View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Apollo

Direct charge measurement in Floating Gate transistors of Flash EEPROM using Scanning Electron Microscopy

Franck Courbon, Sergei Skorobogatov
Computer Laboratory, University of Cambridge, Cambridge, United Kingdom

Christopher Woods
Quo Vadis Lab, London, United Kingdom

Abstract

We present a characterization methodology for fast direct measurement of the charge accumulated on Floating Gate (FG) transistors of Flash EEPROM cells. Using a Scanning Electron Microscope (SEM) in Passive Voltage Contrast (PVC) mode we were able to distinguish between '0' and '1' bit values stored in each memory cell. Moreover, it was possible to characterize the remaining charge on the FG; thus making this technique valuable for Failure Analysis applications for data retention measurements in Flash EEPROM. The technique is at least two orders of magnitude faster than state-of-the-art Scanning Probe Microscopy (SPM) methods. Only a relatively simple backside sample preparation is necessary for accessing the FG of memory transistors. The technique presented was successfully implemented on a 0.35 µm technology node microcontroller and a 0.21 µm smart card integrated circuit. We also show the ease of such technique to cover all cells of a memory (using intrinsic features of SEM) and to automate memory cells characterization using standard image processing technique.

Keywords: Flash EEPROM, Reverse engineering, Scanning Electron Microscope (SEM), Passive Voltage Contrast (PVC), Image processing

Introduction

Embedded systems rely heavily on non-volatile memory (ROM, EEPROM, and Flash) to store code and data. There is a constantly growing demand for the confidentiality of the information stored in embedded devices for Intellectual Property (IP) protection and sensitive data such as passwords and cryptographic keys.

Amongst non-volatile memories many investigations have shown the weaknesses of Mask ROM (factory programmable) against adversaries. A Mask ROM cell consists of a single transistor and some types of Mask ROM memory can be easily observed even under an optical microscope if the information is encoded in the contact layer, metal layer or diffusion layer. It was possible to read even the most secure type of Mask ROM with an ion-implanted doping encoding under a microscope after selective dash etching. In 1999, Kommerling and Kuhn [1] showed how to extract ROM contents using standard Failure Analysis techniques. Since then Mask ROMs have not been considered to be secure unless encrypted or at least obfuscated.

This paper focuses on Flash EEPROM and there are many types of them. Originally EEPROM was referred to as a two-transistor electrically re-programmable cell, while Flash was introduced later and had a single transistor (Figures 1, 2) [2]. These days both structures are usually referred to as a Flash memory. Each semiconductor manufacturer has many different designs with a unique layout for Flash memory cells. But they all have something in common – the information is stored in a form of electric charge inside the memory transistor. The actual number of electrons varies from 10^5 in old technologies to less than 10^3 in modern chips. These electrons shift the threshold voltage of the memory transistor and this is then detected by a readout circuit. The electrons are placed into a memory transistor by applying high voltages to the memory transistor employing either one of two mechanisms: Fowler-Nordheim tunneling or Channel Hot Electron (CHE) injection (Figures 1, 2). In order to erase the cell another combination of high voltages is applied which force the electrons to tunnel through a very thin oxide barrier. The oxide is slowly damaged during program-erase cycles, which result in the limited number of programming cycles – usually between 100 and 10^6.

Flash EEPROM is widely used as a protection against Reverse Engineering because conventional de-processing methods only reveal the transistor structure and not its state. Flash EEPROM is a memory type present in devices where security leaks would lead to different societal and financial consequences. The '0s' and '1s' are a matter of presence or absence of electron charges within the floating gate. The capability to retrieve Flash EEPROM memory contents in a practical and fast way has never yet been published.

However, some key micro-electronics manufacturers, such as Sharp in 2005 [3], Cypress in 2008 [4], Virage Logic in 2009 [5] and Synopsys in 2011 [6] noted the security threat relating to the possibility of memory extraction using SEM. Plus, IBM [7] also disclosed at CHES 2000 the following: “The electron beam of a conventional scanning electron microscope can be used to read, and possibly write, individual bits in an EPROM, EEPROM, or RAM.” However, there are no publications which substantiate this as yet. Several publications exist which refer to Atomic Force Microscopy (AFM) techniques being used to highlight differences between '0' and '1' in Flash

EEPROM. For instance, the use of a current applied on a conductive tip allows seeing some interaction whenever electron charges are present within memory cells. Following Skorobogatov's conclusions [8], the first investigations using SPM-based techniques have been performed by De Nardi *et al.* [9,10] and, recently, similarly performed again by different teams Konopinski *et al.* [11], Hanzii *et al.* [12] and Dhar *et al.* [13,14].

