

Javier Lopez
Sihan Qing
Eiji Okamoto (Eds.)

LNC3 3269

Information and Communications Security

6th International Conference, ICICS 2004
Malaga, Spain, October 2004
Proceedings

Javier Lopez Sihan Qing
Eiji Okamoto (Eds.)

Information and Communications Security

6th International Conference, ICICS 2004
Malaga, Spain, October 27-29, 2004
Proceedings



Springer

Volume Editors

Javier Lopez
University of Malaga
Computer Science Department
E.T.S. Ingeniería Informática, Campus de Teatinos, 29071 Malaga, Spain
E-mail: jlm@lcc.uma.es

Sihan Qing
Chinese Academy of Sciences
Institute of Software
4 4th Street South, ZhongGuanCun, Beijing 100080, China
E-mail: qsihan@ercist.iscas.ac.cn

Eiji Okamoto
University of Tsukuba
Graduate School of Systems and Information Engineering
1-1-1 Ten-nohdai, Tsukuba 305-8573, Japan
E-mail: okamoto@risk.tsukuba.ac.jp

Library of Congress Control Number: 2004113914

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

ISSN 0302-9743

ISBN 3-540-23563-9 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11326922 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

New York University, NY, 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

This volume contains the proceedings of the *6th International Conference on Information and Communications Security* (ICICS 2004), Torremolinos (Málaga), Spain, 27–29 October 2004. The five previous conferences were held in Beijing, Sydney, Xian, Singapore and Huhehaote City, where we had an enthusiastic and well-attended event. The proceedings were released as volumes 1334, 1726, 2229, 2513 and 2836 of the LNCS series of Springer, respectively.

During these last years the conference has placed equal emphasis on the theoretical and practical aspects of information and communications security and has established itself as a forum at which academic and industrial people meet and discuss emerging security challenges and solutions. We hope to uphold this tradition by offering you yet another successful meeting with a rich and interesting program.

The response to the Call for Papers was overwhelming, 245 paper submissions were received. Therefore, the paper selection process was very competitive and difficult – only 42 papers were accepted. The success of the conference depends on the quality of the program. Thus, we are indebted to our Program Committee members and the external referees for the great job they did. These proceedings contain revised versions of the accepted papers. Revisions were not checked and the authors bear full responsibility for the content of their papers.

Other persons deserve many thanks for their contribution to the success of the conference. Prof. José M. Troya was the Conference Chair, and Prof. Eiji Okamoto was General Co-chair. We sincerely thank both of them for their total support and encouragement, and for their contribution to all organizational issues. Our special thanks to José A. Onieva, one of the major driving forces in the organization. He did a great job in the successful promotion of the conference, management of the WebReview application and assistance in the editorial process for the accepted papers. We also thank José A. Montenegro and Isaac Agudo for their help in those tasks. Without the hard work by these colleagues and the other members of the local organization team, this conference would not have been possible.

Finally, we thank all the authors who submitted papers and the participants from all over the world who chose to honor us with their attendance.

October 2004

Javier López
Si-han Qing

ICICS 2004
6th International Conference
on Information and Communications Security

Málaga, Spain
October 27–29, 2004

Organized by
Computer Science Department
University of Málaga
(Spain)

Conference Chairman

José M. Troya

University of Málaga, Spain

Program Co-chair

Si Han Qing

Chinese Academy of Sciences, China

Program Co-chair, General Co-chair

Javier López

University of Málaga, Spain

General Co-chair

Eiji Okamoto

University of Tsukuba, Japan

Program Committee

Tuomas Aura

Microsoft Research, UK

Tom Berson

Anagram Laboratories, USA

Jeremy Bryans

University of Newcastle, UK

Alex Biryukov

Katholieke Universiteit Leuven, Belgium

Colin Boyd

Queensland Univ. of Technology, Australia

Chin-Chen Chang

National Chung Cheng University, Taiwan

Joris Claessens

European Microsoft Innov. Center, Germany

George Davida

University of Wisconsin-Milwaukee, USA

Ed Dawson

Queensland Univ. of Technology, Australia

Robert Deng

Institute for Infocomm Research, Singapore

Yvo Desmedt

University College London, UK

Josep Domingo

Universitat Rovira i Virgili, Spain

Pierre-Alain Fouque

École Normale Supérieure, France

Yair Frankel

TechTegrity LLC, USA

Dieter Gollmann	TU Hamburg-Harburg, Germany
Yongfei Han	ONETS, China
Goichiro Hanaoka	University of Tokyo, Japan
Ki-Yoong Hong	Secuve, Korea
Sokratis Katsikas	University of the Aegean, Greece
Kwangjo Kim	Information and Comm. University, Korea
Chi-Sung Laih	National Cheng Kung University, Taiwan
Wenbo Mao	HP Labs Bristol, UK
Masahiro Mambo	Tohoku University, Japan
Fabio Massacci	Università di Trento, Italy
Catherine Meadows	Naval Research Laboratory, USA
Chris Mitchell	Royal Holloway, UK
Guevara Noubir	Northeastern University, USA
Rene Peralta	Yale University, USA
Giuseppe Persiano	Università di Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	École Normale Supérieure, France
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Kouichi Sakurai	Kyushu University, Japan
Miguel Soriano	Universidad Politécnica de Catalunya, Spain
Routo Terada	University of Sao Paulo, Brazil
Victor K. Wei	Chinese Univ. Hong Kong, China
Vijay Varadharajan	Macquarie University, Australia
Moti Yung	Columbia University, USA
Yulian Zheng	University of North Carolina, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

