1.	Record Nr.	UNISA996465744003316
	Titolo	Information Security and Cryptology – ICISC 2016 [[electronic resource]] : 19th International Conference, Seoul, South Korea, November 30 – December 2, 2016, Revised Selected Papers / / edited by Seokhie Hong, Jong Hwan Park
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
	ISBN	3-319-53177-8
	Edizione	[1st ed. 2017.]
	Descrizione fisica	1 online resource (XVI, 351 p. 31 illus.)
	Collana	Security and Cryptology ; ; 10157
	Disciplina	005.8
	Soggetti	Computer security Data protection Data encryption (Computer science) Management information systems Computer science Systems and Data Security Security Cryptology Management of Computing and Information Systems
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Protocols -- Secure and Private, yet Lightweight, Authentication for the IoT via PUF and CBKA -- Lattice Cryptography -- Practical post-quantum public key cryptosystem based on LWE -- Analysis of Error Terms of Signatures Based on Learning with Errors -- Encryption -- Transforming Hidden Vector Encryption Schemes from Composite-Order Groups into Prime-Order Groups -- Lossy Key Encapsulation Mechanism and Its Applications -- Expanded Framework for Dual System Encryption and its Application -- Adaptively Secure Broadcast Encryption with Dealership -- Implementation and Algorithms -- A new algorithm for residue multiplication modulo $2^{521}-1$ -- Enhancing Data Parallelism of Fully Homomorphic Encryption -- An Improvement of Optimal Ate Pairing on KSS curve with Pseudo 12-sparse

Multiplication -- Signatures (and Protocol) -- Revisiting the Cubic UOV Signature Scheme -- Network Coding Signature Schemes against Related-Key Attacks in the Random Oracle Model -- New Realizations of Efficient and Secure Private Set Intersection Protocols Preserving Fairness -- Analysis -- Improved Results on Cryptanalysis of Prime Power RSA -- On Computing the Immunity of Boolean Power Functions against Fast Algebraic Attacks -- Improved Fault Analysis on the Block Cipher SPECK by Injecting Faults in the Same Round -- On the Effectiveness of Code-reuse based Android Application Obfuscation.

Sommario/riassunto

This book constitutes revised selected papers from the 19th International Conference on Information Security and Cryptology, ICISC 2016, held in Seoul, South Korea, in November/December 2016. The 18 full papers presented in this volume were carefully reviewed and selected from 69 submissions. There were organized in topical sections named: protocols; lattice cryptography; encryption; implementation and algorithms; signatures and protocol; and analysis. .