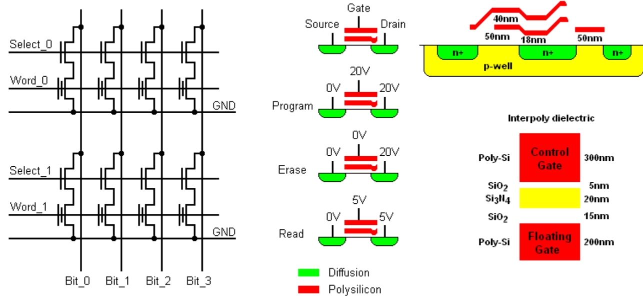

Figure 1: Structure and operation of 2T Flash EEPROM

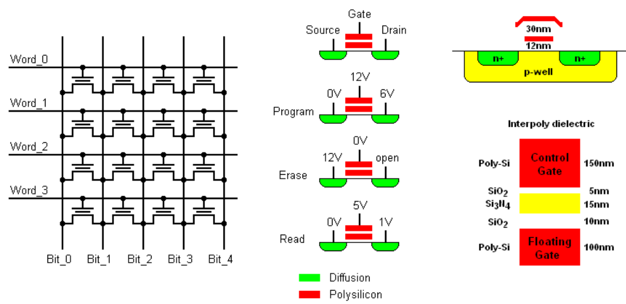

Figure 2: Structure and operation of 1T Flash EEPROM

Due to SPM system limitations, only slow and reduced area Flash EEPROM charge measurements are documented to date. The main drawbacks of SPM techniques are the low scanning speed (approximately 10 minutes per 20×20 µm image), the small area covered (approximately 100×100 µm), the need to replace the tip (as it becomes unusable after days of continuous scanning) and the necessity of operator interventions (moving to the scanning area). This results in an impractical technique of characterizing a complete memory of several mm^2.

To satisfy the large number of transistors in integrated circuits, recent investigations have shown the advantages of using SEM in the security community. Courbon *et al.* [15] showed the capability in practice of accessing a transistor's active region with the help of an easy, fast and low-cost front-side sample preparation, based on wet etching. They use standard SEM imagery and image processing techniques to observe and process different shapes present in chips' synthesized logic. Sugawara *et al.* [16] prepare their sample at the contact layer before using a SEM. They are able to distinguish the different p/n junctions and conclude on the underlying dopant profile.

This current paper also deals with Scanning Electron Microscopy for a different need, reverse engineering Flash EEPROM memory contents commonly thought unreachable.

Background and proposed technique

The electrons accumulated in the floating gate are representative of a '0' or a '1' bit value depending on the memory manufacturer's convention. The proposed technique deals with accessing the floating gate transistors, probing in situ electrons. Since decades, Voltage Contrast has been used under SEM microscopes [18], ie for detecting shorts or open contacts in integrated circuits [19]. In this case, the change in contrast comes from the non-connection to the ground for a conductor. The secondary electrons signal resulting from an incident beam/matter interaction is dependent on several parameters such as the primary beam features, the sample's atomic number, the nature of the area scanned, the doping level. We validate that it is also possible to image local charges trapped in an oxide using SEM in PVC mode. SEM allows the imaging of a sample using an electron beam and PVC imaging corresponds to the voltage contrast setup where no external bias is applied to the sample. Secondary electrons in-lens detectors (also known as TLD: Through-the-Lens Detector) are particularly adapted to observe surface potential rather than observing topography [20] due to collection efficiency.. No work relating to the characterization of integrated circuit embedded memory using a SEM in PVC mode has been published to date. The goal is to be able to characterize memory cells in a fast and efficient way. This could have many applications in Failure and Forensic Analysis by helping to measure the precise charge inside memory transistors; especially in cases when the device was electrically or physically damaged thus preventing conventional access paths.

Step	*Task*	*Goal*	*Overview*
Sample preparation	Polishing, lapping, wet etching	Successively remove Si down to $20\mu m$, get a mirror aspect and then remove remaining substrate by wet etching	
Image acquisition	Move to & define area of interest, apply SEM parameters, load acquisition macro	Set best SEM parameters for charge differenciation and perform automated large scan	
Image processing	Multiple image registration, contrast enhancement (if necessary), image segmentation	Gather individual images to cover all memory, '0s' and '1s' bit value extraction	F101112131415161718191A1B1C1D1E1FE4 F303132333435363738393A3B3C3D3E3FC4 F505152535455565758595A5B5C5D5E5FA4 F707172737475767778797A7B7C7D7E7F84 F909192939495969798999A9B9C9D9E9F64

Table 1: Proposed technique global flow

We propose the technique outlined in Table 1, which combines backside sample preparation, SEM acquisition and image processing. For our dedicated application the image acquisition step is based on three principles: having sufficient spatial resolution to distinguish memory states, not creating a conductive path between the control gate and the floating gate, limiting charge-up effects inherent to the use of an electron beam over a dielectric. Several fine-tuned parameters therefore have to be used. Sample preparation is crucial too as all silicon

is removed down to the tunnel oxide while leaving the charge blocking layer intact over a large area.

We acknowledge that neither the sample preparation nor the fine-tuned SEM nor the image processing techniques are new but their combination results in a fast and effective approach for characterizing Flash EEPROM and its practical implementation is about 250 times faster than AFM based technique state of the art. Also, Scanning Electron Microscopes are wide- spread in companies, organizations and universities, renting one is open to everyone and costs less than a $100 per hour.

Sample preparation

Devices Under Test

We applied our methodology on the Atmel ATmega32U4 microcontroller [21] and the Inside Secure AT90SCxx ROM/EEPROM smart-card [22]. The microcontroller was fabricated with a 0.35 µm CMOS process with 3 metal layers, while the smartcard chip is 0.21 µm CMOS with 6 metal layers. Using a universal programmer we programmed a set of identical ATmega32U4 samples with a specific pattern to ensure that charge differences would be noticeable no matter what the physical layout of the memory. However, due to the higher security of the smartcard we were unable to program arbitrary data; still, some regions were readable, so that at least we knew the data structure.

Accessing the area of interest

The PVC technique requires access to the region of interest, i.e. the floating gate of the memory transistor. Two approaches are currently documented regarding accessing floating gate transistors (for AFM measurement techniques application): either frontside with delayering down to the inter-poly dielectric layer or backside down to the tunnel oxide layer. Due to the charge nature, high energetic solutions cannot be used (plasma etching or a high temperature approach). Moreover, the surface roughness needs to be even over a large surface. Thus, as in previous successful sample preparation experiments reported in several publications, we use a backside approach where most of the silicon substrate is removed using mechanical polishing before a selective wet etching is used to remove the remaining Silicon thickness, without affecting the floating gates tunnel oxides.

