On Non-uniformity in Threshold Sharings

Joan Daemen
Radboud University
Nijmegen
The Netherlands
joan@cs.ru.nl

ABSTRACT

In threshold schemes one represents each sensitive variable by a number n of shares such that their (usually) bitwise sum equals that variable. These shares are initially generated in such a way that any subset of $n-1$ shares gives no information about the sensitive variable. Functions (S-boxes, mixing layers, round functions ...) are computed on the shares of the inputs resulting in the output as a number of shares. An essential property of a threshold implementation of a function is that each output share is computed from at most $n-1$ input shares. This is called *incompleteness* and guarantees that that computation cannot leak information about sensitive variables. The resulting output is then typically subject to some further computation, again in the form of separate, incomplete, computation on shares. For these subsequent computations to not leak information about the sensitive variables, the output of the previous stage must still be uniform. Hence, in an iterative cryptographic primitive such as a block cipher, we need a threshold implementation of the round function that yields a uniformly shared output if its input is uniformly shared. This property of the threshold implementation is called *uniformity.*

Threshold schemes form a good protection mechanism against differential power analysis (DPA). In particular, using it allows building cryptographic hardware that is guaranteed to be unattackable with first-order DPA, assuming certain leakage models of the cryptographic hardware at hand and for a plausible definition of "first order".

Constructing an incomplete threshold implementation of a non-linear function is rather straightforward. To offer resistance against first-order DPA, the number of shares equals the algebraic degree of the function plus one. However, constructing one that is at the same time incomplete and uniform may present a challenge. For instance, for the KECCAK non-linear layer, incomplete 3-share threshold implementations are easy to generate but no uniform one is known. Exhaustive investigations have been performed on all small S-boxes (3 to 5 bits) and there are many S-boxes for which it is not known to build uniform threshold implementations with $d+1$ shares if their algebraic degree is d.

Uniformity of a threshold implementation is essential in its information-theoretical proof of resistance against first-order DPA. However, given a non-uniform threshold implementation, it is not immediate how to exploit its non-uniformity in an attack.

In my talk I discuss the local and global effects of non-uniformity in iterated functions and their significance on the resistance against DPA. I treat methods to quantitatively limit the amount of non-uniformity and to keep it away from where it may be harmful. These techniques are relatively cheap and can reduce non-uniformity to such a low level that it would require an astronomical amount of samples to measure it.

Keywords

Threshold implementations; Uniformity; first-order DPA

1. BIO

Joan Daemen is full Professor symmetric cryptography at Radboud University and is also affiliated to STmicroelectronics as a security architect.

He works in symmetric cryptography and is best known for the design of Rijndael together with Vincent Rijmen and the conception of sponge functions and KECCAK, together with Guido Bertoni, Gilles Van Assche and MichaÃńl Peeters. The former won the AES contest in 2000 and the latter won the SHA-3 contest in 2012. His current research interests include sponge-based authenticated encryption, secure implementations and correlation matrices.

Tis'16 October 24-24 2016, Vienna, Austria

ACM ISBN 978-1-4503-4575-0/16/10.
DOI: http://dx.doi.org/10.1145/2996366.2996374