Preface

It was a real pleasure to have taken part in organizing the 10th International Conference on Cryptography and Network Security (CANS 2011). It was held during December 10–12, 2011, at the International Asia Pacific Convention Center in Sanya, on the subtropical island of Hainan (China). CANS 2011 was sponsored by the National Natural Science Foundation of China (NSFC) and Shandong University (SDU). It was also held in cooperation with the International Association for Cryptologic Research (IACR).

The CANS 2011 Program Committee (PC) consisted of 46 internationally recognized researchers with combined expertise covering the entire scope of the conference.

The recent growth in the number of cryptography venues prompted stiff competition for high-quality papers. Nonetheless, CANS has consistently attracted a number of strong submissions. This year, we received a total of 65 submissions. A few were incomplete and/or were rejected without review. Each remaining paper was reviewed by at least four reviewers. After intensive deliberations by the Program Committee, 18 submissions were accepted for presentation.

In addition to regular papers, the conference program included four excellent invited talks, by Colin Boyd (QUT), Xavier Boyen (PARC), Phong Nguyen (ENS) and Joan Daemen (STMicroelectronics).

A number of people selflessly contributed to the success of CANS 2011. First and foremost, we thank the authors of all submissions. They are the backbone of this conference and their confidence and support are highly appreciated. We are similarly grateful to the dedicated, knowledgeable and hard-working Program Committee members who provided excellent and timely reviews as well as took part in post-review discussions. Their altruistic dedication and community service spirit are commendable. Special thanks to “shepherds” for their extra efforts.

We gratefully acknowledge the organizational contributions by CANS 2011 General Chair, Dongdai Lin, without whom the conference would have been impossible. We wish to thank Meiqin Wang as well as all the members of Organizing Committee for the local arrangements, and Claudio Soriente for publicity. We are also indebted to the CANS Steering Committee members for their guidance. Last, but not least, we thank CANS 2011 sponsors: NSFC and SDU.

December 2011

Gene Tsudik
Xiaoyun Wang
Program Co-chairs
CANS 2011

The 10th International Conference on Cryptography and Network Security
(In Cooperation with IACR)

Sanya, China
December 10–12, 2011

Sponsored and organized by
Shandong University
and
National Natural Science Foundation of China

Steering Committee

Yvo Desmedt University College London, UK
Matt Franklin University of California, Davis, USA
Juan Garay AT&T Labs - Research, USA
Yi Mu University of Wollongong, Australia
David Pointcheval CNRS and ENS, France
Huaxiong Wang NTU, Singapore

General Chair

Dongdai Lin SKLOIS, Chinese Academy of Sciences, China

Program Co-chairs

Gene Tsudik University of California, Irvine, USA
Xiaoyun Wang Shandong University, China

Program Committee

Jean-Philippe Aumasson Nagravision, Switzerland
Feng Bao I2R, Singapore
Jean-Luc Beuchat University of Tsukuba, Japan
Mike Burmester Florida State University, USA
Sherman S.M. Chow University of Waterloo, Canada
Giovanni Di Crescenzo Telcordia, USA
Emiliano De Cristofaro University of California, Irvine, USA
Reza Curtmola NJIT, USA
Xuhua Ding  
SMU, Singapore

David Galindo  
University of Luxembourg, Luxembourg

Amir Herzberg  
Bar-Ilan University, Israel

Nick Hopper  
University of Minnesota, USA

Tetsu Iwata  
Nagoya University, Japan

Charanjit Jutla  
IBM Research, USA

Khoongming Khoo  
DSO National Laboratories, Singapore

Loukas Lazos  
University of Arizona, USA

Gaëtan Leurent  
University of Luxembourg, Luxembourg

Helger Lipmaa  
Cybernetica AS and Tallinn University, Estonia

Feifei Li  
Florida State University, USA

Di Ma  
University of Michigan, USA

Mark Manulis  
TU Darmstadt, Germany

Florian Mendel  
Graz University of Technology, Austria

Atsuko Miyaji  
JAIST, Japan

Jorge Nakahara Jr.  
Independent Researcher

Melek Önen  
EURECOM, France

Bryan Parno  
Microsoft Research, USA

Andreas Pashalidis  
KU Leuven, Belgium

Thomas Peyrin  
NTU, Singapore

Raphael C.-W. Phan  
Loughborough University, UK

Josef Pieprzyk  
Macquarie University, Australia

Rei Safavi-Naini  
University of Calgary, Canada

Yu Sasaki  
NTT Research, Japan

Martin Schläffer  
Graz University of Technology, Austria

Michael Scott  
Dublin City University, Ireland

Elaine Shi  
Berkeley / PARC, USA

Claudio Soriente  
Universidad Politecnica de Madrid, Spain

Damien Stehlé  
CNRS and ENS de Lyon, France

Ron Steinfeld  
Macquarie University, Australia

Søren Steffensen Thomsen  
Technical University of Denmark, Denmark

Ersin Uzun  
PARC, USA

Ivan Visconti  
University of Salerno, Italy / UCLA, USA

Huaxiong Wang  
NTU, Singapore

Meiqin Wang  
Shandong University, China

Wenling Wu  
Institute of Software, CAS, China

Shouhuai Xu  
University of Texas, San Antonio, USA

Jianying Zhou  
I2R, Singapore

Local Arrangements Chair

Meiqin Wang  
Shandong University, China
Local Organizing Committee

Hongbo Yu  Tsinghua University, China
Keting Jia  Tsinghua University, China
Puwen Wei  Shandong University, China
Lidong Han  Tsinghua University, China

