Lecture Notes in Computer Science 6917

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Bart Preneel Tsuyoshi Takagi (Eds.)

Cryptographic Hardware and Embedded Systems – CHES 2011

13th International Workshop
Nara, Japan, September 28 – October 1, 2011
Proceedings

Springer

Volume Editors

Bart Preneel
Katholieke Universiteit Leuven
3001 Leuven, Belgium
E-mail: bart.preneel@esat.kuleuven.be

Tsuyoshi Takagi
Kyushu University
Institute of Mathematics for Industry
Fukuoka, 819-0395, Japan
E-mail: takagi@imi.kyushu-u.ac.jp

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-23950-2 e-ISBN 978-3-642-23951-9
DOI 10.1007/978-3-642-23951-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011935857

CR Subject Classification (1998): E.3, D.4.6, K.6.5, E.4, C.2, G.2.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 13th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011) was held at Todai-ji Cultural Center, Nara, Japan, from September 28 to October 1, 2011. The workshop was sponsored by the International Association for Cryptologic Research.

CHES 2011 received 119 submissions from 26 countries all over the world. Each paper was reviewed by at least 4 committee members, for a total of 517 reviews; papers with a committee member as co-author received at least 5 reviews. More than 150 external subreviewers contributed to the review process in their particular areas of expertise. One article was identified as an irregular submission. The Program Committee selected 32 papers for publication in the proceedings. Two of these papers are the result of merging two pairs of closely related submissions. The program was completed with two excellent invited talks given by Ernie Brickell (Intel) and Tetsuya Tominaga (NTT Laboratories). Nominations for the best paper award were solicited among the Program Committee; an ad hoc committee with no conflicts with the shortlisted papers made the final selection. They decided to award the best paper award of CHES 2011 to Michael Hutter and Erich Wenger for their work "Fast Multi-Precision Multiplication for Public-Key Cryptography on Embedded Microprocessors." The runners-up were the papers "To Infinity and Beyond: Combined Attack on ECC Using Points of Low Order" by Junfeng Fan, Benedikt Gierlichs and Frederik Vercauteren, and "Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World" by David Oswald and Christof Paar. The authors of these articles were invited to submit an extended version to the *Journal of Cryptology*.

Many people contributed to the success of CHES 2011. First we would like to thank all the authors who submitted their research results. The selection of 32 papers from 119 submissions was a challenging task and we sincerely thank the 42 Program Committee members, as well as the external reviewers, who volunteered to read and discuss the papers over several months. We are greatly indebted to the General Chair, Akashi Satoh, for his relentless efforts that include relocating the conference within short notice because of the earthquake and tsunami in March 2011. We would also like to thank the local Organizing Committee from the Japanese cryptologic community for their continuous support. The submission and review process as well as the editing of the final proceedings were facilitated by the software written by Shai Halevi. The CHES 2011 website was maintained by Jens-Peter Kaps. We would like to thank Shai and Jens-Peter for their excellent support. Finally we want to express our gratitude to our generous sponsors: Cryptographic Research, SASEBO project, Nara Visitors Bureau, NTT, IPA, Mitsubishi Elecric, Morita Tech, NICT, Riscure, ETRI, Tokyo Electron Device, Kayamori Foundation, Technicolor, Telecom ParisTech,

Intrinsic-ID, Hitachi, Oberthur Technologies, IIJ, Toshiba, SPACES project, LG CNS, and Fujitsu.

As embedded systems become ever more pervasive, there is a growing need to develop efficient and secure implementations that help to safeguard our security and privacy. We hope that the papers in this volume prove valuable for your research and professional activities in this area.

September 2011

Bart Preneel
Tsuyoshi Takagi

CHES 2011

Workshop on Cryptographic Hardware and Embedded Systems
Nara, Japan, September 28 – October 1, 2011.

