Chapter 2

The secureness of the SQISIGN digital signature scheme involves the difficulty of finding isogenies between supersingular elliptic curves that are defined over finite fields.

Section 2.1 - Finite Fields

To define a field, we can build up from the essential element of algebraic structures, the notion of a set. A set is an unordered collection of distinct elements. If you add a binary operation on the elements and have the property of closure (applying the binary operation on two elements of the set results in an element of the same set) you end up with a magma. If the binary operation is associative (the order in which you evaluate the binary operations when there is a chain of the operation i.e. the placement of parentheses doesn’t matter) then you form a semigroup. If the set has an identity element (applying the binary operation to any element along with the identity yields that same original element), the result is a monoid. Adding the existence of an inverse for every element (applying the binary operation to any element and its inverse yields the identity) you form a group. Finally if you add commutativity (you can arrange the elements in any order when applying the binary operation to two elements) your result is an abelian group.

A field is a set enhanced with two binary operations (called addition and multiplication) such that considering the set with each of the two binary operations individually form an abelian group (but for multiplication we exclude the additive identity, known as 0, because it has no multiplicative inverse in the set). Also distributivity of multiplication across addition should hold () [KL 584]. An example of a field is the rational numbers ℚ equipped with the usual notions of addition, subtraction (addition with the inverse), multiplication, and division (multiplication with the inverse). A finite field (aka a Galois field) is a field with finite order (the number of elements or cardinality of the underlying set).

The finite fields considered in this paper are ones of prime order, , or the square of a single prime order, where p is congruent to 3 (mod 4). All finite fields are of prime power order. The characteristic of a field is the minimum positive number of times you must add the multiplicative identity element to get the additive identity. An illustrative example is the field (ℤp, +, ✕) where the operations are done modulo p. The characteristic of this field is p because adding 1 p times yields 0 (because it equals p which is congruent to 0 mod p). The characteristic of a field where q = pr is p.

A quadratic residue is the remainder when a perfect square is reduced modulo p. To test if an element of the field = (ℤp, +, ✕) is a perfect square, that is, there is an element b such that b2 is congruent to a mod p, then raising both sides of the congruence by yields mod p. By Fermat’s little theorem which states that where c and p are relatively prime means that . If this is not true, then wasn’t a perfect square to begin with. In the special case where , the positive square root is given by . A verifying example is if p = 7, then . Testing if a = 2 is a square and if so what the square root is follows. so 2 is a square mod 7. Indeed, . A natural ordering of ’s elements is considered.

If was analogous to the real integers, is analogous to the complex integers. The imaginary unit, , is the root of the equation . The multiplicative inverse of an element, denoted can be written with a “real” denominator by multiplying the numerator and denominator by the complex conjugate, . A lexicographical ordering of (based on the real parts and then based on imaginary parts if the real parts are equal) is defined.