POSTER: A Novel Wavelet Denoising Method Based on Robust Principal Component Analysis in Side Channel Attacks

Juan Ai[1,2], Zhu Wang[1(✉)], Xinping Zhou[1,2], and Changhai Ou[1,2]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, People's Republic of China
{aijuan,wangzhu,zhouxinping,ouchanghai}@iie.ac.cn
[2] University of Chinese Academy of Sciences, Beijing, People's Republic of China

Abstract. In the context of side channel attacks (SCA), multiple preprocessing methods proposed are used to improve the quality of measurements and enhance the attack performance. Different from existing preprocessing methods which accord to the spectral distribution of noise or depend on some objective functions to search optimal linear transform, we treat noise as an ensemble and separate it by discrete wavelet transform and robust principal component analysis (RPCA) blindly. All experiments show that the proposed method has a great impact on the noise reduction of a typical hardware implementation of AES when comparing to some existing methods.

Keywords: Side channel attacks · Robust principal component analysis · Wavelet transform · Denoising

1 Introduction

Noise in side channel attacks (SCA) has been a hot topic since the threat is posed. Not only the multiple kinds of noise affect the analysis performance but also can be difficult to deal with efficiently. Actually, measurements from the device under target (DUT) are contaminated by different noise.

One solution to noise reduction is based on signal processing tools, including but not limited to wavelet transform (WT) [6], empirical mode decomposition (EMD) [4], least squares [3]. The majority of them consider that the leakage concentrates on specific frequencies. However, the commonly used threshold for filtering out interference frequencies limits the denoising efficiency. The other one is the method related to linear transform. For example, a known technique for dimension reduction, i.e., principal component analysis (PCA), is used to preprocess raw measurements [5] in SCA. The biggest challenge of PCA is that the principal components may not contain the most useful leakages, which results that less confidential data can be retrieved eventually.

In this paper, we propose a novel denoising method that combine the discrete wavelet transform and robust principal component analysis before performing

R. Deng et al. (Eds.): SecureComm 2016, LNICST 198, pp. 766–769, 2017.
DOI: 10.1007/978-3-319-59608-2_47

correlation power analysis (CPA). A comparison is made between the proposed method and some existing methods on a typical hardware implementation of AES. The proposed method outperforms other denoising methods significantly.

2 Background

2.1 Robust Principal Component Analysis

For a data matrix $X \in \Re^{m\times n}$ composed of a low-rank matrix L and a sparse matrix S, for the purpose of separation, the problem can be formulated by

$$\begin{aligned} \min_{L,S\in\Re^{m\times n}} \quad & rank(L) + \lambda \| S \|_0 \\ s.t. \quad & X = L + S, \end{aligned} \tag{1}$$

where $rank(\cdot)$ is the rank of a matrix, $\| \cdot \|_0$ is the number of non-zero elements in a matrix, λ represents the parameter to balance two object functions. The problem can be solved by augmented Lagrange multiplier algorithm (ALM) for guaranteeing good accuracy and convergence as suggested by [2].

3 Proposed Denoising Method

Since wavelet transform has the advantage of transforming a signal into such a representation with only several sparse coefficients, we first transform a single trace into the wavelet domain and construct a trajectory matrix on these approximation coefficients. Then, reconstructed approximation coefficients are obtained such as follows.

Separation. For a measurement l of length T, a Hankel matrix is constructed by a window with width of N, such as

$$X_{N\times K} = \begin{pmatrix} l_0 & l_1 & l_2 & \cdots & l_{K-1} \\ l_1 & l_2 & l_3 & \cdots & l_K \\ l_2 & l_3 & l_4 & \cdots & l_K + 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ l_{N-1} & l_N & l_N + 1 & \cdots & l_{T-1} \end{pmatrix}, \tag{2}$$

where $K = T - N + 1$.

Reconstruction. A new measurement y can be obtained by averaging along cross-diagonals of the sparse matrix S, such as

$$y_t = \begin{cases} \frac{1}{t+1}\sum_{k=1}^{t+1} s^*_{k,t-k+2} & 0 \le t \le N^* - 1, \\ \frac{1}{L^*}\sum_{k=1}^{L^*} s^*_{k,t-k+2} & N^* - 1 \le t \le K^*, \\ \frac{1}{T-t}\sum_{k=t-K^*+2}^{T-K^*+1} s^*_{k,t-k+2} & K^* \le t \le T, \end{cases} \tag{3}$$

where s^* is the element of S, and $N^* = min\{N, K\}$, $K^* = max\{N, K\}$. The denoising method is summarized in Algorithm 1.

