

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

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

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

Josef Pieprzyk Ahmad-Reza Sadeghi
Mark Manulis (Eds.)

Cryptology and Network Security

11th International Conference, CANS 2012
Darmstadt, Germany, December 12-14, 2012
Proceedings



Springer

Volume Editors

Josef Pieprzyk
Macquarie University
Department of Computing
Sydney, NSW 2109, Australia
E-mail: josef.pieprzyk@mq.edu.au

Ahmad-Reza Sadeghi
Technische Universität Darmstadt
System Security Lab.
64293 Darmstadt, Germany
E-mail: ahmad.sadeghi@trust.cased.de

Mark Manulis
University of Surrey
Department of Computing
Guildford, GU2 7XH, UK
E-mail: m.manulis@surrey.ac.uk

ISSN 0302-9743
ISBN 978-3-642-35403-8
DOI 10.1007/978-3-642-35404-5
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-35404-5

Library of Congress Control Number: 2012953024

CR Subject Classification (1998): E.3, C.2, K.6.5, D.4.6, G.2.1, E.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

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

CANS 2012 was held at the Darmstadtium Congress Center in Darmstadt, Germany, during December 12–14, 2012. The conference was organized in cooperation with the International Association for Cryptologic Research (IACR).

The history of CANS started in 2001, when the first edition of the conference was organized in Taipei, followed by San Francisco (2002), Miami (2003), Xiamen (2005), Suzhou (2006), Singapore (2007), Hong Kong (2008), Kanazawa (2009), Kuala Lumpur (2010), and Sanya (2011). CANS 2012 was the 11th event in this series and it was the first time that the conference came to Europe.

Since 2005, CANS proceedings have been published by Springer in their Lecture Notes in Computer Science (LNCS) series. We thank Alfred Hofmann from Springer for his support in the publication of the CANS 2012 proceedings.

CANS 2012 received 99 submissions of which the Program Committee chose 22 papers to be included in the conference program. Each submitted paper got assigned to three reviewers. However, papers submitted by Program Committee members were reviewed by five referees. The double-blind review process consisted of two stages. In the first stage, papers were evaluated by reviewers and their comments very submitted to the EasyChair server. In the second stage, the papers were scrutinized in extensive anonymous discussions among the committee members. Some papers received up to 21 discussion comments. We hope that all good submissions that did not make it into the program of CANS 2012 will eventually be accepted elsewhere and that the papers that got accepted to the conference are interesting to the readers.

Special words of appreciation go to Nicolas Courtois, Sherman Chow, and Vincent Rijmen, who kindly agreed to shepherd three papers that were accepted to the conference. The authors of the accepted papers had two weeks for revision and preparation of final versions. The revised papers were not subject to editorial review and the authors bear full responsibility for their contents. The submission and review process was supported by EasyChair and we thank the EasyChair team for letting us use their server.

The paper “*A Simple Key-Recovery Attack on McOE-X*” by Florian Mendel, Bart Mennink, Vincent Rijmen and Elmar Tischhauser won the best paper award.

CANS 2012 also featured two invited talks

- “*Confined Guessing: Practical Signatures from Standard Assumptions*” by Dennis Hofheinz, Karlsruhe Institute of Technology, Germany.
- “*Cryptographic Failures and Successes*” by Bart Preneel, Katholieke Universiteit Leuven, Belgium.

There are many people who contributed to the success of CANS 2012. First, we would like to thank the authors of all papers (both accepted and rejected) for submitting their results to the conference. A special thanks goes to the members

of the Program Committee and the external referees who gave their time, expertise, and enthusiasm in order to ensure that each paper received a thorough and fair review. Last but not least, we thank Stanislav Bulygin, Heike Meissner, and Anette Mittenhuber for their support in the organization of the conference.

December 2012

Josef Pieprzyk
Ahmad-Reza Sadeghi
Mark Manulis

CANS 2012

The 11th Cryptology and Network Security Conference
Darmstadt, Germany
December 12–14, 2012