External Referees

Michel Abdalla	Ioanna Kantzavelou	Bart Preneel
Habtamu Abie	Tansel Kaya	Wei Qian
Mohammed Anish	Hyung Kim	Nataliya Rassadko
Nuttapong Attrapadung	Shinsaku Kiyomoto	Jason Reid
Mauro Barni	Tetsutaro Kobayashi	Michael Roe
Lejla Batina	Satoshi Koga	Rodrigo Roman
Giampaolo Bella	Spyros Kokolakis	Carsten Rudolph
Siddika Berna Ors	Hristo Koshutanski	Tatsiana Sabel
Enrico Blanzieri	Hartono Kurnio	Ryuichi Sakai
Andrea Boni	Kaoru Kurosawa	Taiichi Saito
An Braeken	Costas Lambrinoudakis	Francesc Sebé
Mauro Brunato	Joseph Lano	Stefaan Seys
Dario Catalano	Dimitrios Lekkas	SeongHan Shin
Christophe De Canniere	Dequan Li	Leonie Simpson
Roberto Caso	Gaicheng Li	Igor Shparlinski
Jordi Castellà	Jung-Shian Li	Ron Steinfeld
Jung-Hui Chiu	Guolong Lin	Makoto Sugita
Andrew Clark	Liping Li	Toshihiro Tabata
Yang Cui	Anna Lysyanskaya	Keisuke Takemori
Claudia Diaz	Hengtai Ma	Keisuke Tanaka
Jiang Du	Antonio Maña	Liuying Tang
Marcel Fernandez	Carlo Marchetti	Vrizlynn Thing
Ernest Foo	Gwenaëlle Martinet	Theodoros Tzouramanis
Jordi Forne	Antoni Martínez	ZhiMin Sun
Cedric Fournet	Bill Millan	Yoshifumi Ueshige
Martin Gagne	Kunihiko Miyazaki	Chao Wang
Paolo Giorgini	Anish Mohammed	Huaxiong Wang
Andy Gordon	Costas Moulinos	Shuhong Wang
Louis Granboulan	Jose A. Montenegro	Yin Wang
Fabrizio Granelli	Haris Mouratidis	Weiping Wen
Stefanos Gritzalis	Frédéric Muller	Duncan S. Wong
Joshua Goodman	Bill Munro	Hongjun Wu
Juanma Gonzalez-Nieto	Jose L. Muñoz	Mariemma Yague
Jaime Gutierrez	Anderson C.A.	Kira Yamada
DongGu Han	Nascimento	Ching-Nung Yang
Matt Henricksen	Svetla Nikova	Robbie Ye
Yvonne Hitchcock	Masayuki Numao	Nicola Zannone
Yoshiaki Hori	Koji Okada	Rui Zhang
Luigi Lo Iacono	Jose A. Onieva	Yongbin Zhou
John Iliadis	Juan J. Ortega	Xukai Zou
Kenji Imamoto	Thea Peacock	Feng Zhu
QingGuang Ji	Josep Pegueroles	Alf Zugenmaier
Jianchun Jiang	Kun Peng	

Lecture Notes in Computer Science

For information about Vols. 1–3180

please contact your bookseller or Springer

Vol. 3293: C.-H. Chi, M. van Steen, C. Wills (Eds.), *Web Content Caching and Distribution*. IX, 283 pages. 2004.

Vol. 3274: R. Guerraoui (Ed.), *Distributed Computing*. XIII, 465 pages. 2004.

Vol. 3273: T. Baar, A. Strohmeier, A. Moreira, S.J. Mellor (Eds.), *<<UML>> 2004 - The Unified Modelling Language*. XIII, 454 pages. 2004.

Vol. 3271: J. Vicente, D. Hutchison (Eds.), *Management of Multimedia Networks and Services*. XIII, 335 pages. 2004.

Vol. 3270: M. Jeckle, R. Kowalczyk, P. Braun (Eds.), *Grid Services Engineering and Management*. X, 165 pages. 2004.

Vol. 3269: J. López, S. Qing, E. Okamoto (Eds.), *Information and Communications Security*. XI, 564 pages. 2004.