Algorithm 1. RPCA based denoising (RPCA-D)

Input: l, N (l represent a single trace, N reprents the window width)
Output: y (represent the reconstructed approximation coefficients)
1: Transform l into the wavelet domain to obtain approximation coefficients APP
2: Construct a Hankel matrix $X_{N\times K}$ on coefficients APP
3: Perform RPCA on X to obtain a sparse matrix S
4: Reconstruct y by averaging along cross-diagonals of the matrix S
5: **return** y

4 Experiment

In this section, a series of experiments on hardware implementation of AES are performed, and the actual power traces are from the second stage of DPA Contest [1]. CPA can be performed either in the wavelet domain after the proposed denoising method or in the time domain by inverse wavelet transform after the proposed one. Firstly, two analysis methods will be compared to some existing methods, including unprocessed condition, wavelet transform from [6], empirical mode decomposition from [4], trend removing from [3] and combination method from [4], and corresponding attacks are named as Unprocessed-CPA, WT-CPA, EMD-IIT-CPA, TR-CPA, EMD-IIT-TR-CPA. Success rate (SR) will be used to evaluate the analysis efficiency proposed in [7], which is widely used in the cryptographic implementation evaluation. The comparison result is shown in Fig. 1. Secondly, the proposed analysis methods will be used to preprocess the traces with different level of signal to noise ratio (SNR). It can interpret the robustness of the proposed method in denoising. The result is shown in Fig. 2.

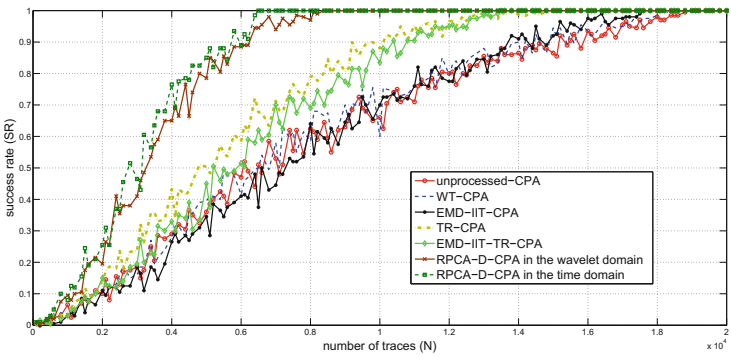
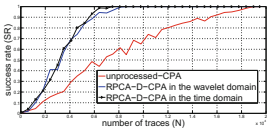
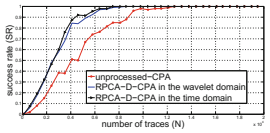


Fig. 1. Success rate of CPA by using different denoising methods

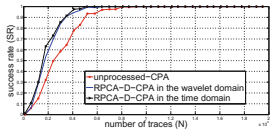
The results showed that the proposed method improves the success rate of CPA significantly both in the time domain and wavelet domain. Especially, even in the condition of low SNR, the proposed method shows excellent denoising performance.



(a) Traces with a low level of SNR



(b) Traces with a middle level of SNR



(c) Traces with a high level of SNR

Fig. 2. Success rate of CPA in different level of SNR by using the proposed denoising method

5 Conclusion

In this paper, we presented a novel denoising method that using robust principal component analysis to separate approximation coefficients in the wavelet domain. Different from the methods proposed in the open literatures, the proposed denoising method has no restriction on the type of noise or the number of power traces for parameters setting. The proposed method outperforms some existing methods significantly and has great robustness ability in denoising.

Acknowledgments. This research is supported by the Nation Natural Science Foundation of China(No.61372062).

References

1. http://www.dpacontest.org/home/
2. Candès, E.J., Li, X., Ma, Y., Wright, J.: Robust principal component analysis? J. ACM **58**(3), 11 (2011)
3. Cao, Y., Zhou, Y., Yu, Z.: On the negative effects of trend noise and its applications in side-channel cryptanalysis. Chinese J. Electron. **23**(CJE–2), 366–370 (2014). http://eprint.iacr.org/2013/102.pdf
4. Feng, M., Zhou, Y., Yu, Z.: EMD-based denoising for side-channel attacks and relationships between the noises extracted with different denoising methods. In: Qing, S., Zhou, J., Liu, D. (eds.) ICICS 2013. LNCS, vol. 8233, pp. 259–274. Springer, Cham (2013). doi:10.1007/978-3-319-02726-5_19
5. Hogenboom, J., Batina, L.: Principal component analysis and side-channel attacks-master. Thesis (2010)
6. Souissi, Y., Elaabid, M.A., Debande, N., Guilley, S., Danger, J.L.: Novel applications of wavelet transforms based side-channel analysis. In: Non-Invasive Attack Testing Workshop. Citeseer (2011)
7. Standaert, F.-X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 443–461. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_26