A Wavelet-based Power Analysis Attack against Random Delay Countermeasure

Xiaofei Dong*†, Fan Zhang*†‡, Samiya Queshi*, Yiran Zhang*, Ziyuan Liang*‡, Bolin Yang* and Feng Gao§
*College of Information Science & Electronic Engineering, Zhejiang University, Hangzhou, 310027, China
†State Key Laboratory of Cryptology, P.O.Box 5159, Beijing, 100878, China
‡Institute of Cyberspace Research, Zhejiang University, Hangzhou, 310027, China
§Hangzhou National Chip Science & Technology Co. Ltd., Hangzhou, 310012, China
Corresponding Author: Fan Zhang, email: fanzhang@zju.edu.cn

***Abstract*—Random delay insertion is a simple yet rather effective technique to increase the difficulty for traditional power analysis. However as compared to the random masking technique, it is uncommonly used as a countermeasure considering the frequency analysis. In this paper, it is investigated that the frequency analysis may not work as efficiently as expected when facing to advanced random delay countermeasures. Hence, a novel attack is proposed which is in the wavelet domain. After preprocessing the wavelet coefficients of power traces with wavelet decomposition, the effects of multiple random delays can be removed. Two attack strategies are proposed to recover the secret key: either indirectly from the reconstructed power traces without random delays or directly from the processed wavelet coefficients. Our experimental results show that the wavelet-based power analysis attack can perform much better than those frequency-based ones, which is evaluated through several standard metrics to show the efficiency and robustness.**

***Keywords*-Wavelet attack, Wavelet preprocessing, Random delay countermeasure, Side-channel analysis, Power analysis**

I. Introduction

Side channel attack can easily recover the encryption keys using physical leakages such as power, electromagnetic emission and more. *Power analysis* [1] is one of the most powerful tools which exploits the power consumption leaked through cryptographic devices. The instantaneous power consumption is closely related to the operations or the intermediate data, so it may disclose the secret key. Differential power analysis (DPA) and correlation power analysis (CPA) [1] are two mainstream power analysis methods. To exploit the dependence of the power characteristics of cryptographic devices and the operations that are executed, the targeted parts of those power traces have to be aligned to the same position. In order to ensure the security of encryption, different countermeasures are proposed to increase the difficulty for potential attack.

In [2], *Random Delay Insertion* (RDI) countermeasure against side channel attack was proposed. Through unsynchronized power traces, random delay insertion reduces the correlation and dependence of the consumed power and the executed operations. Hence, it significantly increases the attack complexity. The research of implementation of random delays is currently trending due to its mitigation against side channel attack. In CHES 2009 and 2010, Coron et al. proposed effective countermeasures of random delays in [3] and [4], which are our main targets and will be elaborated in Section III.

A. Related Work

Traditional attack methods against random delay countermeasures are divided into two categories. One is to attack the power traces in time domain as usual after aligning the power traces. Kocher et al. proposed the static alignment in [1] which is easy to execute, but it mainly works in the scenario of intrinsic jitter and small delays. The elastic alignment was proposed in [5] which matches different parts at different offsets and performs nonlinear resampling of the traces. The elastic alignment has a better performance in terms of alignment yet its computational complexity is very high. Muijrers et al. proposed the rapid alignment method in [6] whose computational complexity is greatly reduced as compared to the elastic alignment. In addition, some other alignment methods based on waveform matching, pattern recognition and hidden Markov models were proposed in [7], [8] and [9]. However, the operation of alignment itself still experiences a great deterioration in performance.

The other category is to transform the power signals from time domain to frequency domain and to conduct the attack directly in frequency domain. Gebotys et al. firstly put forward differential power frequency analysis (DPFA) in [10]. The core idea is that the shifts in time domain will only cause the changes of phase spectrum in frequency domain and the amplitude spectrum will not be influenced. Then, Schimmel et al. introduced correlation power frequency analysis (CPFA) based on power spectral density of the signal, where the CPA is carried out in frequency domain [11]. However, Lu et al. showed that the frequency attack could not succeed when the maximum window size of Discrete Fourier Transform (DFT) is smaller than the length of delays [12]. So it is very critical to choose an appropriate window size for DFT in such attacks.

