Lecture Notes in Computer Science 8898

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

Editorial Board

More information about this series at http://www.springer.com/series/7410

Thomas Eisenbarth · Erdinç Öztürk (Eds.)

Lightweight Cryptography for Security and Privacy

Third International Workshop, LightSec 2014
Istanbul, Turkey, September 1–2, 2014
Revised Selected Papers

Springer

Editors
Thomas Eisenbarth
Worcester Polytechnic Institute
Worcester, MA
USA

Erdinç Öztürk
Istanbul Commerce University
Istanbul
Turkey

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-16362-8 ISBN 978-3-319-16363-5 (eBook)
DOI 10.1007/978-3-319-16363-5

Library of Congress Control Number: 2015932981

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

LightSec 2014 is the Third International Workshop on Lightweight Cryptography for Security and Privacy, which was held in Eminönü, Istanbul, Turkey, during September 1–2, 2014. The workshop was sponsored by TÜBİTAK BİLGEM UEKAE (The Scientific and Technological Research Council of Turkey, National Research Institute of Electronics and Cryptology) and held in cooperation with the International Association of Cryptologic Research (IACR).

The Program Committee (PC) consisted of 31 members representing 13 countries. There were 24 papers from 15 countries submitted to the workshop. Submitted papers were reviewed by the PC members themselves or by assigned subreviewers. Each submission was double-blind reviewed by at least three PC members and the submissions by PC members were assigned to 14 subreviewers. The vast majority of the papers were reviewed by four reviewers. Twelve of the papers were accepted for presentation at the workshop, whereas two of them were conditionally accepted. These two conditionally accepted papers were later withdrawn.

The program also included three excellent invited talks by experts in the field. The first talk was given by Tolga Acar from Microsoft Research titled "Selecting and Deploying Elliptic Curves in Security Protocols." The second talk was given by Guido Marco Bertoni from ST Microelectronics titled "Permutation-based encryption for lightweight applications." The final invited talk was delivered by Johann Heyszl from Fraunhofer AISEC titled "High-Resolution Magnetic Field Side-Channels and their Affect on Cryptographic Implementations."

We would like to thank all the people and organizations who contributed to making the workshop successful. First, we greatly appreciate the valuable work of the authors and we thank them for submitting their manuscripts to LightSec 2014. We are also grateful to the PC members and the External Reviewers whose admirable effort in reviewing the submissions definitely enhanced the scientific quality of the program. Thanks also to the invited speakers, Tolga Acar, Guido Marco Bertoni, and Johann Heyszl, for their willingness to participate in LightSec 2014. We would like to also thank Istanbul Chamber of Commerce and Istanbul Commerce University, who made this workshop possible by letting us use their facilities. We would like to thank Ali Boyacı and Serhan Yarkan from EE Engineering Department at Istanbul Commerce University for their admirable help in organizing the workshop. Last but not least, we would like to thank students of the EE Engineering Department at Istanbul Commerce University, for their help in running the workshop.

September 2014

Erdinç Öztürk
Thomas Eisenbarth

Organization

Organizing Committee

General Chair

Erdinç Öztürk	Istanbul Commerce University, Turkey

Program Committee

Program Chairs

Erdinç Öztürk	Istanbul Commerce University, Turkey
Thomas Eisenbarth	Worcester Polytechnic Institute, USA

Technical Program Committee

Tolga Acar	Microsoft Research, USA
Onur Aciicmez	Samsung, USA
Elena Andreeva	COSIC, KU Leuven, Belgium
Jean-Philippe Aumasson	Kudelski Security, Switzerland
Paulo Barreto	University of São Paulo, Brazil
Lejla Batina	Radboud University Nijmegen, The Netherlands
Guido Bertoni	ST Microelectronics, Italy
Andrey Bogdanov	Technical University of Denmark, Denmark
Elke De Mulder	Cryptography Research Inc., USA
Kris Gaj	George Mason University, USA
Berndt Gammel	Infineon Technologies, Germany
Shay Gueron	University of Haifa, Israel
Francisco Rodríguez Henríquez	CINVESTAV-IPN, Mexico
Pascal Junod	HEIG-VD, Switzerland
Jens-Peter Kaps	George Mason University, USA
Mehran Mozaffari Kermani	Rochester Institute of Technology, USA
Mehmet Sabir Kiraz	TÜBİTAK BİLGEM UEKAE, Turkey
Xuejia Lai	Shanghai Jiao Tong University, China
Albert Levi	Sabanci University, Turkey
Amir Moradi	Ruhr University Bochum Germany
Axel Poschmann	NXP Semiconductors, Germany
Francesco Regazzoni	ALaRI, Lugano, Switzerland
Arash Reyhani-Masoleh	University of Western Ontario, Canada
Erkay Savaş	Sabanci University, Turkey
Nitesh Saxena	University of Alabama at Birmingham, USA
Ali Aydin Selçuk	TOBB University of Economics and Technology, Turkey
Georg Sigl	Technische Universität München, Germany

