ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.14, No.7, 1–6

An efficient stream cipher for resistive RAM

Joobeom Yun[1a)], **Ki-Woong Park**[1], **Youngjoo Shin**[2b)], **and Hee-Dong Kim**[3c)]

[1] *Department of Computer and Information Security, Sejong University, Neungdong-ro 209, Gwangjin-gu, Seoul 05006, South Korea*

[2] *Department of Computer Engineering, Kwangwoon University, Kwangwoon-ro 20, Nowon-gu, Seoul 01897, South Korea*

[3] *Department of Electrical Engineering, Sejong University, Neungdong-ro 209, Gwangjin-gu, Seoul 05006, South Korea*

a) *jbyun@sejong.ac.kr*

b) *yjshin@kw.ac.kr*

c) *khd0708@sejong.ac.kr*

Abstract: Resistive Random Access Memory (RRAM) is considered as one of the most competitive candidate for next-generation embedded system memories but data security for it has not yet been studied in detail. Since data security of embedded system is becoming more and more important nowadays, we think that it is necessary to study about data encryption for RRAM. In this paper, we studied data encryption candidates for RRAM and conducted several stream ciphers performance experiments for RRAM. As a consequence, we showed that Trivium is the most suitable stream cipher algorithm for RRAM. Also, we analyzed the experimental results.

Keywords: RRAM (resistive RAM), embedded system, Trivium, data encryption, stream cipher

Classification: Circuits and modules for storage

References

[1] S. Kim, *et al.*: "Tuning resistive switching parameters in Si_3N_4-based RRAM for three-dimensional vertical resistive memory applications," J. Alloys Compd. **663** (2016) 419 (DOI: 10.1016/j.jallcom.2015.10.142).

[2] Y. Fujisaki: "Overview of emerging semiconductor non-volatile memories," IEICE Electron. Express **9** (2012) 908 (DOI: 10.1587/elex.9.908).

[3] W. Kang, *et al.*: "Reconfigurable codesign of STT-MRAM under process variations in deeply scaled technology," IEEE Trans. Electron Devices **62** (2015) 1769 (DOI: 10.1109/TED.2015.2412960).

[4] G. Niu, *et al.*: "Material insights of HfO2-based integrated 1-transistor-1-resistor resistive random access memory devices processed by batch atomic layer deposition," Sci. Rep. **6** (2016) 28155 (DOI: 10.1038/srep28155).

[5] S. Hong, *et al.*: "Effect of work function difference between top and bottom electrodes on the resistive switching properties of SiN films," IEEE Electron Device Lett. **34** (2013) 1181 (DOI: 10.1109/LED.2013.2272631).

[6] S. Park, *et al.*: "Resistive switching characteristics of sol–gel based ZnO nanorods fabricated on flexible substrates," Phys. Status Solidi Rapid Res. Lett. **7** (2013) 493 (DOI: 10.1002/pssr.201307187).

DOI: 10.1587/elex.14.20170179
Received February 28, 2017
Accepted March 6, 2017
Publicized March 21, 2017
Copyedited April 10, 2017

[7] H.-D. Kim, *et al.*: "Stable bipolar resistive switching characteristics observed in 8 × 8 Pt/NiN$_x$/Ti/TiN crossbar array structures for resistive random access memories," J. Nanosci. Nanotechnol. **16** (2016) 10276 (DOI: 10.1166/jnn.2016.13143).
[8] H. W. Stallings: *Network Security Essentials: Applications and Standards* (Pearson, New Work, 2014) 5th ed. 59.
[9] C. De Canniere, *et al.*: *TRIVIUM Specifications*. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/001, 2005. http://www.ecrypt.eu.org/stream.
[10] M. Hell, *et al.*: "Grain-a stream cipher for constrained environments," Int. J. Wireless Mobile Comput. **2** (2007) 86 (DOI: 10.1504/IJWMC.2007.013798).
[11] S. Babbage, *et al.*: *The stream cipher Mickey-128*. http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey128_p3.pdf.
[12] N. J. AlFardan, *et al.*: "On the security of RC4 in TLS," USENIX Security 13 Proc. (2013) 305.
[13] C.-C. Lin, *et al.*: "Voltage-polarity-independent and high-speed resistive switching properties of V-doped SrZrO$_3$ thin films," IEEE Trans. Electron Devices **54** (2007) 3146 (DOI: 10.1109/TED.2007.908867).
[14] S. Banik, *et al.*: "A differential fault attack on the grain family of stream ciphers," CHES 2012. LNCS **7428** (2012) (DOI: 10.1007/978-3-642-33027-8_8).
[15] S. Banik, *et al.*: "A differential fault attack on MICKEY 2.0," CHES 2013. LNCS **8086** (2013) (DOI: 10.1007/978-3-642-40349-1_13).

