Preface

The 2009 RSA conference was held in San Francisco, USA, during April 20-24. The conference is devoted to security-related topics and, as part of this, hosts a distinguished track for cryptographic research. Since 2001 the proceedings of this Cryptographers’ Track (CT-RSA) have been published in the series Lecture Notes in Computer Science of Springer.

The proceedings of CT-RSA 2009 contain 31 papers selected from 93 submissions, covering a wide variety of cryptographic areas. Each submission was anonymized for the reviewing process and was assigned to at least three of the 25 Program Committee members. Submissions co-authored by committee members were assigned to at least five members. After carefully considering more than 15,000 lines (more than 100,000 words) of reviews and online discussions, the committee selected 31 submissions for acceptance. The program also included an invited talk by Kenny Paterson entitled “Cryptography and Secure Channels.”

I would like to thank all the authors who submitted papers. I am also indebted to the Program Committee members and all external reviewers for their voluntary work. The committee’s work was tremendously simplified by Shai Halevi’s submission software and his support. I would also like to thank the CT-RSA Steering Committee for electing me as Chair, and all the people from the RSA conference team for their support, especially Bree LaBollita.

January 2009

Marc Fischlin
CT-RSA 2009

RSA Conference 2009, Cryptographers’ Track
Moscone Center, San Francisco, CA, USA
April 20–24, 2009

Program Chair
Marc Fischlin
Darmstadt University of Technology, Germany

Program Committee
Michel Abdalla
ENS & CNRS, France
Zuzana Beerliova-Trubiniova
ETH Zurich, Switzerland
Alex Biryukov
University of Luxembourg, Luxembourg
Melissa Chase
Microsoft Research, USA
Alex Dent
Royal Holloway, UK
Nelly Fazio
City University of New York, USA
Juan Garay
AT&T Labs - Research, USA
Amir Herzberg
Bar-Ilan University, Israel
Dennis Hofheinz
CWI, The Netherlands
Nick Howgrave-Graham
NTRU Cryptosystems, USA
Stanislaw Jarecki
UC Irvine, USA
Marc Joye
Thomson, France
Alexander May
Bochum University, Germany
Jesper Buus Nielsen
University of Aarhus, Denmark
Giuseppe Persiano
University of Salerno, Italy
Josef Pieprzyk
Macquarie University, Australia
Vincent Rijmen
K.U. Leuven, Belgium, and Graz University of Technology, Austria
Kazue Sako
NEC, Japan
Christian Schaffner
CWI, The Netherlands
Berry Schoenmakers
TU Eindhoven, The Netherlands
Willy Susilo
University of Wollongong, Australia
Pim Tuyls
Philips, The Netherlands
Jorge Villar
UPC Barcelona, Spain
Bogdan Warinschi
University of Bristol, UK
External Reviewers

Divesh Aggarwal
Toshinori Araki
Giuseppe Ateniese
Man Ho Au
Roberto Avanzi
Rikke Bendlin
Johannes Blömer
Colin Boyd
Christoph de Canniere
Srdjan Capkun
Rafik Chaabouni
Donghoon Chang
Sherman Chow
Christophe Clavier
Erik Dahmen
Jean-François Dhem
Orr Dunkelman
Serge Fehr
Jun Feng
Pierre-Alain Fouque
Jakob Funder
Steven Galbraith
Martin Geisler
Rosario Gennaro
Benedikt Gierlichs
Aline Gouget
Tim Gueneysu
Carmiy Hazay
Martin Hirt
Qiong Huang
Xinyi Huang
Sebastiaan Indesteege
Vicenzo Iovino
Vincenzo Iovino
Toshiyuki Isshiki
Gene Itkis
Emilia Kasper
Dmitry Khovratovich
Eike Kiltz
Ilya Kizhvatov
Sandeep Kumar
Alptekin Kupcu
Gregor Leander
Anja Lehmann
Helger Lipmaa
Xiaomin Liu
Jiqiang Lu
Christoph Lucas
Roel Maes
Mark Manulis
Krystian Matusiewicz
Sigurd Torkel Meldgaard
Florian Mendel
Nele Mentens
Kazuhiko Mihematsu
Gert Lassøe Mikkelsen
Paul Morrissey
Nicky Mouha
Elke De Mulder
Tomislav Nad
Gregory Neven
Long Nguyen
Phong Nguyen
Antonio Nicolosi
Ivica Nikolic
Svetla Nikova
Satoshi Obana
Francis Olivier
Claudio Orlandi
Elisabeth Oswald
Dan Page
Kenny Paterson
Giuseppe Persiano
Krzysztof Pietrzak
Thomas Popp
Dominik Raub
Thomas Ristenpart
Matt Robshaw
Pankaj Rohatgi
Dries Schellekens
Martin Schlaeffe
Jacob Schuldt
Gautham Sekar
Haya Shulman
Nigel Smart
Martijn Stam
Ron Steinfeld
Marc Stevens
Bjoern Tackmann
Christophe Tartary
Tamir Tassa
Isamu Teranishi
Stefano Tessaro
Elmar Tischhauser
Nikos Triandopoulos
Michael Tunstall
Mike Tunstall
Osman Ugus
Frederic Vercauteren
Damien Vergnaud
Peishun Wang
Benne de Weger
Ralf-Philipp Weinmann
Enav Weinreb
Christopher Wolf
Oliver Wuebbolt
Ng Ching Yu
Tsz Hon Yuen
Hong-Sheng Zhou
Vassilis Zikas
# Table of Contents

