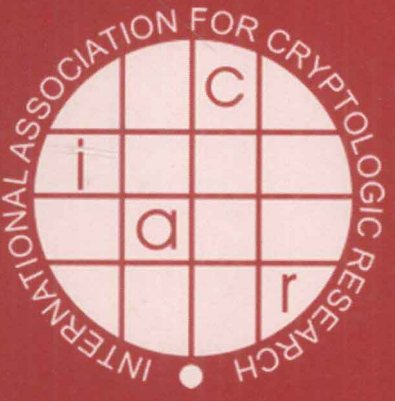
Bimal Roy (Ed.)

LNCS 3788

Advances in Cryptology – ASIACRYPT 2005

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



Springer

Bimal Roy (Ed.)

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

Volume Editor

Bimal Roy
Indian Statistical Institute, Applied Statistics Unit
203 B.T. Road, Kolkata 700 108, India
E-mail: bimal@isical.ac.in

Library of Congress Control Number: 2005936460

CR Subject Classification (1998): E.3, D.4.6, F.2.1-2, K.6.5, C.2, J.1, G.2

ISSN 0302-9743
ISBN-10 3-540-30684-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30684-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11593447 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3788

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Program Committee

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

External Reviewers

Michel Abdalla
Raju Agarwal
Omran Ahmadi
Sattam Al-Riyami
Daniel Augot
Roberto Avanzi
Steve Babbage
Joonsang 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
Liqun 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
Benoit Libert
Yehuda Lindell
Yu Long
Chi-Jen Lu
Ling Lu
Stefan Lucks
Subhomay Maitra
John Malone-Lee
Stephane Manuel
Keith Martin
Atefeh Mashatan
Luke McAven
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

Antonio Nicolosi
Juan Gonzalez Nieto
Ryuzou Nishi
Takeshi Okamoto
Tatsuaki Okamoto
Harold Ollivier
Rafi Ostrovsky
Haruki Ota
S.K. Pal
Dan Page
Pascal Pallier
Dong Jin Park
Jung Hyung Park
Young Ho Park
Raphael Pass
Kenny Paterson
Kun Peng
Slobodan Petrovic
Duong Hieu Phan
N. Rajesh Pillai
Benny Pinkas
Norbert Pramstaller
J. Radhakrishnan
Christian Rechberger
Eric Rescorla
Leo Reyzin
Gal Rouvroy
Yasuyuki Sakai
Palash Sarkar
Reg Sawilla
Ruediger Schack
Renate Scheidler
Werner Schindler
Alice Silverberg
Jae Woo Seo
Nicholas Sheppard
Jong Hoon Shin
Tom Shrimpton
M.C. Shrivastava
Andrey Sidorenko
Sanjeet Singh
Martijn Stam
Hung-Min Sun
Jae Chul Sung
Krishna Suri
Willy Susilo
Gelareh Taban
Keisuke Tanaka
Edlyn Teske
Jean-Pierre Tillich
Rajeev Thamman
Nicolas Theriault
Dongvu Tonien
Wen-Guey Tzeng
Shinegori Uchiyama
Yoshifumi Ueshige
Damien Vergnaud
Eric Verheul
Neelam Verma
Guilin Wang
Huaxiong Wang
Dai Watanabe
Brent Waters
Benne de Weger
William Whyte
Peter Wild
Christopher Wolf
Kjell Wooding
Yongdong Wu
Tianbing Xia
Pratibha Yadav
Bo-Yin Yang
Yeon Hyeong Yang
Jeong Il Yoon
Young Tae Youn
Yuliang Zheng
Huafei Zhu

Lecture Notes in Computer Science

For information about Vols. 1–3708

please contact your bookseller or Springer

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Subseries LNAI).

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Subseries LNAI).

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Subseries LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3804: G. Bebis, R. Boyle, D. Koracin, B. Parvin (Eds.), Advances in Visual Computing. XX, 755 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

Vol. 3798: A. Dearle, S. Eisenbach (Eds.), Component Deployment. X, 197 pages. 2005.

