Applications of Finite Fields

Based on the proceedings of a conference organized by The Institute of Mathematics and its Applications on the Applications of Finite Fields held at Royal Holloway, University of London in July 1994

Edited by

DIETER GOLLMANN

Royal Holloway
University of London

CLARENDON PRESS • OXFORD • 1996

CONTENTS

G.L. Mullen
Bases and the Distribution of Irreducible and Primitive Polynomials over Finite Fields 1

I.F. Blake, S. Gao and R.J. Lambert
Construction and Distribution Problems for Irreducible Trinomials over Finite Fields 19

P.T. Young
Congruences for Generalised Dickson Polynomials 33

A. Scheerhorn
Dickson Polynomials and Completely Normal Elements over Finite Fields 47

H. Meyn
An Iterated Normal Presentation of GF(q^{2^m}) 57

W. Geiselmann
Weakly Self-Dual Normal Bases in Finite Fields 67

S. Dodunekov and I. Landgev
On the Quarternary [11,6,5] and [12,6,6] Codes 75

R. Hill and I. Landgev
On the Nonexistence of some Quaternary Codes 85

H. Kuwakado and K. Koyama
A New RSA-type Cryptosystem Based on Singular Cubic Curves 99

S.R. Blackburn
A Generalisation of the Discrete Fourier Transform 111

R.E. Peile
On a Generalised Minimum Distance Reed–Solomon Decoding Algorithm 117