Parallel lapping

The samples were prepared using a simple polishing/lapping machine with devices mounted on a sample holding jig to assist precise thickness control and parallel lapping surface. The cost of this machine, shown in Table 1, is about 6000 $. As we are using a backside approach, we first encounter and remove a copper heatsink with the mechanical grinding tool. Once removed, we use successively hard diamond discs to remove silicon down to a 100 µm thickness. Then we use high grit abrasive discs to slowly reduce the thickness down to 20±5 µm. Then, using polishing paste, we remove scratches and obtain a mirror polish aspect with a fairly constant roughness. The results of the different stages of the silicon removal process are shown in Figure 3.

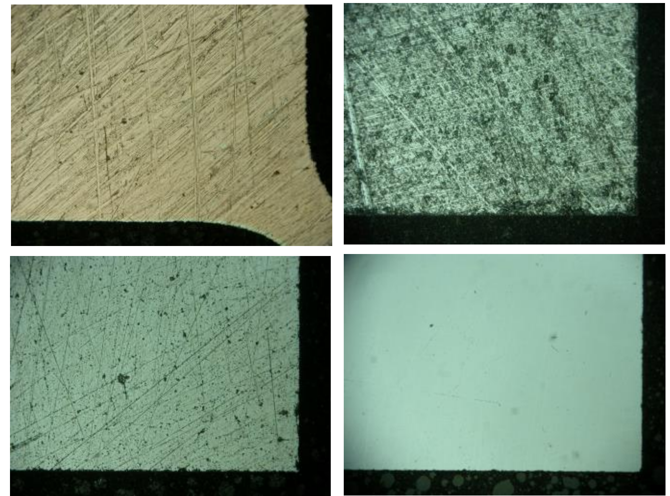

Figure 3: Successive silicon removal process down to: a) Copper heatsink; b) 100µm Si; c) 20µm Si; d) polished

Wet etching

Once the 20±5 µm thickness is obtained, we use wet chemical etching to access the floating gate transistor's tunnel oxide. We use the same approach as the one developed by Korchnoy [17] and re-used in various AFM works [11]. We use Choline Hydroxide to remove the remaining substrate without damaging the thin tunnel oxide of 10 nm. The solution was heated to 90ºC to increase the etching process speed while keeping a sufficient Si/SiO_2 selectivity ratio of about 5000. The result of the selective silicon etching is presented in Figure 4.

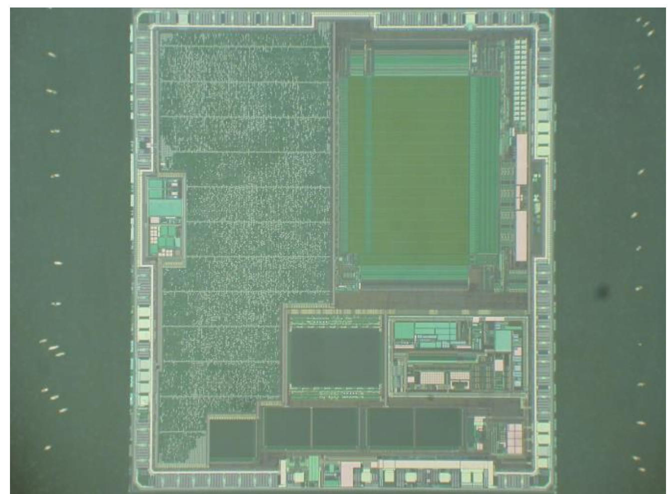

Figure 4: Sample after selective chemical etching

Image acquisition

Using SEM to characterize trapped charge

Parameters were chosen in accordance with PVC state-of-the-art approaches. Once integrated circuits prepared, we used a SEM microscope with both Field and InLens detectors available. No success was achieved with standard secondary electrons detectors. Therefore, we selected the InLens detector and used a small working distance of 2 to 5 mm to maximise secondary electrons collection. A low accelerating voltage of 1 kV to 3 kV was used, as charge-up is limited by taking an energy close to the characterization energy of SiO_2.. The penetration depth of such a beam will not create a conductive path between floating and control gates which lead to data vanishing. A strong probe current degrades the signal to noise ratio, spatial and voltage resolution. We try to use a small diaphragm aperture to limit the probe current value. We limit the number of incident electrons using a low magnification. The chosen magnification (1 to 5 kX) needs to permit sufficient pixels to characterize each memory cell though. With regard to pixels, the chosen spatial resolution in our experiments was 1024x768, it affects the scanning time (and therefore the time spent on a memory point). We also limit the number of incident electrons by using a scanning speed as fast as tens ms per frame. At such a fast scanning speed the noise becomes an issue, therefore, we integrated over multiple acquisitions to achieve the final, high quality image.

Atmega32U4 content extraction

Sample preparation

Figure 5 is an optical image of the Flash EEPROM memory array, it shows a uniform sample preparation over the full memory array thanks to our setup.