Vol. 3266: J. Solé-Pareta, M. Smirnov, P.V. Mieghem, J. Domingo-Pascual, E. Monteiro, P. Reichl, B. Stiller, R.J. Gibbens (Eds.), *Quality of Service in the Emerging Networking Panorama*. XVI, 390 pages. 2004.

Vol. 3265: R.E. Frederking, K.B. Taylor (Eds.), *Machine Translation: From Real Users to Research*. XI, 392 pages. 2004. (Subseries LNAI).

Vol. 3264: G. Paliouras, Y. Sakakibara (Eds.), *Grammatical Inference: Algorithms and Applications*. XI, 291 pages. 2004. (Subseries LNAI).

Vol. 3263: M. Weske, P. Liggesmeyer (Eds.), *Object-Oriented and Internet-Based Technologies*. XII, 239 pages. 2004.

Vol. 3262: M.M. Freire, P. Chemouil, P. Lorenz, A. Gravey (Eds.), *Universal Multiservice Networks*. XIII, 556 pages. 2004.

Vol. 3261: T. Yakhno (Ed.), *Advances in Information Systems*. XIV, 617 pages. 2004.

Vol. 3260: I.G.M.M. Niemegeers, S.H. de Groot (Eds.), *Personal Wireless Communications*. XIV, 478 pages. 2004.

Vol. 3258: M. Wallace (Ed.), *Principles and Practice of Constraint Programming – CP 2004*. XVII, 822 pages. 2004.

Vol. 3257: E. Motta, N.R. Shadbolt, A. Stutt, N. Gibbins (Eds.), *Engineering Knowledge in the Age of the Semantic Web*. XVII, 517 pages. 2004. (Subseries LNAI).

Vol. 3256: H. Ehrig, G. Engels, F. Parisi-Presicce, G. Rozenberg (Eds.), *Graph Transformations*. XII, 451 pages. 2004.

Vol. 3255: A. Benczúr, J. Demetrovics, G. Gottlob (Eds.), *Advances in Databases and Information Systems*. XI, 423 pages. 2004.

Vol. 3254: E. Macii, V. Paliouras, O. Koufopavlou (Eds.), *Integrated Circuit and System Design*. XVI, 910 pages. 2004.

Vol. 3253: Y. Lakhnech, S. Yovine (Eds.), *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*. X, 397 pages. 2004.

Vol. 3250: L.-J. (LJ) Zhang, M. Jeckle (Eds.), *Web Services*. X, 301 pages. 2004.

Vol. 3249: B. Buchberger, J.A. Campbell (Eds.), *Artificial Intelligence and Symbolic Computation*. X, 285 pages. 2004. (Subseries LNAI).

Vol. 3246: A. Apostolico, M. Melucci (Eds.), *String Processing and Information Retrieval*. XIV, 332 pages. 2004.

Vol. 3245: E. Suzuki, S. Arikawa (Eds.), *Discovery Science*. XIV, 430 pages. 2004. (Subseries LNAI).

Vol. 3244: S. Ben-David, J. Case, A. Maruoka (Eds.), *Algorithmic Learning Theory*. XIV, 505 pages. 2004. (Subseries LNAI).

Vol. 3243: S. Leonardi (Ed.), *Algorithms and Models for the Web-Graph*. VIII, 189 pages. 2004.

Vol. 3242: X. Yao, E. Burke, J.A. Lozano, J. Smith, J.J. Merelo-Guervós, J.A. Bullinaria, J. Rowe, P. Tiño, A. Kabán, H.-P. Schwefel (Eds.), *Parallel Problem Solving from Nature - PPSN VIII*. XX, 1185 pages. 2004.

Vol. 3241: D. Kranzlmüller, P. Kacsuk, J.J. Dongarra (Eds.), *Recent Advances in Parallel Virtual Machine and Message Passing Interface*. XIII, 452 pages. 2004.

Vol. 3240: I. Jonassen, J. Kim (Eds.), *Algorithms in Bioinformatics*. IX, 476 pages. 2004. (Subseries LNBI).

Vol. 3239: G. Nicosia, V. Cutello, P.J. Bentley, J. Timmis (Eds.), *Artificial Immune Systems*. XII, 444 pages. 2004.

Vol. 3238: S. Biundo, T. Frühwirth, G. Palm (Eds.), *KI 2004: Advances in Artificial Intelligence*. XI, 467 pages. 2004. (Subseries LNAI).

Vol. 3236: M. Núñez, Z. Maamar, F.L. Pelayo, K. Pousttchi, F. Rubio (Eds.), *Applying Formal Methods: Testing, Performance, and M/E-Commerce*. XI, 381 pages. 2004.

Vol. 3235: D. de Frutos-Escrig, M. Nunez (Eds.), *Formal Techniques for Networked and Distributed Systems – FORTE 2004*. X, 377 pages. 2004.

Vol. 3232: R. Heery, L. Lyon (Eds.), *Research and Advanced Technology for Digital Libraries*. XV, 528 pages. 2004.

