eprint.iacr.org, April 2007

Estimation of keys stored in CMOS cryptographic device after baking by using the charge shift

by
Osman Kocar[1]

Abstract:
The threshold voltage V_T of EEPROM cells is a very important technological parameter for storing data and keys in a cryptographic device like smartcards. Furthermore, main objective of this paper is to check whether it is possible to get the key stored in the EEPROM cell through measuring the current consumption of the cryptographic device during read key command for encryption before and after baking at a certain temperature. This stress (baking) of the charge in the floating gate of the cells shifts the threshold voltage. Especially this effect will be considered whether the unknown key in the EEPROM cells can be estimated by using the charge shift in the floating gate. The test labs might need to check during an evaluation procedure of the smartcards if parts or whole key can be estimated successfully by stressing the threshold parameter V_T. The result of this evaluation is (will be) an input for countermeasures against possible attacks. It is also an additional input for further design structures in order to avoid information gain after baking the EEPROM cells at a certain temperature.

1. Introduction

The immense development of technology has led to the fact that our life without silicon chips would be unimaginable. Of course, this technological development of microchips is useful for our life, but technology has also weaknesses. These weaknesses can be hidden in different integrated components of a microchip, may it be that the microchip suspends its functionality at a certain temperature, that the chip is manipulated by invasive attacks, or else that an attacker uses the technological behavior in order to get the stored information from the microchip. One of the technological behaviors is the charge shift of the EEPROM cells (Electrically Erasable Programmable Read Only Memory) under stress (e.g. temperature). This shift is located in the floating gate. This technological behavior of the charge could possibly be used by an attacker in order to gain information stored in the microchip. Today, this charge shift after baking can be used during a read key operation before encryption (e.g.: before 3DES-operation) to estimate parts or the whole key. This could be performed by measuring the current consumption of the cryptographic device during a read key command for encryption before and after baking. The method of estimating keys by measuring the current consumption during read key commend will be named Differential Charge Analysis (DCA). Named DCA, because the difference of the current consumption before and after baking at a temperature is a size for the shifted charge of the written cells. That means, the number of the bits '1' or '0' stored as a key in the EEPROM cells of the CMOS cryptographic device can be calculated or estimated. The reason why DCA analysis for each new developed

[1] Osman Kocar received M.Sc. degree in Physics from the University of Munich, Germany in 1981. He worked as a test, quality and design engineer between 1982 and1993 at Temic Telefunken Semiconductor Group for low power integrated CMOS circuits, Eching in Germany. He joined the Federal Office for Information Security (BSI), Bonn, Germany in 1994 as a certifier for IT products and systems. His current task is the certifying of smartcard products regarding the IT security at BSI. email: osman.kocar@bsi.bund.de

cryptographic chip shall be performed is to examine if the integrated security circuit are masked against DCA methods. This behavior will be the main issue of this paper.

2. EEPROM cells and their function

Figure 1a shows a cell structure of an EEPROM. In this structure, information can be stored in the floating gate of the EEPROM cell as a charge. If the EEPROM cell is erased, the floating gate has a negative charge performed with a high voltage pulse,

