To what extent can elliptic curves be used to establish a shared secret over an insecure channel?

Contents

Group Theory

$\mathbb{Z}_p^\times$: The Multiplicative Group Over a Prime

Fermat's Little Theorem suggests the following to be true for any integer a and prime p:

$$a^{p-1} \equiv 1 \pmod{p}$$

Extracting a factor of a, we get

$$a \cdot a^{p-2} \equiv 1 \pmod{p}$$

Thus, under multiplication modulo p, any integer a multiplied by a^{p-2} results in 1. As 1 is the multiplicative identity ($1 \cdot x = x$), a^{p-2} is said to be a's *multiplicative inverse*. Consider the numbers from 1 to $p - 1$. Every number has a multiplicative inverse modulo p, and 1 is the identity element as shown above. Further more, multiplication is associative ($a \cdot (b \cdot c) = (a \cdot b) \cdot c$) and each multiplication will always result in a number between 1 to $p - 1$ since it is performed modulo p. These properties (existence of an identity element and inverses, associativity and closure of operations) form a group.

We will refer to the group as $\mathbb{Z}_p^\times$. The *order* of a group refers to the number of elements in a group. For $\mathbb{Z}_p^\times$, the order is $p - 1$ since the elements are $1, 2, ..., p - 1$. Using notation, we write $|\mathbb{Z}_p^\times| = p - 1$.

The *order* of a specific element x, refers to the smallest integer k such that $x^k = 1$, where 1 is the identity element.[1] For example, the order of 17 in $\mathbb{Z}_{1009}^\times$ is 1008, because 1008 is the smallest integer such that $17^{1008} = 1$, whereas the order 2 in the same group is 504, since $2^{504} = 1$. Therefore, we have $|17| = 1008$ and $|2| = 504$.

The Discrete Log Problem

Under a specific group $\mathbb{Z}_{1009}^\times$, we ask for an integer n for which $17^n = 24$. In this case,

$$17^{456} \equiv 24 \pmod{1009}$$

Therefore $n = 456$ is the solution to this question. More generally, the discrete log problem asks for a smallest exponent n for a given group g and its elements a and b such that

$$a^n = b$$

Given this problem, one might take the brute-force or complete search approach, repeatedly performing the group multiplication, calculating a^2, a^3, a^4 and so on to find b. Assuming the exponent n is taken at random, this algorithm would take on average $\frac{1}{2}|a|$ operations. As the order $|a|$ gets big (towards numbers as big as 2^{200}), this approach quickly becomes infeasible.

The assumption that the discrete log cannot be solved trivially in specific groups is the core of cryptographic protocols and algorithms. There are known techniques better than a brute-force search which can solve the discrete log problem either for specific groups or for all groups in general. We shall discuss those methods in a later section, though cryptography is done on well-chosen groups such that even those attacks become infeasible.

[1] On a first glance, the definitions of order for a group and its elements seem to be unrelated. While in fact, the order of an element is also the order of a *subgroup* generated by that element. The meanings of "subgroup" and "generated" are outside the scope of this essay.

Finite Field Cryptography and Attacks

Diffie-Hellman Key Exchange

When two people communicate through the Internet, they must do so through their internet service providers (ISPs). In the case of a public network, there may be malicious people pretending to be the router, thus making it so that your internet traffic goes through them. This is called a man-in-the-middle attack.

If the information being communicated is encrypted, then man-in-the-middle attacks would not work. Common encryption algorithms require the people involved to have a **shared secret**, for example a string of characters that only the two parties know. This is hard to do when the only form of communication is through an **insecure channel**, as in the case of internet connections. The Diffie-Hellman Key Exchange proposes a way to establish a shared secret even if the only channel to communicate in is insecure through the difficulty of the discrete log problem.

The mechanism is as follows:

Given a known base g in a group G (with exponentiation meaning repeated application of the group operation), Alice can establish a shared secret with Bob by generating secret integers. Alice can secretly generate a and send Bob g^a, while Bob can secretly generate b and send Alice g^b.

Alice can then compute $\left(g^b\right)^a$ and Bob can compute $\left(g^a\right)^b$. As both of these are equivalent to multiplying g to itself ab times, $\left(g^b\right)^a = \left(g^a\right)^b = g^{ab}$ can be used as the shared secret.

Because only g, g^a, and g^b are sent across the channel, any third party observer will not be able to compute g^{ab} without solving the discrete log problem to determine a or b. As we have assumed that the discrete log problem is difficult, this is a secure way for Alice to establish a shared secret with Bob if the only form of communication between the two is insecure.

