DPA[1] attacks on keys stored in CMOS cryptographic devices through the influence of the leakage behavior

by
Osman Kocar[2]

Abstract:
This paper describes the influences of the threshold voltage V_T on the leakage behavior of the dice after a fabrication process. By measuring the current consumption (leakage) on a CMOS cryptographic device like smartcard security controller and using the DPA analysis it is possible to make the key visible which is used during a cryptographic operation. Therefore, in this paper not only the security risks by using the smartcard security controller will be shown where no DPA attacks have been performed. Furthermore, it will be shown that the results of DPA analysis only on a coincidentally selected die cannot be representative for the whole production. Rather the DPA analysis must be performed on a particularly selected die with the smallest V_T parameter (worst case in the leakage behavior), so that the result for all other dice on the wafer (or for the whole production) can be considered as relevant. Thus, it will be shown that the test labs must use different methods regarding the DPA analysis in order to be able to cover the leakage behavior on all wafers of a production. For further re-evaluation of smartcards it is important that the manufacturer and the test labs can save time and costs by DPA measuring on the special selected worst case die.

1. Introduction to the DPA and side channel attack

The immense development of the technology of microchips clearly changed our behavior in society. This development has led to the fact that our life without silicon chips would be unimaginable. The technological progress, the miniaturization of microchips and the integrated measures against attacks also have 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 weaknesses in order to get the stored information from the chip. One of the technological weaknesses is the leakage behavior of the CMOS technology (Complimentary Metal Oxide Semiconductor). This leakage behavior can be used by an attacker in order to gain information stored in the microchip. This technological weakness is used today during a encryption operation (e.g.: 3DES-operation) to make parts or the whole key visible. This could be performed by measuring the current consumption of the cryptographic device during an encryption operation (3DES, RSA operation or elliptical curves). This method of getting keys by measuring the leakage is called Differential Power Analysis (DPA). The theory of the differential power analysis method (DPA) was developed first by P. Kocher [1]. With this well defined DPA you can make parts or the whole key visible saved in the microchip by measuring

[1] Differential Power Analysis
[2] Osman Kocar received M.S. 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.

the current consumption several times during a cryptographic operation and using the algorithm defined in [1]. That means you can calculate the key from the leakage behavior of the cryptographic device in the current consumption. In the last years the developer of the microchip realized this technological weakness and developed countermeasures integrated in the smartcards to mask the leakage behavior and to avoid such DPA attacks. The reason why today DPA analysis for each new developed cryptographic chip are still performed is to examine if the integrated countermeasures are effective. The question is whether the results of DPA analysis on a coincidentally selected die (cryptographic device) of a wafer can be representative for all wafers of a production. The answer for the above question will be the main issue of this article.

2. Leakage

What is the cause for leakage? The answer to this question lies in CMOS technology (Complimentary Metal oxide Semiconductor). Therefore it will be tried to explain the cause of the leakage by CMOS technology parameter of the transistors (N and P) without going into detail of the technology. If the CMOS inverter and its switch behavior is considered, it will be clear that the different N-channel transistors (NMOS) react differently to the input voltage Vin at different times for switching from ' 0 ' to ' 1 ' (turning on) and the opposite way (turning off). The same behavior can be observed for a P-channel transistors for the PMOS technology. Therefore there is a range on an inverter (figure 1) caused by a Vin signal during a transition, within this range one of the transistors is slowly turning on, the other is slowly turning off and a current flows from Vdd to Vss. This cross current (from Vdd to Vss) in figure 1 is called leakage. The mentioned range for

