Curves and Jacobians : number extractors and efficient arithmetic

Curves and Jacobians:

Number Extractors and Efficient Arithmetic

Reza Rezaeian Farashahi

Curves and Jacobians: Number Extractors and Efficient Arithmetic

PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr.ir. C.J. van Duijn, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op maandag 27 oktober 2008 om 16.00 uur

door

Reza Rezaeian Farashahi

geboren te Teheran, Iran

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr.ir. H.C.A. van Tilborg
en
prof.dr. T. Lange

Copromotor:
dr. G.R. Pellikaan

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

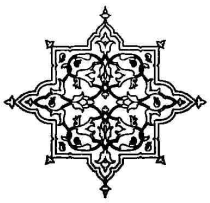
Rezaeian Farashahi, Reza

Curves and Jacobians: Number Extractors and Efficient Arithmetic/ door Reza Rezaeian Farashahi. - Eindhoven : Technische Universiteit Eindhoven, 2008.
Proefschrift. - ISBN 978-90-386-1410-6
NUR 918
Subject headings: Algebraic geometry, Cryptology
2000 Mathematics Subject Classification: 11G20, 14H40, 14H52, 14G50, 94A60

Promotor: prof.dr.ir. H.C.A. van Tilborg (Technische Universiteit Eindhoven)
Promotor: prof.dr. T. Lange (Technische Universiteit Eindhoven)

Copromotor: dr. G.R. Pellikaan (Technische Universiteit Eindhoven)

Commissie:
prof.dr.ir. A.E. Brouwer (Technische Universiteit Eindhoven)
prof.dr. S.J. Edixhoven (Universiteit Leiden)
prof.dr.dr.h.c. G. Frey (Universität Duisburg-Essen)
prof.dr. I.E. Shparlinski (Macquarie University)



The work in this thesis is supported by the Ministry of Science, Research and Technology of I. R. Iran under scholarship no. 800.147.

Printing: Eindhoven University Press

Cover design: S.E. Baha

Contents

Preface

به نام خداوند جان و خرد کزین برتر اندیشه برنگذرد

This momentous time of my life would have been impossible without the support, enthusiasm and encouragement of many incredibly precious people. I devote this preface to thank them.

First of all, I would like to express my deep and sincere gratitude to my supervisors, Henk van Tilborg, Tanja Lange and Ruud Pellikaan for giving me the possibility to work under their supervision. Thanks to Henk for accepting me as a Ph.D. student in his group and for his friendship throughout these four years. Tanja and Ruud were my daily supervisors and always ready to discuss various issues concerning my research and to answer my questions. This work would not have been possible without their support and encouragement, and I am grateful for their valuable friendship.

The results in this thesis are the fruits of joint work with my distinguished co-authors: Dan Bernstein, Bas Edixhoven, Tanja Lange, Ruud Pellikaan and Andrey Sidorenko. So my best thanks go to them. I would also like to express my great appreciation to the rest of my co-authors: Wouter Castryck, Steven Galbraith, Berry Schoenmaker and Igor Shparlinski with whom I worked on papers that are not in this thesis. It was my pleasure to work with all of them, and it made me realize the value of working together as a team. Thank you all.

The members of my thesis committee are gratefully acknowledged for reading the thesis, providing useful comments and being present in my defense session. It was my privilege to have Andries Brouwer, Bas Edixhoven, Kees van Hee, Tanja Lange, Ruud Pellikaan, Igor Shparlinski and Henk van Tilborg in the reading committee and Gerhard Frey in the defense opposition.

In the past four years, I had the opportunity to cooperate with many people and several groups from different institutes. For these opportunities, I am obliged to

Gerhard Frey from Institute of Experimental Mathematics, University of Duisburg-Essen, Germany, Bas Edixhoven from Mathematical Institute, University of Leiden, The Netherlands, Steven Galbraith from Mathematics Department, Royal Holloway University of London, UK, and Igor Shparlinski from the Department of Computing, Macquarie University, Australia. Although I could not fit all the results of cooperations with these good colleagues in this thesis, they have certainly influenced the state of my mind and hence they are indirectly present in this thesis.

The great working atmosphere in the Coding Theory and Cryptology group at Eindhoven University of Technology is certainly never forgotten. I express my best thanks to all members of the group for being so friendly, helping me from time to time, organizing enjoyable meetings, social events and tea breaks. Discussion sessions with the supervisors Henk, Ruud, Tanja, Benne, Berry, Dan, and with students Ellen, Andrey, Mehmet, José, Peter (Birkner), Christiane, Peter (van Liesdonk), Michael, Peter (Schwabe), Sebastiaan and Gaetan were a nice way to think about new research problems and learn from their research interest and problems. Anita, Bram, Wil and Henny completed this nice group as well. I have been fortunate to be an office-mate of many nice people in the group. I would like to thank all my office-mates for their help, conversations and discussions. I also would like to thank all members of Security group as well as the Discrete Algebra and Geometry group for sharing the friendly and creative atmosphere with our group.

My PhD study was supported by a scholarship from the Ministry of Science, Research and Technology of I. R. Iran. I would like to take this opportunity to thank them for their support. I also would like to thank Farhad Rahmati and Mohammad Hossein Abdollahi, Mohammad Nazemi, academic representatives and directors of Iranian students in Europe for their help.

I would like to express my gratitude to my professors at the University of Tehran and Chamran University of Ahvaz for their advice and insights. Special thanks go to Mansoor Motamedi (my ex-supervisor). I would also like to thank my teachers in Maleksabet high school whom I am greatly indebted to them for their help and encouragement that stimulated my interest in mathematics.

I express my best thanks to the Iranian families Baha, Farshi, Fatemi, Eslami, Mousavi, Moosavi Nejad, Nikoufard, Sedghi, Shojaei and Talebi for their help and support and for the great time we had with them. I would also like to express my gratitude to Mohammad Ali Abam, Ehsan Baha, Mohammad Eslami, Mohammad Farshi, Hamed Fatemi, Amir Hossein Ghamarian, Kamyar Malakpoor, Mohammad Reza Mousavi, Mohammad Moosavi Nejad, Iman Mosavat, Mahmoud Nikoufard, Pooyan Sakian, Mohammad Samimi, Saeed Sedghi, Hamid Shojaei, Saeid Talebi and many other wonderful Iranian students in the Netherlands for their kind friendship. Finally, thanks to many other good friends, specially the members of Saturday's soccer team.

I am grateful beyond expression to my dearest family. Words cannot express the extent to which I feel indebted and grateful to them for all their unconditional help and support throughout my whole life and in particular, during the last four years. My special thanks go for my wife Maryam, my daughter Fatemeh and my son Mohammad for sharing the beautiful moments of their life with me. I dedicate this thesis to them, *with love and gratitude*.

Reza Rezaeian Farashahi

September 2008

Chapter 1

Introduction

Algebraic curves over finite fields are being extensively studied in the context of public-key cryptographic schemes. Koblitz [65] and Miller [82] were the first to show that the group of rational points on an elliptic curve over a finite field can be used for the discrete logarithm problem in a public-key cryptosystem. Elliptic curves have received a lot of attention throughout the past 2 decades and many researchers became interested in computational problems related to the efficient arithmetic in the group law and solving the discrete logarithm problem in the group [8, 23, 50]. They have been proposed for applications in cryptography due to their fast group law and because so far no subexponential attack on their discrete logarithm problem is known (see [23]). The most efficient methods for solving the DL problem for ordinary elliptic curve have exponential running time. For supersingular elliptic curves there exist subexponential methods, (see [80]) so supersingular elliptic curves should be avoided for DL based cryptosystem.

Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, which results in faster computations, lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity.

Koblitz, [66], was the first to suggest using the discrete logarithm problem in the Jacobian of a hyperelliptic curve over a finite field in public key cryptography. Hyperelliptic curves of genus 2 are undergoing intensive study (e.g. see [23]) and have been shown to be competitive with elliptic curves in speed and security and for suitably chosen curves the best attacks are generic attacks. Many researchers have optimized genus 2 arithmetic so that in several families of curves they are

faster than elliptic curves [46, 47, 73]. The security of genus 2 hyperelliptic curves is in general assumed to be similar to that of elliptic curves of the same group size [44].

The use of the Kummer surface associated to the Jacobian of a genus 2 curve is proposed for faster arithmetic (see [25, 46, 68]). The scalar multiplication on the Jacobian can be used to define a scalar multiplication on the Kummer surface. This can be applied in cryptography; e.g. in the Diffie-Hellman protocol (see [93]). In addition, it is shown there, that solving the discrete logarithm problem on the Jacobian is polynomial time equivalent to solving the discrete logarithm problem on the Kummer surface.

The problem of converting random points of a group into random bits has several cryptographic applications. Examples are key derivation functions, key exchange protocols and the design of cryptographically secure pseudorandom number generators. For instance, at the end of the Diffie-Hellman key exchange protocol (e.g. the well-known (hyper)elliptic curve Diffie-Hellman protocol), the parties agree on a common secret element of the group G. This element is indistinguishable from a uniformly random group element under the decisional Diffie-Hellman assumption (denoted by DDH). However, the binary representation of the common secret element is *distinguishable* from a uniformly random bit-string of the same length. Therefore one has to convert this group element into a bit string statistically close to uniformly random. The classical solution is to use a hash function. Then, the indistinguishability cannot be proved in the standard model but only in the random oracle model. An alternative solution is to use extractors for the group G.

An extractor on a set is a function that converts a random element of the set to a random bit-string, which is statistically close to a uniformly random bit-string. There exists vast literature on extractors in the general setting of a map between arbitrarily distributed (long) bit-strings to almost uniformly distributed (shorter) bit-strings (see [21, 40, 89, 96] and references there in).

The security of extractors is based on standard assumptions and so they allow us to avoid the random oracle model for key exchange protocols. The DLP in a group G can always be solved in time $O(\sqrt{\#G})$ and for suitably chosen groups there are no faster attacks known. To match security levels, the key for a symmetric cipher with k bits key should be derived from a group element of a group of size $2k$ bits, i.e. the extractor could reduce the bit-length by at least a factor of 2.

In this thesis, we deal with number extractors based on elliptic and hyperelliptic curves. Then, we generalize the number extractors to the genus-2 Jacobians and associated Kummer surfaces. As a second related topic we study fast arithmetic on binary elliptic curves and introduce a new representation for these curves.

1.1 Extractors on curves and Jacobians

The construction of provable and more efficient pseudorandom generators based on some standard and non-standard assumptions is a requirement for cryptographic schemes. The literature on pseudorandom number generators on curves and Jacobians is mostly concerned with studying the distribution of the coordinates or the coordinate pairs [5, 28, 53, 61, 71, 72, 90] or considers only the extreme case of extracting one bit per point [48]. The extractors for curves and Jacobians, which output as many bits as possible, can be used to construct cryptographically secure pseudorandom generators.

So far, several deterministic randomness extractors for elliptic curves have been proposed. Kaliski [61] shows that if a point is taken uniformly at random from the union of an elliptic curve and its quadratic twist then the x-coordinate of this point is uniformly distributed in the finite field. Then, the TAU technique [20] allows to extract almost all the bits of the abscissa of a point of the union of an elliptic curve and its quadratic twist. This technique uses the idea in [61], that if a point is taken uniformly at random from the union of an elliptic curve and its quadratic twist then the abscissa of this point is uniformly distributed in the finite field. Gürel [49] proposed an extractor for an elliptic curve defined over a quadratic extension of a prime field. It extracts almost half of the bits of the abscissa of a point on the curve. Another extractor for elliptic curves over prime fields is proposed by Gürel in the same paper. However, the latter extracts significantly less than half of the bits of the abscissa of a point on the curve.

A simple way to construct an extractor based on curves, Jacobians and in general varieties over finite fields is as follows. Consider a variety of dimension n over a finite field $\mathbb{F}_q$. Suppose each point of this variety is represented by n independent coefficients plus some other dependent coefficients. An extractor can be defined that, for a given point on the variety, outputs some k independent coefficients of the point, where k is a positive integer less than or equal to n. This means, the extractor outputs k numbers in $\mathbb{F}_q$, from a point of the variety that is compactly represented by n numbers in $\mathbb{F}_q$. Obviously a smaller k implies a smaller output, but also a more uniformly distributed output. This extractor can be generalized to a variety over an extension finite field of $\mathbb{F}_q$ by means of restriction techniques from the extension field to the ground field $\mathbb{F}_q$.

Our contributions. In Chapters 4 and 5, we present a simple and efficient extractor, called `Ext`, based on (hyper)elliptic curves defined over a quadratic extension of the finite field $\mathbb{F}_q$. For a given point on the (hyper)elliptic curve, our extractor outputs the first $\mathbb{F}_q$-coefficient of the x-coordinate of the point. Further, one can define an extractor that, for a given point on the curve, outputs an $\mathbb{F}_q$-linear combination of both coefficients of the x-coordinate of this point. The analysis of our extractor shows that, for randomly distributed points on the curve, the distribution of the $\mathbb{F}_q$-sequence is indistinguishable from the uniform distribution

on $\mathbb{F}_q$.

We note that the x-coordinate of a uniformly random point on a (hyper)elliptic curve can be easily distinguished from a uniformly random field element. Our extractor, `Ext`, provides only part of the x-coordinate and thereby avoids the obvious problem; the proof shows that actual uniformity is achieved. Our approach is somewhat similar to the basic idea of pseudorandom generators proposed by Gong et al. [48] and Beelen and Doumen [5] in that they use a function that maps the set of points on an elliptic curve to a set of smaller cardinality. In the former reference, this function outputs the trace map of the x-coordinate of the point on a binary curve. So, each point gives rise only to one bit. The latter studied more general functions so that some more bits per point can be obtained. Our aim is to extract as many bits as possible while keeping the output distribution statistically close to uniform.

So far, the all known deterministic randomness extractors for elliptic curves can be applied only for elliptic curves over odd prime fields and their extensions, although in many cases elliptic curves over binary fields can be implemented more efficiently in hardware (see, e.g., [50]). Till now, the problem of constructing an efficient deterministic extractor for elliptic curves over binary fields remained open.

In Chapter 4, the extractor `Ext` is presented for a binary elliptic curve E defined over $\mathbb{F}_{q^2}$, where $q = 2^\ell$ and ℓ is a positive integer. So, by means of `Ext`, exactly ℓ bits can be extracted from a given point on E. Also, in this chapter, we present an extractor for the main subgroup G of E, where E has minimal 2-torsion. This extractor has more practical applications in cryptography, if both ℓ and the order of G are primes. The results of this chapter are based on [33, 34].

In many cases, it is recommended to use elliptic curves over $\mathbb{F}_{2^m}$, where m is a prime number. Recall that in Chapter 4 we consider elliptic curves over $E(\mathbb{F}_{2^m})$, where $m = 2\ell$. To the best of our knowledge, the DL problem for the latter curves is as hard as the one for the former curves provided that the GGHS attack is infeasible, that is, ℓ is a prime number and $\ell \neq 127$ (for more details see [22, 41, 42, 52, 79, 81]). The finite fields $\mathbb{F}_{2^{178}}, \mathbb{F}_{2^{226}}, \mathbb{F}_{2^{1018}}$ and $\mathbb{F}_{2^{1186}}$ are suggested for elliptic curve cryptography in [22]. For these fields the GGHS attack is infeasible. Furthermore by the *ghost bit bases* technique, the arithmetic operations in these fields can be performed more efficiently than in prime extension of $\mathbb{F}_2$ of the same size (see [54, 92]).

An efficient pseudorandom generator based on elliptic curves is proposed by Barker and Kelsey [4]. Unfortunately, their generator (called Dual Elliptic Curve generator) is insecure, the reason being that random bits are extracted from random points of the elliptic curve in an improper way [16, 35, 85]. Replacing the extractor used by Barker and Kelsey with one of our extractors yields a pseudorandom generator which is provably secure under the DDH assumption and the x-logarithm assumption [16].

In Chapter 5, the extractor `Ext` is described for (hyper)elliptic curves over finite fields with odd characteristic. In particular, the definition of `Ext` for elliptic curves is similar to the proposed extractor in [49], yet the analysis is improved by means of our proof techniques. The results of this chapter are based on [32].

The main part of the analysis of extractor `Ext` is the counting part; i.e., to find bounds on the number of points of all fibers of `Ext`. In other words, we need to estimate the number of points on the curve with a fixed first coefficient of the x-coordinate. We can find these estimates by means of the Weil descent technique and Hasse-Weil Theorem as follows. First we consider the Weil descent of the curve from a quadratic extension to the ground field. So, we obtain a surface over $\mathbb{F}_q$, algebraically defined by a system of two equations with 4 variables. Then, we fix the corresponding variable to the first coefficient of the x-coordinate. This means, we intersect the Weil descent surface with a coordinate hyperplane, so we obtain in general a curve defined by a system of two equations with 3 variables. Next, we need to estimate the number of points on this intersection. We can use the *resultant* technique or *Gröebner basis* algorithm to eliminate one variable in the later system and obtain a bi-variate equation. A curve can be defined by this bi-variate equation and the number of points on this curve can be shown to be almost equal to the number of points on the corresponding fiber of `Ext`. After that, we investigate the irreducibility of this curve. If it is absolutely irreducible, we examine the singularity and compute the genus of the curve. Further, we obtain bounds for the number of points on this curve by means of the Hasse-Weil Theorem. This implies a solution for the counting problem. We note that the estimates by the later curve are not tight, so a suitable transformation is needed to obtain tight estimates.

Our approaches to finding bounds on the number of points of the fibers of `Ext` in Chapters 4 and 5 are similar to the above, but we use alternative restriction techniques. We replace the Weil descent surface with other related surfaces. They are called *trace* and *norm* surfaces and used respectively in Chapters 4 and 5. These surfaces are algebraically defined by one equation over $\mathbb{F}_q$ with 3 variables. Then, we consider the intersections of these surfaces with coordinate hyperplanes. We show that the number of points on each intersection equals the number of points of the related fiber of `Ext`. Next, we need to estimate the number of points on the intersections. We show that these intersections are in general absolutely irreducible nonsingular curves. After that, by means of the Hasse-Weil Theorem for these curves, we obtain estimates for the number of points on fibers of `Ext`.

We used the *trace* and the *norm* techniques instead of the Weil-descent, because of the following reasons. First of all, with these techniques, it is easier to handle the algebraic analysis of the geometry of the hyperplanes intersections. So, our claims are provided with shorter proof techniques. Secondly, by the *norm* and the *trace* techniques, tight estimates can be obtained after the intersection step. We note that, in the first approach, because of using the resultant technique, the equations

of the intersections are of higher degree and tight estimates can not be obtained directly.

In Chapter 3, the idea of the *trace* surface is generalized to curves of the Artin-Schreier form. In fact, an Artin-Schreier curve defined over an extension of $\mathbb{F}_q$ of degree n is related to an n-dimensional hypersurface defined over $\mathbb{F}_q$. This generalization is based on a particular case, namely that of binary elliptic curves over quadratic extension finite fields, introduced as the *trace* surface in [33]. Also, the idea of the *norm* surface is generalized to the Kummer curves. Indeed, a Kummer curve over an extension of $\mathbb{F}_q$ of degree n is related to an n-dimensional hypersurface defined over $\mathbb{F}_q$. For the particular case of hyperelliptic curves over quadratic extension fields $\mathbb{F}_{q^2}$, the *norm* surface was proposed in [32]. We hope that the study of the geometry of the intersections of the *trace* and the *norm* hypersurfaces with hyperplanes enables us to generalize the definition of the extractor `Ext` to Artin-Schreier and Kummer curves over finite fields.

In Chapters 6 and 7, we present two simple and efficient extractors for Jacobians of genus-2 hyperellipic curves. They are called the *sum* and the *product* extractors. The *sum* (respectively the *product*) extractor, for a given point D on the Jacobian of a hyperelliptic curve H over $\mathbb{F}_q$, outputs the sum (respectively the product) of x-coordinates of points on H in the support of D, considering D as a reduced divisor. It is shown that, if the point D is chosen uniformly at random in the Jacobian of H over $\mathbb{F}_q$, the element extracted from the point D is indistinguishable from a uniformly random variable in $\mathbb{F}_q$.

Again, the main part in the *sum* and *product* extractors is the counting part. We follow a similar above approach to finding bounds on the number of points on the fibers of these extractors. In Chapter 2, we introduce a surface related to the Jacobian of genus 2-hyperelliptic curves over $\mathbb{F}_q$. This surface is defined by an algebraic equation with 3 variables, where the two independent variables correspond to the sum and the product of the x-coordinates of points on H in the support of reduced divisors in the Jacobian of H over $\mathbb{F}_q$. We obtain bounds on the number of points on the intersections of this surface with coordinate hyperplanes, which enables us to estimate the number of points on the fibers of the sum and product extractors.

In Chapter 6, we describe the *sum* and the *product* extractors for Jacobians of genus-2 hyperellipic curves over $\mathbb{F}_q$ with odd characteristic. Further, in this chapter, modified versions of the *sum* and the *product* extractors are proposed for the Kummer surface associated to the Jacoobian of a genus-2 hyperelliptic curve. The results of this chapter are based on [29].

In Chapter 7, we extend definitions of the *sum* and the *product* extractors to Jacobians of genus-2 hyperellipic curves over binary fields. Further, the modified *sum* and *product* extractors are suggested for the main subgroup of the Jacobian of H over $\mathbb{F}_q$ with group order $2m$, where m is odd. We note that, for cryptographic

application m, the order of the subgroup, is chosen to be prime. The results of this chapter are based on [30].

1.2 Efficient arithmetic on elliptic curves

The points on a Weierstrass-form elliptic curve

$$\mathbf{y}^2 + a_1\mathbf{xy} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6$$

include not only the affine points (x_1, y_1) satisfying the curve equation but also an extra point at infinity serving as the neutral element. The standard formulas to compute a sum $P + Q$ fail if P is at infinity, or if Q is at infinity, or if $P + Q$ is at infinity, or if P is equal to Q. Each of these possibilities needs to be tested for and handled separately; a complete addition *algorithm* is produced by gluing together several incomplete addition *formulas*.

This plethora of cases has caused a seemingly neverending string of problems for implementors of elliptic-curve cryptography, especially in cryptographic hardware subject to side-channel attacks. Consider, for example, computing $nP + mQ$. A typical two-scalar-multiplication algorithm would double P, add P, add Q, etc., where the exact pattern of additions and doublings depends on the values of n and m. What happens if $3P = Q$? Does the implementation take the time to see that $3P = Q$ and to switch from the addition formulas to doubling formulas? Can the attacker detect the switch through timing analysis, power analysis, etc.? If the implementation fails to check for $3P = Q$, what does it end up computing? What about $3P = -Q$? Can an attacker trigger failure cases—and incorrect computations—by choosing inputs cleverly? Can these failures compromise cryptographic security?

Some papers have presented "unified" addition formulas that can be used for doublings. See, e.g., [12], [14], [15], [58], and [74]; for overviews see [9, Section 5], [57], and [69]. "Strongly unified" addition formulas eliminate the need to check for equal inputs. However, they do not eliminate the need to check for inputs and outputs at infinity and for other exceptional cases. The exceptional-points attack presented in [56] targets the exceptional cases in these unified formulas.

Edwards curves. Edwards [26] proposed a new normal form for elliptic curves and gave an addition law that is remarkably symmetric in the x and y coordinates. In the recent paper [9], Bernstein and Lange show for fields $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$ that if d is not a square in $\mathbb{F}$ then the affine points on the "Edwards curve"

$$\mathbf{x}^2 + \mathbf{y}^2 = 1 + d\mathbf{x}^2\mathbf{y}^2$$

form a group. The affine addition law introduced by Edwards in [26] is complete for this curve, as are the fast projective formulas introduced in [9].

"Complete" is stronger than "unified": it means that the addition formulas work for *all* pairs of input points. There are no troublesome points at infinity. In particular, the neutral element of the curve is an affine point $(0, 1)$.

If $\mathbb{F}$ is finite then approximately $1/4$ of all elliptic curves over $\mathbb{F}$ are birationally equivalent to complete Edwards curves, i.e., Edwards curves with non-square d. The formulas in [9] can therefore be used for elliptic-curve computations, and in particular for elliptic-curve cryptography.

Implementors can—although they are not forced to!—gain speed by switching from the addition formulas to dedicated doubling formulas when the inputs are known to be equal. Bernstein and Lange show, for typical scalar-multiplication problems, that their addition formulas and doubling formulas for Edwards curves use fewer multiplications than the best available formulas for previous curve shapes.

Our Contributions. In Chapter 8, we present a new shape for ordinary elliptic curves over fields of characteristic 2. Using the new shape, we present the first complete addition formulas for binary elliptic curves, i.e., addition formulas that work for all pairs of input points, with no exceptional cases. If $n \geq 3$ then the complete curves cover all isomorphism classes of ordinary elliptic curves over $\mathbb{F}_{2^n}$.

In this chapter, we also present dedicated doubling formulas for these curves. The doubling formulas are the first complete doubling formulas in the literature, with no exceptions for the neutral element, points of order 2, etc. Finally, we present complete formulas for differential addition, i.e., addition of points with known difference. Indeed, our doubling formulas and differential-addition formulas are extremely fast. The results of this chapter are based on [11].

Chapter 2

Mathematical Background

In this chapter we define the important notions that are used throughout this thesis. We also provide the mathematical background that is necessary for understanding the context of the number extractors based on curves and Jacobians.

We let $\mathbb{N}_0$ denote the set of non-negative integers and $\mathbb{R}_0$ the set of non-negative real numbers. A field is denoted by $\mathbb{F}$ and its algebraic closure by $\overline{\mathbb{F}}$. Further, let $\mathbb{F}^*$ denote the set of nonzero elements of $\mathbb{F}$. The finite field with q elements is denoted by $\mathbb{F}_q$, and its algebraic closure by $\overline{\mathbb{F}}_q$. The cardinality of a finite set S is denoted by $\#S$. We make a distinction between a variable $\mathbf{x}$ and a specific value x in $\mathbb{F}$.

2.1 Finite fields notation

Consider the finite field $\mathbb{F}_{q^n}$, where q is a prime power and n is a positive integer. Then $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_q$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This means that every element x in $\mathbb{F}_{q^n}$ can be uniquely represented by the form $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$, where $x_i \in \mathbb{F}_q$. We recall [75] that $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \ldots & \alpha_n^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_1^{q^{n-1}} & \ldots & \alpha_n^{q^{n-1}} \end{vmatrix} \neq 0.$$

Let $\phi : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$ be the Frobenius map defined by $\phi(x) = x^q$. Let $\phi^{(i)}$, for a positive integer i, be the i-th iterated function of ϕ. That is $\phi^{(i)}(x) = x^{q^i}$.

Let $x \in \mathbb{F}_{q^n}$. The *norm* and *trace* of x are defined by the formulas

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \prod_{i=0}^{n-1} \phi^{(i)}(x) \quad \text{and} \quad \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \sum_{i=0}^{n-1} \phi^{(i)}(x).$$

Now, we extend the definition of *norm* and *trace* to the field of fractions of a multivariate polynomial ring as follows.

Let $\overline{\mathbb{F}}_q(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ be the field of fractions of the polynomial ring $\overline{\mathbb{F}}_q[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$. We extend the Frobenius map ϕ from $\overline{\mathbb{F}}_q$ to $\overline{\mathbb{F}}_q(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ linearly by means of $\phi(\mathbf{x}_i) = \mathbf{x}_i$, for $1 \leq i \leq n$. Similarly, let $\phi^{(i)}$ be the i-th iterated function of ϕ. Clearly, f is a rational function defined over $\mathbb{F}_q$ if and only if $\phi(f) = f$.

Whenever the fields are clear from the context we omit the indices, i.e., we write $\mathrm{N}(x) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$ and $\mathrm{Tr}(x) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$ for $x \in \mathbb{F}_{q^n}$.

For a rational function f in $\mathbb{F}_{q^n}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$, we define

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) = \prod_{i=0}^{n-1} \phi^{(i)}(f) \quad \text{and} \quad \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) = \sum_{i=0}^{n-1} \phi^{(i)}(f).$$

We note that $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)$ and $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)$ belong to $\mathbb{F}_q(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$, where f is a rational function in $\mathbb{F}_{q^n}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$.

The following lemmas are similar to Hilbert's Theorem 90 and deal with the solvability of equations.

Lemma 2.1 *Let m be a positive integer dividing $q-1$. Let $x \in \mathbb{F}_{q^n}$. Then x is an m-th power in $\mathbb{F}_{q^n}$ if and only if $\mathrm{N}(x)$ is an m-th power in $\mathbb{F}_q$.*

Proof. Let α be a primitive element of $\mathbb{F}_{q^n}$. So every $x \in \mathbb{F}_{q^n}^*$ is a power of α. Then $\mathrm{N}(\alpha)$ is a primitive element of $\mathbb{F}_q$. Let $x \in \mathbb{F}_{q^n}^*$. Then x is an m-th power in $\mathbb{F}_{q^n}$ if and only if $x = \alpha^{mi}$, for some integer i. Similarly $\mathrm{N}(x)$ is an m-th power in $\mathbb{F}_q$ if and only if $\mathrm{N}(x) = (\mathrm{N}(\alpha))^{mi}$, for some integer i. Furthermore $x = \alpha^{mi}$, for some integer i, if and only if $\mathrm{N}(x) = (\mathrm{N}(\alpha))^{mj}$, for some integer j, since m divides $q-1$. Obviously $\mathrm{N}(0) = 0$. Therefore x is an m-th power in $\mathbb{F}_{q^n}$ if and only if $\mathrm{N}(x)$ is an m-th power in $\mathbb{F}_q$. □

Lemma 2.2 *Let $x \in \mathbb{F}_{q^n}$. Then $y^p - y = x$, for some $y \in \mathbb{F}_{q^n}$, if and only if $z^p - z = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$, for some $z \in \mathbb{F}_q$.*

Proof. Assume $y^p - y = x$, for some $y \in \mathbb{F}_{q^n}$. Let $z = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y)$. Clearly $z^p - z = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$. Now assume that $z^p - z = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$, for some $z \in \mathbb{F}_q$. Then

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(z^p - z) = 0.$$

Hence $x = y^p - y$, for some $y \in \mathbb{F}_{q^n}$ (see Theorem 2.25 [75]). □

2.2 Arithmetic of curves

In the sequel we briefly review the algebraic geometry background on curves that is needed for future discussions on curves. We refer to [23, 39, 51] for a general background to this section.

Affine and projective varieties. Affine n-space over $\mathbb{F}$, written $\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{F}})$, is the set of n-tuples of elements of $\overline{\mathbb{F}}$. Similarly, the set of $\mathbb{F}$-rational points in $\mathbb{A}^n$ is the set of n-tuples of elements of $\mathbb{F}$. Let f be in the polynomial ring $\overline{\mathbb{F}}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$. A point $P = (x_1, x_2, \ldots, x_n) \in \mathbb{A}^n(\overline{\mathbb{F}})$ is a zero of f if $f(P) = f(x_1, x_2, \ldots, x_n) = 0$. The set of zeros of f, where f is not constant, is called the *hypersurface* defined by f, and is denoted by V_f. If f is a polynomial of degree 1, then V_f is called a *hyperplane* in $\mathbb{A}^n(\overline{\mathbb{F}})$. More generally, if S is any set of polynomials in $\overline{\mathbb{F}}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$, then V_S equals the set of points $P \in \mathbb{A}^n(\overline{\mathbb{F}})$ such that $f(P) = 0$ for all $f \in S$. For any subset V of $\mathbb{A}^n(\overline{\mathbb{F}})$, the set of polynomials vanishing on V is an ideal in $\overline{\mathbb{F}}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$, called the *ideal* of V and written $I(V)$. A subset $V \subset \mathbb{A}^n(\overline{\mathbb{F}})$ is called an *affine algebraic set*, if $V = V_S$ for some S. An affine algebraic set V is defined over $\mathbb{F}$ if its ideal $I(V)$ can be generated by polynomials in $\mathbb{F}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$. If V is defined over $\mathbb{F}$, the set of $\mathbb{F}$-rational points of V is the set $V(\mathbb{F}) = V \cap \mathbb{A}^n(\mathbb{F})$.

The projective n-space over $\mathbb{F}$, denoted $\mathbb{P}^n$ or $\mathbb{P}^n(\overline{\mathbb{F}})$, is defined to be the set of all lines through $(0, 0, \ldots, 0)$ in $\mathbb{A}^{n+1}(\overline{\mathbb{F}})$. More precisely, $\mathbb{P}^n(\overline{\mathbb{F}})$ can be identified with the set of equivalence classes of points in $\mathbb{A}^{n+1}(\overline{\mathbb{F}}) \setminus \{(0, 0, \ldots, 0)\}$ where two points $(x_1, x_2, \ldots, x_{n+1})$ and $(y_1, y_2, \ldots, y_{n+1})$ are equivalent if there exist a $\gamma \in \overline{\mathbb{F}}$ such that $x_i = \gamma y_i$ for $i = 1, \ldots, n+1$. The equivalence classes are called *projective points*. A projective point is denoted by its representative as $(x_1 : x_2 : \ldots : x_{n+1})$. The set of $\mathbb{F}$-rational points in $\mathbb{P}^n$ is the set

$$\mathbb{P}^n(\mathbb{F}) = \{(x_1 : x_2 : \ldots : x_{n+1}) \in \mathbb{P}^n : \text{ all } x_i \in \mathbb{F}\}.$$

A polynomial F in $\overline{\mathbb{F}}[X_1, X_2, \ldots, X_{n+1}]$ is called homogeneous if it is a linear combination of monomials of the same degree. Then, the set

$$V_F = \left\{P \in \mathbb{P}^n(\overline{\mathbb{F}}) : F(P) = 0\right\}$$

is well defined, where F is homogeneous. The set V_F is called the *projective hypersurface* defined by a homogeneous polynomial F. For any set $V \subset \mathbb{P}^n(\overline{\mathbb{F}})$, the ideal of V, is the ideal generated by homogeneous polynomials vanish on V. A *projective algebraic set* is the set of simultaneous zeros of a set homogenous polynomials in $\overline{\mathbb{F}}[X_1, X_2, \ldots, X_{n+1}]$. A projective algebraic set V is defined over $\mathbb{F}$ if its ideal $I(V)$ can be generated by homogenous polynomials in $\mathbb{F}[X_1, X_2, \ldots, X_{n+1}]$. If V is defined over $\mathbb{F}$, the set of $\mathbb{F}$-rational points of V is the set $V(\mathbb{F}) = V \cap \mathbb{P}^n(\mathbb{F})$.

Let f be a polynomial of total degree d in $\overline{\mathbb{F}}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$. The process of *homogenization* maps f to a polynomial

$$F = X_{n+1}^d f(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}})$$

in $\overline{\mathbb{F}}[X_1, X_2, \ldots, X_{n+1}]$. For the reverse direction, let $F \in \overline{\mathbb{F}}[X_1, X_2, \ldots, X_{n+1}]$ be a homogenous polynomial of degree d. The process of replacing F by

$$F_i = F(\mathbf{x}_1, \ldots, \mathbf{x}_i, 1, \mathbf{x}_{i+1}, \ldots, \mathbf{x}_n) \in \mathbb{F}[\mathbf{x}_1, \ldots, \mathbf{x}_n]$$

is called *dehomogenization* with respect to X_i.

An affine (projective) algebraic set is irreducible if it is not the union of two smaller affine (projective) algebraic sets. An affine (projective) algebraic set is called an affine (projective) *variety* if it is irreducible. Further, a subset V is an affine (projective) variety if and only if $I(V)$ is a prime ideal.

The dimension of an affine (projective) variety V, written $\dim(V)$, is defined to be the supremum of the lengths of all chains $X_0 \supset X_1 \supset \cdots \supset X_n$ of distinct irreducible algebraic subsets X_i of V. A variety of dimension 1 is called a *curve*.

Let V be an affine variety defined over $\mathbb{F}$. Denote by $\mathbb{F}[V] = \mathbb{F}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]/I(V)$ the quotient ring of $\mathbb{F}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$ over the prime ideal $I(V)$. Then, $\mathbb{F}[V]$ is an integral domain, called the *coordinate ring* of V. The *function field* $\mathbb{F}(V)$ of V is the field of fractions of $\mathbb{F}[V]$. Similarly, $\overline{\mathbb{F}}[V]$ and $\overline{\mathbb{F}}(V)$ are defined by replacing $\mathbb{F}$ with $\overline{\mathbb{F}}$.

Nonsingularity. Let V be an affine variety defined over $\mathbb{F}$, and let $f_1, \ldots, f_t \in \mathbb{F}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$ be a set of generators for $I(V)$. The variety V is *nonsingular* at a *point* $P \in V$ if the rank of the matrix $((\partial f_i/\partial \mathbf{x}_j)(P))_{t \times n}$, called the Jacobian matrix at P, is $n - \dim(V)$. The variety V is *nonsingular* if it is nonsingular at every point.

For example, let $\mathcal{C}$ be an affine curve corresponding to a polynomial $f \in \mathbb{F}[\mathbf{x}, \mathbf{y}]$. A point $P = (x, y)$, where $f(x, y) = 0$, is a nonsingular point of $\mathcal{C}$ if $\partial(f)/\partial(\mathbf{x})(P) \neq 0$ or $\partial(f)/\partial(\mathbf{y})(P) \neq 0$. The curve $\mathcal{C}$ is nonsingular if it is nonsingular for all $P \in \mathbb{A}^2(\overline{\mathbb{F}})$, where $f(P) = 0$.

In case that $\mathcal{C}$ is a singular curve, we shall denote the nonsingular projective model of $\mathcal{C}$ by $\widetilde{\mathcal{C}}$. A morphism $\varphi : \widetilde{\mathcal{C}} \longrightarrow \mathcal{C}$ exists which is a local isomorphism

on the nonsingular points on $\mathcal{C}$. It is called the *resolution* or *normalization* of $\mathcal{C}$ (see [39, 51]).

We shall now continue with the arithmetic of curves. We recall some useful techniques for the computation of the *genus* of a curve. We also recall the Hasse-Weil Theorem for the number of points on curves over finite fields.

The delta invariant and the genus. The *genus* of a curve is a birational invariant which plays an important role in the geometry of algebraic curves. The *arithmetic genus* g of a plane curve of degree d, where d is the degree of a defining polynomial for the curve, is equal to $(d-1)(d-2)/2$. Here, we describe how the *geometric genus* g of the curve can be determined by computing the delta invariants of all singular points. First, we provide the definition of the *delta invariant* of a point on a curve.

Definition 2.3 *Let $\mathcal{C}$ be a reduced projective plane curve of degree d defined over an algebraically closed field $\mathbb{F}$. Let P be a point of $\mathcal{C}$. Let $\mathcal{O}_P$ be the local ring of all rational functions on $\mathcal{C}$ that are regular at P and $\widetilde{\mathcal{O}}_P$ be the normalization of $\mathcal{O}_P$ (see [23, 51]). The delta invariant of P is defined by*

$$\delta_P = \dim_{\mathbb{F}} \widetilde{\mathcal{O}}_P / \mathcal{O}_P.$$

The following Theorem is an extension of *Plücker's formula* for singular plane curves. It gives the genus of the nonsingular model of the curve in terms of the degree of the curve and $\sum_P \delta_P$, the summation of the delta invariants over all points of the curve. This sum is finite, since $\delta_P = 0$ for a nonsingular point P and the number of singular points on the curve is finite.

Theorem 2.4 *Let $\mathcal{C}$ be an absolutely irreducible projective plane curve of degree d. Then the geometric genus of the nonsingular model of $\mathcal{C}$ is*

$$g = \tfrac{1}{2}(d-1)(d-2) - \textstyle\sum_{P \in \mathcal{C}} \delta_P. \tag{2.1}$$

Proof. See ([51], Chapter IV, Exercise 1.8). □

In this thesis, by the genus of a curve we mean the geometric genus of that curve.

The Newton polygon and the genus. Here, we give an upper bound for the genus of a curve by means of the Newton polygon of the curve. Now, we provide the definition of the Newton polygon of a bi variate polynomial.

Definition 2.5 *Let $\mathbb{F}$ be a field and let*

$$F(\mathbf{x}, \mathbf{y}) = \sum_{(i,j) \in \mathcal{I}} a_{i,j} \mathbf{x}^i \mathbf{y}^j$$

be a bivariate polynomial, where $\mathcal{I}$ is a finite subset of $\mathbb{N}_0 \times \mathbb{N}_0$ and $a_{i,j} \in \mathbb{F}^*$ for all $(i,j) \in \mathcal{I}$. Denote by $\Gamma(F)$ the convex hull of the points $(i,j) \in \mathcal{I}$ in $\mathbb{R}_0 \times \mathbb{R}_0$. The set $\Gamma(F)$ is called the Newton Polygon of F and the boundary of F is denoted by $\partial\Gamma(F)$.

In the following theorem we recall *Baker's formula* [3, 62, 67] that gives an upper bound for the genus of an irreducible plane curve.

Theorem 2.6 *Let $\mathcal{C}$ be an irreducible curve defined by the equation $F(\mathbf{x},\mathbf{y}) = 0$ over an algebraic closed field. Then the genus of the nonsingular model of $\mathcal{C}$ satisfies*

$$g \leq 1 + area\ \Gamma(F) - \tfrac{1}{2}\#\left\{\, \partial\Gamma(F) \bigcap \mathbb{N}_0 \times \mathbb{N}_0 \,\right\}.$$

The right hand side of the above is equal to the number of integral points in the interior of $\Gamma(F)$.

Proof. See [6] or [67]. □

Example 2.7 Let $\mathcal{C}$ be a curve defined over $\mathbb{F}_{2^n}$ by the equation

$$f(\mathbf{x},\mathbf{y}) = (\mathbf{x}+\mathbf{y})(\mathbf{x}+\mathbf{y}+1) + \mathbf{x}\mathbf{y}(\mathbf{x}+1)(\mathbf{y}+1) = 0.$$

One can show that $\mathcal{C}$ is an absolutely irreducible curve. From the Newton polygon of f (see Figure 2.1), the genus g of $\mathcal{C}$ satisfies $g \leq 1$.

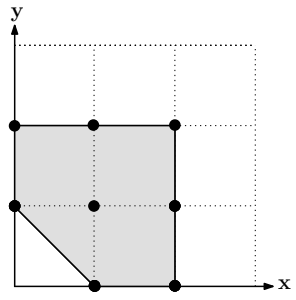


Figure 2.1: $\Gamma(f)$.

The Newton diagram. The Newton diagram corresponding to a singular point on a curve gives some information about this point, such as a lower bound for the delta invariant and the number of points lying over this point in the resolution map. Here, we define the notation of the Newton diagram of a bivariate polynomial.

Definition 2.8 *Let $\mathbb{F}$ be a field and let*

$$F(\mathbf{x},\mathbf{y}) = \sum_{(i,j)\in\mathcal{I}} a_{i,j}\mathbf{x}^i\mathbf{y}^j$$

be a polynomial in two variables, where $\mathcal{I}$ is a finite subset of $\mathbb{N}_0^2$ and $a_{i,j} \in \mathbb{F}^*$ for all $(i,j) \in \mathcal{I}$. Denote by $\Gamma_+(F)$ the convex hull of the union of the quadrants $(i,j)+\mathbb{R}_0^2$ in $\mathbb{R}_0^2$, for all $(i,j) \in \mathcal{I}$. The union of the compact edges of $\Gamma_+(F)$ is denoted by $\partial\Gamma_+(F)$. Then denote the closure of the set $\mathbb{R}_0^2 \setminus \Gamma_+(F)$ in $\mathbb{R}_0^2$ by $\Gamma_-(F)$. The boundary of $\Gamma_-(F)$ is denoted by $\partial\Gamma_-(F)$. The set $\Gamma_-(F)$ is called the Newton diagram *of F.*

Remark 2.9 Let $\mathcal{C}$ be a reduced plane curve that is defined by an equation $F(\mathbf{x},\mathbf{y}) = 0$ and let $P = (0,0)$ be a singular point on $\mathcal{C}$. Let $\Gamma_-(F)$ be the Newton diagram of F. Then $\delta_P \geq \nu_P$, where δ_P is the delta invariant of P and ν_P is equal to the number of unit-squares with integral vertices, so sets of the form $(m,n)+[0,1]^2, m,n \in \mathbb{N}_0^2$, contained in the $\Gamma_-(F)$. For more details see [6, Corollary 3.12].

Definition 2.10 *Let γ be a line segment of $\partial\Gamma_+(F)$ (see Definition 2.8) and let $\mathcal{I}_\gamma$ be the set of points on γ and $\mathcal{I}$. Define*

$$F_\gamma(\mathbf{x},\mathbf{y}) = \sum_{(i,j)\in\mathcal{I}_\gamma} a_{i,j}\mathbf{x}^i\mathbf{y}^j.$$

Remark 2.11 Let $\mathcal{C}$ be a reduced plane curve over $\mathbb{F}_q$ defined by the equation $F(\mathbf{x},\mathbf{y}) = 0$. Let $P = (0,0)$ be a singular point on $\mathcal{C}$. Let γ be the line segment of $\partial\Gamma_+(F)$ with endpoints (m_1,n_1) and (m_2,n_2). Let $m = m_2 - m_1$ and $n = n_1 - n_2$. Define $d = \gcd(m,n)$, $m' = \frac{m}{d}$ and $n' = \frac{n}{d}$. Then, there exist a unique univariate polynomial $f_\gamma(T) \in \mathbb{F}[T]$ of degree d such that $F_\gamma(\mathbf{x},\mathbf{y}) = \mathbf{x}^{m_2}\mathbf{y}^{n_2} f_\gamma(\mathbf{x}^{-m'}\mathbf{y}^{n'})$. The number of $\mathbb{F}_q$-rational points on the nonsingular model of $\mathcal{C}$, lying over P in the resolution map, is at most d and depends on the coefficients of the polynomial F_γ or the roots of f_γ in $\mathbb{F}$ (see [6, Remark 3.16 and 3.18]).

The number of points on a curve. Let $\mathcal{C}$ be an absolutely irreducible projective plane curve of degree d defined over the finite field $\mathbb{F}_q$.

In case that $\mathcal{C}$ is a nonsingular curve with genus g, the well-known Hasse-Weil bound gives the following estimate for the number of $\mathbb{F}_q$-rational points on $\mathcal{C}$.

$$|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}. \tag{2.2}$$

A sharper estimate by Serre [88] is

$$|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq g\lfloor 2\sqrt{q}\rfloor.$$

In case that $\mathcal{C}$ is a singular curve, we consider the resolution of $\mathcal{C}$. For an $\mathbb{F}_q$-rational point P on $\mathcal{C}$, let ϑ_P be the number of $\mathbb{F}_q$-rational points on $\widetilde{\mathcal{C}}$, lying over P in the resolution map φ. Then

$$\#\widetilde{\mathcal{C}}(\mathbb{F}_q) - \#\mathcal{C}(\mathbb{F}_q) = \sum_{P \in \mathcal{C}(\mathbb{F}_q)} (\vartheta_P - 1).$$

Let $\mathcal{C}_s(\mathbb{F}_q)$ be the set of singular points of $\mathcal{C}(\mathbb{F}_q)$. For a nonsingular point P we have $\vartheta_P = 1$. Hence,

$$\#\widetilde{\mathcal{C}}(\mathbb{F}_q) - \#\mathcal{C}(\mathbb{F}_q) = \sum_{P \in \mathcal{C}_s(\mathbb{F}_q)} (\vartheta_P - 1).$$

Example 2.12 Let $\mathcal{C}$ be the curve that is defined in Example 2.7. The projective model of $\mathcal{C}$, written $\overline{\mathcal{C}}$, is defined by the equation

$$F(X, Y, Z) = (X + Y)(X + Y + Z)Z^2 + XY(X + Z)(Y + Z) = 0.$$

The points $P_1 = (1 : 0 : 0)$ and $P_2 = (0 : 1 : 0)$, called the points at infinity, are the only singular points of $\overline{\mathcal{C}}$. Now, we compute ϑ_{P_1} by means of the Newton diagram corresponding to P_1. From the process of dehomogenization with respect to X, we consider the polynomial $F_1(\mathbf{y}, \mathbf{z}) = (\mathbf{y} + 1)(\mathbf{y} + \mathbf{z} + 1)\mathbf{z}^2 + \mathbf{y}(\mathbf{z} + 1)(\mathbf{y} + \mathbf{z})$.

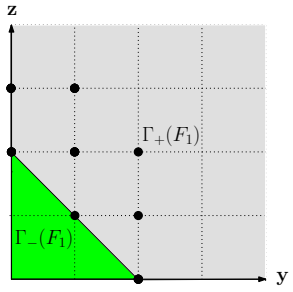


Figure 2.2: $\Gamma_-(F_1), \Gamma_+(F_1)$.

Let γ be the line segment of Diagram 2.2 with endpoints $(0, 2)$ and $(2, 0)$. Then, $F_\gamma(\mathbf{y}, \mathbf{z}) = \mathbf{y}^2 + \mathbf{yz} + \mathbf{z}^2 = \mathbf{y}^2 f_\gamma(\mathbf{z}/\mathbf{y})$, where $f_\gamma(T) = T^2 + T + 1 \in \mathbb{F}_{2^n}[T]$. Then, the number of roots of f_γ in $\mathbb{F}_{2^n}$ implies that $\vartheta_{P_1} = 2$, if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1) = 0$, and $\vartheta_{P_1} = 0$, if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(1) = 1$. Because of the symmetry between $\mathbf{x}$ and $\mathbf{y}$, we have $\vartheta_{P_1} = \vartheta_{P_2}$. Therefore, if n is odd, the number of $\mathbb{F}_{2^n}$-rational points on $\mathcal{C}$ equals the number of $\mathbb{F}_{2^n}$-rational points on the nonsingular model of $\mathcal{C}$.

2.3 Elliptic curves

Now, we briefly review the background on elliptic curves to the extent needed in this thesis. For a more general presentation of elliptic curves, see [23, 50, 91, 97].

Definition 2.13 *A nonsingular absolutely irreducible projective curve defined over $\mathbb{F}$ of genus 1 with at least one $\mathbb{F}$-rational point is called an elliptic curve over $\mathbb{F}$.*

An elliptic curve E over $\mathbb{F}$ can be given by the so-called Weierstrass equation

$$E : \mathbf{y}^2 + a_1\mathbf{xy} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6, \tag{2.3}$$

where the coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. We note that E has to be nonsingular. The set of $\mathbb{F}$-rational points on E, written $E(\mathbb{F})$, is defined by the set of points $(x, y) \in \mathbb{F} \times \mathbb{F}$ satisfying Equation 2.3 plus the point at infinity, written P_∞. The set of $\mathbb{F}$-rational points on E by means of the chord-tangent process turns $E(\mathbb{F})$ into an abelian group with P_∞ as the neutral element. For finite fields $\mathbb{F}_q$ the subgroups of $E(\mathbb{F}_q)$ are used for cryptosystems based on the Discrete Logarithm problem. The use of elliptic curves in public-key cryptography can offer improved efficiency and bandwidth.

