Lecture Notes in Computer Science 8479

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

Ioana Boureanu Philippe Owesarski
Serge Vaudenay (Eds.)

Applied Cryptography and Network Security

12th International Conference, ACNS 2014
Lausanne, Switzerland, June 10-13, 2014
Proceedings

Springer

Volume Editors

Ioana Boureanu
Akamai EMEA
Addlestone, UK
E-mail: icboureanu@gmail.com

Philippe Owesarski
LAAS-CNRS, SARA
Toulouse, France
E-mail: owe@laas.fr

Serge Vaudenay
EPFL, IC LASEC
Lausanne, Switzerland
E-mail: serge.vaudenay@epfl.ch

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-07535-8 e-ISBN 978-3-319-07536-5
DOI 10.1007/978-3-319-07536-5
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014939351

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 12th International Conference on Applied Cryptography and Network Security (ACNS) was held during June 10–13, 2014 in Lausanne, Switzerland. It was hosted by the Ecole Polytechnique Fédérale de Lausanne (EPFL).

The conference received 147 submissions. They went through a doubly-anonymous review process and 33 papers were selected. We were helped by 41 Program Committee members and 156 external reviewers.

We were honored to host Phillip Rogaway and Nadia Heninger as invited speakers.

This volume represents the revised version of the accepted papers along with the abstract of the invited talks.

Following the ACNS tradition, the Program Committee selected a paper to award. To be eligible, the paper had to be co-authored by one full time student who presented the paper at the conference. This year, the Best Student Paper Award was given to Annelie Heuser for her paper

"Detecting Hidden Leakages"

written in collaboration with Amir Moradi and Sylvain Guilley.

The submission and review process was done using the iChair Web-based software system developed by Thomas Baignères and Matthieu Finiasz. They provided us with great help by updating iChair to our needs.

We would like to thank the authors of all submitted papers. Moreover, we are grateful to the members of the Program Committee and the external subreviewers for their diligent work, as well as to the staff members of the Security and Cryptography Laboratory (LASEC) of EPFL for their kind help in the organization of the event. We would also like to acknowledge the Steering Committee for supporting us.

Finally, we heartily thank the following bodies, for their kind financial support: the Swiss National Science Foundation, the Hasler Foundation, the Federal Office of Communications, the Center of Risk Analysis and Risk Governance (CRAG) of EPFL, Baidu, and the Distributed Systems Laboratory (LSR) of EPFL, headed by André Schiper. All financial risks were taken by LASEC at EPFL.

April 2014

Ioana Boureanu
Philippe Owesarski
Serge Vaudenay

Organization

Program Committee

Frederik Armknecht	University of Mannheim, Germany
Gildas Avoine	INSA Rennes and UCL, France and Belgium
Marinho P. Barcellos	Federal University of Rio Grande do Sul, Brasil
Alex Biryukov	University of Luxembourg, Luxembourg
Christina Brzuska	Tel-Aviv University, Israel
Anne Canteaut	Inria Paris-Rocquencourt, France
Barbara Carminati	University of Insubria, Italy
Isabelle Chrisment	University of Lorraine, France
Véronique Cortier	CNRS, France
Xuhua Ding	Singapore Management University, Singapore
Jordi Forné	Technical University of Catalonia, Spain
Peter Gutmann	University of Auckland, New Zealand
Cătălin Hriţcu	University of Pennsylvania and Inria Paris-Rocquencourt, USA and France
Marc Joye	Technicolor, France
Steve Kremer	Inria, France
Kaoru Kurosawa	Ibaraki University, Japan
Ralf Küsters	University of Trier, Germany
Xuejia Lai	Shanghai Jiao Tong University, China
Javier Lopez	University of Malaga, Spain
Matteo Maffei	Saarland University, Germany
Wojciech Mazurczyk	Warsaw University of Technology, Poland
Ludovic Mé	Supelec, France
Ilya Mironov	Microsoft Research Silicon Valley, USA
Katerina Mitrokotsa	Chalmers University of Technology, Sweden
Atsuko Miyaji	JAIST, Japan
Svetla Nikova	KU Leuven, Belgium
Miyako Ohkubo	NICT, Japan
Kenny Paterson	Royal Holloway, UK
Goutam Paul	Indian Statistical Institute Kolkata, India
Christophe Petit	UCL, Belgium
Carla Ràfols	Ruhr University Bochum, Germany
Christian Rechberger	DTU, Denmark
Reza Reyhanitabar	EPFL, Switzerland
Mark Ryan	University of Birmingham, UK
Rei Safavi-Naini	University of Calgary, Canada
Jennifer Seberry	University of Wollongong, Australia
Asia Slowinska	Vrije Universiteit Amsterdam, The Netherlands

