Successful Profiling Attacks with Different Measurement Environments for Each Phase

Yongdae Kim(✉)

The Attached Institute of Electronics and Telecommunications Research Institute,
P.O.Box 1, Yuseong, Daejeon 305-600, Korea
kimyd@ensec.re.kr

Abstract. Power analysis attacks have received a great deal of attention, because they can be carried out easily than conventional cryptanalysis. Profiling attacks are one of the most efficient attacks among power analysis attacks. However, profiling attacks have the limitation of using the same experimental environment for both the profiling and attacking phases. If two sets of power traces are obtained from different setups, then the attack may not be feasible. We propose a new method to overcome this limitation with different measurement environments using multivariate regression analysis. Our results show that the proposed method can successfully retrieve a secret key using two different types of power traces. Moreover, the success rate is higher than for non-profiling attacks, i.e., Correlation Power Analysis (CPA).

Keywords: Power analysis attack · Profiling attack · Multivariate regression analysis · Advanced Encryption Standard (AES)

1 Introduction

Kocher et al. introduced the first power analysis attack in 1999. Since then, various types of attacks have been proposed. Among them, the so-called 'profiling attack' is the most efficient method [1]. Profiling attacks, involve an adversary deploying prior leakage information obtained with a reference module, that has the identical physical characteristics as the target module. Profiling attacks have existed for years and come in many forms, e.g. template attacks [2], stochastic model attacks [3], and multivariate regression analysis attacks [4].

Several researchers have studied the performance and effectiveness of profiling attacks [5–9]. However, all of the prior research assumes that an adversary will utilize the exact same measurement environment in both the profiling and attacking phases. Profiling attacks use a set of captured traces in the profiling phase when an attack is performed. Therefore, to retain the physical features of the traces, the adversary deploys the same measurement setup in both phases. In other words, if an adversary deploys two different measurement setups for each phase, the physical characteristics of the measured traces obtained from each phase will be widely dissimilar. Therefore, a naive approach to profiling attacks may not be feasible.

K.-H. Rhee and J.H. Yi (Eds.): WISA 2014, LNCS 8909, pp. 321–330, 2015.
DOI: 10.1007/978-3-319-15087-1_25

Elaabid et al. showed that the template attacks almost have same success rate even though they used two different acquisition campaign for each phase [10]. In addition, Choudary et al. introduced very interesting experimental results using 4 different devices and 5 different types of traces (4 types of traces are obtained from each devices, 1 type of traces is captured from same device, but different date) [11]. In [10,11], they argue that they utilized different acquition campaigns, the major different parameters for each measurement are VCC for target device, acquition date, and resistor. However, the most of other parameters are fixed for measurement yet. Mainly, they used a same acquisition board which have an exact same measurement mechanism. In this paper, we utilized totally different measurement environments for each phase. We propose a method to resolve the limitation to acquitision environments. In this paper, we demonstrate concrete results using two sets of power traces.

Our proposed method is examined through the Advanced Encryption Standard (AES) implementation on an 8-bit Atmel AVR microcontroller. From the results, the proposed method is robust against these types of the measurement environments. In this study, we utilized two different commercial measurement tools, Differential Power Analysis (DPA) Workstation from Cryptographic Research, and Inspector from Riscure. We deployed two different tools for each phase and still, we successfully retrieved the secret AES key in the attacking phase. We also show results for non-profiling attacks, i.e., Correlation Power Analysis (CPA) [12], and the typical multivariate regression attack using same types of traces for comparison purposes.

2 Profiling Attacks

2.1 Discussion

Various types of attack have been introduced to date, e.g., CPA [12], Mutual Information Analysis (MIA) [13], Template Attack [2], etc. These power analysis attacks can be divided into two classes: (i) attacks without a reference module (non-profiling attacks), and (ii) attacks with a reference module (profiling attacks). The reference module is identical to the target module, and is fully controllable by the adversary. For example, the adversary is able to modify the secret key in the reference module and run the encryption (or decryption) process as he can with any plaintext (or ciphertext) value. Profiling attack adversaries exploit not only power traces directly measured from the target module, that non-profiling attack adversaries do, but also exploit power traces from the reference module with known plaintext (or ciphertext) and a secret key. Therefore, profiling attacks, can retrieve a secret key from inside a module with a smaller amount of information (fewer power traces) than typical non-profiling attacks.