Let E be a curve defined over $\mathbb{F}$ by Equation 2.3. The discriminant of the curve E, denoted by Δ_E, satisfies

$$\Delta_E = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6,$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1 a_3 + 2a_4,$$
$$b_6 = a_3^2 + 4a_6, \quad b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2.$$

The curve E is nonsingular, and thus is an elliptic curve, if and only if Δ_E is nonzero. In this case, the j-invariant of E is defined by $j(E) = (b_2^2 - 24b_4)^3/\Delta_E$. If two elliptic curves E_1, E_2 over $\mathbb{F}$ are isomorphic then they have the same j-invariant. Conversely, if $j(E_1) = j(E_2)$, then E_1 and E_2 are isomorphic over $\overline{\mathbb{F}}$.

An elliptic curve E can be defined via the short Weierstrass form. This actually depends on the characteristic of the field and on the value of the j-invariant. All the cases and equations are summarized in Table 2.1.

There are many other ways to represent an elliptic curve such as *Legendre form*, *Jacobi model*, *Hessian form*, the intersection of two quadratic surfaces and so on (see e.g. [23, Chapter 13] or [97, Chapter 2]). In [36], the explicit formulas are given for the number of distinct elliptic curves (up to isomoroprism) in several families of curves of cryptographic interest.

char($\mathbb{F}$)	Equation	Δ_E	$j(E)$
$\neq 2, 3$	$\mathbf{y}^2 = \mathbf{x}^3 + a_4\mathbf{x} + a_6$	$-16(4a_4^3 + 27a_6^2)$	$1728a_4^3/4\Delta_E$
3	$\mathbf{y}^2 = \mathbf{x}^3 + a_4\mathbf{x} + a_6$	$-a_4^3$	0
3	$\mathbf{y}^2 = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_6$	$-a_2^3 a_6$	$-a_2^3/a_6$
2	$\mathbf{y}^2 + a_3\mathbf{y} = \mathbf{x}^3 + a_4\mathbf{x} + a_6$	a_3^4	0
2	$\mathbf{y}^2 + \mathbf{xy} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_6$	a_6	$1/a_6$

Table 2.1: Short Weierstrass equations.

Further, several coordinate systems are proposed to improve the efficiency and the speed of the addition and doubling formulas in the group of points on elliptic curves over finite fields (see e.g. [8, 23, 50] and references therein).

2.3.1 Edwards curve

Recently, Edwards [26] introduced a new form for elliptic curves. He showed that every elliptic curve over a field $\mathbb{F}$ with char($\mathbb{F}$) $\neq 2$ is birationally equivalent (in an appropriate sense) to one in the form $\mathbf{x}^2+\mathbf{y}^2 = c^2(1+\mathbf{x}^2\mathbf{y}^2)$, where c is a constant in $\mathbb{F}$ such that $c^5 \neq c$. The simple addition law on this form is given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{c(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)} \right).$$

After that, Bernstein and Lange [9] proposed a slightly generalized form

$$\mathbf{x}^2 + \mathbf{y}^2 = c^2(1 + d\mathbf{x}^2\mathbf{y}^2),$$

called *Edwards curve*, for elliptic curves over $\mathbb{F}$ with char($\mathbb{F}$) $\neq 2$. The addition law on Edwards curve is similar to that of the original Edwards curve. If c and d are nonzero constants in $\mathbb{F}$ such that $dc^4 \neq 1$, the addition law is given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \right).$$

The point $(0, 1)$ is the neutral element of the addition law. The negative of a point $P = (x_1, y_1)$ can be computed by reflecting the x-coordinate across the y-axis: $-P = (-x_1, y_1)$. The addition law is strongly unified; i.e., the same formulas can also be used for doubling. If d is not a square then the addition law is complete; i.e., the addition law holds for all inputs.

A sequence of papers [7, 9, 10] showed that, for cryptographic applications, Edwards curves involve significantly fewer multiplications than short Weierstrass form curves in Jacobian coordinates, which so far was considered as the faster system.

In Chapter 8, we generalize the idea of Edwards curve to fields with characteristic 2.

2.4 Weil descent

Weil descent is a well known technique in algebraic geometry. It relates a geometric d-dimensional object over a field $\mathbb{K}$ to a nd-dimensional object over a field $\mathbb{F}$, where $\mathbb{K}$ is a field of degree n over $\mathbb{F}$. The use of Weil descent technique is suggested by Frey [38] for cryptographic applications such as DL system.

Here we explain the easiest case. Let $\mathbb{K}$ be a field extension of degree n over $\mathbb{F}$ and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of $\mathbb{K}$ over $\mathbb{F}$. Let V be an affine variety in $\mathbb{A}^d(\mathbb{K})$ defined by the m equations

$$F_i(\mathbf{x}_1, \ldots, \mathbf{x}_d) = 0, \text{ for } i = 1, \ldots, m,$$

with $F_i \in \mathbb{K}[\mathbf{x}_1, \ldots, \mathbf{x}_d]$. Then, we consider dn variables $\mathbf{y}_{i,j}$ by $\mathbf{x}_i = \sum_{j=1}^{n} \alpha_j \mathbf{y}_{i,j}$. We replace the variables $\mathbf{x}_i$ in the equations defining V by these expressions. Next, we write the coefficients of the resulting relations as $\mathbb{F}$-linear combinations of the basis $\{\alpha_1, \ldots, \alpha_n\}$ and order these relations according to this basis. As result we obtain the m equations

$$G_i(\mathbf{y}_{1,1}, \ldots, \mathbf{y}_{d,n}) = \sum_{j=1}^{n} \alpha_j g_{i,j}(\mathbf{y}_{1,1}, \ldots, \mathbf{y}_{d,n}) = 0,$$

where $g_{i,j} \in \mathbb{F}[\mathbf{y}_{1,1}, \ldots, \mathbf{y}_{d,n}]$. The Weil descent of V over $\mathbb{F}$, written $W_{\mathbb{K}/\mathbb{F}}(V)$, is defined by the mn equations

$$g_{i,j}(\mathbf{y}_{1,1}, \ldots, \mathbf{y}_{d,n}) = 0, \text{ for } i = 1, \ldots, m, \ j = 1, \ldots, n.$$

Example 2.14 Let $\mathcal{C}$ be an affine curve over $\mathbb{F}_{2^{2\ell}}$ given by the equation

$$\mathbf{y}^2 + \mathbf{xy} = f(\mathbf{x}),$$

where ℓ is a positive integer and f is a polynomial in $\mathbb{F}_{2^{2\ell}}[\mathbf{x}]$. Consider $\mathbb{F}_{2^{2\ell}}$ as a quadratic extension of $\mathbb{F}_{2^\ell}$ with a basis $\{1, t\}$, where $t^2 + t + c = 0$ for an element $c \in \mathbb{F}_{2^\ell}$. So, for all x in $\mathbb{F}_{2^n}$, we can write $x = x_0 + x_1 t$, where x_0 and x_1 are in $\mathbb{F}_{2^\ell}$. Here, we compute the Weil descent $W_{\mathbb{F}_{2^{2\ell}}/\mathbb{F}_{2^\ell}}(\mathcal{C})$ of $\mathcal{C}$. We consider the variables $\mathbf{x}_0$, $\mathbf{x}_1$, $\mathbf{y}_0$ and $\mathbf{y}_1$ by $\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_1 t$ and $\mathbf{y} = \mathbf{y}_0 + \mathbf{y}_1 t$. Then $\mathbf{y}^2 + \mathbf{xy} = f(\mathbf{x})$ becomes

$$(\mathbf{y}_0 + \mathbf{y}_1 t)^2 + (\mathbf{x}_0 + \mathbf{x}_1 t)(\mathbf{y}_0 + \mathbf{y}_1 t) = f(\mathbf{x}_0 + \mathbf{x}_1 t).$$

After expansion this is of the form

$$\mathbf{y}_0^2 + c\mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_0 + c\mathbf{x}_1\mathbf{y}_1 + (\mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_1 + \mathbf{x}_1\mathbf{y}_0 + \mathbf{x}_1\mathbf{y}_1)t = f_0(\mathbf{x}_0, \mathbf{x}_1) + f_1(\mathbf{x}_0, \mathbf{x}_1)t,$$

where f_0 and f_1 are in $\mathbb{F}_{2^\ell}[\mathbf{x}_0, \mathbf{x}_1]$. Hence, the Weil descent $W_{\mathbb{F}_{2^{2\ell}}/\mathbb{F}_{2^\ell}}(\mathcal{C})$ of $\mathcal{C}$ is defined by the following system of equations.

$$\begin{cases} \mathbf{y}_0^2 + c\mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_0 + c\mathbf{x}_1\mathbf{y}_1 + f_0(\mathbf{x}_0, \mathbf{x}_1) = 0 \\ \mathbf{y}_1^2 + \mathbf{x}_0\mathbf{y}_1 + \mathbf{x}_1\mathbf{y}_0 + \mathbf{x}_1\mathbf{y}_1 + f_1(\mathbf{x}_0, \mathbf{x}_1) = 0. \end{cases} \tag{2.4}$$

Note that from a set theoretic point of view $W_{\mathbb{F}_{2^{2\ell}}/\mathbb{F}_{2^\ell}}(\mathcal{C})(\mathbb{F}_{2^\ell}) = \mathcal{C}(\mathbb{F}_{2^{2\ell}})$.

2.5 Hyperelliptic curves

Now, we recall the definition of hyperelliptic curves. For a more general background on hyperelliptic curves we refer to [23] and the references therein.

Definition 2.15 *An absolutely irreducible nonsingular projective curve H of genus at least 2 is called* hyperelliptic *if there exists a morphism of degree 2 from H to the projective line.*

The following theorem describes plane singular models of hyperelliptic curves defined over $\mathbb{F}_q$.

Theorem 2.16 *Let H be a hyperelliptic curve of genus g over $\mathbb{F}_q$. Then, if q is odd, H has a plane model of the form*

$$\mathbf{y}^2 = f(\mathbf{x}),$$

where f is a square free polynomial in $\mathbb{F}_q[\mathbf{x}]$ and $2g + 1 \leq \deg(f) \leq 2g + 2$. The plane model is singular at infinity. If $\deg(f) = 2g + 1$ then the point at infinity ramifies and H has only one point at infinity. If $\deg(f) = 2g + 2$ then H has zero or two $\mathbb{F}_q$-rational points at infinity.

If q is even, H has a plane model of the form

$$\mathbf{y}^2 + h(\mathbf{x})\mathbf{y} = f(\mathbf{x}),$$

where h, f are polynomials in $\mathbb{F}_q[\mathbf{x}]$, f monic and either $\deg(h) \leq g$, $\deg(f) = 2g+1$ or $\deg(h) = g + 1$, $\deg(f) \leq 2g + 2$. Furthermore, if $y^2 + h(x)y = f(x)$ for $(x, y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$, then $2y + h(x) \neq 0$ or $h'(x)y - f'(x) \neq 0$. The plane model is singular at infinity. If $\deg(f) = 2g + 1$, $\deg(h) \leq g$ then the point at infinity ramifies and H has only one point at infinity. If $\deg(f) \leq 2g + 2$, $\deg(h) = g + 1$ then H has zero or two $\mathbb{F}_q$-rational points at infinity.

Proof. See [2]. □

In this thesis, we concentrate on hyperelliptic curves with exactly one point at infinity. They are called *imaginary hyperelliptic* curves.

Definition 2.17 *An imaginary hyperelliptic curve H of genus g over $\mathbb{F}_q$ is defined by an equation of the form*

$$\mathbf{y}^2 + h(\mathbf{x})\mathbf{y} = f(\mathbf{x}),$$

where $h, f \in \mathbb{F}_q[\mathbf{x}]$, f is monic, $\deg(f) = 2g+1$, $\deg(h) \leq g$.

For any subfield $\mathbb{F}$ of $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$, the set

$$H(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 + h(x)y = f(x)\} \cup \{P_\infty\},$$

is called the set of $\mathbb{F}$-*rational points* on H. The point P_∞ is called the *point at infinity* for H. A point P on H, also written $P \in H$, is a point $P \in H(\overline{\mathbb{F}}_q)$. The opposite of a point $P = (x, y)$ on H is defined by the hyperelliptic involution σ as $\sigma(P) = (x, -h(x) - y)$ and $\sigma(P_\infty) = P_\infty$.

2.6 The Jacobian of hyperelliptic curves

For elliptic curves one can take the set of points together with the point at infinity as a group. This is no longer possible for hyperelliptic curves. Instead, a group law is defined via the set of $\mathbb{F}_q$-rational point of the Jacobian of H over $\mathbb{F}_q$, denoted by $J(\mathbb{F}_q)$. One can efficiently compute the sum of two points in the Jacobian of H over $\mathbb{F}_q$, using the algorithms described in [17, 23, 66]. There are two isomorphic representations of the Jacobian of an imaginary hyperelliptic curve H, namely as the divisor class group of H and as the ideal class group of the maximal order in the function field of H. The latter representation is often called Mumford representation [84].

First, we define the notion of the Jacobian in terms of the divisor class group. Let H be an imaginary hyperelliptic curve defined over $\mathbb{F}_q$. A *divisor* D on H is a formal sum of points on $H(\overline{\mathbb{F}}_q)$, $D = \sum_{P \in H} m_P P$, where the $m_P \in \mathbb{Z}$ are zero except for a finite number of $P \in H(\overline{\mathbb{F}}_q)$. The *degree* of D is defined by $\deg D = \sum_{P \in H} m_P$. Let $\mathbb{F}$ be a subfield of $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$. A divisor D is said to be *defined over* $\mathbb{F}$, if for all automorphisms φ in the Galois group of $\mathbb{F}$, $\varphi(D) = \sum_{P \in H} m_P \, \varphi(P)$ is equal to D, where $\varphi(P) = (\varphi(x), \varphi(y))$ if $P = (x, y)$ and $\varphi(P_\infty) = P_\infty$.

The set of all divisors on H defined over $\mathbb{F}$, denoted by $Div(\mathbb{F})$, forms an additive abelian group under the addition rule

$$\sum_{P \in H} m_P P + \sum_{P \in H} n_P P = \sum_{P \in H} (m_P + n_P) P.$$

The set $Div^0(\mathbb{F})$ of all divisors on H of degree zero defined over $\mathbb{F}$ is a subgroup of $Div(\mathbb{F})$.

Let $\mathbb{F}[H] = \mathbb{F}[\mathbf{x}, \mathbf{y}]/(\mathbf{y}^2 + h(\mathbf{x})\mathbf{y} - f(\mathbf{x}))$ be the *coordinate ring* of H *over* $\mathbb{F}$. Then the *function field* of H over $\mathbb{F}$ is the field of fractions $\mathbb{F}(H)$ of $\mathbb{F}[H]$. For a non-zero element R in $\mathbb{F}[H]$, the divisor of R is defined by $\mathrm{div}(R) = \sum_{P \in H} \mathrm{ord}_P(R)P$, where $\mathrm{ord}_P(R)$ is the order of vanishing of R at P. For a rational function $R = F/G$, where F, $G \in \mathbb{F}[H]$, the divisor of R is defined by $\mathrm{div}(R) = \mathrm{div}(F) - \mathrm{div}(G)$ and is called a *principal divisor*. The *group of principal divisors* on H *over* $\mathbb{F}$ is denoted by $\mathcal{P}(\mathbb{F}) = \{\mathrm{div}(R) : R \in \mathbb{F}(H)\}$.

Definition 2.18 *The divisor class group of* H over $\mathbb{F}$ *is the quotient group*

$$Div^0(\mathbb{F})/\mathcal{P}(\mathbb{F}).$$

This group is also called Picard group of H*.*

The *Jacobian* of H over $\mathbb{F}_q$, denoted by J, is an abelian variety of dimension g. In particular, the set of $\mathbb{F}$-rational points of the Jacobian of H over $\mathbb{F}$, denoted by $J(\mathbb{F})$ is a group which is isomorphic to the divisor class group of H over $\mathbb{F}$.

For each nontrivial point on the Jacobian of H over $\mathbb{F}$ there exists a unique divisor D on H defined over $\mathbb{F}$ of the form

$$D = \sum_{i=1}^{r} P_i - rP_\infty,$$

where $P_i = (x_i, y_i) \in H(\overline{\mathbb{F}})$, $P_i \neq P_\infty$ and $P_i \neq \sigma(P_j)$, for $i \neq j$, $r \leq g$. Such a divisor is called a *reduced* divisor on H over $\mathbb{F}$. By means of Mumford representation [84], each nontrivial point on $J(\mathbb{F})$ can be uniquely represented by a pair of polynomials $[u(\mathbf{x}), v(\mathbf{x})]$, $u, v \in \mathbb{F}[\mathbf{x}]$, where u is monic, $\deg(v) < \deg(u) \leq g$ and u divides $v^2 + hv - f$. The neutral element of $J(\mathbb{F})$, denoted by $\mathcal{O}$, is represented by $[1, 0]$.

Hasse-Weil Theorem for the Jacobians. Let H be a genus-g hyperelliptic curve defined over a finite field $\mathbb{F}_q$ and let $J(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational points of the Jacobian of H over $\mathbb{F}_q$. The Hasse-Weil Theorem gives bounds on the number of points on H over $\mathbb{F}_q$ (see Equation 2.2). Further, by means of the Hasse-Weil Theorem, we have bounds on the group order of the divisor class group. The following bounds depend only on the finite field and the genus of the curve:

$$(\sqrt{q} - 1)^{2g} \leq \#J(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}.$$

2.6.1 On the Jacobian of genus-2 curves

In Chapters 6 and 7, we consider genus-2 imaginary hyperelliptic curves. We now summarize the main properties and notions on the Jacobian of these curves.

Let H be an imaginary hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$. Let $J(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational points of the Jacobian of H over $\mathbb{F}_q$. We partition $J(\mathbb{F}_q)$ as $J(\mathbb{F}_q) = J_0 \cup J_1 \cup J_2$, where $J_0 = \{\mathcal{O}\}$ and J_r, for $r = 1, 2$ is defined as

$$J_r = \left\{ D \in J(\mathbb{F}_q) : D = \sum_{i=1}^{r} P_i - rP_\infty \right\}.$$

Let $D \in J(\mathbb{F}_q)$. Note that $\phi(D) = D$, where $\phi : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q$ is the Frobenius map defined by $\phi(x) = x^q$ and extended to the Jacobian of H as above. Let D have Mumford representation $D = [u(\mathbf{x}), v(\mathbf{x})]$, for some $u, v \in \overline{\mathbb{F}}_q[\mathbf{x}]$. Then $D \in J_r$ if and only if $\deg(u) = r$ and u, v are defined over $\mathbb{F}_q$. We shall explain this in more detail.

If $D \in J_1$, then $D = P - P_\infty$, where $P \neq P_\infty$ and $P = (x_P, y_P) \in H(\mathbb{F}_q)$. Furthermore, D is represented by $[\mathbf{x} - x_P, y_P]$.

If $D \in J_2$, then $D = P_1 + P_2 - 2P_\infty$ for some points P_1, P_2, where $P_1, P_2 \neq P_\infty$ and $P_1 \neq \sigma(P_2)$. Furthermore, D is represented by $[u(\mathbf{x}), v(\mathbf{x})]$, where $u(\mathbf{x}) = (\mathbf{x} - x_{P_1})(\mathbf{x} - x_{P_2})$, $v(x_{P_1}) = y_{P_1}$ and $v(x_{P_2}) = y_{P_2}$. There are two possibilities for D:

- First, $\phi(P_1) = P_1$. Since $\phi(D) = D$, we have $\phi(P_2) = P_2$. So, P_1, $P_2 \in H(\mathbb{F}_q)$. Hence, $x_{P_1}, x_{P_2} \in \mathbb{F}_q$. So, in this case, u is a reducible polynomial over $\mathbb{F}_q$.
- Secondly, $\phi(P_1) \neq P_1$. Since $\phi(D) = D$, it follows that $\phi(P_1) = P_2$ and $\phi(P_2) = P_1$. So, $\phi(\phi(P_1)) = P_1$, $\phi(P_1) \neq P_1$ and $\phi(P_1) \neq \sigma(P_1)$. Hence, $P_1 \in H(\mathbb{F}_{q^2})$ and $x_{P_1} \notin \mathbb{F}_q$. If $x_{P_1} \in \mathbb{F}_q$, then $\phi(P_1) = (\phi(x_{P_1}), \phi(y_{P_1})) = (x_{P_1}, \phi(y_{P_1}))$, so $\phi(P_1)$ is equal to either P_1 or $\sigma(P_1)$, which is a contradiction. Hence, u is an irreducible polynomial over $\mathbb{F}_q$.

2.7 Kummer surface

Now, we briefly recall the notion of a Kummer surface associated to the Jacobian of genus-2 hyperelliptic curves. For the general background, we refer to [18].

Let H be an imaginary hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$, for odd q. Then H has a plane model of the form

$$\mathbf{y}^2 = f(\mathbf{x}) = \mathbf{x}^5 + f_4\mathbf{x}^4 + f_3\mathbf{x}^3 + f_2\mathbf{x}^2 + f_1\mathbf{x} + f_0, \tag{2.5}$$

where $f_i \in \mathbb{F}_q$ and f is a square-free polynomial. Associated with the curve H, there exists a quartic surface $\mathcal{K}$ in $\mathbb{P}^3$, called the *Kummer surface*, which is given by the equation

$$A(k_1, k_2, k_3)k_4^2 + B(k_1, k_2, k_3)k_4 + C(k_1, k_2, k_3) = 0,$$

where

$$\begin{aligned}
A(k_1, k_2, k_3) =& k_2^2 - 4k_1k_3, \\
B(k_1, k_2, k_3) =& -2(2f_0k_1^3 + f_1k_1^2k_2 + 2f_2k_1^2k_3 + f_3k_1k_2k_3 + 2f_4k_1k_3^2 + k_2k_3^2), \\
C(k_1, k_2, k_3) =& -4f_0f_2k_1^4 + f_1^2k_1^4 - 4f_0f_3k_1^3k_2 - 2f_1f_3k_1^3k_3 - 4f_0f_4k_1^2k_2^2 \\
&+ 4f_0k_1^2k_2k_3 - 4f_1f_4k_1^2k_2k_3 + 2f_1k_1^2k_3^2 - 4f_2f_4k_1^2k_3^2 + f_3^2k_1^2k_3^2 \\
&- 4f_0k_1k_2^3 - 4f_1k_1k_2^2k_3 - 4f_2k_1k_2k_3^2 - 2f_3k_1k_3^3 + k_3^4.
\end{aligned}$$

Let J be the Jacobian of H over $\mathbb{F}_q$ (see Subsection 2.6.1). Then there exists a particular map

$$\kappa : J(\mathbb{F}_q) \longrightarrow \mathcal{K}(\mathbb{F}_q),$$

where $\kappa(D) = \kappa(-D)$, for all $D \in J(\mathbb{F}_q)$ and $\kappa(\mathcal{O}) = (0, 0, 0, 1)$. This map does not preserve the group structure, however, it endows a pseudo-group structure upon $\mathcal{K}$ (see [18]). In particular, a scalar multiplication on the image of κ is defined by

$$m\kappa(D) = \kappa(mD),$$

for $m \in \mathbb{Z}$ and $D \in J(\mathbb{F}_q)$. Furthermore, the above definition can be extended to have a scalar multiplication on $\mathcal{K}$, since each point on $\mathcal{K}$ can be pulled back to the Jacobian of H or to the Jacobian of the quadratic twist of H. So, the Kummer surface $\mathcal{K}$ could be used for a Diffie-Hellman key exchange protocol (see [93]).

2.8 A surface related to the Jacobian in odd characteristic

In this section we introduce a surface related to the Jacobian of a genus-2 hyperelliptic curve over a finite field with odd characteristic. The result of this section will be used as mathematical background for the proofs of main theorems in Chapter 6.

Let H be an imaginary genus-2 hyperelliptic curve over $\mathbb{F}_q$, where q is odd. Then H has a plane model of the form

$$\mathbf{y}^2 = f(\mathbf{x}) = \prod_{i=1}^{5}(\mathbf{x} - \lambda_i), \tag{2.6}$$

where the λ_i's are pairwise distinct elements of $\overline{\mathbb{F}}_q$. Let $J(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational points of the Jacobian of H over $\mathbb{F}_q$ (see Subsection 2.6.1). The neutral element of $J(\mathbb{F}_q)$ is denoted by $\mathcal{O}$. Let H^t be a quadratic twist of H that has a plane model of the form

$$\alpha \mathbf{y}^2 = f(\mathbf{x}), \tag{2.7}$$

where α is a non-square element of $\mathbb{F}_q$. Let J^t be the Jacobian of H^t over $\mathbb{F}_q$.

We define the bivariate polynomial $\Phi \in \mathbb{F}_q[\mathbf{x}_1, \mathbf{x}_2]$ by

$$\Phi(\mathbf{x}_1, \mathbf{x}_2) = f(\mathbf{x}_1) f(\mathbf{x}_2).$$

Clearly, Φ is a symmetric polynomial. From Equation (2.6), we obtain

$$\Phi(\mathbf{x}_1, \mathbf{x}_2) = \prod_{i=1}^{5} (\mathbf{x}_1 - \lambda_i)(\mathbf{x}_2 - \lambda_i) = \prod_{i=1}^{5} (\mathbf{x}_1 \mathbf{x}_2 - \lambda_i(\mathbf{x}_1 + \mathbf{x}_2) + \lambda_i^2).$$

We define the bivariate polynomial Ψ in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ by

$$\Psi(\mathbf{a}, \mathbf{b}) = \prod_{i=1}^{5} (\mathbf{b} - \lambda_i \mathbf{a} + \lambda_i^2). \tag{2.8}$$

Definition 2.19 *Let $\mathcal{R}$ be the affine surface defined over $\mathbb{F}_q$ by the equation*

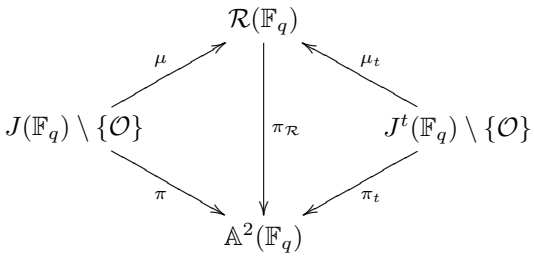
$$\mathbf{z}^2 = \Psi(\mathbf{a}, \mathbf{b}).$$

Let S_2 be the symmetric group acting on $\{1, 2\}$. It acts in a natural way on $H \times H$. Then, one can see that $\mathcal{R} = (H \times H)/(\langle (\sigma, \sigma) \rangle \times S_2)$, where σ is the hyperelliptic involution. The surface $\mathcal{R}$ is almost the same as the Kummer surface $\mathcal{K}$ associated to the Jacobian of H.

Remark 2.20 Let $D \in J(\mathbb{F}_q)$ be represented by $D = P_1 + P_2 - 2P_\infty$, where $P_1, P_2 \in H(\overline{\mathbb{F}}_q)$, $P_1, P_2 \neq P_\infty$ and $P_1 \neq \sigma(P_2)$. Then, $y_{P_1}^2 = f(x_{P_1})$ and $y_{P_2}^2 = f(x_{P_2})$. Let $z = y_{P_1} y_{P_2}$. Then, $z^2 = \Phi(x_{P_1}, x_{P_2})$. Let $a = x_{P_1} + x_{P_2}, b = x_{P_1} x_{P_2}$. Then $z^2 = \Psi(a, b)$. This means that (a, b, z) is a point of $\mathcal{R}$. Furthermore, $(a, b, z) \in \mathcal{R}(\mathbb{F}_q)$.

Remark 2.21 Let $D \in J^t(\mathbb{F}_q)$ be represented by $D = P_1 + P_2 - 2P_\infty$, where P_1, P_2 are points on $H^t(\overline{\mathbb{F}}_q)$, $P_1, P_2 \neq P_\infty$ and $P_1 \neq \sigma(P_2)$. So, $\alpha y_{P_1}^2 = f(x_{P_1})$ and $\alpha y_{P_2}^2 = f(x_{P_2})$. Let $z = \alpha y_{P_1} y_{P_2}$. Then $z^2 = \Phi(x_{P_1}, x_{P_2})$. Let $a = x_{P_1} + x_{P_2}, b = x_{P_1} x_{P_2}$. Then $z^2 = \Psi(a, b)$ and hence $(a, b, z) \in \mathcal{R}(\mathbb{F}_q)$.

We now consider the following diagram:



(2.9)

where

$$\begin{aligned}
\mu : J(\mathbb{F}_q) \setminus \{\mathcal{O}\} &\longrightarrow \mathcal{R}(\mathbb{F}_q) \\
P_1 + P_2 - 2P_\infty &\longmapsto (x_{P_1} + x_{P_2}, x_{P_1}x_{P_2}, y_{P_1}y_{P_2}) \\
P_1 - P_\infty &\longmapsto (2x_{P_1}, x_{P_1}^2, y_{P_1}^2),
\end{aligned}$$

$$\begin{aligned}
\mu_t : J^t(\mathbb{F}_q) \setminus \{\mathcal{O}\} &\longrightarrow \mathcal{R}(\mathbb{F}_q) \\
P_1 + P_2 - 2P_\infty &\longmapsto (x_{P_1} + x_{P_2}, x_{P_1}x_{P_2}, \alpha y_{P_1}y_{P_2}) \\
P_1 - P_\infty &\longmapsto (2x_{P_1}, x_{P_1}^2, \alpha y_{P_1}^2),
\end{aligned}$$

$$\begin{aligned}
\pi_{\mathcal{R}} : \mathcal{R}(\mathbb{F}_q) &\longrightarrow \mathbb{A}^2(\mathbb{F}_q) \\
(a, b, z) &\longmapsto (a, b),
\end{aligned}$$

$$\begin{aligned}
\pi : J(\mathbb{F}_q) \setminus \{\mathcal{O}\} &\longrightarrow \mathbb{A}^2(\mathbb{F}_q) \\
P_1 + P_2 - 2P_\infty &\longmapsto (x_{P_1} + x_{P_2}, x_{P_1}x_{P_2}) \\
P_1 - P_\infty &\longmapsto (2x_{P_1}, x_{P_1}^2)
\end{aligned}$$

and π_t is defined like π. Clearly, Diagram 2.9 is commutative, since $\pi = \pi_{\mathcal{R}} \circ \mu$ and $\pi_t = \pi_{\mathcal{R}} \circ \mu_t$.

Proposition 2.22 *For all* $(a, b) \in \mathbb{A}^2(\mathbb{F}_q)$,

$$\#\pi^{-1}(a, b) + \#\pi_t^{-1}(a, b) = 2\#\pi_{\mathcal{R}}^{-1}(a, b).$$

Proof. Let $a, b \in \mathbb{F}_q$. First, assume that $\pi_{\mathcal{R}}^{-1}(a, b) \neq \emptyset$. So, there exist a point $(a, b, z) \in \mathcal{R}(\mathbb{F}_q)$. Hence, $z^2 = \Psi(a, b)$ (see Definition 2.19). Clearly $(a, b, -z) \in \mathcal{R}(\mathbb{F}_q)$. If $z = 0$ then $\#\pi_{\mathcal{R}}^{-1}(a, b) = 1$, otherwise $\#\pi_{\mathcal{R}}^{-1}(a, b) = 2$. Let u be the polynomial in $\mathbb{F}_q[\mathbf{x}]$ defined by $u(\mathbf{x}) = \mathbf{x}^2 - a\mathbf{x} + b$. We consider the following cases.

1. Assume that u has two distinct roots x_1, x_2 in $\mathbb{F}_q$. Then there exist $y_1, y_2 \in \mathbb{F}_q$, such that $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ are points either on $H(\mathbb{F}_q)$ or on $H^t(\mathbb{F}_q)$. Indeed, $f(x_1)f(x_2) = \Psi(a, b) = z^2$, since $a = x_1 + x_2$ and $b = x_1x_2$. We distinguish two possibilities.

   (a) Suppose $z \neq 0$. Without loss of generality, let $P_1 \in H(\mathbb{F}_q)$. So, $y_1^2 = f(x_1)$. Since $f(x_1)f(x_2) = z^2 \neq 0$, it follows that $f(x_2)$ is a square in $\mathbb{F}_q$. Hence $P_2 \in H(\mathbb{F}_q)$. Note that $P_1 \neq P_2, P_1 \neq \sigma(P_2)$, $P_1 \neq \sigma(P_1)$ and $P_2 \neq \sigma(P_2)$, because $x_1 \neq x_2$ and $y_1, y_2 \neq 0$. So, $P_1, P_2 \notin H^t(\mathbb{F}_q)$. Further, the divisors $P_1 + P_2 - 2P_\infty$ and $\sigma(P_1) + \sigma(P_2) - 2P_\infty$ are the only points of $\pi^{-1}(a, b)$. Therefore $\#\pi^{-1}(a, b) = 4$ and $\#\pi_t^{-1}(a, b) = 0$.

   (b) Suppose $z = 0$. So $f(x_1)f(x_2) = 0$. Without loss of generality, let $f(x_1) = 0$. Then P_1 is a common point of $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$. This implies that $P_1 = \sigma(P_1)$. We can assume $P_2 \in H(\mathbb{F}_q)$. If $f(x_2) \neq 0$, then $P_2 \neq \sigma(P_2)$ and $P_2 \notin H^t(\mathbb{F}_q)$. Hence the divisors $P_1 + P_2 - 2P_\infty$ and $P_1 + \sigma(P_2) - 2P_\infty$ are the only points of $\pi^{-1}(a, b)$. So $\#\pi^{-1}(a, b) = 2$ and $\#\pi_t^{-1}(a, b) = 0$. If $f(x_2) = 0$, then $P_2 = \sigma(P_2)$ and $P_2 \in H^t(\mathbb{F}_q)$. Therefore the divisor $P_1 + P_2 - 2P_\infty$ is the only point of $\pi^{-1}(a, b)$ and $\pi_t^{-1}(a, b)$. So $\#\pi^{-1}(a, b) = \#\pi_t^{-1}(a, b) = 1$.

2. Assume u has one double root x_1 in $\mathbb{F}_q$. Then there exists $y_1 \in \mathbb{F}_q$, such that $P_1 = (x_1, y_1)$ and P_1 is a point of $H(\mathbb{F}_q)$ or $H^t(\mathbb{F}_q)$. Furthermore, $(f(x_1))^2 = \Psi(a, b) = z^2$, since $a = 2x_1$ and $b = x_1^2$. We consider two possibilities.

   (a) Suppose $z \neq 0$. So $f(x_1) \neq 0$, i.e. $P_1 \neq \sigma(P_1)$. Without loss of generality, assume $P_1 \in H(\mathbb{F}_q)$. So $P_1 \notin H^t(\mathbb{F}_q)$. Then, the divisors $2P_1 - 2P_\infty$, $2\sigma(P_1) - 2P_\infty$, $P_1 - P_\infty$ and $\sigma(P_1) - P_\infty$ are the only points of $\pi^{-1}(a, b)$. Hence, $\#\pi^{-1}(a, b) = 4$. Also $\#\pi_t^{-1}(a, b) = 0$, since $P_1, \sigma(P_1) \notin H^t(\mathbb{F}_q)$.

   (b) Suppose $z = 0$. So $f(x_1) = 0$. Then $P_1 = \sigma(P_1)$ and P_1 is a common point of $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$. Hence, the divisor $P_1 - P_\infty$ is the only point of $\pi^{-1}(a, b)$ and $\pi_t^{-1}(a, b)$. Therefore, $\#\pi^{-1}(a, b) = \#\pi_t^{-1}(a, b) = 1$.

3. Assume u has no root in $\mathbb{F}_q$. Let x_1, x_1^q be the distinct roots of u in $\mathbb{F}_{q^2}$. From the definition of Ψ (see Equation (2.8)), we have $f(x_1)f(x_1^q) = \Psi(a, b) = z^2$, since $a = x_1 + x_1^q$, $b = x_1x_1^q$. Then, $\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(f(x_1)) = f(x_1)f(x_1^q) = z^2 \in \mathbb{F}_q$. From Lemma 2.1, $f(x_1)$ is a square in $\mathbb{F}_{q^2}$. So there exists $y_1 \in \mathbb{F}_{q^2}$ such that $y_1^2 = f(x_1)$. Let $P_1 = (x_1, y_1)$, so $\phi(P_1) = (x_1^q, y_1^q)$. Indeed, P_1 and $\phi(P_1)$ are points of $H(\mathbb{F}_{q^2})$.

   Let β be a square root of α in $\mathbb{F}_{q^2}$. Then $Q_1 = (x_1, \frac{y_1}{\beta})$ and $\phi(Q_1) = (x_1^q, -\frac{y_1^q}{\beta})$ are points of $H^t(\mathbb{F}_{q^2})$. Then, we distinguish the following possibilities.

(a) Suppose $z \neq 0$. So $f(x_1), f(x_2) \neq 0$, i.e. $y_1, y_2 \neq 0$. Thus $P_1 \neq \sigma(P_1)$, $\phi(P_1) \neq \sigma(\phi(P_1))$, $Q_1 \neq \sigma(Q_1)$ and $\phi(Q_1) \neq \sigma(\phi(Q_1))$. Therefore

$$\pi^{-1}(a,b) = \{P_1 + \phi(P_1) - 2P_\infty, \sigma(P_1) + \sigma(\phi(P_1)) - 2P_\infty\},$$

$$\pi_t^{-1}(a,b) = \{Q_1 + \phi(Q_1) - 2P_\infty, \sigma(Q_1) + \sigma(\phi(Q_1)) - 2P_\infty\}.$$

Hence $\#\pi^{-1}(a,b) = \#\pi_t^{-1}(a,b) = 2$.

(b) Suppose $z = 0$. Then $f(x_1) = f(x_1^q) = 0$, i.e., $y_1 = y_2 = 0$. So, $P_1 = \sigma(P_1)$ and $\phi(P_1) = \sigma(\phi(P_1))$. Hence, $P_1 + \phi(P_1)$ is the only point of $\pi^{-1}(a,b)$. Likewise, $Q_1 = P_1$ and $P_1 + \phi(P_1)$ is also the only point of $\pi_t^{-1}(a,b)$. Hence $\#\pi^{-1}(a,b) = \pi_t^{-1}(a,b) = 1$.

Now, assume that $\pi_{\mathcal{R}}^{-1}(a,b) = \emptyset$. Then $\#\pi^{-1}(a,b) = \#\pi_t^{-1}(a,b) = 0$, since Diagram 2.9 is commutative (see Remarks 2.20 and 2.21). Therefore, the proof of this proposition is complete. □

Theorem 2.23

$$\#J(\mathbb{F}_q) + \#J^t(\mathbb{F}_q) = 2\#\mathcal{R}(\mathbb{F}_q) + 2.$$

Proof. We consider the projection maps π, π_t and $\pi_{\mathcal{R}}$ in Diagram 2.9. From Proposition 2.22, we have

$$\begin{aligned}
\#J(\mathbb{F}_q) + \#J^t(\mathbb{F}_q) &= 2 + \sum_{(a,b)\in\mathbb{A}^2(\mathbb{F}_q)} \#\pi^{-1}(a,b) + \#\pi_t^{-1}(a,b) \\
&= 2 + \sum_{(a,b)\in\mathbb{A}^2(\mathbb{F}_q)} 2\#\pi_{\mathcal{R}}^{-1}(a,b) \\
&= 2 + 2\#\mathcal{R}(\mathbb{F}_q).
\end{aligned}$$

□

2.9 A surface related to the binary Jacobian

Now, we extend the result of Section 2.8 to the Jacobians of genus-2 hyperelliptic curves over binary finite fields. This section gives the mathematical background for the proofs of the main theorems in Chapter 7.

Let H be an imaginary hyperelliptic curve of genus 2 over $\mathbb{F}_q$, with $q = 2^n$, defined by an equation of the form

$$\mathbf{y}^2 + h(\mathbf{x})\mathbf{y} = f(\mathbf{x}),$$

where $h = h_2\mathbf{x}^2 + h_1\mathbf{x} + h_0$ and $f = \mathbf{x}^5 + f_4\mathbf{x}^4 + f_3\mathbf{x}^3 + f_2\mathbf{x}^2 + f_1\mathbf{x} + f_0$. Let $J(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational points of the Jacobian of H over $\mathbb{F}_q$. Let $\mathcal{O}$ be the neutral element of $J(\mathbb{F}_q)$.

Let $\alpha \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha) = 1$. Then, there exist an element $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\beta^2 + \beta = \alpha$. Let H^t be a projective curve with a plane model of the form

$$\mathbf{y}^2 + h(\mathbf{x})\mathbf{y} = f(\mathbf{x}) + \alpha h^2(\mathbf{x}). \tag{2.10}$$

The identification $(\mathbf{x}, \mathbf{y}) \longrightarrow (\mathbf{x}, \mathbf{y} + \beta h(\mathbf{x}))$ shows that H^t is isomorphic to H over $\mathbb{F}_{q^2}$. Moreover, theses curves are not isomorphic over $\mathbb{F}_q$. This means H^t is a quadratic twist of H. Let J^t be the Jacobian of H^t over $\mathbb{F}_q$.

Remark 2.24 For a point $P = (x, y) \in H(\mathbb{F}_q)$, we have $\sigma(P) = (x, y + h(x))$. For P_∞, the point at infinity of H, we have $\sigma(P_\infty) = P_\infty$. Let

$$\mathcal{I}_H = \{P \in H(\mathbb{F}_q) : P = \sigma(P)\}.$$

Clearly $P \in \mathcal{I}_H$ if and only if $P = P_\infty$ or $h(x) = 0$. These points of $\mathcal{I}_H$ are exactly those which correspond to points on both, $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$.

Let ν and ω be the polynomials in $\mathbb{F}_q[\mathbf{x}_1, \mathbf{x}_2]$ defined by

$$\nu(\mathbf{x}_1, \mathbf{x}_2) = h(\mathbf{x}_1)h(\mathbf{x}_2),$$

$$\omega(\mathbf{x}_1, \mathbf{x}_2) = f(\mathbf{x}_1)h^2(\mathbf{x}_2) + f(\mathbf{x}_2)h^2(\mathbf{x}_1).$$

Clearly, ν and ω are symmetric polynomials. Consider the bivariate polynomials $\theta, \psi \in \mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ such that

$$\theta(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}_1\mathbf{x}_2) = \nu(\mathbf{x}_1, \mathbf{x}_2), \quad \psi(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}_1\mathbf{x}_2) = \omega(\mathbf{x}_1, \mathbf{x}_2).$$

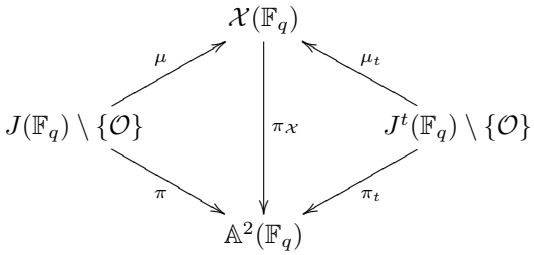
Definition 2.25 *Let $\mathcal{X}$ be the affine surface defined over $\mathbb{F}_q$ by the equation*

$$F(\mathbf{a}, \mathbf{b}, \mathbf{z}) = \mathbf{z}^2 + \theta(\mathbf{a}, \mathbf{b})\mathbf{z} + \psi(\mathbf{a}, \mathbf{b}) = 0.$$

Remark 2.26 Let $D = P_1 + P_2 - 2P_\infty$ be a divisor of $J(\mathbb{F}_q)$, where $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on $H(\overline{\mathbb{F}}_q)$, $P_1, P_2 \neq P_\infty$ and $P_1 \neq \sigma(P_2)$. Hence, $y_1^2 + h(x_1)y_1 = f(x_1)$ and $y_2^2 + h(x_2)y_2 = f(x_2)$. Let $z = h(x_1)y_2 + h(x_2)y_1$. Then $z^2 + \nu(x_1, x_2)z = \omega(x_1, x_2)$. Let $a = x_1 + x_2, b = x_1x_2$. Then $z^2 + \theta(a, b)z = \psi(a, b)$. This means that (a, b, z) is a point of $\mathcal{X}$. In fact $(a, b, z) \in \mathcal{X}(\mathbb{F}_q)$, since $a, b, z \in \mathbb{F}_q$.

Remark 2.27 Let $D = P_1 + P_2 - 2P_\infty$ be a divisor of $J^t(\mathbb{F}_q)$, where $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on $H^t(\overline{\mathbb{F}}_q)$, $P_1, P_2 \neq P_\infty$ and $P_1 \neq \sigma(P_2)$. Let $z = h(x_1)y_2 + h(x_2)y_1$. Similarly to Remark 2.26, one can show that $(x_1 + x_2, x_1x_2, z)$ is a point of $\mathcal{X}(\mathbb{F}_q)$.

Following Remarks 2.26 and 2.27, we consider the diagram



(2.11)

where

$$\begin{aligned}
\mu : J(\mathbb{F}_q) \setminus \{\mathcal{O}\} &\longrightarrow \mathcal{R}(\mathbb{F}_q) \\
P_1 + P_2 - 2P_\infty &\longmapsto (x_{P_1} + x_{P_2}, x_{P_1}x_{P_2}, h(x_{P_1})y_{P_2} + h(x_{P_2})y_{P_1}) \\
P_1 - P_\infty &\longmapsto (0, x_{P_1}^2, 0),
\end{aligned}$$

$$\begin{aligned}
\pi_{\mathcal{X}} : \mathcal{X}(\mathbb{F}_q) &\longrightarrow \mathbb{A}^2(\mathbb{F}_q) \\
(a, b, z) &\longmapsto (a, b),
\end{aligned}$$

$$\begin{aligned}
\pi : J(\mathbb{F}_q) \setminus \{\mathcal{O}\} &\longrightarrow \mathbb{A}^2(\mathbb{F}_q) \\
P_1 + P_2 - 2P_\infty &\longmapsto (x_{P_1} + x_{P_2}, x_{P_1}x_{P_2}) \\
P_1 - P_\infty &\longmapsto (0, x_{P_1}^2)
\end{aligned}$$

and μ_t, π_t are defined respectively similar to μ, π. Clearly, Diagram 2.11 is commutative, since $\pi = \pi_{\mathcal{X}} \circ \mu$ and $\pi_t = \pi_{\mathcal{X}} \circ \mu_t$.

Proposition 2.28 *For all* $(a, b) \in \mathbb{A}^2(\mathbb{F}_q)$,

$$\#\pi^{-1}(a, b) + \#\pi_t^{-1}(a, b) = 2\#\pi_{\mathcal{X}}^{-1}(a, b).$$

Proof. Let $a, b \in \mathbb{F}_q$. First, assume that $\pi^{-1}(a, b) \neq \emptyset$. So, there exist a point $(a, b, z) \in \mathcal{X}(\mathbb{F}_q)$. Hence $z^2 + \theta(a, b)z + \psi(a, b) = 0$ (see Definition 2.25). Also $(a, b, z + \theta(a, b)) \in \mathcal{X}(\mathbb{F}_q)$. If $\theta(a, b) = 0$ then $\#\pi_{\mathcal{X}}^{-1}(a, b) = 1$, otherwise $\#\pi_{\mathcal{X}}^{-1}(a, b) = 2$. Let u be the polynomial in $\mathbb{F}_q[\mathbf{x}]$ defined by $u(\mathbf{x}) = \mathbf{x}^2 + a\mathbf{x} + b$. We consider the following cases.

1. Assume u has two distinct roots x_1, x_2 in $\mathbb{F}_q$. Then there exist $y_1, y_2 \in \mathbb{F}_q$, such that $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ are points either on $H(\mathbb{F}_q)$ or on $H^\tau(\mathbb{F}_q)$. Furthermore, $\theta(a, b) = h(x_1)h(x_2)$ and $\psi(a, b) = f(x_1)h^2(x_2) + f(x_2)h^2(x_1)$, because $a = x_1 + x_2$ and $b = x_1x_2$. We distinguish the following possibilities.

(a) Suppose $\theta(a,b) \neq 0$. So, $h(x_1), h(x_2) \neq 0$. Without loss of generality, let $P_1 \in H(\mathbb{F}_q)$. We note that

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\tfrac{\psi(a,b)}{\theta^2(a,b)}) &= \mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\tfrac{f(x_1)h^2(x_2)+f(x_2)h^2(x_1)}{h^2(x_1)h^2(x_2)}) \\ &= \mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\tfrac{f(x_1)}{h^2(x_1)}) + \mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\tfrac{f(x_2)}{h^2(x_2)}).\end{aligned}$$

So $\mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\frac{f(x_2)}{h^2(x_2)}) = 0$, since $\mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\frac{\psi(a,b)}{\theta^2(a,b)}) = \mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\frac{f(x_1)}{h^2(x_1)}) = 0$. Hence $P_2 \in H(\mathbb{F}_q)$. Indeed, $P_1, P_2 \notin H^t(\mathbb{F}_q)$, since $h(x_1), h(x_2) \neq 0$ (see Remark 2.24). Furthermore, $P_1 \neq P_2$, $P_1 \neq \sigma(P_2)$, $P_1 \neq \sigma(P_1)$ and $P_2 \neq \sigma(P_2)$. Hence, the divisors $P_1 + P_2 - 2P_\infty$, $P_1 + \sigma(P_2) - 2P_\infty$, $\sigma(P_1) + P_2 - 2P_\infty$ and $\sigma(P_1) + \sigma(P_2) - 2P_\infty$ are the only points of $\pi^{-1}(a,b)$. So, $\#\pi^{-1}(a,b) = 4$ and $\#\pi_t^{-1}(a,b) = 0$.

(b) Suppose $\theta(a,b) = 0$. So $h(x_1)h(x_2) = 0$. Without loss of generality, let $h(x_1) = 0$. Then P_1 is a common point of $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$ (see Remark 2.24). This implies that $P_1 = \sigma(P_1)$. We may assume $P_2 \in H(\mathbb{F}_q)$. If $h(x_2) \neq 0$, then $P_2 \neq \sigma(P_2)$ and $P_2 \notin H^t(\mathbb{F}_q)$. Hence the divisors $P_1 + P_2 - 2P_\infty$ and $P_1 + \sigma(P_2) - 2P_\infty$ are the only points of $\pi^{-1}(a,b)$. So $\#\pi^{-1}(a,b) = 2$ and $\#\pi_t^{-1}(a,b) = 0$. If $h(x_2) = 0$, then $P_2 = \sigma(P_2)$ and $P_2 \in H^t(\mathbb{F}_q)$. Hence, the divisor $P_1 + P_2 - 2P_\infty$ is the only point of $\pi^{-1}(a,b)$ and $\pi_t^{-1}(a,b)$. Therefore, $\#\pi^{-1}(a,b) = \#\pi_t^{-1}(a,b) = 1$.

2. Assume u has a double root x_1 in $\mathbb{F}_q$. Then there exists $y_1 \in \mathbb{F}_q$, such that $P_1 = (x_1, y_1)$ is a point of $H(\mathbb{F}_q)$ or $H^t(\mathbb{F}_q)$. Furthermore, $\theta(a,b) = h^2(x_1)$ and $\psi(a,b) = 0$, because $a = 0$ and $b = x_1^2$. We distinguish two possibilities:

   (a) Suppose $\theta(a,b) \neq 0$. So $h(x_1) \neq 0$. Without loss of generality, we assume $P_1 \in H(\mathbb{F}_q)$. Then $P_1 \notin H^t(\mathbb{F}_q)$, since $h(x_1) \neq 0$. This implies that $P_1 \neq \sigma(P_1)$. So, the divisors $2P_1 - 2P_\infty$, $2\sigma(P_1) - 2P_\infty$, $P_1 - P_\infty$ and $\sigma(P_1) - P_\infty$ are the only points of $\pi^{-1}(a,b)$. Hence $\#\pi^{-1}(a,b) = 4$. Also $\#\pi_t^{-1}(a,b) = 0$, since $P_1, \sigma(P_1) \notin H^t(\mathbb{F}_q)$.

