

*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*

Andrew S. Patrick Moti Yung (Eds.)

# Financial Cryptography and Data Security

9th International Conference, FC 2005  
Roseau, The Commonwealth of Dominica  
February 28 – March 3, 2005  
Revised Papers



Springer

## Volume Editors

Andrew S. Patrick  
National Research Council of Canada  
1200 Montreal Road, Ottawa, ON, Canada K1A 0R6  
E-mail: Andrew.Patrick@nrc-cnrc.gc.ca

Moti Yung  
RSA Laboratories and Columbia University  
Computer Science, 1214 Amsterdam Ave., New York, NY, USA  
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2005928164

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

ISSN	0302-9743
ISBN-10	3-540-26656-9 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-26656-3 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](http://springeronline.com)

© Springer-Verlag Berlin Heidelberg 2005  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 11507840      06/3142      5 4 3 2 1 0

## Preface

The 9th International Conference on Financial Cryptography and Data Security (FC 2005) was held in the Commonwealth of Dominica from February 28 to March 3, 2005. This conference, organized by the International Financial Cryptography Association (IFCA), continues to be the premier international forum for research, exploration, and debate regarding security in the context of finance and commerce. The conference title and scope was expanded this year to cover all aspects of securing transactions and systems. The goal is to build an interdisciplinary meeting, bringing together cryptographers, data-security specialists, business and economy researchers, as well as economists, IT professionals, implementers, and policy makers.

We think that this goal was met this year. The conference received 90 submissions and 24 papers were accepted, 22 in the Research track and 2 in the Systems and Applications track. In addition, the conference featured two distinguished invited speakers, Bezalel Gavish and Lynne Coventry, and two interesting panel sessions, one on phishing and the other on economics and information security. Also, for the first time, some of the papers that were judged to be very strong but did not make the final program were selected for special invitation to our Works in Progress (Rump) Session that took place on Wednesday evening. Three papers were highlighted in this forum this year, and short versions of the papers are included here. As always, other conference attendees were also invited to make presentations during the rump session, and the evening lived up to its colorful reputation.

Putting together such a strong program would not be possible without the hard work of the Program Committee, whose members are listed on a separate page. In addition, a large number of external reviewers were recruited because of their special expertise in particular areas, and their names are also listed in these proceedings. Each of the submissions was reviewed by at least three experts, who then engaged in vigorous online discussions. The selection process was difficult because there were many excellent papers that could not be fit into the program. We want to thank all the authors who submitted papers, and we hope that the feedback they received was useful for continuing to develop their work, whether their papers were accepted or not.

We also want to thank this year's General Chair, Stuart Schechter, for valuable assistance and for handling the arrangements in Dominica, and Ari Juels for moderating the rump session. Special thanks also go out to Aggelos Kiayias for setting up and operating the Web-based reviewing system that was essential for handling such a large number of submissions and reviewers.

We hope that this year's program was in the spirit of the conference goals as envisioned, and that the conference continues its colorful tradition as an interdisciplinary, high diversity meeting that helps foster cooperation and the fruitful exchange of ideas among its international participants.

# Financial Cryptography and Data Security 2005

**Program Chairs:** Andrew Patrick and Moti Yung

**General Chair:** Stuart Schechter

## Program Committee

Colin Boyd	Queensland University of Technology
Suresh Chari	IBM
Liquan Chen	HP Labs
Lynne Coventry	NCR
Yvo Desmedt	University College London
Giovanni Di Crescenzo	Telcordia Technologies
Roger Dingledine	Moria Research Labs
Scott Flinn	National Research Council of Canada
Juan Garay	Bell Labs, Lucent Technologies
Dan Geer	Geer Risk Services
Craig Gentry	DoCoMo Labs USA
Mike Just	Treasury Board of Canada
Aggelos Kiayias	University of Connecticut
Helger Lipmaa	Helsinki University of Technology
David M'Raihi	Verisign
Kobbi Nissim	Microsoft
Satoshi Obana	Columbia University and NEC
Andrew Odlyzko	University Minnesota
Pascal Paillier	Gemplus
David Pointcheval	Ecole Normale Supérieure
Bart Preneel	Katholieke Universiteit Leuven
Angela Sasse	University College London
Berry Schoenmakers	Technische Universiteit Eindhoven
Sean Smith	Dartmouth College
Jessica Staddon	Palo Alto Research Center (PARC)
Michael Szydło	RSA Laboratories
Jacques Traore	France Télécom
Gene Tsudik	University of California, Irvine
Alma Whitten	Google
Adam Young	Cigital
Bill Yurcik	NCSA

## Sponsors

Gold Sponsor:	Interactive Investor ( <a href="http://www.iii.co.uk">www.iii.co.uk</a> )
Bronze Sponsors:	RSA Security France Télécom
In-Kind Sponsor:	Bibit Global Payment Services

## External Reviewers

Michel Abdalla  
Gildas Avoine  
Alexandra Boldyreva  
Calude Castelluccia  
George Danezis  
Alex Deacon  
Glenn Durfee  
Renwei Ge  
Rosario Gennaro  
Henri Gilbert  
Marc Girault  
David Goldberg  
Philippe Golle  
Juan Gonzalez  
Rachel Greenstadt  
Shai Halevi  
Helena Handschuh  
Yvonne Hitchcock  
Kevin Soo Hoo  
Markus Jakobsson  
Stas Jarecki  
Charanjit Jutla  
Sébastien Kunz-Jacques  
Joseph Lano