1 Introduction

Recently, two-terminal based resistance random access memory (RRAM), phase change RRAM (PC-RAM), and spin-torque magnetoresistive RAM (ST-MRAM), based on resistive switching (RS) phenomena, have been widely investigated [1, 2, 3]. Among them, RRAM is considered as one of the most competitive candidates for next-generation nonvolatile memories, due to the simple structure, low power consumption, long retention nondestructive readout, good complementary metal oxide semiconductor (CMOS) compatibility and high density integration. Its basic structure is the combination of metal–insulator–metal (M–I–M) [4]. The insulators such as metal-nitride [5] and metal oxides [6] have been explored as RS materials for RRAM devices. However, the low endurance and device yield limit the practical applications of RRAM. Especially, to realize the high density of the RRAM devices, it is necessary to develop cross-bar array (CBA) based RRAM devices having stable RS characteristics through an improvement of reliability and devices yield by optimizing RS material. To overcome them, in our previous work [7], we have proposed 8 × 8 Pt/NiN$_x$/Ti/TiN CBA RRAM devices and successfully demonstrated a feasibility of being able to obtain reliable resistive switching properties, i.e., stable RS, small variation of operating voltage and current, long retention and good endurance, in this structure.

Since RRAM is high density integrated and low power consumption, it can be used in computers and embedded devices. Although RRAM is considered as one of the most competitive candidate for embedded system memories, data security for it has not yet been studied in detail. Because RRAM is high density integrated and has simple structure, fast and compact encryption module is needed. If it is used in

DOI: 10.1587/elex.14.20170179
Received February 28, 2017
Accepted March 6, 2017
Publicized March 21, 2017
Copyedited April 10, 2017

embedded devices, a stream cipher module is more suitable than a block cipher module in terms of speed and compactness. In this work, to protect RRAM data, we simulated the RRAM cells and the stream cipher modules for the RRAM. In order to find out the most suitable stream cipher module for RRAM, we compared several stream cipher performances. We considered four stream ciphers as data encryption modules for RRAM; they are RC4 which is a widely used stream cipher among several software stream ciphers and three well-known hardware stream ciphers. As a result, we will propose the most suitable stream cipher for RRAM and the RRAM data can be communicated securely by encrypted forms.

2 Stream ciphers for RRAM

2.1 Stream cipher

Fig. 1. Encryption and decryption examples of stream cipher [8]

Block ciphers process the input blocks one by one at a time and produce an output block for each input block. On the other hand, stream ciphers process the input elements continuously and produce an output element at a time as they goes along. Because stream ciphers tend to be small and fast, they are particularly relevant for applications with little computational resources, e.g., for cell phones or other small embedded devices. Furthermore, it is assumed that stream ciphers tended to encrypt more efficiently than block ciphers. Therefore, we think stream ciphers are more suitable for RRAM device than block ciphers.

Usually stream ciphers encrypt a plaintext one byte at a time, although stream ciphers may be designed to operate on one bit at a time. Fig. 1 shows the stream cipher operation. Key stream is calculated from input key and becomes a random value. Some algorithms use an initialization vector (IV) as the first input when key streams are changing owing to secure key creation. Thus, IV length is usually the same as key length. Stream cipher encryption module receives a plaintext stream and a key stream, does exclusive-OR (XOR) operation, and produces a ciphertext stream shown in Fig. 1. Decryption is the reverse. It receives a ciphertext and a key stream, and produces a plaintext stream. If the next key stream byte is 01101100 and the next plaintext byte is 11001100, then the resulting ciphertext byte is 10100000. Decryption also requires the same key stream.

2.2 Stream cipher module for RRAM

In order to find out the most suitable stream cipher for the RRAM, we chose stream cipher candidates first. We chose four stream cipher algorithms: these are RC4 [8], Trivium [9], Grain [10], and MICKEY [11]. RC4 is a famous software stream cipher algorithm. It had been widely used due to its simplicity and speed. The other three algorithms are well-known hardware stream cipher algorithms. Usually a hardware stream cipher shows better performance than a software stream cipher and

DOI: 10.1587/elex.14.20170179
Received February 28, 2017
Accepted March 6, 2017
Publicized March 21, 2017
Copyedited April 10, 2017

can be easily implemented in embedded device circuits. Trivium stream cipher is designed to be compact in constrained environments and fast in applications that requires a high throughput [9]. Grain is implemented with two shift registers; one with linear feedback and the second with nonlinear feedback. It has simple structure and can be implemented hardware-efficiently [10]. Mutual Irregular Clocking KEYstream generator (MICKEY) consists of two 100-bit shift registers, one linear and one nonlinear, each of which is irregularly clocked under control of the other. MICKEY can be implemented with a particularly small hardware footprint, making it a good candidate where low gate count or low power are the primary requirements [11].