Previously, wavelet analysis related techniques have already been adopted to side channel attacks in practice. Most of them are about denoising [13]–[16], which improves the performance of attack to a certain extent. Furthermore, the idea of recovering the keys based on wavelet coefficients was proposed in [17] for the first time. However, it could only be applied to those implementations without countermeasures and the concrete method was not detailed. Recently, the machine

978-1-5386-7471-0/18/$31.00 ©2018 IEEE

learning technique is applied to those side channel attacks using wavelet transform. For example, in [18], the power traces are preprocessed using wavelet transform and then used to train the probabilistic neural network (PNN). In [19], wavelet analysis and support vector machine (SVM) algorithm were linked and wavelet SVM was used to recover the keys of unmasked or masked ASE implementations. So, the wavelet analysis becomes more and more important in side channel attack and a new type of novel application of wavelet analysis is explored in this paper.

B. Contribution

Our contribution can be summarized as below:

- We propose a new processing method using wavelet decomposition which can efficiently improve the attack on the multiple random-delay countermeasure. After transforming the power traces to wavelet coefficients, random delays can be distinguished from other encryption operations clearly and removed.
- We propose two attack strategies to retrieve the secret keys based on wavelet analysis. The first one is to indirectly attack the time domain signals reconstructed from wavelet coefficients. The other is to directly attack the processed wavelet coefficients in wavelet domain.
- Through physical experiments on microcontrollers, we evaluate the performance of the two types of wavelet-based attacks. Our experimental analysis showed that wavelet-based attacks have a better performance in comparison to those frequency-based ones.

C. Organization

This paper is organized as follows: Section II gives the background of wavelet analysis. Section III introduces our implementation of random delay countermeasure and explains the attack difficulty. Section IV describes our proposal that is based on wavelet decomposition and two attack strategies based on wavelet analysis. Section V demonstrates the experimental results and the performance of wavelet-based attack. Section VI concludes the paper.

II. Background of Wavelet Analysis

Wavelet analysis can provide time and frequency analysis of a signal based on variant time resolution and frequency resolution. It describes the similarity of a time domain signal $f(t)$ using a wavelet basis function ψ with two parameters: s (scaling) and l (shift). Eq.(1) shows an example of wavelet basis function called as *mother wavelet*. Eq.(2) is the definition of wavelet transform where the transformation WT is calculated as the integration of the product of $f(t)$ and ψ.

$$\psi_{l,s}(t) = \frac{1}{\sqrt{s}}\psi(\frac{t-l}{s}) \tag{1}$$

$$WT(s,l) = \frac{1}{\sqrt{s}}\int_{-\infty}^{+\infty} f(t) * \psi(\frac{t-l}{s})dt \tag{2}$$

The wavelet decomposition of a signal consists of two processes: filtering and down-sampling operations. The signal $f(t)$ is initially filtered though a low pass filter LPF and a high pass filter HPF. Then in order to remove the redundant information, each filtered signal is down-sampled by two. Therefore, the time signal is transformed into two parts: the detailed wavelet coefficients (cD_i) and the approximation wavelet coefficients (cA_i), where i is the decomposition level. Note that cA_i can be further decomposed at the $(i+1)$ level, denoted as cD_{i+1} and cA_{i+1}. If three levels decomposition are applied to a signal, cA_3, cD_3, cD_2, cD_1 are obtained, which can represent the whole information of this signal. The approximation wavelet coefficients cA_i generally represent patterns and pivotal information of the signal and they are critical to side channel attack. While, cD_i generally represent noise and irrelevant information in attacks.

Conversely, wavelet coefficients cA_i and cD_i can be reconstructed to time domain signals A_i and D_i using inverse discrete wavelet transform (IDWT). For example, cA_3 can be reconstructed to A_3, cD_3 can be reconstructed to D_3 and so on. And $f(t) = A_3 + D_3 + D_2 + D_1$.

III. Random Delay Countermeasure

Inserting the constructed random delays will influence the performance of countermeasure against side channel attacks. Therefore, it is important to select appropriate strategies to ensure the effectiveness.

