

Contents

Java Cards

Memory Forensics of a Java Card Dump	3
<i>Jean-Louis Lanet, Guillaume Bouffard, Rokia Lamrani, Ranim Chakra, Afef Mestiri, Mohammed Monsif, and Abdellatif Fandi</i>	
Heap . . . Hop! Heap Is Also Vulnerable	18
<i>Guillaume Bouffard, Michael Lackner, Jean-Louis Lanet, and Johannes Loinig</i>	

Software Countermeasures

Study of a Novel Software Constant Weight Implementation	35
<i>Victor Servant, Nicolas Debande, Housseem Maghrebi, and Julien Bringer</i>	
Balanced Encoding to Mitigate Power Analysis: A Case Study	49
<i>Cong Chen, Thomas Eisenbarth, Aria Shahverdi, and Xin Ye</i>	
On the Cost of Lazy Engineering for Masked Software Implementations	64
<i>Josep Balasch, Benedikt Gierlichs, Vincent Grosso, Oscar Reparaz, and François-Xavier Standaert</i>	

Side-Channel Analysis

Efficient Stochastic Methods: Profiled Attacks Beyond 8 Bits	85
<i>Marios O. Choudary and Markus G. Kuhn</i>	
Kangaroos in Side-Channel Attacks	104
<i>Tanja Lange, Christine van Vredendaal, and Marnix Wakker</i>	
Combining Leakage-Resilient PRFs and Shuffling: Towards Bounded Security for Small Embedded Devices	122
<i>Vincent Grosso, Romain Poussier, François-Xavier Standaert, and Lubos Gaspar</i>	

Embedded Implementations

Double Level Montgomery Cox-Rower Architecture, New Bounds	139
<i>Jean-Claude Bajard and Nabil Merkiche</i>	
How to Use Koblitz Curves on Small Devices?	154
<i>Kimmo Järvinen and Ingrid Verbauwhede</i>	

Public-Key Cryptography

Cam1 Crush: A PKCS#11 Filtering Proxy	173
<i>Ryad Benadjila, Thomas Calderon, and Marion Daubignard</i>	
Algorithms for Outsourcing Pairing Computation	193
<i>Aurore Guillevic and Damien Vergnaud</i>	

Leakage and Fault Attacks

Bounded, yet Sufficient? How to Determine Whether Limited Side Channel Information Enables Key Recovery	215
<i>Xin Ye, Thomas Eisenbarth, and William Martin</i>	
On the Security of Fresh Re-keying to Counteract Side-Channel and Fault Attacks	233
<i>Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, and Florian Mendel</i>	
Evidence of a Larger EM-Induced Fault Model.	245
<i>S. Ordas, L. Guillaume-Sage, K. Tobich, J.-M. Dutertre, and P. Maurine</i>	
Author Index	261

Smart Card Research and Advanced Applications
13th International Conference, CARDIS 2014, Paris,
France, November 5-7, 2014. Revised Selected Papers
Joye, M.; Moradi, A. (Eds.)
2015, X, 261 p. 76 illus., Softcover
ISBN: 978-3-319-16762-6