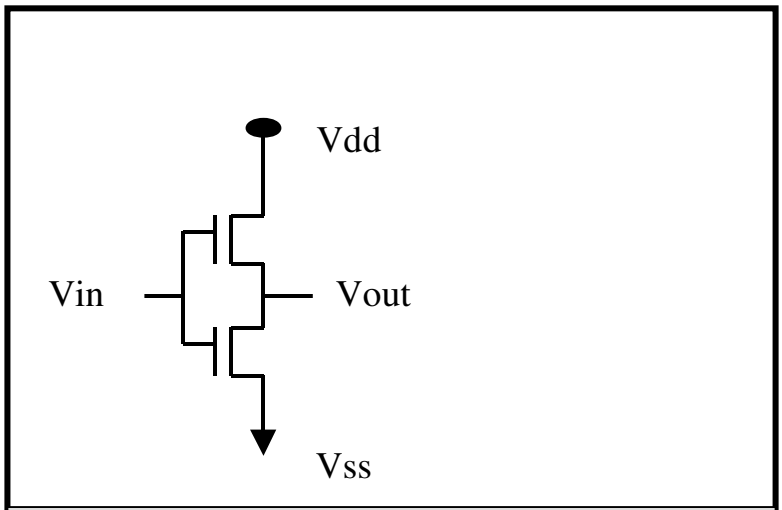

Figure 1: CMOS Inverter

the leakage depends on the threshold voltage V_T of the two transistors. It is emphasized that the threshold voltages concern only V_T on CMOS transistors, not the EEPROMS [3] (EEPROMS are also CMOS circuits but with another leakage behavior). This leakage current for a N-channel transistor (NMOS) is given in [5]:

$$I_N = \mu_N C_{ox} \frac{W}{L} V_t^2 \; e^{\frac{V_{GS}-V_T}{nV_t}} \left(1-e^{\frac{-V_{DS}}{V_t}}\right) \qquad \text{Equation 1}$$

where

u_N	electron carrier mobility
Cox	gate capacity
W/L	W is the channel width, L is the channel length
V_t	thermal voltage (V_t =kT/q)
V_T	threshold Voltage V_T
n	subthreshold swing coefficient
V_{DS}	voltage between drain and source
V_{GS}	voltage between gate and source

A similar equation can be indicated analog to a P-channel transistor (PMOS). The equation 1 shows that the leakage strongly depends on topology (W/L, diffusion parameter), on the threshold voltage (V_T), on supply voltage V_{DS} (and/or Vdd), and also on the temperature Vt (and/or T). The leakage increases linearly with the topological parameters in equation 1, while the leakage increases exponentially

