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

March 13, 2014

Publications January 2013–December 2013

1 Published papers

Journal Papers

1. A. Bogdanov, K. Shibutani: "Generalized Feistel Networks Revisited". *Designs, Codes and Cryptography*, Vol. 66, Issue 1-3, (2013), pp. 75-97, Springer-Verlag, 2013.(PR)

2. A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, I. Verbauwhede: "The Design Space of Lightweight Cryptographic Hashing". *IEEE-Trans. Computers* vol. 62 no. 10,pp.2041-2053 , 2013.(PR)

3. X. Li, Q. Zhou, H. Qian, Y. Yu, S. Tang: "Balanced 2p-variable rotation symmetric Boolean functions with optimal algebraic immunity, good nonlinearity and good algebraic degree". *Journal of Mathematical Analysis and Applications*, Volume 4036, pp. 63-71 (2013).(PR)

4. H. Chen:"On a generalization of Graig lattices" *Journal de Théorie des Nombres Bordeaux*Vol.25, pp. 59-70, 2013. (PR)

5. P. Beelen. D. Ruano:"Bounding the number of points on a curve using a generalization of Weierstrass semigroups" *Designs, Codes and Cryptography* Vol. 66, no,1, pp. 221-230, 2013.(PR)

6. P. Beelen, T.Høholdt, J.S.R. Nielsen, and Y. Wu:"On Rational-Interpolation Based List-Decoding and List-Decoding Binary Goppa Codes." *IEEE-Trans.Inform.Theory*Vol.59, no. 6, pp. 3269-3281, 2013.(PR)

7. O. Geil, C. Thomsen, "Weighted Reed-Muller codes – revisited". *Designs, Codes and Cryptography*, Vol. 66, Issue 1-3, pages 195–220 (2013).(PR)

8. R. Matsumoto, D. Ruano, O. Geil: "Generalization of the Lee-O'Sullivan list decoding for one-point AG codes". *Journal of Symbolic Computation*, Volume 55, pages 1–9 (2013).(PR)

9. O. Geil, R. Matsumoto, D. Ruano: "Feng-Rao decoding of primary codes". *Finite Fields and their Applications*, Volume 23, pages 35–52 (2013).(PR)

10. P. Beelen, D. Ruano: "Bounding the number of points on a curve using a generalization of Weierstrass semigroups". *In Designs, Codes and Cryptography*, Vol. 66, Issue 1-3, pages 221–230 (2013) (PR)

11. F. Hernando, D. Ruano: "Decoding of matrix-product codes". *Journal of Algebra and its Applications*, Volume 12, Issue 4, Article ID 1250185, 15 pages (2013).(PR)

12. F. Hernando, M. O'Sullivan, D. Ruano: "List decoding of repeated codes". *Applicable Algebra in Engineering, Communication and Computing.* Volume 24, Issue 3-4, pages 237-253 (2013)(PR)

Conference Contributions

1. A. Bogdanov, C. Boura, V. Rijmen, M. Wang, L. Wen, J. Zhao:" Key Difference Invariant Bias in Block Ciphers" *ASIACRYPT' 13* Lecture Notes in Computer Science Vol. 8269, pp. 357-376, Springer-Verlag. 2013.(PR)

2. A. Bogdanov, A. Luykx, B. Mennik, E. Tischhauser, K. Yasuda:" Parallelelizable and Authenticated Online Ciphers" *ASIACRYPT' 13* Lecture Notes in Computer Science Vol. 8269, pp. 424-443, Springer-Verlag. 2013.(PR)

3. B. Bilgin, A. Bogdanov, M. Knesevic, F. Mendel, Q. Wang:"Fides:Ligthweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware" *CHES'13* Lecture Notes in Computer Science Vol. 8086, pp. 142-158, Springer-Verlag 2013.(PR)

4. C. Blondeau, A. Bogdanov, G. Leander :"Bounds in Shallows and in Miseries" *Crypto'13* Lecture Notes in Computer Science Vol.. 8042, pp.204-221, Springer-Verlag 2013.pp. 45-62.(PR)

5. E. Andreeva, A. Bogdanov, Y. Dodis, B. Mennick, J.P. Steinberger:"On the Indifferentiability of Key-Alternating Ciphers" *Crypto'13* Lecture Notes in Computer Science Vol.. 8042, pp.204-221, Springer-Verlag 2013.pp. 513-550.(PR)

6. Y. Yu, X. Li,, L. Weng:"Pseudorandom Generators from Regularr One-Way Functions: New Constructions with Improved Parameters" *Asiacrypt 2013* Lecture Notes in Computer Science, Vol.8270, pp.261-279,Springer-Verlag 2013.(PR)

7. X. Li, H. Qian, Y. Yu, Y. Zhou, J. Weng:" Constructing Practical Signcryption KEM from Standard Assumptions without Random Oracles" *ACNS 2013* Lecture Notes in Computer Science Vol.7954, pp. 186-201, Springer-Verlag 2013.(PR)

8. P. Beelen, F. Pinero, J. Justesen, T. Høholdt:" On the Dimension of Graph Codes with Reed-Solomon Component Codes" *IEEE International Symposium on Information Theory 2013* Proceedings Istanbul pp.1227-1231, 2013.(PR)

