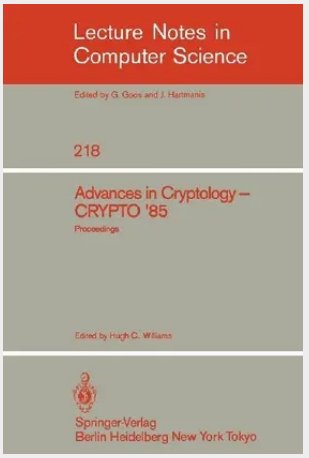
Williams

Advances in Cryptology

Proceedings of CRYPTO '85



In the summer of 1981 Allen Gersho organized the first major open co,ifcrcncc c~ci devoted to cryptologic research This meeting, Crypto '81, was held at the Universitc nl California campus in Santa Barbara Since then the Crypto' conference has become dii annual event These are the proceedings of the fifth1 of these confercnces, Crypt0 XS Each section of this volume corresponds to a session at the meeting. Thr paperk were accepted by the program committee, sometimes on the basis of an abstract only. and appear here without having been otherwise refereed. The last section contains papers lor some of the impromptu talks given at the traditional rump session. Each of thew pq1ci-k was refereed by a single member of the program committee. An author index;is wcll;l\ 'l keyword index, the entries for which were mainly supplied by the authors. appear at 11ic end of the volume. Unfortunately, two of the papers accepted for presentation at Crypto '85 could noi be included in this book they are: Unique Extrapolation of Polynomial Recurrences J. C. Lagarias and J. A. Reeds (A. T. & T Bell Labs) Some Cryptographic Applications of Permutation l'olynomials and Permutation Functions Rupert Nobarer (Universitat fur Bildungswissenschaftttn, Austria) It is my great pleasure to acknowledge the efforts of all of those who contributed to making these proceedings possible: the authors, program committee, other orgmizrrs ot the meeting, IACR officers and directors. and aU the attendees.

Signatures and authentication.- Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields.- Another Birthday Attack.- Attacks on Some RSA Signatures.- An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi.- A Secure Subliminal Channel (?).- Unconditionally Secure Authentication Schemes and Practical and Theoretical Consequences.- Protocols.- On the Security of Ping-Pong Protocols when Implemented using the RSA (Extended Abstract).- A Secure Poker Protocol that Minimizes the Effect of Player Coalitions.- A Framework for the Study of Cryptographic Protocols.- Cheating at Mental Poker.- Security for the DoD Transmission Control Protocol.- Symmetric Public-Key Encryption.- Copy Protection.- Software Protection: Myth or Reality?.- Public Protection of Software.- Fingerprinting Long Forgiving Messages.- Single Key Cryptology.- Cryptanalysis of des with a Reduced Number of Rounds.- Is DES a Pure Cipher? (Results of More Cycling Experiments on DES) (Preliminary Abstract).- A Layered Approach to the Design of Private Key Cryptosystems.- Lifetimes of Keys in Cryptographic Key Management Systems.- Correlation Immunity and the Summation Generator.- Design of Combiners to Prevent Divide and Conquer Attacks.- On the Security of DES.- Information theory without the finiteness assumption, II. Unfolding the DES.- Two Key Cryptology.- Analysis of a Public Key Approach Based on Polynomial Substitution.- Developing an RSA Chip.- An M3 Public-Key Encryption Scheme.- Trapdoor Rings And Their Use In Cryptography.- On Computing Logarithms Over Finite Fields.- N Using RSA with Low Exponent in a Public Key Network.- Lenstra's Factorisation Method Based on Elliptic Curves.- Use of Elliptic Curves in Cryptography.- Randomness and Other Problems.- Cryptography withCellular Automata.- Efficient Parallel Pseudo-Random Number Generation.- How to Construct Pseudo-random Permutations from Pseudo-random Functions.- The Bit Security of Modular Squaring given Partial Factorization of the Modulos.- Some Cryptographic Aspects of Womcodes.- How to Reduce your Enemy's Information (extended abstract).- Encrypting Problem Instances.- Divergence Bounds on Key Equivocation and Error Probability in Cryptanalysis.- Impromptu Talks.- A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes.- On the Design of S-Boxes.- The Real Reason for Rivest's Phenomenon.- The Importance of "Good" Key Scheduling Schemes (How to Make a Secure DES* Scheme with ? 48 Bit Keys?).- Access Control at the Netherlands Postal and Telecommunications Services.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540164630
Medium: Buch
ISBN: 978-3-540-16463-0
Verlag: Springer
Erscheinungstermin: 01.04.1986
Sprache(n): Englisch
Auflage: 1. Auflage 1986
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1720 g
Seiten: 552
Format (B x H): 155 x 235 mm