

# Abelian Variety Cryptosystems

Kevin Johnson 6017605

March 10, 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 [3] 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 known about the group in use.

### 0.1.1 The Diffie-Hellman Key Exchange

This one-way property of discrete exponentiation has proven to be very useful for cryptographic purposes. The most notable of these is in the Diffie-Hellman Key Exchange Protocol 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  $g$ .
2.  $A$  chooses a random private exponent  $a$  and computes  $g^a$ .
3.  $B$  chooses a random private exponent  $b$  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 [2] to be equivalent to computing discrete logarithms.

Another nice property about this protocol is it's applicable to any finite cyclic group. The simplest example of this is in the multiplicative units of the integers modulo a prime  $\mathbb{Z}_p^*$ . Let  $g$  be a primitive 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, Genus and Dimension

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  $\mathbb{Z}_p$  will be considered.

## 0.3 Elliptic Curves

## 0.4 Hyperelliptic Curves

Unlike elliptic curves, when the genus  $g$  of a curve  $\mathcal{C}$  is greater than 1, the set of points on  $\mathcal{C}$  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  $\mathcal{C}$ . We call elements of  $\mathfrak{D}$  divisors of  $\mathcal{C}$ . Given a rational function  $f$  in  $\mathbb{Z}_p[\mathcal{C}]$ , 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

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

then  $\mathfrak{D}$  becomes an abelian group. Unfortunately, this group is far too large for cryptographic purposes. So we consider the subgroup  $\mathfrak{D}^0$  of all divisors of  $\mathfrak{D}$  whose 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  $\mathcal{C}$ . That is,  $D_1 - D_2 = (f)$  for  $f \in \mathbb{Z}_p[\mathcal{C}]$ . This new quotient group, denoted

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

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

### 0.4.3 Representation of Divisors

Although 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

## 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 Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **IT-22** (1976), no. 644-654.
- 3 Victor Shoup, *Lower bounds for discrete logarithms and related problems*, Theory and Application of Cryptographic Techniques, 1997, pp. 256 - 266.