1.

Record Nr.	UNISA996465789603316
Titolo	Financial Cryptography and Data Security [[electronic resource]] : 14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28, 2010, Revised Selected Papers / / edited by Radu Sion
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38809-9 9786613566010 3-642-14577-9
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XII, 432p. 77 illus.)
Collana	Security and Cryptology ; ; 6052
Disciplina	005.82
Soggetti	Data encryption (Computer science) Cryptology
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	Constructive Cryptography – A Primer -- Security Mechanisms with Selfish Players in Wireless Networks -- Users Do the Darndest Things: True Stories from the CyLab Usable Privacy and Security Laboratory -- Multichannel Protocols to Prevent Relay Attacks -- A Traceability Attack against e-Passports -- Secure Computation with Fixed-Point Numbers -- Implementing a High-Assurance Smart-Card OS -- Unlinkable Priced Oblivious Transfer with Rechargeable Wallets -- Multiple Denominations in E-cash with Compact Transaction Data -- What's in a Name? -- Cryptographic Protocol Analysis of AN.ON -- A CDH-Based Ring Signature Scheme with Short Signatures and Public Keys -- Practical Private Set Intersection Protocols with Linear Complexity -- Design and Implementation of a Key-Lifecycle Management System -- Measuring the Perpetrators and Funders of Typosquatting -- A Learning-Based Approach to Reactive Security -- Embedded SFE: Offloading Server and Network Using Hardware Tokens -- The Phish-Market Protocol: Securely Sharing Attack Data between Competitors -- Building Incentives into Tor -- Tree-Homomorphic Encryption and Scalable Hierarchical Secret-Ballot Elections -- Automatically Preparing Safe SQL Queries -- PKI Layer Cake: New Collision Attacks against the

Global X.509 Infrastructure -- Three-Round Abuse-Free Optimistic Contract Signing with Everlasting Secrecy -- Designing for Audit: A Voting Machine with a Tiny TCB -- Attacking of SmartCard-Based Banking Applications with JavaScript-Based Rootkits -- Security Applications of Diodes with Unique Current-Voltage Characteristics -- Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication -- All You Can Eat or Breaking a Real-World Contactless Payment System -- Shoulder-Surfing Safe Login in a Partially Observable Attacker Model -- Using Sphinx to Improve Onion Routing Circuit Construction -- Secure Multiparty AES -- Modulo Reduction for Paillier Encryptions and Application to Secure Statistical Analysis -- On Robust Key Agreement Based on Public Key Authentication -- A Formal Approach for Automated Reasoning about Off-Line and Undetectable On-Line Guessing -- Signatures of Reputation -- Intention-Disguised Algorithmic Trading -- When Information Improves Information Security -- BetterThanPin: Empowering Users to Fight Phishing (Poster) -- Certification Intermediaries and the Alternative (Poster) -- SeDiCi: An Authentication Service Taking Advantage of Zero-Knowledge Proofs -- Poster Abstract: Security in Commercial Applications of Vehicular Ad-Hoc Networks -- Domain Engineering for Automatic Analysis of Financial Applications of Cryptographic Protocols -- hPIN/hTAN: Low-Cost e-Banking Secure against Untrusted Computers.