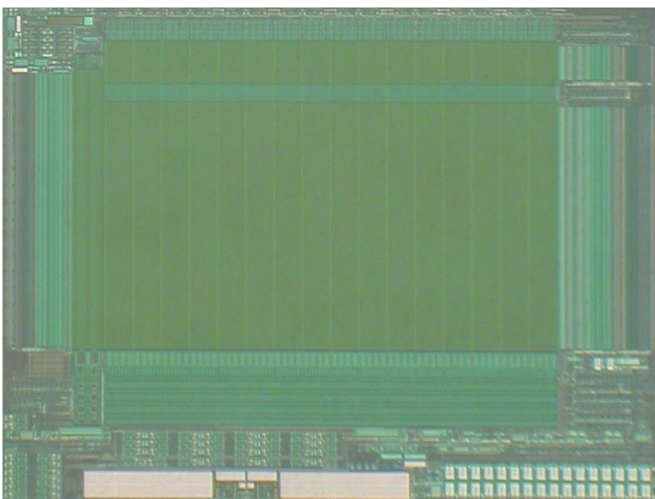

Figure 5: Optical image of memory array in ATmega32U4

Figure 6 shows a SEM image of four Flash EEPROM memory cells rows each containing 8 bits of information. One can distinguish the different properties of each memory cell (2-T design, drain contacts, tunnel oxide, word lines and a source line in the middle of Figure 6).

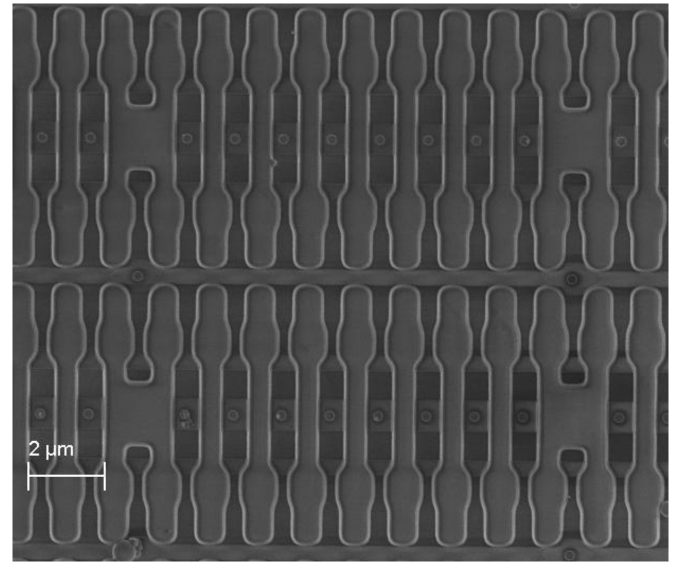

Figure 6: SEM image of the memory array in ATmega32U4

Results

Depending on the capabilities of a particular SEM there are a certain number of parameters which can be adjusted, apart from the accelerating voltage and magnification. Aperture size, scanning speed, dwelling time and spot size are those affecting the PVC quality. However, we were not able to achieve a good image quality with large apertures. Working distance was set to 3.3 mm. When using the minimal dwelling time of 50 ns (time on a pixel) we had to increase the probe current to improve the signal-to-noise ratio. Although that permitted a fair image quality, we were only able to integrate over 8 frames before the difference between cells programmed to '0' and '1' disappeared completely. The best image contrast was achieved at 2.5 kV with the estimated probe current of approximately 75 pA. This resulted in a very noisy picture presented in Figure 7.

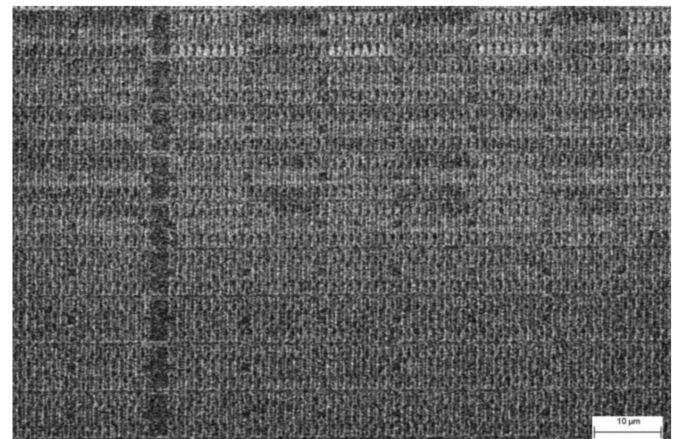

Figure 7: Extracting memory contents at 2.5 kV with 75 pA probe current, images integrated over 8 frames

We continued working on improving the image quality and found that at lower probe currents the charge was staying longer thus permitting larger number of frames to be scanned. As a result we were able to integrate over tens of frames, thus significantly reducing the noise. Figure 8 shows the result of such an acquisition at the highest scanning speed at 2 kV with 15 pA probe current at a larger working distance of 5.3 mm.

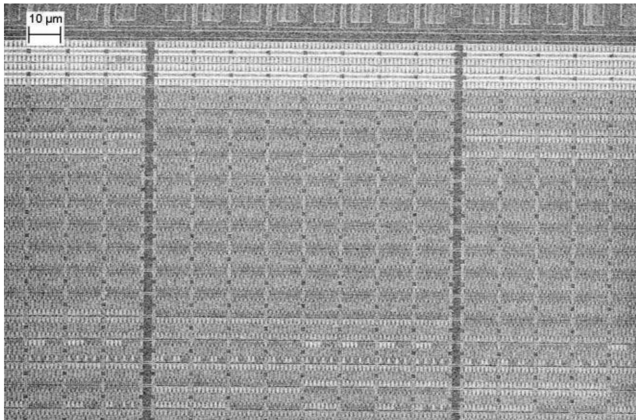

Figure 8: Extracting memory contents at 2kV with 15pA probe current, images integrated over 50 frames

The best image quality and contrast was achieved for the same working distance of 5.3 mm at 2.5 kV – a compromise between the best contrast and a reasonable number of frames we can acquire before the charge disappears from the floating gate of the memory transistors. The probe current was about 20 pA with these settings. All those parameters allowed us to obtain clear differences between '0' and '1' states as seen in Figure 9. It has to be noted that all images were obtained without additional image processing to highlight differences between '0' and '1' states. From the programmed test data we worked out that '0' state of a programmed cell corresponds to the darker memory cell, while '1' state of an erased cell corresponds to the brighter cell**.** After several acquisitions with such parameters, all cells become dark. It is possible to control the process of "injecting and removing charge" by adjusting the accelerating voltage and probe current. Also, one can notice a bright surface if a high density electron beam interacts with the sample.

