1.	Record Nr.	UNISA996393703703316
	Titolo	A declaration and ordinance of the Lords and Commons assembled in Parliament [[electronic resource]] : for the better securing and setling of the peace of the county of Kent, and for enabling them to associate with the City of London, or any other counties adjacent. And to raise forces within the said county, as well horse as foot, and therewith to give, or cause battell to be given to all such forces as are or shal be raised without the consent of both houses of Parliament; and all such persons with their abbettors and adherents to invade, resist, put to flight, pursue, suppresse, kill, slay, put to execution of death, and by all means to destroy, as enemies to the kingdom. Likewise, instructions for the lord-lieutenant, deputy-lieutenants, and other offiers [sic], and commanders in the county of Kent. And, that every person which shall be imployed as souldiers in this service, of the age of 16. yeers and upwards, shall solemnly take an oath, to be approved of by the Parliament, and they that wilfully neglect the same shall be proceeded against as delinquents, and enemies of the peace of the kingdom. Die Martis, 30 Maii. 1643. Ordered by the Lords and Commons assembled in Parliament, that this declaration and ordinance with the instructions shall be forthwith printed and published. J. Brown Cler. Parliamentorum
	Pubbl/distr/stampa	London, : Printed for I. Wright in the Old-baily, Iune 1. 1643
	Descrizione fisica	[12] p
	Soggetti	Kent (England) History Great Britain History Civil War, 1642-1649
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Reproduction of original in Thomason Collection, British Library.
	Sommario/riassunto	eebo-0018

2.	Record Nr.	UNINA9910413448103321
	Titolo	Progress in Cryptology - AFRICACRYPT 2020 : 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20 – 22, 2020, Proceedings / / edited by Abderrahmane Nitaj, Amr Youssef
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
	ISBN	3-030-51938-4
	Edizione	[1st ed. 2020.]
	Descrizione fisica	1 online resource (XI, 453 p. 193 illus., 47 illus. in color.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 12174
	Disciplina	005.82
	Soggetti	Data protection
		Data structures (Computer science)
		Information theory
		Computer engineering
		Computer networks
		Computers
		Data and Information Security
		Data Structures and Information Theory
		Computer Engineering and Networks
		Computing Milieux
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	QA-NIZK Arguments of Same Opening for Bilateral Commitments -- Signatures of Knowledge for Boolean Circuits under Standard Assumptions -- LESS is More: Code-Based Signatures without Syndromes -- UC Updatable Databases and Applications -- Symmetric Key Cryptography -- Impossible Di erential Cryptanalysis of Reduced-Round Tweakable TWINE -- MixColumns Coe cient Property and Security of the AES withA Secret S-Box -- New Results on the SymSum Distinguisher on Round-Reduced SHA3.-Cryptanalysis of FlexAEAD -- BBB Secure Nonce Based MAC Using Public Permutations -- Elliptic Curves -- On Adaptive Attacks against Jao-Urbanik's Isogeny-Based Protocol -- A SAT-Based Approach for Index Calculus on Binary Elliptic Curves -- Post Quantum Cryptography -- Hash-based Signatures

Revisited: A Dynamic FORS with Adaptive Chosen Message Security -- LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4 -- Lattice Based Cryptography -- Round Optimal Secure Multisignature Schemes from Lattice with Public Key Aggregation and Signature Compression -- Sieve, Enumerate, Slice, and Lift: Hybrid Lattice Algorithms for SVP via CVPP.-Side Channel Attacks -- Online Template Attack On ECDSA: Extracting Keys Via The Other Side -- When similarities among devices are taken for granted: Another look at portability -- A Tale of Three Signatures: Practical Attack of ECDSA with wNAF -- Attacking RSA Using an Arbitrary Parameter -- New Algorithms and Schemes -- A New Encoding Algorithm for a Multidimensional Version of the Montgomery Ladder -- New Ideas to Build Noise-Free Homomorphic Cryptosystems -- Zero Knowledge.

| Sommario/riassunto | This book constitutes the refereed proceedings of the 12th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2020, held in Cairo, Egypt, in July 2020. The 21 papers presented in this book were carefully reviewed and selected from 49 submissions. The papers are organized in topical sections on zero knowledge, symmetric key cryptography, elliptic curves, post quantum cryptography, lattice based cryptography, side channel attacks, cryptanalysis and new algorithms and schemes. AFRICACRYPT is a major scientific event that seeks to advance and promote the field of cryptology on the African continent. The conference has systematically drawn some excellent contributions to the field. The conference has always been organized in cooperation with the International Association for Cryptologic Research (IACR). |