AGC^{2}T-16 Conference

Arithmetic, Geometry, Cryptography and Coding Theory

June 19th–23th 2017

C.I.R.M. — France

Yves Aubry, Everett Howe and Christophe Ritzenthaler

Program and abstracts

	Monday	Tuesday	Wednesday	Thursday	Friday
9.00 - 10.00	Bouw	Hindry	Voight	Cojocaru	Castryck
10.00 - 10.30	Lorenzo	Lebacque	Marseglia	Achter	Katz
10.30- 11.00					
11.00 - 11h30	Kılıçer	Pogildiakov	Kedlaya	Devin	Lachaud
11.30 - 12h00	Karemaker	Tsfasman	Yu	Kaplan	Sutherland
12.30- 14.00	Lunch	Lunch	Lunch	Lunch	Lunch
16.00 - 17.00	Poonen	Voloch	Free	Silverberg	
17.00- 17.30	Trepalin	Ghorpade		Egorova	
17.30- 18.00					
18.00- 18.30	Bruin	Singh		Barelli	
18.30- 19.00	Duursma	Rambaud		Tibouchi	
19.00- 19.30	Pries	Datta		Vuille	
19.30-	Dinner	Dinner	Dinner	Conference dinner	Dinner

Abstracts.

1 Monday morning session

Irène Bouw (Plenary) Picard curves with small conductor.
We study the conductor of Picard curves defined over $\mathbb{Q}$. We describe the restrictions on the local contribution to the conductor, by carefully analyzing the possibilities for the stable reduction of the curve. We show that Picard curves over $\mathbb{Q}$ always have bad reduction at $p = 3$. As an application we discuss the question of finding Picard curves with small conductor.

Elisa Lorenzo García Primes of bad reduction of curves of genus 3 with CM.
In Bouw et al. 15, we show that for each prime of bad reduction for a curve of genus 3 with CM, there is a solution to the so-called embedding problem. In that way we give a bound for the primes of bad reduction under some conditions: on the field K of CM and on the type of bad reduction of the curve. In this new work, we give an unconditional bound. In particular, we show that if $K = Q(u)$ with u^2 totally negative and $B = -\mathrm{Tr}(u^2)/2$, then any prime of bad reduction is smaller than $B^{10}/8$. For example, this bound can be translated into a bound for the primes appearing in the denominators of class polynomials of hyperelliptic curves of genus 3 or of Picard curves. Joint work with P. Kilicer, K. Lauter, R. Newton, E. Ozman, M. Streng.

Pınar Kılıçer On primes dividing the invariants of Picard curves.
The j-invariants of elliptic curves with complex multiplication (CM) are algebraic integers. For invariants of genus $g = 2$ or 3, this is not the case, though suitably chosen invariants do have smooth denominators in many cases. Bounds on the primes in these denominators have been given for g=2 (Goren-Lauter) and some cases of $g = 3$. For Picard curves of genus 3, we give a new approach based not on bad reduction of curves but on a very explicit type of good reduction. This approach simultaneously yields much sharper bounds and a simplification of the proof. This is a joint work with Marco Streng and Elisa Lorenzo García.

Valentijn Karemaker Fully maximal and minimal supersingular abelian varieties.
We consider a supersingular abelian variety A defined over a finite field K; we say that A is maximal (resp. minimal) over K if all its normalised Weil numbers over K are -1 (resp. 1). The (normalised) Weil numbers of A determine A up to isogeny. We ask whether A and its K-twists (which may have different Weil numbers) become maximal over a finite extension of K, and classify this behaviour by defining three possible types for A: fully maximal, fully minimal, and mixed. We analyse these types for supersingular abelian varieties and curves, under restrictions on their automorphism group.

