1. Record Nr. UNISA996465565203316

Titolo	Financial Cryptography [[electronic resource]] : 8th International Conference, FC 2004, Key West, FL, USA, February 9-12, 2004. Revised Papers / / edited by Ari Juels
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-27809-5
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XI, 286 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3110
Disciplina	332/.0285/582
Soggetti	Finance Data encryption (Computer science) Operating systems (Computers) Management information systems Computer science Computers and civilization Computer communication systems Finance, general Cryptology Operating Systems Management of Computing and Information Systems Computers and Society Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Invited Talks -- Analyzing the Success and Failure of Recent e-Payment Schemes -- Peppercoin Micropayments -- Loyalty and Micropayment Systems -- Microcredits for Verifiable Foreign Service Provider Metering -- A Privacy-Friendly Loyalty System Based on Discrete Logarithms over Elliptic Curves -- User Authentication -- Addressing Online Dictionary Attacks with Login Histories and Humans-in-the-Loop -- Call Center Customer Verification by Query-Directed Passwords -- Invited Talks -- Cryptography and the French Banking Cards: Past, Present, Future --

PayPass Security and Risk -- e-Voting -- The Vector-Ballot e-Voting Approach -- Efficient Maximal Privacy in Boardroom Voting and Anonymous Broadcast -- Panel Session: Building Usable Security Systems -- Usability and Acceptability of Biometric Security Systems -- Mental Models of Computer Security -- Visualization Tools for Security Administrators -- Secure Interaction Design -- Invited Talk -- Bringing Payment Technology to the Unbanked -- Auctions and Lotteries -- Interleaving Cryptography and Mechanism Design -- Secure Generalized Vickrey Auction without Third-party Servers -- Electronic National Lotteries -- Identity-Based Chameleon Hash and Applications -- Game Theoretic and Cryptographic Tools -- Selecting Correlated Random Actions -- An Efficient and Usable Multi-show Non-transferable Anonymous Credential System -- The Ephemeral Pairing Problem -- Mix Networks and Anonymous Communications -- Mixminion: Strong Anonymity for Financial Cryptography -- Practical Anonymity for the Masses with MorphMix -- Timing Attacks in Low-Latency Mix Systems -- Provable Unlinkability against Traffic Analysis.

Sommario/riassunto

The 8th Annual Financial Cryptography Conference was held during 9–12 February 2004 in Key West, Florida, USA. The conference was organized by the - international Financial Cryptography Association (IFCA). The program committee, which comprised 25 members, reviewed 78 submissions, of which only 17 were accepted for presentation at the conference. This year’s conference differed somewhat from those of previous years in its consideration of papers devoted to implementation, rather than purely conceptual research; one of these submissions was presented at the conference. This represented a movement in the conference toward practical problems and real-world perspectives as a complement to more traditional academic forms of research. In this spirit, the program included a number of excellent invited speakers. In the opening talk of the conference, Jack Selby threw down the gauntlet, - scribing some of the achievements of the PayPal system, but also enumerating reasons for the failures of many elegant e-cash schemes in the past. Ron Rivest, in contrast, described an emerging success in the cleverly conceived Peppercoin micropayment system. Jacques Stern enlightened us with his experience in the cryptographic design of banking cards in France. Simon Pugh unveiled some - tails of anew generation of wireless credit card. Finally,in deference to the many consumers in the world lacking either techno-savvy or technological resources that we often too easily take for granted, Jon Peha described a elded banking system that avoids reliance on conventional financial infrastructures. Thanks to all of these speakers for rounding out the conference with their expertise and breadth of vision.