   (b) Suppose $\theta(a,b) = 0$. So $h(x_1) = 0$. Then $P_1 = \sigma(P_1)$ and P_1 is a common point of $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$. So, the divisor $P_1 - P_\infty$ is the only point of $\pi^{-1}(a,b)$ and $\pi_t^{-1}(a,b)$. Hence $\#\pi^{-1}(a,b) = \#\pi_t^{-1}(a,b) = 1$.

3. Assume u has no root in $\mathbb{F}_q$. Let x_1, x_1^q be the roots of u in $\mathbb{F}_{q^2}$. It follows from the definitions of θ and ψ that $\theta(a,b) = h(x_1)h(x_1^q)$ and $\psi(a,b) = f(x_1)h^2(x_1^q) + f(x_1^q)h^2(x_1)$. We distinguish the following possibilities.

   (a) Suppose $\theta(a,b) \neq 0$. Then $h(x_1), h(x_1^q) \neq 0$. We note that

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}q^2/\mathbb{F}_2}(\tfrac{f(x_1)}{h^2(x_1)}) &= \mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}q^2/\mathbb{F}_q}(\tfrac{f(x_1)}{h^2(x_1)})) \\ &= \mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\tfrac{f(x_1)}{h^2(x_1)} + \tfrac{f(x_1^q)}{h^2(x_1^q)}) \\ &= \mathrm{Tr}_{\mathbb{F}q/\mathbb{F}_2}(\tfrac{\psi(a,b)}{\theta^2(a,b)}) = 0.\end{aligned}$$

Then there exists $y_1 \in \mathbb{F}_{q^2}$ such that $P_1 = (x_1, y_1) \in H(\mathbb{F}_{q^2})$. Also $\phi(P_1) = (x_1^q, y_1^q) \in H(\mathbb{F}_{q^2})$. Let $\beta \in \mathbb{F}_{q^2}$ such that $\beta^2 + \beta = \alpha$. Then $Q_1 = (x_1, y_1 + \beta h(x_1))$ and $\phi(Q_1) = (x_1^q, y_1^q + (\beta + 1)h(x_1^q))$ are points of $H^t(\mathbb{F}_{q^2})$. One sees that $P_1 \neq \sigma(P_1)$, $\phi(P_1) \neq \sigma(\phi(P_1))$, $Q_1 \neq \sigma(Q_1)$ and $\phi(Q_1) \neq \sigma(\phi(Q_1))$. Therefore

$$\pi^{-1}(a,b) = \{P_1 + \phi(P_1) - 2P_\infty, \sigma(P_1) + \sigma(\phi(P_1)) - 2P_\infty\},$$

$$\pi_t^{-1}(a,b) = \{Q_1 + \phi(Q_1) - 2P_\infty, \sigma(Q_1) + \sigma(\phi(Q_1)) - 2P_\infty\}.$$

So $\#\pi^{-1}(a,b) = \#\pi_t^{-1}(a,b) = 2$.

(b) Suppose $\theta(a,b) = 0$. So, $h(x_1) = h(x_1^q) = 0$. Thus $P_1 = (x_1, \sqrt{f(x_1)}) \in H(\mathbb{F}_{q^2})$ and $\phi(P_1) = (x_1^q, \sqrt{f(x_1^q)}) \in H(\mathbb{F}_{q^2})$. Furthermore, $P_1 = \sigma(P_1)$ and $\phi(P_1) = \sigma(\phi(P_1))$. Also $P_1, \phi(P_1) \in H^t(\mathbb{F}_{q^2})$. Therefore, $P_1 + \phi(P_1)$ is the only point of $\pi^{-1}(a,b)$ and $\pi_t^{-1}(a,b)$. Hence, $\#\pi^{-1}(a,b) = \pi_t^{-1}(a,b) = 1$.

Now, assume that $\pi_{\mathcal{R}}^{-1}(a,b) = \emptyset$. Then $\#\pi^{-1}(a,b) = \#\pi_t^{-1}(a,b) = 0$, since Diagram 2.11 is commutative (see Remarks 2.26 and 2.27). So, the proof of this proposition is complete. □

Theorem 2.29

$$\#J(\mathbb{F}_q) + \#J^t(\mathbb{F}_q) = 2\#\mathcal{X}(\mathbb{F}_q) + 2.$$

Proof. Proposition 2.28 concludes the proof of this theorem. □

2.10 Deterministic extractor

Here, we define the notion of a *deterministic extractor* and a quality measure called *statistical distance*. For a general definition of extractors we refer to [89, 96].

Definition 2.30 *Let X and Y be S-valued random variables, where S is a finite set. Then the* statistical distance $\Delta(X,Y)$ *of X and Y is*

$$\Delta(X,Y) = \tfrac{1}{2}\sum_{s\in S} |\Pr[X = s] - \Pr[Y = s]|.$$

Let U_S denote a random variable uniformly distributed on S. We say that an S-valued random variable X is δ-uniform, *if $\Delta(X, U_S) \leq \delta$.*

Note that if the random variable X is δ-*uniform*, then no algorithm can distinguish X from U_S with advantage larger than δ, that is, for all algorithms $D : S \longrightarrow \{0,1\}$

$$|\Pr[D(X) = 1] - \Pr[D(U_S) = 1]| \leq \delta.$$

See [78].

Definition 2.31 *Let S, T be finite sets. Consider a function* Ext $: S \longrightarrow T$. *We say that* Ext *is a* deterministic (T, δ)-extractor *for S if* Ext(U_S) *is δ-uniform on T. That is*

$$\Delta(\text{Ext}(U_S), U_T) \leq \delta.$$

In the case that $T = \{0,1\}^k$, we say that Ext *is a* (k, δ)-deterministic extractor *for S.*

In Chapters 4, 5, 6 and 7, we consider deterministic $(\mathbb{F}_q, \delta)$-extractors, where q is a prime power. Observe that converting random elements of $\mathbb{F}_q$ into random bit strings is a relatively easy problem. For instance, one can represent an element of $\mathbb{F}_q$ by a number in $\mathbb{Z}_q$ and convert this number to a bit-string of a length equal or very close to the bit length of q (e.g. see [60]). Furthermore, if q is close to a power of 2, that is, $0 \leq (2^n - q)/2^n \leq \delta$ for a small δ, then the bit-string representation of the uniform element $U_{\mathbb{F}_q}$ is statistically close to n uniformly random bits. The following simple lemma is a well-known result (the proof can be found, for instance, in [20]).

Lemma 2.32 *Let* `bits` $: \mathbb{F}_q \longrightarrow \{0,1\}^n$ *be a bit-representation function for $\mathbb{F}_q$. Suppose $0 \leq (2^n - q)/2^n \leq \delta$. Then* `bits` *is an (n, δ)-deterministic extractor.*

2.10.1 Extractor for a subgroup

One application of extractors is to extract bits from a shared secret element in the final step of key exchange protocols, e.g. the Diffie-Hellman key exchange protocol. It is assumed that this group element is uniformly distributed if the Decisional Diffie-Hellman problem (DDH) in this group is believed as a hard problem.

We note that, if the order of the group is divisible by a small number, the DDH problem in the corresponding group is easy. In this case, the main subgroup is suggested for cryptographic applications. Further, the DDH problem in the main subgroup is assumed to be intractable.

Let A be an additive group of order $2m$, where m is odd. Let G be the *main subgroup* of A of order m. If we have an extractor for A with some additional requirement, then we can propose an extractor for the main subgroup G.

Let 0 be the neutral element of A and t be the element of order 2. Let β be a bit distinguishing a from $-a$ satisfying

$$\begin{aligned}&\beta : A \to \{0,1\},\\ &\beta(a) = 0, \text{ if } a = -a,\\ &\beta(a) + \beta(-a) = 1, \text{ if } a \neq -a.\end{aligned}$$

Let $\mathtt{Ext}$ be a deterministic (T,δ)-extractor for A, for some T and δ. Suppose $\mathtt{Ext}(a) = \mathtt{Ext}(-a)$ for all $a \in A$. Furthermore, assume $\mathtt{Ext}(0) = \mathtt{Ext}(t)$. We propose an extractor $\mathtt{ext}$ for G as a modified version of $\mathtt{Ext}$. The extractor $\mathtt{ext}$ is defined by the function

$$\begin{aligned}&\mathtt{ext} : G \to T,\\ &\mathtt{ext}(a) = \mathtt{Ext}(a + \beta(a)t).\end{aligned}$$

Proposition 2.33 *Let $z \in T$. Then*

$$\#\mathtt{Ext}^{-1}(z) = 2\#\mathtt{ext}^{-1}(z).$$

Proof. We consider the map $\xi : \mathtt{Ext}^{-1}(z) \longrightarrow \mathtt{ext}^{-1}(z)$ defined by

$$\xi(a) = \begin{cases} a, & \text{if } a \in G,\ \beta(a) = 0,\\ -a, & \text{if } a \in G,\ \beta(a) = 1,\\ -a + t, & \text{if } a \notin G,\ \beta(a + t) = 0,\\ a + t, & \text{if } a \notin G,\ \beta(a + t) = 1.\end{cases}$$

The map ξ is surjective. Indeed it is a $2:1$ map, since $\mathtt{Ext}(a) = \mathtt{Ext}(-a)$ for all $a \in A$ and $\mathtt{Ext}(0) = \mathtt{Ext}(t)$. □

Proposition 2.34 $\mathtt{Ext}$ *is a (T,δ)-deterministic extractor for A if and only if* $\mathtt{ext}$ *is a (T,δ)-deterministic extractor for G.*

Proof. Let X_A and X_G be the T-valued random variables that are defined by

$$X_A = \mathtt{Ext}(a), \text{ for } a \in_R A \text{ and } X_G = \mathtt{ext}(a), \text{ for } a \in_R G.$$

Let $z \in T$. Proposition 2.33 now implies

$$\Pr[X_A = z] = \frac{\#\mathtt{Ext}^{-1}(z)}{\#A} = \frac{\#\mathtt{ext}^{-1}(z)}{\#G} = \Pr[X_G = z].$$

Hence $\Delta(X_A, U_T) = \Delta(X_G, U_T)$, for the uniform random variable U_T in T. □

2.11 Deterministic extractors for varieties

In this section, we describe a simple way to construct an extractor based on curves, Jacobians and in general varieties over finite fields.

Let $\mathcal{A}$ be a variety of dimension n defined over a finite field $\mathbb{F}_q$. Consider a finite map from the variety $\mathcal{A}$ to the affine space of dimension n, i.e., a Noether normalization of the variety $\mathcal{A}$ (see [27]). Such a map always exists, but it is not unique. So, in general, we can assume that each point P of $\mathcal{A}(\mathbb{F}_q)$ has a compressed representation by n coordinates $(x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_q$. We note that this representation does not uniquely determine points on $\mathcal{A}$, extra coordinates are necessary to represent a point uniquely. On the other hand, for each choice $(x_1, \ldots, x_n) \in \overline{\mathbb{F}}_q^n$, there exist only finitely many points on $\mathcal{A}$. Assume that each point belongs to no more than e points on $\mathcal{A}$.

For example, if $\mathcal{A}$ is a (hyper)elliptic curve in Weierstrass form, we can consider the x-coordinate of the point as a compact representation. In the case where $\mathcal{A}$ is the Jacobian of a hyperelliptic curve, we can compactly represent each point by the coefficients of the first polynomial in Mumford representation.

We can define a deterministic extractor, based on $\mathcal{A}$, that for a given point P on $\mathcal{A}$ outputs some fixed coordinates of the compact representation of P.

Definition 2.35 *Let $\mathcal{A}$ be a variety of dimension n and degree d defined over a finite field $\mathbb{F}_q$. Suppose each point P of $\mathcal{A}$ has a compressed representation $(x_1, x_2, \ldots, x_n)$, where $x_i \in \mathbb{F}_q$. Let k be a positive integer less than or equal to n. Fix numbers $i_1, i_2, \ldots, i_k$, such that $1 \leq i_1 < i_2 < \ldots < i_k \leq n$. The extractor $\mathtt{Ext}_{i_1,i_2,\ldots,i_k}$ for $\mathcal{A}$ is defined as*

$$\mathtt{Ext}_{i_1,i_2,\ldots,i_k} : \mathcal{A}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^k$$
$$\mathtt{Ext}_{i_1,i_2,\ldots,i_k}(P) = (x_{i_1}, x_{i_2}, \ldots, x_{i_k}).$$

In the following, we give some examples of the extractor $\mathtt{Ext}_{i_1,i_2,\ldots,i_k}$ based on curves and the Jacobians.

Example 2.36 Consider the finite field $\mathbb{F}_{q^n}$, where q is a prime power and n is a positive integer. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $\mathcal{C}$ be an absolutely irreducible curve defined over $\mathbb{F}_{q^n}$ by the equation $f(\mathbf{x}, \mathbf{y}) = 0$, where $f \in \mathbb{F}_{q^n}[\mathbf{x}, \mathbf{y}]$. By means of the Weil descent technique (see Section 2.4), we define $\mathcal{A}$ as $W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathcal{C})$. So, $\mathcal{A}$ is a variety of dimension n. Furthermore, a point $P = (x, y)$ on $\mathcal{C}(\mathbb{F}_{q^n})$ has a compressed representation $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$, where $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$. Now, Definition 2.35 defines extractor for $\mathcal{C}$.

Example 2.37 Let H be an imaginary hyperelliptic curve defined over $\mathbb{F}_q$ of genus n. Here, we let $\mathcal{A} = J$ be the Jacobian of H over $\mathbb{F}_q$. We note that $\mathcal{A}$ is a

variety of dimension n over $\mathbb{F}_q$. A point P on $\mathcal{A}(\mathbb{F}_q)$ has Mumford representation $[u(\mathbf{x}), v(\mathbf{x})]$, where $u, v \in \mathbb{F}_q[\mathbf{x}]$ and u is monic of degree d less than or equal to n (see Section 2.6). The point P has a compressed representation $(u_0, u_1, \ldots, u_{n-1})$, where $u(\mathbf{x}) = \mathbf{x}^d + u_{d-1}\mathbf{x}^{d-1} + \ldots + u_1\mathbf{x} + u_0$ and $u_i = 0$, for $d \leq i \leq n-1$. Now, Definition 2.35 suggests the extractor $\mathtt{Ext}$ based on the Jacobian of H over $\mathbb{F}_q$.

Analysis of the extractor. Now, we investigate the distribution of the output $\mathtt{Ext}_{i_1,i_2,\ldots,i_k}(P)$, where points P are chosen uniformly at random in $\mathcal{A}$. Fix k and some $1 \leq i_1 < i_2 < \ldots < i_k \leq n$. In the following we abbreviate $\mathtt{Ext}_{i_1,i_2,\ldots,i_k}(P)$ by $\mathtt{Ext}_k$.

Let $U_{\mathbb{F}_q^k}$ be a uniform random variable and let X be an $\mathbb{F}_q^k$-valued random variable defined by

$$X = \mathtt{Ext}_k(P), \quad \text{for} \quad P \in_R \mathcal{A}(\mathbb{F}_q).$$

Let $a \in \mathbb{F}_q^k$. The uniform random variable $U_{\mathbb{F}_q^k}$ satisfies $\Pr[U_{\mathbb{F}_q^k} = a] = 1/q^k$. For the $\mathbb{F}_q^k$-valued random variable X we have $\Pr[X = a] = \frac{\#\mathtt{Ext}_k^{-1}(a)}{\#\mathcal{A}(\mathbb{F}_q)}$. In the following, we compute the statistical distance between the random variable X and the uniform random variable $U_{\mathbb{F}_q^k}$.

$$\Delta(X, U_{\mathbb{F}_q^k}) = \frac{1}{2} \sum_{a \in \mathbb{F}_q^k} \left| \Pr[X = a] - \Pr[U_{\mathbb{F}_q^k} = a] \right| = \frac{1}{2} \sum_{a \in \mathbb{F}_q^k} \left| \frac{\#\mathtt{Ext}_k^{-1}(a)}{\#\mathcal{A}(\mathbb{F}_q)} - \frac{1}{q^k} \right|.$$

From the Lang-Weil Theorem, we can consider a bound on the number of points on $\mathcal{A}$ as

$$|\#\mathcal{A}(\mathbb{F}_q) - q^n| \leq Aq^{n-\frac{1}{2}},$$

where A is a constant in terms of the parameters of $\mathcal{A}$ such as the degree and the dimension of $\mathcal{A}$. The fibers of $\mathtt{Ext}_k$ are generally varieties of dimension $n-k$, but there are exceptional fibers which are reducible. It is necessary to distinguish the reducible fibers, so let $I_{\mathtt{Ext}_k} = \left\{ a \in \mathbb{F}_q^k : \mathtt{Ext}_k^{-1}(a) \text{ is reducible} \right\}$. Then, by means of the Lang-Weil Theorem, we obtain a number B such that the following bound is satisfied for all fibers $\mathtt{Ext}_k^{-1}(a)$, where $a \notin I_{\mathtt{Ext}_k}$.

$$\left| \#\mathtt{Ext}_k^{-1}(a)(\mathbb{F}_q) - q^{n-k} \right| \leq Bq^{n-k-\frac{1}{2}}.$$

Further, for all $a \in I_{\mathtt{Ext}_k}$, we can consider a trivial bound

$$0 \leq \#\mathtt{Ext}_k^{-1}(a)(\mathbb{F}_q) \leq eq^{n-k}.$$

Hence,

$$\Delta(X, U_{\mathbb{F}_q^k}) = \sum_{a \in I_{\mathtt{Ext}_k}} \frac{\left| q^k \#\mathtt{Ext}_k^{-1}(a) - \#\mathcal{A}(\mathbb{F}_q) \right|}{2q^k \#\mathcal{A}(\mathbb{F}_q)} + \sum_{a \in \mathbb{F}_q^k \setminus I_{\mathtt{Ext}_k}} \frac{\left| q^k \#\mathtt{Ext}_k^{-1}(a) - \#\mathcal{A}(\mathbb{F}_q) \right|}{2q^k \#\mathcal{A}(\mathbb{F}_q)}.$$

Let $w = \#I_{\mathtt{Ext}_k}$. Then

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_q^k}) \leq & \frac{((e-1)q^n + Aq^{n-\frac{1}{2}})w + (A+B)q^{n-\frac{1}{2}}(q^k - w)}{2q^k(q^n - Aq^{n-\frac{1}{2}})} \\ = & \frac{((e-1)\sqrt{q} - B)w + (A+B)q^k}{2q^k(\sqrt{q} - A)} = \frac{\frac{A+B}{2} + \epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q) = \frac{A(A+B)+((e-1)\sqrt{q}-B)wq^{-k+\frac{1}{2}}}{2(\sqrt{q}-A)}$. In the case that $w = 0$, $\epsilon(q) < 1$, for $q \geq \frac{A^2(A+B+2)^2}{4}$.

For an accurate analysis of the extractor, it is necessary to have proper bounds on the number of points on fibres of $\mathtt{Ext}_k$. This means, a detailed study on the geometry of the fibers of $\mathtt{Ext}_k$ is required. Further, some counting techniques are needed to find tight estimates for the number of points on the fibres. Clearly, the analysis will be more precise, if we consider extractors based on particular families of varieties. For example, the analysis of the proposed extractor $\mathtt{Ext}_k$ for the families of curves and Jacobians given by Examples 2.36 and 2.37, will be more precise that in general. In this thesis we concentrate of some families given by these examples.

The following example presents an extractor for an affine curve C. Provided that the point P is chosen uniformly at random in C, the bits extracted from the point P are uniformly distributed.

Example 2.38 Consider the finite field $\mathbb{F}_{2^k}$, where k is odd. So, every element $y \in \mathbb{F}_{2^k}$ can be represented by $(y_1, y_2, \ldots, y_k)$, where $y_i \in \{0, 1\}$. Let C be the affine model of an elliptic curve over $\mathbb{F}_{2^k}$ defined by the equation

$$\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3 + b,$$

where $b \in \mathbb{F}_{2^k}$. We define an extractor $\mathtt{ext}$ for the curve C by the function:

$$\begin{aligned}&\mathtt{ext} : C(\mathbb{F}_{2^k}) \longrightarrow \{0,1\}^k \\ &\mathtt{ext}(x, y) = (y_1, y_2, \ldots, y_k).\end{aligned}$$

Then, $\mathtt{ext}$ is a $(k, 0)$-deterministic extractor for C, because $\mathtt{ext}$ is a bijection.

Chapter 3

Norm and Trace Varieties

In this chapter, we describe two scalar restriction techniques for the families of Kummer and Artin-Schreier curves. These techniques enable us to associate a curve from these families defined over $\mathbb{F}_{q^n}$ to an n-dimensional affine hypersurface defined over $\mathbb{F}_q$.

Let $\mathcal{C}$ be an absolutely irreducible smooth Kummer curve defined by $\mathbf{y}^m = f(\mathbf{x})$, where f is a polynomial in $\mathbb{F}_{q^n}[\mathbf{x}]$ and m is a positive integer dividing $q-1$. The *norm variety* $\mathcal{N}$ is an n-dimensional hypersurface over $\mathbb{F}_q$ related to the curve $\mathcal{C}$. An $\mathbb{F}_{q^n}$-rational point (x, y) on $\mathcal{C}$ is mapped to an $\mathbb{F}_q$-rational point $(x_1, x_2, \ldots, x_n, z)$ on $\mathcal{N}$, where $x \in \mathbb{F}_{q^n}$ is represented by $(x_1, x_2, \ldots, x_n)$ in $\mathbb{F}_q^n$ and z equals the *norm* of y over $\mathbb{F}_q$. This map is $m:1$ for points (x, y) with $y \neq 0$ and $1:1$ for points (x, y) with $y = 0$. Theorem 3.7 will show that the number of $\mathbb{F}_{q^n}$-rational points of $\mathcal{C}$ equals the number of $\mathbb{F}_q$-rational points of $\mathcal{N}$.

A similar idea can be applied to an absolutely irreducible smooth curve $\mathcal{X}$ in the Artin-Schreier form $\mathbf{y}^p - \mathbf{y} = F(\mathbf{x})$, where F is a rational function in $\mathbb{F}_{q^n}(\mathbf{x})$ and p is the characteristic of the field $\mathbb{F}_q$. The curve $\mathcal{X}$ over $\mathbb{F}_{q^n}$ is related to the *trace variety* which is an n-dimensional hypersurface $\mathcal{T}$ over $\mathbb{F}_q$. The corresponding map

---

The result of this chapter is based on: R. R. Farashahi. Norm and Trace Varieties. preprint, 2008. Moreover, other proofs of Theorems 3.7 and 3.13 are presented by B. Edixhoven in the appendix of the latter. The idea of Section 3.1 is based on: R. R. Farashahi and R. Pellikaan, The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic. In *International Workshop on the Arithmetic of Finite Fields–WAIFI 2007*, volume 4547 of *Lecture Notes in Computer Science*, pages 219–236. Springer-Verlag, 2007. The result of Subsection 3.2.1 is based on: R. R. Farashahi and R. Pellikaan, and A. Sidorenko, Extractors for Binary Elliptic Curves. In *Designs, Codes and Cryptography*, 49(1–3):171–186, 2008. Open access at `http://www.springerlink.com/content/lm35kv103x34j754`.

assigns an $\mathbb{F}_{q^n}$-rational point (x, y) on $\mathcal{X}$ to an $\mathbb{F}_q$-rational point $(x_1, x_2, \ldots, x_n, z)$ on $\mathcal{T}$, where z equals the *trace* of y over $\mathbb{F}_q$. This map is a $p : 1$ map. Moreover, Theorem 3.13 will show that the number of $\mathbb{F}_{q^n}$-rational points of $\mathcal{X}$ equals the number of $\mathbb{F}_q$-rational points of $\mathcal{N}$.

In Chapter 4 and Chapter 5 we will use norm and trace surfaces to analyse the proposed extractor for binary elliptic curves and so-called quadratic extension extractor for hyper elliptic curves. Furthermore, we will investigate the geometry of the intersections of norm and trace surfaces with coordinate hyperplanes.

In the appendix of [31] a cohomological interpretation of the *norm* and the *trace* varieties are presented by B. Edixhoven. Furthermore, the proofs of Theorems 3.7 and 3.13 are given by means of etale cohomology.

The next section presents the *norm* variety related to a Kummer curve. Similarly, Section 3.2 presents the *trace* variety related to an Artin Schreier curve.

3.1 Norm variety

Consider an absolutely irreducible nonsingular affine curve $\mathcal{C}$ defined over $\mathbb{F}_{q^n}$ in Kummer form. We shall define an affine variety $\mathcal{N}$ in $\mathbb{A}^{n+1}_{\mathbb{F}_q}$ related to this curve $\mathcal{C}$ and we shall show that the number of $\mathbb{F}_{q^n}$-rational points on the affine curve $\mathcal{C}$ equals the number of $\mathbb{F}_q$-rational points on the affine variety $\mathcal{N}$.

Let $\mathcal{C}$ be an absolutely irreducible nonsingular affine curve defined over $\mathbb{F}_{q^n}$ by the equation

$$\mathbf{y}^m = f(\mathbf{x}), \tag{3.1}$$

where $f(\mathbf{x}) \in \mathbb{F}_{q^n}[\mathbf{x}]$ is a monic square-free polynomial of degree d and m is a positive integer dividing $q - 1$.

Let $\mathcal{F}$ be the polynomial in $\mathbb{F}_q[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$ defined by

$$\mathcal{F}(\mathbf{x}_1, \mathbf{x}_2, , \ldots, \mathbf{x}_n) = \mathrm{N}(f(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2 + \ldots + \mathbf{x}_n\alpha_n)). \tag{3.2}$$

Proposition 3.1 *The polynomial $\mathcal{F}$ defined by Equation (3.2) is square-free.*

Proof. Let $f(\mathbf{x}) = \prod_{i=1}^{d}(\mathbf{x} - \lambda_i)$, where $\lambda_i \in \overline{\mathbb{F}}_q$. We note that $\lambda_i \neq \lambda_j$, for $i \neq j$, since f is square-free. Then

$$\mathcal{F}(\mathbf{x}_1, \mathbf{x}_2, , \ldots, \mathbf{x}_n) = \prod_{j=0}^{n-1} \prod_{i=1}^{d} (\mathbf{x}_1\alpha_1^{q^j} + \cdots + \mathbf{x}_n\alpha_n^{q^j} - \lambda_i^{q^j}).$$

Suppose $\mathcal{F}$ is not square-free. Then $\sum_{k=1}^{n} \mathbf{x}_k\alpha_k^{q^j} - \lambda_i^{q^j} = \gamma(\sum_{k=1}^{n} \mathbf{x}_k\alpha_k^{q^{j'}} - \lambda_{i'}^{q^{j'}})$ for a $\gamma \in \mathbb{F}_{q^n}$ and some $1 \leq i, j, i', j' \leq d$, where the pairs i, j and i', j' are distinct. So $\alpha_k^{q^j} = \gamma\alpha_k^{q^{j'}}$, for all $1 \leq k \leq n$. Now there are two possibilities. If $j \neq j'$

the determinant of the matrix associated to the basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ (see Subsection 2.1) is zero, which is a contradiction. If $j = j'$, then $\gamma = 1$ and $\lambda_i^{q^j} = \lambda_{i'}^{q^j}$. So $\lambda_i = \lambda_i'$. Thus $i = i'$, which is also a contradiction. Therefore $\mathcal{F}$ is a square-free polynomial. □

In particular, Proposition 3.1 shows that $\mathcal{F}$ is not an ℓ-th power of a polynomial in $\overline{\mathbb{F}}_q[\mathbf{x}_1, \ldots, \mathbf{x}_n]$, for any positive integer $\ell \geq 2$. So, the polynomial $\mathbf{z}^m - \mathcal{F}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is absolutely irreducible.

Definition 3.2 *Let $\mathcal{N}$ be the affine variety defined over $\mathbb{F}_q$ by the equation*

$$\mathbf{z}^m - \mathcal{F}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) = 0.$$

The affine variety $\mathcal{N}$ is absolutely irreducible, since the polynomial $\mathbf{z}^m - \mathcal{F}$ is absolutely irreducible.

Remark 3.3 Let $P = (x, y) \in \mathcal{C}(\mathbb{F}_{q^n})$, where $x = \sum_{k=1}^{n} x_k \alpha_k$ and $x_k \in \mathbb{F}_q$. So $y^m = f(x)$. Let $z = \mathrm{N}(y)$. Then $z^m = (\mathrm{N}(y))^m = \mathrm{N}(y^m) = \mathrm{N}(f(x)) = \mathcal{F}(x_1, \ldots, x_n)$ (see Equation (3.2)). That means $(x_1, \ldots, x_n, z) \in \mathcal{N}(\mathbb{F}_q)$.

Consider the following diagram.

$$(x, y) \longmapsto (x_1, \ldots, x_n, \mathrm{N}(y))$$

$$\begin{array}{ccc} (x,y) & \mathcal{C}(\mathbb{F}_{q^n}) \longrightarrow \mathcal{N}(\mathbb{F}_q) & (x_1,\ldots,x_n,z) \\ \downarrow \pi_{\mathcal{C}} & \downarrow \pi_{\mathcal{C}} \quad\quad \downarrow \pi_{\mathcal{N}} & \downarrow \pi_{\mathcal{N}} \\ (x_1,\ldots,x_n) & \mathbb{A}^n(\mathbb{F}_q) \xrightarrow{id} \mathbb{A}^n(\mathbb{F}_q) & (x_1,\ldots,x_n) \end{array} \tag{3.3}$$

In Theorem 3.7, we show that the number of $\mathbb{F}_{q^n}$-rational points on the affine curve $\mathcal{C}$ equals the number of $\mathbb{F}_q$-rational points on the affine variety $\mathcal{N}$. To prove this theorem, we need to discuss fibers of the projection maps $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{N}}$. In fact, we show that the numbers of points on the fibers of $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{N}}$ at the same point of $\mathbb{A}^n(\mathbb{F}_q)$ are equal.

Remark 3.4 Let $P_0 = (x, y) \in \mathcal{C}(\mathbb{F}_{q^n})$. Let $P_i = (x, \beta^i y)$, for all $0 \leq i < m$, where β is an element in $\mathbb{F}_q$ of order m. Obviously $P_i \in \mathcal{C}(\mathbb{F}_{q^n})$. In fact, the points P_i are the only points of $\mathcal{C}(\mathbb{F}_{q^n})$ having the same x-coordinate as P. If $y \neq 0$, then the points P_i are pairwise distinct. It follows that $\pi_{\mathcal{C}}(P_i) = (x_1, \ldots, x_n)$, for all $0 \leq i < m$, where $x = \sum_{k=1}^{n} x_k \alpha_k$. Hence, if $\pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$, then

$$\#\pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n) = \begin{cases} 1, & \text{if } \mathcal{F}(x_1, \ldots, x_n) = 0, \\ m, & \text{otherwise.} \end{cases}$$

We note that $\mathcal{F}(x_1, \ldots, x_n) = 0$ if and only if $y = 0$, since $\mathcal{F}(x_1, \ldots, x_n) = (\mathrm{N}(y))^m$ (see Remark 3.3).

Remark 3.5 Let $P_0 = (x_1, \ldots, x_n, z) \in \mathcal{N}(\mathbb{F}_q)$ and let $P_i = (x_1, \ldots, x_n, \beta^i z)$, for all $0 \leq i < m$, where β is an element in $\mathbb{F}_q$ of order m. Then $P_i \in \mathcal{N}(\mathbb{F}_q)$. If $z \neq 0$, the points P_i are pairwise distinct and are the only points on $\mathcal{N}$ whose first n coordinates equal $x_1, \ldots, x_n$. Hence, if $\pi_{\mathcal{N}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$, then

$$\#\pi_{\mathcal{N}}^{-1}(x_1, \ldots, x_n) = \begin{cases} 1, & \text{if } \mathcal{F}(x_1, \ldots, x_n) = 0, \\ m, & \text{otherwise.} \end{cases}$$

Proposition 3.6 *For all* $(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_q)$,

$$\#\pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n) = \#\pi_{\mathcal{N}}^{-1}(x_1, \ldots, x_n).$$

Proof. If $\pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$, then Remark 3.3 shows that $\pi_{\mathcal{N}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$.

Now assume that $\pi_{\mathcal{N}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$. Then there exists a point $(x_1, \ldots, x_n, z)$ on $\mathcal{N}(\mathbb{F}_q)$. Thus $z^m = \mathcal{F}(x_1, \ldots, x_n)$. Let $x = \sum_{j=1}^{n} x_j \alpha_j$. Then, by Equation (3.2), $z^m = \mathrm{N}(f(x))$. So, $\mathrm{N}(f(x))$ is an m-th power in $\mathbb{F}_q$. Lemma 2.1 implies that $f(x)$ is an m-th power in $\mathbb{F}_{q^n}$. Hence, there exists an element $y \in \mathbb{F}_{q^n}$ such that $y^m = f(x)$. So $(x, y) \in \mathcal{C}(\mathbb{F}_{q^n})$. That means $(x, y) \in \pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n)$ and $\pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$.

Hence $\pi_{\mathcal{N}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$ if and only if $\pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$. Remarks 3.4 and 3.5 conclude the proof of this proposition. □

Theorem 3.7 *The number of* $\mathbb{F}_{q^n}$*-rational points on the affine curve* $\mathcal{C}$ *equals the number of* $\mathbb{F}_q$*-rational points on the affine variety* $\mathcal{N}$*; in formula*

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = \#\mathcal{N}(\mathbb{F}_q).$$

Proof. We consider the projection maps $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{N}}$. Then

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = \sum_{(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_q)} \#\pi_{\mathcal{C}}^{-1}(x_1, \ldots, x_n),$$

and

$$\#\mathcal{N}(\mathbb{F}_q) = \sum_{(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_q)} \#\pi_{\mathcal{N}}^{-1}(x_1, \ldots, x_n).$$

Now, Proposition 3.6 completes the proof of this theorem. □

In fact, one can show that the number of $\mathbb{F}_{q^n}$-rational points on the projective model of $\mathcal{C}$ equals the number of $\mathbb{F}_q$-rational points on the projective closure of $\mathcal{N}$ in $\mathbb{P}^{n+1}_{\mathbb{F}_q}$.

3.2 Trace variety

In this section, we define a hypersurface $\mathcal{T}$ over $\mathbb{F}_q$, called the *trace variety*, associated to a curve $\mathcal{X}$ over $\mathbb{F}_{q^n}$ in Artin-Schreier form. We shall show that the number of $\mathbb{F}_q$-rational points on $\mathcal{T}$ equals the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}$.

Let $\mathcal{X}$ be an absolutely irreducible nonsingular affine curve defined by an equation

$$\mathbf{y}^p - \mathbf{y} = F(\mathbf{x}), \tag{3.4}$$

where F is a rational function in $\mathbb{F}_{q^n}(\mathbf{x})$. So, let $F = \frac{u}{v}$ with u and v in $\mathbb{F}_{q^n}[\mathbf{x}]$, relatively prime and v monic. Let $U = \{x \in \mathbb{F}_{q^n} : v(x) \neq 0\}$. Then, to be precise,

$$\mathcal{X}(\mathbb{F}_{q^n}) = \{(x, y) \in U \times \mathbb{F}_{q^n} : y^p - y = F(x)\}.$$

Let $\mathcal{G}$ be the rational function in $\mathbb{F}_q(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ defined by

$$\mathcal{G}(\mathbf{x}_1, \mathbf{x}_2, , \ldots, \mathbf{x}_n) = \mathrm{Tr}(F(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2 + \ldots + \mathbf{x}_n\alpha_n)). \tag{3.5}$$

We write $\mathcal{G}$ as $\mathcal{F}/\mathcal{H}$, where $\mathcal{F}$, $\mathcal{H}$ are in $\mathbb{F}_q[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$ and

$$\mathcal{H}(\mathbf{x}_1, \mathbf{x}_2, , \ldots, \mathbf{x}_n) = \mathrm{N}(v(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2 + \ldots + \mathbf{x}_n\alpha_n)).$$

Let $W = \left\{(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n : \mathcal{H}(x_1, x_2, \ldots, x_n) \neq 0\right\}$ and let $x \in \mathbb{F}_{q^n}$, where $x = \sum_{i=1}^n x_i\alpha_i$, $x_i \in \mathbb{F}_q$. Then, $x \in U$ if and only if $(x_1, x_2, \ldots, x_n) \in W$.

Definition 3.8 *Let $\mathcal{T}$ be the affine variety defined by*

$$\mathbf{z}^p - \mathbf{z} - \mathcal{G}(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) = 0.$$

More precisely,

$$\mathcal{T}(\mathbb{F}_q) = \{(x_1, x_2, \ldots, x_n, z) \in W \times \mathbb{F}_q : z^p - z = \mathcal{G}(x_1, x_2, \ldots, x_n)\}.$$

Remark 3.9 Let $P = (x, y) \in \mathcal{X}(\mathbb{F}_{q^n})$, where $x = \sum_{j=1}^n x_j\alpha_j$ and $x_j \in \mathbb{F}_q$. So $y^p - y = F(x)$. Let $z = \mathrm{Tr}(y)$. Then $z^p - z = \mathrm{Tr}(y^p - y) = \mathrm{Tr}(F(x)) = \mathcal{G}(x_1, \ldots, x_n)$ (see Equation (3.5)). This implies that $(x_1, \ldots, x_n, z) \in \mathcal{T}(\mathbb{F}_q)$.

Consider the following diagram.

$$(x, y) \longmapsto (x_1, \ldots, x_n, \mathrm{Tr}(y))$$

$$\begin{array}{ccc} (x,y) & \mathcal{X}(\mathbb{F}_{q^n}) \longrightarrow \mathcal{T}(\mathbb{F}_q) & (x_1,\ldots,x_n,z) \\ \downarrow \pi_{\mathcal{X}} & \downarrow \pi_{\mathcal{X}} \quad\quad \downarrow \pi_{\mathcal{T}} & \downarrow \pi_{\mathcal{T}} \\ (x_1,\ldots,x_n) & \mathbb{A}^n(\mathbb{F}_q) \xrightarrow{id} \mathbb{A}^n(\mathbb{F}_q) & (x_1,\ldots,x_n) \end{array} \tag{3.6}$$

In Theorem 3.13, we show that the number of $\mathbb{F}_{q^n}$-rational points on the affine curve $\mathcal{X}$ equals the number of $\mathbb{F}_q$-rational points on the affine variety $\mathcal{T}$. For a proof of this theorem, we first make some remarks on the projection maps $\pi_{\mathcal{X}}$ and $\pi_{\mathcal{T}}$. Then, in Proposition 3.12, we show that fibers of $\pi_{\mathcal{X}}$ and $\pi_{\mathcal{T}}$ at the same point on $\mathbb{A}^n(\mathbb{F}_q)$ have equal cardinalities. This will conclude the proof of Theorem 3.13.

Remark 3.10 Let $P_0 = (x, y) \in \mathcal{X}(\mathbb{F}_{q^n})$ and let $P_i = (x, y + i)$, for all $0 \leq i < p$. Obviously $P_i \in \mathcal{X}(\mathbb{F}_{q^n})$. Also $\pi_{\mathcal{X}}(P_i) = (x_1, \ldots, x_n)$, for all $0 \leq i < p$, where $x = \sum_{k=1}^{n} x_k \alpha_k$. Furthermore $\pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n) = \{P_0, P_1, \ldots, P_{p-1}\}$. Therefore, if $\pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$, then $\#\pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n) = p$.

Remark 3.11 Let $P_0 = (x_1, \ldots, x_n, z) \in \mathcal{T}(\mathbb{F}_q)$ and let $P_i = (x_1, \ldots, x_n, z + i)$, for all all $0 \leq i < p$. Then $P_i \in \mathcal{T}(\mathbb{F}_q)$. The points P_i are pairwise distinct and are the only points on $\mathcal{T}$ whose first n coordinates equal $x_1, \ldots, x_n$. Hence, if $\pi_{\mathcal{T}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$, then $\#\pi_{\mathcal{T}}^{-1}(x_1, \ldots, x_n) = p$.

Proposition 3.12 *For all* $(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_q)$,

$$\#\pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n) = \#\pi_{\mathcal{T}}^{-1}(x_1, \ldots, x_n).$$

Proof. If $\pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$, then Remark 3.9 shows that $\pi_{\mathcal{T}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$.

Now assume that $\pi_{\mathcal{T}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$. Then there exists a point $(x_1, \ldots, x_n, z)$ on $\mathcal{T}(\mathbb{F}_q)$. Thus $z^p - z = \mathcal{G}(x_1, \ldots, x_n)$. Let $x = \sum_{j=1}^{n} x_j \alpha_j$. Then $z^p - z = \mathrm{Tr}(F(x))$ (see Equation (3.5)). Lemma 2.2 implies that there exists an element $y \in \mathbb{F}_{q^n}$ such that $y^p - y = F(x)$. So $(x, y) \in \mathcal{X}(\mathbb{F}_{q^n})$. This means $(x, y) \in \pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n)$ and $\pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$.

Hence $\pi_{\mathcal{T}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$ if and only if $\pi_{\mathcal{X}}^{-1}(x_1, \ldots, x_n) \neq \emptyset$. Remarks 3.10 and 3.11 conclude the proof of this proposition. □

Theorem 3.13 *The number of* $\mathbb{F}_{q^n}$*-rational points on the affine curve* $\mathcal{X}$ *equals the number of* $\mathbb{F}_q$*-rational points on the affine variety* $\mathcal{T}$*.*

$$\#\mathcal{X}(\mathbb{F}_{q^n}) = \#\mathcal{T}(\mathbb{F}_q).$$

Proof. Consider the projection maps $\pi_{\mathcal{X}}$ and $\pi_{\mathcal{T}}$. Then, Proposition 3.12 concludes the proof of this theorem. □

3.2.1 Example: trace surface for binary elliptic curve

Here, we provide an example of trace variety $\mathcal{T}$ associated to a binary elliptic curve E defined over a quadratic extension of a binary finite field. In this case $\mathcal{T}$

is an affine variety of dimension 2, and so-called a *trace surface*. In Chapter 4, we estimate the number of points on the intersections of trace surface $\mathcal{T}$ with coordinate hyperplanes.

Consider the finite field $\mathbb{F}_{q^2}$, where $q = 2^\ell$ and ℓ is a positive integer. Let E be an ordinary elliptic curve defined over $\mathbb{F}_{q^2}$ by the equation

$$\mathbf{y}^2 + \mathbf{xy} = \mathbf{x}^3 + a\mathbf{x}^2 + b,$$

where a and $b \neq 0$ are in $\mathbb{F}_{q^2}$. In this example, we describe the *trace surface* $\mathcal{T}$ associated to the elliptic curve E.

The Artin-Schreier form of E is defined by the equation $\mathbf{y}^2 + \mathbf{y} = F(\mathbf{x})$, where

$$F(\mathbf{x}) = \mathbf{x} + a + \frac{b}{\mathbf{x}^2}.$$

The rational function $\mathcal{G}$ in $\mathbb{F}_q(\mathbf{x}_1, \mathbf{x}_2)$ is defined by

$$\mathcal{G}(\mathbf{x}_1, \mathbf{x}_2) = \mathrm{Tr}(F(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2)).$$

So

$$\mathcal{G}(\mathbf{x}_1, \mathbf{x}_2) = \mathrm{Tr}(\alpha_1)\mathbf{x}_1 + \mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a) + \frac{\mathcal{D}^2(s_2\mathbf{x}_1 + s_1\mathbf{x}_2)^2}{\mathcal{H}^2(\mathbf{x}_1, \mathbf{x}_2)},$$

where

$$\begin{aligned}\mathcal{H}(\mathbf{x}_1, \mathbf{x}_2) &= \mathrm{N}(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2) \\ &= \mathrm{N}(\alpha_1)\mathbf{x}_1^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2^2 + \mathcal{D}\mathbf{x}_1\mathbf{x}_2,\end{aligned}$$

$\sqrt{b} = s_1\alpha_1 + s_2\alpha_2$ and $\mathcal{D} = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha_1^q & \alpha_2^q \end{vmatrix}$. Furthermore,

$$\mathcal{F}(\mathbf{x}_1, \mathbf{x}_2) = (\mathrm{Tr}(\alpha_1)\mathbf{x}_1 + \mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a))\mathcal{H}^2(\mathbf{x}_1, \mathbf{x}_2) + (\mathcal{D}(s_2\mathbf{x}_1 + s_1\mathbf{x}_2))^2.$$

The affine surface $\mathcal{T}$ is defined over $\mathbb{F}_q$ by the equation

$$\mathbf{z}^2 + \mathcal{H}(\mathbf{x}_1, \mathbf{x}_2)\mathbf{z} = \mathcal{F}(\mathbf{x}_1, \mathbf{x}_2). \tag{3.7}$$

Let $P = (x, y) \in E(\mathbb{F}_{q^2})$, where $x = x_1\alpha_1 + x_2\alpha_2$, $x_1, x_2 \in \mathbb{F}_q$. If $x = 0$, we have $(0, \sqrt{b}) \in E(\mathbb{F}_{q^2})$ and $(0, 0, 0) \in \mathcal{T}(\mathbb{F}_q)$. Assume $x \neq 0$. So, $(\frac{y}{x})^2 + \frac{y}{x} = F(x)$. Let $w = \mathrm{Tr}(\frac{y}{x})$. From Remark 3.9 we have

$$w^2 + w = \mathrm{Tr}(F(x)) = \mathcal{G}(x_1, x_2).$$

Let $z = wN(x) = w\mathcal{H}(x_1, x_2)$. Then

$$z^2 + h(x_1, x_2)z = \mathcal{H}^2(x_1, x_2)(w^2 + w) = \mathcal{H}^2(x_1, x_2)\mathcal{G}(x_1, x_2) = \mathcal{F}(x_1, x_2).$$

Hence $(x_1, x_2, z) \in \mathcal{T}(\mathbb{F}_q)$. So, similar to Diagram (3.6), we can consider the following diagram:

$$(x, y) \longmapsto (x_1, x_2, \mathrm{Tr}(\tfrac{y}{x})\mathrm{N}(x)), \qquad \text{for } x \neq 0$$

$$(0, \sqrt{b}) \longmapsto (0, 0, 0)$$

$$\begin{array}{ccccc} (x,y) & & E(\mathbb{F}_{q^2}) \setminus \{P_\infty\} & \longrightarrow & \mathcal{T}(\mathbb{F}_q) \\ \downarrow \pi_E & & \downarrow \pi_E & & \downarrow \pi_{\mathcal{T}} \\ (x_1, x_2) & & \mathbb{A}^2(\mathbb{F}_q) & \xrightarrow{id} & \mathbb{A}^2(\mathbb{F}_q) \end{array} \qquad \begin{array}{c} (x_1, x_2, z) \\ \downarrow \pi_{\mathcal{T}} \\ (x_1, x_2) \end{array}$$

Remark 3.14 From Proposition 3.12, for all $(x_1, x_2) \in \mathbb{A}^2(\mathbb{F}_q)$,

$$\#\pi_E^{-1}(x_1, x_2) = \#\pi_{\mathcal{T}}^{-1}(x_1, x_2).$$

It follows that

$$\#E(\mathbb{F}_{q^2}) = \#\mathcal{T}(\mathbb{F}_q) + 1.$$

Chapter 4

Extractors for Binary Elliptic Curves

In this chapter, we propose a simple and efficient deterministic extractor called `Ext` for an ordinary elliptic curve E, defined over $\mathbb{F}_{q^2}$, where $q = 2^\ell$ and ℓ is a positive integer. Our extractor, for a given point P on E, outputs the first $\mathbb{F}_q$-coefficient of the abscissa of the point P. Similarly one could define an extractor that, for a given point P on the curve E, outputs a $\mathbb{F}_q$-linear combination of $\mathbb{F}_q$-coordinates of the abscissa of P. We show that the output of this extractor, for a given uniformly random point of E, is statistically close to a uniform random variable in $\mathbb{F}_q$.

The reason why we consider ordinary elliptic curves is that solving the discrete logarithm (DL) problem in the group of points of a supersingular elliptic curve is easier than that in a ordinary elliptic curve (see [80]).

Note that the number of points of any ordinary elliptic curve defined over a finite field with characteristic two is even. Therefore, DDH problem in the corresponding group is easy and thus the group is not suitable for many cryptographic applications. In the case that the order of E equals $2m$ for odd m, we propose a deterministic extractor `ext` for the subgroup G of order m. This subgroup if often called the *main subgroup*. In particular, m can be chosen to be prime, so the DDH problem in the subgroup is assumed to be intractable. The extractor `ext` is a modified version of the extractor `Ext`.

An extended abstract of this chapter was previously published as: R. R. Farashahi and R. Pellikaan, and A. Sidorenko, Extractors for Binary Elliptic Curves, In *Proc. Workshop on Coding and Cryptography*, pages 127–136, 2007. The full version was published in *Designs, Codes and Cryptography*, 49(1–3):171–186, 2008. Open access at `http://www.springerlink.com/content/lm35kv103x34j754`.

In the next section, we define the extractor Ext based on E. By Theorem 4.3, we show tight estimates for the number of points on fibers of Ext. We give a proof of this theorem and by means of this theorem, we analyze our extractor.

4.1 The extractor for the elliptic curve E

Consider $\mathbb{F}_{q^2}$ as a quadratic extension of $\mathbb{F}_q$, where $q = 2^\ell$ and ℓ is a positive integer. Let $\{\alpha_1, \alpha_2\}$ be a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Let E be an ordinary elliptic curve defined over $\mathbb{F}_{q^2}$ by the equation

$$\mathbf{y}^2 + \mathbf{xy} = \mathbf{x}^3 + a\mathbf{x}^2 + b,$$

where a and $b \neq 0$ are in $\mathbb{F}_{q^2}$. The point at infinity of E is denoted by P_∞.

4.1.1 The extractor for E

Here, we give the definition of the extractor Ext based on the elliptic curve E over $\mathbb{F}_{q^2}$.

Definition 4.1 *The extractor* Ext *is defined by a function*

$$\begin{aligned} \texttt{Ext} : E(\mathbb{F}_{q^2}) &\longrightarrow \mathbb{F}_q \\ \texttt{Ext}(x, y) &= x_1, \\ \texttt{Ext}(P_\infty) &= 0. \end{aligned}$$

Remark 4.2 Similarly one could define an extractor that, for a given point P on the curve, outputs a $\mathbb{F}_q$-linear combination of the $\mathbb{F}_q$-coordinates of the x-coordinate of P. The analysis of this extractor is exactly the same as our extractor Ext, since one could interchange the basis $\{\alpha_1, \alpha_2\}$ with a suitable one. So without loss of generality we consider the extractor Ext.

The following theorem gives tight estimates for $\#\texttt{Ext}^{-1}(x_1)$, for all $x_1 \in \mathbb{F}_q$. The result of this theorem is used to analyze the extractor Ext.