Vol. 3796: N.P. Smart (Ed.), Cryptography and Coding. XI, 461 pages. 2005.

Vol. 3795: H. Zhuge, G.C. Fox (Eds.), Grid and Cooperative Computing - GCC 2005. XXI, 1203 pages. 2005.

Vol. 3793: T. Conte, N. Navarro, W.-m.W. Hwu, M. Valero, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XIII, 317 pages. 2005.

Vol. 3792: I. Richardson, P. Abrahamsson, R. Messnarz (Eds.), Software Process Improvement. VIII, 215 pages. 2005.

Vol. 3791: A. Adi, S. Stoutenburg, S. Tabet (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 225 pages. 2005.

Vol. 3790: G. Alonso (Ed.), Middleware 2005. XIII, 443 pages. 2005.

Vol. 3789: A. Gelbukh, Á. de Albornoz, H. Terashima-Marín (Eds.), MICAI 2005: Advances in Artificial Intelligence. XXVI, 1198 pages. 2005. (Subseries LNAI).

Vol. 3788: B. Roy (Ed.), Advances in Cryptology - ASIACRYPT 2005. XIV, 703 pages. 2005.

Vol. 3785: K.-K. Lau, R. Banach (Eds.), Formal Methods and Software Engineering. XIV, 496 pages. 2005.

Vol. 3784: J. Tao, T. Tan, R.W. Picard (Eds.), Affective Computing and Intelligent Interaction. XIX, 1008 pages. 2005.

Vol. 3781: S.Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, D. Zhang (Eds.), Advances in Biometric Person Authentication. XI, 250 pages. 2005.

Vol. 3780: K. Yi (Ed.), Programming Languages and Systems. XI, 435 pages. 2005.

Vol. 3779: H. Jin, D. Reed, W. Jiang (Eds.), Network and Parallel Computing. XV, 513 pages. 2005.

Vol. 3777: O.B. Lupanov, O.M. Kasim-Zade, A.V. Chaskin, K. Steinhöfel (Eds.), Stochastic Algorithms: Foundations and Applications. VIII, 239 pages. 2005.

Vol. 3775: J. Schönwälder, J. Serrat (Eds.), Ambient Networks. XIII, 281 pages. 2005.

Vol. 3773: A. Sanfeliu, M.L. Cortés (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XX, 1094 pages. 2005.

Vol. 3772: M. Consens, G. Navarro (Eds.), String Processing and Information Retrieval. XIV, 406 pages. 2005.

Vol. 3771: J.M.T. Romijn, G.P. Smith, J. van de Pol (Eds.), Integrated Formal Methods. XI, 407 pages. 2005.

Vol. 3770: J. Akoka, S.W. Liddle, I.-Y. Song, M. Bertolotto, I. Comyn-Wattiau, W.-J. van den Heuvel, M. Kolp, J. Trujillo, C. Kop, H.C. Mayr (Eds.), Perspectives in Conceptual Modeling. XXII, 476 pages. 2005.

Vol. 3768: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part II. XXVIII, 1088 pages. 2005.

Vol. 3767: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part I. XXVIII, 1022 pages. 2005.

Vol. 3766: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 231 pages. 2005.

Vol. 3765: Y. Liu, T. Jiang, C. Zhang (Eds.), Computer Vision for Biomedical Image Applications. X, 563 pages. 2005.

Vol. 3764: S. Tixeuil, T. Herman (Eds.), Self-Stabilizing Systems. VIII, 229 pages. 2005.

Vol. 3762: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops. XXXI, 1228 pages. 2005.

Vol. 3761: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part II. XXVII, 653 pages. 2005.

Vol. 3760: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part I. XXVII, 921 pages. 2005.

Vol. 3759: G. Chen, Y. Pan, M. Guo, J. Lu (Eds.), Parallel and Distributed Processing and Applications - ISPA 2005 Workshops. XIII, 669 pages. 2005.

