Post-Quantum Cryptography and Elliptic Curves

Jake Garcia and Kyle Stanfield

University of California, Santa Barbara

Introduction

From antiquity to the present, there has been a sustained interest in developing mathematically rigorous algorithms for the encryption of information. Without modern cryptography, it would be impossible to communicate securely over a computer network, and companies like Amazon could not do business. Furthermore, the capabilities of quantum computers continue to advance, and it is likely that these computers will be able to easily crack a certain subset of the most popular cryptographic techniques. We give an overview of one of the most widely used public-key cryptosystems, RSA, and explain how it will be made obsolete by quantum computers. Then we introduce elliptic curves, and explain how their algebraic structure allows us to use them as the basis for a much stronger cryptosystem.

Public-Key Cryptography

One of the central problems in cryptography is the distribution of keys to communicating parties. Let us consider the case of two people, Alice and Bob, communicating over an insecure channel.

Alice and Bob each have their own procedures for encryption and decryption: E_A, D_A, E_B, D_B, respectively. In a public key cryptosystem, each user reveals their encryption procedure, which is distinct from their (secret) decryption procedure. To send a message to Bob, Alice will encrypt her message with Bob's procedure to get $C = E_B(P)$. Alice can then securely send this ciphertext over the insecure channel, and Bob will recover the plaintext by applying his decryption algorithm, $P = D_B(C) = D_B(E_B(P))$.

We now examine one of the earliest and most widely used public key cryptosystems, RSA. To start, choose two distinct primes p and q. Let $n = p * q$, and compute $\phi(n) = (p-1)*(q-1)$. Note that the plaintext message P must be converted to an integer between 0 and $n-1$. Next, select a positive integer e, with $gcd(\phi(n), e) = 1$. Then we know there exists a unique positive integer $d \pmod{\phi(n)}$ such that $e*d \equiv 1 \pmod{\phi(n)}$. We can make use of Euclid's algorithm to efficiently calculate e and d. With that in mind, the RSA algorithm is:

$$Encryption : C = E(P) \equiv P^e \pmod{n}$$

$$Decryption : P = D(C) \equiv C^d \pmod{n}.$$

In 1994, Peter Shor invented an algorithm for quantum computers which is capable of factoring arbitrary integers, with runtime polynomial in $\log n$. Thus, with a quantum computer, and given encryption exponent e and n, one could easily solve for d by factoring n. Therefore RSA will be rendered obselete by quantum computers.

Projective Space and Elliptic Curves

We define an elliptic curve as a curve given by an equation of the form

$$y^2 = x^3 + Ax^2 + Bx + C,$$

where A, B, C are elements of a field F containing either the field of rational numbers, $\mathbb{Q}$, or a finite field $\mathbb{F}_p$ where p is a prime larger than 3.

We establish notation to help distinguish some of the known settings from the ones we wish to introduce. Let F be an arbitrary field. We define affine n-space over F,

$$\mathbb{A}^n(F) = F^n = \{(a_1, \ldots, a_n) : a_i \in F\},$$

as the set of ordered n-tuples of elements of F. We give a construction that embeds an affine space of a given dimension into a corresponding projective space, starting with a careful definition of the projective line. Consider the set S of all nonzero vectors in the affine plane, $\mathbb{A}^2(\mathbb{R})$. That is, $(a, b) \sim (a', b')$ if there is a nonzero real number t such that $(a, b) = t(a', b'.)$.

Projective Space and Elliptic Curves cont.

Let $[a, b]$ denote the equivalence class of the point (a, b), so that the set of equivalence classes on S is the set

$$\{[a, b] : a, b \in \mathbb{R}\} = \{[r, 1] | r \in \mathbb{R}\} \cup \{[1, 0]\}$$

since the x-axis is generated by $(a, 0)$ and $[a, 0] \sim [1, 0]$. We define the projective line to be this set of equivalence classes. The projective plane is the set of equivalence classes

$$\mathbb{P}^2(\mathbb{R}) = \{[a, b, 1] : (a, b) \in \mathbb{A}^2(\mathbb{R})\} \cup \{[a, b, 0] : (a, b, 0) \neq (0, 0, 0)\}.$$

In general,

$$\mathbb{P}^n(\mathbb{F}) = \{[a_1, \ldots, a_n, 1] : (a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbb{F})\} \cup \{[a_1, \ldots, a_n, 0] : (a_1, \ldots, a_n, 0) \neq (0, 0, \ldots, 0)\}.$$

Note that, on the projective plane, every vertical line intersects the line at infinity at the point $[0, 1, 0]$.

