IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 13, 2020, accepted April 30, 2020, date of publication May 11, 2020, date of current version May 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2993701

An Energy Trace Compression Method for Differential Power Analysis Attack

XIAOMIN CAI, RENFA LI, (Senior Member, IEEE), SHIJIE KUANG, AND JINHUI TAN
College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

Corresponding author: Renfa Li (lirenfa@hnu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672217, Grant 61832018, and Grant 61472123.

ABSTRACT Differential power analysis attacks are the most commonly used means to break cryptographic devices within the side-channel attack technology. Since there is a lot of noise in the energy trace of cryptographic devices, a large number of energy traces are needed to carry out the attack, resulting in a high computational cost. To solve this problem, this study starts with an analysis of the characteristics of power waveform formation from the inherent properties of the complementary metal oxide semiconductor circuit. Then, based on the Hamming distance classification method and the results of power waveform analysis, the useful information interval in the energy trace is located, that is, the interval with a strong correlation with the key. Thus, we achieve energy trace compression. Finally, a system on chip with a 128-bit AES algorithm is used to conduct various attack experiments in the effective interval. The results show that the calculation is cut off by 96%, which greatly reduces the computational cost for differential power analysis attacks.

INDEX TERMS Differential power attacks, hamming distance, effective interval, energy traces.

I. INTRODUCTION

Cryptographic devices inevitably leak some physical information, such as power consumption, electromagnetic radiation, and runtime, when performing encryption or encryption operations. Side-channel attacks (SCAs) use the physical information to reveal secret keys of cryptographic devices. According to different types of physical information, the most important SCAs are of three types: timing attacks [1], power analysis attacks [2], and electromagnetic radiation attacks [3]. Timing attacks [1] were first proposed in the field of cryptographic devices in 1996. Since then, non-intrusive SCAs technology has set off a wave of research in the field of information security [4]–[8]. Power analysis attacks [2] use the energy consumption characteristics of cryptographic devices rather than the mathematical characteristics of cryptographic algorithms. Because of its simple operation, wide application range, and high success rates, power analysis attacks have become one of the most commonly used and effective methods in SCAs. The power analysis attack has successfully attacked various cryptographic algorithms, for example, AES [9], DES [10], and RSA [11]. It can also attack various encryption devices, such as smart cards, field programmable logic devices (FPGA), microcontroller, and ASIC and crypto SoC [12]–[15].

Differential power analysis (DPA) attacks use statistical tools (also known as distinguishers) to reveal the relationship between the key and power consumption. DPA attack results are greatly affected by the signal-to-noise ratio [16] of the leaked information. In order to improve the success rate and efficiency of DPA attacks, it is particularly important to pre-process the power traces. This has two main purposes: one is to reduce the power consumption samples and the other is to decrease the sample calculation. Pre-processing techniques include digital signal processing (DSP) technology [17], principal component analysis (PCA) [18], interception [19], and integration [20]. DSP methods mainly include wavelet transform denoising technology [21], [22], the Fourier transform [23], [24], low-pass filters [25], and so on. However, DSP technology needs to know all kinds of parameters and ensure that the signal and noise are not in the same frequency domain, which needs high requirements of the attacked device and attacker. Thus, it is difficult to implement the DSP technology. The literature [26]ower traces were selected according to the principal components. Compared with the common correlation power attack (CPA) [27],

The associate editor coordinating the review of this manuscript and approving it for publication was Noor Zaman.

the attack efficiency was greatly improved. Clavier [28], [29] looked for points of interest in power tracking and applied collision-related techniques to recover the entire key. Meanwhile, Park *et al.* [30] proposed subtraction algorithm analysis on equidistant data subtraction algorithm analysis on equidistant data (SAED), which extracted sensitive information using the event information of the subtraction operation in a reduction algorithm; however, an attacker still needed 256 power traces to obtain a data block. Based on the singular value decomposition, Zhou *et al.* [31] selected high-quality energy traces for DPA attacks, but did not reduce the sample calculation. Focused on template attacks [32], Zhang and Zhou [33] evaluated the optimal number of interest points in the simulation scene and provided a useful empirical formula; however, this was only applicable to Gaussian template attacks. Finally, Wang *et al.* [34] proposed a feature point extraction scheme based on the difference, but the experimental results still needed to be extracted manually; they also lacked objectivity and sufficient theoretical support.

Our contributions in this study are as follows. In order to reduce the amount of sample calculation and manual intervention, this paper studies the energy trace data preprocessing scheme for SoC. Based on the current characteristics of complementary metal oxide semiconductor (CMOS) circuits, the position and range of the power consumption difference interval are analysed, which provides a theoretical basis for extracting the effective interval. This study then proposes a method for locating marker points based on the Hamming distance, which accurately locates the position of power consumption data in the energy trace that has the strongest correlation with the key. Through a large number of experiments, it is confirmed that only a small number of data near the markers are needed to form an effective interval, and the attack effect is the best when 10 sampling points are intercepted to form an effective interval near the marker.

The rest of the study is organized as follows. In Section 2, we will briefly introduce the relevant research background. The power consumption difference interval will be analysed in Section 3. In Section 4 follows explanations of the use of the Hamming distance classification to locate markers. The experimental verification of the effective interval will be discussed in Section 5. Finally, Section 6 will conclude the whole study.

II. RELATED BACKGROUND

A. ENERGY MODEL

DPA attacks use an energy model as a criterion for distinguishing between right and wrong keys. The commonly used energy models are the Hamming distance (HD) model [35] and the Hamming weight (HW) model [36], both of which represent the correlation between input data (i.e., plaintext and key) and power consumption. The HD model is simple in principle, convenient to implement, and more widely used. The HD represents the number of distinct bits between v_0 and v_1, and is equal to the HW of $v_0 \oplus v_1$. The HW is equal to the number of bits with a logical value of "1" in a binary string. The HD model assumes that all components have the same influence on power consumption, that is, the $0 \rightarrow 1$ conversion and the $1 \rightarrow 0$ conversion have the same power consumption. Then, the total number of conversions is used to characterize the power consumption of the circuit during this period. Therefore, the energy model based on the HD is expressed as follows:

$$E = aHW(v_0 \oplus v_1) + b. \tag{1}$$

where E is the energy consumed by the circuit during the register switching from v_0 state to v_1 state, a is the energy consumption ratio coefficient, and b is the power consumption and noise that are not related to the processed data.