John Malone-Lee  
Nick Mathewson  
Sean Murphy  
Steve Myers  
Gregory Neven  
Jean-Claude Pailles  
Valeria de Paiva  
Duong Hieu Phan  
Tal Rabin  
Yona Raekow  
Zulfikar Ramzan  
Josyula R. Rao  
Jason Reid  
Pankaj Rohatgi  
Markku-Juhani O. Saarinen  
Marius Schilder  
Umesh Shankar  
Vitaly Shmatikov  
Paul Syverson  
Jun'ichi Takeuchi  
Yiannis Tsiounis  
Yunlei Zhao  
Hong-Sheng Zhou

# Table of Contents

## Threat and Attacks

Fraud Within Asymmetric Multi-hop Cellular Networks <i>Gildas Avoine</i> .....	1
Protecting Secret Data from Insider Attacks <i>David Dagon, Wenke Lee, Richard Lipton</i> .....	16
Countering Identity Theft Through Digital Uniqueness, Location Cross-Checking, and Funneling <i>Paul C. van Oorschot, S. Stubblebine</i> .....	31

## Invited Speaker

Trust and Swindling on the Internet <i>Bezael Gavish</i> .....	44
---	----

## Digital Signing Methods

Identity-Based Partial Message Recovery Signatures (or How to Shorten ID-Based Signatures) <i>Fanguo Zhang, Willy Susilo, Yi Mu</i> .....	45
Time Capsule Signature <i>Yevgeniy Dodis, Dae Hyun Yum</i> .....	57
Policy-Based Cryptography and Applications <i>Walid Bagga, Refik Molva</i> .....	72

## Panel

A Chat at the Old Phishin' Hole <i>Richard Clayton, Drew Dean, Markus Jakobsson, Steven Myers, Stuart Stubblebine, Michael Szydlo</i> .....	88
Modeling and Preventing Phishing Attacks <i>Markus Jakobsson</i> .....	89

Helping the Phish Detect the Lure <i>Steven Myers</i> .....	90
Who'd Phish from the Summit of Kilimanjaro? <i>Richard Clayton</i> .....	91

## Privacy

A Privacy-Protecting Coupon System <i>Liqun Chen, Matthias Enzmann, Ahmad-Reza Sadeghi, Markus Schneider, Michael Steiner</i> .....	93
Testing Disjointness of Private Datasets <i>Aggelos Kiayias, Antonina Mitrofanova</i> .....	109

## Hardware Oriented Mechanisms

RFID Traceability: A Multilayer Problem <i>Gildas Avoine, Philippe Oechslin</i> .....	125
Information-Theoretic Security Analysis of Physical Uncloable Functions <i>Pim Tuyls, Boris Škorić, Sjoerd Stallinga, A.H.M. Akkermans, Wil Ophey</i> .....	141

## Supporting Financial Transactions

Risk Assurance for Hedge Funds Using Zero Knowledge Proofs <i>Michael Szydlo</i> .....	156
Probabilistic Escrow of Financial Transactions with Cumulative Threshold Disclosure <i>Stanisław Jarecki, Vitaly Shmatikov</i> .....	172

## Systems, Applications, and Experiences

Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce <i>Simson L. Garfinkel, Jeffrey I. Schiller, Erik Nordlander, David Margrave, Robert C. Miller</i> .....	188
Securing Sensitive Data with the Ingrian DataSecure Platform <i>Andrew Koyfman</i> .....	203

Ciphire Mail Email Encryption and Authentication <i>Lars Eilebrecht</i> .....	211
--	-----

## Message Authentication

A User-Friendly Approach to Human Authentication of Messages <i>Jeff King, Andre dos Santos</i> .....	225
--	-----

Approximate Message Authentication and Biometric Entity Authentication <i>Giovanni Di Crescenzo, Richard Graveman, Renwei Ge, Gonzalo Arce ....</i>	240
--	-----

## Exchanges and Contracts

Analysis of a Multi-party Fair Exchange Protocol and Formal Proof of Correctness in the Strand Space Model <i>Aybek Mukhamedov, Steve Kremer, Eike Ritter</i> .....	255
---	-----

Achieving Fairness in Private Contract Negotiation <i>Keith Frikken, Mikhail Atallah</i> .....	270
---	-----

## Auctions and Voting

Small Coalitions Cannot Manipulate Voting <i>Edith Elkind, Helger Lipmaa</i> .....	285
---	-----

Efficient Privacy-Preserving Protocols for Multi-unit Auctions <i>Felix Brandt, Tuomas Sandholm</i> .....	298
--	-----

Event Driven Private Counters <i>Eu-Jin Goh, Philippe Golle</i> .....	313
--	-----

## Works in Progress

Secure Distributed <i>Human</i> Computation <i>Craig Gentry, Zulfikar Ramzan, Stuart Stubblebine</i> .....	328
---	-----

Secure Multi-attribute Procurement Auction <i>Koutarou Suzuki, Makoto Yokoo</i> .....	333
--	-----

Audit File Reduction Using N-Gram Models <i>Fernando Godínez, Dieter Hutter, Raúl Monroy</i> .....	336
---	-----

**User Authentication**

Interactive Diffie-Hellman Assumptions with Applications  
to Password-Based Authentication  
    *Michel Abdalla, David Pointcheval* ..... 341

Secure Biometric Authentication for Weak Computational Devices  
    *Mikhail J. Atallah, Keith B. Frikken, Michael T. Goodrich,*  
    *Roberto Tamassia* ..... 357

Panel Summary: Incentives, Markets and Information Security  
    *Allan Friedman* ..... 372

**Author Index** ..... 375