Financial Cryptography and Data Security

April 1 – 5, 2013, Busena Terrace Beach Resort, Okinawa, Japan

http://fc13.ifca.ai/

Financial Cryptography and Data Security is a major international forum for research, advanced development, education, exploration, and debate regarding information assurance, with a specific focus on commercial contexts. The conference covers all aspects of securing transactions and systems. Original works focusing on both fundamental and applied real- world deployments on all aspects surrounding commerce security are solicited. Submissions need not be exclusively concerned with cryptography. Systems security and inter-disciplinary works are particularly encouraged.

TOPICS

Anonymity & Privacy,
Auctions & Audits,
Authentication & Identification,
Biometrics,
Certification & Authorization,
Cloud Computing Security,
Commercial Cryptographic Applications,
Data Outsourcing Security,
Information Security,
Game Theoretic Security,
Securing Emerging Computational Paradigms,
Identity Theft,
Fraud Detection,
Phishing & Social Engineering,
Digital Rights Management,

Digital Cash & Payment Systems,
Digital Incentive & Loyalty Systems,
Microfinance & Micropayments,
Contactless Payment & Ticketing Systems,
Secure Banking & Financial Web Services,
Security & Privacy in Mobile Devices & Applications,
Security & Privacy in Automotive & Transport Systems & Applications
Smartcards, Secure Tokens & Secure Hardware,
Privacy-enhancing Systems,
Reputation Systems,
Security & Privacy in Social Networks,
Security & Privacy in Sound & Secure Financial Systems Based on Social

Networks,
Smart Meters Security and Privacy,
Risk Assessment & Management,
Risk Perceptions & Judgments,
Legal & Regulatory Issues,
Security Economics,
Spam,
Transactions & Contracts,
Trust Management,
Underground-Market Economics,
Usable Security,
Virtual Economies,
Voting Systems.

CALL FOR PAPERS, PANELS, WORKSHOPS & IMPORTANT DATES

Submissions are sought in the following categories: *(i)* **regular papers** (15 pg LNCS format including references and maximum of 18 pg, i.e., 3 pg appendices), *(ii)* **short papers** (8 pg LNCS format in total), *(iii)* **panels** and **workshops** (2 pg), and *(iv)* posters (1 pg). Committee members are not required to read the appendices, so the full papers should be intelligible without them. **The paper submission must be anonymous, with no author names, affiliations, acknowledgements, or obvious references.** More information at: **http://fc13.ifca.ai/**

Workshop Proposal Submission: **July 23, 2012** (notification on August 20, 2012)
Paper Submission: **October 13, 2012** (notification on December 23, 2012)
Poster and Panel Submission: **December 22, 2012** (notification on January 14, 2013)
Final Papers: **January 12, 2013**

ORGANIZERS & PROGRAM COMMITTEE

General Chair: Kazue Sako, NEC, Japan
Program Chair: Ahmad-Reza Sadeghi, Technische Universität Darmstadt and Fraunhofer SIT Darmstadt, Germany

Alessandro Acquisti, *Carnegie Mellon University, USA*
Ross Anderson, *Cambridge University, UK*
Rainer Boehme, *University of Münster, Germany*
Jens Bohli, *NEC Laboritories Europe, Germany*
Colin Boyd, *Queensland University of Technology, Australia*
Liqun Chen, *Hewlett-Packard Laboratories, UK*
Sherman S.M. Chow, *University of Waterloo, Canada / Chinese University of Hong Kong, China*
Nicolas Christin, *Carnegie Mellon University, USA*
Reza Curtmola, *New Jersey Institute of Technology, USA*
George Danezis, *Microsoft Research Cambridge, UK*
Emiliano De Cristofaro, *PARC, USA*
Mina Deng, *Philips Research, The Netherlands*
Loïc Duflot, *ANSSI - French Network and Information Security Agency, France*
William Enck, *North Carolina State University, USA*
Feng Bao, *Institute for Infocomm Research, Singapore*

Jens Grossklags, *Penn State University, USA*
Xuxian Jiang, *North Carolina State University, USA*
Ari Juels, *RSA Laboratories, USA*
Stefan Katzenbeisser, *TU Darmstadt, Germany*
Angelos Keromytis, *Columbia University, USA*
Florian Kerschbaum, *SAP Research, Germany*
Aggelos Kiayias, *University of Connecticut, USA*
Yuichi Komano, *Toshiba Corporation, Japan*
Kari Kostiainen, *Nokia Research Center, Finland*
Farinaz Koushanfar, *Rice University, USA*
Xuejia Lai, *Shanghai Jiaotong University, China*
Jiangtao Li, *Intel Corporation, USA*
Benoit Libert, *Universite Catholique de Louvain, Belgium*
Di Ma, *University of Michigan-Dearborn, USA*
Mark Manulis, *University of Surrey, UK*
Kanta Matsuura, *University of Tokyo, Japan*
Atsuko Miyaji, *Japan Advanced Institute of Science and Technology, Japan*
Refik Molva, *EURECOM, France*