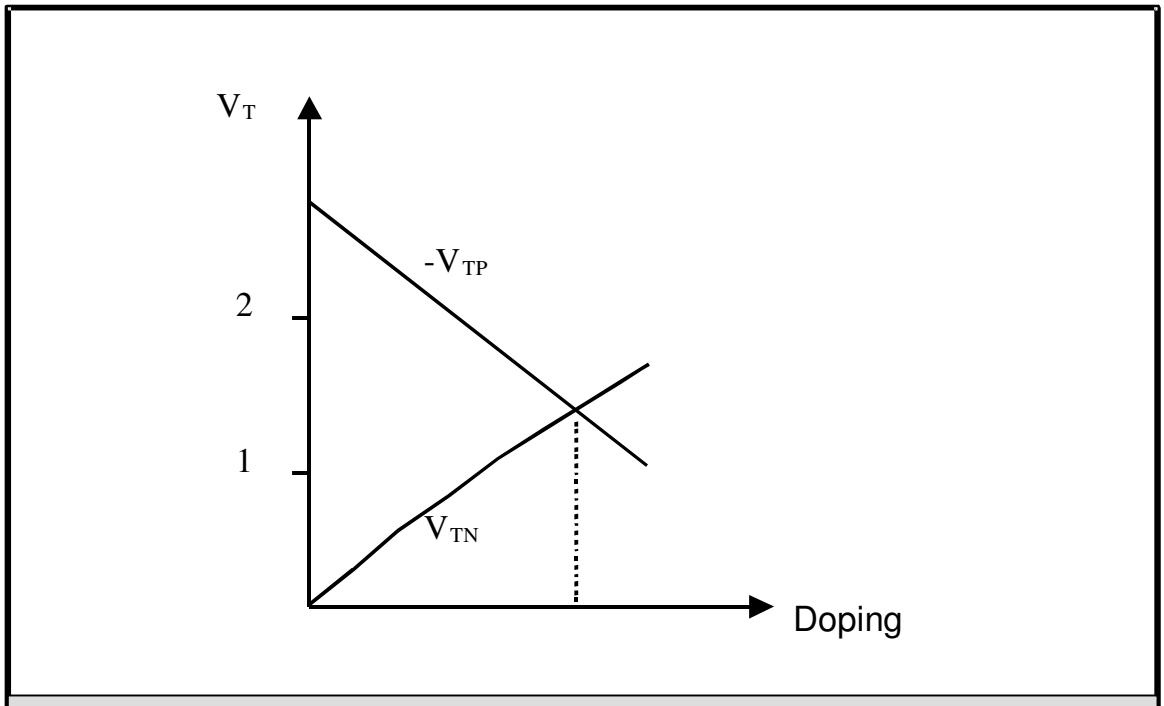

Figure 2: V_T as a function of well doping (doping only schematically)

with the remaining parameters above (see also [4] and [6]). The fact that the channel becomes conducting depends on its threshold voltage V_T of the transistors. The threshold voltage is a measure for the occurrence of the inversion layer in the channel of both CMOS transistors. Figure 2 illustrates the dependence of the V_T as a function of well doping only schematically. In figure 2 we also see that the threshold voltages of V_{TP} and V_{TN} can only be symmetrical at one point. This symmetry states that during one transistor switches on, the other switches off abruptly. Whether this symmetry for a given technology is applicable, remains still open. It is to be noticed that the leakage would not be expected if the

V_T had symmetrical leakage behavior for both transistors (P and N) illustrated in figure 2. Usually symmetry for a given CMOS process is not possible. It is only realizable at the cost of the yield. The larger the distance between V_{TP} and V_{TN} (figure 2), the higher is the leakage, which flows between Vdd and Vss (figure 1). In figure 2 is illustrated that the leakage is largest, if V_T is smallest in both transistors.

3. V_T Distribution on Wafer

On the one hand, according to Fick's law [2] the ion flow for the doping of the transistors depends on the coordinate of the die on the wafer and on the other hand, the fluctuations of the diffusion temperature affects the V_T during a diffusion process. That means we cannot expect identical values of V_T over a whole wafer, let alone over all wafer in a production. Therefore, each V_T of a die on a wafer should depend on diffusion geometry and on diffusion temperature. That means each individual die should have different threshold voltages ($V_{T)}$ because of their place on the wafer. In accordance to the experiences in the semiconductor industry the V_T distribution on a wafer is not constant, which is also explainable with Fick's law for the diffusion model [2]. It is a matter of fact that each die on the wafer has another V_T. If the measured V_T on a wafer (or lot) were illustrated graphically, it would look like a Gauss distribution for both V_{TP} and V_{TN} [2] (see also figure 7). Therefore each die has a different leakage behavior caused by the V_T differences on the wafer. That means the DPA analysis performed only on a coincidentally selected die can not be representative for whole wafers or productions. Rather the DPA analysis should be performed on particularly selected die with the smallest V_T parameter (worst case in the Leakage behavior), so that the results can be considered representative for all other dice on the wafer. Therefore the test labs must change their selection process for a die regarding the side channel analysis like DPA in order to be able to cover the Leakage behavior of all dice in a production.

4. Power Supply for DPA Measuring

Another important parameter for leakage forcing is the supply voltage (Vdd) with which DPA measuring will be performed on a die. The question is with which supply voltage DPA analysis should be performed. The answer to this question becomes clear, if we consider the leakage behavior of an CMOS inverter illustrated in figure 3 as a function of the threshold voltage Vin with different supply voltages (Vdd). Figure 3 shows the characteristic of a CMOS inverter and the leakage current Iq as a function of threshold voltage Vin in dependency on supply voltage (Vdd). The illustration in figure 3 is drawn schematically and shows the leakage distribution depending on supply voltage. Figure 3 shows that the leakage current increases exponentially with increasing supply voltage (also compare [2] and [4]). Therefore it is indispensable that the DPA analysis must be performed at the highest supply voltage defined in the functional specification of the cryptographic circuit (e.g smartcard) for well defined cryptographic DES operations (e.g. RSA operation, etc.) in order to force leakage and to increase the resolution of the measuring of the leakage current (compare figure 3).