$\boxed{\text{Alice}}$ $\boxed{\text{Bob}}$

Index Calculus

As an attacker stalking the communication could obtain g, g^a, and g^b, obtaining the secret g^{ab} could be done by finding a from the discrete log, then finding $\left(g^b\right)^a$. Below we will describe one method for finding the discrete log in finite fields named Index Calculus

It is best to illustrate with an example. We'll reuse the one presented earlier:

$$17^n \equiv 24 \pmod{1009}$$

We first define a logarithm function L. $L(x)$ is defined such that

$$17^{L(x)} \equiv x \pmod{1009}$$

Note that when we have

$$17^{L(x)+L(y)} \equiv 17^{L(x)} \times 17^{L(y)} \equiv xy \equiv 17^{L(xy)} \pmod{1009}$$

So then

$$17^{L(x)+L(y)-L(xy)} = 1 \pmod{1009}$$

Elliptic Curve Cryptography

Let an elliptic curve be denoted by the equation $y^2 = x^3 + Ax + B$ where A and B are constants. Note that the curve is symmetric about the x-axis, since if (x, y) is a point on the curve, $(x, -y)$ is also on the curve.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be distinct points on the curve, where $x_1 \neq x_2$. We can find a new point on the curve by defining a line that goes across the two points, with slope

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

And line equation

$$y = m(x - x_1) + y_1$$

We substitute this into the equation of the curve:

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

Expanding and rearranging gives:

$$x^3 - m^2x^2 + (2m^2x_1 - 2y_1m + A)x + 2y_1mx_1 - m^2x_1^2 - y_1 = 0$$

With Vieta's formulas, the sum of roots for the cubic is m^2. We already know two roots of this polynomial as P_1 and P_2 are common points on the curve and the line, so we can find the x coordinate of the third point:

$$x_3 = m^2 - x_1 - x_2$$

In the group law, the y coordinate of the resulting point is flipped: (TODO: explain why)

$$y_3 = -(m(x_3 - x_1) + y_1) = m(x_1 - x_3) - y_1$$

Therefore, we have arrived at $P_3 = (x_3, y_3)$, a third point distinct from P_1 and P_2.

If only one point $P_1 = (x_1, y_1)$ is known, we can use implicit differentiation to find the tangent line:

$$y^2 = x^3 + Ax + B$$

$$2y\frac{\mathrm{d}y}{\mathrm{d}x} = 3x^2 + A$$

$$m = \frac{\mathrm{d}y}{\mathrm{d}x} = \frac{3x^2 + A}{2y} = \frac{3x_1^2 + A}{2y_1}$$

With the same line equation $y = m(x - x_1) + y_1$, with the same expanded formula:

$$x^3 - m^2x^2 + \dots = 0$$

But this time, x_1 is a repeated root, as a tangent line either touches no other points at all (the case when $y = 0$) or touch one other point.

Therefore, we can find the third point with

$$x_3 = m^2 - 2x_1$$

And

$$y_3 = -(m(x_3 - x_1) + y_1) = m(x_1 - x_3) - y_1$$

Therefore, we can begin to define a group law for points on elliptic curves.

Let $C : y^2 = x^3 + Ax + B$ be the elliptic curve with the set of points that satisfy the given equation. We now show that $C \cup \{\infty\}$ forms a group.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points that are on the curve. Define $P_3 = P_1 + P_2$ to be as follows:

- If $P_1 = P_2 = (x_1, y_1)$, let

$$P_3 = (m^2 - 2x_1, m(x_1 - x_3) - y_1), \text{where } m = \frac{3x_1^2 + A}{2y_1}$$

- If $x_1 = x_2$ but $y_1 \neq y_2$ (N.B. the only case where this happens is $y_1 = -y_2$): let $P_3 = \infty$.
- Otherwise, let

$$P_3 = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1), \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}$$