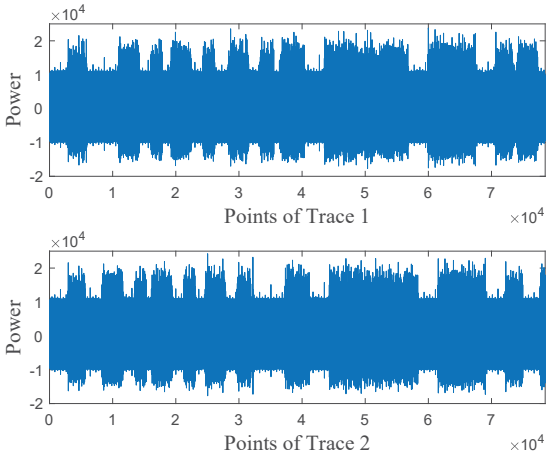


Fig. 1. Two illustrative power traces inserted with four random delays.

A. Our Implementation of Random Delays

In CHES 2009, a new method of construction and insertion of random delays called Float Mean (FM) is proposed in [3] which is more secure and lightweight in software. With the same mean, it can generate a much greater variance. However, it was pointed out in [4] that the parameters chosen of Float Mean were inappropriate and the Improved Float Mean scheme was proposed, which is also adopted in our experiments. Random delays are generated according to those assembly codes given by [4]. Considering the trade-off between the performance and overhead merely for the purpose of illustration, 4 random delays are inserted into the 16 S-Box

lookups in the first round of AES cipher, which is also the same target as in [3] and [4]. Fig. 1 shows two illustrative power traces inserted with random delays which are referred to as Trace 1 and 2, respectively. It is observed that 16 lookups are separated randomly due to those delays and the operations in these two encryptions are not synchronous.

B. The Difficulty In Attacking Against Random Delays

It is not easy to adopt a direct DPA or CPA attack on those power traces with multiple random delays because the instantaneous power consumption of the same moment is not caused by the same operation. Even though in theory, the RDI countermeasure cannot prevent the leakages completely. In practice, it can cause great difficulty in key recovery. For example, it requires more coverage of points of interest, more pattern recognitions of target operation, and more alignments to compensate the side-effect of delays.

Trace alignments and frequency attacks are normally considered as efficient mitigations against RDI. Unfortunately, there are some shortcomings to be discussed in following descriptions.

As for trace alignments, it is difficult to align all the traces completely if the random delays are complex enough. In terms of multiple delay insertions, multiple alignments have to be conducted, each of which has to go through all traces. In addition, the process of alignment itself is time consuming, so that the attack efficiency is quite low.

As for frequency attacks, DPFA could not succeed when the window size of DFT is smaller than the length of delays as mentioned in [12]. Moreover, frequency analysis completely discards the time information which can actually be well exploited in traditional side channel analysis. For instance, in DPFA, attackers can not know at which moment the target operation is executed. As claimed in [1], whether frequency attack works well or not essentially depends on the spectral characteristics of the leakage and the random delays.

Due to the listed difficulties of those mainstream analysis on random delay countermeasures, it is interesting and worth to explore a new type of analysis, which could enhance the attack efficiency especially towards those multiple insertions.

IV. Our Wavelet-based Analysis on RDI

In this section, a novel wavelet-based attack is introduced which includes two procedures: preprocessing of traces to remove the random delays and key recovery from processed wavelet coefficients or reconstructed power traces.

A. Trace Preprocessing based on Wavelet Decomposition

Wavelet analysis is a powerful tool to identify the characteristics of signals using wavelet coefficients. The underlying fact is that the power dissipation of random delays and encryption operations have different wavelet characteristics. Therefore, the main objective is to determine the threshold of differentiation and also to apply this thresholding to remove random delays.

