References

[1] Olivier Billet and Marc Joye. The jacobi model of an elliptic curve and side-channel analysis. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 34–42. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[2] Thanasis Bouganis. Error correcting codes over algebraic surfaces. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 169–179. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[3] Thanasis Bouganis and Drue Coles. A geometric view of decoding ag codes. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 180–190. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[4] Maria Bras-Amorós. Improvements to evaluation codes and new characterizations of arf semigroups. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 204–215. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[5] Eric Brier and Marc Joye. Fast point multiplication on elliptic curves through isogenies. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003*

(Toulouse, France, May 12-16, 2003), volume 2643 of *LNCS*, pages 43–50. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[6] Rodrigo Gusmão Cavalcante and Jr. Palazzo, Reginaldo. Performance analysis of m-psk signal constellations in riemannian varieties. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 191–203. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[7] Cunsheng Ding, Arto Salomaa, Patrick Solé, and Xiaojian Tian. Three constructions of authentication/secrecy codes. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 24–33. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[8] Ivana Djurdjevic, Jun Xu, Khaled Abdel-Ghaffar, and Shu Lin. A class of low-density parity-check codes constructed based on reed-solomon codes with two information symbols. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 98–107. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[9] Sylvia Encheva and Gérard Cohen. Copyright control and separating systems. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 79–86. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[10] Andreas Enge and François Morain. Fast decomposition of polynomials with known galois group. In Marc Fossorier, Tom Høholdt, and

Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 254–264. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[11] F. Galand. On the minimum distance of some families of z_{2^k}-linear codes. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 235–243. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[12] Yasuo Hatano, Hidema Tanaka, and Toshinobu Kaneko. An optimized algebraic method for higher order differential attack. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 61–70. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[13] K.J. Horadam. Differentially 2-uniform cocycles — the binary case. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 150–157. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[14] H. Janwa. Good expander graphs and expander codes: Parameters and decoding. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 119–128. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[15] L.S. Kazarin, V.M. Sidelnikov, and I.B. Gashkov. Relative duality in macwilliams identity. In Marc Fossorier, Tom Høholdt, and Alain Poli,

editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 108–118. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[16] Andreas Klappenecker and Martin Rötteler. Unitary error bases: Constructions, equivalence, and applications. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 139–149. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[17] Kristine Lally. Quasicyclic codes of index l over f_q viewed as $f_q[x]$-submodules of $f_{q^l}[x]/\langle x^m - 1\rangle$. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 244–253. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[18] Tanja Lange and Arne Winterhof. Interpolation of the elliptic curve diffie-hellman mapping. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 51–60. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[19] Alan G.B. Lauder. Homotopy methods for equations over finite fields. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 18–23. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[20] Oscar Moreno and Francis N. Castro. On the covering radius of certain cyclic codes. In Marc Fossorier, Tom Høholdt, and Alain Poli,

editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 129–138. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[21] Anderson C.A. Nascimento, Akira Otsuka, Hideki Imai, and Joern Mueller-Quade. Unconditionally secure homomorphic pre-distributed commitments. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 87–97. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[22] Harald Niederreiter and Igor E. Shparlinski. Dynamical systems generated by rational functions. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 6–17. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[23] Domingo Ramirez-Alzola. The second and third generalized hamming weights of algebraic geometry codes. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 158–168. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[24] Hans Georg Schaathun. Fighting two pirates. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 71–78. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[25] Moshe Schwartz and Tuvi Etzion. Optimal 2-dimensional 3-dispersion lattices. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors,

Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003), volume 2643 of *LNCS*, pages 216–225. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[26] Keisuke Shiromoto. On $g - th$ mds codes and matroids. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 226–234. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.

[27] Jacques Stern. Cryptography and the methodology of provable security. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2003 (Toulouse, France, May 12-16, 2003)*, volume 2643 of *LNCS*, pages 1–5. Springer-Verlag, Berlin-Heidelberg-New York-Hong Kong-London-Milan-Paris-Tokyo, 2003.