References

[1] Dang Hoai Bac, Nguyen Binh, and Nguyen Xuan Quynh. Novel algebraic structure for cyclic codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 301–310. Springer-Verlag, Berlin-Heidelberg, 2007.

[2] Grégory Berhuy and Frédérique Oggier. Space-time codes from crossed product algebras of degree 4. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 90–99. Springer-Verlag, Berlin-Heidelberg, 2007.

[3] Daniel J. Bernstein. The tangent fft. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 291–300. Springer-Verlag, Berlin-Heidelberg, 2007.

[4] Daniel J. Bernstein and Tanja Lange. Inverted edwards coordinates. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 20–27. Springer-Verlag, Berlin-Heidelberg, 2007.

[5] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. Determining the nonlinearity of a new family of apn functions. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 72–79. Springer-Verlag, Berlin-Heidelberg, 2007.

[6] Maria Bras-Amorós and Michael E. O'Sullivan. Extended norm-trace codes with optimized correction capability. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Sym-*

posium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007), volume 4851 of *LNCS*, pages 337–346. Springer-Verlag, Berlin-Heidelberg, 2007.

[7] Irène Charon, Gérard Cohen, Olivier Hudry, and Antoine Lobstein. Links between discriminating and identifying codes in the binary hamming space. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 267–270. Springer-Verlag, Berlin-Heidelberg, 2007.

[8] M. Prem Laxman Das and Kripasindhu Sikdar. On the computation of non-uniform input for list decoding on bezerra-garcia tower. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 237–246. Springer-Verlag, Berlin-Heidelberg, 2007.

[9] P. Embury and A. Rao. A path to hadamard matrices. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 281–290. Springer-Verlag, Berlin-Heidelberg, 2007.

[10] Olav Geil and Ryutaroh Matsumoto. Generalized sudan's list decoding for order domain codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 50–59. Springer-Verlag, Berlin-Heidelberg, 2007.

[11] Venkatesan Guruswami. List decoding and pseudorandom constructions. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 1–6. Springer-Verlag, Berlin-Heidelberg, 2007.

[12] Tom Høholdt and Jørn Justesen. Iterative list decoding of ldpc codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 18–19. Springer-Verlag, Berlin-Heidelberg, 2007.

[13] Camilla Hollanti and Hsiao-feng (Francis) Lu. Normalized minimum determinant calculation for multi-block and asymmetric space-time codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 227–236. Springer-Verlag, Berlin-Heidelberg, 2007.

[14] H. Janwa and A.K. Lal. On generalized hamming weights and the covering radius of linear codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 347–356. Springer-Verlag, Berlin-Heidelberg, 2007.

[15] Haruhiko Kaneko and Eiji Fujiwara. Joint source-cryptographic-channel coding based on linear block codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 158–167. Springer-Verlag, Berlin-Heidelberg, 2007.

[16] Navin Kashyap. The "art of trellis decoding" is *np*-hard. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 198–207. Springer-Verlag, Berlin-Heidelberg, 2007.

[17] Selçuk Kavut and Melek Diker Yücel. Generalized rotation symmetric and dihedral symmetric boolean functions — 9 variable boolean functions with nonlinearity 242. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on*

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007), volume 4851 of *LNCS*, pages 321–329. Springer-Verlag, Berlin-Heidelberg, 2007.

[18] Young-Joon Kim, Seok-Yong Jin, and Hong-Yeop Song. Linear complexity and autocorrelation of prime cube sequences. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 188–197. Springer-Verlag, Berlin-Heidelberg, 2007.

[19] Dinesh Krithivasan and S. Sandeep Pradhan. Lattices for distributed source coding: Jointly gaussian sources and reconstruction of a linear function. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 178–187. Springer-Verlag, Berlin-Heidelberg, 2007.

[20] Jyrki Lahtonen and Roope Vehkalahti. Dense mimo matrix lattices — a meeting point for class field theory and invariant theory. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 247–256. Springer-Verlag, Berlin-Heidelberg, 2007.

[21] Yann Laigle-Chapuy. A note on a class of quadratic permutations over f_{2^n}. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 130–137. Springer-Verlag, Berlin-Heidelberg, 2007.

[22] Maheshanand and Siri Krishan Wasan. On quasi-cyclic codes over integer residue rings. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007*

(Bangalore, India, December 16-20, 2007), volume 4851 of *LNCS*, pages 330–336. Springer-Verlag, Berlin-Heidelberg, 2007.

