1. Record Nr. UNISA996465824003316

Titolo	Financial Cryptography and Data Security [[electronic resource]] : 9th International Conference, FC 2005, Roseau, The Commonwealth Of Dominica, February 28 - March 3, 2005, Revised Papers / / edited by Andrew S. Patrick, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 376 p.)
Collana	Security and Cryptology ; ; 3570
Disciplina	005.8/2
Soggetti	Cryptography Data encryption (Computer science) Operating systems (Computers) Electronic data processing—Management Computers and civilization Computer networks Algorithms Cryptology Operating Systems IT Operations 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	Threat and Attacks -- Fraud Within Asymmetric Multi-hop Cellular Networks -- Protecting Secret Data from Insider Attacks -- Countering Identity Theft Through Digital Uniqueness, Location Cross-Checking, and Funneling -- Invited Speaker -- Trust and Swindling on the Internet -- Digital Signing Methods -- Identity-Based Partial Message Recovery Signatures (or How to Shorten ID-Based Signatures) -- Time Capsule Signature -- Policy-Based Cryptography and Applications -- Panel -- A Chat at the Old Phishin’ Hole -- Modeling and Preventing

Phishing Attacks -- Helping the Phish Detect the Lure -- Who'd Phish from the Summit of Kilimanjaro? -- Privacy -- A Privacy-Protecting Coupon System -- Testing Disjointness of Private Datasets -- Hardware Oriented Mechanisms -- RFID Traceability: A Multilayer Problem -- Information-Theoretic Security Analysis of Physical Uncloneable Functions -- Supporting Financial Transactions -- Risk Assurance for Hedge Funds Using Zero Knowledge Proofs -- Probabilistic Escrow of Financial Transactions with Cumulative Threshold Disclosure -- Systems, Applications, and Experiences -- Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce -- Securing Sensitive Data with the Ingrian DataSecure Platform -- Ciphire Mail Email Encryption and Authentication -- Message Authentication -- A User-Friendly Approach to Human Authentication of Messages -- Approximate Message Authentication and Biometric Entity Authentication -- Exchanges and Contracts -- Analysis of a Multi-party Fair Exchange Protocol and Formal Proof of Correctness in the Strand Space Model -- Achieving Fairness in Private Contract Negotiation -- Auctions and Voting -- Small Coalitions Cannot Manipulate Voting -- Efficient Privacy-Preserving Protocols for Multi-unit Auctions -- Event Driven Private Counters -- Works in Progress -- Secure Distributed Human Computation -- Secure Multi-attribute Procurement Auction -- Audit File Reduction Using N-Gram Models -- User Authentication -- Interactive Diffie-Hellman Assumptions with Applications to Password-Based Authentication -- Secure Biometric Authentication for Weak Computational Devices -- Panel Summary: Incentives, Markets and Information Security.

Sommario/riassunto

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.