1. Record Nr.   UNINA9910695899103321

   Titolo   Secure border initiative [[electronic resource]] : SBInet expenditure plan needs to better support oversight and accountability : report to congressional committees

   Pubbl/distr/stampa   [Washington, D.C.] : , : U.S. Govt. Accountability Office, , [2007]

   Descrizione fisica   i, 65 pages : digital, PDF file

   Soggetti   Noncitizens - Prevention - Government policy - United States
                        Illegal immigration - Prevention - Government policy - United States
                        Illegal immigration
                        United States Boundaries Management

   Lingua di pubblicazione   Inglese

   Formato   Materiale a stampa

   Livello bibliografico   Monografia

   Note generali   Title from title screen (viewed on Apr. 18, 2007).
                        "February 2007."
                        Paper version available from: U.S. Govt. Accountability Office, 441 G St., NW, Rm. LM, Washington, D.C. 20548.
                        "GAO-07-309."

   Nota di bibliografia   Includes bibliographical references.

2.	Record Nr.	UNINA9910143880803321
	Titolo	Selected Areas in Cryptography : 9th Annual International Workshop, SAC 2002, St. John's, Newfoundland, Canada, August 15-16, 2002, Revised Papers / / edited by Kaisa Nyberg, Howard Heys
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
	ISBN	3-540-36492-7
	Edizione	[1st ed. 2003.]
	Descrizione fisica	1 online resource (XII, 412 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2595
	Disciplina	005.8/2
	Soggetti	Data encryption (Computer science)
		Computer networks
		Operating systems (Computers)
		Algorithms
		Management information systems
		Computer science
		Cryptology
		Science, Humanities and Social Sciences, multidisciplinary
		Computer Communication Networks
		Operating Systems
		Algorithm Analysis and Problem Complexity
		Management of Computing and Information Systems
	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	Elliptic Curve Enhancements -- Modifications of ECDSA -- Integer Decomposition for Fast Scalar Multiplication on Elliptic Curves -- Analysis of the Gallant-Lambert-Vanstone Method Based on Efficient Endomorphisms: Elliptic and Hyperelliptic Curves -- SNOW -- Guess-and-Determine Attacks on SNOW -- A New Version of the Stream Cipher SNOW -- Encryption Schemes -- Encryption-Scheme Security in the Presence of Key-Dependent Messages -- On the Security of CTR + CBC-MAC -- Single-Path Authenticated-Encryption Scheme Based on Universal Hashing -- Differential Attacks -- Markov Truncated

Differential Cryptanalysis of Skipjack -- Higher Order Differential Attack of Camellia(II) -- Square-like Attacks on Reduced Rounds of IDEA -- Full-Round Differential Attack on the Original Version of the Hash Function Proposed at PKC'98 -- Boolean Functions and Stream Ciphers -- On Propagation Characteristics of Resilient Functions -- Two Alerts for Design of Certain Stream Ciphers: Trapped LFSR and Weak Resilient Function over GF(q) -- Multiples of Primitive Polynomials and Their Products over GF(2) -- A New Cryptanalytic Attack for PN-generators Filtered by a Boolean Function -- Block Cipher Security -- White-Box Cryptography and an AES Implementation -- Luby-Racko. Ciphers: Why XOR Is Not So Exclusive -- Signatures and Secret Sharing -- New Results on Unconditionally Secure Distributed Oblivious Transfer -- Efficient Identity Based Signature Schemes Based on Pairings -- The Group Diffie-Hellman Problems -- MAC and Hash Constructions -- Secure Block Ciphers Are Not Sufficient for One-Way Hash Functions in the Preneel-Govaerts-Vandewalle Model -- An Efficient MAC for Short Messages -- RSA and XTR Enhancements -- Optimal Extension Fields for XTR -- On Some Attacks on Multi-prime RSA.

| Sommario/riassunto | This book constitutes the thoroughly refereed post-proceedings of the 9th Annual International Workshop on Selected Areas in Cryptology, SAC 2002, held in St. John's, Newfoundland, Canada, in August 2002. The 25 revised full papers presented were carefully selected from 90 submissions during two rounds of reviewing and improvement. The papers are organized in topical sections on elliptic curve enhancements, SNOW, encryption schemes, differential attacks, Boolean functions and stream ciphers, block cipher security, signatures and secret sharing, MAC and hash constructions, and RSA and XTR enhancements. |