Vol. 3758: Y. Pan, D.-x. Chen, M. Guo, J. Cao, J.J. Dongarra (Eds.), Parallel and Distributed Processing and Applications. XXIII, 1162 pages. 2005.

Vol. 3757: A. Rangarajan, B. Vemuri, A.L. Yuille (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. XII, 666 pages. 2005.

Vol. 3756: J. Cao, W. Nejdl, M. Xu (Eds.), Advanced Parallel Processing Technologies. XIV, 526 pages. 2005.

Vol. 3754: J. Dalmau Royo, G. Hasegawa (Eds.), Management of Multimedia Networks and Services. XII, 384 pages. 2005.

Vol. 3753: O.F. Olsen, L.M.J. Florack, A. Kuijper (Eds.), Deep Structure, Singularities, and Computer Vision. X, 259 pages. 2005.

Vol. 3752: N. Paragios, O. Faugeras, T. Chan, C. Schnörr (Eds.), Variational, Geometric, and Level Set Methods in Computer Vision. XI, 369 pages. 2005.

Vol. 3751: T. Magedanz, E.R. M. Madeira, P. Dini (Eds.), Operations and Management in IP-Based Networks. X, 213 pages. 2005.

Vol. 3750: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part II. XL, 1018 pages. 2005.

Vol. 3749: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part I. XXXIX, 942 pages. 2005.

Vol. 3748: A. Hartman, D. Kreische (Eds.), Model Driven Architecture – Foundations and Applications. IX, 349 pages. 2005.

Vol. 3747: C.A. Maziero, J.G. Silva, A.M.S. Andrade, F.M.d. Assis Silva (Eds.), Dependable Computing. XV, 267 pages. 2005.

Vol. 3746: P. Bozanis, E.N. Houstis (Eds.), Advances in Informatics. XIX, 879 pages. 2005.

Vol. 3745: J.L. Oliveira, V. Maojo, F. Martín-Sánchez, A.S. Pereira (Eds.), Biological and Medical Data Analysis. XII, 422 pages. 2005. (Subseries LNBI).

Vol. 3744: T. Magedanz, A. Karmouch, S. Pierre, I. Venieris (Eds.), Mobility Aware Technologies and Applications. XIV, 418 pages. 2005.

Vol. 3740: T. Srikanthan, J. Xue, C.-H. Chang (Eds.), Advances in Computer Systems Architecture. XVII, 833 pages. 2005.

Vol. 3739: W. Fan, Z.-h. Wu, J. Yang (Eds.), Advances in Web-Age Information Management. XXIV, 930 pages. 2005.

Vol. 3738: V.R. Syrotiuk, E. Chávez (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XI, 360 pages. 2005.

Vol. 3735: A. Hoffmann, H. Motoda, T. Scheffer (Eds.), Discovery Science. XVI, 400 pages. 2005. (Subseries LNAI).

Vol. 3734: S. Jain, H.U. Simon, E. Tomita (Eds.), Algorithmic Learning Theory. XII, 490 pages. 2005. (Subseries LNAI).

Vol. 3733: P. Yolum, T. Güngör, F. Gürgen, C. Özturan (Eds.), Computer and Information Sciences - ISCIS 2005. XXI, 973 pages. 2005.

Vol. 3731: F. Wang (Ed.), Formal Techniques for Networked and Distributed Systems - FORTE 2005. XII, 558 pages. 2005.

Vol. 3729: Y. Gil, E. Motta, V. R. Benjamins, M.A. Musen (Eds.), The Semantic Web – ISWC 2005. XXIII, 1073 pages. 2005.

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3726: L.T. Yang, O.F. Rana, B. Di Martino, J.J. Dongarra (Eds.), High Performance Computing and Communications. XXVI, 1116 pages. 2005.

Vol. 3725: D. Borrione, W. Paul (Eds.), Correct Hardware Design and Verification Methods. XII, 412 pages. 2005.

