Lecture Notes in Computer Science

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
The 9th International Conference on Cryptology and Network Security (CANS 2010) was held in Kuala Lumpur, Malaysia during December 12–14, 2010. The conference was co-organized by the Multimedia University (MMU), Malaysia, and Universiti Tunku Abdul Rahman (UTAR), Malaysia.

The conference received 64 submissions from 22 countries, out of which 21 were accepted after a careful and thorough review process. These proceedings also contain abstracts for two invited talks. All submissions were reviewed by at least three members of the Program Committee; those authored or co-authored by Program Committee members were reviewed by at least five reviewers. Program Committee members were allowed to use external reviewers to assist with their reviews, but remained responsible for the contents of the review and representing papers during the discussion and decision making. The review phase was followed by a 10-day discussion phase in which each paper with at least one supporting review was discussed, additional experts were consulted where needed, and final decisions were made.

We thank the Program Committee for their hard work in selecting the program. We also thank the external reviewers who assisted with reviewing and the CANS Steering Committee for their help. We thank Shai Halevi for use of his Web-Submission-and-Review software that was used for the electronic submission and review of the submitted papers, and we thank the International Association for Cryptologic Research (IACR) for Web hosting of the software.

The main goal of the conference is to promote research on all aspects of network security, as well as to build a bridge between research on cryptography and network security. The current edition continues to fulfill this goal with the broad range of areas covered by the high-quality accepted papers, including both theoretical and practical analysis of cryptographic primitives and protocols; secure systems and mechanisms for networked applications such as cloud computing, electronic voting, and mobile computing; and advances in anonymous credentials and their use. In addition, the conference featured two invited speakers to present their cutting-edge research: Kaoru Kurosawa of Ibaraki University, Japan, on “Cryptography for Unconditionally Secure Message Transmission in Networks” and Ahmad-Reza Sadeghi of Technical University Darmstadt, Germany, on “Cryptography Meets Hardware: Selected Topics of Hardware-based Cryptography”; these talks contributed greatly to the conference program.
Finally, we thank the local Organizing Committee for their dedication and commitment in organizing the conference. We also thank all authors who submitted papers, whether or not they were accepted, and all conference attendees for their contribution to a lively and energetic conference.

December 2010

Swee-Huay Heng
Rebecca N. Wright
Bok-Min Goi
CANS 2010

The 9th International Conference on Cryptology and Network Security

Kuala Lumpur, Malaysia
December 12–14, 2010

Jointly organized by
Multimedia University, Malaysia
and
Universiti Tunku Abdul Rahman, Malaysia

General Chair
Bok-Min Goi  Universiti Tunku Abdul Rahman, Malaysia

Program Co-chairs
Swee-Huay Heng  Multimedia University, Malaysia
Rebecca N. Wright  Rutgers University, USA

Program Committee
Michel Abdalla  Ecole Normale Superieure, France
William Arbaugh  University of Maryland, USA
John Black  University of Colorado at Boulder, USA
Carlo Blundo  University of Salerno, Italy
Xavier Boyen  University of Liege, Belgium
Melissa Chase  Microsoft Research, USA
Sherman S.M. Chow  New York University, USA
Giovanni Di Crescenzo  Telcordia Technologies, USA
Rosario Gennaro  IBM Research, USA
Bok-Min Goi  Universiti Tunku Abdul Rahman, Malaysia
Matthew Green  Johns Hopkins University, USA
Tetsu Iwata  Nagoya University, Japan
Aaron D. Jaggard  Rutgers University, USA
Trevor Jim  AT&T Labs Research, USA
Charanjit Jutla  IBM Research, USA
Seny Kamara  Microsoft, USA
Jonathan Katz  University of Maryland, USA
Khoongming Khoo  
Aggelos Kiayias  
Kwangjo Kim  
Vladimir Kolesnikov  
Lee Kai (Joseph) Liu  
Javier Lopez  
Mark Manulis  
Adam O’Neill  
Wakaha Ogata  
Raphael C.-W. Phan  
Josef Pieprzyk  
David Pointcheval  
Georgios Portokalidis  
C. Pandu Rangan  
Rei Safavi-Naini  
Tomas Sander  
Nitesh Saxena  
William Skeith  
Jessica Staddon  
Angelos Stavrou  
Douglas Stinson  
Ivan Visconti  
Poorvi Vora  
Xiaoyun Wang  
Hoeteck Wee  
Susanne Wetzel  
Danfeng Yao  
Sung-Ming Yen

Steering Committee

Yvo Desmedt  
Matthew Franklin  
Juan A. Garay  
Yi Mu  
David Pointcheval  
Huaxiong Wang

Organizing Committee

Local Organizing Chair  
Secretariat  
Publicity  
Finance
Webmaster  Goh Kah-Ong Michael, MMU
Logistics  Tommy Tong-Yuen Chai, UTAR
Zan-Kai Chong, UTAR
Swee-Eng Khor, MMU
Priya a/p Kulampurath Govindan Nair, UTAR
Huo-Chong Ling, MMU
Syh-Yuan Tan, UTAR
Yar-Ling Tan, UTAR
Wei-Chuen Yau, MMU

External Reviewers

Shweta Agrawal  Jian Guo  Alessandra Scafuro
Hadi Ahmadi  Tzipora Halevi  Elaine Shi
Werner Backes  Islam Hegazy  Jaechul Sung
Angelo De Caro  Vincenzo Iovino  Syh-Yuan Tan
David Cash  Srinivas Krishnan  Jheng-Hong Tu
Chien-Ning Chen  Virendra Kumar  Ashraful Tuhin
Ashish Choudhary  Wei-Chih Lien  Jonathan Voris
Jiali Choy  Yasuda Masaya  Douglas Wikstrom
Cheng-Kang Chu  Marine Minier  Huihui Yap
Dario Fiore  Sai Teja Peddinti  Aileen Zhang
Pierre-Alain Fouque  Nashad Safav  Tongjie Zhang
# Table of Contents

