1.	Record Nr.	UNISA996466280603316
	Titolo	Financial Cryptography and Data Security [[electronic resource]] : FC 2010 Workshops, WLC, RLCPS, and WECSR, Tenerife, Canary Islands, Spain, January 25-28, 2010, Revised Selected Papers / / edited by Radu Sion, Reza Curtmola, Sven Dietrich, Aggelos Kiayias, Josep M Miret, Kazue Sako, Francesc Sebé
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
	ISBN	3-642-14992-8
	Edizione	[1st ed. 2010.]
	Descrizione fisica	1 online resource (XII, 256 p.)
	Collana	Security and Cryptology ; ; 6054
	Disciplina	004.6
	Soggetti	Computer communication systems Data encryption (Computer science) Computer engineering E-commerce Management information systems Computer science Computers and civilization Computer Communication Networks Cryptology Computer Engineering e-Commerce/e-business Management of Computing and Information Systems Computers and Society Conference proceedings. Kongress Teneriffa <2010>
	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	WLC Preface -- Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices -- Lighten Encryption Schemes for Secure and Private RFID Systems -- Analysis and Improvement of a

Pseudorandom Number Generator for EPC Gen2 Tags -- A Note on a Fatal Error of Optimized LFC Private Information Retrieval Scheme and Its Corrected Results -- Reliable Food Traceability Using RFID Tagging -- Lightweight Cryptography and DPA Countermeasures: A Survey -- Securing the Use of RFID-Enabled Banknotes -- Increasing Privacy Threats in the Cyberspace: The Case of Italian E-Passports -- RLCPS Preface -- SPAKE: A Single-Party Public-Key Authenticated Key Exchange Protocol for Contact-Less Applications -- A Secure and Privacy-Preserving Targeted Ad-System -- Cryptographic Cloud Storage -- Extending IPsec for Efficient Remote Attestation -- Open Mobile Alliance Secure Content Exchange: Introducing Key Management Constructs and Protocols for Compromise-Resilient Easing of DRM Restrictions -- How to Evaluate the Security of Real-Life Cryptographic Protocols? -- WECSR Preface -- Preaching What We Practice: Teaching Ethical Decision-Making to Computer Security Professionals -- A Case Study on Measuring Statistical Data in the Tor Anonymity Network -- A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets -- Ethical Proactive Threat Research -- A Framework for Understanding and Applying Ethical Principles in Network and Security Research -- Ethical Concerns in Computer Security and Privacy Research Involving Human Subjects -- Ethical Guidelines for Computer Security Researchers: "Be Reasonable".

| Sommario/riassunto | This volume contains the workshopproceedings of the accompanying workshops of the 14th Financial Cryptograpy and Data Security International Conference 2010, held on Tenerife, Canary Islands, Spain, January 25-28, 2010. FinancialCryptographyandData Securityis a majorinternationalforumfor research, advanced development, education, exploration, and debate regarding information assurance, with a speci?c focus on commercial contexts. The c- ference covers all aspects of securing transactions and systems and especially encourages original work focusing on both fundamental and applied real-world deployments on all aspects surrounding commerce security. Three workshops were co-located with FC 2010: the Workshop on Real-Life CryptographicProtocolsandStandardization(RLCPS), theWorkshoponEthics in Computer Security Research (WECSR), and the Workshop on Lightweight Cryptography for Resource-Constrained Devices (WLC). Intimate and colorful by tradition, the high-quality program was not the only attraction of FC. In the past, FC conferences have been held in highly research-synergistic locations such as Tobago, Anguilla, Dominica, Key West, Guadelupe, Bermuda, the Grand Cayman, and Cozumel Mexico. 2010 was the ?rst year that the conference was held on European soil, in the Spanish Canary Islands, in Atlantic waters, a few miles across Morocco. Over 100 researchers from more than 20 countries were in attendance. |