How can elliptic curves be used to establish a shared secret over an insecure channel?

Introduction

Internet connections and data go through Internet Service Providers (ISP) which snoop on users' information. [citation needed] An often used method to prevent eavesdropping is through TLS, commonly known as the green padlock next to the address bar or HTTPS, [citation needed] which establishes a secure connection between the user and the website that they are connecting to, such that the ISP only knows which website they have connected to but does not know the content that the user has downloaded or uploaded.

TLS has many different cryptographic techniques to establishing a secure connection. One of which is the Elliptic Curve Diffie-Hellman (ECDH). In this paper, we will examine the mathematical theory underlying the ECDH operation and evaluate its practical application in cybersecurity.

The Discrete Log Problem in $\mathbb{Z}_p^\times$

As a consequence of Fermat's Little Theorem, we can write:

$$a^{p-1} \equiv 1 (\operatorname{mod} p)$$
$$a \cdot a^{p-2} \equiv 1 (\operatorname{mod} p)$$

For any integer a and prime p. We have found a^{p-2} as a's multiplicative inverse, therefore integers modulo p with multiplication forms a group, as the operation is associative, has an identity element, and every element has an inverse.

Elliptic curves

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 substitude this into the equation of the curve:

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

Expanding and rearranging gives:

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

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: why?)

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