Rana Barua
Tanja Lange (Eds.)

LNCS 4329

Progress in Cryptology – INDOCRYPT 2006

7th International Conference on Cryptology in India
Kolkata, India, December 2006
Proceedings

Springer

Rana Barua Tanja Lange (Eds.)

Progress in Cryptology – INDOCRYPT 2006

7th International Conference on Cryptology in India
Kolkata, India, December 11-13, 2006
Proceedings

Springer

Volume Editors

Rana Barua
Indian Statistical Institute
Division of Theoretical Statistics and Mathematics
Kolkata, India
E-mail: rana@isical.ac.in

Tanja Lange
Eindhoven University of Technology
Department of Mathematics and Computer Science
Eindhoven, Netherlands
E-mail: tanja@hyperelliptic.org

Library of Congress Control Number: 2006937160

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, K.4, F.2.1-2, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-49767-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49767-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11941378 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4329

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

Editorial Board

Preface

Indocrypt 2006, the 7th International Conference on Cryptology in India, took place December 11-13, 2006 in Kolkata, India. As in previous years, it was organized by the Cryptology Research Society of India, and the General Chair Bimal Roy did an excellent job in keeping all strands together by ensuring an excellent collaboration between the local organizers and the Program Committee and making the conference memorable for the talks and the social program.

Two invited lectures were presented at Indocrypt 2006: James L. Massey spoke about *Whither Cryptography?* and Alfred J. Menezes presented *Another Look at "Provable Security". II*, which is a joint work with Neal Koblitz.

The submission deadline for Indocrypt was on August 18 and we received 186 submissions. To give the authors maximal time to modify their papers and at the same time guarantee the maximal review time for the Program Committee, we had separate submission and revision deadlines. After the submission deadline it was no longer possible to submit a new paper and so the PC members could enter the selection phase during which they only got to see the abstracts of the papers. Out of the 186 papers originally submitted, 20 were withdrawn before the revision deadline on August 21 and 81 were revised at least once. Our experience with this approach of separating the deadlines was entirely positive. We would also like to take this opportunity to thank the developers of iChair, Thomas Baignéres and Matthieu Finiasz at EPFL, for making iChair available and for answering several questions which allowed us to extend the functionality of iChair to handle separate deadlines. The software was very useful for the submission process, the collection of reviews, and the discussion.

The Program Committee did a remarkable job of finishing refereeing almost all papers by September 8, even though 166 papers marked a new record in submissions. In the following discussion phase many more reports were added and the Program Committee worked intensively to gain confidence in its decisions. The 39 Program Committee members produced 422 comments during the 2 weeks of discussion. It is our pleasure to thank all Program Committee members for their very timely and concentrated effort that allowed us to notify the authors on time on September 22 and even send out the comments the same day.

Finally, we would like to thank all authors for submitting interesting new research papers to Indocrypt, providing us with an embarrassment of riches out of which we could only accept 29 contributed papers, even though many more would have been worth publishing. It is a pleasure to see Indocrypt being a well-accepted cryptography conference where fresh results are submitted.

December 2006

Rana Barua and Tanja Lange
Program Chairs, Indocrypt 2006

Organization

Indocrypt 2006 was organized by the Indian Statistical Institute, Kolkata, in collaboration with the Cryptology Research Society of India.

General Chair

Bimal Roy	Indian Statistical Institute, Kolkata, India

Local Organizers

Sumanta Sarkar	Indian Statistical Institute, Kolkata, India
Somitra Sanadhya	Indian Statistical Institute, Kolkata, India
Susmita Ruj	Indian Statistical Institute, Kolkata, India
Siddheswar Rathi	Indian Statistical Institute, Kolkata, India
Snehashis Mukherjee	Indian Statistical Institute, Kolkata, India
Kuntal Ghosh	Indian Statistical Institute, Kolkata, India
Amitava Sinha	Indian Statistical Institute, Kolkata, India
Mahabir Prasad	Indian Statistical Institute, Kolkata, India
Deepak Kumar Dalai	Indian Institute of Science Education and Research, Kolkata, India
Sanjit Chatterjee	Indian Institute of Science Education and Research, Kolkata, India
Subhomay Maitra	Indian Statistical Institute, India
Goutam Paul	Jadavpur University, Kolkata, India
Pinaki Sarkar	Jadavpur University, Kolkata, India