In particular, we give a complete characterisation of the type of all supersingular abelian varieties of dimension $g = 1, 2$ in arbitrary characteristic. This uses the classifications of isogeny classes due to Tate and Waterhouse ($g = 1$), and Maisner-Nart and Howe-Nart-Ritzenthaler ($g = 2$). Moreover, we obtain a similar characterisation for supersingular genus 3 curves in characteristic 2, using a parametrisation of the moduli space by Viana-Rodriguez, and performing a careful analysis on the automorphism groups.

This is joint work with Rachel Pries.

2 Monday afternoon session

Bjorn Poonen (Plenary) Abelian varieties isogenous to a power of an elliptic curve.
Let E be an elliptic curve over a field. Let $R = \mathrm{End}(E)$. Then $\mathrm{Hom}(-, E)$ is a functor from the category of abelian varieties isogenous to a power of E to the category of finitely presented torsion-free left R-modules. We find necessary and sufficient conditions on E for this functor to be an equivalence of categories. This is joint work with B. Jordan, A. Keeton, E. Rains, N. Shepherd-Barron, and J. Tate.

Andrey Trepalin Del Pezzo surfaces over finite fields.
Let X be a del Pezzo surface of degree d over a finite field $\mathbb{F}_q$, where $2 \leqslant d \leqslant 6$. Then the Galois group $\mathrm{Gal}\left(\overline{\mathbb{F}}_q/\mathbb{F}_q\right)$ acts on the Picard group $\mathrm{Pic}\left(X \otimes \overline{\mathbb{F}}_q\right)$, and its image Γ is a cyclic group in the corresponding Weyl group, that is the group of automorphisms of the Picard group $\mathrm{Pic}\left(X \otimes \overline{\mathbb{F}}_q\right)$ preserving the intersection form. Classification of such cyclic subgroups up to conjugation is well-known. We discuss methods how to construct a del Pezzo surface X, such that the group Γ has a given conjugacy class in the Weyl group.

Nils Bruin Arithmetic of the moduli space of abelian surfaces with full level 3 structure.
The moduli space of abelian surfaces with full level 3 structure has been well-studied. It is birational to the Burkhardt quartic 3-fold. It is classically known that this variety is rational over C. We show that in fact it is already rational over Q. An explicit description of this birational map also allows us to compute the zeta function of the Burkhardt quartic for primes that are 2 modulo 3 (previously, this was only done for primes that are 1 modulo 3).

Since this space is a fine moduli space, there exists a universal genus 2 curve over an open part of it. We construct such a curve arithmetically. Furthermore, we identify explicitly how the level 3 structure is morked on this curve.

This is joint work with Brett Nasserden.

Iwan Duursma Rank two root systems and maximal curves.
The three families of curves of Deligne-Lusztig type (Hermitian, Suzuki and Ree) have automorphism groups of type 2A2, 2B2, 2G2 with natural representations of degree 3, 4 and 7. The Giullietti-Korchmaros curves cover the Hermitian curve. In recent work, Skabelund gives new maximal curves that cover the Suzuki and Ree curves. We describe each of the three covers in a unified way in terms of the root systems A2, B2 and G2.

Rachel Pries Galois action on homology of Fermat curves.
Anderson determined information about rational points on the generalized Jacobian of the Fermat curve. His method involves the action of the absolute Galois group of a cyclotomic field on a relative homology group of the Fermat curve. We find an explicit formula for this action, which allows us to explicitly determine the maps between several Galois cohomology groups which arise in connection with obstructions for rational points on the Fermat curve over cyclotomic fields. The proof is a blend of number theory, algebraic topology, commutative algebra, and computer algebra. This is joint work with R. Davis, V. Stojanoska, and K. Wickelgren.

3 Tuesday morning session: in memory of Alexey Zykin

Marc Hindry (Plenary) Brauer-Siegel theorem and analogues for varieties over global fields.
The classical Brauer-Siegel theorem can be seen as one of the first instances of description of asymptotical arithmetic: it states that, for a family of number fields K_i, under mild conditions (e.g. bounded degree), the product of the regulator by the class number behaves asymptotically like the square root of the discriminant. This can be reformulated as saying that the Brauer-Siegel ratio $\log(hR)/\log\sqrt{D}$ has limit 1.

