Chapter 2

The secureness of the $\mathrm{SQI}_{\mathrm{SIGN}}$ 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 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) forms 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 the set paired with each of the two binary operations individually each 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 ($a(b + c) = ab + ac$). An example of a field is the rational numbers $\mathbb{Q}$ 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 is finite).

The finite fields considered in this paper are ones of prime order, F_p, or the square of a single prime order, F_{p^2} where $p \equiv 3 \ (mod\ 4)$. All finite fields are of prime power (a power of a single prime) 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 ($\mathbb{Z}_p$, +, $\cdot$) 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 F_q where $q = p^r$ is p.

A quadratic residue is the remainder when a perfect square is reduced modulo p (i.e. it is congruent to a square). To test if an element of the field F_p = ($\mathbb{Z}_p$, +, $\cdot$) is a perfect square, that is, there is an element b such that $b^2 \equiv a \ (mod\ p)$, then raising both sides of the congruence by $(p - 1)$ / 2 yields $b^{p-1} \equiv a^{(p-1)/2} \ (mod\ p)$. By Fermat's little theorem which states that $c^{p-1} \equiv 1\ mod\ p$ where c and p are relatively prime means that $a^{(p-1)/2} \equiv 1\ mod\ p$. If this is not true, then a wasn't a perfect square to begin with. In the special case where $p \equiv 3 \ (mod\ 4)$, the positive square root is given by $\sqrt{a} = a^{(p+1)\,/\,4}$. A verifying example is if p = 7, then

$\sqrt{a} = a^{(7+1)/4} = a^2$. Testing if $a = 2$ is a square and if so what the square root is follows. $2^{(7-1)/2} \equiv 8 \equiv 1\ (mod\ 7)$ so 2 is a square mod 7. $\sqrt{2} \equiv 2^{(7+1)/4} \equiv 4\ (mod\ 7)$. Indeed, $4^2 \equiv 16 \equiv 2\ (mod\ 7)$. A natural ordering of F_p's elements is considered (0, then 1, then … $p - 1$).

If F_p was analogous to the real integers, F_{p^2} is analogous to the complex integers. The imaginary unit, i , is the root of the equation $i^2 + 1 = 0$. The multiplicative inverse of an element, denoted $1/(a + bi)$ can be written with a "real" denominator by multiplying the numerator and denominator by the complex conjugate, $a - bi$. A lexicographical ordering of F_{p^2} (based on the real parts and then based on imaginary parts if the real parts are equal) is defined.

Section 2.2 - Elliptic Curves

The class of function we are interested in for SQI$_{\text{SIGN}}$ are called elliptic curves. In particular, we are interested in so-called Montgomery curves over the field F_q of the form: $By^2 = x^3 + Ax^2 + x$ where A and B are elements of the field that satisfy $B(A^2 - 4) \neq 0$. In addition, we include a "point at infinity", ∞. Two curves are isomorphic (there is a bijective mapping between them) if the mapping is of the form: $(x, y) \rightarrow (D(x + R), Cy)$ i.e. is linear since there is only shifting and scaling performed. Two elliptic curves are quadratic twists of one another if $C = \sqrt{B/B'}$ where B' is the leading coefficient on the y^2 term of the first curve.

If N, the number of solutions to the elliptic curve, is congruent to: $1\ mod\ char(F_q)$, then the elliptic curve is called supersingular. We are concerned with the field F_{p^2} where $p \equiv 3\ (mod\ 4)$ so for instance if $p = 7$, the curve is supersingular if it has 1, 8, 15, … many solutions. With B = 1, a supersingular curve has precisely $(p + 1)^2$ points. So for $p = 7$, there are 64 points (verifying this: $64 \equiv 1\ (mod\ 7)$ as expected).

Algorithm 1 (pg. 8) takes in an A value (take B = 1 here for now) and outputs an A' (which corresponds to a curve isomorphic to the curve corresponding to A) and the isomorphic mapping itself.

A very interesting fact is that we can define an addition operation that when paired with the set of points on the Montgomery curve form an abelian group! For an elliptic curve, if a line intersects it at two points, then it must intersect it at a third point given that tangent points are counted twice and the aforementioned "point at infinity" is the third point for vertical lines of intersection.