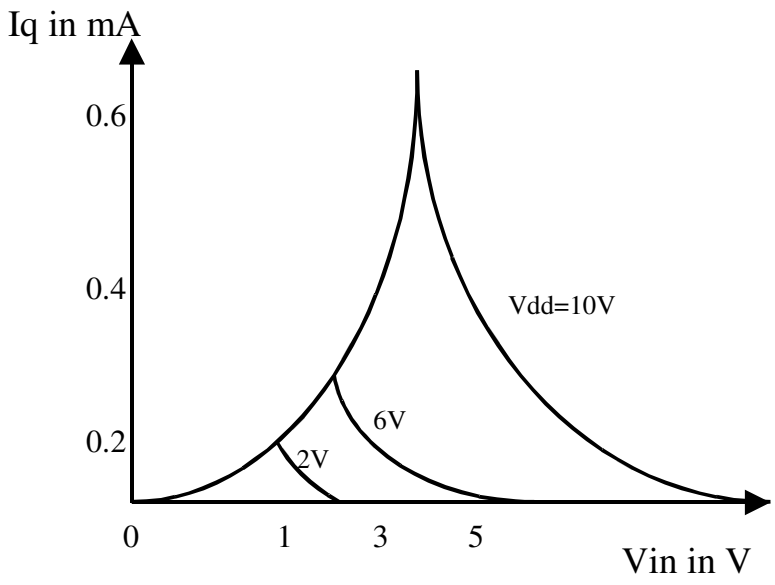

Figure 3: Iq Leakage as a function of Vin depending on Vdd

Additionally figure 3 shows that the leakage reacts very sensitively to changes of the supply voltage (e.g. from 2V to 6 V). This means the supply voltage at the cryptographic chip must be stabilized during a DPA measuring in order not to falsify the results of the measurement. If the supply voltage at the cryptographic chip is not stable, the leakage will strongly vary illustrated in figure 3.

5. Test Circuit for DPA Measurements

Knowing that the supply voltage of the smartcard must be stable in order not to falsify the Leakage behavior of the integrated circuit, two measuring methods should be discussed. One of them is the direct measuring on a pre-resistor as in figure 4 and the other one is the measuring with a stabilized power supply at the smartcard realized with a amplifier (figure 5). Before the measuring of the current consumption on a pre-resistor during a cryptographic operation (like DES) we have to consider three cases in the test circuit in figure 4: R1<<Ri, R1=Ri and R1>>Ri.

R1>Ri and R1=Ri: The two cases do not make sense due to the voltage divider of the pre-resistor. In this case the IC has not enough supply voltage (U1) for functioning.
R1<<Ri: In this case R1 must be selected so small that:

a) the supply voltage U1 at the IC is substantially non-varying
b) Ri becomes not comparable with R1 during a cryptographic operation
c) the measuring voltage at R1 (pre-resistor) is not too low.

On the one hand we know from figure 3 that the Leakage reacts very sensitively to changes of the supply voltage, on the other hand we know from figure 4 that the internal resistance Ri of the IC varies during an operation. The internal

