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
Preface

The 7th International Workshop on Security (IWSEC 2012) was held at Nishi-jin Plaza, Kyushu University, in Fukuoka, Japan, during November 7–9, 2012. The workshop was co-organized by ISEC in ESS of IEICE (Technical Committee on Information Security in Engineering Sciences Society of the Institute of Electronics, Information and Communication Engineers) and CSEC of IPSJ (Special Interest Group on Computer Security of Information Processing Society of Japan).

This year, the workshop received 53 submissions, of which 16 were accepted for presentation. Each submission was anonymously reviewed by at least five reviewers, and these proceedings contain the revised versions of the accepted papers. In addition to the presentations of the papers, the workshop also featured a poster session and four invited talks. The invited talks were given by James Hughes, Matt Bishop, Suguru Yamaguchi, and Katsuyuki Takashima.

The best paper award was given to “Boomerang Distinguishers for Full HAS-160 Compression Function” by Yu Sasaki, Lei Wang, Yasuhiro Takasaki, Kazuo Sakiyama, and Kazuo Ohta, and the best student paper award was given to “Efficient Concurrent Oblivious Transfer in Super-Polynomial-Simulation Security” by Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto.

A number of people contributed to the success of IWSEC 2012. We would like to thank the authors for submitting their papers to the workshop. The selection of the papers was a challenging and delicate task, and we are deeply grateful to the members of Program Committee and the external reviewers for their in-depth reviews and detailed discussions. We are also grateful to Andrei Voronkov for developing EasyChair, which was used for the paper submission, reviews, discussions, and preparation of these proceedings.

Last but not least, we would like to thank the General Co-chairs, Tsutomu Matsumoto and Kanta Matsuura, for leading the Local Organizing Committee, and we also would like to thank the members of the Local Organizing Committee for their efforts to ensure the smooth running of the workshop.

August 2012

Goichiro Hanaoka
Toshihiro Yamauchi
IWSEC 2012
7th International Workshop on Security

Fukuoka, Japan, November 7–9, 2012

Co-organized by
ISEC in ESS of IEICE
(Technical Committee on Information Security in Engineering Sciences Society of the Institute of Electronics, Information and Communication Engineers)

and

CSEC of IPSJ
(Special Interest Group on Computer Security of Information Processing Society of Japan)

General Co-chairs
Tsutomu Matsumoto Yokohama National University, Japan
Kanta Matsuura The University of Tokyo, Japan

Advisory Committee
Hideki Imai Chuo University, Japan
Kwangjo Kim Korea Advanced Institute of Science and Technology, Korea
Günter Müller University of Freiburg, Germany
Yuko Murayama Iwate Prefectural University, Japan
Koji Nakao National Institute of Information and Communications Technology, Japan
Eiji Okamoto University of Tsukuba, Japan
C. Pandu Rangan Indian Institute of Technology, Madras, India

Program Co-chairs
Goichiro Hanaoka AIST, Japan
Toshihiro Yamauchi Okayama University, Japan

Local Organizing Committee
Yoshiaki Hori Kyushu University, Japan
Takuro Hosoi The University of Tokyo, Japan
Mitsugu Iwamoto The University of Electro-Communications, Japan
Takehisa Kato Toshiba Solutions Corporation, Japan
Akinori Kawachi Tokyo Institute of Technology, Japan
Fagen Li Kyushu University, Japan
Kirill Morozov Kyushu University, Japan
Takashi Nishide Kyushu University, Japan
Masayuki Numao The University of Electro-Communications, Japan
Naoyuki Shinohara National Institute of Information and Communications Technology, Japan
Mio Suzuki National Institute of Information and Communications Technology, Japan
Tsuyoshi Takagi Kyushu University, Japan
Kenji Yasunaga Institute of Systems, Information Technologies and Nanotechnologies, Japan

Program Committee

Rafael Accorsi University of Freiburg, Germany
Claudio Ardagna Università degli Studi di Milano, Italy
Nuttapong Attrapadung AIST, Japan
Andrey Bogdanov Katholieke Universiteit Leuven, Belgium
Kevin Butler University of Oregon, USA
Sanjit Chatterjee Indian Institute of Science, India
Haibo Chen Shanghai Jiao Tong University, China
Pau-Chen Cheng IBM Thomas J. Watson Research Center, USA
Koji Chida NTT, Japan
Bart De Decker Katholieke Universiteit Leuven, Belgium
Isao Echizen National Institute of Informatics, Japan
Dario Fiore New York University, USA
Georg Fuchsbauer University of Bristol, UK
Eiichiro Fujisaki NTT, Japan
Steven Furnell University of Plymouth, UK
David Galindo University of Malaga, Spain
Dieter Gollmann Hamburg University of Technology, Germany
Swee-Huay Heng Multimedia University, Malaysia
Jin Hong Seoul National University, Korea
Tetsu Iwata Nagoya University, Japan
Angelos D. Keromytis Columbia University, USA
Hyung Chan Kim ETRI, Korea
Takeshi Koshiba Saitama University, Japan
Noboru Kunihiro University of Tokyo, Japan
Kwok-Yan Lam Tsinghua University, China
Benoît Libert Université Catholique de Louvain, Belgium
Javier Lopez University of Malaga, Spain
Keith Martin Royal Holloway, University of London, UK
Masakatsu Nishigaki Shizuoka University, Japan
Wakah Ogata Tokyo Institute of Technology, Japan
Thomas Peyrin Nanyang Technological University, Singapore
Raphael Phan Loughborough University, UK
Axel Poschmann Nanyang Technological University, Singapore
Bart Preneel Katholieke Universiteit Leuven, Belgium
Kai Rannenberg Goethe University Frankfurt, Germany
Kazuo Sakiyama University of Electro-Communications, Japan
Ryoichi Sasaki Tokyo Denki University, Japan
Joshua Schiffman Pennsylvania State University, USA
Jae Hong Seo NICT, Japan
Francesco Sica University of Waterloo, Canada
Tsuyoshi Takagi Kyushu University, Japan
Keisuke Takemori KDDI R&D Laboratories Inc., Japan
Keisuke Tanaka Tokyo Institute of Technology, Japan
Masayuki Terada NTT DoCoMo, Japan
Ryuya Uda Tokyo University of Technology, Japan
Damien Vergnaud ENS, France
Sandra De Capitani University of Milan, Italy
di Vimercati
Guilin Wang University of Wollongong, Australia
Jian Weng Jinan University, China
Sven Wohlgemuth Sirrix AG security technologies, Germany
Keita Xagawa NTT, Japan
Chung-Huang Yang National Kaohsiung Normal University, Taiwan
Kazuki Yoneyama NTT, Japan
Katsunari Yoshioka Yokohama National University, Japan
Hirosi Yoshiura University of Electro-Communications, Japan
Rui Zhang CAS, China
Yunlei Zhao Fudan University, China

