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

February 22, 2013

Abstracts of Publications January 2012 - December 2012

1 Abstracts

The numbers in brackets refer to the complete list of publications.

1.1 Algebraic Geometry Codes

- In[1.JP1] Some techniques from coding theory are used to derive upper bounds for the number of rational places of a function field of an algebraic curve defined over a finite field. The used techniques yield upper bounds if the (generalized Weierstrass semigroup for an n-tuple of places is known, even if the exact defining equation of the curve is not known. As shown in examples, this sometimes enables one to get an upper bound for the number of rational places for families of function fields. The results entend results in (J. Pure Appl. Algebra 213(6) pp. 1152-1156, 2009).

- A fast algorithms using Gröbner bases is used in [1.JP4] to compute the dimensions of subfield subcodes of Hermitian codes. With these algorithms it is possible to compute the exact values of the dimension of all subfield subcodes up to $q \leq 32$ and length up to 2^{15}. It is also shown that some of the subfield subcodes of Hermitian codes are at least as good as the previously known codes, and furthermore the existence of good long codes are demonstrated.

1.2 Algebraic Geometry and Algebraic Function Fields

- The paper [3.7] contains a construction of some recursive towers of function fields over all non-prime finite fields with many rational places. This gives a substantial improvement on all known lower bounds for Ihara's quantity A_q), for $q = p^n$ with p prime and $n > 3$ odd. A modular interpretation of the towers is given as well.

- In [1.JP9] a closed form expression for the Drinfeld modular polynomial $\Phi_T(X, Y) \in \mathbb{F}_q(T)[X, Y]$, for arbitrary q is given and a conjecture of Schweizer is proven. A new identity involving the Catalan numbers play a central role in the proofs.

- In [1.JP14] and [2.JP3] the authors give upper and lower bounds on the number of points on abelian varietes over finite fields, and lower bounds specific to Jacobian varieties. They also give exact formulas for the maximum and minimum number of points on Jacobian surfaces.

1.3 Algebraic Geometry Codes

- Affine Grassmann Codes are a variant of generalized Reed-Muller codes and are closely related to Grassmann codes. The codes were introduced in 2011. In [1.JP7], more generally, affine Grassmann codes of a given level is treated. The Dual of an affine grassmann code of every level is explicitly

determined and the minimum distance is computed. An earlier result on the automorphism group of the codes is ameliorated. It is also proven that both affine Grassmann codes and their duals are generated by their minimum wight codewords. This provides a clean analogue of a corresponding result for genralized Reed-Muller codes.

- The paper [1.JP2] considers weighted Reed-Muller codes over point ensemble $S_1 \times ... \times S_m$ where S_i needs not be of the same size as S_j. For $m = 2$ we determine optimal weights and analyze in detail what is the impact of the ratio $|S_1|/|S_2|$ on the minimum distance. In conclusion the weighted Reed-Muller code construction is much better than its reputation. For a class of affine variety codes that contains the weighted Reed-Muller codes we then present two list decoding algorithms. With a small modification one of these algorithms is able to correct up to 31 errors of the [49, 11, 28] Joyner code.

1.4 Graph Codes and Expander Graphs

- In [1.JP6] the authors prove lower bounds on the largest and the second largest eigenvalue of the adjacency matrix of connected bipartite graphs and give necessary and sufficient conditions for equality. Several examples of classes of graphs taht are optimal with respect to the bounds are give. It is proved that BIBD-graphs are characterized by their eigenvalues. The paper also contains a new bound on the expansion coefficient of (c, d)-regular graphs and this is compared with a classical bound.

- The paper [3.6] contains lower bounds for the minimum distance of graph codes based on expander graphs. The bounds depend only on the second eigenvalue of the graph and the parameters of the component codes. The paper also contains an upper bound on the size of a degree regular graph with given second eigenvalue.

- In the paper [3.8] A class of graph based codes with Reed-Solomon component codes are treated as affine variety codes. This gives a general method for determining the exact dimension of graph codes. It also contains an algebraic description of these codes which allows for an explicite formula for the dimension of the codes in the most important cases.

1.5 Decoding of Algebraic Codes

- In [2.JP2] the Wu list decoding algorithm for Generalized Reed-Solomon Codes by using Gröbner bases over modules and the Euclidean algorithm as the initial algorithm instead of the Berlekamp-Massy algorithm is presented. It contains a novel method for constructing the interpolation polynomial fast. A new application of of the Wu list decoder to the decoding of irreducible binary Goppa codes up to the binary Johnson radius is given. Finally a connection between the governing equations of the Wu algorithm and the Guruswami-Sudan algorithm is given, this leads immediately to equality in the decoding range and a duality in the choice of parameters needed for decoding, both in the case of generalised Reed-Solomon codes and in the case of Goppa codes.