Sponsored by the *International Association for Cryptologic Research.*

General Chair

Akashi Satoh	National Institute of Advanced Industrial Science and Technology, Japan

Program Co-chairs

Bart Preneel	Katholieke Universiteit Leuven, Belgium
Tsuyoshi Takagi	Kyushu University, Japan

Program Committee

Toru Akishita	Sony Corporation, Japan
Paulo Barreto	University of São Paulo, Brazil
Lejla Batina	Radboud University Nijmegen, The Netherlands and Katholieke Universiteit Leuven, Belgium
Daniel J. Bernstein	University of Illinois at Chicago, USA
Guido Bertoni	STMicroelectronics, Italy
Swarup Bhunia	Case Western Reserve University, USA
Chen-Mou Cheng	National Taiwan University, Taiwan
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Emmanuelle Dottax	Oberthur Technologies, France
Hermann Drexler	Giesecke & Devrient, Germany
Martin Feldhofer	Graz University of Technology, Austria
Pierre-Alain Fouque	ENS, France
Kris Gaj	George Mason University, USA
Benedikt Gierlichs	Katholieke Universiteit Leuven, Belgium
Louis Goubin	Université de Versailles, France
Jorge Guajardo	Robert Bosch LLC, Research and Technology Center, USA
Dong-Guk Han	Kookmin University, Korea
Helena Handschuh	Intrinsic-ID, USA and Katholieke Universiteit Leuven, Belgium
Anwar Hasan	University of Waterloo, Canada
Naofumi Homma	Tohoku University, Japan

Marc Joye	Technicolor, France
Pascal Junod	HEIG-VD, Switzerland
Shinichi Kawamura	AIST, Japan
Paris Kitsos	Hellenic Open University, Greece
Markus Kuhn	Cambridge University, UK
Kerstin Lemke-Rust	University of Applied Sciences Bonn-Rhein-Sieg, Germany
Stefan Mangard	Infineon Technologies, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
David Naccache	ENS, France
Heike Neumann	NXP, Germany
Elisabeth Oswald	University of Bristol, UK
Christof Paar	Ruhr University of Bochum, Germany
Matt Robshaw	Orange Labs, France
Pankaj Rohatgi	Cryptography Research, USA
Ahmad-Reza Sadeghi	TU Darmstadt and Fraunhofer SIT, Germany
Kazuo Sakiyama	University of Electro Communications, Japan
Erkay Savas	Sabancı University, Turkey
Patrick Schaumont	Virginia Tech, USA
Nigel P. Smart	University of Bristol, UK
Masahiko Takenaka	Fujitsu Laboratories, Japan
Colin Walter	Royal Holloway, University of London, UK

External Reviewers

Diego F. Aranha	Fabrizio De Santis	Harunaga Hiwatari
Frederik Armknecht	Benedikt Driessen	Michael Hutter
Jean-Philippe Aumasson	Orr Dunkelman	Sebastiaan Indesteege
Selcuk Baktir	Paul Duplys	Mawa N. Ismail
Josep Balasch	Ilze Eichhorn	Takanori Isobe
Alessandro Barenghi	Wieland Fischer	Kouichi Itoh
Claude Barral	Nicolas Gama	Tetsuya Izu
Timo Bartkewitz	Berndt Gammel	Josh Jaffe
Georg T. Becker	Christophe Giraud	Dipti Kapadia
Thomas Behling	Robert Granger	Markus Kasper
Alexandre Berzati	Johann Großschädl	Michael Kasper
Markus Bockes	Eric Guo	Timo Kasper
Arnaud Boscher	Anwar Hasan	Jonathan Katz
Murat Cenk	Yuichi Hayashi	Hee Seok Kim
Zhimin Chen	Olaf Heemskerk	Inyoung Kim
Tung Chou	Francisco R. Henriquez	Mario Kirschbaum
Christophe Clavier	Christoph Herbst	Aswin Kishna
Jeremy Cooper	Clemens Heuberger	Miroslav Knežević
Joan Daemen	Stefan Heyse	Kazuyuki Kobayashi
Elke De Mulder	Markus Hinkelmann	Ünal Kocabas

