Cryptology ePrint Archive: Report 2013/091

Systematic Construction and Comprehensive Evaluation of Kolmogorov-Smirnov Test based Side-Channel Distinguishers

Hui Zhao, Yongbin Zhou, Francois-Xavier Standaert, Hailong Zhang

Abstract: Generic side-channel distinguishers aim at revealing the correct key embedded in cryptographic modules even when few assumptions can be made about their physical leakages. In this context, Kolmogorov-Smirnov Analysis (KSA) and Partial Kolmogorov-Smirnov analysis (PKS) were proposed respectively. Although both KSA and PKS are based on the Kolmogorov-Smirnov (KS) test, they really differ a lot from each other in terms of construction strategies. Inspired by this, we construct nine new variants by combining their strategies in a systematic way. Furthermore, we explore the effectiveness and efficiency of all these twelve KS test based distinguishers under various simulated scenarios in a univariate setting within a unified comparison framework, and also investigate how these distinguishers behave in practical scenarios. For these purposes, we perform a series of attacks against both simulated traces and real traces. Evaluation metrics such as Success Rate (SR) and Guessing Entropy (GE) are used to measure the efficiency of key recovery attacks in our evaluation. Our experimental results not only show how to choose the most suitable KS test based distinguisher in a particular scenario, but also clarify the practical meaning of all these KS test based distinguishers in practice.

Category / Keywords: implementation / side-channel cryptanalysis

Date: received 20 Feb 2013, last revised 22 Feb 2013

Contact author: zhouyongbin at iie ac cn