[23] Gary McGuire. Spectra of boolean functions, subspaces of matrices, and going up versus going down. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 28–37. Springer-Verlag, Berlin-Heidelberg, 2007.

[24] Silvana Medoš and Serdar Boztaş. Fault-tolerant finite field computation in the public key cryptosystems. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 120–129. Springer-Verlag, Berlin-Heidelberg, 2007.

[25] Harald Niederreiter and Arne Winterhof. On the structure of inversive pseudorandom number generators. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 208–216. Springer-Verlag, Berlin-Heidelberg, 2007.

[26] Koji Nuida, Satoshi Fujitsu, Manabu Hagiwara, Takashi Kitagawa, Hajime Watanabe, Kazuto Ogawa, and Hideki Imai. An improvement of tardos's collusion-secure fingerprinting codes with very short lengths. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 80–89. Springer-Verlag, Berlin-Heidelberg, 2007.

[27] Goutam Paul, Subhamoy Maitra, and Rohit Srivastava. On non-randomness of the permutation after rc4 key scheduling. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 100–109. Springer-Verlag, Berlin-Heidelberg, 2007.

[28] N. Pinnawala, A. Rao, and T.A. Gulliver. Distribution of trace values and two-weight, self-orthogonal codes over $gf(p, 2)$. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 311–320. Springer-Verlag, Berlin-Heidelberg, 2007.

[29] J. Pujol, J. Rifà, and F.I. Solov'eva. Quaternary plotkin constructions and quaternary reed-muller codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 148–157. Springer-Verlag, Berlin-Heidelberg, 2007.

[30] Safitha J. Raj and Andrew Thangaraj. Subcodes of reed-solomon codes suitable for soft decoding. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 217–226. Springer-Verlag, Berlin-Heidelberg, 2007.

[31] Sondre Rønjom, Guang Gong, and Tor Helleseth. A survey of recent attacks on the filter generator. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 7–17. Springer-Verlag, Berlin-Heidelberg, 2007.

[32] Atri Rudra. Efficient list decoding of explicit codes with optimal redundancy. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 38–46. Springer-Verlag, Berlin-Heidelberg, 2007.

[33] Sumanta Sarkar and Subhamoy Maitra. Construction of rotation symmetric boolean functions on odd number of variables with maximum

algebraic immunity. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 271–280. Springer-Verlag, Berlin-Heidelberg, 2007.

[34] B.A. Sethuraman and Frédérique Oggier. Constructions of orthonormal lattices and quaternion division algebras for totally real number fields. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 138–147. Springer-Verlag, Berlin-Heidelberg, 2007.

[35] Priti Shankar. Algebraic structure theory of tail-biting trellises. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 47–47. Springer-Verlag, Berlin-Heidelberg, 2007.

[36] Henning Stichtenoth. Nice codes from nice curves. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 48–49. Springer-Verlag, Berlin-Heidelberg, 2007.

[37] Shigenori Yamakawa, Yang Cui, Kazukuni Kobara, Manabu Hagiwara, and Hideki Imai. On the key-privacy issue of mceliece public-key encryption. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 168–177. Springer-Verlag, Berlin-Heidelberg, 2007.

[38] Akihiro Yamamura. Homomorphic encryptions of sums of groups. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms*

and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007), volume 4851 of *LNCS*, pages 357–366. Springer-Verlag, Berlin-Heidelberg, 2007.

[39] Kenji Yasunaga and Toru Fujiwara. Correctable errors of weight half the minimum distance plus one for the first-order reed-muller codes. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 110–119. Springer-Verlag, Berlin-Heidelberg, 2007.

[40] Kazuki Yoneyama, Haruki Ota, and Kazuo Ohta. Secure cross-realm client-to-client password-based authenticated key exchange against undetectable on-line dictionary attacks. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 257–266. Springer-Verlag, Berlin-Heidelberg, 2007.

[41] Jianqin Zhou, Wai Ho Mow, and Xiaoping Dai. Bent functions and codes with low peak-to-average power ratio for multi-code cdma. In Serdar Boztaş and Hsiao-Feng (Francis) Lu, editors, *Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2007 (Bangalore, India, December 16-20, 2007)*, volume 4851 of *LNCS*, pages 60–71. Springer-Verlag, Berlin-Heidelberg, 2007.