Even if some of the fundamental problems like the existence or non-existence of Siegel zeroes remains unsolved, several generalisations and analog have been developed: Tsfasman-Vladuts, Kunyavskii-Tsfasman, Lebacque-Zykin, Hindry-Pacheco and lately Griffon. These analogues deal with number fields for which the limit is different from 1 or with elliptic curves and abelian varieties either for a fixed variety and varying field or over a fixed field with a family of varieties.

I will survey these topics and present the latest results and open questions.

Philippe Lebacque On M-functions associated with modular forms.
The study of the distribution of values of L-functions is a classical topic in number theory. In the last decade, motivated by the questions arising in the asymptotic theory of global fields, Y. Ihara proposed a novel view on the problem by studying the distrubution of logarithms and logarithmic derivatives of Dirichlet character

L-functions $L(s,\chi)$ over number fields and function fields. Our talk is devoted to the extension of Ihara's approach to the case of L-functions of modular forms. We treat both the case of twists of a fixed modular for f by a varying Dirichlet character χ, where fairly complete equidistribution results are obtained under GRH, and the case of averages over the space all primitive forms of given weight k and level N going to infinity.

This is a joint work with our late friend Alexey Zykin.

Ivan Pogildiakov On the linear bounds on the genus of pointless curves.
The study of the existence of pointless curves originates from the problem of the attainability of the lower Hasse–Weil–Serre bound. Given a prime power q and a number g such that this bound is non-positive, we ask whether a non-singular genus g curve over the finite field $\mathbb{F}_q$ having no rational points exists. In the case when q is fixed, the bound implies that the genus of a smooth pointless curve must be greater than $(q+1)/\lfloor 2\sqrt{q}\rfloor$.

Let g_q be the minimal integer such that for any $g \geq g_q$ there is a non-singular pointless curve of genus g over $\mathbb{F}_q$. By considering families of hyperelliptic curves, we establish two new linear upper bounds on g_q (for odd and even q respectively), improving the previous results due to R. Becker and D. Glass. If time permits, we will discuss another approach to this question related to coding theory.

Michael Tsfasman Measures associated to curves and abelian varieties over finite fields.
We study measures corresponding to families of abelian varieties over a fixed finite field. These measures play an important role in the Tsfasman–Vlăduț theory of asymptotic zeta-functions defining completely the limit zeta-function of the family. Many years ago J.-P. Serre used a beautiful number-theoretic argument to prove the theorem limiting the set of measures that can actually occur on families of abelian varieties. This theorem was never published. First we present this theorem and its proof. Then we show that for jacobians of curves other methods characterize this set better, at least when the cardinality of the ground field is an even power of a prime. We are however very far from describing completely the set of measures corresponding to abelian varieties.

4 Tuesday afternoon session

Felipe Voloch (Plenary) Maps between curves and diophantine obstructions.
Given two algebraic curves X, Y over a finite field we might want to know if there is a rational map from Y to X. This has been looked at from a number of perspectives and we will look at it from the point of view of diophantine geometry by viewing the set of maps as $X(K)$ where K is the function field of Y. We will review some of the known obstructions to the existence of rational points on curves over global fields, apply them to this situation and present some results and conjectures that arise.

Sudhir Ghorpade Linear codes associated to Grassmann and flag varieties.
It has been about three decades since Grassmann codes were introduced. We know a lot about these codes now and many interesting properties have been obtained in the last few years. The study of linear codes associated to partial flag varieties over finite fields is relatively more recent and was initiated by F. Rodier in 2003 who considered the special case of line-hyperplane incidence. Barring a subsequent work by G. Hana (2005), not much is known about these codes. In this talk, I will review some of the known results and outline some new developments, including a recent joint work with Prasant Singh on linear codes associated to some flag varieties.

