A Chemical Memory Snapshot

Jörn-Marc Schmidt[1,2]

[1] Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
joern-marc.schmidt@iaik.at
[2] Secure Business Austria (SBA),
Favoritenstraße 16, 1040 Vienna, Austria

Abstract. Smart cards and embedded systems are part of everyday life. A lot of them contain sensitive data like keys used in secure applications. These keys have to be transferred from non-volatile to static memory to generate signatures or encrypt data. Hence, the possibility to read out the static memory of a device is a crucial security threat. This paper presents a new technique to read out secret data from the internal static memory of a cryptographic device. A chemical reaction of the top metal layer of a decapsulated chip is used to identify lines connected to the positive power supply. Using this information, we are able to obtain the content of memory cells like the secret key of a cryptographic system.

Keywords: Smart cards, physical security, electrolysis

1 Introduction

Evaluating the security of a cryptographic device, not only the used protocol and its underlying cryptographic algorithms are important. The device itself and the way the algorithms are implemented on it may also reveal valuable information. Attacks that exploit properties of the device are called implementation attacks. Depending on whether the behavior of a device is influenced or just measured, an attack is called active or passive. Furthermore, implementation attacks can be non-invasive, semi-invasive, or invasive. Non-invasive attacks do not modify the package of the device, while semi-invasive attacks apply a decapsulation procedure to expose the chip. In addition, if direct electrical contact is established to the surface of the chip, the attack is called invasive.

Non-invasive, passive ones are called side-channel attacks [1]. Paul Kocher utilized differences in the execution time depending on secret data to reveal it in 1996 [2]. In 1997, it has been shown by Eli Biham and Adi Shamir [3] and in parallel by Dan Boneh et al. [4] that actively provoking faults in cryptographic devices can also be exploit to uncover secret information. That passive measurement of the power consumption of a device may also reveal secret data was demonstrated by Paul Kocher et al. in 1999. Subsequently, it has been shown by Dakshi Agrawal et al. in 2002 that measuring electromagnetic emissions of a device allows to attack it. Side channel as well as fault attacks have become

a popular topic in research. Mostly, multiple calculations of encryptions or signatures, a previous characterization of the device, or a precise fault injection are necessary for an attack. Another way to disclose a secret key is reading it directly out of the memory of a device, which can be done without using the reading operations of the device. This method is independent of the implemented algorithm as long as the key is processed inside the static memory.

A common way to read out secret data directly is probing [5, 6]. Thereby, a probing needle establishes electrical contact to the surface of the chip. As the technology size is getting smaller, this becomes more and more difficult.

Another way to reveal content of memory cells was presented by David Samyde et al. [7]. They scanned the surface of an active chip with a laser beam. At each position of the laser, the current injected by the beam was measured. In this way, cells containing zeros could be distinguished from those containing ones. Their method is semi-invasive, as a decapsulation procedure has to be applied. As several points have to be scanned, the technique is rather slow. To read out important data during a computation that cannot be stopped in the target state, they suggest freezing the memory to increase the remanence of the data in the cells [8].

Our Contribution. We present a new method to produce a quick one-time snapshot of the state the memory cells are in. Our method makes use of a chemical reaction called electrolysis. For this purpose, the chip has to be decapsulated and parts of the passivation must be removed. The reaction shows the current state of the exposed memory cells. A standard procedure for decapsulation as described in [9] is sufficient. Exposing the top metal layer can be done with different procedures. Wet etching for removing the whole passivation or a laser cutter as well as a focused ion beam (FIB) for a selective removal can be used. We will elaborate on these possibilities in Section 4. For our experiments we decided to use a laser cutter, as it is the cheapest choice.

This paper is organized as follows. After describing the target device including details on SRAM cells in Section 2, the chemical process called electrolysis is explained in Section 3. Possible ways to remove the passivation of a chip are discussed in Section 4. Section 5 shows the results of our experiments. Conclusion is drawn in Section 6.

