1. Record Nr. UNISA996465951703316

Titolo	Financial Cryptography and Data Security [[electronic resource]] : 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers / / edited by Ahmad-Reza Sadeghi
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-39884-7
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XVI, 406 p. 70 illus.)
Collana	Security and Cryptology ; ; 7859
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security E-commerce Application software Cryptology Systems and Data Security e-Commerce/e-business Computer Appl. in Administrative Data Processing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Keynote -- Can Nature Help Us Solve Risk Management Issues? Position Paper -- Electronic Payment (Bitcoin) -- Quantitative Analysis of the Full Bitcoin Transaction Graph -- Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk (Short Paper) -- Evaluating User Privacy in Bitcoin -- Usability Aspects -- The Importance of Being Earnest [In Security Warnings] (Short Paper) -- Exploring Extrinsic Motivation for Better Security: A Usability Study of Scoring-Enhanced Device Pairing (Short Paper) -- RelationGram: Tie-Strength Visualization for User-Controlled Online Identity Authentication (Short Paper) -- Secure Computation -- Practical Fully Simulatable Oblivious Transfer with Sublinear Communication -- Unconditionally-Secure Robust Secret Sharing with Minimum Share Size -- A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data -- Passwords -- “Give Me Letters 2, 3 and 6!”: Partial Password Implementations and

Attacks -- Hey, You, Get Off of My Clipboard: On How Usability Trumps Security in Android Password Managers -- Privacy Primitives and Non-repudiation -- Unique Ring Signatures: A Practical Construction (Short Paper) -- Aggregating CL-Signatures Revisited: Extended Functionality and Better Efficiency -- Accumulators and U-Prove Revocation (Short Paper) -- Anonymity -- Towards a Publicly-Verifiable Mix-Net Providing Everlasting Privacy (Short Paper) -- P4R: Privacy-Preserving Pre-Payments with Refunds for Transportation Systems (Short Paper) -- Hardware Security -- Coupon Collector's Problem for Fault Analysis against AES – High Tolerance for Noisy Fault Injections (Short Paper) -- Mitigating Smart Card Fault Injection with Link-Time Code Rewriting: A Feasibility Study (Short Paper) -- On the Need of Physical Security for Small Embedded Devices: A Case Study with COMP128-1 Implementations in SIM Cards (Short Paper) -- Secure Computation and Secret Sharing -- Securely Solving Simple Combinatorial Graph Problems -- Parallel and Dynamic Searchable Symmetric Encryption -- GMW vs. Yao? Efficient Secure Two-Party Computation with Low Depth Circuits -- Invited Talk -- The Untapped Potential of Trusted Execution Environments on Mobile Devices: Extended Abstract -- Authentication Attacks and Countermeasures -- Stark: Tamperproof Authentication to Resist Keylogging -- Risks of Offline Verify PIN on Contactless Cards (Short Paper) -- How to Attack Two-Factor Authentication Internet Banking (Short Paper) -- CAge: Taming Certificate Authorities by Inferring Restricted Scopes (Short Paper) -- Privacy of Data and Communication -- Interdependent Privacy: Let Me Share Your Data -- A Secure Submission System for Online Whistle blowing Platforms (Short Paper) -- Securing Anonymous Communication Channels under the Selective DoS Attack (Short Paper) -- Private Data Retrieval -- PIRMAP: Efficient Private Information Retrieval for MapReduce -- Avoiding Theoretical Optimality to Efficiently and Privately Retrieve Security Updates (Short Paper) -- Posters -- Three-Factor User Authentication Method Using Biometrics Challenge Response -- Synthetic Logs Generator for Fraud Detection in Mobile Transfer Services -- Onions for Sale: Putting Privacy on the Market -- Searchable Encryption Supporting General Boolean Expression Queries -- A Privacy Preserving E-Payment Architecture -- Communication Services Empowered with a Classical Chaos Based Cryptosystem.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 17th International Conference on Financial Cryptography and Data Security (FC 2013), held at Bankoku Shinryokan Busena Terrace Beach Resort, Okinawa, Japan, April 1-5, 2013. The 14 revised full papers and 17 short papers were carefully selected and reviewed from 125 submissions. The papers are grouped in the following topical sections: electronic payment (Bitcoin), usability aspects, secure computation, passwords, privacy primitives and non-repudiation, anonymity, hardware security, secure computation and secret sharing, authentication attacks and countermeasures, privacy of data and communication, and private data retrieval.