

Serge Vaudenay (Ed.)

LNCS 4004

Advances in Cryptology – EUROCRYPT 2006

24th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
St. Petersburg, Russia, May/June 2006, Proceedings



Springer

TN 918-53

T396.4

2006

Serge Vaudenay (Ed.)

Advances in Cryptology – EUROCRYPT 2006

24th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
St. Petersburg, Russia, May 28 – June 1, 2006
Proceedings



E200603607

 Springer

Volume Editor

Serge Vaudenay
EPFL, I&C, LASEC, Station 14
INF Building, 1015 Lausanne, Switzerland
E-mail: serge.vaudenay@epfl.ch

Library of Congress Control Number: 2006925895

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-34546-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34546-6 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© International Association for Cryptologic Research 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11761679 06/3142 5 4 3 2 1 0

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Preface

The 2006 edition of the Eurocrypt conference was held in St. Petersburg, Russia from May 28 to June 1, 2006. It was the 25th Eurocrypt conference. Eurocrypt is sponsored by the International Association for Cryptologic Research (IACR). Eurocrypt 2006 was chaired by Anatoly Lebedev, and I had the privilege to chair the Program Committee.

Eurocrypt collected 198 submissions on November 21, 2005. The Program Committee carried out a thorough review process. In total, 863 review reports were written by renowned experts, Program Committee members as well as external referees. Online discussions led to 1,114 additional discussion messages and about 1,000 emails. The review process was run using e-mail and the iChair software by Thomas Baignères and Matthieu Finiasz. Every submitted paper received at least three review reports. The Program Committee had a meeting in Lausanne on February 4, 2006. We selected 33 papers, notified acceptance or rejection to the authors, and had a cheese fondue. Authors were then invited to revise their submission. The present proceedings include all the revised papers. Due to time constraints the revised versions could not be reviewed again.

We delivered a “Eurocrypt Best Paper Award.” The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize excellence in the cryptographic research fields. Committee members were invited to nominate papers for this award. A poll then yielded a clear majority. This year, we were pleased to deliver the Eurocrypt Best Paper Award to Phong Q. Nguyen and Oded Regev for their brilliant paper “Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures.”

The Program Committee invited two speakers: David Naccache and Kevin McCurley. The current proceedings include papers about their presentation.

I would like to thank Anatoly Lebedev for organizing the conference. I would like to thank the IACR Board for honoring me by asking me to chair the Program Committee. The Program Committee and external reviewers worked extremely hard. I deeply thank them for this volunteer work. Acknowledgments also go to the authors of submitted papers, the speakers, and the invited speakers. I am grateful to Thomas Baignères and Matthieu Finiasz for their hard work developing the iChair software and constantly adding features. I also thank Shai Halevi and Amr Youssef, who participated in the software testing. Finally, I heartily thank Christine and Emilien, my family, for letting me spend some time on Eurocrypt.

This year, we celebrated the 30th anniversary of the publication of the Diffie-Hellman seminal paper “New Directions in Cryptography.” As cryptography was becoming a new academic research area, this pioneer paper invented public-key cryptography. My wish is that research in cryptography will lead us to 30 more years of fun.

March 2006

Serge Vaudenay
Lausanne

Eurocrypt 06

May 28–June 1, 2006, Saint Petersburg, Russia

General Chair

Anatoly Lebedev, LAN Crypto
Moscow, Russia

Program Chair

Serge Vaudenay, EPFL
Lausanne, Switzerland

Program Committee

Feng Bao	Institute for Infocomm Research
Eli Biham	Technion
Alex Biryukov	Katholieke Universiteit Leuven
Alexandra Boldyreva	Georgia Institute of Technology
Colin Boyd	Queensland University of Technology
Jean-Sébastien Coron	University of Luxembourg
Yevgeniy Dodis	New York University
Matt Franklin	University of California Davis
Eiichiro Fujisaki	NTT Laboratories
Juan Garay	Bell Labs — Lucent Technologies
Martin Hirt	ETH Zurich
Tetsu Iwata	Ibaraki University
Pil Joong Lee	Pohang University of Science and Technology
Antoine Joux	DGA and University of Versailles
Jonathan Katz	University of Maryland
Arjen Lenstra	Bell Labs – Lucent Technologies and Technische Universiteit Eindhoven
Helger Lipmaa	Cybernetica AS and University of Tartu
Javier Lopez	University of Malaga
Stefan Lucks	University of Mannheim
Philip MacKenzie	DoCoMo USA Labs
Mitsuru Matsui	Mitsubishi Electric
Alexander May	University of Paderborn
Willi Meier	FH Aargau
Atsuko Miyaji	JAIST
Kaisa Nyberg	Helsinki University of Technology and Nokia
Kenny Paterson	Royal Holloway University of London
Greg Rose	Qualcomm
Berry Schoenmakers	Technische Universiteit Eindhoven
Serge Vaudenay (Chair)	EPFL
Michael Wiener	Cryptographic Clarity
Robert Zuccherato	Entrust, Inc.