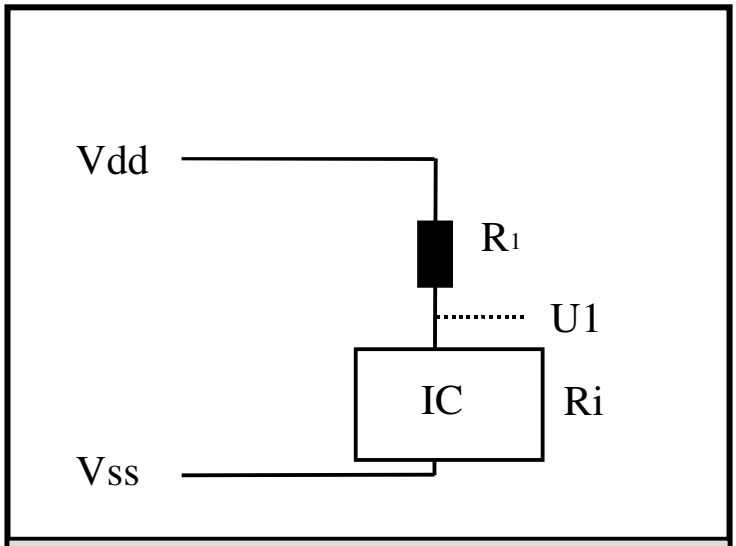

Figure 4: DPA test circuit on a pre-resistor R_1

resistance Ri of IC changes while switching the CMOS transistors on and off. Therefore the supply voltage U1 must change according to Ohm's law. That means it is impossible to keep the supply voltage U1 constant at the IC. Hence, the Leakage is varying with the supply voltage and the current on R1 cannot be measured exactly. If R1 is chosen too small to keep the varying of U1 very small, we would make a digitalization failure in this case (1bit measuring failure on a smaller voltage is bigger than 1 Bit measuring failure on a higher voltage on the pre-resistor R1). Due to the aspects mentioned above the pre-resistor R1 must be selected in such a manner that the measuring failure is minimized. The question is how do we know that the measuring failure can be considered small enough? It is a fact that the supply voltage U1 will always vary more or less during a cryptographic operation. As long as U1 varies, the leakage measurement is not precise. Therefore which fluctuation size of the supply voltage U1 can be accepted is unclarified. It must be expected that the evaluator justifies why the selected pre-resistor is suitable for the performing of a DPA measuring.

If the test circuit illustrated in figure 5 is used, we will not need to consider as many aspects as in the first method in figure 4. Figure 5 shows a test circuit with