## Block Ciphers

- Cryptanalysis of Reduced-Round MIBS Block Cipher .......................... 1  
  *Asli Bay, Jorge Nakahara Jr., and Serge Vaudenay*

- Impossible Differential Cryptanalysis of ARIA Reduced to 7 Rounds ... 20  
  *Chenghang Du and Jiaze Chen*

- An Algorithm Based Concurrent Error Detection Scheme for AES....... 31  
  *Chang N. Zhang, Qian Yu, and Xiao Wei Liu*

## Invited Talk I

- Cryptography for Unconditionally Secure Message Transmission in Networks (Abstract) ................................................................. 43  
  *Kaoru Kurosawa*

## Wireless Network Security

- Performance and Security Aspects of Client-Side SSL/TLS Processing on Mobile Devices ................................................................. 44  
  *Johann Großschädl and Ilya Kizhvatov*

- A Practical Cryptographic Denial of Service Attack against 802.11i TKIP and CCMP ................................................................. 62  
  *Martin Eian*

- User Tracking Based on Behavioral Fingerprints ............................ 76  
  * Günther Lackner, Peter Teufl, and Roman Weinberger*

## Hash Functions

- On the Collision and Preimage Resistance of Certain Two-Call Hash Functions ................................................................. 96  
  *Nasour Bagheri, Praveen Gauravaram, Majid Naderi, and Søren S. Thomsen*

- Integral Distinguishers of Some SHA-3 Candidates ......................... 106  
  *Marine Minier, Raphael C.-W. Phan, and Benjamin Pousse*

- Near-Collisions on the Reduced-Round Compression Functions of Skein and BLAKE ................................................................. 124  
  *Bozhan Su, Wenling Wu, Shuang Wu, and Le Dong*
# Public Key Cryptography

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical Algebraic Cryptanalysis for Dragon-Based Cryptosystems</td>
<td>140</td>
</tr>
<tr>
<td>Johannes Buchmann, Stanislav Bulygin, Jintai Ding, Wael Said Abd Elmageed Mohamed, and Fabian Werner</td>
<td></td>
</tr>
<tr>
<td>Generating Parameters for Algebraic Torus-Based Cryptosystems</td>
<td>156</td>
</tr>
<tr>
<td>Tomoko Yonemura, Yoshikazu Hanatani, Taichi Isogai, Kenji Ohkuma, and Hirofumi Muratani</td>
<td></td>
</tr>
<tr>
<td>Analysis of the MQQ Public Key Cryptosystem</td>
<td>169</td>
</tr>
<tr>
<td>Jean-Charles Faugère, Rune Steinsmo Ødegård, Ludovic Perret, and Danilo Gligoroski</td>
<td></td>
</tr>
<tr>
<td>Efficient Scalar Multiplications for Elliptic Curve Cryptosystems Using Mixed Coordinates Strategy and Direct Computations</td>
<td>184</td>
</tr>
<tr>
<td>Roghaie Mahdavi and Abolghasem Saiadian</td>
<td></td>
</tr>
</tbody>
</table>

# Invited Talk II

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography Meets Hardware: Selected Topics of Hardware-Based Cryptography (Abstract)</td>
<td>199</td>
</tr>
<tr>
<td>Ahmad-Reza Sadeghi</td>
<td></td>
</tr>
</tbody>
</table>

# Secure Mechanisms

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Towards a Cryptographic Treatment of Publish/Subscribe Systems</td>
<td>201</td>
</tr>
<tr>
<td>Tsz Hon Yuen, Willy Susilo, and Yi Mu</td>
<td></td>
</tr>
<tr>
<td>STE3D-CAP: Stereoscopic 3D CAPTCHA</td>
<td>221</td>
</tr>
<tr>
<td>Willy Susilo, Yang-Wai Chow, and Hua-Yu Zhou</td>
<td></td>
</tr>
<tr>
<td>TRIOB: A Trusted Virtual Computing Environment Based on Remote I/O Binding Mechanism</td>
<td>241</td>
</tr>
<tr>
<td>Haifeng Fang, Hui Wang, Yiqiang Zhao, Yuzhong Sun, and Zhiyong Liu</td>
<td></td>
</tr>
</tbody>
</table>

# Cryptographic Protocols

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Group Key Exchange Revisited</td>
<td>261</td>
</tr>
<tr>
<td>Guomin Yang and Chik How Tan</td>
<td></td>
</tr>
<tr>
<td>Towards Practical and Secure Coercion-Resistant Electronic Elections</td>
<td>278</td>
</tr>
<tr>
<td>Roberto Araújo, Narjes Ben Rajeb, Riadh Robbana, Jacques Traoré, and Souheib Yousfi</td>
<td></td>
</tr>
</tbody>
</table>
Anonymous Credentials

Predicate Encryption with Partial Public Keys ..................... 298

Carlo Blundo, Vincenzo Iovino, and Giuseppe Persiano

Anonymous Credential Schemes with Encrypted Attributes .......... 314

Jorge Guajardo, Bart Mennink, and Berry Schoenmakers

One Time Anonymous Certificate: X.509 Supporting Anonymity .... 334

Aymen Abed and Sébastien Canard

Author Index ............................................................ 355