Cryptology ePrint Archive: Report 2013/102

On the Negative Effects of Trend Noise and Its Applications in Side-Channel Cryptanalysis

Yuchen Cao, Yongbin Zhou and Zhenmei Yu

Abstract: Side-channel information leaked during the execution of cryptographic modules usually contains various noises. Normally, these noises have negative effects on the performance of side-channel attacks exploiting noisy leakages. Therefore, to reduce noise in leakages usually serves to be an effective approach to enhance the performance of side-channel attacks. However, most existing noise reduction methods treat all noises as a whole, instead of identifying and dealing with each of them individually. Motivated by this, this paper investigates the feasibility and implications of identifying trend noise from any other noises in side-channel acquisitions and then dealing with it accordingly. Specifically, we discuss the effectiveness of applying least square method (LSM for short) to remove inherent trend noise in side-channel leakages, and also clarify the limited capability of existing noise reduction methods in dealing with trend noise. For this purpose, we perform a series of correlation power analysis attacks, as a case of study, against a set of real power traces, published in the second stage of international DPA contest which provides a public set of original power traces without any preprocessing, from an unprotected FPGA implementation of AES encryption. The experimental results firmly confirmed the soundness and validity of our analysis and observations.

Category / Keywords: implementation / side-channel cryptanalysis

Date: received 22 Feb 2013, last revised 28 Feb 2013

Contact author: zhouyongbin at iie ac cn

Available formats: PDF | BibTeX Citation

Version: 20130228:084031 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]