Cryptology ePrint Archive: Report 2011/516

Protecting AES with Shamir's Secret Sharing Scheme

Louis Goubin and Ange Martinelli

Abstract: Cryptographic algorithms embedded on physical devices are particularly vulnerable to Side Channel Analysis (SCA). The most common countermeasure for block cipher implementations is masking, which randomizes the variables to be protected by combining them with one or several random values. In this paper, we propose an original masking scheme based on Shamir's Secret Sharing scheme~\cite{Sha79} as an alternative to Boolean masking. We detail its implementation for the AES using the same tool than Rivain and Prouff in CHES 2010~\cite{RP10}: multi-party computation. We then conduct a security analysis of our scheme in order to compare it to Boolean masking. Our results show that for a given amount of noise the proposed scheme - implemented to the first order - provides the same security level as 3^{rd} up to 4^{th} order boolean masking, together with a better efficiency.

Category / Keywords: Side Channel Analysis (SCA), Masking, AES Implementation, Shamir's Secret Sharing, Multi-party computation

Publication Info: Full version of the paper published in the proceedings of CHES 2011

Date: received 19 Sep 2011

Contact author: martinelli ange at gmail com