Publications and Preprints
updated January 2013

Elisa Gorla
University of Neuchâtel, Department of Mathematics

1. N. Budur, M. Casanellas, E. Gorla, *Hilbert functions of irreducible arithmetically Gorenstein schemes*, J. of Algebra 272 (2004) 292-310.

2. E. Gorla, *The general hyperplane section of a curve*, Trans. Amer. Math. Soc. 358, no. 2 (2006), 819–869.

3. E. Gorla, *The G-biliaison class of symmetric determinantal schemes*, J. of Algebra 310, no. 2 (2007), 880–902.

4. J. J. Climent, E. Gorla, J. Rosenthal, *Cryptanalysis of the CFVZ cryptosystem*, Adv. Math. Comm. 1, no. 1 (2007), 1–11.

5. E. Gorla, *Mixed ladder determinantal varieties from two-sided ladders*, J. of Pure and Appl. Algebra 211, no. 2 (2007) 433–444 (previously appeared in the Max-Planck-Institut für Mathematik Preprint Series 2005, 97).

6. E. Gorla, *Lifting the determinantal property*, in "Algebra, Geometry and their Interactions", Contemporary Mathematics 448 (2007), 69–89.

7. E. Gorla, C. Putmann, J. Shokrollahi, *Explicit formulas for efficient multiplication in* $\mathbb{F}_{3^{6m}}$, in "Selected Areas in Cryptography, 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17 2007", Lecture Notes in Computer Science 4876, Springer Verlag (2007), 173–183.

8. J. Shokrollahi, E. Gorla, C. Putmann, *Efficient FPGA-based multipliers for* $\mathbb{F}_{3^{97}}$ *and* $\mathbb{F}_{3^{6\cdot 97}}$, International Conference on Field Programmable Logic and Applications, 2007 - FPL 2007, IEEE Conference Proceedings, 339–344.

9. E. Gorla, *A generalized Gaeta's Theorem*, Compositio Math. 144, no. 3 (2008), 689–704.

10. F. Manganiello, E. Gorla, J. Rosenthal, *Spread codes and spread decoding in network coding*, ISIT 2008 - IEEE International Symposium on 6-11 July 2008 881–885.

11. E. De Negri, E. Gorla, *G-biliaison of ladder Pfaffian varieties*, J. Algebra 321, no. 9 (2009), 2637–2649.

12. E. Gorla, *Symmetric ladders and G-biliaison*, in "Liaison, Schottky Problem and Invariant Theory - Remembering Federico Gaeta", Progress in Mathematics 280 (M.E. Alonso, E. Arrondo, R. Mallavibarrena, I. Sols Editors), Birkhäuser (2010), 49–62.

13. E. Gorla, J. Rosenthal, *Pole placement with fields of positive characteristic*, Three Decades of Progress in Control Sciences - Dedicated to Chris Byrnes and Anders Lindquist, X. Hu, U. Jonsson, B. Wahlberg, B. Ghosh Editors, Springer-Verlag (2010), 315–329.

14. E. Gorla, *Torus-based cryptography*, invited contribution to the "Encyclopedia of Cryptography and Security" (2nd ed.), S. Jajodia and H. Van Tilborg Editors, Springer-Verlag (2011).

15. E. De Negri, E. Gorla, *Invariants of ideals generated by pfaffians*, Commutative Algebra and Its Connections to Geometry, A. Corso and C. Polini Editors, Contemporary Mathematics 555 (2011), 47–62.

16. F. Manganiello, E. Gorla, J. Rosenthal, *An algebraic approach for decoding spread codes*, Advances in Mathematics of Communications 6, no. 4 (2012), 443–466.

17. E. Gorla, J. C. Migliore, U. Nagel, *Gröbner bases via linkage*, to appear in J. Algebra.