General Chair

Mark Manulis

University of Surrey, UK

Program Chair

Josef Pieprzyk

Ahmad-Reza Sadegh

Macquarie University, Australia

Technische Universität Darmstadt / Fraunhofer
SIT, Germany

Program Committee

Michel Abdalla

Gildas Avoine

Feng Bao

Sébastien Canard

Sherman Chow

ENS, France

Université Catholique de Louvain, Belgium

Institute for Infocomm Research, Singapore

Orange Labs, France

University of Waterloo, Canada and

Chinese University of Hong Kong,
Hong Kong

Nicolas Courtois

Emiliano De Cristofaro

Reza Curtmola

George Danezis

Roberto Di Pietro

Juan Garay

Philip Hawkes

Amir Herzberg

Nick Hopper

Stanisław Jarecki

Xuxian Jiang

Seny Kamara

Angelos Keromytis

Svein Johan Knapskog

Benôit Libert

Atsuko Miyaji

Refik Molva

Fabian Monrose

University College London, UK

PARC Research, USA

New Jersey Institute of Technology, USA

Microsoft Research Cambridge, UK

Università di Roma Tre, Italy

AT&T Labs Research, USA

Qualcomm, Australia

Bar-Ilan University, Israel

University of Minnesota, USA

University of California, Irvine, USA

North Carolina State University, USA

Microsoft Research, USA

Columbia University, USA

NTNU Trondheim, Norway

Université Catholique de Louvain, Belgium

JAIST, Japan

Eurecom, France

University of North Carolina, USA

David Naccache	Ecole Normale Superieure, France
Michael Naehrig	Microsoft Research Redmond, USA
Eiji Okamoto	University of Tsubuka, Japan
Claudio Orlandi	Aarhus University, Denmark
Jacques Patarin	Université de Versailles, France
Raphael C.-W. Phan	Loughborough University, UK
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Vincent Rijmen	TU Graz, Austria
Matt Robshaw	Orange Labs, France
Rei Safavi-Naini	University of Calgary, Canada
Thomas Schneider	TU Darmstadt, Germany
Elaine Shi (Rungting)	UC Berkeley, USA
Francois-Xavier Standaert	Université Catholique de Louvain, Belgium
Douglas Stebila	Queensland University of Technology, Australia
Ron Steinfeld	Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Markus Ullmann	Federal Office for Information Security (BSI), Germany
Ersin Uzun	PARC Research, USA
Frederik Vercauteren	Katholieke Universiteit Leuven, Belgium
Huaxiong Wang	Nanyang Technological University, Singapore
Michael J. Wiener	Irdeco, Canada
Xinwen Zhang	Huawei Research Center, USA

Steering Committee

Yvo Desmedt (Chair)	University College London, UK
Matt Franklin	University of California, Davis, USA
Juan A. Garay	AT&T Labs - Research, USA
Yi Mu	University of Wollongong, Australia
David Pointcheval	CNRS and ENS Paris, France
Huaxiong Wang	Nanyang Technological University, Singapore

External Reviewers

Akishita, Toru	Chen, Jiageng
Athanasopoulos, Elias	Chen, Jie
Aumasson, Jean-Philippe	Chu, Cheng-Kang
Beaujeant, Antonin	Collard, Baudoin
Bogdanov, Andrey	Costello, Craig
Bos, Joppe	Cuvelier, Edouard
Bouillaguet, Charles	Devigne, Julien
Cai, Shaoying	Elkhiyaoui, Kaoutar
Chase, Melissa	Escott, Adrian
Chatterjee, Sanjit	Gasti, Paolo

Gérard, Benoît
Gouget, Aline
Hermans, Jens
Hsiao, Hsu-Chun
Huang, Yan
Hubacek, Pavel
Isshiki, Toshiyuki
Jee, Kangkook
Jhawar, Mahavir
Joux, Antoine
Kemerlis, Vasileios P.
Khoo, Khoongming
Kolesnikov, Vladimir
Kontaxis, Georgios
Kügler, Dennis
Lampe, Rodolphe
Le, Hoi
Leontiadis, Iraklis
Lin, Changlu
Liu, Lei
Loftus, Jake
Lu, Jiqiang
Lyubashevsky, Vadim
Malozemoff, Alex
Martin, Benjamin
Mendel, Florian
Mennink, Bart
Mittal, Prateek
Mohaisen, Abedelaziz
Nachef, Valerie
Nikova, Svetla
Nithyanand, Rishab
Norcie, Gregory
Olivier, Pereira
Omote, Kazumasa
Önen, Melek
Pappas, Vasilis
Peters, Thomas
Petit, Christophe
Plaga, Rainer
Polychronakis, Michalis
Portokalidis, Georgios
Quaglia, Elizabeth
Rasmussen, Kasper Bonne
Regazzoni, Francesco
Reparaz, Oscar
Riva, Ben
Sadeghian, Saeed
Sarkar, Sumanta
Sarr, Augustin
Schwabe, Peter
Seyalioglu, Hakan
Shao, Jun
Stehlé, Damien
Tan, Syh-Yuan
Tartary, Christophe
Thoma, Achint
Traoré, Jacques
Trujillo-Rasua, Rolando
Tselekounis, Yiannis
Tuhin, Ashraful
Varıcı, Kerem
Vergnaud, Damien
Volte, Emmanuel
Wang, Pengwei
Wieschebrink, Christian
Yang, Guomin
Zhang, Haibin
Zhang, Tongjie
Zhang, Xin
Zhang, Yun
Zheng, Qingji
Zohner, Michael

Invited Talks

Confined Guessing: Practical Signatures from Standard Assumptions

Dennis Hofheinz

Karlsruhe Institute of Technology
email: Dennis.Hofheinz@kit.edu

Abstract. In the first part of the talk, we survey existing paradigms to construct digital signature schemes. We highlight the surprising difficulty to build practical schemes. Namely, from a theoretic point of view, digital signatures are equivalent to one-way functions, which in turn appear to be a weaker primitive than public-key encryption (PKE). However, while we know how to construct practical PKE schemes from standard complexity assumptions, it seems much harder to construct practical signature schemes.

