CERIAS Tech Report 2007-22

FINITE FIELD OF LOW CHARACTERISTIC IN ELLIPTIC CURVE CRYPTOGRAPHY

by Shuo Shen

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Graduate School ETD Form 9
(01/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis Acceptance

This is to certify that the thesis prepared

By Shuo Shen

Entitled Finite Fields of Low Characteristic in Elliptic Curve Crytography

Complies with University regulations and meets the standards of the Graduate School for originality and quality

For the degree of Doctor of Philosophy

Final examining committee members

Samuel Wagstaff, Chair

Andreas Stein

William Heinzer

Freydoon Shahidi

Approved by Major Professor(s): Samuel Wagstaff

Approved by Head of Graduate Program: Fabio A. Milner

Date of Graduate Program Head's Approval: 04/13/07

FINITE FIELDS OF LOW CHARACTERISTIC

IN ELLIPTIC CURVE CRYPTOGRAPHY

A Thesis

Submitted to the Faculty

of

Purdue University

by

Shuo Shen

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

May 2007

Purdue University

West Lafayette, Indiana

dedicated to all of my family.

ACKNOWLEDGMENTS

I would like to express my deep gratitude to my advisor, Samuel Wagstaff, Professor of Mathematics and Computer Science at Purdue. His wide knowledge and attitude in research and study have been of great value for me. His understanding, encouragement and personal guidance have provided a good basis for the present thesis.

I am deeply grateful to my coadvisor, Professor Andreas Stein in the Department of Mathematics at the University of Wyoming, for his constant help in the research and valuable suggestions in career. I enjoyed the soccer games in Wyoming with Andreas and all the other players.

Also I am very grateful to Professor Michael Jacobson and Professor Renate Scheidler, which supervised the research project with Andreas in the summer school in Wyoming. Their constant help in and after the summer school helped me to enter a new research area.

I thank all the members of my committee, Professors Shahidi, Heinzer, Wagstaff and Stein. They always offered their kind help when I had questions. I appreciate their guidance, patience, and careful reading of this thesis.

I owe my loving thanks to my dear wife Ya Li, who is also a Ph.D student in Purdue Math Dept. Her warm support and love is my treasure of my whole life. I also deeply appreciate the help from my parents and parents in law, Furong and Manqiu, Xihai and Xiuzhi. Their unconditional help ensured my time and energy for my research. Also my lovely daughter, Xiaoyi, gave us great pleasure in my busy time.

I owe a lot of thanks to my friends; their support and friendship means a lot to me. I could always get their help during tough times.

Finally, I want to thank Jason Gower, also a student of Samuel, for his helpful comments, which I appreciate.

TABLE OF CONTENTS

ABSTRACT

Shen, Shuo Ph.D., Purdue University, May, 2007. Finite Fields of Low Characteristic in Elliptic Curve Cryptography. Major Professor: Samuel S. Wagstaff, Jr.

The use of finite fields of low characteristic can make the implementation of elliptic curve cryptography more efficient. There are two approaches to lower the characteristic of the finite field in ECC while maintaining the same security level: Elliptic curves over a finite field extension and hyperelliptic curves over a finite field. This thesis solves some problems in both approaches.

The group orders of elliptic curves over finite field extensions are described as polynomials. The irreducibility of these polynomials is proved, and hence the primality of the group orders can be studied. Asymptotic formulas for the number of traces of elliptic curves over field extensions with almost prime orders are given and a proof based on Bateman-Horn's conjecture is given. Hence the number of curves for cryptographic use is known. Experimental data is given. The formulas fit the actual data remarkably well.

Finally, the arithmetic of real hyperelliptic curves is studied. We study the algorithm for divisor addition on the real hyperlliptic curves and give the explicit formulas.

1. INTRODUCTION

1.1 Elliptic/Hyperelliptic Curve Cryptography

It is well known that the sets of rational points on elliptic curves over finite fields form finite groups and the sizes of these finite groups are of the same magnitude as the size of the base fields. Elliptic curve cryptosystems (ECC) were first proposed in 1985 independently by Neal Koblitz and Victor Miller based on the group structure of elliptic curves over finite fields. ECC's security depends on the computational complexity of the discrete logarithm problem(DLP) over elliptic curve groups, i.e., looking for m given rational points P and mP in an elliptic curve group, where m is a natural number less than the order of the elliptic curve group. Thus, large elliptic curve groups or prime order subgroups of elliptic curve groups are needed to guarantee that m can be large and the discrete logarithm problem hard. To reach the same security level[1] as 1024-bit RSA, the size of of the elliptic curve groups should be over 163 bits according to NIST guidelines for public key sizes. For more details about the ECC standard, see NIST FIPS 186-2.

The curves used in cryptography ares are those over $\mathbb{F}_{2^m}$:

$$y^2 + xy = x^3 + ax^2 + b \qquad \text{with } a, b \in \mathbb{F}_{2^m}, \tag{1.1}$$

and the elliptic curves over $\mathbb{F}_p$, where p is an odd prime greater than 3, in short Weierstrass form:

$$y^2 = x^3 + ax + b \qquad \text{with } a, b \in \mathbb{F}_p. \tag{1.2}$$

The use of hyperelliptic curves in cryptography was started in 1989 by Koblitz [18]. As with the elliptic curve cryptosystem, the discrete logarithm problem over the

[1] The security level usually refers to the size of key space, for example: one has to try 2^{1024} keys to launch a brute force attack on a 1024-bit security level cryptosystm.

