# Differential Power Analysis Attacks Based on the Multiple Correlation Coefficient

Xiaoke Tang[1,a], Jie Gan[1,b], Jiachao Chen[2,c], Junrong Liu[3,d]

[1]Beijing smartchip Microelectronics Technology Company Limited, China

[2]Shanghai Jiao Tong University, China

[3]Shanghai Viewsource Information Science and Technology Company, China

[a]tangxiaoke@sgitg.sgcc.com.cn

[b]ganjie@sgepri.sgcc.com.cn

[c]cjc87267137@sjtu.edu.cn

[d]junrong.liu@viewsources.com

**Keywords:** side-channel attack, power analysis attack, DPA, second-order DPA, CPA, MCPA, AES.

**Abstract.** In this paper we research a new power analysis attack method: the differential power analysis attacks based on the multiple correlation coefficient (MCPA). This attack method is based on statistical theory that multiple linear regression. Conditions of the MCPA method of attack are weaker than ones of CPA attacks. In this paper, we indicate that MCPA attacks have same effect with CPA attacks in this weak condition. We perform the simulated attacks and the practical attacks for the two kinds of attack methods to verify this conclusion. The results show that the conclusion is correct for the first-order DPA. We also describe the CPA attacks using simple linear regression model for comparison of two attack methods. The experiments results show that this chosen traces attack is stronger than the previous methods.

## Introduction

Classical cryptanalysis of cryptographic algorithms is to find out secret key information only through mathematical computation or statistical techniques. But on the other hand, these algorithms have to be implemented in a specific cryptographic device, and will leakage some physical information such as timing information, power consumption, or electromagnetic radiation. The side-channel attacks are a class of physical attacks that allow the extraction of the leakage information from cryptographic devices.

Power analysis attacks are the most effective and the most easily implemented side-channel attacks methods. Power analysis attacks were divided into SPA (simply power analysis) and DPA (differential power analysis). SPA is generally based on looking at and interpreting the visual representation of the power consumption during cryptographic operations. DPA are the most popular type of power analysis attacks which use statistical analysis.

The DPA attacks technique explores weaknesses of allowing an attacker to extract the secret of a device by monitoring its power leakage, if no special countermeasures are taken. A successful DPA attack is subject to two conditions: 1) there exists an intermediate variable in the implementation that is correlated with the power consumption and 2) this variable can be predicted with knowledge of the plaintext (or ciphertext) and by guessing a small part of the key and possibly other constants. Currently, there are four main statistical methods used in DPA attacks: difference of means [1, 2], distance of means [5], correlation coefficient [3] and generalized maximum-likelihood test [4]. Among them, the DPA attacks based on the correlation coefficient are the most effective one.

The power leakage model of CPA is that the (instantaneous) power consumption $P$ is linearly related to Hamming weight of processing data. But in practice, this linear relationship is not accurate. In this paper, we assume that processing data with same Hamming weight will consume same power. Under this power leakage model, we researched a new power analysis statistics method: Differential Power Analysis Attacks based on the multiple correlation coefficient (MCPA). We indicate that MCPA attacks have same effect with CPA attacks in this weak condition. We perform the simulated attacks and the practical attacks for this kind of attack. The experiments results show that this chosen traces attack is stronger than the previous methods.

## Statistics Theory

**Simple Linear Regression.** Let $x_1, x_2, \ldots, x_n$ be specific setting of the predictor variable and $y_1, y_2, \ldots, y_n$ be the corresponding values of response variable. We assume that $y_i$ is the observed value of the random variable $Y_i$, which depends on $x_i$ according to the following model:

$$Y_i = \alpha x_i + \beta + \epsilon_i. \qquad (1)$$

Here $\epsilon_i$ is a random error with $E(\epsilon_i)=0$ and $Var(\epsilon_i)=\sigma^2$.

We use the least squares method to fit the model. We look at the deviations between the observed $y_i$'s and the corresponding points on the straight line $y=\alpha x+\beta$:

$$y_i - (\alpha x_i + \beta) \ \ (i = 1,2,\ldots,n). \qquad (2)$$

For the fit to be good, these deviations should be small. We use the sum of squared deviations:

$$Q = \sum_{i=1}^{n} [y_i - (\alpha x_i + \beta)]^2. \qquad (3)$$

as an overall measure of distance of the data points from the fitted line; the smaller the value of Q, the better the fit. The lease squares (LS) method gives the best fitting straight line in the sense of minimizing Q. The values $\alpha$ and $\beta$ that minimize Q are referred to as the LS estimates and denoted by $\hat{\alpha}$ and $\hat{\beta}$, respectively. We have:

$$\hat{\alpha} = \frac{S_{xy}}{S_{xx}}, \qquad \hat{\beta} = \bar{y} - \hat{\alpha}\bar{x} \qquad (4)$$

Then the equation

$$\hat{y} = \hat{\alpha}x + \hat{\beta} \qquad (5)$$

is an estimate of the true regression line.

