

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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
ISBN 978-3-319-07535-8
DOI 10.1007/978-3-319-07536-5
Springer Cham Heidelberg New York Dordrecht London

e-ISSN 1611-3349
e-ISBN 978-3-319-07536-5

Library of Congress Control Number: 2014939351

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer International Publishing Switzerland 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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 sub-reviewers 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 Boureau
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 Hrițcu	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
Michael Waidner
Bogdan Warinschi
Jianying Zhou

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

New Modular Compilers for Authenticated Key Exchange	1
<i>Yong Li, Sven Schäge, Zheng Yang, Christoph Bader, and Jörg Schwenk</i>	
Password-Based Authenticated Key Exchange without Centralized Trusted Setup	19
<i>Kazuki Yoneyama</i>	
A Linear Algebra Attack to Group-Ring-Based Key Exchange Protocols	37
<i>M. Kreuzer, A.D. Myasnikov, and A. Ushakov</i>	

Primitive Construction

Improved Constructions of PRFs Secure against Related-Key Attacks	44
<i>Kevin Lewi, Hart Montgomery, and Ananth Raghunathan</i>	
Verifiable Multi-server Private Information Retrieval	62
<i>Liang Feng Zhang and Reihaneh Safavi-Naini</i>	
Certified Bitcoins	80
<i>Giuseppe Ateniese, Antonio Faonio, Bernardo Magri, and Breno de Medeiros</i>	
Leakage Resilient Proofs of Ownership in Cloud Storage, Revisited	97
<i>Jia Xu and Jianying Zhou</i>	
Private Message Transmission Using Disjoint Paths	116
<i>Hadi Ahmadi and Reihaneh Safavi-Naini</i>	

Attacks (Public-Key Cryptography)

Partial Key Exposure Attacks on Takagi's Variant of RSA	134
<i>Zhangjie Huang, Lei Hu, Jun Xu, Liqiang Peng, and Yonghong Xie</i>	
New Partial Key Exposure Attacks on CRT-RSA with Large Public Exponents	151
<i>Yao Lu, Rui Zhang, and Dongdai Lin</i>	
Bit-Flip Faults on Elliptic Curve Base Fields, Revisited	163
<i>Taechan Kim and Mehdi Tibouchi</i>	

Hashing

All-but-One Dual Projective Hashing and Its Applications	181
<i>Zongyang Zhang, Yu Chen, Sherman S.M. Chow, Goichiro Hanaoka, Zhenfu Cao, and Yunlei Zhao</i>	
Distributed Smooth Projective Hashing and Its Application to Two-Server Password Authenticated Key Exchange	199
<i>Franziskus Kiefer and Mark Manulis</i>	
Sakura: A Flexible Coding for Tree Hashing	217
<i>Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche</i>	
Reset Indifferentiability from Weakened Random Oracle Salvages One-Pass Hash Functions	235
<i>Yusuke Naito, Kazuki Yoneyama, and Kazuo Ohta</i>	

Cryptanalysis & Attacks (Symmetric Cryptography)

Memoryless Unbalanced Meet-in-the-Middle Attacks: Impossible Results and Applications	253
<i>Yu Sasaki</i>	
On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers	271
<i>Céline Blondeau, Andrey Bogdanov, and Meiqin Wang</i>	
Improved Cryptanalysis on Reduced-Round GOST and Whirlpool Hash Function	289
<i>Bingke Ma, Bao Li, Ronglin Hao, and Xiaoqian Li</i>	
Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro	308
<i>Yanfeng Wang, Wenling Wu, Zhiyuan Guo, and Xiaoli Yu</i>	
Detecting Hidden Leakages	324
<i>Amir Moradi, Sylvain Guilley, and Annelie Heuser</i>	

Network Security

Improving Intrusion Detection Systems for Wireless Sensor Networks . . .	343
<i>Andriy Stetsko, Tobiáš Smolka, Vashek Matyjáš, and Martin Stehlík</i>	
MoTE-ECC: Energy-Scalable Elliptic Curve Cryptography for Wireless Sensor Networks	361
<i>Zhe Liu, Erich Wenger, and Johann Großschädl</i>	

BackRef: Accountability in Anonymous Communication Networks	380
<i>Michael Backes, Jeremy Clark, Aniket Kate, Milivoj Simeonovski, and Peter Druschel</i>	

WebTrust – A Comprehensive Authenticity and Integrity Framework for HTTP	401
<i>Michael Backes, Rainer W. Gerling, Sebastian Gerling, Stefan Nürnberger, Dominique Schröder, and Mark Simkin</i>	

Signatures

A Revocable Group Signature Scheme from Identity-Based Revocation Techniques: Achieving Constant-Size Revocation List	419
<i>Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Yusuke Sakai</i>	

Faster Batch Verification of Standard ECDSA Signatures Using Summation Polynomials	438
<i>Sabyasachi Karati and Abhijit Das</i>	

On Updatable Redactable Signatures	457
<i>Henrich C. Pöhls and Kai Samelin</i>	

Practical Signatures from the Partial Fourier Recovery Problem	476
<i>Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte</i>	

System Security

Activity Spoofing and Its Defense in Android Smartphones	494
<i>Brett Cooley, Haining Wang, and Angelos Stavrou</i>	

Polymorphism as a Defense for Automated Attack of Websites	513
<i>Xinran Wang, Tadayoshi Kohno, and Bob Blakley</i>	

Fragmentation Considered Leaking: Port Inference for DNS Poisoning	531
<i>Haya Shulman and Michael Waidner</i>	

Secure Computation

Delegating a Pairing Can Be Both Secure and Efficient	549
<i>Sébastien Canard, Julien Devigne, and Olivier Sanders</i>	

Automatic Protocol Selection in Secure Two-Party Computations	566
<i>Florian Kerschbaum, Thomas Schneider, and Axel Schröpfer</i>	

Author Index	585
-------------------------------	-----