Profiling attacks consist of two phases: (i) the profiling phase, and (ii) the attacking phase. In the first phase, an adversary captures power traces from a reference module, and determines the physical characteristics for the next phase. In the attacking phase, the adversary measures the power traces from a target module to reveal a secret key.

However, if the two sets of power traces obtained from each phase have different physical characteristics, it is difficult to apply the profiling attacks, because the prior information (e.g. mean and covariance of power traces in the template attack) obtained from the profiling phase is not similar to the physical characteristics of the measured power traces from the target module. Therefore, profiling attacks assumed that an adversary is able to use the reference module. However, even if the reference module is deployed, if different measurement environments are used for each phase, the physical characteristics will also be varied. Actually, all previous profiling attack research is assumed to use exactly the same measurement environment for both phases. We propose a new method using a multivariate regression attack to overcome this limitation to measurement setups. We have shown, for the first time to the best of our knowledge, a concrete experimental results using two different sets of power traces for each phase in the profiling attacks. However, other profiling attacks (i.e., template attacks and stochastic model attacks) are not feasible if an adversary deploys different types of traces. Therefore, we do not show results for other types of profiling attacks in this paper. Next, we describe multivariate regression attacks.

2.2 Multivariate Regression Attacks

Multivariate regression attacks are robust against selection of *interesting points*, which are time instants containing data-dependent variations, and efficient for modeling in the profiling phase with fewer power traces than other profiling attacks [4]. This type of attack has two phases as follows.

Profiling Phase. First, the hypothetical power consumption, h_i (given by the i-th input) is the response variable in the multivariate regression model. Normally, h_i is equivalent to the hamming weight (or distance) value seen in many cases. The CPA result provides the k interesting points, $\boldsymbol{p} = (p_1, p_2, \cdots, p_k)$, and each point is sorted in descending order of the CPA correlation coefficient value. The explanatory variables are selected as follows:

$$w_{i,p_1}, w_{i,p_2}, \cdots, w_{i,p_k}. \tag{1}$$

In this phase, the multivariate regression model is built as,

$$\hat{s_i} = \hat{\beta}_0 + \sum_{n \in \boldsymbol{p}} \hat{\beta}_n w_{i,n}, \tag{2}$$

where $\hat{s_i}, \hat{\beta}$ are represented by the fitted value of the hamming weight (or distance) and the estimator of coefficients, respectively.

Attacking Phase. In this phase, an adversary deploys the regression model, Eq. 2 to estimate the hamming weight (or distance) value using measured traces from the target module. Then, it finds the highest correlation value between the estimated value and calculated hamming weight (or distance) value, i.e., s_{i,k_j}, for each key candidates, k_j as follows:

$$k_{ck} = \underset{k_j \in k^*}{\operatorname{argmax}}\, corr(\hat{s_i}, s_{i,k_j}), \tag{3}$$

where $corr(a, b)$ is the correlation coefficient between a and b.

3 Experimental Method

In this section, we explain in detail, how we utilize the multivariate regression attack in two different measurement environments. First, we briefly describe the two commercial tools that we used in this study. Those tools have different measurement mechanism for power consumption.

3.1 Commercial Tools

There are several tools used to examine cryptographic modules against side-channel attacks. In this paper, we used the following two commercial tools.

DPA Workstation. The DPA Workstation from Cryptographic Research is the pioneering testing tool for side-channel attacks [14]. The DPA Workstation consists of hardware and software. The hardware includes a workstation, high-speed Peripheral Component Interconnect (PCI) data acquisition hardware, a digital oscilloscope and a smart card test fixture to measure power consumption or Electromagnetic (EM) emanation from a smart card. The main board for measurement is isolated from the communication board by an optical cable to the reduce noise effect. Users are required to write a script to operate the DPA Workstation. The script may include encryption and data acquisition commands for the digital oscilloscope.

