Lecture Notes in Computer Science 5747

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

Christophe Clavier Kris Gaj (Eds.)

Cryptographic Hardware and Embedded Systems – CHES 2009

11th International Workshop
Lausanne, Switzerland, September 6-9, 2009
Proceedings

Springer

Volume Editors

Christophe Clavier
Université de Limoges
Département de Mathématiques et d'Informatique
83 rue d'Isle, 87000 Limoges, France
E-mail: christophe.clavier@unilim.fr
and
Institut d'Ingénierie Informatique de Limoges (3iL)
42 rue Sainte Anne, 87000 Limoges, France
E-mail: christophe.clavier@3il.fr

Kris Gaj
George Mason University
Department of Electrical and Computer Engineering
Fairfax, VA 22030, USA
E-mail: kgaj@gmu.edu

Library of Congress Control Number: 2009933191

CR Subject Classification (1998): E.3, D.4.6, K.6.5, E.4, C.2, H.2.7

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-04137-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-04137-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12753017 06/3180 5 4 3 2 1 0

Preface

CHES 2009, the 11th workshop on Cryptographic Hardware and Embedded Systems, was held in Lausanne, Switzerland, September 6–9, 2009. The workshop was sponsored by the International Association for Cryptologic Research (IACR).

The workshop attracted a record number of 148 submissions from 29 countries, of which the Program Committee selected 29 for publication in the workshop proceedings, resulting in an acceptance rate of 19.6%, the lowest in the history of CHES. The review process followed strict standards: each paper received at least four reviews, and some as many as eight reviews. Members of the Program Committee were restricted to co-authoring at most two submissions, and their papers were evaluated by an extended number of reviewers.

The Program Committee included 53 members representing 20 countries and five continents. These members were carefully selected to represent academia, industry, and government, as well as to include world-class experts in various research fields of interest to CHES. The Program Committee was supported by 148 external reviewers. The total number of people contributing to the review process, including Program Committee members, external reviewers, and Program Co-chairs, exceeded 200.

The papers collected in this volume represent cutting-edge worldwide research in the rapidly growing and evolving area of cryptographic engineering. The submissions were sought in several general areas, including, but not limited to, cryptographic hardware, cryptographic software, attacks against implementations and countermeasures against these attacks, tools and methodologies of cryptographic engineering, and applications and implementation environments of cryptographic systems. Ten years after its first workshop, CHES is now very firmly established as the premier international forum for presenting scientific and technological advances in cryptographic engineering research, the event that bridges the gap between theoretical advances and their practical application in commercial products.

In order to further extend the scope of CHES, this year's CHES included for the first time a special Hot Topic Session. The goal of this session was to attract new authors and attendees to CHES by highlighting a new area, not represented at CHES before, but of potential interest to CHES participants. The topic of this year's Hot Topic Session was: Hardware Trojans and Trusted ICs. The session was chaired by Anand Raghunathan from Purdue University, USA, who prepared a separate call for papers, and oversaw an evaluation of papers submitted to this session. This evaluation was supported by a special Hot Topic Session Committee, composed of six experts in the field of trusted integrated circuit manufacturing. The session included two regular presentations, and an

invited talk, entitled "The State-of-the-Art in IC Reverse Engineering," delivered by Randy Torrance from Chipworks, Inc., Canada.

Additionally, the workshop included two other excellent invited talks. Christof Paar from Ruhr-Universität Bochum, one of the two founders of CHES, discussed his vision of cryptographic engineering, and its evolution over years, in a talk entitled "Crypto Engineering: Some History and Some Case Studies." Srini Devadas, MIT, an inventor of PUF (Physical Unclonable Function), and a founder of a company that develops practical products based on this new technology, described his experiences in a talk entitled "Physical Unclonable Functions and Secure Processors."