Gilles Van Assche	STMicroelectronics, Belgium
Michael Waidner	Fraunhofer SIT & TU Darmstadt, Germany
Bogdan Warinschi	University of Bristol, UK
Jianying Zhou	Institute for Infocomm Research, Singapore

External Reviewers

Aysajan Abidin
Isaac Agudo
Ahmad Ahmadi
Martin Albrecht
Cristina Alcaraz
Mohsen Alimomeni
Hoda A. Alkhzaimi
Elena Andreeva
Radoniaina Andriatsimandefitra
Subhadeep Banik
David Bernhard
Rishiraj Bhattacharyya
Christophe Bidan
Olivier Blazy
Céline Blondeau
Alexandra Boldyreva
Özkan Boztaş
Krzysztof Cabaj
Eleonora Cagli
Angelo De Caro
Xavier Carpent
Anrin Chakraborti
Kaushik Chakraborty
Anupam Chattopadhyay
Jiageng Chen
Céline Chevalier
Thibault Cholez
Sherman S.M. Chow
Oana Ciobotaru
Cas Cremers
Joan Daemen
Gareth T. Davies
Antoine Delignat-Lavaud
Patrick Derbez
Xinshu Dong
Alexandre Duc
Xiwen Fang
Sebastian Faust
Florian Feldmann
Gerardo Fernandez
Daniel Fett
Nils Fleischhacker
Jun Furukawa
Yuichi Futa
David Galindo
Sébastien Gambs
Wei Gao
Pierrick Gaudry
Asadullah Ghalib
Benedikt Gierlichs
Zheng Gong
Vincent Grosso
Felix Günther
Siyao Guo
Jens Hermans
Geshi Huang
Jialin Huang
Mitsugu Iwamoto
Angela Jäschke
Jérémy Jean
Mahavir Jhawar
Han Jinguang
Saqib A. Kakvi
Aniket Kate
Dmitry Khovratovich
Stefan Kölbl
Junzuo Lai
Virginie Lallemand
Enrique Larraia
Liran Lerman
Gaëtan Leurent
Wei Li
Kaitai Liang
Benoît Libert
Jia Liu
Joseph K. Liu
Zhe Liu
Yu Long

Atul Luykx
Vadim Lyubashevsky
Xianping Mao
Giorgia Azzurra Marson
Takahiro Matsuda
Matthijs Melissen
Bart Mennink
Marine Minier
Francisco Moyano
Imon Mukherjee
Shishir Nagaraja
Pablo Najera
Gregory Neven
Ana Nieto
David Nuñez
Kazumasa Omote
Cristina Onete
Mihai Ordean
Kim Pecina
Roel Peeters
Léo Paul Perrin
Joshua Phillips
Le Trieu Phong
David Pointcheval
Gordon Proctor
Ivan Pustogarov
Elizabeth Quaglia
Sasa Radomirovic
David Rebollo-Monedero
Manuel Reinert
Christian Reuter
Vincent Rijmen
Ruben Rios
Arnab Roy
Elzbieta Rzeszutko
Kai Samelin
Somitra Sanadhya
Pratik Sarkar
Santanu Sarkar
Alessandra Scafuro
Enrico Scapin
Guido Schmitz
Peter Scholl
Stefaan Seys
Ben Smyth
Chunhua Su
Koutarou Suzuki
Tsuyoshi Takagi
Keisuke Tanaka
Satoru Tanaka
Qiang Tang
Susan Thomson
Tyge Tiessen
Valérie Viet Triem Tong
Tomasz Truderung
Mathieu Turuani
Kerem Varici
Vesselin Velichkov
Srinivas Vivek Venkatesh
Frederik Vercauteren
Lei Wang
Pengwei Wang
Gaven Watson
Hoeteck Wee
Patrick Weiden
Jakob Wenzel
Hong Xu
Jia Xu
Rui Xu
Shota Yamada
Anjia Yang
Masaya Yasuda
Kazuki Yoneyama
Maki Yoshida
Tsz Hon Yuen
Jiangshan Yu
Liang Feng Zhang
Tongjie Zhang