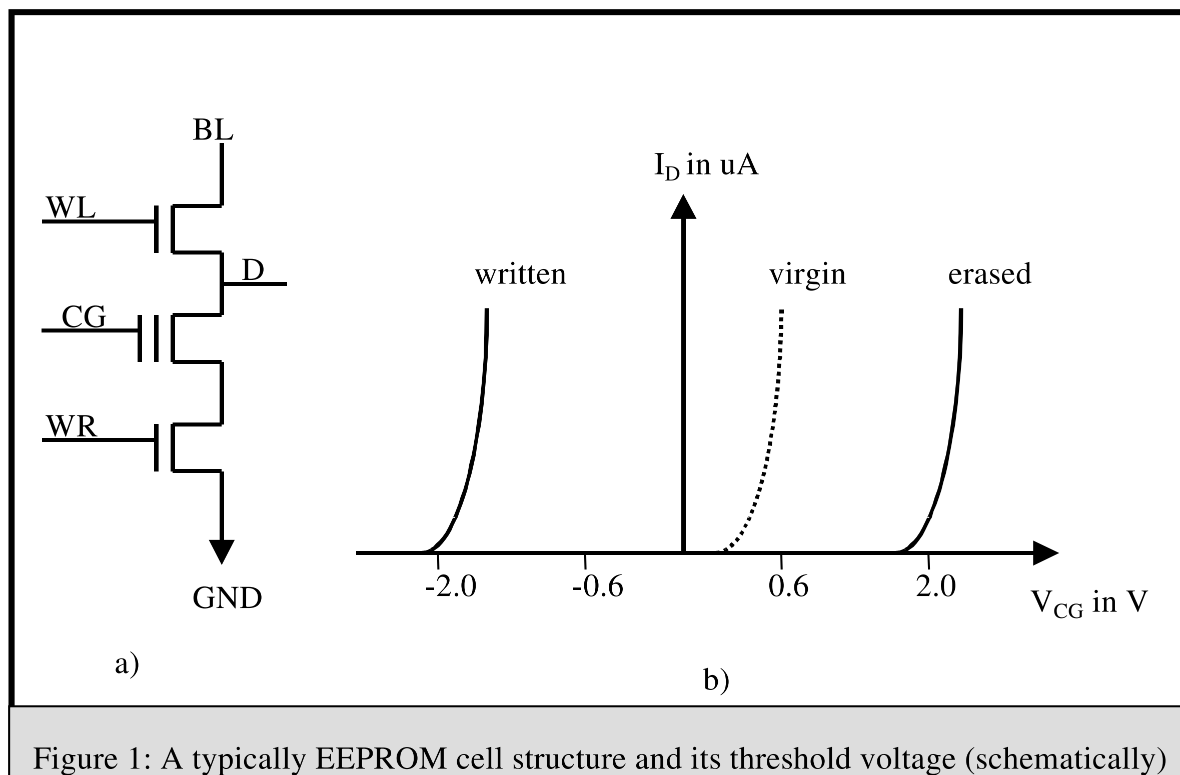

Figure 1: A typically EEPROM cell structure and its threshold voltage (schematically)

15V and 1ms, between drain (D) and control gate (CG). In this case the cell has the logical value ‘1’. Otherwise, if the pulse is between CG and source (S), the cell is written (-15V and 1ms). A written cell has a positive charge in the floating gate (FG) and the logical value ‘0’ [1], [2]. A single erased EEPROM cell current I_D is illustrated in figure 1b as a function of voltage applied on the control gate V_{CG}. A written current characteristic is also illustrated in the figure 1b. After the manufacturing process in the high temperature environment, we observe the virgin current characteristic shown as dotted line in figure 1b. This dotted line shows a cell which is either written or erased, but the floating gate contains negative charge. The reason why we have this virgin current characteristic lies in the mobility of the negative charges (electrons). The electrons have a smaller mass than the holes, so they have higher mobility. In case of balance, the floating gate has more negative charges than the holes.

3. The read operation of a single EEPROM cell

The kind of charge stored in the floating gate can easily be checked in a single isolated EEPROM cell. If a single EEPROM Transistor and its switch behavior is considered, it will be clear that the different charge in the floating gate influences the switch behavior depending on positive or negative charges. This behavior will be considered during a read operation. The figure 2b shows the timing for a read operation. The control gate (CG) is always connected to the 0 Volt during a read

operation. For the timing given in figure 2b the CG is grounded. Whether a current

