Abelian Variety Cryptosystems

Kevin Johnson 6017605

March 17, 2015

0.1 The Discrete Logarithm Problem

Given an arbitrary finite cyclic group $\mathfrak{G}$ with group operation $\cdot$ and generator $g \in \mathfrak{G}$, discrete exponentiation by a in $\mathfrak{G}$ is defined by

$$g^a = \overbrace{g \cdot g \cdots g}^{a \text{ times}}$$

If $y = g^a$ is known, computing a is called finding the discrete logarithm of y. With the method of fast exponentiation, y can be computed quickly, only $O(\log a)$ group operations. On the other hand, computing a can be much harder. In fact, in [2] it was shown that in an arbitrary group for which only the group operation and discrete exponentiation can be applied to group elements, computing discrete logarithms will take at least $O(\sqrt{|\mathfrak{G}|})$ operations. In most cases though, more structure is know about the group in use.

0.1.1 The Diffie-Hellman Key Exchange

This one-way property of discrete exponention has proven to be very useful for cryptographic purposes. The most notable of these is in the Diffie-Hellman Key Exchange Protocal in which two parties A and B wish to share a secret key k.

1. A and B share a publicly known group $\mathfrak{G}$ and generator $\mathfrak{g}$.

2. A chooses a random private exponent a and computes g^a.

3. B chooses a random private exponent a and computes g^b.

4. A sends g^a to B and B sends g^b to A.

5. A raises g^b to their private exponent a to obtain $k = (g^b)^a = g^{ab}$.

6. B raises g^a to their private exponent b to obtain $k = (g^a)^b = g^{ba}$.

The two parties may now use k to communicate with a cryptographically secure communication protocol. The described protocol relies on the hardness of computing g^{ab} given g^a and g^b, which was conjectured in [3] to be equivalent to computing discrete logarithms.

Another nice property about this protocol is it's applicable to any finite cyclic group. The simplist example of this is in the multiplicative units of the integers modulo a prime $\mathbb{Z}_p^*$. Let g be a primite root mod p, then every element of $y \in \mathbb{Z}_p^*$ can be written in the form $y = g^a$ for some $a < p - 1$. Thus $\mathbb{Z}_p^*$ is a finite cyclic group and one can compute discrete logarithms in $\mathbb{Z}_p^*$.

0.2 Algebraic Varieties, Dimension and Genus

When working with polynomials in more than one variable, it is sometimes simpler to use the formalism of classic algebraic geometry as found in [1]. From this point on, only the field $\mathbb{Z}_p$ where $p > 3$ will be considered.

0.3 Elliptic Curves

0.4 Hyperelliptic Curves

Unlike 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 0.4.1.

0.4.2 The Jacobian of a Hyperelliptic Curve

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.

Example 0.4.3.

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 and unstructured 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 $\sum_i m_i = 0$.

This subgroup is still infinite, but that can be remedied by defining 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 cyclic group. This will be the group used to build hyperelliptic cryptosystems.

0.4.4 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 0.4.5.

To make the group operation in $\mathfrak{J}$ tractable, we ustilize the mumford representation of a divisor which is described as follows. Let D be a semi-reduced with points $P_i = (x_i, y_i)$. We associate to D polynomials $a, b \in \mathbb{Z}_p[x]$ such that

$$a(x) = \prod_i (x - x_i)$$

$$b(x_i) = y_i \ 1 \le i \le r$$

where $\deg b < \deg a$ and $(x - x_i)^{k_i} \mid b - y_i$, if k_i is the multiplicity of P_i. Denote this representation $D \overset{\text{def}}{=} \text{div}(a, b)$.

0.4.6 The Group Law

The group operation can be divided into two parts - *Composition* and *reduction* as described in [4].

Composition

Given two divisors represented as $D_1 = \text{div}(a_1, b_1)$, $D_2 = \text{div}(a_2, b_2)$

1. compute $d_0 = \gcd(a_1, a_2)$ and find the unique $c_1, e_1 \in \mathbb{Z}_p[x]$ such that $d_0 = c_1 a_1 + e_1 a_2$

2. compute $d = \gcd(d_1, b_1 + b_2)$ and find the unique $c_2, e_2 \in \mathbb{Z}_p[x]$ such that $d = c_2 d_1 + e_2(b_1 + b_2)$

3. compute $a_3 = \frac{a_1, a_1}{d^2}$

4. compute $b_3 = \frac{c_2 c_2 a_1 + c_2 e_1 a_2 + e_2(b_1 b_2 + f)}{d} \bmod \frac{a_1, a_1}{d^2}$

5. compute $a_3' = \frac{f - b_3^2}{a_3}$ and $b_3' = -b_3 \bmod a_3'$

6. while $\deg(a_3') > g$, reassign $a_3 = a_3', b_3 = b_3'$ and repeat step 5

7. divide a_3' by its leading coefficient so that a_3' becomes monic

8. the output $div(a_3', b_3') = D_1 + D_2$

Why Does this work?

Example 0.4.7.

0.5 Abelian Varieties

0.6 Applications

0.7 References

1 Robin Hartshorne, *Algebraic Geometry, Graduate Texts in Mathematics, vol. 52*, Springer-Verlag, New York, 1977, ISBN 0-387-90244-9.

2 Victor Shoup, *Lower bounds for discrete logarithms and related problems*, Theory and Application of Cryptographic Techniques, 1997, pp. 256 - 266.

3 Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **IT-22** (1976), no. 644-654.

4 Tanja Lange, *Formulae for Arithmetic on Genus 2 Hyperelliptic Curves*, ... not complete.