Inspector SCA. Riscure developed Inspector Side-Channel Attack (SCA) as a side-channel test platform [15]. This tool provides a smart card reader (Power Tracer) with measurement points, a trigger signal generator, and accompanying software (Inspector) to control the Power Tracer and analyze captured traces. Moreover, they provide additional optional equipment such as an EM probe XYZ-station and a CleanWave to remove carrier wave noise from contactless smart cards, current probes, etc. Inspector is based on JAVA; therefore, users may write and compile the code to extend its usage. In addition to Inspector's source code, an open API, hardware SDK, and an integrated development environment are provided. Power Tracer is a hardware tool with a smart card insert, trigger generation module, and many other detailed configurations modules (e.g., card voltage, delay, clock frequency) that are controlled by Inspector.

3.2 Method

We implemented the AES on a smart card based on an 8-bit AVR microcontroller as the reference and the target modules. We measured 400 power traces both from DPA Workstation and Inspector SCA. The sampling rate of two sets of traces may differ from each other, due to a different digital oscilloscope parameter. Therefore, all traces are resampled at a constant frequency rate, to maintain the equivalent sampling rate. We merely calculate the average value of multiple points, and make one point as follows:

$$w'_i = \sum_{j=T\times(i-1)+1}^{T\times i} \frac{w_j}{T}, \tag{4}$$

where $w_j(w'_i)$, T represents power traces at j-th (i-th) time instants and a parameter for resampling, respectively. For example, if the original traces are captured at 200 MHz, then T will be 50 in order to resample traces at 4 MHz.

Even if we set the exact same parameter on the digital oscilloscope for capturing, the two sets of traces captured from the tools will have different physical characteristics, because they include different shunt resistors, circuit boards noise characteristics, electronic components, etc. Therefore, we need to normalize the different scales to a common scale as follows:

$$w'_i = \sum_{i=1}^{P} \frac{w_i - \mu_w}{\sigma_w}, \tag{5}$$

where P, μ_w, and σ_w represents the total number of sample points, average value of traces, and standard deviation value of traces, respectively.

Once all preprocessing has finished, we determine the *interesting points* in power traces with a data-dependent order for each measurement environment. There are alternative methods for deciding the order of points, and this remains an open problem. However, in this paper, we do not discuss the detailed method used for point selection.

Next, we describe the detail of the setup. We set the same master key and the interesting points for all cases. The first round of AES encryption was our target; therefore we adjusted the range of the oscilloscope and captured power traces to include the first round encryption.

Case 1. We utilized 400 power traces captured from DPA Workstation for the profiling phase, and deployed Inspector to capture another 400 traces for the attacking phase.

Case 2. On the contrary, we used the same number of traces from Inspector and DPA Workstation for the profiling and the attacking phase, respectively.

Case 3. For comparison, we carried out typical profiling attacks. In this case, we used the DPA Workstation for both phases.

Case 4. The Inspector SCA is deployed for both phase.

4 Results

Figure 1 shows the measured traces for both tools after resampling and normalization. Figure 1 shows that, both traces Y-axis (the magnitude in Eq. 5) show almost the same range (between -4 and 4), because we normalized the scales for both traces.

At first, we explain why the template attack is not feasible of our measurements. In the attacking phase of template attack, an adversary find out which template (i.e. mean, $\boldsymbol{m}$ and covariance, $\boldsymbol{C}$ obtained in profiling phase) is well matched with power trace, $\boldsymbol{w} = (w_1, \cdots, w_W)$. It is conducted by calculating probability density function of multivariate normal distribution as follows:

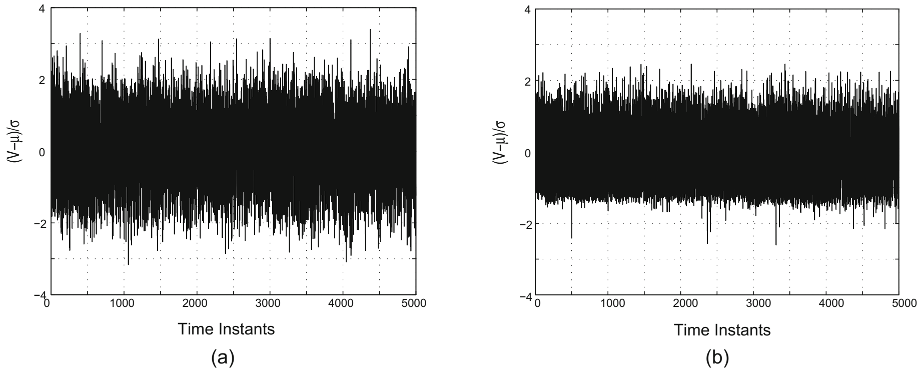


Fig. 1. Measured trace from (a) DPA Workstation, and (b) Inspector SCA

$$p(\boldsymbol{w};(\boldsymbol{m},\boldsymbol{C})_h)=\frac{exp\left(-\frac{1}{2}(\boldsymbol{w}-\boldsymbol{m})^T\boldsymbol{C}^{-1}(\boldsymbol{w}-\boldsymbol{m})\right)}{\sqrt{(2\pi)^W det(\boldsymbol{C})}}, \tag{6}$$

where $det(\boldsymbol{C})$, $\boldsymbol{q}^T$ and h denote the determinant of $\boldsymbol{C}$, the transpose of vector $\boldsymbol{q}$ and the hamming weight (or distance) value. Therefore, an adversary find the hamming weight (or distance) value by finding the highest probability when the power trace $\boldsymbol{w}$ is given in attacking phase. The value can be used to retrive a secret key finally. If any of templates is not matched, the probability is extremely low.

We used 3 sets of traces: (i) DPA WS (Profiling) and (ii) DPA WS (Attack) is traces from DPA Workstation in profiling phase and attacking phase. (iii) Inspector (Attack) is traces from Inspector SCA in attacking phase. In Fig. 2 represents mean and variance of traces (we use the main diagonal of covariance

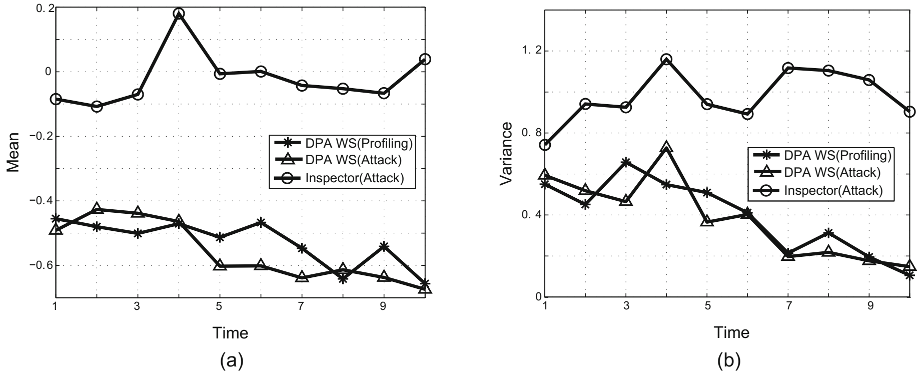


Fig. 2. Mean and variance of traces obtained different acquisition campaign (a) Mean, and (b) Variance

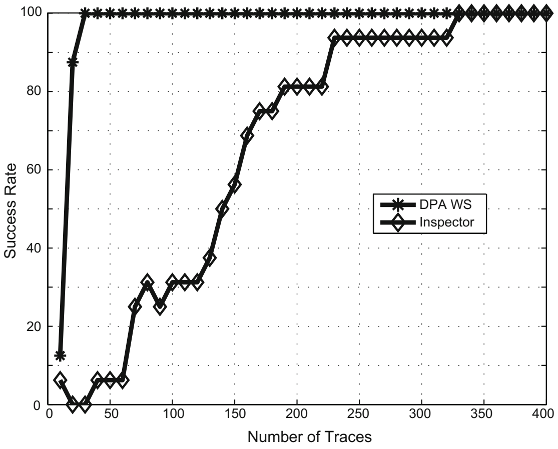


Fig. 3. CPA result

for a reason of visualization) on 10 interesting points, and the corresponding hamming weight value is 3. As shown in the figure, (i) and (ii) traces are very similar in mean and variance, however (i) and (iii) traces are widely different forms. However, in [10,11], the main differences of each trace from different acquision campaigns is a constant offset, so it is relatively easy to compensate it to apply template attack. The probabilities (Eq. 6) are 0.8158 and 1.0054×10^{-8} using (i)–(ii) and (i)–(iii) pairs, respectively. Therefore, it is hard to apply template attack by just adjusting the offset using our experimental environments.