Theorem 4.3 *For all* $x_1 \in \mathbb{F}_q^*$,

$$\left|\#\texttt{Ext}^{-1}(x_1) - q\right| \leq \begin{cases} [\,4\sqrt{q}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0, \\ [\,2\sqrt{q}\,] + 1 & \text{otherwise.} \end{cases}$$

and

$$\left|\#\texttt{Ext}^{-1}(0) - (q+1)\right| \leq \begin{cases} [\,2\sqrt{q}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0 \text{ and } s_1 \neq 0, \\ q - 1 & \text{if } \mathrm{Tr}(\alpha_2) = s_1 = 0, \\ 1 & \text{otherwise.} \end{cases}$$

For the proof of this theorem we need several propositions and lemmas. Consider the trace surface $\mathcal{T}$ related to the elliptic curve E (see Subsection 3.2.1). The surface $\mathcal{T}$ is defined over $\mathbb{F}_q$ by the equation

$$\mathbf{z}^2 + \mathcal{H}(\mathbf{x}_1, \mathbf{x}_2)\mathbf{z} = \mathcal{F}(\mathbf{x}_1, \mathbf{x}_2),$$

where

$$\mathcal{H}(\mathbf{x}_1, \mathbf{x}_2) = \mathrm{N}(\alpha_1)\mathbf{x}_1^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2^2 + \mathcal{D}\mathbf{x}_1\mathbf{x}_2,$$

$$\mathcal{F}(\mathbf{x}_1, \mathbf{x}_2) = (\mathrm{Tr}(\alpha_1)\mathbf{x}_1 + \mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a))\mathcal{H}^2(\mathbf{x}_1, \mathbf{x}_2) + (\mathcal{D}(s_2\mathbf{x}_1 + s_1\mathbf{x}_2))^2, \quad (4.1)$$

and where $\sqrt{b} = s_1\alpha_1 + s_2\alpha_2$ and $\mathcal{D} = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha_1^q & \alpha_2^q \end{vmatrix}$.

Fix the element x_1 in $\mathbb{F}_q$. Then the points of $\mathcal{T}$ that have the first coordinate equal to x_1 form a curve which we call $\mathcal{T}_{x_1}$.

Let $x_1 \in \mathbb{F}_q$. We define the affine curve $\mathcal{T}_{x_1}$ by the equation

$$T_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + \mathcal{H}_{x_1}(\mathbf{x}_2)\mathbf{z} + \mathcal{F}_{x_1}(\mathbf{x}_2) = 0, \quad (4.2)$$

where $\mathcal{F}_{x_1}(\mathbf{x}_2) = \mathcal{F}(x_1, \mathbf{x}_2)$ and $\mathcal{H}_{x_1}(\mathbf{x}_2) = \mathcal{H}(x_1, \mathbf{x}_2)$.

Proposition 4.4 *For all x_1 in $\mathbb{F}_q^*$,*

$$\#\mathtt{Ext}^{-1}(x_1) = \#\mathcal{T}_{x_1}(\mathbb{F}_q)$$

and

$$\#\mathtt{Ext}^{-1}(0) = 1 + \#\mathcal{T}_0(\mathbb{F}_q).$$

Proof. Let $x_1 \in \mathbb{F}_q^*$. Consider the projection maps π_E and $\pi_{\mathcal{T}}$ from Subsection 3.2.1. Then

$$\#\mathcal{T}_{x_1}(\mathbb{F}_q) = \sum_{x_2 \in \mathbb{F}_q} \#\pi_{\mathcal{T}}^{-1}(x_1, x_2)$$

and

$$\#\mathtt{Ext}^{-1}(x_1) = \sum_{x_2 \in \mathbb{F}_q} \#\pi_E^{-1}(x_1, x_2).$$

Remark 3.14 shows that $\#\pi_E^{-1}(x_1, x_2) = \#\pi_{\mathcal{T}}^{-1}(x_1, x_2)$, for all $x_1, x_2 \in \mathbb{F}_q$. Furthermore $P_\infty \in \mathtt{Ext}^{-1}(0)$. So the proof of this proposition is completed. □

The goal is now to estimate $\#\mathcal{T}_{x_1}(\mathbb{F}_q)$, for all $x_1 \in \mathbb{F}_q$. First we discuss this problem for all $x_1 \in \mathbb{F}_q^*$. In Propositions 4.5 and 4.6 we show that $\mathcal{T}_{x_1}$ is an absolutely irreducible nonsingular curve, for all $x_1 \in \mathbb{F}_q^*$. Then in Proposition 4.7 we give the bounds for $\#\mathcal{T}_{x_1}(\mathbb{F}_q)$, for all $x_1 \in \mathbb{F}_q^*$.

Proposition 4.5 *The affine curve $\mathcal{T}_{x_1}$ is absolutely irreducible, for all $x_1 \in \mathbb{F}_q^*$.*

Proof. The affine curve $\mathcal{T}_{x_1}$, for $x_1 \in \mathbb{F}_q^*$, is defined by the Equation (4.2). So, we consider the polynomial

$$T_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + \mathcal{H}_{x_1}(\mathbf{x}_2)\mathbf{z} + \mathcal{F}_{x_1}(\mathbf{x}_2).$$

First suppose $\mathrm{Tr}(\alpha_2) \neq 0$. Then the leading terms of $\mathcal{H}_{x_1}$ and $\mathcal{F}_{x_1}$ are respectively $\mathrm{N}(\alpha_2)\mathbf{x}_2^2$ and $\mathrm{Tr}(\alpha_2)(\mathrm{N}(\alpha_2))^2\mathbf{x}_2^5$. Hence $\deg(\mathcal{H}_{x_1}) = 2$ and $\deg(\mathcal{F}_{x_1}) = 5$. One can show that T_{x_1} is absolutely irreducible, e.g., by considering the Newton polygon of T_{x_1} (see [6, 43]).

Now suppose $\mathrm{Tr}(\alpha_2) = 0$. Then

$$\mathcal{F}_{x_1}(\mathbf{x}_2) = (\mathrm{Tr}(\alpha_1)x_1 + \mathrm{Tr}(a))\mathcal{H}_{x_1}^2(\mathbf{x}_2) + (\mathcal{D}(s_1\mathbf{x}_2 + s_2x_1))^2.$$

Let

$$R_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + \mathcal{H}_{x_1}(\mathbf{x}_2)\mathbf{z} + (\mathcal{D}(s_1\mathbf{x}_2 + s_2x_1))^2.$$

It is easy to see that a polynomial $\mathbf{z} + m(\mathbf{x}_2)$ in $\overline{\mathbb{F}}_q[\mathbf{x}_2, \mathbf{z}]$ is a factor of R_{x_1} if and only if the polynomial $\mathbf{z} + m(\mathbf{x}_2) + \gamma\mathcal{H}_{x_1}(\mathbf{x}_2)$ is a factor of T_{x_1}, where $\gamma \in \mathbb{F}_{q^2}$ such that $\gamma^2 + \gamma = \mathrm{Tr}(\alpha_1)x_1 + \mathrm{Tr}(a)$. So, T_{x_1} is absolutely irreducible if and only if R_{x_1} is so. Suppose R_{x_1} is reducible. So there exists a bivariate polynomial M in $\overline{\mathbb{F}}_q[\mathbf{x}_2, \mathbf{z}]$, which is a factor of R_{x_1}. We can consider

$$M(\mathbf{x}_2, \mathbf{z}) = \mathbf{z} + m(\mathbf{x}_2) = \mathbf{z} + m_1\mathbf{x}_2 + m_0.$$

We substitute $\mathbf{z}$ by m in the equation of R_{x_1}. Then we have the remainder

$$r(\mathbf{x}_2) = r_3\mathbf{x}_2^3 + r_2\mathbf{x}_2^2 + r_1\mathbf{x}_2 + r_0.$$

Since $r(\mathbf{x}_2) = 0$, we obtain the following equations.

$$\begin{cases} r_3 = m_1\mathrm{N}(\alpha_2) = 0 \\ r_2 = m_1^2 + \mathcal{D}m_1x_1 + m_0\mathrm{N}(\alpha_2) + (\mathcal{D}s_1)^2 = 0 \\ r_1 = m_1x_1^2\mathrm{N}(\alpha_1) + \mathcal{D}m_0x_1 = 0 \\ r_0 = m_0^2 + m_0x_1^2\mathrm{N}(\alpha_1) + (\mathcal{D}s_2x_1)^2 = 0. \end{cases}$$

It follows that $m_1 = 0$. Since $x_1 \neq 0$, also $m_0 = 0$. Hence $s_1 = s_2 = 0$ and thus $b = 0$, which is a contradiction. □

Proposition 4.6 *The affine curve $\mathcal{T}_{x_1}$ is nonsingular, for all $x_1 \in \mathbb{F}_q^*$.*

Proof. Suppose the affine curve $\mathcal{T}_{x_1}$ is singular, for some $x_1 \in \mathbb{F}_q^*$. Then the following system of equations has a solution $(x_2, z) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$:

$$\begin{cases} T_{x_1}(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + \mathcal{H}_{x_1}(\mathbf{x}_2)\mathbf{z} + \mathcal{F}_{x_1}(\mathbf{x}_2) = 0, \\ \dfrac{\partial T_{x_1}}{\partial \mathbf{x}_2}(\mathbf{x}_2, \mathbf{z}) = \mathcal{H}'_{x_1}(\mathbf{x}_2)\mathbf{z} + \mathcal{F}'_{x_1}(\mathbf{x}_2) = 0, \\ \dfrac{\partial T_{x_1}}{\partial \mathbf{z}}(\mathbf{x}_2, \mathbf{z}) = \mathcal{H}_{x_1}(\mathbf{x}_2) = 0, \end{cases} \tag{4.3}$$

where $\mathcal{H}'_{x_1}(\mathbf{x}_2)$ and $\mathcal{F}'_{x_1}(\mathbf{x}_2)$ are respectively the derivatives of $\mathcal{H}_{x_1}(\mathbf{x}_2)$ and $\mathcal{F}_{x_1}(\mathbf{x}_2)$ with respect to $\mathbf{x}_2$. We recall that $\mathcal{H}_{x_1}(\mathbf{x}_2) = \mathcal{H}(x_1, \mathbf{x}_2)$ and $\mathcal{F}_{x_1}(\mathbf{x}_2) = \mathcal{F}(x_1, \mathbf{x}_2)$. Then from System (4.3) and Equation (4.1) we obtain

$$z = \mathcal{D}(s_2 x_1 + s_1 x_2).$$

Because $\mathcal{H}'_{x_1}(x_2) = \mathcal{D}x_1$ and $\mathcal{F}'_{x_1}(x_2) = 0$, the second equation implies that $\mathcal{D}x_1 z = 0$. Since $x_1 \neq 0$, so $z = 0$. Thus $s_2 x_1 + s_1 x_2 = 0$. Then

$$s_1^2 \mathcal{H}(x_1, x_2) = x_1^2 \mathcal{H}(s_1, s_2) = x_1^2 \mathrm{N}(\sqrt{b}).$$

Hence $\mathrm{N}(\sqrt{b}) = 0$, since $x_1 \neq 0$. Therefore $b = 0$, which is a contradiction, because E is nonsingular. So the affine curve $\mathcal{T}_{x_1}$ is nonsingular. □

Proposition 4.7 *For all* $x_1 \in \mathbb{F}_q^*$,

$$|\#\mathcal{T}_{x_1}(\mathbb{F}_q) - q| \leq \begin{cases} [\,4\sqrt{q}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0, \\ [\,2\sqrt{q}\,] + 1 & \text{otherwise.} \end{cases}$$

Proof. The affine curve $\mathcal{T}_{x_1}$ is absolutely irreducible and nonsingular by Propositions 4.5 and 4.6, for $x_1 \in \mathbb{F}_q^*$. Let $\widetilde{\mathcal{T}}_{x_1}$ be the nonsingular projective model of $\mathcal{T}_{x_1}$.

First suppose $\mathrm{Tr}(\alpha_2) \neq 0$. Then $\widetilde{\mathcal{T}}_{x_1}$ is an imaginary hyperelliptic curve of genus 2. Since $\widetilde{\mathcal{T}}_{x_1}$ has exactly one point at infinity, it follow that

$$\#\mathcal{T}_{x_1}(\mathbb{F}_q) = \#\widetilde{\mathcal{T}}_{x_1}(\mathbb{F}_q) - 1.$$

Now suppose $\mathrm{Tr}(\alpha_2) = 0$. If $\mathrm{Tr}(\alpha_1)x_1 + \mathrm{Tr}(a) \neq 0$, then $\deg(\mathcal{F}_{x_1}) = 4$. By means of the Newton polygon of T_{x_1} we see that the genus of the nonsingular model of $\mathcal{T}_{x_1}$ is at most 1 (see Subsection 2.2). The projective model of $\mathcal{T}_{x_1}$ has only one point at infinity which is a singular point. The number of $\mathbb{F}_q$-rational points on $\widetilde{\mathcal{T}}_{x_1}$, which are lying over the point at infinity in the resolution map, is at most 2 (see Subsection 2.2). Hence

$$\left|\#\mathcal{T}_{x_1}(\mathbb{F}_q) - \#\widetilde{\mathcal{T}}_{x_1}(\mathbb{F}_q) + 1\right| \leq 1.$$

If $\mathrm{Tr}(\alpha_1)x_1 + \mathrm{Tr}(a) = 0$, then $\deg(\mathcal{F}_{x_1}) \leq 2$. The projective model of $\mathcal{T}_{x_1}$ has two points at infinity which are nonsingular points. The genus of the projective model of $\mathcal{T}_{x_1}$ is 1, since the degree of T_{x_1} is 3. Hence

$$\#\mathcal{T}_{x_1}(\mathbb{F}_q) = \#\widetilde{\mathcal{T}}_{x_1}(\mathbb{F}_q) - 2.$$

By means of the Hasse-Weil Theorem for $\widetilde{\mathcal{T}}_{x_1}$, we obtain the desired estimates for $\#\mathcal{T}_{x_1}(\mathbb{F}_q)$, which concludes the proof of this proposition. □

Now we consider the case that $x_1 = 0$. The curve $\mathcal{T}_0$ is defined by the equation

$$T_0(\mathbf{x}_2, \mathbf{z}) = \mathbf{z}^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2^2\mathbf{z} + \mathcal{F}_0(\mathbf{x}_2) = 0,$$

where $\mathcal{F}_0(\mathbf{x}_2) = (\mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a))(\mathrm{N}(\alpha_2))^2\mathbf{x}_2^4 + (\mathcal{D}s_1\mathbf{x}_2)^2$. Let $\mathbf{w} = \frac{\mathbf{z}}{\mathbf{x}_2}$. By means of this transformation, we define the affine curve $\widehat{\mathcal{T}}_0$ by the equation

$$\widehat{T}_0(\mathbf{x}_2, \mathbf{w}) = \mathbf{w}^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2\mathbf{w} + \widehat{\mathcal{F}}_0(\mathbf{x}_2) = 0, \tag{4.4}$$

where $\widehat{\mathcal{F}}_0(\mathbf{x}_2) = (\mathrm{Tr}(\alpha_2)\mathbf{x}_2 + \mathrm{Tr}(a))(\mathrm{N}(\alpha_2))^2\mathbf{x}_2^2 + (\mathcal{D}s_1)^2$.

Lemma 4.8 *The affine curves $\mathcal{T}_0$ and $\widehat{\mathcal{T}}_0$ have the same number of $\mathbb{F}_q$-rational points.*

Proof. Let $x \in \mathbb{F}_q^*$. One can see that $(x, z) \in \mathcal{T}_0(\mathbb{F}_q)$ if and only if $(x, \frac{z}{x}) \in \widehat{\mathcal{T}}_0(\mathbb{F}_q)$. Furthermore, the points $(0, 0)$ and $(0, \mathcal{D}s_1)$ are the only points with x-coordinate equal to 0 respectively on $\mathcal{T}_0$ and $\widehat{\mathcal{T}}_0$. □

We discuss the irreducibility and nonsingularity of $\widehat{\mathcal{T}}_0$ in Propositions 4.9 and 4.10. Then in Proposition 4.11 we give bounds for $\#\widehat{\mathcal{T}}_0(\mathbb{F}_q)$.

Proposition 4.9 *The curve $\widehat{\mathcal{T}}_0$ is reducible if and only if* $\mathrm{Tr}(\alpha_2) = s_1 = 0$.

Proof. The affine curve $\widehat{\mathcal{T}}_0$ is defined by the Equation (4.4). If $\mathrm{Tr}(\alpha_2) \neq 0$, then $\deg(\widehat{\mathcal{F}}_0) = 3$ and clearly $\widehat{\mathcal{T}}_0$ is absolutely irreducible. Now assume $\mathrm{Tr}(\alpha_2) = 0$. Let

$$\widehat{R}_0(\mathbf{x}_2, \mathbf{w}) = \mathbf{w}^2 + \mathrm{N}(\alpha_2)\mathbf{x}_2\mathbf{w} + (\mathcal{D}s_1)^2.$$

Then $\widehat{\mathcal{T}}_0$ is absolutely irreducible if and only if $\widehat{R}_0$ is so. Furthermore $\widehat{R}_0$ is absolutely irreducible if and only if $s_1 \neq 0$. □

Proposition 4.10 *The affine curve $\widehat{\mathcal{T}}_0$ is singular if and only if* $s_1 = 0$.

Proof. It is easy to see that the affine curve $\widehat{\mathcal{T}}_0$ has a singular point P if and only if $P = (0, 0)$ and $s_1 = 0$. □

Proposition 4.11 *The number of $\mathbb{F}_q$-rational points on the affine curve $\widehat{\mathcal{T}}_0$ satisfies*

$$\left|\#\widehat{\mathcal{T}}_0(\mathbb{F}_q) - q\right| \leq \begin{cases} [\,2\sqrt{q}\,] & \text{if } \mathrm{Tr}(\alpha_2) \neq 0 \text{ and } s_1 \neq 0, \\ q-1 & \text{if } \mathrm{Tr}(\alpha_2) = s_1 = 0, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let $\widetilde{\mathcal{T}}_0$ be the nonsingular projective model of $\widehat{\mathcal{T}}_0$. First suppose $s_1 \neq 0$. Propositions 4.9 and 4.10 imply, the curve $\widehat{\mathcal{T}}_0$ is absolutely irreducible and nonsingular. The curve $\widetilde{\mathcal{T}}_0$ is an elliptic curve, if $\mathrm{Tr}(\alpha_2) \neq 0$. Hence

$$\#\widehat{\mathcal{T}}_0(\mathbb{F}_q) = \#\widetilde{\mathcal{T}}_0(\mathbb{F}_q) - 1.$$

If $\mathrm{Tr}(\alpha_2) = 0$, the curve $\widetilde{\mathcal{T}}_0$ has genus 0. Also it has two points at infinity. So

$$\#\widehat{\mathcal{T}}_0(\mathbb{F}_q) = \#\widetilde{\mathcal{T}}_0(\mathbb{F}_q) - 2.$$

Now, suppose $s_1 = 0$. If $\mathrm{Tr}(\alpha_2) \neq 0$, from Proposition 4.9, the curve $\widehat{\mathcal{T}}_0$ is absolutely irreducible. But it has the singular point $(0,0)$. Hence the genus of the curve $\widetilde{\mathcal{T}}_0$ equals 0. The number of $\mathbb{F}_q$-rational points on $\widetilde{\mathcal{T}}_0$, which are lying over the point $(0,0)$ in the resolution map, is 0 or 2. Furthermore the point at infinity is ramified. Hence

$$\#\widehat{\mathcal{T}}_0(\mathbb{F}_q) = \#\widetilde{\mathcal{T}}_0(\mathbb{F}_q) \pm 2.$$

From the Hasse-Weil Theorem for curve $\widetilde{\mathcal{T}}_0$, we can obtain the estimates for $\#\widehat{\mathcal{T}}_0(\mathbb{F}_q)$. If $\mathrm{Tr}(\alpha_2) = 0$, from Proposition 4.9, the curve $\widehat{\mathcal{T}}_0$ is reducible. So we have a trivial bound for $\#\widehat{\mathcal{T}}_0(\mathbb{F}_q)$. □

Proof of Theorem 4.3. Propositions 4.4 and 4.7 show the proof of Theorem 4.3, for $x_1 \in \mathbb{F}_q^*$. Furthermore, Propositions 4.4, 4.11 and Lemma 4.8 show the proof of this theorem, for $x_1 = 0$. □

4.1.2 Analysis of the extractor

In this subsection we show that provided the point P is chosen uniformly at random in $E(\mathbb{F}_{q^2})$, the element extracted from the point P by `Ext` is indistinguishable from a uniformly random element in $\mathbb{F}_q$.

Let X be an $\mathbb{F}_q$-valued random variable that is defined by

$$X = \mathtt{Ext}(P), \text{ for } P \in_R E(\mathbb{F}_{q^2}).$$

Proposition 4.12 *The random variable X is statistically close to the the uniform random variable $U_{\mathbb{F}_q}$.*

$$\Delta(X, U_{\mathbb{F}_q}) = O\left(\frac{1}{\sqrt{q}}\right).$$

Proof. Let $z \in \mathbb{F}_q$. Then, for the uniform random variable $U_{\mathbb{F}_q}$ in $\mathbb{F}_q$, we have $\Pr[U_{\mathbb{F}_q} = z] = 1/q$, while for the $\mathbb{F}_q$-valued random variable X,

$$\Pr[X = z] = \frac{\#\mathtt{Ext}^{-1}(z)}{\#E(\mathbb{F}_{q^2})}.$$

Hence

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_q}) =& \frac{1}{2}\sum_{z\in\mathbb{F}_q}\left|\Pr[X = z] - \Pr[U_{\mathbb{F}_q} = z]\right| \\ =& \frac{1}{2}\sum_{z\in\mathbb{F}_q}\left|\frac{\#\mathtt{Ext}^{-1}(z)}{\#E(\mathbb{F}_{q^2})} - \frac{1}{q}\right|.\end{aligned}$$

The Hasse-Weil Theorem gives the bound for $\#E(\mathbb{F}_{q^2})$ and Theorem 4.3 gives the bound for the cardinality of $\mathtt{Ext}^{-1}(z)$, for all $z \in \mathbb{F}_q$.

Let $g = 2$ if $\mathrm{Tr}(\alpha_2) \neq 0$, otherwise let $g = 1$. In fact g is the maximum genus of curves $\mathcal{T}_{x_1}$, for all $x_1 \in \mathbb{F}_{q^2}$ (see the proof of Proposition 4.7). First assume $s_1 \neq 0$ or $\mathrm{Tr}(\alpha_2) \neq 0$. So

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_q}) =& \frac{1}{2q\#E(\mathbb{F}_{q^2})}\sum_{z\in\mathbb{F}_q}\left|q\#\mathtt{Ext}^{-1}(z) - \#E(\mathbb{F}_{q^2})\right| \\ \leq& \frac{q(q(q + g\sqrt{q} + 2 - g) - (q^2 - 2q + 1))}{2q(q^2 - 2q + 1)} \\ =& \frac{2q\sqrt{q}g + (4 - g)q - 1}{2(q - 1)^2} = \frac{g + \epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q) = \frac{(4-g)q\sqrt{q}+4gq-\sqrt{q}-2g}{2(q-1)^2}$. Indeed $\epsilon(q) < 1$, for $\ell \geq 3$.

Now assume $\mathrm{Tr}(\alpha_2) = s_1 = 0$. Theorem 4.3 gives a trivial bound for $\#\mathtt{Ext}^{-1}(0)$. Then

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_q}) =& \frac{\left|q\#\mathtt{Ext}^{-1}(0) - \#E(\mathbb{F}_{q^2})\right|}{2q\#E(\mathbb{F}_{q^2})} + \sum_{z\in\mathbb{F}_q^*}\frac{\left|q\#\mathtt{Ext}^{-1}(z) - \#E(\mathbb{F}_{q^2})\right|}{2q\#E(\mathbb{F}_{q^2})}. \\ \leq& \frac{(q^2 + 2q - 1) + (q - 1)(2q\sqrt{q} + 3q - 1)}{(q - 1)^2} \\ =& \frac{q\sqrt{q} + 2q - \sqrt{q} - 1}{(q - 1)^2} = \frac{1 + \epsilon(q)}{\sqrt{q}} = \frac{g + \epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q) = \frac{2q\sqrt{q}+q-\sqrt{q}-1}{(q-1)^2}$. Furthermore $\epsilon(q) < 1$, for $\ell \geq 4$. □

Corollary 4.13 *The extractor* `Ext` *is* $(\ell, \frac{3}{\sqrt{q}})$*-deterministic for* $E(\mathbb{F}_{q^2})$*, for* $\ell \geq 4$.

Proof. The proof of Proposition 4.12 gives $\Delta(X, U_{\mathbb{F}_q}) \leq \frac{g+\epsilon(q)}{\sqrt{q}}$, where $g \leq 2$ and $\epsilon(q) < 1$, for $\ell \geq 4$. □

4.2 The extractor for a subgroup

In Section 2.10.1, we proposed a way to construct an extractor for the main subgroup based on an extractor of the full group in order to use only the subgroup of cryptographic interest. Here, we provide an example of that construction and in particular we explain how to choose the distinguishing function. We define a modified version of the extractor `Ext` for the *main subgroup* of the elliptic curve E defined over $\mathbb{F}_{q^2}$, where E has minimal 2-torsion.

Let $\#E(\mathbb{F}_{q^2}) = 2^d m$, where m is odd. If $d = 1$, then E is said to have minimal 2-torsion. We note that E has minimal 2-torsion if and only if $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(a) = 1$ (e.g., see [64, 86]). This means half of the elliptic curves defined over $\mathbb{F}_{q^2}$, have minimal 2-torsion.

Assume that E has minimal 2-torsion. Hence $\#E(\mathbb{F}_{q^2}) = 2m$. Let G be the subgroup of E of odd order m. E has point $P_0 = (0, \sqrt{b})$ of order 2. The point P is in the subgroup G if and only if $P = 2Q$, for some point $Q \in E(\mathbb{F}_{q^2})$. In [87, 94] it is shown a point $P = (x, y) \in E(\mathbb{F}_{q^2})$ is in G if and only if $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(x) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(a) = 1$.

Let β be a bit distinguishing $P = (x, y)$ from $-P = (x, x + y)$ satisfying

$$\begin{aligned} &\beta : E(\mathbb{F}_{q^2}) \longrightarrow \{0, 1\} \\ &\beta(P) = 0, \text{ if } P = -P, \\ &\beta(P) + \beta(-P) = 1, \text{ if } P \neq -P. \end{aligned}$$

Note that if $P \in G$ and $P \neq P_\infty$, then $-P \neq P$, since the order of G is odd. For example the function β can be defined as the least significant bit of y/x, if we consider the polynomial basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_2$. Furthermore the point $P = (x, y)$ can be represented by (x, λ), where $\lambda = x + y/x$, is the slope of the doubling. If we represent $P = (x, y)$, by (x, λ), then $-P = (x, x + y)$ is represented by $(x, \lambda + 1)$. Hence the function β can be defined as the least significant bit of λ. Another way to define the function β is to define an order on the representation of elements

in $\mathbb{F}_{q^2}$. Every element in $\mathbb{F}_{q^2}$ is represented by a bit string. Hence this order, for instance, can be the lexicographical order. Then this order distinguishes y from $x+y$ or P from $-P$.

Consider the extractor $\texttt{Ext}$ for E presented in Section 4.1. The extractor $\texttt{ext}$ for the main subgroup G is defined by

$$\begin{aligned}&\texttt{ext} : G \longrightarrow \mathbb{F}_q\\ &\texttt{ext}(P) = \texttt{Ext}(P + \beta(P)P_0).\end{aligned}$$

Let $P = (x, y) \in G$. If $\beta(P) = 0$, then $\texttt{ext}(P) = \texttt{Ext}(P)$. If $\beta(P) = 1$, then $\texttt{ext}(P) = \texttt{Ext}(P + P_0)$. It is easy to see that the abscissa of the point $P + P_0$ is $\frac{\sqrt{b}}{x}$. Hence

$$\texttt{ext}(P) = \begin{cases} x_1, & \text{if } \beta(P) = 0\\ (\dfrac{\sqrt{b}}{x})_1, & \text{if } \beta(P) = 1.\end{cases}$$

Proposition 4.14 *The extractor* $\texttt{ext}$ *is* $(\ell, \frac{3}{\sqrt{q}})$*-deterministic for* G*, for* $\ell \geq 4$*.*

Proof. We note that $\texttt{Ext}(P) = \texttt{Ext}(-P)$ for all $P \in E(\mathbb{F}_{q^2})$. Furthermore, $\texttt{Ext}(P_\infty) = \texttt{Ext}(P_0)$. Then Proposition 2.34 and Corollary 4.13 conclude the proof of this proposition. □

Chapter 5

The Quadratic Extension Extractor for (Hyper)elliptic Curves

In this chapter, we propose a simple and efficient deterministic extractor, called `Ext`, for an (hyper)elliptic curve $\mathcal{C}$, defined over $\mathbb{F}_{q^2}$, where q is some power of an odd prime. For a given point P on $\mathcal{C}$, the extractor `Ext` outputs the *first* $\mathbb{F}_q$-coefficient of the abscissa of the point P. Similarly one could define an extractor that, for a given point on the curve, outputs a $\mathbb{F}_q$-linear combination of $\mathbb{F}_q$-coordinates of the abscissa of the point.

Gürel [49] proposed an extractor for an elliptic curve E defined over a quadratic extension of a prime field. Given a point P on $\mathrm{E}(\mathbb{F}_{p^2})$, it extracts half of the bits of the abscissa of P. If the point P is chosen uniformly at random, the statistical distance between the bits extracted from the point P and uniformly random bits is shown to be negligible [49]. We recall this extractor for E in Subsection 5.2.2 and we improve that result in Theorem 5.16. The definition of our extractor is similar, yet more general. Our extractor `Ext` is defined for $\mathcal{C}$.

This chapter is organized as follows. In the next section, we define the extractor `Ext` based on the affine curve $\mathcal{C}$. In Theorem 5.16, we give the estimates for the number of points on fibers of `Ext`. Further, by means of this theorem, we analyze

The result of this chapter was previously published as: R. R. Farashahi and R. Pellikaan, The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic. In *International Workshop on the Arithmetic of Finite Fields–WAIFI 2007*, volume 4547 of *Lecture Notes in Computer Science*, pages 219–236. Springer-Verlag, 2007.

our extractor; we show that if a point is chosen uniformly at random in $\mathcal{C}$, the element extracted from the point is indistinguishable from a uniformly random variable in $\mathbb{F}_q$. At the end, we give examples of the extractor `Ext`. In Section 5.2, we provide some examples for the extractors `Ext`.

5.1 The quadratic extension extractor

Consider the finite field $\mathbb{F}_{q^2}$, where q is a power of a prime p, and let $\{\alpha_1, \alpha_2\}$ be a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Let $\mathcal{C}$ be an affine curve defined over $\mathbb{F}_{q^2}$ by the equation

$$\mathbf{y}^2 = f(\mathbf{x}), \tag{5.1}$$

where $f(\mathbf{x}) \in \mathbb{F}_{q^2}[\mathbf{x}]$ is a monic square-free polynomial of odd degree d. Let

$$f(\mathbf{x}) = \mathbf{x}^d + \sum_{i=0}^{d-1} f_i \mathbf{x}^i = \prod_{i=1}^{d} (\mathbf{x} - \lambda_i), \tag{5.2}$$

where $f_i \in \mathbb{F}_{q^2}$ and $\lambda_i \in \overline{\mathbb{F}}_q$. Then $\lambda_i \neq \lambda_j$, for $i \neq j$, since $f(\mathbf{x})$ is square-free.

In this section we introduce an extractor that works for the affine curve $\mathcal{C}$. The extractor, for a given point on the curve, outputs the *first* $\mathbb{F}_q$-coordinate of the abscissa of the point. Then, we show that the output of this extractor, for a given uniformly random point of $\mathcal{C}$, is statistically close to a uniform random variable in $\mathbb{F}_q$.

5.1.1 The extractor for $\mathcal{C}$

Now, we provide the definition of the extractor `Ext` based on the affine curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$.

Definition 5.1 *The extractor* `Ext` *is defined by a function*

$$\begin{aligned} &\texttt{Ext} : \mathcal{C}(\mathbb{F}_{q^2}) \longrightarrow \mathbb{F}_q \\ &\texttt{Ext}(x, y) = x_1. \end{aligned}$$

In Theorem 5.16, we give bounds for $\#\texttt{Ext}^{-1}(x_1)$, for all x_1 in $\mathbb{F}_q$. For the proof of this theorem, we need several lemmas and propositions. We consider the norm surface $\mathcal{N}$ related to the curve $\mathcal{C}$. Then, we define the affine curve $\mathcal{N}_{x_1}$ as the intersection of the affine variety $\mathcal{N}$ and the hyperplane $\mathbf{x}_1 = x_1$, for x_1 in $\mathbb{F}_q$. Next, in Proposition 5.3, we show that $\#\mathcal{N}_{x_1}(\mathbb{F}_q) = \#\texttt{Ext}^{-1}(x_1)$, for all x_1 in $\mathbb{F}_q$. We show that the curve $\mathcal{N}_{x_1}$ is reducible if and only if $x_1 \in \mathcal{I}$ (Proposition 5.8) and the curve $\mathcal{N}_{x_1}$ is singular if and only if $x_1 \in \mathcal{S}$ (Proposition 5.10), where the sets

$\mathcal{I}$, $\mathcal{S}$ are defined in Definition 5.6. If the curve $\mathcal{N}_{x_1}$ is absolutely irreducible and singular, we consider the curve $\mathcal{X}_{x_1}$, that is a nonsingular plane model of $\mathcal{N}_{x_1}$. By using the Hasse-Weil bound for the curve $\mathcal{X}_{x_1}$, we obtain a bound for $\#\mathcal{N}_{x_1}(\mathbb{F}_q)$, where $x_1 \notin \mathcal{I}$ (Proposition 5.15). Note that we have a trivial bound for $\#\mathcal{N}_{x_1}(\mathbb{F}_q)$, if $x_1 \in \mathcal{I}$. Then Proposition 5.3 concludes the proof of Theorem 5.16.

Let $\mathcal{N}$ be the *norm surface* related to the curve $\mathcal{C}$ (see Section 3.1). So, the affine surface $\mathcal{N}$ is defined over $\mathbb{F}_q$ by the equation

$$\mathbf{z}^2 - \mathcal{F}(\mathbf{x}_1, \mathbf{x}_2) = 0,$$

where $\mathcal{F}$ is a polynomial in $\mathbb{F}_q[\mathbf{x}_1, \mathbf{x}_2]$ defined by

$$\mathcal{F}(\mathbf{x}_1, \mathbf{x}_2) = \mathrm{N}(f(\mathbf{x}_1\alpha_1 + \mathbf{x}_2\alpha_2)).$$

Fix the element x_1 in $\mathbb{F}_q$. Then the points of $\mathcal{N}$ that have the first coordinate equal to x_1 form a curve which we call $\mathcal{N}_{x_1}$.

Definition 5.2 *Let $x_1 \in \mathbb{F}_q$. Let $\mathcal{N}_{x_1}$ be the affine curve defined by the equation*

$$\mathbf{z}^2 - \mathcal{F}_{x_1}(\mathbf{x}_2) = 0,$$

where $\mathcal{F}_{x_1}(\mathbf{x}_2) = \mathcal{F}(x_1, \mathbf{x}_2)$.

Proposition 5.3 *$\#\mathcal{N}_{x_1}(\mathbb{F}_q) = \#\mathtt{Ext}^{-1}(x_1)$, for all x_1 in $\mathbb{F}_q$.*

Proof. Let $x_1 \in \mathbb{F}_q$. We consider the projection maps $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{N}}$ from Diagram 3.3. Then

$$\#\mathcal{N}_{x_1}(\mathbb{F}_q) = \sum_{x_2 \in \mathbb{F}_q} \#\pi_{\mathcal{N}}^{-1}(x_1, x_2),$$

and

$$\#\mathtt{Ext}^{-1}(x_1) = \sum_{x_2 \in \mathbb{F}_q} \#\pi_{\mathcal{C}}^{-1}(x_1, x_2).$$

Proposition 3.6 shows that $\#\pi_{\mathcal{C}}^{-1}(x_1, x_2) = \#\pi_{\mathcal{N}}^{-1}(x_1, x_2)$, for all $x_1, x_2 \in \mathbb{F}_q$. So the proof of this proposition is complete. □

Remark 5.4 For $x_1 \in \mathbb{F}_q$, we have $\mathcal{F}_{x_1}(\mathbf{x}_2) = \mathrm{N}(f(x_1\alpha_1 + \mathbf{x}_2\alpha_2))$. From Equation (5.2), we obtain

$$\mathcal{F}_{x_1}(\mathbf{x}_2) = \prod_{i=1}^{d} (x_1\alpha_1 + \mathbf{x}_2\alpha_2 - \lambda_i)(x_1\phi(\alpha_1) + \mathbf{x}_2\phi(\alpha_2) - \phi(\lambda_i)).$$

Let $\theta_i = \frac{\lambda_i - x_1\alpha_1}{\alpha_2}$, for $i \in \{1, 2, \ldots, d\}$. Then $\phi(\theta_i) = \frac{\phi(\lambda_i) - x_1\phi(\alpha_1)}{\phi(\alpha_2)}$. Hence

$$\mathcal{F}_{x_1}(\mathbf{x}_2) = (\mathrm{N}(\alpha_2))^d \prod_{i=1}^{d}((\mathbf{x}_2 - \theta_i)(\mathbf{x}_2 - \phi(\theta_i)). \tag{5.3}$$

We note that $\theta_i \neq \theta_j$ and $\phi(\theta_i) \neq \phi(\theta_j)$, for $i \neq j$, since $\lambda_i \neq \lambda_j$, for $i \neq j$.

Definition 5.5 *For $x_1 \in \mathbb{F}_q$, let $\theta_i = \frac{\lambda_i - x_1\alpha_1}{\alpha_2}$, for $i \in \{1, 2, \ldots, d\}$. Let*

$$S_{x_1} = \{\theta_1, \theta_2, \ldots, \theta_d\} \cap \{\phi(\theta_1), \phi(\theta_2), \ldots, \phi(\theta_d)\},$$

and let $d_{x_1} = \#S_{x_1}$.

In Proposition 5.10, we show that a point $(\theta, 0)$ with $\theta \in S_{x_1}$ is a singular point of $\mathcal{N}_{x_1}$. Hence the curve $\mathcal{N}_{x_1}$ has d_{x_1} singular points.

Definition 5.6 *For $i, j \in \{1, 2, \ldots, d\}$, let*

$$s_{i,j} = \frac{\begin{vmatrix} \lambda_i & \alpha_2 \\ \phi(\lambda_j) & \phi(\alpha_2) \end{vmatrix}}{\begin{vmatrix} \alpha_1 & \alpha_2 \\ \phi(\alpha_1) & \phi(\alpha_2) \end{vmatrix}}.$$

Put $\mathcal{S} = \{s_{i,j} : i, j \in \{1, 2, \ldots, d\}\} \bigcap \mathbb{F}_q$ and $\mathcal{I} = \{s \in \mathcal{S} : d_s = d\}$.

Remark 5.7 Suppose $\theta_i = \phi(\theta_j)$, for some indexes i, j. Then

$$\frac{\lambda_i - x_1\alpha_1}{\alpha_2} = \frac{\phi(\lambda_j) - x_1\phi(\alpha_1)}{\phi(\alpha_2)}.$$

Thus

$$x_1 = \frac{\lambda_i\phi(\alpha_2) - \phi(\lambda_j)\alpha_2}{\alpha_1\phi(\alpha_2) - \phi(\alpha_1)\alpha_2} = s_{i,j}.$$

The converse is also true. That means $x_1 = s_{i,j}$ if and only if $\theta_i = \phi(\theta_j)$. Furthermore

$$d_{x_1} = \#\{(i, j) : s_{i,j} = x_1\}.$$

So $x_1 \notin \mathcal{S}$ if and only if $d_{x_1} = 0$.

Proposition 5.8 *Let $x_1 \in \mathbb{F}_q$. The affine plane curve $\mathcal{N}_{x_1}$ is absolutely irreducible if and only if $x_1 \notin \mathcal{I}$.*

Proof. The affine curve $\mathcal{N}_{x_1}$ is defined by the equation $\mathbf{z}^2 = \mathcal{F}_{x_1}(\mathbf{x}_2)$. The curve $\mathcal{N}_{x_1}$ is reducible if and only if $\mathcal{F}_{x_1}$ is a square in $\overline{\mathbb{F}}_q[\mathbf{x}_2]$. From Equation (5.3), $\mathcal{F}_{x_1}$ is a square in $\overline{\mathbb{F}}_q[\mathbf{x}_2]$ if and only if $\{\theta_1, \theta_2, \ldots, \theta_d\} = \{\phi(\theta_1), \phi(\theta_2), \ldots, \phi(\theta_d)\}$. Remark 5.7 explains that this is equivalent to $d_{x_1} = d$. □

Remark 5.9 Assume that the affine curve $\mathcal{N}_{x_1}$, for some $x_1 \in \mathbb{F}_q$, is reducible. So from the proof of Proposition 5.8 we have

$$\{\theta_1, \theta_2, \ldots, \theta_d\} = \{\phi(\theta_1), \phi(\theta_2), \ldots, \phi(\theta_d)\}.$$

Hence $\sum_{i=1}^{d} \theta_i = \sum_{i=1}^{d} \phi(\theta_i)$. Therefore

$$\sum_{i=1}^{d} \frac{\lambda_i - x_1\alpha_1}{\alpha_2} = \sum_{i=1}^{d} \frac{\phi(\lambda_i) - x_1\phi(\alpha_1)}{\phi(\alpha_2)}.$$

Because $\sum_{i=1}^{d} \lambda_i = -f_{d-1}$ (see Equation (5.2)), we have

$$-dx_1 = \frac{f_{d-1}\phi(\alpha_2) - \phi(f_{d-1})\alpha_2}{\alpha_1\phi(\alpha_2) - \phi(\alpha_1)\alpha_2}.$$

In other words, if $x_1 \in \mathcal{I}$, then

$$-dx_1 = \frac{\begin{vmatrix} f_{d-1} & \alpha_2 \\ \phi(f_{d-1}) & \phi(\alpha_2) \end{vmatrix}}{\begin{vmatrix} \alpha_1 & \alpha_2 \\ \phi(\alpha_1) & \phi(\alpha_2) \end{vmatrix}}.$$

Note that the converse is not true. If d is not divisible by p, then $\#\mathcal{I} \leq 1$. If d is divisible by p we only have $\#\mathcal{I} \leq d$.

Proposition 5.10 *Let $x_1 \in \mathbb{F}_q$. The affine curve $\mathcal{N}_{x_1}$ is singular if and only if $x_1 \in \mathcal{S}$. The curve $\mathcal{N}_{x_1}$ has d_{x_1} singular points.*

Proof. The point $(x_2, z) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ is a singular point on $\mathcal{N}_{x_1}$ if and only if $z = 0$ and x_2 is a double root of $\mathcal{F}_{x_1}(\mathbf{x}_2)$. From Equation (5.3), x_2 is a double root of $\mathcal{F}_{x_1}(\mathbf{x}_2)$ if and only if $x_2 \in S_{x_1}$. So $\mathcal{N}_{x_1}$ has d_{x_1} singular points. Remark 5.7 explains that there exists $x_2 \in S_{x_1}$ if and only if $x_1 = s_{i,j}$, for some indexes i, j. Since $x_1 \in \mathbb{F}_q$, we conclude that $x_1 \in \mathcal{S}$ if and only if $\mathcal{N}_{x_1}$ is singular. □

For $x_1 \in \mathbb{F}_q$, let $g_{x_1}(\mathbf{x}_2) = \prod_{\theta \in S_{x_1}} (\mathbf{x}_2 - \theta)$. We note that $\theta \in S_{x_1}$ if and only if $\phi(\theta) \in S_{x_1}$. Hence $\phi(g_{x_1)} = g_{x_1}$. So g_{x_1} is defined over $\mathbb{F}_q[\mathbf{x}_2]$, its degree degree is d_{x_1}. Let

$$\mathcal{F}_{x_1}(\mathbf{x}_2) = g_{x_1}^2(\mathbf{x}_2)\mathcal{H}_{x_1}(\mathbf{x}_2),$$

where $\mathcal{H}_{x_1}$ is a square free polynomial of degree $2(d - d_{x_1})$ in $\mathbb{F}_q[\mathbf{x}_2]$ (see Equation (5.3)).

Definition 5.11 *For $x_1 \in \mathbb{F}_q$, let $\mathcal{X}_{x_1}$ be the affine curve given by the equation*

$$\mathbf{w}^2 - \mathcal{H}_{x_1}(\mathbf{x}_2) = 0.$$

Proposition 5.12 *Let $x_1 \in \mathbb{F}_q$. The affine curve $\mathcal{X}_{x_1}$ is absolutely irreducible and nonsingular if and only if $x_1 \notin \mathcal{I}$.*

Proof. The affine curve $\mathcal{X}_{x_1}$ is defined by the equation $\mathbf{w}^2 = \mathcal{H}_{x_1}(\mathbf{x}_2)$. Since $\mathcal{H}_{x_1}$ is a square-free polynomial of degree $2(d - d_{x_1})$ in $\mathbb{F}_q[\mathbf{x}_2]$, $\mathcal{X}_{x_1}$ is absolutely irreducible and nonsingular if and only if $\mathcal{H}_{x_1}$ is not constant. Clearly $\mathcal{H}_{x_1}$ is constant if and only if $d_{x_1} = d$. That means $\mathcal{H}_{x_1}$ is reducible if and only if $x_1 \in \mathcal{I}$. □

Remark 5.13 Let $x_1 \in \mathbb{F}_q$. If $\mathcal{H}_{x_1}$ is not constant, the affine curve $\mathcal{X}_{x_1}$ is a nonsingular plane model of $\mathcal{N}_{x_1}$.

Proposition 5.14 *For $x_1 \in \mathbb{F}_q$, $|\#\mathcal{N}_{x_1}(\mathbb{F}_q) - \#\mathcal{X}_{x_1}(\mathbb{F}_q)| \leq d_{x_1}$.*

Proof. Affine curves $\mathcal{N}_{x_1}$ and $\mathcal{X}_{x_1}$ are defined by the equations $\mathbf{z}^2 = \mathcal{F}_{x_1}(\mathbf{x}_2)$ and $\mathbf{w}^2 = \mathcal{H}_{x_1}(\mathbf{x}_2)$ respectively. We recall that $\mathcal{F}_{x_1}(\mathbf{x}_2) = g_{x_1}^2(\mathbf{x}_2)\mathcal{H}_{x_1}(\mathbf{x}_2)$. Define the projection maps $\pi_{\mathcal{N}} : \mathcal{N}_{x_1}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, by $\pi_{\mathcal{N}}(x_2, z) = x_2$ and $\pi_{\mathcal{X}} : \mathcal{X}_{x_1}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, by $\pi_{\mathcal{X}}(x_2, w) = x_2$.

Let $x_2 \in \mathbb{F}_q$. First assume that $g_{x_1}(x_2) \neq 0$. Then

$$\#\pi_{\mathcal{N}}^{-1}(x_2) = \#\pi_{\mathcal{X}}^{-1}(x_2) = \begin{cases} 0, & \text{if } \mathcal{H}_{x_1}(x_2) \text{ is a non-square in } \mathbb{F}_q, \\ 1, & \text{if } \mathcal{H}_{x_1}(x_2) = 0, \\ 2, & \text{if } \mathcal{H}_{x_1}(x_2) \text{ is a square in } \mathbb{F}_q^*. \end{cases}$$

Now assume that $g_{x_1}(x_2) = 0$. Then $\#\pi_{\mathcal{N}}^{-1}(x_2) = 1$ and $\#\pi_{\mathcal{X}}^{-1}(x_2)$ equals 0 or 2. Then

$$\begin{aligned} |\#\mathcal{N}_{x_1}(\mathbb{F}_q) - \#\mathcal{X}_{x_1}(\mathbb{F}_q)| &= \left| \sum_{x_2 \in \mathbb{F}_q} \#\pi_{\mathcal{N}}^{-1}(x_2) - \sum_{x_2 \in \mathbb{F}_q} \#\pi_{\mathcal{X}}^{-1}(x_2) \right| \\ &\leq \sum_{x_2 \in \mathbb{F}_q} \left| \#\pi_{\mathcal{N}}^{-1}(x_2) - \#\pi_{\mathcal{X}}^{-1}(x_2) \right| \\ &= \sum_{x_2 \in \mathbb{F}_q \,,\, g_{x_1}(x_2) = 0} 1 \leq d_{x_1}. \end{aligned}$$

□

Proposition 5.15 *Let $x_1 \in \mathbb{F}_q$. If $x_1 \notin \mathcal{I}$, then*

$$|\#\mathcal{N}_{x_1}(\mathbb{F}_q) - q| \leq 2(d - d_{x_1} - 1)\sqrt{q} + d_{x_1} + 1.$$

Proof. Let $x_1 \in \mathbb{F}_q \setminus \mathcal{I}$. Then the affine curve $\mathcal{X}_{x_1}$ is absolutely irreducible and nonsingular (see Proposition 5.12). The degree of $\mathcal{X}_{x_1}$ is $2(d - d_{x_1})$. Let $\widetilde{\mathcal{X}}_{x_1}$ be the nonsingular projective model of $\mathcal{X}_{x_1}$. So $\widetilde{\mathcal{X}}_{x_1}$ is a hyperelliptic curve of genus $d - d_{x_1} - 1$. Furthermore, $\#\widetilde{\mathcal{X}}_{x_1}(\mathbb{F}_q) - \#\mathcal{X}_{x_1}(\mathbb{F}_q)$ equals zero or two. (see Theorem 2.16). By using the Hasse-Weil bound, we have

$$\left|\#\widetilde{\mathcal{X}}(\mathbb{F}_q) - (q+1)\right| \leq 2(d - d_{x_1} - 1)\sqrt{q}.$$

Hence $|\#\mathcal{X}(\mathbb{F}_q) - q| \leq 2(d - d_{x_1} - 1)\sqrt{q} + 1$. Proposition 5.14 concludes the proof. □

Theorem 5.16 *Let $x_1 \in \mathbb{F}_q$. Then*

$$\left|\#\mathtt{Ext}^{-1}(x_1) - q\right| \leq \begin{cases} 2(d - d_{x_1} - 1)\sqrt{q} + d_{x_1} + 1, & \text{if } x_1 \notin \mathcal{I}, \\ q, & \text{if } x_1 \in \mathcal{I}. \end{cases}$$

Proof. Let $x_1 \in \mathbb{F}_q$. Then Proposition 5.3 shows that $\#\mathcal{N}_{x_1}(\mathbb{F}_q) = \#\mathtt{Ext}^{-1}(x_1)$. If $x_1 \notin \mathcal{I}$, Proposition 5.15 gives the desired estimate for $\#\mathtt{Ext}^{-1}(x_1)$. If $x_1 \in \mathcal{I}$, then curve $\mathcal{N}_{x_1}$ is reducible (see Proposition 5.8). So in this case we have the trivial estimate for $\#\mathtt{Ext}^{-1}(x_1)$. □

5.1.2 Analysis of the extractor

In this subsection we show that provided the point P is chosen uniformly at random in $\mathcal{C}(\mathbb{F}_{q^2})$, the element extracted from the point P by $\mathtt{Ext}$ is indistinguishable from a uniformly random element in $\mathbb{F}_q$.