External Reviewers

Michel Abdalla	Nelly Fazio	Caroline Kudla
Masayuki Abe	Serge Fehr	Ulrich Kühn
Carlisle Adams	Matthieu Finiasz	Simon Künzli
Luis von Ahn	Marc Fischlin	Kaoru Kurosawa
Koichiro Akiyama	Matthias Fitzi	Tanja Lange
Elena Andreeva	Pierre-Alain Fouque	Joseph Lano
Kazumaro Aoki	Felix Freiling	Peeter Laud
Seigo Arita	Jun Furukawa	Sven Laur
Frederik Armknecht	Soichi Furuya	Jung Wook Lee
Tomoyuki Asano	Martin Gagne	Reynald Lercier
Gildas Avoine	Steven Galbraith	Christina Lindenberg
Thomas Baignères	David Galindo	Moses Liskov
Elad Barkan	Ran Gelles	Yi Lu
Don Beaver	Mark Gondree	Christoph Ludwig
Zuzana Beerliová	Daniel Gottesman	Anna Lysyanskaya
Mihir Bellare	Louis Goubin	Greg Maitland
Vicente Benjumea	Ignacio Gracia	John Malone-Lee
Dan Bernstein	Safuat Hamdy	Keith Martin
John Black	Goichiro Hanaoka	Sebastiá Martín
Daniel Bleichenbacher	Phil Hawkes	Natsume Matsuzaki
Johannes Blömer	Ryotaro Hayashi	Lorenz Minder
Jean Christian Boileau	Javier Herranz	Serge Mister
Xavier Boyen	Florian Hess	Payman Mohassel
Harry Buhrman	Shoichi Hirose	Jean Monnerat
Jan Camenisch	Dennis Hofheinz	Paz Morillo
Ran Canetti	Thomas Holenstein	Tim Moses
Juyoung Cha	Nick Howgrave-Graham	Siguna Mueller
Liqun Chen	Yong Ho Hwang	Frederic Muller
Rafi Chen	Yuval Ishai	Sean Murphy
Kookrae Cho	Stanislaw Jarecki	Toru Nakanishi
Sherman Chow	Jorge Jiménez	Deholo Nali
Carlos Cid	Ellen Jochemsz	Anderson Nascimento
Scott Contini	Pascal Junod	Gregory Neven
Yang Cui	Senny Kamara	Phong Nguyen
Reza Curtmola	Akinori Kawachi	Antonio Nicolosi
Ivan Damgård	John Kelsey	Jesper Nielsen
Vanesa Daza	Aggelos Kiayias	Wakaha Ogata
Alex Dent	Joe Killian	Kazuo Ohta
Claus Diem	Mehmet Kiraz	Koji Okada
Yan Zong Ding	Kazukuni Kobara	Takeshi Okamoto
Martin Döring	Vladimir Kolesnikov	Tatsuaki Okamoto
Orr Dunkelman	Chiu-Yuen Koo	Rafail Ostrovsky
Stefan Dziembowski	Matthias Krause	Raphael Overbeck
Daniela Engelbert	Volker Krummel	Michael Paddon

Carles Padro
Adriana Palacio
Saurabh Panjwani
Jung Hyung Park
Sylvain Pasini
Kun Peng
Rene Peralta
Adrian Perrig
Giuseppe Persiano
Krzysztof Pietrzak
Benny Pinkas
Bart Preneel
Bartosz Przydatek
Prashant Puniya
Carla Rafols
Dominik Raub
Omer Reingold
German Saez
Yasuyuki Sakai
Bagus Santoso
Hovav Schaham
Daniel Schepers
Katja Schmidt-Samoa
Jasper Scholten
Jae Woo Seo
Ji Sun Shin

Jong Hoon Shin
Tom Shrimpton
Andrey Sidorenko
Johan Sjödin
Nigel Smart
Adam Smith
Clayton Smith
Miguel Soriano
Masakazu Soshi
Martijn Stam
Heiko Stamer
Dirk Stegemann
Ron Steinfeld
Daisuke Suzuki
Koutarou Suzuki
Mitsuru Tada
Katsuyuki Takashima
Keisuke Tanaka
Lauri Tarkkala
Tamir Tassa
Isamu Teranishi
Stefano Tessaro
Toyohiro Tsurumaru
Pim Tuyls
Shigenori Uchiyama
Maribel Vasco

