1.	Record Nr.	UNISA996466438303316
	Titolo	Security, Privacy, and Applied Cryptography Engineering [[electronic resource]] : 7th International Conference, SPACE 2017, Goa, India, December 13-17, 2017, Proceedings / / edited by Sk Subidh Ali, Jean-Luc Danger, Thomas Eisenbarth
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
	ISBN	3-319-71501-1
	Edizione	[1st ed. 2017.]
	Descrizione fisica	1 online resource (XXIV, 295 p. 55 illus.)
	Collana	Security and Cryptology ; ; 10662
	Disciplina	005.82
	Soggetti	Data protection Computer security Data encryption (Computer science) Coding theory Information theory Computer communication systems Security Systems and Data Security Cryptology Coding and Information Theory Computer Communication Networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	On the (in)Security of ChaCha20 Against Physical Attacks -- An Industrial Outlook on Challenges of Hardware Security in Digital Economy -- How to Digitally Construct and Validate TRNG and PUF Primitives Which Are Based on Physical Phenomenon -- Cache Attacks: From Cloud to Mobile -- May the Fourth Be with You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519 -- The Crisis of Standardizing DRM: The Case of W3C Encrypted Media Extensions -- Parameter Choices for LWE -- Efficient Side Channel Testing of Cryptographic Devices Using TVLA -- IoT Insecurity - Innovation and Incentives in Industry -- Hardware

enabled cryptography: Physically Unclonable Functions and Random Numbers as Roots of Trust -- Tackling the Time-Defence: An Instruction Count Based Microarchitectural Side-channel Attack on Block Ciphers -- Hey Doc, Is This Normal?: Exploring Android Permissions in the Post Marshmallow Era -- Efficient Software Implementation of Laddering Algorithms over Binary Elliptic Curves -- Analysis of Diagonal Constants in Salsa -- Practical Fault Attacks on Minalpher: How to Recover Key with Minimum Faults -- eSPF: A Family of Format-Preserving Encryption Algorithms Using MDS Matrices -- Similarity Based Interactive Private Information Retrieval -- A Secure and Efficient Implementation of the Quotient Digital Signature Algorithm (qDSA) -- Variable-Length Bit Mapping and Error Correcting Codes for Higher-Order Alphabet PUFs -- Mutual Friend Attack Prevention in Social Network Data Publishing -- Short Integrated PKE+PEKS in Standard Model -- Differential Fault Attack on Grain v1, ACORN v3 and Lizard -- Certain observations on ACORN v3 and the Implications to TMDTO Attacks -- Efficient Implementation of Private License Plate Matching Protocols. .

| Sommario/riassunto | This book constitutes the refereed proceedings of the 7th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2017, held in Goa, India, in December 2017. The 13 revised full papers presented together with 1 short paper, 7 invited talks, and 4 tutorials were carefully reviewed and selected from 49 initial submissions. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is indeed a very challenging field, requiring the expertise from diverse domains, ranging from mathematics to solid-state circuit design. |