Cryptology ePrint Archive: Report 2011/694

Generic Side-channel Distinguisher Based on Kolmogorov-Smirnov Test: Explicit Construction and Practical Evaluation

Jiye Liu, Yongbin Zhou, Shuguo Yang, Dengguo Feng

Abstract: Construction and evaluation of efficient distinguishers with broad generality is one fundamental problem in the area of side-channel cryptanalysis. Due to their capabilities to deal with general correlations, MIA-like distinguishers have received wide attention from academia. In this paper, we conduct a comprehensive comparison investigation of existing MIA-like distinguishers, and then propose a new generic side-channel distinguisher based on partial Kolmogorov-Smirnov test, namely PKS distinguisher. Theoretical analysis and experimental attacks unanimously justify that PKS distinguisher works remarkably well with both linear and non-linear leakage models. Specifically, PKS distinguisher has obvious advantages over existing MIA-like distinguishers in terms of both success rate and guessing entropy. Additionally, lower computational complexity of PKS distinguisher further shows its better applicability than MIA-like distinguishers.

Category / Keywords: implementation / Side-Channel Cryptanalysis; Power Analysis Attack; Distinguisher; Distribution Similarity; Kolmogorov-Smirnov Test

Publication Info: The abridged version of this paper was submitted on April 1, 2011 and was accepted by Chinese Journal of Electronics on June 20, 2011 after anonymous peer reviews, and will appear in 2012.

Date: received 20 Dec 2011, last revised 29 Dec 2011

Contact author: yongbin at iscas ac cn

Available formats: PDF | BibTeX Citation

Version: 20111229:134239 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]