Stealth Address

Sammy

2017-09-22

1 Foreword

This article is motivated by the blog [lui16].

2 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.

3 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. Then to share a secret key, they can interact with each other as Figure 1.

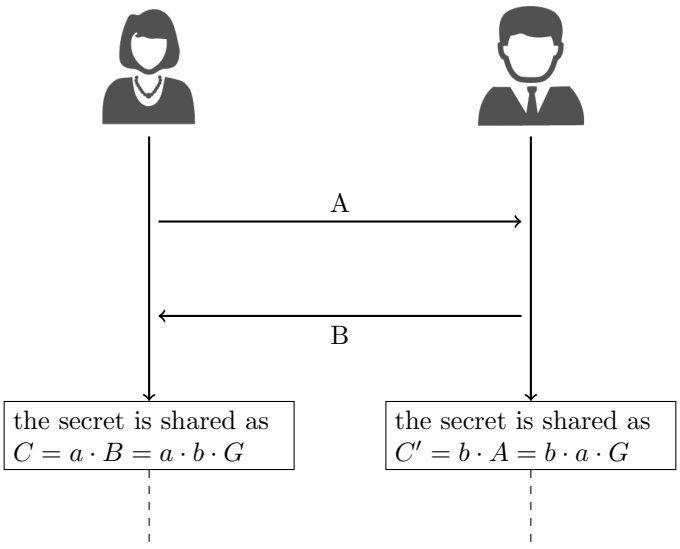

Figure 1: Workflow of ECDH

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

4 Concrete Algorithm

Suppose Alice wants to pay Bob, then the stealth address for Bob (assuming view key pair as (a, A) and spend key pair as (b, B)) to receive to the payment can be depicted as Figure 2.

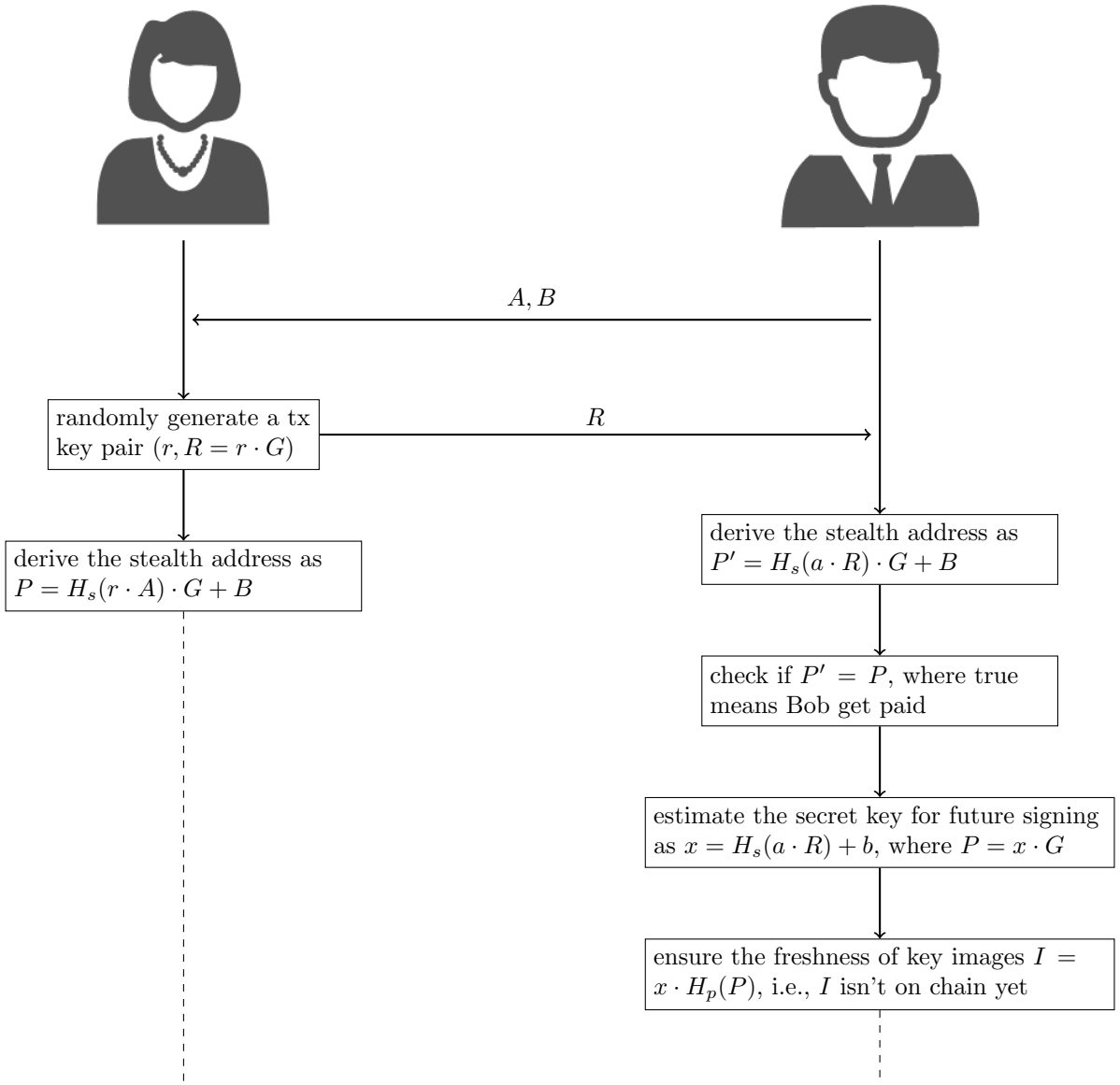

Figure 2: Derivation of Stealth Address

5 Some notes

- Computing $r \cdot A$ and $a \cdot R$ requires secret data: either r (Alice) or a (Bob). Thus, external observers are prevented from proceeding past calculating $(r \cdot A)$. Furthermore, because r is randomly chosen, even if the observer suspects Alice is sending to Bob's public address (which the observer knows), due to the ECDLP they still can't link this address to P without knowledge of r or a (or pedantically the later steps' values, namely $r \cdot G$ and $H_s(r \cdot G)$).
- Back to the **dual-key** concept ((a, A) and (b, B)), Bob (or someone working on his behalf with knowledge of a and B) can "scan" for and detect/link outputs without knowledge of b, which is required below to actually spend that output. The whitepaper calls (a, B) the **"tracking key"**.
- It is possible to do a non-dual-key stealth addressing scheme, but you must make one of two trade-offs. You can either:
  - use the concept in the whitepaper called a **truncated address**, which means the view key pair is publicly known and all incoming transactions can be linked ($a = H_s(B)$); or
  - forego a view key pair entirely, which means scanning requires spending ability ($P = H_s(rB) \cdot G + B$).

References

[lui16] luigi111. *Understanding Monero Cryptography, Privacy Part 2 – Stealth Addresses*. 2016. URL: https://steemit.com/monero/@luigi1111/understanding-monero-cryptography-privacy-part-2-stealth-addresses.