Cryptology ePrint Archive: Report 2011/413

Higher-Order Glitches Free Implementation of the AES using Secure Multi-Party Computation Protocols – Extended Version –

Thomas Roche and Emmanuel Prouff

Abstract: Higher-order side channel attacks (HO-SCA) is a powerful technique against cryptographic implementations and the design of appropriate countermeasures is nowadays an important topic. In parallel, another class of attacks, called glitches attacks, have been investigated which exploit the hardware glitches phenomena occurring during the physical execution of algorithms. Some solutions have been proposed to counteract HO-SCA at any order or to defeat glitches attacks, but no work has until now focussed on the definition of a sound countermeasure thwarting both attacks. We introduce in this paper a circuit model in which side-channel resistance in presence of glitches effects can be characterized. This allows us to construct the first glitches free HO-SCA countermeasure. The new construction can be built from any Secure Multi-Party Computation protocol and, as an illustration, we propose to apply the protocol introduced by Ben'Or et al. at STOC in 1988. The adaptation of the latter protocol to the context of side-channel analysis results in a completely new higher-order masking scheme, particularly interesting when addressing resistance in the presence of glitches. An application of our scheme to the AES block cipher is detailed, as well as an information theoretic evaluation of the new masking function that we call polynomial masking.

Category / Keywords: implementation / Side-Channel, HO-SCA, Glitches, AES

Publication Info: This is the extended version of a paper accepted at the workshop CHES 2011

Date: received 1 Aug 2011, last revised 28 Feb 2012

Contact author: thomas roche at ssi gouv fr