Information Sciences 466 (2018) 92–108

Contents lists available at ScienceDirect

Information Sciences

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

Multiple leakage samples based higher order optimal distinguisher

Hailong Zhang[a,*], Yongbin Zhou[a,b]

[a] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Minzhuang Road 89-A, Beijing 100093, PR China
[b] School of Cyber Security, University of Chinese Academy of Sciences, Yuquan Road 19-A, Beijing 100049, PR China

ARTICLE INFO

Article history:
Received 18 March 2018
Revised 11 July 2018
Accepted 22 July 2018
Available online 23 July 2018

Keywords:
Side channel attacks
Higher order optimal distinguisher
Masking
Multiple leakage samples

ABSTRACT

In practice, in order to recover the secret key used by a masking device, higher order side channel attacks (HOSCA) are needed. In HOSCA, physical leakages corresponding to the processing of different sensitive intermediate values can be exploited to recover the secret key used by the target device. At ASIACRYPT 2014, Bruneau et al. proposed higher order optimal distinguisher (HOOD) to recover the secret key used by the target device, and they proved that among different styles of HOSCA, HOOD shows the best efficiency in different scenarios. In HOOD, in order to recover the secret key used by the target device, physical leakages at one leakage sample corresponding to the processing of a certain sensitive intermediate value are exploited. However, there exist more than one leakage sample that correspond to the processing of a certain sensitive intermediate value, and physical leakages contained in multiple leakage samples can be exploited to recover the secret key used by the target device. In light of this, we propose multiple leakage samples based HOOD (MLS-HOOD). We note that with MLS-HOOD, physical leakages of the target device can be sufficiently exploited to efficiently recover its secret key. In fact, we will show its advantage over HOOD and another style of HOSCA in both simulated and real scenarios.

1. Introduction

In real scenarios, different types of physical leakages, such as power signal [31], electromagnetic emanation [25] and timing information [30] can be measured when a cryptographic device is in operation. Different types of physical leakages can be exploited to recover the secret key used by the target device. We call this kind of attacks as side channel attacks (SCA). The working principle of different styles of SCA is that there exists a statistical relationship between different types of physical leakages and the sensitive intermediate value processed by the target device. In practice, this statistical relationship can be used to recover the secret key used by the target device. In real scenarios, different styles of SCA are relatively easy to be implemented. For example, in order to measure the power signal of a target device, only an oscilloscope is needed. Besides, compared with traditional cryptanalysis, different styles of SCA are powerful in practice. For example, the whole secret key of an AES-128 algorithm cannot be recovered with traditional cryptanalysis yet. However, with power traces measured from the AES-128 based cryptographic device, power analysis attacks can be used to recover its secret key. In fact,

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

https://doi.org/10.1016/j.ins.2018.07.042
0020-0255/© 2018 Elsevier Inc. All rights reserved.

in practice different styles of SCA have posed a serious threat on the physical security of different types of cryptographic devices.

Then, in order to protect cryptographic devices against different styles of SCA, different styles of countermeasures, such as random delay [9], shuffling [42], masking [26] and blinding [29] were proposed. Among these different styles of countermeasures, masking is the most widely used style. We note that reasons for this phenomenon are two folds. Firstly, masking can be implemented in the algorithmic level, which is relatively easy to be designed and implemented. Secondly, in theory masking can be proven to secure against different styles of SCA. In fact, masking can randomize the sensitive intermediate value so that the statistical relationship between the sensitive intermediate value and different types of physical leakages is eliminated, which can make different styles of SCA lose their effects. However, it does not mean that masking devices are fully secure. It only means that traditional styles of SCA (e.g., ridge based DPA [48]) cannot be used to recover the secret key used by the target device. However, higher order side channel attacks (HOSCA) can be used to recover the secret key used by the target device.

