POSTER: Using Improved Singular Value Decomposition to Enhance Correlation Power Analysis

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

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

Abstract. Correlation Power Analysis (CPA) is one of effective means of power analysis in side channel analysis. The noisy power traces can affect the power of CPA. It is significant to select the helpful power traces to improve the efficiency of analysis. In this paper, we present a new preprocessing method that is based on Improved Singular Value Decomposition (ISVD) for selecting the traces when using CPA to attack. The ISVD is a combination of SVD and Z-score. Experimental results show that our method is effective to improve the efficiency when analyzing both the unprotected implementation and the masked implementation.

Keywords: Improved Singular Value Decomposition · Side Channel Attack · Correlation Power Analysis · Selecting traces

1 Introduction

When performing a real power analysis attack on cryptographic device, the number and dimension of power traces are always very large. For the goal of high efficiency of attack, many researches pay attention on how to decrease the dimension. We think it is necessary to select a helpful subset of power traces to improve the efficiency when performing CPA. However, of the today,there are rare literature on selecting power traces for CPA. In paper [4],the authors present a method by using the mean and variance of the power consumption on the most relevant time to the processed data. This method require the exact time when processing data. We think this assumption is stringent, our method just need the near range that contains the point of data processing. Paper [3] proposed a method that is based on Principal Component Analysis (PCA). They sort the power traces by the first principle component of the noise matrix. The efficiency is desirable. Nevertheless, the methods proposed in these papers only focus on the unprotected implementation and did not demonstrate whether it is effective on protected implementation.

B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 598–601, 2015.
DOI: 10.1007/978-3-319-28865-9_39

In this paper, we propose a new method that combine the SVD and Z-score to develop improved singular value decomposition to select power traces when performing CPA. The selected traces by this method can easily recover the key. We utilize this method both on unprotected implementation and masked implementation. The efficiency is outstanding and it can practically improve the effiency of CPA.

2 Background Knowledge

2.1 SVD

In the fields such as picture processing and machine learning, the data is always very large. In this scenario, the feature should be extracted to present the original data. Eigenvector is one of the methods that can achieve the purpose. We denote the original data is $A \in \mathbf{R^{n \times n}}$. The eigenvector $\nu \in \mathbf{R^{n \times 1}}$ can be computed by $A\nu = \lambda\nu$. The eigenvalue decomposition is a good method to extract the characteristic but the precondition is that the array of data must be square matrix. In the condition where data is not square matrix, the SVD is an alternate method. SVD is a method that can decompose any kind of array into lower dimension matrix and extract the characteristic of the original data. Further details on SVD may be found in [2].

2.2 ISVD

Before calculating the singular value, we introduce the *Z-score* to eliminate the huge difference of row vectors of $A^T A$. The calculation of *Z-score* as follow,

$$z = \frac{x - u}{\sigma} \tag{1}$$

where x is row vectors of matrix,u is the mean vector of all row vectors of matrix, σ is the standard deviation of x,z is the row vectors after processing.

3 Using ISVD in CPA

Let m power traces also known as samples and each of them contain n variables also known as sample points be $L \in \mathbf{R^{m \times n}}$. This is not a square matrix. However, we can calculate its singular values and corresponding singular vectors. We first let L be the A^T of Equation (3), so it is converted into

$$(LL^T)\nu = \lambda\nu \tag{2}$$

Before calculating Equation (2). We normalize the matrix LL^T by Z-score described in subsection 2.2 to ensure the amount of positive eigenvalue is equal to m.We denote B=*Z-score*$(LL^T)(B \in \mathbf{R^{m \times m}})$, the problem changes to calculate

$$B\nu = \lambda\nu \tag{3}$$

From Equation (3), we can acquire all the singular values λ_i and corresponding singular vectors $\nu_i \in \mathbf{R^{m\times 1}}(i \in [1, m])$. The eigenvectors can be used to represent the original data, so we suppose the singular vector corresponding to the biggest singular value should contain most of information about the original data. Note that the dimension of singular vector is equal to the number of samples. So we can sort the first singular vector ν' from large to small and get the corresponding index. The algorithm of this method is presented in Algorithm 1.