Let X be a $\mathbb{F}_q$-valued random variable that is defined by

$$X = \mathtt{Ext}(P), \text{ for } P \in_R \mathcal{C}(\mathbb{F}_{q^2}).$$

Proposition 5.17 *The random variable X is statistically close to the uniform random variable $U_{\mathbb{F}_q}$, more precisely*

$$\Delta(X, U_{\mathbb{F}_q}) = O\left(\frac{1}{\sqrt{q}}\right).$$

Proof. Let $z \in \mathbb{F}_q$. The uniform random variable $U_{\mathbb{F}_q}$ satisfies $\Pr[U_{\mathbb{F}_q} = z] = 1/q$. For the $\mathbb{F}_q$-valued random variable X,

$$\Pr[X = z] = \frac{\#\mathtt{Ext}^{-1}(z)}{\#\mathcal{C}(\mathbb{F}_{q^2})}.$$

The Hasse-Weil Theorem gives a bound for $\#\mathcal{C}(\mathbb{F}_{q^2})$ and Theorem 5.16 gives a bound for $\#\mathtt{Ext}^{-1}(z)$. Combining these we get

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_q}) =& \frac{1}{2}\sum_{z\in\mathbb{F}_q}\left|\Pr[X=z]-\Pr[U_{\mathbb{F}_q}=z]\right| \\ =& \frac{1}{2}\sum_{z\in\mathbb{F}_q}\left|\frac{\#\mathtt{Ext}^{-1}(z)}{\#\mathcal{C}(\mathbb{F}_{q^2})}-\frac{1}{q}\right| \\ =& \sum_{z\in\mathcal{I}}\frac{\left|q\#\mathtt{Ext}^{-1}(z)-\#\mathcal{C}(\mathbb{F}_{q^2})\right|}{2q\#\mathcal{C}(\mathbb{F}_{q^2})}+\sum_{z\in\mathbb{F}_q\setminus\mathcal{I}}\frac{\left|q\#\mathtt{Ext}^{-1}(z)-\#\mathcal{C}(\mathbb{F}_{q^2})\right|}{2q\#\mathcal{C}(\mathbb{F}_{q^2})}.\end{aligned}$$

Let $r = \#\mathcal{I}$. Then

$$\begin{aligned}\Delta(X, U_{\mathbb{F}_q}) \leq& \frac{r(q^2+(d-1)q+1)+(q-r)(2(d-1)q\sqrt{q}+dq+1)}{2q(q^2-(d-1)q+1)} \\ =& \frac{2(d-1)q\sqrt{q}+(d+r)q-2(d-1)r\sqrt{q}-r+1}{2(q^2-(d-1)q+1)} = \frac{d-1+\epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q) = \frac{(d+r)q\sqrt{q}+2(d-1)(d-r-1)q-(r-1)\sqrt{q}-2(d-1)}{2(q^2-(d-1)q+1)}$. If $q \geq 2d^2$, then $\epsilon(q) < 1$. □

Corollary 5.18 *If $q \geq 2d^2$, $\mathtt{Ext}$ is a deterministic $(\mathbb{F}_q, \frac{d}{\sqrt{q}})$-extractor for $\mathcal{C}(\mathbb{F}_{q^2})$.*

5.2 Examples

In this section we give some examples for the extractors $\mathtt{Ext}$. The first example is the extractor for the subgroup of quadratic residues of $\mathbb{F}_{q^2}^*$. For the second example, we recall an extractor in [49] for an elliptic curve defined over $\mathbb{F}_{q^2}$. Theorem 5.16 enables us to improve the result of [49].

5.2.1 The extractor for a subgroup of $\mathbb{F}_{q^2}^*$

In this subsection we propose a simple extractor for the subgroup of quadratic residues of $\mathbb{F}_{q^2}^*$. This extractor is the result of Theorem 5.16, where $f(\mathbf{x}) = \mathbf{x}$.

Let G be the subgroup of quadratic residues of $\mathbb{F}_{q^2}^*$. We recall that every element x in $\mathbb{F}_{q^2}$ is represented in the form $x = x_1\alpha_1 + x_2\alpha_2$, where $x_1, x_2 \in \mathbb{F}_q$. Define the extractor $\mathtt{ext}$ for G by the function

$$\begin{aligned}&\mathtt{ext} : G \longrightarrow \mathbb{F}_q \\ &\mathtt{ext}(x) = x_1.\end{aligned}$$

Proposition 5.19 *For all $z \in \mathbb{F}_q^*$,*

$$\#\mathtt{ext}^{-1}(z) = \frac{q \pm 1}{2},$$

and for $z = 0$, $\#\mathtt{ext}^{-1}(0) = 0$ or $\#\mathtt{ext}^{-1}(0) = q - 1$.

Proof. Let the affine curve $\mathcal{C}$ be defined by the equation $\mathcal{C} : \mathbf{y}^2 = f(\mathbf{x}) = \mathbf{x}$. This curve is of the type considered in Section 5.1. Clearly for each element $x \in G$, there are exactly two points (x, y) and $(x, -y)$ on $\mathcal{C}$. In fact there is a bijection between G and the set of nonzero abscissa of points on $\mathcal{C}$. Then $\#\mathtt{Ext}^{-1}(z) = 2\#\mathtt{ext}^{-1}(z)$, for all $z \in \mathbb{F}_q^*$. It is easy to see that $\mathcal{I} = \{0\}$. Then Theorem 5.16 implies the proof of this proposition. Also the bound for $\#\mathtt{ext}^{-1}(0)$ is obvious. □

Corollary 5.20 *The extractor* ext *is $(\mathbb{F}_q, \frac{1}{q})$-deterministic for G.*

Proof. For $d = 1$, the estimate for $\epsilon(q)$ can be made tighter (see proof of Proposition 5.17), so that $\epsilon(q) < \frac{1}{q}$. □

5.2.2 The extractor for elliptic curves

In this subsection we recall the extractor introduced by Gürel in [49], that works for an elliptic curve defined over $\mathbb{F}_{q^2}$. This extractor, for a given random point on elliptic curve, outputs the first $\mathbb{F}_q$-coordinate of the abscissa of the point. Theorem 5.16 allows to improve the bounds which are proposed in [49].

Let E be an elliptic curve defined over $\mathbb{F}_{q^2}$, where q is a power of a prime $p > 3$. Then

$$E(\mathbb{F}_{q^2}) = \{(x, y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} : y^2 = f(x) = x^3 + ax + b\} \cup \{\mathcal{O}_E\},$$

where a and b are in $\mathbb{F}_{q^2}$. Since E is nonsingular $f(\mathbf{x})$ is a square free polynomial in $\overline{\mathbb{F}}_q[\mathbf{x}]$.

Let $\alpha_1 = 1$ and $\alpha_2 = t$, where $t \in \mathbb{F}_{q^2}$, such that $t^2 = c$ and c is a non-square element in $\mathbb{F}_q$. So, every element x in $\mathbb{F}_{q^2}$ can be represented by the form $x = x_1 + x_2 t$, where $x_1, x_2 \in \mathbb{F}_q$.

The extractor ext for E is defined as a function

$$\begin{aligned}
&\mathtt{ext} : E(\mathbb{F}_{q^2}) \longrightarrow \mathbb{F}_q \\
&\mathtt{ext}(x, y) = x_1, \\
&\mathtt{ext}(\mathcal{O}_E) = 0.
\end{aligned}$$

The following theorem gives tight bounds for $\#\mathtt{ext}^{-1}(z)$, for all z in $\mathbb{F}_q$.

Proposition 5.21 *For all $z \in \mathbb{F}_q^*$,*

$$\left|\#\mathtt{ext}^{-1}(z) - q\right| \leq 4\sqrt{q} + 1.$$

If $a_2 \neq 0$ or $b_1 \neq 0$,

$$\left|\#\mathtt{ext}^{-1}(0) - (q+1)\right| \leq 4\sqrt{q} + 1.$$

If $a_2 = b_1 = 0$,

$$\left|\#\mathtt{ext}^{-1}(0) - (q+1)\right| \leq q.$$

Proof. The proof of this theorem follows from Theorem 5.16, in the case that $f(\mathbf{x}) = \mathbf{x}^3 + a\mathbf{x} + b$. Define the variables $\mathbf{x}_1$ and $\mathbf{x}_2$ by $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2 t$. Then

$$f(\mathbf{x}_1 + \mathbf{x}_2 t) = f_0(\mathbf{x}_1, \mathbf{x}_2) + f_1(\mathbf{x}_1, \mathbf{x}_2)t,$$

where

$$f_0(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{x}_1^3 + 3c\mathbf{x}_1\mathbf{x}_2^2 + a_1\mathbf{x}_1 + ca_1\mathbf{x}_2 + b_1$$
$$f_1(\mathbf{x}_1, \mathbf{x}_2) = c\mathbf{x}_2^3 + 3\mathbf{x}_1^2\mathbf{x}_2 + a_2\mathbf{x}_1 + a_1\mathbf{x}_2 + b_2.$$

Then we fix $\mathbf{x}_1$ by z. It is easy to see that $\mathcal{I} = \{0\}$ if and only if $f_0(z, \mathbf{x}_2) = 0$. Clearly $f_0(z, \mathbf{x}_2) = 0$, if and only if $z = a_2 = b_1 = 0$, since $p \neq 3$. Recall that p is the characteristic of $\mathbb{F}_q$. Also note that $\#\mathtt{ext}^{-1}(0) = \#\mathtt{Ext}^{-1}(0) + 1$, since $\mathtt{ext}(\mathcal{O}_E) = 0$. □

Corollary 5.22 *If $q \geq 18$, then* ext *is a deterministic $(\mathbb{F}_q, \frac{3}{\sqrt{q}})$-extractor for $E(\mathbb{F}_{q^2})$,*

Proof. The proof of this corollary is similar to the proof of Proposition 5.17, in the case that $d = 3$ and $r \leq 1$. □

Chapter 6

Extractors for Jacobians of Genus-2 Curves in Odd Characteristic

In this chapter we propose two simple and efficient deterministic extractors for $J(\mathbb{F}_q)$, the set of $\mathbb{F}_q$-rational points of the Jacobian of a genus 2 hyperelliptic curve H defined over $\mathbb{F}_q$, where q is odd. The first extractor, `SEJ`, called *sum extractor*, outputs the sum of abscissas of rational points on H in the support of D, for a given reduced divisor D on $J(\mathbb{F}_q)$. Similarly the second extractor, `PEJ`, called *product extractor*, outputs the product of abscissas of rational points in the support of D, for a given point D on $J(\mathbb{F}_q)$. Provided that the point D is chosen uniformly at random in $J(\mathbb{F}_q)$, the element extracted from the point D is indistinguishable from a uniformly random variable in $\mathbb{F}_q$.

Let $\mathcal{K}$ be the Kummer surface associated to the Jacobian of H over $\mathbb{F}_q$. Then there is a map κ from $J(\mathbb{F}_q)$ to $\mathcal{K}(\mathbb{F}_q)$, so that a point and it's opposite in $J(\mathbb{F}_q)$ are mapped to the same value. By means of this map, we propose two simple and efficient deterministic extractors, `SEK` and `PEK`, for the Kummer surface $\mathcal{K}$. If a point K is chosen uniformly at random in $\mathcal{K}$, the element extracted from the point K is statistically close to a uniformly random variable in $\mathbb{F}_q$.

This chapter is organized as follows. In the next section, we describe the proposed extractors `SEJ` and `PEJ` for the Jacobian of a genus 2 hyperelliptic curve H over

The result of this chapter was previously published as: R. R. Farashahi, Extractors for Jacobian of Hyperelliptic Curves of Genus 2 in Odd Characteristic. In *Cryptography and Coding: 11th IMA International Conference*, volume 4887 of *Lecture Notes in Computer Science*, pages 313–335. Springer-Verlag, 2007.

$\mathbb{F}_q$. We show that the outputs of these extractors, for a given uniformly random point of $J(\mathbb{F}_q)$, are statistically close to a uniformly random variable in $\mathbb{F}_q$. For the analysis of these extractors, bounds on the cardinalities of $\mathtt{SEJ}^{-1}(a)$ and $\mathtt{PEJ}^{-1}(b)$, for all $a, b \in \mathbb{F}_q$, are needed. We give tight estimates for them in Theorems 6.3 and 6.6. Then, in Section 6.2, we give the proofs of the main Theorems 6.3 and 6.6. In Section 6.3, we describe two extractors SEK and PEK for the Kummer surface $\mathcal{K}$ associated to the Jacobian of H over $\mathbb{F}_q$. These extractors are modified versions of the previous extractors, using the map κ from $J(\mathbb{F}_q)$ to $\mathcal{K}(\mathbb{F}_q)$.

6.1 The extractors for the Jacobian

Let H be an imaginary hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$, for odd q. Then H has a plane model of the form

$$\mathbf{y}^2 = f(\mathbf{x}) = \mathbf{x}^5 + f_4\mathbf{x}^4 + f_3\mathbf{x}^3 + f_2\mathbf{x}^2 + f_1\mathbf{x} + f_0, \tag{6.1}$$

where $f_i \in \mathbb{F}_q$ and f is a square-free polynomial.

Let J be the Jacobian of H over $\mathbb{F}_q$. We recall from Subsection 2.6, that for each nontrivial point on $J(\mathbb{F}_q)$ there exist a unique divisor D on H defined over $\mathbb{F}_q$ of the form

$$D = \sum_{i=1}^{r} P_i - rP_\infty,$$

where $P_i = (x_i, y_i) \in H(\overline{\mathbb{F}}_q)$, $P_i \neq P_\infty$ and $P_i \neq \sigma(P_j)$, for $i \neq j$, $r \leq 2$. By means of the Mumford representation [84], each nontrivial point on $J(\mathbb{F}_q)$ can be uniquely represented by a pair of polynomials $[u(\mathbf{x}), v(\mathbf{x})]$, $u, v \in \mathbb{F}_q[\mathbf{x}]$, where u is monic, $\deg(v) < \deg(u) \leq 2$ and u divides $(v^2 + hv - f)$. The neutral element of $J(\mathbb{F}_q)$, denoted by $\mathcal{O}$, is represented by $[1, 0]$.

6.1.1 The sum extractor for the Jacobian

We shall now define the *sum extractor* for $J(\mathbb{F}_q)$ using the notation of divisor classes to explain the name. Then we translate the definition to the Mumford representation.

Definition 6.1 *The sum extractor* SEJ *for the Jacobian of H over $\mathbb{F}_q$ is defined as the function* $\mathtt{SEJ} : J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, *by*

$$\mathtt{SEJ}(D) = \begin{cases} \sum_{i=1}^{r} x_{P_i}, & \text{if } D = \sum_{i=1}^{r} P_i - rP_\infty,\ 1 \leq r \leq 2, \\ 0, & \text{if } D = \mathcal{O}. \end{cases}$$

Remark 6.2 By means of the Mumford representation for the points of $J(\mathbb{F}_q)$, the function $\mathtt{SEJ}$ can alternatively be defined by

$$\mathtt{SEJ}(D) = \begin{cases} -u_1, & \text{if } D = [x^2 + u_1 x + u_0, v_1 x + v_0], \\ -u_0, & \text{if } D = [x + u_0, v_0], \\ 0, & \text{if } D = [1, 0]. \end{cases}$$

To analyze the extractor $\mathtt{SEJ}$, we need to examine the distribution of the random variable $\mathtt{SEJ}(D)$, for D chosen uniformly at random in $J(\mathbb{F}_q)$. So we need to obtain estimates for the cardinalities of preimages of $\mathtt{SEJ}(D)$. We note that by the Hasse-Weil bound $\#J(\mathbb{F}_q) \approx q^2$ and that $J(\mathbb{F}_q) = \bigcup_{a \in \mathbb{F}_q} \mathtt{SEJ}^{-1}(a)$. For a uniformly distributed sequence we expect $\#\mathtt{SEJ}^{-1}(a) \approx q$, for $a \in \mathbb{F}_q$. The following theorem shows that the expected cardinality of each fiber essentially equals q. It also gives a precise bound on the deviation.

Theorem 6.3 *For all $a \in \mathbb{F}_q^*$,*

$$\left|\#\mathtt{SEJ}^{-1}(a) - q\right| \leq 8\sqrt{q} + 1$$

and

$$\left|\#\mathtt{SEJ}^{-1}(0) - (q+1)\right| \leq 8\sqrt{q} + 1.$$

We give the proof of this theorem in Subsection 6.2.1.

6.1.2 The product extractor for the Jacobian

In a similar way, we propose the *product extractor* for $J(\mathbb{F}_q)$.

Definition 6.4 *The product extractor $\mathtt{PEJ}$ for the Jacobian of H over $\mathbb{F}_q$ is defined as the function $\mathtt{PEJ} : J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, by*

$$\mathtt{PEJ}(D) = \begin{cases} \prod_{i=1}^{r} x_{P_i}, & \text{if } D = \sum_{i=1}^{r} P_i - rP_\infty,\ 1 \leq r \leq 2, \\ 0, & \text{if } D = \mathcal{O}. \end{cases}$$

Remark 6.5 By using Mumford representation for the points of $J(\mathbb{F}_q)$, the function $\mathtt{PEJ}$ can alternatively be defined by

$$\mathtt{PEJ}(D) = \begin{cases} u_0, & \text{if } D = [x^2 + u_1 x + u_0, v_1 x + v_0], \\ -u_0, & \text{if } D = [x + u_0, v_0], \\ 0, & \text{if } D = [1, 0]. \end{cases}$$

The next theorem shows estimates for $\#\mathtt{PEJ}^{-1}(b)$, for all b in $\mathbb{F}_q$.

Theorem 6.6 *Let $b \in \mathbb{F}_q^*$. Let $I_f = \{z \in \mathbb{F}_q^* : f_1 = z^2, f_2 = zf_4\}$. Then*

$$\left|\#\mathtt{PEJ}^{-1}(b) - q\right| \leq \begin{cases} 8\sqrt{q}+3, & \text{if } f_0 \neq 0, \\ 6\sqrt{q}+3, & \text{if } f_0 = 0 \text{ and } b \notin I_f, \\ q+4\sqrt{q}, & \text{if } f_0 = 0 \text{ and } b \in I_f. \end{cases}$$

Also

$$\left|\#\mathtt{PEJ}^{-1}(0) - (eq+1)\right| \leq 4e\sqrt{q},$$

where e equals the number of square roots of f_0 in $\mathbb{F}_q$.

We give the proof of this theorem in Subsection 6.2.2.

6.1.3 Analysis of the extractors

In this subsection we show that provided the divisor D is chosen uniformly at random in $J(\mathbb{F}_q)$, the element extracted from the divisor D by SEJ or PEJ is indistinguishable from a uniformly random element in $\mathbb{F}_q$.

Let $\mathtt{A}$ be a $\mathbb{F}_q$-valued random variable that is defined by

$$\mathtt{A} = \mathtt{SEJ}(D), \quad \text{for} \quad D \in_R J(\mathbb{F}_q).$$

Proposition 6.7 *The random variable $\mathtt{A}$ is statistically close to the uniform random variable $U_{\mathbb{F}_q}$, more precisely*

$$\Delta(\mathtt{A}, U_{\mathbb{F}_q}) = O\left(\frac{1}{\sqrt{q}}\right).$$

Proof. Let $a \in \mathbb{F}_q$. For the uniform random variable $U_{\mathbb{F}_q}$, $\Pr[U_{\mathbb{F}_q} = a] = 1/q$. For the $\mathbb{F}_q$-valued random variable $\mathtt{A}$,

$$\Pr[\mathtt{A} = a] = \frac{\#\mathtt{SEJ}^{-1}(a)}{\#J(\mathbb{F}_q)}.$$

The genus of H is 2, so by the Hasse-Weil Theorem we have

$$(\sqrt{q}-1)^4 \leq \#J(\mathbb{F}_q) \leq (\sqrt{q}+1)^4.$$

Theorem 6.3 gives a bound for $\#\mathtt{SEJ}^{-1}(a)$, for all $a \in \mathbb{F}_q$. It follows from this bound that

$$\begin{aligned}\Delta(\mathtt{A}, U_{\mathbb{F}_q}) =& \frac{1}{2}\sum_{a\in\mathbb{F}_q}\left|\Pr[\mathtt{A}=a]-\Pr[U_{\mathbb{F}_q}=a]\right| \\ =& \frac{1}{2}\sum_{a\in\mathbb{F}_q}\left|\frac{\#\mathtt{SEJ}^{-1}(a)}{\#J(\mathbb{F}_q)}-\frac{1}{q}\right| \\ =& \frac{\left|q\#\mathtt{SEJ}^{-1}(0)-\#J(\mathbb{F}_q)\right|}{2q\#J(\mathbb{F}_q)}+\sum_{a\in\mathbb{F}_q^*}\frac{\left|q\#\mathtt{SEJ}^{-1}(a)-\#J(\mathbb{F}_q)\right|}{2q\#J(\mathbb{F}_q)}.\end{aligned}$$

So

$$\begin{aligned}\Delta(\mathtt{A}, U_{\mathbb{F}_q}) \leq& \frac{(12q\sqrt{q}-4q+4\sqrt{q}-1)+(q-1)(12q\sqrt{q}-5q+4\sqrt{q}-1)}{2q(\sqrt{q}-1)^4} \\ =& \frac{12q\sqrt{q}-5q+4\sqrt{q}}{2(\sqrt{q}-1)^4}=\frac{6+\epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q)=\frac{43q\sqrt{q}-68q+48\sqrt{q}-12}{2(\sqrt{q}-1)^4}$. If $q \geq 570$, then $\epsilon(q)<1$. □

Corollary 6.8 *Let $q \geq 570$. $\mathtt{SEJ}$ is a deterministic $(\mathbb{F}_q, \frac{7}{\sqrt{q}})$-extractor for $J(\mathbb{F}_q)$.*

Proof. Proposition 6.7 concludes the proof of this corollary. □

Corollary 6.9 $\mathtt{PEJ}$ *is a deterministic $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$-extractor for $J(\mathbb{F}_q)$.*

Proof. the proof follows the same lines as that of Proposition 6.7. □

6.2 Proofs of theorems

In this section we give the proofs of Theorems 6.3 and 6.6. In other words, we give the estimates for the cardinalities of $\#\mathtt{SEJ}^{-1}(a)$, $\#\mathtt{PEJ}^{-1}(b)$, for all $a, b \in \mathbb{F}_q$.

First, we set up the preliminaries for the proofs. As in Subsection 2.6.1, we partition $J(\mathbb{F}_q)$ as $J(\mathbb{F}_q) = J_0 \cup J_1 \cup J_2$, where $J_0 = \{\mathcal{O}\}$ and J_r, for $r = 1, 2$, is defined by

$$J_r = \{D \in J(\mathbb{F}_q) : D = \textstyle\sum_{i=1}^{r} P_i - rP_\infty\}.$$

Let H^t be a quadratic twist of H that has a plane model of the form

$$\alpha \mathbf{y}^2 = f(\mathbf{x}), \tag{6.2}$$

where α is a non-square element of $\mathbb{F}_q$. Let J^t be the Jacobian of H^t over $\mathbb{F}_q$. In a similar way, we partition $J^t(\mathbb{F}_q)$ into $J^t(\mathbb{F}_q) = J_0^t \cup J_1^t \cup J_2^t$.

Now, from Section 2.8, we recall the surface $\mathcal{R}$ related to the Jacobian of H. The hyperelliptic curve H has the plane model defined by

$$\mathbf{y}^2 = f(\mathbf{x}) = \prod_{i=1}^{5} (\mathbf{x} - \lambda_i), \tag{6.3}$$

where λ_i are pairwise distinct elements of $\overline{\mathbb{F}}_q$ (see Equation (6.1)). Let Ψ be the polynomial in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ defined by

$$\Psi(\mathbf{a}, \mathbf{b}) = \prod_{i=1}^{5} (\mathbf{b} - \lambda_i \mathbf{a} + \lambda_i^2).$$

The surface $\mathcal{R}$ is defined over $\mathbb{F}_q$ by the equation $\mathbf{z}^2 = \Psi(\mathbf{a}, \mathbf{b})$ (see Definition 2.19).

6.2.1 Proof of the sum extractor theorem

We partition J_2 into $J_2 = \bigcup_{a \in \mathbb{F}_q} J_{2,a}$, where

$$J_{2,a} = \{P_1 + P_2 - 2P_\infty \in J_2 : x_{P_1} + x_{P_2} = a\}.$$

Obviously, $J_{2,a}$ is equal to $\mathtt{SEJ}^{-1}(a) \cap J_2$. So, we need estimates for the cardinalities of $J_{2,a}$, for all $a \in \mathbb{F}_q$. In a similar way, we partition J_2^t into the subsets $J_{2,a}^t$, for all $a \in \mathbb{F}_q$.

We consider the curve $\mathcal{R}_a$, for $a \in \mathbb{F}_q$, as the intersection of the surface $\mathcal{R}$ with the hyperplane $\mathbf{a} = a$. In Proposition 6.12, we give the number of points on $J_{2,a}$ in terms of the numbers of $\mathbb{F}_q$-rational points on H and $\mathcal{R}_a$. Finally, by means of the Hasse-Weil Theorem, we obtain an estimate for $\#J_{2,a}$.

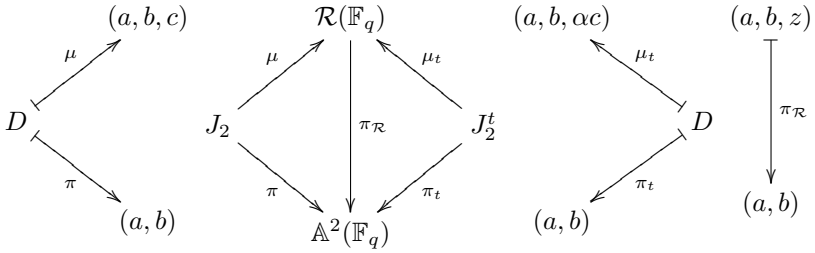
Let $\mathcal{R}_a$, for $a \in \mathbb{F}_q$, be the affine curve defined over $\mathbb{F}_q$, by the equation

$$\mathbf{z}^2 = \Psi_a(\mathbf{b}) = \Psi(a, \mathbf{b}). \tag{6.4}$$

Proposition 6.10 *For all $a \in \mathbb{F}_q$,*

$$\#J_{2,a} + \#J_{2,a}^t = 2\#\mathcal{R}_a(\mathbb{F}_q) - 2.$$

Proof. We restrict Diagram 2.9, from $J(\mathbb{F}_q)\setminus\{\mathcal{O}\}$ and $J^t(\mathbb{F}_q)\setminus\{\mathcal{O}\}$ to respectively J_2 and J_2^t. So, we consider the following diagram:



where D is a divisor either on J_2 or J_2^t represented by $P_1 + P_2 - 2P_\infty$ and where a, b, c, in the outputs of the maps μ, π, μ_t, π_t, are defined by $a = x_{P_1} + x_{P_2}$, $b = x_{P_1}x_{P_2}$ and $c = y_{P_1}y_{P_2}$.

From the proof of Proposition 2.22 (cases 1 and 3) we have

$$\#\pi^{-1}(a,b) + \#\pi_t^{-1}(a,b) = 2\#\pi_{\mathcal{R}}^{-1}(a,b),$$

for all $b \in \mathbb{F}_q \setminus \{a^2/4\}$. Further, from the proof Proposition 2.22 (case 2) we obtain

$$\#\pi^{-1}(a,a^2/4) + \#\pi_t^{-1}(a,a^2/4) = 2\#\pi_{\mathcal{R}}^{-1}(a,a^2/4) - 2,$$

since we do not count the divisors in J_1 and J_1^t. Hence

$$\begin{aligned}\#J_{2,a} + \#J_{2,a}^t &= \sum_{b\in\mathbb{F}_q} \#\pi^{-1}(a,b) + \#\pi_t^{-1}(a,b) \\ &= \sum_{b\in\mathbb{F}_q} 2\#\pi_{\mathcal{R}}^{-1}(a,b) - 2 = 2\#\mathcal{R}_a(\mathbb{F}_q) - 2.\end{aligned}$$

□

Proposition 6.11 *For all $a \in \mathbb{F}_q$,*

$$\#J_{2,a} - \#J_{2,a}^t = \#H(\mathbb{F}_q) - \#H^t(\mathbb{F}_q).$$

Proof. Let $a \in \mathbb{F}_q$. Let S_a be a set defined by

$$S_a = \left\{\{x, a-x\} : x \in \mathbb{F}_{q^2}\right\}.$$

We define the map $\rho : J_{2,a} \longrightarrow S_a$ by $\rho(D) = \{x_{P_1}, x_{P_2}\}$, where D is represented by $P_1 + P_2 - 2P_\infty$. Note that, for $D \in J_{2,a}$, $x_{P_1} + x_{P_2}$ is equal to a. Further, we define the map $\xi : H(\mathbb{F}_q)\setminus\{P_\infty\} \longrightarrow S_a$ by $\xi(P) = \{x_P, a - x_P\}$. In a similar way, we define the maps ρ_t and ξ_t respectively for $J_{2,a}^t$ and $H^t(\mathbb{F}_q)$. In the following, we show that $\#\rho^{-1}(s) - \#\rho_t^{-1}(s) = \#\xi^{-1}(s) - \#\xi_t^{-1}(s)$, for all $s \in S_a$. We consider the following cases in the proof of the later statement.

1. Assume $s = \{x_1, x_2\}$, where $x_1 \in \mathbb{F}_q$, $x_2 = a - x_1$ and $x_1 \neq x_2$. Then there exist $y_1, y_2 \in \mathbb{F}_q$, such that $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ are points on $H(\mathbb{F}_q)$ or $H^t(\mathbb{F}_q)$. We distinguish three subcases.

   (a) Suppose $y_1, y_2 \neq 0$. Without loss of generality, assume $P_1 \in H(\mathbb{F}_q)$. So $P_1 \notin H^t(\mathbb{F}_q)$. First assume $P_2 \in H(\mathbb{F}_q)$. So $P_2 \notin H^t(\mathbb{F}_q)$. Hence the divisors $P_1 + P_2 - 2P_\infty$, $P_1 + \sigma(P_2) - 2P_\infty$, $\sigma(P_1) + P_2 - 2P_\infty$ and $\sigma(P_1) + \sigma(P_2) - 2P_\infty$ are the only points of $\rho^{-1}(s)$. Furthermore, $\rho_t^{-1}(s) = \emptyset$. Also $\xi^{-1}(s) = \{P_1, P_2, \sigma(P_1), \sigma(P_2)\}$ and $\xi_t^{-1}(s) = \emptyset$. Therefore $\#\rho^{-1}(s) = \#\xi^{-1}(s) = 4$ and $\#\rho_t^{-1}(s) = \#\xi_t^{-1}(s) = 0$.
   Now assume $P_2 \notin H(\mathbb{F}_q)$. So $P_2 \in H^t(\mathbb{F}_q)$. Therefore, in this case, $\rho^{-1}(s) = \rho_t^{-1}(s) = \emptyset$. Also $\xi^{-1}(s) = \{P_1, \sigma(P_1)\}$, $\xi_t^{-1}(s) = \{P_2, \sigma(P_2)\}$. Hence $\#\rho^{-1}(s) = \#\rho_t^{-1}(s) = 0$ and $\#\xi^{-1}(s) = \#\xi_t^{-1}(s) = 2$.

   (b) Suppose exactly one of y_1, y_2 is equal to 0. Without loss of generality assume $y_1 = 0$ and $y_2 \neq 0$. So, P_1 is a common point of $H(\mathbb{F}_q)$ or $H^t(\mathbb{F}_q)$. Without loss of generality, assume $P_2 \in H(\mathbb{F}_q)$. Thus $P_2 \notin H^t(\mathbb{F}_q)$. Hence the divisors $P_1 + P_2 - 2P_\infty$ and $P_1 + \sigma(P_2) - 2P_\infty$ are the only points of $\rho^{-1}(s)$. Furthermore, $\rho_t^{-1}(s) = \emptyset$, $\xi^{-1}(s) = \{P_1, P_2, \sigma(P_2)\}$ and $\xi_t^{-1}(s) = \{P_1\}$. Therefore, $\#\rho^{-1}(s) = 2$, $\#\rho_t^{-1}(s) = 0$, $\#\xi^{-1}(s) = 3$ and $\#\xi_t^{-1}(s) = 1$.

   (c) Suppose $y_1 = y_2 = 0$. So P_1, P_2 belong to both $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$. Hence the divisor $P_1 + P_2 - 2P_\infty$ is the only point of $\rho^{-1}(s)$ and $\rho_t^{-1}(s)$. Also $\xi^{-1}(s) = \xi_t^{-1}(s) = \{P_1, P_2\}$. Therefore $\#\rho^{-1}(s) = \#\rho_t^{-1}(s) = 1$ and $\#\xi^{-1}(s) = \#\xi_t^{-1}(s) = 2$.

2. Assume $s = \{x_1\}$, where $x_1 = \frac{a}{2}$. Then there exists $y \in \mathbb{F}_q$, such that $P_1 = (x_1, y_1)$ is a point on $H(\mathbb{F}_q)$ or $H^t(\mathbb{F}_q)$. We consider the following subcases.

   (a) Suppose $y_1 \neq 0$. Without loss of generality, assume $P_1 \in H(\mathbb{F}_q)$. So $P_1 \notin H^t(\mathbb{F}_q)$. Hence the divisors $2P_1 - 2P_\infty$ and $2\sigma(P_1) - 2P_\infty$ are the only points of $\rho^{-1}(s)$. Further, $\rho_t^{-1}(s) = \emptyset$. Also $\xi^{-1}(s) = \{P_1, \sigma(P_1)\}$ and $\xi_t^{-1}(s) = \emptyset$. Therefore $\#\rho^{-1}(s) = \#\xi^{-1}(s) = 2$ and $\#\rho_t^{-1}(s) = \#\xi_t^{-1}(s) = 0$.

   (b) Suppose $y_1 = 0$. So P_1 is a common point of $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$, i.e., $P_1 = \sigma(P_1)$. So, $\rho^{-1}(s) = \rho_t^{-1}(s) = \emptyset$ and $\xi^{-1}(s) = \xi_t^{-1}(s) = \{P_1\}$. This means $\#\rho^{-1}(s) = \#\rho_t^{-1}(s) = 0$, $\#\xi^{-1}(s) = \#\xi_t^{-1}(s) = 1$.

3. Assume $s = \{x_1, x_2\}$, where $x_1 \in \mathbb{F}_{q^2}$ and $x_2 = a - x_1$. Clearly $x_1 \neq x_2$. Let β be a square root of α in $\mathbb{F}_{q^2}$. Then, for $i = 1, 2$, the point $P_i = (x_i, y_i)$, for $y_i \in \mathbb{F}_{q^2}$, is a point of $H(\mathbb{F}_{q^2})$ if and only if $Q_i = (x_i, \frac{y_i}{\beta})$ is a point of $H^t(\mathbb{F}_{q^2})$. Thus, $P_1 + P_2 - 2P_\infty$ is a divisor of $J_{2,a}$ if and only if $Q_1 + Q_2 - 2P_\infty$ is a divisor of $J_{2,a}^t$. Hence $\#\rho^{-1}(s) = \#\rho_t^{-1}(s)$. Furthermore, $\#\xi^{-1}(s) = \#\xi_t^{-1}(s) = 0$.

Hence, in all three cases $\#\rho^{-1}(s) - \#\rho_t^{-1}(s) = \#\xi^{-1}(s) - \#\xi_t^{-1}(s)$, for all $s \in S_a$. So,

$$\begin{aligned}\#J_{2,a} - \#J_{2,a}^t &= \sum_{s \in S_a} \#\rho^{-1}(s) - \#\rho_t^{-1}(s) \\ &= \sum_{s \in S_a} \#\xi^{-1}(s) - \#\xi_t^{-1}(s) = \#H(\mathbb{F}_q) - \#H^t(\mathbb{F}_q).\end{aligned}$$

□

Proposition 6.12 *For all $a \in \mathbb{F}_q$,*

$$\#J_{2,a} = \#H(\mathbb{F}_q) + \#\mathcal{R}_a(\mathbb{F}_q) - q - 2.$$

Proof. This proposition is a direct consequence of Propositions 6.10 and 6.11. □

Now, we need an estimate for the cardinality of the curve $\mathcal{R}_a(\mathbb{F}_q)$. The affine curve $\mathcal{R}_a$, for $a \in \mathbb{F}_q$, is absolutely irreducible. Also $\mathcal{R}_a$ is nonsingular for almost all $a \in \mathbb{F}_q$. Furthermore, the genus of the nonsingular model of $\mathcal{R}_a$ is at most 2. By using the Hasse-Weil bound for the nonsingular model of $\mathcal{R}_a$, we obtain the following estimate for $\#\mathcal{R}_a(\mathbb{F}_q)$.

Proposition 6.13 *For all $a \in \mathbb{F}_q$,*

$$|\#\mathcal{R}_a(\mathbb{F}_q) - q| \leq 4\sqrt{q}.$$

Proof. Clearly, the affine curve $\mathcal{R}_a$ is absolutely irreducible for all $a \in \mathbb{F}_q$. The affine curve $\mathcal{R}_a$ may be singular. Let $\gamma_{i,j} = \lambda_i + \lambda_j$, for all integers i, j such that $1 \leq i < j \leq 5$. Let s_a be the number of $\gamma_{i,j}$ that are equal to a. Then polynomial $\Psi_a(\mathbf{b})$ has s_a double roots, since the λ_i are pairwise distinct. This means that $\mathcal{R}_a$ has s_a singular points. Note that $0 \leq s_a \leq 2$. If $s_a = 0$, then $\mathcal{R}_a$ is an absolutely nonsingular affine curve of genus 2. In fact, the genus of the nonsingular model of $\mathcal{R}_a$ equals $2 - s_a$. By using the Hasse-Weil bound for the nonsingular model of $\mathcal{R}_a$, we obtain

$$|\#\mathcal{R}_a(\mathbb{F}_q) - q| \leq 2(2 - s_a)\sqrt{q} + s_a \leq 4\sqrt{q}.$$

This concludes the proof of this proposition. □

Proof of Theorem 6.3. Let $a \in \mathbb{F}_q$. Proposition 6.12 shows that

$$\#(\mathtt{SEJ}^{-1}(a) \cap J_2) = \#H(\mathbb{F}_q) + \#\mathcal{R}_a(\mathbb{F}_q) - q - 2.$$

By using the Hasse-Weil bound for H we obtain

$$|\#H(\mathbb{F}_q) - q - 1| \leq 4\sqrt{q}.$$

Furthermore, from Proposition 6.13 we have

$$|\#\mathcal{R}_a(\mathbb{F}_q) - q| \leq 4\sqrt{q}.$$

Hence

$$\left|\#(\mathtt{SEJ}^{-1}(a) \cap J_2) - q + 1\right| \leq 8\sqrt{q}.$$

Clearly $\#(\mathtt{SEJ}^{-1}(a) \cap J_1)$ equals $0, 1$ or 2. If $a = 0$, then $\#(\mathtt{SEJ}^{-1}(a) \cap J_0)$ equals 1, otherwise equals 0. So the proof of Theorem 6.3 is completed. □

6.2.2 Proof of the product extractor theorem

The proof of Theorem 6.6 is similar to the proof of Theorem 6.3. Here, we partition J_2 as $J_2 = \bigcup_{b \in \mathbb{F}_q} J_{2,b}$, where

$$J_{2,b} = \{P_1 + P_2 - 2P_\infty \in J_2 : x_{P_1} x_{P_2} = b\}.$$

Similarly, we partition J_2^t into the subsets $J_{2,b}^t$, for all $b \in \mathbb{F}_q$.

Let $\mathcal{R}_b$, for $b \in \mathbb{F}_q$, be the affine curve defined over $\mathbb{F}_q$, by the equation

$$\mathbf{z}^2 = \Psi_b(\mathbf{a}) = \Psi(\mathbf{a}, b). \tag{6.5}$$

Proposition 6.14 *For all $b \in \mathbb{F}_q$,*

$$\#J_{2,b} + \#J_{2,b}^t = 2\#\mathcal{R}_b(\mathbb{F}_q) - 2r_b,$$

where r_b equals the number of square roots of b in $\mathbb{F}_q$.

Proof. The proof is similar to that of Proposition 6.10, which follows from Proposition 2.22. □

Proposition 6.15 *For all $b \in \mathbb{F}_q^*$,*

$$\#J_{2,b} - \#J_{2,b}^t = \#H(\mathbb{F}_q) - \#H^t(\mathbb{F}_q) - 2e + 2,$$

where e equals the number of square roots of f_0 in $\mathbb{F}_q$.

Proof. The proof of this proposition is similar to the proof of Proposition 6.11. □

Proposition 6.16 *For all $b \in \mathbb{F}_q^*$,*

$$\#J_{2,b} = \#H(\mathbb{F}_q) + \#\mathcal{R}_b(\mathbb{F}_q) - q - e - r_b,$$

where e, r_b are respectively equal to the numbers of square roots of f_0 and b in $\mathbb{F}_q$.

Proof. This proposition is a direct consequence of Proposition 6.14 and 6.15. □

The following proposition gives an estimate for the number of $\mathbb{F}_q$-rational points on curves $\mathcal{R}_b$. The affine curve $\mathcal{R}_b$ is absolutely irreducible and nonsingular, for almost all $b \in \mathbb{F}_q$. In fact, the curve $\mathcal{R}_b$ is reducible if and only if $\lambda_i = 0$, for some i, and $b \in I_f$, where $I_f = \{z \in \mathbb{F}_q^* : f_1 = z^2, f_2 = zf_4\}$. Provided the curve $\mathcal{R}_b$ is absolutely irreducible, the genus of the nonsingular model of $\mathcal{R}_b$ is at most 2. Then the Hasse-Weil Theorem gives the estimates for $\#\mathcal{R}_b(\mathbb{F}_q)$.

Proposition 6.17 *Let $b \in \mathbb{F}_q$. Then*

$$|\#\mathcal{R}_b(\mathbb{F}_q) - q| \leq \begin{cases} 4\sqrt{q} & \text{if } f_0 \neq 0, \\ 2\sqrt{q} & \text{if } f_0 = 0 \text{ and } b \notin I_f, \\ q & \text{if } f_0 = 0 \text{ and } b \in I_f. \end{cases}$$

Proof. Let $b \in \mathbb{F}_q$. Let $\delta_{i,j} = \lambda_i \lambda_j$, for all integers i, j such that $1 \leq i < j \leq 5$. Let s_b be the number of $\delta_{i,j}$ that are equal to b. Then the polynomial $\Psi_b(\mathbf{a})$ has s_b double roots, since the λ_i are pairwise distinct.

If $f(0) \neq 0$, then $\lambda_i \neq 0$, for all integer $0 \leq i \leq 5$. Then the degree of $\Psi_b(\mathbf{a})$ equals 5. So, the affine curve $\mathcal{R}_b$ is absolutely irreducible for all $b \in \mathbb{F}_q$. Since $\Psi_b(\mathbf{a})$ has s_b double roots, $\mathcal{R}_b$ has s_b singular points. In fact, the genus of the nonsingular model of $\mathcal{R}_b$ equals $2 - s_b$. By using the Hasse-Weil bound for the number of $\mathbb{F}_q$-rational points of the nonsingular model of $\mathcal{R}_b$, we obtain

$$|\#\mathcal{R}_b(\mathbb{F}_q) - q| \leq 2(2 - s_b)\sqrt{q} + s_b \leq 4\sqrt{q}.$$

If $f(0) = 0$, there exists an integer i such that $\lambda_i = 0$. If $b = 0$,clearly $\#\mathcal{R}_b(\mathbb{F}_q) = q$. Now assume that $b \neq 0$. Then the degree of $\Psi_b(\mathbf{a})$ equals 4. In this case, one can show that $s_b = 2$ if and only if $b \in I_f$. If $s_b = 2$, then $\Psi_b(\mathbf{a})$ is square, so the affine curve $\mathcal{R}_b$ is reducible. Hence we have only the trivial bound for $\#\mathcal{R}_b(\mathbb{F}_q)$, that is

$$|\#\mathcal{R}_b(\mathbb{F}_q) - q| \leq q.$$

Otherwise $s_b \leq 1$. So, $\Psi_b(\mathbf{a})$ is a non-square. Hence, the affine curve $\mathcal{R}_b$ is absolutely irreducible. Furthermore, $\mathcal{R}_b$ has s_b singular points and the genus of the nonsingular model of $\mathcal{R}_b$ equals $1 - s_b$. Also, the nonsingular model of $\mathcal{R}_b$

has zero or two $\mathbb{F}_q$-rational points at infinity (see Theorem 2.16). By using the Hasse-Weil bound we obtain

$$|\#\mathcal{R}_b(\mathbb{F}_q) - q| \leq 2(1 - s_b)\sqrt{q} + s_b + 1 \leq 2\sqrt{q} + 1.$$

This completes the proof of this proposition. □

Proof of Theorem 6.6. Let $b \in \mathbb{F}_q^*$. Proposition 6.16 shows that

$$\#(\mathtt{PEJ}^{-1}(b) \cap J_2) = \#J_{2,b} = \#H(\mathbb{F}_q) + \#\mathcal{R}_b(\mathbb{F}_q) - q - e - r_b,$$

where e, r_b are respectively equal to the numbers of square roots of f_0 and b in $\mathbb{F}_q$. We note that $0 \leq e, r_b \leq 2$. By the Hasse-Weil Theorem we have a bound for $\#H(\mathbb{F}_q)$. Further, Proposition 6.17 gives an estimate for $\#\mathcal{R}_b(\mathbb{F}_q)$. So,

$$\left|\#(\mathtt{PEJ}^{-1}(b) \cap J_2) - q + 1\right| \leq \begin{cases} 8\sqrt{q} + 2, & \text{if } f_0 \neq 0, \\ 6\sqrt{q} + 2, & \text{if } f_0 = 0 \text{ and } b \notin I_f, \\ q + 4\sqrt{q} - 1, & \text{if } f_0 = 0 \text{ and } b \in I_f. \end{cases}$$

It is easy to see that $0 \leq \#(\mathtt{PEJ}^{-1}(b) \cap J_1) \leq 2$ and $\#(\mathtt{PEJ}^{-1}(b) \cap J_0) = 0$. Hence, the proof is completed for all $b \in \mathbb{F}_q^*$.

Now assume that $b = 0$. It is easy to see that $\#\mathtt{PEJ}^{-1}(0) = e\#H(\mathbb{F}_q) - e + 1$, where e equals the number of points of $H(\mathbb{F}_q)$ whose abscissa equals zero. This concludes the proof of Theorem 6.6. □

6.3 Extractors for the Kummer surface

In this section, we propose the modified version of the *sum* and *product* extractor for the Kummer surface associated to the Jacobian of a genus-2 hyperelliptic curve over $\mathbb{F}_q$.

Let H be the hyperelliptic curve defined by Equation (6.1). Let $\mathcal{K}$ be the Kummer surface related to J, the Jacobian of H over $\mathbb{F}_q$ (see Section 2.7). We recall that each point of $J(\mathbb{F}_q)$ can be uniquely represented by at most 2 points on H. Then there exist a map

$$\begin{aligned} \kappa : J(\mathbb{F}_q) &\longrightarrow \mathcal{K}(\mathbb{F}_q) \\ P + Q - 2P_\infty &\longmapsto (1 : a : b : c) \\ P - P_\infty &\longmapsto (0 : 1 : x_P : x_P^2) \\ \mathcal{O} &\longmapsto (0 : 0 : 0 : 1), \end{aligned}$$

where $a = x_P + x_Q$, $b = x_P x_Q$ and

$$c = \begin{cases} \dfrac{\widetilde{B}(a,b) - 2y_P y_Q}{(x_P - x_Q)^2}, & \text{if } P \neq Q, \\ \dfrac{\widetilde{C}(a,b)}{4y_P^2}, & \text{if } P = Q, \end{cases}$$

with

$$\widetilde{B}(a,b) = ab^2 + f_3 ab + f_1 a + 2f_4 b^2 + 2f_2 b + 2f_0,$$
$$\widetilde{C}(a,b) = C(1,a,b).$$

We define the *sum* and *product* extractors for $\mathcal{K}$, by means of the map κ.

6.3.1 The sum extractor for the Kummer surface

Here, we define the *sum extractor* SEK for the Kummer surface $\mathcal{K}$ and the *sum extractor* SEKJ which will be the restriction of SEK to the image of κ. We briefly mention the analysis of these extractors.

Definition 6.18 *The sum extractor* SEK *for the Kummer surface $\mathcal{K}$ is defined as the function* $\mathtt{SEK} : \mathcal{K}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$, *by*

$$\mathtt{SEK}(k_1 : k_2 : k_3 : k_4) = \begin{cases} \dfrac{k_2}{k_1}, & \text{if } k_1 \neq 0, \\ \dfrac{k_3}{k_2}, & \text{if } k_1 = 0, k_2 \neq 0, \\ 0, & \text{otherwise.} \end{cases}$$

The following theorem gives estimates for $\#\mathtt{SEK}^{-1}(a)$, for all a in $\mathbb{F}_q$. By using the result of this theorem, one can show that SEK is a deterministic $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$-extractor for $\mathcal{K}(\mathbb{F}_q)$.

Theorem 6.19 *For all $a \in \mathbb{F}_q^*$,*

$$\left|\#\mathtt{SEK}^{-1}(a) - q\right| \leq 4\sqrt{q}$$

and

$$\left|\#\mathtt{SEK}^{-1}(0) - (q+1)\right| \leq 4\sqrt{q}.$$

Proof. Note that each point on $\mathcal{K}$ can be pulled back to the Jacobian of H or to the Jacobian of the quadratic twist of H. Furthermore, the map κ is $2:1$ on all points except the points of order 2 in the Jacobian of H where it is $1:1$. Then,

the proof of Theorem 6.3 and the application of that proof for the sum extractor for the Jacobian of the quadratic twist of H conclude the proof of this Theorem. □

It is possible to compute scalar multiples on $\kappa(J(\mathbb{F}_q))$ using differential addition chains so that $[n]\kappa(D) = \kappa(nD)$, where $[n]$ refers to the scalar multiplication on $\kappa(J(\mathbb{F}_q))$. This can be used for a variant of Diffie-Hellman key exchange (see [93]). Thus it is interesting to study extractors on $\kappa(J(\mathbb{F}_q)$.

Definition 6.20 *The sum extractor* $\mathtt{SEKJ}$ *for* $\kappa(J(\mathbb{F}_q))$*, is defined as the restriction of the extractor* $\mathtt{SEK}$ *to* $\kappa(J(\mathbb{F}_q))$*.*

The following theorem shows that $\#\mathtt{SEJ}^{-1}(a) = 2\#\mathtt{SEKJ}^{-1}(a)$, for almost all a in $\mathbb{F}_q$. One can show that $\mathtt{SEKJ}$ is a deterministic $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$-extractor for $\kappa(J(\mathbb{F}_q))$ (see Subsection 6.1.3).