Prasant Singh Minimum Weight Codewords of Schubert Codes.
Let $\mathbb{F}_q$ be the finite field with q elements. Let ℓ, m be positive integers satisfying $\ell \leq m$ and V be a vector space of dimension m over $\mathbb{F}_q$. Let $G_{\ell,m}$ denote the Grassmannian of all ℓ-planes of V. Let $\mathfrak{a} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell)$ be a sequence of positive integers satisfying $\mathfrak{a}_1 < \cdots < \mathfrak{a}_\ell \leq m$ and let $\mathcal{O}$ be the Schubert variety in $G_{\ell,m}$ corresponding to $\mathfrak{a}$. Let $\mathbb{C}$ be the Grassmann code corresponding to the Grassmann variety $G_{\ell,m}$ and

$C_{\mathfrak{a}}(\ell, m)$ be the Schubert code corresponding to the Schubert variety $\mathcal{O}$. Schubert codes were introduced by Ghorpade and Lachaud around 2000 and it was conjectured that the minimum distance of $C_{\mathfrak{a}}(\ell, m)$ is $q^{\delta(\mathfrak{a})}$ where $\delta(\mathfrak{a}) = \sum_{i=1}^{\ell}(\mathfrak{a}_i - i)$. This conjecture is known as the *Minimum Distance Conjecture* or the MDC. The MDC is proved in affirmative in 2008 by Xiang. We will outline an alternative and transparent solution of the MDC. We will further take up the problem of classification of minimum weight codewords in Schubert codes. For the Grassmann code $\mathbb{C}$, a classification of minimum weight codewords is well-known, namely, the minimum weight codewords of $\mathbb{C}$ correspond precisely to the decomposable elements of $\bigwedge^{m-\ell} V$. But for Schubert codes, such a classification is not known. We introduce a more subtle variant of decomposability, called Schubert decomposability, and use it to propose a new conjecture concerning the classification of minimum weight codewords in the Schubert code $C_{\mathfrak{a}}(\ell, m)$. We will prove several aspects of this new conjecture and settle it in the special case when $\mathfrak{a}$ is completely non-consecutive, i.e., when $\mathfrak{a}_i - \mathfrak{a}_{i-1} \geq 2$ for $1 < i \leq \ell$.

This is a joint work with Sudhir R. Ghorpade.

Matthieu Rambaud Dense families of curves over prime fields with many points after field extension.
A folklore conjecture ([CCXY] "Lemma IV.4" for applications and [BPRS] 3 for counterexamples) states that, for all p prime number and $2t$ an even integer, there exists a family of function fields over the prime field $\mathbb{F}_p$ such that

- the genera tend to infinity ;
- the ratio of two successive genera tends to 1 (density condition) and
- after field extension to $\mathbb{F}_{p^{2t}}$, the asymptotic number of points reaches the Ihara bound.

The only cases known so far are for $t = 1$, with the classical modular curves $X_0(N)/\mathbb{F}_p$. We present here an explicit family of Shimura curves solving the case $p = 3$ and $2t = 6$. The talk will possibly illustrate facts and methods on (non Galois) covering maps (determination of an arithmetic cover from its geometric monodromy [Sza],[KMSV], descent of a Belyi map of genus 1 when allowed to move the branch points [SV2]).
References:
[$CCXY$] I. Cascudo, R. Cramer, C. Xing, and A. Yang. Asymptotic bound for multiplication complexity... IEEE Trans. Inf. Theory, 2012.
[$BPRS$] S. Ballet, J. Pieltant, M. Rambaud, J. Sijsling, On some bounds for symmetric tensor rank of multiplication in finite fields. AGCT15 (to appear)
[$SV2$] J. Sijsling, J. Voight, On explicit descent of marked curves and maps. Research in Number theory, 2016.
[Sza] T. Szamuely, Galois groups and fundamental groups. Cambridge studies in adv. math., 2009.
[$KMSV$] M. Klug, M. Musty, S. Schiavone, J. Voight, Numerical calculation of three-point branched covers of the projective line. J. Comput. Math. 2014.