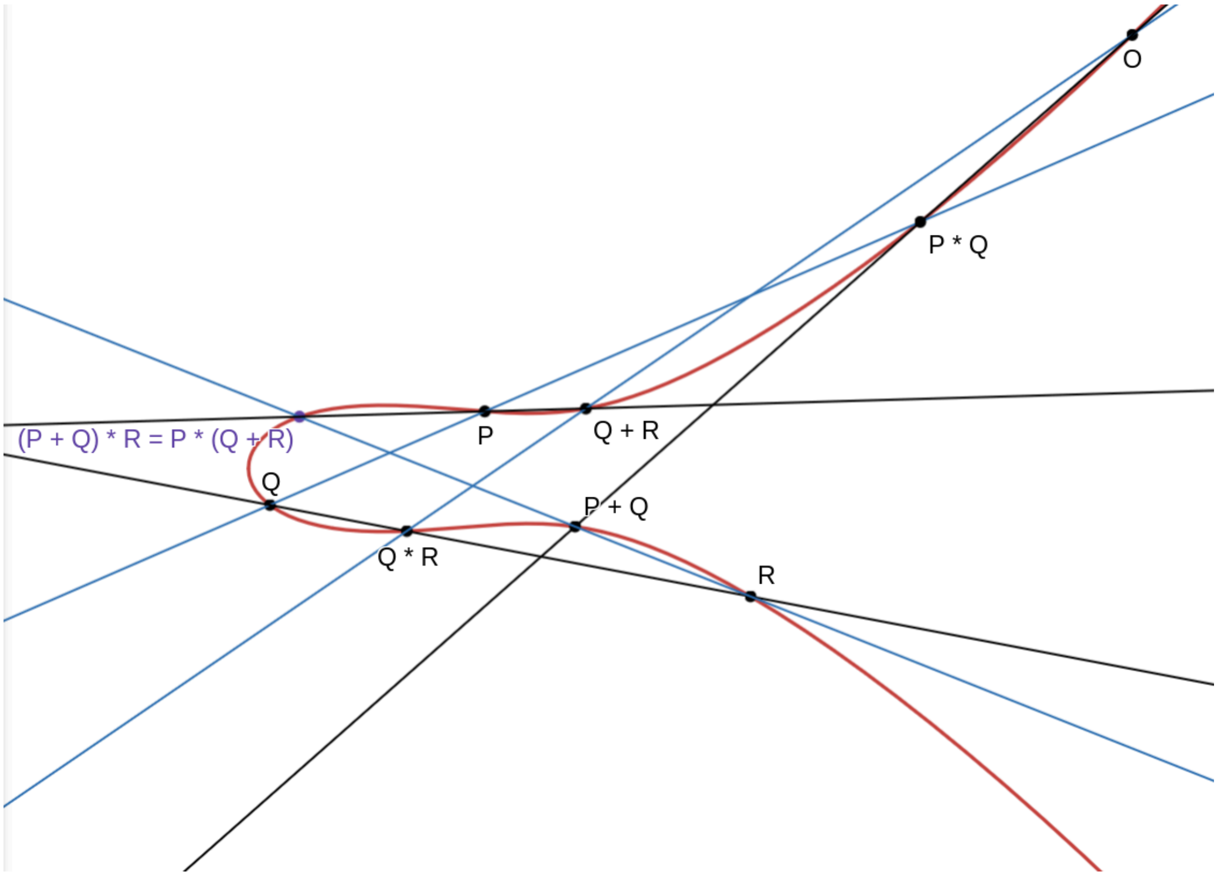
Additionally, define $P_1 + \infty = \infty + P_1 = P_1$, as well as $\infty + \infty = \infty$.

Perhaps the most surprising result of defining this operation is that the operation is associative, that is, $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for any three points P_1, P_2, P_3 that belong to the set $C \cup \{\infty\}$. Proving this algebraicly becomes very tedious, but there is a geometric argument using cubics and Bézout's theorem for the case where the points are distinct and none of them have the same x value.

Proof of Associativity

Bézout's theorem states that in general two plane curves given in the equations $a(x, y) = 0$ and $b(x, y) = 0$ with degrees d_a and d_b will have $d_a d_b$ intersections.

Formally, the group of elliptic curves can be defined in projective space where the point at infinity can be treated like any other point. For ease of presentation, the point at infinity will be denote as O.



Note that the intersections between the blue lines and the curve are $(P + Q) * R$, P, Q, R, $Q * R$, $Q + R$, $P * R$, $P + Q$, and O.

The intersections between the black lines and the elliptic curve are $P * (Q + R)$, P, Q, R, $Q * R$, $Q + R$, $P * R$, $P + Q$, and O.

As three lines form a cubic, and the two groups of three lines both intersect the same eight out of the nine points with the elliptic curve, it can be shown that the ninth point is the same for both cubics that intersect with the elliptic curve, thus proving that $(P + Q) * R = P * (Q + R)$.