B. STEPS OF DPA ATTACK BASED ON THE MEAN DIFFERENCE

The general method of the DPA attack requires computing the correlation between two matrices. The correlation calculation process is cumbersome when the matrix is large. In order to simplify the calculation steps, the mean difference is used instead of the correlation coefficient calculation. The steps of the DPA attack based on the mean difference are as follows:

- **Step 1**: Choosing an Intermediate Result of the Algorithm Executed in the Device. This intermediate value is a function $f(d_m, k_n)$, where d_m is the m^{th} plaintext and k_n is the n^{th} value of a small part of the key.
- **Step 2**: Measuring the Power Consumption. For each plaintext $d_m(m = 1, \ldots, M)$, an encryption operation is performed to generate an energy trace of length L. Then, the traces can be written as matrix $\boldsymbol{T}$ of size $M \times L$.
- **Step 3**: Calculating the Hypothetical Intermediate Value. For each d_m and $k_n(n = 1, \ldots, N, N$ is the number of all possible kn values), calculate the corresponding hypothetical intermediate value, and obtain a hypothetical intermediate value matrix $\boldsymbol{V}$ of size $M \times N$, where $v_{m,n} = f(dm, kn)$.
- **Step 4**: Mapping Hypothetical Intermediate Values to Hypothetical Power Consumption Values. Map each hypothetical intermediate value $v_{m,n}$ to a bivariate hypothetical power consumption value $h_{m,n}$ to obtain a bivariate hypothetical power consumption value matrix $\boldsymbol{H}$.
- **Step 5**: Calculating the Mean Difference of the Energy Traces. According to each column vector in matrix $\boldsymbol{H}$, $\boldsymbol{T}$ is divided into two subsets. The first subset contains the rows in $\boldsymbol{T}$ whose index value is equal to the index of 0 in the column vector, and the second subset contains all the remaining rows in $\boldsymbol{T}$. Then, calculate the averages of the two subsets separately to get two rows. Finally, find the difference between the two mean values to get 1 row. A total of N rows are obtained for all of the N column vectors of $\boldsymbol{H}$.
- **Step 6**: Comparing All Mean Differences. Compare the N average difference rows obtained in step 5. The key corresponding to the row with the largest value is the key

obtained by the attack, and the time corresponding to the column is the maximum information leakage moment.

C. ENERGY TRACE COMPRESSION

Not all data in the energy trace are related to the hypothesized power consumption, that is, there is redundancy in the energy trace. Energy trace compression is designed to try to remove redundant data. In fact, on the premise of retaining information, reducing the amount of data in the energy trace as much as possible can greatly improve the time efficiency of the attack.

A previous analysis [37] has shown that the peaks appearing in the energy traces are the most relevant points for energy analysis attacks. Based on this conclusion, two commonly used energy trace compression techniques have been proposed: one is maximum value extraction and the other is integration. The former only keeps the maximum value of the energy trace in each clock cycle, and the latter integrates the energy traces near the peaks into a value, such as summing or square summing. However, it is still impossible to know which segment of the energy trace has a strong correlation with the hypothesized power consumption value.

D. ATTACK SUCCESS RATE AND RELIABILITY

The attack success rate was first proposed by Standaert *et al.* [38]. Since then, the success rate has been widely used to evaluate the probability of key recovery in DPA attacks. The success rate is defined as the probability that the keys of the attacked device is successfully recovered under a certain number of power traces. Generally, it is not necessary to recover all the key bits to prove that the encryption device has failed. If 8-bit sub-keys are proven to have serious sensitive information leakage, the device may fail [37]. Therefore, the partial success rate (PSR) is also often used. The PSR in this paper also refers to the success rate.

In addition, in order to evaluate the reliability of the result key, this paper uses Euclidean distance fluctuation Devia, which is defined as follows:

$$Devia = 1 - \frac{E - submin}{E - min}. \tag{2}$$

where min, submin, and E represent the minimum value, the next smallest value, and the average value of the Euclidean distance of all keys, respectively. The greater the difference between E-min and E-submin, the closer Devia is to 1, the more prominent the uniqueness of the minimum value, and the higher the reliability of the successful attack.

III. POWER CONSUMPTION DIFFERENCE INTERVAL AND INTERMEDIATE VALUE SELECTION

Digital circuits are made up of logic components, including combinational components and sequential components. The output of a combinational component is used as the input of another. Such a circuit is called a multi-stage combinational circuit. When an input of a combinational circuit changes, the output does not necessarily change with it. This phenomenon is more serious in multi-level circuits, that is, in a multi-level circuit, the output does not easily change with a change in input. The input signal is considered blocked at this moment.

Assume that the probability of each input value being 0 or 1 is 0.5; then, the probability of the input signal of a two-input AND gate, NAND gate, OR gate, and NOR gate being blocked is 5/8, that is to say, the probability of the output of these logic gates changing due to input changes is 3/8. Therefore, for a multi-stage circuit composed of such logic gates, the input signal can usually only pass a few gates to the output. For example, the probability that the output signal of the register reaches the output terminal after passing through a six-stage combinational circuit is approximately $(3/8)^6 \approx 0.003$, which is almost zero. Therefore, passing through six stage gates after the register output signal enters the combinational circuit, the signal tends to be stable and the dynamic energy consumption almost disappears.