Addition can be defined as follows. The "point at infinity" serves as the additive identity so if P is a point on the curve, $P + \infty = \infty + P = P$. Now to add two general points on the curve, draw a line of intersection through the two points, P_1 and P_2. The third point of intersection, P_3, is defined as -($P_1 + P_2$). So the three points, P_1, P_2, -($P_1 + P_2$) add to "zero" which here is the additive identity, ∞. This summing to identity will always be true. Reflecting this point over the x-axis yields the additive inverse $(P_1 + P_2)$, the desired sum (this is because a vertical line through -$(P_1 + P_2)$ and $(P_1 + P_2)$ also intersect the point at infinity, ∞, and these three points should sum to “zero” as they do: -$(P_1 + P_2)$ + $(P_1 + P_2)$ + ∞ = ∞ again because the point at infinity is the additive identity). The addition rule is closed because it always results in a point on the curve. The addition rule is commutative because the order of points of intersection we add doesn’t matter. Associativity turns out to also be true. Because of these properties, the points on the Montgomery curve with the defined addition operation truly do form an abelian group.

Point doubling can be achieved by drawing the tangent line to the curve at the desired point to be doubled, finding the third point of intersection (since the tangent point counts as two points), and reflecting as before. Note that by this definition a vertical tangent yields $P = - P$ (because this occurs on the x-axis) and $P + - P + \infty = \infty$ (by the addition law) so $[2]P = \infty$ (because $[2]P + \infty = [2]P$ since ∞ is the identity point). General scalar multiplication can be achieved with repeated addition, that is, summing copies of the point: $[k]P = P + P + ... + P$ k times, using doubling and addition as defined above. The order of a point is the smallest positive integer m such that $[m]P = \infty$. The geometric definition of addition outlined here can be translated to a coordinate-based algebraic one using the formulas on (pg. 9).

We consider a subgroup of an elliptic curve E, defined over F_{p^2} and integer m, called the m-torsion subgroup denoted $E[m]$ that consists of the points in E that yield $[m]P = \infty$. This means it consists of all points each with the property that when you add m copies of the point using the line intersection and reflection method previously mentioned, you end up on a vertical line, that is, the sum is ∞. If m^2 divides the number of points on the curve, then $E[m]$ is isomorphic to $Z_m \times Z_m$ so it consists of m^2 points. There exists non-unique points R and S (that is, possibly multiple pairs exist) in $E[m]$ that generate the group $E[m]$. (R, S) is called a basis for $E[m]$. Algorithm 3 on pg. 10 essentially finds R and calls Algorithm 2 on pg. 10 which finds S and returns the basis (R, S).

Since we are working with repeated applications of an abelian group’s operator, we can naturally define a discrete logarithm problem. That is, given a point P and the point $[k]P$ (with scalar multiplication as defined above), extract the value of k, the number of times the addition operator was applied. You can imagine the difficulty of this because as defined above, the sum of two points on an elliptic curve seem to have little relation to what the initial points were (so repeatedly applying this is like bouncing around the elliptic curve). All you have is the initial point (P) and the final point $([k]P)$ and you need to find out how many times, k, the operator was applied. For points of large prime order (that is, they bounce around a lot before reaching the “steady state” of ∞ through a vertical line), the DLP is believed to be difficult for classical computers because you can basically only do an exhaustive search (try all possible k).

However for points of smooth order (that is, the order is a composite number with small prime factors), the problem is efficiently solvable. For a particular m-torsion subgroup where m is a power of 2 or 3 (therefore the points in this subgroup $E[m]$ are of smooth order) where a basis of this group (R, S) is known, any point on the elliptic curve in $E[m]$ can be represented as a “linear combination” of the basis points, that is, $P = [a]R + [b]S$. So such points are characterized by two integers, a and b, in a way similar to how vectors are described when the basis is implicitly understood. An algorithm based on the Pohlig-Hellman algorithm (which solves the DLP for a finite abelian group with a smooth number of elements) is used to find a and b.

This analysis of supersingular elliptic curves defined over finite fields gives the background required to understand isogenies between elliptic curves and eventually the correspondence between quaternion ideals and isogenies.

Bibliography

1. Jorge Chavez-Saab, Maria Corte-Real Santos, Luca DeFeo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. $\mathrm{SQI}_{\mathrm{SIGN}}$ (June 2023)
2. Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography* (3rd edition), (Chapman & Hall/CRC Cryptography and Network Security Series)(2020)
3. “Algebraic structure.” *Wikipedia*, https://en.wikipedia.org/wiki/Algebraic_structure
4. “Field.” *Wikipedia*, https://en.wikipedia.org/wiki/Field_(mathematics)
5. “Finite field.” *Wikipedia*, https://en.wikipedia.org/wiki/Finite_field
6. “Elliptic curve.” *Wikipedia*, https://en.wikipedia.org/wiki/Elliptic_curve