Various characteristics of signals can be represented with different wavelet decomposition levels and wavelet function families, including Haar, Daubechies (dbN), Mexican Hat (mexh), Morlet, Meyer and so on. Since the power consumption of random delays is smaller than that of the encryption operations, the granularity of the power amplitude is very important in identifying delays. Observed by multiple experiments since the db9 wavelet function (one of the Daubechies family where $N = 9$) can depict the amplitude features more clearly, it is selected to fulfill the wavelet decomposition. Note that in theory, with the increase of decomposition levels, the frequency resolution will increase and the time resolution will decrease. Therefore, the level of decompositions should be appropriately chosen to satisfy the requirements of resolutions. According to our empirical experience, the features of random delays can not be obviously distinguished from others until the level of decomposition reaches at 8. Hence 8 levels are finally applied to all decompositions throughout this paper.

Suppose the whole power trace is denoted as $h(t)$ which consists of the random delay part $f(t)$ and the encryption part $g(t)$. The method to find the differentiating threshold is listed in Algorithm 1. Discrete wavelet transform (DWT) is applied to $f(t)$ and $g(t)$, respectively. Due to the difference of amplitude features, $cA8_{f(t)}(i)$, the coefficients for $f(t)$, are distinctively smaller than that for encryption operations $cA8_{g(t)}(i)$. Through calculating the maximum value of wavelet coefficients corresponding to random delays (denoted as A) and the minimum value corresponding to encryption operations (denoted as B), the differentiating threshold T to be determined will be narrowed down within the range of $[A, B]$. In order to keep as much information for encryption as possible, the final thresholding T is empirically chosen as the mean of A and B, which is verified in experiments.

Algorithm 1: The method to find the thresholding

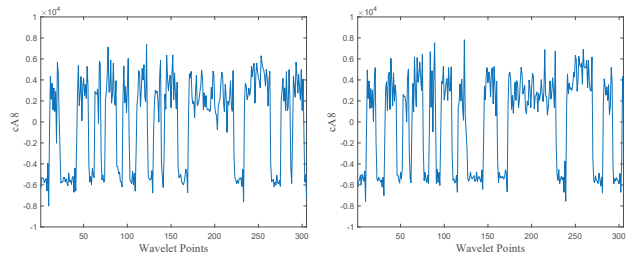
1: Random Delays: $f(t)$; Encryption Operations:$g(t)$;
2: $DWT(f(t)) \rightarrow cA8_{f(t)}(i), i \in [0, length(f(t))/2^8]$;
3: $DWT(g(t)) \rightarrow cA8_{g(t)}(i), i \in [0, length(g(t))/2^8]$;
4: $max(cA8_{f(t)}(i)) \rightarrow A$;
5: $min(cA8_{g(t)}(i)) \rightarrow B$;
6: THRESHOLD: $T \in [A, B]$;
7: THE FINAL THRESHOLD: $T = (A + B)/2$;

The procedure of trace processing using the threshold T is detailed in Algorithm 2. First, those power traces $h(t)$ are transformed to wavelet coefficients $cA8_{h(t)}(i)$ through DWT. Then some comparisons are conducted: if $cA8_{h(t)}(i)$ is less than T, this wavelet coefficient is discarded; otherwise it is reserved. During this process, some points in wavelet domain are removed, where the rest can be denoted as $cA8_{processed}$. As a result, the influences of random delays are eliminated and $cA8_{processed}$ actually correspond to the encryption operations.

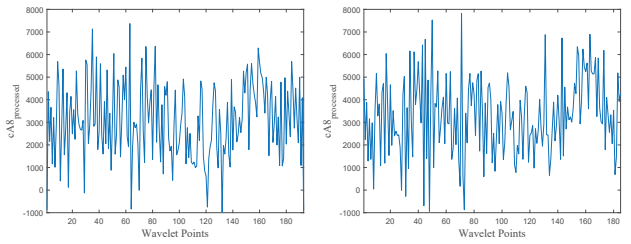
Fig. 2 shows the results of wavelet decomposition and the trace processing of those two traces in Fig. 1. The results of wavelet decomposition using db9 and the decomposition level of 8 are shown in Fig. 2(a) and 2(b), where the features of random delays and encryptions can be clearly identified. Fig. 2(c) and 2(d) depict two wavelet coefficient traces where all the random delays are removed using the differentiating