When a signal passes through a logic component, or even a wire, there is a delay. In a clock cycle, due to the phenomenon that the signal is blocked, the maintenance time of the power consumption waveform of the circuit generally does not exceed 6t (here it is assumed that t is the average transmission delay time of each logic gate, and the transmission delay of the wire is not considered), and the amplitude of the waveform gradually decays with time. Therefore, the closer the power waveform is to the starting point, the more the circuit activity can be reflected.

The energy consumption of a cryptographic device depends on the intermediate value processed during the algorithm execution process. Choosing an appropriate intermediate value for the attacker can increase the success rate. The first encryption process of the 128-bit AES algorithm is shown in Fig.1. The plaintext and the key are exclusive-ORed before the data register, and the combinational circuit starts the first round of encryption operation. Each round consists of four round transformations, which are called AddRoundkey, SubByte, ShiftRows, and MixColumns (the 10th round does not perform AddRoundkey). According to the above discussion, the power consumption data with the strongest correlation with the key should be concentrated near the register, that is, the place marked "Position A" in the figure,

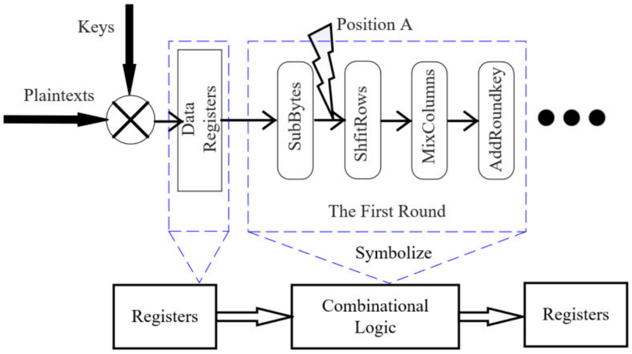

FIGURE 1. Structure of the first-round transformations of AES.

which is why people often choose the output of Sbox as the intermediate value.

Different input data leads to different energy consumption, that is, a different plaintext or key produces different power consumption waveforms. This phenomenon is called the correlation between energy traces and input data. In DPA attacks, the absolute value of energy traces is meaningless. What is important is only the difference between the power consumption caused by different inputs. The so-called power consumption difference interval refers to the part of an energy trace that is different from others due to different input data. According to the above analysis, the length of this part usually does not exceed 6t. If the length is too large, then more noise will be introduced, which not only increases the amount of sample calculation, but also causes the attack to fail. If it is too small, then it may directly cause the attack to fail because it does not cover the effective information leakage interval. Therefore, the number of sampling points N_{diff} should be appropriate and adequate and can be calculated using (3), where f_{sample} is the frequency for the sampling energy trace:

$$N_{diff} \approx 6t \times f_{sample}. \tag{3}$$

IV. ENERGY TRACE MARKER LOCATION

From the above discussion, it is known that the selected intermediate value should correspond to a vicinity of a certain peak in the energy trace; this peak is called an energy trace marker point. However, generally, it is not known where the peak is because there are many peaks in the energy trace. The following approach is taken to obtain the location of the marker.

1) For M groups of random plaintexts $d_1, d_2 \ldots d_m \ldots d_M$, collect M energy traces, and each energy trace has L points. The m^{th} energy trace is represented by a row vector $t_m = (t_{m,1}, t_{m,2}, \ldots, t_{m,L})$, and the original matrix $\boldsymbol{T}$ of the energy trace is expressed as in (4)):

$$T = \begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,L} \\ t_{2,1} & t_{2,2} & & t_{2,L} \\ \vdots & & \ddots & \vdots \\ t_{M,1} & t_{M,2} & \cdots & t_{M,L} \end{pmatrix}. \tag{4}$$

2) Select the correct key hypothesis kcorrect, and use the intermediate value function f(dm, kn) to calculate the M set of hypothetical intermediate values (here, the output value of the first round of encryption Sbox operation is selected as the intermediate value, which is the value of Position A in Fig.1) to obtain an hypothetical intermediate value column vector $\boldsymbol{V}$:

$$V = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_M \end{pmatrix}. \tag{5}$$

3) Using the HD energy model, map the vector V to the hypothetical energy consumption column vector $\boldsymbol{H}$, where each component of $\boldsymbol{H}$ is the HD value of an 8-bit sub-key. Then, M HD values in this vector are divided into 3 categories: (1) HD values of 0, 1, and 2; (2) HD values of 6, 7, and 8; and (3) all other HD values. Finally, the rows in $\boldsymbol{T}$ are also divided into 3 categories. The first category T_1contains the rows in T whose index values are equal to the HD index values of the first category. The second category T_2 contains the rows in $\boldsymbol{T}$ whose index values are equal to the HD index values of category 2, and the last category contains the rest. Since the energy traces in the third category have little effect on the positioning of the markers, they will not be processed:

$$\begin{aligned} T_1 &= \{HD\,(t_m) = (0, 1, 2)\}. \\ T_2 &= \{HD\,(t_m) = (6, 7, 8)\}. \\ T_3 &= \{HD\,(t_m) = (3, 4, 5)\}. \end{aligned} \tag{6}$$

4) Average category T_1 and category T_2 separately to obtain two energy trace classification center traces $\overline{CM_k}$ under the correct key, where k = 1, 2:

$$\overline{CM_k} = \frac{\sum_{t_m \in T_k} t_m}{|T_k|} \cdot \sum_{k \in 1,2} |T_k| = M - |T_3|. \tag{7}$$

5) Select the wrong key hypothesis k_{wrong}, and repeat steps 2, 3, and 4 to get two classification centre traces $\overline{WM_k}$ under the wrong key. Subtract $\overline{WM_k}$ from $\overline{CM_k}$ to get two differential centre traces ΔDM_k

$$\Delta DM_k = \overline{CM_k} - \overline{WM_k}. \tag{8}$$

The position where two $\overline{CM_k}$ curves show the largest peak at the same time is the position where the energy trace has the strongest correlation with the intermediate value, which is the so-called marker point. After obtaining the marker, a small number of sampling points near the marker are taken to constitute an effective attack interval. Fig.2 shows an example in which there are two energy centre trace difference curves in the left subgraph. It is clear that there are many peaks on both curves near the 6000th point. By amplifying the waveform near this point, we get the right subgraph in which two curves