Vol. 3231: H.-A. Jacobsen (Ed.), *Middleware 2004*. XV, 514 pages. 2004.

Vol. 3230: J.L. Vicedo, P. Martínez-Barco, R. Muñoz, M.S. Noeda (Eds.), *Advances in Natural Language Processing*. XII, 488 pages. 2004. (Subseries LNAI).

- Vol. 3229: J.J. Alferes, J. Leite (Eds.), *Logics in Artificial Intelligence*. XIV, 744 pages. 2004. (Subseries LNAI).
- Vol. 3225: K. Zhang, Y. Zheng (Eds.), *Information Security*. XII, 442 pages. 2004.
- Vol. 3224: E. Jonsson, A. Valdes, M. Almgren (Eds.), *Recent Advances in Intrusion Detection*. XII, 315 pages. 2004.
- Vol. 3223: K. Slind, A. Bunker, G. Gopalakrishnan (Eds.), *Theorem Proving in Higher Order Logics*. VIII, 337 pages. 2004.
- Vol. 3222: H. Jin, G.R. Gao, Z. Xu, H. Chen (Eds.), *Network and Parallel Computing*. XX, 694 pages. 2004.
- Vol. 3221: S. Albers, T. Radzik (Eds.), *Algorithms – ESA 2004*. XVIII, 836 pages. 2004.
- Vol. 3220: J.C. Lester, R.M. Vicari, F. Paragauçu (Eds.), *Intelligent Tutoring Systems*. XXI, 920 pages. 2004.
- Vol. 3219: M. Heisel, P. Liggesmeyer, S. Wittmann (Eds.), *Computer Safety, Reliability, and Security*. XI, 339 pages. 2004.
- Vol. 3217: C. Barillot, D.R. Haynor, P. Hellier (Eds.), *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2004*. XXXVIII, 1114 pages. 2004.
- Vol. 3216: C. Barillot, D.R. Haynor, P. Hellier (Eds.), *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2004*. XXXVIII, 930 pages. 2004.
- Vol. 3215: M.G. Negoita, R.J. Howlett, L.C. Jain (Eds.), *Knowledge-Based Intelligent Information and Engineering Systems*. LVII, 906 pages. 2004. (Subseries LNAI).
- Vol. 3214: M.G. Negoita, R.J. Howlett, L.C. Jain (Eds.), *Knowledge-Based Intelligent Information and Engineering Systems*. LVIII, 1302 pages. 2004. (Subseries LNAI).
- Vol. 3213: M.G. Negoita, R.J. Howlett, L.C. Jain (Eds.), *Knowledge-Based Intelligent Information and Engineering Systems*. LVIII, 1280 pages. 2004. (Subseries LNAI).
- Vol. 3212: A. Campilho, M. Kamel (Eds.), *Image Analysis and Recognition*. XXIX, 862 pages. 2004.
- Vol. 3211: A. Campilho, M. Kamel (Eds.), *Image Analysis and Recognition*. XXIX, 880 pages. 2004.
- Vol. 3210: J. Marcinkowski, A. Tarlecki (Eds.), *Computer Science Logic*. XI, 520 pages. 2004.
- Vol. 3209: B. Berendt, A. Hotho, D. Mladenec, M. van Someren, M. Spiliopoulou, G. Stumme (Eds.), *Web Mining: From Web to Semantic Web*. IX, 201 pages. 2004. (Subseries LNAI).
- Vol. 3208: H.J. Ohlbach, S. Schaffert (Eds.), *Principles and Practice of Semantic Web Reasoning*. VII, 165 pages. 2004.
- Vol. 3207: L.T. Yang, M. Guo, G.R. Gao, N.K. Jha (Eds.), *Embedded and Ubiquitous Computing*. XX, 1116 pages. 2004.
- Vol. 3206: P. Sojka, I. Kopecek, K. Pala (Eds.), *Text, Speech and Dialogue*. XIII, 667 pages. 2004. (Subseries LNAI).
- Vol. 3205: N. Davies, E. Mynatt, I. Siiro (Eds.), *UbiComp 2004: Ubiquitous Computing*. XVI, 452 pages. 2004.
- Vol. 3204: C.A. Peña Reyes, *Coevolutionary Fuzzy Modeling*. XIII, 129 pages. 2004.
- Vol. 3203: J. Becker, M. Platzner, S. Vernalde (Eds.), *Field Programmable Logic and Application*. XXX, 1198 pages. 2004.
- Vol. 3202: J.-F. Boulicaut, F. Esposito, F. Giannotti, D. Pedreschi (Eds.), *Knowledge Discovery in Databases: PKDD 2004*. XIX, 560 pages. 2004. (Subseries LNAI).
- Vol. 3201: J.-F. Boulicaut, F. Esposito, F. Giannotti, D. Pedreschi (Eds.), *Machine Learning: ECML 2004*. XVIII, 580 pages. 2004. (Subseries LNAI).
- Vol. 3199: H. Schepers (Ed.), *Software and Compilers for Embedded Systems*. X, 259 pages. 2004.
- Vol. 3198: G.-J. de Vreede, L.A. Guerrero, G. Marín Raventós (Eds.), *Groupware: Design, Implementation and Use*. XI, 378 pages. 2004.
- Vol. 3196: C. Stary, C. Stephanidis (Eds.), *User-Centered Interaction Paradigms for Universal Access in the Information Society*. XII, 488 pages. 2004.
- Vol. 3195: C.G. Puntonet, A. Prieto (Eds.), *Independent Component Analysis and Blind Signal Separation*. XXIII, 1266 pages. 2004.
- Vol. 3194: R. Camacho, R. King, A. Srinivasan (Eds.), *Inductive Logic Programming*. XI, 361 pages. 2004. (Subseries LNAI).
- Vol. 3193: P. Samarati, P. Ryan, D. Gollmann, R. Molva (Eds.), *Computer Security – ESORICS 2004*. X, 457 pages. 2004.
- Vol. 3192: C. Bussler, D. Fensel (Eds.), *Artificial Intelligence: Methodology, Systems, and Applications*. XIII, 522 pages. 2004. (Subseries LNAI).
- Vol. 3191: M. Klusch, S. Ossowski, V. Kashyap, R. Unland (Eds.), *Cooperative Information Agents VIII*. XI, 303 pages. 2004. (Subseries LNAI).
- Vol. 3190: Y. Luo (Ed.), *Cooperative Design, Visualization, and Engineering*. IX, 248 pages. 2004.
- Vol. 3189: P.-C. Yew, J. Xue (Eds.), *Advances in Computer Systems Architecture*. XVII, 598 pages. 2004.
- Vol. 3188: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), *Formal Methods for Components and Objects*. VIII, 373 pages. 2004.
- Vol. 3187: G. Lindemann, J. Denzinger, I.J. Timm, R. Unland (Eds.), *Multiagent System Technologies*. XIII, 341 pages. 2004. (Subseries LNAI).
- Vol. 3186: Z. Bellahsene, T. Milo, M. Rys, D. Suciu, R. Unland (Eds.), *Database and XML Technologies*. X, 235 pages. 2004.
- Vol. 3185: M. Bernardo, F. Corradini (Eds.), *Formal Methods for the Design of Real-Time Systems*. VII, 295 pages. 2004.
- Vol. 3184: S. Katsikas, J. Lopez, G. Pernul (Eds.), *Trust and Privacy in Digital Business*. XI, 299 pages. 2004.
- Vol. 3183: R. Traummüller (Ed.), *Electronic Government*. XIX, 583 pages. 2004.
- Vol. 3182: K. Bauknecht, M. Bichler, B. Pröll (Eds.), *E-Commerce and Web Technologies*. XI, 370 pages. 2004.
- Vol. 3181: Y. Kambayashi, M. Mohania, W. Wöb (Eds.), *Data Warehousing and Knowledge Discovery*. XIV, 412 pages. 2004.