Group of elliptic curve points

Therefore, $C \cup \{\infty\}$ forms a group since:

1. The operation $+$ is well-defined for any points $P_a + P_b$ where $P_a, P_b \in C \cup \{\infty\}$ as above.
2. ∞ is the identity element, where $P_a + \infty = P_a$ for all $P_a \in C \cup \{\infty\}$.
3. Every element has an inverse: let $P_a = (x, y)$, its inverse is $-P_a = (x, -y)$. We know that $-P_a \in C$ since the curve is given as $y^2 = x^3 + Ax + B$ and swapping y with $-y$ will still hold.
4. The operation is associative.

Since elliptic curve points form a group, cryptographic techniques such as diffie-hellman key exchange which relies on group operations can also be applied to elliptic curves.

Elliptic curve diffie-hellman

One important difference between elliptic curve operations and modular multiplicative group operations is in notation. In elliptic curve, the operation is commonly represented as addition of two points. Therefore $A + B$ is the normal operation on two points A and B while kA is the operation repeated (e.g. $2A = A + A$). In the multiplicative group modulo p, the correspondence goes to AB and A^k. Thus, in previous sections about the multiplicative groups, an operation such as A^k will now be written as kA in the context of elliptic curves.

With that note, diffie-hellman in elliptic curves follows the exact same procedure: two parties agree on a curve group to use, then decide on a base point G. Alice generates a secret integer a and sends Bob aG. Bob generates a secret integer b and sends Alice bG. They can now both calculate abG, which cannot be known by third parties unless they can solve the discrete log problem in elliptic curves.

Finding the Discrete Log with Pollard's ρ algorithm

Pollard's ρ algorithm is a general algorithm for solving the discrete log problem for any abelian group. It is less efficient than the general number field sieve on discrete log in finite fields, taking $\sqrt{N}$ on average with N being the order of the group.

We first take an example adapted from page 164 of Silverman and Tate's book: $y^2 = x^3 + 6692x + 9667$, in F_{10037}, with $P = (3354, 7358)$, $Q = (5403, 5437)$. Find k such that $kP = Q$.

Generate 10 random points on the curve based on multiples of P and Q:

$$\begin{aligned}
M_0 &= 42P + 37Q \\
M_1 &= 21P + 12Q \\
M_2 &= 25P + 20Q \\
M_3 &= 39P + 15Q \\
M_4 &= 23P + 29Q \\
M_5 &= 45P + 25Q \\
M_6 &= 14P + 37Q \\
M_7 &= 30P + 12Q \\
M_8 &= 45P + 49Q \\
M_9 &= 40P + 45Q
\end{aligned}$$

Then pick, in the same way, a random initial point:

$$A_0 = 15P + 36Q = (7895, 3157)$$

Then, choose an M_i point to add to based on the ones digit of the x coordinate of the point. As A_0 has $x = 7895$, $A_1 = A_0 + M_5 = (7895, 3157) + (5361, 3335) = (6201, 273)$.

Formally, define

$$A_{n+1} = A_n + M_i \text{ where } i \equiv x_n \pmod{10}$$

for $A_n = (x_n, y_n)$. The choice of random M_i points creates a kind of "random walk" of the points in the elliptic curve. As we keep calculating, we get:

$$\begin{aligned}
A_0 &= (7895, 3157), A_1 &&= (6201, 273), ..., \\
A_{95} &= (170, 7172), A_{96} &&= (7004, 514), ..., \\
A_{100} &= (170, 7172), A_{101} &&= (7004, 514)
\end{aligned}$$

We reach a cycle with $A_{95} = A_{100}$. Since we know the multiples of P and Q for all of the M_i points and thus all A_n points, keeping track of them gives us $A_{95} = 3126P + 2682Q$, we also have $A_{100} = 3298P + 2817Q$. With $3126P + 2682Q = 3298P + 2817Q$, we have:

$$\infty = 172P + 135Q = (172 + 135n)P$$
$$172 + 135n \equiv 0 \pmod{10151} \; n \equiv 1277 \pmod{10151}$$

With verification, we indeed have $1277P = Q$.

Evaluation

Pollard's ρ algorithm works on average with $\sqrt{\frac{\pi}{4} N}$ elliptic curve additions with N being the order for the base point P. [1]

Bibliography

[1] D. J. Bernstein, T. Lange, and P. Schwabe, "On the Correct Use of the Negation Map in the Pollard rho Method," in *Public Key Cryptography – PKC 2011*, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds., Berlin, Heidelberg: Springer, 2011, pp. 128–146. doi: 10.1007/978-3-642-19379-8_8.