1. Andrzej BIEŃ[1], 2. Szymon BARCZENTEWICZ[1], 3. Tomasz FILIPÓW[2]

AGH Akademia Górniczo-Hutnicza (1), Diskus Polska (2)
ORCID: 1. 0000-0001-8635-1407; 2. 0000-0001-9409-2169

doi:10.15199/48.2024.07.33

Irreversible destruction of the content of Flash memory

***Abstract**. The paper presents a laboratory model of a novel device for irreversible destruction of Flash memory. In the paper a short literature review on the topic of Flash memory destruction was performed. A basic description of laboratory model was given. Results of tests for the functionality of the Flash destruction device were presented. Tests proved usefulness of proposed solution.*

***Streszczenie.** W artykule przedstawiono laboratoryjny model nowatorskiego urządzenia do nieodwracalnego niszczenia pamięci Flash. W artykule dokonano krótkiego przeglądu literatury na temat niszczenia pamięci Flash. Podano podstawowy opis modelu laboratoryjnego. Zaprezentowano wyniki badań funkcjonalności urządzenia niszczącego Flash. Testy wykazały przydatność zaproponowanego rozwiązania. (**Bezpowrotne zniszczenie zawartości pamięci typu Flash**)*

Keywords: Flash drive, data security, electromagnetic impulse, irreversible destruction of data.
Słowa kluczowe: pamięć Flash, bezpieczeństwo danych, impuls elektromagnetyczny, bezpowrotne niszczenie danych

Introduction

The need of irreversible destruction of data from memory storage devices arise mainly due to data security issues. Nowadays this data are personal, confidential professional or government data. As a rule a data storage device is irreversibly destroyed when their service life expires. The issue of irreversible data erasure has been effectively solved in the case of HDD drives by demagnetizing, fragmenting or chemically dissolving them. A separate issue is the destruction of data stored in Flash memory.

One of methods for Flash memory erasure is software based. There is a limited number of scientific publications concerning this topic. In [1], a method that involves overwriting the stored data is proposed. Authors in [1] suggest this solution because, during Flash memory erasure operations, there is a problem of data remaining in at least one unmapped memory block. Similar solutions can be found in [2] and [3]. In [4] the software solution not directly reliant on effectively encrypting data. Another approach involves the manufacturer's preparation of memory, such as incorporating circuits for destruction through a specific voltage impulse into their hardware. Patents [5] also describe the possibility of constructing an integrated circuit with the capability of rapidly erasing its contents, but such functionality is not provided by manufacturers of popular hardware. While all these methods yield positive results, they require specialized tools and knowledge. For data carriers with FLASH memories, instead of demagnetization, subjecting them to an electromagnetic impulse has been proposed. The outcomes of this method are described in the later part of the article. All of these methods produce positive results however, their require specialized tools and knowledge.

In this paper a simple method based on the electromagnetic impulse is presented.

Flash memory

Flash memory can be understood as a combination of EPROM and EEPROM technologies. They are currently used in almost every electronic device: from several kilobyte memories storing controller firmware, through memory cards, phone memories, to SSD drives. The greatest advantages of Flash memory are: high efficiency, low energy consumption, small size and weight, and high resistance to damage.

Flash memory was developed in Toshiba laboratories by Dr. Fujio Masuoka in the early 1980s [6]. The term "Flash" for this technology comes from the fact that a large part of the memory can be erased at one time. This functionality distinguishes this type of memory from EEPROM memory, where each byte of data must be erased individually. The principle of operation is based on storing information in MOSFET field-effect transistors.

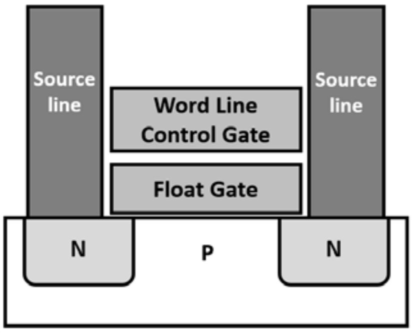

Fig.1. Cell of Flash memory [6].