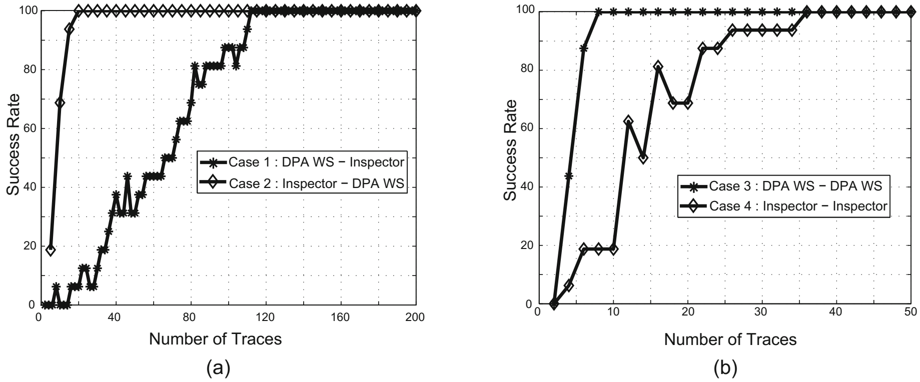
Figure 3 presents the result of a non-profiling attacks, i.e., CPA, for the sake of comparison. The y-axis represents the percentage of success rate calculated as follows:

$$SuccessRate_i = \frac{N_i^{ck}}{16} \times 100, \tag{7}$$

where N_i^{ck} denotes the number of correctly estimated keys using i traces. For example, $SuccessRate_{120} = 100$ means that 16 subkeys of AES were correctly retrieved using 120 traces. The minimum number of traces to have 100 % success rate is defined as Measurements To Disclosure (MTD) as an evaluation criteria for performance of attacks in this paper. Our results confirmed that the MTD of CPA by using DPA Workstation and Inspector is 30 and 340, respectively. We assumed that the Signal-to-Noise Ratio (SNR) of traces using DPA Workstation was higher than those using Inspector.[1]

Figure 4 uses the traces from Fig. 1 to show the results for all cases. This confirmed that the profiling attack was successfully conducted, even though two different measurement environments were used. The performance of attacks for

[1] We do not represent DPA Workstation is better than Inspector SCA. Because the SNR can be very varied depends on target device, environmental settings, etc. Therefore, SNR of traces from Inspector SCA can be higher in some case.

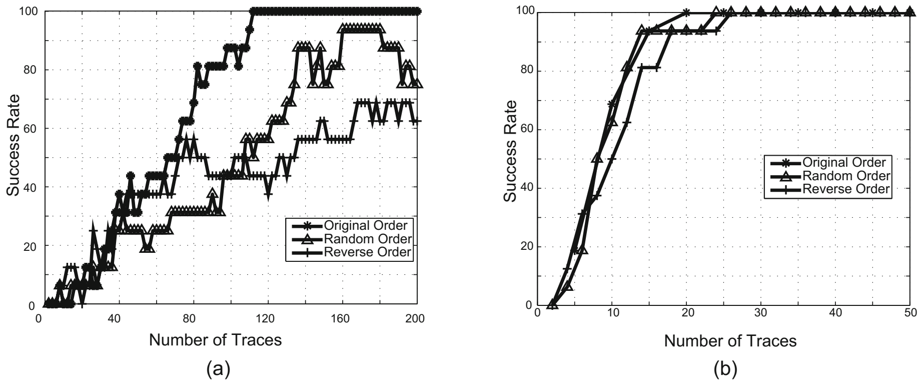


(a) (b)

Fig. 4. Success rate (a) Case 1, 2, and (b) Case 3, 4

cases 1 and 2 are obviously lower than those for cases 3 and 4. However, this is the first concrete result that an adversary can utilize different types of traces for the profiling and attacking phases and still successfully retrieve a secret key.

