1.

Record Nr.	UNINA9910482832103321
Autore	Winstrup Peder Jensen <1549-1614.>
Titolo	Om det euige Liff oc Død. Christelig Vnderuisning, huad Løn oc betalning Gud ved sin Søn Jesum Christum blant alle Menniske, Onde og Gode, paa Domsens Dag skal vddele, Aff den hellige Scrifft kortelige forfattet ved Peder Vinstrup [[electronic resource]]
Pubbl/distr/stampa	Copenhagen, : Mads Vingaard, 1587
Descrizione fisica	Online resource ([176] bl.)
Lingua di pubblicazione	Danese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Reproduction of original in Det Kongelige Bibliotek / The Royal Library (Copenhagen).

2.

Record Nr.	UNINA9910484202103321
Titolo	Advances in Cryptology – EUROCRYPT 2005 : 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings / / edited by Ronald Cramer
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XIV, 578 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3494
Altri autori (Persone)	CramerRonald L
Disciplina	003.54
Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Computer science - Mathematics Discrete mathematics Coding and Information Theory Cryptology

	Computer Communication Networks Operating Systems Discrete Mathematics in Computer Science
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 and index.
Nota di contenuto	Cryptanalysis I -- Cryptanalysis of the Hash Functions MD4 and RIPEMD -- How to Break MD5 and Other Hash Functions -- Collisions of SHA-0 and Reduced SHA-1 -- Theory I -- Reducing Complexity Assumptions for Statistically-Hiding Commitment -- Smooth Projective Hashing and Two-Message Oblivious Transfer -- On Robust Combiners for Oblivious Transfer and Other Primitives -- Encryption I -- Efficient Identity-Based Encryption Without Random Oracles -- Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM -- Signatures and Authentication -- Secure Remote Authentication Using Biometric Data -- Stronger Security Bounds for Wegman-Carter-Shoup Authenticators -- 3-Move Undeniable Signature Scheme -- Group Signatures with Efficient Concurrent Join -- Algebra and Number Theory I -- Floating-Point LLL Revisited -- Practical Cryptography in High Dimensional Tori -- A Tool Kit for Finding Small Roots of Bivariate Polynomials over the Integers -- Quantum Cryptography -- Computational Indistinguishability Between Quantum States and Its Cryptographic Application -- Approximate Quantum Error-Correcting Codes and Secret Sharing Schemes -- Secure Protocols -- Compact E-Cash -- Cryptographic Asynchronous Multi-party Computation with Optimal Resilience -- Algebra and Number Theory II -- Differential Cryptanalysis for Multivariate Schemes -- A Fast Cryptanalysis of the Isomorphism of Polynomials with One Secret Problem -- Partial Key Exposure Attacks on RSA up to Full Size Exponents -- The RSA Group is Pseudo-Free -- Theory II -- Universally Composable Password-Based Key Exchange -- Mercurial Commitments with Applications to Zero-Knowledge Sets -- Encryption II -- Hierarchical Identity Based Encryption with Constant Size Ciphertext -- Fuzzy Identity-Based Encryption -- Cryptanalysis II -- Second Preimages on n-Bit Hash Functions for Much Less than 2 n Work -- Predicting and Distinguishing Attacks on RC4 Keystream Generator -- Related-Key Boomerang and Rectangle Attacks -- On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions -- Broadcast Encryption and Traitor Tracing -- Public Traceability in Traitor Tracing Schemes -- One-Way Chain Based Broadcast Encryption Schemes.
Sommario/riassunto	These are the proceedings of the 24th Annual IACR Eurocrypt Conference. The conference was sponsored by the International Association for Cryptologic Research(IACR;seewww.iacr.org), thisyearincooperationwiththeComputer Science Department of the University of Aarhus, Denmark. As General Chair, Ivan Damg? ard was responsible for local organization. TheEurocrypt2005ProgramCommittee(PC)consistedof30internationally renowned experts. Their names and a?liations are listed on pages VII and VIII of these proceedings. By the November 15, 2004 submission deadline the PC had received a total of 190 submissions via the IACR

Electronic Submission Server. The subsequent selection process was divided into two phases, as usual. In the review phase each submission was carefully scrutinized by at least three independent reviewers, and the review reports, often extensive, were committed to the IACR Web Review System. These were taken as the starting point for the PC-wideWeb-baseddiscussionphase.Duringthisphase,additionalreportswere provided as needed, and the PC eventually had some 700 reports at its disposal. In addition, the discussions generated more than 850 messages, all posted in the system. During the entire PC phase, which started in August 2003 with my earliest invitations to PC members and which continued until March 2005, more than 1000 email messages were communicated. Moreover, the PC received much appreciated assistance from a large body of external reviewers. Their names are listed on page VIII of these proceedings.