Mrinmoy Datta An upper bound for the number of zeros of a system of homogeneous polynomials
For a prime power q, let $\mathbb{F}_q$ be a finite field with q elements. Fix positive integers r, d, m with $d < q$. For homogeneous polynomials $F_1, \ldots, F_r \in \mathbb{F}_q[x_0, ..., x_m]$, denote by $V(F_1, \ldots, F_r)$, the set of common zeroes of $F_1, \ldots, F_r \in \mathbb{P}^m(\mathbb{F}_q)$. In this talk, we present a new combinatorial upper bound for $|V(F_1, \ldots, F_r)|$ where $F_1, \ldots, F_r$ are linearly independent and of degree d. This bound generalizes the results of Wei and Heijnen-Pellikaan to a projective setting. Note that these upper bounds give rise to lower bounds for the generalized Hamming weights of projective Reed-Muller codes. We show that this bound is tight for some values of r. This is a joint work with Peter Beelen and Sudhir R. Ghorpade.

5 Wednesday morning session

John Voight (Plenary) Computing classical modular forms as orthogonal modular forms.
Birch gave an extremely efficient algorithm to compute a certain subspace of classical modular forms using the Hecke action on classes of ternary quadratic forms. We extend this method to compute all forms of non-square level using the spinor norm, and we exhibit an implementation that is very fast in practice. This is joint work with Jeffery Hein and Gonzalo Tornaria.

Stefano Marseglia Computing isomorphism classes of abelian varieties over finite fields.
Deligne proved that the category of ordinary abelian varieties over a finite field is equivalent to the category of free finitely generated abelian groups endowed with an endomorphism satisfying certain easy-to-state axioms. Centeleghe and Stix extended this equivalence to all isogeny classes of abelian varieties over $\mathbb{F}_p$ for which $\sqrt{p}$ is not among the corresponding Weil numbers. Using these descriptions, we obtain that in order to compute the isomorphism classes of abelian varieties we need to calculate the isomorphism classes of (non necessarily invertible) fractional ideals of some orders in certain étale algebras over $\mathbb{Q}$. We present a concrete algorithm to do this and, in the ordinary case, also to compute the polarizations and the automorphisms of the polarized abelian variety.

Kiran Kedlaya Computing zeta functions of nondegenerate toric hypersurfaces.
We report on an ongoing joint project with Edgar Costa and David Harvey to implement the computation of zeta functions of nondegenerate toric hypersurfaces over finite fields using rigid p-adic cohomology (in the style of my work with Abbott and Roe from AGCT 2005).

Chia-Fu Yu Explicit formulas for superspecial abelian surfaces over finite fields.
In this talk i plan to describe explicit formulas for the number of superspecial abelian surfaces over finite fields, and of the isomorphism classes of their endomorphism rings. i will also explain key ingredients in the computation. This is joint work with Jiangwei Xue and Tse-Chung Yang.

6 Thursday morning session

Alina Cojocaru (Plenary) Arithmetic properties of the Frobenius traces defined by a rational abelian variety.
Let $A/\mathbb{Q}$ be an abelian variety of dimension g, such that the image of its associated Galois representation ρ_A is open in $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$. We investigate the arithmetic of the traces of the Frobenius at p under ρ_A. In particular, we bound from above the number of primes $p < x$ for which the Frobenius trace at p is fixed; we prove an Erdös-Kac type result for the number of prime factors of the Frobenius trace; and we propose a conjecture that generalizes a well-known conjecture of Lang and Trotter about elliptic curves. This is joint work with R. Davis (University of Wisconsin, Madison), A. Silverberg (University of California, Irvine), and K.E. Stange (University of Colorado, Boulder), with contributions by J-P. Serre (Collège de France).

