| | |
|---|---|
| **Acronyme/*short title*** | **CHIC** |
| **Titre du projet en français** | Courbes Hyperelliptiques Isogénies et Comptage |
| **Titre du projet en anglais** | Hyperelliptic Curves Isogenies and Point Counting |
| **CSD Principale** | 1. Sciences et technologies de l'information et de la communication |
| **CSD Secondaire (si interdisciplinaire)** | 5. Mathématiques et interactions |

| | | | |
|---|---|---|---|
| **Aide totale demandée** | *** *** Euros | **Durée du projet** | 36 mois |

# Table of contents

# 1 Context and positioning of the proposal

With the advent of digital networks, public key (or asymmetric) cryptography has entered our daily life: it can be found for instance in credit cards, web browsers or even certain game consoles. Compared to more classical symmetric cryptography, public key cryptography brings a large number of features which are particularly interesting for practical applications. For instance, truly non repudiable signature schemes are only possible with public key cryptography. It also allows a more efficient key management over large networks. As a result, it covers a wide range of different services and has become an unavoidable technique for any activity where security of communication or information systems is critical.

In most instances, the operation of public key schemes relies on the computational hardness of some problems. From this, it is possible to deduce one-way functions, trapdoor functions and then design and prove by reduction protocols to achieve a variety of security objectives. The most common of these security objectives are encryption or digital signature. For the initial hard problem, there is not much choice: if we put aside problems which have not received enough attention by the scientific community to consider them safe, the only available problems come from coding theory (for instance MacEliece), lattice reduction theory (for example NTRU) or number theory. In fact, the size of the public key discourages the use of coding theory cryptosystems while lattice-based cryptosystems have a bad track record of being easily broken.

On the other side, hard problems coming from number theory have been extensively studied in the past years and most of the currently used asymmetric cryptosystems are based upon them. They can be separated into two categories depending on whether they are related to the factorisation problem (RSA) or the discrete logarithm problem (Diffie–Hellman). The discrete logarithm problem provides a general framework for the design of one-way functions from the knowledge of a family of groups enjoying certain good properties. Examples of groups which can be used for the discrete logarithm problem include the group of invertible elements of a finite field or the group of rational points of an elliptic curve defined over a finite field.

A family of groups typically provides several instances per group size. In order to be relevant for cryptography, candidate groups should first have a highly difficult discrete logarithm problem – this generally provides security, which increases together with the group size. On the other hand, the arithmetic in the group must be fast – this provides efficiency, and exceedingly large groups are a clear impediment towards this.

The elliptic curve discrete logarithm problem seems to offer the best security/efficiency trade-off. The quickest known algorithms to solve a general instance of the elliptic curve discrete logarithm problem do not use any information other than the knowledge of the group structure. These algorithms, also called generic algorithms because they work in any family of groups, have exponential time complexity. As a consequence, for a given level of security, the key size of an elliptic curve cryptosystem is smaller compared to RSA for instance. It makes elliptic curve discrete logarithm cryptosystems very suitable in constrained environment such as smart cards. The standards IEEE P1363, FIPS 186-2, NIST SP800-56A, and ANSI X9.63 describe their use, and the NSA adopted only elliptic

curve-based signature and key exchange protocols for U.S. government use as of 2005.

In the paper [36], Koblitz considers the family of groups given by the Jacobian of hyperelliptic curves as a possible replacement or generalisation of elliptic curves for the discrete logarithm problem. Hyperelliptic curves are classified with respect to their genus which is an integer. The genus one case corresponds to the usual elliptic curves. An interesting point is that for a base field of cardinality $q$, the size of the group of the Jacobian of a genus $g$ hyperelliptic curve is in the order of $q^g$. As the security of a discrete logarithm cryptosystem depends on the size of the group in which the computation takes place, this means that we obtain the same security as an elliptic curve with a genus $\geq 2$ hyperelliptic curve by using a smaller base field. This has the potential to result in significant speed up in the implementation when it is possible to fit an element of the base field in a single processor register.

Unfortunately, the representation of a point on a Jacobian of hyperelliptic curve is less compact than the representation of a point on an elliptic curve and the computation of the group law is slower. Moreover, a series of papers [1, 23, 74, 30] shows that the discrete logarithm problem in the family of Jacobian of hyperelliptic curves of large genus can be computed faster than with a generic algorithm. The critical case for these attacks is genus 3. This last consideration explains why the main focus of the CHIC project is the case of genus 2 or 3 curves.

As explained above, a family of groups must enjoy certain properties to be useful in a discrete logarithm cryptosystem. First, in order to have good performances, we have to be able to compute the group law as quickly as possible. Second, for security reasons, we have to be able to avoid groups corresponding to easy (or even relatively easy) instances of the discrete logarithm problem. Because of the Pohlig-Hellman algorithm [61], this last condition implies that we can count easily the number of rational points on the Jacobian of a curve in order to check that the group order is divisible by a large prime number. This consideration has spurred a considerable research effort in the past years in order to design efficient point counting algorithms (see the state of the art section). The point counting problem can be considered as solved in the case of curves of small genus defined over a field of small characteristic [56, 63, 48, 8]. Unfortunately, at this time there exists no satisfactory point counting algorithms to determine the number of rational points on the Jacobian of a general hyperelliptic curve of genus 2 defined over a prime field. In this case, the computation of the group order of a curve of cryptographic size is still painful [29]. This constitutes a real drawback of genus 2 curves in comparison with elliptic curves, since the discrete logarithm problem is believed to be easier in the family of curves defined over non-prime fields.

The main objective of this project is to bridge the gap in terms of performance and security between the genus 1 and small genus cases over prime fields. We project to expand the algorithmic toolbox applicable to small genus abelian varieties with new algorithms aiming at:

- improving the representation and group law computation;
- obtaining efficient point counting for curves.

