Reverse engineering Flash EEPROM memories using Scanning Electron Microscopy

Franck Courbon[1], Sergei Skorobogatov[1], and Christopher Woods[2]

[1] Computer Laboratory, University of Cambridge
[2] Quo Vadis Labs, London, UK

Abstract. In this article, a methodology to extract Flash EEPROM memory contents is presented. Samples are first backside prepared to expose the tunnel oxide of floating gate transistors. Then, a Scanning Electron Microscope (SEM) in the so called Passive Voltage Contrast (PVC) mode allows distinguishing '0' and '1' bit values stored in individual memory cell. Using SEM operator-free acquisition and standard image processing technique we demonstrate the possible automating of such technique over a full memory. The presented fast, efficient and low cost technique is successfully implemented on $0.35\mu m$ technology node microcontrollers and on a $0.21\mu m$ smart card type integrated circuit. The technique is at least two orders of magnitude faster than state-of-the-art Scanning Probe Microscopy (SPM) methods. Without adequate protection an adversary could obtain the full memory array content within minutes. The technique is a first step for reverse engineering secure embedded systems.

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

1 Introduction

Reverse engineering techniques have historically been developed to perform the opposite of a typical process flow used to build Integrated Circuits (IC). IC reverse engineering can be used for validation, debugging, patent infringment/malicious circuit modification/backdoors detection and failure analysis. Typical reverse engineering flow [22] is expensive in terms of equipements, time and skills and is composed of:

- circuit depackaging
- layer by layer deprocessing
- hundreds of SEM acquisitions for each layer
- cross-layer alignment
- individual element annotation
- netlist reconstruction and analysis

Today, embedded systems rely heavily on non-volatile memory (ROM, EEPROM, 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. Hence the interest of using reverse engineering to extract memory contents such as performed by Kommerling and Kuhn in 1999 [14]. They show that Mask ROM contents (most secure type of ROM) can be revealed using a microscope after sample preparation (selective dash etching). Since then Mask ROMs have not been considered to be secure unless encrypted or at least obfuscated. This paper targets EEPROM/FLASH non volatile memories.

Originally EEPROM was referred to as a two-transistor electrically re-programmable cell, while Flash was introduced later and had a single transistor [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 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. 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.

Several publications exist which refer to Scanning Probe Microscopy (SPM) 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 us to see some interaction whenever electron charges are present within memory cells. Following Skorobogatov’s conclusions [18], the first investigations using SPM-based techniques have been performed by De Nardi et al. [6, 7] and, recently, similarly performed again by different teams; Konopinski et al. [15], Hanzii et al. [11] and Dhar et al. [9, 10].

Nevertheless, some key micro-electronics companies, such as Sharp in 2005 [19], Cypress in 2008 [17], Virage Logic in 2009 [12] and Synopsys in 2011 [25] noted the security threat relating to the possibility of memory extraction using SEM. Actually, without waves, at CHES 2000, Weingart [24] first introduced that a Scanning Electron Microscope can be used to read individual bits in a EEPROM. Later, De Nardi’s inconspicuous PhD. manuscript details the technique applied with success [8]. Today, we open the technique to the community with our own application. We thus disclose a low cost sample preparation, validate the methodology on smaller technology node EEPROM and show that some ‘0’/‘1’ contrast can be seen in single transistor technology. We also anticipate on the capability to have a non destructive readout and give different image processing approaches to effectively extract memory contents.

However, due to SPM limitations, only slow and reduced area Flash EEPROM cell measurements are documented to date. The main drawbacks of SPM techniques are the low scanning speed, the small area covered, replacement of the tip, and an operator intervention to read a full memory array. This results in an impractical technique of reading out the complete memory of several mm^2. Whereas in the security community, Scanning Electron Microscopy has been recently used for hardware trojan detection [21] [5] and for spatially resolved laser fault injection [4]. Following those investigations, we show in this paper how Flash EEPROM contents commonly thought unreachable are retrieved using artefact free backside sample preparation, fined tuned SEM acquisitions (Voltage Contrast mode) and efficient image processing.

Voltage Contrast imaging is one of the first use of Scanning Electron Microscope [20]. The depicted technique is actually based on a mode which corresponds to the setup where no external bias is applied to the sample while setup parameters permit to obtain various information on the sample. In the literature, one can also find PVC variants as Capacitive Coupling Voltage Contrast (CCVC) [23] and Low Energy Electron Microscopy (LEEM) [1].