Jeff Achter Local densities compute isogeny classes.
Consider an ordinary isogeny class of elliptic curves over a finite, prime field. Inspired by a random matrix heuristic (which is so strong it's false), Gekeler defines a local factor for each rational prime. Using the analytic class number formula, he shows that the associated infinite product computes the size of the isogeny class.

I'll explain a transparent proof of this formula; it turns out that this product actually computes an adelic orbital integral which visibly counts the desired cardinality. Moreover, the new perspective allows a natural generalization to higher-dimensional abelian varieties. This is joint work with Julia Gordon and S. Ali Altug.

Lucile Devin Divisibility properties of the number of $\mathbb{F}_p$-points of schemes defined over $\mathbb{Z}$.
Let X be a scheme of finite type over $\mathbb{Z}$. For any prime p we consider $N(X, p)$ the number of $\mathbb{F}_p$-points

of the scheme $X/\mathbb{F}_p$. Given a in $\mathbb{Z}$, we study the set $\{p : p \text{ does not divide } N(X,p) - a\}$. In case $\dim X$ is small (lower than 3), we give a simple criterion for this set to be infinite and in this case we prove it has positive lower density.

Nathan Kaplan Rational Point Count Distributions for del Pezzo Surfaces over Finite Fields.
A del Pezzo surface of degree d over a finite field of size q has at most $q^2 + (10-d)q + 1$ $\mathbb{F}_q$-rational points. A surface attaining this maximum is called 'split', and if all of these rational points lie on the exceptional curves of the surface, then it is called 'full'. Can we count and classify these extremal surfaces? We focus on del Pezzo surfaces of degree 3, cubic surfaces, and of degree 2, double covers of the projective plane branched over a quartic curve. We will see connections to the geometry of bitangents of plane quartics, counting formulas for points in general position, and error-correcting codes.

7 Thursday afternoon session

Alice Silverberg (Plenary) Orders, lattices, and an application to principal ideal testing.
We give a deterministic polynomial-time algorithm for a problem that may be viewed as a special case of a principal ideal testing problem in CM-orders. (A CM-order is an order equipped with an involution that mimics complex conjugation; examples include orders in CM-fields.) In the process we study nilpotents, idempotents, and roots of unity in graded orders, and show that every reduced order has a universal grading by some finite abelian group. This is joint work with Hendrik Lenstra.

Elena Egorova Zero-error coding for multiple-access channels as a new test bed for AG-codes.
We consider the problem of constructing so-called signature codes for the main known models of multiple-access channels. Recently these models had found new applications in different scenarios of digital fingerprinting codes. We discuss known constructions which are in fact mainly nonconstructive but random-coding and we formulate also possible applications of AG-codes for multiple-access channels, especially for the non-binary adder channel, for weighted noisy adder channel and for multifrequencies channel with intensity information.

Élise Barelli Short McEliece Keys from Algebraic-geometry codes with automorphisms.
In 1978, McEliece [2] introduced a public key encryption scheme based on linear codes and suggested to use classical Goppa codes, ie: subfield subcodes of algebraic geometric (AG) codes built on a curve of genus 0. This proposition remains secure and in order to have a generalization of classical Goppa codes, in 1996, H. Janwa and O. Moreno [1] suggested to use subfield subcode of AG codes, which we call AG alternant codes. This proposition give a bigger choice of code because we can vary the curve, the genus, and the rational points of the divisor which generate the code. The principal limitation is the very large public keys of these codes compared to other public-key cryptosystems. To overcome this limitation, we decrease the key size by choosing codes which admit very compact public matrix. A way to obtained short key is to use codes having a non-trivial automorphisme group, for instance here we deal with quasi- cyclic AG alternant codes.