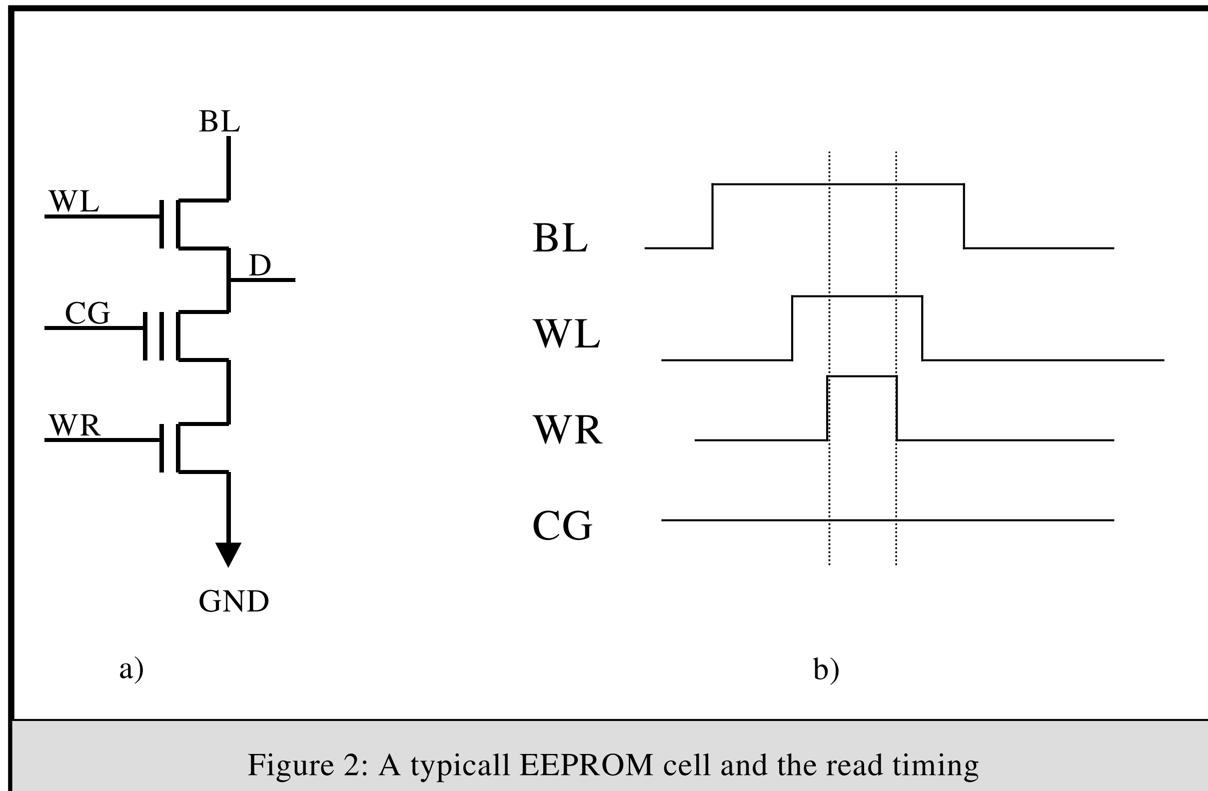

Figure 2: A typicall EEPROM cell and the read timing

flows from BL to GND or not depends on the threshold voltage (V_T) of the EEPROM cell. When the voltage of control gate is higher than the threshold voltage of the EEPROM cell, a current flows from BL to GND. Otherwise no current can be detected in this line. If the cell is written, we can observe a current flowing from BL to GND during WR pules duration (dotted line in figure 2b). That means, this current can be detected by an integrated sense amplifier (logical '0' state). This current can be observed also in the power line VDD during WR pulses. In case we had only one EEPROM cell, we would know whether the cell is written or erased by measuring the behavior of the current conception during a read operation.

4. Influence of the Temperature on EEPROM cells

One of the important parameter is the data retention for erased and written cells. Knowing that the negative charges (electrons) have higher mobility than the holes (positive charges), it should only be focused on a written cell with increasing temperature. The erased cells (logical '1') would also lose electrons if the cell was baked (e.g. at 250℃ for 24 hours). The loss of the electrons would be insignificant, since the state of the erased cell would still be logical '1' during a read process. The experiments on erased cells proof that the threshold voltages before and after are always higher than 0 Volt, although they were baked at 250 ℃ for 24 hours [3]. That means the erased cells have the same information (logical '1') before and after temperature storage at 250 ℃ for 24 hours. This process causes only a shifting of the threshold voltages, meaning it is smaller than before. This threshold shifting process never changes the logical state if the cells are erased. Therefore, it makes more sense to consider the written cell for temperature storage. The illustration in figure 3a shows a written EEPROM cell