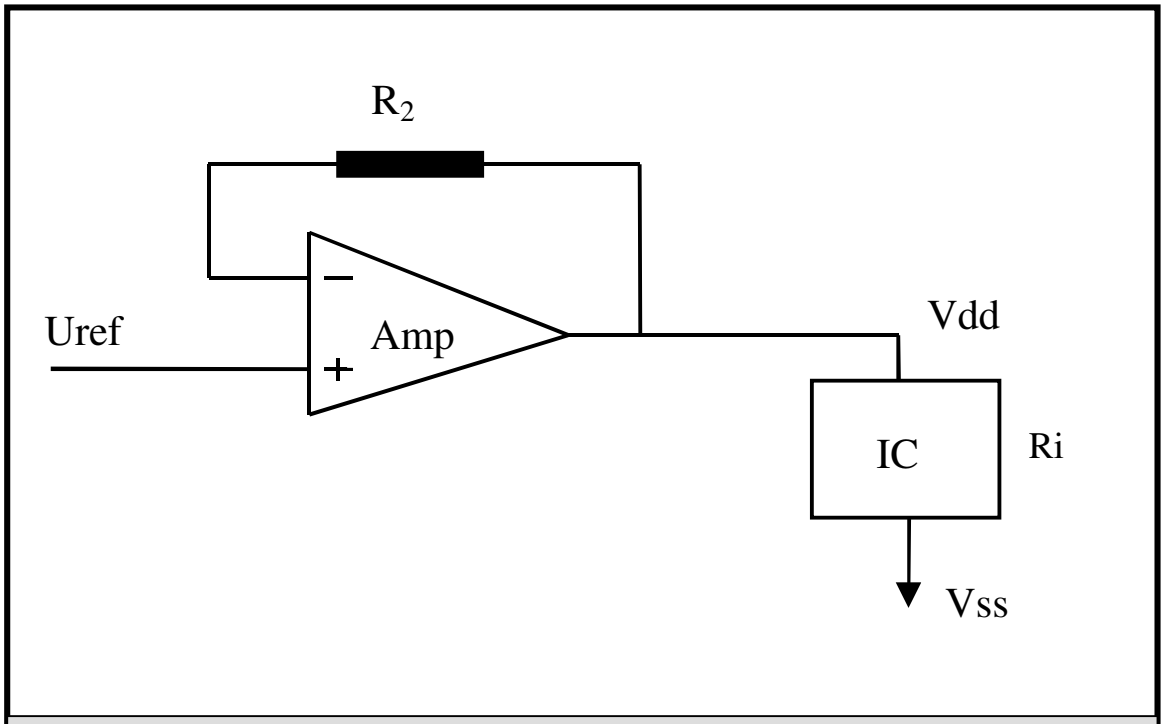

Figure 5: DPA test circuit on R2 with a amplifier

an amplifier used for the stabilization of the supply voltage on the cryptographic circuit (here IC) and for measuring the leakage on the resistance R2. If the reference voltage Uref (in the test circuit in figure 5) as power supply defined in the technical specification is set to the maximum, Vdd will be set automatically to Uref. Even if Ri changes during an cryptographic operation, the Vdd will automatically adjust to the stabilized Uref. The power supply Vdd is always stable as long as Uref is stable. The Vdd stabilization is independent from fluctuations of Ri. Furthermore R2 can be selected in such a manner that the voltage for current consumption at R2 is large enough to avoid a digitalization failure. The disadvantage of this test circuit (figure 5) is that we have to choose an operation amplifier (amp) which input regulation (here ' - ' input) is very fast and which output can perform enough current for the IC used for DPA analysis. The experiments made show that the ratio of the regulation speed to the IC clock frequency must have the factor 100 at least. The noise must be filtered before starting the measuring of the power signals for side channel attacks in both test circuits, because the signal to be measured can be extremely small. Additionally, the noise will be reduced during sampling the power signals by the A/D-converter used. This noise behavior is published in the article in [7]. Furthermore it should be checked whether it is advantageous to measure the small signal with an active probe.

6. Leakage at Temperature

The question is at which temperature the DPA measuring should be performed, because the leakage also strongly depends on the temperature (equation 1) (compare with [4] -- [6]). The leakage current I_N of a N-channel transistor, (NMOS) illustrated schematically in figure 7, increases exponentially with temperature [6]. There also exist structures with smallest NMOS transistors, where the leakage increases with temperature, too (measured on a transistor with parameters 45 nm and V_T=200mV in [8]). These measures also show that the leakage increases exponentially, although in this structures smartcards do not exist at this time. The experiments show that the leakage current increases not only with decreasing V_T exponentially, but also with increasing temperature [8]. Other experiments also show that V_T decreases with increasing temperature. That means that the leakage current increases exponentially [4]. Therefore leakage measuring on smartcards should be performed at higher temperatures, defined in the functional specification, in order to force leakage and to show that the integrated countermeasures are effective against DPA attacks.