We denote the fitted values of yi by $\hat{y}_i$ given by

$$\hat{y}_i = \hat{\alpha}x_i + \hat{\beta} \qquad (6)$$

The residuals

$$e_i = y_i - \hat{y}_i = y_i - (\hat{\alpha}x_i + \hat{\beta}), i = 1,2,\ldots,n \qquad (7)$$

are used to evaluate the goodness of fit of the LS line. The $Q_{min} = \sum e_i^2$ obtained using the LS method is called the error sum of squares (SSE).

The total sum of squares (SST) which measures the variability of the yi's around $\bar{y}$ can be denoted by

$$ST = \sum_{i=1}^{n}(y_i - \bar{y})^2 = \sum_{i=1}^{n} y_i^2 - \frac{1}{n}\left(\sum_{i=1}^{n} y_i\right)^2 = S_{yy} \qquad (8)$$

We decompose the SST:

$$SST = \sum_{i=1}^{n}(y_i - \bar{y})^2 = \sum_{i=1}^{n}(\hat{y}_i - \bar{y})^2 + \sum_{i=1}^{n}(y_i - \hat{y}_i)^2 + 2\sum_{i=1}^{n}(\hat{y}_i - \bar{y})(y_i - \hat{y}_i) \qquad (9)$$

The second term is SSE. the first term is called the regression sum of squares (SSR), which represents the variation in y that is accounted for by regression on x. The third is equal to 0 we can prove. This yields the identity

$$SST=SSR+SSE \qquad (10)$$

The ratio

$$r^2 = \frac{SSR}{SST} = 1 - \frac{SSE}{SST} \qquad (11)$$

represents the proportion of variation in y that is accounted for by regression on x; it is called the coefficient of determination.

Theorem1 [6]: The sample correlation coefficient r which measures linear association between random variable x and y equals to the square root of $r^2$. The sign of r is the same of $\hat{\alpha}$.

**Multiple Linear Regressions.** Similar to simple linear regression, we shall regard the response variable as random and the predictor variables as nonrandom. The data for multiple regression consist of n vectors of observations $(x_{i1}, x_{i2}, \ldots, x_{im}; y_i)$ for $i$=1, 2, …, $n$. We regard $y_i$ as the observed value of the random variable $Y_i$ which depends on fixed predictor values $x_{i1}, x_{i2}, \ldots, x_{ik}$ according to the following model:

$$Y_i = \alpha_1 \cdot x_{i1} + \alpha_2 \cdot x_{i2} + \cdots + \alpha_m \cdot x_{im} + \beta + \epsilon_i \tag{12}$$

where $\epsilon_i$ is a random error with $E(\epsilon_i)=0$ and $Var(\epsilon_i)=\sigma^2$.

As simple linear regression, we use least squares method to fit the model. The goodness of fit of the model is called the coefficient of multiple determination:

$$r^2 = \frac{SSR}{SST} = 1 - \frac{SSE}{SST}, \tag{13}$$

The positive square root of $r^2$,

$$r = +\sqrt{r^2} = \sqrt{1 - \frac{SSE}{SST}}, \tag{14}$$

is called the multiple correlation coefficient.

## Differential Power analysis attacks

**Power Leakage Model.** Let H($x$) denote the Hamming weight of $x$. A simple model for power leakage is the (generalized) Hamming-weight model. This model assumes that the (instantaneous) power consumption $P$ is linearly related to Hamming weight:

$$P\,(t) = \alpha \cdot H(w) + \beta \tag{15}$$

for some hardware-dependent constants $\alpha$ and $\beta$, and where $w$ is the $n$-bit word manipulated at time period $t$.

Our research has confirmed that this relationship is roughly linear. Experiments show that $\alpha$ with higher Hamming weight is bigger than which with lower Hamming weight. For other cases, such as encryption algorithm using XOR operation, the situation becomes more complicated.

For the attacks described in this paper, we assume that processing data with same Hamming weight will consume same power. This condition is weaker than which power consumption is linearly related to Hamming weight.