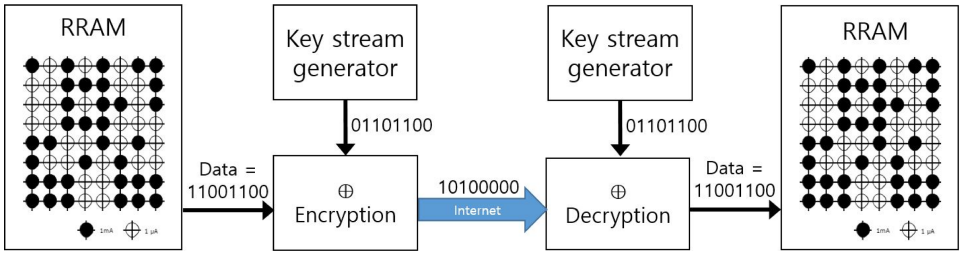

Fig. 2. RRAM and stream cipher modules for communication

Fig. 2 shows RRAM and a stream cipher diagram for communication. There is a RRAM having programmed data of bipolar resistive switching cells. When some data is transmitted from one device to the other device through insecure channel such as the Internet, the data should be encrypted because of security. The data in a RRAM is encrypted by a stream cipher module and is sent to the other device. The received data is decrypted by a stream cipher module with the same key stream. Key streams are generated by pseudorandom byte generator. As a consequence, the data in the sender's RRAM is transmitted securely to the receiver's RRAM.

3 Performance evaluation

In order to choose the most suitable stream cipher for the RRAM, we modeled and evaluated four stream cipher algorithms as described in 2.2 section. We measured performances of four stream cipher modules in this experiment. We simulated four stream cipher algorithms on a machine with a 2.7 GHz Intel® Core i5-6400 CPU and 2 GB RAM. Experiments were performed under Ubuntu Linux 2.6.10-5. We used GCC 4.0 to build binary executables. We repeated the experiment 300 times. And then, we analyzed RRAM read/write operation time and cipher module operation time.

First, we measured four stream cipher algorithm throughputs. We set key and IV length as 128 bits because, with current technology, this length is sufficiently long [8]. However, because RC4 algorithm doesn't use an IV, we marked it with 0-bit IV. Fig. 3(a) shows encryption speed of four algorithms. Trivium and RC4 show better throughput; RC4 shows 2810 Mbps on average and Trivium shows 3878 Mbps on average. The notation is *algorithm name(key, initialization vector (IV))*, both of key and IV are the number of bits. Secondly, we measured

DOI: 10.1587/elex.14.20170179
Received February 28, 2017
Accepted March 6, 2017
Publicized March 21, 2017
Copyedited April 10, 2017

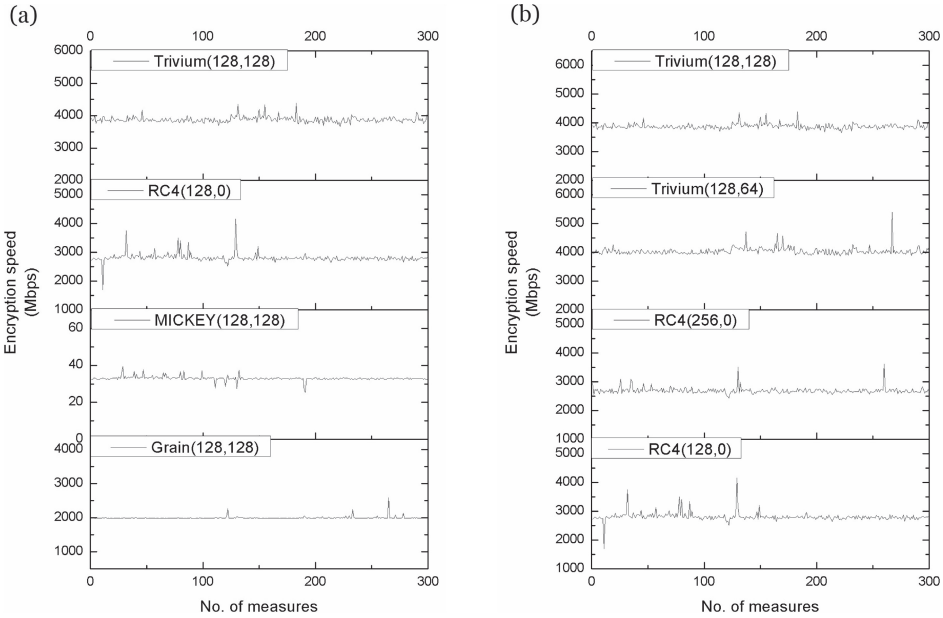

Fig. 3. (a) Encryption speed (Mbps) of four algorithms. The notation is *algorithm name(key, initialization vector (IV))*, both of key and IV are the number of bits. (b) Encryption speed (Mbps) by changing key and IV sizes.