In the second part of the talk, we put forward a new technique to construct very efficient and compact signature schemes. Our technique combines several instances of an only mildly secure signature scheme to obtain a fully secure scheme. Since the mild security notion we require is much easier to achieve than full security, we can combine our strategy with existing techniques to obtain a number of interesting new (and fully secure) signature schemes. Concretely, we obtain efficient and compact new signature schemes from the Computational Diffie-Hellman, RSA, and Short Integer Solutions assumptions. Each of the arising schemes provides significant improvements upon state-of-the-art schemes.

Cryptographic Failures and Successes

Bart Preneel

Katholieke Universiteit Leuven, ESAT/COSIC
Kasteelpark Arenberg 10 Bus 2446, B-3001 Leuven, Belgium
email: bart.preneel@esat.kuleuven.be

Abstract. This talk discusses a broad range of applications of cryptography and tries to make the balance of the achievements. Topics that will be covered include credit card payments (EMV), e-commerce (SSL/TLS and PKI), mobile communications (GSM and 3G) and identification technologies (eID and e-passport). We will also evaluate how cryptography can lead to new architectures, that result in distributed solutions for privacy-friendly metering, that have applications in insurance pricing, road pricing and smart electricity grids.

Table of Contents

Cryptanalysis

Conditional Differential Cryptanalysis of Grain-128a	1
<i>Michael Lehmann and Willi Meier</i>	
A Real-Time Key Recovery Attack on the Lightweight Stream Cipher A2U2	12
<i>Zhenqing Shi, Xiutao Feng, Dengguo Feng, and Chuankun Wu</i>	
A Simple Key-Recovery Attack on McOE-X	23
<i>Florian Mendel, Bart Mennink, Vincent Rijmen, and Elmar Tischhauser</i>	
Cryptanalysis of a Lattice-Knapsack Mixed Public Key Cryptosystem	32
<i>Jun Xu, Lei Hu, Siwei Sun, and Ping Wang</i>	
Biclique Cryptanalysis of TWINE	43
<i>Mustafa Çoban, Ferhat Karakoç, and Özkan Boztaş</i>	
Differential and Linear Attacks on the Full WIDEA- n Block Ciphers (Under Weak Keys)	56
<i>Jorge Nakahara Jr.</i>	
Improved Linear Analysis on Block Cipher MULTI2	72
<i>Yi Lu, Liping Ding, and Yongji Wang</i>	
Fixed Points of Special Type and Cryptanalysis of Full GOST	86
<i>Orhun Kara and Ferhat Karakoç</i>	

Network Security

Attacking Animated CAPTCHAs via Character Extraction	98
<i>Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo</i>	
Analysis of Rogue Anti-Virus Campaigns Using Hidden Structures in k -Partite Graphs	114
<i>Orestis Tsigkas and Dimitrios Tzovaras</i>	
Mobile Evil Twin Malnets – The Worst of Both Worlds	126
<i>Christian Szongott, Benjamin Henne, and Matthew Smith</i>	
Firm Grip Handshakes: A Tool for Bidirectional Vouching	142
<i>Omer Berkman, Benny Pinkas, and Moti Yung</i>	

Cryptographic Protocols

Group Key Establishment: Adding Perfect Forward Secrecy at the Cost of One Round	158
<i>Kashi Neupane, Rainer Steinwandt, and Adriana Suárez Corona</i>	
Applicability of OR-Proof Techniques to Hierarchical Identity-Based Identification	169
<i>Atsushi Fujioka, Taiichi Saito, and Keita Xagawa</i>	
LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks	185
<i>Bogdan Groza, Stefan Murvay, Anthony van Herrewege, and Ingrid Verbauwhede</i>	
Efficient Verification of Input Consistency in Server-Assisted Secure Function Evaluation	201
<i>Vladimir Kolesnikov, Ranjit Kumaresan, and Abdullatif Shikfa</i>	
Fast and Private Computation of Cardinality of Set Intersection and Union	218
<i>Emiliano De Cristofaro, Paolo Gasti, and Gene Tsudik</i>	

Encryption

Fast and Secure Root Finding for Code-Based Cryptosystems	232
<i>Falko Strenzke</i>	
Strong Privacy for RFID Systems from Plaintext-Aware Encryption	247
<i>Khaled Ouafi and Serge Vaudenay</i>	
How to Enhance the Security on the Least Significant Bit	263
<i>Atsuko Miyaji and Yiren Mo</i>	

S-Box Theory

Improvement in Non-linearity of Carlet-Feng Infinite Class of Boolean Functions	280
<i>Mansoor Ahmed Khan and Ferruh Özbudak</i>	
Some Representations of the S-Box of Camellia in $GF(((2^2)^2)^2)$	296
<i>Alberto F. Martínez-Herrera, J. Carlos Mex-Perera, and Juan A. Nolasco-Flores</i>	

Author Index	311
-------------------------------	-----