1. Record Nr. UNINA9910483461703321

Titolo	Financial Cryptography and Data Security : FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers / / edited by Andrew A. Adams, Michael Brenner, Matthew Smith
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-41320-X
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XII, 239 p. 64 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 7862
Disciplina	005.8
Soggetti	Data protection Cryptography Data encryption (Computer science) Electronic commerce Information technology - Management Data and Information Security Cryptology e-Commerce and e-Business Computer Application 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	The Workshop on Usable Security (USEC 13) -- I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves -- Usability and Security of Gaze-Based Graphical Grid Passwords -- The impact of length and mathematical operators on the usability and security of system-assigned one-time PINs -- QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks -- “Comply or Die" Is Dead: Long live security-aware principal agents -- Information Security as a Credence Good -- Sorry, I Don't Get It: An Analysis of Warning Message Texts -- Soulmate or Acquaintance? Visualizing Tie Strength for Trust Inference -- Awareness about photos on the Web and how privacy-privacy-tradeoffs could help -- Bootstrapping Trust in Online Dating: Social Verification of Online Dating Profiles -- The Workshop on Applied Homomorphic Cryptography (WAHC 13) -- SHADE: Secure

Hamming Distance computation from oblivious transfer -- Garbled Circuits via Structured Encryption -- On the Minimal Number of Bootstrappings in Homomorphic Circuits -- Privacy Preserving Data Processing with Collaboration of Homomorphic -- Parallel Homomorphic Encryption -- Targeting FPGA DSP Slices for a Large Integer Multiplier for Integer Based FHE.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the workshop on Usable Security, USEC 2013, and the third Workshop on Applied Homomorphic Cryptography, WAHC 2013, held in conjunction with the 17th International Conference on Financial Cryptology and Data Security, FC 2013, in Okinawa, Japan. The 16 revised full papers presented were carefully selected from numerous submissions and cover all aspects of data security. The goal of the USEC workshop was to engage on all aspects of human factors and usability in the context of security. The goal of the WAHC workshop was to bring together professionals, researchers and practitioners in the area of computer security and applied cryptography with an interest in practical applications of homomorphic encryption, secure function evaluation, private information retrieval or searchable encryption to present, discuss, and share the latest findings in the field, and to exchange ideas that address real-world problems with practical solutions using homomorphic cryptography.