encryption speed varying key and IV sizes. Fig. 3(b) shows this result. Shorter key size such as RC4(128, 0) shows better performance than longer key size such as RC4(256, 0). This means that longer key size takes more time but it is more secure than shorter key size because it takes more time during the cryptoanalysis with the longer key size. This is the same as initialization vector (IV). Shorter IV such Trivium(128, **64**) shows better performance than longer IV such as Trivium(128, **128**). Although longer key and IV have better security, performance is more important in a resource restricted environment, for example an embedded device. Meanwhile, MICKEY did not show good encryption speed, they show under 40 Mbps throughput.

From a security standpoint, we considered security concerns of four candidates. Although RC4 had been widely used so far, it is not used any more due to its multiple vulnerabilities [12]. It is known that Grain and MICKEY also have a vulnerability against the fault attack [14, 15]. However, valid Trivium's vulner-

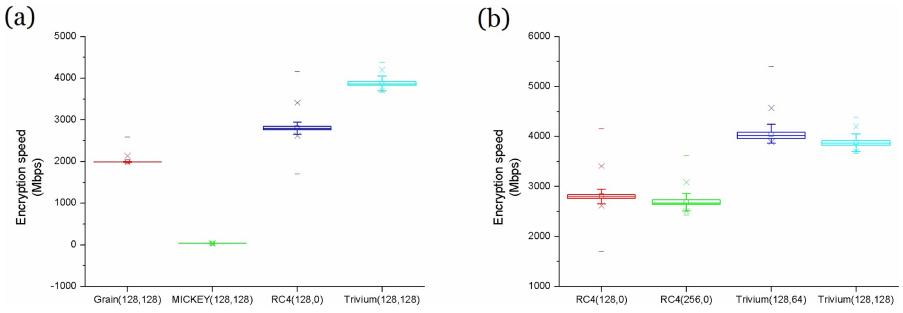

Fig. 4. (a) Encryption speed (Mbps) box chart of four algorithm. The notation is *algorithm name(key, initialization vector (IV))*, both of key and IV are the number of bits. (b) Encryption speed box chart by changing key and IV sizes.

DOI: 10.1587/elex.14.20170179
Received February 28, 2017
Accepted March 6, 2017
Publicized March 21, 2017
Copyedited April 10, 2017

ability has not been known until now. Thus, this is another reason that Trivium is the most suitable stream cipher for RRAM.

Fig. 4 shows box chart of the encryption speed. Trivium stream cipher shows the best performance. This is caused by its compact design and fastness in applications that requires a high throughput. In particular, the cipher's design is such that the basic throughput can be improved through parallelization (allowing computing 64 iterations at once), without much increase to the area required for its implementation. That feature allows the clock frequency to be divided by a factor 64 without affecting the throughput. As a consequence, Trivium has the best performance and the simplest structure among all the stream ciphers. In addition, it can be designed and fabricated on 0.18 µm CMOS. Thus, Trivium having high speed, the compact design, and security is the most suitable for our RRAM cipher module. According to [13], RRAM average read/write time is 10 ns and our experiments shows that Trivium cipher stream takes 0.4 ns on average. We think this overhead is reasonable in most cases.

4 Conclusion

Nowadays RRAM is used or can be used as an embedded system nonvolatile memory. In order to make embedded system more secure, stream cipher module is necessary. Compact and efficient stream cipher module is required for RRAM which have simple structure and high density integration. Therefore, we experimented stream ciphers performance in order to find out the most suitable stream cipher for RRAM. We showed that Trivium is the most suitable stream cipher for RRAM, due to the performance, the compact design, and security. And then, we showed that stream cipher module is not big overhead compared to its importance.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2015R1C1A1A02036511). Hee-Dong Kim and Youngjoo Shin are corresponding authors of this paper.

DOI: 10.1587/elex.14.20170179
Received February 28, 2017
Accepted March 6, 2017
Publicized March 21, 2017
Copyedited April 10, 2017