- The paper [2 CC1] contains an iterated refinement procedure for the Guruswami-Sudan list decoding algorithm for generalised Reed-Solomon codes based on Alekhnovich's module minmisation. The method is parametrisable and allows variants of the usual list decoding approach. In particular, finding the list of *closests* codewords within the intermediate radius can be performed with improved average-case complexity while retaining the worst-case complexity.

- In [1.CC2] the authors generalize the list decoding algorithm for Hermitian codes proposed by Lee and O'Sullivan [K. Lee and M. E. O'Sullivan, "List decoding of Hermitian codes using Gröbner bases," J. Symbolic Comput., vol. 44, no. 12, pp. 1662-1675, Dec. 2009, arXiv:cs/0610132] based on Gröbner bases to general one-point AG codes, under an assumption weaker than one used by Beelen and Brander [P. Beelen and K. Brander, "Efficient list decoding of a class of algebraic-geometry codes," Adv. Math. Commun., vol. 4, no. 4, pp. 485-518, 2010]. By using the same principle, we also generalize the unique decoding algorithm for one-point AG codes over the Miura-Kamiya Cab curves proposed by Lee, Bras-Amorós and O'Sullivan [K. Lee, M. Bras-Amorós, and M. E. O'Sullivan, "Unique decoding of

plane AG codes via interpolation," 2012, IEEE Trans. Inform. Theory,] to general one-point AG codes, without any assumption. Finally we extend the latter unique decoding algorithm to list decoding, modify it so that it can be used with the Feng-Rao improved code construction, prove equality between its error correcting capability and half the minimum distance lower bound by Andersen and Geil [H. E. Andersen and O. Geil, "Evaluation codes from order domain theory," Finite Fields Appl., vol. 14, no. 1, pp. 92-123, Jan. 2008] that has not been done in the original proposal, and remove the unnecessary computational steps so that it can run faster.

- A list decoding algorithm for matrix-product codes is provided in [1.JP3] when C1,...,Cs are nested linear codes and A is a non-singular by columns matrix. We estimate the probability of getting more than one codeword as output when the constituent codes are Reed-Solomon codes. We extend this list decoding algorithm for matrix-product codes with polynomial units, which are quasi-cyclic codes. Furthermore, it allows us to consider unique decoding for matrix-product codes with polynomial units.

- In the paper [2.JP1] the authors propose a decoding algorithm for the $(u \mid u+v)$-construction that decodes up to half of the minimum distance of the linear code. We extend this algorithm for a class of matrix-product codes in two different ways. In some cases, one can decode beyond the error correction capability of the code.

- The paper [3.1] contains a generalization of the the unique decoding algorithm for one-point AG codes over the Miura-Kamiya C_{ab} curves proposed by Lee, Bras-Amorós and O'Sullivan to general one-point AG codes, without any assumption. We also extend their unique decoding algorithm to list decoding, modify it so that it can be used with the Feng-Rao improved code construction, prove equality between its error correcting capability and half the minimum distance lower bound by Andersen and Geil that has not been done in the original proposal except for one-point Hermitian codes, remove the unnecessary computational steps so that it can run faster, and analyze its computational complexity in terms of multiplications and divisions in the finite field. As a unique decoding algorithm, the proposed one is as fast as the BMS algorithm for one-point Hermitian codes, and as a list decoding algorithm it is much faster than the algorithm by Beelen and Brander.

- In [3.2] a generalization of the list decoding algorithm for Hermitian codes proposed by Lee and O'Sullivan is proposed, based on Gröbner bases to general one-point AG codes, under an assumption weaker than one used by Beelen and Brander. Our generalization enables us to apply the fast algorithm to compute a Gröbner basis of a module proposed by Lee and O'Sullivan, which was not possible in another generalization by Lax.

- Assuming that we have a soft-decision list decoding algorithm of a linear code, a new hard-decision list decoding algorithm of its repeated code is proposed in [3.4]. Although repeated codes are not used for encoding data, due to their parameters, we show that they have a good performance with this algorithm. We compare, by computer simulations, our algorithm for the repeated code of a Reed-Solomon code against a decoding algorithm of a Reed-Solomon code. Finally, we estimate the decoding capability of the algorithm for Reed-Solomon codes.

