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:

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

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.