The Journal of Systems and Software 120 (2016) 105–113

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

How many interesting points should be used in a template attack?

Hailong Zhang*, Yongbin Zhou

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Minzhuang Road 89-A, Beijing, 100093, P.R. China

ARTICLE INFO

Article history:
Received 6 August 2015
Revised 16 July 2016
Accepted 19 July 2016
Available online 21 July 2016

Keywords:
Side channel attacks
Power analysis attacks
Template attack
Interesting points
Profiling efficiency

ABSTRACT

Considering that one can fully characterize and exploit the power leakages of the reference device in the process of recovering the secret key used by the target device, template attack (TA) is broadly accepted as the strongest power analysis attack from the perspective of information theory. In order to fully exploit the power leakages of the reference device, one usually has to concern the power leakages at different interesting points. Then, a natural question is how many interesting points should be used in a TA? We note that the number of interesting points one uses directly decides the profiling efficiency of TA. In light of this, we evaluate the optimal number of interesting points in simulated scenarios, and the evaluation results bring us an empirically useful formula. Then, in order to validate the empirical formula, we perform TA using power traces provided by DPA Contest v4.1. In the real scenario, the correlation method is used to select the interesting points, and the S-Box output of the 1st round AES encryption is chosen as the target intermediate value. Evaluation results show that the empirical formula is indeed correct and can be useful in practice.

1. Introduction

In practice, crypto algorithms are always implemented on crypto devices (e.g., microcontrollers, FPGA, ASIC, etc.). Different forms of side channel leakages exist when a crypto device is in operation. The side channel leakages of a crypto device can be used to recover the secret key, and that is the idea of side channel attacks. Typical side channel attacks include timing attacks (Kocher, 1996; Kelsey et al., 1998), electromagnetic attacks (Agrawal et al., 2003a; Gandolfi et al., 2001), power analysis attacks (Kocher et al., 1999; Akkar et al., 2000), and their combinations (Agrawal et al., 2003b; Souissi et al., 2012). Among different types of side channel attacks, power analysis attacks have received the most attention over the last two decades. The reasons are that power analysis attacks are relatively easy to implement, and the attack price is relatively low (Mangard et al., 2007).

The first successful power analysis attack was reported by Kocher et al. (1999). Since then, different forms of attacks, such as template attack (TA) (Chari et al., 2003), correlation power analysis (CPA) (Brier et al., 2004; Le et al., 2006), stochastic model based power analysis (SMPA) (Schindler et al., 2005; Lemke-Rust and Paar, 2007), and mutual information analysis (MIA) (Girelichs et al., 2008; Veyrat-Charvillon and Standaert, 2009) were proposed. Among them, TA is accepted as the strongest power analysis attack from the perspective of information theory. The reasons are that in TA a reference device identical to the target device can be used to accurately characterize the power leakages of the target device, and the characterized power leakages can be used to efficiently recover the secret key used by the target device.

Specifically, TA was proposed by Chari et al. (2003). In TA, the power leakages of the target device at different interesting points can be used to recover the secret key. The working procedure of TA consists of two phases, i.e., profiling and key-recovery. In profiling, mean vectors and covariance matrices are respectively used to characterize signals and noises at different interesting points, and one can obtain the so called templates. In order to accurately characterize signals and noises at different interesting points, a large number of power traces is usually needed in profiling. In key-recovery, a small number of power traces measured from the target device is used to recover the secret key. Under the assumption that noises at different interesting points follow the multivariate normal distribution, one can compute the match probability between the power leakages contained in a small number of power traces measured from the target device and the characterized templates. Among different key hypotheses, the key hypothesis that makes the match probability the largest is accepted as the secret key used by the target device.

Considering that it is the strongest form of power analysis attack, TA is widely used to practically evaluate the physical security of crypto devices, either unprotected or protected. However, problems still exist in TA, and they influence the effect of TA. In light of this, previous works (Rechberger and Oswald, 2004;

* Corresponding author.
E-mail addresses: zhanghailong@iie.ac.cn (H. Zhang), zhouyongbin@iie.ac.cn (Y. Zhou).

http://dx.doi.org/10.1016/j.jss.2016.07.028
0164-1212/

Agrawal et al., 2005; Oswald and Mangard, 2007; Gierlichs et al., 2006; Batina et al., 2008; Bär et al., 2010; Durvaux and Standaert, 2016; Archambeau et al., 2006; Elaabid and Guilley, 2010; Standaert and Archambeau, 2008) partially addressed problems exist in TA, which makes TA more applicable. First, in order to exploit the power leakages of the target device at different interesting points, one needs to use certain technique to effectively choose interesting points. In fact, the quality of the chosen interesting points directly decides the profiling efficiency of TA. Therefore, different interesting points chosen methods were proposed. Depending on their working principles, these methods can be divided into two groups. Methods in the first group choose the interesting points by using the data dependence property of the power leakages. Typical ones include the difference of means method (Rechberger and Oswald, 2004), the correlation method (Agrawal et al., 2005; Oswald and Mangard, 2007), and the T-Test method (Gierlichs et al., 2006; Batina et al., 2008; Bär et al., 2010; Durvaux and Standaert, 2016). On the other hand, some classification methods (e.g., principal component analysis (Archambeau et al., 2006; Elaabid and Guilley, 2010) and fisher linear discriminant analysis (Standaert and Archambeau, 2008)) are used to transform power traces, and the components that induce significant characterizations are exploited to recover the secret key.