Frederik Vercauteren
Jorge L. Villar
Ulrich Vollmer
Martin Vuagnoux
Shabsi Walfish
Johan Wallén
Guilin Wang
Yongge Wang
Bogdan Warinschi
Benne de Weger
Ralf-Philipp Weinmann
William Whyte
Christopher Wolf
Stefan Wolf
Yongdong Wu
Jürg Wullschleger
Alex Yampolskiy
Ke Yang
Yeon Hyeong Yang
Yiqun Lisa Yin
Shoko Yonezawa
Dae Hyun Yum
Yunlei Zhao
Huafei Zhu

Lecture Notes in Computer Science

For information about Vols. 1–3899

please contact your bookseller or Springer

Vol. 4004: S. Vaudenay (Ed.), *Advances in Cryptology - EUROCRYPT 2006*. XIV, 613 pages. 2006.

Vol. 3998: T. Calamoneri, I. Finocchi, G.F. Italiano (Eds.), *Algorithms and Complexity*. XII, 394 pages. 2006.

Vol. 3994: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), *Computational Science - ICCS 2006*, Part IV. XXIX, 1094 pages. 2006.

Vol. 3993: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), *Computational Science - ICCS 2006*, Part III. XXX, 1138 pages. 2006.

Vol. 3992: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), *Computational Science - ICCS 2006*, Part II. XXIX, 1121 pages. 2006.

Vol. 3991: V.N. Alexandrov, G.D. van Albada, P.M.A. Sloot, J. Dongarra (Eds.), *Computational Science - ICCS 2006*, Part I. CCXX, 1090 pages. 2006.

Vol. 3990: J. C. Beck, B.M. Smith (Eds.), *Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems*. X, 301 pages. 2006.

Vol. 3987: M. Hazas, J. Krumm, T. Strang (Eds.), *Location- and Context-Awareness*. X, 289 pages. 2006.

Vol. 3986: K. Stølen, W.H. Winsborough, F. Martinelli, F. Massacci (Eds.), *Trust Management*. XIV, 474 pages. 2006.

Vol. 3984: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part V. XXV, 1045 pages. 2006.

Vol. 3983: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part IV. XXVI, 1191 pages. 2006.

Vol. 3982: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part III. XXV, 1243 pages. 2006.

Vol. 3981: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part II. XXVI, 1255 pages. 2006.

Vol. 3980: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part I. LXXV, 1199 pages. 2006.

Vol. 3979: T.S. Huang, N. Sebe, M.S. Lew, V. Pavlović, M. Kölsch, A. Galata, B. Kisačanin (Eds.), *Computer Vision in Human-Computer Interaction*. XII, 121 pages. 2006.

Vol. 3978: B. Hnich, M. Carlsson, F. Fages, F. Rossi (Eds.), *Recent Advances in Constraints*. VIII, 179 pages. 2006. (Sublibrary LNAI).

Vol. 3976: F. Boavida, T. Plagemann, B. Stiller, C. Westphal, E. Monteiro (Eds.), *Networking 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems*. XXVI, 1276 pages. 2006.

Vol. 3975: S. Mehrotra, D.D. Zeng, H. Chen, B. Thuraisingham, F.Y. Wang (Eds.), *Intelligence and Security Informatics*. XXII, 772 pages. 2006.

Vol. 3970: T. Braun, G. Carle, S. Fahmy, Y. Koucheryavy (Eds.), *Wired/Wireless Internet Communications*. XIV, 350 pages. 2006.

Vol. 3968: K.P. Fishkin, B. Schiele, P. Nixon, A. Quigley (Eds.), *Pervasive Computing*. XV, 402 pages. 2006.

Vol. 3967: D. Grigoriev, J. Harrison, E.A. Hirsch (Eds.), *Computer Science - Theory and Applications*. XVI, 684 pages. 2006.

Vol. 3966: Q. Wang, D. Pfahl, D.M. Raffo, P. Wernick (Eds.), *Software Process Change*. XIV, 356 pages. 2006.

Vol. 3965: M. Bernardo, A. Cimatti (Eds.), *Formal Methods for Hardware Verification*. VII, 243 pages. 2006.