2 Target Device

An 8-bit microcontroller with 128 byte internal static memory was chosen for the experiments. Its passivation consists of silicon-dioxide, the top metal layer of aluminum with a titanium-nitride barrier. The size of a memory cell in the device is $474\,\mu m^2$. In the following, its structure will be explained in more detail.

A standard static memory cell consists of six transistors. Four of them build two inverters. Each output of the invertors is connected to the input of the other one. Read and write functions of the cell are realized by the two remaining transistors. Figure 1 shows a schematic of a standard cell. For programming a

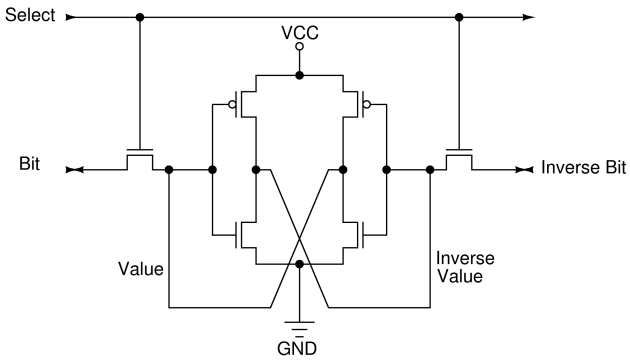

Fig. 1. Schematic of a standard SRAM cell

cell the appropriate value is put onto the bit line, its inverse onto the inverse bit line. Programming is enabled by the select line. As the drivers of the write circuit are stronger than the transistors inside the cell, the old state is replaced by the one put onto the bit lines. Sense amplifiers are used to read a cell. They recognize the state of the cell activated by the select line.

Fig. 2. Array of SRAM cells (metal layer)

If the cell contains one, the value line is connected to the positive power supply (VCC) and the inverse value line to ground (GND); vice versa if it contains zero. Figure 2 shows the top metal layer of three times four memory cells. In the chip considered, parts of the circuit lines containing the value and the inverse value of the cell are realized on the top metal layer. Thus, these two lines

indicate whether a cell contains zero or one. If the metal layer is exposed, this information can be gained by electrolysis.

3 Electrolysis

Electrolysis is a chemical process. Thereby, electrical energy is converted into chemical energy in liquids containing ions. Such a liquid is called electrolyte. The electrical energy has to be supplied as direct current to it. The supplying conductors are called electrodes. Electric charge in electrolytes is carried by its ions. These ions move within the electrolyte and cause chemical reactions at the electrodes.

In an electrolytic process the electrode that emits electrons is called cathode. Its opposite is called anode. At anode and cathode different chemical reactions take place: at the cathode positive charged ions, named cations, are reduced; at the anode negative charged ions, named anions, are oxidized. Thus, the conduction of an electrolyte depends on the mobility of its ions. The electrolyte itself stays electrical neutral [10]. Industrial processes commonly use electrolyze for separating chemicals, as well as for putting a protective layer on materials.

Here, electrolysis is applied for attacking a device. As the distance between the metal lines, which will act as anode and cathode, is very small, a liquid that conducts only sparely is necessary. This reduces the damage caused by the current flowing over the liquid. Pure water is only sparely conducting. Therefore, distilled water from the local tool store was used. The conductivity of tap water is much higher, because it contains dissolved salts and thus free ions. For electrolyze to take place on the chip, it is necessary that the liquid has direct contact to the surface of the top metal layer. Thus, the passivation of the chip has to be removed, at least from the memory cells of interest.

4 Removal of the Passivation

Removing the passivation is a quite more challenging task than the package decapsulation. The passivation of a common chip consists of silicon oxide, often in combination with a layer of silicon nitride. Those layers can be removed from the whole chip at once or in a selective way, which exposes only small parts of the chip.