**Simple Linear Regression Description of CPA.** Power leakage model of differential power analysis attacks based on the correlation coefficient (CPA) assumes that the instantaneous power consumption $P$ is linearly related to Hamming weight. For description simply, we transform (15) to

$$p_i = \alpha \cdot h_i + \beta \tag{16}$$

where $h_i$ represents the Hamming weight of the intermediate data result at time $i$. According to the description of simple linear regression, we let $h_1, h_2, \ldots, h_n$ be specific setting of the predictor variable and $p_1$, $p_2, \ldots$, $p_n$ be the corresponding values of response variable. We assume that $p_i$ is the observed value of the random variable $P_i$, which depends on $h_i$ according to the following model:

$$P_i = \alpha \cdot h_i + \beta + \epsilon_i. \tag{17}$$

Here $\epsilon_i$ is an electronic noise power consumption with $E(\epsilon_i)=0$ and $Var(\epsilon_i)=\sigma^2$.

We use lease squares (LS) method to fit the simple linear regression model and use sample correlation coefficient $r$ to denote the fitted values.

$$r = \pm\sqrt{r^2} = \pm\sqrt{\frac{SSR}{SST}} = \pm\sqrt{1 - \frac{SSE}{SST}}, \tag{18}$$

Another method of compute $r$ is:

$$r = \frac{\sum_{i=1}^{n}(h_i - \bar{h}) \cdot (p_i - \bar{p})}{\sqrt{\sum_{i=1}^{n}(h_i - \bar{h})^2 \sum_{i=1}^{n}(p_i - \bar{p})^2}}, \tag{19}$$

This method of power analysis attack is called differential power analysis attacks based on the correlation coefficient (CPA). The detail descriptions see [3, 5].

## Differential Power analysis attacks based on the multiple correlation coefficient

**Power Leakage Model.** In last section, we mentioned that the (instantaneous) power consumption $P$ is roughly linearly related to Hamming weight. We measured the smartcard with AES algorithm. We measure average power consumption according to same Hamming weight. The result see Fig. 1.

The result shows that $\alpha$ with higher Hamming weight is smaller than which with lower Hamming weight. An explanation comes from the fact that the measured power consumption is instantaneous one (the peak value of the power trace). Another comes from characteristics of CMOS circuits.

For our power leakage model, we assume that processing data with same Hamming weight will consume same power:

$$p_i = \alpha_{date=di} \cdot h_i + \beta, \quad h_i \in \{0,1,\dots,m\} \tag{20}$$

where $m$ is the length of processing data.

This condition is weaker than which power consumption is linearly related to Hamming weight. The model is more accurate description of relationship between instantaneous power consumption and Hamming weight of processing data.

**Differential Power analysis attacks based on the multiple correlation coefficient.** In CPA, it uses simple linear regression to fit the specific of the predictor variable and the corresponding of the response variable, and use correlation coefficient r to denote goodness of fit. In our attacks, we use multiple linear regression to descript our attack model.

In formula (20), for each of $d_i$, we define $x_{i0}$, $x_{i1}$, …, $x_{im}$:

$$x_{ik} = \begin{cases} 1, & \text{if } h_i = k \\ 0, & \text{otherwise} \end{cases} \; ; k = 0,1,\cdots,m \tag{21}$$

Therefore we get a multiple linear regression model:

$$P_i = \alpha_0 \cdot x_{i0} + \alpha_1 \cdot x_{i1} + \cdots + \alpha_m \cdot x_{im} + \beta + \epsilon_i \tag{22}$$

where $P_i$ is the random variable of the observed value $p_i$ .

We will use multiple linear regression model to fit the predictor variable and the response variable. Note that this is a kind of special model which consist of m+1 simplest possible model:

$$P_i = \alpha_k + \beta + \epsilon_i \; ; \; k = 0,1,\cdots,m \tag{23}$$

For each simplest possible model, we assume that the number of specific of the predictor variable is $n_k$. And we have

$$\sum_{k=0}^{m} n_k = n. \tag{24}$$

In the simplest possible model the $x_{ik}$'s are ignored and all $P_i$'s have the mean:

$$\bar{p}_k = \frac{1}{n_k} \sum_{i=1}^{n_k} p_{d_i=k}. \tag{25}$$

It is easily seen that least square estimate of the common mean is $\bar{p}_k$. Therefore the corresponding $Q_{min}$ (the least square) equals

$$\sum_{i=1}^{n_k} \left(p_{d_i=k} - \bar{p}_k\right)^2 = SST_{h_i=k} = SSE_{h_i=k}. \tag{26}$$