External Reviewers

Elena Andreeva Toshiyuki Isshiki
Lejla Batina Malika Izabachene
Ji-Jian Chin Charanjit Jutla
Angelo De Caro Christian Kahl
Junfeng Fan Chethan Kamath
Pooya Farshim Akinori Kawachi
Yanfei Guo Ryo Kikuchi
Keisuke Hakuta Ilya Kizhvatov
Takuya Hayashi Ulrich Kuehn
Jens Hermans Sebastian Kutzner
Johann Heyszl Shugo Mikami
Takashi Horiyama Kirill Morozov
Kota Ideguchi Nicky Mouha
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Divya Muthukumaran</td>
<td>Leif Uhsadel</td>
</tr>
<tr>
<td>Phuong Ha Nguyen</td>
<td>Kerem Varici</td>
</tr>
<tr>
<td>Hannah Pruse</td>
<td>Hayawardh Vijayakumar</td>
</tr>
<tr>
<td>Arnab Roy</td>
<td>Lei Wang</td>
</tr>
<tr>
<td>Ahmad Sabouri</td>
<td>Lei Wei</td>
</tr>
<tr>
<td>Seog Chung Seo</td>
<td>Wun-She Yap</td>
</tr>
<tr>
<td>Kyoji Shibutani</td>
<td>Takanori Yasuda</td>
</tr>
<tr>
<td>Wook Shin</td>
<td>Kenji Yasunaga</td>
</tr>
<tr>
<td>Ingo Stengel</td>
<td>Wei-Chuen Yau</td>
</tr>
<tr>
<td>Mario Strefler</td>
<td>Wei Zhang</td>
</tr>
<tr>
<td>Susan Thomson</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

## Implementation

Model-Based Conformance Testing for Android .......................... 1  
*Yiming Jing, Gail-Joon Ahn, and Hongxin Hu*

Application of Scalar Multiplication of Edwards Curves to Pairing-Based Cryptography .................................... 19  
*Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai*

Standardized Signature Algorithms on Ultra-constrained 4-Bit MCU ... 37  
*Chien-Ning Chen, Nisha Jacob, Sebastian Kutzner, San Ling, Axel Poschmann, and Sirote Saetang*

Very Short Critical Path Implementation of AES with Direct Logic Gates ................................................................. 51  
*Kenta Nekado, Yasuyuki Nogami, and Kengo Iokibe*

## Encryption and Key Exchange

One-Round Authenticated Key Exchange with Strong Forward Secrecy in the Standard Model against Constrained Adversary ................ 69  
*Kazuki Yoneyama*

Compact Stateful Encryption Schemes with Ciphertext Verifiability .... 87  
*S. Sree Vivek, S. Sharmila Deva Selvi, and C. Pandu Rangan*

Structured Encryption for Conceptual Graphs ............................. 105  
*Geong Sen Poh, Moesfa Soheila Mohamad, and Muhammad Reza Z’aba*

Symmetric-Key Encryption Scheme with Multi-ciphertext Non-malleability ................................................................. 123  
*Akinori Kawachi, Hirotoshi Takebe, and Keisuke Tanaka*

## Cryptanalysis

Slide Cryptanalysis of Lightweight Stream Cipher RAKAPOSHI ........ 138  
*Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii*

Boomerang Distinguishers for Full HAS-160 Compression Function ..... 156  
*Yu Sasaki, Lei Wang, Yasuhiro Takasaki, Kazuo Sakiyama, and Kazuo Ohta*
Polynomial-Advantage Cryptanalysis of 3D Cipher and 3D-Based Hash Function ........................................................ 170
   Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta

Annihilators of Fast Discrete Fourier Spectra Attacks .................. 182
   Jingjing Wang, Kefei Chen, and Shixiong Zhu

Meet-in-the-Middle Attack on Reduced Versions of the Camellia Block Cipher ................................................................. 197
   Jiqiang Lu, Yongzhuang Wei, Enes Pasalic, and Pierre-Alain Fouque

Secure Protocols

Efficient Concurrent Oblivious Transfer in Super-Polynomial-Simulation Security .......................................................... 216
   Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto

Efficient Secure Primitive for Privacy Preserving Distributed Computations ................................................................. 233
   Youwen Zhu, Tsuyoshi Takagi, and Liusheng Huang

Generic Construction of GUC Secure Commitment in the KRK Model ................................................................. 244
   Itsuki Suzuki, Maki Yoshida, and Toru Fujiwara

Author Index ................................................................. 261