Lecture Notes in Computer Science 7712

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

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 e-ISSN 1611-3349
ISBN 978-3-642-35403-8 e-ISBN 978-3-642-35404-5
DOI 10.1007/978-3-642-35404-5
Springer Heidelberg Dordrecht London New York

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

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	Macquarie University, Australia
Ahmad-Reza Sadegh	Technische Universität Darmstadt / Fraunhofer SIT, Germany

Program Committee

Michel Abdalla	ENS, France
Gildas Avoine	Université Catholique de Louvain, Belgium
Feng Bao	Institute for Infocomm Research, Singapore
Sébastien Canard	Orange Labs, France
Sherman Chow	University of Waterloo, Canada and Chinese University of Hong Kong, Hong Kong
Nicolas Courtois	University College London, UK
Emiliano De Cristofaro	PARC Research, USA
Reza Curtmola	New Jersey Institute of Technology, USA
George Danezis	Microsoft Research Cambridge, UK
Roberto Di Pietro	Università di Roma Tre, Italy
Juan Garay	AT&T Labs Research, USA
Philip Hawkes	Qualcomm, Australia
Amir Herzberg	Bar-Ilan University, Israel
Nick Hopper	University of Minnesota, USA
Stanisław Jarecki	University of California, Irvine, USA
Xuxian Jiang	North Carolina State University, USA
Seny Kamara	Microsoft Research, USA
Angelos Keromytis	Columbia University, USA
Svein Johan Knapskog	NTNU Trondheim, Norway
Benoît Libert	Université Catholique de Louvain, Belgium
Atsuko Miyaji	JAIST, Japan
Refik Molva	Eurecom, France
Fabian Monrose	University of North Carolina, USA

Steering Committee

External Reviewers

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

Network Security

Cryptographic Protocols

Encryption

S-Box Theory