1.	Record Nr.	UNISA996466315603316
	Titolo	Codes, Cryptology and Information Security [[electronic resource]] : Third International Conference, C2SI 2019, Rabat, Morocco, April 22–24, 2019, Proceedings - In Honor of Said El Hajji / / edited by Claude Carlet, Sylvain Guilley, Abderrahmane Nitaj, El Mamoun Souidi
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
	ISBN	3-030-16458-6
	Edizione	[1st ed. 2019.]
	Descrizione fisica	1 online resource (XIX, 482 p. 244 illus., 23 illus. in color.)
	Collana	Security and Cryptology ; ; 11445
	Disciplina	005.82
	Soggetti	Computer security Data encryption (Computer science) Software engineering Coding theory Information theory Systems and Data Security Cryptology Software Engineering Coding and Information Theory
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Side-channel analysis -- Virtual Security Evaluation -- Cache-Timing Attacks still threaten IoT devices -- Speed-up of SCA attacks on 32-bit multiplications. Cryptography -- Arabic Cryptography and Steganography in Morocco -- An AEAD variant of the Grain stream cipher -- Construction for a Nominative Signature Scheme from Lattice with Enhanced Security -- Reinterpreting and Improving the Cryptanalysis of the Flash Player PRNG -- A Key Exchange Based on the Short Integer Solution Problem and the Learning with Errors Problem -- Non-Interactive Zero Knowledge Proofs in the Random Oracle Model -- From Quadratic Functions to Polynomials: Generic Functional Encryption from Standard Assumptions -- Secret sharing -- Efficient Proactive Secret Sharing for Large Data via Concise Vector

Commitments -- Secret Sharing using Near-MDS Codes -- Mathematics for cryptography -- On Plateaued Functions, Linear Structures and Permutation Polynomials -- Faster Scalar Multiplication on the x-line: Three-dimensional GLV Method with Three-dimensional Differential Addition Chains -- Codes and their applications -- On good polynomials over finite fields for optimal locally recoverable codes -- A New Gabidulin-like Code and its Application in Cryptography -- Perfect, Hamming and Simplex Linear Error-Block Codes with Minimum-distance 3 -- Quasi-Dyadic Girault Identification Scheme -- Homomorphic encryption -- Securely aggregating testimonies with Threshold Multi-key FHE -- Improved Efficiency of a Linearly Homomorphic Cryptosystem -- Applied cryptography -- On the Tracing Traitors Math Dedicated to the memory of Bob Blakley - pioneer of digital fingerprinting and inventor of secret sharing -- Reusable Garbled Turing Machines without FHE -- An Extension of Formal Analysis Method with Reasoning: A Case Study of Flaw Detection for Non-repudiation and Fairness -- A Practical and Insider Secure Signcryption with Non-Interactive Non-Repudiation -- Security -- Analysis of Neural Network Training and Cost Functions Impact on the Accuracy of IDS and SIEM Systems -- Managing Your Kleptographic Subscription Plan -- Model Checking Speculation-Dependent Security Properties: Abstracting and Reducing Processor Models for Sound and Complete Verification -- .

Sommario/riassunto

This book constitutes the proceedings of the Third International Conference on Codes, Cryptology and Information Security, C2SI 2019, held in Rabat, Morocco, in April 2019. The 19 regular papers presented together with 5 invited talks were carefully reviewed and selected from 90 submissions. The first aim of this conference is to pay homage to Said El Hajji for his valuable contribution in research, teaching and disseminating knowledge in numerical analysis, modeling and information security in Morocco, Africa, and worldwide. The second aim of the conference is to provide an international forum for researchers from academia and practitioners from industry from all over the world for discussion of all forms of cryptology, coding theory, and information security.