Table of Contents

On the Minimal Assumptions of Group Signature Schemes	1
<i>Michel Abdalla and Bogdan Warinschi</i>	
Perfect Concurrent Signature Schemes	14
<i>Willy Susilo, Yi Mu, and Fangguo Zhang</i>	
New Identity-Based Ring Signature Schemes	27
<i>Javier Herranz and Germán Sáez</i>	
On the Security of a Multi-party Certified Email Protocol	40
<i>Jianying Zhou</i>	
Robust Metering Schemes for General Access Structures	53
<i>Ventzislav Nikov, Svetla Nikova, and Bart Preneel</i>	
PAYFLUX – Secure Electronic Payment in Mobile Ad Hoc Networks	66
<i>Klaus Herrmann and Michael A. Jaeger</i>	
Flexible Verification of MPEG-4 Stream in Peer-to-Peer CDN	79
<i>Tieyan Li, Yongdong Wu, Di Ma, Huafei Zhu, and Robert H. Deng</i>	
Provably Secure Authenticated Tree Based Group Key Agreement	92
<i>Ratna Dutta, Rana Barua, and Palash Sarkar</i>	
Taxonomic Consideration to OAEP Variants and Their Security	105
<i>Yuichi Komano and Kazuo Ohta</i>	
Factorization-Based Fail-Stop Signatures Revisited	118
<i>Katja Schmidt-Samoa</i>	
A Qualitative Evaluation of Security Patterns	132
<i>Spyros T. Halkidis, Alexander Chatzigeorgiou, and George Stephanides</i>	
Type Inferability and Decidability of the Security Problem Against Inference Attacks on Object-Oriented Databases	145
<i>Yasunori Ishihara, Yumi Shimakawa, and Toru Fujiwara</i>	
Volatile Memory Computer Forensics to Detect Kernel Level Compromise	158
<i>Sandra Ring and Eric Cole</i>	
A Secure Workflow Model Based on Distributed Constrained Role and Task Assignment for the Internet	171
<i>Ilanit Moodahi, Ehud Gudes, Oz Lavee, and Amnon Meisels</i>	

