Stefan Lucks Ahmad-Reza Sadeghi
Christopher Wolf (Eds.)

Research in Cryptology

Second Western European Workshop, WEWoRC 2007
Bochum, Germany, July 4-6, 2007
Revised Selected Papers

Springer

Volume Editors

Stefan Lucks
Bauhaus-Universität Weimar, Fakultät Medien
Bauhausstr. 11, 99423 Weimar, Germany
E-mail: stefan.lucks@medien.uni-weimar.de

Ahmad-Reza Sadeghi
Ruhr-Universität Bochum, Lehrstuhl für Systemsicherheit
Universitätsstr. 150, 44780 Bochum, Germany
E-mail: ahmad.sadeghi@trust.rub.de

Christopher Wolf
Ruhr-Universität Bochum
Horst-Görtz-Institut für Sicherheit in der Informationstechnik
Universitätsstr. 150, 44780 Bochum, Germany
E-mail: cbw@hgi.rub.de

Library of Congress Control Number: 2008935901

CR Subject Classification (1998): E.3, D.4.6, I.1, K.6.5, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-88352-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-88352-4 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12536580 06/3180 5 4 3 2 1 0

Preface

The Western European Workshop on Research in Cryptology (WEWoRC 2007) was the second of its kind. It was organized as a joint venture between the Horst Görtz Institute for Security in Information Systems (HGI), and the Special Interest Group on Cryptology (*FG Krypto*) of the German Computer Science Society (Gesellschaft für Informatik e.V.). The aim was to bring together researchers in the field of cryptology. The workshop focused on research from Masters and PhD students, and brought them together with more experienced senior researchers. The first workshop (WEWoRC 2005) was held in Leuven.

WEWoRC 2007 was held in the German Ruhr region, more particularly in Bochum, during July 4–6, 2007. Formerly a mining town, Bochum is currently growing into a knowledge-based economy. Aided by the city council, IT security is a special focus for economic development. Hence, it provided the perfect scenery for hosting this event. In total, we had 81 participants from 13 different countries (Belgium, Finland, France, Germany, Iran, Japan, Luxembourg, Malawi, Slovenia, Taiwan, Tunisia, UK, USA).

In total, we received 39 submissions of which 36 where chosen for presenting in 14 sessions. In addition, the program was enriched by two invited talks, namely, by George Danezis on *"Cryptography in Anonymous Communications"* and David Naccache on *"Products of Small Primes in Cryptography and Error-Correction."* Selecting papers for publication in these postproceedings was done in two phases. In the first phase, during the workshop, the authors of 24 of the 36 talks were invited to submit a full paper for these postproceedings. In the second phase, after we received the 24 invited submissions, these were reviewed by the members of our Program Committee. Each paper was reviewed in a careful refereeing process by at least three experts in the area. If one of the authors was a member of the Program Committee, at least five reviews were requested. We used a total of 73 reviews for finally selecting the 12 papers presented here.

We are very grateful to all the Program Committee members who devoted much effort and valuable time to reading and selecting the papers. These postproceedings contain the final versions of each paper revised after the conference. Since the revised versions were not checked by the Program Committee members rigorously, the authors must bear full responsibility for the contents of their papers. We also want to thank the external experts who assisted the Program Committee in evaluating various papers.

Special thanks to our sponsors who made it possible to offer WEWoRC for a competitive price. Their logos are on the first page of these post-proceedings. Similarly, we want to mention the cooperation with our academic partners EIDMA and Ecrypt. In addition, we want to thank the local Organizing Committee for their skillful, professional, and enthusiastic support of WEWoRC. Keep in mind that all work was done voluntarily. Special thanks go in this context to the

Horst Görtz Institute, which kindly agreed to host the workshop in Bochum and for allowing us to use the HGI infrastructure (both technical and administrative) for WEWoRC.

Finally, we would like to thank all authors — including those whose submissions were not successful, as well as the workshop participants from around the world for their support, which made WEWoRC a big success.