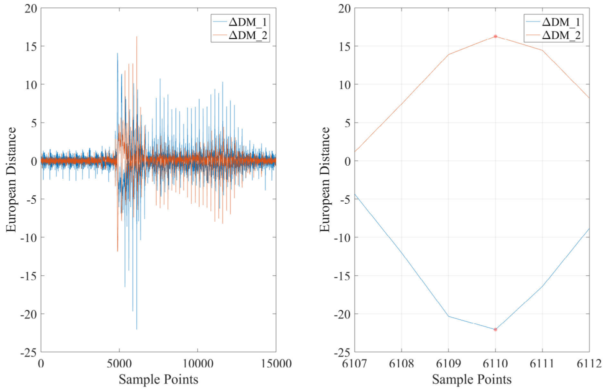

FIGURE 2. Two difference palpitations and partial enlargement.

have the largest peak value at the 6110th point. Therefore, point 6110 is the marker we found.

V. EXPERIMENT

A. EXPERIMENTAL ENVIRONMENT

The experimental object is an SoC chip with a cryptographic coprocessor. The coprocessor is implemented with SMIC130 nm process. The total area of the SoC is 124 mm^2, and the total power is 6.25 mW. The coprocessor runs a 128-bit AES algorithm, with an area of 0.06 mm^2, an average gate delay of 0.25 ns, and a power consumption of only 0.04 mW, which accounts for a very small percentage of the total power consumption. Because the coprocessor and the CPU are packaged together and cannot be isolated, various noise interferences from the same PCB are relatively large. These factors greatly increase the difficulty of the attack.

In order to reduce interference, a custom acquisition card is used in the experiment. The specific parameters of the environment are shown in Table.1. During the execution of the algorithm, the acquisition card collects the energy consumed by the SoC by measuring the voltage on a 0.1Ω sampling resistor connected in series to the power ground wire. Fig.3 shows the experimental platform. The acquisition work is controlled by the PowerAnalysis software.

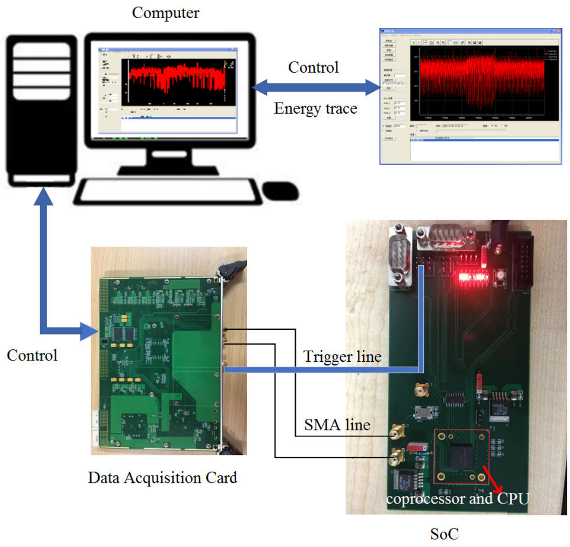

FIGURE 3. Energy acquisition platform.

B. EXPERIMENTAL METHODS AND STEPS

The sampling frequency of the acquisition card is fixed at 5 Gsps, and the working frequency of the cryptographic device is 20 MHz. Two hundred and fifty points are sampled per clock cycle, and each point is quantized to 10 bits. A complete original energy trace has 15,000 sampling points in total. According to (3), N_{diff} is about 8. The average difference DPA method is used for the attack, and the attack results are evaluated using Devia and PSR. The experimental steps are as follows:

TABLE 1. Experimental environment.

Items	Name/Parameters
Acquisition tool	Data Acquisition Card
Upper software	Power Analysis
Sampling rate	5 Gsps
Sampling bit	10 bit
Sampling depth	2 G
Algorithm	128-bit AES
sampling resistor	0.1Ω
Device under test (DUT)	SoC
DUT voltage	1.2 V
DUT frequency	20 M

- **Step 1**: Measuring Energy Traces. First, 256 different keys are moved sequentially from memory to registers and 2000 energy traces are collected for each of these keys. Thus, a total of 512,000 energy traces are obtained.
- **Step 2**: Obtaining Marker Points. For 10 randomly selected correct keys 18, 148, 197, 228, 58, 59, 96, 98, 188, and 232, 2550 marker points of 10 groups of energy traces are obtained by the method described in Section 4, respectively.
- **Step 3**: Count the frequency of 2550 marker points, and select one marker point through attack for subsequent experiments.
- **Step 4**: Attacking and Selecting the Best Attack Interval. Intercept 2, 5, 10, 20, 50, 100, 200, and 400 sample points around the selected marker point as the attack interval to attack all 256 keys. By comparing the attack effects at different attack intervals, the best attack interval can be obtained.
- **Step 5**: Attacking Again After Reducing the Sampling Frequency. Reduce the sampling frequency to 2.5 Gsps, 1.25 Gsps, and 0.625 Gsps by equal interval sampling, and attack the 10 selected keys in the best attack interval obtained in step 4.

C. EXPERIMENTAL RESULTS AND ANALYSIS

1) MARKER POINTS

For each of the 10 randomly selected correct keys, we record the marker points obtained under the 255 wrong keys in sequence, count all 2550 marker points, and get the frequency histogram as shown in Fig.4. It can be seen that the markers have a high repeatability at the positions of 5610 and 6110, and the sum of the number of occurrences of the two points accounts for 83% of the total number. Therefore, it can be considered that the strongest points of information leakage are mainly concentrated at these two locations. Either one of them can be selected as a marker. In order to confirm the attack effect of the two markers, points 5610 and 6110 are selected as the marker points. The attacks are performed on the 10 keys, and the number of successful attacks is shown in Table.2.