The workshop also included two special sessions. Elisabeth Oswald chaired a session on the DPA contest, which included an introduction and discussion of the contest by one of the primary contest organizers, Sylvain Guilley from Telecom ParisTech. Following the introduction was a short presentation by the winners of the contest and a panel discussion devoted to the current and future rules of the contest and the ethical issues associated with inadvertently facilitating through the contest practical attacks against implementations of cryptography. The second special session, chaired by Patrick Schaumont from Virginia Tech, was on benchmarking of cryptographic hardware. The session included several interesting short talks on problems and solutions related to fair and comprehensive evaluation of the performance of cryptographic hardware. This session was of particular significance in light of the ongoing evaluation of the SHA-3 candidates competing to become a new American, and a de-facto worldwide, hash function standard. Additionally, the workshop included two traditional events: a rump session, chaired by Guido Bertoni from STMicroelectronics, Italy, and a poster session chaired by Stefan Mangard, Infineon Technologies, Germany. Our great thanks go to all Special Session Chairs for their initiative, enthusiasm, commitment, innovative spirit, and attention to every detail of their respective sessions.

Through a nomination process and a vote, the Program Committee awarded three CHES 2009 Best Paper Awards. The selected papers represent three distinct areas of cryptographic engineering research: efficient hardware implementations of public key cryptography, efficient and secure software implementations of secret key cryptography, and side-channel attacks and countermeasures. The winners of the three equivalent awards were: Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto, and Francisco Rodríguez-Henríquez for their paper "Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers," Emilia Käsper and Peter Schwabe for their paper "Faster and Timing-Attack Resistant AES-GCM," and Thomas Finke, Max Gebhardt, and Werner Schindler for their paper "A New Side-Channel Attack on RSA Prime Generation."

The selection of 29 best papers out of 148 predominantly very strong submissions was a very challenging and difficult task. The Program Committee members dedicated a very significant amount of time and effort in order to comprehensively and fairly evaluate all submitted papers and provide useful feedback to

the authors. Our deepest thanks go to the members of the Program Committee for their hard work, expertise, dedication, professionalism, fairness, and team spirit.

We deeply thank Marcelo Kaihara, the General Chair of CHES 2009, for his excellent and always timely work on managing the local organization and orchestrating conference logistics. Only because of his tireless effort, flexibility, and team spirit were we able to fit so many additional events and special sessions in the program of this year's CHES. We would like to also thank EPFL for providing an excellent venue for holding the workshop, and for assisting with many local arrangements. Our gratitude also goes to the generous sponsors of CHES 2009, namely, Cryptography Research, Inc., Nagravision Kudelski Group, Oberthur Technologies, RCIS AIST Japan, Riscure, and Telecom ParisTech.

We are also very grateful to Çetin Kaya Koç for managing conference announcements and advertising as the Publicity Chair, and to Jens-Peter Kaps for diligently maintaining the CHES website. The review and discussion process was run using an excellent Web Submission and Review System developed and maintained by Shai Halevi, who was always very quick and precise in addressing our questions and concerns regarding the operation of the system.

We would like to deeply thank the Steering Committee of CHES, for their trust, constant support, guidance, and kind advice on many occasions. Special thanks go to Jean-Jacques Quisquater and Colin Walter, who were always first to respond to our questions and concerns, and often volunteered the advice and support needed to resolve a wide array of challenging issues associated with the fair, firm, and transparent management of the evaluation process.

Finally, we would like to profoundly thank and salute all the authors from all over the world who submitted their papers to this workshop, and entrusted us with a fair and objective evaluation of their work. We appreciate your creativity, hard work, and commitment to push forward the frontiers of science. All your submissions, no matter whether accepted or rejected at this year's CHES, represent the vibrant field of research that CHES is proud to exemplify.