As a result, we would obtain a new family of cryptosystems comparing favorably to elliptic curves, with the same level of security and equal or improved performance. Such cryptosystems would enjoy very interesting features such as the possibility for a given level of security to do all the computations with a smaller base field. This would constitute a real achievement for a line of research which started twenty years ago, with concrete applications for the implementation of discrete logarithms cryptosystems in constrained environments such as smart cards.

# 2 Scientific and technical description

## 2.1 Background, state of the art

### 2.1.1 The arithmetic of hyperelliptic curves

From a mathematical point of view, all the different representations of a certain algebraic curve or abelian variety are isomorphic and consequently may be viewed as the same object. From a computational prospect, the various representations may have very different properties with huge consequences on actual implementations. Most of the time, but not always, the main virtue of a representation is to provide a very compact and efficient way to compute with the objects used in cryptographic protocols.

For the genus one case, there exist different ways to improve the efficiency of the group law computation depending on the technological constraints of the implementation. For instance, projective coordinates will be a right choice if the inversion on the base field is costly. Various other choices of coordinates are available [11] with some of them available in genus 2 [43]. Recently, it has been discovered that alternative representations of elliptic curves can provide very efficient arithmetic. Indeed, an addition and a doubling require respectively only 10 and 7 multiplications in the Edwards model of elliptic curves [4] which is the best known complexity to date. There is, as yet, no analogue in genus 2 for this approach.

A way to obtain a more compact representation is to use point compression to save memory or bandwidth. Point compression relies on the fact that it is easy to recover the $y$-coordinate of a point on an elliptic curve in Weierstrass form from the knowledge of its $x$-coordinate and a sign bit. If one drops this last sign bit, the group addition is no longer well-defined, so that one has to adapt the algorithms in the same way as the Montgomery ladder [57]. The genus 2 case has been studied by Duquesne [16] and Gaudry [26] in terms of their Kummer surfaces.

Another property of certain representations, interesting for instance in order to protect from side channel attacks, is to present unified group law formulas. This means that the same formulas can be applied for both addition and doubling. These unified group laws have been described for the Hessian model of elliptic curves [34] or the Jacobi model [51].

Finally, specific improvements are required in pairing-based cryptography and are well developed for elliptic curves (use of the characteristic 3 pairing friendly curves) but not yet available for genus 2 curves.

### 2.1.2 Point counting for curves defined over prime fields

**General point counting algorithms** The known point counting algorithms for a curve $C$ over a finite field $k$ with Jacobian $J(C)$ can roughly be divided in two large classes, the $\ell$-adic algorithms and the $p$-adic algorithms.

The $p$-adic point counting algorithms can be interpreted as the computation of the action of the Frobenius morphism on some $p$-adic cohomology group. The first such algorithm has been described by Satoh [64]. The algorithm of Satoh relies on the computation of the action of the Frobenius morphism on the invariant differential forms of the canonical lift of an ordinary Jacobian. It has been generalised and made more efficient in a series of papers [66, 55, 56, 25, 47, 48]. Other authors have explored other possible representations of the Frobenius morphism. In [35], Kedlaya explains how to obtain a basis of the Monsky-Washnitzer cohomology of a hyperelliptic curve and compute the Frobenius morphism acting on it. Lauder used Dwork cohomology to obtain general point counting algorithms [45, 46]. Later on, Lauder introduced deformation techniques in which one considers a one parameter family of curves and use the Gauss-Manin connection in order to carry over this family the action of the Frobenius morphism [44]. This deformation approach has been studied later on by several people, pursuing in particular the goal of computing the zeta function of several abelian varieties simultaneously [33, 32, 10].

On the other side, the $\ell$-adic point counting algorithms can be interpreted as the computation of the action of the Frobenius morphism on the $\ell$-adic Tate module of the Jacobian, $\ell$ being prime to the characteristic of the base field. The $\ell$-adic point counting algorithms all follow an original idea of Schoof [67] which consists in computing the action of the Frobenius morphism on the group of $\ell$-torsion points of $J(C)$ for primes $\ell$ big enough to recover the zeta function of the curve by the Chinese remainder theorem. In the case that $C$ is an elliptic curve, this first algorithm has subsequently been improved by Elkies, Atkin and other authors [19, 67], resulting in the very efficient so-called SEA algorithm. Some of these techniques have been adapted in the case of higher genus curves [60] but some improvement have yet to be done in order to be able to easily reach cryptographic sizes. Nevertheless some progress has been made [24, 29] in that direction and one of the main goals of this project is to improve these last results.

**Special curves and point counting** The study of special curves follows a tradition going back to Koblitz [37]. On the other hand, the discovery of cryptographically weak special curves (supersingular curves, open to MOV reduction [52], or anomalous curves [65, 68, 70]), discouraged their study. More recent work has rehabilitated ordinary Koblitz elliptic curves and their hyperelliptic analogues [42], and applications to pairing-based cryptography renewed interest in supersingular curves. Examples include the generation of pairing-friendly curves, curves useful for ECM factorization or the ECPP primality test.

The *CM method* was introduced by Atkin and Morain [2] in order to construct elliptic curves with a prescribed endomorphism ring. This technique, originally intended to improve the ECPP algorithm, has since then found many applications. From the knowledge of the endomorphism ring, it is possible to immediately recover the number of points of the

curve and as a consequence the CM method can be used to obtain curves with a prescribed number of points. The usual CM method consists of computing complex analytic approximations to the $j$-invariants of elliptic curves with complex multiplication by a given order. More recently, Couveignes and Henocq introduced a $p$-adic approach [13, 62], which has been adapted to hyperelliptic curves of genus 2 by members of the project [9, 28]. Recent work of Sutherland for elliptic curves motivate a closer study of the higher dimensional CRT analogues [18, 3, 72]. Aside from cutting edge research [27, 29], the CM method has been the only practical method for constructing hyperelliptic curves suitable for cryptography in large characteristic. Although this project aims to break this monopoly by improving point counting algorithms for random curves, CM curves will continue to play an important role in cryptography, particularly in pairing-based cryptography where random curve selection is not sufficient to generate suitable curves.