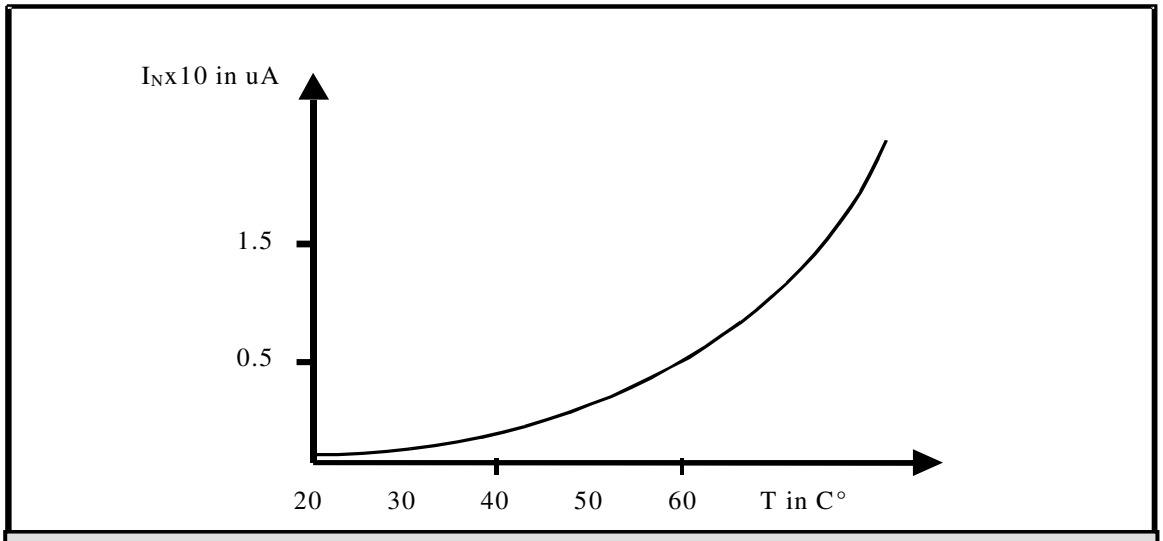

Figure 7: Leakage I_N as a Function of Temperature C° (schematically)

7. Leakage Coverage on Smartcard Evaluations

The dice have different V_T parameters on the Wafers and therefore have different leakage behaviors (chapter 3). The question is whether it is appropriate to perform the DPA measuring on a coincidentally selected die to cover the whole leakage behavior for all dice of the wafers (or lots) for the smartcard evaluation. The answer to the question above can only be 'No'. The illustration in figure 7 is drawn schematically and shows the V_{TN} distribution (accordingly V_{TP}) of a lots (consisting of several wafers) as a bar diagram that looks like a Gauss distribution for V_{TN} (accordingly for V_{TP}). These V_{TN} distribution have a min and a max value belonging to a die (or dice) still functioning. Therefore there are values like V_{TNMin}, V_{TNNom} and V_{TNMax} in each V_T distribution. Similar considerations also lead to V_{TPMin}, V_{TPNom} and V_{TPMax} for a P-channel transistor (PMOS). In principle the

V_{TNNom} and V_{TPNom} are defined in such a manner that the yield on good dice has a maximum on the wafers. As you can see we have a V_T matrix. Hence, one DPA measuring on a coincidentally selected die cannot cover all leakage behavior on the wafer caused by the V_T matrix. Which combination of the matrix is applicable for a DPA measuring depends on the countermeasures integrated by the manufacturer. Therefore, two cases for the leakage coverage must be considered: in one case the circuit has countermeasures and in the other case the circuit has no countermeasures. At this time all smartcards to be certified have integrated countermeasures against DPA attacks regarding leakage behavior. For this reason, the manufacturer try to mask the leakage behavior of the smartcard. Whether the countermeasure are effective or not, can be examined by a DPA analysis on a particularly selected cryptographic chip (die). The selection of the dice must be done in such a manner that the V_T of the die has the smallest V_Ts (V_{TN} and V_{TP}). Knowing from chapter 2 that the die with the smallest V_Ts (V_{TNmin} and V_{Tpmin}) have a higher leakage and this die is representing the worst case in the leakage behavior. If, after a DPA analysis, it is not possible to make the key (or parts of it) saved in the smartcard and used during a cryptographic operation on a worst case die visible, it makes no sense to perform a DPA analysis on another die again, because we know that the other dice have the same or less leakage.

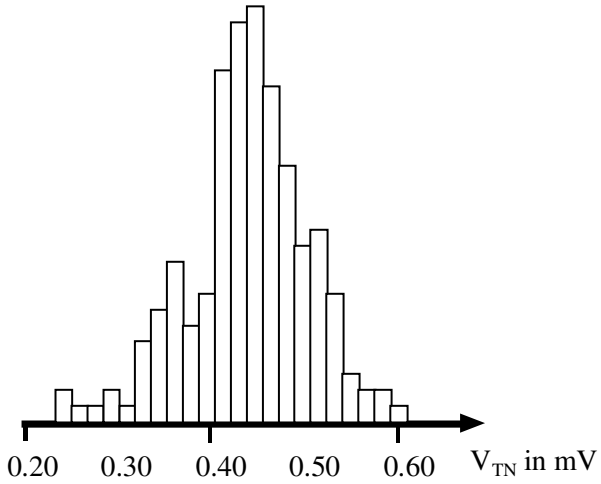

Figure 7: V_{TN} Distrubation from several Wafer

This DPA analysis performed on a worst case die states that the manufacturer with a predefined V_T can produce the same TOE (Target of Evaluation) in all production sites without performing the DPA analysis again for evaluation or re-evaluation. This approach brings immense benefits for saving time and costs for the manufacturer and the evaluation facilities. This leads less evaluation costs for the manufacturer and they can offer the smartcards competitively and act on the market.