- In [3.3] it is shown that the Feng-Rao bound for dual codes and a similar bound by Andersen and Geil [H.E. Andersen and O. Geil, Evaluation codes from order domain theory, Finite Fields Appl., 14 (2008), pp. 92-123] for primary codes are consequences of each other. This implies that the Feng-Rao decoding algorithm can be applied to decode primary codes up to half their designed minimum distance. The technique applies to any linear code for which information on well-behaving pairs is available. Consequently we are able to decode efficiently a large class of codes for which no non-trivial decoding algorithm was previously known. Among those are important families of multivariate polynomial codes. Matsumoto and Miura in [R. Matsumoto and S. Miura, On the Feng-Rao bound for the L-construction of algebraic geometry codes, IEICE Trans. Fundamentals, E83-A (2000), pp. 926-930] (See also [P. Beelen and T. Høholdt, The decoding of algebraic geometry codes, in Advances in algebraic geometry codes, pp. 49-98]) derived from the Feng-Rao bound a bound for primary one-point algebraic geometric codes and showed how to decode up to what is guaranteed by their bound. The

exposition by Matsumoto and Miura requires the use of differentials which was not needed in [Andersen and Geil 2008]. Nevertheless we demonstrate a very strong connection between Matsumoto and Miura's bound and Andersen and Geil's bound when applied to primary one-point algebraic geometric codes.

1.6 Lattices

- In [3.9] the author proposes a generalization of Craig lattices. Based on this generalization of Craig lattices new lattices in Euclid spaces of many dimensions in the range 3332 - 4096 which are denser than the known densest Mordell-Weil lattices of these dimensions are constructed. Moreover it is proved that if there were some nice linear binary codes we could construct lattices denser than the Mordell-Weil lattices of dimensions in the range 128 - 3272. Some lattices of dimensions in the range 4098 - 8232 better than present records are also presented. We give some new lattices of moderate dimensions such as 68; 84; 85; 86 denser than the previously known densest sphere packings of these dimensions.

1.7 Cryptography

- The paper [1.JP5] gives a new construction of highly nonlinear vectorial Boolean functions. The construction is based on coding theory, more precisely concatenation is used to construct Boolean functions from codes over $\mathbb{F}_q$ containing a first order generalized Reed-Muller code. As it turns out this construction has a very compact description in terms of Boolean functions, which is of independent interest. The construction allows one to design functions with better nonlinearities than known before.

- Despite the fact that we evidently have very good block ciphers at hand today, some fundamental questions on their security is still unsolved. One such fundamental problem is to precisely assess the security of a given block cipher with respect to linear cryptanalysis. In by far most of the cases we have to make (clearly wrong) assumptions, e. g. independent round keys. Besides being unsatisfactory from a scientific perspective, the lack of fundamental understanding might have an impact on the performance of the ciphers we use. As we do not understand the security sufficiently enough, we often tend to embed a security margin- from an efficiency perspective nothing else than wasted performance. The aim of [1.CC3] is to stimulate research on these foundations of block ciphers. This is done by presenting three examples of ciphers that behave differently to what is normally assumed. Thus, on the one hand these examples serve as counter examples to common beliefs and on the other hand serve as guidelines for future work.

- The paper [1.CC4] presents a block cipher that is optimized with respect to latency when implemented in hardware. Such ciphers are desirable for many future pervasive applications with real-time security needs. The cipher, named PRINCE, allows encryption of data within one clock cycle with a very competitive chip area compared to known solutions. The fully unrolled fashion in which such algorithms need to be implemented calls for innovative design choices. The number of rounds must be moderate and rounds must have short delays in hardware. At the same time, the traditional need that a cipher has to be iterative with similar round functions disappears, and observation that increases the design space for the algorithm. An important further requirement is that realizing decryption and encryption results in minimum additional costs. PRINCE is designed in such a way that the overhead for decryption on top of encryption is negligible. More precisely for our cipher it holds that decryption for one key corresponds to encryption with a related key. This property is of independent interest and a proof of its soundness against generic attacks is given.

- Zero-correlation cryptanalysis uses linear approximations holding with probability exactly 1/2. The paper[1.CC5] reveals fundamental links of zero-correlations distinguishers to integral distinguishers and multidimensional linear distinguishers. It is shown that integral implies zero-correlation linear approximations and that a zero-correlation linear distinguisher is actually a special case of multidimensional linear distinguishers. These observations provide new insight into zero-correlation cryptanalysis which is illustrated by attacking a Skipjack variant and round-reduced CAST-256 without weak key assumptions.