Other examples of curves with extra structure are curves which admit RM (by a small fixed discriminant) and curves with a large automorphism group. Recent thesis work of Gruenewald [31] has resulted in better algorithms for computing defining polynomials for the *Humbert surfaces* which describe moduli of genus 2 curves with real multiplication. To date, RM curves have been underexploited in cryptography, but will have impact on the CM method, point counting and semi-random curve generation. Curves with large automorphism group may be used in cryptography, subject to the condition that their Jacobians decompose only over a proper extension of the base field. The determination of all possible automorphism groups is known in characteristic 0 but not for small characteristic. In this last case, the computation of all possible geometric automorphism groups already have solutions for genus 2, and for genus 3 models are sometimes known [59, 69]. The computation of twists has to be completed, as well as the correspondence with Frobenius characteristic polynomials.

## 2.2 Rationale highlighting the originality and novelty of the proposal

Section 2.1 presents problems of high cryptographic relevance for small genus hyperelliptic curves. We plan to work on substantially improving the algorithmic knowledge related to these questions. Consequently, small genus abelian varieties will become ready for prime-time cryptography.

In response to the challenges presented in Section 2.1, we will aim to improve the arithmetic of small genus abelian varieties, and the computation of their zeta functions (point counting). A key ingredient for the latter will be the study of explicit isogeny computations. The paragraphs below give more detail about these goals.

### 2.2.1 The arithmetic of hyperelliptic curves

The main objective of this part of the project is to find new representations for the Jacobian of genus 2 curves with very efficient group law formulas. This is a very competitive area of research with an extensive literature proposing a vast number of different representations.

In order to give an idea of how difficult it is to compare the various models, we just have to mention that Lange and Bernstein have set up a database, with all the published genus 1 representations classified with respect to different criteria.

Surprisingly, even considering the thoroughly studied pure performance aspect, very recent publications have shown that there is still room for improvement. In the genus one case, a series of papers have put in light the interest of elliptic curves in Edwards form [17]. With these new coordinates, elliptic curves have the lead over genus two curves in terms of the ratio of security to time complexity.

One of the main goals of this sub-project is to reduce the gap (or better, to inverse the gap) between genus one and genus two curves by designing new representations for abelian surfaces inspired by the Edwards model. We will publish our algorithms along with a precise complexity analysis in terms of the number of multiplications, squares, additions etc. needed to perform group operation. We will do a careful implementation on a realistic platform and provide the community with benchmarks allowing comparisons with already known representations.

### 2.2.2 Isogeny computation

The aim of this sub-project in to develop algorithms in order to compute efficiently isogenies between abelian varieties. The main approach that we want to develop is based on the use of theta functions. This is an important goal for three reasons:

- Isogenies can be used in order to transport a discrete logarithm problem from an abelian variety to another one which may be insecure. This technique has been used for instance by Smith [71] in order to show that most genus 3 curves are insecure. As pointed out by this last paper, with an efficient and general algorithm to compute isogenies of small degree between 3-dimensional abelian varieties, it would be possible to obtain a more general result.

- Isogeny computation is an important ingredient of the SEA algorithm for computing the zeta function of an elliptic curve defined over a prime field. Our aim is to use the tools developed in the isogeny sub-project in order to generalise the SEA algorithm to the higher dimensional case.

- We want to use algorithms to compute isogenies in order to explore the endomorphism ring of abelian varieties. The structure of this endomorphism ring is well known by general classification theorems and is algorithmically very important for instance in the CM method.

In principle, the formulas that we seek exist and can be obtained by using the general formalism of theta functions. The main difficulty of this sub-project is to obtain a compact representation for the abelian varieties and their moduli spaces and derive efficient formulas to compute isogenies.

We will give a description of our algorithm with a proof of correctness and a detailed complexity analysis. The main parameters that we want to take into account in the

complexity analysis is the genus, the degree of the isogeny and the size of the base field. We will provide the algorithms with a full implementation which can be built on top of computer algebra systems such as SAGE or MAGMA.

### 2.2.3 Point counting on curves defined over prime fields

The goal of this sub-project is to address the problem of the computation of the zeta function of a genus 2 curve defined over a finite field. We consider two different cases:

- the case of a general genus 2 curve;
- the case of curves with extra structure such as CM, RM or a large automorphism group that can be used to obtain highly efficient point counting algorithms.

In the following paragraphs, we detail the aim of this sub-project in each case.

**General point counting algorithm** The current record for point counting on an arbitrary genus 2 curve defined over a prime field [29] was set during the summer 2008 with a computation of a group order of about 254 bits for a Jacobian defined over the base field $\mathbb{F}_{2^{127}-1}$. The group order is not prime, not even nearly prime, hence not suitable for cryptography. The authors have shown that this computation can be done in about a month of CPU time, and many such curves would have to be tried in order to obtain an almost-prime cardinality, well suited for cryptographic purposes. The goal of this sub-project is to make it possible to do a computation of a group order of cryptographic size which means between 256 and 384 bits in a matter of hours (or even minutes) on a personal computer. It should be remarked that this goal can not be achieved just by improving the available implementations and as a consequence, we will have to design new algorithms. In particular, we expect to improve the computation of the action of the Frobenius morphism on suitable torsion sub-groups of an abelian surface by using the algorithms to compute isogenies developed in the first part of the project.

We plan to publish scientific papers describing our new algorithms with a detailed complexity analysis. The algorithms will be implemented carefully and benchmarks will be provided to the community. We would like to emphasize the fact that the results of this part of the project will depend upon our capacity to obtain a combination of new mathematical results and efficient implementations of the resulting algorithms.