8. Conclusion and Discussion

There are different V_T parameter after a fabrication process causing different leakage behaviors of the dice. For this reason, it is necessary to perform the DPA analysis. The conclusion of this paper can be given as following:

- In case of countermeasures integrated by the manufactures we have to select one die according to worst case conditions regarding to the thereshold voltage parameter (V_{TNmin}, V_{TPmin}) for performing DPA analysis. This specially chosen die represents the worst case in the behavior of the leakage. If the DPA analysis is performed on this specially selected die having no weakness, the manufacturer can produce in all production sites with the same process parameter without performing the DPA analysis again for further evaluations or re-evaluations by test labs.
- The DPA analysis should be performed with a highest power supply with which the cryptographic chip (e.g smartcard) is still functioning well (chapter 4). Usually the power supply range for the cryptographic chip is defined in the functional specification. During this DPA measuring the cryptographic chip should be clocked with a minimum frequency defined in the functional specification in order to get more time for digitalization of the current consumption (leakage signal) and for the documentation of the measured value.
- The leakage current depends on the temperature exponentially (higher temperature means higher leakage). Furthermore the DPA measuring should be performed at the highest temperature defined in the functional specification. During this measuring the temperature should be kept constant. It is recommended to perform the DPA measuring at two temperatures (at room and higher temperature) in order to compare the results of both analysis, because we still have no experience with the results of the two temperatures.
- For the leakage measuring, as we discussed in chapter 5, the test circuit defined in figure 5 with an amplifier has certain advantages. In this test circuit the resistor R2 should be chosen in such a manner that the voltage drop on it is not too low. Thus, the voltage drop can be selected by varying the resistance freely. The input of the operation amplifier (' - ' input) must be regulated fast and the output must be able to perform enough current for the IC used for the DPA analysis. The experiments made, show that the ratio of the regulation speed to the IC clock frequency must have the factor 100 at least. The noise of the test circuit and the noise caused by the equipment for digitalization must be checked and filtered during the DPA measuring, because the signal to be measured can be extremely small.

At present time, for the evaluation of such smartcard products, the DPA analysis is performed on a coincidentally selected die of a wafer without thinking of the V_T parameter of the fabrication process. In the future the DPA analysis should be performed on a specially selected die regarding the V_T parameter (worst case die) in order to cover the leakage behavior for a defined CMOS process for all production sites.

Acknowledgement: This work has been supported by my wife R. Bauer-Kocar and it reflects the opinion of me (the author) only.

9. Reference

[1] P. Kocher, J. Jaffe and B. Jun, *Differential Power Analysis*, Proceedings of Advances in Cryptology-CRYPTO'99, Springer-Verlag, 1999, pp. 388-397

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

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

[4] Yan Zhang, Dharmesh Parikh, Kathik Sankaranarayanan, Kevin Skadron and Mircea Stan, HotLeakage: A Temperature-Aware Model of Subthreshold and Gate Leakage for Arcitects, University of Virginia, March 2003

[5] Antoni Ferre and Joan Figuras, On Estimating Leakage Power Consumption for Submicron CMOS Digital Circuits, Universitat Politecnica de Catalunya, Diagonal 647, 08028 Barcelona

[6] Prof. Wayne Burleson and Ning Wenig, Leakage Power Control and Estimation, from a presentation

[7] Thomas S. Messerges and Ezzy A. Dabbish (Motorola labs), Robert H. Sloan (University of Illimonis at Chicago), Investigation of Power Analysis Attackt on Smartcards, USENIX , May 10-11, 1999

[8] Volkan Kursun and Zhiyu Liu, Wide Temperature Spectrum Low Leakage Dynamics Circuit Tecnnique for Sub-65nm CMOS Technologies, Proceedings of the IEEE International Symposium on Circuits and Systems, May 2006.