Extended Abstracts of the 2016 International Conference on Solid State Devices and Materials, Tsukuba, 2016, pp81-82

B-2-05

Long-Term Reliable Physically Unclonable Function using Oxide Tunnel Barrier Breakdown on 2T-2MTJ Based Embedded-STT-MRAM

Satoshi Takaya, Tetsufumi Tanamoto, Hiroki Noguchi, Kazutaka Ikegami, Keiko Abe, and Shinobu Fujita

Corporate R&D Center, Toshiba Corporation, Kawasaki, Japan, E-mail: satoshi1.takaya@toshiba.co.jp

Abstract

Spintronics has wide variety of applications and security is one of important fields on IoT devices. A physically unclonable function (PUF) with spin device (STT-MRAM) is presented. Oxide tunnel barrier breakdown is used to realize long-term stability for PUF. Secure PUF has been confirmed by evaluating Hamming distance of 32 bit STT-MRAM-PUF fabricated in a 65 nm CMOS technology.

1. Introduction

For huge number of mobile/wearable devices and Internet of Thing (IoT) devices, as information security is becoming very important, secure, reliable and low-cost ID is required to be implemented in every semiconductor chip. For this purpose, PUF is one of the most promising modules because uncontrollable process variations of semiconductor devices can be applied to generate unique ID. Recently, SRAM-PUF [1-2], flip-flop-PUF [3] and nonvolatile memory based PUF [4] has been proposed simply using device characteristics distribution, as shown in Fig. 1. In these memory-based PUFs, the spatial distribution of the initial variations of coupled inverters or defective memory cell is used as the unique ID. However, stability of ID produced by these PUFs is fundamentally unreliable, since characteristics of transistors or memory devices are inevitably shifted at high temperatures, for a long-term usage or variation of power supply voltage. Additional ID recovery scheme with area overhead is, hence, needed. To solve this issue, we propose reliable oxide tunnel barrier breakdown (OTB-) based PUF with 2T-2MTJ STT-MRAM and "stress termination circuit".

2. "Unreliable" STT-MRAM PUF using Initial Memory Device Variation

STT-MRAM is the most promising spin devices and STT-MRAM is the most promising embedded nonvolatile memory for mobile/wearable and IoT semiconductor chips. In STT-MRAM, magnetic tunnel junction (MTJ) has low resistance (parallel, P) state and high resistance (anti-parallel, AP) state to store the data (Fig. 2). If MRAM-PUF writes the data with the condition that switching probability of P and AP is both close to 50%, the ideally unique and secure ID can be simply created using pattern of P and AP [5]. However, it is entirely difficult to tune the write condition that switching probability is 50%, and the generated ID has no steadiness due to the switching probability of MTJ changed by temperature, long-time retention, and other environments. Figure 3 shows the switching probability and the Hamming distance (HD) of 128 bit PUF ID measured in 1.6 Kb STT-MRAM arrays, indicating there is no difference between intra- and inter-PUF. The correlation between generated 32 bit IDs is measured in 3 conditions (Fig. 4), and Fig. 4(b) shows favorable dispersion of IDs, since the same ID was not generated compared with others. However, it needs to detect the probability of 0/1 and tune condition of ID generation by changing the write voltage. Thus, simple MRAM-PUF cannot meet security system requirement.

3. Reliable STT-MRAM PUF using Oxide Tunnel Barrier Breakdown

Oxide barrier of MTJ between fixed layer and storage layer can be broken down by applying higher voltage (V_{STRESS}). The resistance of barrier breakdown MTJ is much lower than that of P or AP state with smaller distribution, and never changes even at high temperatures or for a long-term use. Also, barrier breakdown MTJs have larger read margin and higher repeatability. However, it is still difficult to control the balance between "0" (no breakdown) and "1" (breakdown) for 1T-1MTJ cell. Hence, we adopt 2T-2MTJ cell [6] based STT-MRAM (Fig. 5) to break only one side of MTJ pair and all of the bits can read as data "0" or "1". 1 bit 2T-2MTJ cell consists of symmetric 2 transistors (2T) and 2 MTJs, and shares source line (SL). When the left and the right MTJs have been broken, "0" and "1" are assigned, respectively. The probability of "0" and "1" is practically close to 50% and the same ID cannot be reproduced because MTJ breakdown has randomness. While applying V_{STRESS} through SL driver, both of the MTJ pair are stressed. When one side of MTJ has been broken, the stress voltage applying the other MTJ is automatically and immediately reduced, which makes the other MTJ difficult to be broken down. It is because stress voltage reduction on MTJ (V_{MTJ}) largely increases the time to breakdown of oxide barrier [7], as shown by simulation results in Fig. 6. However, there is still some risk that longer-time stress induces breakdown of the other MTJ.