Proposition 6.21 *For all* $a \in \mathbb{F}_q$*,*

$$\#\mathtt{SEKJ}^{-1}(a) = \frac{\#\mathtt{SEJ}^{-1}(a) + d_a}{2},$$

where d_a *is the number of two torsion points of* $J(\mathbb{F}_q)$ *in* $\mathtt{SEJ}^{-1}(a)$*.*

Proof. The fact that the map κ is $2:1$ on all points except the points of order 2 in the Jacobian of H where it is $1:1$, concludes the proof of this proposition. □

Remark 6.22 It is easy to see that $0 \leq d_a \leq 3$ and $\sum_{a\in\mathbb{F}_q} d_a$ equals the number of two torsion points of $J(\mathbb{F}_q)$, which is bounded by 16.

6.3.2 The product extractor for the Kummer surface

Similar to Subsection 6.3.1, we now define the *product extractor* $\mathtt{PEK}$ for the $\mathcal{K}$. We briefly mention the analysis of this extractor.

Definition 6.23 *The product extractor* $\mathtt{PEK}$ *for the Kummer surface* $\mathcal{K}$ *is defined as the function* $\mathtt{PEK} : \mathcal{K}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$*, by*

$$\mathtt{PEK}(k_1 : k_2 : k_3 : k_4) = \begin{cases} \dfrac{k_3}{k_1}, & \text{if } k_1 \neq 0, \\ \dfrac{k_3}{k_2}, & \text{if } k_1 = 0, k_2 \neq 0, \\ 0, & \text{otherwise.} \end{cases}$$

The next theorem gives estimates for $\#\mathtt{PEK}^{-1}(b)$, for all b in $\mathbb{F}_q$. The result of this theorem implies that PEK is a deterministic $(\mathbb{F}_q, O(\frac{1}{\sqrt{q}}))$-extractor for $\mathcal{K}(\mathbb{F}_q)$.

Theorem 6.24 *Let $b \in \mathbb{F}_q$. Let $I_f = \{z \in \mathbb{F}_q^* : f_1 = z^2, f_2 = zf_4\}$. Then*

$$\left|\#\mathtt{PEK}^{-1}(b) - q\right| \leq \begin{cases} 4\sqrt{q}+1 & \text{if } f_0 \neq 0, \\ 2\sqrt{q}+1 & \text{if } f_0 = 0 \text{ and } b \notin I_f, \\ q-1 & \text{if } f_0 = 0 \text{ and } b \in I_f. \end{cases}$$

Furthermore, one can define the *product extractor* PEKJ for $\kappa(J(\mathbb{F}_q))$ as the restriction of the extractor PEK to $\kappa(J(\mathbb{F}_q))$.

Chapter 7

Extractors for Jacobians of Genus-2 Binary Curves

In Chapter 6 we proposed the *sum* and *product* extractors for the Jacobian of a genus-2 hyper elliptic curve over a finite field with odd characteristic. Binary fields offer particularly good performance for hardware implementations (see, e.g., [50]) and genus 2 curves over binary fields were the first ones to beat elliptic curves in speed. In this chapter we investigate these extractors for $J(\mathbb{F}_q)$, the set of $\mathbb{F}_q$-rational points of the Jacobian of a genus 2 hyperelliptic curve H defined over $\mathbb{F}_q$, where $q = 2^n$.

For non-supersingular hyperelliptic curves having a Jacobian with group order $2m$, where m is odd, we describe modified *sum* and *product* extractors for the main subgroup of $J(\mathbb{F}_q)$. We show that, if $D \in J(\mathbb{F}_q)$ is chosen uniformly at random, the bits extracted from D are indistinguishable from a uniformly random bit-string of length n.

In this chapter, we first examine the sum and product extractors for $J(\mathbb{F}_q)$. To analyze these extractors, the estimates for the number of points on all fibers of `SEJ` and `PEJ` are needed. We give tight estimates in Theorems 7.2 and 7.4. The proofs follow similar lines to those in the previous chapter tacking into account

The result of this chapter was previously published as: R. R. Farashahi. Extractors for Jacobians of Binary Genus-2 Hyperelliptic Curves. In *Information Security and Privacy, 13th Australian Conference – ACISP 2008*, volume 5107 of *Lecture Notes in Computer Science*, pages 447–462. Springer-Verlag, 2008.

the different curve shape in the binary case.

7.1 The extractors for the Jacobian

Let H be an imaginary hyperelliptic curve of genus 2 over $\mathbb{F}_q$, where $q = 2^n$. Then H has a plane model defined by the equation

$$\mathbf{y}^2 + h(\mathbf{x})\mathbf{y} = f(\mathbf{x}),$$

where $h = h_2\mathbf{x}^2 + h_1\mathbf{x} + h_0$ and $f = \mathbf{x}^5 + f_4\mathbf{x}^4 + f_3\mathbf{x}^3 + f_2\mathbf{x}^2 + f_1\mathbf{x} + f_0$.

Let J be the Jacobian of H over $\mathbb{F}_q$. See Section 2.6 for the notation on $J(\mathbb{F}_q)$.

In this section, we consider the *sum* and *product extractors*, called `SEJ` and `PEJ`, for the Jacobian of H over $\mathbb{F}_q$ (see Definition 6.1 and Definition 6.4). Furthermore, we give analysis of these extractor.

7.1.1 The sum extractor

The following theorem shows the estimates for the cardinalities of all fibers $\mathtt{SEJ}^{-1}(a)$, where $a \in \mathbb{F}_q$. These estimates are needed to analyze the extractor `SEJ`. This theorem shows that the expected cardinality of each fiber essentially equals q. It also gives a precise bound on the deviation. Furthermore an exceptional case is discussed, which rarely occurs. To state the number of preimages, we first need a rather technical definition. We refer to Subsection 7.2.1 for an explanation of the case distinction.

Definition 7.1 *The set $I_{\mathtt{SEJ}} \subset \mathbb{F}_q^*$, corresponding to the hyperelliptic curve H, is defined by*

$$I_{\mathtt{SEJ}} = \begin{cases} \left\{\frac{h_1}{h_2}\right\}, & \text{if } h_2 \neq 0 \text{ and } d_1 = 0, \\ \left\{z \in \mathbb{F}_q^* : z^5 + zf_3^2 + h_0^2 = 0\right\}, & \text{if } h_2 = h_1 = 0, \\ \emptyset, & \text{otherwise,} \end{cases}$$

where $d_1 = h_2^4h_1^3f_4 + h_2^4h_1f_3^2 + h_2^5(h_2h_0 + h_1^2)f_3 + h_2^6h_1f_2 + h_2^7f_1 + h_2^5h_0^2 + h_2^4h_1^2h_0 + h_2^3h_1^4 + h_1^5$.

We will show later that for $a \in I_{\mathtt{SEJ}}$ we can only give a trivial estimate for $\#\mathtt{SEJ}^{-1}(a) - q$. However, we note that $\#I_{\mathtt{SEJ}} \leq 1$ unless the curve has $h_2 = h_1 = 0$. Curves of the latter type are supersingular. They are interesting for pairing based protocols but should be avoided if only the DL setting is needed. Even in the case of supersingular curves, the cardinality of $I_{\mathtt{SEJ}}$ is easily bounded by 5.

Theorem 7.2 *For all* $a \in \mathbb{F}_q^*$,

$$\left|\#\mathtt{SEJ}^{-1}(a) - (q+1)\right| \leq \begin{cases} 6\sqrt{q}+2, & \text{if } h_2 \neq 0 \text{ and } a \notin I_{\mathtt{SEJ}}, \\ 6\sqrt{q}+1, & \text{if } h_2 = 0 \text{ and } h_1 \neq 0, \\ 4\sqrt{q}+1, & \text{if } h_2 = h_1 = 0 \text{ and } a \notin I_{\mathtt{SEJ}}, \\ q+4\sqrt{q}+1, & \text{if } a \in I_{\mathtt{SEJ}}. \end{cases}$$

Also

$$\left|\#\mathtt{SEJ}^{-1}(0) - (q+1)\right| \leq 4\sqrt{q}+2.$$

We give a proof of this theorem in Section 7.2.

7.1.2 The product extractor

In the next theorem we give estimates for the number of points on the fibers of PEJ. The proof of this theorem will be given in Section 7.2.

Definition 7.3 *The set* $I_{\mathtt{PEJ}} \subset \mathbb{F}_q^*$, *corresponding to the hyperelliptic curve* H, *is defined by*

$$I_{\mathtt{PEJ}} = \begin{cases} \left\{(\frac{h_1}{h_2})^2\right\}, & \text{if } h_2 \neq 0, h_0 = 0 \text{ and } d = 0, \\ \emptyset, & \text{otherwise,} \end{cases}$$

where $d = h_2^4(f_1 + h_1\sqrt{f_0}) + h_1^4$.

Theorem 7.4 *For all* $b \in \mathbb{F}_q^*$,

$$\left|\#\mathtt{PEJ}^{-1}(b) - q\right| \leq \begin{cases} 8\sqrt{q}+2, & \text{if } h_0 \neq 0, \\ 6\sqrt{q}+2, & \text{if } h_0 = 0 \text{ and } b \notin I_{\mathtt{PEJ}}, \\ q+4\sqrt{q}+2, & \text{if } b \in I_{\mathtt{PEJ}}. \end{cases}$$

Also

$$\left|\#\mathtt{PEJ}^{-1}(0) - (eq+1)\right| \leq 4e\sqrt{q}\,,$$

where $e = \#\{(x,y) \in H(\mathbb{F}_q) : x = 0\}$.

7.1.3 Analysis of the extractors

In this subsection we show that, provided the divisor D is chosen uniformly at random in $J(\mathbb{F}_q)$, the bits extracted from the divisor D by the extractors SEJ or PEJ are indistinguishable from a uniformly random bit-string of length n.

Let $U_{\mathbb{F}_q}$ be a uniform random variable. Let $\mathtt{A}$ be a $\mathbb{F}_q$-valued random variable that is defined as $\mathtt{A} = \mathtt{SEJ}(D)$, for $D \in_R J(\mathbb{F}_q)$.

Proposition 7.5 *The random variable* $\mathtt{A}$ *is statistically close to uniform, more precisely,*

$$\Delta(\mathtt{A}, U_{\mathbb{F}_q}) = O\left(\frac{1}{\sqrt{q}}\right).$$

Proof. Let $a \in \mathbb{F}_q$. The uniform random variable $U_{\mathbb{F}_q}$ satisfies $\Pr[U_{\mathbb{F}_q} = a] = 1/q$. For the $\mathbb{F}_q$-valued random variable $\mathtt{A}$ we have $\Pr[\mathtt{A} = a] = \frac{\#\mathtt{SEJ}^{-1}(a)}{\#J(\mathbb{F}_q)}$. The genus of the curves we consider is 2 and so the Hasse-Weil theorem bounds the number of points as follows.

$$(\sqrt{q}-1)^4 \leq \#J(\mathbb{F}_q) \leq (\sqrt{q}+1)^4.$$

Theorem 7.2 gives a bound for $\#\mathtt{SEJ}^{-1}(a)$, for all $a \in \mathbb{F}_q$, that implies

$$\begin{aligned}\Delta(\mathtt{A}, U_{\mathbb{F}_q}) =& \frac{1}{2}\sum_{a\in\mathbb{F}_q}\left|\Pr[\mathtt{A}=a] - \Pr[U_{\mathbb{F}_q}=a]\right| = \frac{1}{2}\sum_{a\in\mathbb{F}_q}\left|\frac{\#\mathtt{SEJ}^{-1}(a)}{\#J(\mathbb{F}_q)} - \frac{1}{q}\right| \\ =& \sum_{a\in I_{SEJ}}\frac{\left|q\#\mathtt{SEJ}^{-1}(a) - \#J(\mathbb{F}_q)\right|}{2q\#J(\mathbb{F}_q)} + \sum_{a\in\mathbb{F}_q\setminus I_{SEJ}}\frac{\left|q\#\mathtt{SEJ}^{-1}(a) - \#J(\mathbb{F}_q)\right|}{2q\#J(\mathbb{F}_q)}.\end{aligned}$$

Let $w = \#I_{SEJ}$. Then

$$\begin{aligned}\Delta(\mathtt{A}, U_{\mathbb{F}_q}) \leq& \frac{(q^2+8q\sqrt{q}-4q+4\sqrt{q}-1)w+(10q\sqrt{q}-3q+4\sqrt{q}-1)(q-w)}{2q(\sqrt{q}-1)^4} \\ =& \frac{(q-2\sqrt{q}-1)w+10q\sqrt{q}-3q+4\sqrt{q}-1}{2(\sqrt{q}-1)^4} = \frac{5+\epsilon(q)}{\sqrt{q}},\end{aligned}$$

where $\epsilon(q) = \frac{\sqrt{q}(q-2\sqrt{q}-1)w+37q\sqrt{q}-56q+39\sqrt{q}-10}{2(\sqrt{q}-1)^4}$. In general w equals 0. In this case, $\epsilon(q) < 1$ for $n \geq 9$. In case that w equals 5, $\epsilon(q) < 1$ for $n \geq 10$. □

Corollary 7.6 SEJ *is a deterministic* $(n, \frac{6}{\sqrt{q}})$*-extractor for* $J(\mathbb{F}_q)$*, for* $n \geq 10$.

Similarly, by Theorem 7.4, we obtain the following analysis for the *product extractor*.

Corollary 7.7 PEJ *is a deterministic* $(n, \frac{7}{\sqrt{q}})$*-extractor for* $J(\mathbb{F}_q)$*, for* $n \geq 10$.

7.1.4 The extractor for a subgroup

Here, we provide another example of the proposed construction in Section 2.10.1. In particular we explain how to choose a distinguishing function for $J(\mathbb{F}_q)$.

Let H be an imaginary hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$, such that the order of $J(\mathbb{F}_q)$ is even. In particular let $\#J(\mathbb{F}_q) = 2m$, where m is odd. Let G be

the main subgroup of $J(\mathbb{F}_q)$ of order m. Assume T is the point of order 2 in $J(\mathbb{F}_q)$. Let β be a bit distinguishing D from $-D$ in $J(\mathbb{F}_q)$ introduced in Section 2.10.1.

For example, the function β can be defined as follows. Let $D \in J(\mathbb{F}_q)$ have Mumford representation $[u(\mathbf{x}), v(\mathbf{x})]$, where $v(\mathbf{x}) = v_1\mathbf{x} + v_0$. Let r be the remainder of h divided by u. Write $r(\mathbf{x}) = r_1\mathbf{x} + r_0$. Then $-D = [u(\mathbf{x}), v(\mathbf{x}) + r(\mathbf{x})]$. Clearly $D = -D$ if and only if $r_1 = r_0 = 0$. The function β at the point D is defined as the least significant bit of v_0/r_0 if $r_0 \neq 0$ and defined as the least significant bit of v_1/r_1 if $r_0 = 0, r_1 \neq 0$. Furthermore, $\beta(D)$ is defined as 0, if $r_1 = r_0 = 0$.

Assume $\mathtt{Ext}$ is an extractor for $J(\mathbb{F}_q)$ such that $\mathtt{Ext}(D) = \mathtt{Ext}(-D)$ for all D in $J(\mathbb{F}_q)$. Examples are the *sum* and *product* extractors. Furthermore, assume $\mathtt{Ext}(\mathcal{O}) = \mathtt{Ext}(T)$. From Subsection 2.10.1, we can define an extractor $\mathtt{ext}$ for G as a modified version of $\mathtt{Ext}$. The extractor $\mathtt{ext}$ is defined by

$$\begin{aligned} &\mathtt{ext} : G \to \mathbb{F}_q, \\ &\mathtt{ext}(D) = \mathtt{Ext}(D + \beta(D)T). \end{aligned}$$

Proposition 2.34 implies that $\mathtt{Ext}$ is an $(\mathbb{F}_q, \delta)$-deterministic extractor for $J(\mathbb{F}_q)$ if and only if $\mathtt{ext}$ is an $(\mathbb{F}_q, \delta)$-deterministic extractor for G.

Example 7.8 Let H_1 be a hyperelliptic curve defined over $\mathbb{F}_{2^{113}}$ by the equation $\mathbf{y}^2+\mathbf{xy} = \mathbf{x}^5+\mathbf{x}^2+1$. Then $\#J(\mathbb{F}_{2^{113}}) = 2p$, where $p = 5391989333430127871582329767384123076064280271501904354976419336838 1$ is a prime number. Let G_1 be the main subgroup of $J(\mathbb{F}_{2^{113}})$ of order p. Let $\mathtt{se}_1$ be the modified version of the *sum extractor* for G_1. Then $\mathtt{se}_1$ is a deterministic $(113, \frac{3.83}{\sqrt{2^{113}}})$-extractor for G_1.

Example 7.9 Let H_2 be a hyperelliptic curve defined over $\mathbb{F}_{2^{167}}$ by the equation $\mathbf{y}^2+\mathbf{xy} = \mathbf{x}^5+\mathbf{x}^2+1$. Then $\#J(\mathbb{F}_{2^{167}}) = 2p$, where $p = 1749800579826409539498002018017070262005393320797160760139803906342208135194781865436692471749 7887493$ is a prime number. Let G_2 be the main subgroup of $J(\mathbb{F}_{2^{167}})$ of order p. Let $\mathtt{se}_2$ be the modified version of the *sum extractor* for G_2. Then $\mathtt{se}_2$ is a deterministic $(167, \frac{2.08}{\sqrt{2^{167}}})$-extractor for G_2.

7.2 Proofs of theorems

In this section we give the proofs of Theorems 7.2 and 7.4. First, we introduce the preliminaries for the proofs. We also discuss the background of the case distinction in Theorems 7.2 and 7.4.

Let H^τ be a quadratic twist of H that has a plane model of the form

$$\mathbf{y}^2 + h(\mathbf{x})\mathbf{y} = f(\mathbf{x}) + \alpha h^2(\mathbf{x}), \tag{7.1}$$

where $\alpha \in \mathbb{F}_q$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha) = 1$. Let J^t be the Jacobian of H^t over $\mathbb{F}_q$. We consider partitions for $J(\mathbb{F}_q)$ and $J^t(\mathbb{F}_q)$ as introduced in Subsection 2.6.1.

Now, from Section 2.9, we recall the surface $\mathcal{X}$ defined over $\mathbb{F}_q$ by the equation

$$F(\mathbf{a}, \mathbf{b}, \mathbf{z}) = \mathbf{z}^2 + \theta(\mathbf{a}, \mathbf{b})\mathbf{z} + \psi(\mathbf{a}, \mathbf{b}) = 0, \tag{7.2}$$

where

$$\theta(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}_1\mathbf{x}_2) = h(\mathbf{x}_1)h(\mathbf{x}_2),$$
$$\psi(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{x}_1\mathbf{x}_2) = f(\mathbf{x}_1)h^2(\mathbf{x}_2) + f(\mathbf{x}_2)h^2(\mathbf{x}_1).$$

One can show that

$$\begin{aligned}\theta(\mathbf{a}, \mathbf{b}) =& h_2h_0\mathbf{a}^2 + h_2h_1\mathbf{ab} + h_1h_0\mathbf{a} + h_2^2\mathbf{b}^2 + h_1^2\mathbf{b} + h_0^2,\\ \psi(\mathbf{a}, \mathbf{b}) =& h_0^2\mathbf{a}^5 + (h_2^2f_0 + h_0^2f_4)\mathbf{a}^4 + h_1^2\mathbf{a}^3\mathbf{b}^2 + (h_2^2f_1 + h_0^2)\mathbf{a}^3\mathbf{b} + h_0^2f_3\mathbf{a}^3 +\\ & (h_2^2f_2 + h_1^2f_4)\mathbf{a}^2\mathbf{b}^2 + (h_1^2f_0 + h_0^2f_2)\mathbf{a}^2 + h_2^2\mathbf{ab}^4 + (h_2^2f_3 + h_1^2)\mathbf{ab}^3 +\\ & (h_2^2f_1 + h_1^2f_3 + h_0^2)\mathbf{ab}^2 + (h_1^2f_1 + h_0^2f_3)\mathbf{ab} + h_0^2f_1\mathbf{a}.\end{aligned}$$

In the proofs of Theorems 7.2 and 7.4, we need to study the geometry of the intersections of the surface $\mathcal{X}$ with the coordinate hyperplanes.

7.2.1 Relation between discriminant and the case distinction

In the following remark we discuss the nonsingularity of the hyperelliptic curve H. The description of the extractors required stating some special cases. The parameter d_1 in the definition of the *sum extractor* is intimately related to the discriminant of H. Indeed the description of the discriminant of H is needed to explain the nonsingularity of the fibers of the extractors.

Remark 7.10 We remark that the plane model of H is assumed not to have any affine singularities. So for $H : \mathbf{y}^2 + h(\mathbf{x})y = f(\mathbf{x})$ the following system of equations has no solution in $\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$.

$$\begin{cases} \mathbf{y}^2 + h(\mathbf{x})\mathbf{y} = f(\mathbf{x}) \\ h'(\mathbf{x})\mathbf{y} = f'(\mathbf{x}) \\ h(\mathbf{x}) = 0, \end{cases} \tag{7.3}$$

where h' and f' are respectively the derivatives of h and f. System (7.3) has a solution in $\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ if and only if the following equations have a common root in $\overline{\mathbb{F}}_q$.

$$\begin{cases} \zeta(\mathbf{x}) = h'^2(\mathbf{x})f(\mathbf{x}) + f'^2(\mathbf{x}) = 0, \\ h(\mathbf{x}) = 0. \end{cases} \tag{7.4}$$

Let $\mathcal{D} = \mathbf{Res}(h, \zeta)$. System (7.4) has a solution in $\overline{\mathbb{F}}_q$ if and only if $\mathcal{D} = 0$. That means $\mathcal{D} \neq 0$, since the curve H is nonsingular. We consider the following types for H.

1. If $h_2 \neq 0$, then
$$\mathcal{D} = \frac{h_0 h_1^4 d_1^2 + h_1^3 d_1 d_0 + h_2 d_0^2}{h_2^7},$$
where
$$\begin{aligned} d_1 = {} & h_2^4 h_1^3 f_4 + h_2^4 h_1 f_3^2 + h_2^5 (h_2 h_0 + h_1^2) f_3 + h_2^6 h_1 f_2 + h_2^7 f_1 + h_2^5 h_0^2 \\ & + h_2^4 h_1^2 h_0 + h_2^3 h_1^4 + h_1^5, \\ d_0 = {} & h_2^4 h_1^2 h_0 (h_2 h_0 + h_1^2) f_4 + h_2^4 h_0 (h_2 h_0 + h_1^2) f_3^2 + h_2^5 h_1^3 h_0 f_3 + h_2^6 h_1^2 h_0 f_2 \\ & + h_2^7 f_1^2 + h_2^7 h_1^2 f_0 + h_2^3 h_1^5 h_0 + h_2^3 h_0^4 + h_2 h_1^4 h_0^2 + h_1^6 h_0. \end{aligned}$$

2. If $h_2 = 0$ and $h_1 \neq 0$, then
$$\mathcal{D} = h_1^6 h_0^4 f_4 + h_1^4 h_0^4 f_3^2 + h_1^7 h_0^3 f_3 + h_1^8 h_0^2 f_2 + h_1^8 f_1^2 + h_1^9 h_0 f_1 + h_1^{10} f_0 + h_1^5 h_0^5 + h_0^8.$$

3. If $h_2 = h_1 = 0$ and $h_0 \neq 0$, then $\mathcal{D} = h_0^8$.

7.2.2 Proof of the sum extractor theorem

We partition J_2 into $J_2 = \bigcup_{a \in \mathbb{F}_q} J_{2,a}$, where

$$J_{2,a} = \{P_1 + P_2 - 2P_\infty \in J_2 : x_{P_1} + x_{P_2} = a\}.$$

Clearly, $J_{2,a}$ is equal to $\mathtt{SEJ}^{-1}(a) \cap J_2$. Now, our goal is to find estimates for the cardinalities of $J_{2,a}$, for all $a \in \mathbb{F}_q$. Similarly, we partition J_2^t into the subsets $J_{2,a}^t$, for all $a \in \mathbb{F}_q$.

We view the curve $\mathcal{X}_a$, for $a \in \mathbb{F}_q$, as the intersection of the surface $\mathcal{X}$ with the hyperplane $\mathbf{a} = a$. In Proposition 7.13, we shall show that the number of points on $J_{2,a}$ is related to the numbers of $\mathbb{F}_q$-rational points on the curves H and $\mathcal{X}_a$. Finally, by means of the Hasse-Weil Theorem, we obtain bounds for $\#J_{2,a}$.

Let $\mathcal{X}_a$, for $a \in \mathbb{F}_q$, be the affine curve defined over $\mathbb{F}_q$, by the equation

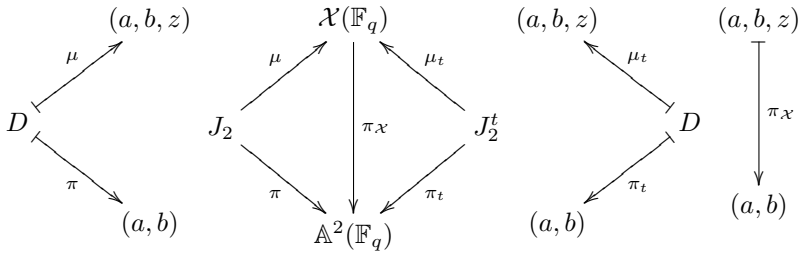
$$F_a(\mathbf{b}, \mathbf{z}) = \mathbf{z}^2 + \theta_a(\mathbf{b})\mathbf{z} + \psi_a(\mathbf{b}) = 0, \tag{7.5}$$

where $\theta_a(\mathbf{b}) = \theta(a, \mathbf{b})$ and $\psi_a(\mathbf{b}) = \psi(a, \mathbf{b})$.

Proposition 7.11 *For all $a \in \mathbb{F}_q^*$,*

$$\#J_{2,a} + \#J_{2,a}^t = 2\#\mathcal{X}_a(\mathbb{F}_q).$$

Proof. We restrict Diagram 2.11, from $J(\mathbb{F}_q) \setminus \{\mathcal{O}\}$ and $J^t(\mathbb{F}_q) \setminus \{\mathcal{O}\}$ to respectively J_2 and J_2^t. So, we consider the following diagram:



where D is a divisor either on J_2 or J_2^t represented by $P_1 + P_2 - 2P_\infty$ and where a, b, z, in the outputs of the maps μ, π, μ_t, π_t, are defined by $a = x_{P_1} + x_{P_2}$, $b = x_{P_1} x_{P_2}$ and $z = h(x_{P_1})y_{P_2} + h(x_{P_2})y_{P_1}$.

Fix $a \in \mathbb{F}_q^*$. From the proof of Proposition 2.28 (cases 1 and 3) we have

$$\#\pi^{-1}(a,b) + \#\pi_t^{-1}(a,b) = 2\#\pi_{\mathcal{X}}^{-1}(a,b),$$

for all $b \in \mathbb{F}_q$. Hence

$$\#J_{2,a} + \#J_{2,a}^t = \textstyle\sum_{b\in\mathbb{F}_q} \#\pi^{-1}(a,b) + \#\pi_t^{-1}(a,b) = \sum_{b\in\mathbb{F}_q} 2\#\pi_{\mathcal{X}}^{-1}(a,b) = 2\#\mathcal{X}_a(\mathbb{F}_q).$$

□

Proposition 7.12 *For all $a \in \mathbb{F}_q^*$,*

$$\#J_{2,a} - \#J_{2,a}^t = \#H(\mathbb{F}_q) - \#H^t(\mathbb{F}_q).$$

Proof. Let $a \in \mathbb{F}_q^*$. Let S_a be the set defined by

$$S_a = \left\{\{x, a+x\} : x \in \mathbb{F}_{q^2}\right\}.$$

We define the map $\rho : J_{2,a} \longrightarrow S_a$ by $\rho(D) = \{x_{P_1}, x_{P_2}\}$, where D is represented by $P_1 + P_2 - 2P_\infty$. Note that $x_{P_1} + x_{P_2}$ is equal to a, for $D \in J_{2,a}$. Further, we define the map $\xi : H(\mathbb{F}_q) \setminus \{P_\infty\} \longrightarrow S_a$ by $\xi(P) = \{x_P, a + x_P\}$. In a similar way, we define the maps ρ_t and ξ_t respectively for $J_{2,a}^t$ and $H^t(\mathbb{F}_q)$. We consider the following cases to show that $\#\rho^{-1}(s) - \#\rho_t^{-1}(s) = \#\xi^{-1}(s) - \#\xi_t^{-1}(s)$, for all $s \in S_a$.

1. Assume $s = \{x_1, x_2\}$, where $x_1 \in \mathbb{F}_q$, $x_2 = a + x_1$. We note that $x_1 \neq x_2$. Then there exist $y_1, y_2 \in \mathbb{F}_q$, such that $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ are points on $H(\mathbb{F}_q)$ or $H^t(\mathbb{F}_q)$. We distinguish three subcases.

(a) Suppose $h(x_1), h(x_2) \neq 0$. Without loss of generality, assume $P_1 \in H(\mathbb{F}_q)$. So, $P_1 \notin H^t(\mathbb{F}_q)$ (see Remark 2.24). First assume $P_2 \in H(\mathbb{F}_q)$ and thus $P_2 \notin H^t(\mathbb{F}_q)$. Hence $P_1 + P_2 - 2P_\infty$, $P_1 + \sigma(P_2) - 2P_\infty$, $\sigma(P_1) + P_2 - 2P_\infty$ and $\sigma(P_1) + \sigma(P_2) - 2P_\infty$ are the only divisors of $\rho^{-1}(s)$. Further, $\rho_t^{-1}(s) = \emptyset$. Also $\xi^{-1}(s) = \{P_1, P_2, \sigma(P_1), \sigma(P_2)\}$ and $\xi_t^{-1}(s) = \emptyset$.
Now assume $P_2 \notin H(\mathbb{F}_q)$ and thus $P_2 \in H^t(\mathbb{F}_q)$. So, in this case, $\rho^{-1}(s) = \rho_t^{-1}(s) = \emptyset$. Also $\xi^{-1}(s) = \{P_1, \sigma(P_1)\}$, $\xi_t^{-1}(s) = \{P_2, \sigma(P_2)\}$.

(b) Suppose exactly one of $h(x_1), h(x_2)$ is equal to 0. Without loss of generality assume $h(x_1) = 0$ and $h(x_2) \neq 0$. So, P_1 is a common point of $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$. Without loss of generality, assume $P_2 \in H(\mathbb{F}_q)$. So, $P_2 \notin H^t(\mathbb{F}_q)$. Thus, $P_1+P_2-2P_\infty$ and $P_1+\sigma(P_2)-2P_\infty$ are the only divisors of $\rho^{-1}(s)$. Furthermore, $\rho_t^{-1}(s) = \emptyset$, $\xi^{-1}(s) = \{P_1, P_2, \sigma(P_2)\}$ and $\xi_t^{-1}(s) = \{P_1\}$.

(c) Suppose $h(x_1) = h(x_2) = 0$. So P_1, P_2 belong to both $H(\mathbb{F}_q)$ and $H^t(\mathbb{F}_q)$. Hence the divisor $P_1 + P_2 - 2P_\infty$ is the only point of $\rho^{-1}(s)$ and $\rho_t^{-1}(s)$. Also $\xi^{-1}(s) = \xi_t^{-1}(s) = \{P_1, P_2\}$.

2. Assume $s = \{x_1, x_2\}$, where $x_1 \in \mathbb{F}_{q^2}$, $x_2 = a + x_1$. Note that $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(\alpha) = 0$. So, there exists a $\beta \in \mathbb{F}_{q^2}$ such that $\beta^2 + \beta = \alpha$. Then, (x, y) is a point of $H(\mathbb{F}_{q^2})$ if and only if $(x, y + \beta h(x))$ is a point of $H^t(\mathbb{F}_{q^2})$. Therefore, $(x_1, y_1) + (x_2, y_2) - 2P_\infty$ is a divisor of $J_{2,a}$ if and only if $(x_1, y_1 + \beta h(x_1)) + (x_2, y_2 + \beta h(x_2)) - 2P_\infty$ is a divisor of $J_{2,a}^t$. Hence $\#\rho^{-1}(s) = \#\rho_t^{-1}(s)$. Further, $\#\xi^{-1}(s) = \#\xi_t^{-1}(s) = 0$.

We conclude that, in both cases $\#\rho^{-1}(s) - \#\rho_t^{-1}(s) = \#\xi^{-1}(s) - \#\xi_t^{-1}(s)$, for all $s \in S_a$. Then, by summing over all $s \in S_a$, the proof of this proposition is complete. □

Proposition 7.13 *For all $a \in \mathbb{F}_q$,*

$$\#J_{2,a} = \#H(\mathbb{F}_q) + \#\mathcal{X}_a(\mathbb{F}_q) - q - 1.$$

Proof. This proposition is a direct consequence of Propositions 7.11 and 7.12. □

Now, an estimate for the cardinality of the curve $\mathcal{X}_a$ is needed. For almost all $a \in \mathbb{F}_q^*$ the affine curve $\mathcal{X}_a$ is absolutely irreducible and nonsingular. We will now show that, in fact, the curve $\mathcal{X}_a$ is reducible if and only if $a \in I_{\mathtt{SEJ}}$. Provided that the curve $\mathcal{X}_a$ is absolutely irreducible, the genus of the nonsingular model of $\mathcal{X}_a$ is at most 1. We give conditions for $\mathcal{X}_a$ to be nonsingular. For a nonsingular curve we can use the Hasse-Weil theorem to bound $\#\mathcal{X}_a(\mathbb{F}_q)$ which leads to a proof of Theorem 7.2.

Proposition 7.14 *The affine curve $\mathcal{X}_a$, for $a \in \mathbb{F}_q^*$, is absolutely irreducible if and only if $a \notin I_{SEJ}$.*

Proof. The affine curve $\mathcal{X}_a$, for $a \in \mathbb{F}_q^*$, is defined by Equation (7.5). So, we consider the polynomial

$$F_a(\mathbf{b}, \mathbf{z}) = \mathbf{z}^2 + \theta_a(\mathbf{b})\mathbf{z} + \psi_a(\mathbf{b}).$$

First, we assume $h_2 \neq 0$. Then the leading terms of θ_a and ψ_a are respectively $h_2^2\mathbf{b}^2$ and $h_2^2 a\mathbf{b}^4$. Suppose F_a is reducible. So, there exists a bivariate polynomial M in $\overline{\mathbb{F}}_q[\mathbf{b}, \mathbf{z}]$, which is a nontrivial factor of F_a and thus has degree 1 in variable $\mathbf{z}$. We can put

$$M(\mathbf{b}, \mathbf{z}) = \mathbf{z} + e(\mathbf{b}) = \mathbf{z} + c_2\mathbf{b}^2 + c_1\mathbf{b} + c_0,$$

where c_2, c_1 and c_0 are unknowns in $\overline{\mathbb{F}}_q$. Since M is a factor of F_a, the substitution of $e(\mathbf{b})$ for $\mathbf{z}$ in F_a must lead to $r(\mathbf{b}) = F_a(\mathbf{b}, e(\mathbf{b})) = 0$. The remainder is

$$r(\mathbf{b}) = r_4\mathbf{b}^4 + r_3\mathbf{b}^3 + r_2\mathbf{b}^2 + r_1\mathbf{b} + r_0 = 0.$$

We obtain the following set of equations:

$$\begin{cases} r_4 = \ c_2^2 + h_2^2 c_2 + h_2^2 a = 0, \\ r_3 = \ tc_2 + h_2^2 c_1 + (h_2^2 f_3 + h_1^2)a = 0, \\ r_2 = \ sc_2 + c_1^2 + tc_1 + h_2^2 c_0 + h_1^2 a^3 + (h_2^2 f_2 + h_1^2 f_4)a^2 \\ \qquad + (h_2^2 f_1 + h_1^2 f_3 + h_0^2)a = 0, \\ r_1 = \ sc_1 + tc_0 + (h_2^2 f_1 + h_0^2)a^3 + (h_1^2 f_1 + h_0^2 f_3)a = 0, \\ r_0 = \ c_0^2 + sc_0 + h_0^2 a^5 + (h_2^2 f_0 + h_0^2 f_4)a^4 + h_0^2 f_3 a^3 \\ \qquad + (h_1^2 f_0 + h_0^2 f_2)a^2 + h_0^2 f_1 a = 0, \end{cases} \tag{7.6}$$

where $s = h_0(h_2a^2 + h_1a + h_0)$ and $t = h_1(h_2a + h_1)$. We compute c_1 from the equation of r_3 and substitute the outcome in the equations for r_2 and r_1. Then, from the new equation of r_2, we compute c_0 and substitute this in the equations of r_1 and r_0. Then

$$\begin{cases} r_4 = \ c_2^2 + h_2^2 c_2 + h_2^2 a = 0, \\ h_2^6 r_1 = \ t^3 r_4 + a^2(h_2a + h_1)d_1 = 0, \\ h_2^{12} h_1^2 r_0 = \ t^4 r_4^2 + h_2^6 h_1^2 (h_2^2 s^2 + st^2) r_4 \\ \qquad + a^2(a^2 d_1^2 + h_2^5(h_2a + h_1)^2 d_0 + h_2^5 h_1^2 h_0(h_2a + h_1)d_1) = 0. \end{cases}$$

From the first two equations above, we have $(h_2a + h_1)d_1 = 0$, since $a \neq 0$. If $h_2a + h_1 = 0$, by the third equation, $d_1 = 0$. And if $d_1 = 0$, then $h_2a + h_1 = 0$, since $d_0 \neq 0$ (see Remark 7.10). So $a \in I_{\mathtt{SEJ}}$.
Now, to prove the reverse direction, suppose $a \in I_{\mathtt{SEJ}}$. Then $(h_2a + h_1) = d_1 = 0$.

We note that $h_1 \neq 0$, since $a \neq 0$. The above shows that System (7.6) has a solution. So, F_a is reducible.

Secondly we assume that $h_2 = 0$ and $h_1 \neq 0$. Then the leading terms of θ_a and ψ_a are respectively $h_1^2\mathbf{b}$ and $h_1^2 a\mathbf{b}^3$. Clearly F_a, for all $a \in \mathbb{F}_q$, is absolutely irreducible. Indeed in this case $I_{\mathtt{SEJ}} = \emptyset$.

Finally we assume $h_2 = h_1 = 0$ and $h_0 \neq 0$. The leading terms of θ_a and ψ_a are respectively h_0^2 and $h_0^2 a\mathbf{b}^2$. Suppose that the polynomial $\mathbf{z} + e(\mathbf{b})$ in $\overline{\mathbb{F}}_q[\mathbf{b}, \mathbf{z}]$, where $e(\mathbf{b}) = c_1\mathbf{b} + c_0$, is a factor of F_a. We substitute $\mathbf{z}$ by e in the equation of F_a. Then we have the remainder $r_2\mathbf{b}^2 + r_1\mathbf{b} + r_0$. Then

$$\begin{cases} r_2 = \ c_1^2 + h_0^2 a = 0, \\ r_1 = \ h_0^2 c_1 + h_0^2 a(a^2 + f_3) = 0, \\ r_0 = \ c_0^2 + h_0^2 c_0 + h_0^2(a^5 + f_4 a^4 + f_3 a^3 + f_2 a^2 + f_1 a) = 0. \end{cases}$$

We compute c_1 from the second equation and substitute it in the first one. We obtain $a(a^5 + f_3^2 a + h_0^2) = 0$. So, F_a is reducible if and only if $a^5 + f_3^2 a + h_0^2$, since $a \neq 0$. □

Proposition 7.15 *The affine curve $\mathcal{X}_a$, for $a \in \mathbb{F}_q^*$, is singular if and only if $h_2 \neq 0$ and $ah_2 + h_1 = 0$.*

Proof. Suppose the affine curve $\mathcal{X}_a$, for $a \in \mathbb{F}_q^*$, is singular. Then the following system of equations has a solution in $\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$:

$$\begin{cases} F_a(\mathbf{b}, \mathbf{z}) = \mathbf{z}^2 + \theta_a(\mathbf{b})\mathbf{z} + \psi_a(\mathbf{b}) = 0, \\ \dfrac{\partial F_a}{\partial \mathbf{b}}(\mathbf{b}, \mathbf{z}) = \theta_a'(\mathbf{b})\mathbf{z} + \psi_a'(\mathbf{b}) = 0, \\ \dfrac{\partial F_a}{\partial \mathbf{z}}(\mathbf{b}, \mathbf{z}) = \theta_a(\mathbf{b}) = 0, \end{cases} \tag{7.7}$$

where θ_a' and ψ_a' are respectively the derivatives of θ_a and ψ_a with respect to $\mathbf{b}$. Then, from System (7.7), the following equations have a common root in $\overline{\mathbb{F}}_q$.

$$\begin{cases} \zeta_a(\mathbf{b}) = {\theta'}_a^2(\mathbf{b})\psi_a(\mathbf{b}) + {\psi'}_a^2(\mathbf{b}) = 0, \\ \theta_a(\mathbf{b}) = 0. \end{cases}$$

So, the resultant of ζ_a and θ_a equals 0. Let $R = \mathbf{Res}(\zeta_a, \theta_a)$. First assume $h_2 \neq 0$. Then $R = a^4(ah_2 + h_1)^8\mathcal{D}$. So $ah_2 + h_1 = 0$, since $\mathcal{D} \neq 0$ (see Remark 7.10). Now assume $h_2 = 0$. If $h_1 \neq 0$, then $R = a^2 h_1^4 \mathcal{D}$. Hence $R \neq 0$, which is a contradiction. If $h_1 = 0$ and $h_0 \neq 0$, then $\theta_a(\mathbf{b}) = h_0^2 \neq 0$.

To prove the reverse direction, suppose $h_2 \neq 0$ and $h_2 a + h_1 = 0$, so $a = \frac{h_1}{h_2}$. Then, one can see that point $(\frac{h_0}{h_2}, 0)$ is a zero of System 7.7, i.e., a singular point of $\mathcal{X}_{\frac{h_1}{h_2}}$. □

Proposition 7.16 *For all $a \in \mathbb{F}_q^*$, we have*

$$|\#\mathcal{X}_a(\mathbb{F}_q) - q| \leq \begin{cases} 2\sqrt{q}+1, & \text{if } h_2 \neq 0 \text{ and } a \notin I_{\mathtt{SEJ}}, \\ 2\sqrt{q}, & \text{if } h_2 = 0 \text{ and } h_1 \neq 0, \\ 0, & \text{if } h_2 = h_1 = 0 \text{ and } a \notin I_{\mathtt{SEJ}}, \\ q, & \text{if } a \in I_{\mathtt{SEJ}}. \end{cases}$$

Proof. Let $a \in \mathbb{F}_q^*$. Let $\widetilde{\mathcal{X}}_a$ be the nonsingular projective model of $\mathcal{X}_a$. First assume $h_2 \neq 0$. Suppose $a \notin I_{\mathtt{SEJ}}$. Proposition 7.14 implies that the affine curve $\mathcal{X}_a$ is absolutely irreducible. The projective model of $\mathcal{X}_a$ has one point at infinity which is a singular point. By means of the Newton polygon of F_a, one can see that the genus of $\widetilde{\mathcal{X}}_a$ is at most 1. If $a \neq \frac{h_1}{h_2}$, by Proposition 7.15, the affine curve $\mathcal{X}_a$ is nonsingular. If $a = \frac{h_1}{h_2}$, the curve $\mathcal{X}_a$ has a singular point, so the genus of $\widetilde{\mathcal{X}}_a$ equals 0. The number of $\mathbb{F}_q$-rational points on $\widetilde{\mathcal{X}}_a$, which are lying over this singular point in the resolution map, equals 1 (see e.g. see [6], Remark 3.16 and 3.18). The number of $\mathbb{F}_q$-rational points on $\widetilde{\mathcal{X}}_a$, which are lying over the point at infinity, is at most 2. Hence

$$\left|\#\mathcal{X}_a(\mathbb{F}_q) - \#\widetilde{\mathcal{X}}_a(\mathbb{F}_q) + 1\right| \leq 1.$$

By means of the Hasse-Weil Theorem for $\widetilde{\mathcal{X}}_a$, we obtain an estimate for $\#\mathcal{X}_a(\mathbb{F}_q)$.

Secondly assume $h_2 = 0$ and $h_1 \neq 0$. Propositions 7.14 and 7.15 imply that $\mathcal{X}_a$ is an absolutely irreducible nonsingular curve. Indeed the projective model of $\mathcal{X}_a$ is an elliptic curve. Hence

$$|\#\mathcal{X}_a(\mathbb{F}_q) - q| \leq 2\sqrt{q}.$$

Now assume $h_2 = h_1 = 0$ and $h_0 \neq 0$. Suppose $a \notin I_{\mathtt{SEJ}}$. Then $\mathcal{X}_a$ is an absolutely irreducible nonsingular curve (see Propositions 7.14 and 7.15). The projective model of $\mathcal{X}_a$ is a nonsingular curve of genus 0. It has one point at infinity. Hence, $\#\mathcal{X}_a(\mathbb{F}_q) = q$.

If $a \in I_{\mathtt{SEJ}}$ the curve $\mathcal{X}_a$ is reducible. Then we have a trivial bound for $\#\mathcal{X}_a(\mathbb{F}_q)$. □

Proof of Theorem 7.2. Let $a \in \mathbb{F}_q^*$. Proposition 7.13 shows that

$$\#(\mathtt{SEJ}^{-1}(a) \cap J_2) = \#H(\mathbb{F}_q) + \#\mathcal{X}_a(\mathbb{F}_q) - q - 1.$$

Since $\mathtt{SEJ}^{-1}(a) \subset J(\mathbb{F}_q)$ and $J(\mathbb{F}_q) = J_0 \cup J_1 \cup J_2$ we can estimate $\#\mathtt{SEJ}^{-1}(a)$ from bounds on $\#(\mathtt{SEJ}^{-1}(a) \cap J_1)$ and $\#(\mathtt{SEJ}^{-1}(a) \cap J_0)$. The latter is 0 since $a \neq 0$ while the former equals $0, 1$ or 2. Hence

$$\left|\#\mathtt{SEJ}^{-1}(a) - \#H(\mathbb{F}_q) - \#\mathcal{X}_a(\mathbb{F}_q) + q\right| \leq 1.$$

By the Hasse-Weil Theorem, we have $|\#H(\mathbb{F}_q) - q - 1| \leq 4\sqrt{q}$. Then, Proposition 7.16 concludes the proof of Theorem 7.2, for all $a \in \mathbb{F}_q^*$.

If $a = 0$, then it is easy to show that $\#\mathtt{SEJ}^{-1}(0) = \#H(\mathbb{F}_q) + e - s$, where $e = \#\{(x, y) \in H(\mathbb{F}_q) : x = 0\}$ and $s = \#\{(x, y) \in H(\mathbb{F}_q) : h(x) = 0\}$. Hence, the proof of this theorem is completed. □

7.2.3 Proof of the product extractor theorem

We follow a similar approach for the proof of this theorem as we did in Subsection 7.4. We consider the partition $J_2 = \bigcup_{b \in \mathbb{F}_q} J_{2,b}$, where

$$J_{2,b} = \{P_1 + P_2 - 2P_\infty \in J_2 : x_{P_1} x_{P_2} = b\}.$$

Also, we partition J_2^t into the subsets $J_{2,b}^t$, for all $b \in \mathbb{F}_q$.

For for $b \in \mathbb{F}_q^*$, let $\mathcal{X}_b$, be the affine curve defined by the equation

$$F_b(\mathbf{a}, \mathbf{z}) = \mathbf{z}^2 + \theta_b(\mathbf{a})\mathbf{z} + \psi_b(\mathbf{a}) = 0, \tag{7.8}$$

where $\theta_b(\mathbf{a}) = \theta(\mathbf{a}, b)$ and $\psi_b(\mathbf{a}) = \psi(\mathbf{a}, b)$.

Proposition 7.17 *For all $b \in \mathbb{F}_q^*$,*

$$\#J_{2,b} = \#H(\mathbb{F}_q) + \#\mathcal{X}_b(\mathbb{F}_q) - q - e - 1,$$

where $e = \#\{(x, y) \in H(\mathbb{F}_q) : x = 0\}$.

Proof. Let $b \in \mathbb{F}_q^*$. Similar to Proposition 7.11, we can express the sum of the cardinalities of $J_{2,b}$ and $J_{2,b}^t$ in terms of the number of $\mathbb{F}_q$-rational points on $\mathcal{X}_b$. In fact,

$$\#J_{2,b} + \#J_{2,b}^t = 2\#\mathcal{X}_b(\mathbb{F}_q) - 2.$$

Also, as in Proposition 7.12, we can show that

$$\#J_{2,b} - \#J_{2,b}^t = \#H(\mathbb{F}_q) - \#H^t(\mathbb{F}_q) - 2e + 2,$$

where e is the number of points on $H(\mathbb{F}_q)$ with x-coordinate equal to 0. Noticing that $\#H(\mathbb{F}_q) + \#H^t(\mathbb{F}_q) = 2q + 2$ concludes the proof of this proposition. □

Proposition 7.18 *The affine curve $\mathcal{X}_b$, for $b \in \mathbb{F}_q^*$, is absolutely irreducible if and only if $b \notin I_{PEJ}$.*

Proof. The affine curve $\mathcal{X}_b$, for $b \in \mathbb{F}_q^*$, is defined by Equation (7.8). So, we consider the polynomial

$$F_b(\mathbf{a}, \mathbf{z}) = \mathbf{z}^2 + \theta_b(\mathbf{a})\mathbf{z} + \psi_b(\mathbf{a}).$$

First, assume $h_0 \neq 0$. So, the leading term of ψ_b equals $h_0^2\mathbf{a}^5$, i.e., ψ_b is a polynomial of degree 5. Further, the degree of the polynomial θ_b is less than or equal to 2. Hence, the polynomial F_b is absolutely irreducible.