Masanobu Koike
Yuichi Komano
Daniel Krenn
Po-Chun Kuo
Masafumi Kusakawa
Soonhak Kwon
Tanja Lange
Mun-Kyu Lee
Yang Li
Raimondo Luzzi
Gilles Macariot-Rat
Marco Macchetti
Abhranil Maiti
Mark Marson
Ange Martinelli
Pedro Maat C. Massolino
Nicolas Meloni
Filippo Melzani
Atsushi Mitsuda
Hideyuki Miyake
Atsushi Miyamoto
Amir Moradi
Carlos Moreno
Andrew Moss
Bruce Murray
Daisuke Nakatsu
Seetharam Narasimhan
Phong Nguyen
Ruben Niederhagen
Ventzi Nikov
Hanae Nozaki
Katsuyuki Okeya
David Oswald
Dan Page
Jing Pan
Jacques Patarin
Gerardo Pelosi
Geovandro Pereira
Gilles Piret
Thomas Plos
Jerome Plut
Axel Poschmann
Emmanuel Prouff
Jürgen Pulkus
Michaël Quisquater
Francesco Regazzoni
Christof Rempel
Matthieu Rivain
Thomas Roche
Marcin Rogawski
Carsten Rudolph
Koichi Sakumoto
Gokay Saldamli
Jörn-Marc Schmidt
Geert-Jan Schrijen
Steffen Schulz
Peter Schwabe
Michael Scott
Rabia Shahid
Umar Sharif
Kyoji Shibutani
Kouichi Shimizu
Hideo Shimizu
Taizo Shirai
Herve Sibert
Yannick Sierra
Peter Simons
Marcos A. Simplicio Jr.
Dave Singelée
Martijn Stam
Daehyun Strobel
Takeshi Sugawara
Ruggero Susella
Daisuke Suzuki
Robert Szerwinski
Masahiko Takenaka
Shigeki Teramoto
Gilles Van Assche
Vincent van der Leest
Erik van der Sluis
Marten van Hulst
Jasper van Woudenberg
Marc Vauclair
Ingrid Verbauwhede
Frederik Vercauteren
Marion Videau
Christian Wachsmann
Lei Wang
Xinmu Wang
Erich Wenger
Carolyn Whitnall
Jun Yajima
Tolga Yalcin
Panasayya Yalla
Dai Yamamoto
Ralf Zimmermann

Table of Contents

FPGA Implementation

An Exploration of Mechanisms for Dynamic Cryptographic Instruction Set Extension 1
Philipp Grabher, Johann Großschädl, Simon Hoerder, Kimmo Järvinen, Dan Page, Stefan Tillich, and Marcin Wójcik

FPGA-Based True Random Number Generation Using Circuit Metastability with Adaptive Feedback Control 17
Mehrdad Majzoobi, Farinaz Koushanfar, and Srinivas Devadas

Generic Side-Channel Countermeasures for Reconfigurable Devices 33
Tim Güneysu and Amir Moradi

AES

Improved Collision-Correlation Power Analysis on First Order Protected AES 49
Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylène Roussellet, and Vincent Verneuil

Higher-Order Glitches Free Implementation of the AES Using Secure Multi-party Computation Protocols 63
Emmanuel Prouff and Thomas Roche

Protecting AES with Shamir's Secret Sharing Scheme 79
Louis Goubin and Ange Martinelli

A Fast and Provably Secure Higher-Order Masking of AES S-Box 95
HeeSeok Kim, Seokhie Hong, and Jongin Lim

Elliptic Curve Cryptosystems

Software Implementation of Binary Elliptic Curves: Impact of the Carry-Less Multiplier on Scalar Multiplication 108
Jonathan Taverne, Armando Faz-Hernández, Diego F. Aranha, Francisco Rodríguez-Henríquez, Darrel Hankerson, and Julio López

High-Speed High-Security Signatures 124
Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang

To Infinity and Beyond: Combined Attack on ECC Using Points of Low Order 143
Junfeng Fan, Benedikt Gierlichs, and Frederik Vercauteren