Program Chairs

Rana Barua	Indian Statistical Institute, Kolkata, India
Tanja Lange	Technical University of Denmark and Eindhoven Technical University, Netherlands

Program Committee

Michel Abdalla	Ecole Normale Supérieure and CNRS, France
Roberto M. Avanzi	Ruhr University Bochum, Germany
Paulo Barreto	University of Saõ Paulo, Brazil
Daniel J. Bernstein	University of Illinois at Chicago, USA

Colin Boyd	Queensland University of Technology, Australia
Anne Canteaut	INRIA Rocquencourt, France
Claude Carlet	University of Paris 8, France
Yvo Desmedt	University College London, UK
Orr Dunkelman	Technion - Israel Institute of Technology, Israel
Krishnan Gopalakrishnan	East Carolina University, USA
Kishan C. Gupta	University of Waterloo, Canada
Tom Høholdt	Technical University of Denmark, Denmark
Jin Hong	Seoul National University, Korea
Laurent Imbert	LIRMM, CRNS, France
Tetsu Iwata	Nagoya University, Japan
Antoine Joux	DGA and Université de Versailles Saint-Quentin-en-Yvelines, France
Marc Joye	Thomson R&D France, France
Charanjit Jutla	IBM T.J. Watson Research Center, USA
Chi Sung Laih	National Cheng Kung University, Taiwan
Kerstin Lemke-Rust	Ruhr University Bochum, Germany
C.E. Veni Madhavan	Indian Institute of Science, Bangalore, India
John Malone-Lee	UK
Pradeep Kumar Mishra	University of Calgary, Canada
Gregory Neven	Katholieke Universiteit Leuven, Belgium and Ecole Normale Supérieure, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium
C. Pandu Rangan	Department of Computer Science and Engineering, IIT Madras, India
Bimal Roy	Indian Statistical Institute, Kolkata, India
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Rei Safavi-Naini	University of Wollongong, Australia
Pramod K. Saxena	Scientific Analysis Group, Delhi, India
Jennifer Seberry	University of Wollongong, Australia
Nicolas Sendrier	INRIA Rocquencourt, France
Nigel Smart	University of Bristol, UK
Martijn Stam	EPFL, Switzerland
Bo-Yin Yang	Academia Sinica, Taiwan
Melek D. Yücel	Middle East Technical University, Turkey
Jianying Zhou	Institute for Infocomm Research, Singapore

Referees

Andre Adelsbach	Daniel Augot	Jean-Claude Bajard
Andris Ambainis	Joonsang Baek	Lejla Batina