It can be seen from Table.2 that when intercepting 10 and 200 sampling points near the marker points 5610 and 6110 for attack, the number of successful attacks at marker point

TABLE 2. Results of attacks at different markers.

Number of sampling points	Number of successful attacks when the marker point is 5610	Number of successful attacks when the marker point is 6110
2	9	9
5	10	10
10	9	10
20	10	10
50	10	10
100	10	10
200	5	6
400	0	0

5610 is less than that at marker point 6110. At the same time, Fig.4 shows that the most frequent occurrence of the marker 6110 is 1180, accounting for 46% of the total. Therefore, due to the space limitation, only the experimental results with point 6110 as the marker are given below.

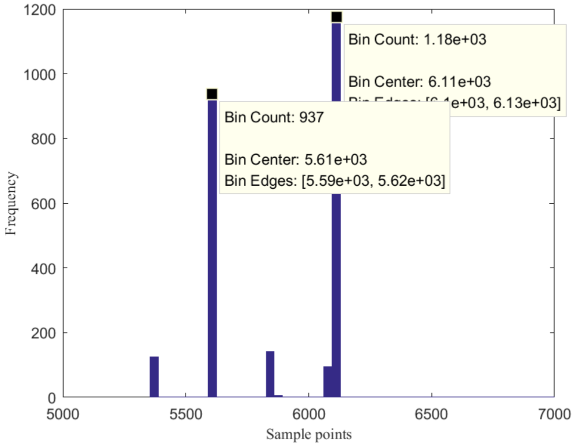

FIGURE 4. Mark statistics for different keys.

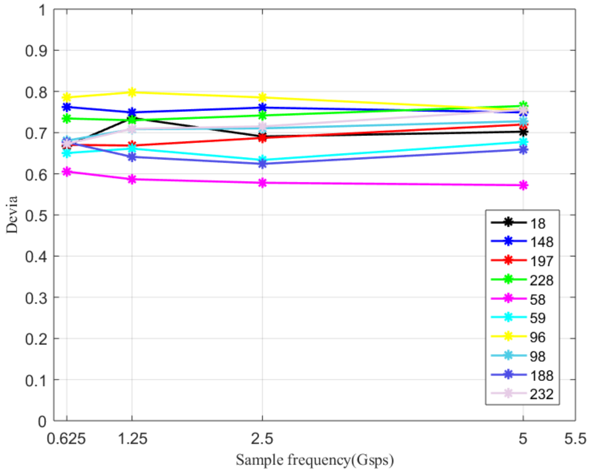

FIGURE 5. Devia value at different sampling rates.

2) THE ATTACK INTERVAL

In this study, 2, 5, 10, 20, 50, 100, 200, and 400 sampling points are intercepted around marker 6110 at eight different effective attack intervals, and the attack results for all 256 keys in each interval are shown in Fig.6, Fig.7, and Table.3.

TABLE 3. Partial success rate and Devia value under different effective intervals.

Number of sampling points	PSR	Median Devia value
2	242/256	0.656
5	256/256	0.692
10	256/256	0.702
20	256/256	0.679
50	225/256	0.666
100	224/256	0.64
200	103/256	0.239
400	0/256	0.029

Fig.6 shows the attack on key 58. The horizontal axis of the figure represents the keys and the vertical axis is the Euclidean distance. The sub-map in the figure corresponds to 8 different attack intervals from top to bottom and from left to right. The first seven sub-graphs show that the attack result key is 58 and the attack is successful. The last sub-map shows that the attack result key is 181, and attack fails. Among the first 7 correct results, the third *Devia* value is the largest, reaching 0.71. This result shows that for key 58, the optimal attack interval is [6105: 6114]. Therefore, the optimal number of points in the valid interval is 10, including the marker point itself.

The horizontal axis of Fig.7 represents different intervals, and the vertical axis denotes Devia values. The maximum, minimum, and median values of Devia are given for each interval. It can be seen that 10 intercepting points around marker 6110 as the effective attack interval has the best effect because the maximum, minimum, and median values of the corresponding *Devia* values are the largest among the 8 intervals. From this, three conclusions can be drawn. First, the circuit does leak a lot of secret information at 6110. Second, the effective interval should not be too small or too large. If it is too small, the selected range may not cover the information leakage range of the energy trace; if it is too large, it will introduce too much noise. Third, the size of the best effective interval is basically consistent with the result that N_{diff} is about 8 (as calculated according to (3)).

Table.3 shows the PSR and the median corresponding Devia values, which represent the attack success rate for each interval. When the number of points is 5, 10, and 20 in the interval, the attack with each sub-key is successful. As the number of points gradually increases, the PSR decreases and the attack success rate goes down. When there are more than 400 points, no attack is successful. If there are only two points, the attack success rate is only 95%. At the same time, when the number of points in the interval is 10, the median Devia value, 0.702, is the largest. Therefore, from the PSR and Devia values, it is best to intercept 10 points around marker 6110 as the effective attack interval.