Toru Nakanishi, *Okayama University, Japan*
Satoshi Obana, *Hosei University, Japan*
Eiji Okamoto, *University of Tsukuba, Japan*
Claudio Orlandi, *Bar-Ilan University, Israel*
Josef Pieprzyk, *Macquarie University, Australia*
Benny Pinkas, *Bar Ilan University, Israel*
Bart Preneel, *Katholieke Universiteit Leuven (COSIC), Belgium*
Thomas Schneider, *TU Darmstadt, Germany*
Jamshid Shokrollahi, *Robert Bosch GmbH, Germany*
Matthew Smith, *Leibniz Universität Hannover, Germany*
Keiji Takeda, *Keio University, Japan*
Isamu Teranishi, *NEC, Japan*
Patrick Traynor, *Georgia Institute of Technology, USA*
Ersin Uzun, *PARC, USA*
Michael Wiener, *Irdeto, Canada*
Akira Yamada, *KDDI R&D Labs, Japan*

FURTHER SUBMISSION INFORMATION

Papers must be formatted in standard LNCS format and submitted as PDF files. Submissions in other formats will be rejected. All papers must be submitted electronically according to the instructions and forms found on the submission site. Post-proceedings of the event will be published by Springer in the Lecture Notes in Computer Science series.

Authors may only submit work that does not substantially overlap with work that is currently submitted or has been accepted for publication to a conference/workshop with proceedings or a journal. We consider double submission serious research fraud and will treat it as such. In case of doubt contact the program chair for any clarifications at *fc13chair@ifca.ai.*

Regular Research Papers. Research papers should describe novel, previously unpublished scientific contributions to the field, and they will be subject to rigorous peer review. Accepted submissions will be included in the conference proceedings to be published in the Springer-Verlag Lecture Notes in Computer Science (LNCS) series. Submissions are limited to 15 pages including references and maximum of 18 pages (i.e., 3 pages of appendices). Committee members are not required to read the appendices, so the full papers should be intelligible without them.

Short Papers. Short papers are also subject to peer review, however, the intention is to encourage authors to introduce work in progress, novel applications and corporate/industrial experiences. Short papers will be evaluated with a focus on novelty and potential for sparking participants' interest and future research avenues. Short paper submissions are limited to 8 pages in standard LNCS format in total. The paper title for short papers must include the text '(short paper)'.

Panel Proposals. We especially would like to encourage submissions of panel proposals. These should include a very brief description of the panel topics, as well as of the prospective panelists. Accepted panel sessions will be presented at the conference. Moreover, each participant will contribute a one-page abstract to be published in the conference proceedings. Please feel free to contact us directly if you would like to further discuss the suitability of a certain topic. Panel submissions should be up to 2 pages, sent to *fc13chair@ifca.ai.*

Posters. The poster session is the perfect venue to share a provocative opinion, interesting established or preliminary work, or a cool idea that will spark discussion. Poster presenters will benefit from a multi-hour session to discuss their work, get exposure, and receive feedback from attendees. Poster submissions should be 1 page (in the same LNCS format). Please keep in mind that the poster deadline is later than the main paper submission deadline. The posters will be published in the proceedings. Poster proposals should be sent to the posters chair at *fc13chair@ifca.ai.*

Workshop Proposals. Proposals for workshops to be held at FC 2013 are also solicited. A workshop can be full day or half day in length. Workshop proposals should include: (i) a title, (ii) a call for papers, (iii) a brief summary and justification – including how it would fit into the greater FC scope, (iv) a (tentative) Program Committee and its Chair, (v) one-paragraph biographies for key organizers, and (vi) the expected (or previous – if workshop has been held in previous years) number of submissions, participants and acceptance rates. Workshop proposals should be sent *fc13workshops@ifca.ai.*

The Rump Session. FC'13 will also include the popular "rump session" held on one of the evenings in an informal, social atmosphere. The rump session is a program of short (5-7 minute), informal presentations on works in progress, off-the- cuff ideas, and any other matters pertinent to the conference. Any conference attendee is welcome to submit a presentation to the Rump Session Chair (to be announced at the conference). This submission should consist of a talk title, the name of the presenter, and, if desired, a very brief abstract. Submissions may be sent via e-mail, or submitted in person in the morning on the day of the session.

The Financial Cryptography and Data Security Conference is organized by The International Financial Cryptography Association (IFCA).