Vol. 3964: M. Ü. Uyar, A.Y. Duale, M.A. Fecko (Eds.), *Testing of Communicating Systems*. XI, 373 pages. 2006.

Vol. 3962: W. IJsselstein, Y. de Kort, C. Midden, B. Eggen, E. van den Hoven (Eds.), *Persuasive Technology*. XII, 216 pages. 2006.

Vol. 3960: R. Vieira, P. Quaresma, M.d.G.V. Nunes, N.J. Mamede, C. Oliveira, M.C. Dias (Eds.), *Computational Processing of the Portuguese Language*. XII, 274 pages. 2006. (Sublibrary LNAI).

Vol. 3959: J.-Y. Cai, S. B. Cooper, A. Li (Eds.), *Theory and Applications of Models of Computation*. XV, 794 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T. Malkin (Eds.), *Public Key Cryptography - PKC 2006*. XIV, 543 pages. 2006.

Vol. 3956: G. Barthe, B. Gregoire, M. Huisman, J.-L. Lanet (Eds.), *Construction and Analysis of Safe, Secure, and Interoperable Smart Devices*. IX, 175 pages. 2006.

Vol. 3955: G. Antoniou, G. Potamias, C. Spyropoulos, D. Plexousakis (Eds.), *Advances in Artificial Intelligence*. XVII, 611 pages. 2006. (Sublibrary LNAI).

Vol. 3954: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision - ECCV 2006*, Part IV. XVII, 613 pages. 2006.

Vol. 3953: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision - ECCV 2006*, Part III. XVII, 649 pages. 2006.

Vol. 3952: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision - ECCV 2006*, Part II. XVII, 661 pages. 2006.