- The paper [1.CC6] considers-for the first time- the concept of key-alternating ciphers in a provable security setting. Key-alternating ciphers can be seen as a generalization of a construction proposed by Even and Mansour in 1991. This construction builds a block cipher PX from an n-bit permutation P and two n-bit keys k_0 and k_1, setting $PX_{k_0,k_1}(x) = k_1 \oplus P(x \oplus k_0)$. A (natural) extension of the Even-Mansour construction with t permutations $P_1, \ldots P_t$ and keys $k_0, \ldots, k_t$ is considered. It is demonstrated in a formal model that such a cipher is secure in the sense that an attacker needs to make at least $2^{\frac{2n}{3}}$ queries to the underlying permutations to be able to distinguish the construction from random. It is further argued that the bound is tight for some cases but that there is a gap in the bounds for other cases which leaves an open interesting problem. Additionally, in terms of statistical attacks, it is shown that the distribution of Fourier coefficients for the cipher over all keys is close to ideal. Lastly a practical instance of the construction using AES called AES^2 is defined and it is shown that any attack on AES^2 with complexity below 2^{85} will have to make use of AES with a fixed known key in a non-black box manner. However it is conjectured that the security is 2^{128}.

- In[1.CC1] the authors propose a new method for constructing small-bias spaces through a combination of Hermitian codes. For a class of parameters our multisets are much faster to construct than what can be achieved by use of the traditional algebraic geometric code construction. So, if speed is important, our construction is competitive with all other known constructions in that region. And if speed is not a matter of interest the small-bias spaces of the present paper still perform better than the ones related to norm-trace codes reported in [Matthews, G.L., Peachey, J.: Small-bias sets from extended norm-trace codes. To appear in Proceedings of F_q12, Contemporary Mathematics, AMS]

- Code-based cryptography is an interesting alternative to classic number-theory PKC since it is conjectured to be secure against quantum computer attacks. Many families of codes have been proposed for these cryptosystems such as algebraic geometry codes. In previous papers [Márquez-Corbella et al. On the unique representation of very strong algebraic geometry codes. Designs, Codes and Cryptography, 2012], [Márquez-Corbella et al. Evaluation of public-key cryptosystems based on algebraic geometry codes in Proceedings of the Third International Castle Meeting on Coding Theory and Applications, 2011] for so called very strong algebraic geometry codes $\mathcal{C} = C_L(\mathcal{X}, \mathcal{P}, E)$, where $\mathcal{X}$ is an algebraic curve over $\mathbb{F}_q$ and $\mathcal{P}$ is an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$ and E is a divisor of $\mathcal{X}$ with disjoint support from $\mathcal{P}$ — it was shown that an equivalent representation $\mathcal{C} = C_L(\mathcal{Y}, \mathcal{Q}, F)$ can be found. The n-tuple of points are obtained directly from a generator matrix of $\mathcal{C}$, where the columns are viewed as homogeneous coordinates of these points. The curve $\mathcal{Y}$ is given by $I_2(\mathcal{Y})$, the homogeneous elements of degree 2 of the vanishing ideal $I(\mathcal{Y})$. Furthermore it was shown that $I_2(\mathcal{Y})$ can be computed efficiently as the kernel of certain linear map. What was not shown was how to get the divisor F and a decoding algorithm in an efficient way. In [3.5] the authors give an efficient computational approach to these problems.

- . Proxy signatures allow a proxy signer to sign messages on behalf of an original signer within a given context. They are widely used in distributed systems, grid computing, mobile agent applications, distributed shared object systems, global distribution networks, and mobile communications. Multi-proxy signature is a variation of the proxy signature primitive. In such a scheme, an original signer delegates his signing power to a group of proxy signers, and then only the cooperation of all the proxy signers can generate valid proxy signatures, referred to as multiproxy signatures, on behalf of the original signer. Recently, a multi-proxy signature scheme is presented in certificateless public key cryptosystem. We show in [1.JP10] that this scheme is insecure.

- Advances in mobile networking and information processing technologies have triggered vehicular ad hoc networks (VANETs) for traffic safety and value-added applications. Most efforts have been made to address the security concerns while little work has been done to investigate security and privacy for value-added applications in VANETs. To fill this gap, we propose in [1.CC8] a value-added application, specifically, a security and privacy preserving location-based service (LBS) scheme for VANETs. For each LBS transaction, the scheme provides authentication, integrity and non-repudiation for both the service provider and the user. A user can obtain the service in an anonymous way and hence user

privacy is well protected. However, a tracing procedure can be invoked to find malicious users, thereby efficiently preventing users from abusing the anonymity provided by the system.

