1. Record Nr. UNISA996466045503316

Titolo	The New Codebreakers [[electronic resource]] : Essays Dedicated to David Kahn on the Occasion of His 85th Birthday / / edited by Peter Y. A. Ryan, David Naccache, Jean-Jacques Quisquater
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
ISBN	3-662-49301-2
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XIV, 551 p. 135 illus.)
Collana	Security and Cryptology ; ; 9100
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Management information systems Computer science Algorithms Application software Cryptology Systems and Data Security Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Information Systems Applications (incl. Internet)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	History -- Mary of Guise’s enciphered letters -- About Professionalisation in the Intelligence Community: the French Cryptologists (ca 1870-ca 1945) -- Myths and legends -- The One-Time Pad and the Index of Coincidence -- Technology - Past, Present, Future -- The Fall of a Tiny Star -- Post-Quantum Cryptography: State of the Art -- What is the future of cryptography? -- Efficient Cryptographic Implementations -- Bitsliced High-Performance AES-ECB on GPUs -- Buying AES Design Resistance with Speed and Energy -- Double-Speed Barrett Moduli -- Treachery and Perfidy -- Failure is Also an Option -- How to (Carefully) Breach a Service Contract? -- Information Security -- SpoofKiller: You can teach people how to pay,

but not how to pay attention -- Cyber-Physical Systems Security -- Practical Techniques Building on Encryption for Protecting and Managing Data in the Cloud -- Cryptanalysis -- Cryptography as an Attack Technology: Proving the RSA/Factoring Kleptographic Attack -- Dual EC: A Standardized Back Door -- An Improved Differential Attack on Full GOST -- Cryptographic Hash Functions and Expander Graphs: The End of the Story? -- Side-Channel Attacks -- Polynomial Evaluation and Side Channel Analysis -- Photonic Power Firewalls -- A Heuristic Approach to Assist Side Channel Analysis of the Data Encryption Standard -- Improving the Big Mac attack on Elliptic Curve Cryptography -- Randomness -- Randomness testing: result interpretation and speed -- A fully-digital Chaos-based Random Bit Generator -- Embedded System Security -- Secure Application Execution in Mobile Devices -- Hardware-enforced Protection against Buffer Overflow using Masked Program Counter -- Public-Key Cryptography -- Hierarchical Identities from Group Signatures and Pseudonymous Signatures -- Secure ElGamal-type Cryptosystems Without Message Encoding -- Safe-Errors on SPA Protected implementations with the Atomicity Technique -- Models and Protocols -- Clever Arbiters versus Malicious Adversaries: On the Gap between Known-Input Security and Chosen-Input Security -- Security Analysis of the Modular Enhanced Symmetric Role Authentication (mERA) Protocol -- Crypto Santa. .

Sommario/riassunto

This Festschrift volume is published in honor of David Kahn and is the outcome of a Fest held in Luxembourg in 2010 on the occasion of David Kahn’s 80th birthday. The title of this books leans on the title of a serious history of cryptology named “The Codebreakers”, written by David Kahn and published in 1967. This book contains 35 talks dealing with cryptography as a whole. They are organized in topical section named: history; technology – past, present, future; efficient cryptographic implementations; treachery and perfidy; information security; cryptanalysis; side-channel attacks; randomness embedded system security; public-key cryptography; and models and protocols. .