

Advances in Cryptology

Proceedings of EUROCRYPT 84. A Workshop on the Theory and Application of Cryptographic Techniques - Paris, France, April 9-11, 1984

This book contains the proceedings of EUROCRYPT 84, held in Paris in 1984, April 9-11, at the University of Paris, Sorbonne. EUROCRYPT is now an annual international European meeting in cryptology, intended primarily for the international of researchers in this area. EUROCRYPT 84 was community following previous meetings held at Burg Feuerstein in 1982 and at IJline in 1983. In fact EUROCRYPT 84 was the first such meeting being organized under IXCR (International Association of Cryptology Research). Other sponsors were the well-known French association on cybernetics research AFCET, the LITP (Laboratoire d'Informatique théorique et de Programmation), which is a laboratory of computer science associated with CNRS, and the department of mathematics and computer science at the University René Descartes, Sorbonne. EUROCRYPT 83 was very successful, with about 180 participants from a great variety of foreign countries and 50 papers addressing all aspects of cryptology, close to applied as well as theoretical. It also had a special feature, i.e. a special session on smart cards particularly welcome at the time, since France was then carrying on an ambitious program on smart cards. EUROCRYPT 84 was a great experience. We like to thank all the sponsors and all the authors for their submission of papers. Paris, December 74th. CONTENTS SECTION I: GENERAL THEORY, CLASSICAL METHODS 3 Cryptology and Complexity Theories. G. RINGGUT 10 On Cryptosystems based on Polynomials and finite Fields. R. Rivest 16 Algebraic Structures of Cryptographic Transformations.

This book contains the proceedings of EUROCRYPT 84, held in Paris in 1984, April 9-11, at the University of Paris, Sorbonne. EUROCRYPT is now an annual international European meeting in cryptology, intended primarily for the international of researchers in this area. EUROCRYPT 84 was community following previous meetings held at Burg Feuerstein in 1982 and at IJline in 1983. In fact EUROCRYPT 84 was the first such meeting being organized under IXCR (International Association of Cryptology Research). Other sponsors were the well-known French association on cybernetics research AFCET, the LITP (Laboratoire d'Informatique théorique et de Programmation), which is a laboratory of computer science associated with CNRS, and the department of mathematics and computer science at the University René Descartes, Sorbonne. EUROCRYPT 83 was very successful, with about 180 participants from a great variety of foreign countries and 50 papers addressing all aspects of cryptology, close to applied as well as theoretical. It also had a special feature, i.e. a special session on smart cards particularly welcome at the time, since France was then carrying on an ambitious program on smart cards. EUROCRYPT 84 was a great experience. We like to thank all the sponsors and all the authors for their submission of papers. Paris, December 74th. CONTENTS SECTION I: GENERAL THEORY, CLASSICAL METHODS 3 Cryptology and Complexity Theories G. RINGGUT 10 On Cryptosystems based on Polynomials and finite Fields. R. Rivest 16 Algebraic Structures of Cryptographic Transformations.



50,28 €

46,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540160762

Medium: Buch

ISBN: 978-3-540-16076-2

Verlag: Springer

Erscheinungstermin: 01.12.1985

Sprache(n): Englisch

Auflage: 1985

Serie: Lecture Notes in Computer Science

Produktform: Kartoniert

Gewicht: 1540 g

Seiten: 494

Format (B x H): 155 x 235 mm