After a primary electron beam hits a specimen surface, a secondary electron signal results from the sample interaction. This collected signal depends on the primary beam features, the sample's atomic number, the nature of the area scanned, the doping level, short/open circuit [13] and as depicted in this communication the presence of local charges trapped in an oxide.

We thus open to the academic community the technique where floating gate accumulated electrons (image of '0' and '1' memory cell content) can be probed by SEM as illustrated in Figure 1. It can be seen as a first step for secure IC reverse engineering investigations.

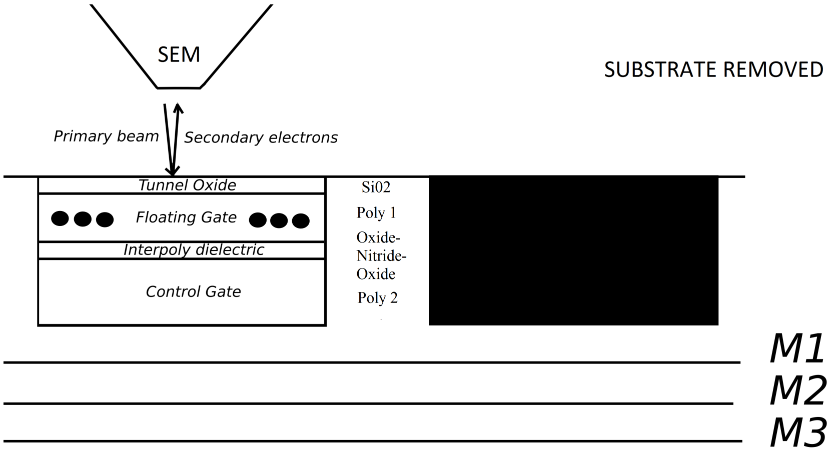


Fig. 1. Technique global flow, use of SEM after backside removal

2 Passive Voltage Contrast (PVC) for Flash/EEPROM memory content extraction

We acknowledge that neither the sample preparation nor the passive voltage contrast nor the image processing are new techniques but their combination results in a fast and effective approach for characterizing Flash EEPROM. On one hand, the sample preparation consisting in removing the substrate until tunnel oxides follows Korchnoy's approach [16]. On the other hand, the image acquisition using SEM is based on previous work of Cole [3]. The complete methodology is illustrated in Table 1.

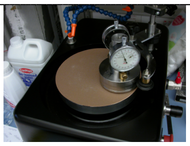
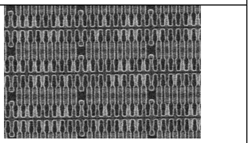
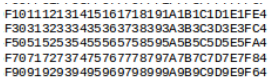
Step	*Task*	*Goal*	*Overview*
Sample preparation	Lapping, polishing, wet etching	Successively remove Si down to $20\mu m$, get a mirror aspect and then remove remaining substrate by wet etching	
Image acquisition	Move to & define area of interest, apply SEM parameters, load acquisition macro	Set best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

Table 1. Methodology recipe

Sample preparation goal is to remove all Silicon down to the tunnel oxide while leaving the charge blocking layer intact and such over a large area. Once the sample preparation performed, the acquisition is based on two principles for the dedicated application :

- Have sufficient spatial resolution to distinguish memory states
- Limit charge-up inherent to the use of an electron beam over a dielectric

The bit cell information is present at the Floating Gate/$Si0_2$ interface. However we do not directly probe the memory information stored in the Floating Gate. Indeed, a mirrored charge is SEM acquired at the tunnel oxide surface. The image contrast varies if a charge is present. This might be due to a local field modification that in fine leads to a different number of secondary electrons collected. To successfully obtain such image contrast, we give some information about the SEM parameters to use. They follow state of the art publications about passive voltage contrast or capacitive coupling voltage contrast [23].

No success was achieved with standard secondary electrons detectors. We select the through the lens (or InLens) detector combined with a small working distance to maximise the number of secondary electrons collected. To limit the charge-up phenomenon, we use an accelerating voltage around 2.5 keV, the characteristic energy of SiO_2. At such low accelerating voltage, the beam does not create a conductive path between floating and control gates (so the memory information remains). Regarding the probe current, a small diaphragm aperture is chosen for this . We also limit the number of incident electrons using a low magnification. The chosen magnification still requires enough pixels to characterize each memory cell individually. The magnification directly affects the time spent on a memory point. It also affects the global scanning time for large scans. To still limit the incidence of the primary beam, the fastest scanning speed possible is used. At such a fast scanning speed (25/50ns per pixel) the noise becomes an issue, thus, multiple acquisitions are taken and integrated to achieve a final, high quality image.