Both Fig.7 and Table.3 show that the best attack effect can be achieved by selecting 10 points near 6110 as the effective attack interval. Therefore, the number of data used for attacking from each energy trace is reduced from 250 points in one

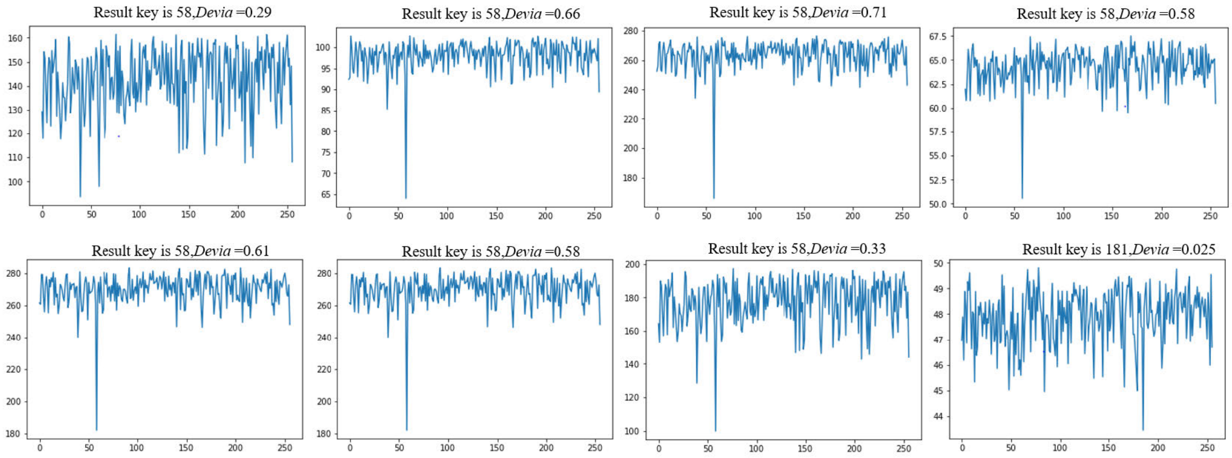

FIGURE 6. Attack results of different effective interval when the key is 58.

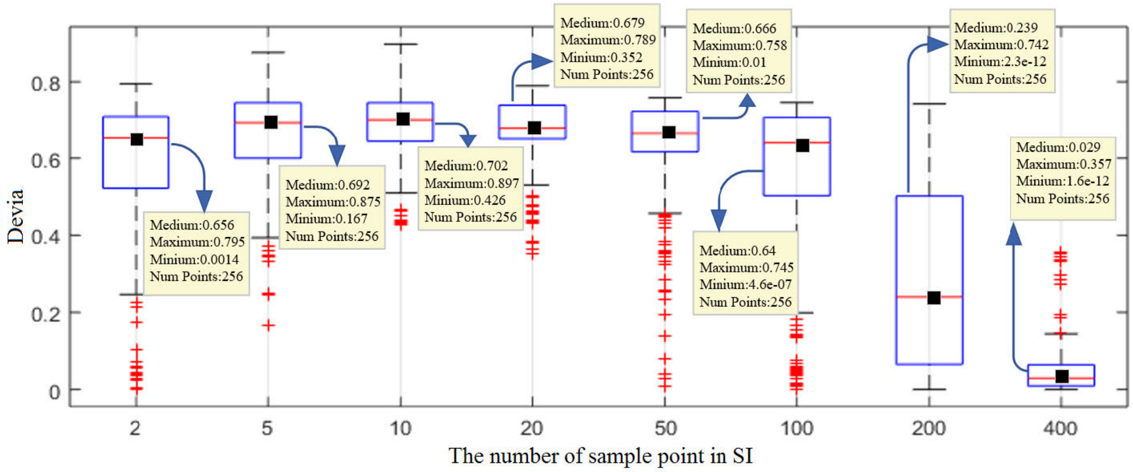

FIGURE 7. Devia statistics under different keys and different effective intervals.

cycle to 10 points, a reduction of 96%, thus improving the time efficiency of DPA attack.

3) SAMPLING FREQUENCY

In this experiment, a custom-made acquisition card is used, and the sampling frequency is fixed at 5 Gsps. Can the sampling rate be reduced? To answer this, the sampling frequency is decreased to 2.5 Gsps, 1.25 Gsps, and 0.625 Gsps by equal interval sampling. Within the best effective attack interval determined in step 4 of the experiment, the 10 selected keys are attacked again. The experimental results are shown in Fig.8.

The horizontal axis of Fig.8 represents different sampling rates, and the vertical axis represents Devia values. The figure shows that when the sampling rate gradually reduces from 5 Gsps to 0.625 Gsps, all attacks are successful and the Devia value changes little. For example, for key 18, the maximum value of Devia is about 0.70 and the minimum 0.67 (the difference is 0.03, that is, only about 5%). It should be noted that when the sampling rate is reduced to 0.625 Gsps, the attack range only contains one point, that is, the marker point itself (6110). This proves again that the circuit does leak a lot of secret information at the sampling point 6110.

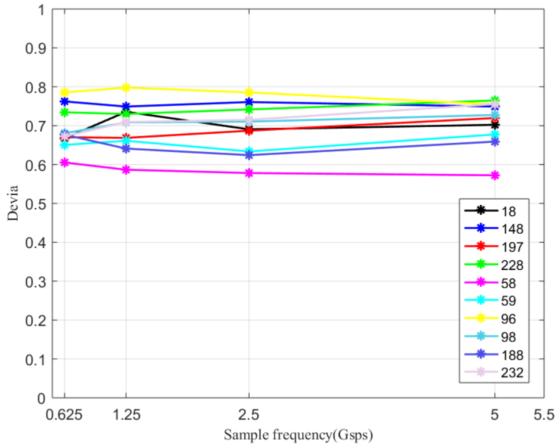

FIGURE 8. Devia value at different sampling rates.

4) COMPARISON WITH OTHER METHODS

When comparing the results of DPA attacks, the type, energy model, target device, and implementation mode of DPA attacks should be considered. To make a fair comparison,We choose paper [39] as the comparison object, because it has the same cryptographic algorithm and energy trace compression purpose as this article. We include as much information as possible in Table.4.

TABLE 4. Comparison of information of different methods.

Item	Pre-processing method	Algorithm	Target device	Length of one power trace	Used points
Kim [39]	Principal Component Analysis	AES	Xilinx Virtex-5 LX30	6000	500
This paper	Marker location	AES	SoC	15000	10

Kim and Ko [39] proposed a new selection method to improve power analysis attacks using principal component analysis and utilized the SASEBO-GII platform in experiments, which includes a main FPGA and control FPGA. The encryption component in the main FPGA (Xilinx Virtex-5 LX30) is completely separated from the control FPGA, minimizing the transmitted noise from the same PCB. Compared with the FGPA, the energy traces measured from the SoC are more complex and more difficult to attack. For one energy trace, the final sampling points used by [39] were 500, while 10 points near the marker are used in this paper, which greatly reduces the calculation cost.

