Cryptology ePrint Archive: Report 2011/322

A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework

Carolyn Whitnall and Elisabeth Oswald

Abstract: The resistance of cryptographic implementations to side channel analysis is matter of considerable interest to those concerned with information security. It is particularly desirable to identify the attack methodology (e.g. differential power analysis using correlation or distance-of-means as the distinguisher) able to produce the best results. Attempts to answer this question are complicated by the many and varied factors contributing to attack success: the device power consumption characteristics, an attacker's power model, the distinguisher by which measurements and model predictions are compared, the quality of the estimations, and so on. Previous work has delivered partial answers for certain restricted scenarios. In this paper we assess the effectiveness of mutual information analysis within a generic and comprehensive evaluation framework. Complementary to existing work, we present several notions/characterisations of attack success, as well as a means of indicating the amount of data required by an attack. We are thus able to identify scenarios in which mutual information offers performance advantages over other distinguishers. Furthermore we observe an interesting feature -- unique to the mutual information based distinguisher -- resembling a type of stochastic resonance, which could potentially enhance the effectiveness of such attacks over other methods in certain noisy scenarios.

Category / Keywords: implementation / side-channel analysis, mutual information

Publication Info: To appear in the proceedings of CRYPTO 2011 (preliminary version).

Date: received 16 Jun 2011, last revised 17 Jun 2011

Contact author: carolyn whitnall at bristol ac uk