

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Dieter Gollmann Jean-Louis Lanet
Julien Iguchi-Cartigny (Eds.)

Smart Card Research and Advanced Application

9th IFIP WG 8.8/11.2 International Conference
CARDIS 2010
Passau, Germany, April 14-16, 2010
Proceedings

Volume Editors

Dieter Gollmann
Hamburg University of Technology
Institute for Security in Distributed Applications
21071 Hamburg, Germany
E-mail: diego@tu-harburg.de

Jean-Louis Lanet
Julien Iguchi-Cartigny
University of Limoges, XLIM
87000 Limoges, France
E-mail: {jean-louis.lanet, julien.cartigny}@unilim.fr

Library of Congress Control Number: 2010924121

CR Subject Classification (1998): E.3, C.2, K.6.5, D.4.6, H.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-12509-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-12509-6 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© IFIP International Federation for Information Processing 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

These proceedings contain the papers selected for presentation at CARDIS 2010, the 9th IFIP Conference on Smart Card Research and Advanced Application hosted by the Institute of IT-Security and Security Law (ISL) of the University of Passau, Germany. CARDIS is organized by IFIP Working Groups WG 8.8 and WG 11.2. Since 1994, CARDIS has been the foremost international conference dedicated to smart card research and applications. Every second year leading researchers and practitioners meet to present new ideas and discuss recent developments in smart card technologies.

The fast evolution in the field of information security requires adequate means for representing the user in human-machine interactions. Smart cards, and by extension smart devices with their processing power and their direct association with the user, are considered the first choice for this purpose. A wide range of areas including hardware design, operating systems, systems modelling, cryptography, and distributed systems contribute to this fast-growing technology.

The submissions to CARDIS were reviewed by at least three members of the Program Committee, followed by a two-week discussion phase held electronically, where committee members could comment on all papers and all reviews. Finally, 16 papers were selected for presentation at CARDIS.

There are many volunteers who offered their time and energy to put together the symposium and who deserve our acknowledgment. We want to thank all the members of the Program Committee and the external reviewers for their hard work in evaluating and discussing the submissions. We are also very grateful to Joachim Posegga, the General Chair of CARDIS 2010, and his team for the local conference management.

Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you find the proceedings stimulating.

March 2010

Jean-Louis Lanet
Dieter Gollmann

Organization

General Chair

Joachim Posegga University of Passau, Germany

Program Chairs

Jean-Louis Lanet Université de Limoges, France
Dieter Gollmann Hamburg University of Technology, Germany

Program Committee

Liqun Chen	Hewlett-Packard, UK
Christophe Clavier	XLIM, France
Wolfgang Effing	Giesecke & Devrient, Germany
Benoit Feix	Inside Contactless, France
Benedikt Gierlichs	COSIC Leuven, Belgium
Louis Goubin	Université de Versailles, France
Gilles Grimaud	Université de Lille, France
Marc Joye	Technicolor, France
Josef Langer	CDE Hagenberg, Austria
Cédric Lauradoux	INRIA Rhône-Alpes, Equipe SWING, France
Kostas Markantonakis	Royal Holloway, UK
Vaclav Matyas	Masaryk University, Czech Republic
Bernd Meyer	Siemens AG, Germany
Wojciech Mostowski	University of Nijmegen, The Netherlands
Pierre Paradinas	INRIA, France
Emmanuel Prouff	Oberthur Technology, France
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Jean Marc Robert	Ecole de technologie supérieure Montréal, Canada
Jean-Jacques Vandewalle	Gemalto, France

Additional Reviewers

Lejla Batina	Junfeng Fan
Samia Bouzefrane	Lars Hoffmann
Guillaume Dabosville	Jan Krhovjak
Elke De Mulder	François-Xavier Marseille
Simon Duquennoy	Nathalie Mitton
Hermann Drexler	Kenny Paterson

VIII Organization

Michael Roland
Martin Seysen
Petr Svenda
Hugues Thiebauld

Vincent Verneuil
Colin Walter
Marc Witteman

Local Organization

Arne Bilzhause
Sigline Böck
Bastian Braun
Agnes Grützner
Peter Häring
Daniel Hausknecht
Michael Kaeuff

Markus Karwe
Guido Lenk-Blochowitz
Simon Niechzial
Henrich Pöhls
Daniel Schreckling
Martin Steininger
Marita Ward

Table of Contents

Mathematical Algorithms

The Polynomial Composition Problem in $(\mathbb{Z}/n\mathbb{Z})[X]$	1
<i>Marc Joye, David Naccache, and Stéphanie Porte</i>	
Enhance Multi-bit Spectral Analysis on Hiding in Temporal Dimension	13
<i>Qiasi Luo</i>	
Secure Delegation of Elliptic-Curve Pairing	24
<i>Benoît Chevallier-Mames, Jean-Sébastien Coron, Noel McCullagh, David Naccache, and Michael Scott</i>	

Side Channel Analysis

Side-Channel Leakage across Borders	36
<i>Jörn-Marc Schmidt, Thomas Plos, Mario Kirschbaum, Michael Hutter, Marcel Medwed, and Christoph Herbst</i>	
Designing a Side Channel Resistant Random Number Generator	49
<i>Suresh N. Chari, Vincenzo V. D'Luoffo, Paul A. Karger, Elaine R. Palmer, Tal Rabin, Josyula R. Rao, Pankaj Rohotgi, Helmut Scherzer, Michael Steiner, and David C. Toll</i>	
Simple Power Analysis on Exponentiation Revisited	65
<i>Jean-Christophe Courrège, Benoit Feix, and Mylène Roussellet</i>	
Atomicity Improvement for Elliptic Curve Scalar Multiplication	80
<i>Christophe Giraud and Vincent Verneuil</i>	

Systems

Key-Study to Execute Code Using Demand Paging and NAND Flash at Smart Card Scale	102
<i>Geoffroy Cogniaux and Gilles Grimaud</i>	
Firewall Mechanism in a User Centric Smart Card Ownership Model ...	118
<i>Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes</i>	

Logical Attacks

Combined Attacks and Countermeasures	133
<i>Eric Vetillard and Anthony Ferrari</i>	

Attacks on Java Card 3.0 Combining Fault and Logical Attacks 148
Guillaume Barbu, Hugues Thiebauld, and Vincent Guerin

Fault Analysis

Improved Fault Analysis of Signature Schemes 164
Christophe Giraud, Erik W. Knudsen, and Michael Tunstall

When Clocks Fail: On Critical Paths and Clock Faults 182
Michel Agoyan, Jean-Max Dutertre, David Naccache, Bruno Robisson, and Assia Tria

Privacy

Modeling Privacy for Off-Line RFID Systems 194
Flavio D. Garcia and Peter van Rossum

Developing Efficient Blinded Attribute Certificates on Smart Cards via
Pairings 209
Lejla Batina, Jaap-Henk Hoepman, Bart Jacobs, Wojciech Mostowski, and Pim Vullers

On the Design and Implementation of an Efficient DAA Scheme 223
Liqun Chen, Dan Page, and Nigel P. Smart

Author Index 239