Conference Chairs

Ioana Boureanu	HEIG-VD, Switzerland
Philippe Owezarski	CNRS, France
Serge Vaudenay	EPFL, Switzerland

Invited Talks

How Not to Generate Random Numbers

Nadia Heninger

Department of Computer and Information Science,
University of Pennsylvania

Abstract. Randomness is essential to cryptography: cryptographic security depends on private keys that are unpredictable to an attacker. But how good are the random number generators that are actually used in practice? In this talk, I will discuss several large-scale surveys of cryptographic deployments, including TLS, SSH, Bitcoin, and secure smart cards, and show that random number generation flaws are surprisingly widespread. We will see how many of the most commonly used public key encryption and signature schemes can fail catastrophically if used with faulty random number generators, and trace many of the random number generation flaws we encountered to specific implementations and vulnerable implementation patterns.

The Emergence of Authenticated Encryption

Phillip Rogaway

Dept. of Computer Science,
University of California, Davis, USA

Abstract. Although practical schemes for symmetric encryption (eg, blockcipher modes) are one of the main "exports" of cryptography, for years serious cryptographers mostly ignored this corner of our field. In recent years this has dramatically changed: there has been a quiet revolution in our understanding of *what definitions* general-purpose symmetric encryption schemes should meet and *what algorithms* should be employed to satisfy them. On the definitional side we have come to recognize that semantic security under a chosen-plaintext attack is too weak a notion for a general-purpose scheme. Notions for *authenticated encryption* (AE), which deliver both privacy and authenticity, have emerged as a stronger alternative. On the algorithmic side, security practitioners have increasingly abandoned classical modes like CBC, choosing AE schemes like CCM and GCM in their place.

One reason for this evolution in definitions and schemes is recognition of the fact that a scheme that delivers both privacy and authenticity can be more efficient than the amalgamation of separate privacy and authenticity techniques. Another reason for the change is the realization that an encryption scheme that delivers more is less likely to be misused.

In this talk I'll trace the history of AE, exploring why it emerged, how it evolved, and what some new schemes have come to look like. We'll explore how the basic syntax of AE has changed, and how security notions for AE continue to evolve, including the introduction of misuse-resistance, online, and robust AE. I'll look afresh at generic composition. I'll describe a new AE scheme that I recently co-developed, AEZ. Finally, I'll talk about the CAESAR competition for AE schemes, a contest that has drawn a remarkable 57 round-1 submissions.

AE is rare topic insofar as cryptographic theory and practice have been tightly linked; in particular, practice-oriented provable security has been at the center of this area. The dialectic around AE between theory-oriented and practice-oriented individuals has been unusually strong, with the interaction resulting in better theory and better practice.

Keywords: Authenticated encryption, modes of operation, practice-oriented provable security, symmetric encryption.

Table of Contents

Key Exchange

Primitive Construction

Attacks (Public-Key Cryptography)

Hashing

Cryptanalysis & Attacks (Symmetric Cryptography)

Network Security

Signatures

System Security

Secure Computation