1. Record Nr. UNINA9910715010603321

Titolo	Respirator users notice: increased inspection frequency for certain self-contained breathing appparatus air cylinders
Pubbl/distr/stampa	Washington, DC : , : United States Nuclear Regulatory Commission, Office of Inspection and Enforcement, , 1986
Descrizione fisica	1 online resource
Collana	Information notice ; ; no. 86-24
Soggetti	Nuclear power plants - Safety measures Breathing apparatus Gas cylinders - Inspection
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"April 11, 1986."

2. Record Nr. UNINA9910143918103321

Titolo	Selected Areas in Cryptography : 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001. Revised Papers / / edited by Serge Vaudenay, Amr M. Youssef
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-45537-X
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (XII, 364 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2259
Disciplina	005.82
Soggetti	Data encryption (Computer science) Operating systems (Computers) Computers and civilization Algorithms Computer networks Computer science - Mathematics Cryptology Operating Systems Computers and Society Algorithm Analysis and Problem Complexity Computer Communication Networks Computational Science and Engineering
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 at the end of each chapters and index.
Nota di contenuto	Cryptanalysis I -- Weaknesses in the Key Scheduling Algorithm of RC4 -- A Practical Cryptanalysis of SSC2 -- Analysis of the E 0 Encryption System -- Boolean Functions -- Boolean Functions with Large Distance to All Bijective Monomials: N Odd Case -- Linear Codes in Constructing Resilient Functions with High Nonlinearity -- New Covering Radius of Reed-Muller Codes for t-Resilient Functions -- Generalized Zig-zag Functions and Oblivious Transfer Reductions -- Rijndael -- A Simple Algebraic Representation of Rijndael -- Improving the Upper Bound on the Maximum Average Linear Hull Probability for Rijndael -- Invited

Talk I -- Polynomial Reconstruction Based Cryptography -- Elliptic Curves and Efficient Implementation I -- An Improved Implementation of Elliptic Curves over GF(2 n) when Using Projective Point Arithmetic -- Fast Generation of Pairs (k, [k]P) for Koblitz Elliptic Curves -- Algorithms for Multi-exponentiation -- Two Topics in Hyperelliptic Cryptography -- Cryptanalysis II -- A Differential Attack on Reduced-Round SC2000 -- On the Complexity of Matsui's Attack -- Random Walks Revisited: Extensions of Pollard's Rho Algorithm for Computing Multiple Discrete Logarithms -- Elliptic Curves and Efficient Implementation II -- Fast Normal Basis Multiplication Using General Purpose Processors -- Fast Multiplication of Integers for Public-Key Applications -- Fast Simultaneous Scalar Multiplication on Elliptic Curve with Montgomery Form -- On the Power of Multidoubling in Speeding Up Elliptic Scalar Multiplication -- Public Key Systems -- The GH Public-Key Cryptosystem -- XTR Extended to GF(p 6m) -- Invited Talk II -- The Two Faces of Lattices in Cryptology -- Protocols and Mac -- New (Two-Track-)MAC Based on the Two Trails of RIPEMD -- Key Revocation with Interval Cover Families -- Timed-Release Cryptography.

Sommario/riassunto

SAC 2001, the eighth annual workshop on selected areas in cryptography, was held at the Fields Institute in Toronto, Ontario, Canada. Previous SAC wo- shops were held at Queen's University in Kingston (1994, 1996, 1998, and 1999), at Carlton University in Ottawa (1995 and 1997) and at the University of Wat- loo (2000). The conference was sponsored by the center for applied cryptographic research (CACR) at the University of Waterloo, Certicom Corporation, C-munications and Information Technology Ontario (CITO), Ecole Polytechnique F´ed´erale de Lausanne, Entrust Technologies, and ZeroKnowledge. We are gra- ful to these organizations for their support of the conference. The current SAC board includes Carlisle Adams, Doug Stinson, Ed Dawson, Henk Meijer, Howard Heys, Michael Wiener, Serge Vaudenay, Sta'ord Tavares, and Tom Cusick. We would like to thank all of them for giving us the mandate to organize SAC 2001. The themes for SAC 2001 workshop were: - Design and analysis of symmetric key cryptosystems. - Primitives for private key cryptography, including block and stream ciphers, hash functions, and MACs. - E'cient implementations of cryptographic systems in public and private key cryptography. - Cryptographic solutions for web and internet security.