The working principle of different styles of HOSCA is that even if the statistical relationship between physical leakages of the target device and the sensitive intermediate value processed by the target device is eliminated, the combination or the joint distribution of physical leakages corresponding to the processing of the randomized sensitive intermediate value and masks may still leak information about the secret key used by the target device, i.e., the statistical relationship between the sensitive intermediate value and the combined leakages or the joint distribution of leakages still exists. In light of this, in HOSCA the statistical relationship between the sensitive intermediate value and the combined leakages or the joint distribution of leakages can be exploited to recover the secret key used by the target device. Overall, compared with different styles of SCA, the characteristic of HOSCA is that the combined leakages or the joint distribution of leakages should be used to recover the secret key used by the target device.

1.1. Related work

The first style of HOSCA was proposed at CHES 2000. In detail, Messerges proposed second order differential power analysis (SODPA) to recover the secret key used by a 1st order masking device. In SODPA, power leakages corresponding to the processing of two sensitive intermediate values can be combined to recover the secret key used by the target device, and the absolute difference is used as the leakage combination style [33]. Then, at CHES 2004, Waddle and Wagner proposed SODPA for hardware devices, which they called zero-offset 2DPA [47]. On hardware devices, different sensitive intermediate values can be processed at the same time. In this case, power leakages of the target device should be squared. Statistically the squared power leakages depend on the processing of the unmasked sensitive intermediate value, which can be used to recover the secret key used by the target device. Indeed, at CHES 2005, Peeters et al. used zero-offset 2DPA to attack a FPGA, and they showed the feasibility of zero-offset 2DPA on hardware devices. However, as estimated, compared with traditional styles of SCA, zero-offset 2DPA needs to use a larger number of power traces to successfully recover the secret key used by hardware devices [37].

In terms of the working efficiency of SODPA, at CHES 2005, Joye et al. theoretically analyzed the quantitative relationship between the attack result of SODPA and different influential factors, such as the number of power traces, the signal-to-noise level and the leakage model, which can help practitioners deepen understanding the working efficiency of SODPA [28]; while at ITCC 2005, Standaert et al. practically evaluated the working efficiency of SODPA under different leakage models, and they summarized that compared to software devices, hardware devices are normally harder to be attacked [44]. Considering that leakage samples corresponding to different sensitive intermediate values are not easy to be found, Oswald et al. proposed at CT-RSA 2006 that a time interval can be empirically chosen, and either two leakage samples in this time interval can be combined to obtain the preprocessed power traces [35]. As long as the time interval includes leakage samples corresponding to the processing of different sensitive intermediate values, a certain leakage sample in the preprocessed power traces corresponds to the processing of the secret key used by the target device, and traditional styles of SCA can be used to recover the value of the secret key used by the target device.

In 2009, Prouff et al. theoretically showed that, under the hamming weight (HW) leakage model, the normalized product is the most efficient leakage combination style among existing leakage combination styles [36]. Indeed, at ASIACRYPT 2010, Standaert et al. supported this idea with theoretical and experimental analysis [45]. On the other hand, at CT-RSA 2010, Gierlichs et al. proposed multivariate mutual information analysis (MMIA) to recover the secret key used by the target device [23]. In this case, physical leakages of the target device at different leakage samples do not need to be combined, and simply by evaluating the multivariate mutual information between the sensitive intermediate value and physical leakages at different leakage samples, the secret key used by the target device can be recovered. However, we note that the accurate estimation of the probability density function is a notorious problem in the area of statistics, which hindered the practical application of MMIA. Recently, Bruneau et al. proposed higher order optimal distinguisher (HOOD) at ASIACRYPT 2014 [5]. Contrary to previous styles of HOSCA, in HOOD physical leakages corresponding to the processing of sensitive intermediate values should be first characterized. Then, maximum likelihood principle (MLP) can be used as the distinguisher to recover the secret key used by the target device. Because physical leakages of the target device can be accurately characterized, and the characterized physical leakages can be exploited to recover the secret key used by the target device, Bruneau et al. showed in simulated scenarios that HOOD indeed performs the best among different styles of HOSCA.