- A proxy signature scheme allows a proxy signer to sign messages on behalf of an original signer within a given context. It has lots of practical applications in distributed systems, grid computing, mobile agent applications, distributed shared object systems, global distribution networks, and mobile communications. In the last years, fruitful achievements have been seen in certificateless public key cryptography which has the advantages of no certificate management and no key escrow compared with traditional public key cryptography and identity-based public key cryptography respectively. However, the existing certificateless proxy signature schemes is either insecure or without formal security analysis. In [1.CC7], we formalize the security model of certificateless proxy signature schemes and propose a provably secure certificateless proxy signature scheme with formal security proof under the computational Diffie-Hellman assumption.

- Recently, Zhang et al. proposed two encryption schemes using an elliptic curve combined public key. We show in[1.JP11], via the trick of using a linear equation system, that both proposals are vulnerable to key recovery attack, and thus in the present form must be considered as insecure. We simulate our trick on a common personal laptop and always get the results at a sub-second level.

- Identity-based signcryption (IBSC) is a cryptographic primitive which combines both the functions of identity-based signature and identity-based encryption in a single logical step, but with the cost of computation and communication significantly less than those needed by the signature-then-encryption approach. The first proposal Yu et al. (2009) for IBSC schemes without random oracles and its improvement Zhang (2010) were found insecure. Recently Li and Takagi (2011) presented an improved IBSC, but at the price of large signcryptext expansion and more exponentiation computation. In [1.JP12] we reconsider the first (but insecure) IBSC proposal, and find that a small modification will result in a secure IBSC. Unlike that of Li and Takagi, our scheme does not sacrifice the bandwidth and computation efficiency to achieve the security goals. We use the proof techniques of Li and Takagi to prove in the standard model its indistinguishability against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen message attack. Through comparison of computational cost and communication overhead, our scheme is amongst the most efficient IBSC schemes without random oracles.

- Multisignature scheme allows a group of signers to generate a compact signature on a common document that certifies they endorsed the message. However, the existing state of the art multisignatures often suffers from the following problems: impractical key setup assumptions, loose security reductions and inefficient signature verification. In this paper, we propose a noninteractive multisignature scheme with tight security reduction in the random oracle model. In [1.JP13]we propose a multisignatures address the above three problems by achieving: provable security in the plain public key model; tight security reduction under the standard Computational Diffie- Hellman (CDH) assumption and O(1) computational time for signature verification through precomputation. Hence, our non-interactive multisignatures are of great use in routing authentication of networks.

1.8 Other publications

- In [1.JP8] a new class of relative equilibria of identical point vortices in which the vortices are constrained to be on two perpendicular lines, conveniently taken to be the x- and y-axes of a Cartesian coordinate system, is introduced and studied. In the general problem there are m vortices on the y-axis and n on the x-axis. Generating polynomials $q(z)$ and $p(z)$ are defined, respectively, for each set of vortices. A second-order, linear ODE for $p(z)$ and $q(z)$ is derived. Several results relating the general solution of the ODE to relative equilibrium configurations are established. The strongest result, obtained using Sturm's comparison theorem, is that if $p(z)$ satisfies the ODE for a given $q(z)$ with its imaginary zeroes symmetric relative to the x-axis, then it must have at least $n - m + 2$ simple real zeros. For $m = 2$this provides a characterization of all zeros, and this case is studied in some detail. In particular, it is shown that, given $q(z) = z^2 + \eta^2$, where η is real, there is a unique $p(z)$ of degree n, and a unique value of

$\eta^2 = A_n$, such that the zeros of $q(z)$ and $p(z)$ form a relative equilibrium of $n+2$ point vortices. It is also shown that$A_n \approx \frac{2}{3}n + \frac{1}{2}$, as n tends to infinity, where the coefficient of n is determined analytically,and the next order term numerically. The paper includes extensive numerical documentation on this family or relative equilibria.

- On the 9th of September 2012 Hassan Aref suddenly passed away in his home, just a few weeks before his 61st anniversary.
  With Hassan Aref's death the fluid dynamic community has lost a great and original scientist. Also a good friend an inspiring teacher and aprominent leader and organizer is lost. The paper [2.CC2] is focussed on Hassan Aref's favourite topics, relative equilibria of point vortices. Some of his research in the field is summarized, in particular his latest work on bilinear equilibria which was submitted for publication shortly before his death.