The Group Law

We define an operation $\oplus$ that can be paired with the set of points on an elliptic curve to define an abelian group. [4] Let E be some elliptic curve, $E = x^3 + ax + b$, in projective space and let P and Q be two points that lie on E. Note that considering the curve in projective space ensures that the set of points on E with coordinates in some field F, $E(F)$, is nonempty since it always contains the point at infinity: $[0, 1, 0]$. We begin by defining the operator $\cdot$ such that $P \cdot Q$ is the third point of intersection of the line connecting the points P and Q with E. If $P = Q$, we say $P \cdot P = P$. Now define the operation $\oplus$ by

$$P \oplus Q = \vec{0} \cdot (P \cdot Q),$$

where $\vec{0}$ is the point at infinity on the projective plane. That is, $P \oplus Q$ is the second intersection of the vertical line at $P \cdot Q$ with the curve, as seen in the following graph:

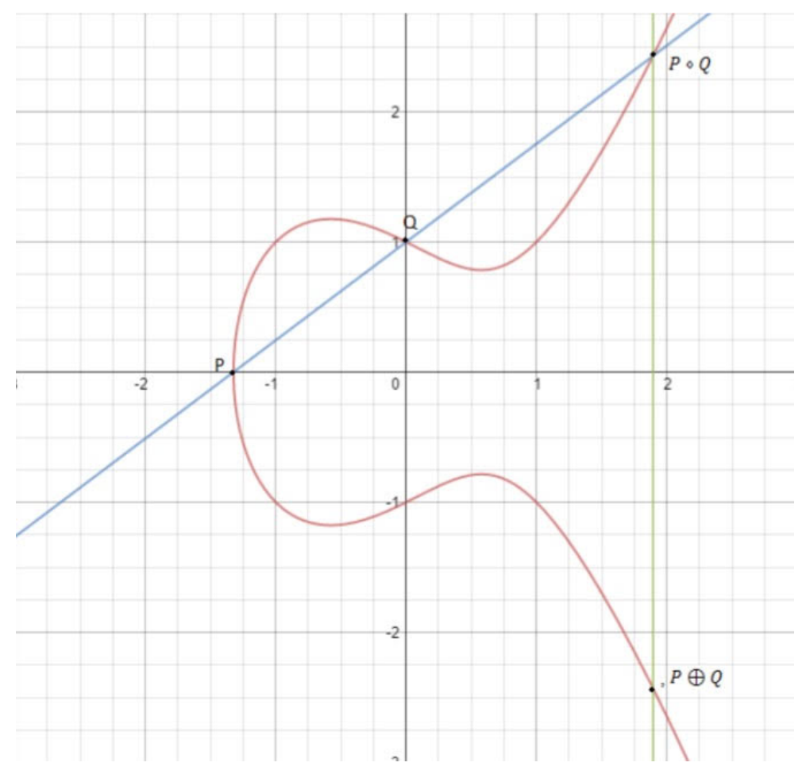

Fig. 1: The group law on elliptic curves.

In the case that when one of the points is $\vec{0}$, we define $P \oplus \vec{0} = P = \vec{0} \oplus P$. Next, if P and Q are opposite each other, we define $P \oplus Q = \vec{0}$. If $P = Q$, then we can't define the line between them. In this case, we use the tangent line to the curve at this point as our line. Finally, if P is a point of inflection (a point where the concavity of the curve changes), we take $P \oplus P$ to be the point opposite itself. The following rules give the points on an elliptic curve $E(F)$, along with the operation $\oplus$, the structure of a group: (1) The identity element is the point at infinity, $[0, 1, 0]$. (2) If $P = [x, y, 1]$ is an affine point on the elliptic curve, then we define its inverse to be $-P = [x, -y, 1]$. (3) Inverses are unique: For two affine points on an elliptic curve, $P_1 \oplus P_2 = \vec{0}$ if and only if $P_1 \oplus P_2$. That is, $P_1 \oplus P_2 = \vec{0}$ if and only if P_1 and P_2 lie on a vertical line. (4) If $P_2 \neq P_1$, then $P_1 \oplus P_2 = P_3 = [x_3, y_3, 1]$, where

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = -m(x_3 - x_1) - y_1,$$

and

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & x_1 = x_2 \end{cases}$$

Note that if the coordinates of the points P_1 and P_2 lie in F, then the coordinates of P_3 also lie in F since the formulas for x_3 and y_3 use only arithmetic operations.