A transistor consists of a source and a drain - N+ (P+) semiconductor separated by a P (N) semiconductor, over which an electrode - the gate - is placed. If the gate voltage is equal to the substrate voltage, meaning there is no electric field in the P-type (N-type) semiconductor, current will not flow from the source to the drain - the transistor is turned off. Applying voltage to the gate creates an electric field in the P-type (N-type) semiconductor, forming a region with the same type as the source and drain - the transistor is turned on. A transistor of this type only draws current during the state-switching moment. Figure 1 presents a scheme of a single cell of Flash memory.

Laboratory model

Figure 2 presents a laboratory model. Laboratory model consists of few basic elements. The most important are: capacitor for energy storage, active element which is a coil for field excitation and spark gap. The capacitor used is an Elektronikon 51.S35-513R20 with a capacitance of 51.25 uF and a rated voltage of 6,3 kV DC. Numerous variations of individual components were tested. The selection of the capacitor was guided by the choice of appropriate dynamic parameters. In the case of the excitation coil, it was crucial to select suitable electrical parameters, with a primary focus on choosing the appropriate materials (such as ferromagnetic cores).

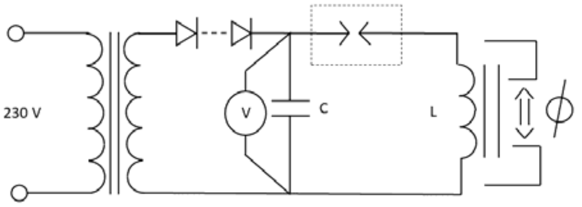

Fig.2. A device for destroying Flash memory (C-capacitor, an L-coil with a ferromagnetic core, and a sliding device for closing the circuit).

Figure 3 shows a picture of a laboratory model of a device for destroying Flash memory.

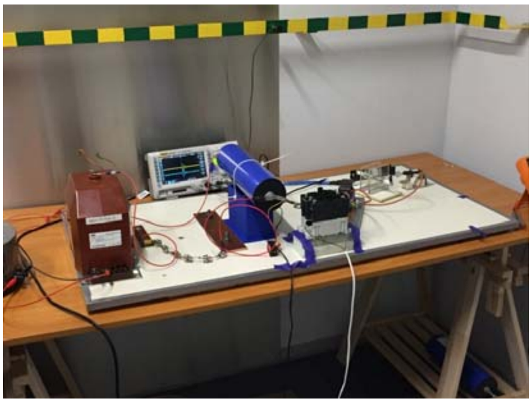

Fig.3. A picture of a laboratory model of a device for destroying Flash memory .

Verification of the model

Figure 4 depicts the shape of the induced waveform in the laboratory model's coil. The impulse generated in the coil has the character of a damped oscillatory waveform with a distinct pulse at the peaks of the oscillation.

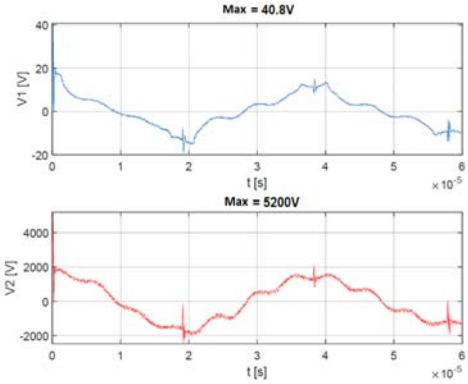

Fig.4. The shape of the induced waveform in the laboratory model's coil, where: V1 - induced voltage in the active element; V2 - voltage across the capacitor.

The primary device for verifying the operation of the laboratory model was the ruSolut Visual NAND Reconstructor (VNR). This device enables the recovery and digital examination of NAND Flash memory, commonly used in forensic investigations. The VNR kit includes a NAND memory reader, adapters for various memory types, and software. The reader can read the physical image of the memory through a specialized adapter and convert it to a supported file system. Analyzing individual memory blocks allows for the recovery of old or "erased" data [4]. The device supports multiple types of memory currently available on the market: Micron (2Ch), Toshiba (98h), Sandisk (45h), Hynix (ADh), Samsung (ECh).

