

Journal of Discrete Mathematical Sciences & Cryptography

VOLUME 10

NUMBER 2

APRIL 2007

ISSN 0972-0529

CONTENTS

M. BORGES-QUINTANA, M. A. BORGES-TRENARD AND E. MARTÍNEZ-MORO : On a Gröbner bases structure associated to linear codes	151–191
C. C. WU AND C. C. CHANG : Attacks on provably secure proxy-protected signature schemes based on factoring	193–204
J. RATSABY : On the VC-dimension and boolean functions with long runs	205–225
H. L. JEN, T. C. HSIA AND M. B. HASAN : A study of methods for construction of balanced incomplete block design	227–243
A. P. SANTHAKUMARAN : Periphery with respect to cliques in graphs	245–254
S. GEORGIU, C. KOUKOUVINOS AND E. LAPPAS : Self-dual codes over some prime fields constructed from skew-Hadamard matrices	255–266
D. MUKHOPADHYAY AND D. ROYCHOWDHURY : Fault based attack of the Rijndael cryptosystem	267–290
M. KUMARI : Indices to measure the cryptographic strength of S-box	291–312

Published by:

Taru Publications
NEW DELHI