Advances in Cryptology – ASIACRYPT 2005

11th International Conference on the Theory and Application of Cryptology and Information Security
Chennai, India, December 4-8, 2005
Proceedings
Preface

Asiacrypt, the annual conference of cryptology sponsored by IACR is now 11 years old. Asiacrypt 2005 was held during December 4–8, 2005, at Hotel Taj Coromandel, Chennai, India. This conference was organized by the International Association for Cryptologic Research (IACR) in cooperation with the Indian Institute of Technology (IIT), Chennai.

This year a total of 237 papers were submitted to Asiacrypt 2005. The submissions covered all areas of cryptographic research representing the current state of work in the crypto community worldwide. Each paper was blind reviewed by at least three members of the Program Committee and papers co-authored by the PC members were reviewed by at least six members. This first phase of review by the PC members was followed by a detailed discussion on the papers. At the end of the reviewing process 37 papers were accepted and were presented at the conference. The proceedings contain the revised versions of the accepted papers. In addition we were fortunate to have Prof. Andrew Yao and Prof. Bart Preneel as invited speakers.

Based on a discussion and subsequent voting among the PC members, the Best Paper Award for this year’s Asiacrypt was conferred to Pascal Paillier and Damien Vergnaud for the paper entitled “Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log.”

I would like to thank the following people. First, the General Chair, Prof. Pandu Rangan. Next, Springer for publishing the proceedings in the Lecture Notes in Computer Science series. I would also like to thank the submitting authors, the Program Committee members, the external reviewers, and the local Organizing Committee consisting of Mr. Veeraraghavan and Mr. E. Boopal. I acknowledge the partial financial support provided by Microsoft Research Labs, India. I thank Dr. Debrup Chakraborty for his help in managing the submissions and the final preparation of the proceedings. Thanks also goes to Mr. Sanjit Chatterjee for his assistance in the process.

December 2005

Bimal Roy
Asiacrypt 2005
December 3–7, 2005, Chennai, India

Sponsored by the
International Association for Cryptologic Research

in cooperation with
Indian Institute of Technology, Chennai, India

General Chair
C. Pandu Rangan, Indian Institute of Technology, Chennai, India

Program Chair
Bimal Roy, Indian Statistical Institute, Kolkata, India
<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manindra Agarwal</td>
<td>Indian Institute of Technology, Kanpur, India, and National University of Singapore, Singapore</td>
</tr>
<tr>
<td>Feng Bao</td>
<td>Institute for Infocomm Research, Singapore</td>
</tr>
<tr>
<td>Rana Barua</td>
<td>Indian Statistical Institute, India</td>
</tr>
<tr>
<td>P.S.L.M. Barreto</td>
<td>University of São Paulo, Brazil</td>
</tr>
<tr>
<td>Alex Biryukov</td>
<td>Katholieke Universiteit, Leuven, Belgium</td>
</tr>
<tr>
<td>Simon R. Blackburn</td>
<td>Royal Holloway College, University of London, UK</td>
</tr>
<tr>
<td>Colin Boyd</td>
<td>Queensland University of Technology, Australia</td>
</tr>
<tr>
<td>Nicolas T. Courtois</td>
<td>Axalto Smart Cards, France</td>
</tr>
<tr>
<td>Cunsheng Ding</td>
<td>Hong Kong University of Science and Technology, Hong Kong, China</td>
</tr>
<tr>
<td>Orr Dunkelman</td>
<td>Technion, Israel</td>
</tr>
<tr>
<td>Jovan Golic</td>
<td>Telecom Italia, Italy</td>
</tr>
<tr>
<td>Lai Xue Jia</td>
<td>Shanghai Jiaotong University, China</td>
</tr>
<tr>
<td>Thomas Johansson</td>
<td>Lund University, Sweden</td>
</tr>
<tr>
<td>Chi Sung Laih</td>
<td>National Cheng Kung University, Taiwan</td>
</tr>
<tr>
<td>Tanja Lange</td>
<td>Ruhr University Bochum, Germany</td>
</tr>
<tr>
<td>Pil Joong Lee</td>
<td>Pohang University of Science &amp; Technology, Korea</td>
</tr>
<tr>
<td>Arjen K. Lenstra</td>
<td>Lucent Technologies, USA, and Technische Universiteit Eindhoven, Netherlands</td>
</tr>
<tr>
<td>Chae Hoon Lim</td>
<td>Sejong University, Korea</td>
</tr>
<tr>
<td>C.E. Veni Madhavan</td>
<td>Indian Institute of Science, India</td>
</tr>
<tr>
<td>Alfred Menezes</td>
<td>University of Waterloo, Canada</td>
</tr>
<tr>
<td>Phong Q. Nguyen</td>
<td>CNRS/École Normale Supérieure, France</td>
</tr>
<tr>
<td>Kapil Paranjape</td>
<td>Institute of Mathematical Sciences, India</td>
</tr>
<tr>
<td>David Pointcheval</td>
<td>CNRS/École Normale Supérieure, France</td>
</tr>
<tr>
<td>Jean-Jacques Quisquater</td>
<td>Université Catholique de Louvain, Belgium</td>
</tr>
<tr>
<td>C. Pandu Rangan</td>
<td>Indian Institute of Technology, Madras, India</td>
</tr>
<tr>
<td>Vincent Rijmen</td>
<td>Technical University of Graz, Austria</td>
</tr>
<tr>
<td>Rei Safavi-Naini</td>
<td>University of Wollongong, Australia</td>
</tr>
<tr>
<td>Amit Sahai</td>
<td>University of California, Los Angeles, USA</td>
</tr>
<tr>
<td>Kouichi Sakurai</td>
<td>Kyushu University, Japan</td>
</tr>
<tr>
<td>P.K. Saxena</td>
<td>SAG, India</td>
</tr>
<tr>
<td>Nicolas Sendrier</td>
<td>INRIA, France</td>
</tr>
<tr>
<td>Hovav Shacham</td>
<td>Stanford University, USA</td>
</tr>
<tr>
<td>Nigel Smart</td>
<td>University of Bristol, UK</td>
</tr>
<tr>
<td>Douglas R. Stinson</td>
<td>University of Waterloo, Canada</td>
</tr>
<tr>
<td>Xiaoyun Wang</td>
<td>Shandong University, China</td>
</tr>
<tr>
<td>Hugh Williams</td>
<td>University of Calgary, Canada</td>
</tr>
</tbody>
</table>
External Reviewers