The methodology for verifying the performance of the developed laboratory model involved creating an image of the memory both before and after subjecting it to the effects of the developed model. Figure 5 presents a comparison of 5000 bytes from one of the tested memories in the early stages of the work. The images before and after use of the model were subtracted from each other, and then the percentage difference between them was calculated. At this stage, a hundred percent effectiveness of the model has not yet been achieved.

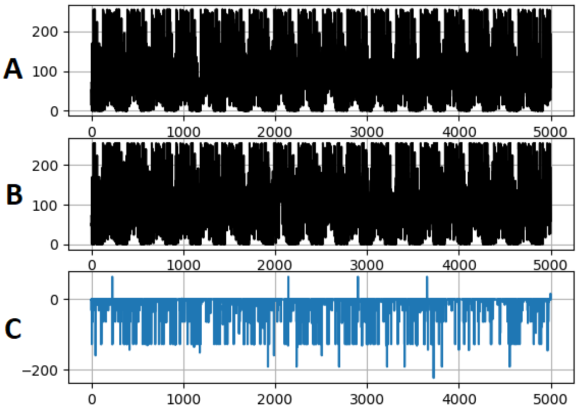

Fig.5. The difference in memory bytes before and after subjecting it to the operation of the developed laboratory model (A-before model use, B-after model use, C – B-A)

In the last stage of tests, the tested memories exposed to the model were not recognized by the memory reader. It was impossible to read the memory identifier and, consequently to recover data. From the point of view of the memory reader device, the model was 100% effective.

With the refinement of the laboratory model, an increasingly better effectiveness of its operation was achieved. To confirm the obtained results, a device for basic analysis of Flash memory was developed. A series of memories from various manufacturers were examined, and the results were validated. Memories subjected to the model's operation were not recognized by both readers, and their content could not be retrieved.

Another type of verification were tests using X-ray based analysis. Figure 6 shows the memory. In the lower part, faintly outlined wire connections between the chip and the lattice are visible. Figure 7 shows a bottom view in an isometric projection with clearly visible wire connections between the chip and the lattice. In addition to a large number of long connections, there are also two pairs of short connections constituting a short circuit between the fields.

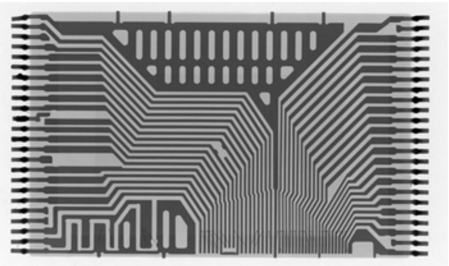

Fig.6. Device for verification of the developed laboratory model

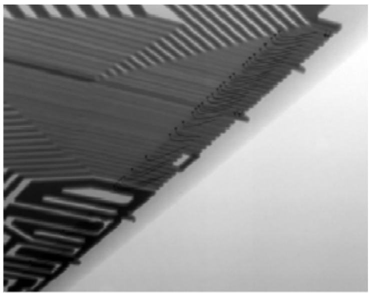

Fig.7. Bottom view photo showing the majority of wire connections between the chip and lattice.

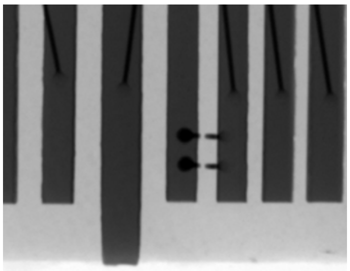

Fig.8. Discontinuous short connection between adjacent fields.