- Vol. 3951: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision – ECCV 2006, Part I*. XXXV, 639 pages. 2006.
- Vol. 3950: J.P. Müller, F. Zambonelli (Eds.), *Agent-Oriented Software Engineering VI*. XVI, 249 pages. 2006.
- Vol. 3947: Y.-C. Chung, J.E. Moreira (Eds.), *Advances in Grid and Pervasive Computing*. XXI, 667 pages. 2006.
- Vol. 3946: T.R. Roth-Berghofer, S. Schulz, D.B. Leake (Eds.), *Modeling and Retrieval of Context*. XI, 149 pages. 2006. (Sublibrary LNAI).
- Vol. 3945: M. Hagiya, P. Wadler (Eds.), *Functional and Logic Programming*. X, 295 pages. 2006.
- Vol. 3944: J. Quiñero-Candela, I. Dagan, B. Magnini, F. d'Alché-Buc (Eds.), *Machine Learning Challenges*. XIII, 462 pages. 2006. (Sublibrary LNAI).
- Vol. 3943: N. Guelfi, A. Savidis (Eds.), *Rapid Integration of Software Engineering Techniques*. X, 289 pages. 2006.
- Vol. 3942: Z. Pan, R. Aylett, H. Diener, X. Jin, S. Göbel, L. Li (Eds.), *Technologies for E-Learning and Digital Entertainment*. XXV, 1396 pages. 2006.
- Vol. 3941: S.W. Gilroy, M.D. Harrison (Eds.), *Interactive Systems*. XI, 267 pages. 2006.
- Vol. 3940: C. Saunders, M. Grobelnik, S. Gunn, J. Shawe-Taylor (Eds.), *Subspace, Latent Structure and Feature Selection*. X, 209 pages. 2006.
- Vol. 3939: C. Priami, L. Cardelli, S. Emmott (Eds.), *Transactions on Computational Systems Biology IV*. VII, 141 pages. 2006. (Sublibrary LNBI).
- Vol. 3936: M. Lalmas, A. MacFarlane, S. Rüger, A. Tombros, T. Tsikrika, A. Yavlinsky (Eds.), *Advances in Information Retrieval*. XIX, 584 pages. 2006.
- Vol. 3935: D. Won, S. Kim (Eds.), *Information Security and Cryptology - ICISC 2005*. XIV, 458 pages. 2006.
- Vol. 3934: J.A. Clark, R.F. Paige, F.A. C. Polack, P.J. Brooke (Eds.), *Security in Pervasive Computing*. X, 243 pages. 2006.
- Vol. 3933: F. Bonchi, J.-F. Boulicaut (Eds.), *Knowledge Discovery in Inductive Databases*. VIII, 251 pages. 2006.
- Vol. 3931: B. Apolloni, M. Marinaro, G. Nicosia, R. Tagliaferri (Eds.), *Neural Nets*. XIII, 370 pages. 2006.
- Vol. 3930: D.S. Yeung, Z.-Q. Liu, X.-Z. Wang, H. Yan (Eds.), *Advances in Machine Learning and Cybernetics*. XXI, 1110 pages. 2006. (Sublibrary LNAI).
- Vol. 3929: W. MacCaull, M. Winter, I. Düntsch (Eds.), *Relational Methods in Computer Science*. VIII, 263 pages. 2006.
- Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), *Smart Card Research and Advanced Applications*. XI, 359 pages. 2006.
- Vol. 3927: J. Hespanha, A. Tiwari (Eds.), *Hybrid Systems: Computation and Control*. XII, 584 pages. 2006.
- Vol. 3925: A. Valmari (Ed.), *Model Checking Software*. X, 307 pages. 2006.
- Vol. 3924: P. Sestoft (Ed.), *Programming Languages and Systems*. XII, 343 pages. 2006.
- Vol. 3923: A. Mycroft, A. Zeller (Eds.), *Compiler Construction*. XIII, 277 pages. 2006.
- Vol. 3922: L. Baresi, R. Heckel (Eds.), *Fundamental Approaches to Software Engineering*. XIII, 427 pages. 2006.
- Vol. 3921: L. Aceto, A. Ingólfssdóttir (Eds.), *Foundations of Software Science and Computation Structures*. XV, 447 pages. 2006.
- Vol. 3920: H. Hermanns, J. Palsberg (Eds.), *Tools and Algorithms for the Construction and Analysis of Systems*. XIV, 506 pages. 2006.
- Vol. 3918: W.K. Ng, M. Kitsuregawa, J. Li, K. Chang (Eds.), *Advances in Knowledge Discovery and Data Mining*. XXIV, 879 pages. 2006. (Sublibrary LNAI).
- Vol. 3917: H. Chen, F.Y. Wang, C.C. Yang, D. Zeng, M. Chau, K. Chang (Eds.), *Intelligence and Security Informatics*. XII, 186 pages. 2006.
- Vol. 3916: J. Li, Q. Yang, A.-H. Tan (Eds.), *Data Mining for Biomedical Applications*. VIII, 155 pages. 2006. (Sublibrary LNBI).
- Vol. 3915: R. Nayak, M.J. Zaki (Eds.), *Knowledge Discovery from XML Documents*. VIII, 105 pages. 2006.
- Vol. 3914: A. Garcia, R. Choren, C. Lucena, P. Giorgini, T. Holvoet, A. Romanovsky (Eds.), *Software Engineering for Multi-Agent Systems IV*. XIV, 255 pages. 2006.
- Vol. 3911: R. Wyrzykowski, J. Dongarra, N. Meyer, J. Waśniewski (Eds.), *Parallel Processing and Applied Mathematics*. XXIII, 1126 pages. 2006.
- Vol. 3910: S.A. Brueckner, G.D.M. Serugendo, D. Hales, F. Zambonelli (Eds.), *Engineering Self-Organising Systems*. XII, 245 pages. 2006. (Sublibrary LNAI).
- Vol. 3909: A. Apostolico, C. Guerra, S. Istrail, P. Pevzner, M. Waterman (Eds.), *Research in Computational Molecular Biology*. XVII, 612 pages. 2006. (Sublibrary LNBI).
- Vol. 3908: A. Bui, M. Bui, T. Böhme, H. Unger (Eds.), *Innovative Internet Community Systems*. VIII, 207 pages. 2006.
- Vol. 3907: F. Rothlauf, J. Branke, S. Cagnoni, E. Costa, C. Cotta, R. Drechsler, E. Lutton, P. Machado, J.H. Moore, J. Romero, G.D. Smith, G. Squillero, H. Takagi (Eds.), *Applications of Evolutionary Computing*. XXIV, 813 pages. 2006.
- Vol. 3906: J. Gottlieb, G.R. Raidl (Eds.), *Evolutionary Computation in Combinatorial Optimization*. XI, 293 pages. 2006.
- Vol. 3905: P. Collet, M. Tomassini, M. Ebner, S. Gustafson, A. Ékár (Eds.), *Genetic Programming*. XI, 361 pages. 2006.
- Vol. 3904: M. Baldoni, U. Endriss, A. Omicini, P. Torroni (Eds.), *Declarative Agent Languages and Technologies III*. XII, 245 pages. 2006. (Sublibrary LNAI).
- Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), *Information Security Practice and Experience*. XIV, 392 pages. 2006.
- Vol. 3902: R. Kronland-Martinet, T. Voinier, S. Ystad (Eds.), *Computer Music Modeling and Retrieval*. XI, 275 pages. 2006.
- Vol. 3901: P.M. Hill (Ed.), *Logic Based Program Synthesis and Transformation*. X, 179 pages. 2006.
- Vol. 3900: F. Toni, P. Torroni (Eds.), *Computational Logic in Multi-Agent Systems*. XVII, 427 pages. 2006. (Sublibrary LNAI).

