

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, 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, Saarbrücken, Germany

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

Sara Foresti · Giuseppe Persiano (Eds.)

Cryptology and Network Security

15th International Conference, CANS 2016
Milan, Italy, November 14–16, 2016
Proceedings

Editors

Sara Foresti
Università degli Studi di Milano
Crema
Italy

Giuseppe Persiano
Università degli Studi di Salerno
Fisciano
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-48964-3 ISBN 978-3-319-48965-0 (eBook)
DOI 10.1007/978-3-319-48965-0

Library of Congress Control Number: 2016955512

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2016

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.

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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

These proceedings contain the papers selected for presentation at the 15th International Conference on Cryptology and Network Security (CANS 2016), held in Milan, Italy, on November 14–16, 2016. The conference was held in cooperation with the International Association of Cryptologic Research and focuses on technical aspects of cryptology and of data, network, and computer security. These proceedings contain 30 full papers (with an acceptance rate of 25.86 %) and 18 short papers selected by the Program Committee from 116 submissions. The proceedings also contain an extended abstract for the 8 posters presented at the conference.

The many high-quality submissions made it easy to build a strong program but also required rejecting good papers. Each submission was judged by at least three reviewers and the whole selection process included about six weeks of reading and discussion in the Program Committee.

The credit for the success of an event like CANS 2016 belongs to a number of people, who devoted their time and energy to put together the conference and who deserve acknowledgment. There is a long list of people who volunteered their time and energy to organize the conference, and who deserve special thanks. We would like to thank all the members of the Program Committee and all the external reviewers, for all their hard work in evaluating all the papers during the summer. We are grateful to CANS Steering Committee for their support. Thanks to Giovanni Livraga, for taking care of publicity and chairing local organization. We are very grateful to the local organizers for their support in the conference organization and logistics. We would like to thank the keynote speakers for accepting our invitation to deliver a talk at the conference.

Special thanks are due to the Università degli Studi di Milano for its support and for hosting the event, and to the Italian Association for Information Processing (AICA) for support in the secretarial and registration process.

Last but certainly not least, our thanks go to all the authors who submitted papers and posters and to all the conference's attendees. We hope you find the program of CANS 2016 interesting, stimulating, and inspiring for your future research.

November 2016

Sara Foresti
Pino Persiano
Pierangela Samarati

Organization

General Chair

Pierangela Samarati Università degli Studi di Milano, Italy

Program Chairs

Sara Foresti Università degli Studi di Milano, Italy
Giuseppe Persiano Università degli Studi di Salerno, Italy

Poster Chairs

Sara Foresti Università degli Studi di Milano, Italy
Giuseppe Persiano Università degli Studi di Salerno, Italy
Pierangela Samarati Università degli Studi di Milano, Italy

Publicity Chair

Giovanni Livraga Università degli Studi di Milano, Italy

Local Arrangements Chair

Giovanni Livraga Università degli Studi di Milano, Italy

Steering Committee

Yvo Desmedt (Chair) The University of Texas at Dallas, USA
Juan A. Garay Yahoo! Labs, USA
Amir Herzberg Bar Ilan University, Israel
Yi Mu University of Wollongong, Australia
David Pointcheval CNRS and ENS Paris, France
Huaxiong Wang Nanyang Technological University, Singapore

Program Committee

Lejla Batina Radboud University, The Netherlands
Carlo Blundo Università degli Studi di Salerno, Italy
Henry Carter Villanova University, USA
Nishanth Chandran Microsoft Research, India
Yingying Chen Stevens Institute of Technology, USA

Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong
Ricardo Dahab	IC-UNICAMP, Brazil
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Angelo De Caro	IBM Research, Zurich, Switzerland
Yvo Desmedt	The University of Texas at Dallas, USA
Nelly Fazio	City University of New York, USA
Georg Fuchsbauer	Ecole Normale Supérieure, France
Rosario Gennaro	City University of New York, USA
Amir Herzberg	Bar Ilan University, Israel
Vincenzo Iovino	University of Luxembourg, Luxembourg
Rob Johnson	Stony Brook University, USA
Florian Kerschbaum	SAP, Germany
Aggelos Kiayias	University of Athens, Greece
Albert Levi	Sabanci University, Turkey
Ming Li	University of Arizona, USA
Dongdai Lin	Chinese Academy of Sciences, China
Peng Liu	The Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Steve Lu	Stealth Software Technologies Inc., USA
Atsuko Miyaji	Osaka University/JAIST, Japan
Evangelos Markatos	University of Crete, Greece
Refik Molva	Eurecom, France
Yi Mu	University of Wollongong, Australia
Gregory Neven	IBM Research, Zurich, Switzerland
Antonio Nicolosi	Stevens Institute of Technology, USA
Svetla Nikova	KU Leuven, Belgium
Emmanuela Orsini	University of Bristol, UK
Panos Papadimitratos	KTH, Stockholm, Sweden
Stefano Paraboschi	Università di Bergamo, Italy
Gerardo Pelosi	Politecnico di Milano, Italy
Benny Pinkas	Bar Ilan University, Israel
Pierangela Samarati	Università degli Studi di Milano, Italy
Nitesh Saxena	University of Alabama at Birmingham, USA
Andreas Schaad	Huawei Research, Germany
Dominique Schroeder	Saarland University, Germany
Peter Schwabe	Radboud University, The Netherlands
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Mitsubishi Electric, Japan
Qiang Tang	University of Luxembourg, Luxembourg
Meng Yu	University of Texas at San Antonio, USA
Huaxiong Wang	Nanyang Technological University, Singapore

External Reviewers

Hamza Abusalah
 Zakir Akram
 Duygu Karaođlan Altop
 S. Abhishek Anand
 Diego Aranha
 Tomer Ashur
 Seiko Arita
 Arash Atashpendar
 Pol Van Aubel
 Monir Azraoui
 Saikrishna
 Badrinarayanan
 Amos Beimel
 Daniel Bernau
 Jonas Boehler
 Carl Bootland
 Raphael Bost
 Christina Boura
 Florian Bourse
 Alexandre Braga
 Luigi Catuogno
 Rongmao Chen
 Michele Ciampi
 Guo Chun
 Mario Cornejo
 Joan Daemen
 Christophe Doche
 Kaoutar Elkhiyaoui
 Keita Emura
 Martianus
 Frederic Ezerman
 Nils Fleischhacker
 Atsushi Fujioka
 Yuichi Futa
 Marios Georgiou
 Esha Ghosh
 Rishab Goyal
 Le Guan
 Xue Haiyang
 Jin Han
 Wenhui Hu

Yupeng Jiang
 Süleyman Kardaş
 Aniket Kate
 Akinori Kawachi
 Anselme Kemgne Tueno
 Mathias Kohler
 Anna Krasnova
 Ashutosh Kumar
 Jianchang Lai
 Russell W.F. Lai
 Obbattu Sai
 Lakshmi Bhavana
 Hyung Tae Lee
 Iraklis Leontiadis
 Hemi Leibowitz
 Bin Liu
 Meicheng Liu
 Naiwei Liu
 Yunwen Liu
 Zhen Liu
 Jose M. Lopez
 Isis Lovecruft
 Atul Luykx
 Chang Lv
 Jack P.K. Ma
 Mohammad Mamun
 Pedro Maat Massolino
 Peihan Miao
 Christoph Michel
 Shigeo Mitsunari
 Eduardo Morais
 Toru Nakanishi
 Luiz Navarro
 Ajaya Neupane
 Khoa Nguyen
 Hod Bin Noon
 Maciej Obremski
 Kazumasa Omote
 Adam O'Neill
 Melek Önen
 Stjepan Picek

Fabio Piva
 Elizabeth Quaglia
 Srinivasan Raghuraman
 Manuel Reinert
 Oscar Reparaz
 Vincent Rijmen
 Ruben Rios
 Adeline Roux-Langlois
 Vipin Singh Sehrawat
 Sruthi Sekar
 Babins Shrestha
 Maliheh Shirvanian
 Roe Shlomo
 Prakash Shrestha
 Luisa Siniscalchi
 William Skeith
 Maciej Skórski
 Akshayaram Srinivasan
 Raymond K.H. Tai
 Sri Aravinda
 Krishnan Thyagarajan
 Chenyang Tu
 Miguel Urquidi
 Cédric Van Rompay
 Dimitrios Vasilopoulos
 Gabriele Vigliani
 Xiao Wang
 Xiuhua Wang
 Yongge Wang
 Harry W.H. Wong
 Brecht Wyseur
 Tran Phuong Viet Xuan
 Bohan Yang
 Eunjung Yoon
 Libo Zhang
 Miaomiao Zhang
 Shiwei Zhang
 Tao Zhang
 Yongjun Zhao
 Jingyuan Zhao
 Jincheng Zhuang