Algorithm 2: The procedure of traces preprocessing

1: Power Traces: $h(t) = f(t) + g(t)$;
2: $DWT(h(t)) \rightarrow cA8_{h(t)}(i), i \in [0, length(h(t))/2^8]$;
3: **for** $i = 1; i < length(cA8_{h(t)}(i)); i++$ **do**
4: **if** $cA8_{h(t)}(i) > T$ **then**
5: $cA8_{processed}(k) = cA8_{h(t)}(i)$;
6: $k = k + 1$;
7: **end if**
8: **end for**



(a) Wavelet decomposition of Trace 1 (b) Wavelet decomposition of Trace 2



(c) Wavelet processing of Trace 1 (d) Wavelet processing of Trace 2

Fig. 2. Wavelet decomposition of two power traces with random delays and traces processing to remove random delays.

threshold T. The two traces become quite similar, and those $cA8_{processed}$ of both traces are synchronized.

B. Key Recovery based on Wavelet Analysis

After the trace processing, only synchronous wavelet coefficients are kept rather than time domain power traces, which can be used in further analysis. Two attack strategies are proposed. One is to attack the power traces reconstructed from wavelet coefficients. The another is to attack the processed wavelet coefficients directly in wavelet domain.

Strategy 1*: Indirect attack on power traces reconstructed from wavelet coefficients.* A set of time-domain power traces, denoted as $r(t)$, can be reconstructed from the processed wavelet coefficients $cA8_{processed}$ through IDWT. Note that, random delays have been removed from those $r(t)$. Fig. 3 shows two reconstructed power traces after processing those in Fig. 1. These two power traces are synchronized well so that the mitigation from RDI countermeasure is minimized to some extent. Thus, $r(t)$ can be used to retrieve the keys as traditional DPA or CPA. The results of this attack strategy are shown in Section V.

Strategy 2*: Direct attack on wavelet coefficients.* In this case, the processed wavelet coefficients $cA8_{processed}$ can be

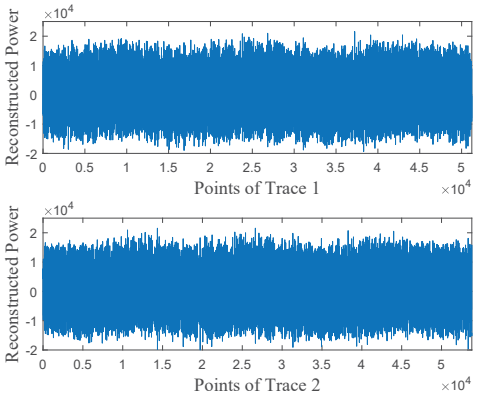


Fig. 3. Two power traces reconstructed from $cA8_{processed}$.

directly used to deduce the keys. This is because they still preserve most of the useful information of original power traces and each $cA8_{processed}$ is synchronous. Algorithm 3 describes the practical attack process in wavelet domain. First, for each key hypothesis $key_{hypothesis}$, the hypothetical intermediate value $V_{i,j}$ is calculated as the output of S-Box table lookup. Then the hypothetical power consumption value $H_{i,j}$ is calculated from $V_{i,j}$, assuming that the hamming weight power model is used. N is the number of power traces and L is the length of $cA8_{processed}$. Finally, the correlation between $H_{i,j}$ and $cA8_{processed}$ is computed. The hypothesis with the maximal coefficient might be the correct key byte. The results of this attack strategy are shown in Section V.

Algorithm 3: The procedure of wavelet attack

1: **for** $key_{hypotheses} = 0$ to 255 **do**
2: $V_{i,j} = SBOX(plaintext \oplus key_{hypothesis}), i = 1..N, j = 1..256$;
3: **end for**
4: **for** each $V_{i,j}$ **do**
5: $H_{i,j} = HW(V_{i,j}), i = 1..N, j = 1..256$;
6: **end for**
7: **for** each wavelet point in $cA8_{processed}$ **do**
8: $r_{j,k} = corr(H_{i,j}, cA8_{processed}(k)), j = 1..256, k = 1..L$;
9: **end for**

Summary*:* The reconstructed traces contain more information than wavelet coefficients, so Strategy 1 should be better than Strategy 2 in terms of the number of key bytes to be extracted. However, note that the time of key recovery is proportional to the length of traces. Since the length of reconstructed signals is far greater than that of wavelet coefficients, it takes more time for analysis using Strategy 1. Whether to choose Strategy 1 or 2 is just an appropriate trade-off to be balanced, considering the experimental factors and those resources available in practical attacks.