S.S. Bedi
Peter Birkner
Carlo Blundo
Jean Christian Boileau
Alexandra Boldyreva
Xavier Boyen
Emmanuel Bresson
Jan Cappaert
Sanjit Chatterjee
Liqun Chen
Benoit Chevallier-Mames
Jung-Hui Chiu
Yvonne Cliff
Deepak Kumar Dalai
Ivan Damgaard
Tanmoy Kanti Das
Tom St Denis
Alex Dent
Vassil Dimitrov
Christophe Doche
Gwenael Doerr
Sylvain Duquesne
Alain Durand
Thomas Eisenbarth
Xinxin Fan
Pooya Farshim
Serge Fehr
Dacio Luiz Gazzoni Filho
Caroline Fontaine
Pierre-Alain Fouque
Philippe Gaborit
Sebastian Gajek
Fabien Galand
Steven Galbraith
Gagan Garg
Rosario Gennaro
Pascal Giorgi
Philippe Golle
Louis Goubin
Robert Granger
Johannes Groszschaedl
Indivar Gupta
Robbert de Haan
Tor Helleseth
Katrin Hoeper
Susan Hohenberger
Nick Howgrave-Graham
Po-Yi Huang
Ulrich Huber
Shaoquan Jiang
Thomas Johansson
Shri Kant
Guruprasad Kar
Stefan Katzenbeisser
Jonathan Katz
John Kelsey
Dalia Khader
Alexander Kholosha
Eike Kiltz
Lars Ramkilde Knudsen
Ulrich Kuehn
H.V. Kumar Swamy
Meena Kumari
Sandeep Kumar
Sébastien Kunz-Jacques
Kaoru Kurosawa
Fabien Laguillaumie
Joseph Lano
Cédric Lauradoux
Dong Hoon Lee
Frédéric Lefebvre
Stephane Lemieux
Arjen K. Lenstra
Pierre-Yvan Liardet
Helger Lipmaa
Joseph Liu
Zhijun Li
Pierre Loidreau
Spyros Magliveras
Subhamoy Maitra
Stéphane Manuel
Mark Manulis
Keith Martin
Nicolas Meloni
Sihem Mesnager
J. Mohapatra
Abhradeep Mondal
Michele Mosca
Mridul Nandi
Yassir Nawaz
Christophe Negre
Afonso Araújo Neto
Michael Neve
Rafail Ostrovsky
Daniel Page
Pascal Paillier
Saibal K. Pal
Je Hong Park
Kenny Paterson
Anindya Patthak
Souradyuti Paul
Jan Pelzl
Kun Peng
Pino Persiano
Duong Hieu Phan
N. Rajesh Pillai
Alessandro Piva
David Pointcheval
Axel Poschmann
Emmanuel Prouff
Frederic Raynal
Vincent Rijmen
Matt Robshaw
Jörg Rothe
Pieter Rozenhart
Andy Rupp
Palash Sarkar
Berry Schoenmakers
Jörg Schwenk
Siamak Fayyaz Shahandashti
Nicholas Sheppard
Igor Shparlinski
Thomas Shrimpton
Herve Sibert
Francesco Sica
Alice Silverberg
Rainer Steinwandt
Hung-Min Sun
V. Suresh
Michael Szydlo
Adrian Tang

Nicolas Thériault
Soeren S. Thomsen
Dongvu Tonien
Mårten Trolin
Boaz Tsaban
Wen-Guey Tzeng
Damien Vergnaud
Nicolas Veyrat-Charvillon
Charlotte Vikkelsoe
Ryan Vogt
Melanie Volkamer
Brent Waters
Andreas Westfeld
Kjell Wooding
Hongjun Wu
Brecht Wyseur
Yongjin Yeom
Aaram Yun
Nam Yul Yu
Moti Yung

Sponsoring Institutions

Cranes Software
Microsoft India
Metalogic Systems
Tata Consultancy Services

Lecture Notes in Computer Science

For information about Vols. 1–4231

please contact your bookseller or Springer

Vol. 4337: S. Arun-Kumar, N. Garg (Eds.), FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science. XIII, 430 pages. 2006.

Vol. 4331: G. Min, B. Di Martino, L.T. Yang, M. Guo, G. Ruenger (Eds.), Frontiers of High Performance Computing and Networking – ISPA 2006 Workshops. XXVII, 1141 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4313: T. Margaria, B. Steffen (Eds.), Leveraging Applications of Formal Methods. IX, 197 pages. 2006.

Vol. 4312: S. Sugimoto, J. Hunter, A. Rauber, A. Morishima (Eds.), Digital Libraries: Achievements, Challenges and Opportunities. XVIII, 571 pages. 2006.

Vol. 4311: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks II. XI, 253 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4306: Y. Avrithis, Y. Kompatsiaris, S. Staab, N.E. O'Connor (Eds.), Semantic Multimedia. XII, 241 pages. 2006.

Vol. 4304: A. Sattar, B.-H. Kang (Eds.), AI 2006: Advances in Artificial Intelligence. XXVII, 1303 pages. 2006. (Sublibrary LNAI).