Author Index

- Almansa, Jesús F. 593
Armknacht, Frederik 147
Bellare, Mihir 409
Berbain, Côme 109
Boneh, Dan 573
Boyen, Xavier 427
Carlet, Claude 147
Chang, Ee-Chien 59
Cheon, Jung Hee 1
Contini, Scott 165
Crépeau, Claude 201, 538
Damgård, Ivan 555, 593
Dent, Alexander W. 289
Dupont, Kasper 555
Dwork, Cynthia 486
Faugère, Jean-Charles 30
Gaborit, Philippe 147
Gama, Nicolas 233
Gentry, Craig 445
Gilbert, Henri 109
Gouget, Aline 129
Gratzer, Vanessa 48
Groth, Jens 339
Hofheinz, Dennis 504
Howgrave-Graham, Nick 233
Ishai, Yuval 308
Joux, Antoine 254
Katz, Jonathan 73
Kelsey, John 183
Kenthapadi, Krishnam 486
Kohno, Tadayoshi 183
Künzli, Simon 147
Lenstra, Arjen K. 165
Lercier, Reynald 254
Li, Qiming 59
Lu, Steve 465
Maurer, Ueli 391
McCurley, Kevin S. 359
McSherry, Frank 486
Meier, Willi 147
Mironov, Ilya 486
Moran, Tal 88
Müller-Quade, Jörn 504
Naccache, David 48
Naor, Moni 88, 486
Nguyen, Phong Q. 233, 271
Nielsen, Jesper Buus 593
Østergaard Pedersen, Michael 555
Ostrovsky, Rafail 339, 465
Oswald, Yvonne Anne 391
Patarin, Jacques 109
Paterson, Kenneth G. 12
Perret, Ludovic 30
Pietrzak, Krzysztof 328, 391
Prabhakaran, Manoj 308
Regev, Oded 271
Rogaway, Phillip 373, 409
Ruatta, Olivier 147
Sahai, Amit 308, 339, 465, 573
Savvides, George 201, 538
Schaffner, Christian 538
Schoenmakers, Berry 522
Shacham, Hovav 465
Shin, Ji Sun 73
Shrimpton, Thomas 373
Sibert, Hervé 129
Sjödín, Johan 391
Steinfeld, Ron 165
Tuyls, Pim 522
Unruh, Dominique 504
Wagner, David 308
Waters, Brent 427, 465, 573
Wolf, Stefan 222
Wullschlegel, Jürg 222, 538
Yau, Arnold K.L. 12

Table of Contents

Cryptanalysis

Security Analysis of the Strong Diffie-Hellman Problem <i>Jung Hee Cheon</i>	1
Cryptography in Theory and Practice: The Case of Encryption in IPsec <i>Kenneth G. Paterson, Arnold K.L. Yau</i>	12
Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects <i>Jean-Charles Faugère, Ludovic Perret</i>	30

Invited Talk I

Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt <i>Vanessa Gratzner, David Naccache</i>	48
--	----

Cryptography Meets Humans

Hiding Secret Points Amidst Chaff <i>Ee-Chien Chang, Qiming Li</i>	59
Parallel and Concurrent Security of the HB and HB ⁺ Protocols <i>Jonathan Katz, Ji Sun Shin</i>	73
Polling with Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol <i>Tal Moran, Moni Naor</i>	88

Stream Ciphers

QUAD: A Practical Stream Cipher with Provable Security <i>Côme Berbain, Henri Gilbert, Jacques Patarin</i>	109
How to Strengthen Pseudo-random Generators by Using Compression <i>Aline Gouget, Hervé Sibert</i>	129

Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks <i>Frederik Armknecht, Claude Carlet, Philippe Gaborit, Simon Künzli, Willi Meier, Olivier Ruatta</i>	147
---	-----

Hash Functions

VSH, an Efficient and Provable Collision-Resistant Hash Function <i>Scott Contini, Arjen K. Lenstra, Ron Steinfeld</i>	165
Herdin Hash Functions and the Nostradamus Attack <i>John Kelsey, Tadayoshi Kohno</i>	183