Publicity Chair

Claudio Soriente  Polytechnic University of Madrid, Spain

Secretary and Treasurer

Puwen Wei  Shandong University, China

WEB/Registration

Jiazhe Chen  Shandong University, China

External Reviewers

Filipe Beato  Choy Jia Li Valerie  Yasuhide Sakai
Xavier Boyen  Markulf Kohlweiss  Alessandra Scafuro
Aldar C-F. Chan  Simon Kramer  Jun Shao
Kai-Yuen Cheong  Mario Lamberger  Haya Shulman
Kim-Kwang Raymond Choo  Gregor Leander  Ashraful Tuhin
Cheng-Kang Chu  Zi Lin  Frederik Vercauteren
Yi Deng  Weiliang Luo  Cong Wang
Orr Dunkelman  Avradip Mandal  Wei Wu
Nicolas Estibals  Tomislav Nad  Brecht Wyseur
Kazuhide Fukushima  Kris Narayan  Huihui Yap
David Gardner  Maria Naya-Plasencia  Shucheng Yu
Paolo Gasti  Lan Nguyen  Tsz Hon Yuen
Pierrick Gaudry  Ryo Nojima  Kai Zeng
Zahra Aghazadeh Gaven Watson  Wakaha Ogata  Lei Zhang
Moti Geva  Kazumasa Omote  Liangfeng Zhang
Jian Guo  Andreas Peter  Xin Zhang
Francis Hsu  Natasha Portier  Yun Zhang
Xinyi Huang  Axel Poschmann  Qingji Zheng
Francisco Rodriguez-Henrquez
Table of Contents

Invited Talks
Expressive Encryption Systems from Lattices ................................. 1
  Xavier Boyen

Breaking Fully-Homomorphic-Encryption Challenges (Abstract) .......... 13
  Phong Q. Nguyen

Symmetric Cryptanalysis
Cube Cryptanalysis of Hitag2 Stream Cipher ................................. 15
  Siwei Sun, Lei Hu, Yonghong Xie, and Xiangyong Zeng

New Impossible Differential Cryptanalysis of Reduced-Round Camellia ................................................................. 26
  Leibo Li, Jiazhe Chen, and Keting Jia

The Initialization Stage Analysis of ZUC v1.5 ............................... 40
  Chunfang Zhou, Xiutao Feng, and Dongdai Lin

Algebraic Cryptanalysis of the Round-Reduced and Side Channel Analysis of the Full PRINTCipher-48 ................................. 54
  Stanislav Bulygin and Johannes Buchmann

Symmetric Ciphers
EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption ................................................................. 76
  Huihui Yap, Khoongming Khoo, Axel Poschmann, and Matt Henricksen

On Permutation Layer of Type 1, Source-Heavy, and Target-Heavy Generalized Feistel Structures ............................................. 98
  Shingo Yanagihara and Tetsu Iwata

Public Key Cryptography
Security Analysis of an Improved MFE Public Key Cryptosystem ........ 118
  Xuyun Nie, Zhaohu Xu, Li Lu, and Yongjian Liao

A New Lattice-Based Public-Key Cryptosystem Mixed with a Knapsack ............................................................................ 126
  Yanbin Pan, Yingpu Deng, Yupeng Jiang, and Ziran Tu
Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption

138

Tatsuaki Okamoto and Katsuyuki Takashima

Protocol Attacks

Comments on the SM2 Key Exchange Protocol

160

Jing Xu and Dengguo Feng

Cryptanalysis of a Provably Secure Cross-Realm Client-to-Client Password-Authenticated Key Agreement Protocol of CANS ’09

172

Wei-Chuen Yau, Raphael C.-W. Phan, Bok-Min Goi, and Swee-Huay Heng

Passive Attack on RFID LMAP++ Authentication Protocol

185

Shao-hui Wang and Wei-wei Zhang

Privacy Techniques

Multi-show Anonymous Credentials with Encrypted Attributes in the Standard Model

194

Sébastien Canard, Roch Lescuyer, and Jacques Traoré

Group Signature with Constant Revocation Costs for Signers and Verifiers

214

Chun-I Fan, Ruei-Hau Hsu, and Mark Manulis

Fast Computation on Encrypted Polynomials and Applications

234

Payman Mohassel

Varia

AniCAP: An Animated 3D CAPTCHA Scheme Based on Motion Parallax

255

Yang-Wai Chow and Willy Susilo

Towards Attribute Revocation in Key-Policy Attribute Based Encryption

272

Pengpian Wang, Dengguo Feng, and Liwu Zhang

A Note on (Im)Possibilities of Obfuscating Programs of Zero-Knowledge Proofs of Knowledge

292

Ning Ding and Dawu Gu

Author Index

313