Vol. 4302: J. Domingo-Ferrer, L. Franconi (Eds.), Privacy in Statistical Databases. XI, 383 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC. XIII, 358 pages. 2006.

Vol. 4295: J.D. Carswell, T. Tezuka (Eds.), Web and Wireless Geographical Information Systems. XI, 269 pages. 2006.

Vol. 4293: A. Gelbukh, C.A. Reyes-Garcia (Eds.), MICAI 2006: Advances in Artificial Intelligence. XXVIII, 1232 pages. 2006. (Sublibrary LNAI).

Vol. 4292: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part II. XXXII, 906 pages. 2006.

Vol. 4291: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part I. XXXI, 916 pages. 2006.

Vol. 4290: M. van Steen, M. Henning (Eds.), Middleware 2006. XIII, 425 pages. 2006.

Vol. 4289: M. Ackermann, B. Berendt, M. Grobelnik, A. Hotho, D. Mladenič, G. Semeraro, M. Spiliopoulou, G. Stumme, V. Svatek, M. van Someren (Eds.), Semantics, Web and Mining. X, 197 pages. 2006. (Sublibrary LNAI).

Vol. 4288: T. Asano (Ed.), Algorithms and Computation. XX, 766 pages. 2006.

Vol. 4285: Y. Matsumoto, R. Sproat, K.-F. Wong, M. Zhang (Eds.), Computer Processing of Oriental Languages. XVII, 544 pages. 2006. (Sublibrary LNAI).

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4282: Z. Pan, A. Cheok, M. Haller, R.W.H. Lau, H. Saito, R. Liang (Eds.), Advances in Artificial Reality and Tele-Existence. XXIII, 1347 pages. 2006.

Vol. 4281: K. Barkaoui, A. Cavalcanti, A. Cerone (Eds.), Theoretical Aspects of Computing - ICTAC 2006. XV, 371 pages. 2006.

Vol. 4280: A.K. Datta, M. Gradinariu (Eds.), Stabilization, Safety, and Security of Distributed Systems. XVII, 590 pages. 2006.

Vol. 4279: N. Kobayashi (Ed.), Programming Languages and Systems. XI, 423 pages. 2006.

Vol. 4278: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part II. XLV, 1004 pages. 2006.

Vol. 4277: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part I. XLV, 1009 pages. 2006.

Vol. 4276: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part II. XXXII, 752 pages. 2006.

Vol. 4275: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part I. XXXI, 1115 pages. 2006.

Vol. 4274: Q. Huo, B. Ma, E.-S. Chng, H. Li (Eds.), Chinese Spoken Language Processing. XXIV, 805 pages. 2006. (Sublibrary LNAI).

Vol. 4273: I. Cruz, S. Decker, D. Allemang, C. Preist, D. Schwabe, P. Mika, M. Uschold, L. Aroyo (Eds.), The Semantic Web - ISWC 2006. XXIV, 1001 pages. 2006.

Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), Smart Sensing and Context. XI, 267 pages. 2006.

Vol. 4271: F.V. Fomin (Ed.), Graph-Theoretic Concepts in Computer Science. XIII, 358 pages. 2006.

Vol. 4270: H. Zha, Z. Pan, H. Thwaites, A.C. Addison, M. Forte (Eds.), Interactive Technologies and Sociotechnical Systems. XVI, 547 pages. 2006.

Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), Large Scale Management of Distributed Systems. XIII, 282 pages. 2006.

Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), Autonomic Principles of IP Operations and Management. XIII, 237 pages. 2006.

Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), Autonomic Management of Mobile Multimedia Services. XIII, 257 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4265: L. Todorovski, N. Lavrač, K.P. Jantke (Eds.), Discovery Science. XIV, 384 pages. 2006. (Sublibrary LNAI).

Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), Algorithmic Learning Theory. XIII, 393 pages. 2006. (Sublibrary LNAI).

