Cryptology ePrint Archive: Report 2011/425

Thwarting Higher-Order Side Channel Analysis with Additive and Multiplicative Maskings

Laurie Genelle and Emmanuel Prouff and Michaël Quisquater

Abstract: Higher-order side channel attacks is a class of powerful techniques against cryptographic implementations. Their complexity grows exponentially with the order, but for small orders (e.g. 2 and 3) recent studies have demonstrated that they pose a serious threat in practice. In this context, it is today of great importance to design software countermeasures enabling to counteract higher-order side channel attacks for any arbitrary chosen order. At CHES 2010, Rivain and Prouff have introduced such a countermeasure for the AES. It works for any arbitrary chosen order and benefits from a formal resistance proof. Until now, it was the single one with such assets. By generalizing at any order a countermeasure introduced at ACNS 2010 by Genelle et al. , we propose in this paper an alternative to Rivain and Prouff's solution. The new scheme can also be proven secure at any order and has the advantage of being at least 2 times more efficient than the existing solutions for orders 2 and 3, while maintaining the RAM consumption lower than 200 bytes.

Category / Keywords: implementation / Higher-Order Side Channel Analysis, Mix of Additive and Multiplicative Masking

Publication Info: Published at CHES 2011

Date: received 8 Aug 2011, last revised 13 Sep 2011

Contact author: l genelle at oberthur com, e prouff@oberthur com, Michael Quisquater@prism uvsq fr