Abelian Variety Cryptosystems

Kevin Johnson 6017605
February 23, 2015

0.1 The Discrete Logarithm Problem

0.2 Polynomials, Algebraic Sets and Genus

0.3 Elliptic Curves

0.4 Hyperelliptic Curves

0.4.1 The Jacobian of a Hyperelliptic Curve

Unlike the case of elliptic curves, when the genus $\mathfrak{g}$ of a curve $\mathfrak{C}$ is greater than 1, the set of points on $\mathfrak{C}$ will not always form a group.

Example 0.4.2.

Luckily, there is another way to form an abelian group with hyperelliptic curves. Indeed, let $\mathfrak{D}$ be the set of all formal finite sums

$$\sum_i m_i P_i$$

where $m_i \in \mathbb{Z}$ and P_i are points on the curve $\mathfrak{C}$. We call elements of $\mathfrak{D}$ divisors of $\mathfrak{C}$. Given a rational function f in $\mathbb{Z}_p[\mathfrak{C}]$, we can define the corresponding divisor to f as

$$(f) = \sum_i m_i P_i$$

where P_i are the zeros and poles of f with multiplicities m_i. Divisors of this form are called principal divisors and we let $\mathfrak{P}$ denote the subset of all of them in $\mathfrak{D}$. If we define the operation on $\mathfrak{D}$ by

$$\sum_i m_i P_i + \sum_i m_i' P_i = \sum_i (m_i + m') P_i$$

then $\mathfrak{D}$ becomes and abelian group. Unfortunetly, this group is far too large for cryptographic purposes. So we consider the subgroup $\mathfrak{D}^0$ of all divisors of $\mathfrak{D}$ whos coefficients sum to 0. That is, divisors $\sum_i m_i P_i$ such that $\sum_i m_i = 0$.

Even though this subgroup is still infinite, we can define two divisors D_1, D_2 of $\mathfrak{D}^0$ to be equal if $D_1 - D_2$ is equal to the divisor of a rational function on $\mathfrak{C}$. That is, $D_1 - D_2 = (f)$ for $f \in \mathbb{Z}_p[\mathfrak{C}]$. This new quotient group, denoted

$$\mathfrak{J} = \mathfrak{D}^0 / \mathfrak{P}$$

is called the jacobian of the curve $\mathfrak{C}$ and is a finite abelian group. This will be the group used to build hyperelliptic cryptosystems.

0.4.3 Representation of Divisors

Athough the Jacobian $\mathfrak{J}$ of an hyperelliptic curve $\mathfrak{C}$ is a finite abelian group, elements of $\mathfrak{J}$ are very hard to represent.

Example 0.4.4.

0.5 Abelian Varieties