V. Experiments and Evaluations

To illustrate the performance of proposed attack, four standard metrics are used to fairly evaluate practical attack results. The first is the minimum traces to detect the correct key byte (MTD). The second is the maximum correlation coefficient value of the correct key byte (MCV). The third is the minimum

time to recover the key byte (MTR). And, the last is the time of traces preprocessing (TOP).

A. Measurement Setup

To measure the power leakage of cryptographic devices, the side-channel attack standard evaluation board (SASEBO-W) is served as our main experiment platform. The AES-128 with random delay countermeasure is implemented in the Atmega163 microcontroller inside a smartcard. In addition, an oscilloscope (Agilent DSO-X3034T) is used to collect the power traces whose bandwidth is 350MHz and the maximum sampling frequency is 5GSa/s. Here 10000 power traces are collected at a sampling rate of 100MHz. The offline key recovery is implemented in MATLAB2017b.

B. Experimental Results of Strategy 1

Fig. 4(a) and 4(d) show the results of applying Strategy 1 to recover the first byte of the secret key. In Fig. 4(a), the correlation coefficient is significantly larger than the rest when the number of power traces is 134. So, MTD for this case is 134. Fig. 4(d) shows that there is a visible peak of correlation coefficient at the 3965th point. It can be concluded that the encryption using the first key byte is executed roughly around the 3965th time point. And from the value of this peak, it can be seen that MCV is about 0.4911. Recorded by MATLAB, the time to recover the first key byte (MTR) is 3383.4 seconds. In this case, TOP is 151.3 seconds, which includes the time for wavelet decomposition, wavelet coefficients reduction, and the reconstruction from remained wavelet coefficients.

TABLE I
COMPARISONS OF ATTACKS AGAINST RDI COUNTERMEASURE.

Attack Method	MTD	MCV	MTR	TOP
Reconstructed Signals (Strategy 1)	**134**	**0.4911**	3383.4	151.3
Wavelet Domain (Strategy 2)	554	0.2014	**48.7**	131.8
Frequency Domain	1230	0.095	3121.3	30.5

C. Experimental Results of Strategy 2

Similarly, Fig. 4(b) and 4(e) show the attack results in wavelet domain using Strategy 2. Four metrics are shown in the second row of Table I. It can be seen that even if the number of traces required is larger and the peak is smaller than those with Strategy 1, the effect of using Strategy 2 is still outstanding. Note that the time to recover the key byte using Strategy 2 (MTR=48.7) is about 70x times smaller than that with Strategy 1 (MTR=3383.4), which is a significant improvement of performance. Moreover, the reconstruction is not required in the preprocessing of traces, so it saves more time when the attack is on the wavelet coefficients directly.

D. Performance Comparison to Frequency Attack

To evaluate the performance of wavelet-based attack (both Strategy 1 and 2) against random delays, the more commonly used frequency attack is performed. The results are shown in Fig. 4(c) and 4(f), and the detailed values of metrics are listed in the third row of Table I. With 1230 traces, the MCV for frequency attack is only about 0.095, resulting in the difficulty of detecting the target peak that should be ideally distinct from the noise. More specifically, there exist many peaks in Fig. 4(f), which lead to a weak correlation. This is mainly because the frequency of encryption operations is scattered to multiple points in the frequency domain.

Generally speaking, as shown in Fig. 4, the performance of wavelet-based attack is better than that in frequency domain, no matter the attack is indirectly based on the reconstructed signals or directly based on the wavelet coefficients. In addition, attacks on reconstructed signals (Strategy 1) could have a better value of MTD and MCV. However, the MTR is relatively larger because the length of reconstructed signals reaches 50190. In contrast, attacks in wavelet domain (Strategy 2) can lead to a very small MTR because the length of processed wavelet coefficients is only 200. Due to operations of preprocessing based on wavelet analysis, it consumes a little more additional time to process traces than frequency attack. However, the cost of preprocessing is relatively small and its contribution to key analysis is of much more importance.