To build quasi-cyclic AG alternant codes, we need to use curves with non-trivial automorphisms for which we can easily compute Riemann-Roch spaces. The first example that we studied was cyclic cover of the projective line. With a good choice of the set of rational points $\mathcal{P}$ and the divisor G, an automorphism σ of a cyclic extension of the projective line induces a permutation on the code $\mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)$. These codes could be good candidates for compact McEliece keys, unfortunately we can show that the security of these codes reduces to the security of smaller codes. Indeed, studying the code fixed by the automorphism σ, we prove that this invariant code $\mathrm{Inv}(\mathcal{C}_{\mathcal{L}})$ is an AG alternant code on the quotient curve $\mathcal{X}/ < \sigma >$. In the particular case of cyclic cover of the projective line, the quotient curve is exactly the projective line and so the invariant code is a classical Goppa code for which we can build an algebraic system to recover its support $\tilde{\mathcal{P}}$. Moreover we can show a relation between the support $\mathcal{P}$ defining $\mathcal{C}_{\mathcal{L}}(\mathcal{X}, \mathcal{P}, G)$ and the support $\tilde{\mathcal{P}}$ defining $\mathrm{Inv}(\mathcal{C}_{\mathcal{L}})$. Finally we are able to build an algebraic system to recover $\mathcal{P}$ from the knowledge of $\tilde{\mathcal{P}}$. To avoid this kind of attacks, we look at other curves with automorphisms, for instance cyclic covers of planes curves

of genus > 0.

References

[1] Heeralal Janwa and Oscar Moreno, *McEliece public key cryptosystems using algebraic- geometric codes*, Des. Codes Cryptogr. 8 (1996), no. 3, 293–307.

[2] Robert J. McEliece, *A public-key system based on algebraic coding theory*, pp. 114–116, Jet Propulsion Lab, 1978, DSN Progress Report 44.

Mehdi Tibouchi Generalized Howgrave-Graham–Szydlo and Side-Channel Attacks Against BLISS
As the advent of quantum computers draws closer, standardization bodies are initiating the transition towards quantum-resistant cryptography. Many such schemes have been described in the research literature, but implementing them securely is not necessarily an easy task. In this talk, we look in particular at the lattice-based signature scheme BLISS, which is one of the most efficient quantum-resistant candidates for signatures, and show that one of its major security components (the "rejection sampling") actually leaks a considerable amount of information about the secret signing key through side-channels.

More precisely, the signing key is an element of a cyclotomic field, and the recommended way of implementing rejection sampling leaks the relative norm of that element in the totally real subfield of that cyclotomic field. Using a generalization of an algorithm due to Howgrave-Graham and Szydlo (ANTS-VI), we can use that norm to recover the key up to multiplication by a root of unity, which is sufficient to completely break the scheme.

Marius Vuille Computing cyclic isogenies between abelian surfaces over finite fields.
Abelian varieties such as elliptic curves or Jacobian varieties of higher genus curves, are nowadays widely used for cryptographic schemes. The security of the scheme, however, depends on the chosen variety. This reveals the importance of computing isogenies between them. For abelian surfaces, isogenies with maximally isotropic kernels (for the Weil pairing) are known and due to Robert and Cosset. These are called (l, l)-isogenies and have kernel isomorphic to $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$. In this talk we will explain how to compute cyclic isogenies, i.e., with kernel isomorphic to $Z/l\mathbb{Z}$.

8 Friday morning session

Wouter Castryck (Plenary) A heuristic for the secondary term in the counting function for quartic extensions of $\mathbb{F}_q(t)$.
There is a folklore conjecture stating that for a fixed integer $d > 1$ the amount of number fields K such that $[K : \mathbb{Q}] = d$ and $|\mathrm{Disc}(K)| < X$ equals $cX + o(X)$ for some constant $c > 0$. This is known up to $d \leq 5$, and in the cubic case it was moreover shown that there is a secondary term of the form $c'X^{5/6}$ for some other constant $c' < 0$. This was formerly known as the Roberts conjecture, now proven by Bhargava–Shankar–Tsimerman and Taniguchi–Thorne. In the quartic case it is believed that there is a similar error term $c'X^{5/6}$ but this is open.

