Outline scription

Gijsbert van Vliet

January 14, 2015

1 Introduction

Here I will explain the necessary mathematical background which will be:

- Some basic knowledge of algebra. (the reader should be familiar with groups/ rings/ finite fields ect.)
- Some knowledge of algebraic geometry. For example, reading and understanding the first two chapters of Silverman's "The arithmetic of Elliptic Curves" will suffice.
- Just general mathematical maturity. For example I will use the chinese remainder theorem without stating it.

2 Introduction to cryptography

In this chapter I will give the general outlay of Public-key cryptography and the DLP.

2.1 Public-key cryptography

2.2 complexity

2.3 the discrete logarithm problem

2.4 General attacks on the DLP

2.4.1 The Pohlig-Hellman Method

2.4.2 The baby step-giant step algorithm

2.4.3 the Pollard ρ and λ method

3 Elliptic Curves

In this section I will give the basic theory of elliptic curves. Most proofs will be omitted. For those I will refer to the book of Silverman.
Standard notation:
-E/K: E is defined over K.
-$\bar{K}(C)$: the function field of E over $\bar{K}$.
-$K(C)$: the function field of E over K.

3.1 Weierstrass Equations

-Define general/simplified Weierstrass equations.
-Define discriminant Δ,j-invariant j and the invariant differential ω.
-Proposition 1.4.
-Remark: Curves given by a Weierstrass equation are curves of genus 1.

3.2 Group law

-Definition of the group law.
-Proposition: The group law makes E into an abelian group.
-Proposition: The K rational points form a subgroup of E.
-Remark: $P = (x, y) \in E \Rightarrow -P = (x, -y)$.
-Notation $[m]P$.

3.3 Elliptic Curves

-Define Elliptic Curve E.
-Proposition 3.1. (Possibly with outlay of the proof.)
-Example.
-Remark: Using RR to give group law on any elliptic curve. Proposition 3.4/3.6.
-Corollary 3.5.

3.4 Isogenies

-Define Isogeny ϕ for elliptic curves.
-Remark: Either $\phi(E_1) = \{O\}$ or $\phi(E_1) = E2$.
-Define (in)separable degree of ϕ.
-Define Endomorphism and Automorphism ring.
-Example 4.1.
-Proposition 4.2.(a)
-Define $E[m]$.
-Explane complex multiplication.
-Example(s).
-Theorem 4.8.
-Remark: Corollary 4.9.
-Theorem 4.10.

3.5 The Frobenius morphism

-Define the q-th Frobenius morphism for Curve of Characteristic p.
-Example.
-Proposition II.2.11.
-Corollary II.2.12.
-Proposition 1.5.
-Proposition 5.1.
-Theorem 5.2.
-Corollary 5.3.
-Corollary 5.5. (with prooof)

3.6 The dual isogeny

-Theorem 6.1. (a)
-Define the dual isogeny.
-Theorem 6.2.
-Corollary 6.4.

3.7 The Tate module

-introductory remarks.
-Define Tate module.
-Proposition 7.1.
-Define the l-adic representation of the Galois group.
-Theorem 7.4.

3.8 The Weil Pairing

-Justification construction.
-Construction.
-Proposition 8.1.
-Corollary 8.1.1.
-Proposition 8.2.
-Proposition 8.3.
-Proposition 8.6.

3.9 the endomorphism ring

-Define complex quadratic order.
-Define quaternion algebra.
-Corollary 9.2.
-Remark: endomorphism ring of elliptic curve over finite field is never $\mathbb{Z}$.

4 Elliptic Curves over Finite Fields

Standard notation:
-q is a power of a prime p.
-$\mathbb{F}_q$ is a finite field with q elements.
-$\bar{\mathbb{F}}_q$ is an algebraic Closure of $\mathbb{F}_q$.
-Remark ECDLP.
-Give small improvement for baby step- giant step algorithm.

4.1 The number of rational points

-Rough estimate $\leq 2q + 1$.
-Hasse's theorem.
-Use of legendre symbol to calculate number of rational points.
-Define Trace of frobenius morphism.
-Theorem 2.3.1.
-Linear recurrence for trace of q^n-frobenius morphism.

4.2 The endomorphism ring

-Theorem 3.1.(With proof)
-definition supersingular, ordinary and Hasse invariant.
-Theorem: E is supersingular iff p divides the trace of the frobenius morphism.

4.3 The group structure of elliptic Curves

-Proposition: type of elliptic curve over finite field.
-Lemma1 from article MOV-attack.
-Lemma2 from article MOV-attack.
-Lemma3 from article MOV-attack.

4.4 Determining the Hasse Invariant

-Theorem 4.1.
-examples.

5 Schoof's algorithm

5.1 The division polynomials

-Define division polynomials ψ_n, the polynomials f_n and give recurrence relations.
-Proposition 2.1 from Schoof's Algorithm.
-Proposition 2.2 from Schoof's Algorithm.

5.2 General outlay of the algorithm

-give relation determining the trace of frobenius mod l.
-Explain Estimation for number of primes.
-Give the relations to be tested.

5.3 Detailed description of the algorithm

-Give definition of gcd determining case distinction.
-Give detailed description of case 1.
-Give detailed description of case 2.

5.4 Efficiency of Schoof's algorithm

-Give theoretical complexity of algorithm.
-Give examined running times for several different primes.
-Draw conclusion.
-Remark on existing improvements of algorithm.

6 The MOV Attack

-Introductory remarks.

6.1 Index calculus

-General outlay.
-Worked out example.

6.2 Calculating the Weil Pairing

-description of algorithm.
-remark on complexity of the algorithm.

6.3 The Reduction

(The referrals are here to the article about the MOV attack.)
-Lemma 4.
-Lemma 5.
-Example.
-Lemma 6.
-Lemma 7.
-Theorem 10.
-Give algorithm.

6.4 Supersingular Curves

-Give Table 1 about supersingular curves.
-Give example(s) about how information of Table 1 was obtained.
-Give algorithm.
-Remarks on why the algorithm works.

6.5 Complexity

-Give theoretical estimation of the complexity of the algorithm.
-(If this algorithm is actually implemented) give examined running times and draw appropriate conclusions.

7 Anomalous curves

-Define Anomalous curves.
-Example.

7.1 The case $p = q$.

7.2 The general case.

8 Elliptic Curve cryptography

8.1 Diffie-Hellman Key Exchange

8.2 Massey-Omura Encryption

8.3 ElGamal Public Key Encryption

8.4 A cryptosystem based on the Weil Pairing