Hydan: Hiding Information in Program Binaries	187
<i>Rakan El-Khalil and Angelos D. Keromytis</i>	
A Semi-fragile Steganographic Digital Signature for Images	200
<i>Luke Hebbes and Andrew Lenaghan</i>	
Identification of Traitors Using a Trellis	211
<i>Marcel Fernandez and Miguel Soriano</i>	
Decentralized Publish-Subscribe System to Prevent Coordinated Attacks via Alert Correlation	223
<i>Joaquin Garcia, Fabien Autrel, Joan Borrell, Sergio Castillo, Frederic Cuppens, and Guillermo Navarro</i>	
Reflector Attack Traceback System with Pushback Based iTrace Mechanism	236
<i>Hyung-Woo Lee, Sung-Hyun Yun, Taekyoung Kwon, Jae-Sung Kim, Hee-Un Park, and Nam-Ho Oh</i>	
Automatic Covert Channel Analysis of a Multilevel Secure Component	249
<i>Ruggero Lanotte, Andrea Maggiolo-Schettini, Simone Tini, Angelo Troina, and Enrico Tronci</i>	
Sound Approximations to Diffie-Hellman Using Rewrite Rules	262
<i>Christopher Lynch and Catherine Meadows</i>	
On Randomized Addition-Subtraction Chains to Counteract Differential Power Attacks	278
<i>Anton Kargl and Götz Wiesend</i>	
New Power Analysis on the Ha-Moon Algorithm and the MIST Algorithm	291
<i>Sang Gyoo Sim, Dong Jin Park, and Pil Joong Lee</i>	
Modified Power-Analysis Attacks on XTR and an Efficient Countermeasure	305
<i>Dong-Guk Han, Tetsuya Izu, Jongin Lim, and Kouichi Sakurai</i>	
Modelling Dependencies Between Classifiers in Mobile Masquerader Detection . .	318
<i>Oleksiy Mazhelis, Seppo Puuronen, and Jari Veijalainen</i>	
Threat Analysis on Network MObility (NEMO)	331
<i>Souhwan Jung, Fan Zhao, S. Felix Wu, and HyunGon Kim</i>	
Macro-level Attention to Mobile Agent Security: Introducing the Mobile Agent Secure Hub Infrastructure Concept	343
<i>Michelangelo Giansiracusa, Selwyn Russell, Andrew Clark, and Volker Roth</i>	
Securing the Destination-Sequenced Distance Vector Routing Protocol (S-DSDV)	358
<i>Tao Wan, Evangelos Kranakis, and Paul C. van Oorschot</i>	

Secret-Public Storage Trade-Off for Broadcast Encryption Key Management	375
<i>Miodrag J. Mihaljević, Marc P.C. Fossorier, and Hideki Imai</i>	
Security Analysis of the Generalized Self-shrinking Generator	388
<i>Bin Zhang, Hongjun Wu, Dengguo Feng, and Feng Bao</i>	
On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis	401
<i>Bo-Yin Yang, Jiun-Ming Chen, and Nicolas T. Courtois</i>	
On Some Weak Extensions of AES and BES	414
<i>Jean Monnerat and Serge Vaudenay</i>	
Clock Control Sequence Reconstruction in the Ciphertext Only Attack Scenario . .	427
<i>Slobodan Petrović and Amparo Fúster-Sabater</i>	
Transient Fault Induction Attacks on XTR	440
<i>Mathieu Ciet and Christophe Giraud</i>	
Adaptive-CCA on OpenPGP Revisited	452
<i>Hsi-Chung Lin, Sung-Ming Yen, and Guan-Ting Chen</i>	
A New Key-Insulated Signature Scheme	465
<i>Nicolás González-Deleito, Olivier Markowitch, and Emmanuel Dall'Olio</i>	
Secure Hierarchical Identity Based Signature and Its Application	480
<i>Sherman S.M. Chow, Lucas C.K. Hui, Siu Ming Yiu, and K.P. Chow</i>	
Multi-designated Verifiers Signatures	495
<i>Fabien Laguillaumie and Damien Vergnaud</i>	
Dynamic Access Control for Multi-privileged Group Communications	508
<i>Di Ma, Robert H. Deng, Yongdong Wu, and Teyan Li</i>	
An Efficient Authentication Scheme Using Recovery Information in Signature . . .	520
<i>Kihun Hong and Souhwan Jung</i>	
Time-Scoped Searching of Encrypted Audit Logs	532
<i>Darren Davis, Fabian Monrose, and Michael K. Reiter</i>	
Rights-Carrying and Self-enforcing Information Objects for Information Distribution Systems	546
<i>Habtamu Abie, Pål Spilling, and Bent Foyen</i>	
Author Index	563