VI. CONCLUSIONS

Based on the current consumption characteristics of CMOS circuits, this study discusses the location and range of the critical data needed for DPA attacks. Based on the Hamming distance classification method, the power consumption data with the strongest correlation with the key are found, which solves the difficulty of manually locating the power consumption difference interval when analysing the power consumption trajectory. Under the premise of ensuring the success rate, the energy trace compression method in this paper reduces the sample calculation and attack cost. Since the location of the marker method must know the correct key in advance, the method, in this article, is suitable for designers of cryptographic devices or people who actually own the same device as the target device. In future research, we intend to apply these methods to other cryptographic algorithms and different practical scenarios to expand their universality.

REFERENCES

[1] P. C. Kocher, "Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems," in *Proc. CRYPTO*, Santa Barbara, CA, USA, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. CRYPTO*, Santa Barbara, CA, USA, 1999, pp. 388–397.

[3] J.-J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and counter-measures for smart cards," in *Smart Card Programming and Security*. Berlin, Germany: Springer, Sep. 2001, pp. 200–210, doi: 10.1007/3-540-45418-7_17.

[4] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2001, pp. 251–261.

[5] F.-X. Standaert, S. B. Örs, and B. Preneel, "Power analysis of an FPGA," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2004, pp. 30–44.

[6] T. Plos, "Susceptibility of UHF RFID tags to electromagnetic analysis," in *Topics in Cryptology—CT-RSA*. Berlin, Germany: Springer, 2008, pp. 288–300.

[7] A. R. Kazmi, M. Afzal, M. F. Amjad, H. Abbas, and X. Yang, "Algebraic side channel attack on trivium and grain ciphers," *IEEE Access*, vol. 5, pp. 23958–23968, 2017, doi: 10.1109/ACCESS.2017.2766234.

[8] A. F. Rodriguez, L. H. Encinas, A. M. Munoz, and B. A. Alcazar, "A modular and optimized toolbox for side-channel analysis," *IEEE Access*, vol. 7, pp. 21889–21903, 2019, doi: 10.1109/ACCESS.2019.2897938.

[9] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, "Practical second-order DPA attacks for masked smart card implementations of block ciphers," in *Topics in Cryptology—CT-RSA*. Berlin, Germany: Springer, 2006, pp. 192–207.

[10] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2001, pp. 309–318.

[11] P.-A. Fouque, S. Kunz-Jacques, G. Martinet, F. Muller, and F. Valette, "Power attack on small RSA public exponent," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2006, pp. 339–353.

[12] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks of modular exponentiation in smartcards," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 1999, pp. 144–157.

[13] R. Xu, L. Zhu, A. Wang, X. Du, K.-K.-R. Choo, G. Zhang, and K. Gai, "Side-channel attack on a protected RFID card," *IEEE Access*, vol. 6, pp. 58395–58404, 2018, doi: 10.1109/ACCESS.2018.2870663.

[14] M. Zhao and G. E. Suh, "FPGA-based remote power side-channel attacks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2018, pp. 229–244, doi: 10.1109/SP.2018.00049.

[15] W. Wang, Y. Yu, F.-X. Standaert, J. Liu, Z. Guo, and D. Gu, "Ridge-based DPA: Improvement of differential power analysis for nanoscale chips," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1301–1316, May 2018, doi: 10.1109/TIFS.2017.2787985.

[16] S. Mangard, "Hardware countermeasures against DPA—A statistical analysis of their effectiveness," in *Topics in Cryptology—CT-RSA*. Berlin, Germany: Springer, 2004, pp. 222–235, doi: 10.1007/978-3-540-24660-2_18.

[17] A. Barenghi, G. Pelosi, and Y. Teglia, "Improving first order differential power attacks through digital signal processing," in *Proc. 3rd Int. Conf. Secur. Inf. Netw. (SIN)*, Taganrog, Russian, Sep. 2010, pp. 124–133, doi: 10.1145/1854099.1854126.

[18] C. Archambeau, E. Peeters, F. Standaert, and J. Quisquater, "Template attacks in principal subspaces," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, vol. 4249, 2006, pp. 1–14.

[19] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2000, pp. 252–263.

[20] C. Herbst, E. Oswald, and S. Mangard, "An AES smart card implementation resistant to power analysis attacks," in *Applied Cryptography and Network Security*. Berlin, Germany: Springer, 2006, pp. 239–252.

[21] J. Ai, Z. Wang, X. Zhou, and C. Ou, "Improved wavelet transform for noise reduction in power analysis attacks," in *Proc. IEEE Int. Conf. Signal Image Process. (ICSIP)*, Aug. 2016, pp. 602–606, doi: 10.1109/SIPROCESS.2016.7888333.

[22] N. Debande, Y. Souissi, M. A. E. Aabid, S. Guilley, and J.-L. Danger, "Wavelet transform based pre-processing for side channel analysis," in *Proc. 45th Annu. IEEE/ACM Int. Symp. Microarchitecture Workshops*, Dec. 2012, pp. 32–38, doi: 10.1109/MICROW.2012.15.

[23] C. H. Gebotys and B. A. White, "A phase substitution technique for DEMA of embedded cryptographic systems," in *Proc. 4th Int. Conf. Inf. Technol. (ITNG)*, Apr. 2007, pp. 868–869, doi: 10.1109/ITNG.2007.16.

[24] C. H. Gebotys, S. Ho, and C. C. Tiu, "EM analysis of Rijndael and ECC on a wireless Java-based PDA," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2005, pp. 250–264, doi: 10.1007/11545262_19.