Michel Abdalla
Raju Agarwal
Omran Ahmadi
Sattam Al-Riyami
Daniel Augot
Roberto Avanzi
Steve Babbage
Joongsang Baek
Vittorio Bagini
Boaz Barak
Mark Bauer
S.S. Bedi
Daniel J. Bernstein
Amnon Besser
Raghav Bhaskar
A.K. Bhateja
Dan Boneh
Xavier Boyen
An Braeken
Emmanuel Bresson
Christophe De Canniere
Anne Canteaut
Dario Catalano
Juyoung Cha
Sucheta Chakraborty
Pascale Charpin
Sanjit Chatterjee
Liquin Chen
Jung Hee Cheon
Benoit Chevallier-Mames
Kookrae Cho
Kim-Kwang R. Choo
Sherman Chow
Carlos Cid
Ricardo Dahab
Blandine Debraize
Alex Dent
Claus Diem
Ratna Dutta
Andreas Enge
Chun-I Fan
Nelly Fazio
Serge Fehr
Decio Luiz Gazzoni Filho
Gerhard Frey
Pierre-Alain Fouque
Navneet Gaba
Fabien Galand
Steven Galbraith
David Galindo
Juan Garay
Pierrick Gaudry
Craig Gentry
Eu-Jin Goh
Louis Goubin
Rob Granger
Jens Groth
D.J. Guan
Indivar Gupta
Saoshi Hada
Darrel Hankerson
Yong-Sork Her
Julio Cesar L. Hernández
Jason Hinek
Yvonne Hitchcock
Andreas Hirt
Martin Hirt
Susan Hohenberger
Yoshiaki Hori
Wang Chih Hung
Yong Ho Hwang
Kenji Imamoto
Yuval Ishai
Mike Jacobson
Rahul Jain
Devendra Jha
Shaoquan Jiang
Ari Juels
Pascal Junod
Guruprasad Kar
Jonathan Katz
Chong Hee Kim
Seung Joo Kim
Shinsaku Kiyomoto
Yuichi Komano
Caroline Kudla
Sandeep Kumar
Meena Kumari
Sébastien Kunz-Jacques
Kaoru Kurosawa
Hidenori Kuwakado
Yann Laigle-Chapuy
Joseph Lano
Cedric Lauradoux
Dong Hoon Lee
Jooyoung Lee
Jung Wook Lee
Wei-Bin Lee
Stephane Lemieux
Manuel Leone
Francois Levy-dit-Vehel
Benoît Libert
Yehuda Lindell
Yu Long
Chi-Jen Lu
Ling Lu
Stefan Lucks
Subhomay Maitra
John Malone-Lee
Stephane Manuel
Keith Martin
Atefeh Mashatan
Luke McAvan
Renato Menicocci
Miodrag Mihaljevic
Marine Minier
Pradeep Mishra
P.R. Mishra
Chris Mitchell
Bodo Moeller
Guglielmo Morgari
Bernard Mourrain
Yi Mu
Siguna Mueller
Frédéric Muller
Mats Naeslund
Mridul Nandi
Anderson Nascimento
Gregory Neven
Table of Contents

Algebra and Number Theory

Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log
  Pascal Paillier, Damien Vergnaud ........................................ 1

Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?
  David Jao, Stephen D. Miller, Ramarathnam Venkatesan ............. 21

Adapting Density Attacks to Low-Weight Knapsacks
  Phong Q. Nguyêñ, Jacques Stern ........................................... 41

Efficient and Secure Elliptic Curve Point Multiplication Using Double-Base Chains
  Vassil Dimitrov, Laurent Imbert,
  Pradeep Kumar Mishra ..................................................... 59

