Cryptology ePrint Archive: Report 2011/380

An Exploration of the Kolmogorov-Smirnov Test as Competitor to Mutual Information Analysis

Carolyn Whitnall and Elisabeth Oswald and Luke Mather

Abstract: A theme of recent side-channel research has been the quest for distinguishers which remain effective even when few assumptions can be made about the underlying distribution of the measured leakage traces. The Kolmogorov-Smirnov (KS) test is a well known non-parametric method for distinguishing between distributions, and, as such, a perfect candidate and an interesting competitor to the (already much discussed) mutual information (MI) based attacks. However, the side-channel distinguisher based on the KS test statistic has received only cursory evaluation so far, which is the gap we narrow here. This contribution explores the effectiveness and effciency of Kolmogorov-Smirnov analysis (KSA), and compares it with mutual information analysis (MIA) in a number of relevant scenarios ranging from optimistic first-order DPA to multivariate settings. We show that KSA shares certain ‘generic’ capabilities in common with MIA whilst being more robust to noise than MIA in univariate settings. This has the practical implication that designers should consider results of KSA to determine the resilience of their designs against univariate power analysis attacks.

Category / Keywords: implementation / side-channel analysis, mutual information analysis, differential power analysis, Kolmogorov-Smirnov

Date: received 12 Jul 2011, last revised 13 Jul 2011

Contact author: carolyn whitnall at bris ac uk