Stealth Address

Sammy

2017-09-22

1 Definitions

Stealth addressing is a technique whereby a **sender** can take a **recipient**'s public address and transform it to a one-time address such that:

- For anyone other than the recipient, the address is
  - **publicly unlinkable** to the original public address;
  - **publicly unlinkable** to **any** other one-time address;
- The recipient can
  - link all their payments together
  - derive the secret key associated with the one-time address

Using stealth addressing, a recipient can publish one address and receive unlimited publicly unlinkable payments.

2 Requisites – ECDH

Elliptic Curve Diffie-Hellman is a variant of the original Diffie-Hellman key agreement protocol extended for use with ECC. In simple terms, two parties can independently generate a shared secret over an unsecured connection (implying that no observer can discover the secret by simply watching their communication).

Suppose the two parties to share secret keys are Alice and Bob, and their (sk, pk) pair are $(a, A = a \cdot G)$ and $(b, B = b \cdot G)$ respectively, where G is a base point of the EC employed.

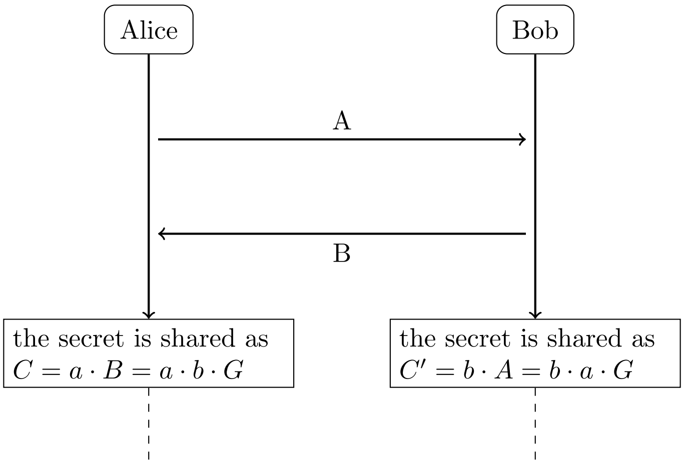
Alice
Bob
A
B
the secret is shared as $C = a \cdot B = a \cdot b \cdot G$
the secret is shared as $C' = b \cdot A = b \cdot a \cdot G$

Figure 1: Workflow of ECDH

And the final shared secret key is $C = C'$.