September 2009

Christophe Clavier
Kris Gaj

CHES 2009

Workshop on Cryptographic Hardware and Embedded Systems
Lausanne, Switzerland, September 6–9, 2009

Sponsored by *International Association for Cryptologic Research*

General Chair

Marcelo Kaihara	EPFL, Switzerland

Program Co-chairs

Christophe Clavier	Université de Limoges, France
Kris Gaj	George Mason University, USA

Publicity Chair

Çetin Kaya Koç	University of California Santa Barbara, USA

Program Committee

Lejla Batina	Katholieke Universiteit Leuven, Belgium
Daniel J. Bernstein	University of Illinois at Chicago, USA
Guido Bertoni	STMicroelectronics, Italy
Jean-Luc Beuchat	University of Tsukuba, Japan
Luca Breveglieri	Politecnico di Milano, Italy
Ernie Brickell	Intel, USA
Dipanwita Roy Chowdhury	Indian Institute of Technology, Kharagpur, India
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Joan Daemen	STMicroelectronics, Belgium
Ricardo Dahab	University of Campinas, Brazil
Markus Dichtl	Siemens AG, Germany
Benoît Feix	Inside Contactless, France
Viktor Fischer	Université de Saint-Étienne, France
Pierre-Alain Fouque	ENS, France
Catherine H. Gebotys	University of Waterloo, Canada
Christophe Giraud	Oberthur Technologies, France

Louis Goubin	Université de Versailles, France
Jorge Guajardo	Philips Research Europe, The Netherlands
Frank K. Gürkaynak	ETH Zurich, Switzerland
Peter Gutmann	University of Auckland, New Zealand
Helena Handschuh	Katholieke Universiteit Leuven, Belgium
Naofumi Homma	Tohoku University, Japan
Josh Jaffe	Cryptography Research, USA
Marc Joye	Thomson R&D, France
Jens-Peter Kaps	George Mason University, USA
Howon Kim	Pusan National University, South Korea
Çetin Kaya Koç	University of California Santa Barbara, USA
Markus Kuhn	University of Cambridge, UK
Soonhak Kwon	Sungkyunkwan University, South Korea
Kerstin Lemke-Rust	University of Applied Sciences Bonn-Rhein-Sieg, Germany
Marco Macchetti	Nagracard SA, Switzerland
Stefan Mangard	Infineon Technologies, Germany
Liam Marnane	University College Cork, Ireland
Mitsuru Matsui	Mitsubishi Electric, Japan
David Naccache	ENS, France
Dag Arne Osvik	EPFL, Switzerland
Elisabeth Oswald	University of Bristol, UK
Christof Paar	Ruhr-Universität Bochum, Germany
Dan Page	University of Bristol, UK
Pascal Paillier	Gemalto, France
Jean-Jacques Quisquater	Université catholique de Louvain, Belgium
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Pankaj Rohatgi	IBM T.J. Watson Research Center, USA
Erkay Savas	Sabanci University, Turkey
Patrick Schaumont	Virginia Tech, USA
Rainer Steinwandt	Florida Atlantic University, USA
Berk Sunar	Worcester Polytechnic Institute, USA
Elena Trichina	STMicroelectronics, France
Colin Walter	Royal Holloway, UK
Michael J. Wiener	Cryptographic Clarity, Canada
Johannes Wolkerstorfer	IAIK TU Graz, Austria
Sung-Ming Yen	National Central University, Taiwan

Program Committee Advisory Member

François-Xavier Standaert	Université catholique de Louvain, Belgium

Hot Topic Session Committee

Anand Raghunathan (Chair)	Purdue University, USA
Farinaz Koushanfar	Rice University, USA
Jim Plusquellic	University of New Mexico, USA
Pankaj Rohatgi	IBM T.J. Watson Research Center, USA
Patrick Schaumont	Virginia Tech, USA
Berk Sunar	Worcester Polytechnic Institute, USA