On the Minimal Assumptions of Group Signature Schemes

Michel Abdalla¹ and Bogdan Warinschi²

¹ Departement d'Informatique
École Normale Supérieure
45 rue d'Ulm, 75230 Paris Cedex 05, France
Michel.Abdalla@ens.fr

<http://www.michelabdalla.net>

² Computer Science Department
University of California at Santa Cruz
1156 High Street, Santa Cruz, CA 95064, USA
bogdan@cse.ucsc.edu
<http://www.cs.ucsd.edu/~bogdan>

Abstract. One of the central lines of cryptographic research is identifying the weakest assumptions required for the construction of secure primitives. In the context of group signatures the gap between what is known to be necessary (one-way functions) and what is known to be sufficient (trapdoor permutations) is quite large. In this paper, we provide the first step towards closing this gap by showing that the existence of secure group signature schemes implies the existence of secure public-key encryption schemes. Our result shows that the construction of secure group signature schemes based solely on the existence of one-way functions is unlikely. This is in contrast to what is known for standard signature schemes, which can be constructed from any one-way function.

Keywords: Group signatures, one-way functions, trapdoor permutations, minimal assumptions.

1 Introduction

MOTIVATION. One of the central lines of cryptographic research is identifying the weakest assumptions required for the construction of secure primitives. This is important not only to better understand the different relations among existing primitives, but also to learn the minimal conditions without which a certain primitive cannot exist. Yet another reason for finding the weakest assumptions is that stronger assumptions may later be found to be false while weaker assumptions may still hold. Therefore, by closing the gap between which primitive is sufficient and what is necessary to build a given cryptographic function such as encryption or group signatures, one can determine the exact conditions that need be met for them to exist.

While several implications and separations are known in the literature for primitives such as standard signatures and public-key encryption, very little is

known for group signatures despite the intuition that the latter appears to be a stronger primitive than standard signatures. Currently, group signatures are only known to be implied by trapdoor permutations [9] and to imply one-way functions [30], a quite large gap. Addressing this problem is the main goal of this paper.

PRELIMINARIES. In order to better understand our results, let us briefly recall the definitions for the basic primitives given in Figure 1. The most basic of the cryptographic primitives is a *one-way function*. Loosely speaking, a function is said to be one-way if it is easy to compute (on any input) but hard to invert (on average), where easy means computable in polynomial time on the length of the input. Another basic primitive is a *trapdoor one-way function*, or simply trapdoor function, introduced by Diffie and Hellman [16] in the seminal work which laid out the foundations of public-key cryptography. Informally, a one-way function is said to be trapdoor if it has associated to it a secret trapdoor which allows anyone in its possession to easily invert it. The notions of *one-way permutations* and *trapdoor permutations* are defined in a similar manner. The notion of *trapdoor predicates*, introduced by Goldwasser and Micali [21], is slightly different. Approximately, trapdoor predicates are probabilistic functions over $\{0, 1\}$ which are easy to compute given a public key but whose output distributions on inputs 0 and 1 are hard to distinguish by any algorithm not in possession of the trapdoor information.

Since we will be using terms such as implications and separations throughout the paper, we should also recall what we mean by that. Consider for example two cryptographic primitives S and P . In order to properly relate their security, one usually makes use of reductions. More precisely, a primitive P is said to *imply* a primitive S if the security of P has been demonstrated to imply the security of S . More precisely, we use this phrase when someone has formally defined the goals G_P and G_S for primitives P and S , respectively, and then has proven that the existence of an adversary A_S who breaks primitive S , in the sense of violating G_S , implies the existence of an adversary A_P who breaks primitive P , in the sense of violating G_P .

Proving a separation between two primitives, however, is a more subtle problem since it is not clear what it means to say that a given primitive does not imply another primitive. To overcome this problem, one usually uses the method due to Impagliazzo and Rudich [25] of restricting the class of reductions for which the separation holds. More specifically, they noted the fact that the vast majority of the reductions in cryptography uses the underlying primitive as a black-box and based on that, they introduced a method for proving separations between primitives with respect to these types of reductions.

