1. Record Nr.   UNINA9910144125403321

Titolo   Financial cryptography : 6th International Conference, FC 2002, Southampton, Bermuda, March 11-14, 2002 : revised papers / / Matt Blaze, editor

Pubbl/distr/stampa   Berlin, Germany : , : Springer, , [2003]
©2003

ISBN   3-540-36504-4

Edizione   [1st ed. 2003.]

Descrizione fisica   1 online resource (309 p.)

Collana   Lecture Notes in Computer Science, , 0302-9743 ; ; 2357

Disciplina   332.10285

Soggetti   Electronic funds transfers - Security measures
Data encryption (Computer science)
Electronic commerce - Security measures

Lingua di pubblicazione   Inglese

Formato   Materiale a stampa

Livello bibliografico   Monografia

Note generali   Description based upon print version of record.

Nota di bibliografia   Includes bibliographical references and index.

Nota di contenuto   E-voting without 'Cryptography' -- An Implementation of a Universally Verifiable Electronic Voting Scheme Based on Shuffling -- Financial Instruments in Recommendation Mechanisms -- Secure Combinatorial Auctions by Dynamic Programming with Polynomial Secret Sharing -- A Second-Price Sealed-Bid Auction with Verifiable Discriminant of p 0-th Root -- A Two-Server, Sealed-Bid Auction Protocol -- Secure Vickrey Auctions without Threshold Trust -- Almost Optimal Hash Sequence Traversal -- Cryptographic Primitives Enforcing Communication and Storage Complexity -- CryptoComputing with Rationals -- Privacy Tradeoffs: Myth or Reality? -- An Improved Fast Signature Scheme without Online Multiplication -- Timed Release of Standard Digital Signatures -- Quasi-Efficient Revocation of Group Signatures -- The Dark Side of Threshold Cryptography -- Split-and-Delegate: Threshold Cryptography for the Masses -- Redistribution of Mechanical Secret Shares -- Reliable MIX Cascade Networks through Reputation -- Offline Payments with Auditable Tracing -- Fileteller: Paying and Getting Paid for File Storage.

Sommario/riassunto   The Sixth International Financial Cryptography Conference was held during March 11-14, 2002, in Southampton, Bermuda. As is customary

at FC, these proceedings represent "final" versions of the papers presented, revised to take into account comments and discussions from the conference. Submissions to the conference were strong, with 74 papers submitted and 19 accepted for presentation and publication. (Regrettably, three of the submit- ted papers had to be summarily rejected after it was discovered that they had been improperly submitted in parallel to other conferences.) The small program committee worked very hard under a tight schedule (working through Christmas day) to select the program. No program chair could ask for a better committee; my thanks to everyone for their hard work and dedication. In addition to the refereed papers, the program included a welcome from the Minister of Telecommunications and e-Commerce, Renee Webb, a keynote address by Nigel Hickson, and a panel on privacy tradeoffs cheiired by Rebecca Wright (with panelists Ian Goldberg, Ron Rivest, and Graham Wood). The traditional Tuesday evening "rump session" was skillfully officiated by Markus Jakobsson. My job as program chair was made much, much easier by the excellent work of our general chair, Nicko van Someren, who performed the miracle of hiding from me any evidence of the innumerable logistical nightmares associated with conducting this conference. I have no idea how he did it, but it must have involved many sleepless nights.