**Special curves and point counting** In this project, we consider three different types of special properties: complex multiplication (CM) curves, for which the endomorphism ring of their Jacobians are orders in CM fields of small discriminant, families of curves with real multiplication (RM), or curves with large automorphism group. In these cases, we use the extra structure in order to obtain efficient point counting algorithms, and exploit the special properties.

Explicit real multiplication families are of interest for semi-generic random curve selection. Random genus 2 curves have invariants which vary in a three-dimensional moduli

space. By restricting to a two-dimensional subspace, called a Humbert surface, the subring of real multiplication remains fixed, reducing by half the number of undetermined bits in the characteristic polynomial of Frobenius. Additionally, for known real multiplication we can exploit the decomposition of the $\ell$-torsion at prescribed primes $\ell$ in the style of Atkin and Elkies.

For a curve with a large automorphism group, the group generally induces a decomposition (up to isogeny) of the Jacobian into smaller dimensional factors, in which a discrete logarithm can be computed more efficiently. We will study exceptions to this rule. In particular, if a Jacobian decomposes only over an extension of the finite base field, it may well have large prime number of points. Additionally, such curves may have useful properties for pairing-based cryptography or in terms of efficient scalar multiplication. Within this framework, we will furthermore investigate the potential role of other curves with special properties (such as geometric configurations of Weierstrass points of plane quartics). We will also investigate higher genus curves with large automorphism group as a means of constructing special curves with efficient automorphisms: as an example the families of genus 2 curves with RM by $\mathbb{Z}[(1+\sqrt{5})/2]$ and $\mathbb{Z}[\sqrt{2}]$ arise as quotients of higher genus curves with CM by $\zeta_5$ and $\zeta_8$, respectively (see [41, 54, 73]).

We will also study twists of curves with a large automorphism group as ways to circumvent potential security weaknesses of such curves. In particular, we will do a systematic study of hyperelliptic curves of genus 2 and hyperelliptic and generic curves of genus 3 curves over finite fields with large geometric automorphism groups. We will deduce fast algorithms to enumerate twists and compute the zeta function of such curves, results of both cryptographic and mathematical interest.

We will provide the community with a database of curves with special properties which are of interest for cryptographic applications. The database will be accessible from a web interface. All the programs used to build the data base will be released under a free software license.

# 3 Scientific and technical program, project management

## 3.1 Scientific program, specific aims of the proposal

The project will be divided in 4 main tasks:

1. The arithmetic of hyperelliptic curves and their Jacobians (led by Rennes);
2. Isogeny computation between general abelian varieties (led by Rennes);
3. General point counting algorithms over prime fields (led by Nancy);
4. Special curves and point counting (led by Marseille).

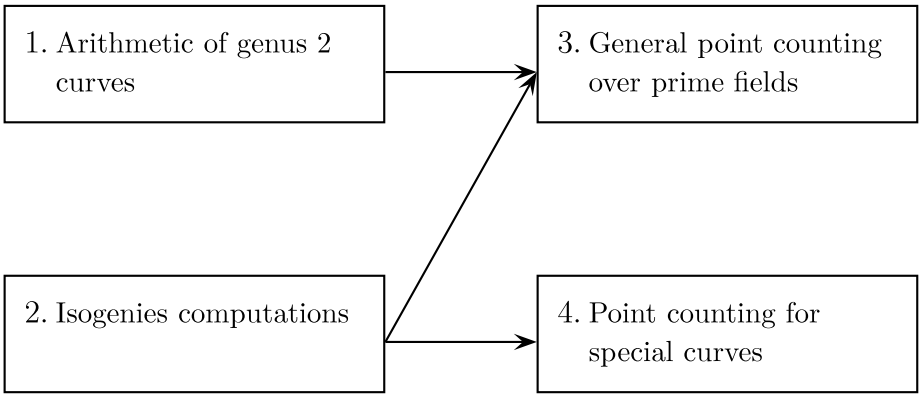


Figure 1: Dependency diagram

Of course the involvement of each partner of the project will depend of the particular task. While each task is followed primarily by one of the partners, the strong dependency of the different tasks will naturally lead all partners to be involved at some level within most tasks.

The figure 1 gives a description of the dependence between the different tasks. An arrow from task $A$ to task $B$ means that the completion of task $B$ depends on the output of task $A$.

It should be remarked that each task stands for itself as a scientific project. Putting them altogether forms a coherent approach to obtain a generalisation in the higher dimensional case of the SEA algorithm.

Of course the second task "Isogeny computation" is the most critical for the advancement of the project but it is also a task for which we have a clear point of view of what has to be done.

## 3.2 Project management

The project will involve three different partners:

- IRMAR (Institut de Recherche en Mathématiques de Rennes) with the team "Géométrie algébrique réelle, calcul formel et cryptographie" which hosts a group a specialists of cryptography;
- LORIA (Laboratoire Lorrain de Recherche en Informatique et ses Applications ; Nancy) with the project-team CACAO devoted to algorithmic and cryptography.
- IML (Institut Mathématiques de Luminy ; Marseille) with a group interested in effective aspects of arithmetic geometry;

The project will be divided in 4 tasks as described in Section 3.3. For each task a member of the project is responsible (see Figure 2). This responsible member will write annual

progress reports and will be accountable for the schedule of the task and the release of the deliverables.

The project coordinator will have to check that the different tasks are proceeding in a coherent manner. He will write the final report.

There will be two meetings organized each year where all the members of the project will gather and discuss the progress of each task. In particular, we plan to organise one kick-off and one closing meeting. We also plan to organise two important scientific events around the topics of the present proposal, expecting a wide audience. Tentative planning information for these meetings and events is suggested in Section 3.4.

Several week-long visits are planned for members of the project amongst the different partners, so as to foster joint work.

In order to organize and share the work, we will use all the means provided by a modern information system. For instance, we will set up a mailing-list for communication among the group, use a SVN server in order to carry out common work, and gather all our results on a web page.