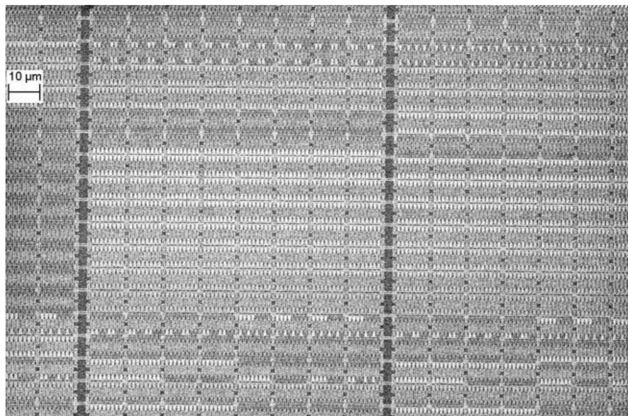

Figure 9: Extracting memory contents at 2.5kV with 20pA probe current, images integrated over 50 frames

Over Figure 9, we note 40 lines of information each containing 16 bytes (128 bits). It results in 640 bytes per acquisition. In terms of time, we require approximately 9.5 seconds to achieve this image (factor of scanning speed, and noise reduction setup). Thus, the final acquisition throughput is approximately 67 bytes per second, or approximately 4 kilobytes per minute.

Figure 10 outlines the characterization information that can be extracted. Some memory cells look brighter than the others. This is likely to be caused by the difference in the trapped charge on the floating gates of the memory cells. For chip manufacturers this could present a valuable tool to map the actual charge trapped inside each memory transistor for Failure Analysis purposes.

Figure 10: Zoom into SEM image for characterization

Blocked or passing transistors states (convention '0' and '1' for this ATMEL sample) can be clearly distinguished as the dark (holes, positive charge) and the bright (electrons, negative charge) areas respectively. The intermediary contrast seen at the word line is confirmed by the theory. Indeed, unlike 1T cell, the theoretical 2T cell contrast difference between programmed and erased are equal to twice the charge (as a 1T depleted cell has a null charge).

From the test pattern that was programmed into samples we also figured out the physical layout of the memory. The array was split into 16 blocks each representing one bit of data from the bit0 being the most right one to the bit15 located on the left. The addresses were going sequentially from right to left and each upper line had its corresponding address 128 bytes higher. Taking the example of the device under test, the complete memory content extraction (32 kbytes) would take approximately 8 minutes of SEM acquisitions (less than 10 minutes including a 10 per cent image overlap).

AT90SCxx content extraction

We then validate the PVC reading technique over a second sample, which uses a more recent technology node (0.21 µm vs 0.35 µm). The idea is to see how far the technique could work, despite the smaller number of electrons to be probed.

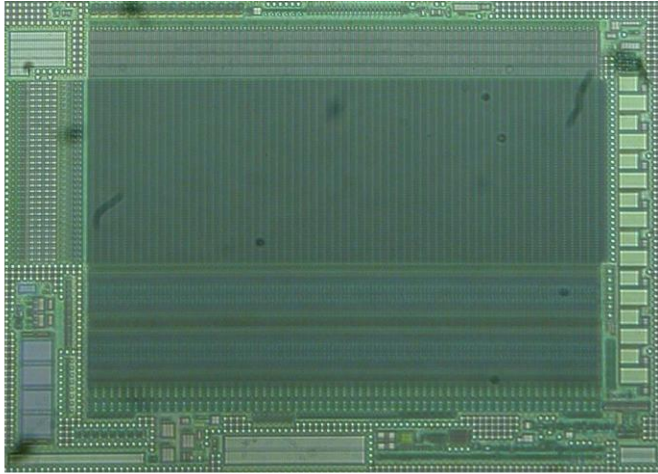

Figure 11: Optical image of memory array in AT90SCxx

Sample preparation

Figure 11 is an optical image of the AT90SCxx Flash EEPROM memory array. The sample preparation step remains identical as we use a backside sample preparation and therefore we are independent of the number of metal layers.

Figure 12 shows a SEM image of three Flash EEPROM memory cells columns each containing 2 times of 8 bits of information.