Under a SEM, an automated acquisition routine can be launched. Scanning area and magnification need to be first defined. It permits to collect a large set of images over a full memory without the presence of an operator. At last, image processing enables us to align all acquisitions together, to enhance the image contrast and to extract '0s' and '1s' in an automate way. It also allows us correlating the extracted data with the one load into the samples.

The technique combines steps coming from different field. To clarify the technique and for a better understanding, orders of magnitude of setup/tuning and operating time are given in Table 2 along the main considerations for each step.

Step	*Parameters/Considerations*	*Operating time*	*Setup/tuning time*
Sample preparation	Rotation speed, disks roughness& grit, time, acid concentration, temperature/etch time, final etch control	Half a day	Days
Image acquisition	Detector type, accelerating voltage, probe current, working distance, scanning speed, contrast/luminosity, tilt, scan orientation and type	A couple of hours	A couple of days
Image processing	Method, algorithm, threshold value, array size, data convention, bit number, MSB/LSB direction	Minutes	Days

Table 2. List of parameters and considerations to have all along the methodology

3 Flash/EEPROM reverse engineering: sample preparation

Device Under Test We demonstrate the technique on three different samples:

- ATMEL ATmega32U4 0.35μm 2T memory cell (microcontroller)
- ATMEL AT90SCxx 0.21μm 2T memory cell (smart card type IC)
- Texas Instruments MSP430 0.35μm 1T memory cell (microcontroller)

Using an universal programmer it was possible to load a specific pattern into the microcontrollers samples 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 Two approaches are currently documented regarding accessing floating gate transistors: 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. Frontside approach has shown that tunnel oxides are affected by the preparation. Thus, as in previous successful experiments, we use a backside approach where most of the silicon substrate is removed using mechanical polishing before a selective wet etching allows removing the remaining Silicon thickness. Floating gates tunnel oxides remain unspoiled.

Parallel polishing The samples are prepared using a simple polishing/lapping machine with devices mounted on a sample holding jig to assist precise thickness control and parallel lapping surface. As a backside approach is used, the mechanical grinding tool first encounters and removes a copper heatsink. Once removed, we successively use 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. Scratches are removed using polishing paste, a mirror polish aspect with a fairly constant roughness is obtained. We show, in Figure 2, intermediate backside Silicon removal images at the copper heatsink level, at 100 μm Si, at 20 μm Si and once polished at 20 μm Si for the ATmega32U4 sample.

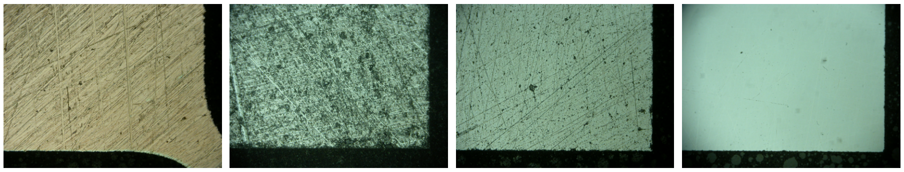


Fig. 2. Si. removal down to copper heatsink, 100μm Si., 20μm Si. and once polished

Wet etching Once the 20(+/-5) μm thickness is obtained, we use wet chemical etching to access the floating gate transistor's tunnel oxide for all samples, Figure 3. We use the same approach as the one developed by Korchnoy [16] and re-used in various AFM works [10]. We use Choline Hydroxide to remove the remaining substrate (20 μm) without damaging the thin tunnel oxide (10 nm). The solution was heated to 90°C to speed the etching process up while keeping a sufficient Si/SiO$_2$ selectivity ratio (about 5000).

