早稲田大学大学院情報生産システム研究科

博士論文概要

論文題目

Research on Performance Enhancement for Electromagnetic Analysis and Power Analysis in Cryptographic LSI

申請者
Hongying LIU

情報生産システム工学専攻
マルチメディアシステム研究

2012 年 11 月

Nowadays, various cryptographic devices, such as smart cards, RFID tags, voting machines, cryptographic coprocessor, are widely used to provide authentication of users and to store secrete information for secure systems. Recently, not only the mathematical cryptanalysis, but also the side channel analysis which is based on the physical leakage, such as electromagnetic emission and power consumption, is performed. The security of cryptographic devices becomes a significant research topic.

Among the side channel analysis, the electromagnetic analysis (EMA) and power analysis (PA) can be performed with inexpensive equipment, and hence are powerful and play important roles in security fields. They are included in the fundamental research and involved in practical development. Lots of designs are contrived to prevent cryptographic devices from these attacks. In particularly, the security evaluations on the resistance of these designs based on EMA and PA are also actively conducted. However, due to the complexities of the implementation environment of cryptographic algorithms, there are still problems with conventional analysis for the security evaluation shown as follows: (1) The Gaussian noise in the side channels has been reduced by Le (IEEE TIFS07). Diversified non-Gaussian noises that especially occur to EM side channel because of the coupling of encryption modules are still unsolved. (2) Although the Hamming Distance leakage model proposed by Brier (CHES04) is generally effective, it overlooks the Glitch power consumption and is not device-specific. (3)The classical statistical tests-based leakage localization method, which was proposed by Sauvage (ACM TRTS09), is inaccurate for determining the locations of EM emission. All these problems lead to the deficient performance (the correctness of key detection and computational time) of EMA and PA.

The target of this dissertation is to enhance the performance of EMA and PA. Because the performance of EMA and PA depends on the following key factors: less noisy signals, accurate leakage model and sound statistical test. This dissertation proposes effective methods for them respectively. The contributions of this dissertation also cover three main aspects: (1) Addressing the noise issue that occurs to the EM side channel, especially, for correlated noise and simultaneous noise, several effective algorithms are proposed to decrease their influence on EMA. (2) Considering the Glitch power consumption, a new Switching Glitch leakage model is proposed to improve the performance of both EMA and PA. (3) To improve the localization accuracy, a novel leakage localization method using instant signal variance based on near-field scan is proposed to enhance the performance of EMA. With all these proposed methods for EMA and PA, the correct key is detected with less computational time, and efficient security evaluation is also made possible.

Therefore, this dissertation consists of 6 chapters as follows.

Chapter 1 [Introduction] gives a brief introduction to side channel analysis. The main principles of PA and EMA are explained. The researches on performance enhancement are overviewed. The motivation and contribution of this dissertation are summarized.

Chapter 2 [Correlated Noise Reduction for EMA] proposes three techniques to reduce the correlated noise for EMA. The correlated noise is caused by the interferences of clock network to the cryptographic module and exhibits strong correlation with encryption signal. The Discrete Wavelet Transform (DWT) proposed by Pelletier (NIST 05) cannot separate this noise because the noise has overlapped frequency bands with encryption signal. It is discovered that unlike the encryption signal, the clock signal has a high variance at the signal edges. Based on this property, the first and second techniques: single-sample SVD and multi-sample SVD reduce the correlated noise by extracting the high variance component from encryption signal. And the third technique: averaged subtraction is efficient when background samplings are included. These techniques are validated by the EM emission acquired from the AES (Advanced Encryption Standard) implementation on both ASIC (Application-Specific Integrated Circuit) and FPGA. Compared with existed methods, the proposed techniques increase the SNR as high as 22.94dB, and the success rates of EMA shows that the data-independent information is retained and the performance of EMA is enhanced.

Chapter 3 [Simultaneous Noise Reduction for EMA] presents the Source Recovery algorithm to reduce simultaneous noise for EMA. The simultaneous noise is introduced in the EM side channel by running multiple encryption modules simultaneously, which is probably used as an effective countermeasure. However, the fourth-order cumulant-based Gaussian noise reduction strategy presented by Le (IEEE TIFS07) fails to deal with this type of noise. The proposed Source Recovery algorithm takes advantage of the FastICA algorithm (Hyvärinen, IEEE TNN99) to separate the single encryption from mixed encryptions, and then by the amplitude recovery follows the correlation judgment to attenuate the noise. The effectiveness is demonstrated through the analyses of multiple AES and Camellia encryption modules on synthesized ASIC. The number of signals needed to detect keys has been dramatically reduced by 47.8% compared with standard EMA, and the performance of EMA is greatly enhanced.

Chapter 4 [The Switching Glitch Leakage Model for EMA and PA] presents a new leakage model for EMA and PA. The conventional leakage model: Hamming Distance model, which was formalized by Brier(CHES 04), is widely used due to its generality. However Glitch (Glitch is the unnecessary signal transition due to the unbalanced path delays to the inputs of a logic gate in a circuit) effects, which account for 20% to 40% of the dynamic switching power in CMOS circuits, are not involved. This leads to a low performance for EMA and PA. The proposed leakage model not only considers the data dependent switching activities but also includes Glitch power consumptions in cryptographic module. Furthermore, the switching factor and Glitch factor are introduced in the model. The estimation of these factors is shown. The advantage of this model is that the factors can be adjusted according to the analyzed devices during evaluation. Compared with Hamming Distance model, the power traces of recovering keys have been decreased by as much as 24.5%, and the EM traces has been decreased by as much as 17.1%. Namely, the performance of EMA and PA are both enhanced.

Chapter 5 [A novel Leakage Localization Method for EMA] proposes a novel leakage localization method for EMA. Due to the locality of EM emission, namely, secret information leaks from multiple locations around cryptographic devices, it is challenging to determine the exact location before conducting an EMA. Sauvage (ACM TRTS09)'s localization method has limitation in finding all the data-dependent EM emissions. Based on the EM emission acquired from near field scan, the instant signal variance of EM emission is proved as an equivalent statistical test to DoM (Difference-of-Means) test. Thus, it is proposed to identify the locations that have data-dependent EM emission. Additionally a small and low-cost probe is made to verify the proposed EMA on ASIC implementations. The EMA against unprotected AES indicates that the localization accuracy is improved by 48.6% compared with Sauvage (ACM TRTS09)'s method. Moreover, the EMA on AES WDDL (Wave Dynamic Differential Logic) implementation shows that proposed method is also effective to expose the leakage locations in the presence of countermeasure.

Chapter 6 [Conclusion] concludes this dissertation.