References

[1] Yves Aubry and Philippe Langevin. On the semiprimitivity of cyclic codes. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 284–293. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[2] Roberto Avanzi and Emanuele Cesena. Trace zero varieties over fields of characteristic 2 for cryptographic applications. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 188–215. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[3] Stéphane Ballet. A note on the tensor rank of the multiplication in certain finite fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 332–342. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[4] Peter Beelen and Tom Høholdt. List decoding using syndromes. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 315–331. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[5] Kristian Brander. An optimal unramified tower of function fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 351–365. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[6] Claude Carlet. Partial covering sequences: a method for designing classes of cryptographic functions. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 366–387. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[7] Jean Chaumine. Multiplication in small finite fields using elliptic curves. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 343–350. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[8] Ran Cohen. Group law algorithms for Jacobian varieties of curves over finite fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and*

Its Applications, pages 216–240. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[9] Jean-Marc Couveignes and Reynald Lercier. Galois invariant smoothness basis. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 142–167. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[10] Eric Férard and François Rodier. Non linéarité des fonctions booléennes données par des traces de plolynômes de degré binaire 3. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 388–409. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[11] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler. Fast addition on non-hyperelliptic genus 3 curves. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 1–28. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[12] David Freeman and Kristin Lauter. Computing endomorphism rings of Jacobian of genus 2 curves over finite fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 29–66. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[13] Gerhard Frey. Discrete logarithms, duality, and arithmetic in Brauer groups. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 241–272. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[14] Emmanuel Hallouin and Marc Perret. On generators of the group $\widehat{H}^{-1}(Gal(L/K), E_L)$ in some abelian p-extension L/K. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 273–283. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[15] James Hirschfeld, Jean Chaumine, and Robert Rolland, editors. *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[16] George Hitching and Trygve Johnsen. Decoding of scroll codes. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 294–314. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[17] Mikko Kiviharju. Fuzzy pairings-based CL-PKC. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 168–187. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[18] David Kohel. Complex multiplication and canonical lifts. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 67–83. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[19] Gilles Lachaud and Christophe Ritzenthaler. On some questions of Serre on abelian threefolds. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 88–115. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[20] Hui Fai Law and Philip Wong. On quadratic extensions of cyclic projective planes. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 434–466. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[21] Gregor Leander and Philippe Langevin. On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 410–418. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[22] Dimitry Malinin. Some integral representations of finite groups and their arithmetic applications. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 467–480. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[23] Sihem Mesnager. On the number of resilient boolean functions. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 419–433. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[24] Robert Rolland. Number of points of non-absolutely irreducible hypersurfaces. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 481–487. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[25] Jean-Pierre Serre. Two letters to Jaap Top. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 84–87. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[26] Igor Shparlinski. Pseudorandom points on elliptic curves over finite fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 116–134. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[27] Felipe Voloch. Symmetric cryptography and algebraic curves. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 135–141. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[28] Norman Wildberger. Neuberg cubics over finite fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 488–504. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.

[29] Yevhen Zelenyuk. Partitions of vector spaces over finite fields. In James Hirschfeld, Jean Chaumine, and Robert Rolland, editors, *Algebraic geometry and its applications*, volume 5 of *Number Theory and Its Applications*, pages 505–511. World Scientific, 2008. Proceedings of the first SAGA conference, 7-11 May 2007, Papeete.