Jacobian of hyperelliptic curves of low genus is computationally infeasible when the size of the Jacobians is large. See Müller et al. [26], Gaudry [13], Enge [10] and Theriault [34].

Hyperelliptic curves have the form $y^2 + h(x)y = f(x)$, where h and f are polynomials. The degree of f is $2g+1$ or $2g+2$ and the degree of h is no higher than $g+1$, where g is the genus of the curve; see Cohen et al. [7] for details. Formal definitions will be given in Chapter 3.

1.2 Elliptic Curves over Finite Fields

Elliptic curves over finite fields of characteristic 2 are very efficient and widely used because of their convenience in implementation, fast addition operation on binary computer systems and the key-per-bit-strength is good. But the elliptic curves with coefficients in $\mathbb{F}_2$ are very limited:

$$E(\mathbb{F}_2) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.3}$$

Of the $2^5 = 32$ possible curves, most are singular, supersingular or anomalous, which are either trivial or vulnerable curves in elliptic cryptography. $E(\mathbb{F}_{2^p})$ (p is a prime) are the most casually used elliptic curves.

The number of possible elliptic curves over a large prime order finite field $\mathbb{F}_p$ is enormous because for each integer $n \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$, we can find an elliptic curve with group order n (see Section 2.1.1). We want n to be a prime because we need a large prime order elliptic curve group to make the discrete logarithm problem hard. The number of group orders we could choose is the number of primes in $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ and the number of curves is even more than that.

Multiplications in extension fields of characteristic 2 are usually slower than in prime fields, while the the inversion in prime fields can be very expensive. To overcome these two difficulties, some optimal extension fields are explored, i.e., some special chosen small prime p and extension degree l make the extension field F_{q^l} have optimal performance in both multiplications and inversions. See Cohen et al. [7] for details. In this thesis, we generally study the amount of elliptic curves over extension fields that are possible for cryptographic use, further studies particular for the choices of p and l are expected to be done soon.

1.3 Contribution of This Thesis

Two approaches have been tried to make the algebraic operations fast while allowing many choices of elliptic curves. The first approach is to use elliptic curves over a finite field extension, with curve coefficients in a small finite field, i.e.:

$$E : y^2 = x^3 + Ax + B \text{ over } \mathbb{F}_{q^k} \qquad (q \text{ and } k \text{ are odd primes}, A, B \in \mathbb{F}_q). \tag{1.4}$$

This type of curves over finite field extension and with coefficients in small finite field are called Koblitz curves. Group orders of such type of elliptic curves are easier to calculate and use of Frobenius equation (Theorem 2.1.2) make make scalar multiplication over such type of curves faster. See Section 2.1 for more details.

The implementation is faster than for elliptic curves over a huge prime order field and there are many more choices than for curves with binary coefficients. It turns out that the order of E in Formula (1.4) can not be prime when $k > 1$. However, the order may be "almost prime," that is, have one large prime factor near q^{k-1}. This size of order is good enough for use in cryptography.

In this thesis, we give and prove a condition for an elliptic curve over a finite field extension to have almost prime order. We also give and prove an asymptotic formula for the number of traces of elliptic curves with almost prime orders. Formulas and experimental data show that there is a huge space of such elliptic curves for use in ECC. The safety property of these curves under certain attacks is also studied.

The second approach is to use hyperelliptic curves. A hyperelliptic curve with genus g over $\mathbb{F}_q$ has Jacobian of size about q^g. To have the same size of Jacobian as the size of elliptic curve groups, the base field of a hyperelliptic curve is smaller, thus the parameters of the curve are smaller. Algorithms for imaginary hyperelliptic curves have been widely studied. In this thesis, the explicit formulas for for the addition operation for a real hyperelliptic curve is given. More improvements for algorithms for real hyperelliptic curves are being explored with other mathematicians.

1.4 Outline of the Thesis

Chapter 2 studies elliptic curves over finite field extensions. Necessary background and related material will be introduced briefly. Proofs and experimental data are given in detail. Chapter 3 focuses on the algorithms for real hyperelliptic curves. Further work in both approaches is mentioned in both chapters.

2. ELLIPTIC CURVES OVER FINITE FIELD EXTENTIONS

2.1 Background

The work in this part of the thesis was started with the counting of elliptic curves of "almost prime" order by MAGMA. It was found that the ratio $|E(\mathbb{F}_{q^k})|/|E(\mathbb{F}_q)|$ can be described by the value of an irreducible polynomial determined by q and k. This fact is proved below along with other interesting results. This expression as an irreducible polynomial makes it possible to find an asymptotic formula for the number of elliptic curves of "almost prime" order if we assume Bateman-Horn's conjecture.

2.1.1 Basic Definitions

The classical theory of elliptic curves over a finite field is the basis of the work of this thesis. See Silverman [30] and Washington [36]. Some important related research in ECC and number theory will be introduced first.

All elliptic curves over finite fields of characteristic greater than 3 can be written in short Weierstrass normal form:

$$y^2 = x^3 + Ax + B \tag{2.1}$$

with A and B constants in some base field and the discriminant $\Delta = -4A^3 - 27B^2 \neq 0$. Modifications to the Weierstrass form must be made in characteristics 2 and 3. See Washington [36], page 11, for more details.

Let $\mathbb{F}_{q^k}$ be a finite field, $k \geq 1$ and $k \in \mathbb{Z}$. For fixed $A, B \in \mathbb{F}_{q^k}$, the set

$$E(\mathbb{F}_{q^k}) = \{\infty\} \cup \{(x, y) \in \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \mid \ y^2 = x^3 + Ax + B\} \tag{2.2}$$