Now, assume $h_0 = 0$. So, $\deg(\theta_b) \leq 1$ and $\deg(\psi_b) \leq 4$. Suppose F_b is reducible. So, there exists a bivariate polynomial M in $\overline{\mathbb{F}}_q[\mathbf{a}, \mathbf{z}]$, which is a nontrivial factor of F_b and thus has degree 1 in variable $\mathbf{z}$. We can put

$$M(\mathbf{a}, \mathbf{z}) = \mathbf{z} + e(\mathbf{a}) = \mathbf{z} + c_2\mathbf{a}^2 + c_1\mathbf{a} + c_0,$$

where c_2, c_1 and c_0 are unknowns in $\overline{\mathbb{F}}_q$. Because M is a factor of F_b, $r(\mathbf{a}) = F_b(\mathbf{a}, e(\mathbf{a}))$ must be equal to 0. The remainder is

$$r(\mathbf{a}) = r_4\mathbf{a}^4 + r_3\mathbf{a}^3 + r_2\mathbf{a}^2 + r_1\mathbf{a} + r_0 = 0.$$

We obtain the following set of equations:

$$\begin{cases} r_4 = \ c_2^2 + h_2^2 f_0 = 0, \\ r_3 = \ h_2 h_1 b c_2 + h_1^2 b^2 + h_2^2 f_1 b = 0, \\ r_2 = \ s c_2 + c_1^2 + h_2 h_1 b c_1 + (h_2^2 f_2 + h_1^2 f_4) b^2 + h_1^2 f_0 = 0, \\ r_1 = \ s(c_1 + b^2 + f_3 b + f_1) + h_2 h_1 b c_0 = 0, \\ r_0 = \ c_0^2 + s c_0 = 0, \end{cases} \tag{7.9}$$

where $s = b(h_2^2 b + h_1^2)$. From the equation of r_4, we obtain $c_2 = h_2\sqrt{f_0}$. Then, we substitute $h_2\sqrt{f_0}$ for c_2 in equations r_3 and r_2. From the new equation of r_3, we have

$$b(h_2^2 h_1\sqrt{f_0} + h_1^2 b + h_2^2 f_1) = 0. \tag{7.10}$$

Suppose $s \neq 0$. From the equation of r_0, we easily see that c_0 equals 0 or s. Suppose $c_0 = 0$. Then, from the equation of r_1, we get $c_1 = b^2 + f_3 b + f_1$. We replace c_1 by $b^2 + f_3 b + f_1$ in the new equation of r_2. Then, Equation 7.10 implies $h_1^8 r_2 = \mathcal{D}$, which is a contradiction, since $\mathcal{D} \neq 0$ (see Remark 7.10). The same statement can be proven if $c_0 = s$. So, suppose $s = 0$, i.e., $h_2^2 b + h_1^2 = 0$, since $b \neq 0$. We note that $h_2 \neq 0$. If $h_2 = 0$, then $h_1 = 0$, so $h = 0$, which makes H singular. So, $b = (\frac{h_1}{h_2})^2$. From Equation 7.10, we get $(h_2^4(f_1 + h_1\sqrt{f_0}) + h_1^4)/h_2^2 = 0$. This means $d = 0$, which implies $b \in I_{\mathtt{PEJ}}$.

Now, to prove the opposite direction, suppose $b \in I_{\mathtt{PEJ}}$. Then, $h_1 = 0$ and $h_2^2 b + h_1^2 = 0$, so $s = 0$. The above shows that the System (7.9) has a solution. Hence, F_b is reducible. □

Proposition 7.19 *For $b \in \mathbb{F}_q^*$, the affine curve $\mathcal{X}_b$ is singular if and only if $b \in S_{\texttt{PEJ}}$, where*

$$S_{\texttt{PEJ}} = \begin{cases} \left\{\frac{h_0}{h_2}\right\} \bigcup \left\{z \in \mathbb{F}_q^* : z^2 + (\frac{h_1}{h_2})^2 z + (\frac{h_0}{h_2})^2 = 0\right\}, & \text{if } h_2 \neq 0 \text{ and } h_0 \neq 0, \\ \left\{(\frac{h_1}{h_2})^2\right\}, & \text{if } h_2 \neq 0, h_0 = 0 \text{ and } h_1 \neq 0, \\ \left\{(\frac{h_0}{h_1})^2\right\}, & \text{if } h_2 = 0, h_0 \neq 0 \text{ and } h_1 \neq 0, \\ \emptyset, & \text{otherwise.} \end{cases}$$

Proof. Suppose the affine curve $\mathcal{X}_b$, for $b \in \mathbb{F}_q^*$, is singular. Then, similar to the proof of Proposition 7.15, the following equations must have a common root in $\overline{\mathbb{F}}_q$.

$$\begin{cases} \zeta_b(\mathbf{a}) = {\theta'}_b^2(\mathbf{a})\psi_b(\mathbf{a}) + {\psi'}_b^2(\mathbf{a}) = 0, \\ \theta_b(\mathbf{a}) = 0. \end{cases}$$

So, $R = \mathbf{Res}(\zeta_b, \theta_b)$, the resultant of ζ_b and θ_b, is equal to 0. First assume $h_2 \neq 0$. If $h_0 \neq 0$, then $R = h_0^4(h_2 b + h_0)^8(h_2^2 b^2 + h_1^2 b + h_0^2)^2\mathcal{D}$. Hence, $b \in S_{\texttt{PEJ}}$, since $\mathcal{D} \neq 0$ (see Remark 7.10). If $h_0 = 0$, then $(h_1^2 f_0 + f_1^2)R = b^8(h_2^2 b + h_1^2)^2\mathcal{D}$, so, $h_2^2 b + h_1^2 = 0$. If $h_1 = 0$, then $b = 0$, which contradicts our assumption, so $h_1 \neq 0$. Hence, $b \in S_{\texttt{PEJ}}$. Now assume $h_2 = 0$. If $h_0, h_1 \neq 0$, we have $R = h_0^8(h_1^2 b + h_0^2)^2\mathcal{D}$. So, $h_1^2 b + h_0^2 = 0$, i.e., $b \in S_{\texttt{PEJ}}$. If $h_0 = 0$, then $\theta_b(\mathbf{a}) = h_1^2 b \neq 0$, which is a contradiction. Also, if $h_1 = 0$, then $\theta_b(\mathbf{a}) = h_0^2 \neq 0$, which is again a contradiction. We note that if $h_2 = h_1 = h_0 = 0$, H is singular.

To prove the equivalence in the opposite direction, suppose $b \in \mathbb{F}_q^*$. If $h_2, h_0 \neq 0$ and $b = \frac{h_0}{h_2}$, then the point $(\frac{h_1}{h_2}, 0)$ is a singular point of $\mathcal{X}_b$. In other cases, the point $(0, 0)$ is a singular point of $\mathcal{X}_b$. □

Proposition 7.20 *For all $b \in \mathbb{F}_q^*$ we have*

$$|\#\mathcal{X}_b(\mathbb{F}_q) - q| \leq \begin{cases} 4\sqrt{q}, & \text{if } h_0 \neq 0, \\ 2\sqrt{q}, & \text{if } h_0 = 0 \text{ and } b \notin I_{\texttt{PEJ}}, \\ q, & \text{if } b \in I_{\texttt{PEJ}}. \end{cases}$$

Proof. Let $b \in \mathbb{F}_q^*$. Let $\widetilde{\mathcal{X}}_b$ be the nonsingular projective model of $\mathcal{X}_b$. First assume $h_0 \neq 0$. Proposition 7.18 shows that $\mathcal{X}_b$ is an absolutely irreducible curve. If $b \notin S_{\texttt{PEJ}}$, from Proposition 7.19, affine curve $\mathcal{X}_b$ is nonsingular. So, $\widetilde{\mathcal{X}}_b$ is a genus-2 hyperelliptic curve. If $b \in S_{\texttt{PEJ}}$, affine curve $\mathcal{X}_b$ has a singular point, so the genus of $\widetilde{\mathcal{X}}_b$ equals 1. So, in both cases, by means of the Hasse-Weil Theorem, we have

$$|\#\mathcal{X}_b(\mathbb{F}_q) - q| \leq 4\sqrt{q}.$$

Secondly assume $h_0 = 0$ and $b \notin I_{\mathtt{PEJ}}$. Now, Proposition 7.18 shows that $\mathcal{X}_b$ is an absolutely irreducible curve. The projective model of $\mathcal{X}_b$ has one point at infinity, which may be a singular point that is ramified. So, $\#\widetilde{\mathcal{X}}_a(\mathbb{F}_q) = \#\mathcal{X}_a(\mathbb{F}_q) + 1$. If $b \notin S_{\mathtt{PEJ}}$, then $\mathcal{X}_b$ is a nonsingular genus-1 curve. Otherwise, $\mathcal{X}_b$ has singular points, which implies that the genus of $\widetilde{\mathcal{X}}_b$ is equal 0. Then, from the Hasse-Weil Theorem, we have

$$|\#\mathcal{X}_b(\mathbb{F}_q) - q| \leq 2\sqrt{q}.$$

If $b \in I_{\mathtt{SEJ}}$ the curve $\mathcal{X}_b$ is reducible. Then, we have a trivial estimate for $\#\mathcal{X}_b(\mathbb{F}_q)$. □

Proof of Theorem 7.4 Let $b \in \mathbb{F}_q^*$. Proposition 7.17 shows that

$$\#(\mathtt{PEJ}^{-1}(b) \cap J_2) = \#H(\mathbb{F}_q) + \#\mathcal{X}_b(\mathbb{F}_q) - q - e - 1,$$

where $0 \leq e \leq 2$. Obviously $\#(\mathtt{PEJ}^{-1}(b) \cap J_1)$ equals $0, 1$ or 2. Furthermore, $\#(\mathtt{PEJ}^{-1}(b) \cap J_0) = 0$, since $b \neq 0$. So

$$\left|\#\mathtt{PEJ}^{-1}(b) - \#H(\mathbb{F}_q) - \#\mathcal{X}_b(\mathbb{F}_q) + q + 1\right| \leq 2.$$

By means of the Hasse-Weil bound for the cardinality of $H(\mathbb{F}_q)$ and Proposition 7.20 for bounds on the cardinality of $\mathcal{X}_b(\mathbb{F}_q)$, we obtain bounds for the number of points on $\mathtt{PEJ}^{-1}(b)$, where $b \in \mathbb{F}_q^*$.

If $b = 0$, then it is easy to show that $\#\mathtt{PEJ}^{-1}(a) = e\#H(\mathbb{F}_q) - e + 1$. This completes the proof. □

Chapter 8

Binary Edwards Curves

In this chapter, we introduce a new method of carrying out computations on binary elliptic curves, i.e., elliptic curves over fields $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) = 2$. In particular, we introduce "complete binary Edwards curves." We present explicit formulas for addition on these curves, an explicit birational equivalence to an elliptic curve in short Weierstrass form, explicit formulas for doubling, and explicit formulas for Montgomery-type differential addition. See Section 8.1 for the curve shape and birational equivalence; Sections 8.2 and 8.4 for the addition law; Section 8.5 for doubling; and Section 8.6 for differential addition.

Our curve equation has a surprisingly large number of terms but shares many geometric features with non-binary Edwards curves $\mathbf{x}^2 + \mathbf{y}^2 = 1 + d\mathbf{x}^2\mathbf{y}^2$. In particular, we prove that our formulas are complete. We also show that if $n \geq 3$ then every ordinary elliptic curve over $\mathbb{F}_{2^n}$ is birationally equivalent to a complete binary Edwards curve. See Section 8.3.

Our doubling formulas and differential-addition formulas are extremely fast: for example, $2\mathbf{M} + 6\mathbf{S}$ for projective doubling, and $5\mathbf{M} + 4\mathbf{S}$ for one step of a Montgomery ladder, when curves are chosen to have small parameters. Here $\mathbf{M}$ is a field multiplication and $\mathbf{S}$ is a field squaring. For comparison, state-of-the-art formulas for small-parameter Weierstrass curves—the best formulas in the literature, and some new speedups that we present—use $2\mathbf{M} + 4\mathbf{S}$ for projective doubling and $5\mathbf{M} + 4\mathbf{S}$ for one step of a Montgomery ladder. There is one caveat, namely that

The result of this chapter was previously published as: D. J. Bernstein, T. Lange, and R. R. Farashahi. Binary Edwards Curves. In *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 244–265. Springer-Verlag, 2008.

our general addition formulas use at best $16\mathbf{M}+1\mathbf{S}$ and are therefore not as fast as previous (incomplete) formulas; we can nevertheless recommend binary Edwards curves for a wide variety of applications.

8.1 Binary Edwards curves

In this section we introduce the new curve shape and show that the affine points are nonsingular. The points at infinity are singular; we give details on the blowup. To prove that the curve describes an elliptic curve we state a birational map to an ordinary elliptic curve in Weierstrass form.

Definition 8.1 (Binary Edwards curve) *Let $\mathbb{F}$ be a field with* $\mathrm{char}(\mathbb{F}) = 2$. *Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The* binary Edwards curve with coefficients d_1 and d_2 *is the affine curve*

$$\mathrm{E}_{\mathrm{B},d_1,d_2} : d_1(\mathbf{x}+\mathbf{y}) + d_2(\mathbf{x}^2+\mathbf{y}^2) = \mathbf{xy} + \mathbf{xy}(\mathbf{x}+\mathbf{y}) + \mathbf{x}^2\mathbf{y}^2.$$

This curve is symmetric in $\mathbf{x}$ and $\mathbf{y}$ and thus has the property that if (x_1, y_1) is a point on the curve then so is (y_1, x_1). We will see in Section 8.2 that (y_1, x_1) is the negative of (x_1, y_1). The only curve points invariant under this negation law are $(0, 0)$ and $(1, 1)$; $(0, 0)$ will be the neutral element of the addition law while $(1, 1)$ will have order 2. We will also see that $(x_1, y_1) + (1, 1) = (x_1 + 1, y_1 + 1)$.

Theorem 8.2 (Nonsingularity) *Each binary Edwards curve is nonsingular.*

Proof. By definition the curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ has $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The partial derivatives of the curve equation are $d_1 + y + y^2$ and $d_1 + x + x^2$. A singular point (x_1, y_1) must have $d_1 + y_1 + y_1^2 = 0$ and $d_1 + x_1 + x_1^2 = 0$, and therefore $(x_1 + y_1)^2 = x_1 + y_1$, implying $x_1 = y_1$ or $x_1 = y_1 + 1$.

The case $x_1 = y_1$ implies $0 = x_1^2 + x_1^4$ by the curve equation and therefore $d_1^2 = x_1^2 + x_1^4 = 0$, contradicting the hypothesis that $d_1 \neq 0$.

The case $x_1 = y_1 + 1$ implies $d_1 + d_2 = y_1^2 + y_1^4$ by the curve equation and therefore $d_1^2 = y_1^2 + y_1^4 = d_1 + d_2$, contradicting the hypothesis that $d_2 \neq d_1^2 + d_1$. □

Singularities of the projective closure. The projective closure of the curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ is

$$d_1(X+Y)Z^3 + d_2(X^2+Y^2)Z^2 = XYZ^2 + XY(X+Y)Z + X^2Y^2.$$

It has the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ at infinity. Both are singular. We present details on the blowup for the first point; by the symmetry of the curve equation all considerations also hold for the second point.

To study the curve around $(1:0:0)$ we consider the affine curve

$$d_1(1+\mathbf{y})\mathbf{z}^3 + d_2(1+\mathbf{y}^2)\mathbf{z}^2 = \mathbf{y}\mathbf{z}^2 + \mathbf{y}(1+\mathbf{y})\mathbf{z} + \mathbf{y}^2.$$

The partial derivatives $d_1\mathbf{z}^3 + \mathbf{z}^2 + \mathbf{z}$ and $d_1(1+\mathbf{y})\mathbf{z}^2 + \mathbf{y}(1+\mathbf{y})$ both vanish in $(0,0)$ which shows that the point is singular. We blow up the singularity by putting $\mathbf{y} = \mathbf{t}\mathbf{z}$ and dividing by $\mathbf{z}^2$, obtaining the curve

$$d_1(1+\mathbf{t}\mathbf{z})\mathbf{z} + d_2(1+\mathbf{t}^2\mathbf{z}^2) = \mathbf{t}\mathbf{z} + \mathbf{t}(1+\mathbf{t}\mathbf{z}) + \mathbf{t}^2.$$

Substituting $\mathbf{z} = 0$ produces the equation $d_2 + \mathbf{t} + \mathbf{t}^2 = 0$, which has two distinct roots in the algebraic closure of the base field $\mathbb{F}$, corresponding to two distinct points of the blowup. These points are nonsingular since the partial derivative $d_1\mathbf{z}^2 + \mathbf{z} + 1$ does not vanish for $\mathbf{z} = 0$. These blowups are defined over the smallest extension of $\mathbb{F}$ in which $d_2 + \mathbf{t} + \mathbf{t}^2 = 0$ has roots.

An alternate curve shape. The curve

$$d_1(1+\mathbf{x}+\mathbf{y}) + d_2(1+\mathbf{x}^2+\mathbf{y}^2) = \mathbf{x}\mathbf{y} + \mathbf{x}\mathbf{y}(\mathbf{x}+\mathbf{y}) + \mathbf{x}^2\mathbf{y}^2$$

is isomorphic to $\mathrm{E}_{\mathrm{B},d_1,d_2}$ via the map $(\mathbf{x},\mathbf{y}) \mapsto (\mathbf{x},\mathbf{y}+1)$, and is another suitable generalization of Edwards curves to the binary case. Since the addition and doubling formulas look slightly simpler on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ we picked that one but would like to point out here that all considerations also apply to this shifted curve.

Birational equivalence. Traditionally elliptic curves are given in Weierstrass form; see, e.g., [24]. An ordinary elliptic curve over $\mathbb{F}$ can be expressed in short Weierstrass form

$$\mathbf{v}^2 + \mathbf{u}\mathbf{v} = \mathbf{u}^3 + a_2\mathbf{u}^2 + a_6$$

with $a_6 \neq 0$. The neutral element of the addition law is the point at infinity and negation is defined as $-(u_1, v_1) = (u_1, v_1 + u_1)$.

The map $(\mathbf{x},\mathbf{y}) \mapsto (\mathbf{u},\mathbf{v})$ defined by

$$\begin{aligned}\mathbf{u} &= d_1(d_1^2 + d_1 + d_2)(\mathbf{x}+\mathbf{y})/(\mathbf{x}\mathbf{y} + d_1(\mathbf{x}+\mathbf{y})),\\ \mathbf{v} &= d_1(d_1^2 + d_1 + d_2)(\mathbf{x}/(\mathbf{x}\mathbf{y} + d_1(\mathbf{x}+\mathbf{y})) + d_1 + 1)\end{aligned}$$

is a birational equivalence from $\mathrm{E}_{\mathrm{B},d_1,d_2}$ to the elliptic curve

$$\mathbf{v}^2 + \mathbf{u}\mathbf{v} = \mathbf{u}^3 + (d_1^2 + d_2)\mathbf{u}^2 + d_1^4(d_1^4 + d_1^2 + d_2^2)$$

with j-invariant $1/(d_1^4(d_1^4 + d_1^2 + d_2^2))$. An inverse map is given as follows:

$$\begin{aligned}\mathbf{x} &= d_1(\mathbf{u} + d_1^2 + d_1 + d_2)/(\mathbf{u} + \mathbf{v} + (d_1^2 + d_1)(d_1^2 + d_1 + d_2)),\\ \mathbf{y} &= d_1(\mathbf{u} + d_1^2 + d_1 + d_2)/(\mathbf{v} + (d_1^2 + d_1)(d_1^2 + d_1 + d_2)).\end{aligned}$$

We define a function φ on all affine points of E_{B,d_1,d_2} by extending the rational map $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{u}, \mathbf{v})$ given above. Specifically, the rational map is undefined at $(0, 0)$; we define $\varphi(0, 0) = P_\infty$. There are no other exceptional cases: if $xy + d_1(x + y) = 0$ then $d_2(x^2 + y^2) = xy(x + y) + x^2y^2 = d_1(x + y)^2 + d_1^2(x + y)^2$ so $(d_2 + d_1^2 + d_1)(x^2 + y^2) = 0$ so $x^2 + y^2 = 0$ so $x = y$. Use $xy + d_1(x + y) = 0$ again to see that $xy = 0$ so $x^2 = 0$ so $x = 0$ so $(x, y) = (0, 0)$.

8.2 The addition law

This section presents an addition law for the binary Edwards curve E_{B,d_1,d_2} and proves that the addition law corresponds to the usual addition law on an elliptic curve in Weierstrass form. One consequence of the proof is that the addition law on E_{B,d_1,d_2} is strongly unified: it can be used with two identical inputs, i.e., to double.

Here is the addition law. The sum of two points $(x_1, y_1), (x_2, y_2)$ on E_{B,d_1,d_2} is the point (x_3, y_3) defined as follows:

$$x_3 = \frac{d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)},$$
$$y_3 = \frac{d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + (y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1x_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)}.$$

If the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero then the sum (x_3, y_3) is a point on E_{B,d_1,d_2}: i.e.,

$$d_1(x_3 + y_3) + d_2(x_3^2 + y_3^2) = x_3y_3 + x_3y_3(x_3 + y_3) + x_3^2y_3^2.$$

We present a script in the Sage computer-algebra system [95] that verifies this:

```
R.<d1,d2,x1,y1,x2,y2>=GF(2)[]
S=R.quotient([
  d1*(x1+y1)+d2*(x1^2+y1^2)+x1*y1+x1*y1*(x1+y1)+x1^2*y1^2,
  d1*(x2+y2)+d2*(x2^2+y2^2)+x2*y2+x2*y2*(x2+y2)+x2^2*y2^2
])
x3 = (
  d1*(x1+x2)+d2*(x1+y1)*(x2+y2)+(x1+x1^2)*(x2*(y1+y2+1)+y1*y2)
) / (d1+(x1+x1^2)*(x2+y2))
y3 = (
  d1*(y1+y2)+d2*(x1+y1)*(x2+y2)+(y1+y1^2)*(y2*(x1+x2+1)+x1*x2)
) / (d1+(y1+y1^2)*(x2+y2))
verif = d1*(x3+y3)+d2*(x3^2+y3^2)+x3*y3+x3*y3*(x3+y3)+x3^2*y3^2
0 == S(numerator(verif))
```

Inserting $(x_1, y_1) = (0, 0)$ or $(x_2, y_2) = (0, 0)$ into the addition law shows that $(0, 0)$ is the neutral element. Similarly $(x_1, y_1) + (1, 1) = (x_1 + 1, y_1 + 1)$; in particular $(1, 1) + (1, 1) = (0, 0)$. Furthermore $(x_1, y_1) + (y_1, x_1) = (0, 0)$, so $-(x_1, y_1) = (y_1, x_1)$. We emphasize that the addition law works without change for all of these inputs.

The following lemma will be useful in Section 8.6 and later in this section.

Lemma 8.3 *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_3, y_3), (x_2, y_2) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(\mathbb{F})$. Assume that $(x_3, y_3) + (x_2, y_2)$ is defined. Then $(x_3, y_3) + (y_2, x_2)$ is also defined. Furthermore define $(x_5, y_5) = (x_3, y_3) + (x_2, y_2)$ and $(x_1, y_1) = (x_3, y_3) + (y_2, x_2)$. Then $d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3) \neq 0$ and*

$$w_5 = \frac{d_1(d_1(w_2+w_3) + x_2x_3(x_2+x_3+1) + y_2y_3(y_2+y_3+1) + (x_2x_3+y_2y_3)^2)}{d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3)},$$

$$w_1w_5 = \frac{d_1^2(w_2 + w_3)^2}{d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3)},$$

where $w_i = x_i + y_i$.

Proof. The denominators of the coordinates of $(x_3, y_3) + (x_2, y_2)$ are $d_1 + (x_3 + x_3^2)(x_2 + y_2)$ and $d_1 + (y_3 + y_3^2)(x_2 + y_2)$; these formulas are symmetric in x_2, y_2, so they are the same as the denominators of $(x_3, y_3) + (y_2, x_2)$. Furthermore, their product is

$$\begin{aligned}
&(d_1 + (x_3 + x_3^2)(x_2 + y_2))(d_1 + (y_3 + y_3^2)(x_2 + y_2)) \\
&\quad = d_1^2 + d_1(x_3 + x_3^2 + y_3 + y_3^2)(x_2 + y_2) + (x_3 + x_3^2)(y_3 + y_3^2)(x_2 + y_2)^2 \\
&\quad = d_1^2 + d_1(w_3 + w_3^2)w_2 + (d_1w_3 + d_2w_3^2)w_2^2 \\
&\quad = d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3),
\end{aligned}$$

so $d_1^2 + w_2w_3(d_1(1 + w_2 + w_3) + d_2w_2w_3)$ is nonzero. Note that we used the curve equation in the second-to-last equality.

Cross-multiplying and using the curve equation again gives the stated numerator of w_5; we omit the details. Similarly we obtain the numerator of w_1. Multiplying, using the curve equation again, and cancelling $d_1^2+w_2w_3(d_1(1+w_2+w_3)+d_2w_2w_3)$ produces the stated formula for w_1w_5. □

The rest of this section is devoted to the proof that this addition law corresponds to the addition law on the elliptic curve

$$\mathbf{v}^2 + \mathbf{uv} = \mathbf{u}^3 + (d_1^2 + d_2)\mathbf{u}^2 + d_1^4(d_1^4 + d_1^2 + d_2^2)$$

under the function φ defined in the previous section: i.e., that $\varphi(x_3, y_3) = \varphi(x_1, y_1)+ \varphi(x_2, y_2)$.

Lemma 8.4 *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_2, y_2), (x_3, y_3) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(\mathbb{F})$. If $(x_3, y_3) + (x_2, y_2) = (0, 0)$ then $(x_3, y_3) = (y_2, x_2)$.*

Proof. Define w_i as in Lemma 8.3. Then $w_5 = 0$ so

$$d_1^2(w_2 + w_3)^2 = w_1 w_5(d_1^2 + w_2 w_3(d_1(1 + w_2 + w_3) + d_2 w_2 w_3)) = 0$$

so $w_2 + w_3 = 0$; i.e., $x_2 + y_2 + x_3 + y_3 = 0$. Similarly

$$d_1(d_1(w_2 + w_3) + x_2 x_3(x_2 + x_3 + 1) + y_2 y_3(y_2 + y_3 + 1) + (x_2 x_3 + y_2 y_3)^2) = 0$$

so $x_2 x_3(x_2 + x_3 + 1) + y_2 y_3(y_2 + y_3 + 1) + (x_2 x_3 + y_2 y_3)^2 = 0$. Substitute $y_3 = x_2 + y_2 + x_3$ to see that $x_2 x_3(x_2 + x_3 + 1) + y_2(x_2 + y_2 + x_3)(y_2 + (x_2 + y_2 + x_3) + 1) + (x_2 x_3 + y_2(x_2 + y_2 + x_3))^2 = 0$, and simplify to see that $(x_2 + y_2)(x_2 + y_2 + 1)(x_3 + y_2)(x_3 + y_2 + 1) = 0$. We now separately consider the four factors.

Case 1: $x_2 + y_2 = 0$. Then (x_2, y_2) is either $(0, 0)$ or $(1, 1)$. Furthermore $x_3 + y_3 = 0$ so (x_3, y_3) is either $(0, 0)$ or $(1, 1)$. We must have $(x_3, y_3) = (x_2, y_2)$ since $(0, 0) + (1, 1) \neq (0, 0)$. Thus also $(x_3, y_3) = (y_2, x_2)$.

Case 2: $x_2 + y_2 = 1$. Then $x_2^4 + x_2^2 = d_1 + d_2$ from the curve equation. Furthermore $x_3 + y_3 = 1$ so $x_3^4 + x_3^2 = d_1 + d_2$ so $x_3 = x_2$ or $x_3 = x_2 + 1$. If $x_3 = x_2$ then $(x_3, y_3) + (x_2, y_2) = (1, 1) \neq (0, 0)$. Thus $x_3 = x_2 + 1$ so $(x_3, y_3) = (x_2 + 1, x_2) = (y_2, x_2)$.

Case 3: $x_3 + y_2 = 0$. Then $x_2 + y_3 = 0$. Hence $(x_3, y_3) = (y_2, x_2)$.

Case 4: $x_3 + y_2 = 1$. Then $x_2 + y_3 = 1$. Hence $(x_3, y_3) + (x_2, y_2) = (y_2 + 1, x_2 + 1) + (x_2, y_2) = (1, 1)$, contradiction. □

Lemma 8.5 *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_1, y_1), (x_2, y_2) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(\mathbb{F})$. If $\varphi(x_1, y_1) = \varphi(x_2, y_2)$ then $(x_1, y_1) = (x_2, y_2)$.*

Proof. If $(x_1, y_1) = (0, 0)$ then $\varphi(x_1, y_1) = P_\infty$ so $\varphi(x_2, y_2) = P_\infty$ so $(x_2, y_2) = (0, 0) = (x_1, y_1)$ as claimed. Similar comments apply if $(x_2, y_2) = (0, 0)$. Assume from now on that $(x_1, y_1) \neq (0, 0)$ and $(x_2, y_2) \neq (0, 0)$.

By definition of φ we have

$$y_1(x_2 y_2 + d_1(x_2 + y_2)) = y_2(x_1 y_1 + d_1(x_1 + y_1)),$$
$$x_1(x_2 y_2 + d_1(x_2 + y_2)) = x_2(x_1 y_1 + d_1(x_1 + y_1)).$$

Note for future reference that this system of equations is symmetric between 1 and 2, and between x and y. Multiply the first equation by x_1 and the second

by y_1 and add to obtain $(x_1y_2 + x_2y_1)(x_1y_1 + d_1(x_1 + y_1)) = 0$. Recall that $x_1y_1 + d_1(x_1 + y_1) \neq 0$ so $x_1y_2 + x_2y_1 = 0$. Now replace x_1y_2 with x_2y_1 in the second equation and simplify to obtain $x_2(x_1 + x_2)y_1 = 0$.

If $y_1 = 0$ then $x_1 \neq 0$. The curve equation now says $d_1x_1 + d_2x_1^2 = 0$ so $x_1 = d_1/d_2$. Furthermore $y_2 = x_2y_1/x_1 = 0$ so also $x_2 = d_1/d_2$ so $(x_1, y_1) = (x_2, y_2)$.

Assume from now on that $y_1 \neq 0$. Apply symmetry between 1 and 2, and between x and y, to obtain also $x_2 \neq 0$. Then $x_1 + x_2 = 0$. Apply symmetry between x and y to see that $y_1 + y_2 = 0$. Thus $(x_1, y_1) = (x_2, y_2)$. □

Lemma 8.6 *Let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_1, y_1) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(\mathbb{F})$. Then $\varphi(y_1, x_1) = -\varphi(x_1, y_1)$.*

Proof. If $(x_1, y_1) = (0, 0)$ then $\varphi(y_1, x_1) = P_\infty = \varphi(x_1, y_1)$. Assume from now on that $(x_1, y_1) \neq (0, 0)$. Write $(u_1, v_1) = \varphi(x_1, y_1)$ and $(u_2, v_2) = \varphi(y_1, x_1)$. Then $u_1 = u_2$ and $v_1 + v_2 = u_1$ from the definition of φ. Hence $(u_2, v_2) = (u_1, v_1 + u_1) = -(u_1, v_1)$. □

Theorem 8.7 *Let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. Fix $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(\mathbb{F})$. Assume that $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$. Then $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_3, y_3)$.*

Proof. Write $a_2 = d_1^2 + d_2$ and $a_6 = d_1^4(d_1^4 + d_1^2 + d_2^2)$. There are two cases in the definition of φ and several cases in the definition of addition on the Weierstrass curve $v^2 + uv = u^3 + a_2u^2 + a_6$; the proof splits into several cases correspondingly.

If $(x_1, y_1) = (0, 0)$ then $(x_2, y_2) = (x_3, y_3)$. Now $\varphi(x_2, y_2) = \varphi(x_3, y_3)$ and $\varphi(x_1, y_1) = P_\infty$, so $\varphi(x_1, y_1) + \varphi(x_2, y_2) = P_\infty + \varphi(x_2, y_2) = \varphi(x_2, y_2) = \varphi(x_3, y_3)$. Similar comments apply if $(x_2, y_2) = (0, 0)$.

If $(x_3, y_3) = (0, 0)$ then $(x_2, y_2) = (y_1, x_1)$ by Lemma 8.4. Now $\varphi(x_3, y_3) = \varphi(0, 0) = P_\infty$ and $\varphi(x_2, y_2) = \varphi(y_1, x_1) = -\varphi(x_1, y_1)$ by Lemma 8.6. Thus $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_1, y_1) - \varphi(x_1, y_1) = P_\infty = \varphi(x_3, y_3)$.

Assume from now on that $(x_1, y_1) \neq (0, 0)$, $(x_2, y_2) \neq (0, 0)$, and $(x_3, y_3) \neq (0, 0)$. Write $(u_i, v_i) = \varphi(x_i, y_i)$.

Case 1: $(u_1, v_1) = (u_2, v_2)$. Then $(x_1, y_1) = (x_2, y_2)$ by Lemma 8.5. If $u_1 = 0$ then $x_1 = y_1$ from the definition of φ so either $(x_1, y_1) = (0, 0)$ or $(x_1, y_1) = (1, 1)$; in either case $(x_1, y_1) + (x_2, y_2) = (x_1, y_1) + (x_1, y_1) = (0, 0)$, already handled above. Assume from now on that $u_1 \neq 0$. The usual doubling formulas for Weierstrass coordinates say that $2(u_1, v_1) = (u_4, v_4)$ where $u_4 = \lambda^2 + \lambda + d_1^2 + d_2$, $v_4 = v_1 + \lambda(u_1 + u_4) + u_4$, and $\lambda = (u_1^2 + v_1)/u_1$. A lengthy but straightforward

calculation then shows that $(u_3, v_3) = (u_4, v_4)$; here is the corresponding Sage script:

```
R.<d1,d2,x1,y1>=GF(2)[]
S=R.quotient([
  d1*(x1+y1)+d2*(x1^2+y1^2)+x1*y1+x1*y1*(x1+y1)+x1^2*y1^2
])
x2 = x1
y2 = y1
x3 = (
  d1*(x1+x2)+d2*(x1+y1)*(x2+y2)+(x1+x1^2)*(x2*(y1+y2+1)+y1*y2)
) / (d1+(x1+x1^2)*(x2+y2))
y3 = (
  d1*(y1+y2)+d2*(x1+y1)*(x2+y2)+(y1+y1^2)*(y2*(x1+x2+1)+x1*x2)
) / (d1+(y1+y1^2)*(x2+y2))
u1 = d1*(d1^2+d1+d2)*(x1+y1)/(x1*y1+d1*(x1+y1))
v1 = d1*(d1^2+d1+d2)*(x1/(x1*y1+d1*(x1+y1))+d1+1)
u3 = d1*(d1^2+d1+d2)*(x3+y3)/(x3*y3+d1*(x3+y3))
v3 = d1*(d1^2+d1+d2)*(x3/(x3*y3+d1*(x3+y3))+d1+1)
lam = (u1^2+v1)/u1
u4 = lam^2+lam+d1^2+d2
v4 = v1+lam*(u1+u4)+u4
0 == S(numerator(u3-u4))
0 == S(numerator(v3-v4))
```

Hence $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_3, y_3)$.

Case 2: $(u_1, v_1) \neq (u_2, v_2)$. If $u_1 = u_2$ then $(u_1, v_1) = -(u_2, v_2)$ so $\varphi(x_1, y_1) = -\varphi(x_2, y_2) = \varphi(y_2, x_2)$ by Lemma 8.6 so $(x_1, y_1) = (y_2, x_2)$ by Lemma 8.5 so $(x_1, y_1) + (x_2, y_2) = (0, 0)$, already handled above. Assume from now on that $u_1 \neq u_2$. The usual addition formulas for Weierstrass coordinates say that $(u_1, v_1) + (u_2, v_2) = (u_4, v_4)$ where $u_4 = \lambda^2 + \lambda + u_1 + u_2 + d_1^2 + d_2$, $v_4 = v_1 + \lambda(u_1 + u_4) + u_4$, and $\lambda = (v_1 + v_2)/(u_1 + u_2)$. Another lengthy but straightforward calculation then shows that $(u_3, v_3) = (u_4, v_4)$; here is the corresponding Sage script:

```
R.<d1,d2,x1,y1,x2,y2>=GF(2)[]
S=R.quotient([
  d1*(x1+y1)+d2*(x1^2+y1^2)+x1*y1+x1*y1*(x1+y1)+x1^2*y1^2,
  d1*(x2+y2)+d2*(x2^2+y2^2)+x2*y2+x2*y2*(x2+y2)+x2^2*y2^2
])
x3 = (
  d1*(x1+x2)+d2*(x1+y1)*(x2+y2)+(x1+x1^2)*(x2*(y1+y2+1)+y1*y2)
) / (d1+(x1+x1^2)*(x2+y2))
y3 = (
  d1*(y1+y2)+d2*(x1+y1)*(x2+y2)+(y1+y1^2)*(y2*(x1+x2+1)+x1*x2)
```

```
) / (d1+(y1+y1^2)*(x2+y2))
u1 = d1*(d1^2+d1+d2)*(x1+y1)/(x1*y1+d1*(x1+y1))
v1 = d1*(d1^2+d1+d2)*(x1/(x1*y1+d1*(x1+y1))+d1+1)
u2 = d1*(d1^2+d1+d2)*(x2+y2)/(x2*y2+d1*(x2+y2))
v2 = d1*(d1^2+d1+d2)*(x2/(x2*y2+d1*(x2+y2))+d1+1)
u3 = d1*(d1^2+d1+d2)*(x3+y3)/(x3*y3+d1*(x3+y3))
v3 = d1*(d1^2+d1+d2)*(x3/(x3*y3+d1*(x3+y3))+d1+1)
lam = (v2+v1)/(u2+u1)
u4 = lam^2+lam+u1+u2+d1^2+d2
v4 = v1+lam*(u1+u4)+u4
0 == S(numerator(u3-u4))
0 == S(numerator(v3-v4))
```

Hence $\varphi(x_1, y_1) + \varphi(x_2, y_2) = \varphi(x_3, y_3)$. □

8.3 Complete binary Edwards curves

If d_2 does not have the form $t^2 + t$, with $t \in \mathbb{F}$, then the addition law on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ has the very nice feature of *completeness*. This means that there are *no* exceptions to the addition law: the denominators $d_1+(x_1+x_1^2)(x_2+y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ never vanish. The addition law *always* produces a point on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ corresponding to the usual sum of points on elliptic curves in Weierstrass form.

In this section we prove completeness for these d_2's. We also prove that over finite fields $\mathbb{F}_{2^n}$ with $n \geq 3$ all ordinary curves are birationally equivalent to complete binary Edwards curves.

Theorem 8.8 (Completeness of the addition law) *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$. Assume that no element $t \in \mathbb{F}$ satisfies $t^2 + t + d_2 = 0$. Then the addition law on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}(\mathbb{F})$ is complete.*

Proof. We show for all $(x_1, y_1), (x_2, y_2) \in \mathrm{E}_{\mathrm{B},d_1,d_2}(\mathbb{F})$ that the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero.

If $x_2 + y_2 = 0$ then the denominators are d_1, which is nonzero by hypothesis. Assume from now on that $x_2 + y_2 \neq 0$, and suppose that $d_1/(x_2 + y_2) = x_1 + x_1^2$.

Use the curve equation to see that

$$\begin{aligned}\frac{d_1}{x_2+y_2} &= \frac{d_1(x_2+y_2)}{x_2^2+y_2^2} = \frac{d_2(x_2^2+y_2^2)+x_2y_2+x_2y_2(x_2+y_2)+x_2^2y_2^2}{x_2^2+y_2^2} \\ &= d_2 + \frac{x_2y_2+x_2y_2(x_2+y_2)+y_2^2}{x_2^2+y_2^2} + \frac{y_2^2+x_2^2y_2^2}{x_2^2+y_2^2} \\ &= d_2 + \frac{y_2+x_2y_2}{x_2+y_2} + \frac{y_2^2+x_2^2y_2^2}{x_2^2+y_2^2}\end{aligned}$$

and hence that $t^2+t+d_2=0$ where $t = x_1 + (y_2+x_2y_2)/(x_2+y_2) \in \mathbb{F}$. Contradiction. Hence $d_1+(x_1+x_1^2)(x_2+y_2) \neq 0$. Similarly $d_1+(y_1+y_1^2)(x_2+y_2) \neq 0$. □

Definition 8.9 (Complete binary Edwards curve) *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$. Assume that no element $t \in \mathbb{F}$ satisfies $t^2+t+d_2 = 0$. The* complete binary Edwards curve with coefficients d_1 and d_2 *is the affine curve*

$$\mathrm{E}_{\mathrm{B},d_1,d_2} : d_1(\mathbf{x}+\mathbf{y}) + d_2(\mathbf{x}^2+\mathbf{y}^2) = \mathbf{xy} + \mathbf{xy}(\mathbf{x}+\mathbf{y}) + \mathbf{x}^2\mathbf{y}^2.$$

There is no conflict in notation or terminology here: the complete binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ is the same as the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$. The complete case has the extra requirement that $t^2+t+d_2 \neq 0$ for *all* $t \in \mathbb{F}$, not just for $t = d_1$. If $\mathbb{F}$ is a finite field $\mathbb{F}_{2^n}$ then an equivalent requirement is that $\mathrm{Tr}(d_2) = 1$, where Tr is the absolute trace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Generality of $\mathbf{E_{B,d_1,d_2}}$. We now study which isomorphism classes of elliptic curves over a finite field $\mathbb{F}_{2^n}$ are birationally equivalent to complete binary Edwards curves $\mathrm{E}_{\mathrm{B},d_1,d_2}$.

Theorem 8.10 *Let n be an integer with $n \geq 3$. Each ordinary elliptic curve over $\mathbb{F}_{2^n}$ is birationally equivalent over $\mathbb{F}_{2^n}$ to a complete binary Edwards curve.*

Proof. Each ordinary elliptic curve over $\mathbb{F}_{2^n}$ is isomorphic to $\mathbf{v}^2+\mathbf{uv} = \mathbf{u}^3 + a_2\mathbf{u}^2 + a_6$ for some $a_2 \in \mathbb{F}_{2^n}$ and $a_6 \in \mathbb{F}_{2^n}^*$. Note that if $\mathrm{Tr}(a_2) = \mathrm{Tr}(a_2')$ then the two curves $\mathbf{v}^2+\mathbf{uv} = \mathbf{u}^3+a_2\mathbf{u}^2+a_6$ and $\mathbf{v}^2+\mathbf{uv} = \mathbf{u}^3+a_2'\mathbf{u}^2+a_6$ are isomorphic: there exists b such that $a_2' = a_2+b+b^2$, and the map $\mathbf{v} \mapsto \mathbf{v}+b\mathbf{u}$ is an isomorphism from $\mathbf{v}^2+\mathbf{uv} = \mathbf{u}^3+a_2\mathbf{u}^2+a_6$ to $\mathbf{v}^2+\mathbf{uv} = \mathbf{u}^3+(a_2+b+b^2)\mathbf{u}^2+a_6$.

Fix a_2, a_6 for the rest of the proof. For each $\delta, \epsilon \in \mathbb{F}_2$ define

$$D_{\delta,\epsilon} = \left\{d_1 \in \mathbb{F}_{2^n}^* : \mathrm{Tr}(d_1) = \delta,\ \mathrm{Tr}(\sqrt{a_6}/d_1^2) = \epsilon\right\}.$$

If $d_1 \in D_{\mathrm{Tr}(a_2)+1,1}$ then the pair (d_1, d_2) with $d_2 = d_1^2+d_1+\sqrt{a_6}/d_1^2$ has $\mathrm{Tr}(d_2) = \mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$ and therefore defines a complete binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$.

This curve is birationally equivalent to $\mathbf{v}^2 + \mathbf{uv} = \mathbf{u}^3 + (d_1^2 + d_2)\mathbf{u}^2 + a_6$, since $d_1^4(d_1^4 + d_1^2 + d_2^2) = a_6$, and therefore birationally equivalent to $\mathbf{v}^2 + \mathbf{uv} = \mathbf{u}^3 + a_2\mathbf{u}^2 + a_6$, since $\mathrm{Tr}(d_1^2 + d_2) = \mathrm{Tr}(d_1) + \mathrm{Tr}(d_2) = \mathrm{Tr}(a_2)$.

Our goal is to show that $D_{\mathrm{Tr}(a_2)+1,1}$ is nonempty. We will do this by counting the number of elements in both D_{01} and D_{11}.

Observe first that $\#D_{00} + \#D_{01} = 2^{n-1} - 1$. Indeed, $\#D_{00} + \#D_{01}$ is the number of $d_1 \in \mathbb{F}_{2^n}^*$ with $\mathrm{Tr}(d_1) = 0$.

Observe next that $\#D_{01} + \#D_{11} = 2^{n-1}$. Indeed, $\#D_{01} + \#D_{11}$ is the number of $d_1 \in \mathbb{F}_{2^n}^*$ with $\mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$. As d_1 runs through $\mathbb{F}_{2^n}^*$, the quotient $\sqrt{a_6}/d_1^2$ also runs through $\mathbb{F}_{2^n}^*$, so it has trace 1 exactly 2^{n-1} times.

The heart of the proof is a bound on $\#D_{00} + \#D_{11}$, the number of $d_1 \in \mathbb{F}_{2^n}^*$ with $\mathrm{Tr}(d_1 + \sqrt{a_6}/d_1^2) = 0$. For each such d_1 there are exactly two choices of $s \in \mathbb{F}_{2^n}$ such that $s^2 + s = d_1 + \sqrt{a_6}/d_1^2$, producing two choices of point $(U_1, V_1) = (d_1, d_1 s)$ on the elliptic curve $V^2 + UV = U^3 + \sqrt{a_6}$. All points on this elliptic curve appear uniquely in this way, except that the point at infinity and the point $(0, 0)$ do not appear. By the Hasse-Weil Theorem, this curve has $2^n + 1 + t$ points for some integer t in the interval $[-2\sqrt{2^n}, 2\sqrt{2^n}]$. Therefore $\#D_{00} + \#D_{11} = 2^{n-1} + (t-1)/2$.

Now $2\#D_{01} = (\#D_{00} + \#D_{01}) + (\#D_{01} + \#D_{11}) - (\#D_{00} + \#D_{11}) = 2^{n-1} - 1 + 2^{n-1} - 2^{n-1} - (t-1)/2 = 2^{n-1} - (t+1)/2$ and $2\#D_{11} = 2^n - 2\#D_{01} = 2^{n-1} + (t+1)/2$. The crude bound $(\sqrt{2^n} - 1)^2 \geq (\sqrt{8} - 1)^2 > 2$ implies $2^n > 2\sqrt{2^n} + 1 \geq |t| + 1$, so both D_{01} and D_{11} are nonempty. □

Given a_2, a_6 defining a Weierstrass curve, one can choose a random d_1 with $\mathrm{Tr}(d_1) = \mathrm{Tr}(a_2) + 1$, check whether $\mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$, and if so compute $d_2 = d_1^2 + d_1 + \sqrt{a_6}/d_1^2$, obtaining a complete binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$ birationally equivalent to the original curve. The theorem says that this procedure succeeds for *at least one* d_1, but the proof actually shows more: the procedure succeeds for approximately 50% of all d_1 with $\mathrm{Tr}(d_1) = \mathrm{Tr}(a_2) + 1$. Computer experiments show that it suffices to search a few *small* field elements d_1, where "small" means "allowing very fast multiplications."

8.4 Explicit addition formulas

This section presents explicit formulas for affine addition, projective addition, and mixed addition on binary Edwards curves. The formulas are not as fast as known formulas for Weierstrass curves but have the advantage of being strongly unified and, for suitable d_2, the advantage of completeness. We are continuing to investigate addition speed; we have already found several speedups and incorporated those speedups into the formulas here.

See Section 8.5 for much faster doubling formulas, and Section 8.6 for much faster differential-addition formulas. All formulas of this chapter have been incorporated to the Explicit-Formulas Database [8].

Affine addition. The following formulas, given (x_1, y_1) and (x_2, y_2) on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, compute the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ if it is defined:

$$w_1 = x_1 + y_1,\ w_2 = x_2 + y_2,\ A = x_1^2 + x_1,\ B = y_1^2 + y_1,\ C = d_2 w_1 \cdot w_2,$$
$$D = x_2 \cdot y_2,\ x_3 = y_1 + (C + d_1(w_1 + x_2) + A \cdot (D + x_2))/(d_1 + A \cdot w_2),$$
$$y_3 = x_1 + (C + d_1(w_1 + y_2) + B \cdot (D + y_2))/(d_1 + B \cdot w_2).$$

These formulas use $2\mathbf{I}+8\mathbf{M}+2\mathbf{S}+3\mathbf{D}$, where $\mathbf{I}$ is the cost of a field inversion, $\mathbf{M}$ is the cost of a field multiplication, $\mathbf{S}$ is the cost of a field squaring, and $\mathbf{D}$ is the cost of a multiplication by a curve parameter. The $3\mathbf{D}$ here are two multiplications by d_1 and one multiplication by d_2. One can replace $2\mathbf{I}$ with $1\mathbf{I} + 3\mathbf{M}$ using Montgomery's inversion trick.

For complete binary Edwards curves the denominators $d_1 + A \cdot w_2 = d_1 + (x_1^2 + x_1)(x_2 + y_2)$ and $d_1 + B \cdot w_2 = d_1 + (y_1^2 + y_1)(x_2 + y_2)$ cannot be zero. See Theorem 8.8.

Mixed addition. The following formulas, given $(X_1 : Y_1 : Z_1)$ and (x_2, y_2) on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, compute the sum $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (x_2, y_2)$ if it is defined:

$$W_1 = X_1 + Y_1,\ w_2 = x_2 + y_2,\ A = x_2^2 + x_2,\ B = y_2^2 + y_2,$$
$$D = W_1 \cdot Z_1,\ E = d_1 Z_1^2,\ H = (E + d_2 D) \cdot w_2,$$
$$I = d_1 Z_1,\ U = E + A \cdot D,\ V = E + B \cdot D,\ Z_3 = U \cdot V,$$
$$X_3 = Z_3 \cdot y_2 + (H + X_1 \cdot (I + A \cdot (Y_1 + Z_1))) \cdot V,$$
$$Y_3 = Z_3 \cdot x_2 + (H + Y_1 \cdot (I + B \cdot (X_1 + Z_1))) \cdot U.$$

These formulas use $13\mathbf{M} + 3\mathbf{S} + 3\mathbf{D}$. As above the $3\mathbf{D}$ are two multiplications by d_1 and one multiplication by d_2. For complete binary Edwards curves the product $Z_3 = Z_1^4(d_1 + (x_2^2 + x_2)(x_1 + y_1))(d_1 + (y_2^2 + y_2)(x_1 + y_1))$ cannot be zero.

Projective addition. The following formulas, given $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, compute the sum $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ if it is defined:

$$W_1 = X_1 + Y_1,\ W_2 = X_2 + Y_2,\ A = X_1 \cdot (X_1 + Z_1),\ B = Y_1 \cdot (Y_1 + Z_1),$$
$$C = Z_1 \cdot Z_2,\ D = W_2 \cdot Z_2,\ E = d_1 C^2,\ H = (d_1 Z_2 + d_2 W_2) \cdot W_1 \cdot C,$$
$$I = d_1 C \cdot Z_1,\ U = E + A \cdot D,\ V = E + B \cdot D,\ S = U \cdot V,$$
$$X_3 = S \cdot Y_1 + (H + X_2 \cdot (I + A \cdot (Y_2 + Z_2))) \cdot V \cdot Z_1,$$
$$Y_3 = S \cdot X_1 + (H + Y_2 \cdot (I + B \cdot (X_2 + Z_2))) \cdot U \cdot Z_1,\ Z_3 = S \cdot Z_1.$$

These formulas use $21\mathbf{M} + 1\mathbf{S} + 4\mathbf{D}$. The $4\mathbf{D}$ are three multiplications by d_1 and one multiplication by d_2. For complete binary Edwards curves the product $Z_3 = Z_1^5 Z_2^4 (d_1 + (x_2^2 + x_2)(x_1 + y_1))(d_1 + (y_2^2 + y_2)(x_1 + y_1))$ cannot be zero.