[25] T. Kasper, D. Oswald, and C. Paar, ''Side-channel analysis of cryptographic RFIDs with analog demodulation,'' in *RFID. Security and Privacy*. Berlin, Germany: Springer, 2012, pp. 61–77, doi: 10.1007/978-3-642-25286-0_5.

[26] L. Batina, J. Hogenboom, and J. G. J. van Woudenberg, ''Getting more from PCA: First results of using principal component analysis for extensive power analysis,'' in *Topics in Cryptology—CT-RSA*. Berlin, Germany: Springer, 2012, pp. 383–397.

[27] E. Brier, C. Clavier, and F. Olivier, ''Correlation power analysis with a leakage model,'' in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2004, pp. 16–29, doi: 10.1007/978-3-540-28632-5_2.

[28] C. Clavier, B. Feix, G. Gagnerot, C. Giraud, M. Roussellet, and V. Verneuil, ''ROSETTA for single trace analysis,'' in *Progress in Cryptology—INDOCRYPT*. Berlin, Germany: Springer, 2012, pp. 140–155.

[29] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, and V. Verneuil, ''Horizontal correlation analysis on exponentiation,'' in *Proc. 12th Int. Conf. Inf. Commun. Secur.*, Dec. 2010, pp. 46–61. [Online]. Available: https://hal.inria.fr/inria-00540384/

[30] J.-Y. Park, D.-G. Han, O. Yi, and J. Kim, ''An improved side channel attack using event information of subtraction,'' *J. Netw. Comput. Appl.*, vol. 38, pp. 99–105, Feb. 2014, doi: 10.1016/j.jnca.2013.05.001.

[31] L. Zhou, D. Sun, Z. Wang, and C. Ou, ''A method based on singular value decomposition for enhancement of differential power analysis,'' *Chin. J. Electron.*, vol. 45, no. 9, pp. 2250–2255, 2017

[32] S. Chari, J. R. Rao, and P. Rohatgi, ''Template attacks,'' in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2003, pp. 13–28, doi: 10.1007/3-540-36400-5_3.

[33] H. Zhang and Y. Zhou, ''How many interesting points should be used in a template attack?'' *J. Syst. Softw.*, vol. 120, pp. 105–113, Oct. 2016, doi: 10.1016/j.jss.2016.07.028.

[34] Z. Wang, P. Zhang, C. Chen, and H. Hu, ''Pre-processing of power traces in power analysis,'' *Chin. J. Commun. Technol.*, vol. 50, no. 4, pp. 765–770, 2017.

[35] W. Shan, S. Zhang, and Y. He, ''Machine learning based side-channel-attack countermeasure with Hamming-distance redistribution and its application on advanced encryption standard,'' *Electron. Lett.*, vol. 53, no. 14, pp. 926–928, Jul. 2017, doi: 10.1049/el.2017.1460.

[36] A. Moradi, S. Guilley, and A. Heuser, ''Detecting hidden leakages,'' in *Applied Cryptography and Network Security*. Berlin, Germany: Springer, 2014, pp. 324–342.

[37] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, ''Introduction to differential power analysis,'' *J. Cryptogr. Eng.*, vol. 1, no. 1, pp. 5–27, 2011, doi: 10.1007/s13389-011-0006-y.

[38] F.-X. Standaert, T. G. Malkin, and M. Yung, ''A unified framework for the analysis of side-channel key recovery attacks,'' in *Advances in Cryptology—EUROCRYPT 2009*, vol. 5479. Berlin, Germany: Springer, 2009, pp. 443–461.

[39] Y. Kim and H. Ko, ''Using principal component analysis for practical biasing of power traces to improve power analysis attacks,'' in *Information Security and Cryptology—ICISC 2013*. Cham, Switzerland: Springer, 2014, pp. 109–120, doi: 10.1007/978-3-319-12160-4_7.

XIAOMIN CAI was born in Guzheng, Anhui, China, in 1989. She received the B.E. degree in machine design from the Anhui University of Architecture, Hefei, China, in 2012, and the M.E. degree in software engineering from the National University of Defense Technology, Changsha, China, in 2015. She is currently pursuing the Ph.D. degree with the College of Computer Science and Electronic Engineering, Hunan University, China. Her main research interests include VISI design and side channel attacks techniques.

RENFA LI (Senior Member, IEEE) was born in 1957. He received the B.E. and M.E. degrees from Tianjin University, Tianjin, China, and the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China.

He is currently a Professor of computer science and electronic engineering and the Dean of the College of Computer Science and Electronic Engineering, Hunan University, China. He is also the Director of the Key Laboratory for Embedded and Network Computing of Hunan Province, China. He is also an Expert Committee Member of the National Supercomputing Center, Changsha, China. His major research interests include computer architectures, embedded computing systems, cyber-physical systems, and the Internet of Things. He is a member of the council of CCF and a Senior Member of ACM.

SHIJIE KUANG was born in Changsha, Hunan, China, in 1986. He received the B.E. degree in communication design from Hunan University, Changsha, China, in 2009, and the M.E. degree in software engineering from the National University of Defense Technology, Changsha, in 2015. He is currently pursuing the Ph.D. degree with the College of Computer Science and Electronic Engineering, Hunan University, and the Academy of Military Sciences PLA China.

From 2009 to 2011, he was a Mobile Phone Engineer in Shenzhen. From 2015 to 2019, he was worked with the National Supercomputing Center, Changsha. His main research interests include network engineering and information security, VLSI design, and high-performance computing.

JINHUI TAN was born in Hengyang, Hunan, China, in 1991. She received the B.E. degree in IC design and systems integration from Huaqiao University, Xiamen, China, in 2013, and the M.E. degree in microelectronics and solid state electronics from Guizhou University, Guiyang, China, in 2013. She is currently pursuing the Ph.D. degree with the College of Computer Science and Electronic Engineering, Hunan University, China. Her main research interest is in mixed-signal IC design.