

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

Giovanni Di Crescenzo Avi Rubin (Eds.)

Financial Cryptography and Data Security

10th International Conference, FC 2006
Anguilla, British West Indies, February 27-March 2, 2006
Revised Selected Papers

Volume Editors

Giovanni Di Crescenzo
Telcordia Technologies
One Telcordia Drive 1K325, Piscataway, NJ, USA
E-mail: giovanni@research.telcordia.com

Avi Rubin
Johns Hopkins University (JHUI SI)
3100 Wyman Park Drive, Baltimore, MD 21211 USA
E-mail: rubin@jhu.edu

Library of Congress Control Number: 2006933057

CR Subject Classification (1998): E.3, D.4.6, K.6.5, K.4.4, C.2, J.1, F.2.1-2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-46255-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-46255-2 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

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11889663 06/3142 5 4 3 2 1 0

Preface

The 10th International Conference on Financial Cryptography and Data Security (FC 2006) was held in Anguilla, British West Indies, from February 27 to March 2, 2006. This conference continues to be the premier international forum for research, advanced development, education, exploration, and debate regarding security in the context of finance and commerce.

As we were honoured to put together the program in this conference's 10th edition, we attempted to combine the naturally festive mood with its interdisciplinary nature. Kicking off the 10th-year festivities were a welcome speech by Victor Banks, the Minister of Finance of Anguilla, and our Keynote Address by the renowned cryptographer Ron Rivest. One of the most influential figures in cryptography, Ron reviewed some of his past predictions and lessons learned over the last 10 years, and prognosticated directions for the next decade. The conference also featured an invited talk by Michael Froomkin about the current legal landscape of financial cryptography, and two interesting panel sessions: one on identity management and a second one providing further reflections on the past 10 years of financial cryptography, featuring talks by Jacques Stern, and Nicko van Someren, representing reflections from the academic and industrial world, respectively. The technical program featured 19 regular papers and 6 short papers, selected out of 64 submissions, and as always, other conference attendees were invited to make short presentations during the rump session, which maintained its lively and colorful reputation.

Putting together such a strong program would not be possible without the hard work of the Program Committee and of a large number of external reviewers, whose names are listed on separate pages. Each submission was refereed by at least three experts, and often detailed technical discussions were necessary before decisions could be made. These were often challenging due to the high quality of the submitted papers, many of which could not be included in the program. Additional thanks go to all researchers who submitted papers, hoping that enough feedback was given to them for further developments of their work.

We also would like to thank this year's General Chair, Patrick McDaniel, for valuable assistance on several aspects of the conference organization, and the Local Arrangements Chair, Rafael Hirschfeld, for handling several logistics in Anguilla. Special thanks also go to Ted Lu for helping with setting up the Web-based submission and reviewing system, which was essential for handling such a large number of submissions and reviewers, and to William Enck for on-site logistic help. We hope to have fulfilled our goal of a successful conference. Like all its participants, we look forward to (at least) 10 more years of Financial Cryptography and Data Security!

Organization

The Financial Cryptography and Data Security 2006 conference was organized by the International Financial Cryptography Association (IFCA).

Program Chairs

Giovanni Di Crescenzo
Avi Rubin

Telcordia Technologies
Johns Hopkins University

General Chair

Patrick Mc Daniel

Penn State University

Local Arrangements Chair

Rafael Hirschfeld

Unipay Technologies

Program Committee

Matt Blaze
Alfredo De Santis
Sven Dietrich
Juan Garay
Dan Geer
Ari Juels
Yoshi Kohno
Arjen Lenstra

University of Pennsylvania
Università di Salerno
Carnegie Mellon University
Bell Labs
Verdasys
RSA
University of California San Diego
Bell Labs and Technische Universiteit
Eindhoven
Cybernetica AS and University of Tartu
Indiana University
University of Minnesota
NTT
Universitat Politecnica de Catalunya
NRC Canada
Ruhr-University Bochum
NEC
Carnegie Mellon University

Helger Lipmaa
Steve Myers
Andrew Odlyzko
Tatsuaki Okamoto
Carles Padro
Andrew Patrick
Ahmad-Reza Sadeghi
Kazue Sako
Dawn Song

Stuart Stubblebine	Univ. of California Davis and Stubblebine Labs
Adam Stubblefield	Independent Security Evaluators
Paul Syverson	Naval Research Lab
Mike Szydlo	RSA
Gene Tsudik	University of California Irvine
Doug Tygar	Berkeley University
Alma Whitten	Google
Yacov Yacobi	Microsoft Research
Yuliang Zheng	University of North Carolina
Moti Yung	RSA and Columbia University