Vol. 4263: A. Levi, E. Savas, H. Yenigün, S. Balcisoy, Y. Saygin (Eds.), Computer and Information Sciences – ISCIS 2006. XXIII, 1084 pages. 2006.

Vol. 4262: K. Havelund, M. Núñez, G. Roçsu, B. Wolff (Eds.), Formal Approaches to Software Testing and Runtime Verification. VIII, 255 pages. 2006.

Vol. 4261: Y. Zhuang, S. Yang, Y. Rui, Q. He (Eds.), Advances in Multimedia Information Processing - PCM 2006. XXII, 1040 pages. 2006.

Vol. 4260: Z. Liu, J. He (Eds.), Formal Methods and Software Engineering. XII, 778 pages. 2006.

Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), Rough Sets and Current Trends in Computing. XXII, 951 pages. 2006. (Sublibrary LNAI).

Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), Software Process Improvement. XI, 219 pages. 2006.

Vol. 4256: L. Feng, G. Wang, C. Zeng, R. Huang (Eds.), Web Information Systems – WISE 2006 Workshops. XIV, 320 pages. 2006.

Vol. 4255: K. Aberer, Z. Peng, E.A. Rundensteiner, Y. Zhang, X. Li (Eds.), Web Information Systems – WISE 2006. XIV, 563 pages. 2006.

Vol. 4254: T. Grust, H. Höpfner, A. Illarramendi, S. Jablonski, M. Mesiti, S. Müller, P.-L. Patranjan, K.-U. Sattler, M. Spiliopoulou, J. Wijsen (Eds.), Current Trends in Database Technology – EDBT 2006. XXXI, 932 pages. 2006.

Vol. 4253: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. XXXII, 1301 pages. 2006. (Sublibrary LNAI).

Vol. 4252: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. XXXIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4251: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXVI, 1297 pages. 2006. (Sublibrary LNAI).

Vol. 4250: H.J. van den Herik, S.-C. Hsu, T.-s. Hsu, H.H.L.M. Donkers (Eds.), Advances in Computer Games. XIV, 273 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4248: S. Staab, V. Svátek (Eds.), Managing Knowledge in a World of Networks. XIV, 400 pages. 2006. (Sublibrary LNAI).

Vol. 4247: T.-D. Wang, X. Li, S.-H. Chen, X. Wang, H. Abbass, H. Iba, G. Chen, X. Yao (Eds.), Simulated Evolution and Learning. XXI, 940 pages. 2006.

Vol. 4246: M. Hermann, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIII, 588 pages. 2006. (Sublibrary LNAI).

Vol. 4245: A. Kuba, L.G. Nyúl, K. Palágyi (Eds.), Discrete Geometry for Computer Imagery. XIII, 688 pages. 2006.

Vol. 4244: S. Spaccapietra (Ed.), Journal on Data Semantics VII. XI, 267 pages. 2006.

Vol. 4243: T. Yakhno, E.J. Neuhold (Eds.), Advances in Information Systems. XIII, 420 pages. 2006.

Vol. 4242: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development II. IX, 289 pages. 2006.

Vol. 4241: R.R. Beichel, M. Sonka (Eds.), Computer Vision Approaches to Medical Image Analysis. XI, 262 pages. 2006.

Vol. 4239: H.Y. Youn, M. Kim, H. Morikawa (Eds.), Ubiquitous Computing Systems. XVI, 548 pages. 2006.

Vol. 4238: Y.-T. Kim, M. Takano (Eds.), Management of Convergence Networks and Services. XVIII, 605 pages. 2006.

Vol. 4237: H. Leitold, E. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4234: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part III. XXII, 1227 pages. 2006.

Vol. 4233: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part II. XXII, 1203 pages. 2006.

Vol. 4232: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part I. XLVI, 1153 pages. 2006.

