

Contents

Java Cards

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

Software Countermeasures

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

Side-Channel Analysis

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

Embedded Implementations

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

Public-Key Cryptography

Cam1 Crush: A PKCS#11 Filtering Proxy 173
Ryad Benadjila, Thomas Calderon, and Marion Daubignard

Algorithms for Outsourcing Pairing Computation 193
Aurore Guillevic and Damien Vergnaud

Leakage and Fault Attacks

Bounded, yet Sufficient? How to Determine Whether Limited
Side Channel Information Enables Key Recovery 215
Xin Ye, Thomas Eisenbarth, and William Martin

On the Security of Fresh Re-keying to Counteract Side-Channel
and Fault Attacks 233
*Christoph Dobraunig, Maria Eichlseder, Stefan Mangard,
and Florian Mendel*

Evidence of a Larger EM-Induced Fault Model. 245
S. Ordas, L. Guillaume-Sage, K. Tobich, J.-M. Dutertre, and P. Maurine

Author Index 261



<http://www.springer.com/978-3-319-16762-6>

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