Elliptic Curve Public Key Cryptography Algorithm

Liangyu

Alice and Bobby both agree on an Elliptic Curve E_p and a generator G of E_p. Alice chooses a random number $a \in (1, p-1)$ and compute $A = a * G$. a is Alice's private key, and A is Alice's public key.

Bobby chooses a random number $b \in (1, p-1)$ and compute $B = b * G$. b is Bobby's private key, and B is Bobby's public key.

To send an encrypted message M to Bobby, Alice uses an invertible encoding function f to encode plaintext message M onto a point P_M of E_p.

Alice chooses another random $k \in (1, p-1)$ and compute the shared secret $S = k * B$, then compute the ciphertext $P_c = (k * G, P_M + S)$. Here k is Alice's ephemeral key.

Upon receiving the ciphertext, Bobby computes the shared secret $S = b * k * G$, then decrypt the message by compute $(P_M + S) - S = P_M$, then $f^{-1}(P_M) = M$.