4. Stress Termination Scheme

To confirm barrier breakdown of only one MTJ in 2T-2MTJ more definitely, we also propose stress termination circuit. Figure 7 shows the circuit having breakdown detector and feed-back loop to the SL driver. Breakdown detector has two current paths, one is the mirror current of the stress current, the other is larger than the one and used as a reference that is held at the initial value of stressing the cell (sample hold). When one of the MTJ has been broken, the mirror current becomes smaller than the reference and the detector output is changed. This output feeds back to SL driver, and voltage stress to the cell is immediately terminated.

5. Integration and Measurement Results

Figure 8 shows the embedded STT-MRAM PUF chip photograph, using 65 nm CMOS technology, and macro size is 1060 um x 140 um. The PUF block uses a part of high-performance embedded 2T-2MTJ cell STT-MRAM (Fig. 9). We measured 12 samples of 32 bit STT-MRAM PUF chips. Figure 10 shows resistance of pair MTJ while applying stress voltage, only one side of the MTJs was broken. The measured PUF ID and HD of 12 samples are shown in Fig. 11. Intra-PUF distance has only one value and the distance between intra- and inter-PUF is long enough.

6. Conclusions

The integration and demonstration of newly proposed embedded STT-MRAM PUF with OTB of 2T-2MTJ has been presented. Measured PUF ID has larger HD than conventional one, and has long-term reliability. In our method, ID is generated just one time after the PUF unit is initially activated by authorized users. This means that ID is never copied and stolen before the chip is shipped and entirely secure.

Acknowledgements

This study has been partly supported by NEDO.

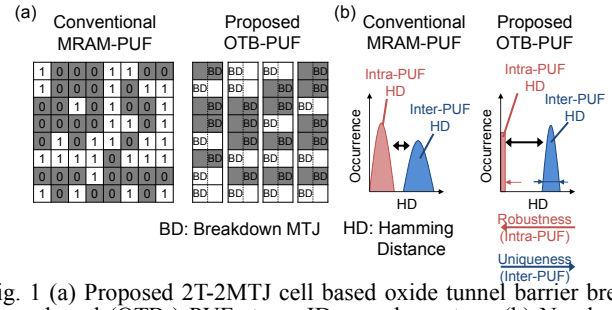

Fig. 1 (a) Proposed 2T-2MTJ cell based oxide tunnel barrier breakdown based (OTB-) PUF stores ID complementary. (b) Number of different bits between generated IDs (Hamming distance, HD) generated in same device (intra-PUF distance), and another device (inter-PUF distance) show robustness and uniqueness. Larger distance between intra- and inter-PUF is required.

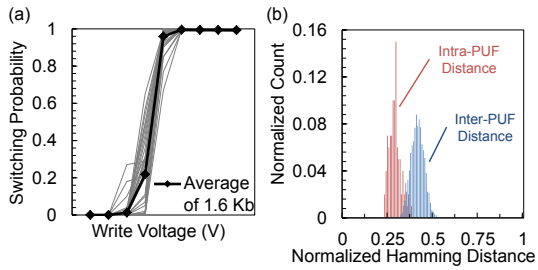

Fig. 3 (a) Switching probability of MTJ cell, measured in 1.6 Kb 2T-2MTJ STT-MRAM array. (b) Measured HD of PUF-ID generated by conventional MRAM-PUF method.

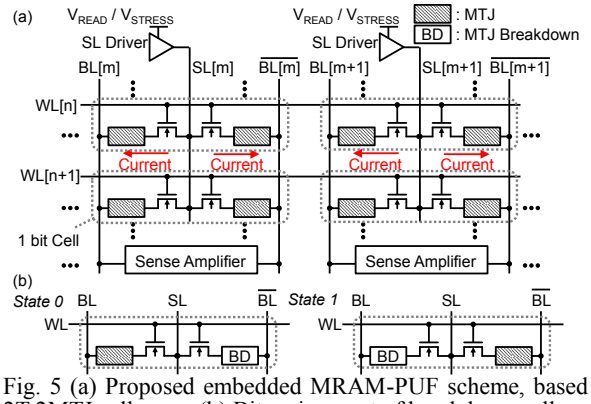

Fig. 5 (a) Proposed embedded MRAM-PUF scheme, based on 2T-2MTJ cell array. (b) Bit assignment of breakdown cell.