## 3.3 Detailed description of the work organised by tasks

Our approach to the different tasks of the project will be a combination of theoretical analysis and computational experimentation or verification of the methods developed, in line with the methodology used by the project partners for most of their existing work.

**Task 1: The arithmetic of genus 2 curves and their Jacobian.** The main objective for this part of the project is to find new representations for the Jacobian of genus 2 curves with very efficient group law formulas. This has recently been done with success for elliptic curves thanks to the Edwards form [17]. One idea is to use the formalism of theta functions. Actually, it is easy to see that Edward's model and group law formulas are an immediate consequence of the classical Riemann quartic relations between theta functions. These relations are very general and exist for any genus. In genus 2, though, things are more complicated: there are 16 level-2 theta functions which give an embedding of a Jacobian surface in the projective space of dimension 15. As a consequence there are 13 algebraically independent Riemann relations. So we need to find a way into this maze of relations in order to find a really compact model with efficient group law.

Another interesting point would be to obtain a genus 2 model with unified formulas. This means that the same formulas can be used for both the addition and the doubling operations. This indistinguishability between the main operations is interesting to protect the implementation of the scalar multiplication against simple side-channel attacks [38]. There exists several models for elliptic curves with unified formulas ([34], [51]) but none is known for genus 2.

Recently, several members of this project have shown that the arithmetic on the Jacobian of genus 2 curves can be significantly improved by considering the associated Kummer surface. We plan to adapt these improvements to the context of pairing based cryptography. The main obstacle is of course the absence of a full addition on the Kummer surface.

There are several natural ways to bypass this problem. We can for instance develop a specific algorithm (as it is already the case for the scalar multiplication) or introduce a new pairing specifically adapted for Kummer surfaces. This kind of idea has been very recently sketched in the case of elliptic curves by Galbraith and Lin [22] who succeeded in the computation of the trace of the Tate Pairing using the $x$-coordinate only.

**Task 2: Isogeny computation between general abelian varieties.** There exist formulas due to Vélu [75] to compute isogenies between elliptic curves given in their Weierstrass model. Vélu's formulas can be obtained using some simple techniques of geometric invariant theory and the canonical characterisation of the coordinate system of the Weierstrass model of an elliptic curve.

There exist at least two known and useful representations of an abelian surface. The first one uses Mumford's representation of an element of the Jacobian of a genus 2 curve. We remark that using this representation there is an efficient algorithm in order to compute the group law [7]. The second kind of representation is based on theta functions. The classical theory of theta functions comes back to Riemann. This theory gives a general formalism in order to compute projective embeddings of abelian varieties. A very interesting fact about this theory is that it is effective. For instance, Mumford has shown [58] that every abelian variety can be described as a set of quadratic equations in the coordinate system provided by theta functions. The group law is also effective in this representation. Moreover, the locus of the projective points defined as the null value of the theta functions describes a projective variety which is a classifying space for abelian varieties together with a certain theta structure.

We plan to use the theory of theta functions in order to compute isogenies. There is a well known isogeny theorem which allows to compute isogenies between abelian varieties. Unfortunately, this theorem relates different models of abelian varieties. This problem should be easy to overcome as explained in [21]. A more serious concern is that the embedding provided by theta functions is very inefficient since it involves computing with a lot of variables. We plan to use the relations between theta functions as well as the existence of a large group acting on the coordinate system in order to improve the computations.

**Task 3: General point counting algorithms over prime fields.** There exists a higher genus adaption of the polynomial time point counting algorithm of Schoof due to Pila [60]. The main idea of the algorithm of Schoof is to compute the action of the Frobenius morphism on $\ell$-torsion sub-groups of an elliptic curve. From the knowledge of this action, one can deduce the characteristic polynomial modulo $\ell$ of the Frobenius morphism, and using the Chinese reminder theorem for different $\ell$, obtain the characteristic polynomial of the Frobenius morphism.

The algorithm of Pila can be improved by using Cartier-Manin operator for instance as explained in [27, 5] but at this moment the main ingredients of the Elkies and Atkin version of the algorithm of Schoof are not available in genus 2.

It should be remarked that the computation of the action of the Frobenius morphism

modulo $\ell$ implies the computation of a 0-dimensional algebraic variety given by the $\ell$-division polynomials. The problem is that the degree of the $\ell$-division polynomial is in the order to $\ell^2$ and it would be preferable to compute with smaller degree polynomials. The idea of Elkies and Atkin is to compute the action of the Frobenius morphism, not anymore on the whole $\ell$-torsion sub-group of $E$ but rather on a 1-dimensional sub-space. This 1-dimensional sub-space is given as the kernel of rational isogeny of degree $\ell$. The existence of such an isogeny can be seen in the factorization pattern of the $\ell^{th}$ modular polynomial. It has been a motivation for a series of papers about the efficient computation of isogenies between elliptic curves [75, 12, 49, 6, 50].

One of the main obstacles for the generalisation of the SEA algorithm to the higher genus case is the absence of an efficient and general algorithm to compute isogenies or kernel of isogenies between abelian varieties. The problem that we would like to solve are the following:

- starting with an abelian surface, compute, in a certain moduli space, points corresponding to $(\ell, \ell)$-isogenous abelian varieties;
- compute the kernel of each such $(\ell, \ell)$-isogeny.

Two approaches have been explored so far leading to partial results:

- generalize the well-known Richelot correspondence of genus 2 curves, which induces a $(2, 2)$-isogeny of their Jacobians, to correspondences which induce $(\ell, \ell)$-isogenies [14];
- generalize the Riemann duplication formulas of theta functions from $(2, 2)$-isogenies, to obtain relations of moduli points of $(\ell, \ell)$-isogenous abelian varieties [8, 9].