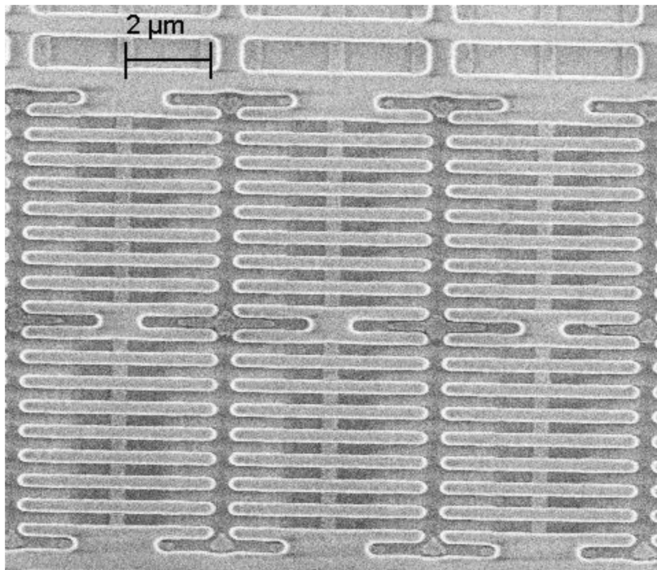

Figure 12: SEM image of the memory array in AT90SCxx

SEM imaging with PVC

The same imaging setting as we used for the microcontroller were initially applied. However, as technology nodes decrease, we had to increase the magnification to have sufficient pixels for characterizing each memory cell. We also decreased the working distance to maximize the number of secondary electrons detected.

Results

Figure 13 is a SEM acquisition showing the differences between '0s' and '1s'. Some contrast enhancement has been performed after acquisition to improve the visibility of the difference between programmed and erased memory cells. Also, due to the higher magnification and smaller cell size it was only possible to integrate over maximum of 40 frames at 2.5 kV accelerating voltage and 20 pA probe current, even at a shorter working distance of 3.0 mm. Beyond that point all memory cells look alike. One of the reasons for that is because incident electron beam density is important.

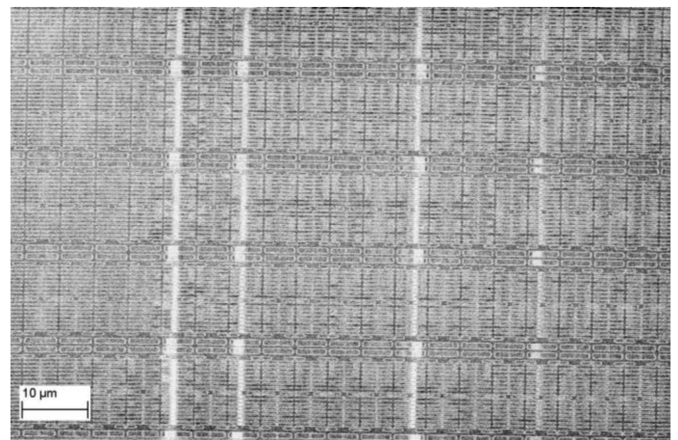

Figure 13: Extracting memory contents at 2.5kV with 20pA probe current, images integrated over 40 frames

On the zoom presented in Figure 14, '0' and '1' states can be distinguished as the bright and the dark areas respectively. Each column represents 8 bit of information from bit7 at the top to bit0 at the bottom. The addresses were going sequentially from left to right and each lower line had its corresponding address 128 bytes higher. The PVC mode in SEM is thus also implemented with success over this 0.21 µm technology node integrated circuit.

Figure 14: Zoom into SEM image for characterization

Complete memory application

The methodology being validated over both previous samples, we then demonstrate the capability to make operator free large scans using intrinsic properties of Scanning Electron Microscopy. The area to characterize, ie the full memory, is set as region of interest thanks to a graphical user interface. We keep the previous set of SEM parameters. Depending on the defined magnification and the size of the memory, a certain amount of images to acquire are indicated. The user can also define an overlap permitting to ease the alignment of individual images covering the entire memory, Figure 15.

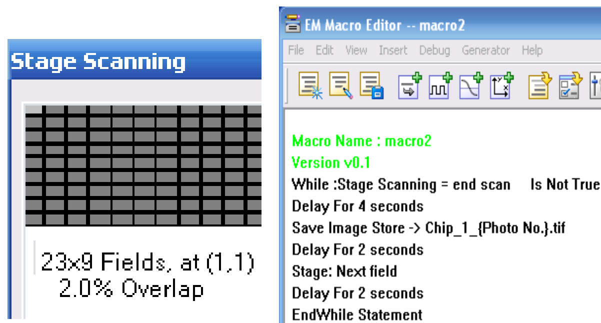

Figure 15: Left: defining area, right: editing macro

Images are thus all saved and the use of SEM is over. Offline, a multiple image alignment can be performed using open source software or standard matlab commands based on phase transform algorithm. In Figure 16, we give such example over two successive acquisitions. No artefacts are obtained, and the image alignment process only requires less than a minute for a complete memory.

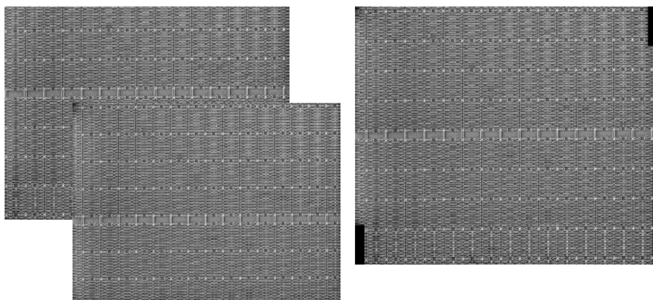

Figure 16: Left: First and second acquisition, right: final 1st and 2nd acquisition alignment

Trapped charge characterization

We have demonstrated how to distinguish intensities variations and to do so over a large area. The next step is to automate the processing of such information. A Failure Analysis engineer can observe multiple information and multiple paths can be taken to outline it. We detail here how such technique could be applied to detect a non-functional memory cell or a memory cell lacking electrons (reducing its lifetime). It could be expressed by a grayscale intensity value much smaller than the intensity values of functional cells. In Figure 17, we extract a 64 bits profile line from the acquisition already seen in Figure 10.

