

FC'05: Financial Cryptography and Data Security

<http://www.ifca.ai/fc05/>



**Ninth International Conference
February 28 - March 3, 2005
Roseau, The Commonwealth Of Dominica**

Call for Papers

Submissions Due Date: September 10, 2004

Program Chairs: Andrew Patrick (NRC Canada) and Moti Yung (Columbia University)

General Chair: Stuart Schechter (Harvard University)

Financial Cryptography and Data Security (FC'05) is the premier international forum for research, advanced development, education, exploration, and debate regarding security in the context of finance and commerce. We have augmented our conference title and expanded our scope to cover all aspects of securing transactions and systems. These aspects include a range of technical areas such as: cryptography, payment systems, secure transaction architectures, software systems and tools, user and operator interfaces, fraud prevention, secure IT infrastructure, and analysis methodologies. Our focus will also encompass legal, financial, business and policy aspects. Material both on theoretical (fundamental) aspects of securing systems and on secure applications and real-world deployments will be considered.

The conference goal is to bring together top cryptographers, data-security specialists, and scientists with economists, bankers, implementers, and policy makers. Intimate and colorful by tradition, the FC'05 program will feature invited talks, academic presentations, technical demonstrations, and panel discussions. This conference is organized annually by the International Financial Cryptography Association (IFCA).

Original papers and presentations on all aspects of financial and commerce security are invited. Submissions must have a visible bearing on financial and commerce security issues, but can be interdisciplinary in nature and need not be exclusively concerned with cryptography or security. Possible topics for submission to the various sessions include, but are not limited to:

- | | |
|---|--|
| <ul style="list-style-type: none">* Anonymity and Privacy* Auctions* Audit and Auditability* Authentication and Identification, including Biometrics* Certification and Authorization* Commercial Cryptographic Applications* Commercial Transactions and Contracts* Digital Cash and Payment Systems* Digital Incentive and Loyalty Systems* Digital Rights Management* Financial Regulation and Reporting* Fraud Detection* Game Theoretic Approaches to Security* Infrastructure Design* Legal and Regulatory Issues | <ul style="list-style-type: none">* Microfinance and Micropayments* Monitoring, Management and Operations* Reputation Systems* RFID-Based and Contactless Payment Systems* Risk Assessment and Management* Secure Banking* Secure Financial Web Services* Securing Emerging Computational Paradigms* Security and Risk Perceptions and Judgments* Security Economics* Smart Cards and Secure Tokens* Trust Management* Trustability and Trustworthiness* Underground-Market Economics* Usability and Acceptance of Security Systems* User and Operator Interfaces |
|---|--|

Submission Instructions

Submission Categories

FC'05 is inviting submissions in three categories: (1) research papers, (2) systems and applications presentations, (3) panel sessions. For all accepted submissions, at least one author must attend the conference and present the work.

Research Papers

Research papers should describe novel scientific contributions to the field, and they will be subject to vigorous peer review. Papers can be a maximum of 15 pages in length (including references and appendices), and accepted submissions will be published in full in the conference proceedings.

Systems and Application Presentations

Submissions in this category should describe novel or successful systems with an emphasis on secure digital commerce applications. Presentations may concern commercial systems, academic prototypes, or open-source projects for any of the topics listed above. Where appropriate, software or hardware demonstrations are encouraged as part of the presentations in these sessions. Submissions in this category should consist of a short summary of the work (1-6 pages in length) to be reviewed by the Program Committee, along with a short biography of the presenters. Accepted submissions will be presented at the conference (25 minutes per presentation), and a one-page abstract will be published in the conference proceedings.

Panel Sessions

Proposals for panel sessions are also solicited, and should include a brief description of the panel as well as prospective participants. Accepted panel sessions will be presented at the conference, and each participant will contribute a one-page abstract to be published in the conference proceedings.

Program Committee:

Colin Boyd	Queensland University of Technology
Liqun 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	U Connecticut
Helger Lipmaa	Helsinki U Technology
David M'Raihi	Verisign
Kobbi Nissim	Microsoft
Satoshi Obana	Columbia U and NEC
Andrew Odlyzko	U 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 Szydlo	RSA Laboratories
Jacques Traore	France Telecom
Gene Tsudik	U California, Irvine
Alma Whitten	Google
Adam Young	Cigital
Bill Yurcik	NCSA