Secondly, the optimal number of interesting points one should use in a certain scenario is still an open problem in TA. On one hand, when a small number of interesting points is chosen, the power leakages of the target device are not exploited efficiently, which means information loss and the key-recovery efficiency of TA is negatively influenced. On the other hand, when a large number of interesting points is chosen, the size of the covariance matrices is too large. In this case, numerical precision problems relate to the inversion of the covariance matrices of different templates will significantly lower the key-recovery efficiency of TA (Choudary and Kuhn, 2014; Lommé et al., 2013). In real scenarios, there exists four factors that may influence the optimal number of interesting points, i.e., the number of profiling traces and key-recovery traces, the signal-to-noise ratio, and the cross correlation between noises at different interesting points. Unfortunately, it is still not clear how different parameters influence the optimal number of interesting points, and one can just empirically choose a certain number of interesting points according to the engineering intuition, which is usually not optimal and therefore will influence the profiling efficiency of TA (Lerman et al., 2015).

In light of this, we evaluate the optimal number of interesting points in simulated scenarios. Specifically, we vary the number of power traces used in profiling and key-recovery, we vary the signal-to-noise ratio, and we vary the cross correlation between noises at different interesting points. We evaluate in each scenario the optimal number of interesting points. Based on the evaluation results, we can obtain an empirical formula. Then, in order to verify the validity of the empirical formula, we perform TA using the power traces provided by DPA Contest v4.1. In the real scenario, we use the correlation method to choose interesting points, and the S-Box output of the 1st round AES encryption is chosen as the target intermediate value. Empirical evaluation results show that the empirical formula reflects the real cases and can be useful in practice.

The organization of is paper is as follows. In Section 2, we present the working procedure of TA. In Section 3, we evaluate in simulated scenarios the optimal number of interesting points, and an empirically useful formula is obtained. In Section 4, we use power traces provided by DPA Contest v4.1 to verify that the empirical formula obtained from the simulated scenarios falls in line with the real cases. Finally, conclusions are given in Section 5.

2. Working procedure of template attack

The working procedure of TA consists of two phases, i.e., profiling and key-recovery. Firstly, the reference device identical to the target device can be used in profiling to accurately characterize the power leakages of the target device at different interesting points; then, in key-recovery, the secret key can be recovered utilizing the characterized power leakages about the target device. We respectively present the working procedure of profiling and key-recovery in this section.

2.1. Profiling

Because the reference device is under full control, power traces measured from the reference device can be used to characterize the power leakages of the target device. Under the assumption that the reference device is identical to the target device, its power leakages should be identical or highly similar to that of the target device. Therefore, the power leakages of the target device can be obtained.

In TA, the power leakages of the target device at different interesting points are exploited to recover the secret key used by the target device. Here, interesting points are those power samples that correspond to the processing of the target intermediate value v. The target intermediate value v is usually a sensitive intermediate value that depend on the secret key used by the target device.

It is assumed in TA that the power leakages at different interesting points follow the multivariate normal distribution. Here, we note that the power leakage of the target device at a single interesting point is usually assumed to be composed of signal and noise, while the signals at different interesting points are assumed to be mutually independent, the noises at different interesting points are usually assumed to be correlated. Therefore, in profiling, the mean vectors and the covariance matrices are used to respectively characterize the signals and the noises at different interesting points.

In order to relatively accurately characterize the signals and the noises at different interesting points, a large number of power traces is needed in profiling. However, the number of power traces available in profiling depends on the practical situation. Usually the number of profiling traces is limited. Under the known plaintext attack scenario, one can randomly feed n plaintexts $p_1, p_2, \ldots, p_n$ into the reference device. Using the leakage measurement setup, n power traces $I_1, I_2, \ldots, I_n$ can be measured and obtained during the operation of the reference device.

With the profiling traces, one needs to use a certain technique (shown in Section 1) to choose the interesting points. Here, we note that the reference device is usually assumed to under full control. Therefore, in profiling the secret key used by the reference device is assumed to be known, and the value of the target intermediate value v is known.

Before using the profiling traces $I_1, I_2, \ldots, I_n$ to characterize signals and noises at different interesting points, one needs to divide power traces into different groups according to the value of the target intermediate value v, i.e., power traces corresponding to the same value of v are placed into the same group. For example, assume the 1st S-Box output of the 1st round AES encryption is chosen as the target intermediate value v; then, one can divide n power traces into 256 groups.

If we denote power traces in the ith group as $I_1, I_2, \ldots, I_{n_i}$; then,

$$\mathbf{m}_i = \frac{1}{n_i}\sum_{j=1}^{n_i}\mathbf{t}_j, \mathbf{C}_i = \frac{1}{n_i - 1}\sum_{j=1}^{n_i}(\mathbf{t}_j - \mathbf{m}_i)^T(\mathbf{t}_j - \mathbf{m}_i), \quad (1)$$