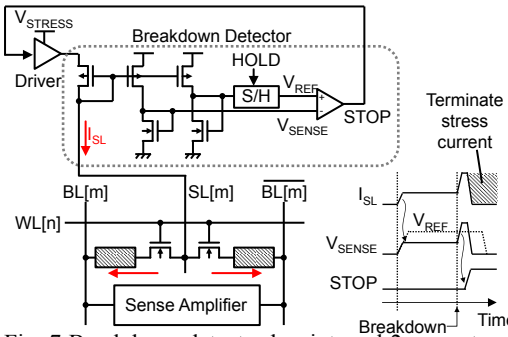

Fig. 7 Breakdown detector has internal 2 current paths, generating sensing voltage (V_{SENSE}), and self-reference voltage (V_{REF}). One current is the mirror current by the stress current, the other current is larger than the one and used as a reference that is held at the initial value of stressing the cell (sample hold). When one of the MTJs has been broken, the mirror current becomes smaller than the reference, and the detector output is changed. This output of detector feeds back to SL driver, and voltage stress to the cell is immediately terminated.

References

[1] Y. Su et al., ISSCC, pp. 406-407, 2007.
[2] S. K. Mathew et al., ISSCC, pp. 278-279, 2014.
[3] J. W. Lee et al., VLSI Circuits, pp. 176-179, 2004.
[4] W. Che et al., ICCAD, pp. 148-153, 2014.
[5] T. Marukame et al., IEEE Trans. on Magnetics, vol. 50, no. 11, pp. 3402004-1 - 3402004-4, 2014.
[6] H. Noguchi et al., VLSI Circuits, pp. 108-109, 2013.
[7] K. Hosotani et al., IRPS, pp. 703-704, 2008.

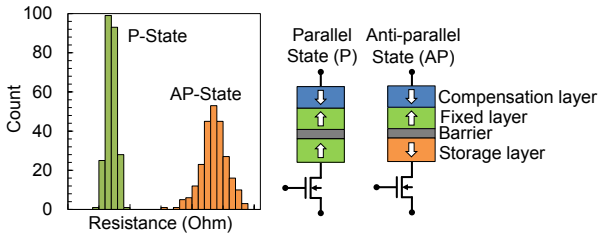

Fig. 2 Measured resistance distribution of MTJ.

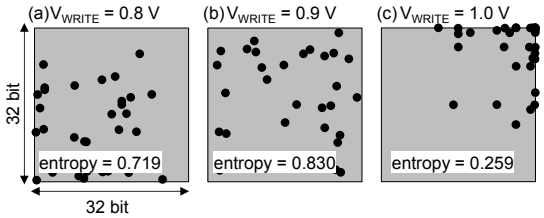

Fig. 4 Correlation of 32 samples PUF-ID generated by conventional MRAM-PUF method. Three conditions (a), (b), (c) are measured using three different write voltages. (b) shows high-quality PUF having high entropy, however, it is difficult to tune this condition after assembled.

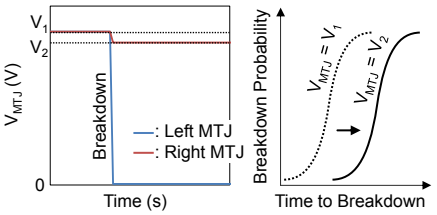

Fig. 6 Simulated stress voltage of MTJ. After breakdown of the one side, stress voltage to the other side decrease and lifetime becomes longer.

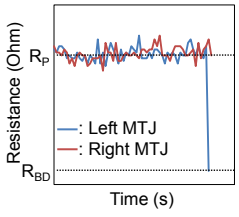

Fig. 10 Measured resistance change of the MTJ while applying stress voltage.

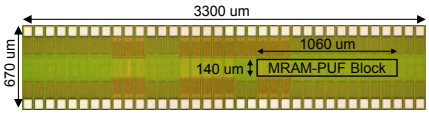

Fig. 8 Chip photograph.

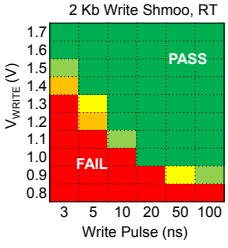

Fig. 9 Write shmoo plot measured in high- performance 2T-2MTJ cell memory array.

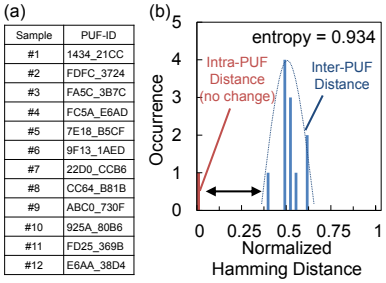

Fig. 11 (a) Measured 12 samples of 32 bit PUF-ID. (b) Hamming distance between sample #1 and the others.