BACKGROUND ON GROUP SIGNATURES. The notion of group signatures was introduced by Chaum and van Heyst [14] and describes a setting in which individuals within a group can sign messages with respect to the group. According to [14], a secure group signature scheme should satisfy two basic requirements, anonymity and traceability. While the former says that the identity of the signer should remain unknown to anyone verifying the signature including other group

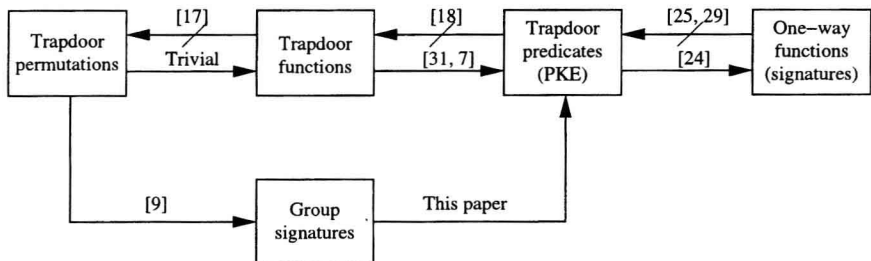


Fig. 1. Implications and black-box separations between primitives.

elements, the latter asks that there should exist an entity, called the group manager, capable of revoking the anonymity of signer whenever necessary.

Since the original work of Chaum and van Heyst [14], several other schemes have been proposed in the literature (e.g., [1, 3, 2, 15, 13, 12, 26]), each with its own set of security properties and requirements. It was only recently, however, that a formal model of security for group signatures was put forward [9], combining the increasing set of security requirements into two basic properties, called full-anonymity and full-traceability. These two basic properties were shown to imply in the case of static groups all of the existing security properties of previous scheme. Subsequent works also give formal definitions for dynamic groups [27, 10].

Such formal definitions have many benefits. They not only allow for concrete and simpler proofs of security (only two properties need be satisfied), but they also allow us to better understand what it means to be a secure group signature scheme and its implications. It also allows us to draw precise relations between group signatures and other cryptographic primitives. In fact, the implications proven in this paper are only possible in the presence of such formal models of security.

CONTRIBUTIONS. In this paper, we provide the first step towards closing the gap between what is known to be sufficient to construct secure group signatures and what is known to be necessary. We do so by showing that group signatures imply public-key encryption and thus are unlikely to be constructed based solely on the existence of one-way functions (see Figure 1).

The separation between group signatures and one-way functions is a direct consequence of our work and that of Impagliazzo and Rudich [25] which showed that any such construction would either make use of non-black-box reduction techniques or prove along the way that $P \neq NP$. Recently, in [29], Reingold, Trevisan, and Vadhan improved on that by removing the condition that $P \neq NP$. In other words, such construction would definitely have to rely on non-black-box reduction techniques. The implications of such results are of great importance since almost all reductions in cryptography are black-box.

RELATED WORK. Over the years, several results proving either implications or separations among different primitives appeared in the literature. Among the

results that are more relevant to our work are those for signatures and public-key encryption.

Since the work of Goldwasser, Micali, and Rivest [22] proposing the construction of a secure signature scheme based on claw-free pairs and laying out the foundations of standard signatures, several other works followed aiming at establishing the weakest computational assumptions on which signature schemes could be based. The first of these works was the one of Bellare and Micali [8] showing how to construct signature schemes based on any trapdoor permutations. Their work was soon followed by the work of Naor and Yung [28] showing how to build signatures from any universal one-way hash functions and by the work of Rompel [30] showing how to build signatures from any one-way function. The latter is in fact also known to be a necessary assumption.

The picture in the case of public-key encryption and other primitives that are known to be implied by it (e.g., key exchange) is not as clear as in the case of standard signatures and is still the subject of active research [29, 18, 17, 7]. Several of these results are discussed in Section 4,

Another work that is similar in spirit to our work is the one of Halevi and Krawczyk [23] which shows that password-based authentication protocols imply public-key cryptography.

ORGANIZATION. In Section 2 we recall the formal models and security definitions for (static) group signatures and public-key encryption schemes. Next, in Section 3, we show how to build a secure public-key encryption scheme from a secure group signature scheme. We then prove the security of our construction based on the anonymity property of group signatures. Finally, we conclude our paper by discussing the implications of our result in Section 4.

2 Definitions

2.1 Preliminaries

We will denote by $|m|$ the bit-length of a bit-string m . For any two arbitrary bit-strings m_0 and m_1 with $|m_0| = |m_1|$ we denote by $\text{diff}(m_0, m_1) = \{i | m_0[i] \neq m_1[i]\}$, i.e. the set of bit positions on which m_0 and m_1 are different.

As usual, a function $f(\cdot)$ is said to be negligible if for any polynomial p , there exists a natural number n_p such that $f(n) \leq \frac{1}{p(n)}$ for all $n_p \leq n$. We will say that a function of two arguments $f(\cdot, \cdot)$ is negligible, if for all polynomials p , the function g defined by $g(k) = f(k, p(k))$ is negligible.

2.2 Public Key Encryption Schemes

ENCRYPTION SCHEMES. A public-key encryption scheme $\mathcal{AE} = (\text{K}_e, \text{Enc}, \text{Dec})$ is specified, as usual, by algorithms for key generation, encryption and decryption. The security property that is most relevant for the results of this paper is *indistinguishability under chosen-plaintext attack*, in short IND-CPA.