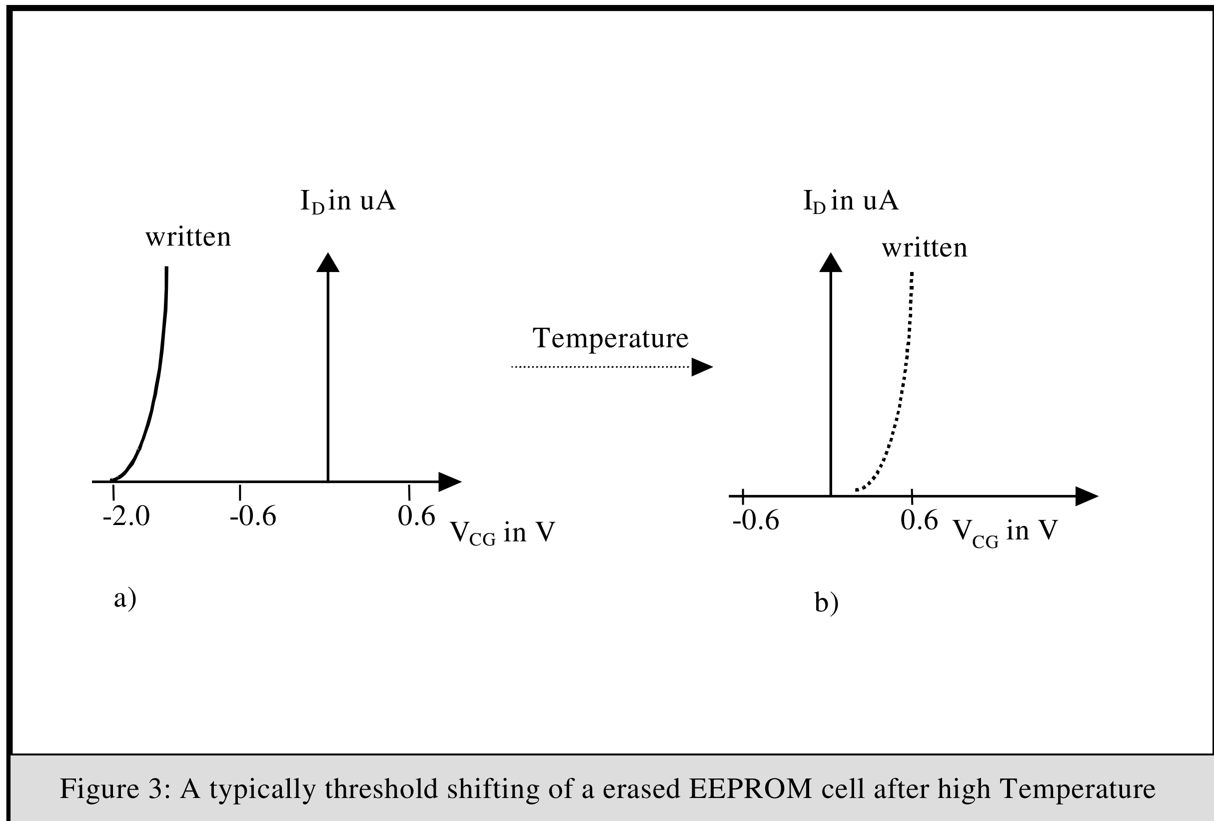

Figure 3: A typically threshold shifting of a erased EEPROM cell after high Temperature

and 3b shows shifted threshold after a baking process for 24 hours at 250 ℃. This experiment is performed on a written EEPROM cell. At the end of the baking process, the threshold curve shifted to the curve shown in 3b. That means the charge (threshold voltage) shifted over 0 Volt. In this case, we will get logical '1' after a read operation defined in figure 2b. The written EEPROM cell changes the logical state from '0' to '1'. This certain effect can be used for getting information stored as charge (positive or negative) in a circuit by measuring the current behavior before and after bake process.

