Evaluating and Designing against Side-Channel Leakage White Box or Black box?

François-Xavier Standaert
Crypto Group, ICTEAM Institute, UCLouvain
Place du Levant, 3, B1348, Louvain-la-Neuve, Belgium
fstandae@uclouvain.be

ABSTRACT

Side-channel analysis is an important concern for the security of cryptographic implementations, and may lead to powerful key recovery attacks if no countermeasures are deployed. Therefore, various types of protection mechanisms have been proposed over the last 20 years. In view of the cost and performance overheads caused by these protections, their fair evaluation and scarce use are a primary concern for hardware and software designers. Yet, the physical nature of side-channel analysis also renders the security evaluation of cryptographic implementations very different from the one of cryptographic algorithms against mathematical cryptanalysis. That is, while the latter can be quantified based on (well-defined) time, data and memory complexities, the evaluation of side-channel security additionally requires to quantify the informativeness and exploitability of the physical leakages. This implies that a part of these security evaluations is inherently heuristic and dependent on engineering expertise. It also raises the question of the capabilities given to the adversary/evaluator. For example, should she get full (unrestricted) access to the implementation to gain a precise understanding of its functioning (which I will denote as the white box approach) or should she be more restricted? In this talk, I will argue that a white box approach is not only desirable in order to avoid designing and evaluating implementations with a "false sense of security" but also that such designs become feasible in view of the research progresses made over the last two decades.

CCS Concepts/ACM Classifiers

Security and privacy **=>** Security in hardware **=>** Hardware attacks and countermeasures**=>** Side-channel analysis

BIOGRAPHY

Francois-Xavier Standaert was born in Brussels, Belgium in 1978. He received the Electrical Engineering degree and PhD degree from the UCLouvain, respectively in 2001 and 2004. In 2004-2005, he was a Fulbright visiting researcher at Columbia University, Department of Computer Science, Crypto Lab (hosted by Tal G. Malkin and Moti Yung) and at the MIT Medialab, Center for Bits and Atoms (hosted by Neil Gershenfeld). In 2006, he was a founding member of IntoPix s.a. From 2005 to 2008, he was a post-doctoral researcher of the Belgian Fund for Scientific Research (FNRS-F.R.S.) at the UCL Crypto Group and a regular visitor of the two aforementioned laboratories. Since 2008 (resp. 2017), he is associate researcher (resp. senior associate researcher) of the Belgian Fund for Scientific Research (FNRS-F.R.S). Since 2013 (resp. 2018), he is associate professor (resp. professor) at the UCL Institute of Information and Communication Technologies, Electronics and Applied Mathematics (ICTEAM). In 2010, he was program co-chair of CHES (which is the flagship workshop on cryptographic hardware). In 2021, he will be program co-chair of EUROCRYPT (one of the flagship IACR conferences). In 2011, he was awarded a Starting Independent Research Grant by the European Research Council (ERC). In 2016, he has been awarded a Consolidator Grant by the European Research Council. From 2017 to 2022, he will be board member (director) of the International Association for Cryptologic Research (IACR). He gave an invited talk at EUROCRYPT 2019. His research interests include cryptographic hardware and embedded systems, low power implementations for constrained environments (RFIDs, sensor networks, ...), the design and cryptanalysis of symmetric cryptographic primitives, physical security issues in general and side-channel/leakage analysis in particular.

URL: https://perso.uclouvain.be/fstandae/

IH&MMSec '21, June 22–25, 2021, Virtual Event, Belgium.

ACM ISBN 978-1-4503-8295-3/21/06.
https://doi.org/10.1145/XXXXXXX.XXXXXXX