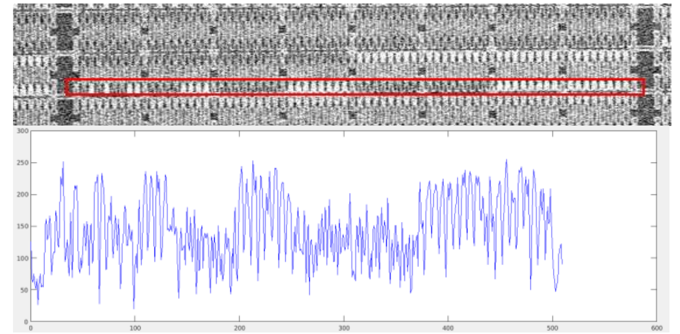

Figure 17: Top: subpart of Figure 10 raw SEM image, bottom: line profile of 64 bits of information

Using grayscale intensities only, Figure 17 does not permit to segment cells. We then go through successive basic image processing steps. Figure 18 shows the same memory location after the use of multiple basic image processing techniques such as histogram equalization and image filtering. Over this figure one can begin to observe a profile line giving more differences between '0s' and '1s'.

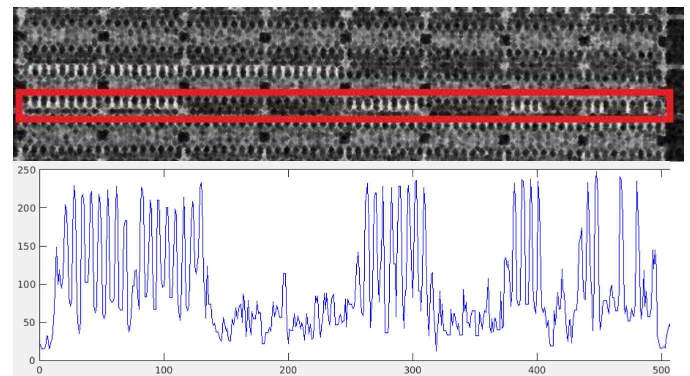

Figure 18: Top: subpart of Figure 10 SEM image after processing, bottom: line profile

We then select an intensity threshold value to characterize memory cells to say if they are uncharged or not. If cells appear black under the microscope and should be at '1' in this memory then those cells present a failure. Figure 19 directly gives the binary pattern: '01010011000011110000000011111-1100000000000000001111111111111111' and working this way allows a direct correlation with the input data file.

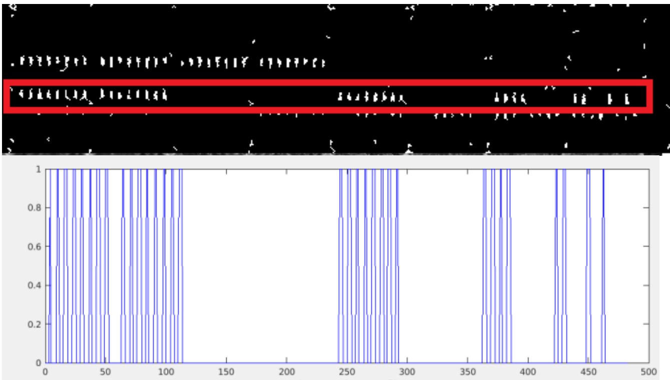

Figure 19: Top: subpart of Figure 10 SEM image after processing and thresholding, bottom: line profile

One can also imagine applying this technique after a certain number of write operations. If some cells do not appear bright, then those can be considered as cells with data retention problem. It can be an input for the failure analysis operator before applying a corrective action to the problem. One can also think about processing points that are along the memory grids made of repetitive rows and columns. The overall success of the methodology is matter of the sample preparation but also of the capability to do not have SEM acquisitions artefacts (such as in Figure 13). Applying image processing could then be possible and of interest in order to quantify the charge level (and indirectly the number of electrons stored).

Further work

It would be interesting to challenge the technique where fewer electrons are stored in Flash EEPROM floating-gate transistors. The applicability of the technique for smaller technology nodes is seen as possible given that improvements and optimizations ways are multiple. They could involve, for example, improving the SEM contrast by adding coatings, improve the data acquisition by having different parameters such as the sample orientation or also process images after acquisition. We will also try to extract the whole memory contents to estimate the error rate and practicality of this technique. Despite an already low magnification chosen in our investigations, Figure 20 shows that it is even possible to get information at a 218 times magnification. It definitely highlights that this dedicated application is open to several improvements.

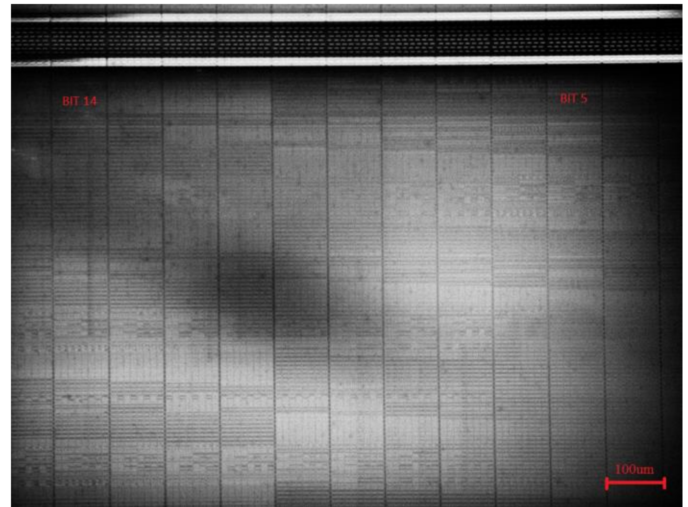

Figure 20: A lot of parameters to optimize, here we can differentiate 0s and 1s despite a large field of view