5. Estimation of the key stored in Smartcards

One of the technological behavior in CMOS (Complimentary Metal Oxide Semiconductor) is the charge shift of the EEPROM cells by baking. This baking process can be used by an attacker in order to estimate parts or the whole key stored in the smartcard for encryption. This could be performed by measuring the current consumption of the cryptographic device (like smartcard) according to read operation defined in figure 2b during a read key command for encryption before and after baking the smartcard (e.g.: before 3DES-operation). This method, named as Differential Charge Analysis (DCA), describes the differences of the current consumption before and after baking and is a size for the shifted charge for written cells (e.g. at 250℃, 24h). The figure 4 shows the current behavior of a written EEPROM cell during a read operation before and after baking (dotted line) at 250℃ for 24 hours. This illustration shows that the information can also be measured on the current line to get the information without baking the written cell. When the cell is integrated in a smartcard, it is difficult to estimate the content of information because of noises and countermeasures integrated by the developer. It will be more difficult if the smartcard has more than one cell. In case we have more than one cells we can use the DCA analysis for filtering intended noises and countermeasures.

A very important information stored in the cells is the key for encryption and

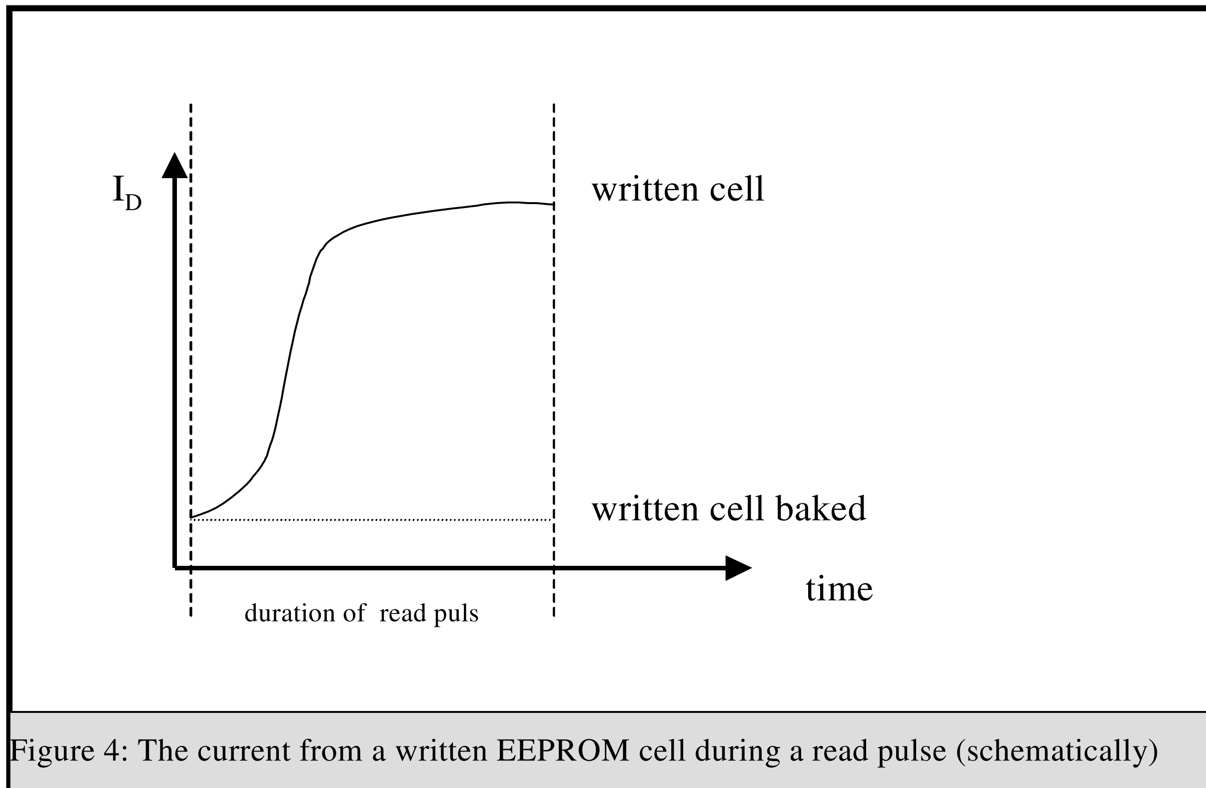

Figure 4: The current from a written EEPROM cell during a read pulse (schematically)