These two approaches are complementary and may be useful in different situations. The theta function point of view seems very promising since in principle, it allows one to obtain formulas to compute isogenies. The problem is that these formulas are very inefficient since it entails computing with models embedded in projective space of very high dimension. One of the goal of this project is to develop the theta function machinery in order to make it explicit and very efficient.

**Task 4: Special curves and point counting.** The preceding tasks concern algorithms for generic curves, however, special curves – those with certain prescribed geometric conditions – play an important role in cryptography. In particular we focus on curves with complex multiplication (CM), families with real multiplication (RM), and twists of curves with large automorphism group. The approach to these special curves is to determine explicit invariants, or *moduli* and find models parametrized by these moduli.

**CM curves.** We intend to extend the 2-adic and 3-adic CM methods (see [9, 28]) to other primes and investigate improvements to the complex analytic CM constructions [15, 76], as well as higher dimensional CRT analogues [18, 72], for which the main component will be to generalise the thesis work of Kohel [39] to higher genus curves. For this latter problem

we will exploit RM computations (indicated below) and explicit isogeny computations (Task 2). New "smaller" invariants will be investigated using moduli with level structure, analogous to Weber functions [77] or Dedekind eta functions [20]. Results will be made available through an extended interface to the definitive database of CM invariants [40] (currently hosted in Sydney).

**RM curves.** We will exploit recent developments in computing explicit moduli for RM in recent thesis work of Gruenewald [31], under supervision by Kohel. The first application to pursue will be explicit endomorphism ring computations, exploiting the known real subring for curves whose moduli lie on an RM surface. In particular, the endomorphism ring computation plays an important role in both the $p$-adic and CRT genus 2 CM methods. The second application of real multiplication is in point counting algorithms. The possibility of exploiting a known RM subring was foreseen by Gaudry [24]. As noted above, the prior knowledge of this subring reduced the information theoretic indeterminacy in the characteristic polynomial of Frobenius by half, hence we expect to require only half as many CRT primes in the genus 2 analogue of Schoof's algorithm. Furthermore, we will exploit the known decomposition of the $\ell$-torsion in this real subring to gain additional information in the style of Atkin and Elkies. Thus for fixed small real discriminant, we expect to develop a semi-generic random cryptographic curve selection – selecting two independent parameters on a Humbert surface – resulting in a more efficient point counting algorithm.

**Large $|\mathrm{Aut}(C)|$.** The cryptographic motivation of this study is to identify those curves $C/k$ such that their Jacobians (or some large isogeny factors) decompose only over a proper extension of $k$. Thus the decomposition can not be used to attack the discrete logarithm problem, and it may be suitable for use in cryptography. In order to approach this question in genus 2 and 3, we treat the following problems:

1. determine all possible geometric automorphism groups;
2. determine explicit invariants and models of a curve for such a group;
3. compute the decomposition of the Jacobian for each such a model;
4. find all twists of a given curve and determine their Frobenius characteristic polynomials.

Subsequently, we will connect this program of research with invariant theory in order to obtain the curves and their twists directly from invariants. For genus 2, this was implemented in Magma by Lercier and Ritzenthaler and included for instance in the Sage computer algebra system. For genus 3, when $(\mathbb{Z}/2\mathbb{Z})^2$ is included in the automorphism group, we can use Shaska's dihedral invariants [69]. For the remaining cases, we will have to generalize Mestre's algorithm [53] for reconstructing a curve from its invariants.

**Deliverables and success criteria** For each of the identified tasks relevant to our project, we develop the following milestones and success criteria:

**Task 1.** Arithmetic of genus 2 curves and their Jacobian.

**Aim.** Bridge the gap in term of performance between genus 1 curves and small genus curves defined over a prime field.

**Deliverables.**
- Scientific papers to be published in major cryptography conferences, algorithmic journals.
- Highly optimized implementation of algorithms, made available as BATs submitted to the SUPERCOP competition[1].
- A final report.

**Success criterion.** On certain platforms, for a given level a security, an implementation of a genus 2 curve which is more efficient than the best implementation available with an elliptic curve.

**Task 2.** Isogeny computation between general abelian varieties.

**Aim.** Obtain efficient algorithms to compute isogenies between abelian varieties.

**Deliverables.**
- Scientific papers to be published in major cryptography conferences, algorithmic journals.
- Implementation of algorithms made available through Magma or Sage modules.
- Publication of benchmarks to the Number theory mailing list.
- A final report.

**Success criterion.** An algorithm to compute $(101, 101)$-isogenies between abelian surfaces in a matter of minutes.

**Task 3.** General point counting algorithms for genus 2 curves defined over a prime field.

**Aim.** Obtain an algorithm to compute the number of points of a genus 2 curve of cryptographic size defined over a prime field in a few hours.

**Deliverables.**
- Scientific papers to be published in major cryptography conferences, algorithmic journals.
- Implementation of algorithms made available through Magma or Sage modules. Critical parts written in C/C++.
- Publication of benchmarks to the Number theory mailing list.
- A final report.

**Success criterion.** Compute the number of points of a general curve defined over a prime field, yielding a secure group of size 384 bits.

**Task 4.** Special curves and point counting.

[1] SUPERCOP is an international benchmark competition for cryptographic primitives, see `http://bench.cr.yp.to/supercop.html`.

**Aim.** Obtain very efficient point counting algorithms taking into account of special structures existing on a curve (CM, RM or big automorphism group).

**Deliverables.**
- Scientific papers to be published in major cryptography conferences, algorithmic journals.
- Implementation of algorithms made available through Magma or Sage modules.
- Publication of benchmarks to the Number theory mailing list.
- A final report.

**Success criteria.**
- Obtain a database of CM and RM curve interesting for cryptographic use;
- Produce a program to compute the twist of a genus 3 curve defined over a field of small characteristic.

### 3.4 Planning of tasks, deliverables and milestones

Figure 2 gives a schedule of the different tasks, the name of the responsible member for each task, the involvement of each partners and the main check points for each task.

