1. Record Nr. UNINA9910349315703321

Titolo	Progress in Cryptology – AFRICACRYPT 2019 : 11th International Conference on Cryptology in Africa, Rabat, Morocco, July 9–11, 2019, Proceedings / / edited by Johannes Buchmann, Abderrahmane Nitaj, Tajjeeddine Rachidi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-23696-X
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XVI, 449 p. 705 illus., 52 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 11627
Disciplina	005.8 005.824
Soggetti	Data protection Computer networks Computers Coding theory Information theory Software engineering Data and Information Security Computer Communication Networks Computing Milieux Coding and Information Theory Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Protocols -- Tiny WireGuard Tweak -- Extended 3-Party ACCE and Application to LoRaWAN 1.1 -- Post-Quantum Cryptography -- The Mersenne Low Hamming Combination Search Problem can be reduced to an ILP Problem -- Simple Oblivious Transfer Protocols Compatible with Supersingular Isogenies -- An IND-CCA-Secure Code-Based Encryption Scheme Using Rank Metric -- Zero-Knowledge -- UC-Secure CRS Generation for SNARKs -- On the Efficiency of Privacy-Preserving Smart Contract Systems -- Lattice Based Cryptography --

Ring Signatures based on Middle-Product Learning with Errors Problems -- Sampling the Integers with Low Relative Error -- A Refined Analysis of the Cost for Solving LWE via uSVP -- New Schemes and Analysis -- Memory-Efficient High-Speed Implementation of Kyber on Cortex-M4 -- Reducing the Cost of Authenticity with Leakages: a CIML2-Secure AE Scheme with One Call to a Strongly Protected Tweakable Block Cipher -- An Improvement of Correlation Analysis for Vectorial Boolean Functions -- Block Ciphers -- On MILP-Based Automatic Search for Differential Trails Through Modular Additions with Application to Bel-T -- Practical Attacks on Reduced-Round AES -- Six Shades of AES -- Side-Channel Attacks and Countermeasures -- Revisiting Location Privacy from a Side-Channel Analysis Viewpoint -- Side Channel Analysis of SPARX-64/128: Cryptanalysis and Countermeasures -- Analysis of Two Countermeasures against the Signal Leakage Attack -- Signatures -- Handling Vinegar Variables to Shorten Rainbow Key Pairs -- Further Lower Bounds for Structure-Preserving Signatures in Asymmetric Bilinear Groups -- A New Approach to Modelling Centralised Reputation Systems.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2019, held in Rabat, Morocco, in July 2019. The 22 papers presented in this book were carefully reviewed and selected from 53 submissions. The papers are organized in topical sections on protocols; post-quantum cryptography; zero-knowledge; lattice based cryptography; new schemes and analysis; block ciphers; side-channel attacks and countermeasures; signatures. AFRICACRYPT is a major scientific event that seeks to advance and promote the field of cryptology on the African continent. The conference has systematically drawn some excellent contributions to the field. The conference has always been organized in cooperation with the International Association for Cryptologic Research (IACR).

2. Record Nr. UNINA9910372801703321

Titolo	Mensch-Computer-Interface : Zur Geschichte und Zukunft der Computerbedienung / Hans Dieter Hellige
Pubbl/distr/stampa	Bielefeld, : transcript Verlag, 2015 2015, c2008
ISBN	9783839405642 3839405645
Edizione	[1st ed.]
Descrizione fisica	1 online resource (400)
Collana	Kultur- und Medientheorie
Classificazione	ST 278
Disciplina	004.019
Soggetti	Computer Media Medien Culture Informationstechnik Technology Human Kultur Technik History of Technology Mensch Digital Media Technikgeschichte Media History Digitale Medien Computer Sciences Mediengeschichte Media Studies Informatik Medienwissenschaft
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Monografia

Nota di contenuto

Sommario/riassunto

Die gegenwärtige Interface-Krise bei digitalen Medien nehmen Informatiker und Informatikhistoriker in diesem Band zum Anlass für eine Langzeitbilanz der Mensch-Computer-Interaktion. Sie legen sowohl Gesamtüberblicke der Entwicklung aus technik- und geistesgeschichtlicher Sicht vor als auch spezielle Studien zur Bedienproblematik einzelner Epochen. Dadurch entsteht ein großer Bogen von den Bedienschnittstellen der frühen Mainframe-Welt über die interaktiven PC-Interfaces bis zu den neuesten Entwicklungen des Wearable Computing und der proaktiven Ambient Intelligence. Die historisch-genetischen Analysen münden in theoretische Betrachtungen und kritische Rückblicke auf die Forschung zu Mensch-Computer-Interfaces sowie Ausblicke auf die Zukunft.
»[E]in lesenswertes Kompendium.«

Besprochen in:c't, 17 (2008), Horst-Joachim Hoffmann

»Die spannende Lektüre bedient Praktiker und Theoretiker gleichermaßen.«