1. Record Nr. UNISA996465820303316

Titolo	Advances in cryptology - EUROCRYPT '90 : Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, proceedings / / I. B. Damgard (ed.)
Pubbl/distr/stampa	Berlin ; ; Heidelberg : , : Springer-Verlag, , [1991] Â©1991
ISBN	3-540-46877-3
Edizione	[1st ed. 1991.]
Descrizione fisica	1 online resource (VIII, 500 p.)
Collana	Lecture Notes in Computer Science ; ; 473
Disciplina	003.54
Soggetti	Coding theory Combinatorial analysis
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Protocols -- All Languages in NP Have Divertible Zero-Knowledge Proofs and Arguments Under Cryptographic Assumptions -- On the Importance of Memory Resources in the Security of Key Exchange Protocols -- Provably Secure Key-Updating Schemes in Identity-Based Systems -- Oblivious transfer protecting secrecy -- Public-Randomness in Public-Key Cryptography -- An Interactive Identification Scheme Based on Discrete Logarithms and Factoring -- Number-Theoretic Algorithms -- Factoring with two large primes -- Which new RSA signatures can be computed from some given RSA signatures? -- Implementation of a Key Exchange Protocol Using Real Quadratic Fields -- Distributed Primality Proving and the Primality of (23539 + 1)/3 -- Boolean Functions -- Properties of binary functions -- How to Construct Pseudorandom Permutations from Single Pseudorandom Functions -- Constructions of bent functions and difference sets -- Propagation Characteristics of Boolean Functions -- Binary Sequences -- The Linear Complexity Profile and the Jump Complexity of Keystream Sequences -- Lower Bounds for the Linear Complexity of Sequences over Residue Rings -- On the Construction of Run Permuted Sequences -- Correlation Properties of Combiners with Memory in Stream Ciphers (Extended Abstract) -- Correlation Functions of Geometric Sequences -- Implementations -- Exponentiating Faster

with Addition Chains -- A Cryptographic Library for the Motorola DSP56000 -- VICTOR an efficient RSA hardware implementation -- Experimental Quantum Cryptography -- Combinatorial Schemes -- A Protocol to Set Up Shared Secret Schemes Without the Assistance of a Mutually Trusted Party -- Lower Bounds for Authentication Codes with Splitting -- Essentially ?-fold secure authentication systems -- On the construction of authentication codes with secrecy and codes withstanding spoofing attacks of order L ? 2 -- Cryptanalysis -- Cryptanalysis of a public-key cryptosystem based on approximations by rational numbers -- A Known-Plaintext Attack on Two-Key Triple Encryption -- Confirmation that Some Hash Functions Are Not Collision Free -- Inverting the Pseudo Exponentiation -- New Cryptosystems -- Cryptosystem for Group Oriented Cryptography -- A Provably-Secure Strongly-Randomized Cipher -- General public key residue cryptosystems and mental poker protocols -- A Proposal for a New Block Encryption Standard -- A new trapdoor in knapsacks -- Signatures and Authentication -- On the Design of Provably-Secure Cryptographic Hash Functions -- Fast Signature Generation with a Fiat Shamir — Like Scheme -- A Remark on a Signature Scheme Where Forgery can be Proved -- Membership Authentication for Hierarchical Multigroups Using the Extended Fiat-Shamir Scheme -- Zero-Knowledge Undeniable Signatures (extended abstract) -- Precautions taken against various potential attacks -- Impromptu Talks -- Software Run-Time Protection: A Cryptographic Issue -- An identity-based identification scheme based on discrete logarithms modulo a composite number -- A Noisy Clock-Controlled Shift Register Cryptanalysis Concept Based on Sequence Comparison Approach -- The MD4 Message Digest Algorithm -- A remark on the efficiency of identification schemes -- On an Implementation of the Mohan-Adiga Algorithm.

Sommario/riassunto

Eurocrypt is a conference devoted to all aspects of cryptologic research, both theoretical and practical, sponsored by the International Association for Cryptologic Research (IACR). Eurocrypt 90 took place in Åarhus, Denmark, in May 1990. From the 85 papers submitted, 42 were selected for presentation at the conference and for inclusion in this volume. In addition to the formal contributions, short abstracts of a number of informal talks are included in these proceedings. The proceedings are organized into sessions on protocols, number-theoretic algorithms, boolean functions, binary sequences, implementations, combinatorial schemes, cryptanalysis, new cryptosystems, signatures and authentication, and impromptu talks.

2. Record Nr. UNINA9910774818703321

Titolo	Participatory Knowledge / / edited by Charlotte A. Lerg [and two others]
Pubbl/distr/stampa	Berlin ; ; Boston : , : De Gruyter Oldenbourg, , 2022
ISBN	3-11-074881-9
Descrizione fisica	1 online resource (v, 253 pages) : illustrations
Collana	History of intellectual culture ; ; Volume 1
Disciplina	100
Soggetti	Religion and science Knowledge, Theory of (Religion) Art and religion
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Frontmatter -- Table of Contents -- Introducing the Yearbook History of Intellectual Culture -- Section I: Individual Articles -- Citation and Mediation: The Evolution of MLA Style -- The Man in the Mirror: Jacques Lacan’s American Reception -- Object Photography, Illustrated Price Catalogues, and the Circulation of Knowledge -- Section II: Participatory Knowledge -- Participatory Knowledge: Conceptual Thoughts -- Empirical Research as a Form of Participatory Knowledge? The Sociological Projects of the Frankfurt School as Democratic Practice -- Amateur Eugenics: The “Great-Mother in Dalecarlia” Genealogy Project and the Collaboration Between the Swedish Institute for Race Biology and the General Public, 19301935 -- Folklore, Teachers, and Collective Knowledge in Argentina in the Early Twentieth Century -- Critical Tendencies and the Production of Knowledge: Contention, Coalition, and Antagonism in the Digital Public Sphere -- Section III: Engaging the Field -- Positive Discourse Analysis: A Method for the History of Knowledge? -- Documenting COVID-19 for Future Historians? -- Contributors
Sommario/riassunto	With concepts of participation discussed in multiple disciplines from media studies to anthropology, from political sciences to sociology, the first issue of the new yearbook History of Intellectual Culture (HIC) dedicates a thematic section to the way knowledge can and arguably must be conceptualized as "participatory". Introducing and exploring

"participatory knowledge", the volume aims to draw attention to the potential of looking at knowledge formation and circulation through a new lens and to open a dialogue about how and what concepts and theories of participation can contribute to the history of knowledge. By asking who gets to participate in defining what counts as knowledge and in deciding whose knowledge is circulated, modes of participation enter into the examination of knowledge on various levels and within multiple cultural contexts. The articles in this volume attest to the great variety of approaches, contexts, and interpretations of "participatory knowledge", from the sociological projects of the Frankfurt School to the Uppsala-based Institute for Race Biology, from the Argentinian National Folklore Survey to current hashtag activism and Covid-19-archive projects. HIC sees knowledge as rooted in social and political structures, determined by modes of transfer and produced in collaborative processes. The notion of "participatory knowledge" highlights in a compelling way how knowledge is rooted in cultural practices and social configurations.