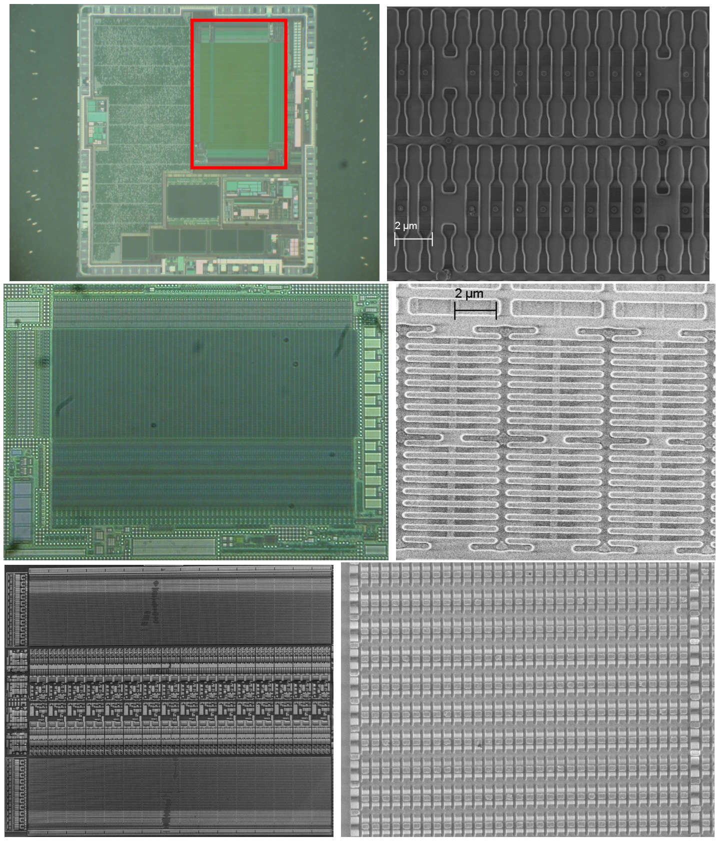


Fig. 3. IC/memory field of view (left col.) and memory structures zoom in (right col.)

4 Flash/EEPROM reverse engineering: Image acquisition

4.1 0.35μm 2T memory cell

We move to the next step of the methodology, the SEM imaging. Parameters were chosen in accordance with PVC state-of-the-art approaches. These involved using an InLens detector, a short working distance of 2 mm to 5 mm, 1 kV to 3 kV accelerating voltage and a minimal probe current. The magnification was chosen to fit the 1024 x 768 resolution of the image in a way that each memory cell was distinguishable from its neighbouring one. Depending on individual settings this resulted in magnifications between 1 kX and 5 kX - leading to about 8 to 16 pixels characterizing each memory cell. The scan speed was set to tens of milliseconds with integration over tens of frames.

Non exhaustively, the best image quality and contrast was achieved for the working distance of 5.3 mm and for the accelerating voltage of 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 4. It has to be noted that this image is 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. Plus, it is possible to control the process of injecting and removing charge by adjusting the accelerating voltage and probe current. For instance, concentrating a high energetic electron beam over a structure will brighten the structure.

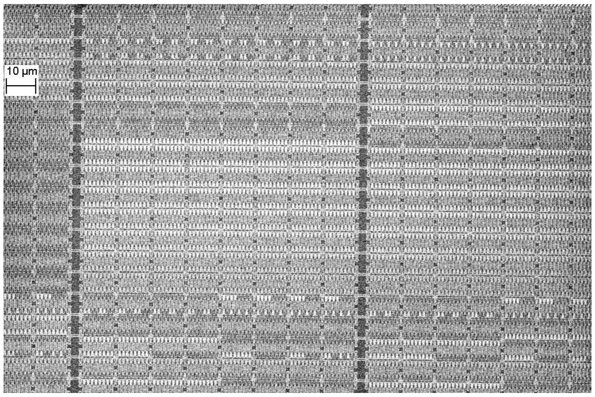


Fig. 4. 0.35μm 2T memory cell content extraction

Using Figure 4, it is quite interesting to analyze the reading out speed of the technique. This image has been obtained in 9.5 seconds (number of frames integration and scanning speed dependant). There are 40 lines containing each 128bits (magnification dependant), 640 bytes in total. The SEM reading throughput is thus about 67 bytes/second, or approximately 241 kbytes per hour.

Transistors states can be clearly distinguished as the dark (holes, positive charge) and the bright (electrons, negative charge) areas respectively. It is convention dependant for each integrated circuit (convention dark = ‘0’ and bright= ‘1’ for this ATMEL sample). The intermediary contrast at the word line is confirmed by the theory. 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).

We also figured out the physical layout of the memory from the test pattern was programmed into this sample. 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. For this sample, the complete memory content extraction (32 kbytes) would approximately take 8 minutes of SEM acquisitions (less than 10 minutes including a 10 percent image overlap). The practical implementation of the depicted technique is about 250 times faster than published state of the art EEPROM reverse engineering techniques (AFM based).

4.2 0.21μm 2T memory cell

We then apply the technique over the AT90SCxx sample, which uses a more recent technology node (0.21μm vs 0.35μm). The idea is to see how far the technique could work, despite the smaller number of electrons to be probed. As a result, Figure 5, the charges are still differentiated for each of the individual memory point.