December 2007

Stefan Lucks
Ahmad-Reza Sadeghi
Christopher Wolf

Organization

Program Committee

Ammar Alkassar	Sirix AG, Germany
Frederik Armknecht	NEC, Germany
N. Asokan	Nokia Research Helsinki, Finland
Roberto Avanzi	Ruhr University Bochum, Germany
Lynn Batten	Deakin University, Australia
Alex Biryukov	University of Luxembourg, Luxembourg
Johannes Blömer	Paderborn, Germany
Colin Boyd	Queensland University of Technology, Australia
Lejla Batina	KU Leuven, Belgium
Dario Catalano	CNRS-ENS, France; Universitá di Catania, Italy
Christophe Clavier	Gemalto, France
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Steven Galbraith	Royal Holloway, University of London, UK
Joachim von zur Gathen	b-it Bonn, Germany
Willi Geiselmann	TU Karlsruhe, Germany
Marc Girault	France Telecom, France
Louis Goubin	University of Versailles, France
Aline Gouget	Gemalto, France
Helena Handschuh	Spansion, France
Florian Hess	TU Berlin, Germany
Erwin Hess	Siemens, Germany
Ellen Jochemsz	TU Eindhoven, The Netherlands
Dogan Kesdogan	RWTH Aachen, Germany
Eike Kiltz	CWI, The Netherlands
Ulrich Kühn	Sirrix AG, Germany
Arjen Lenstra	EPFL, Switzerland
Francoise Levy-dit-Vehel	ENSTA, France
Gregor Leander	Ruhr University Bochum, Germany
Stefan Lucks	Bauhaus University Weimar, Germany
Keith Martin	Royal Holloway, University of London, UK
Alexander May	TU Darmstadt, Germany
Chris Mitchell	Royal Holloway, University of London, UK
David Naccache	ENS Paris, France
Heike Neumann	Philips Semiconductors, Germany
Svetla Nikova	KU Leuven, Belgium
Siddika Berna Ors	Istanbul Technical University, Turkey

Elisabeth Oswald	Bristol, UK
Christof Paar	Ruhr University Bochum, Germany
Kenny Paterson	Royal Holloway, University London, UK
Bart Preneel	KU Leuven, Belgium
Vincent Rijmen	TU Graz, Austria; Cryptomathic, Denmark
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Christian Tobias	Utimaco, Germany
Rei Safavi-Naini	University of Wollongong, Australia
Jörg Schwenk	Ruhr University Bochum, Germany
Nicolas Sendrier	INRIA, France
Stefaan Seys	KU Leuven, Belgium
Heiko Stamer	Kassel, Germany
Henk van Tilborg	TU Eindhoven, The Netherlands
Pim Tuyls	Philips, The Netherlands
Pascal Véron	University of Toulon, France
Moti Yung	Columbia University and RSA Laboratories, USA
Michael Welschenbach	SRC Security Research and Consulting, Germany
Ralf-P. Weinmann	TU Darmstadt, Germany
Thomas Wilke	Kiel, Germany
Ralph Wernsdorf	Rohde & Schwarz SIT GmbH, Germany
Christopher Wolf	PwC Luxembourg; K.U.Leuven, Belgium
Po-Wah Yau	Royal Holloway, University of London, UK
Erik Zenner	Technical University of Denmark

Referees

Ali Akbar Sobhi Afshar
Carlos Aguilar-Melchor
Mohammad Reza Aref
Bechir Ayeb
Michael Beiter
Waldyr Benits
Nicolas T. Courtois
Léonard Dallot
George Danezis
Blandine Debraize
Jintai Ding
Taraneh Eghlidos
Mohammad Ehdaie
Thomas Eisenbarth
Jan-Erik Ekberg
Junfeng Fan
Ewan Fleischmann
Philippe Gaborit
Sebastian Gajek
Steven Galbraith
Timo Gendrullis
Benedikt Gierlichs
Tim Güneysu
Mabrouka Hagui
Rupert J. Hartung
Wei-Hua He
Marko Hölbl
Hideki Imai
Sebastiaan Indesteege
Kare Janussen
Fei-Ming Juan
Timo Kasper
Dalia Khader
Hedi Khammari
Anja Korsten
Paul Kubwalo
Kerstin Lemke-Rust
Lijun Liao
Stéphane Manuel
Mark Manulis
Gordon Meiser
David Naccache
María Naya-Plasencia
Akira Otsuka
Christof Paar
Souradyuti Paul
Selwyn Piramuthu
Joris Plessers
Bart Preneel
Christoph Puttmann
Christian Rechberger

Andrea Röck
Ahmad-Reza Sadeghi
Kazuo Sakiyama
Sven Schäge
Dieter Schmidt
Thomas Schwarzpaul
Jörg Schwenk
Gautham Sekar
Nicolas Sendrier
Rie Shigetomi
Jamshid Shokrollahi
Dirk Stegemann
Yu-Ju Tu
Caroline Vanderheyden
Ingrid Verbauwhede
Tatjana Welzer
Fabian Werner
Ralph Wernsdorf
Rei Yoshida
Kazuki Yoshizoe

Silver Sponsors

vodafone™

ftgroup

NOKIA
Connecting People

PHILIPS

ROHDE&SCHWARZ

Bronze Sponsors

escrypt
Embedded Security

Sirrix AG
security technologies

Table of Contents