Contents

Cryptanalysis of Symmetric Key

Linear Regression Attack with F-test: A New SCARE Technique for Secret Block Ciphers	3
<i>Si Gao, Hua Chen, Wenling Wu, Limin Fan, Jingyi Feng, and Xiangliang Ma</i>	
Compact Representation for Division Property	19
<i>Yosuke Todo and Masakatu Morii</i>	
An Automatic Cryptanalysis of Transposition Ciphers Using Compression . . .	36
<i>Noor R. Al-Kazaz, Sean A. Irvine, and William J. Teahan</i>	

SideChannel Attacks and Implementation

Side-Channel Attacks on Threshold Implementations Using a Glitch Algebra	55
<i>Serge Vaudenay</i>	
Diversity Within the Rijndael Design Principles for Resistance to Differential Power Analysis	71
<i>Merrielle Spain and Mayank Varia</i>	
NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM	88
<i>Brian Koziel, Amir Jalali, Reza Azarderakhsh, David Jao, and Mehran Mozaffari-Kermani</i>	

Lattice-Based Cryptography

Server-Aided Revocable Identity-Based Encryption from Lattices	107
<i>Khoa Nguyen, Huaxiong Wang, and Juanyang Zhang</i>	
Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography	124
<i>Patrick Longa and Michael Naehrig</i>	
An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins	140
<i>Rachid El Bansarkhani and Jan Sturm</i>	

Virtual Private Network

Breaking PPTP VPNs via RADIUS Encryption 159
Matthias Horst, Martin Grothe, Tibor Jager, and Jörg Schwenk

LEAP: A Next-Generation Client VPN and Encrypted Email Provider. 176
Elijah Sparrow, Harry Halpin, Kali Kaneko, and Ruben Pollan

Implementation State of HSTS and HPKP in Both Browsers and Servers. 192
Sergio de los Santos, Carmen Torrano, Yaiza Rubio, and Félix Brezo

Signatures and Hash

Signer-Anonymous Designated-Verifier Redactable Signatures
for Cloud-Based Data Sharing 211
David Derler, Stephan Krenn, and Daniel Slamanig

Group Signature with Deniability: How to Disavow a Signature 228
*Ai Ishida, Keita Emura, Goichiro Hanaoka, Yusuke Sakai,
and Keisuke Tanaka*

Sandwich Construction for Keyed Sponges: Independence Between
Capacity and Online Queries 245
Yusuke Naito

MultiParty Computation

Secure Error-Tolerant Graph Matching Protocols. 265
Kalikinkar Mandal, Basel Alomair, and Radha Poovendran

Efficient Verifiable Computation of XOR for Biometric Authentication 284
*Aysajan Abidin, Abdelrahaman Aly, Enrique Argones Rúa,
and Aikaterini Mitrokotsa*

Verifiable Message-Locked Encryption 299
Sébastien Canard, Fabien Laguillaumie, and Marie Paindavoine

Symmetric Cryptography and Authentication

Security of Online AE Schemes in RUP Setting 319
Jian Zhang and Wenling Wu

An Efficient Entity Authentication Protocol with Enhanced Security
and Privacy Properties 335
Aysajan Abidin, Enrique Argones Rúa, and Bart Preneel

Probabilistic Generation of Trapdoors: Reducing Information Leakage of Searchable Symmetric Encryption 350
Kenichiro Hayasaka, Yutaka Kawai, Yoshihiro Koseki, Takato Hirano, Kazuo Ohta, and Mitsugu Iwamoto

System Security

AAL and Static Conflict Detection in Policy 367
Jean-Claude Royer and Anderson Santana De Oliveira

Component-Oriented Access Control for Deployment of Application Services in Containerized Environments. 383
Kirill Belyaev and Indrakshi Ray

Generic Access Control System for Ad Hoc MCC and Fog Computing 400
Bilel Zaghdoudi, Hella Kaffel-Ben Ayed, and Wafa Harizi

Functional and Homomorphic Encryption

SecReach: Secure Reachability Computation on Encrypted Location Check-in Data 419
Hanyu Quan, Boyang Wang, Iraklis Leontiadis, Ming Li, and Yuqing Zhang

FHE Over the Integers and Modular Arithmetic Circuits 435
Eunkyung Kim and Mehdi Tibouchi

An Efficient Somewhat Homomorphic Encryption Scheme Based on Factorization 451
Gérald Gavin

Information Theoretic Security

Efficient, XOR-Based, Ideal (t, n) -threshold Schemes. 467
Liqun Chen, Thalia M. Laing, and Keith M. Martin

Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards. 484
Takaaki Mizuki

Efficient Card-Based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations 500
Takeshi Nakai, Yuuki Tokushige, Yuto Misawa, Mitsugu Iwamoto, and Kazuo Ohta

Malware and Attacks

Evaluation on Malware Classification by Session Sequence of Common Protocols	521
<i>Shohei Hiruta, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, Takeshi Yagi, and Mitsuaki Akiyama</i>	
An Efficient Approach to Detect TorrentLocker Ransomware in Computer Systems.	532
<i>Faustin Mbol, Jean-Marc Robert, and Alireza Sadighian</i>	
Detecting Malware Through Anti-analysis Signals - A Preliminary Study. . . .	542
<i>Joash W.J. Tan and Roland H.C. Yap</i>	
Attackers in Wireless Sensor Networks Will Be Neither Random Nor Jumping – Secrecy Amplification Case	552
<i>Radim Ošádal, Petr Švenda, and Vashek Matyáš</i>	
Improved Attacks on Extended Generalized Feistel Networks	562
<i>Valérie Nachez, Nicolas Marrière, and Emmanuel Volte</i>	
When Constant-Time Source Yields Variable-Time Binary: Exploiting Curve25519-donna Built with MSVC 2015.	573
<i>Thierry Kaufmann, Hervé Pelletier, Serge Vaudenay, and Karine Villegas</i>	

MultiParty Computation and Functional Encryption

On the Power of Public-key Function-Private Functional Encryption	585
<i>Vincenzo Iovino, Qiang Tang, and Karol Żebrowski</i>	
A New Technique for Compacting Secret Key in Attribute-Based Broadcast Encryption.	594
<i>Sébastien Canard, Duong Hieu Phan, and Viet Cuong Trinh</i>	
An Efficient Construction of Non-Interactive Secure Multiparty Computation.	604
<i>Satoshi Obana and Maki Yoshida</i>	
An MPC-Based Privacy-Preserving Protocol for a Local Electricity Trading Market.	615
<i>Aysajan Abidin, Abdelrahman Aly, Sara Cleemput, and Mustafa A. Mustafa</i>	
Implementation of Verified Set Operation Protocols Based on Bilinear Accumulators.	626
<i>Luca Ferretti, Michele Colajanni, and Mirco Marchetti</i>	

Multi-core FPGA Implementation of ECC with Homogeneous Co-Z
Coordinate Representation 637
*Bo-Yuan Peng, Yuan-Che Hsu, Yu-Jia Chen, Di-Chia Chueh,
Chen-Mou Cheng, and Bo-Yin Yang*

Network Security, Privacy, and Authentication

DNSSEC Misconfigurations in Popular Domains 651
Tianxiang Dai, Haya Shulman, and Michael Waidner

Integral Privacy 661
Vicenç Torra and Guillermo Navarro-Arribas

Sharing Is Caring, or Callous? 670
Yu Pu and Jens Grossklags

Improving the Sphinx Mix Network 681
Filipe Beato, Kimmo Halunen, and Bart Mennink

User Authentication from Mouse Movement Data Using SVM Classifier 692
*Bashira Aker Anima, Mahmood Jasim, Khandaker Abir Rahman,
Adam Rulapaugh, and Md Hasanuzzaman*

Distance Bounding Based on PUF. 701
Mathilde Igier and Serge Vaudenay

Posters

Denying Your Whereabouts: A Secure and Deniable Scheme
for Location-Based Services 713
Tassos Dimitriou and Naser Al-Ibrahim

Range Query Integrity in Cloud Data Streams with Efficient Insertion 719
*Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo,
and Antonino Nocera*

Vulnerability Analysis Using Google and Shodan 725
Kai Simon

Language-Based Hypervisors 731
Enrico Budianto, Richard Chow, Jonathan Ding, and Michael McCool

Internet Censorship in Italy: A First Look at 3G/4G Networks 737
Giuseppe Aceto, Antonio Montieri, and Antonio Pescapè

A Privacy-Preserving Model for Biometric Fusion. 743
Christina-Angeliki Toli, Abdelrahman Aly, and Bart Preneel

Hybrid WBC: Secure and Efficient White-Box Encryption Schemes 749
*Jihoon Cho, Kyu Young Choi, Orr Dunkelman, Nathan Keller,
Dukjae Moon, and Aviya Vaidberg*

Moving in Next Door: Network Flooding as a Side Channel
in Cloud Environments 755
*Yatharth Agarwal, Vishnu Murale, Jason Hennessey, Kyle Hogan,
and Mayank Varia*

Author Index 761