In his Ph.D. thesis Zhao demonstrated an analogue of the Roberts conjecture for cubic extensions of $\mathbb{F}_q(t)$. His proof gives a remarkable explanation for the exponent $5/6$, which shows up as a corollary to a well-known bound on the Maroni invariants e_1, e_2 of a trigonal curve. In this talk we will give a similar (but heuristic) derivation of the secondary term in the counting function for quartic extensions of $\mathbb{F}_q(t)$, where the lead role is now played by the Schreyer invariants b_1, b_2. As it turns out these satisfy a very similar bound, accounting for the appearance of the same exponent $5/6$. This is explained by Casnati's observation that $b_1 + 2, b_2 + 2$ are the Maroni invariants of Recillas' trigonal construction, which is the geometric equivalent of the cubic resolvent. This is joint work in progress with Yongqiang Zhao.

Daniel J. Katz A New Generating Function for Calculating the Igusa Local Zeta Function.
Consider a multivariable polynomial $f(x_1, ..., x_n)$ with integer coefficients. Let p be a prime and k a positive integer and suppose that we want to count the number $N_k(f)$ of zeroes in $(\mathbb{Z}/p^k\mathbb{Z})^n$ of f modulo p^k. The Igusa local zeta function Z_f is a generating function that organizes these zero counts for all k. The poles of this zeta function tell us about the p-divisibility of the counts. More generally, f can have coefficients in a ring R of integers of a p-adic field, and the Igusa local zeta function for f organizes the counts $N_k(f)$ of zeroes of f modulo π^k, where π is a uniformizing parameter for R. These point counts on the hypersurface defined by f are naturally of interest when working with codes over finite fields and rings. We devise a new method for calculating the Igusa local zeta function that involves a new kind of generating function G_f . Our new generating function is a projective limit of a family of generating functions, and contains more data than the local zeta function. Our G_f resides in an algebra whose structure is naturally compatible with operations on the underlying polynomials, thus facilitating calculation of local zeta functions and helping us find zero counts of polynomials over finite fields and rings. This new method enables us to calculate Igusa local zeta functions for a much wider range of quadratic polynomials over 2-adic fields than have been determined previously.

Gilles Lachaud On the distribution of the trace in the compact group of type G_2, and applications to exponential sums.
We provide explicit formulas for the distribution of the trace of the natural seven-dimensional representation of the compact semisimple Lie group of type G_2. We describe the fundamental simplex of G_2 (the space of conjugacy classes) and its image by the fundamental map. The results are given in terms of special functions by using Weyl's integration formula. This answers a question raised by J.-P. Serre and N. M. Katz.

We recall the relevance of this distribution to the equidistribution of the one parameter family of exponential sums

$$\sum_{x \mod p, x \neq 0} \left(\frac{x}{p}\right) \exp \frac{2i\pi}{p}(x^7 + tx)$$

with parameter $t \in \mathbb{F}_p$, where (x/p) is the quadratic character, and p is any prime other than 2 and 7. Actually, thanks to a theorem of Katz, the monodromy group of these sums is the compact group of type G_2.

Andrew Sutherland Strong arithmetic equivalence.
Number fields with the same Dedekind zeta function are said to be arithmetically equivalent. Such number fields necessarily have the same degree, discriminant, signature, Galois closure, and isomorphic unit groups, but may have different regulators, class groups, rings of adeles, and idele class groups. Motivated by a recent result of Prasad, I will discuss three stronger notions of arithmetic equivalence that force isomorphism of some or all of these invariants without forcing an isomorphism of number fields, along with explicit examples. These results also have application to the construction of curves with isomorphic Jacobians (due to Prasad), isospectral Riemannian manifolds (due to Sunada), and isospectral graphs (due to Halbeisen and Hungerbuhler).