Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography

February 18, 2013

Publications January 2012–December 2012

1 Published papers

Journal Papers

1. P. Beelen, D. Ruano: "Bounding the number of points on a curve using a generalization of Weierstrass semigroups". *Designs, Codes and Cryptography*, Vol. 66, Issue 1-3, (2013), DOI: 10.1007/s10623-012-9685-3, pp. 221–230.(PR)

2. O. Geil, C. Thomsen: "Weighted Reed-Muller codes revisited". *Designs, Codes and Cryptography*, Vol. 66, Issue 1-3 (2013), DOI: 10.1007/s10623-012-9680-8, pp. 195–220.(PR)

3. F. Hernando, T. Høholdt, D. Ruano: "List decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes". *Advances in Mathematics of Communications* (AMC), Volume 6, Issue 3, pages 259-272 (2012).(PR)

4. H.Janwa and F.Pinero:"On the Subfield Subcodes of Hermitian Codes" *Designs, Codes and Cryptography* Aug. 2012 17 pages.(PR)

5. P. Beelen, and G. Leander:" A New Construction of Highly Nonlinear S-Boxes" *Cryptography and Communications* Vol. 4/1 pp.65-77 , 2012.(PR)

6. H. Janwa and T. Høholdt:" Eigenvalues and Expansion of Bipartite Graphs" *Designs, Codes and Cryptograpy* Vol. 65/3 pp. 259-273, Dec. 2012(PR)

7. P. Beelen, S. Ghorpade, and T. Høholdt:" Duals of affine Grassmann codes and their relatives" *IEEE Trans. Inform. Theory* vol.58/6 pp. 3843-3855 June 2012.(PR)

8. H. Aref, P. Beelen, and M. Brøns:" Bilinear relative equilibria of identical point vortices" *Journal of Nonlinear Sccience* Vol.22/5 pp.849-885, 2012.(PR)

9. A. Bassa, and P. Beelen:" A closed form expression for the Drinfeld modular polynomial" *Arkiv der Matematik* Vol.99/3 pp. 237-245, 2012.(PR)

10. L. Zhang, F. Zhang, and Q. Wu:"Delegation of signing rights using certificateless proxy signatures" *Information Sciences* Vol.184/1 pp.298-309, 2012.(PR)

11. X. Li, H. Qian ,and Y. Zhou:" Pitfalls in identity based encryption using an elliptic curve combined public key." *Applied Mathematics Letters* Vol.25, 2012 (PR) pp.1111-1113.

12. X. Li, H. Qian, J. Weng, and Y. Yu:" Fully secure identity-based signcryption scheme with shorter signcrytext in the standard model" *Mathematical and Computer Modelling* Vol.57 pp.503-511 2012.(PR)

13. H. Qian, X. Li ,and X. Huang:" Tightly Secure Non-Interactive Multisignatures in the Plain Public Key Model" *Informatica* Vol. 23/3 pp.443-460, 2012(PR)

14. Y. Aubry, S. Haloui, and G. Lachaud:" Sur le nombre de points rationelles des variétés abéliennes et des Jacobiennes sur les corps finis" *C. R. Acad. Sci. Paris* Ser. I 350 (2012) pp.907-910.(PR)

15. T. Høholdt:" Mathematics in Communication" *PUBLIC SERVICE REVIEW* Vol. Europe 24 pp.56-57, 2012

Conference Contributions

1. O. Geil, S. Martin, R. Matsumoto, "A new method for constructing small-bias spaces from Hermitian codes," *in Lecture Notes in Computer Science,* LNCS-7369, Arithmetic of Finite Fields, 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012, Proceedings, Eds. : Ferruh Özbudak, Francisco Rodriguez-Henriquez, pp. 29–44.(PR)

2. O. Geil, R. Matsumoto, D. Ruano: "List decoding algorithms based on Gröbner bases for general one-point AG codes". *Information Theory Proceedings* (ISIT), 2012 IEEE International Symposium on, pages 86-90 (2012).(PR)

3. M. Abdelraheem, M.Ågren, P. Beelen, and G. Leander:"On the Distribution of Linear Biases: Three Instructive Examples" *Lecture Notes in Computer Science* Vol.7414 (CRYPTO 2012) pp.50-67 2012.(PR)

4. J. Borghoff, A. Cantaut, T. Güneysu , E.B. Kavun, M. Knesevic, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechtberger, P. Rombouts, S.S. Thomsen, and T. Yalçin:" PRINCE- A Low-Latency Block Cipher

for Pervasive Computing Applications- Extended Abstract *ASIACRYPT 2012* pp. 208-225.(PR)

