References

[1] Rafael Álvarez, Leandro Tortosa, José Vicent, and Antonio Zamora. A non-abelian group based on block upper triangular matrices with cryptographic applications. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 117–126. Springer-Verlag, Berlin-Heidelberg, 2009.

[2] Víctor Álvarez, José Ándrés Armario, María Dolores Frau, Félix Gudiel, and Amparo Osuna. Rooted trees searching for cocyclic hadamard matrices over d_{4t}. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 204–214. Springer-Verlag, Berlin-Heidelberg, 2009.

[3] Riddhipratim Basu, Subhamoy Maitra, Goutam Paul, and Tanmoy Talukdar. On some sequences of the secret pseudo-random index j in rc4 key scheduling. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 137–148. Springer-Verlag, Berlin-Heidelberg, 2009.

[4] Peter Beelen and Diego Ruano. The order bound for toric codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 1–10. Springer-Verlag, Berlin-Heidelberg, 2009.

[5] José Joaquín Bernal, Ángel del Río, and Juan Jacobo Simón. There are not non-obvious cyclic affine-invariant codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 101–106. Springer-Verlag, Berlin-Heidelberg, 2009.

[6] Jürgen Bierbrauer. New commutative semifields and their nuclei. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 179–185. Springer-Verlag, Berlin-Heidelberg, 2009.

[7] M. Borges-Quintana, M.A. Borges-Trenard, and E. Martínez-Moro. Gröbner representations of binary matroids. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 227–230. Springer-Verlag, Berlin-Heidelberg, 2009.

[8] Maria Bras-Amorós and Michael E. O'Sullivan. From the euclidean algorithm for solving a key equation for dual reed-solomon codes to the berlekamp-massey algorithm. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 32–42. Springer-Verlag, Berlin-Heidelberg, 2009.

[9] John Brevik, Michael E. O'Sullivan, Anya Umlauf, and Rich Wolski. Simulation of the sum-product algorithm using stratified sampling. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 65–72. Springer-Verlag, Berlin-Heidelberg, 2009.

[10] Joan-Josep Climent, Victoria Herranz, Carmen Perea, and Virtudes Tomás. A systems theory approach to periodically time-varying convolutional codes by means of their invariant equivalent. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 73–82. Springer-Verlag, Berlin-Heidelberg, 2009.

[11] Yang Cui, Kirill Morozov, Kazukuni Kobara, and Hideki Imai. Efficient constructions of deterministic encryption from hybrid encryption and code-based pke. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 159–168. Springer-Verlag, Berlin-Heidelberg, 2009.

[12] Iwan Duursma and Radoslav Kirov. An extension of the order bound for ag codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 11–22. Springer-Verlag, Berlin-Heidelberg, 2009.

[13] Edwin D. El-Mahassni and Domingo Gomez. On the distribution of nonlinear congruential pseudorandom numbers of higher orders in residue rings. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 195–203. Springer-Verlag, Berlin-Heidelberg, 2009.

[14] Marta Giorgetti. Interesting examples on maximal irreducible goppa codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 215–218. Springer-Verlag, Berlin-Heidelberg, 2009.

[15] Manabu Hagiwara, Takahiro Yoshida, and Hideki Imai. Bounds on the number of users for random 2-secure codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 239–242. Springer-Verlag, Berlin-Heidelberg, 2009.

[16] Tom Høholdt and Heeralal Janwal. Optimal bipartite ramanujan graphs from balanced incomplete block designs: Their characterizations and applications to expander/ldpc codes. In Maria Bras-Amorós

and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 53–64. Springer-Verlag, Berlin-Heidelberg, 2009.

[17] Álvar Ibeas and Arne Winterhof. Noisy interpolation of multivariate sparse polynomials in finite fields. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 169–178. Springer-Verlag, Berlin-Heidelberg, 2009.

[18] José Ignacio Iglesias Curto. On elliptic convolutional goppa codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 83–91. Springer-Verlag, Berlin-Heidelberg, 2009.

[19] Ivan Landjev. Spreads in projective hjelmslev geometries. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 186–194. Springer-Verlag, Berlin-Heidelberg, 2009.

[20] Sergio R. López-Permouth and Steve Szabo. Repeated root cyclic and negacyclic codes over galois rings. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 219–222. Springer-Verlag, Berlin-Heidelberg, 2009.

[21] David M. Monarres and Michael E. O'Sullivan. A generalization of the zig-zag graph product by means of the sandwich product. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 231–234. Springer-Verlag, Berlin-Heidelberg, 2009.

[22] C. Munuera, F. Torres, and J. Villanueva. Sparse numerical semigroups. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 23–31. Springer-Verlag, Berlin-Heidelberg, 2009.

[23] Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada. On self-dual codes over z_{16}. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 107–116. Springer-Verlag, Berlin-Heidelberg, 2009.

[24] Hakan Özadam and Ferruh Özbudak. The minimum hamming distance of cyclic codes of length $2p^s$. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 92–100. Springer-Verlag, Berlin-Heidelberg, 2009.

[25] Jaume Pernas, Jaume Pujol, and Mercè Villanueva. Rank for some families of quaternary reed-muller codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 43–52. Springer-Verlag, Berlin-Heidelberg, 2009.

[26] Jaume Pujol, J. Rifà, and L. Ronquillo. Construction of additive reed-muller codes. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 223–226. Springer-Verlag, Berlin-Heidelberg, 2009.

[27] SeongHan Shin, Kazukuni Kobara, and Hideki Imai. Very-efficient anonymous password-authenticated key exchange and its extensions. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and

Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009), volume 5527 of *LNCS*, pages 149–158. Springer-Verlag, Berlin-Heidelberg, 2009.

[28] Guang Zeng, Yang Yang, Wenbao Han, and Shuqin Fan. Word oriented cascade jump σ — lfsr. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 127–136. Springer-Verlag, Berlin-Heidelberg, 2009.

[29] Lei Zhang, Bo Qin, Qianhong Wu, and Futai Zhang. Novel efficient certificateless aggregate signatures. In Maria Bras-Amorós and Tom Høholt, editors, *Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2009 (Tarragona, Spain, June 8-12, 2009)*, volume 5527 of *LNCS*, pages 235–238. Springer-Verlag, Berlin-Heidelberg, 2009.