Cryptology ePrint Archive: Report 2011/412

Automatic Insertion of DPA Countermeasures

Andrew Moss and Elisabeth Oswald and Dan Page and Michael Tunstall

Abstract: Differential Power Analysis (DPA) attacks find a statistical correlation between the power consumption of a cryptographic device and intermediate values within the computation. Randomization of intermediate values breaks statistical dependence and thus prevents such attacks. The current state of the art in countermeasures involves manual manipulation of low-level assembly language to insert random masking. This paper introduces an algorithm to automate the process allowing the development of compilers capable of protecting programs against DPA.

Category / Keywords: implementation / Differential Power Analysis, Secure Implementations, Compilers

Date: received 1 Aug 2011, last revised 15 Aug 2011

Contact author: tunstall at cs bris ac uk