1. Record Nr. UNISA996465942703316

Titolo	Financial cryptography and data security : 12th international conference, FC 2008, Cozumel, Mexico, January 28-31, 2008 ; revised selected papers / / Gene Tsudik (eds)
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2008] ©2008
ISBN	3-540-85230-1
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XIII, 326 p.)
Collana	Security and Cryptology ; ; 5143
Disciplina	332.1028
Soggetti	Information Systems Computer security Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Attacks and Counter Measures I -- Quantifying Resistance to the Sybil Attack -- Evaluating the Wisdom of Crowds in Assessing Phishing Websites -- Don’t Clog the Queue! Circuit Clogging and Mitigation in P2P Anonymity Schemes -- An Efficient Deniable Key Exchange Protocol (Extended Abstract) -- Revisiting Pairing Based Group Key Exchange -- Constant-Round Password-Based Authenticated Key Exchange Protocol for Dynamic Groups -- A Practical Universal Circuit Construction and Secure Evaluation of Private Functions -- Generalized Non-Interactive Oblivious Transfer Using Count-Limited Objects with Applications to Secure Mobile Agents -- PBS: Private Bartering Systems -- Breaking Legacy Banking Standards with Special-Purpose Hardware -- ePassport: Securing International Contacts with Contactless Chips -- Good Variants of HB?+? Are Hard to Find -- Augmenting Internet-Based Card Not Present Transactions with Trusted Computing (Extended Abstract) -- Attacks and Counter-Measures II -- Weighing Down “The Unbearable Lightness of PIN Cracking” -- Phishwish: A Stateless Phishing Filter Using Minimal Rules -- Competition and Fraud in Online Advertising Markets -- Identity Theft: Much Too Easy? A Study of Online Systems in Norway -- A Proof of Concept Attack against Norwegian Internet Banking Systems -- Improvement of Efficiency in

(Unconditional) Anonymous Transferable E-Cash -- Proactive RSA with Non-interactive Signing -- Fair Traceable Multi-Group Signatures -- Identity-Based Online/Offline Encryption -- Countermeasures against Government-Scale Monetary Forgery -- OpenPGP-Based Financial Instruments and Dispute Arbitration -- An Efficient Anonymous Credential System -- Practical Anonymous Divisible E-Cash from Bounded Accumulators -- Panel: Usable Cryptography: Manifest Destiny or Oxymoron? -- Real Electronic Cash Versus Academic Electronic Cash Versus Paper Cash (Panel Report) -- Securing Web Banking Applications -- Privacy Threats in Online Stock Quotes -- A Platform for OnBoard Credentials -- ST&E Is the Most Cost Effective Measure for Comply with Payment Card Industry (PCI) Data Security Standard -- Making Quantitative Measurements of Privacy/Analysis Tradeoffs Inherent to Packet Trace Anonymization.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 12th International Conference on Financial Cryptography and Data Security, FC 2008, held in Cozumel, Mexico, in January 2008. The 16 revised full papers and 9 revised short papers presented together with 5 poster papers, 2 panel reports, and 1 invited lecture were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections on attacks and counter measures, protocols, theory, hardware, chips and tags, signatures and encryption, as well as anonymity and e-cash.