Masking AES With *d+1* Shares in Hardware

Thomas De Cnudde
KU Leuven, ESAT-COSIC
iMinds, Belgium
thomas.decnudde@kuleuven.be

Oscar Reparaz
KU Leuven, ESAT-COSIC
iMinds, Belgium
oscar.reparaz@kuleuven.be

Begül Bilgin
KU Leuven, ESAT-COSIC
iMinds, Belgium
begul.bilgin@kuleuven.be

Svetla Nikova
KU Leuven, ESAT-COSIC
iMinds, Belgium
svetla.nikova@kuleuven.be

Ventzislav Nikov
NXP Semiconductors,
Belgium
venci.nikov@gmail.com

Vincent Rijmen
KU Leuven, ESAT-COSIC
iMinds, Belgium
vincent.rijmen@kuleuven.be

ABSTRACT

Masking requires splitting sensitive variables into at least $d+1$ shares to provide security against DPA attacks at order d. To this date, this minimal number has only been deployed in software implementations of cryptographic algorithms and in the linear parts of their hardware counterparts. So far there is no hardware construction that achieves this lower bound if the function is nonlinear and the underlying logic gates can glitch. In this paper, we give practical implementations of the AES using $d+1$ shares aiming at first- and second-order security even in the presence of glitches. To achieve this, we follow the conditions presented by Reparaz et al. at CRYPTO 2015 to allow hardware masking schemes, like Threshold Implementations, to provide theoretical higher-order security with $d+1$ shares. The decrease in number of shares has a direct impact in the area requirements: our second-order DPA resistant core is the smallest in area so far, and its S-box is 50% smaller than the current smallest Threshold Implementation of the AES S-box with similar security and attacker model. We assess the security of our masked cores by practical side-channel evaluations. The security guarantees are met with 100 million traces.

Keywords

AES; DPA; Masking; Threshold Implementations

1. ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for providing constructive and valuable comments. This work was supported in part by NIST with the research grant 60NANB15D346, in part by the Research Council KU Leuven (OT/13/071 and GOA/11/007) and in part by the European Union's Horizon 2020 research and innovation programme under grant agreement No 644052 HECTOR. Begul Bilgin is a Postdoctoral Fellow of the Fund for Scientific Research - Flanders (FWO). Oscar Reparaz is funded by a PhD fellowship of the Fund for Scientific Research - Flanders (FWO). Thomas De Cnudde is funded by a research grant of the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).

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

ACM ISBN 978-1-4503-4575-0/16/10.

DOI: http://dx.doi.org/10.1145/2996366.2996428