The whole passivation can be removed at once by wet etching [11]. This process always acts uniform in all directions. A silicon nitride layer can be removed by 85 % phosphoric acid at $160\,^{\circ}C$. Silicon oxide can only be etched with hydrogen fluoride. In order to be able to stop the reaction before underlying layers are affected, a buffered dissolution of hydrofluoric acid and ammonium fluoride is commonly used. There are several different mixtures. It is necessary to know the etch rate of the used mixture as well as the thickness of the silicon oxide layer to stop the reaction at the right moment.

A selective removal of the layers can be performed by a focused ion beam (FIB) or a laser cutter. Focused ion beams work similar to scanning electron

microscopes (SEMs). The electron beam in the electron microscope is substituted by a beam of gallium ions. At low power this beam can be used for imaging, at higher power for milling. Using the ion beam a milling with a precision of submicron scale can be achieved. In contrast to a focused ion beam, a laser cutter emits a pulsed light beam. This beam is focused by a microscope. Depending on its intensity, the beam can expose or at higher optical output cut wires of the top metal layer.

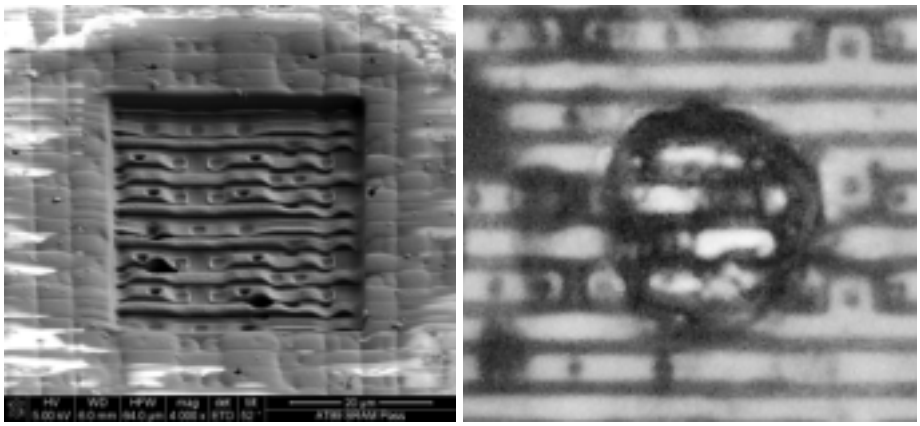

Fig. 3. Passivation removal using a focused ion beam (left) and a laser cutter (right)

While a focused ion beam can remove the passivation in a very careful and well directed way, a laser cutter needs a very precise adjustment. A strong beam can damage the circuit and weak beam may have no effect at all. In Figure 3 the differences between removing the passivation with a focused ion beam and laser cutter are shown. For the experiments a laser cutter was utilized, because of the high cost of a focused ion beam. One shot of the laser cutter exposed parts of the bit and the inverse bit lines. This was sufficient for the attack.

5 Results

With a small pipette a water drop of distillated water was put onto the surface of the powered chip. In order to avoid unwanted inferences, the water should not get in touch with the bonding wires. Using this setup, we were still able to write and read the values of the cells for several minutes with the program of the microcontroller. Afterwards, errors occurred in some memory cells.

Immediately after the water reaches the surface, the chemical reaction begins. This is indicated by a liberated gas. Before and during the experiment, the value one was written to a memory cell. Hence, its value was not changed. Figure 4 shows the result of the reaction. The line containing the bit and the positive