Table of Contents

Invited Talk

Whither Cryptography? 1
James L. Massey

Symmetric Cryptography: Attacks

Non-randomness in eSTREAM Candidates Salsa20 and TSC-4 2
Simon Fischer, Willi Meier, Côme Berbain, Jean-François Biasse, M.J.B. Robshaw

Differential and Rectangle Attacks on Reduced-Round SHACAL-1 17
Jiqiang Lu, Jongsung Kim, Nathan Keller, Orr Dunkelman

Algebraic Attacks on Clock-Controlled Cascade Ciphers 32
Kenneth Koon-Ho Wong, Bernard Colbert, Lynn Batten, Sultan Al-Hinai

An Algorithm for Solving the LPN Problem and Its Application to Security Evaluation of the HB Protocols for RFID Authentication 48
Marc P.C. Fossorier, Miodrag J. Mihaljević, Hideki Imai, Yang Cui, Kanta Matsuura

Hash Functions

Update on Tiger 63
Florian Mendel, Bart Preneel, Vincent Rijmen, Hirotaka Yoshida, Dai Watanabe

RC4-Hash: A New Hash Function Based on RC4 80
Donghoon Chang, Kishan Chand Gupta, Mridul Nandi

Security of VSH in the Real World 95
Markku-Juhani O. Saarinen

Provable Security: Key Agreement

Cryptanalysis of Two Provably Secure Cross-Realm C2C-PAKE Protocols 104
Raphael C.-W. Phan, Bok-Min Goi

Efficient and Provably Secure Generic Construction of Three-Party Password-Based Authenticated Key Exchange Protocols 118
Weijia Wang, Lei Hu

On the Importance of Public-Key Validation in the MQV and HMQV Key Agreement Protocols 133
Alfred Menezes, Berkant Ustaoglu

Invited Talk

Another Look at "Provable Security". II 148
Neal Koblitz, Alfred Menezes

Provable Security: Public Key Cryptography

Efficient CCA-Secure Public-Key Encryption Schemes from RSA-Related Assumptions 176
Jaimee Brown, Juan Manuel González Nieto, Colin Boyd

General Conversion for Obtaining Strongly Existentially Unforgeable Signatures 191
Isamu Teranishi, Takuro Oyama, Wakaha Ogata

Conditionally Verifiable Signature 206
Ian F. Blake, Aldar C-F. Chan

Constant Phase Bit Optimal Protocols for Perfectly Reliable and Secure Message Transmission 221
Arpita Patra, Ashish Choudhary, Kannan Srinathan, Chandrasekaran Pandu Rangan

Symmetric Cryptography: Design

Using Wiedemann's Algorithm to Compute the Immunity Against Algebraic and Fast Algebraic Attacks 236
Frédéric Didier

Enciphering with Arbitrary Small Finite Domains 251
Valery Pryamikov

Enumeration of 9-Variable Rotation Symmetric Boolean Functions Having Nonlinearity > 240 266
Selçuk Kavut, Subhamoy Maitra, Sumanta Sarkar, Melek D. Yücel

Modes of Operation and Message Authentication Codes

Symmetric Nonce Respecting Security Model and the MEM Mode of Operation 280
Peng Wang, Dengguo Feng, Wenling Wu

HCH: A New Tweakable Enciphering Scheme Using the Hash-Encrypt-Hash Approach 287
Debrup Chakraborty, Palash Sarkar

Efficient Shared-Key Authentication Scheme from Any Weak Pseudorandom Function 303
Ryo Nojima, Kazukuni Kobara, Hideki Imai

A Simple and Unified Method of Proving Indistinguishability 317
Mridul Nandi

Fast Implementation of Public Key Cryptography

Extended Double-Base Number System with Applications to Elliptic Curve Cryptography 335
Christophe Doche, Laurent Imbert

CMSS – An Improved Merkle Signature Scheme 349
Johannes Buchmann, Luis Carlos Coronado García, Erik Dahmen, Martin Döring, Elena Klintsevich

ID-Based Cryptography

Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature 364
Man Ho Au, Joseph K. Liu, Willy Susilo, T.H. Yuen

Secure Cryptographic Workflow in the Standard Model 379
Manuel Barbosa, Pooya Farshim