Therefore in our multiple linear regression model, we can calculate each SSE of the simplest possible model. Then the SSE of multiple linear regression model is the sum of each SSE of the simplest possible model.

$$SSE = \sum_{k=0}^{m} SST_{h_i=k} = \sum_{k=0}^{m} \sum_{i=1}^{n_k} \left(p_{h_i=k} - \bar{p}_k\right)^2. \tag{27}$$

We can calculate the multiple correlation coefficient $r$ by following formula:

$$r = \sqrt{r^2} = \sqrt{1 - \frac{SSE}{SST}}, \tag{28}$$

here

$$SST = \sum_{i=1}^{n} (p_i - \bar{p})^2 \; ; \qquad \bar{p} = \frac{1}{n} \sum_{i=1}^{n} p_i \tag{29}$$

## Comparisons with the CPA Attacks

**Comparisons with the CPA Attacks.** In this section, we shall prove that MCPA attacks have same attack effect with CPA attacks in the power leakage model that the (instantaneous) power consumption $P$ is linearly related to Hamming weight. We know that the power leakage model of CPA is

$$P_i = \alpha \cdot h_i + \beta + \epsilon_i. \tag{30}$$

And correlation coefficient is

$$r_{CPA} = \frac{\sum_{i=1}^{n}(h_i - \bar{h})\cdot(p_i - \bar{p})}{\sqrt{\sum_{i=1}^{n}(h_i - \bar{h})^2 \sum_{i=1}^{n}(p_i - \bar{p})^2}}. \tag{31}$$

Now we will calculate multiple correlation coefficient of MCPA attacks in this linear power leakage model. For each simplest linear regression, formula (26) transform to

$$SSE_{h_i=k} = \sum_{i=1}^{n_k}\left(p_{h_i=k} - \bar{p}_k\right)^2 = \sum_{i=1}^{n_k} \epsilon_{h_i=k}^2. \tag{32}$$

Therefore

$$SSE = \sum_{k=0}^{m} SSE_{h_i=k} = \sum_{k=0}^{m}\sum_{i=1}^{n_k} \epsilon_{h_i=k}^2 = \sum_{i=1}^{n} \epsilon_i^2. \tag{33}$$

So according to theorem 1,

$$r_{CPA} = \pm r_{MCPA} = \pm\sqrt{r_{MCPA}^2} = \sqrt{1 - \frac{SSE}{SST}}. \tag{34}$$

**Simulation Attacks Experiment.** Now we perform a simulated CPA attack and a simulated MCPA attack on a specific cryptographic algorithm. We calculate the correlation coefficients and the multiple correlation coefficient in the simulation attacks. We choice the AES[7] algorithm as our attack target and compare the attack effect of two kinds of attack methods.

In attacks, we have performed a generated a vector $\vec{d}$ that contains all input values for the attacked AES S-box, *i.e.* $\vec{d} = (0,1,\cdots,255)'$. Subsequently, we have mapped these input values to simulated power consumption values according to

$$p_i = HW\left(S(d_i \oplus RealKey)\right);\ 0 \le i \le 255 \tag{35}$$

Obviously, the power consumption is linearly related to Hamming weight in this simulated power leakage model. After having simulated $p_i$, we have created hypothetical power consumption values for all keys based on the hamming weight model.

$$h_{i,key} = HW\left(S(d_i \oplus Key)\right);\ 0 \le i \le 255, 0 \le key \le 255 \tag{36}$$

Define vectors:

$$\vec{p} = (p_0, p_1, \cdots, p_{255})'$$
$$\vec{h}_{key} = \left(h_{0,key}, h_{1,key}, \cdots, h_{255,key}\right)';\ 0 \le key \le 255 \tag{37}$$

In order to determinate the correlation coefficient and the multiple correlation coefficient, we have performed simulated CPA attack and MCPA attack.

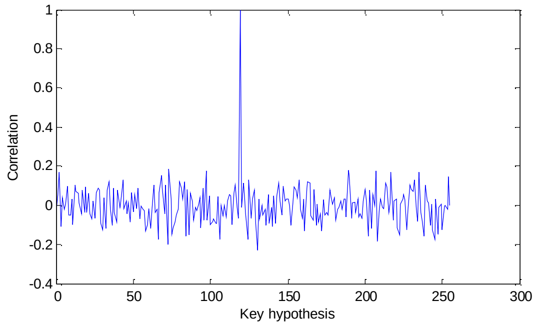

Figure 1. The correlation coefficients occurring in a CPA attack.

