

# Discrete Applied Mathematics

## Volume 154, Issue 2, 1 February 2006

### Special Issue: Coding and Cryptography

**Guest Editors:**  
**Pascale Charpin, Gregory Kabatianski**

## Contents

<i>P. Charpin and G. Kabatianski</i> Editorial	173
Guest Editors	174
<i>J. Camenisch and M. Koprowski</i> Fine-grained forward-secure signature schemes without random oracles	175
<i>S. Canard, B. Schoenmakers, M. Stam and J. Traoré</i> List signature schemes	189
<i>A. Canteaut, M. Daum, H. Dobbertin and G. Leander</i> Finding nonnormal bent functions	202
<i>P. D'Arco, W. Kishimoto and D.R. Stinson</i> Properties and constraints of cheating-immune secret sharing schemes	219
<i>A. De Santis, A.L. Ferrara and B. Masucci</i> Unconditionally secure key assignment schemes	234
<i>I. Dumer and K. Shabunov</i> Recursive error correction for general Reed–Muller codes	253
<i>R. Dupont and A. Enge</i> Provably secure non-interactive key distribution based on pairings	270
<i>S. Ferret and L. Storme</i> A classification result on weighted $\{\delta v_{\mu+1}, \delta v_{\mu}; N, p^3\}$ -minihypers	277
<i>J. Freudenberger and V. Zyablov</i> On the complexity of suboptimal decoding for list and decision feedback schemes	294

(continued)

<i>E.M. Gabidulin and N.I. Pilipchuk</i> Symmetric matrices and codes correcting rank errors beyond the $\lfloor (d-1)/2 \rfloor$ bound	305
<i>X.-d. Hou</i> Anity of permutations of $\mathbb{F}_2^n$	313
<i>E. Kiltz and A. Winterhof</i> Polynomial interpolation of cryptographic functions related to Diffie–Hellman and discrete logarithm problem	326
<i>A.S. Kuzmin, V.T. Markov, A.A. Nechaev and A.S. Neljubin</i> A generalization of the binary Preparata code	337
<i>S. Ling, C. Xing and F. Özbudak</i> An explicit class of codes with good parameters and their duals	346
<i>S. Maitra and E. Pasalic</i> A Maiorana–McFarland type construction for resilient Boolean functions on $n$ variables ( $n$ even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$	357
<i>U. Maurer</i> Secure multi-party computation made simple	370
<i>T. Meskanen and A. Renvall</i> A wrap error attack against NTRUEncrypt	382
<i>R. Quarez</i> Some subsets of points in the plane associated to truncated Reed–Muller codes with good parameters	392
<i>J.A. Ryan and P. Fitzpatrick</i> Enumeration of inequivalent irreducible Goppa codes	399
<i>A. Sălăgean</i> Repeated-root cyclic and negacyclic codes over a finite chain ring	413
<i>H. Sibert, P. Dehornoy and M. Girault</i> Entity authentication schemes using braid word reduction	420