Multi-receiver Identity-Based Key Encapsulation with Shortened Ciphertext 394
Sanjit Chatterjee, Palash Sarkar

Identity-Based Parallel Key-Insulated Encryption Without Random Oracles: Security Notions and Construction 409
Jian Weng, Shengli Liu, Kefei Chen, Changshe Ma

Embedded System and Side Channel Attacks

AES Software Implementations on ARM7TDMI 424
Matthew Darnall, Doug Kuhlman

Galois LFSR, Embedded Devices and Side Channel Weaknesses 436
Antoine Joux, Pascal Delaunay

Author Index 453

Whither Cryptography?

James L. Massey

Prof.-em. ETH-Zurich,
Adj. Prof.: Lund Univ., Sweden, and
Tech. Univ. of Denmark
jamesmassey@compuserve.com

Abstract. Diffie and Hellman's famous 1976 paper, "New Directions in Cryptography," lived up to its title in providing the directions that cryptography has followed in the past thirty years. Where will, or should, cryptography go next? This talk will examine this question and consider many possible answers including: more of the same, number-theoretic algorithms, computational-complexity approaches, quantum cryptography, circuit-complexity methods, and new computational models. Opinions will be offered on what is most likely to happen and what could be most fruitful. These opinions rest not on any special competence by the speaker but rather on his experience as a dabbler in, and spectator of, cryptography for more than forty years.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, p. 1, 2006.

Non-randomness in eSTREAM Candidates Salsa20 and TSC-4

Simon Fischer[1], Willi Meier[1], Côme Berbain[2], Jean-François Biasse[2], and M.J.B. Robshaw[2]

[1] FHNW, 5210 Windisch, Switzerland
{simon.fischer, willi.meier}@fhnw.ch
[2] FTRD, 38–40 rue du Général Leclerc, 92794 Issy les Moulineaux, France
{come.berbain, jeanfrancois.biasse, matt.robshaw}@orange-ft.com

Abstract. Stream cipher initialisation should ensure that the initial state or keystream is not detectably related to the key and initialisation vector. In this paper we analyse the key/IV setup of the eSTREAM Phase 2 candidates Salsa20 and TSC-4. In the case of Salsa20 we demonstrate a key recovery attack on six rounds and observe non-randomness after seven. For TSC-4, non-randomness over the full eight-round initialisation phase is detected, but would also persist for more rounds.

Keywords: Stream Cipher, eSTREAM, Salsa20, TSC-4, Chosen IV Attack.

1 Introduction

Many synchronous stream ciphers use two inputs for keystream generation; a secret key K and a non-secret initialisation vector IV. The IV allows different keystreams to be derived from a single secret key and facilitates resynchronization. In the general model of a synchronous stream cipher there are three functions. During initialisation a function F maps the input pair (K, IV) to a secret initial state X. The state of the cipher then evolves at time t under the action of a function f that updates the state X according to $X^{t+1} = \mathsf{f}(X^t)$. Keystream is generated using an output function g to give a block of keystream $z^t = \mathsf{g}(X^t)$. While TSC-4 follows this model, Salsa20 has no state update function f and g involves reading out the state X. Instead, we view the IV to Salsa20 as being the combination of a 64-bit *nonce* and a 64-bit *counter* and keystream is generated by repeatedly computing $\mathsf{F}(K, IV)$ for an incremented counter.

In the analysis of keystream generators (*i.e.* in the analysis of f and g) it is typical to assume that the initial state X is random. Hence for a stream cipher we require that F has suitable randomness properties, and in particular, that it has good diffusion with regards to both IV and K. (Clearly this applies equally to the case when the output of F is the keystream.) Indeed, if diffusion of the IV is not complete then there may well be statistical or algebraic dependences in the keystreams for different IV's, as chosen-IV attacks on numerous stream ciphers demonstrate (*e.g.*, [6, 9, 8]). Good mixing of the secret key is similarly required and there should not be any identifiable subsets of keys that have a traceable

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 2–16, 2006.