Encryption Scheme

As in RSA, we assume our plaintext message has been converted to some integer equivalent m with $0 \leq m < M$. Let k be an integer such that the probability of failure to embed into a chosen elliptic curve is less than 2^{-k}. Choose some prime $p > M_k$. We can write every integer l between 1 and M_k uniquely as $l = mk + j$ with $1 \leq j \leq k$. Since $M_k < p$, we can think of the integers l (or more precisely, the residues congruent to $l \pmod{p}$) as distinct elements of the finite field $\mathbb{F}_p$. Our plaintext message m can be embedded as a point P_m on an elliptic curve $E(\mathbb{F}_p) = f(x) = x^3 + ax + b$ over $\mathbb{F}_p$ as follows. For each j, we test $x = x(j) = mk + j$ to see if $\overline{x}$ is the x-coordinate on of a point on $E(\mathbb{F}_p)$, where $\overline{x}$ denotes that passage of x to the field $\mathbb{F}_p$. We compute $\overline{f(x)}$ and ask if it is a quadratic residue (A square in $\mathbb{F}_2$). If it is a quadratic residue, take $\overline{y} \in \mathbb{F}_p$ such that $\overline{y}^2 = \overline{f(x)}$ to get our point $P_m = (\overline{x}, \overline{y})$. If $\overline{f(x)}$ is not a quadratic residue, we increment of value of j by one and test again. Since we have k choices for x, the probability that we will fail to produce a point on the curve is 2^{-k}. [2]

Now given a point $P_m = (\overline{x}, \overline{y})$, we consider $x = mk + j$. Notice that $x - 1$ satisfies

$$mk \leq x - 1 \leq mk + (k - 1),$$

giving

$$m \leq \frac{x-1}{k} \leq m + \frac{k-1}{k} < m + 1.$$

It follows that the plaintext message m is recoverable from the point P_m as $m = \lfloor \frac{x-1}{k} \rfloor$.

Thus, we have a means of embedding plaintext onto an elliptic curve, as well as a means to recover the plaintext from a given point on a curve.

In the original versions of Diffie-Hellman and ElGamal, we choose a prime p and use the group $U_p = \{a \pmod{p} : gcd(a, p) = 1\}$ (note that for a prime p, this group is equivalent to $\mathbb{Z}_p$) and an element g which is either a primitive root or simply generates a very large subgroup of U_p.

In the context of elliptic curves, given a prime p, we choose $a, b \in \mathbb{F}_p$ to define the elliptic curve $E : y^2 = x^3 + ax + b$. In this context, the set of points on E with coordinates in $\mathbb{F}_p$, $E(\mathbb{F}_p)$, replaces the group U_p. For elliptic curves, we have many options for our choice of an analogue of g. With encryption schemes based on elliptic curves, a great deal of information about the curve and the finite field are intended to be public. There are lists of recommended domain parameters, like [1], which provide choices for $E = E_{a,b}(\mathbb{F}_p)$ and a basepoint G in E together with the order of G and the cofactor $h = \frac{|E\mathbb{F}_p|}{|G|}$, so that $\frac{1}{h}$ is the proportion of $E(\mathbb{F}_p)$ generated by G. We can proceed supposing these data are given.

As in the classical case, we have two participants Alice and Bob who choose two integers a, b respectively with $1 < a, b < |G|$. Their shared key for any secret-key cryptosystem is computed by $abG = baG$. Alice publishes the field $\mathbb{F}_p$, the chosen curve E over $\mathbb{F}_p$, the basepoint G in $E(\mathbb{F}_2)$, and the multiple aG as her public key. This public key can be used in an ElGamal scheme as follows: Bob embeds a plaintext message m to a point P_m in $E(\mathbb{F}_p)$. He chooses a random integer k and sends the ordered pair $(kG, P_m \oplus k(aG))$ to Alice. Alice computes $a(kG)$ and computes $[P_m \oplus k(aG)] \oplus -akG = P_m$, then recovers the plaintext message m from P_m. [3]

References

[1] Daniel R. L. Brown. *Standards for efficient cryptography 2 (section 2)*. Jan. 2010.

[2] Neal Koblitz. "Elliptic Curve Cryptossystems". In: *Mathematics of Computation* 48 (Jan. 1987), pp. 203–209.

[3] Thomas R. Shermanke. *Modern Cryptography and Elliptic Curves: A Beginner's Guide*. Vol. 83. 2017.

[4] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. 1992.