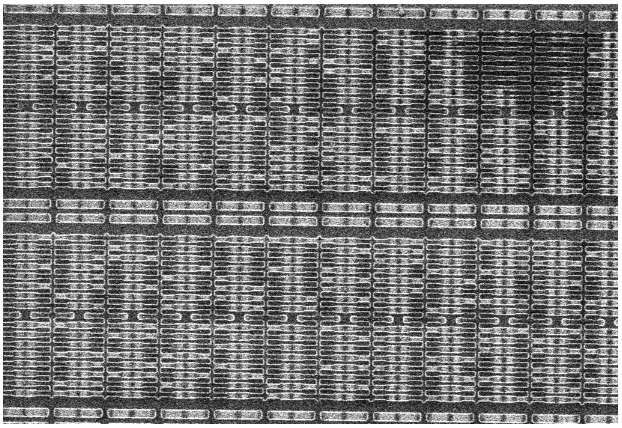


Fig. 5. 0.21μm 2T memory cell content extraction

The sample prepration is not sample depedant, only the SEM parameters were modified for this second sample. Indeed, after initially using the same stetings, we first had to increase the magnification to have enough pixels covering each memory point. The working distance was also decreased to maximize the number of secondary electrons collected.

Moreover, due to the higher magnification and smaller technology node, it was only possible to integrate over less frames. Indeed, beyond a certain number of frames all memory cells look alike. One of the reasons for that is because incident electron beam density is too important for such probing. Observing charge fluctuations with the help of a Scanning Electron Microscope is thus also successful over this $0.21\mu m$ technology node integrated circuit.

4.3 $0.35\mu m$ 1T memory cell

To finish with, we target the memory of the third sample. Each individual cell structure is made of a single transistor. The raw SEM image, Figure 6, does not permit to easily dinstinguish '0' and '1' cells. However, some charge fluctuations can be seen over this 1T memory cell structure. More research on each of the methodology step has to be undertaken to clarify this possibility.

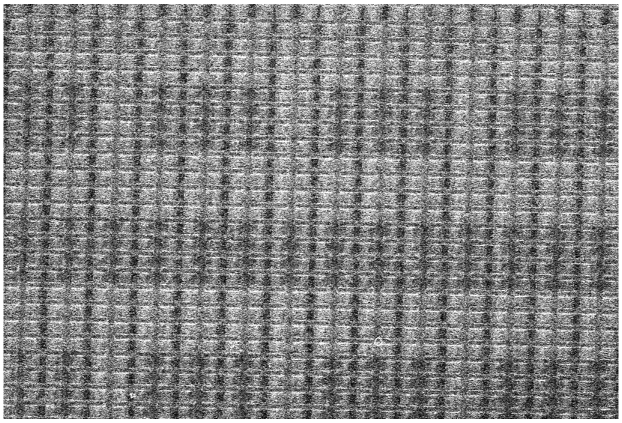


Fig. 6. $0.35\mu m$ 1T memory cell content extraction

4.4 Optimal setup: A look over $0.35\mu m$ 2T

In our investigations, we only use about a 3kX magnification and we are, regarding this parameter, very far from the SEM limitation. However, as seen in Figure 7 - covering about a sixth of the full memory, contrast can still be obtained at very low magnification. Moreover, using such magnification show about no information decay compare to the setup previously defined. The reading step can thus be non destructive. Figure 7 is a first answer towards the technique improvement where a 218 times magnification also allows charge differentiation.

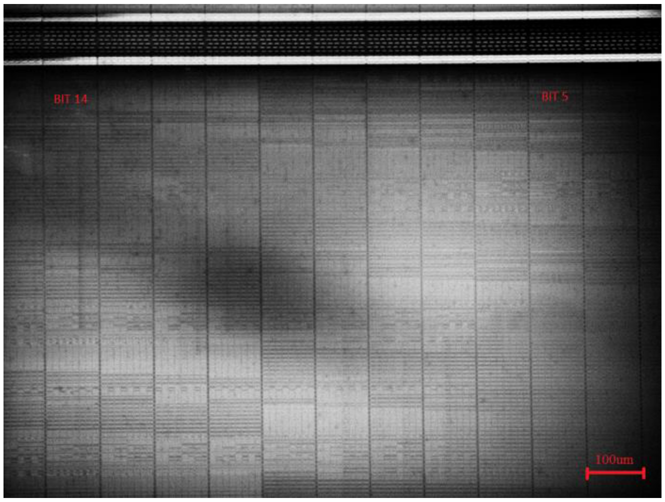


Fig. 7. $0.35\mu m$ 2T '0s' and '1s' differentiating at 218 times magnification

5 Flash/EEPROM reverse engineering: image processing

5.1 Area of acquisition definition and acquisition routine creation

We then want to show that the technique is industry compliant and interesting in the security field - as cell extraction contents can both be operator-free and cover a full memory.

