Cryptology ePrint Archive: Report 2013/104

A Tutorial on White-box AES

James A. Muir

Abstract: White-box cryptography concerns the design and analysis of implementations of cryptographic algorithms engineered to execute on untrusted platforms. Such implementations are said to operate in a \emph{white-box attack context}. This is an attack model where all details of the implementation are completely visible to an attacker: not only do they see input and output, they see every intermediate computation that happens along the way. The goal of a white-box attacker when targeting an implementation of a cipher is typically to extract the cryptographic key; thus, white-box implementations have been designed to thwart this goal (\ie to make key extraction difficult/infeasible). The academic study of white-box cryptography was initiated in 2002 in the seminal work of Chow, Eisen, Johnson and van Oorschot (SAC 2002). Here, we review the first white-box AES implementation proposed by Chow \etal and give detailed information on how to construct it. We provide a number of diagrams that summarize the flow of data through the various look-up tables in the implementation, which helps clarify the overall design. We then briefly review the impressive 2004 cryptanalysis by Billet, Gilbert and Ech-Chatbi (SAC 2004). The BGE attack can be used to extract an AES key from Chow \etal's original white-box AES implementation with a work factor of about 2^{30}, and this fact has motivated subsequent work on improved AES implementations.

Category / Keywords: implementation / software, AES, white-box

Publication Info: workshop version published in "Advances in Network Analysis and its Applications", Mathematics in Industry 18 (2013), 209-229

Date: received 23 Feb 2013, last revised 27 Feb 2013

Contact author: muir james a at gmail com