Given the high dependencies amongst tasks, all partners will naturally have an eye on each aspect of the project. Nonetheless. Some "main" tasks can be identified for each partner.

Along the duration of the project, we plan to hold group meetings at regular intervals in order to coordinate work. A kick-off meeting (M1) will be organised in Fall 2009, followed by meetings M2 to M6 organised alternatively in Spring and Fall. Meeting M6 will serve as a closing meeting in Spring 2012. Two scientific events will be organised during the project. In Spring or Fall 2010, a workshop at CIRM (Marseille) on the topics of the current proposal will be organised. In Fall 2011, we will host the 15th edition of the ECC workshop in Nancy.

## 4 Data management, data sharing, intellectual property and results exploitation

The most important mean that we will use in order to spread our results is scientific publication. We plan to publish all our results in major cryptographic or algorithmic conferences such as Crypto, Eurocrypt, Asiacrypt or ANTS or in international cryptography or mathematical journals.

The main goal of this project is to develop new algorithms and to demonstrate their relevance and efficiency by implementing them. All the programs that we will develop will be placed under a free software license (such as GPL for instance) and made available to the community. We will strive to package our code in libraries ready to use in Magma or Sage computer algebra systems.

| Task | Partners | | | *Year 1* | | *Year 2* | | *Year 3* | |
|---|---|---|---|---|---|---|---|---|---|
| | IRMAR | LORIA | IML | 6 | 12 | 18 | 24 | 30 | 36 |
| **1.** Arithmetic of genus 2 curves Resp. : S. Duquesne | ● | ○ | ○ | ⊢ | — | — | — | — | ⊣ |
| **2.** Isogeny computations Resp. : D. Lubicz | ● | ○ | ○ | ⊢ | — | — | ⊣ | | |
| **3.** General point counting over prime fields Resp. : E. Thomé | ○ | ● | ○ | | | ⊢ | — | — | ⊣ |
| **4.** Point counting for special curves Resp. : D. Kohel | ○ | ○ | ● | ⊢ | — | — | — | — | ⊣ |
| Progress report | | | | | ☆ | | ☆ | | ★ |
| Consortium agreement | | | | ✪ | | | | | |
| Scientific events | | | | | | (1) | | (2) | |

*Key* : ● Primary involvement ; ○ Secondary involvement ; ☆ Annual progress report ; ★ Final report ; ✪ Consortium agreement ; (1) Workshop at CIRM ; (2) ECC 2011 in Nancy.

Figure 2: Task coordination

In order to allow the community to keep track of our progress we will regularly post benchmarks and record breaking computations in mailing lists such as the number theory mailing list.

We also plan to organize two public events, a workshop at mid-term of the project and a conference at the end. We will also maintain a web page. This web page will provide the community with the following information:

- the last available preprints;
- the last version of the implementation of our algorithms;
- announcements for events such as conferences, meetings, seminars.

# 5 Annexes

## 5.1 References

[1] L. M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In *Algorithmic number theory (Ithaca, NY, 1994)*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 28–40. Springer, Berlin, 1994.

[2] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[3] J. Belding, R. Bröker, A. Enge, and K. Lauter. Computing hilbert class polynomials. In *Algorithmic Number Theory Symposium – ANTS VIII*, Lect. Notes in Comput. Sci. Springer–Verlag, may 2008.

[4] D. Bernstein and T. Lange. Inverted Edwards coordinates. *Journal of AAECC*, 2007. to appear.

[5] A. Bostan, P. Gaudry, and É. Schost. Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves. In *Finite fields and applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 40–58. Springer, Berlin, 2004.

[6] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. To appear in Math. Comp.

[7] D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[8] D. Carls, R. and Lubicz. A $p$-adic quasi-quadratic time and quadratic space point counting algorithm. *Int. Math. Res. Not.*, 2008. To appear.

[9] R. Carls, D. Kohel, and D. Lubicz. Higher dimensional 3-adic CM construction. *J. Algebra*, 319:971–2006, 2008.

[10] W. Castryck, H. Hubrechts, and F. Vercauteren. Computing zeta functions in families of $C_{a,b}$ curves using deformation. In *Algorithmic Number Theory Symposium – ANTS 8*, number 5011 in Lect. Notes. in Comput. Sci., pages 296–311. Springer–Verlag, 2008.

[11] H. Cohen and G. Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Math. Appl. Chapman & Hall/CRC, 2006.

[12] J.-M. Couveignes. Computing $l$-isogenies using the $p$-torsion. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 59–65. Springer, Berlin, 1996.

[13] J.-M. Couveignes and T. Henocq. Action of modular correspondences around CM points. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 234–243. Springer, Berlin, 2002.

[14] I. Dolgachev and D. Lehavi. On isogenous principally polarized abelian surfaces, 2007. preprint.

[15] R. Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École Polytechnique, 2006.

[16] S. Duquesne. Montgomery scalar multiplication for genus 2 curves. In *Algorithmic Number Theory Symposium – ANTS VI*, volume 3076 of *Lecture Notes in Computer Science*, pages 153–168. Springer–Verlag, 2004.

[17] H. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007.

[18] K. Eisentraeger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields, 2004. preprint, Available as `http://arxiv.org/abs/math/0405305v2`.

[19] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[20] A. Enge and F. Morain. Comparing invariants for class fields of imaginary quadratric fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 252–266. Springer, Berlin, 2002.

[21] J.-C. Faugère and D. Lubicz. Computing modular correspondence for abelian varieties, 2008. preprint.

[22] S. Galbraith and X. Lin. Computing pairings using x-coordinates only. *Designs, Codes and Cryptography*, 2008. to appear.

[23] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 19–34. Springer, Berlin, 2000.

[24] P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*. PhD thesis, École Polytechnique, 2000.