5. A. Bogdanov, G. Leander, K. Nyberg and M. Wang:"Integral and Multi-dimensional Linear Distinguishers with Correlation Zero." *ASIACRYPT 2012* pp. 244-261.(PR)

6. A. Bogdanov, L.R. Knudsen, G. Leander, F. Standaert, J. P. Steinberger, and E. Tishhauser:"Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations"- (Extended Abstract) *EUROCRYPT 2012* pp. 45-62.(PR)

7. L. Zhang :"Cryptanalysis of a Certificateless Multi-proxy Signature Scheme". 13th international conference on distributed computing and networking, Hong Kong, China , Jan. 3-6 2012 *Lecture Notes in Computer Science* vol.7129 pp.544-548.(PR)

8. L. Zhang, Q. Wu, B. Qin and J.Domingo-Ferrer:" Practical Privacy for Value-Added Applicatiopns in Vehicular Ad Hoc Networks". 5th International conference on internet and distributed computing systems, Wuyishan, Fujian, China Nov.21-23, 2012 *Lecture Notes in Computer Science* Vol.7646 pp.43-57.(PR)

2 Papers accepted for publication

Journal Papers

1. F. Hernando, D. Ruano: "Decoding of matrix-product codes". Accepted for publication in *Journal of Algebra and Its Applications.* Online available at ArXiv:1107.1529, 14 pages (2012).(PR)

2. P. Beelen, T.Høholdt, J.S.R. Nielsen, and Y. Wu:"On Rational-Interpolation Based List-Decoding and List-Decoding Binary Goppa Codes." Accepted for publication in *IEEE-Trans.Inform.Theory*(PR)

3. Y. Aubry, S. Haloui, and G. Lachaud:" Onthe number of points on abelian and Jacobian varieties over finite fields". Accepted for publication in *Acta Aritmetica* 2013.(PR)

4. B. Qin, Q. Wu, L. Zhang, O.Farrás and J. Domingo-Frerrer:" Provably secure threshold public-key encryption with adaptive security and short ciphertexts" . Accepted for publication in *Information Sciences.*(PR)

Conference contributions

1. J.S.R.Nielsen and A. Zeh:"Multi-Trial Guruswami-Sudan Decoding for Generalized Reed-Solomon Codes" accepted for publication *WCC 2013* 5 pages (2012).(PR)

2. P. Beelen, M. Brøns, S. Krishnamurthy and M. A. Stremler:" Recent progress in the relative equilibria of point vortices-in memoriam Hassan Aref". Accepted for publication in *Procedia IUTAM*. 2012(PR)

3 Papers submitted for publication

1. O. Geil, R. Matsumoto, D. Ruano: "List decoding algorithm based on voting in Gröbner bases for general one-point AG codes". Submitted for publication in *Journal of Pure and Applied Algebra.* Online available at ArXiv:1203.6127, 38 pages (2012).

2. O. Geil, R. Matsumoto, D. Ruano: "Generalization of the Lee-O'Sullivan list decoding for one-point AG codes". Submitted for publication in *Journal of Symbolic computation.* Online available at ArXiv:1203.6129, 12 pages (2012).

3. O. Geil, R. Matsumoto, D. Ruano: Feng-Rao decoding of primary codes. Submitted for publication in *Finite Fields and their Applications.* Online available at ArXiv:1210.6722, 23 pages (2012).

4. F. Hernando, M. O'Sullivan, D. Ruano: "List decoding of repeated codes". Submitted for publication in *Applicable Algebra in Engineering, Communication and Computing.* Online available at ArXiv:1202.1238, 18 pages (2012)

5. I. Márquez-Corbella, E. Martínez-Moro, G.R. Pellikaan, D. Ruano: "Computational Aspects of Retrieving a Representation of an Algebraic Geometry Code". Submitted for publication in *Journal of Symbolic Computation*, 21 pages (2012).

6. T.Høholdt and J. Justesen:"On the Sizes of Expander Graphs and Minimum Distance of Graph Codes" submitted to *Discrete Mathematics* 10 pages (2012).

7. A. Garcia, H. Stichtenoth, A. Bassa and P. Beelen:" Towers of Function Fields over Non-prime Finite Fields" submitted to *Duke Mathematical Journal* 2012.

8. P. Beelen, T. Høholdt, J. Justesen and F. Pinero:"On the Dimension of Graph Codes with Reed-Solomon Component Codes" submitted to *ISIT 2013.*

9. H. Chen:"On a generalization of Graig lattices" submitted to Journal de Théorie des Nombres Bordeaux 2012.