Additional Referees

Michel Abdalla	Edith Elkind	Vladimir Kolesnikov
Madhukar Anand	Umberto Ferraro	Howard Lipson
Asokan	Jun Furukawa	Ferran Marques
Giuseppe Ateniese	Sabastian Gajek	Stephen Marsh
Lujo Bauer	Ulrich Huber	James Newsome
Don Beaver	Markus Jakobsson	Lluís Padro
John Bethencourt	Mariusz Jakubowski	Bryan Parno
Ziad Bizri	Mike Just	Nitesh Saxena
Daniel Bleichenbacher	Manoj Kasichainula	Kai Schramm
David Brumley	Aggelos Kiayias	Micah Sherr
Dario Catalano	Larry Korba	Ronggong Song
Liqun Chen	Howard Lipson	Isamu Teranishi
Yuqun Chen	Philip MacKenzie	Ersin Uzun
Monica Chew	Peter Montgomery	Jason Waddle
Paolo D'Arco	Kengo Mori	Shouhuai Xu
Breno de Medeiros	Jihye Kim	
Yevgeniy Dodis	Lea Kissner	

Sponsors

EverBank (Silver sponsor)
Navio (Silver sponsor)
Offshore Information Services (Silver sponsor)
Google (Bronze sponsor)
NCipher (Bronze sponsor)
Bibit (Sponsor in kind)

Table of Contents

Authentication and Fraud Detection

Phoolproof Phishing Prevention	1
<i>Bryan Parno, Cynthia Kuo, Adrian Perrig</i>	
A Protocol for Secure Public Instant Messaging	20
<i>Mohammad Mannan, Paul C. van Oorschot</i>	
Using Automated Banking Certificates to Detect Unauthorised Financial Transactions	36
<i>C. Corzo, F. Corzo S., N. Zhang, A. Carpenter</i>	

Privacy

Privacy in Encrypted Content Distribution Using Private Broadcast Encryption	52
<i>Adam Barth, Dan Boneh, Brent Waters</i>	
A Private Stable Matching Algorithm	65
<i>Philippe Golle</i>	
Private Policy Negotiation	81
<i>Klaus Kursawe, Gregory Neven, Pim Tuyls</i>	

Reputation and Mix-Nets

Uncheatable Reputation for Distributed Computation Markets	96
<i>Bogdan Carbunar, Radu Sion</i>	
An Efficient Publicly Verifiable Mix-Net for Long Inputs	111
<i>Jun Furukawa, Kazuo Sako</i>	
Auditable Privacy: On Tamper-Evident Mix Networks	126
<i>Jong Youl Choi, Philippe Golle, Markus Jakobsson</i>	

Short Papers

A Practical Implementation of Secure Auctions Based on Multiparty Integer Computation	142
<i>Peter Bogetoft, Ivan Damgård, Thomas Jakobsen, Kurt Nielsen, Jakob Pagter, Tomas Toft</i>	

Defeating Malicious Servers in a Blind Signatures Based Voting System 148
Sébastien Canard, Matthieu Gaud, Jacques Traoré

Pairing Based Threshold Cryptography Improving on Libert-Quisquater and Baek-Zheng 154
Yvo Desmedt, Tanja Lange

Credit Transfer for Market-Based Infrastructure 160
Tyler Close

A Note on Chosen-Basis Decisional Diffie-Hellman Assumptions..... 166
Michael Szydło

Cryptanalysis of a Partially Blind Signature Scheme or *How to Make \$100 Bills with \$1 and \$2 Ones* 171
Gwenaëlle Martinet, Guillaume Poupard, Philippe Sola

Conditional Financial Cryptography

A Generic Construction for Token-Controlled Public Key Encryption 177
David Galindo, Javier Herranz

Timed-Release and Key-Insulated Public Key Encryption 191
Jung Hee Cheon, Nicholas Hopper, Yongdae Kim, Ivan Osipkov

Conditional Encrypted Mapping and Comparing Encrypted Numbers 206
Ian F. Blake, Vladimir Kolesnikov

Revisiting Oblivious Signature-Based Envelopes..... 221
Samad Nasserian, Gene Tsudik

Payment Systems

Provably Secure Electronic Cash Based on Blind Multisignature Schemes 236
Yoshikazu Hanatani, Yuichi Komano, Kazuo Ohta, Noboru Kunihiro

Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings 251
Xiaofeng Chen, Fangguo Zhang, Yi Mu, Willy Susilo

Privacy-Protecting Coupon System Revisited	266
<i>Lan Nguyen</i>	

Efficient Protocols

Efficient Broadcast Encryption Scheme with Log-Key Storage	281
<i>Yong Ho Hwang, Pil Joong Lee</i>	

Efficient Correlated Action Selection	296
<i>Mikhail J. Atallah, Marina Blanton, Keith B. Frikken, Jiangtao Li</i>	

Efficient Cryptographic Protocols Realizing E-Markets with Price Discrimination	311
<i>Aggelos Kiayias, Moti Yung</i>	

Author Index	327
-------------------------------	-----