Lecture Notes in Computer Science 7242

Frederik Armknecht Stefan Lucks (Eds.)

Research in Cryptology

4th Western European Workshop, WEWoRC 2011
Weimar, Germany, July 20-22, 2011
Revised Selected Papers

Springer

Volume Editors

Frederik Armknecht
Universität Mannheim
Arbeitsgruppe Theoretische Informatik und IT-Sicherheit
A5,6, 68131 Mannheim, Germany
E-mail: armknecht@uni-mannheim.de

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-34158-8 e-ISBN 978-3-642-34159-5
DOI 10.1007/978-3-642-34159-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012948763

CR Subject Classification (1998): E.3, D.4.6, I.1, K.6.5, K.4.4, 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 Western European Workshop on Research in Cryptology (WEWoRC) is a bi-annual workshop with a specific focus on research performed by junior scientists. The specific focus is exhibited by the rule that at least one of the authors of a paper to be presented and, especially, included in the proceedings must be a junior researcher.

WEWoRC 2011 was held at the Bauhaus-Universität Weimar in Germany, organized by the Department of Media, Bauhaus-Universität Weimar, in cooperation with the Gesellschaft für Informatik e.V. (GI). It was the fourth of its kind, after WEWoRC 2005 in Leuven, Belgium, WEWoRC 2007 in Bochum, Germany, and WEWoRC 2009 in Graz, Austria.

Beyond the rule of requiring at least one junior researcher to (co-) author a paper, the WEWoRC is special because:

1. The authors submit a short abstract for WEWoRC.
2. If the Program Chairs consider the paper on topic for WEWoRC, the authors are asked to present their work at the workshop.
3. At the workshop, the Program Chairs invite the best presenters and the authors of the best abstracts to submit a full version (or an extended abstract) for the final proceedings.
4. These submissions are reviewed by the Program Committee(PC), which eventually decides which will be included in the proceedings.

That means unfinished ideas and, sometimes, unpublishable work can still be presented at the workshop, while the proceedings will only include mature work and good results. We believe that this process addresses the specific needs of junior researchers better than the traditional all-or-nothing approach at cryptographic research meetings, where the review comes first and papers are either presented and published in the proceedings, or neither presented nor published.

The technical program of WEWoRC 2011 consisted of 25 submitted and two invited talks. The invited talks where given by two senior researchers, Heike Neumann from NXP Semiconductors on “The Practice of Cryptography” and Marc Fischlin from TU Darmstad on “Key Exchange – 35 Years and Still Rolling.” The technical program was amended by a social program: A welcome reception on the evening before the conference, the “Bauhaus Walk” at the places where the famous Bauhaus school for crafts and fine arts was founded, and a conference dinner.

After being invited for the final proceedings and reviewed by at least four members of the PC (submissions with a member from the PC as one of the authors where reviewed by six independent PC members), ten papers where finally chosen for these proceedings.

Thank you! We thank all the authors and co-authors of abstracts submitted to WEWoRC for presentation, and, especially all the junior researchers and the invited speakers, who came to Weimar to present their work and participate in the discussions. We are grateful to the the local staff from Bauhaus-Universität Weimar, who worked hard to make WEWoRC 2011 possible and successful (in alphabetical order: Christian, Ewan, Jakob, Nadin, Theresa). We thank the PC members for their reviews and lively discussions. Last, but not least, we thank the sponsors, NXP Semiconductors and NEC Europe, whose contribution allowed us to support some ill-funded presenters and to invite the speakers for the invited talks.

July 2012

Frederik Armknecht
Stefan Lucks

Organization

Program Committee

F. Armknecht
J.-M. Bohli
C. Boyd
C. Cid
O. Dunkelman
J. von zur Gathen
W. Geiselmann
H. Handschuh
F. Hess
S. Katzenbeisser
G. Leander
S. Lucks
R. Maes
A. May
W. Meier
H. Neumann
T. Peyrin
B. Preneel
C. Rechberger
V. Rijmen
A.-R. Sadeghi
J.-P. Seifert
F.-X. Standaert
M. Yung
C. Wolf
E. Zenner

Sponsoring Institutions

NXP Semiconductors N.V., Eindhoven, The Netherlands
NEC Europe Ltd., Heidelberg, Germany

Table of Contents