9. M.R. Albrecht, R. Fitzpatrick, F. Göpfert:" On the Efficacy of Solvin LWE by Reduction to Unique-SVP" in *Proceedings of International Conference on Information Security and Cryptology* 2013.(PR)

10. J.S.R. Nielsen:"Generalised Multi-sequence Shift-Register Synthesis using Module Minimisation" in *IEEE International Symposium on Information Theory 2013*, Proceedings Istanbul 2013.(PR)

11. W. Li, V. Sidorenko,J.S.R. Nielsen:"On Decoding Interleaved Chinese Remainder Codes" in *IEEE International Symposium on Information Theory 2013*, Proceedings Istanbul 2013.(PR)

12. J.S.R. Nielsen, A. Zeh:"Multi-Trial Guruswami-Sudan Decoding for Generalised Reed-Solomon Codes" *International Workshop on Coding and Cryptography 2013*(PR)

    item P. Beelen, M. Brøns , V.S. Krishnamurti, M.A. Stremler:" Recent progress in the relative equilibria of point vortices-In memoriam Hassan Aref" *Procidia IUTAM 7* pp. 3-12, 2013.

13. T. Høholdt, F. Pinero, P. Zeng:"Some Optimal Codes as Tanner Codes with BCH Component Codes" *Applications of Computer Algebra* , Malaga, Spain July 2-6 2013.

2 Papers accepted for publication

Journal Papers

1. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, J.A. Manjon:" Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm " Accepted for publication in *IEEE/ACM Transactions on Networking*(PR)

2. A. Bassa, P. Beelen,N. Nguyen:"Good Towers of Function Fields" Accepted for publication in *Algebraic Curves and Finite Fields:Codes, Cryptography and other Emergent Applications*(H. Niederreiter, A.Ostafe, D.Panario , A.Winterhof, eds.) de Gruyter, Berlin.(PR)

3. M.R. Albrecht, C. Cid, J-C. Faugere, R. Fitzpatrick, L. Perret:" On the Complexity of the BKW Algorithm on LWE" Accepted for publication in *Designs, Codes and Cryptography* 2013.(PR)

4. J.S.R. Nielsen, A. Zeh:"Multi-Trial Guruswami-Sudan Decoding for Generalised Reed-Solomon Codes" Accepted for publication in *Designs, Codes and Cryptography* 2013.(PR)

5. T.Høholdt and J. Justesen:"On the Sizes of Expander Graphs and Minimum Distance of Graph Codes" Accepted for publication in *Discrete Mathematics* 2013.

6. T. Høholdt, F. Pinero, P. Zeng:"Optimal Codes as Tanner Codes with Cyclic Component Codes" Accepted for publication in *Designs, Codes and Cryptography* 2013.(PR)

7. I. Marquez-Corbella, E. Martinez-Moro, G.R. Pellikaan, D. Ruano:"Computational Aspects of Retriving a Representation of an Algebraic Geometry Code" Accepted for publication in *Journal of Symbolic Computation* 2013.(PR)

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

Conference contributions

1. A. Bogdanov, E. Tischhauser:" On the Wrong Key Randomization and Key Equivalence Hypotheses in Matsui's Algorithm2" *FSE'13* Lecture Notes in Computer Science, 2013.(PR)

2. E. Andreeva, A. Bogdanov, B. Mennink:"Towards Understanding the Known-Key Security of Block Ciphers".*FSE'13* Lecture Notes in Computer Science, 2013.(PR) (PR)

3. A. Bogdanov, H. Geng, M. Wang,L. Wen, B. Collard :" Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia an CLEFIA" *SAC'13* Lecture Notes in Computer Science, 2013.

4. M.R. Albrecht, J-C. Faugere, R. Fitzpatrick, L. Perret:" Lazy Modulus Switching for the BKW Algorithm on LWE" *Proceedings of PKC 2014* Springer -Verlag 2014.

5. M.R. Albrecht, J-C. Faugere, R. Fitzpatrick, L. Perret, Y. Todo, K. Xagawa:" Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions" *Proceedings of PKC 2014* Springer -Verlag 2014.

3 Papers submitted for publication

1. O. Geil, S. Martin:"Further improvements on the Feng-Rao bound for dual codes" submitted for publication in *Journal of Finite Fields and Their Applications* 2013.

2. O. Geil, S. Martin:" An improvement of the Feng-rao bound for primary codes" submitted for publication in *Designs, Codes and Cryptography* 2013.

3. 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 Algebra and its Applications* 2013.

4. A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth:" An Improvement of the Gilbert-Varshamov Bound over Non-Prime Fields" submitted for publication in *IEEE Transactions on Information Theory* 2013.

5. A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth:" Galois Towers over Non-Prime Fields" submitted for publication in *Acta Arithmetica* 2013.

6. A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth:" Towers of Function Fields over Non-Prime Finite Fields" submitted for publication in *Mathematische Annalen* 2013.

7. I. Aubry, S. Haloui:" On the number of Rational Points on Prym Varieties over Finite Fields" submitted for publication in *Journal of Algebra* 2013.

4 Ph.D. Theses

1. J.S.R. Nielsen:" List Decoding of Algebraic Codes" *Department of Applied Mathematics and Computer Science, DTU, July 2013.*