Lattices

Random Sampling for Short Lattice Vectors on Graphics Cards 160
Michael Schneider and Norman Göttert

Extreme Enumeration on GPU and in Clouds: How Many Dollars You Need to Break SVP Challenges 176
Po-Chun Kuo, Michael Schneider, Özgür Dagdelen, Jan Reichelt, Johannes Buchmann, Chen-Mou Cheng, and Bo-Yin Yang

Modulus Fault Attacks against RSA-CRT Signatures 192
Éric Brier, David Naccache, Phong Q. Nguyen, and Mehdi Tibouchi

Side Channel Attacks

Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World 207
David Oswald and Christof Paar

Information Theoretic and Security Analysis of a 65-Nanometer DDSLL AES S-Box 223
Mathieu Renauld, Dina Kamel, François-Xavier Standaert, and Denis Flandre

Thwarting Higher-Order Side Channel Analysis with Additive and Multiplicative Maskings 240
Laurie Genelle, Emmanuel Prouff, and Michaël Quisquater

Extractors against Side-Channel Attacks: Weak or Strong? 256
Marcel Medwed and François-Xavier Standaert

Invited Talk

Standardization Works for Security Regarding the Electromagnetic Environment 273
Tetsuya Tominaga

Fault Attacks

Meet-in-the-Middle and Impossible Differential Fault Analysis on AES 274
Patrick Derbez, Pierre-Alain Fouque, and Delphine Leresteux

On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting 292
Amir Moradi, Oliver Mischke, Christof Paar, Yang Li, Kazuo Ohta, and Kazuo Sakiyama

Lightweight Symmetric Algorithms

SPONGENT: A Lightweight Hash Function 312
Andrey Bogdanov, Miroslav Knežević, Gregor Leander, Deniz Toz, Kerem Varıcı, and Ingrid Verbauwhede

The LED Block Cipher 326
Jian Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw

Piccolo: An Ultra-Lightweight Blockcipher 342
Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai

PUFs

Lightweight and Secure PUF Key Storage Using Limits of Machine Learning 358
Meng-Day (Mandel) Yu, David M'Raihi, Richard Sowell, and Srinivas Devadas

Recyclable PUFs: Logically Reconfigurable PUFs 374
Stefan Katzenbeisser, Ünal Koçabas, Vincent van der Leest, Ahmad-Reza Sadeghi, Geert-Jan Schrijen, Heike Schröder, and Christian Wachsmann

Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches 390
Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Takao Ochiai, Masahiko Takenaka, and Kouichi Itoh

MECCA: A Robust Low-Overhead PUF Using Embedded Memory Array 407
Aswin Raghav Krishna, Seetharam Narasimhan, Xinmu Wang, and Swarup Bhunia

Public-Key Cryptosystems

FPGA Implementation of Pairings Using Residue Number System and Lazy Reduction 421
Ray C.C. Cheung, Sylvain Duquesne, Junfeng Fan, Nicolas Guillermin, Ingrid Verbauwhede, and Gavin Xiaoxu Yao

High Speed Cryptoprocessor for η_T Pairing on 128-bit Secure Supersingular Elliptic Curves over Characteristic Two Fields 442
Santosh Ghosh, Dipanwita Roy Chowdhury, and Abhijit Das

Fast Multi-precision Multiplication for Public-Key Cryptography on Embedded Microprocessors 459
Michael Hutter and Erich Wenger

Small Public Keys and Fast Verification for $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic Public Key Systems 475
Albrecht Petzoldt, Enrico Thomae, Stanislav Bulygin, and Christopher Wolf

Hash Functions

Throughput vs. Area Trade-offs in High-Speed Architectures of Five Round 3 SHA-3 Candidates Implemented Using Xilinx and Altera FPGAs 491
Ekawat Homsirikamol, Marcin Rogawski, and Kris Gaj

Efficient Hashing Using the AES Instruction Set 507
Joppe W. Bos, Onur Özen, and Martijn Stam

Author Index 523