The methodology being demonstrated, we then use the intrinsic features of a SEM - the ease to make automated and large scans. The goal is to extract the complete memory. We set the region of interest as the full memory of the integrated circuit by simply drawing a rectangle over it. Then we set the SEM acquisition parameters previously used. Given the magnification and the size of the memory, a certain amount of images to acquire are indicated. This number increases with the percentage of overlap desired. Ideally, we want to have successive images overlapping area where no data are present (between current and next 8 bits and between current and next address).

The area to scan being defined, the process is then to create and launch an acquisition macro saving each image in a repository. No operator is thus needeed to acquire large set of tens or hundreds images. It has to be noted that the capability to create macros is not included for all SEMs.

5.2 Offline image registration

The usage of the SEM over, the multiple image registration is done offline by the use of open source softwares or matlab commands based on phase transform. Such exemple is given for two successive acquisitions (1024 x 768 each) with X (33pix.) and Y (139pix.) shifts. Despite the repetitive cell structure, no artefacts over the final reconstructed image (1057 x 907) are present, Figure 8.

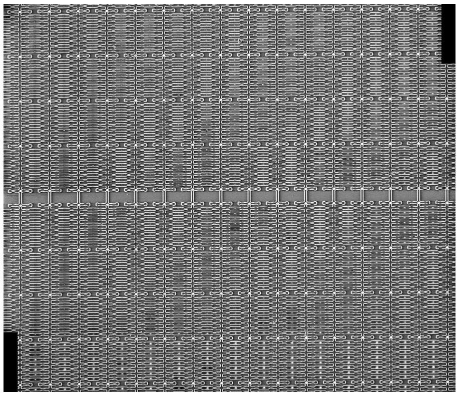


Fig. 8. Image alignment over 2 acquisitions without charges

However, this can be a bit trickier to acquire successive images with charges and to align them. We tackle the typical use case for large memory reverse engineering and give, Figure 9, the registration of two successive images. It is thus possible to obtain an image of the complete memory array without operator. Having such data, the next step is to extract '0s' and '1s' information in an automated way.

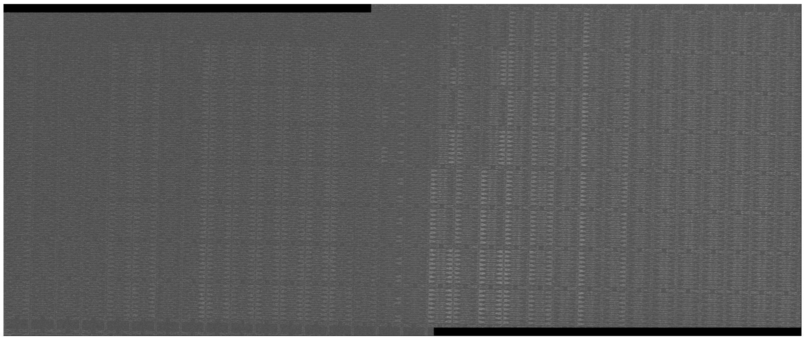


Fig. 9. Image alignment over 2 acquisitions with charge

5.3 0s and 1s extraction using intensity values variation

A straightforward way to extract data is to process gray scale intensities to differentiate cells with a charge to the ones without. High intensity values correspond to the presence of a negative charge and subsequently a '1' for this device. We first use standard image processing technique to enhance the signal contrast of '1s' over '0s'. Then, we set a threshold to distinguish '0s' and '1s' cells. We illustrate such on Figure 10. In fine, a grid can be created as data follows a repetitive pattern (rows and columns).

