Hardware Implementation and Side-channel Analysis of LAPIN

L. Gaspar, G. Leurent and F.-X. Standaert

UCL Crypto Group, Université catholique de Louvain, Louvain-la-Neuve, Belgium

{lubos.gaspar, gaetan.leurent, fstandae}@uclouvain.be

Abstract. Differential power analysis attacks (DPA) are serious threat for implementations of modern cryptographic algorithms. Masking is a particularly appealing countermeasure against such attacks since it increases the security to a well quantifiable level and can be implemented without modifying the underlying technology.

In this paper we propose a masked hardware implementation of the Lapin authentication protocol based on ring-LPN and evaluate its security to DPA. Unlike other cryptographic algorithms containing non-linear S-boxes, ring-LPN-based Lapin involves only linear transformations, so the implementation of masking becomes straightforward and area-efficient. Since Lapin is highly scalable (8, 16, 32, 64 or 128-bit wide datapath), different speed-area tradeoffs can be achieved. Moreover, Lapin's security level can be adjusted by selecting the number of secret shares to which sensitive variables are divided.

In order to evaluate its security masked Lapin was implemented in an FPGA and various DPA attacks on both unmasked and masked Lapin implementations were performed. The attacks confirmed strong robustness of this unique structure.