decryption (e.g. 3DES, RSA or ECC key). As an example it will be tried to estimate the key for a 3DES encryption. Before the 3DES will be started the key must be loaded in the register of the 3DES. It is assumed that the CPU can read the key from a EEPROM block 8 Bit wise (8 Bit CPU, It can be also extended to 16 bit or more). The reading of 8 bit will be done block for block until 64 bit is reached (8 times). The current in the power line VDD will be measured in the saturation of the curve (compare figure 4) for each block cycle (1 Byte). As seen in chapter 4 the written cells can only cause the current shape shown in figure 4 during a read operation. The second step is to bake the smartcard at 250℃ for 24 hours. After that, the current can be measured block for block at the same time during the read pulse as before. We know that each block has the logical state '1' stored in the EEPROM cells after baking. We also have no current coming from the EEPROM cells during the read pulse. Furthermore, the differences of the measured current is a size for the numbers of the '0' in a byte stored before baking.
For the calculation of the bits in a block (from the size) it is necessary to make a model. During the read cycle the current will be measured before baking in the saturation of all transistors involved. In this case of saturation, all involved transistors have fix channel resistors which are illustrated schematically as a block in figure 5. In this illustration, there are max. 8 resistors connected parallel and only one is connected serial during the read pulse duration. In case the current difference in the block is zero, all bits in the block were '1'. That is the trivial case.
The rest of the current can be calculated from following equation:

$$I_n = \frac{U}{\frac{R}{n} + R_{WR}}$$

Where

n Number of the bits which is '0' in a block (where n>0)
I_n Current from n written cells in a block
R Resistor in a block during saturation
R_{WR} Resistor from word line transistor involved
U Power supply in the block line

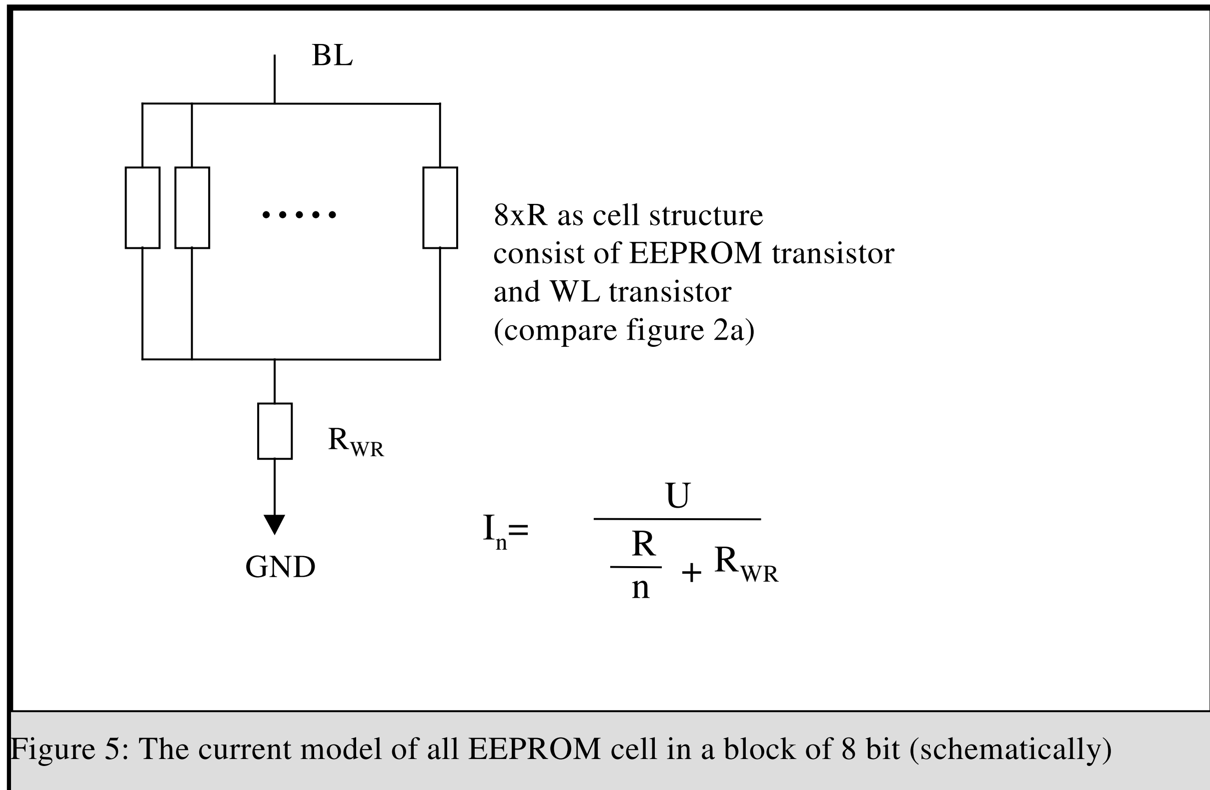

Figure 5: The current model of all EEPROM cell in a block of 8 bit (schematically)