Oblivious Transfer

Optimal Reductions Between Oblivious Transfers Using Interactive Hashing <i>Claude Crépeau, George Savvides</i>	201
Oblivious Transfer Is Symmetric <i>Stefan Wolf, Jürg Wullschleger</i>	222

Numbers and Lattices

Symplectic Lattice Reduction and NTRU <i>Nicolas Gama, Nick Howgrave-Graham, Phong Q. Nguyen</i>	233
The Function Field Sieve in the Medium Prime Case <i>Antoine Joux, Reynald Lercier</i>	254
Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures <i>Phong Q. Nguyen, Oded Regev</i>	271

Foundations

The Cramer-Shoup Encryption Scheme Is Plaintext Aware in the Standard Model <i>Alexander W. Dent</i>	289
Private Circuits II: Keeping Secrets in Tamperable Circuits <i>Yuval Ishai, Manoj Prabhakaran, Amit Sahai, David Wagner</i>	308

Composition Implies Adaptive Security in Minicrypt <i>Krzysztof Pietrzak</i>	328
Perfect Non-interactive Zero Knowledge for NP <i>Jens Groth, Rafail Ostrovsky, Amit Sahai</i>	339

Invited Talk II

Language Modeling and Encryption on Packet Switched Networks <i>Kevin S. McCurley</i>	359
--	-----

Block Ciphers

A Provable-Security Treatment of the Key-Wrap Problem <i>Phillip Rogaway, Thomas Shrimpton</i>	373
Luby-Rackoff Ciphers from Weak Round Functions? <i>Ueli Maurer, Yvonne Anne Oswald, Krzysztof Pietrzak, Johan Sjödin</i>	391
The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs <i>Mihir Bellare, Phillip Rogaway</i>	409

Cryptography Without Random Oracles

Compact Group Signatures Without Random Oracles <i>Xavier Boyen, Brent Waters</i>	427
Practical Identity-Based Encryption Without Random Oracles <i>Craig Gentry</i>	445
Sequential Aggregate Signatures and Multisignatures Without Random Oracles <i>Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, Brent Waters</i>	465

Multiparty Computation

Our Data, Ourselves: Privacy Via Distributed Noise Generation <i>Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, Moni Naor</i>	486
---	-----

On the (Im-)Possibility of Extending Coin Toss
 Dennis Hofheinz, Jörn Müller-Quade, Dominique Unruh 504

Efficient Binary Conversion for Paillier Encrypted Values
 Berry Schoenmakers, Pim Tuyls 522

Information-Theoretic Conditions for Two-Party Secure Function
Evaluation
 Claude Crépeau, George Savvides, Christian Schaffner,
 Jürg Wullschlegler 538

Cryptography for Groups

Unclonable Group Identification
 Ivan Damgård, Kasper Dupont, Michael Østergaard Pedersen 555

Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and
Private Keys
 Dan Boneh, Amit Sahai, Brent Waters 573

Simplified Threshold RSA with Adaptive and Proactive Security
 Jesús F. Almansa, Ivan Damgård, Jesper Buus Nielsen 593

Author Index 613

Security Analysis of the Strong Diffie-Hellman Problem

Jung Hee Cheon

ISaC and Dept. of Mathematics, Seoul National University, Republic of Korea

jhcheon@snu.ac.kr

<http://www.math.snu.ac.kr/~jhcheon>

Abstract. Let g be an element of prime order p in an abelian group and $\alpha \in \mathbb{Z}_p$. We show that if g, g^α , and g^{α^d} are given for a positive divisor d of $p - 1$, we can compute the secret α in $O(\log p \cdot (\sqrt{p/d} + \sqrt{d}))$ group operations using $O(\max\{\sqrt{p/d}, \sqrt{d}\})$ memory. If g^{α^i} ($i = 0, 1, 2, \dots, d$) are provided for a positive divisor d of $p + 1$, α can be computed in $O(\log p \cdot (\sqrt{p/d} + d))$ group operations using $O(\max\{\sqrt{p/d}, \sqrt{d}\})$ memory. This implies that the strong Diffie-Hellman problem and its related problems have computational complexity reduced by $O(\sqrt{d})$ from that of the discrete logarithm problem for such primes.

Further we apply this algorithm to the schemes based on the Diffie-Hellman problem on an abelian group of prime order p . As a result, we reduce the complexity of recovering the secret key from $O(\sqrt{p})$ to $O(\sqrt{p/d})$ for Boldyreva's blind signature and the original ElGamal scheme when $p - 1$ (resp. $p + 1$) has a divisor $d \leq p^{1/2}$ (resp. $d \leq p^{1/3}$) and d signature or decryption queries are allowed.