## Identity-Based Encryption

Adaptive-ID Secure Revocable Identity-Based Encryption .......................... 1

*Benoît Libert and Damien Vergnaud*

An Efficient Encapsulation Scheme from Near Collision Resistant Pseudorandom Generators and Its Application to IBE-to-PKE Transformations .................................................. 16

*Takahiro Matsuda, Goichiro Hanaoka, Kanta Matsuura, and Hideki Imai*

Universally Anonymous IBE Based on the Quadratic Residuosity Assumption ................................................................. 32

*Giuseppe Ateniese and Paolo Gasti*

## Protocol Analysis

Attacks on the DECT Authentication Mechanisms ................................. 48

*Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, and Matthias Wenzel*

Comparison-Based Key Exchange and the Security of the Numeric Comparison Mode in Bluetooth v2.1 ........................................ 66

*Andrew Y. Lindell*

## Two-Party Protocols

Key Insulation and Intrusion Resilience over a Public Channel .............. 84

*Mihir Bellare, Shanshan Duan, and Adriana Palacio*

Statistically Hiding Sets ............................................................... 100

*Manoj Prabhakaran and Rui Xue*

Adaptively Secure Two-Party Computation with Erasures .................... 117

*Andrew Y. Lindell*

## More Than Signatures

Short Redactable Signatures Using Random Trees ............................... 133

*Ee-Chien Chang, Chee Liang Lim, and Jia Xu*

Divisible On-Line/Off-Line Signatures ........................................... 148

*Chong-zhi Gao, Baodian Wei, Dongqing Xie, and Chunming Tang*
# Table of Contents

## Collisions for Hash Functions

Speeding up Collision Search for Byte-Oriented Hash Functions ........ 164

*Dmitry Khovratovich, Alex Biryukov, and Ivica Nikolic*

Hard and Easy Components of Collision Search in the Zémor-Tillich Hash Function: New Attacks and Reduced Variants with Equivalent Security .................................................. 182

*Christophe Petit, Jean-Jacques Quisquater, Jean-Pierre Tillich, and Gilles Zémor*

## Cryptanalysis

A Statistical Saturation Attack against the Block Cipher PRESENT ... 195

*B. Collard and F.-X. Standaert*

Practical Attacks on Masked Hardware ................................. 211

*Thomas Popp, Mario Kirschbaum, and Stefan Mangard*

Cryptanalysis of CTC2 .................................................. 226

*Orr Dunkelman and Nathan Keller*

## Alternative Encryption

A CCA2 Secure Public Key Encryption Scheme Based on the McEliece Assumptions in the Standard Model ..................................... 240

*Rafael Dowsley, Jörn Müller-Quade, and Anderson C.A. Nascimento*

Square, a New Multivariate Encryption Scheme .......................... 252

*Cristal Clough, John Baena, Jintai Ding, Bo-Yin Yang, and Ming-shing Chen*

## Privacy and Anonymity

Communication-Efficient Private Protocols for Longest Common Subsequence ............................................................ 265

*Matthew Franklin, Mark Gondree, and Payman Mohassel*

Key-Private Proxy Re-encryption ........................................... 279

*Giuseppe Ateniese, Karyn Benson, and Susan Hohenberger*

Dynamic Universal Accumulators for DDH Groups and Their Application to Attribute-Based Anonymous Credential Systems .... 295

*Man Ho Au, Patrick P. Tsang, Willy Susilo, and Yi Mu*

## Efficiency Improvements

Practical Short Signature Batch Verification .............................. 309

*Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, and Michael Østergaard Pedersen*
Single-Layer Fractal Hash Chain Traversal with Almost Optimal Complexity .................................................... 325  
Dae Hyun Yum, Jae Woo Seo, Sungwook Eom, and Pil Joong Lee

Recursive Double-Size Modular Multiplications without Extra Cost for Their Quotients .................................................. 340  
Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume

**Multi-Party Protocols**

Constant-Rounds, Almost-Linear Bit-Decomposition of Secret Shared Values .......................................................... 357  
Tomas Toft

Local Sequentiality Does Not Help for Concurrent Composition ............ 372  
Andrew Y. Lindell

**Security of Encryption Schemes**

Breaking and Repairing Damgård et al. Public Key Encryption Scheme with Non-interactive Opening  .............................................. 389  
David Galindo

Strengthening Security of RSA-OAEP ........................................... 399  
Alexandra Boldyreva

**Faults and Countermeasures**

Fault Attacks on RSA Public Keys: Left-To-Right Implementations Are Also Vulnerable ................................................... 414  
Alexandre Berzati, Cécile Canovas, Jean-Guillaume Dumas, and Louis Goubin

Fault Analysis Attack against an AES Prototype Chip Using RSL ...... 429  
Kazuo Sakiyama, Tatsuya Yagi, and Kazuo Ohta

**Countermeasures and Faults**

Evaluation of the Detached Power Supply as Side-Channel Analysis Countermeasure for Passive UHF RFID Tags ......................... 444  
Thomas Plos

Securing RSA against Fault Analysis by Double Addition Chain Exponentiation ....................................................... 459  
Matthieu Rivain

**Author Index** ................................................................. 481