3] S. Yuasa *et al.*, Nature Mater. **3**, 868 (2004); S. S. Parkin *et al.*, Nature Mater. **3**, 862 (2004).
[4] M. Matsumoto *et al.*, TOSHIBA REVIEW **62**, 39 (2007).
[5] A. Uchida *et al.*, Nature Photonics, **2**, 728 (2008).
[6] Y. Yamanashi *et al.*, JSAP 56th Spring meeting, 31p-ZQ-1 (2009).
[7] A. A. Tulapurkar *et al.* Appl. Phys. Lett. **85**, 5358 (2004).
[8] R. H. Koch *et al.*, Phys. Rev. Lett. **92**, 088302 (2004).