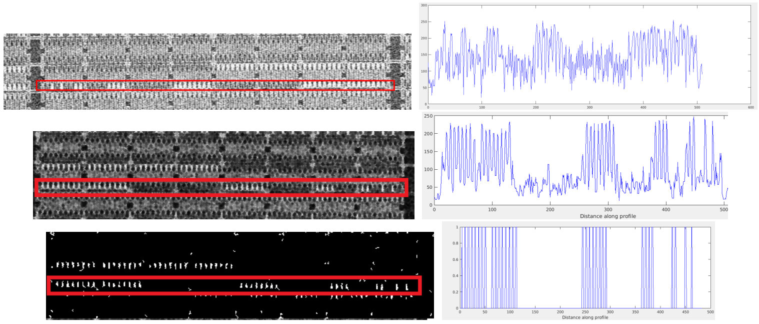


Fig. 10. Top: Raw profile line, middle: after processing bottom: after thresholding

5.4 0s and 1s extraction subtracting successive acquisitions

An other approach for charge differentiation is to acquire a first SEM acquisition followed by a second acquisition where charges are not noticeable anymore. The idea is to get advantage of the incident electron beam effect. In Figure 11 are the two SEM acquisitions (left and middle) and the final subtraction (right) giving the data pattern.

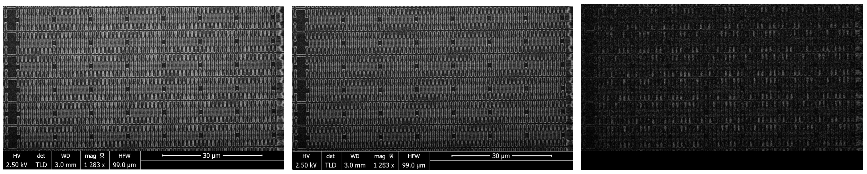


Fig. 11. Left: SEM acq. w/ charge, middle: SEM acq. w/o charges, right: subtraction

Depending on the convention used by the manufacturer, the bit number layout, the MSB/LSB layout, one can correlate an input data pattern loaded into the sample and then read it back using the depicted methodology. The practical methodology is thus theoretically applicable over a large area and automatable.

6 Discussion: Recent Integrated Circuits and methodology pros & cons

6.1 Towards Recent Integrated Circuits application

Within this paper, a reverse engineering attack is discussed and is practically implemented over different integrated circuits. Nevertheless, those integrated circuits are about 15 years old. It would be interesting to challenge the technique where fewer electrons are stored in Flash EEPROM floating-gate transistors (smaller technology node). Multiple approaches seem possible to improve the SEM contrast and they can be located at any step of the methodology. For instance, adding sample coatings, modifying the SEM setup itself, or applying further image processing could be some options. Moreover, reverse engineering the whole memory contents to estimate the error rate and application ease of this technique would also be of interest.

If the technique is proven functional over smaller technology node, attack ratings could be impacted. Indeed, attacks are being ranked (common criteria for instance) and this type of attack show some interesting features, subsection 6.2. We recall that Scanning Electron Microscope are still classified as bespoke (such as FIB) even though they can be rented in many facilities for less than hundreds dollars per hour. The attack time is relatively weak and a small number of samples is required.

6.2 Methodology pros and cons

The technique gets advantages of the inherent SEM features to extract memory cells content, Table 3. However, using this sole depicted technique won't enable the attacker to get over scrambling and encryption. To sum up, the depicted methodology is fast - only a day of work is necessary, low-cost - about 100$ of consumables are necessary and Scanning Electron Microscopes can be rented for an additional 100$ per hour, repeatable - technique is efficient, large scale compliant - SEMs permit to image a full memory area and is non software dependent - as it directly addresses the hardware of the device. The hardware dependancy is also seen as a drawback as SEM parameters needs to be adjusted depending on the hardware structure.

Advantages	*Drawbacks*
Low cost	Data decay
Fast	Invasive approach with destructive reading
Efficient	Do not tackle encryption nor scrambling
Large area compliant	Only validated down to $0.21\mu m$ technology
Hardware dependant	Hardware dependant

Table 3. SEM-based content extraction main features

7 Conclusion

We successfully reverse engineer Flash EEPROM using backside sample preparation and Scanning Electron Microscopy (SEM). The technique only requires a polishing tool, wet etching acid and few hours' access to a SEM. The methodology is proven fast, low-cost and repeatable and above all is shown automatable. Beside explaining methodology steps, we also validate it over different integrated circuits. For a $0.35\mu m$ technology node 2T EEPROM cell microcontroller, we get an imaging throughput of 241k bytes per hour without optimization. It beats published current state of the art memory content extraction (AFM based) by a factor of approximately 250 and it opens a novel research area for hardware security,reverse engineering but also image processing for hardware security purposes. As previous investigations showing weaknesses of ROM (also non volatile memory), this paper highlights the security vulnerabilities of Flash EEPROM. The methodology can definitely be seen as a first step for reverse engineering secure integrated circuit memory contents. Additional research grant would permit to judge the application of such technique over current integrated circuits and to characterize possible encryption/scrambling vulnerabilities.