Keywords: Discrete logarithm, Diffie-Hellman, strong Diffie-Hellman, ElGamal encryption, blind signature.

1 Introduction

Let g be an element of prime order p in an abelian group and $\alpha \in \mathbb{Z}_p$. The ℓ -Strong Diffie-Hellman (ℓ -SDH) problem asks to find $g^{\alpha^{\ell+1}}$ given $g, g^\alpha, \dots, g^{\alpha^\ell}$. Recently, many cryptographic schemes including encryption, signature, and key management schemes are proposed on the basis of the Strong Diffie-Hellman (SDH) problem [MSK02, BB04e, BB04s], or its variants such as the Bilinear Diffie-Hellman problem [BBS04, DY05] and the Bilinear Diffie-Hellman Exponent (BDHE) problem [BBG05, BGW05]. A lower bound on the computational complexity of the SDH problem or its variants for generic groups are known in the sense of Shoup [Sho97], but it does not guarantee the security for specific parameters.

In this paper, we analyze the security of the SDH problem. More precisely, we show that if g, g^α and g^{α^d} are given for a positive divisor d of $p - 1$, the secret $\alpha \in \mathbb{Z}_p$ can be computed in $O(\log p \cdot (\sqrt{p/d} + \sqrt{d}))$ group operations using $O(\max\{\sqrt{p/d}, \sqrt{d}\})$ memory. If g^{α^i} ($i = 0, 1, 2, \dots, d$) are provided for a positive

divisor d of $p + 1$, it can be computed in $O(\log p \cdot (\sqrt{p/d} + d))$ group operations using the same size of memory. This implies that the strong Diffie-Hellman problem and its related problems have computational complexity reduced by $O(\sqrt{d})$ from that of the discrete logarithm problem for such primes. Hence it is necessary to increase by the size of d the key size of the cryptographic schemes based on the ℓ -SDH problem or its variants if the base group has such a prime as its order.

We investigate some known elliptic curve parameters and find that either $p - 1$ or $p + 1$ has many small divisors for the largest prime divisor p of its order for each elliptic curve in [NIST, BLS01, KM05, MIRACL]. For example, if we use the curve E^+ over $GF(3^{155})$ [BLS01] for the broadcast encryption [BGW05], the secret key can be computed in $O(2^{59})$ exponentiations (resp. $O(2^{42})$ exponentiations) when the number of users is 2^{32} (resp. 2^{64}), rather than $O(2^{76})$ group operations.

Moreover, we apply this algorithm to the schemes based on the Diffie-Hellman problem on an abelian group of prime order p . As a result, we show the complexity of recovering the secret key is reduced from $O(\sqrt{p})$ to $O(\sqrt{p/d})$ for Boldyreva's blind signatures [Bol03] when d signature or decryption queries are allowed and $p - 1$ has a divisor $d \leq p^{1/2}$ or $p + 1$ has a divisor $d \leq p^{1/3}$. Similar results hold for the original ElGamal scheme [ElG85] with decryption oracles and the conference keying protocol by Burmester-Desmedt [BD94] with key issuing oracles.

The rest of the paper is organized as follows: In Section 2, we introduce the SDH related problems and some schemes based on them. In Section 3, we present our algorithms. In Section 4, we exploit our algorithms to attack several protocols based on the Diffie-Hellman problem. In Section 5, we investigate some known elliptic curve parameters in order to check if our algorithms are applicable for these parameters. We conclude in Section 6.

2 Strong Diffie-Hellman Problems and Their Variants

Let G be an abelian group of prime order p and g a generator of G . The **Discrete Logarithm (DL) Problem** in G asks to find $a \in \mathbb{Z}_p$ given g and g^a in G . Many cryptosystems are designed on the basis of the DL problem, but most of them have the security equivalent to a weaker variant of the DL problem rather than the DL problem itself. Two most important weaker variants are as follows:

The Computation Diffie-Hellman (CDH) Problem. Given (g, g^a, g^b) , compute g^{ab} .

The Decisional Diffie-Hellman (DDH) Problem. Given (g, g^a, g^b, g^c) , decide whether $c = ab$ in $\mathbb{Z}_p$.

Recently, some weakened variants of the CDH problem are introduced and being used to construct cryptosystems for various functionalities or security without random oracles. One characteristic of these problems is to disclose $g, g^\alpha, \dots, g^{\alpha^\ell}$ for the secret α and some integer ℓ .