1. Record Nr. UNINA9910785651303321

Autore	Okasha Elisabeth
Titolo	Women's names in Old English / / Elisabeth Okasha
Pubbl/distr/stampa	London : , : Routledge, , 2016
ISBN	1-351-87121-8 1-315-23349-5 1-283-04748-9 9786613047489 0-7546-9849-1
Descrizione fisica	1 online resource (151 p.)
Collana	Studies in early medieval Britain
Disciplina	929.40941
Soggetti	Feminine names - Great Britain - History - Anglo-Saxon period, 449-1066 Names, Personal - England Names, English (Old) English language - Old English, ca. 450-1100 - Etymology - Names
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	First published 2011 by Ashgate Publishing.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	CONTENTS; Foreword; List of Abbreviations; Preface; 1 Introduction; 2 The Material; 3 Analysis and Classification of the Material; 4 Discussion of Di-thematic Names; 5 Analysis and Discussion of Mono-thematic Names; 6 Some Implications; 6.1. Assumptions about Sex made from Personal Names; 6.2 Coins and Moneyers; 6.3 Words Used to Describe Women; 6.4 Implications for the Presentation of the Material under Discussion; 7 Vernacular Names in Old English Poetry; 8 General Discussion; 9 Conclusion; Appendix: A Brief Comparison with Some Modern Names; Bibliography; Concordances
Sommario/riassunto	This book provides an in-depth study into the issue of vernacular names in Old English documents. Specifically it challenges the generally accepted notion that the sex of an individual is definitively indicated by the grammatical gender of their name. While modern scholars have generally felt no difficulty is distinguishing male from female names, this book asks how far the Anglo-Saxons themselves recognised this distinction, and in so doing critically examines and tests the general

		principle that grammatical gender is a certain indicator of biological sex. Anyone with an interest in Old Engli

2.	Record Nr.	UNICAMPANIAVAN00291429
	Titolo	1
	Pubbl/distr/stampa	Roma, : Camera dei deputati, 2011
	Descrizione fisica	XLIII, 564 p. ; 25 cm
	Lingua di pubblicazione	Italiano
	Formato	Materiale a stampa
	Livello bibliografico	Monografia

3.	Record Nr.	UNINA9910485587003321
	Titolo	Advances in Cryptology – EUROCRYPT 2021 : 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I / / edited by Anne Canteaut, François-Xavier Standaert
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
	ISBN	3-030-77870-3
	Edizione	[1st ed. 2021.]
	Descrizione fisica	1 online resource (849 pages)
	Collana	Security and Cryptology, , 2946-1863 ; ; 12696
	Disciplina	005.82
	Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Data protection Application software Numerical analysis Cryptology Coding and Information Theory Data and Information Security Computer and Information Systems Applications Numerical Analysis

Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Non-Interactive Zero Knowledge from Sub-exponential DDH -- On the (in)security of ROS -- New Representations of the AES Key Schedule -- Public-Key Cryptography -- Analysing the HPKE Standard -- Tightly-Secure Authenticated Key Exchange, Revisited -- Aggregatable Distributed Key Generation -- Decentralized Multi-Authority ABE for DNFs from LWE -- Isogenies -- Compact, Efficient and UC-Secure Isogeny-Based Oblivious Transfer -- One-way functions and malleability oracles: Hidden shift attacks on isogenybased protocols -- Sieving for twin smooth integers with solutions to the Prouhet-Tarry-Escott problem -- Delay Encryption -- Post-Quantum Cryptography -- The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes -- Improved cryptanalysis of UOV and Rainbow -- Cryptanalytic Applications of the Polynomial Method for Solving Multivariate Equation Systems over GF(2) -- Round-Optimal Blind Signatures in the Plain Model from Classical and Quantum Standard Assumptions -- Post-Quantum Multi-Party Computation -- Lattices -- A 2/² -Time Algorithm for n-SVP and n-Hermite SVP, and an Improved Time-Approximation Tradeoff for (H)SVP -- New Lattice Two-Stage Sampling Technique and its Applications to Functional Encryption – Stronger Security and Smaller Ciphertexts -- On Bounded Distance Decoding with Predicate: Breaking the "Lattice Barrier" for the Hidden Number Problem -- On the ideal shortest vector problem over random rational primes -- Homomorphic Encryption -- Efficient Bootstrapping for Approximate Homomorphic Encryption with Non-Sparse Keys -- High-Precision Bootstrapping of RNS-CKKS Homomorphic Encryption Using Optimal Minimax Polynomial Approximation and Inverse Sine Function -- On the Security of Homomorphic Encryption on Approximate Numbers -- The Rise of Paillier: Homomorphic Secret Sharing and Public-Key Silent OT -- Symmetric Cryptanalysis -- Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha -- Rotational Cryptanalysis From a Differential-Linear Perspective – Practical Distinguishers for Round-reduced FRIET, Xoodoo, and Alzette -- Automatic Search of Meet-in-the-Middle Preimage Attacks on AES-like Hashing -- A Deeper Look at Machine Learning-Based Cryptanalysis. .
Sommario/riassunto	The 3-volume-set LNCS 12696 – 12698 constitutes the refereed proceedings of the 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2021, which was held in Zagreb, Croatia, during October 17-21, 2021. The 78 full papers included in these proceedings were accepted from a total of 400 submissions. They were organized in topical sections as follows: Part I: Best papers; public-key cryptography; isogenies; post-quantum cryptography; lattices; homomorphic encryption; symmetric cryptanalysis; Part II: Symmetric designs; real-world cryptanalysis; implementation issues; masking and secret-sharing; leakage, faults and tampering; quantum constructions and proofs; multiparty computation; Part III: Garbled circuits; indistinguishability obfuscation; non-malleable commitments; zero-knowledge proofs; property-preserving hash functions and ORAM; blockchain; privacy and law enforcement.