Vol. 3724: P. Fraigniaud (Ed.), Distributed Computing. XIV, 520 pages. 2005.

Vol. 3723: W. Zhao, S. Gong, X. Tang (Eds.), Analysis and Modelling of Faces and Gestures. XI, 4234 pages. 2005.

Vol. 3722: D. Van Hung, M. Wirsing (Eds.), Theoretical Aspects of Computing – ICTAC 2005. XIV, 614 pages. 2005.

Vol. 3721: A.M. Jorge, L. Torgo, P.B. Brazdil, R. Camacho, J. Gama (Eds.), Knowledge Discovery in Databases: PKDD 2005. XXIII, 719 pages. 2005. (Subseries LNAI).

Vol. 3720: J. Gama, R. Camacho, P.B. Brazdil, A.M. Jorge, L. Torgo (Eds.), Machine Learning: ECML 2005. XXIII, 769 pages. 2005. (Subseries LNAI).

Vol. 3719: M. Hobbs, A.M. Goscinski, W. Zhou (Eds.), Distributed and Parallel Computing. XI, 448 pages. 2005.

Vol. 3718: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XII, 502 pages. 2005.

Vol. 3717: B. Gramlich (Ed.), Frontiers of Combining Systems. X, 321 pages. 2005. (Subseries LNAI).

Vol. 3716: L. Delcambre, C. Kop, H.C. Mayr, J. Mylopoulos, Ó. Pastor (Eds.), Conceptual Modeling – ER 2005. XVI, 498 pages. 2005.

Vol. 3715: E. Dawson, S. Vaudenay (Eds.), Progress in Cryptology – Mycrypt 2005. XI, 329 pages. 2005.

Vol. 3714: H. Obbink, K. Pohl (Eds.), Software Product Lines. XIII, 235 pages. 2005.

Vol. 3713: L.C. Briand, C. Williams (Eds.), Model Driven Engineering Languages and Systems. XV, 722 pages. 2005.

Vol. 3712: R. Reussner, J. Mayer, J.A. Stafford, S. Overhage, S. Becker, P.J. Schroeder (Eds.), Quality of Software Architectures and Software Quality. XIII, 289 pages. 2005.

Vol. 3711: F. Kishino, Y. Kitamura, H. Kato, N. Nagata (Eds.), Entertainment Computing - ICEC 2005. XXIV, 540 pages. 2005.

Vol. 3710: M. Barni, I. Cox, T. Kalker, H.J. Kim (Eds.), Digital Watermarking. XII, 485 pages. 2005.

Vol. 3709: P. van Beek (Ed.), Principles and Practice of Constraint Programming - CP 2005. XX, 887 pages. 2005.

Table of Contents

Algebra and Number Theory

Multiparty Computation

Zero Knowledge and Secret Sharing

Information and Quantum Theory

Privacy and Anonymity

Cryptanalytic Techniques

Stream Cipher Cryptanalysis

Block Ciphers and Hash Functions

Bilinear Maps

Key Agreement

Provable Security

Signatures

Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log

Pascal Paillier[1] and Damien Vergnaud[2]

[1] Gemplus Card International, Advanced Cryptographic Services,
34, rue Guynemer, 92447 Issy-les-Moulineaux Cedex, France
pascal.paillier@gemplus.com
[2] Laboratoire de Mathématiques Nicolas Oresme,
Université de Caen, Campus II, B.P. 5186,
14032 Caen Cedex, France
vergnaud@math.unicaen.fr

Abstract. We provide evidence that the unforgeability of several discrete-log based signatures like Schnorr signatures cannot be equivalent to the discrete log problem in the standard model. This contradicts in nature well-known proofs standing in weakened proof methodologies, in particular proofs employing various formulations of the Forking Lemma in the random oracle Model. Our impossibility proofs apply to many discrete-log-based signatures like ElGamal signatures and their extensions, DSA, ECDSA and KCDSA as well as standard generalizations of these, and even RSA-based signatures like GQ. We stress that our work sheds more light on the provable (in)security of popular signature schemes but does not explicitly lead to actual attacks on these.

