1. Record Nr. UNISA996466288103316

Titolo	Security, Privacy, and Applied Cryptography Engineering [[electronic resource]] : 9th International Conference, SPACE 2019, Gandhinagar, India, December 3–7, 2019, Proceedings / / edited by Shivam Bhasin, Avi Mendelson, Mridul Nandi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-35869-0
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (X, 237 p. 106 illus., 42 illus. in color.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 11947
Disciplina	005.82
Soggetti	Data protection Software engineering Computers Computer engineering Computer networks Data and Information Security Software Engineering Computer Hardware Computer Engineering and Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Deployment of EMC-Compliant IC Chip Techniques in Design for Hardware Security -- Real Processing-in-Memory with Memristive Memory Processing Unit -- Length Preserving Symmetric Encryption: Is it Important? -- Towards Automatic Application of Side Channel Countermeasures -- Challenges in Deep Learning-based Profiled Side-channel Analysis -- A Study of Persistent Fault Analysis -- Internal state recovery attack on Stream Ciphers : Breaking BIVIUM -- Related-key Differential Cryptanalysis of Full Round CRAFT -- SpookChain: Chaining a Sponge-Based AEAD with Beyond-Birthday Security -- One trace is all it takes: Machine Learning-based Side-channel Attack on EdDSA -- An Efficient Practical Implementation of Impossible-

Differentia Cryptanalysis for Five-Round AES-128 -- Automated Classification of Web-Application Attacks for Intrusion Detection -- Formal Analysis of PUF Instances Leveraging Correlation-Spectra in Boolean Functions -- ProTro: A Probabilistic Counter based Hardware Trojan Attack on FPGA based MACSec enabled Ethernet Switch -- Encrypted Classification Using Secure K-Nearest Neighbour Computation -- A Few Negative Results on Constructions of MDS Matrices Using Low XOR Matrices -- Revisiting the Security of LPN based RFID Authentication Protocol and Potential Exploits in Hardware Implementations.

Sommario/riassunto

This book constitutes the refereed proceedings of the 9th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2019, held in Gandhinagar, India, in December 2019. The 12 full papers presented were carefully reviewed and selected from 24 submissions. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is a very challenging field, requiring the expertise from diverse domains, ranging from mathematics to solid-state circuit design.