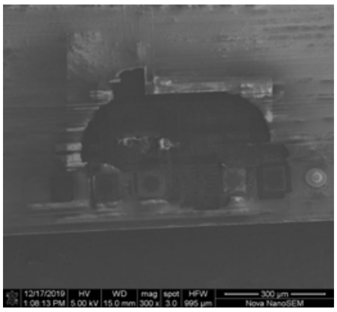

Fig.9. Discontinuous short connection between adjacent fields.

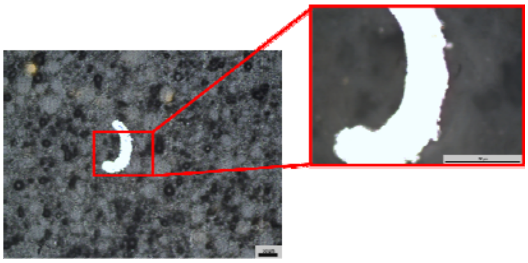

Fig.10 Image of catastrophic Flash memory damage.

The broken bonds correspond to the first and third pins in the upper right corner of the image in Figure 8. It is unclear when these bonds were broken. It is possible that this is an intentional process related to production or is a result of the operation of the developed laboratory model. This does not completely disqualify the memory's functionality, as both fields are accessible externally and can be bridged there.

To find the hardware based proof of successfully destroyed memory additional test using scanning electrode microscope were performed. Figure 9 shows that using SEM macroscopic image delamination extending into deeper technological layers with dimensions on the order of several hundred micrometers can be observed.

The last method of hardware verification of the model was based on the tests using microscopic imaging of the tested memory after previous mechanical wear of the memory. Figure 10 shows a catastrophic memory damage.

Conclusions

In this work a device for irreversible Flash memory destruction was presented. Effectiveness of the developed laboratory model of the Flash memory destruction device was confirmed using specialized data recovery equipment.

In the final stage, memory units subjected to the model's operation, when inserted into the VNR reader, were not recognized by the device. The memory identifier could not be read, consequently rendering it impossible to generate its image. From the VNR device perspective, a one hundred percent effectiveness of the model's operation was achieved.

***Authors**: dr hab. inż.* ***Andrzej Bień**, Akademia Górniczo-Hutnicza w Krakowie, Katedra Energoelektroniki i Automatyki Systemów Przetwarzania Energii, al. Mickiewicza 30, 30-059 Kraków , E-mail: abien@agh.edu.pl;*
dr inż. ***Szymon Barczentewicz**, Akademia Górniczo-Hutnicza w Krakowie, Katedra Energoelektroniki i Automatyki Systemów Przetwarzania Energii, al. Mickiewicza 30, 30-059 Kraków , E-mail: barczent@agh.edu.pl;*
mgr inż. ***Tomasz Filipów**, Diskus Polska, Kościuszki 1, 32-020 Wieliczka, E-mail: tomasz.filipow@diskus.pl*

REFERENCES

[1] N.-Y. Ahn and D. H. Lee, "Schemes for Privacy Data Destruction in a NAND Flash Memory," in IEEE Access, vol. 7, pp. 181305-181313, 2019, doi: 10.1109/ACCESS. 2019.2958628.
[2] R. Zhu, Y. Wang, P. Bai, Z. Liang, W. Wu and L. Tang, "CPSD: A data security deletion algorithm based on copyback command," 2022 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), 2022, pp. 1036-1041, doi: 10.1109/ICAICA54878.2022.9844604.
[3] K. Sun, J. Choi, D. Lee and S. H. Noh, "Secure Deletion of Confidential Data in Consumer Electronics," 2008 Digest of Technical Papers - International Conference on Consumer Electronics, 2008, pp. 1-2, doi: 10.1109/ICCE.2008.4588029.
[4] M. Wang, J. Xiong, R. Ma, Q. Li and B. Jin, "A Novel Data Secure Deletion Scheme for Mobile Devices," 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1-8, doi: 10.1109/ICCCN.2018.8487366.
[5] US9818486B2; Fast secure erase in a flash system, US 2014
[6] Semiconductor memory device and method for manufacturing the same. US Patent 4531203 A. November 13, 1981. Retrieved March 20, 2017.