Multiparty Computation

Upper Bounds on the Communication Complexity of Optimally ResilientCryptographic Multiparty Computation
  Martin Hirt, Jesper Buus Nielsen ........................................... 79

Graph-Decomposition-Based Frameworks for Subset-Cover Broadcast Encryption and Efficient Instantiations
  Nuttapong Attrapadung, Hideki Imai ...................................... 100

Revealing Additional Information in Two-Party Computations
  Andreas Jakoby, Maciej Liškiewicz ....................................... 121

Zero Knowledge and Secret Sharing

Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation
  Vladimir Kolesnikov ......................................................... 136

Parallel Multi-party Computation from Linear Multi-secret Sharing Schemes
  Zhifang Zhang, Mulan Liu, Liangliang Xiao ............................ 156
Updatable Zero-Knowledge Databases

*Moses Liskov* .................................................. 174

**Information and Quantum Theory**

Simple and Tight Bounds for Information Reconciliation and Privacy Amplification

*Renato Renner, Stefan Wolf* .................................... 199

Quantum Anonymous Transmissions

*Matthias Christandl, Stephanie Wehner* ......................... 217

**Privacy and Anonymity**

Privacy-Preserving Graph Algorithms in the Semi-honest Model

*Justin Brickell, Vitaly Shmatikov* .......................... 236

Spreading Alerts Quietly and the Subgroup Escape Problem

*James Aspnes, Zoë Diamadi, Kristian Gjøsteen, René Peralta, Aleksandr Yampolskiy* ............................. 253

A Sender Verifiable Mix-Net and a New Proof of a Shuffle

*Douglas Wikström* .......................................................... 273

Universally Anonymizable Public-Key Encryption

*Ryotaro Hayashi, Keisuke Tanaka* ............................. 293

**Cryptanalytic Techniques**

Fast Computation of Large Distributions and Its Cryptographic Applications

*Alexander Maximov, Thomas Johansson* ......................... 313

An Analysis of the XSL Algorithm

*Carlos Cid, Gaëtan Leurent* ......................................... 333

**Stream Cipher Cryptanalysis**

New Applications of Time Memory Data Tradeoffs

*Jin Hong, Palash Sarkar* .................................................. 353

Linear Cryptanalysis of the TSC Family of Stream Ciphers

*Frédéric Muller, Thomas Peyrin* ..................................... 373
A Practical Attack on the Fixed RC4 in the WEP Mode

I. Mantin ......................................................... 395

A Near-Practical Attack Against B Mode of HBB

Joydip Mitra .................................................. 412

Block Ciphers and Hash Functions

New Improvements of Davies-Murphy Cryptanalysis

Sébastien Kunz-Jacques, Frédéric Muller ......................... 425

A Related-Key Rectangle Attack on the Full KASUMI

Eli Biham, Orr Dunkelman, Nathan Keller ......................... 443

Some Attacks Against a Double Length Hash Proposal

Lars R. Knudsen, Frédéric Muller .............................. 462

A Failure-Friendly Design Principle for Hash Functions

Stefan Lucks .................................................. 474

Bilinear Maps

Identity-Based Hierarchical Strongly Key-Insulated Encryption
and Its Application

Yumiko Hanaoka, Goichiro Hanaoka, Junji Shikata, Hideki Imai .... 495

Efficient and Provably-Secure Identity-Based Signatures and
Signcryption from Bilinear Maps

Paulo S.L.M. Barreto, Benoît Libert, Noel McCullagh,
Jean-Jacques Quisquater ........................................ 515

Verifier-Local Revocation Group Signature Schemes with Backward
Unlinkability from Bilinear Maps

Toru Nakanishi, Nobuo Funabiki ................................ 533

Key Agreement

Modular Security Proofs for Key Agreement Protocols

Caroline Kudla, Kenneth G. Paterson ............................ 549

A Simple Threshold Authenticated Key Exchange from Short Secrets

Michel Abdalla, Olivier Chevassut, Pierre-Alain Fouque,
David Pointcheval ............................................. 566
Examine Indistinguishability-Based Proof Models for Key Establishment Protocols

Kim-Kwang Raymond Choo, Colin Boyd, Yvonne Hitchcock ........ 585

Provable Security

Server-Aided Verification: Theory and Practice
Marc Girault, David Lefranc ........................................... 605

Errors in Computational Complexity Proofs for Protocols
Kim-Kwang Raymond Choo, Colin Boyd, Yvonne Hitchcock ....... 624

Signatures

Universal Designated Verifier Signature Proof (or How to Efficiently Prove Knowledge of a Signature)
Joonsang Baek, Reihaneh Safavi-Naini, Willy Susilo ............... 644

Efficient Designated Confirmer Signatures Without Random Oracles or General Zero-Knowledge Proofs
Craig Gentry, David Molnar, Zulfikar Ramzan..................... 662

Universally Convertible Directed Signatures
Fabien Laguillaumie, Pascal Paillier, Damien Vergnaud .......... 682

Author Index ............................................................ 703