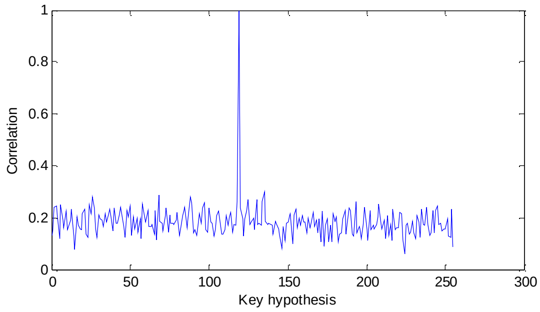

Figure 2. The correlation coefficients occurring in a MCPA attack.

Subsequently, we have determined the correlation coefficient between each $\vec{h}_{key}$ and $\vec{p}$ according to formula 19. Fig. 1 shows the result of CPA attack. Similarly, we have determined the multiple correlation coefficients between each $\vec{h}_{key}$ and $\vec{p}$ according to formula 28. Fig. 2 shows the result of MCPA attack. The result shows that it has almost same correlation coefficients in CPA and MCPA. This result is consistent with the previous analysis only a negative correlation coefficient exists in CPA attack and the correlation coefficients in MCPA attack is little larger than ones in CPA attack for error key hypothesis. The reasons for this result we will explain in later section.

**Practical Attacks Experiment.** We have performed CPA and MCPA attacks target an 8-bit microcontroller executing an AES software implementation. Fig. 3 and Fig. 4 show the attack results for the correct key hypothesis in the MCPA and CPA attacks, respectively. The results show that the correlation coefficients in MCPA attack are slightly larger than ones in CPA attack. Fig. 5 and Fig. 6 show the attack results for the error key hypothesis in the MCPA and CPA attacks, respectively. The results show that the correlation coefficients in MCPA attack are also slightly larger than ones in CPA attack.

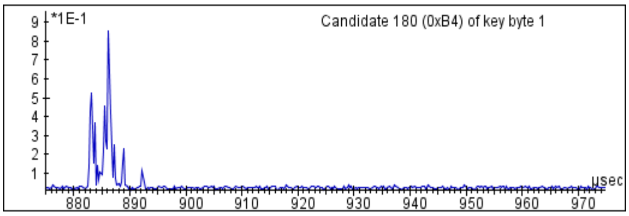

Figure 3. The plot for the correct key hypothesis in MCPA attacks.

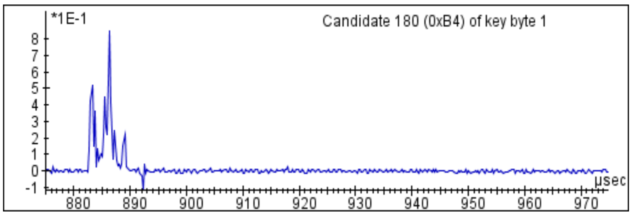

Figure 4. The plot for the correct key hypothesis in CPA attacks.

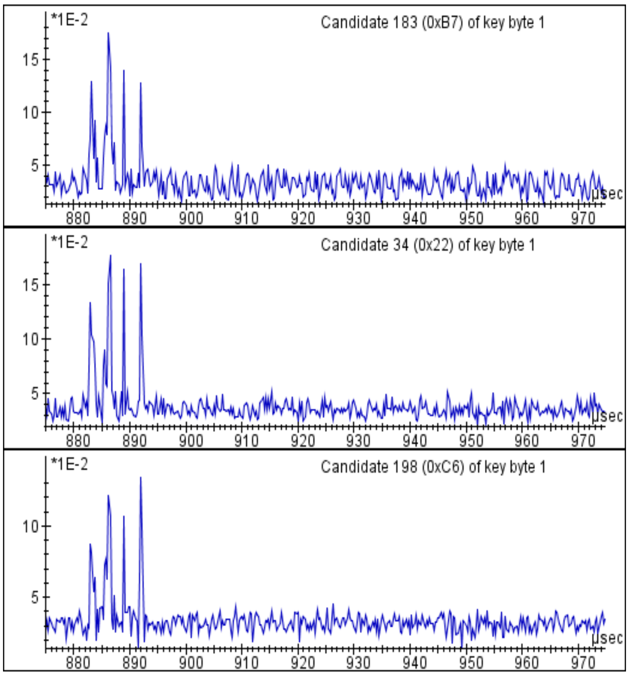

Figure 5. Three plots for the error key hypothesis in MCPA attacks.