Michael Tunstall	Cryptography Research Inc., USA
Meltem Sonmez Turan	National Institute of Standards and Technology, USA
Kerem Varici	Université Catholique de Louvain, Belgium
Amr Youssef	Concordia University, Canada

Steering Committee

Gildas Avoine	Université Catholique de Louvain, Belgium
Hüseyin Demirci	TÜBİTAK BİLGEM, Turkey
Orhun Kara	TÜBİTAK BİLGEM, Turkey
Erkay Savaş	Sabanci University Turkey
Ali Aydın Selçuk	TOBB University of Economics and Technology, Turkey
Berk Sunar	Worcester Polytechnic Institute, USA

Local Committee

Ali Boyacı	Istanbul Commerce University, Turkey
Serhan Yarkan	Istanbul Commerce University, Turkey

Additional Reviewers

S. Abhishek Anand
Shivam Bhasin
Begul Bilgin
Muhammed Ali Bingol
Joppe Bos
Joo Yeon Cho
Benedikt Driessen
Baris Ege
Jialin Huang
Süleyman Kardas
Thomas Korak
Wei Li
Suresh Limkar
John Michener
Manar Mohamed
Lan Nguyen
Kostas Papagiannopoulos
Roel Peeters
Gokay Saldamli
Fabrizio de Santis
Maliheh Shirvanian
Osmanbey Uzunkol
Rajesh Velegalati
Vincent Verneuil
MarkusWamser
Michael Weiner
Hong Xu
Panasayya Yalla
Greg Zaverucha

Sponsoring Institution

TÜBİTAK BİLGEM UEKAE (The Scientific and Technological Research Council of Turkey, National Research Institute of Electronics and Cryptology)

Powered by

INF Technology, Istanbul, Turkey

Invited Talks

Tolga Acar, Microsoft Research, USA

Selecting and Deploying Elliptic Curves in Security Protocols
The development and adoption of a cryptographic standard is a delicate endeavor with competing and conflicting actors, which becomes only harder with integration into security protocols some yet undefined. This talk looks at the use of Elliptic Curves (EC) in a sliver of pervasive security protocols. We cover NIST-defined ECs, impact of new information made available in the past couple of years, and current attempts to alleviate sometimes unsubstantiated yet valid concerns over these curves. This talk also presents an elliptic curve selection algorithm and its analysis from a performance and security perspective including rigid parameter generation, constant-time implementation, and exception-free scalar multiplication.

Guido Marco Bertoni, ST Microelectronics, Italy

Permutation-based encryption for lightweight applications
In the recent years we have seen a rapid development of cryptographic primitives based on permutations. The talk gives an overview on how you can easily build hash functions, stream ciphers, PRNGs, authenticated encryption and other constructions starting from a fixed-width permutation. This flexibility can be particular useful in resource-constrained applications, basically a single primitive can satisfy all the security needs typically requested to symmetric key primitives. Finally there will be the introduction of Ketje, a lightweight authenticated encryption developed in collaboration with Joan Daemen, Michael Peeters, Gilles Van Assche and Ronny Van Keer.

Johann Heyszl, Fraunhofer AISEC, Germany

High-Resolution Magnetic Field Side-Channels & their Affect on Cryptographic Implementations
The last years have again seen many new developments in the field of side-channel analysis. Partly, new insights are driven by side-channel measurement equipment which becomes increasingly sophisticated due to the fact that respective devices are readily available to academics, as well as to industry and potential attackers. This talk discusses the impact of available high-resolution measurement equipment to measure magnetic fields on implementations of cryptographic algorithms. The progress in this segment of side-channel analysis affects different kinds of cryptographic implementations including light-weight implementations of elliptic curve cryptography, symmetric cryptographic algorithms, physical unclonable functions as well as new attempts to achieve leakage resilience for block ciphers by special constructions.

Contents