[25] P. Gaudry. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. In *Advances in cryptology—ASIACRYPT 2002*, Lecture Notes in Comput. Sci. Springer, Berlin, December 2002.

[26] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 1:243–265, 2007.

[27] P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 313–332. Springer, Berlin, 2000.

[28] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in cryptology—ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Comput. Sci.*, pages 114–129. Springer, Berlin, December 2006.

[29] P. Gaudry and E. Schost. Genus 2 point counting record. Email to the Number Theory List, June 2008.

[30] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.*, 76(257):475–492, 2007.

[31] D. Gruenewald. *Explicit Algorithms for Humbert Surfaces*. PhD thesis, University of Sydney, 2008.

[32] H. Hubrechts. Point counting in families of hyperelliptic curves. *Found. Comput. Math*, 2007. to appear.

[33] H. Hubrechts. Point counting in families of hyperelliptic curves in characteristic 2. *LMS J. Comput. Math.*, 10:207–234, 2007.

[34] M. Joye and J. J. Quisquater. Hessian elliptic curves and side-channel attacks. In *Cryptographic Hardware and Embedded Systems – CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 402–410. Springer–Verlag, 2001.

[35] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[36] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.

[37] N. Koblitz. Cm-curves with good cryptographic properties. In *Advances in cryptology—Crypto'91*, volume 576 of *Lecture Notes in Comput. Sci.*, pages 279–287, Berlin, 1992. Springer.

[38] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology – CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer–Verlag, 1996.

[39] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.

[40] D. Kohel. ECHIDNA databases for algebra and geometry experimentation, 2008. `http://echidna.maths.usyd.edu.au/kohel/dbs/index.html`.

[41] D. Kohel and B. Smith. Efficiently computable endomorphisms for hyperelliptic curves. In *Algorithmic number theory (Berlin, 2006)*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 495–509, Berlin, 2000. Springer.

[42] T. Lange. *Efficient Arithmetic on Hyperelliptic Curves*. PhD thesis, Essen, 2001.

[43] T. Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Journal of AAECC*, 15(5):295–328, 2005.

[44] A. G. B. Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc. (3)*, 88(3):565–602, 2004.

[45] A. G. B. Lauder and D. Wan. Computing zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.*, 5:34–55 (electronic), 2002.

[46] A. G. B. Lauder and D. Wan. Computing zeta functions of Artin-Schreier curves over finite fields. II. *J. Complexity*, 20(2-3):331–349, 2004.

[47] R. Lercier and D. Lubicz. Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In E. Biham, editor, *Advances in Cryptology—EUROCRYPT '2003*, Lecture Notes in Computer Science. Springer-Verlag, May 2003.

[48] R. Lercier and D. Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. *Ramanujan J.*, 12(3):399–423, 2006.

[49] R. Lercier and F. Morain. Computing isogenies between elliptic curves over $\mathbf{F}_{p^n}$ using Couveignes's algorithm. *Math. Comp.*, 69(229):351–370, 2000.

[50] R. Lercier and T. Sirvent. On Elkies subgroups of $\ell$-torsion points in elliptic curves defined over a finite field, 2008. To appear in *Journal de Théorie des Nombres de Bordeaux*.

[51] P. Y. Liardet and N. Smart. Preventing spa/dpa in ecc systems using the jacobi form. In *Cryptographic Hardware and Embedded Systems – CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 391–401. Springer–Verlag, 2001.

[52] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve discrete logarithms to a finite field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.

[53] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.

[54] J.-F. Mestre. Familles de courbes hyperelliptiques à multiplications réelles. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 193–208. Birkhäuser Boston, Boston, MA, 1991.

[55] J.-F. Mestre. Lettre à Gaudry et Harley, 2001. Available at http://www.math.jussieu.fr/mestre.

[56] J.-F. Mestre. Notes of a talk given at the seminar of cryptography of Rennes, 2002. Available at http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps.

[57] P. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, 48:243–264, 1987.

[58] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[59] E. Nart and D. Sadornil. Hyperelliptic curves of genus three over finite fields of even characteristic. *Finite Fields and Their Applications*, 10:198–220, 2004.

[60] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.

[61] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF($p$) and its cryptographic significance. *IEEE Trans. Information Theory*, IT-24(1):106–110, 1978.

[62] E. Riboulet-Deyris. *Calculs d'espaces de modules par déformations en égales et inégales caractéristiques*. PhD thesis, Université Toulouse, 2004.

[63] C. Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*. PhD thesis, Université Paris 7 - Denis Diderot, June 2003.

[64] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[65] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comm. Math. Univ. Sancti Pauli*, 47:81–92, 1998.

[66] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields and Their Applications*, 9(1):89–101, 2003.

[67] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie des nombres de Bordeaux*, 7:483–494, 1998.

[68] I. Semaev. Evaluation of discrete logarithms in a group of $p$-torsion points of an elliptic curve in characteristic $p$. *Math. Comp.*, 67:353–356, 1998.

[69] T. Shaska. Computational aspects of hyperelliptic curves. In *Computer mathematics*, volume 10 of *Lecture Notes Ser. Comput.*, pages 248–257. World Sci. Publ., River Edge, NJ, 2003.

[70] N. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Crypto.*, 12:193–196, 1999.

[71] B. Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. In *Advances in Cryptology—EUROCRYPT '2008*, Lecture Notes in Computer Science. Springer-Verlag, 2008.

[72] A. Sutherland. Computing Hilbert class polynomials with the CRT method, sep 2008. Invited talk at ECC workshop.

[73] W. Tautz, J. Top, and A. Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.

[74] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In *Advances in cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, pages 75–92. Springer, Berlin, 2003.

[75] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[76] A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplication*. PhD thesis, Universität GH Essen, 2001.

[77] N. Yui and D. Zagier. On the singular values of Weber modular functions. *Math. Comp.*, 66(220):1645–1662, 1997.