Conclusions

We introduce the first publication detailing Flash EEPROM direct charge measurements using a Scanning Electron Microscope. Using backside sample preparation and Passive Voltage Contrast techniques we successfully extracted memory contents at an imaging throughput of 4 kbytes per minute. It beats current state of the art memory content extraction by a factor of approximately 250. The technique requires a polishing tool, wet etching acid and few hours Scanning Electron Microscope renting. To conclude, the proposed methodology represents an optimization of Failure Analysis techniques but also a threat for security related concerns.

We were not only able to distinguish between memory cells programmed with a '0' and '1' state, but were also able to see the difference in the trapped charge on the Floating Gates of memory cells. For chip manufacturers this could present a valuable tool to map the actual charge trapped inside each memory transistor for Failure Analysis purposes. This could help in addressing the issues with data retention time, radiation hardness testing and data remanence effects in Flash EEPROM memory devices. It could also be useful for Forensic Analysis applications when the contents of the embedded memory needs to be extracted from devices which were electrically or physically damaged as a result of an accident or a deliberate attempt to remove data.

References

[1] O. Kommerling and M. Kuhn: Design principles for tamper-resistant smartcard processors, 1st worskop on Smartcard Technologies, 1999

[2] W. Brown, J. Brewer, Nonvolatile Semiconductor Memory Technology: A Comprehensive Guide to Understanding and Using NVSM Devices, IEEE Press, 1997.

[3] G. Smith: Addressing Security Concerns of Flash Memory in Smart Cards. Application Note, Sharp, 2005 http://www.sharpsma.com/download/Security-Concerns-Flash-Anpdf

[4] K. Ramkumar: Cypress SONOS Technology. White Paper, Cypress Semiconductor, 2008 http://www.element14.com/community/servlet/JiveServlet/previewBody/28069-102-1-77264/cypress_sonos_technology_11.pdf

[5] T. Humes: Ensuring data security in logic non-volatile memory applications: Floating-gate versus oxide rupture. Virage Logic, 2009 http://mil-embedded.com/articles/ensuring-versus-oxide-rupture/

[6] C. Zajac: Protect Your Electronic Wallet Against Hackers. White Paper, Synopsys, 2011 https://www.trust-hub.org/resources/350/download/synopsys_wallet.pdf

[7] S. Weingart: Physical Security Devices for Computer Subsystems: A survey of Attacks and Defences, CHES 2000

[8] S. Skorobogatov: Semi-invasive attacks - A new approach to hardware security analysis. University of Cambridge Technical Report, 2005

[9] C. De Nardi, R. Desplats, P. Perdu, F. Beaudouin and J.-L. Gauffier, Oxide charge measurements in EEPROM devices, Microelectronics Reliability, Vol.45, 2005, pp 1514-1519

[10] C. De Nardi, R. Desplats, P. Perdu, C. Guérin, J.L. Gauffier, T.B. Amundsen: Direct Measurements of Charge in Floating Gate Transistor Channels of Flash Memories Using Scanning Capacitance Microscopy. ISTFA, 2006

[11] D. Konopinski, Forensic applications of atomic force microscopy, 2013

[12] D. Hanzii, E. Kelm, N. Luapunov, R. Milovanov, G. Molodcova, M. Yanul, D. Zubov: Determining the state of non-volatile memory cells with floating-gate using scanning probe microscopy. International Conference Micro- and Nano-Electronics, 2012

[13] R. Dhar, S. Dixon-Warren, J. Campbell, M. Green, D. Ban et al: Direct charge measurements to read back stored data in nonvolatile memory devices using scanning capacitance microscopy. 2013

[14] R. Dhar, S. Dixon-Warren, M. Kawaliye, J. Campbell, M. Green, D. Ban: Read Back of Stored Data in Non Volatile Memory Devices by Scanning Capacitance Microscopy. Materials Res. Soc. Symposium, 2013

[15] F. Courbon, P. Loubet-Moundi, J.A. Fournier, A. Tria: Increasing the efficiency of laser fault injections using fast gate level reverse engineering. HOST Symposium, 2014

[16] T. Sugawara, D. Suzuki, R. Fujii, S. Tawa, R. Hori, M. Shiozaki, T. Fujino: Reversing stealthy dopant-level circuits. CHES Workshop, 2015

[17] V. Korchnoy: Investigation of Choline Hydroxide for selective Silicon etch from a gate oxide failure analysis standpoint. 2002

[18] J. Colvin: A new technique to rapidly identify low level gate oxide leakage in field effect semiconductors using a scanning electron microscope, EOS/ESD Symp., 1990

[19] M. Jenkins, P. Tangyunyong, E. Cole Jr., J. Soden, J. Walraven, A. Pimentel: Floating substrate passive voltage contrast (FSPVC). ISTFA, 2006

[20] E. Cole Jr.: Beam-based localization techniques for IC failure analysis. Microelectronic failure analysis desk reference, 1999

[21] Atmel Atmega32U4 AVR Microcontroller. http://www.atmel.com/devices/ATMEGA32U4.aspx

[22] Inside Secure AT90SC Secure Microcontroller Summary. http://www.insidesecure.com/Products-Technologies