1. Record Nr. UNINA9910143458503321

Titolo	Fast Software Encryption : 6th International Workshop, FSE'99 Rome, Italy, March 24-26, 1999 Proceedings / / edited by Lars Knudsen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1999
ISBN	3-540-48519-8
Edizione	[1st ed. 1999.]
Descrizione fisica	1 online resource (VIII, 324 p.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 1636
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer programming Algorithms Coding theory Information theory Electronic data processing - Management Cryptology Programming Techniques Coding and Information Theory IT Operations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Advanced Encryption Standard -- Improved Analysis of Some Simplified Variants of RC6 -- Linear Cryptanalysis of RC5 and RC6 -- A Revised Version of CRYPTON: CRYPTON V1.0 -- Attack on Six Rounds of CRYPTON -- On the Security of the 128-bit Block Cipher DEAL -- Cryptanalysis of a Reduced Version of the Block Cipher E2 -- On the Decorrelated Fast Cipher (DFC) and Its Theory -- Remotely Keyed Encryption -- Scramble All, Encrypt Small -- Accelerated Remotely Keyed Encryption -- Analysis of Block Ciphers I -- Miss in the Middle Attacks on IDEA and Khufu -- Mod n Cryptanalysis, with Applications against RC5P and M6 -- The Boomerang Attack -- Miscellaneous -- Towards Making Luby-Rackoff Ciphers Optimal and Practical -- A New Characterization of Almost Bent Functions -- Imprimitive Permutation

Groups and Trapdoors in Iterated Block Ciphers -- Modes of Operation -- On the Security of Double and 2-Key Triple Modes of Operation -- On the Construction of Variable-Input-Length Ciphers -- Analysis of Block Ciphers II -- Slide Attacks -- On the Security of CS-Cipher -- Interpolation Attacks of the Block Cipher: SNAKE -- Stream Ciphers -- High-Speed Pseudorandom Number Generation with Small Memory -- SOBER Cryptanalysis.

Sommario/riassunto

TheFastSoftwareEncryptionWorkshop1999isthesixthinaseriesofworksho ps startinginCambridgeinDecember1993. TheworkshopwasorganizedbyGeneralChairWilliamWolfowicz,Fon- zioneU. Bordoni,andProgrammeChairLarsKnudsen,UniversityofBergen, Norway,incooperationwithSecurteam,asfaraslocalarrangementswerec- cerned. TheworkshopwasheldMarch24-26,1999inRome,Italy. Theworkshopconcentratedonallaspectsoffastsecretkeyciphers,inc- dingthedesignandcryptanalysisofblockandstreamciphers,aswellashash functions. Therewere51submissions,allofthemsubmittedelectronically. Ones- missionwaslaterwithdrawnbytheauthors, and22paperswereselectedfor presentation. Allsubmissionswerecarefullyreviewedbyatleast4committee members. Attheworkshop,preliminaryversionsofall22papersweredistri- tedtoallattendees. Aftertheworkshoptherewasa nalreviewingprocesswith additionalcommentstotheauthors. Ithasbeenachallengeformetochairthecommitteeofthisworkshop,andit isapleasuretothankallthemembersoftheprogrammecommitteefortheirhar d work. Thecommitteethisyearconsistedof,inalphabeticorder,RossAnd- son(Cambridge,UK),EliBiham(Technion,Israel),DonCoppersmith(IBM, USA), Cunsheng Ding (Singapore), Dieter Gollmann (Microsoft, UK), James Massey (Denmark), Mitsuru Matsui (Mitsubishi, Japan), Bart Preneel (K. U. Leuven, Belgium), Bruce Schneier (Counterpane, USA), and Serge Vaudenay (ENS,France). ItisagreatpleasuretothankWilliamWolfowiczfororganisingtheworkshop. Also,itisapleasuretothankSecurteamforthelogisticsandTelsyandSunfor supportingtheconference. Finally, abigthankyoutoallsubmittingauthorsfor theircontributions, andtoallattendees(approximately165)oftheworkshop. Finally, I would like to thank Vincent Rijmen for his technical assistance in preparingtheseproceedings. April1999 LarsKnudsen TableofContents AdvancedEncryptionStandard ImprovedAnalysisofSomeSimpli edVariantsofRC6 . . . . . 1 S. Contini,R. L. Rivest, M. J. B. Robshaw,andY. L. Yin LinearCryptanalysisofRC5andRC6. . . . . 16 J. Borst,B. Preneel,andJ. Vandewalle ARevisedVersionofCRYPTON:CRYPTONV1. 0. . . . . 31 C. H. Lim AttackonSixRoundsofCRYPTON. . . . . 46 C. D''Halluin,G. Bijnens,V. Rijmen,andB. Preneel OntheSecurityofthe128-bitBlockCipherDEAL. . . . . 60 S. Lucks CryptanalysisofaReducedVersionoftheBlockCipherE2. . . . . 71 M. MatsuiandT. Tokita OntheDecorrelatedFastCipher(DFC) andItsTheory. . . . . 81 L. R. KnudsenandV. Rijmen RemotelyKeyedEncryption ScrambleAll,EncryptSmall. . . . . 95 M. Jakobsson,J. P. Stern, andM. Yung AcceleratedRemotelyKeyedEncryption. . . . . 112 S. Lucks AnalysisofBlockCiphersI MissintheMiddleAttacksonIDEAandKhufu. . . . . 124 E. Biham,A. Biryukov,andA. Shamir ModnCryptanalysis, withApplicationsagainstRC5PandM6. . . . . 139 J. Kelsey,B. Schneier,andD. Wagner TheBoomerangAttack. . . . . 156 D. Wagner Miscellaneous

 ImprovedAnalysisof SomeSimpli edVariantsofRC6 1 2 1 1 ScottContini ,RonaldL. Rivest ,M. J. B. Robshaw ,andYiqunLisaYin 1 RSALaboratories,2955CampusDrive SanMateo,CA94403,USA fscontini,matt,yiqung@rsa. com 2 M. I. T. LaboratoryforComputerScience,545TechnologySquare Cambridge, MA02139,USA rivest@theory. lcs. mit.