E. Robustness Verification of Wavelet-based Attack

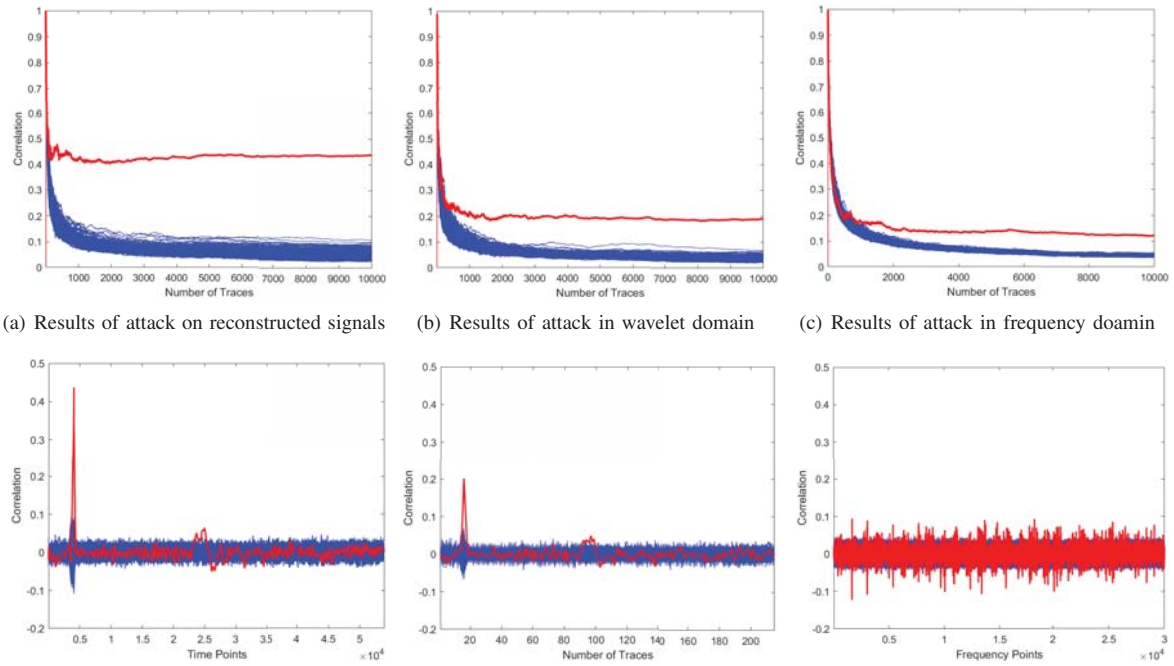
In order to prove the robustness of wavelet-based attack against random delay countermeasure, 10 repeated instances of experiments are carried out. In each instance, 10000 power traces are collected and multiple delays are inserted into the first round of AES randomly. Table II shows the number of disclosed bytes of the full 16-byte master key with wavelet-based attacks. The average number of those recovered key bytes is about 15.5 and 14.6 for attacks on reconstructed traces and in wavelet domain, respectively. Both variances are small enough so the proposed attacks can be considered as robust.

TABLE II
THE STATISTICS OF THE RECOVERED KEY BYTES FOR 10 INSTANCES.

Instance	Strategy 1	Strategy 2
1	15	14
2	16	15
3	16	16
4	15	14
5	15	15
6	16	14
7	16	15
8	16	16
9	15	15
10	15	14

VI. CONCLUSION

In this paper, a novel wavelet-based attack method is proposed against random delay countermeasure. After processing the wavelet coefficients based on wavelet decomposition, the multiple random delays can be removed. Two different strategies (indirect and direct attacks) are also proposed. Our experimental results show that: (1) wavelet-based attacks with both strategies perform much better than those in frequency domain (2) Attacks on the processed wavelet coefficients can



(a) Results of attack on reconstructed signals (b) Results of attack in wavelet domain (c) Results of attack in frequency doamin

(d) Results of attack on reconstructed signals (e) Results of attack in wavelet domain (f) Results of attack in frequency doamin

Fig. 4. The results of three types of attack against random delays.

recover the keys very efficiently as compared with those on the reconstructed signals.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under the grants 61472357, 61571063, in part by the Open Fund of State Key Laboratory of Cryptology and in part by the Fundamental Research Funds for the Central Universities under the grant 2018QNA5005.