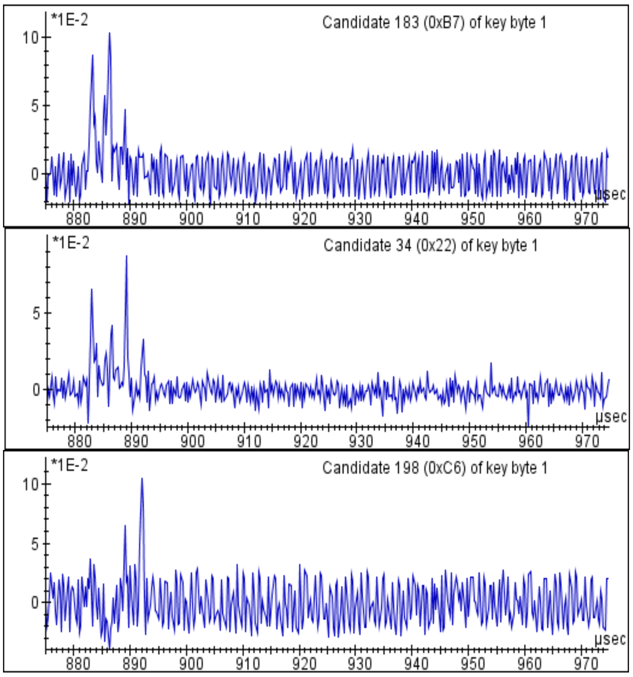

Figure 6. Three plots for the error key hypothesis in CPA attacks.

**Result Analysis.** In simulated attacks, the instantaneous power consumption is accurate linearly related to Hamming weight. The experiment result shows that two types of attacks is almost the same correlation coefficients only is a negative correlation coefficient exists in CPA attack and the correlation coefficients in MCPA attack is little larger than ones in CPA attack for error key hypothesis.

Correlation coefficient less than zero because the correlation coefficient in the CPA attack could have been signed, and MCPA is no sign. The second phenomenon is due to the small specific settings of variable variation is less than the entire specific settings of variable variation. In the MCPA attacks, the specific was divided into several collections. But because the number of specific settings is relatively small, this effect is weak.

In practical attacks, the instantaneous power consumption is not accurate linearly related to hamming weight. The experiment result shows that the correlation coefficients in MCPA attack is little larger than ones in CPA attack for all key hypothesis.

The correlation coefficients in MCPA attack is larger than ones in CPA attack because that our power model is more accurate description of the measured power leakage which is not linearly related to Hamming weight.

## Conclusions

In this paper we research a new power analysis attack method: MCPA. In the power leakage model of CPA, the MCPA attacks have same effect with CPA attacks. But in practical, the MCPA attack is stronger than CPA attack. Then we perform the simulated attack experiment and the practical attack experiment. The results showed that this conclusion is correct.

## Acknowledgements

This work is supported by National Natural Science Foundation of China (No. U1536103，61402286), Minhang District innovation project (No. 2015MH069).

## References

[1] P. C. Kocher, J. Jaffe, and B. Jun: Differential Power Analysis. In M. J. Wiener,editor, *Advances in Cryptology – CRYPTO'99*, Lecture Notes in Computer Science, vol. 1666, pp. 388–397, Springer-Verlag, 1999.

[2] T. Messerges, E. Dabbish, and R. Sloan: Investigation of power analysis attacks on smartcards. In Usenix Workshop on Smartcard Technology 1999. http://www.usenix.org.

[3] Eric Brier, Christophe Clavier, and Francis Olivier: Correlation power analysis with a leakage model. In Marc Joye and Jean-Jacques Quisquater, editors, CHES, volume 3156 of Lecture Notes in Computer Science, pages 16–29. Springer, 2004.

[4] D. Agrawal, J.R. Rao, P. Rohatgi Multi-channel Attacks, in the proceedings of CHES 2003, Lecture Notes in Computer Sciences, vol 2779, pp 2-16, Cologne, Germany, September 2003, Springer-Verlag.

[5] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer, 2007

[6] Ajit C. Tamhane and Dorothy D. Dunlop: Statistics and Data Analysis: From Elementary to Intermediate. Upper Saddle River, NJ: Prentice Hall, 2000, xiv + 722 pp., ISBN: 0-1374-4426-5.

[7] J. Daemen, V. Rijmen: AES Proposal: Rijndael, Document Version 2, 1999.