References

1. Bauer, E.: Low energy electron microscopy. Reports on Progress in Physics 57(9), 895 (1994), http://stacks.iop.org/0034-4885/57/i=9/a=002
2. Brown, W., Brewer, J.: Nonvolatile Semiconductor Memory Technology: A Comprehensive Guide to Understanding and Using NVSM Devices. IEEE Press Series on Microelectronic Systems, Wiley (1997)
3. Cole, E.: Beam-based localization techniques for ic failure analysis (1999)
4. Courbon, F., Loubet-Moundi, P., Fournier, J.J.A., Tria, A.: Increasing the efficiency of laser fault injections using fast gate level reverse engineering. In: IEEE International Symposium on Hardware-Oriented Security and Trust, HOST (2014)
5. Courbon, F., Loubet-Moundi, P., Fournier, J.J.A., Tria, A.: A high efficiency hardware trojan detection technique based on fast SEM imaging. In: Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, DATE 2015, Grenoble, France, March 9-13, 2015. pp. 788–793 (2015)
6. De Nardi, C., Desplats, R., Perdu, P., Beaudoin, F., Gauffier, J.L.: Oxide charge measurements in eeprom devices 45 (2005)
7. De Nardi, C., Desplats, R., Perdu, P., Gurin, C., J.-L., G., Amundse, T.: Direct measurements of charge in floating gate transistor channels of flash memories using scanning capacitance microscopy, ISTFA 2006 (2006)
8. De Nardi, C.: Techniques d'analyse de défaillance de circuits intégrés appliquées au descrambling et à la lecture de données sur des composants mémoires non volatiles. Ph.D. thesis, Toulouse, INSA (2009)
9. Dhar, R., Dixon-Warren, S., Campbell, J., Green, M., Ban, D.: Direct charge measurements to read back stored data in nonvolatile memory devices using scanning capacitance microscopy (2013)
10. Dhar, R., Dixon-Warren, S., Kawaliye, Campbell, J., Green, M., Ban, D.: Read back of stored data in non volatile memory devices by scanning capacitance microscopy (2013)

11. Hanzii, D., Kelm, E., Luapunov, N., Milovanov, R., Molodcova, G., Yanul, M., Zubov, D.: Determining the state of non-volatile memory cells with floating gate using scanning probe microscopy. vol. 8700, pp. 87000V–87000V–11 (2013)
12. Humes, T.: Ensuring data security in logic non-volatile memory applications: Floating-gate versus oxide rupture, virage logic (2009)
13. Jenkins, M., Tangyunyong, P., Cole Jr, E., Soden, J., Walraven, J., Pimentel, A.: Floating substrate passive voltage contrast (2006)
14. Kömmerling, O., Kuhn, M.G.: Design principles for tamper-resistant smartcard processors. In: Proceedings of the USENIX Workshop on Smartcard Technology. pp. 2–2. WOST'99 (1999)
15. Konopinski, D.: Forensic applications of atomic force microscopy (2013)
16. Korchnoy, V.: Investigation of choline hydroxide for selective silicon etch from a gate oxide failure analysis standpoint (2002)
17. Ramkumar, K.: Cypress sonos technology, cypress (2008)
18. Skorobogatov, S.P.: Semi-invasive attacks - a new approach to hardware security analysis (2005)
19. Smith, G.: Addressing security concerns of flash memory in smart cards, Sharp (2005)
20. Smith, K.C., Wells, O.C., McMullan, D.: The fiftieth anniversary of the first applications of the scanning electron microscope in materials research. Physics Procedia 1(1), 3–12 (2008)
21. Sugawara, T., Suzuki, D., Fujii, R., Tawa, S., Hori, R., Shiozaki, M., Fujino, T.: Reversing stealthy dopant-level circuits. J. Cryptographic Engineering (2015)
22. Torrance, R., James, D.: The state-of-the-art in IC reverse engineering. In: Cryptographic Hardware and Embedded Systems - CHES, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings. pp. 363–381 (2009)
23. Watanabe, Y., Fukuda, Y., T., J.: Analysis of capacitive coupling voltage contrast in scanning electron microscopy (1985)
24. Weingart, S.H.: Physical security devices for computer subsystems: A survey of attacks and defences. In: Cryptographic Hardware and Embedded Systems - CHES 2000, Worcester, MA, USA, August 17-18, 2000, Proceedings. pp. 302–317
25. Zajac, C.: Protect your electronic wallet against hackers, Synopsys (2011)