Algorithm 1. ISVD for Selecting Power Traces

Input: $L \in \mathbf{R^{m\times n}}$ (represents m power traces and n sample points),
k(represents the needed number of power traces ,and $k \leq m$)
Output: Select(1:k)(represents the indexes of selected traces)
1: **function** ISVD(L,k)
2: $A = LL^T$
3: $B = Z\text{-}score(A)$
4: Calculate λ_i, ν_i,such that $B\nu_i = \lambda_i\nu_i (i = 1, 2, \ldots, m)$
5: Choose the ν' corresponding to the largest λ
6: Sort ν' by descend, and get the corresponding subscript Order$(1 : m)$
7: Select(1:k)= Order(1:k)
8: Return Select(1:k)
9: **End function**

4 Experiments

In this section, we will perform a series of experiments on both unprotected implementation and protected implementation, the real power traces come from the DPA contest [1](the data of DPA contest are public data and they are widely used in testing methods in side channel attack). We use CPA based on our selecting method and randomly choosing method to analysis. Besides, for comparison, the PCA method that proposed in [3] is also used in the experiments. Success Rate (SR) proposed in [5] will be used as the evaluation metric. SR is defined as the probability that one can successfully recover the correct key, and it is widely used in side channel attacks to evaluate the key-recovery efficiency of an attacking method.

4.1 Unprotected Implementation

The power traces of unprotected implementation comes from DPA Contest v2. This attack is performed by first-order CPA by the selecting methods. The result is shown in Fig. 1 (a).

4.2 Protected Implementation

The power traces are acquired from DPA Contest v4. This attacks is performed by second-order CPA by the selecting methods.The result is showed in Fig. 1

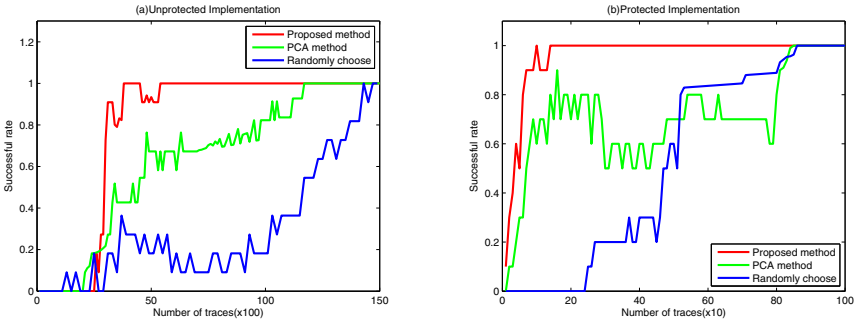

Fig. 1. (a)Success rates by using first-order CPA based different methods of selecting traces on DPA Contest v2.(b)Success rates by using second-order CPA based different methods of selecting traces on DPA Contest v4.

(b). The real experiments on both unprotected and protected implementation verify that the practical advantage of our method is remarkable.

5 Conclusions

In this paper, we proposed a method that using the improved singular value decomposition of the original power traces to select traces in order to enhance the efficiency of CPA. This method can select the power traces of high signal to noise ratio for analysis. This method is useful when performing the first-order CPA on the unprotected implementation and when performing the second-order CPA on the masked implementation. The results of experiments indeed verify the conclusion.

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

References

1. DPA Contest. http://www.dpacontest.org/home/
2. Golub, G.H., Reinsch, C.: Singular value decomposition and least squares solutions. Numerische Mathematik **14**(5), 403–420 (1970)
3. Kim, Y., Ko, H.: Using principal component analysis for practical biasing of power traces to improve power analysis attacks. In: Lee, H.-S., Han, D.-G. (eds.) ICISC 2013. LNCS, vol. 8565, pp. 109–120. Springer, Heidelberg (2014)
4. Kim, Y., Sugawara, T., Homma, N., Aoki, T., Satoh, A.: Biasing power traces to improve correlation power analysis attacks. In: First International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2010), pp. 77–80 (2010)
5. 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)