REFERENCES

[1] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008.

[2] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2000, pp. 252–263.

[3] J.-S. Coron and I. Kizhvatov, "An efficient method for random delay generation in embedded software," in *Cryptographic Hardware and Embedded Systems-CHES 2009*. Springer, 2009, pp. 156–170.

[4] ——, "Analysis and improvement of the random delay countermeasure of CHES 2009," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2010, pp. 95–109.

[5] J. G. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Cryptographers' Track at the RSA Conference*. Springer, 2011, pp. 104–119.

[6] R. A. Muijrers, J. G. van Woudenberg, and L. Batina, "RAM: Rapid alignment method," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2011, pp. 266–282.

[7] S. Nagashima, N. Homma, Y. Imai, T. Aoki, and A. Satoh, "DPA using phase-based waveform matching against random-delay countermeasure," in *Circuits and Systems, 2007. ISCAS 2007. IEEE International Symposium on*. IEEE, 2007, pp. 1807–1810.

[8] D. Strobel and C. Paar, "An efficient method for eliminating random delays in power traces of embedded software," in *International Conference on Information Security and Cryptology*, 2011, pp. 48–60.

[9] F. Durvaux, M. Renauld, F.-X. Standaert, L. v. O. tot Oldenzeel, and N. Veyrat-Charvillon, "Efficient removal of random delays from embedded software implementations using hidden markov models," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2012, pp. 123–140.

[10] C. H. Gebotys, C. C. Tiu, and X. Chen, "A countermeasure for EM attack of a wireless PDA," in *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, vol. 1. IEEE, 2005, pp. 544–549.

[11] O. Schimmel, P. Duplys, E. Boehl, J. Hayek, R. Bosch, and W. Rosenstiel, "Correlation power analysis in frequency domain," in *COSADE 2010 First International Workshop on Constructive SideChannel Analysis and Secure Design*, 2010.

[12] Y. Lu, K. Boey, M. O'Neill, J. V. McCanny, and A. Satoh, "Is the differential frequency-based attack effective against random delay insertion?" in *Signal Processing Systems, 2009. SiPS 2009. IEEE Workshop on*. IEEE, 2009, pp. 051–056.

[13] H. Patel and R. Baldwin, "Differential power analysis using wavelet decomposition," in *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*. IEEE, 2012, pp. 1–5.

[14] X. Charvet and H. Pelletier, "Improving the DPA attack using wavelet transform," in *NIST Physical Security Testing Workshop*, vol. 46, 2005.

[15] W. Liu, L. Wu, X. Zhang, and A. Wang, "Wavelet-based noise reduction in power analysis attack," in *Computational Intelligence and Security (CIS), 2014 Tenth International Conference on*, 2014, pp. 405–409.

[16] J. Ai, Z. Wang, X. Zhou, and C. Ou, "Improved wavelet transform for noise reduction in power analysis attacks," in *Signal and Image Processing (ICSIP), IEEE International Conference on*. IEEE, 2016, pp. 602–606.

[17] N. Debande, Y. Souissi, M. A. El Aabid, S. Guilley, and J.-L. Danger, "Wavelet transform based pre-processing for side channel analysis," in *Microarchitecture Workshops (MICROW), 2012 45th Annual IEEE/ACM International Symposium on*. IEEE, 2012, pp. 32–38.

[18] P. Saravanan and P. Kalpana, "A novel approach to attack smartcards using machine learning method," *Journal of Scientific & Industrial Research*, vol. 76, no. 2, pp. 95–99, 2017.

[19] S. Hou, Y. Zhou, H. Liu, and N. Zhu, "Wavelet support vector machine algorithm in power analysis attacks," *Radioengineering*, vol. 26, no. 3, pp. 890–902, 2017.