According to the equation above: $I_1<I_2<...<I_8$. That means, we take the current differences from each block and sort them from low to high and compare them with the equation above. This leads to the estimation of the numbers of the bits being '0' in a block (e.g. if one bit is '0', we can have a block looking like 01111111 or 10111111 or 11011111 etc.). This DCA analysis is good for filtering the measured current from noises or/and integrated countermeasures after a baking process. This DCA analysis could also be performed without a baking process. In this case, it will be assumed that the smartcard has no noises and no countermeasures intended by the developer. Both methods of DCA analysis can only be used for reading out the contents of the EEPROM cells without being able to say something about the encryption.

6. Design rules for avoiding the DCA Analysis

The question is, how can we avoid the DCA analysis on smartcards which will be developed and used in the future. The second question is, who should test the countermeasures integrated by the designer. It is quite easy to define one of the design rules as exemple for avoiding the DCA analysis. Supposed, the circuit or smartcard should be designed to have 8 sense amplifier selected each time during a read pulse. As we know, the sense amplifier is always selected for the bits which are realized with positive charges (logical '0').

The other cells which have negative charges (as logical '1') must be connected to the dummy cells simulating the read operation as if they were written cells. Therefore we always have the same current during a read pulse duration for each block (e.g. if the content of the EEPROM cells is 01001111, 5 dummy cells must be enabled for the simulation). This leads to the same current for each block for avoiding DCA analysis. Such integrated countermeasures should be checked by an independent instance. In Europe and oversea are a lot of certification bodies which are empowered to monitor the tests performed by licensed evaluation facilities.

7. Conclusion and Discussion

There are two kinds of V_T parameters. One of them has negative charges (erased EEPROM cells) and the other has positive charges (written EEPROM cells). The positive charges change to negative charges during a bake process. For this reason, it is necessary to perform the DCA analysis. The conclusion of this paper can be given as followed:

- In case of countermeasures and noises integrated by the manufactures we coincidentally have to select one die for performing DCA analysis. In this case, it is necessary to perform DCA after a temperature storage.
- In case of no countermeasures and noises we coincidentally have to select one die for performing DCA analysis without temperature storage.
- The DCA analysis should be performed with a highest power supply with which the cryptographic chip (e.g smartcard) is still functioning well [4]. Usually the power supply range for the cryptographic chip is defined in the functional specification. During this DCA measuring the cryptographic chip should be clocked with a minimum frequency defined also in the functional specification in order to get more time for digitalization of the current consumption in saturation.

For the evaluation of such smartcard products, the DCA analysis should be performed on a coincidentally selected die of a wafer without thinking of the V_T parameter of the fabrication process. It is not necessary to perform DCA analysis on a specially selected die regarding the V_T parameter (worst case die) defined in [4].

Note: This paper reflects the opinion of the author only

8. Referenzen

[1] J. M. Portal, H. Aziza and D.Nee, EEPROM Memory: Threshold Voltage in Self Diagnosis, ITC International Test Conference, IEEE 2003

[2] O. Kocar, Hardwaresicherheit von Mikrochips in Chipkarten,1996 DuD, 7/96 Vieweg &Sohn, Wiesbaden.

[3] U. Feldmann, R. Kakoschke, M. Miura-Mattausch and G. Schraud, Concurrent Technology, Device, and Circuit Development for EEPROMs, Proc. Asis South Pacific design Auto. Conf., 1998/02, Page 123-128.

[4] Osman Kocar, DPA attacks on keys stored in CMOS cryptographic devices through the influence of the leakage behavior, International Association for Cryptologic Research (IACR), 2006/192

[5] Günter Zimmer, CMOS-Technologie, Oldenburg 1982