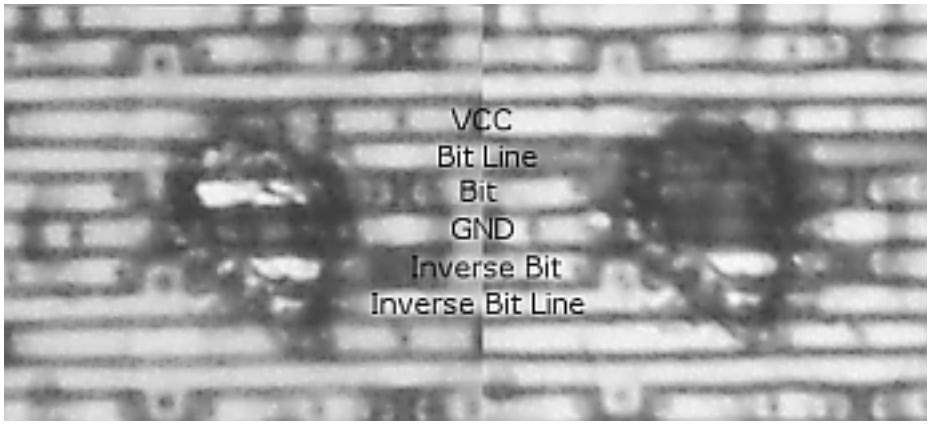

Fig. 4. Memory cell before (left) and after chemical preparation (right)

programming line have been stained, even parts underneath the passivation, while the inverse lines did not change their color. The ground line was hit by the laser cutter without cutting it completely. The chemical process had no influence on it.

If the value is not changed during the procedure, the staining does not change, even if the metal lines are exposed to the water for just a few seconds or several minutes. At cells that change their value while they are in touch with the water, each of the two value lines act as anode and as cathode. Thus, both lines show the same staining. Considering a computation, it is possible to distinguish between memory cells were data is processed and unused or cells with static values. The change of the color is an irreversible process. Once the color of a line has been changed, we were not able to remove the staining.

6 Conclusion

We presented a new way to read out memory without using the functions supplied by the chip. The method makes use of a chemical reaction. It produces a one-time snapshot of the actual state of the memory. Thus, values processed in the static memory of a device can be read out by an attacker, including secret keys.

7 Acknowledgments

The author would like to thank Julian Wagner and the Institute for Electron Microscopy of the TU Graz for their support and the focused ion beam picture. I would also like to thank Peter Söser and Christoph Marschner for their support.

References

1. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks – Revealing the Secrets of Smart Cards. Springer (2007) ISBN 978-0-387-30857-9.
2. Kocher, P.C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Koblitz, N., ed.: Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings. Number 1109 in Lecture Notes in Computer Science, Springer (1996) 104–113
3. Biham, E., Shamir, A.: Differential Fault Analysis of Secret Key Cryptosystems. In Jr., B.S.K., ed.: Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings. Volume 1294 of Lecture Notes in Computer Science., Springer (1997) 513–525
4. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract). In Fumy, W., ed.: Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceedings. Volume 1233 of Lecture Notes in Computer Science., Springer (1997) 37–51
5. Anderson, R.J., Kuhn, M.G.: Tamper Resistance - a Cautionary Note. In: Second Usenix Workshop on Electronic Commerce. (November 1996) 1–11
6. Kömmerling, O., Kuhn, M.G.: Design Principles for Tamper-Resistant Smartcard Processors. In: USENIX Workshop on Smartcard Technology (Smartcard '99). (May 1999) 9–20
7. Samyde, D., Skorobogatov, S.P., Anderson, R.J., Quisquater, J.J.: On a New Way to Read Data from Memory. In: IEEE Security in Storage Workshop (SISW02), IEEE Computer Society (2002) 65–69
8. Skorobogatov, S.: Low temperature data remanence in static RAM. Technical report, University of Cambridge Computer Laboratory (June 2002)
9. Skorobogatov, S.P.: Semi-invasive attacks - A new approach to hardware security analysis. PhD thesis, University of Cambridge - Computer Laboratory (2005) Available online at `http://www.cl.cam.ac.uk/TechReports/`.
10. Gärtner, H., Hoffmann, M., Schaschke, H., Schürmann, I.M.: Das große Buch der Chemie. Compact Verlag (2004)
11. Beck, F.: Integrated Circuit Failure Analysis: A Guide to Preparation Techniques. Wiley (March 1998)