Next, we investigated the effectiveness of the order of interesting points. First, we determined the interesting points in descending order of the correlation, as we described in the previous section. However, sometimes, it is impractical to order the points. Therefore, we examined how much the order of the points affects the performance of the attacks. We randomly selected the index of the interesting points first. In addition, we expected that if we determined the points in reverse order (ascending order), this would have had a negative effect on the results. Therefore, we also determined the reverse order of the interesting points for comparison. Figure 5 show the success rates using the different orderings of the interesting points. Figure 5(a) shows, as we expected, the MTD was the lowest when the reverse order of points was used. In addition, we saw the intermediate



(a) (b)

Fig. 5. Success rate using different order of the points (a) Case 1, and (b) Case 2

performance when random order was used in case 1. However, Fig. 5(b) shows that it was almost the same performance despite using different ordering of the points in case 2. We think that the order of points has a small influence on the performance of attacks if the SNR of traces is relatively high.

Finally, Table 1 presents the MTD of all the case including CPA. We define the improvement as follows for comparison with the non-profiling attack (CPA).

$$Improvement_c(\%) = \frac{M_{CPA} - M_c}{MTD_{CPA}} \times 100, \tag{8}$$

where c and M_{CPA} represents case number and the MTD using CPA. Our results showed that the profiling attacks still performed better that the CPA, in spite of using different sets of power traces.

Table 1. The MTD and improvement of all experimental results

Experiment	Tool	MTD	Improvement (%)
CPA	DPA WS	30	-
CPA	Inspector	340	-
Case 1	DPA WS - Inspector	115	66.2
Case 2	Inspector - DPA WS	20	33.3
Case 3	DPA WS - DPA WS	8	73.3
Case 4	Inspector - Inspector	36	89.4

5 Conclusion

A method to apply profiling attacks using two different sets of power traces captured by different tools, and concrete results were presented in this paper. Conventionally, power traces are obtained using the same measurement environment in both the profiling and attacking phases of a profiling attack, because two sets of power traces should have exactly the same physical characteristics. However, this assumption is unnecessary with the proposed method. For the first time, we have shown that our method can successfully extract all AES keys despite using two different measurement setups. Our method is more practical than others in many cases. Moreover, we have additional types of measurement setups and several cryptographic modules. Therefore, our future research will concern developing a framework to integrate the power traces from all different tools.

References

1. Standaert, F.-X., Gierlichs, B., Verbauwhede, I.: Partition *vs.* comparison side-channel distinguishers: an empirical evaluation of statistical tests for univariate side-channel attacks against two unprotected CMOS devices. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 253–267. Springer, Heidelberg (2009)

2. Chari, S., Rao, J., Rohatgi, P.: Template attacks. In: International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp. 13–28 (2002)
3. Schindler, W., Lemke, K., Paar, C.: A stochastic model for differential side channel cryptanalysis. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 30–46. Springer, Heidelberg (2005)
4. Sugawara, T., Homma, N., Aoki, T., Satoh, A.: Profiling attack using multivariate regression analysis. IEICE Electron. Expr. **7**, 1139–1144 (2010)
5. Standaert, F.-X., Archambeau, C.: Using subspace-based template attacks to compare and combine power and electromagnetic information leakages. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 411–425. Springer, Heidelberg (2008)
6. Archambeau, C., Peeters, E., Standaert, F.-X., Quisquater, J.-J.: Template attacks in principal subspaces. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 1–14. Springer, Heidelberg (2006)
7. Rechberger, C., Oswald, E.: Practical template attacks. In: Lim, C.H., Yung, M. (eds.) WISA 2004. LNCS, vol. 3325, pp. 440–456. Springer, Heidelberg (2005)
8. Kim, Y., Homma, N., Aoki, T., Choi, H.: Security evaluation of cryptographic modules against profiling attacks. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 383–394. Springer, Heidelberg (2013)
9. Gierlichs, B., Lemke-Rust, K., Paar, C.: Templates vs. stochastic methods. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 15–29. Springer, Heidelberg (2006)
10. Abdelaziz, E.M., Sylvain, G.: Portability of templates. J. Cryptographic Eng. **2**, 63–74 (2012)
11. Choudary, O., Kuhn, M.G.: Template attacks on different devices. In: Prouff, E. (ed.) COSADE 2014. LNCS, vol. 8622, pp. 179–198. Springer, Heidelberg (2014)
12. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
13. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual information analysis: a generic side-channel distinguisher. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 426–442. Springer, Heidelberg (2008)
14. Cryptographic Research, DPA Workstation. http://www.cryptography.com/technology/dpa-workstation.html
15. Riscure, Inspector SCA. https://www.riscure.com/security-tools/inspector-sca/