The following formulas are considerably better than the previous formulas when d_1 and d_2 are small:

$$\begin{aligned}
A &= X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2,\ D = d_1 C,\ E = C^2,\ F = d_1^2 E,\\
G &= (X_1 + Z_1) \cdot (X_2 + Z_2),\ H = (Y_1 + Z_1) \cdot (Y_2 + Z_2),\\
I &= A + G,\ J = B + H,\ K = (X_1 + Y_1) \cdot (X_2 + Y_2),\\
U &= C \cdot (F + d_1 K \cdot (K + I + J + C)),\\
V &= U + D \cdot F + K \cdot (d_2(d_1 E + G \cdot H + A \cdot B) + (d_2 + d_1) I \cdot J),\\
X_3 &= V + D \cdot (A + D) \cdot (G + D),\ Y_3 = V + D \cdot (B + D) \cdot (H + D),\\
Z_3 &= U + (d_2 + d_1) C \cdot K^2.
\end{aligned}$$

These formulas use $18\mathbf{M} + 2\mathbf{S} + 7\mathbf{D}$. The $7\mathbf{D}$ are three multiplications by d_1, two multiplications by $d_2 + d_1$, one multiplication by d_1^2, and one multiplication by d_2. One can alternatively compute F as D^2, replacing $1\mathbf{D}$ with $1\mathbf{S}$. For complete binary Edwards curves the denominator Z_3 cannot be zero.

These formulas become simpler in the case $d_1 = d_2$:

$$\begin{aligned}
A &= X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2,\ D = d_1 C,\ E = C^2,\ F = d_1^2 E,\\
G &= (X_1 + Z_1) \cdot (X_2 + Z_2),\ H = (Y_1 + Z_1) \cdot (Y_2 + Z_2),\\
I &= A + G,\ J = B + H,\ K = (X_1 + Y_1) \cdot (X_2 + Y_2),\ L = d_1 K,\\
U &= C \cdot (F + L \cdot (K + I + J + C)),\\
V &= U + D \cdot F + L \cdot (d_1 E + G \cdot H + A \cdot B),\\
X_3 &= V + D \cdot (A + D) \cdot (G + D),\ Y_3 = V + D \cdot (B + D) \cdot (H + D),\\
Z_3 &= U.
\end{aligned}$$

These formulas use $16\mathbf{M} + 1\mathbf{S} + 4\mathbf{D}$. The $4\mathbf{D}$ are three multiplications by d_1 and one multiplication by d_1^2. As above one can replace $1\mathbf{D}$ with $1\mathbf{S}$. For complete binary Edwards curves the denominator Z_3 cannot be zero.

8.5 Doubling

This section presents extremely fast doubling formulas on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$, first in affine coordinates and then in inversion-free projective coordinates. The formulas are complete if the curve is complete.

Since the addition formulas on the curve are strongly unified, they can be used to double. This is an interesting option when doublings occur "by accident" or

when side-channel uniformity is an issue. This section shows the relation of the doubling formulas to the general addition formulas.

This section also reviews the literature on doubling formulas for binary elliptic curves, presents two improvements to the best previous formulas for Weierstrass form, and compares the doubling speeds of binary Edwards curves and Weierstrass curves.

Affine doubling. Let (x_1, y_1) be a point on $\mathrm{E}_{\mathrm{B},d_1,d_2}$, and assume that the sum $(x_1, y_1) + (x_1, y_1)$ is defined. Computing $(x_3, y_3) = (x_1, y_1) + (x_1, y_1)$ we obtain

$$\begin{aligned} x_3 &= \frac{d_2(x_1+y_1)^2 + (x_1+x_1^2)(x_1+y_1^2)}{d_1 + (x_1+y_1)(x_1+x_1^2)} \\ &= \frac{d_1(x_1+y_1) + x_1y_1 + x_1^2(1+x_1+y_1)}{d_1 + x_1y_1 + x_1^2(1+x_1+y_1)} \\ &= 1 + \frac{d_1(1+x_1+y_1)}{d_1 + x_1y_1 + x_1^2(1+x_1+y_1)}, \end{aligned}$$

where the second line uses that $d_2(x_1+y_1)^2+x_1^2y_1^2+x_1y_1^2 = d_1(x_1+y_1)+x_1y_1+x_1^2y_1$ for all points on $\mathrm{E}_{\mathrm{B},d_1,d_2}$. Likewise we have

$$y_3 = 1 + \frac{d_1(1+x_1+y_1)}{d_1 + x_1y_1 + y_1^2(1+x_1+y_1)}.$$

To compute the affine formulas with one inversion we note that the product of the denominators of x_3 and y_3 is

$$\begin{aligned} &(d_1 + x_1y_1 + x_1^2(1+x_1+y_1))(d_1 + x_1y_1 + y_1^2(1+x_1+y_1)) \\ &= d_1^2 + (x_1^2+y_1^2)(d_1(1+x_1+y_1) + x_1y_1(1+x_1+y_1) + x_1^2y_1^2) \\ &= d_1^2 + (x_1^2+y_1^2)(d_1 + d_2(x_1^2+y_1^2)) = d_1(d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4+y_1^4)), \end{aligned}$$

where we used the curve equation again. This leads to the doubling formulas

$$\begin{aligned} x_3 &= 1 + \frac{d_1 + d_2(x_1^2+y_1^2) + y_1^2 + y_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4+y_1^4)}, \\ y_3 &= 1 + \frac{d_1 + d_2(x_1^2+y_1^2) + x_1^2 + x_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4+y_1^4)} \end{aligned}$$

needing $1\mathbf{I} + 2\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$. The $2\mathbf{D}$ are one multiplication by d_2 and one multiplication by d_2/d_1. For complete binary Edwards curves all denominators here are nonzero.

If $d_1 = d_2$ some multiplications can be grouped as follows:

$$\begin{aligned} A &= x_1^2,\ B = A^2,\ C = y_1^2,\ D = C^2,\ E = A + C, \\ F &= 1/(d_1 + E + B + D),\ x_3 = (d_1E + A + B)\cdot F,\ y_3 = x_3 + 1 + d_1F. \end{aligned}$$

These formulas use only $1\mathbf{I} + 1\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$. The $2\mathbf{D}$ are two multiplications by d_1.

Projective doubling. Here are explicit formulas to compute $2(X_1 : Y_1 : Z_1) = (X_3 : Y_3 : Z_3)$ if it is defined:

$$\begin{aligned} A &= X_1^2,\ B = A^2,\ C = Y_1^2,\ D = C^2,\ E = Z_1^2,\ F = d_1E^2, \\ G &= (d_2/d_1)(B + D),\ H = A \cdot E,\ I = C \cdot E,\ J = H + I,\ K = G + d_2J, \\ Z_3 &= F + J + G,\ X_3 = K + H + D,\ Y_3 = K + I + B. \end{aligned}$$

These formulas use $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$. The $3\mathbf{D}$ are multiplications by d_1, d_2/d_1, and d_2. For complete binary Edwards curves the denominator Z_3 is nonzero.

Comparison with previous work. All of the doubling formulas for binary elliptic curves presented in the literature have exceptional cases, such as doubling a point of order 2. Our doubling formulas for complete Edwards curves are the first complete doubling formulas in the literature. The following comparison shows that our doubling formulas also provide quite attractive speeds.

The fastest inversion-free doubling formulas mentioned in [24, Table 13.4] are in López-Dahab coordinates and take $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$; these formulas were introduced by Lange in [70]. The $1\mathbf{D}$ is a multiplication by a_2 and is eliminated by typical curve choices. Formulas in [24, page 294], introduced by López and Dahab in [77], take $3\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ when $a_2 \in \{0, 1\}$; here the $1\mathbf{D}$ is a multiplication by the curve parameter $\sqrt{a_6}$.

For random curves, experiments show that we can always choose d_1 to be small, so our new $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ becomes at worst $4\mathbf{M} + 6\mathbf{S}$, slightly slower than $4\mathbf{M} + 4\mathbf{S}$. By choosing curves where d_1 and d_2/d_1 are both small we achieve $2\mathbf{M} + 6\mathbf{S}$, which is significantly faster than $3\mathbf{M} + 5\mathbf{S}$ and $4\mathbf{M} + 4\mathbf{S}$.

In [63] Kim and Kim present doubling formulas for curves of the form $v^2 + uv = u^3 + u^2 + a_6$ needing $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$, where the $2\mathbf{D}$ are both by a_6. Our $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$ formulas are slightly slower but have the advantages of extra generality and completeness.

Our improvements of previous work. We present here two improvements to doubling formulas in López-Dahab coordinates for binary curves in Weierstrass form. Of course, this makes the speed competition more challenging for Edwards curves!

The first improvement is an easy speedup of the Kim–Kim formulas. Kim and Kim represent an affine point (u_1, v_1) as $(U_1 : V_1 : W_1 : T_1)$, where $u_1 = U_1/W_1$, $v_1 = V_1/W_1^2$, and $T_1 = W_1^2$. Our improved formulas compute $2(U_1 : V_1 : W_1 : T_1) = (U_3 : V_3 : W_3 : T_3)$ as

$$\begin{aligned} A &= U_1^2,\ B = V_1^2,\ W_3 = T_1 \cdot A,\ T_3 = W_3^2, \\ U_3 &= (A + \sqrt{a_6}\, T_1)^2,\ V_3 = B \cdot (B + U_3 + W_3) + a_6T_3 + T_3. \end{aligned}$$

These improved formulas use only $2\mathbf{M}+4\mathbf{S}+2\mathbf{D}$, where the $2\mathbf{D}$ are one multiplication by a_6 and one multiplication by $\sqrt{a_6}$.

The second improvement achieves $2\mathbf{M}+5\mathbf{S}+2\mathbf{D}$ for curves of the shape $v^2+uv = u^3+a_6$. We represent a point by $(U_1 : V_1 : W_1 : T_1 : S_1)$, where additionally $S_1 = U_1W_1$. The idea used by Kim and Kim does not carry over to these curves but we have developed the following formulas to compute

$$2(U_1 : V_1 : W_1 : T_1 : S_1) = (U_3 : V_3 : W_3 : T_3 : S_3) :$$

$$\begin{aligned} A &= U_1^2,\ B = V_1^2,\ W_3 = S_1^2,\ U_3 = (A+\sqrt{a_6}\,T_1)^2, \\ T_3 &= W_3^2,\ S_3 = U_3 \cdot W_3,\ V_3 = B \cdot (B+U_3+W_3) + a_6T_3 + S_3. \end{aligned}$$

We caution the reader that these formulas are not complete.

8.6 Differential addition

This section presents fast explicit formulas for w-coordinate differential addition on binary Edwards curves. Here $w = x + y$. Note that $w(-P) = w(P)$, since $-(x, y) = (y, x)$.

"Differential addition" means computing $Q + P$ given $Q, P, Q - P$: e.g., computing $(2m + 1)P$ given $(m + 1)P, mP, P$, or computing $2mP$ given $mP, mP, 0P$. In particular, "w-coordinate differential addition" means computing $w(Q + P)$ given $w(Q), w(P), w(Q - P)$. This section also discusses "w-coordinate differential addition and doubling": computing both $w(2P)$ and $w(Q + P)$, again given $w(Q), w(P), w(Q - P)$.

More concretely, write $(x_1, y_1) = Q - P$, $(x_2, y_2) = P$, $(x_3, y_3) = Q$, $(x_4, y_4) = 2P$, and $(x_5, y_5) = Q + P$. This section presents fast explicit formulas to compute $x_5 + y_5$ given $x_1 + y_1$, $x_2 + y_2$, and $x_3 + y_3$. This section also presents fast explicit formulas to compute $x_4 + y_4$ and $x_5 + y_5$ given $x_1 + y_1$, $x_2 + y_2$, and $x_3 + y_3$. As in previous sections, the formulas are complete if the curve is complete.

We analyze the costs of our formulas in several situations. The simplest situation is that inputs $x_1+y_1, x_2+y_2, x_3+y_3$ and outputs x_4+y_4, x_5+y_5 are represented in affine form, i.e., as field elements. If inversions are expensive—as they usually are—and storage is available then it is better for each input and output to be represented in projective form, i.e., as a ratio of two field elements. Some applications use mixed differential additions, where $x_1 + y_1$ is given in affine form while everything

else is projective. We achieve the following speeds:

	general case	$d_2 = d_1$
affine diff addition	$1\mathbf{I} + 3\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$	$1\mathbf{I} + 1\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$
affine diff addition+doubling	$2\mathbf{I} + 4\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$	$2\mathbf{I} + 1\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$
mixed diff addition	$6\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$	$5\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$
mixed diff addition+doubling	$6\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$	$5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$
projective diff addition	$8\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$	$7\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$
projective diff addition+doubling	$8\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$	$7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$

Why differential addition is interesting. Montgomery in [83] presented fast formulas for u-coordinate differential addition on non-binary elliptic curves $\mathbf{v}^2 = \mathbf{u}^3 + a_2\mathbf{u}^2 + \mathbf{u}$. As an application, Montgomery suggested what is now called the "Montgomery ladder" to compute $u(mP), u((m+1)P)$ given $u(P)$. The idea is to recursively compute $u(\lfloor m/2 \rfloor P), u((\lfloor m/2 \rfloor + 1)P)$, and then to compute $u(mP), u((m+1)P)$ with a differential addition and doubling.

The Montgomery ladder is one of the most popular scalar-multiplication methods. It has several attractive features: it is fast; it fits into extremely small hardware; and its uniform double-and-add structure adds a natural layer of protection against simple side-channel attacks. See [15], [19], [37], [55], [59] and [76]. The input $u(P)$ is normally given in affine form, creating affine differential additions if inversions are inexpensive and mixed differential additions otherwise.

Montgomery also suggested a more complicated "PRAC" chain of differential additions to compute $u(mP)$ from $u(P)$. This chain uses more memory than the Montgomery ladder and does not have the same simple structure, but it is faster in some situations. This chain rarely reuses the input $u(P)$; it relies mainly on projective differential additions if inversions are expensive.

Differential-addition formulas for binary elliptic curves. Several authors have given formulas for u-coordinate differential additions on binary elliptic curves $\mathbf{v}^2 + a_1\mathbf{uv} = \mathbf{u}^3 + a_2\mathbf{u}^2 + a_6$. The resulting Montgomery ladders for binary elliptic-curve scalar-multiplication fit into even smaller hardware than the ladders for the non-binary case, and they have similar resistance to simple side-channel attacks.

Specifically, u-coordinate differential-addition formulas for the case $a_1 = 1$ were presented by Agnew, Mullin, and Vanstone in [1, page 808]; by López and Dahab in [76, Lemma 2 and Section 4.2]; by Vanstone, Mullin, Antipa, and Gallant, according to [98]; by Stam in [98, Section 3.1], and by Gaudry in [45, page 33]. López and Dahab say that their formulas use $6\mathbf{M} + 5\mathbf{S}$ for a mixed differential addition and doubling; see [76, Lemma 5]. Stam, after pointing out various speedups, says that projective differential addition takes $6\mathbf{M} + 1\mathbf{S}$; that mixed differential addition takes $4\mathbf{M} + 1\mathbf{S}$; and that a doubling takes $1\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$. Stam also presents differential-addition formulas for the case $a_6 = 1/a_1^2$, using only $5\mathbf{M}$ and

an unspecified number of **S** for projective differential addition. Gaudry states a cost of $5\mathbf{M} + 5\mathbf{S} + 1\mathbf{D}$ for mixed differential addition and doubling; Gaudry and Lubicz state the same cost in [47, page 16].

All of the formulas in [1], [76], [98], and [45] fail if the neutral element on the curve appears. Our new formulas have no trouble with the neutral element, and have the advantage of completeness for suitable d_2. Our formulas are also competitive in speed with previous formulas—slightly slower in some situations but slightly faster in others.

The new formulas. Let (x_2, y_2) be a point on the binary Edwards curve $\mathrm{E}_{\mathrm{B},d_1,d_2}$. Assume that the sum $(x_2, y_2)+(x_2, y_2)$ is defined (as it always is on complete binary Edwards curves). Write $(x_4, y_4) = (x_2, y_2)+(x_2, y_2)$, and write $w_i = x_i+y_i$. Then $d_1^2 + d_1 w_2^2 + d_2 w_2^4 \neq 0$ and

$$w_4 = \frac{d_1 w_2^2 + d_1 w_2^4}{d_1^2 + d_1 w_2^2 + d_2 w_2^4} = \frac{w_2^2 + w_2^4}{d_1 + w_2^2 + (d_2/d_1) w_2^4}$$

by Lemma 8.3. In particular, if $d_2 = d_1$, then $d_1 + w_2^2 + w_2^4 \neq 0$ and

$$w_4 = 1 + \frac{d_1}{d_1 + w_2^2 + w_2^4}.$$

More generally, assume that $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_5, y_5)$ are points on $\mathrm{E}_{\mathrm{B},d_1,d_2}$ satisfying $(x_1, y_1) = (x_3, y_3) - (x_2, y_2)$ and $(x_5, y_5) = (x_2, y_2) + (x_3, y_3)$, and write $w_i = x_i + y_i$ as before. Then, by Lemma 8.3,

$$d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3) \neq 0$$

and

$$w_1 + w_5 = \frac{d_1 w_2 w_3 (1 + w_2)(1 + w_3)}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)},$$
$$w_1 w_5 = \frac{d_1^2 (w_2 + w_3)^2}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)}.$$

In particular, if $d_2 = d_1$, then $d_1 + w_2 w_3 (1 + w_2)(1 + w_3) \neq 0$ and

$$w_1 + w_5 = 1 + \frac{d_1}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)},$$
$$w_1 w_5 = \frac{d_1 (w_2 + w_3)^2}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)}.$$

Cost of affine *w*-coordinate differential addition and doubling. The explicit formulas

$$R = w_2 \cdot w_3,\ S = R^2,\ T = R \cdot (1 + w_2 + w_3) + S,$$
$$w_5 = T \cdot \frac{1}{d_1 + T + (d_2/d_1 + 1)S} + w_1$$

use $1\mathbf{I}+3\mathbf{M}+1\mathbf{S}+1\mathbf{D}$, where the $1\mathbf{D}$ is a multiplication by the curve parameter d_2/d_1+1. For complete binary Edwards curves the denominator is never zero.

If $d_2 = d_1$ then the explicit formulas

$$A = w_2^2,\ B = A + w_2,\ C = w_3^2,\ D = C + w_3,\ w_5 = 1 + d_1\frac{1}{d_1 + B \cdot D} + w_1$$

use just $1\mathbf{I}+1\mathbf{M}+2\mathbf{S}+1\mathbf{D}$. For complete binary Edwards curves the denominator is never zero.

Doubling: The explicit formulas

$$A = w_2^2,\ J = A^2,\ K = A + J,\ w_4 = K \cdot \frac{1}{d_1 + K + (d_2/d_1 + 1)J}$$

use $1\mathbf{I}+1\mathbf{M}+2\mathbf{S}+1\mathbf{D}$, where the $1\mathbf{D}$ is a multiplication by the curve parameter d_2/d_1+1. For complete binary Edwards curves the denominator is never zero. The total cost of a differential addition and doubling is $2\mathbf{I}+4\mathbf{M}+3\mathbf{S}+2\mathbf{D}$, or $1\mathbf{I}+7\mathbf{M}+3\mathbf{S}+2\mathbf{D}$ with Montgomery's inversion trick.

If $d_2 = d_1$ then the explicit formulas

$$A = w_2^2,\ B = A + w_2,\ w_4 = 1 + d_1\frac{1}{d_1 + B^2}$$

use just $1\mathbf{I}+2\mathbf{S}+1\mathbf{D}$. For complete binary Edwards curves the denominator is never zero. These formulas can share the computations of A and B with differential addition, reducing the total cost of a differential addition and doubling to $2\mathbf{I}+1\mathbf{M}+3\mathbf{S}+2\mathbf{D}$, or $1\mathbf{I}+4\mathbf{M}+3\mathbf{S}+2\mathbf{D}$ with Montgomery's inversion trick.

Cost of mixed w-coordinate differential addition and doubling. Assume that w_1 is given as a field element, that w_2, w_3 are given as fractions $W_2/Z_2, W_3/Z_3$, and that w_4, w_5 are to be output as fractions $W_4/Z_4, W_5/Z_5$.

The explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ D = W_3 \cdot (Z_3 + W_3),\ E = Z_2 \cdot Z_3,\ F = W_2 \cdot W_3,$$
$$V = C \cdot D,\ U = V + (\sqrt{d_1}\,E + \sqrt{d_2/d_1 + 1}\,F)^2,\ W_5 = V + w_1 \cdot U,\ Z_5 = U$$

use $6\mathbf{M}+1\mathbf{S}+2\mathbf{D}$, where the $2\mathbf{D}$ are multiplications by the curve parameters $\sqrt{d_1}$ and $\sqrt{d_2/d_1+1}$. For complete binary Edwards curves Z_5 cannot be zero.

If $d_2 = d_1$ then the explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ D = W_3 \cdot (Z_3 + W_3),\ E = Z_2 \cdot Z_3,$$
$$V = C \cdot D,\ U = V + d_1E^2,\ W_5 = V + w_1 \cdot U,\ Z_5 = U$$

use only $5\mathbf{M}+1\mathbf{S}+1\mathbf{D}$.

Doubling: The explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ W_4 = C^2,\ Z_4 = W_4 + ((\sqrt[4]{d_1}\, Z_2 + \sqrt[4]{d_2/d_1 + 1}\, W_2)^2)^2$$

use $1\mathbf{M}+3\mathbf{S}+2\mathbf{D}$, where the $2\mathbf{D}$ are multiplications by the curve parameters $\sqrt[4]{d_1}$ and $\sqrt[4]{d_2/d_1+1}$. For complete binary Edwards curves Z_4 cannot be zero. These formulas can share the computation of C with differential addition, reducing the total cost of differential addition and doubling to $6\mathbf{M} + 4\mathbf{S} + 4\mathbf{D}$.

If $d_2 = d_1$ then the explicit formulas

$$C = W_2 \cdot (Z_2 + W_2),\ W_4 = C^2,\ Z_4 = d_1(Z_2^2)^2 + W_4$$

use $1\mathbf{M}+3\mathbf{S}+1\mathbf{D}$ and can share the computation of C with differential addition, reducing the total cost of differential addition and doubling to $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$.

Cost of projective w-coordinate differential addition and doubling. Assume that w_1, w_2, w_3 are given as fractions $W_1/Z_1, W_2/Z_2, W_3/Z_3$, and that w_4, w_5 are to be output as fractions $W_4/Z_4, W_5/Z_5$.

Replacing "$W_5 = V + w_1 \cdot U,\ Z_5 = U$" in any of the mixed formulas with "$W_5 = V \cdot Z_1 + U \cdot W_1,\ Z_5 = U \cdot Z_1$" produces projective formulas costing $2\mathbf{M}$ extra. For example, starting from the $5\mathbf{M}+4\mathbf{S}+2\mathbf{D}$ formulas for mixed differential addition and doubling with $d_2 = d_1$, one obtains $7\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$ formulas for projective differential addition and doubling with $d_2 = d_1$.

Our w_1w_5 formulas offer an interesting alternative. For example, the explicit formulas

$$A = W_2 \cdot W_3,\ B = Z_2 \cdot Z_3,\ C = (W_2 + Z_2) \cdot (W_3 + Z_3),$$
$$W_5 = Z_1 \cdot (d_1(C + A + B)^2),\ Z_5 = W_1 \cdot (A \cdot C + (\sqrt{d_1}\, B + \sqrt{d_2/d_1 + 1}\, A)^2)$$

use only $6\mathbf{M} + 2\mathbf{S} + 3\mathbf{D}$ for differential addition. These formulas assume that w_1 is known, or checked, to be nonzero—if $w_1 = 0$ then one must resort to the previous formulas for w_5—but they still have the virtue of handling arbitrary w_2, w_3, w_4, w_5. Note that w_1 is fixed throughout the Montgomery ladder, and is 0 only if the starting point is $(0, 0)$ or $(1, 1)$.

Recovering $2P$ from $Q - P, w(P), w(Q)$. If $w_1^2 + w_1 \neq 0$ then

$$x_2^2+x_2 = \frac{w_3\left(d_1+w_1w_2(1+w_1+w_2)+\frac{d_2}{d_1}w_1^2w_2^2\right)+d_1(w_1+w_2)+(y_1^2+y_1)(w_2^2+w_2)}{w_1^2+w_1}.$$

One can use this formula to compute $2(x_2, y_2)$ given x_1, y_1, w_2, w_3; i.e., to recover $2P$ given $Q-P, w(P), w(Q)$. The formula produces $x_2^2+x_2$; a "half-trace" computation reveals either x_2 or $x_2 + 1$, and therefore either (x_2, y_2) or $(x_2, y_2) + (1, 1)$. The failure case $w_1^2 + w_1 = 0$ occurs only if $4(Q - P) = (0, 0)$.

In particular, one can recover $2mP$ given $P, w(mP), w((m+1)P)$, except in the easily recognizable case $4P = (0,0)$. The Montgomery ladder can therefore be used not just to compute $w(mP)$ given $w(P)$, but also to compute $2mP$ given P. If P has odd order ℓ, as it does in typical cryptographic applications, then one can replace m by $(m/2) \bmod \ell$, obtaining $mP = 2((m/2) \bmod \ell)P$ from P via $w(((m/2) \bmod \ell)P)$.

Chapter 9

Concluding Remarks

In Chapters 4-7 of this thesis, we proposed several number extractors for curves and the Jacobians. We shall first summarize our contributions.

- In Chapter 4, we introduced a deterministic extractor `Ext` for the ordinary elliptic curve E defined over $\mathbb{F}_{2^n}$, where $n = 2\ell$ and ℓ is a positive integer. The extractor `Ext` for a given point P on E outputs the first $\mathbb{F}_{2^\ell}$-coordinate of the x-coordinate of the point P.
- In Chapter 5, we expressed the deterministic extractor `Ext` based on the (hyper)elliptic curve $\mathcal{C}$, defined over $\mathbb{F}_{q^2}$, where q is some power of an odd prime.
- In Chapter 6, we proposed the first extractors for the Jacobian of a genus 2 hyperelliptic curve H over $\mathbb{F}_q$. These extractors, called the *sum* and *product* extractors, output the sum and product of the x-coordinates of points on H in the support of D, for a given reduced divisor D on $J(\mathbb{F}_q)$.
- In the same chapter, we proposed the modified versions of the sum an product extractors for the Kummer surface $\mathcal{K}$, that is associated to the Jacobian of H over $\mathbb{F}_q$.
- In Chapter 7, we extended the proposed sum and product extractors for binary hyperelliptic curves of genus 2.
- We also proposed a way to construct an extractor for the main subgroup based on an extractor of the full group in order to use only the subgroup of cryptographic interest.

- We gave bounds on the number of points on preimages for the these extractors and showed that the outputs of these extractors are distributed close to uniform.

The main part of the analysis of these extractors was the counting part; i.e., to find bounds on the number of points of all fibers of the extractors. By means of techniques proposed in Chapters 2 and 3, we defined a related surface to the domain of our proposed extractor. We considered a family of curves as intersections of this surface with coordinate hyperplanes. Each fiber of the extractor corresponded to a curve in this family; we showed that the number of points in a fiber equals the number of points on the corresponding curve. Then, by means of Hasse-Weil Theorem, we gave bounds on the number of points on the fibers of the extractor.

The proof techniques used in Chapters 4 and 5 required to work with elliptic curves defined over a binary field of the form $\mathbb{F}_{2^{2\ell}}$ and hyperelliptic curves defined over a quadratic extension of $\mathbb{F}_q$ in order to find a geometric description of the points having fixed part in $\mathbb{F}_q$. For the genus 2 curves studied in Chapters 6 and 7 no such restriction is necessary, in particular, the extractors can be applied to curves defined over fields $\mathbb{F}_q$, where q is a prime, and fields $\mathbb{F}_{2^n}$, where n is a prime. These are the most common choices in cryptographic applications to avoid Weil descent attacks. So the results presented in these chapters are more practical than earlier ones.

Generalization of our extractors. The proposed extractors can be generalized to other families of curves, Jacobians of curves of larger genus and in general to varieties. In Section 2.11, we have suggested a simple way to construct an extractor `Ext` based on varieties. In general, the outputs of this extractor are distributed close to uniform. As we mentioned before, the main part of the analysis of the extractor `Ext` is the investigation of the geometry of the fibers of `Ext`. Obviously, finding tighter bounds for the number of points on fibers of `Ext` implies a more exact analysis on the distribution of the outputs of the extractor.

Consider the extractor $\texttt{Ext} : \mathcal{A}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^k$, given by Examples 2.36 and 2.37, where $\mathcal{A}$ is the Weil descent of a curve $\mathcal{C}$ defined over $\mathbb{F}_{q^n}$ or the Jacobian of a genus-n hyperelliptic curve H defined over $\mathbb{F}_q$. The following conjecture suggests a direction for future research in the context of extractors based on curves and Jacobians.

Conjecture 9.1 *`Ext` is a deterministic* $(\mathbb{F}_q^k, O(\frac{1}{\sqrt{q^{n-k}}}))$*-extractor for* $\mathcal{A}(\mathbb{F}_q)$.

For example, under this assumption the proposed extractor `Ext` in Chapter 4 can be extended to an extractor based on a binary elliptic curve E over $\mathbb{F}_{2^n}$, where n is a positive integer. In particular, n can be prime, which is applicable for cryptographic interests.

Edwards curves and extractors. Edwards curves have presented remarkably symmetric new forms of elliptic curves, which have led to strongly symmetric addition laws in terms of the coordinates of the points. So, one can consider extractors based on variants of Edwards curves, hoping that these extractors give more close to uniform outputs. For instance, an extractor for an Edwards curve can be defined such that, for a given point on an Edwards curve, it outputs part of the sum of the coordinates of the point.

In Chapter 8, we proposed a new form of binary elliptic curves. In the following, we give a summary of our contributions.

- We introduced the notion of *binary Edwards curves*, that is a new shape for ordinary elliptic curves over fields of characteristic 2 given by a symmetric equation. Using the new shape, we presented the first complete addition formulas for binary elliptic curves.
- The complete binary Edwards curves cover all isomorphism classes of ordinary elliptic curves over $\mathbb{F}_{2^n}$, for $n \geq 3$.
- We presented the doubling formulas for binary Edwards curves, which are extremely fast. Indeed, they are the first complete doubling formulas in the literature.
- Finally, we presented complete formulas for differential addition. These formulas propose extremely fast differential-addition for binary elliptic curves.

Edwards curves enable complete and fast arithmetic for elliptic curves. The hope is that future research on Edwards curves will improve several known results in the context of elliptic curves cryptography. Also, the idea can be generalized for hyperelliptic curves to improve the efficiency of the arithmetic of hyperelliptic curves cryptography.

We conclude by providing some related future research in the context of extractors.

Pseudorandom Generators and Extractors. A family of pseudorandom generators based on the decisional Diffie-Hellman assumption is proposed in [35]. This generator can be based on any group of prime order provided that an additional requirement is met (i.e., there exists an efficiently computable function that in some sense enumerates the elements of the group). Indeed, constructing an efficient provably secure pseudorandom generator based on the intractability of the DDH problem on an ordinary elliptic curve is an interesting open problem.

Extractors and Hash Functions. For many pairing-based cryptographic systems hash functions are needed that take values on algebraic curves. Often this is done by taking a hash function that outputs bit strings, followed by a mapping from bitstrings to the algebraic curve (see Boneh-Franklin [13]). Designing hash

functions taking values directly on the algebraic curve may be desirable, which then can be mapped further to bit strings by an extractor.

References

[1] G. B. Agnew, R. C. Mullin, and S. A. Vanstone. An implementation of elliptic curve cryptosystems over $\mathbb{F}_{2^{155}}$. *IEEE Journal of Selected Areas in Communications*, 11(5):804–813, 1993.

[2] E. Artin. *Algebraic Numbers and Algebraic Functions*. Gordon and Breach, New York, 1967.

[3] H. F. Baker. Examples of applications of Newton's polygon to the theory of singular points of algebraic functions. *Trans. Cambridge Phil. Soc.*, 15:403–450, 1893.

[4] E. Barker and J. Kelsey. Recommendation for random number generation using deterministic random bit generators, December 2005. NIST Special Publication (SP) 800-90.

[5] P. Beelen and J. M. Doumen. Pseudorandom sequences from elliptic curves. In *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, pages 37–52. Springer-Verlag, 2002.

[6] P. Beelen and R. Pellikaan. The Newton Polygon of Plane Curves with Many Rational Points. *Designs Codes and Cryptography*, 21:41–67, 2000.

[7] D. J. Bernstein, P. Birkner, T. Lange, and C Peters. Twisted Edwards Curves. In *Africacrypt 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer-Verlag, 2008.

[8] D. J. Bernstein and T. Lange. Explicit-Formulas Database, 2007. `http://www.hyperelliptic.org/EFD/`.

[9] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Advances in Cryptology – Asiacrypt 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer-Verlag, 2007.

[10] D. J. Bernstein and T. Lange. Inverted Edwards coordinates. In *Applied Algebra, Algebraic Algorithms, and Error Correcting Codes – AAECC 2007*, volume 4851 of *Lecture Notes in Computer Science*, pages 20–27. Springer-Verlag, 2007.

[11] D. J. Bernstein, T. Lange, and R. R. Farashahi. Binary Edwards Curves. In *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 244–265. Springer-Verlag, 2008.

[12] O. Billet and M. Joye. The Jacobi Model of an Elliptic Curve and Side-Channel Analysis. In *Applicable Algebra, Algebraic Algorithms and Error-Correcting Codes – AAECC 2003*, volume 2643 of *Lecture Notes in Comput. Sci.*, pages 34–42. Springer-Verlag, Berlin, 2003.

[13] D. Boneh and M. Franklin. Identity based encryption from weil pairing. In *Advances in Cryptology – Crypto 2001*, volume 2139, pages 213–229. Springer-Verlag, 2001.

[14] É. Brier, I. Déchène, and M. Joye. Unified point addition formulæ for elliptic curve cryptosystems. In *Embedded Cryptographic Hardware: Methodologies & Architectures*, pages 247–256. Nova Science Publishers, 2004.

[15] É. Brier and M. Joye. Weierstraß elliptic curves and side channels attacks. In *Public Key Cryptography – PKC 2002*, volume 2274 of *Lecture Notes in Comput. Sci.*, pages 335–345. Springer-Verlag, 2002.

[16] D. Brown and K. Gjøsteen. A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator. In *Advances in Cryptology – Crypto 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 466–481. Springer-Verlag, 2007.

[17] D. Cantor. Computing in the Jacobian of a Hyperelliptic Curve. *Mathematics of Computation*, 48(177):95–101, 1987.

[18] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. Cambridge University Press, Cambridge, 1996.

[19] W. Castryck, S. Galbraith, and R. R. Farashahi. Efficient arithmetic on elliptic curves using a mixed edwards-montgomery representation. Cryptology ePrint Archive, Report 2008/218, 2008. `http://eprint.iacr.org/2008/218.pdf`.

[20] O. Chevassut, P. Fouque, P. Gaudry, and D. Pointcheval. The Twist-Augmented Technique for Key Exchange. In *Public Key Cryptography – PKC 2006*, volume 3958 of *Lecture Notes in Computer Science*, pages 410–426. Springer-Verlag, 2006.

[21] B. Chor, O. Goldreich, J. Håstad, J. Friedman, S. Rudich, and R. Smolensky. The bit Extraction Problem of t-Resilient Functions. In *IEEE Symposium on Foundations of Computer Science*, volume 1462, pages 396–407, 1985.

[22] M. Ciet, J. Quisquater, and F. Sica. A Secure Family of Composite Finite Fields Suitable for Fast Implementation of Elliptic Curve Cryptography. In *INDOCRYPT2001*, volume 2247 of *Lecture Notes in Computer Science*, pages 108–116. Springer-Verlag, 2001.

[23] H. Cohen and G. Frey. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman & Hall/CRC, New York, 2006.

[24] C. Doche and T. Lange. Arithmetic of elliptic curves. In *Handbook of Elliptic and Hyperelliptic Curve Cryptography* [23], pages 267–302. CRC Press, 2005.

[25] S. Duquesne. Montgomery Scalar Multiplication for Genus 2 Curves. In *Algorithmic Number Theory Symposium – ANTS 2004*, volume 3076 of *Lecture Notes in Computer Science*, pages 153–168. Springer-Verlag, 2004.

[26] H. M. Edwards. A Normal Form for Elliptic Curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007. `http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html`.

[27] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Grad. Texts Math, Vol. 150, Springer-Verlag, New York, USA, 1995.

[28] E. El Mahassni and I. E. Shparlinski. On the uniformity of distribution of congruential generators over elliptic curves. In *Sequences and their Applications – SETA 01*, Discrete Mathematics and Theoretical Computer Science, pages 257–264. Springer-Verlag, 2002.

[29] R. R. Farashahi. Extractors for Jacobian of Hyperelliptic Curves of Genus 2 in Odd Characteristic. In *Cryptography and Coding: 11th IMA International Conference*, volume 4887 of *Lecture Notes in Computer Science*, pages 313–335. Springer-Verlag, 2007.

[30] R. R. Farashahi. Extractors for Jacobians of Binary Genus-2 Hyperelliptic Curves. In *Information Security and Privacy, 13th Australian Conference – ACISP 2008*, volume 5107 of *Lecture Notes in Computer Science*, pages 447–462. Springer-Verlag, 2008.

[31] R. R. Farashahi. Norm and Trace Varieties. preprint, 2008.

[32] R. R. Farashahi and R. Pellikaan. The Quadratic Extension Extractor for (Hyper)Elliptic Curves in Odd Characteristic. In *International Workshop on the Arithmetic of Finite Fields – WAIFI 2007*, volume 4547 of *Lecture Notes in Computer Science*, pages 219–236. Springer-Verlag, 2007.

[33] R. R. Farashahi, R. Pellikaan, and A. Sidorenko. Extractors for Binary Elliptic Curves. In *Workshop on Coding and Cryptography – WCC 2007*, pages 127–136, 2007.

[34] R. R. Farashahi, R. Pellikaan, and A. Sidorenko. Extractors for Binary Elliptic Curves. *Designs, Codes and Cryptography*, 49(1–3):171–186, 2008. `http://www.springerlink.com/content/lm35kv103x34j754`.

[35] R. R. Farashahi, B. Schoenmakers, and A. Sidorenko. Efficient pseudorandom generators based on the DDH assumption. In *Public Key Cryptography – PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 426–441. Springer-Verlag, 2007.

[36] R. R. Farashahi and I. E. Shparlinski. On the number of distinct elliptic curves in some families. preprint, 2008.

[37] W. Fischer, C. Giraud, E. W. Knudsen, and J.P. Seifert. Parallel scalar multiplication on general elliptic curves over $\mathbb{F}_p$ hedged against non-differential side-channel attacks. Cryptology ePrint Archive, Report 2002/07, 2002.

[38] G. Frey. How to disguise an elliptic curve. Talk at Waterloo workshop on the ECDLP, 1998. `http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`.

[39] W. Fulton. *Algebraic Curves : An Introduction to Algebraic Geometry.* Addison-Wesley, 1969.

[40] A. Gabizon, R. Raz, and R. Shaltiel. Deterministic Extractors for Bit-Fixing Sources by Obtaining an Independent Seed. *SIAM Journal on Computing*, 36(4):1072–1094, 2006.

[41] S. Galbraith, F. Hess, and N. P. Smart. Constructive and Destructive Facets of Weil Descent on Elliptic Curves. *Journal of Cryptology*, 15(1):19–46, 2002.

[42] S. Galbraith, F. Hess, and N. P. Smart. Extending the GHS Weil Descent Attack. In *Advances in Cryptology – Eurocrypt 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 29–44. Springer-Verlag, 2002.

[43] S. Gao. Absolute Irreducibility of Polynomials via Newton Polytopes. *Journal of the Algebra*, 237:501–520, 2001.

[44] P. Gaudry. An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves. In *Advances in Cryptology – Eurocrypt 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–3448. Springer-Verlag, 2000.

[45] P. Gaudry. Variants of the Montgomery form based on Theta functions, 2006. `http://www.loria.fr/~gaudry/publis/toronto.pdf`.

[46] P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *J. Math. Crypt.*, 1:243–265, 2007.

[47] P. Gaudry and D. Lubicz. The arithmetic of characteristic 2 Kummer surfaces, 2008. `http://www.loria.fr/~gaudry/tmp/c2.pdf`.

[48] G. Gong, T. A. Berson, and D. R. Stinson. Elliptic Curve Pseudorandom Sequence Generators. In *Selected Areas in Cryptography – SAC 1999*, volume 1758 of *Lecture Notes in Computer Science*, pages 34–48. Springer-Verlag, 2000.

[49] N. Gürel. Extracting bits from coordinates of a point of an elliptic curve. Cryptology ePrint Archive, Report 2005/324, 2005. `http://eprint.iacr.org/`.

[50] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, New York, USA, 2004.

[51] R. Hartshorne. *Algebraic Geometry*. Grad. Texts Math, Vol. 52, Springer-Verlag, New York, USA, 1977.

[52] F. Hess. Generalising the GHS Attack on the Elliptic Curve Discrete Logarithm Problem. *LMS Journal of Computation and Mathematics*, 7:167–192, 2004.

[53] F. Hess and I. E. Shparlinski. On the Linear Complexity and Multidimensional Distribution of Congruential Generators over Elliptic Curves. *Designs, Codes and Cryptography*, 35(1):111–117, 2005.

[54] T. Itoh and S. Tsujii. Structure of Parallel Multipliers for a Class of Fields GF(2^m). *Informations and Computers*, 83:21–40, 1989.

[55] T. Izu and T. Takagi. A fast parallel elliptic curve multiplication resistant against Side-Channel Attacks. In *Public Key Cryptography – PKC 2002*, volume 2274 of *Lecture Notes in Comput. Sci*, pages 280–296. Springer-Verlag, Berlin, 2002.

[56] T. Izu and T. Takagi. Exceptional procedure attack on elliptic curve cryptosystems. In *Public Key Cryptography – PKC 2003*, volume 2567 of *Lecture Notes in Comput. Sci*, pages 224–239. Springer-Verlag, Berlin, 2003.

[57] M. Joye. Defences against side-channel analysis. In *Advances in elliptic curve cryptography*, pages 87–100. Cambridge University Press, 2005.

[58] 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 Comput. Sci.*, pages 402–410. Springer-Verlag, Berlin, 2001.

[59] M. Joye and S.-M. Yen. The Montgomery powering ladder. In *Cryptographic Hardware and Embedded Systems – CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 291–302. Springer-Verlag, 2003.

[60] A. Juels, M. Jakobsson, E. Shriver, and B. K. Hillyer. How to turn loaded dice into fair coins. *IEEE Transactions on Information Theory*, 46(3):911–921, May 2000.

[61] B. S. Kaliski. A Pseudo-Random Bit Generator Based on Elliptic Logarithms. In *Advances in Cryptology – Crypto 1986*, volume 263 of *Lecture Notes in Computer Science*, pages 84–103. Springer-Verlag, 1987.

[62] A. G. Khovanskii. Newton polyhedra and the genus of complete intersections. *Functional Analysis and Its Applications*, 12(1):38–46, 1978.

[63] K. H. Kim and S. I. Kim. A new method for speeding up arithmetic on elliptic curves over binary fields, 2007. `http://eprint.iacr.org/2007/181`.

[64] E. W. Knudsen. Elliptic Scalar Multiplication Using Point Halving. In *Advances in Cryptology – Asiacrypt 1999*, volume 1716 of *Lecture Notes in Computer Science*, pages 135–149. Springer-Verlag, 1999.

[65] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[66] N. Koblitz. Hyperelliptic Cryptosystem. *J. of Cryptology*, 1:139–150, 1989.

[67] A. Kresch, J.L. Wetherell, and M.E. Zieve. Curves of Every Genus with Many Points, I: Abelian and Toric Families. *J. Algebra*, 250:353–370, 2002.

[68] T. Lange. Montgomery Addition for Genus Two Curves. In *Algorithmic Number Theory Symposium – ANTS 2004*, volume 3076 of *Lecture Notes in Computer Science*, pages 309–307. Springer-Verlag, 2004.

[69] T. Lange. Mathematical countermeasures against side-channel attacks. In *Handbook of Elliptic and Hyperelliptic Curve Cryptography* [23], pages 687–714. CRC Press, 2005.

[70] T. Lange. A note on López–Dahab coordinates. *Tatra Mountains Mathematical Publications*, 33:75–81, 2006.

[71] T. Lange and I. E. Shparlinski. Certain Exponential Sums and Random Walks on Elliptic Curves. *Canad. J. Math.*, 57(2):338–350, 2005.

[72] T. Lange and I. E. Shparlinski. Distribution of Some Sequences of Points on Elliptic Curves. *J. Math. Crypt.*, 1:1–11, 2007.

[73] T. Lange and M. Stevens. Efficient Doubling on Genus Two Curves over Binary Fields. In *Selected Areas in Cryptography – SAC 2005*, volume 3357 of *Lecture Notes in Computer Science*, pages 170–181. Springer-Verlag, 2005.

[74] P. Y. Liardet and N. P. 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 Comput. Sci.*, pages 391–401. Springer-Verlag, Berlin, 2001.

[75] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge Univ. Pr., 1994.

[76] J. López and R. Dahab. Fast multiplication on elliptic curves over GF(2^m) without precomputation. In *Cryptographic Hardware and Embedded Systems – CHES 1999)*, volume 1717 of *Lecture Notes in Comput. Sci.*, pages 316–327. Springer-Verlag, 1999.

[77] J. López and R. Dahab. Improved algorithms for elliptic curve arithmetic in GF(2^n). In *Selected Areas in Cryptography – SAC 1998*, volume 1556 of *Lecture Notes in Computer Science*, pages 201–212. Springer-Verlag, 1999.

[78] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton University Press, USA, 1994.

[79] M. Maurer, A. Menezes, and E. Teske. Analysis of the GHS Weil Descent Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree. *LMS Journal of Computation and Mathematics*, 5:127–174, 2002.

[80] A. Menezes, T. Okamoto, and S. Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.

[81] A. Menezes and E. Teske. Cryptographic Implications of Hess' Generalized GHS Attack. *Applicable Algebra in Engineering, Communication and Computing*, 16(6):439–460, 2006.

[82] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology – Crypto 1985*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, 1986.

[83] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, 48(177):243–264, 1987.

[84] D. Mumford. *Tata Lectures on Theta II*, volume 43 of *Progress in Mathematics*. Springer-Verlag, 1984.

[85] B. Schoenmakers and A. Sidorenko. Cryptanalysis of the Dual Elliptic Curve pseudorandom generator. Cryptology ePrint Archive, Report 2006/190, 2006. `http://eprint.iacr.org/`.

[86] R. Schroeppel. Elliptic curves: Twice as fast!, 2000. Presentation at the Crypto 2000 Rump Session.

[87] G. Seroussi. Compact Representation of Elliptic Curve Points over $\mathbb{F}_{2^n}$. Technical Report HPL-98-94R1, Hewlett–Packard Laboratories, 1998.

[88] J-P. Serre. Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini. *C.R. Acad. Sci. Paris*, 296(I):397–402, 1983.

[89] R. Shaltiel. Recent Developments in Explicit Constructions of Extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

[90] I. E. Shparlinski. On the Naor-Reingold Pseudo-Random Function from Elliptic Curves. *Applicable Algebra in Engineering, Communication and Computing*, 11(1):27–34, 2000.

[91] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[92] J. H. Silverman. Fast Multipication in Finite Fields GF(2^N). In *Cryptographic Hardware and Embedded Systems – CHES 1999*, volume 1717 of *Lecture Notes in Computer Science*, pages 122–134. Springer-Verlag, 1999.

[93] N. P. Smart and S. Siksek. A Fast Diffie-Hellman Protocol in Genus 2. *Journal of Cryptology*, 12:67–73, 1999.

[94] J. A. Solinas. Efficient Arithmetic on Koblitz Curves. *Designs, Codes and Cryptography*, 19:195–249, 2000.

[95] W. Stein. *Sage Mathematics Software (Version 2.8.13)*. The Sage Group, 2008. `http://www.sagemath.org`.

[96] L. Trevisan and S. Vadhan. Extracting Randomness from Samplable Distributions. In *IEEE Symposium on Foundations of Computer Science*, pages 32–42, 2000.

[97] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Discrete Mathematics and its Applications. CRC Press, 2008.

[98] F. Zhang, R. Safavi-Naini, and W. Susilo. On Montgomery-like representations for elliptic curves over GF(2^k). In *Public Key Cryptography – PKC 2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 240–254. Springer-Verlag, 2002.

Summary

Curves and Jacobians: Number Extractors and Efficient Arithmetic

Algebraic curves over finite fields are being extensively studied in the context of public-key cryptographic schemes. In this thesis, we present several number extractors for (hyper)elliptic curves and Jacobians. We also present efficient arithmetic on binary elliptic curves.

The problem of converting random points on curves and Jacobians into random bits has several cryptographic applications, such as key derivation functions needed as final step of key exchange protocols or in hybrid encryption and the design of cryptographically secure pseudorandom number generators.

We propose a simple number extractor based on elliptic and hyperelliptic curves over quadratic extensions of finite fields. This extractor outputs, for a given point on a curve, the first ground field coordinate of the x-coordinate of the point.

We also introduce two simple number extractors based on Jacobians of genus-2 hyperelliptic curves over finite fields. They are called the *sum* and the *product* extractors. The *sum* (respectively the *product*) extractor outputs, for a given reduced divisor on the Jacobian of a hyperelliptic curve, the sum (respectively the product) of the x-coordinates of the points in the support of the divisor. In addition, we propose modified versions of these extractors for the Kummer surface associated to the Jacobian of a genus-2 hyperelliptic curve.

Moreover, we describe a way to construct an extractor for the main subgroup of a even order group based on an extractor of the full group in order to use only the subgroup of cryptographic interest.

We show that for a given random point in the domain of the above extractors, the outputs of these extractors are distributed closely to uniform.

To analyze the proposed extractors, we need to investigate the geometry of the intersections of the associated variety with coordinate hyperplanes. More precisely, we first study this problem for the surfaces related to Weil descents of elliptic and

hyperelliptic curves over quadratic extensions of finite fields and then for Jacobians of genus-2 hyperelliptic curves over finite fields.

Finally, we introduce a new shape for ordinary elliptic curves over fields of characteristic 2. They are called *binary Edwards curves*. Using the new shape, the first complete addition formulas for binary elliptic curves are presented. Furthermore, fast doubling formulas and differential-addition formulas for binary elliptic curves in the binary Edwards form form are proposed.

Curriculum Vitae

Reza Rezaeian Farashahi was born on the 15th of January 1976 in Tehran, Iran. He graduated from Malek Sabet high-school in Mathematics and Physics in 1994. He received his Bachelor, in Electronics (Electrical Engineering), from University of Tehran in 1998 and his Master, in Pure Mathematics (Algebra), from Shahid Chamran University of Ahvaz in January 2001. In 2002, he was granted a Ph.D. scholarship from Ministry of Science, Research and Technology of I. R. Iran and in December 2004 he started his Ph.D. studies within the department of Mathematics and Computing Science at the Eindhoven University of Technology (TU/e), The Netherlands. The results of his research have been accepted among the research community leading to several publications and to this thesis.

List of Notations

Index