1 Introduction

It is striking to observe that after more that two decades of active research on the matter, the standard-model security of discrete-log based signatures like Schnorr, ElGamal or DSA remains mysteriously unknown. Although dedicated proof techniques do exist in weakened models (*e.g.* the random oracle model (ROM) [19,4,8] or the generic group model (GGM) [7]), none of them provides intuition about the actual security of discrete-log signatures. Even though they have withstood concerted cryptanalytic effort fairly well, we suspect that the real-life security of many of these signature schemes is actually weaker than expected. We provide evidence that most discrete-log-based signatures defined over some prime-order group $\mathbb{G}$ cannot be equivalent to extracting discrete logs over $\mathbb{G}$ in the standard model. Our results are partial in the sense that we disprove equivalence via *algebraic* reductions. In brief, algebraic reductions can only apply group operations on group elements. This restriction is not overly restrictive as we do not know any example of a cryptographic reduction which is not algebraic. Our results suggest that most discrete-log based signature schemes just cannot reach a maximal security level *i.e.* equivalence towards their primitive problem, or that if some of them do, it is through non-algebraic reductions exploiting intricate and subtle relations within the group $\mathbb{G}$.

B. Roy (Ed.): ASIACRYPT 2005, LNCS 3788, pp. 1–20, 2005.

Most interestingly, our work highlights a possible separation between the standard model and the random oracle model in which it is well-known that forging Schnorr signatures (for instance) is equivalent to extracting discrete logs. An interpretation is that random-oracle-based proofs leave unfair advantage to security reductions by probing and modifying the adversary's internal computations and thereby letting the random oracle play a crucial role that cannot be justified in real life. Previous works have observed similar separations in specific contexts [2,18].

The Fiat-Shamir paradigm of transforming identification schemes into digital signature schemes [13] is popular because it yields efficient protocols. However all known results for the security of Fiat-Shamir-transformed signature schemes like Schnorr take place in the ROM[1]. Even worse, they impose the loss of a factor nearly q_H (the number of queries the forger makes to the random oracle) in either execution time or success probability of reductions that convert a forger into an algorithm that extracts discrete logarithms. While no proof exists that the loss of this factor is necessary, the problem seems inherent to the way signature schemes are constructed from identification protocols.

We prove in this paper that any random-oracle-based reduction from computing discrete logarithms to forging Schnorr signatures *must* lose a factor at least $\sqrt{q_H}$. This shows that a proof of equivalence in the ROM, if algebraic, *will never be tight*. We believe our work gives a new perspective as to why no efficient proof of equivalence to the discrete log problem has ever been found for Schnorr signatures despite considerable research efforts.

We emphasize that although our work disproves that Schnorr, ElGamal, DSA, GQ, etc. are maximally secure, no actual attack or weakness of either of these signature schemes arises from our impossibility results. Nothing stated here refutes that forging signatures is likely to be intractable in practice.

1.1 Our Contributions

Our results are manyfold. Introducing a simple way to simulate forgeries, we are able to relate security properties of many signature schemes (Schnorr, (Meta) ElGamal, DSA[2], ECDSA, KCDSA, GQ) to *one-more* computational problems, in a positive or *negative* sense. In the positive sense, we prove the unbreakability of these signatures (meaning that the signing key cannot be recovered) under chosen-message attacks, thereby identifying security properties that have remained unknown for these schemes.

Starting from the same simulation technique, we show that no algebraic reduction can exist that would relate the unforgeability (under any kind of attacks) of these signatures to their primitive problem. This result is extendable to the

[1] It is known that the Fiat-Shamir transform provides a separation between the ROM and the standard model, see [14].

[2] Note that this work constitutes the first proper security analysis of DSA and ECDSA in the standard model. Previous to this work the only known security result on DSA schemes was that of Brown on ECDSA which assumed a generic group [7].