External Reviewers

Onur Aciicmez
Guido Costa Souza de Araújo
Kubilay Atasu
Alain Aubert
Maxime Augier
Jean-Claude Bajard
Brian Baldwin
Alessandro Barenghi
Florent Bernard
Alex Biryukov
Andrey Bogdanov
Simone Borri
Joppe Bos
Arnaud Boscher
Lilian Bossuet
Nicolas Brisebarre
Marco Bucci
Philippe Bulens
Anne Canteaut
Nathalie Casati
Mathieu Chartier
Sanjit Chatterjee
Chien-Ning Chen
Zhimin Chen
Ray Cheung
Fred Chong
Baudoin Collard
René Cumplido
Jean-Luc Danger
Pascal Delaunay
Elke De Mulder
Jérémie Detrey
Guerric Meurice de Dormale
Emmanuelle Dottax
Saar Drimer
Milos Drutarovsky
Sylvain Duquesne
Thomas Eisenbarth
Nicolas Estibals
Martin Feldhofer
Wieland Fischer
Georges Gagnerot
Berndt Gammel
Pierrick Gaudry
Willi Geiselmann
Benedikt Gierlichs
Guy Gogniat
Michael Gora
Aline Gouget
Johann Großschädl
Sylvain Guillet
Eric Xu Guo
Ghaith Hammouri
Dong-Guk Han
Neil Hanley
Guillaume Hanrot
Christoph Herbst
Clemens Heuberger
Michael Hutter
Laurent Imbert
Seyyd Hasan Mir Jalili
Pascal Junod
Marcelo Kaihara
Deniz Karakoyunlu
Markus Kasper
Chang Hoon Kim
Chong Hee Kim
Minkyu Kim
Mario Kirschbaum
Ilya Kizhvatov
Thorsten Kleinjung
Heiko Knospe
Sandeep S. Kumar
Yun-Ki Kwon
Tanja Lange
Cédric Lauradoux
Hee Jung Lee
Arjen K. Lenstra
Gaëtan Leurent
Yann L'Hyver
Wei-Chih Lien
Feng-Hao Liu
Pierre Loidreau
Raimondo Luzzi
François Mace
Abhranil Maiti
Theo Markettos
Marcel Medwed
Filippo Melzani
Nele Mentens
Giacomo de Meulenaer
Bernd Meyer
Atsushi Miyamoto
Amir Moradi
Csaba Andras Moritz
Sergey Morozov
Andrew Moss

Debdeep Mukhopadhyay
David Oswald
Siddika Berna Ors Yalcin
Young-Ho Park
Hervé Pelletier
Gerardo Pelosi
Christophe Petit
Gilles Piret
Thomas Plos
Thomas Popp
Axel Poschmann
Bart Preneel
Emmanuel Prouff
Carine Raynaud
Francesco Regazzoni
Mathieu Renauld
Matthieu Rivain
Bruno Robisson
Mylène Roussellet
Christian Rust
Akashi Satoh
Werner Schindler
Jörn-Marc Schmidt
Michael Scott
Christian Scwarz
Hermann Seuschek
Chang Shu
Hervé Sibert
Sergei Skorobogatov
Takeshi Sugawara
Ruggero Susella
Daisuke Suzuki
Yannick Teglia
Nicolas Thériault
Hugues Thiebeauld
Stefan Tillich
Kris Tiri
Arnaud Tisserand
Lionel Torres
Michael Tunstall
Jonny Valamehr
Gilles Van Assche
Jérôme Vasseur
Ihor Vasyltsov
Vincent Verneuil
Nicolas Veyrat-Charvillon
Karine Villegas
Hassan Wassel
Christopher Wolf
Tugrul Yanik
Yu Yu

Table of Contents

Software Implementations

Invited Talk 1

Side Channel Analysis of Secret Key Cryptosystems

Side Channel Analysis of Public Key Cryptosystems

Side Channel and Fault Analysis Countermeasures

Invited Talk 2

Pairing-Based Cryptography

New Ciphers and Efficient Implementations

TRNGs and Device Identification

Invited Talk 3

Hot Topic Session: Hardware Trojans and Trusted ICs

Theoretical Aspects

Fault Analysis